IOP Conference Series: Materials Science and Engineering

PAPER • **OPEN ACCESS**

Design and Implementation Network Administrators Account Management System Based on Authentication, Authorization, and Accounting Based on TACACS and LDAP

To cite this article: Ardelia Puri Paramitha *et al* 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **803** 012040

View the article online for updates and enhancements.

This content was downloaded from IP address 182.255.0.244 on 22/01/2021 at 01:59

IOP Conf. Series: Materials Science and Engineering **803** (2020) 012040 doi:10.1088/1757-899X/803/1/012040

Design and Implementation Network Administrators Account Management System Based on Authentication, Authorization, and Accounting Based on TACACS and LDAP

Ardelia Puri Paramitha, Adian F. Rochim, Adnan Fauzi

Departement of Computer Engineering, Faculty of Engineering
Diponegoro University, Tembalang, Semarang, 50275, Indonesia

Email: apparamitha@student.ce.undip.ac.id, adian@ce.undip.ac.id, adnan@live.undip.ac.id

Abstract. Authentication is required for to authenticate user administrators for accessing network devices. In large-scale network devices management, firstly administrators need centralized user management to modify their account for logging network devices. Secondly, they must have log monitoring data who modified their account. The goal of this research is to develop and implement Authorization, Authentication, Accounting (AAA) system and making Log Monitoring System (LMS). Objectives of this research are implementing a system that can centralize and manage network administrators account. Design and topology of the network use simple star network. Software design uses Rapid Application Development (RAD) method. Research began with analyzing the research problem, next step is creating a system design, then build the system. After the system has been built, a demo is done whether the system is running well. If the system has not functioning as desired yet, refine the system. If already functioning as desired, a testing is done. If there are no obstacles during testing, the system is ready to be implemented by users who will use the system. The result shown that system is able to centralized authentication and authorization using Terminal Access Controller Access-Control System (TACACS), and processing accounting data into information in graphical form using ELK Stack. The result of the research is developing monitor user login and log review. The test result shown that system can manage network administrators account according to the Authentication, Authorization, Accounting (AAA) principle.

Keyword: Authentication; Authorization; Accounting; TACACS

1. Introduction

Information technology advancement nowadays is very rapid along with the increasingly high information needs. Many technologies produced both hardware and software that can simplify human work. The use of information technology cannot be separated from computer for data management. Computers cannot be separated from the role of computer networks [1].

In managing computer networks, there is the role of the network administrators who are responsible for designing and configuring network devices. Authentication is needed to validate the administrators account to access network devices. In large-scale network devices management, administrators will find it difficult to do repeated authentication with different account. Judging from the approach, a solution is

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

needed to manage network devices only with one account. Single Sign On (SSO) which can simplify the number of accounts and support the AAA protocol (Authentication, Authorization, Accounting) [2].

The family of AAA protocols, which stands for Authentication, Authorization and Accounting, were originally designed as remote access control mechanisms and network service providers through modem and dial-in services, but they continue to be presently implemented in multiple architectures [3].

Terminal Access Controller Access-Control System as known as TACACS is a remote authentication protocol that separates out the authorization functionality, so it enables additional flexibility and granular access controls on who can run which commands on specified devices [4]. These protocols works on client server logic and uses messages/ packets to be exchanged between them to enable AAA service [5].

A. Riyanto et al., in 2014, describe the implementation of SSO using LDAP for information system and hotspot access at Universitas Muhammadiyah Surakarta Campus [6]. The implementation used for hotspot access authentication. The results of their research are to ease students to access information system using one account only. SSO also make it easy for admin to manage user data who is accessing the system. With using LDAP, every data will be centralized in LDAP server.

Sikawar et al., in 2017, describe the study of AAA model with special references to TACACS+ and RADIUS [7]. This research aims to describe the AAA system comparison between TACACS+ and Radius. The result of their research are both the protocols help to deploy the AAA model of security. For deploying the secure and effective security, the TACACS+ is much effective then the RADIUS protocol. Both the protocols are effective and acceptable for different applications and their utilities.

Through this research, the author intends to implement network administrators account management system based on TACACS to centralize network devices authentication in order to facilitate network administrators to manage network devices.

First section describes the background of the research. Second section describe the research methodology. Next section describes the result of research. And finally, the last section explains the conclusions of the research.

2. Research Methodology

Rapid Application Development (RAD) methodology, are used to design the implementation of the system. RAD methodology process consists of analysis and quick design, build, demonstrate, and refine system, testing, and implementation [8].

The first step is analyzing system needs and system design. This step analyzes the user needs and system that will be built. The next step known as prototype cycles. The beginning of the cycle is building the system by determining the specification of the requirements that match the system definition. Furthermore, refines are made to the system in accordance with the design. The third step is system testing. Testing is done by testing the results of authentication and authorization in the accounting. The final step is implementation. If there is no obstacle in the testing phase, the system is ready to be implemented.

2.1. Functional Requirements

Functional requirements of the network administrators account management system are the system can authenticate users account that access network devices. The system can authorize users account to grant access rights according to the privilege level based on the group. The last functional requirement is the system can visualize system logs and users account management into dashboard that is easy to use by network administrators.

2.2. Hardware Requirements

Hardware is used as a system support so the system can run. The system is implemented in a computer. The computer used has the specifications in Table 1.

One Cisco Catalyst WS-C2960-24LC-S switch and 3 Cisco 1841 routers as sample network devices that were tested in the research. One Asus A442U laptop to create the application.

Table 1. Computer Specification

Component	Server
Processor	Intel® Core™ i3-5005U CPU @ 2.00GHz
RAM	8 GB
HDD	1 TB
NIC	1 Fast Ethernet

2.3. Software Requirements

The network administrators account management system requires software to build servers and other supporting components. Network administrators account management server use Windows Server 2019 as the operating system. The application for user account management uses Active Directory. Centralized authentication and authorize accounts using TACACS. Accounting visualization using Kibana with data that collected by Logstash and saved in Elasticsearch [9].

Network devices configuration is done remotely using MobaXterm application. Google Chrome application as a web browser that runs on the Windows 10 x64 operating system and used to test the running of the application.

2.4. Topology Design

The topology design of the network administrators account management system consists of various entities involved in system development. The entity is connected using a star topology with a switch as the center [10]. Figure 1 shows the physical topology of the log management system.

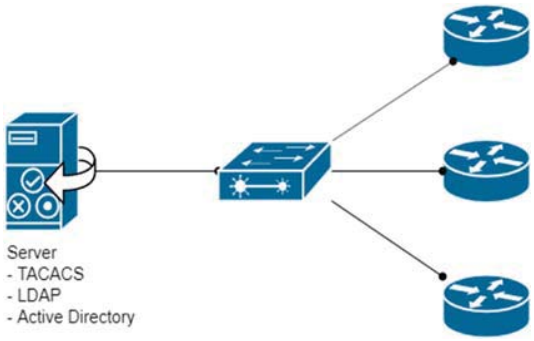

Figure 1. Design and Network Topology System

The server where the system is located will be connected to other network devices and connected to the switch. All devices connected to the server will be authenticated on the TACACS server.

2.5. System Design

System design provides an overview or part of a system. Figure 2 shows the server system design.

2.6. Work Process Design

The design is done on the TACACS configuration including Authentication, Authorization, Clients, and Tacplus. Authentication contains account details that are used to access network devices stored in LDAP. The account will be stored in the Users container and is a member of the group according to the access rights. Authorization contains the distribution of privilege level and commands that can be accessed in each group. Clients contain the IP address of the devices that connected to the server. Tacplus contains the configuration of the server including the IP address and the port used, also contains settings from the TACACS logs.

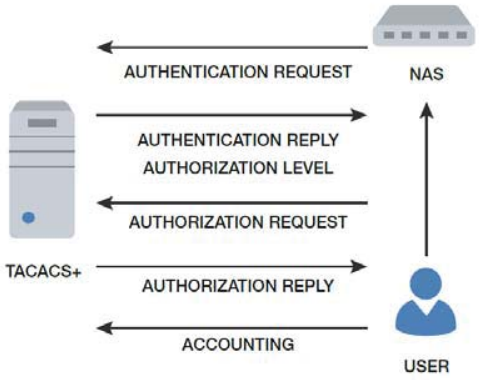

Figure 2. Server System Design [4]

2.7. AAA System Flow Process

The flow chart diagram explains the process of authentication and authorization. Information from both processes will be stored in the accounting files and the information is used to monitor the account who is logging in to the network devices. The work process of the system is shown in Figure 3.

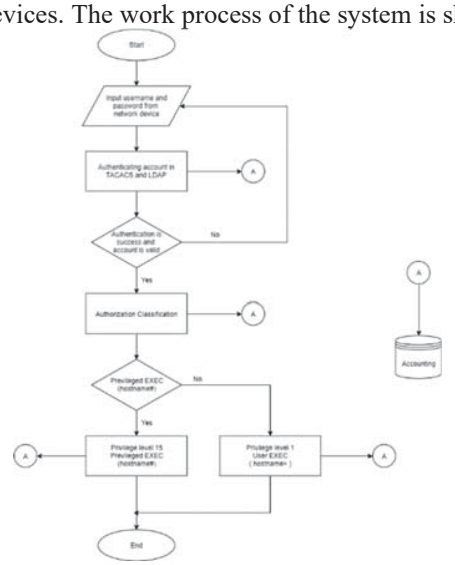

Figure 3. AAA System Flowchart

3. Result and Discussion

System evaluation is done to check the performance of the system being implemented. The main purpose of system evaluation is to ensure that the components of the system are functioning as needed.

3.1. Authentication Evaluation

Based on functional requirements, the network administrators account management must be able to authenticate user account who is accessing network devices. The intended authentication is verifying username and password which is entered by the user when accessing network devices based on Active Directory database.

Testing is done by logging in to network devices using user admin and operator. The data log results example from authentication testing user admin on router 1 shown below.

Table 2. admin1 Authentication Result

No	Code	Information
1	<87>	ID
2	9/23/2019	Access date
3	11:39:34	Access time
4	[10.42.12.185:14224]	IP destination and port used
5	Authentication for user admin1 passed against group admin_tacacs – Passed	Information of authentication result for admin1 against group admin_tacacs is success.

The data log results example from authentication testing user operator on router 1 shown below.

Table 3. op1 Authentication Result

No	Code	Information
1	<87>	ID
2	9/23/2019	Access date
3	11:43:37	Access time
4	[10.42.12.185:36929]	IP destination and port used
5	Authentication for user op1 passed against group op_tacacs - Passed	Information of authentication result for op1 against group op_tacacs is success

Based on authentication data log results above, shown that authentication process is success.

3.2. Authorization Evaluation

Based on the functional requirements of the network administrator account management system is providing authorization to user in accordance with privilege level. In authorization, user who are members of security group admin_tacacs get access rights as administrator which have privilege level 15. Privilege level 15 is the highest privilege to run all commands on network devices. For user who are members of security group op_tacacs get access rights as operator which only have privilege level 1. Privilege level 1 is the lowest privilege and only can run limited commands.

Testing is done by accessing the network devices using user admin and operator. The data log results example from authorization testing user admin on router 1 shown below.

Table 4. admin1 Authorization Result

No	Code	Information
1	<87>	ID
2	9/23/2019	Access date
3	11:39:34	Access time
4	[10.42.12.185:14328]	IP destination and port used
5	User admin1 belong to group admin_tacacs - from cache	User admin1 is member of group admin_tacacs.
6	priv-lvl=15	Have privilege level 15

The data log results example from authorization testing user operator on router 1 shown below.

Table 5. op1 Authorization Result

No	Code	Information
1	<87>	ID
2	9/23/2019	Access date
3	11:39:34	Access time
4	[10.42.12.185:14328]	IP destination and port used
5	User op1 belong to group op_tacacs - from cache	User op1 is member of group op_tacacs.
6	priv-lvl=1	Have privilege level 1

Based on authorization data log results above, shown that authentication process is success.

3.3. Accounting Evaluation

The functional requirements of the network administrator account management system are visualizing TACACS log. The log is stored in TACACS Accounting files. The accounting files content are shown below.

Table 6. Accounting Files Content

No	Code	Information
1	<102>	ID
2	2019-09-23	Access date
3	13:05:31	Access time
4	[10.42.12.187:51565]	IP destination and port used
5	NAS_IP=10.42.12.187	IP destination
6	User=op2	User that accessing the network devices
7	Flags=TAC_PLUS_ACCT_FLAG_START	Log Message

Table 6 shows the contents of accounting files which can be managed by using Elasticsearch also identifying logs which contain AA (Authentication, Authorization) special message. Testing is done starting from September 2nd, 2019 until September 9th, 2019. The testing generates 24.557 log which was collected in server. Processed log is not only from accounting files, it also contains debug and system files. Testing is done by observing Discover page on Kibana as user interface. If there is log detected, the data will show on Kibana's Discover page. Figure 4 shows the results form log receiving.

Figure 4. Log Receiving Test Results

3.4. Application Evaluation

Application evaluation explains the results and appearance of the application that has been created. The initial appearance of the application is a login page that serves to authenticate users who will access the system.

After authenticated, the user will be directed to the main page that contains the main dashboard. The main dashboard displays general information about numbers of registered admin, user, admin tacacs, and user tacacs. There is also information about user lists and graphical form of which port that users use to access the network devices. There are several navigation menus available in the application, those are Monitoring, Account, TACACS Account, and System Configuration. The main page view is shown in Figure 5.

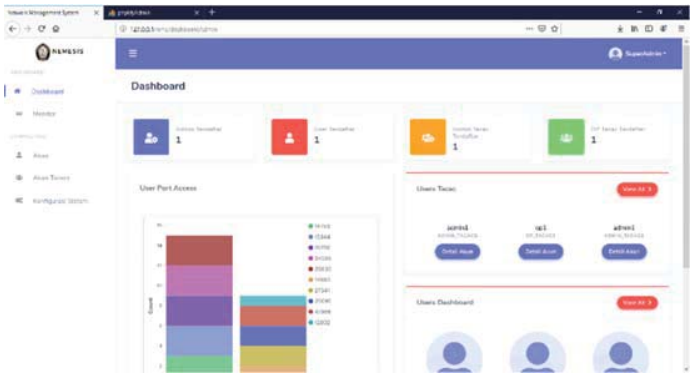

Figure 5. Application Main Page

3.5. Discussion

The result of the research is developing TACACS + LDAP and an application to monitor user login. Secondly, other feature of the application provides early log review.

4. Conclusion

Topology that applied in this research is star topology with Cisco Catalyst WS-C2960-24LC-S Switch as hub. TACACS and server connected using TCP protocols on port number 49. Based on system and application evaluation all functionality run well. Username and password that are not registered either in TACACS or LDAP cannot access the network devices. User operator cannot run configuration commands on network devices because granted privilege level 1. All user's activity when accessing the network devices are recorded and collected as log on TACACS accounting.

User account modification can be logged by LMS system. Priority of the modification filtered by admin to show a password changed, creating user, and failed account logging.

In the future research suggest to build the LMS System to send notification message for admin to notify about the modification account. Suggestions for further research can be developing a function to manage registered network devices on TACACS. Further research can develop the mobile version to ease admin and operator doing the network management efficiently.

Acknowledgement

This research was financially supported by The Faculty of Engineering, Diponegoro University, Semarang, Indonesia through Strategic Research Grant 2019 number: 3161/3/ UNT7.3.3/PG/2019.

References

[1] Mustafa, Hamzah A and Rachmawati Y 2018 Rancangan Infrastruktur Jaringan Backbone Hybrid Di Tiga Kampus IST AKPRIND Yogyakarta *J. JARKOM* vol **5** no 2 pp 122–9

[2] Kerta J M, Adiprabowo P and Kusmiyati E 2011 Penggunaan Single Sign On (SSO) Pada

Jaringan Internet Badan Pengkajian Dan Penerapan Teknologi (BPPT) *ComTech* vol **2** no 2 pp 880–6

[3] López A 2015 *AAA protocols and network access control: Radius* [Online] Available: https://www.incibe-cert.es/en/blog/aaa-radius [Accessed: 10-Feb-2019]

[4] TACACS 2011 *The Advantages of TACACS* + [Online] Available: http://www.tacacs.net/docs/TACACS_Advantages.pdf [Accessed: 19-Mar-2019]

[5] Ravi V, Sunitha N R, Pradeep R and S Verma 2017 Formal methods to verify authentication in TACACS + protocol *2017 2nd Int. Conf. Emerg. Comput. Inf. Technol.* pp 1–4

[6] Riyanto A and Ulinuha A 2014 *Design And Implementation Of SSO (Single Sign On) Using LDAP Authentication For Information System And Hotspot Access At Pesma KH Mas Mansur UMS* thesis (Solo: Universitas Muhammadiyah Surakarta)

[7] Pratap A and Saxena P 2017 An Analytical and Experimental Study of AAA Model with Special Reference to RADIUS and TACACS+ *Int. J. Comput. Appl.* vol **169** no 9 pp 6–10

[8] Rukmana A and Desiyani I D 2017 *Rapid Application Development* pp 2–4

[9] Rochim A F, Fauzi A and Aziz M A 2019 Design Log Management System of Computer Network Devices Infrastructures Based on ELK Stack *ICECOS 2019*

[10] Shekhar A 2016 *What Is Star Topology? Advantages And Disadvantages Of A Star Topology* [Online] Available: https://fossbytes.com/star-topology-advantages-disadvantages-star-topology/ [Accessed: 10-Feb-2019]