Application Note AN2015-08

Understanding When to Use LDAP or RADIUS for Centralized Authentication

Ben Herrmann

INTRODUCTION

Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial-In User Service (RADIUS) protocol are two commonly used protocols for authenticating and authorizing users. Both protocols perform similar tasks, making it hard to determine which to use. This application note describes the differences between both protocols as well as security considerations for implementation.

PROBLEM

LDAP and RADIUS are typically used to authenticate and authorize users, but choosing which protocol to use for certain tasks can be difficult. In addition, setting up these services can be time-consuming and confusing. The two protocols operate differently, which leads to varying levels of security and network traffic.

SOLUTION

Understanding the difference between the protocols can help users select the right protocol for the right task. This application note also provides general security information on SEL implementations of LDAP and RADIUS. For information about specific applications, contact the SEL Engineering Services cybersecurity team.

What Is LDAP?

LDAP is a directory service that is used to search and modify directories over a network, such as those created by Microsoft® Active Directory® service. An LDAP server contains the directory of users in an LDAP directory tree. LDAP clients who wish to gain information about entries in the tree or perform modifications to these entries contact the server. These servers can be replicated to allow for faster, more reliable access to the directory across a network. LDAP servers can store various user attributes, such as telephone numbers, emails, and locations, as well as authentication information. This gives network administrators flexibility when implementing services such as single sign-on.

What Is RADIUS?

RADIUS is a protocol that allows for centralized authentication, authorization, and accounting (AAA) for user and/or network access control. RADIUS clients contact the server with user credentials as part of a RADIUS Access-Request message, and the server responds back with a RADIUS Access-Accept, Access-Reject, or Access-Challenge message. Authentication and authorization are generally performed in one step to minimize traffic flow, although RADIUS can

support multifactor (or two-factor) authentication using one or more Access-Challenge messages. Accounting is then performed via additional messages from the client to the server. RADIUS also supports more complex forms of authentication, such as those described by the Extensible Authentication Protocol (EAP).

Design Differences

LDAP

LDAP provides a means of interfacing to a directory. LDAP does not require any security between the client and server. However, through the use of Transport Layer Security (TLS), LDAP can encrypt user sessions between the client and server. This keeps all information transferred in LDAP transactions over the network secure. LDAP also benefits from a simple implementation process that is easy for network users to access. However, LDAP does not directly support user accounting. Many implementations provide server-side accounting that varies in scope. Other user activity can be captured by additional protocols, such as Syslog. These additional protocols allow an LDAP server to provide user authentication services. Figure 1 shows a basic LDAP network.

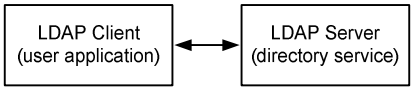

Figure 1 Basic LDAP Network

RADIUS

RADIUS typically acts as an intermediate service that only handles AAA. It can contact a directory service, either its own or that of a different server, and authenticate and authorize the user. This process alleviates some of the performance issues with large directory structures by allowing the caching of user data on the RADIUS server. It also allows the server to integrate with dedicated authentication servers. The RADIUS server talks to other services using other protocols, such as LDAP or Simple Object Access Protocol (SOAP). This adds considerable functionality and security but can complicate setup.

RADIUS protocol lacks encryption on all attributes except for the password field, which can be a cause for concern to network administrators. However, other protocols described later in this application note can alleviate security issues. RADIUS can also perform accounting services, ensuring that sensitive user information is properly tracked. Services such as one-time password (OTP) generation can also be attached to RADIUS servers. These services are supported through the use of Access-Challenge messages. Figure 2 shows a basic RADIUS network structure.

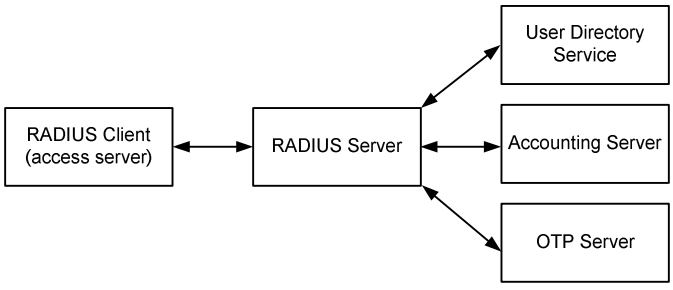

Figure 2 Basic RADIUS Network Using OTPs

Operational Differences

LDAP and RADIUS have some small differences in how they operate. This leads to varying levels of security and network traffic.

LDAP and RADIUS have several differences in how they interact over the network. LDAP uses Transmission Control Protocol (TCP) in order to ensure reliable connection across the network. TCP ensures a connection, but does require more network overhead. RADIUS uses User Datagram Protocol (UDP), which minimizes network overhead but does not ensure a connection. Depending on implementation, this may cause lost packets, errors in packets, and lengthy timeouts. It may also make the network vulnerable to replay attacks if implemented improperly.

By default, RADIUS packets lack encryption, except on the password field, meaning that sensitive user information is sent in clear text over the network. To combat this, users need to implement additional security mechanisms, such as a virtual private network, between RADIUS servers and clients if all RADIUS attributes need to be encrypted. For additional security, RADIUS is also flexible enough to allow for other forms of authentication, such as those implemented using EAP.

By itself, LDAP is unable to support multifactor authentication. Several enterprise solutions are available, but many require additional resources. These solutions often implement other protocols as well, including RADIUS. RADIUS can support services that query directory services for user information as well as additional services, such as OTP servers, for enhanced security. For general security information on SEL implementations of LDAP and RADIUS, see Table 1.

Table 1 SEL LDAP and RADIUS Security

Protocol	Credential Confidentiality	Server Identity Verification	Full Tunnel Encryption
RADIUS with Password Authentication Protocol (PAP)	Yes	Shared key	No
RADIUS with EAP	Yes	Shared key and X.509 validation	Partial
LDAP with TLS	Yes	X.509 validation	Full
LDAP without TLS	No	No	None

Network resources used by the two protocols are also quite different (see Table 2). LDAP sessions often require multiple transactions between the server and the client, which can cause significant delays during user authentication attempts. RADIUS can cache user information from the directory server to decrease login times. RADIUS is a simpler, less verbose protocol than LDAP, which increases the speed of authentication transactions for large databases of users. However, because RADIUS uses UDP, requests may time out and have to be retried if the network quality is poor. Authentication client load is reduced when using RADIUS because the network load is minimized and there is no need for complex settings or directory searches to take place between the user and the directory service.

Table 2 Resource Differences

Resource	RADIUS	LDAP
Transport method	UDP	TCP
Network load	Minimal	Moderate
Client processing	Minimal	Minimal
Server processing	Major	Moderate

While RADIUS can offer considerable functionality, it can be difficult to maintain. Managing multiple backend services can be confusing for network administrators. RADIUS servers often communicate using multiple protocols, quickly making troubleshooting difficult. LDAP provides basic network authentication with minimal hardware requirements and a simpler interface. This can reduce maintenance and overhead costs as well as reduce stress on network administrators.

CONCLUSION

This brief overview of LDAP and RADIUS provides insight into how these protocols are commonly implemented. RADIUS and LDAP both allow for centralized authentication services. LDAP can allow for single sign-on services in the network, but it lacks built-in tools for session accounting. LDAP can easily be encrypted using TLS as a wrapper. The simplicity of LDAP also allows for easy setup and integration with an already established network, such as a Microsoft Active Directory server. RADIUS allows for flexibility in services offered because it can connect to almost any other network service. RADIUS often allows for faster speed in network transactions due to its simplicity. However, setup of these services can be time-consuming and confusing. In short, LDAP excels in situations where simple password authentication is needed while RADIUS offers additional services for authentication but increased complexity during the setup and management of the network.

REFERENCES

[1] Microsoft, “What is LDAP?” 2015. Available: https://msdn.microsoft.com.

[2] Microsoft, “Lightweight Directory Access Protocol,” 2015. Available: https://msdn.microsoft.com.

[3] Microsoft, “RADIUS Server,” March 29, 2012. Available: https://msdn.microsoft.com.

[4] Microsoft, “RADIUS Protocol Security and Best Practices,” January 17, 2002. Available: https://msdn.microsoft.com.

LAN2015-08

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com