Unit 8 RADIUS Implementation

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

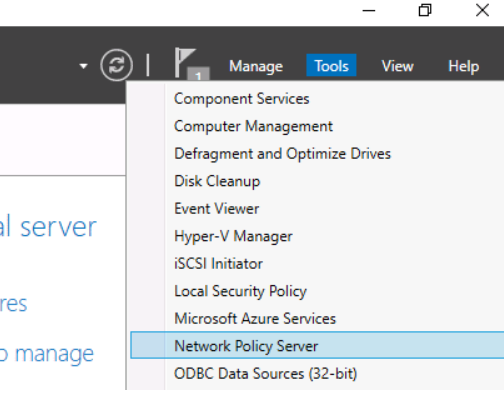
**February 7, 2023**

Before going into a guide on how exactly to set up a RADIUS server, and the clients therewithin, one needs to understand what exactly a RADIUS server does, and how it is useful to cybersecurity disciplines. A RADIUS server ensures security standards through a number of different means. At its most basic, RADIUS is a protocol that is used during a network informational exchange, in which a client is meaning to connect to a server. This server is verified by the RADIUS protocol and uses this in order to facilitate either a connection or rejection for the client (Stanford University, 2018). The RADIUS protocol works with a client’s identity in tandem with what permissions and privileges they may have regarding the network they are trying to access. A RADIUS server will attempt to match users with their access privileges to determine whether or not the user legitimately may have access to the server they are trying to connect to (Stanford University, 2018). Because of this, RADIUS may be a powerful protocol in order to adhere to safety standards within cybersecurity disciplines relating to server connections. Moreover, this can help establish a secure line of communication while taking another step to mitigate the presence of known malicious actors that may attempt to do harm to a network that is being overseen. Much of the RADIUS protocol is automated so there is no need for a Server Administrator to deal with manual bans and network traffic logging. Additionally, RADIUS servers are capable of constantly monitoring network traffic to provide a sense of transparency over the network and how it relates to what the users of it are doing at any given moment in time (The National Science Foundation, 2022). This can be an extreme help to servers that oversee a large number of connections such as business places that may not have the resources to hire a dedicated cybersecurity team to manage the connections of every user on the network and how they utilize it.

There are a few steps to ensure the successful implementation of a RADIUS Server within the Active Directory domain. It can be technically challenging at first, but luckily a concise step-by-step guide is possible. Thankfully, the main overarching architecture can be followed to fork concise steps to implement a RADIUS server. These steps will help system administrators in configuring a RADIUS server on an active directory domain as well as implement the security protocols that RADIUS servers utilize in their daily functions. Although there will be much customization that a Cybersecurity Specialist will be able to perform regarding their own personal RADIUS server, the RADIUS protocol is relatively simple to implement for the organization that requires it (Stevenson University, 2023). When following these steps, Cybersecurity Specialists will have a server utilizing the RADIUS protocol on an active directory domain that they are able to further customize to fit the needs of the organization, or endeavors that they may need the security benefits to pursue. Additionally, as part of the RADIUS protocol monitoring users in their activity while connected to the RADIUS server will also be implemented as part of this step-by-step process (Rosenberg, 2019). This will ensure that Cybersecurity Specialists have access to detailed network logging infrastructure, as well as informational statistics in order to better secure the network that they are a part of. Importantly, this comes with additional securities to manage how exactly is on the administrator’s network, and how they use it in order to better understand use case scenarios, and especially those that may prove malicious to the network and all users that utilize the benefits of a going forward. The following is such a guide utilizing information as detailed by a popular server hardware vendor,

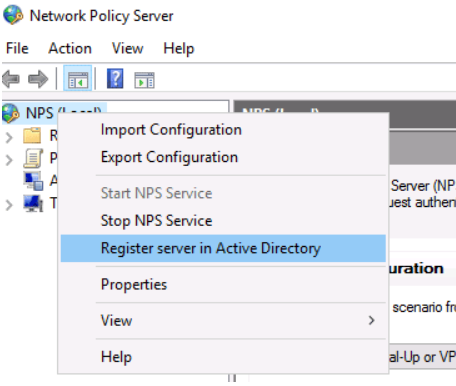
Cloud RADIUS (Raphaely, 2024).

* First and foremost, a Network Administrator will need to set a local Security Group. This can be done in the Active Directory platform, and will allow the Network Administrator to attribute all users that will be utilizing the network with their associated roles and privileges.
* Secondly, the Network Administrator will need to initialize the network policy server. This, the administrator will access the Server Manager console and utilize the “Add roles and features” wizard. Using this wizard, the administrator will then select the “Network Policy and Access Services” role. When this is done, the administrator will have the option to initialize the Network Policy Server in the Tools dropdown list.



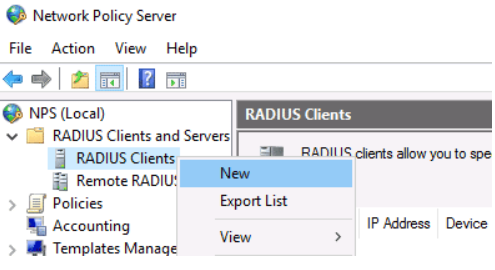
(Raphaely, 2024)

* Third, in the directory browser, the administrator will locate the “NPS (Local)” root, and register it in Active Directory via the right-click context menu. A confirmation Dialogue box will appear to confirm this action.



(Raphaely, 2024)

* Finally, within this NPS (Local) root, a RADIUS Clients and Servers folder will appear. The Administrator will then be able to add new RADIUS clients by expanding this folder, and selecting the “New” option from the right-click context menu of “RADIUS Clients”. A Dialogue box will appear that will allow the administrator to fill in necessary data for the RADIUS client.



(Raphaely, 2024)

Utilizing this guide will give System and Network Administrators The information that they need in order to be successful in their endeavor of securing advanced online communications. With the major setup of a RADIUS server being administered in just four main steps, RADIUS servers can provide as a powerful tool to cybersecurity analysts and specialists to maintain security over the networks they utilize. Additionally, utilization of a RADIUS server may take resources away from needing to implement a team of specialists constantly monitoring network traffic, and cross-examining rule sets and privileges and may save an organization that utilizes RADIUS servers a great deal of time and money that they would otherwise need to spend in order to gain a similar sense of security and transparency over the network that they have incorporated. With all this in mind, the authentication and authorization services that a RADIUS server employs comes with a significant benefit to the organization as a whole. Utilizing this sense of transparency that RADIUS affords, new organization is able to divest time and resources into other ventures to continue growing and expanding into the feature. With a three-pronged approach that RADIUS protocols utilize regarding user authentication, network allowances and network monitoring, server security specialists may employ RADIUS protocols to a great effect in order to secure the network that they oversee.

# **References**

Raphaely, E. (2024). *How to Setup a Windows RADIUS Server*. Retrieved from Cloud Radius Learning Resource Center: https://www.cloudradius.com/how-to-setup-a-windows-radius-server/

Rosenberg, B. (2019, April 26). *Radius Authentication Server*. Retrieved from University of Miami: https://www.cs.miami.edu/home/burt/learning/csc424.192/proj4/

Stanford University. (2018, August 10). *RADIUS Access and Authentication*. Retrieved from Stanford University IT: https://uit.stanford.edu/service/radius/authentication

Stevenson University. (2023). *RADIUS Authentication*. Retrieved from stevenson.edu IT Help Document: https://myaccount.stevenson.edu:8443/help/admin-guide/Configuration/Self-Service/RADIUSAuthentication.html

The National Science Foundation. (2022, May 13). *RADIUS*. Retrieved from kb.ucar.edu: https://kb.ucar.edu/display/EITKB/RADIUS