

LDAP Replication

Insight Server now supports the authentication of accounts against third party LDAP servers like Active Directory for authentication. These accounts are also replicated into Insight Servers local OpenLDAP instance so that the users can gain full access to all available features. The accounts that are created are read only and can not be modified through the web admin interface.

It is important to note that although the account information is replicated locally, the password information is not. Passwords are not extracted and replicated between servers. Whenever an incoming authentication request is made against a replicated account, the SASL Auth Daemon redirects the authentication attempt to the third party LDAP server. Successful authentication is determined via the success of an LDAP bind using the credentials provided.

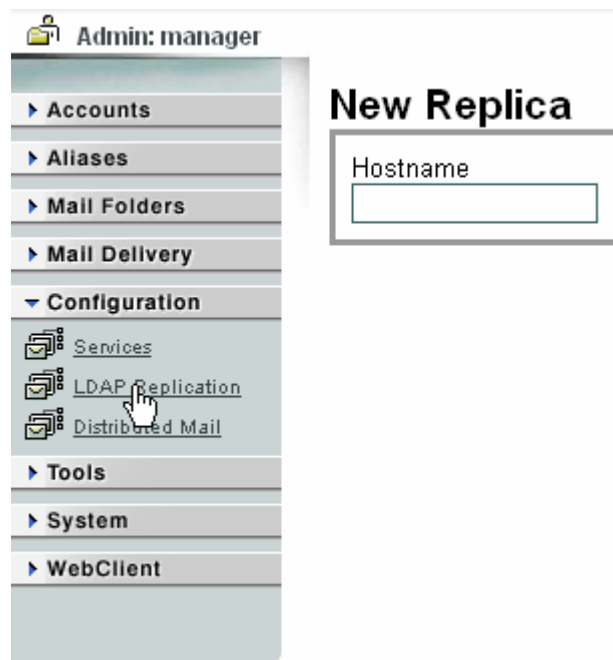


Figure 64 – LDAP Replication

When setting up the replication sequence, an account must be specified for use when binding to the LDAP service. This account must have access to the full schema for Insight Server to perform an ldapsearch of the entire server. In the following example, we will use the Administrator account for this purpose.

Let's examine the information needed when adding an Active Directory server as a New Replica.

New Replica

Hostname <input type="text"/>	Port <input type="text"/>	Administrative DN <input type="text"/>	Password <input type="text"/>	LDAP Suffix <input type="text"/>	<input type="button" value="Add"/>
----------------------------------	------------------------------	---	----------------------------------	-------------------------------------	------------------------------------

Figure 65 – New Replica

Hostname	IP Address or Fully Qualified Domain Name (FQDN)
Port	Default of 389 for LDAP and 3268 for Active Directory
Administrative DN	This is the Bind DN used during replication
Password	This is the Bind Password used during replication
LDAP Suffix	Default search string used during replication

Now let's examine the steps we use to determine the information used for the New Replica entry. The Hostname must be the IP Address or FQDN, and in our case, it will be "192.168.30.123". Since we are adding an Active Directory server as our Replica, we will be using port "3268" for our example. If we were setting up an LDAP server using a Samba schema as our New Replica partner, we would most likely be using port 389.

Now that we have our connection information, we will determine our Administrative DN and LDAP Suffix to complete our example New Replica entry. To do this, open a shell on the server as root. The following command is used to determine administrator accounts full DN as well as the LDAP Suffix.

```
# /opt/insight/bin/ldapsearch -x -h [ip address of the ldap server] -p 3268|more
```

Here is the initial result listing of this command in our example configuration.

```
[root@mail2 root]# /opt/insight/bin/ldapsearch -x -h 192.168.30.123 -p 3268|more
# extended LDIF
#
# LDAPv3
# base <> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#
# example.net
dn: DC=example,DC=net
...

```

Given the 'dn:' results from our example configuration, we now know that our LDAP Suffix will be "CN=Users, DC=example,DC=net".

Using the LDAP Suffix, we can then determine the administrator accounts full DN by appending "CN=Administrator," to the LDAP Suffix.

The Administrator DN is now "CN=Administrator,CN=Users, DC=example,DC=net". To validate the information from these results, you can use the following command.

```
# /opt/insight/bin/ldapsearch -x -h [ip address of the ldap server] -p [port] \  
-D "[Bind DN]" -w [Bind Password] -b '[LDAP Suffix]'
```

This command will produce a user listing from LDAP that will be used by the replication routine for creating the accounts. Below is the command line from our example configuration and the initial results.

```
[root@mail2 root]# /opt/insight/bin/ldapsearch -x -h 192.168.30.123 -p 3268 \  
> -D "CN=Administrator,CN=Users,DC=example,DC=net" -w password \  
> -b 'CN=Users,DC=example,DC=net'|more  
# extended LDIF  
#  
# LDAPv3  
# base <CN=Users,DC=example,DC=net> with scope sub  
# filter: (objectclass=*)  
# requesting: ALL  
#  
  
# Users, example.net  
dn: CN=Users,DC=example,DC=net  
cn: Users  
description: Default container for upgraded user accounts  
dSCorePropagationData: 20050411163721.0Z  
dSCorePropagationData: 16010101000001.0Z  
instanceType: 4  
distinguishedName: CN=Users,DC=example,DC=net  
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=example,DC=net
```

We can now populate the fields in the New Replica entry with this information then select Add.