

LDAP User Service Guide

22 September 2005

This documents usage of the LDAP User Service for the NiagaraAX 3.0.x platform.

INSTALLATION	2
PALETTE	3
LDAPUserService	3
ActiveDirectoryService	3
KEY CONCEPTS	3
Active Directory	3
LDAP	3
COMPONENT GUIDES	4
LDAPUserService	4
User Prototypes	4
LDAPV2	5

Information and specifications published here are current as of the date of publication of this document. Tridium, Inc. reserves the right to change or modify specifications without prior notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia. Products or features contained herein may be covered by one or more U.S. or foreign patents.

Installation

- Using Workbench log into the target station as an administrator.
- Go to the property sheet of the “Niagara Network.” Expand “Fox Service” and change authentication from “digest” to “basic.”
- Open the LDAP palette and you have two choices, the LdapUserService and the ActiveDirectoryUserService. The ActiveDirectoryUserService is a pre-configured version of the LdapUserService for Windows Active Directory.
- Copy one and paste under the “Services” node of your station database.
- Delete the default UserService object also found under “Services.”
- The LDAP user service just pasted allows the creation of local users just like the default user service. In fact, the users “admin” and “guest” are already built in so one can always login, even if LDAP isn’t working.
- Configure the LDAP server information
 - Open the property sheet of the object under the LDAP user service whose name ends with “Config.”
 - For the ActiveDirectoryUserService, most of the properties have been pre-configured.
 - Replace “domain” and “net” in “Connection Url” and “User Base” properties.
 - Provide a valid user account for the “Connection User” property. It would be best if your Network Administrator created a user specifically for this function.
 - There is no quick and easy configuration help for the generic LdapUserService, advance knowledge of the LDAP server’s configuration (or schema) is required.
- Create User Prototypes
 - Not all data about a Niagara user can easily be stored on the LDAP server, especially security permissions. A user prototype allows you to configure default settings for groups of users.
 - In the “Config” object discussed above is a property named “Attr Prototype.” This specifies the LDAP attribute whose value is used to map a user and a user prototype.
 - The ActiveDirectoryUserService uses the “memberOf” attribute from Active Directory’s schema for mapping. Suppose a user belongs to a group called “Engineering.org” in Active Directory. What you should do is create a user prototype named “Engineering.org” and configure the properties that won’t be supplied by the LDAP server (especially security permissions).
 - To create a new prototype, right-click on the “User Prototypes” object below the user service. In “Actions,” select “New Prototype.”
- Save your database and restart your station.
- Log into the station using an LDAP user. The ActiveDirectoryUserService is pre-configured to use the user name without the domain. So for example, “janedoe@tridium.com,” would login at “janedoe.”

Palette

LdapUserService

This is a generic un-configured LDAP user service. The LdapV2 extension is name LdapConfig.

ActiveDirectoryService

This is an LdapUserService pre-configured for Windows Active Directory. The LdapV2 extension is named “ActiveDirectoryConfig.”

Key Concepts

Active Directory

The Windows directory service that stores information about all objects on the computer network and makes this information easy for administrators and users to find and use. With the Active Directory, users can access resources anywhere on the network with a single logon. Similarly, administrators have a single point of administration for all objects on the network, which can be viewed in a hierarchical structure. Active Directory supports and LDAP interface.

LDAP

Lightweight Directory Access Protocol. Typically an LDAP server is a network-accessible database where an organization stores information about authorized users and their privileges. Rather than create a new user account on 50 different computers, the new user is entered into LDAP and granted rights to those 50 systems. If the user leaves the organization, revoking all privileges is as simple as removing one entry in the LDAP directory. LDAP is a bit confusing because original implementations were presented as alternatives to Web and the relational database management system.

Component Guides

- [LdapUserService](#)
- [User Prototypes](#)
- [LdapV2](#)

LdapUserService

The LdapUserService is a service component in the NiagaraAX architecture. It looks and behaves nearly identically to the default user service. It can have both local and remote LDAP users.

Here are the differences:

1. The LdapUserManager view has a column that identifies local versus LDAP users.
2. The LdapUserService has a child object, a subclass of BLdapExt, which encapsulates the LDAP functionality. The name of object does not matter.
3. The LdapUserService has a child called "User Prototypes." Descendants of this object are prototypical users that LDAP users can map to.

User Prototypes

Not all user properties can be retrieved from an LDAP server. Prototypical users provide default property values for LDAP users. They are contained in the "User Prototypes" child of the LDAP user service.

Perhaps the single most important property provided by a prototype user is its permissions.

To create a new user prototype:

- Invoke the "**New Prototype**" command on the User Prototypes container.
 - The name of the prototype user is what maps the prototype to LDAP users.
- Configure the property sheet of the newly created user.
 - Only those properties that will not be provided by the LDAP server need to be configured.
 - Prototypical users can be disabled here which will prevent them from logging in.
 - User expiration is the earliest of: the expiration on the prototype or the expiration of the cached user. This shouldn't matter since cached users are only used when the LDAP server is unreachable.
- Configure the "**Attr Prototype**" property of the LDAP configuration object.
 - This is the LDAP attribute whose value maps to a slot name of a prototype user. If unspecified or it doesn't map properly, the default prototype is the Guest user.
 - If the value of this attribute is a distinguished name, the value of the leaf component is extracted as the profile.
For example, given the DN "OU=Engineering, DC=example, DC=com", the prototype user would be named "engineering".
 - If this attribute has multiple values (distinguished or not), the profile with the lowest index (highest on the property sheet) wins.

LdapV2

LdapV2 is an LDAP Version 2 extension to the LdapUserService. It must be a child of the service, but its slot name does not matter.

The following properties have special importance:

- **Connection Url** – URL to the LDAP server. If the port is not the default LDAP port of 389, then it must be explicit (ie ldap://host.com:123). The scheme of the url must always be 'ldap', even if SSL is being used; 'ldaps' is not supported.
- **Connection User** – This is the user name for the connection. If the LDAP server supports anonymous connections, this property may be empty. Otherwise, it is recommended a special user be created solely for the purpose of this connection.
- **Connection Pwd** – Password for the user configured in “Connection User.”
- **SSL** – The CryptoService must be installed to use LDAP over SSL. The “Connection Url” must point to a secure LDAP port: the common secure LDAP port is 636. Do not use the “ldaps” scheme.
- **User Login Attr** – This is the LDAP property whose value would match a user's login name. On Active Directory this would probably be "sAMAccountName" and on Unix it might be "uid."
- **User Base** – The sub-tree of the LDAP server where users who can login will be found. At the very least, the value of this property must contain the domain components of the server's domain. For example: "DC=example, DC=com"
- **Attr Email** – This is the LDAP attribute whose value would be the user's email address.
- **Attr Full Name** – This is the LDAP attribute whose value would be the user's full name.
- **Attr Language** – This is the LDAP attribute whose value would be the user's ISO 639 two-letter language code.
- **Attr Prototype** – This is the LDAP attribute whose value maps to a prototype user. If unspecified or it doesn't map properly, the default prototype is the Guest user.
 - If the value of this attribute is a distinguished name, the value of the leaf component is extracted as the profile. For example, given the DN "OU=Engineering, DC=example, DC=com", the prototype user would be named "Engineering".
 - If this attribute has multiple values (distinguished or not), the profile with the lowest index (highest on the property sheet) wins.
- **Cache Expiration** – Users will be cached for this period of time. If configured for 0 time, there is no expiration. The cache is only used when the server cannot be reached. If a connection is established to the server, cached users are not used.