What to Consider When Switching IBM InfoSphere Information Server to Use LDAP Authentication

Most companies today have one or more types of LDAP installed for authentication; IBM® Tivoli® Directory Server, Active Directory, OpenLDAP, and others. In many cases, having IBM InfoSphere® Information Server use that same LDAP domain for its authentication is beneficial. In this way, user administration becomes easier because there is a single set of users and passwords to maintain. As simple as this might sound, you must consider many questions before switching to LDAP with InfoSphere Information Server.

- What types of LDAP repositories are available?
- What is the difference between the two types of LDAP repositories?
- Which is the better choice for my company?
- What information will I need to configure my LDAP repository?

What types of LDAP repositories are available

The first consideration is deciding which of the two types of LDAP repositories is right for your configuration. InfoSphere Information Server uses IBM WebSphere® Application Server to do the initial authentication. WebSphere Application Server allows for two types of LDAP repositories:

- Stand-alone LDAP
- Federated repositories

What is the difference between the two types of LDAP repositories

Federated repositories have several key features that make it more flexible and easier to maintain than stand-alone LDAP:

- Multiple repositories can be defined for authentication.

  o These repositories can be different LDAP domains, file-based repositories, or a combination of the two.
  o They are useful when your company employs different LDAP domains for user authentication.

- An internal WebSphere Application Server file-based repository is automatically created.

  o This is useful when a requirement exists to have users who are not in LDAP, such as service accounts, also be able to log in to the InfoSphere Information Server.

- LDAP attribute mapping is supported. This allows the InfoSphere Information Server to automatically populate LDAP attributes, such as first and last name into the InfoSphere Information Server Web console.

  o This is useful with the InfoSphere Information Server tools, such as IBM InfoSphere Information Governance Catalog, where the first and last names of users are frequently displayed.

- Allows for multiple search bases and separate search bases for users and groups.
  - o This helps to increase search performance and decrease the number of users returned by LDAP.
- User and group filtering is easier to configure.

Stand-alone LDAP repository allows you to define only one LDAP domain. All users, including service accounts such as `isadmin` and `wasadmin` must exist in the LDAP domain. Stand-alone LDAP does not support LDAP attribute mapping so all user attributes, such as first and last name, must be entered manually into the InfoSphere Information Server Web console. Also, stand-alone LDAP allows for only one search base to be defined.

Which is the better choice for my company

Both stand-alone LDAP and federated repositories will work in large and small environments. The choice of which one to use simply depends on your requirements.

If your company requires authentication against multiple LDAP domains, then the choice is simple, you must use federated repositories.

Most users also tend to go with federated repositories when they are using InfoSphere Information Server tools such as IBM InfoSphere Information Governance Catalog. InfoSphere Information Governance Catalog displays the first and last names of users in many areas of the product. If this information is not entered into the user record in the InfoSphere Information Server Web console, the user name or the user's distinguished name will be displayed instead. When a large number of users are using the IBM InfoSphere Information Governance Catalog, manually entering the first and last name of each user can be time-consuming.

Federated repositories support attribute mapping, which allows selected LDAP attributes to automatically be populated for each user.

For companies that are using only IBM InfoSphere DataStage®, the use of the first and last name might not be as important because it is not displayed anywhere in InfoSphere DataStage. If only one LDAP domain is required for authentication, then stand-alone LDAP can work as well as federated repositories.

What information will I need to configure my repository

After you determine what type of LDAP repository you want to configure, the next step is to obtain the necessary information from the LDAP administrator.

- The type of LDAP that is configured. Examples include IBM Tivoli Directory Server, Active Directory, OpenLDAP.
- LDAP server name (or names).
- LDAP port.
- Full distinguished name for the bind user.
- Password for the bind user.
- The user name that will be used for the WebSphere Application Server administrator. This user must be an LDAP user when configuring stand-alone LDAP.
- Best base distinguished name (or names) to use. Federated repositories allow multiple search bases.
- Determine whether any LDAP groups are designated for InfoSphere Information Server users. If so, what are they?

After gathering the information, the next step is to configure the repository. IBM has several helpful IBM Education Assistant modules designed to guide you through the configuration of stand-alone LDAP and federated repositories. These Education Assistant modules are valid for InfoSphere Information Server version 11.5 also.

Before you begin your configuration, be sure you know whether your WebSphere Application Server installation that is used with the InfoSphere Information Server is configured as stand-alone or a cluster. For IBM InfoSphere Information Server 11.3 and later, the configuration for the repositories is slightly different for clustered WebSphere Application Server.

Federated repositories

With federated repositories, you can apply attribute mapping to map LDAP user attributes so that they automatically appear in the IBM Information Server Web console. You can also configure multiple and different search bases for users and groups.

Applying LDAP attribute mapping

When federated repositories are configured, a useful step is to *configure attribute mapping* so that the desired LDAP attributes such as first and last name, will automatically populate to the IBM InfoSphere Information Server Web console. See the following Technote to configure attribute mapping: https://ibm.biz/Bd4vb5

This feature is helpful when using the InfoSphere Information Server tools, such as IBM InfoSphere Information Governance Catalog. For example, Figure 1 shows how the IBM InfoSphere Information Server Web console appears after configuring federated repositories and configuring attribute mapping.
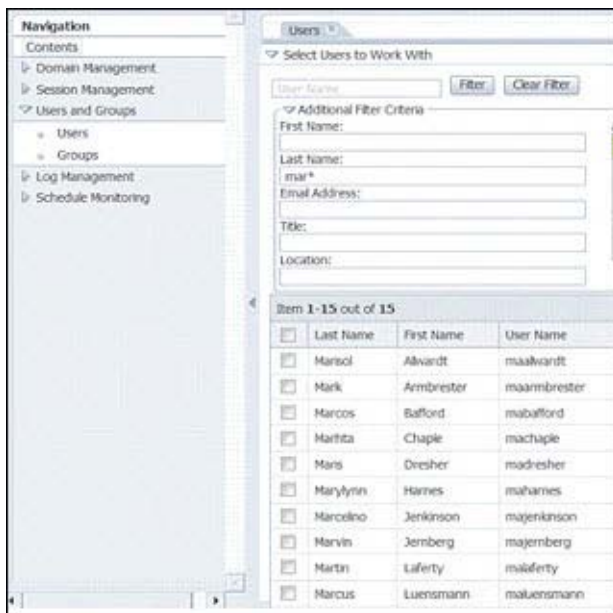

Figure 1. IBM InfoSphere Information Server Web console

Adding extra search bases for users and groups

An LDAP domain is set up much like a tree. If you know which branches of the tree your users and groups live on, then you can set up additional search bases to help the search performance. You can think of finding a user or group in LDAP like searching for a file on your computer. If you know which folder the file is in, finding the file becomes much faster. For example, if you know that your file is located under `c:\MyFiles\IBM`, you can have the search start in that folder and search from there. This way is much more efficient than starting your search from `c:\` folder.

The LDAP search works the same way. The base is the starting point of your search. For example, you know that all of your InfoSphere Information Server users are under this location:

`DC=IT,DC=Newco,DC=com`

Therefore, setting `DC=IT,DC=Newco,DC=com` as your user search base is more efficient. When a user or user list is requested, LDAP would start the search on the `DC=IT,DC=Newco,DC=com` branch instead of `DC=Newco,DC=com`. If the search base was set to `DC=Newco, DC=com`, the entire LDAP domain would be searched instead and the amount of time to complete the search would increase.

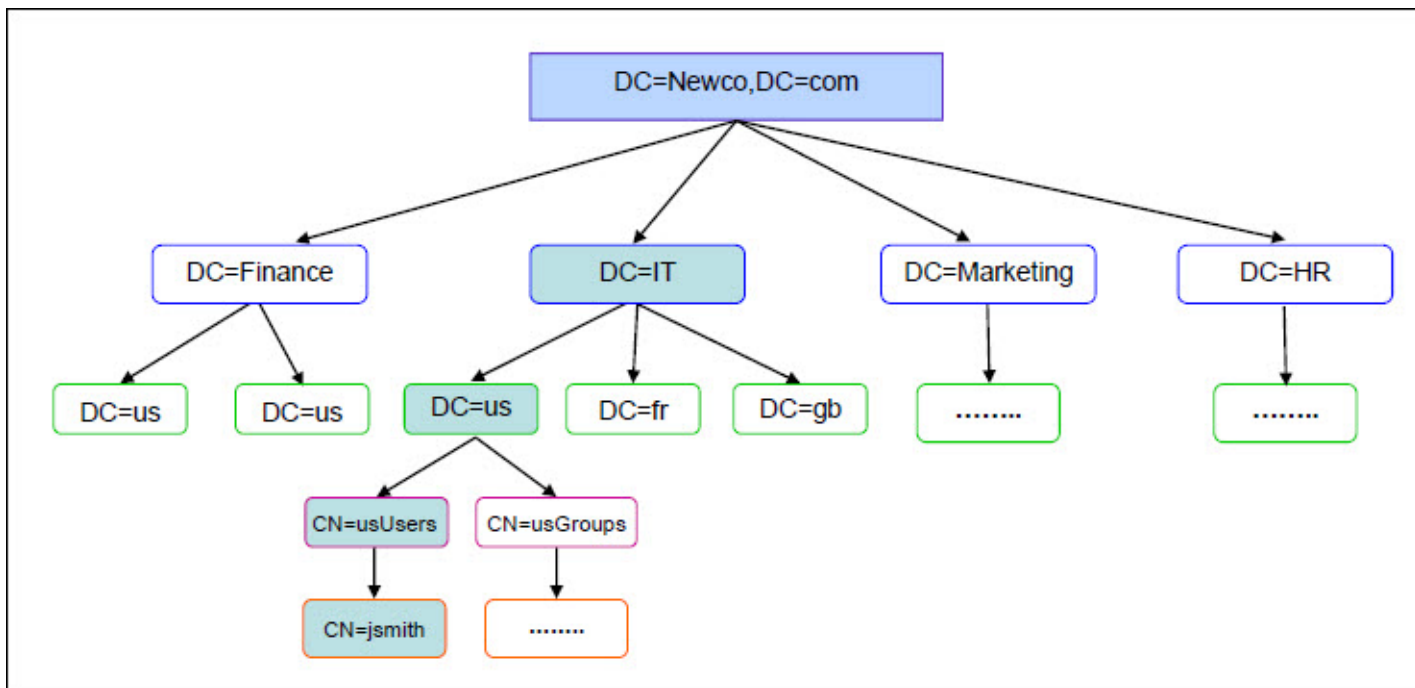Figure 2 shows the LDAP directory structure used in this example.

Figure 2. Example LDAP directory structure

Related information

See the following web pages:

- Education Assistant: Switching Information Server 9.1 and 11.3 and WebSphere to use Standalone LDAP for authentication
  https://ibm.biz/Bd4vbL

- Education Assistant: Switching Information Server 9.1 and 11.3 to use Federated Repositories for LDAP authentication
  https://ibm.biz/Bd4vbQ

- Education Assistant: Configuring Information Server 11.3 to use federated repositories with a WebSphere cluster
  https://ibm.biz/Bd4vb3

- Education Assistant: Configuring Information Server 11.3 to use stand-alone LDAP with a WebSphere cluster
  https://ibm.biz/Bd4vbt

- Education Assistant: Information Server - Advanced LDAP filtering techniques to minimize Information Server user list
  https://ibm.biz/Bd4vbU

- Technote: Information Server Web Console - Using Attribute Mapping to populate users' first and last names when using an LDAP repository for authentication
  https://ibm.biz/Bd4vb5

- Education Assistant: Adding additional search bases to Federated Repositories
  https://ibm.biz/Bd4vb7

These resources are also useful:

- IBM InfoSphere Information Server welcome page (with links to documentation) in the IBM Knowledge Center
  https://ibm.biz/Bd4vpF

- IBM Education Assistant videos
  https://ibm.biz/Bd4vpX

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law : INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document was created or updated on April 18, 2016.

Send us your comments in one of the following ways:
- Use the online **Contact us** review form found at:
  ibm.com/redbooks
- Send your comments in an e-mail to:
  redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

This document is available online at http://www.ibm.com/redbooks/abstracts/tips1338.html .

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

DataStage®
IBM®
InfoSphere®
Redbooks (logo)®
Tivoli®
WebSphere®
Other company, product, or service names may be trademarks or service marks of others.