



IMPROVE SAP SECURITY WITH ACTIVE DIRECTORY LOGON

- Join Linux and Unix computers running SAP to Active Directory
- Use Active Directory credentials for single sign-on to SAP
- One user, one ID
- Securely authenticate SAP users with Kerberos
- Manage computers running SAP with group policies
- Consistently implement security settings across the enterprise

Generate reports to help improve regulatory compliance

Using Likewise for AD-Based Single Sign-On With SAP R/3

Overview

Likewise Enterprise lets you join Linux and Unix computers running the SAP R/3 Application Server to Microsoft Active Directory, yielding a range of benefits for users, system administrators, and managers.

Users can log on SAP systems by using their Active Directory logon names and passwords. System administrators rest easy with the knowledge that SAP users are securely authenticated with Kerberos 5 and authorized for access to SAP by Active Directory. Managers see their operational costs drop as their Linux and Unix systems running SAP are centrally managed within Active Directory. Security managers find help in their quest for regulatory compliance.

About Likewise Enterprise

By joining Linux, Unix, and Mac computers to Active Directory – a secure, scalable, stable, and proven identity management system – Likewise gives you the power to manage all your users' identities in one place, use the highly secure Kerberos 5 protocol to authenticate users in the same way on all your systems, apply granular access controls to sensitive resources, and centrally administer Linux, Unix, Mac, and Windows computers with group policies. Likewise includes reporting capabilities that can help improve regulatory compliance.

How Likewise Provides Single Sign-On for SAP

Likewise allows Linux, Unix, and Mac OS X computers to authenticate users with Active Directory. Since Microsoft Windows 2000, Active Directory's primary authentication protocol has been Kerberos. When a user logs on a Linux or Unix computer that is joined to an Active Directory domain, Likewise uses Kerberos to establish a key and to request a ticket for the user from Active Directory, which is in effect a Kerberos key distribution center. The user's ticket is subsequently used to implement SSO with other applications, such as SAP.

The Role of Kerberos in Single Sign-On for SAP

Described in RFC 4120, Kerberos is an authentication protocol that fosters the implementation of single sign-on. Kerberos is considered a secure authentication mechanism, having been designed to withstand common network attacks (for example, man-in-the-middle and replay attacks).

In a nutshell, Kerberos works like this:

- Kerberos uses encrypted tickets to represent credentials.
- The encryption technique relies on a shared secret (a key) known to the Kerberos client and the Kerberos key distribution center, or KDC. This secret is based on an account password. When a user account is created at the KDC, Kerberos stores the shared secret and uses it to encrypt tickets sent to a client on behalf of the user. When the user logs on the client machine, he or she provides a username and password, establishing the shared secret on the client as well. This allows the KDC and client machines to communicate in a safe, encrypted, fashion.
- Applications such as SAP that want to use Kerberos need to be associated with service accounts that establish shared secrets on the KDC. This allows the KDC to encrypt tickets in a form that can be understood only by relevant applications.
- User and applications keys (shared secrets) are usually stored in a key table, or keytab, for subsequent use. These keytabs must be available to SAP so that it can decrypt Kerberos data. With Likewise, a user's keytab is established when the user logs on a computer. Application keytabs are longer-lived and are only created when passwords are changed on service accounts.

- When a user needs to access a Kerberized application, he or she (indirectly, via a client application) requests the KDC for a service ticket for that application. A portion of this ticket is encrypted with the user's shared secret and another portion is encrypted with the application's shared secret. This allows both the user's client computer and the application's client computer to verify that the incoming ticket is valid.
- Kerberized applications frequently support other forms of authentication and make it necessary for application clients to negotiate what type of authentication they're going to perform. Operating systems typically provide software for this negotiation. Windows systems provide SSPI whereas Linux and Unix provide GSSAPI. These two systems are, mostly, interoperable.

Although Kerberos facilitates the implementation of SSO, it can be extremely difficult and frustrating to get it to work properly. Many individual steps are involved and mistakes anywhere along the way typically only manifest themselves by a failure of authentication. It can be difficult to diagnose where errors have crept into the process.

Likewise fosters the use of Kerberos by automating its configuration and use. To ensure that the Kerberos authentication infrastructure is properly configured for SAP, Likewise does the following:

- Ensures that DNS is properly configured to resolve names associated with Active Directory.
- Provides tools to join Linux, Unix, and Mac OS X computers to AD.
- Performs secure *dynamic* DNS updates to ensure that Linux and Unix computer names can be resolved with AD-integrated DNS servers.
- Configures Kerberos. In an environment with multiple KDCs, Likewise makes sure that Kerberos selects the appropriate server.
- Configures SSHD to support SSO through Kerberos (by using GSSAPI).
- Creates a keytab for the computer (when it is joined to AD) and one for the user (during logon).

- Provides tools to generate keytabs for applications.

Although it might be possible to perform some of these operations by manually configuring a Linux or Unix system, the Likewise solution greatly simplifies the process. It is easy to spend hours tinkering with a system to accomplish what Likewise does in an instant.

Configuring SAP R/3 Application Server for SSO with Likewise

To integrate SAP with Likewise and Active Directory, you must reconfigure the SAP server and the SAP client graphical user interface (GUI) to use Secure Network Communications (SNC) and Kerberos. This approach provides not only strong authentication but also ensures that application data is securely transmitted over the network. For detailed information about how to configure the SAP server and client GUI to use SNC and Kerberos, see your SAP technical documentation or go to <http://help.sap.com/>.

Because the Kerberos protocol specifies that the TGT acquired during logon can be presented to the KDC to generate a service ticket, the service ticket can authenticate the SAP R/3 Application Server after the SAP server either has been joined to Active Directory or has been provisioned with a Service Principal Name (SPN) in Active Directory and the resulting keytab file has been copied to the SAP server.

The result of this process is an SSO experience for the user. The user simply logs on the Linux or Unix computer and can then securely access SAP without having to resubmit credentials to the SAP server.

Because the Likewise solution eliminates the need for a separate SAP password, the overhead of managing multiple passwords for multiple systems is reduced substantially, cutting operational costs.

Here's the single sign-on process with Likewise and SAP:

1. After logging on the computer, the user launches the SAP GUI from the desktop and selects the Kerberos protocol logon option. The SAP GUI, through the Generic Security Service API (GSS-API) wrapper for the Kerberos authentication package, requests a Kerberos service ticket for the SAP R/3 Application Server by using the settings stored in SAP GUI profile.

2. If needed, the Kerberos package requests a new ticket from the Active Directory domain controller, or the Kerberos package gets an existing ticket from the ticket cache.
3. The SAP GUI connects to the SAP server and presents the ticket upon request.
4. The SAP server gets the service ticket and validates it by invoking the Kerberos authentication package on the server through the GSS-API wrapper.
5. If the Kerberos package on the SAP server validates the ticket, the SAP server extracts the user's principal name and maps it to an account handled by the SAP server.
6. The user is logged on the SAP server using the account maintained by SAP.
7. An encrypted session is established between the client and the server for application data.

Because Likewise authenticated the user to the SAP server with the user's default Kerberos credentials, an SSO experience is achieved for the user.

Note: Likewise Software can help you configure your SAP server and the SAP client graphical user interface to use Secure Network Communications and Kerberos.

ABOUT LIKewise

Likewise Software is an open source company that provides audit and authentication solutions designed to improve security, reduce operational costs and help demonstrate regulatory compliance in mixed network environments. Likewise Open allows large organizations to securely authenticate Linux, UNIX and Mac systems with a unified directory such as Microsoft Active Directory. Additionally, Likewise Enterprise includes world-class group policy, audit and reporting modules.

Likewise Software is a Bellevue, WA-based software company funded by leading venture capital firms Ignition Partners, Intel Capital, and Trinity Ventures. Likewise has experienced management and engineering teams in place and is led by senior executives from leading technology companies such as Microsoft, F5 Networks, EMC and Mercury.