



USE LIKewise WITH IBM TIVOLI IDENTITY MANAGER

- IBM Tivoli Identity Manager can be adapted to provision users who are configured for UNIX and Linux access with Likewise.
- Tivoli Identity Manager can be adapted to work with any of the Likewise configurations.

Integrating Likewise Enterprise With IBM Tivoli Identity Manager

Overview

Likewise Enterprise is the premier solution to integrate non-Windows systems into Microsoft Active Directory. IBM Tivoli Identity Manager provides a secure, automated, policy-based user management solution that helps enterprises set up new accounts and passwords quickly, including the ability for users to reset and synchronize their own passwords.

This technical note describes how Tivoli Identity Manager can be adapted to provision users configured for UNIX or Linux access through Likewise.

With Likewise, UNIX and Linux computers can join an Active Directory domain just as a Windows desktop or server can. As a result, users can log on the member UNIX or Linux system using their Active Directory credentials. Similarly, Active Directory users on Windows desktops can seamlessly access resources on UNIX or Linux servers that have been joined to Active Directory.

Configuring Likewise

Likewise can be configured in several ways depending on the customer's requirements.

- **Extending or not extending the Active Directory schema:** There are several attributes and classes required if a UNIX or Linux system needs to be integrated into Active Directory. These attributes typically extend the user and group object with UNIX specific information. The set of attributes and classes are collectively known as the RFC 2307 schema extensions. In general, enterprise AD Administrators are reluctant to extend the schema because schema changes are permanent and irreversible. As a result, Likewise gives customers the choice of integrating their UNIX or Linux systems into Active Directory with or without extending the schema.
- **One-to-many UID mappings:** In several scenarios, customers have already deployed a centralized authentication system such as a NIS database or an LDAP directory for users of their UNIX and Linux systems. Users have already been configured with specific UIDs when they log on these managed UNIX and Linux systems. Resources across the network such as files would have already been controlled by access control lists with these UIDs. When the customer plans on migrating away from the NIS database into Active Directory, there is the need to maintain these existing UID mappings either for the period of the migration or in some case indefinitely. For this reason, customers require that an AD user have multiple UIDs depending on the system the user logs on. Likewise provides this feature by mapping organizational units to Likewise Cells. If a UNIX system resides in a cell, it is possible for the administrator to provide a cell-specific configuration of the user's UNIX or Linux attributes. A default cell is the user's UNIX or Linux attribute information that is valid across the enterprise forest.
- **Choice of storage of attributes:** Recall that Likewise can be configured so that the Active Directory schema is not extended. In this case, the UNIX or Linux information for the user is stored in a separate AD container and that information is stored on a separate object linked to the actual Active Directory object. If the schema is not extended, this object is a `container` object and the information is stored in the `description` and `keywords`

attributes. If the schema is extended, this object is still stored in a separate AD container but the object is a `posixAccount` object and the information is stored on individual RFC 2307 attributes. Finally, in the scenario where the schema is extended, the `posixAccount` class information can also be directly attached to the AD user object.

The flexibility of Likewise gives rise to several possible configurations:

1. Extended schema, default cell only, information stored directly on the user object.
2. Non-extended schema, default cell only, information stored in a separate container with UNIX or Linux properties linked to user object.
3. Extended schema, default and additional cells, information stored in a separate container with UNIX or Linux properties linked to user object.
4. Non-extended schema, default and additional cells, information stored in a separate container with UNIX or Linux properties linked to user object.

IBM Tivoli Identity Manager

IBM Tivoli Identity Manager is a security rich, automated, policy-based enterprise user management system. Tivoli Identity Manager provides centralized identity lifecycle management. It is a robust enterprise user provisioning and deprovisioning system that interacts with managed directory and identity stores through adapter plugins. Tivoli Identity Manager adapters function as virtual administrators on the target platform, performing tasks such as creating users, managing users, updating user properties, deleting users and other identity lifecycle management operations. A variety of adapters are available from IBM.

The Tivoli Identity Manager Active Directory Adapter enables connectivity between the IMS and an Active Directory domain controller. By default, the Tivoli Identity Manager Active Directory Adapter supports a fixed set of user object attributes. However the adapter can be configured to support custom (extended attributes). For information on how to configure the AD adapter to support additional attributes, see the IBM Tivoli Active Directory Adapter Installation and Configuration Guide.

In addition to the pre-canned adapters, Tivoli Identity Manager also allows ISVs to easily write custom Tivoli Identity Manager Adapters.

Configuring Tivoli Identity Manager to support Likewise

The following is a summary of how Tivoli Identity Manager can be configured to work with each of the four Likewise configurations.

1. **Extended schema, default cell only, information stored directly on the user object.** This is the easiest scenario. The default Active Directory Adapter can be configured to support the additional RFC 2307 attributes which are directly stored on the user object. There is a 1:1 mapping between the Active Directory user and the user's associated UID.
2. **Non-extended schema, default cell only, information stored in a separate container with UNIX or Linux properties linked to user object.** This scenario is also simple. However, a custom adapter is required to write the attributes into a separate object and to ensure that the object is linked to the real user object. The custom adapter is simple because there is a 1:1 mapping between an Active Directory user and the user's associated UID.
3. **Extended schema, default and additional cells, information stored in a separate container with UNIX or Linux properties linked to user object.**
4. **Non-extended schema, default and additional cells, information stored in a separate container with UNIX or Linux properties linked to user object.**

Scenarios 4 and 5 are more complicated. The issue is not whether the schema has been extended or not. The issue is more that a single AD user can have multiple UNIX or Linux personalities depending on the machine that the user logs into. A customized Tivoli adapter is required to store the information tuple, which contains the user name, the organizational unit, and the associated UID pairs. The adapter must also write this information to Active Directory. The architecture of the custom adapter would be specific to the environment where the solution is deployed.

Summary

Likewise provides multiple possible configurations to integrate UNIX and Linux systems into Active Directory. All of these configurations require that a user's UNIX- and Linux-specific information be associated with the user's Active Directory object. All of these configurations can be automatically provisioned using IBM's Tivoli Identity Manager solution.

Likewise can help you configure Tivoli Identity Manager to work with Likewise Enterprise.

ABOUT LIKewise

Likewise® Software solutions improve management and interoperability of Windows, Linux, and UNIX systems with easy to use software for Linux administration and cross-platform identity management.

Likewise provides familiar Windows-based tools for system administrators to seamlessly integrate Linux and UNIX systems with Microsoft Active Directory. This enables companies running mixed networks to utilize existing Windows skills and resources, maximize the value of their Active Directory investment, strengthen the security of their network and lower the total cost of ownership of Linux servers.

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.