

AAA und Radius

AAA

Was ist AAA?

AAA ist ein System, welches vor unberechtigten Zugriff auf Netzwerke und Netzwerkdienste schützt. Dadurch kann kontrolliert werden, wer eine Verbindung zum Netzwerk herstellen kann, und auf welche Dienste diese Benutzer zugreifen dürfen. Außerdem kann ein Prüfprotokoll der Benutzeraktivitäten erstellt werden.

Die Abkürzung AAA, auch **Triple-A-System** genannt, steht für **Authentication**, **Authorization** und **Accounting**. Bei dem Triple-A-System handelt es sich also um ein System für Zugangskontroll-, Zugangssteuerungs- und Zugangsabrechnungsmethode, welches in Netzwerkgeräten verwendet wird. [1]

Aufgaben des AAA

- **Authentication:** Ist man berechtigt zuzugreifen?
- **Authorization:** Ist man berechtigt dieses Kommando auszuführen?
- **Accounting:** In welchen Umfang wurde der Dienst benutzt?

AAA-Server

Ist ein Serverprogramm, welches die Anwenderanfragen mit Hilfe der AAA-Prozesse verwaltet. Dazu verwendet er externe Datenbanken und Verzeichnisse, welche er von Netzwerkzugriffs- und Gateway-Servern erhält. Die Kommunikation zwischen einem Gerät und einem AAA-Client findet häufig mittel **RADIUS** statt. [2]

Funktionsweise des AAA

Authentication-Prozess:

User senden eine Login-Request zum Client, welcher sich am Server erkundet, ob der Login erlaubt ist. Bei positiver Rückmeldung findet ein Passwortvergleich statt und man wird eingeloggt.

Accounting-Prozess:

Der Accounting-Prozess protokolliert jede Interaktion zwischen Client und User, sowohl als auch den Login.

Authorization-Prozess:

Der Authorization-Prozess sieht bei jeder Interaktion zwischen Client und User nach, ob der User berechtigt ist diese auszuführen.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, dass die Authentifizierungen von Gerätezugriffen innerhalb eines Netzwerkes verwaltet. Es ist für alle drei A's des Tripple-A-Systems zuständig, und wird in Form eines RADIUS -Servers, an denen sich diverse IT-Dienste zur Authentifizierung wenden können, eingesetzt. [3]

Nachdem sich in einem Netzwerk, in dem die Authentifizierung über das RADIUS-Protokoll gehandhabt wird, ein neues Gerät mit diesem Authentifizieren will, leitet der Access-Point die Authentifizierungs-Anfrage an den RADIUS-Server weiter. Je nach Erfolg lässt der Access-Point im Anschluss die neue Verbindung zu oder lehnt sie ab. Dies wird öfter als WPA-Enterprise bezeichnet. [4]

Für die Übertragung der Authentifizierungs-Daten wie Username und Password wir meist das EAP (Extensible Authentication Protocol) verwendet. [3]

Radius Server müssen als Software auf einem Server aufgesetzt werden, manche Router bieten allerdings bereits simple Implementationen selbst. [6]

Geschichte zu RADIUS

RADIUS wurde erstmals in RFC 2058 und RFC 2059, dies sind technische und organisatorische Dokumente zum Internet, beschrieben. Der Standard IEEE 802.1X regelte später die Authentifizierung von Rechnernetzen einheitlich. [5]

Heutzutage gibt es verschiedene Implementationen, darunter gehören diverse freie als auch proprietäre. [3]

Einsatzgebiete vom RADIUS

RADIUS wird meist in größeren Netzwerken eingesetzt, um die Zugriffsberechtigungen dieser Netzwerke zu verwalten. Somit können also nur berechtigte Nutzer, oder bei Bedarf auch nur berechtigte Endgeräte, auf das Netzwerk zugreifen. [3]

Vorteile vom RADIUS-Protokoll [7]

- + Da kein einfacher Preshared-Key vorhanden ist, der möglicherweise beliebig weitergegeben wurden, ist das System um ein Vielfaches sicherer
- + Trotz einer verteilten Netzwerkinfrastruktur werden die Zugangsdaten der Nutzer zentral gespeichert
- + Benutzerfreundlich

Nachteile vom RADIUS-Protokoll [7]

- Eine Störung des RADIUS-Servers wirkt sich auf das gesamte Netzwerk aus
- Ein RADIUS-Server muss bereitgestellt und konfiguriert werden
- Damit verbundene Kosten und Aufwand

Verwendete Quellen:

https://blog.adacor.com/was-ist-triple-a-system_986.html [1]

[https://www.computerweekly.com/de/definition/AAA-Server-Authentifizierung-Autorisierung-und-Accounting#:~:text=AAA%2DServer%20\(Authentifizierung%2C%20Autorisierung%20und%20Accounting\)&text=Ein%20AAA%2DServer%20ist%20ein,sind%20Authentifizierung%2C%20Autorisierung%20und%20Accounting](https://www.computerweekly.com/de/definition/AAA-Server-Authentifizierung-Autorisierung-und-Accounting#:~:text=AAA%2DServer%20(Authentifizierung%2C%20Autorisierung%20und%20Accounting)&text=Ein%20AAA%2DServer%20ist%20ein,sind%20Authentifizierung%2C%20Autorisierung%20und%20Accounting) [2]

<https://www.univention.de/blog-de/2016/09/kurz-erklaert-radius/> [3]

<https://de.wikipedia.org/wiki/WPA2> [4]

https://de.wikipedia.org/wiki/IEEE_802.1X [5]

<https://www.heise.de/ct/artikel/WLAN-sichern-mit-Radius-1075339.html> [6]

<https://www.security-insider.de/wie-funktioniert-radius-a-613266/> [7]