SolarWinds Technical Reference

Configuring and Integrating LDAP

This document includes information about LDAP and its role with SolarWinds SAM.

Copyright© 1995-2012 SolarWinds. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft® and Windows 2000® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

Document Revised 6/21/2012- DJR

The Basics of LDAP

Lightweight **D**irectory **A**ccess **P**rotocol (LDAP) is a protocol for accessing directory servers. In other words, LDAP is a directory, not a database. There are no rows or tables in LDAP's directory and there are no relational links. The result is a simple yet structured directory design that is easy to navigate.

Every object in LDAP can contain one or more sub-objects, much like the folder and sub-folder relationship used in Windows operating systems. LDAP runs directly over TCP port **389** by default. It is used to store information about users, including the network privileges assigned to each user. Revoking or changing privileges can be done from one entry in the LDAP directory, rather than at many machines across the network. LDAP also supports SSL and TLS for security.

LDAP Key Terms and Components

Following is a list of key terms and components along with their respective definitions.

Distinguished Names

Distinguished **N**ames (DNs) are a fundamental part of LDAP. LDAP uses path syntax to identify objects in the store.

Typical Windows path syntax:

```
C:\Files\Pictures\Pic1.jpg
```

DNs work in reverse order, meaning the most specific node is on the left of the path syntax. Typical example of a DN:

```
CN=SomeUser,OU=SomeContainer,DC=SomeDomain,DC=com
```

This DN is composed of four **R**elative **D**istinguished **N**ame (RDN) parts:

```
CN=SomeUser
OU=SomeContainer
DC=SomeDomain
DC=com
```

Each RDN is a child of the object whose RDN is to its right. The object deepest in the tree in this DN example is the object, `CN=SomeUser`.

Each RDN is composed of two parts: the name of the attribute that provides the primary name of the object, and the value of that attribute. In this example, *CN*, which stands for **C**ommon **N**ame, is the name of the attribute that provides the primary name for objects of its class. *SomeUser* is the value of this attribute. There are also RDN attributes for *OU* (**O**rganizational **U**nit) and *DC* (**D**omain **C**omponent).

Like any file system, the name for an object in an LDAP container must be unique. Thus, `CN=Kate` uniquely identifies this object within its container, `OU=CustomerSupport`. As a result, the entire DN uniquely identifies this particular object in the entire directory tree.

Search Operation

The most important operation in LDAP is the ability to search. This is how objects are found in the directory tree and how values are read. The syntax is somewhat different from more familiar query syntaxes such as SQL. However, LDAP is also much simpler than SQL with SQL's joins, sub-queries, ordering, and grouping.

An LDAP query is composed of four basic parts: a search root, a search scope, a filter, and a list of attributes to return. There are more parameters and options, but these basic four are enough for most cases.

Search Root

The search root determines the place in the tree from which the search will start. This value is passed as a DN in string format. To search the entire directory, pass the DN of the object that is the root of the tree. To search lower in the hierarchy, specify a lower-level DN.

Search Filter

The search filter determines which objects will be returned in the query. It is analogous to the `Where` clause in a SQL statement. Each object in the scope of the query will be evaluated against the filter to determine whether or not it matches. Objects that do not meet the filter criteria are eliminated from the search.

Basic LDAP Syntax

The following table outlines basic operators for use with LDAP:

Operator	Operator Definition	Definition	Example
`=`	Equal to	This argument means an attribute must be equal to a certain value to be true.	`(givenName=Kate)` This will return all objects that have the first name of "Kate." **Note:** Because there is only one argument in this example, it is surrounded with parentheses for illustration.
`&`	And	Use `&` when you have more than one condition and you want all conditions to be true. For example, if you want to find all of the people that have the first name of Kate and live in Austin, you would use the example in the right-hand column.	`(&(givenName=Kate)(l=Austin))`
`!`	Not	The `!` operator is used to exclude objects that have a certain attribute. If you need to find all objects except those that have the first name of Kate, you would use the example in the right-hand column. This would find all objects that do not have the first name of Kate. **Note:** The `!` operator goes directly in front of the argument and inside the argument's set of parentheses.	`(!givenName=Kate)` **Note:** Because there is only one argument in this example, it is surrounded with parentheses for illustration.
`*`	Wildcard	Use the * operator to represent a value that could be equal to anything. If you	`(title=*)`

		wanted to find all objects that have a value for title, you would then use the example in the right-hand column. This would return all objects that have the title attribute populated with any value.	
*	Wildcard	This would apply to all objects whose first name starts with "Ka."	(givenName=Ka*)

<u>Advanced Examples of LDAP Syntax:</u>

- You need a filter to find all objects that are in NYC or Austin, and that have the first name of "Kate." This would be:

  ```
  (&(givenName=Kate)(|(l=NYC)(l=Austin)))
  ```

- You have received 9,360 events in the Application log and you need to find all of the objects that are causing this logging event. In this case, you need to find all of the disabled users `(msExchUserAccountControl=2)` that do not have a value for `msExchMasterAccountSID`. This would be:

  ```
  (&(msExchUserAccountControl=2)(!msExchMasterAccountSID=*))
  ```

  Note: Using the `!` operator with the * operator will look for objects where that attribute is not set to anything.

The LDAP User Experience Monitor

<u>Use the LDAP Monitor to test that:</u>

- An LDAP client can open a connection with an LDAP server.
- Specified objects exist and can be located in the LDAP catalogue.
- The server responds within a required time frame.

The LDAP Monitor supports LDAP version 2, which is the most commonly supported version. Most LDAP version 3 servers will support LDAP version 2 client requests.

<u>How this Monitor Works:</u>

1. It creates an instance of the LDAP Connection class using the specified directory identifier.
2. It configures the connection which can be encrypted.
3. It establishes an LDAP connection and passes user authentication with the “bind” operation.
4. It prepares and sends an LDAP search request. *LDAP Search Root* and *LDAP Filter* monitor settings are used.
5. It reads and proceeds with an LDAP response. The monitor returns the number of found entries as statistic data. It also calculates and shows the server response time.

LDAP User Experience Monitor

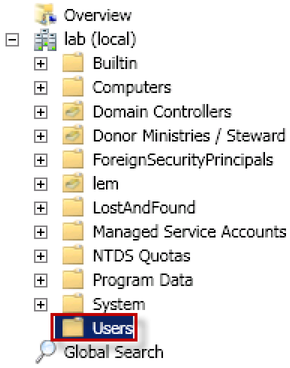
Prerequisites

The target LDAP server IP address and name must be successfully DNS resolved from the SolarWinds server.

Fields Defined

The fields highlighted below are unique to this monitor, therefore, only they are defined immediately following this illustration:

- **Port Number:** Port **389** is the default port for a non-encrypted connection. Use port **636** if you use encryption.
- **Encryption Method:** Choose either *SSL* or *StartTLS* to encrypt your data.
- **Authentication Method:** Below are the five available options:
    - **Anonymous:** Indicates that the connection should be made without passing credentials.
    - **Simple:** Indicates that basic authentication should be used with the connection. This only requires a valid username and password.
    - **NTLM:** Indicates that Windows NT Challenge/Response (NTLM) authentication should be used on the connection. This requires user name, password, and domain (Realm).
    - **Kerberos:** Indicates that Kerberos authentication should be used on the connection. This requires a user name, password and domain (Realm).
    - **Negotiate:** Indicates that Microsoft's Negotiate authentication should be used with the connection. This only requires a valid username and password.
- **Realm** (User Domain): This is the user's domain (e.g. for DC=solarwinds,DC=com the realm would be solarwinds).
- **LDAP Search Root:** This is the place in the LDAP tree that you want to start your search. (e.g. The *Users* folder, as illustrated below):



This example is based on the Active Directory Domain Controller *lab.rio*. The LDAP search root would be `CN=Users,DC=lab,DC=rio` because the context name *Folder* is *Users*, and the domain *DC* is *lab.rio*.

In general, you may specify just the domain root (`DC=lab,DC=rio`) to begin a search because the monitor always applies the *SearchScope.Subtree* request option. The query will search the entire domain tree for the requested object from the specified root.

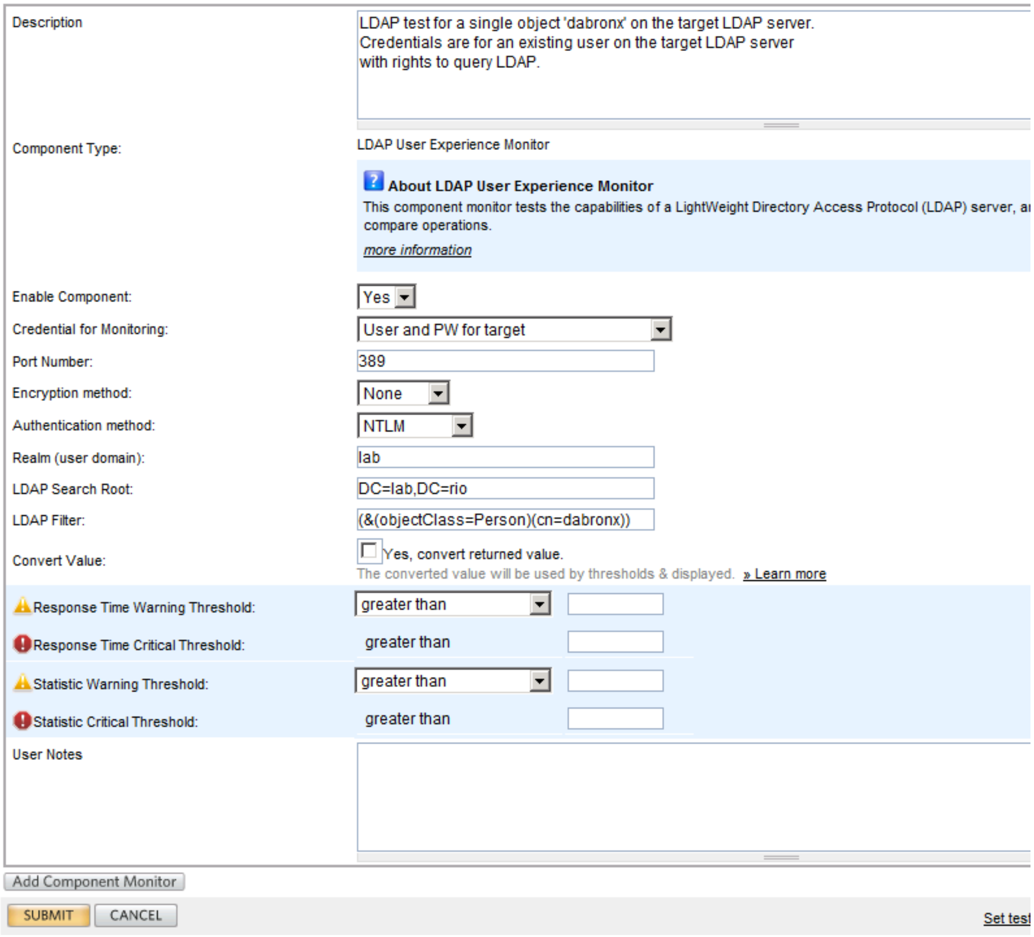
- **LDAP Filter:** This describes the search condition for an LDAP query and matching attributes.

Credentials

Credentials should be used without the domain because the *Realm* field is defined with this information.

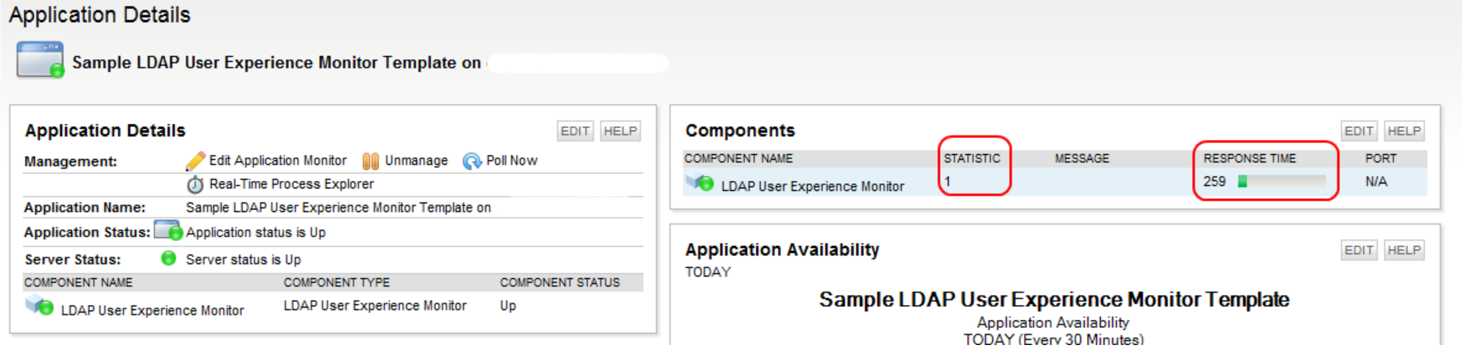
LDAP Monitor Statistics.

The following illustrates typical field entries for a working LDAP User Experience monitor within SAM:



Description	LDAP test for a single object 'dabronx' on the target LDAP server. Credentials are for an existing user on the target LDAP server with rights to query LDAP.	
Component Type:	LDAP User Experience Monitor **About LDAP User Experience Monitor** This component monitor tests the capabilities of a LightWeight Directory Access Protocol (LDAP) server, a compare operations. more information	
Enable Component:	Yes	
Credential for Monitoring:	User and PW for target	
Port Number:	389	
Encryption method:	None	
Authentication method:	NTLM	
Realm (user domain):	lab	
LDAP Search Root:	DC=lab,DC=rio	
LDAP Filter:	(&(objectClass=Person)(cn=dabronx))	
Convert Value:	□ Yes, convert returned value. The converted value will be used by thresholds & displayed. » Learn more	
Response Time Warning Threshold:	greater than	
Response Time Critical Threshold:	greater than	
Statistic Warning Threshold:	greater than	
Statistic Critical Threshold:	greater than	
User Notes		

In the illustration below, the *Statistic* and the *Response Time* values are highlighted. A statistic of 1 is returned indicating that 1 user was found that matched the filter criteria. This query took 259 milliseconds, as indicated by the *Response Time* value of 259. A **Message** is not returned by this monitor.



Application Details

Sample LDAP User Experience Monitor Template on

Application Details

Management:	Edit Application Monitor Unmanage Poll Now Real-Time Process Explorer
Application Name:	Sample LDAP User Experience Monitor Template on
Application Status:	Application status is Up
Server Status:	Server status is Up

COMPONENT NAME	COMPONENT TYPE	COMPONENT STATUS
LDAP User Experience Monitor	LDAP User Experience Monitor	Up

Components

COMPONENT NAME	STATISTIC	MESSAGE	RESPONSE TIME	PORT
LDAP User Experience Monitor	1		259	N/A

Application Availability

TODAY

Sample LDAP User Experience Monitor Template

Application Availability

TODAY (Every 30 Minutes)