Providing Secure LDAP Authentication With SEL Computers During a WAN Link Failure

Mike Brown

INTRODUCTION

One of the most secure means of authenticating users is to use a central authorization and authentication system, such as Microsoft® Active Directory® Domain Services (AD DS). Typically, your information technology (IT) department maintains this central authentication system and uses it to grant access to network resources, such as office computers or laptops. A server with the AD DS role is called a domain controller (DC) and is one of the most critical systems in an Active Directory environment. In some configurations, if the device you are attempting to access cannot communicate with a DC, you cannot gain access to that device.

This application note discusses how to use a read-only domain controller (RODC) on an SEL rugged computer for user authentication during a wide-area network (WAN) link failure.

For more information on AD DS and Lightweight Directory Access Protocol (LDAP), refer to SEL application guide AG2013-14, “Configuring a Windows® Server for Centralized Authentication With LDAP-Enabled SEL Devices.”

PROBLEM

Devices connected to local-area networks (LANs) and WANs can authenticate to an Active Directory server by using LDAP. Consider the case of a remote site, such as a utility substation, where a WAN connection is not always available. When technicians come on site to perform service or maintenance, there must be a reliable way to verify who they are. If no central authentication mechanism exists, then you must rely on local authentication. With local authentication, each user account must be created and maintained (password, password expiration, and so on) on each device independently. This is the most reliable means of granting users access to systems, but it has some pitfalls. Namely, if a user departs the company, that user will still have access to systems until the account is disabled or each system password the user knows is changed. Keeping track of which systems these are is another challenge entirely.

Centralized authentication is effective, but DCs are typically in IT data centers and not out in the field. What happens, then, when you have an unreliable WAN link? Again, if your devices cannot communicate with a DC, they will not allow you access and you will be effectively locked out of the systems you are there to service.

SOLUTION

DCs should never be placed into service at physically insecure locations. These servers house all of the structure and credentials for the Active Directory infrastructure of an entire organization. This is very valuable information for hackers, and it would be devastating if the data were tampered with or lost. Furthermore, full read-write domain controllers (RWDCs) can and should only be used for that dedicated purpose. It is a bad idea to put business-line or other applications on an RWDC because if those applications are compromised, a hacker can easily steal or manipulate Active Directory data. In fact, Windows explicitly prohibits non-administrator accounts from logging in to an RWDC as a security precaution.

A perfect solution for this scenario is an RODC running on an SEL rugged computer, such as the SEL-3355 Computer or SEL-3360 Compact Industrial Computer. An RODC proxies authentication requests upstream to an RWDC (e.g., across a WAN link). If the provided credentials are valid, the upstream DC passes a success message back to the RODC, which authenticates the user for access to the system. A second message is sent to the upstream DC requesting to cache the user credentials on the RODC in order to service future authentication requests. If the user is in the right security group, his or her credentials will be transferred to the RODC and cached there. All future authentication requests by that user at the remote site will be serviced by the RODC. If the user account has not been explicitly placed into the security group, the user credentials will never be cached. If the user ever departs the company, IT staff only need to disable his or her Active Directory account (a regular operation when employment is terminated) to lock the user out of all of the systems he or she had access to.

Combining RODC services with the SEL rugged line of high-performance hardened computers gives you the added benefit of using that same computer for business-line or other applications. RODCs do not inherently restrict who can log in to the server itself, so your RODC server can also function as your supervisory control and data acquisition (SCADA) human-machine interface (HMI) or protocol conversion server, all while maintaining the highest level of security.

CONCLUSION

Protecting your data is more important than ever, and the first line of defense is a well-maintained authentication and authorization system. Microsoft Active Directory is widely used and very often already present within business networks. With the addition of RODCs, combined with SEL rugged computers, you can secure and closely monitor access to devices anywhere in your organization.

LAN2015-01

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