Authenticating Users With Active Directory And LDAP In Nagios Log Server 2024

Purpose

This document describes how to use Active Directory (AD) or LDAP to authenticate users in Nagios Log Server.

Prerequisites

You will need the following prerequisites in order to follow the documentation:

- Nagios Log Server installation
- A separate Microsoft Windows-based AD infrastructure that is accessible to the Nagios Log Server machine
    - OR
- A separate LDAP infrastructure (like OpenLDAP) that is accessible to the Nagios Log Server machine

Cluster Considerations

Nagios Log Server is a clustered application, it consists of one or more instances of Nagios Log Server. Being a clustered application, it does not matter which instance a user connects to when logging in to the web interface. With this in mind, each instance of Nagios Log Server will need to be able to communicate with the AD or LDAP servers when authenticating user credentials.

Nagios Log Server DNS Resolution

It is assumed that the DNS settings for each of your Nagios Log Server instances use DNS servers that are:

- Domain Controllers (DC) in your AD domain
    - OR
- Capable of resolving the DNS entries used to contact your LDAP server(s)

If you are having issues, you can edit the `resolv.conf` file to use a DNS server within the AD infrastructure as the primary name server.

- Edit the `resolv.conf` file in a text editor:

```
vi /etc/resolv.conf
```

- Before all other lines starting with `nameserver`, enter the following:

```
nameserver [IP address of DNS server]
```

Caching options in PHP may prevent changes to the `resolv.conf` from taking effect and require restarting the Apache service. If you do edit the file, you will need to restart the Apache web server:

RHEL | CentOS | Oracle Linux

```
systemctl restart httpd.service
```

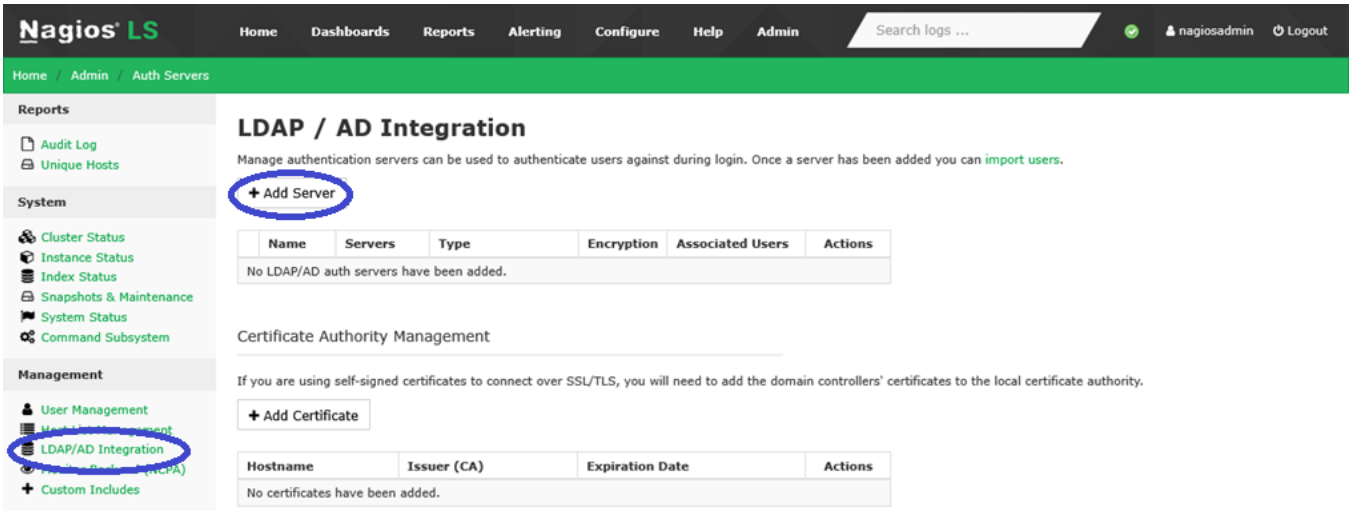
Debian | Ubuntu

```
systemctl restart apache2.service
```

Be aware that the `/etc/resolv.conf` file can be automatically overwritten by the networking stack in RHEL/CentOS/Oracle. Please consult the RHEL/CentOS/Oracle documentation for more information on correctly configuring the DNS servers for Linux.

Configuring The Authentication Servers

First you must configure the Authentication Server(s) that Nagios Log Server will use. Navigate to **Admin > Management > LDAP/AD Integration**.

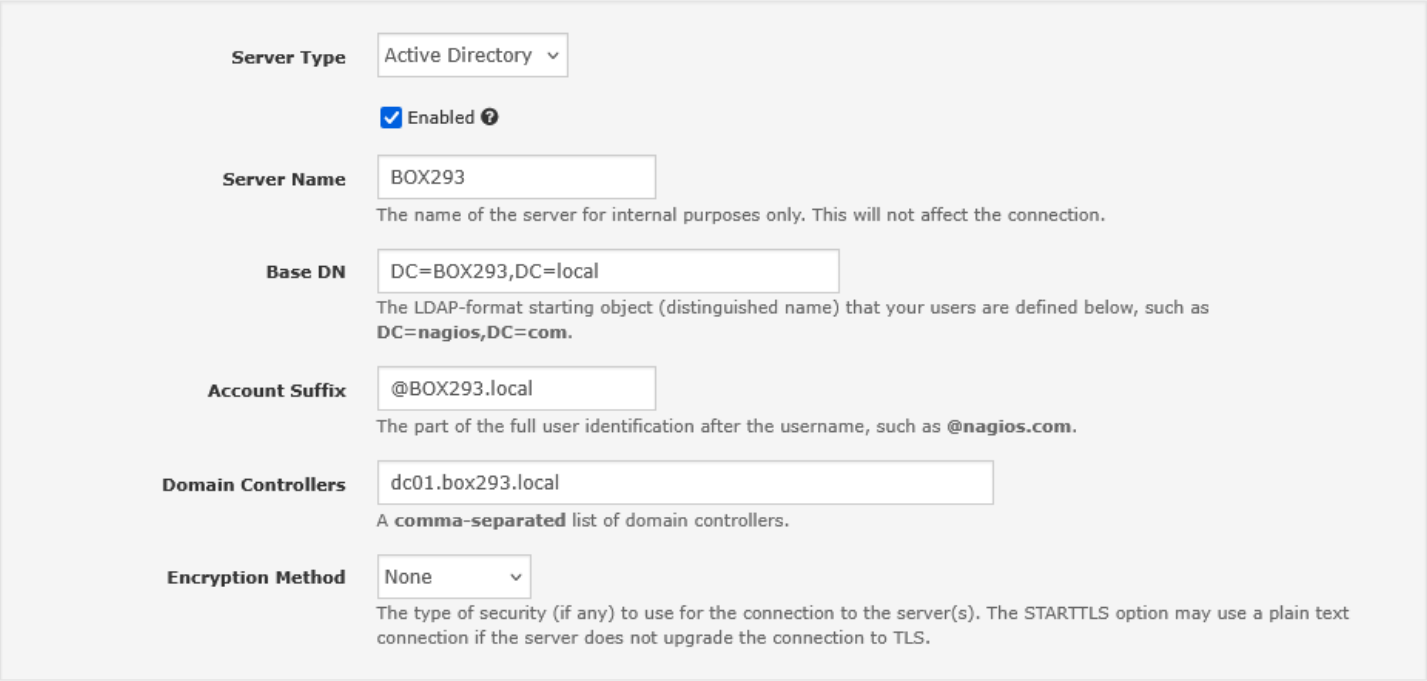


To add an Authentication Server, click the **Add Server** button. There are different options for Active Directory and LDAP.

Active Directory

You will need to provide the following details:

- **Server Type**: **Active Directory**
- **Enabled**: Checked
- **Server Name**:
  - Provide a name to associate with this authentication method.
- **Base DN**:
  - An LDAP formatted string where the users are located.
  - Example: `DC=BOX293,DC=local`
- **Account Suffix**:
  - An `@your-domain.suffix` (the part of the full user identification after the username).
  - Example `@BOX293.local`
- **Domain Controllers**:
  - A comma separated list of DC servers that Nagios Log Server can use to authenticate against. This can be a combination of IP addresses, short names, and fully qualified domain names.
  - **Note:** When using SSL or TLS for security, it is important that these entries match the Common Name (CN) in the SSL/TLS certificate that these DCs will present to the Nagios Log Server instance.
  - Example: `dc01.box293.local,dc02.box293.local`
- **Encryption Method**:
  - Select the security method (or not) to use. This guide will choose **None**.
  - If you are in a domain forest that has been raised to a functional level of 2012, then TLS is needed along with additional steps in the following guide: Using SSL with AD and LDAP.
  - If SSL or TLS is required, then please refer to the same guide.



Once completed click the **Create Server** button.

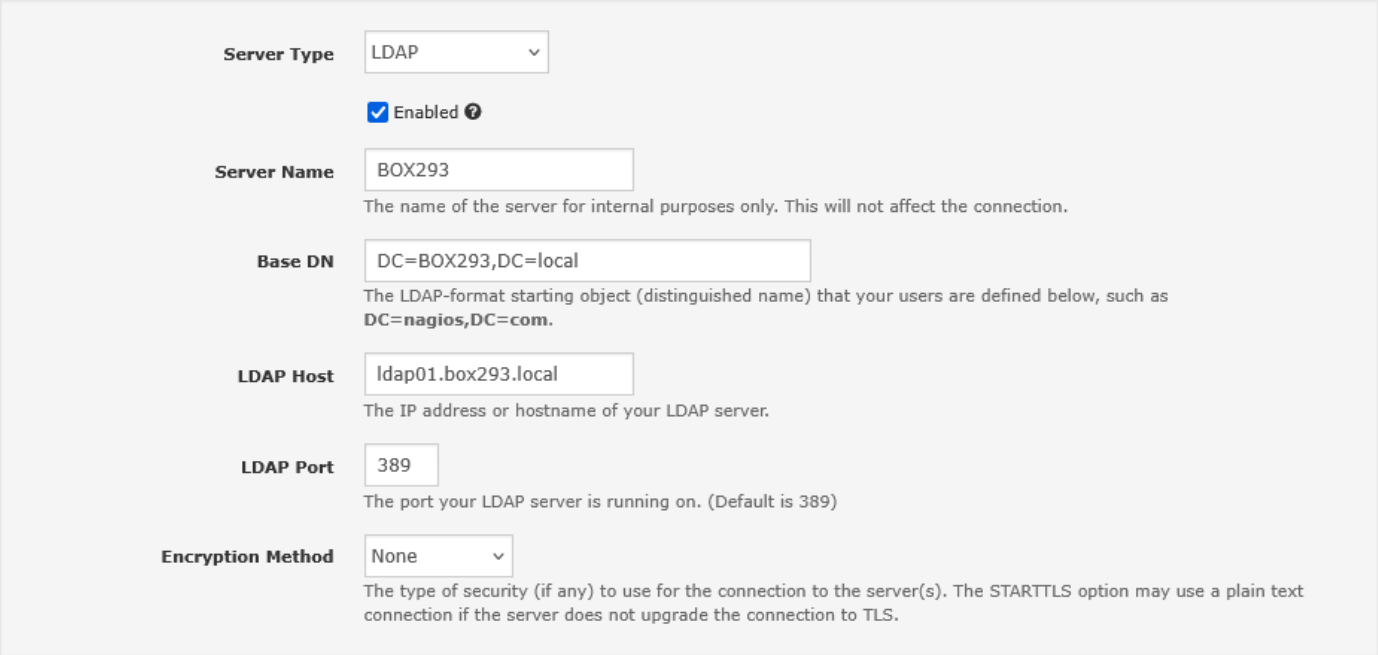
You can now proceed to the Importing Users section.

LDAP

You will need to provide the following details:

- **Server Type: LDAP**
- **Enabled**: Checked
- **Server Name**:
  - Provide a name to associate with this authentication method.
- **Base DN:**
  - An LDAP formatted string where the users are located.
  - Example: `dc=box293,dc=local`

- **LDAP Host:**
  - The LDAP server that Nagios Log Server can use to authenticate against. This can be an IP address, short name or fully qualified domain name.
  - Example: `ldap01.box293.local`
  - **Note:** When using SSL or TLS for security, it is important that this entry matches the Common Name (CN) in the SSL/TLS certificate that this LDAP server will present to the Nagios Log Server instance.
- **LDAP Port:**
  - The TCP network port used to communicate with the LDAP server.
  - Example: `389`
- **Encryption Method:**
  - Select the security method (or not) to use. This guide will choose **None**.
  - If SSL or TLS is required then please refer to the Using SSL with AD and LDAP documentation.



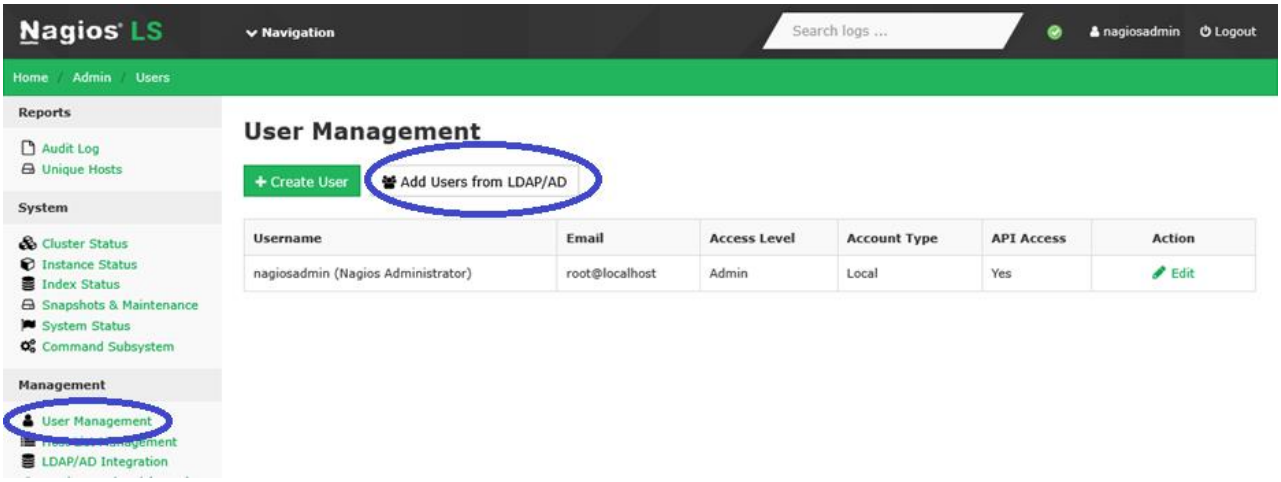
Once completed, click the **Create Server** button.

You can now proceed to the Importing Users section.

Importing Users

The next step is to import users from Active Directory or LDAP. Once the user has been imported, Nagios Log Server will query the DCs or LDAP server each time the user logs in to validate credentials. The following steps are the same for Active Directory or LDAP.

1. Navigate to **Admin > Management > User Management** and click the **Add Users from LDAP/AD** button.



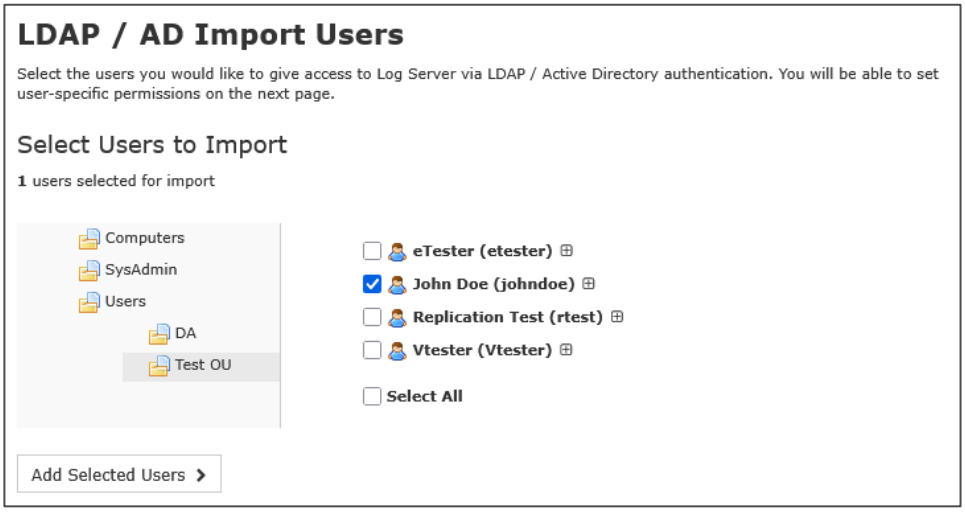
2. Select the authentication server(s) you previously defined and provide credentials to connect to the server(s).

   The account credentials you are providing here are only required to authenticate against AD / LDAP to retrieve the directory contents. They are not saved or used in the actual user authentication.

3. Click **Next.**

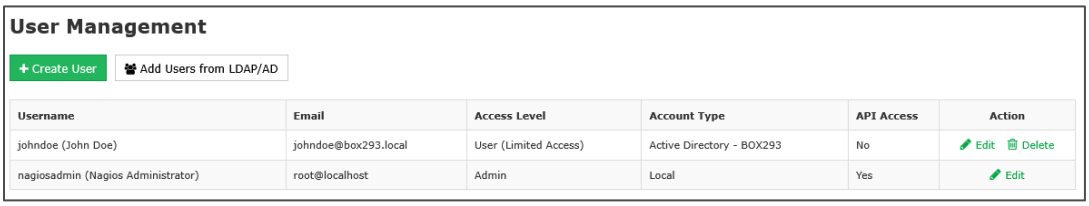
4. Once you've successfully authenticated, you'll be presented with the node of your directory tree (relative to the Base DN that was defined).

   In the screenshot, the **Test OU** node is selected. The user **John Doe** has been selected to import, and this is summarized at the top of the screen.



5. When you've chosen all the users to import, click the **Add Selected Users** button.
6. On the next screen, you'll see a list of users selected for import along with a summary of how they will be imported. Ensure all required fields (marked with an *) are defined, then click the **Create Users** button to proceed.

7. The user accounts will be imported into Nagios Log Server, and once complete, you will be returned to the **User Management** screen.

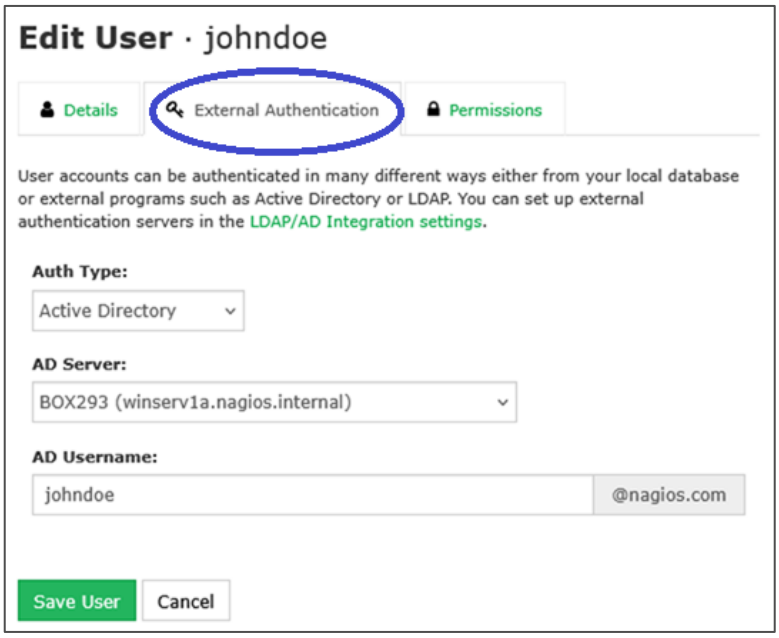


This completes importing users into Nagios Log Server from Active Directory/LDAP.

Linking Existing Nagios Log Server Users to Active Directory Users

If you already have Nagios Log Server users that have been created, you can easily link these local accounts to Active Directory accounts.

1. Navigate to **Admin > Management > User Management**.
2. Click the **Edit** link for the user you want to update, the settings are on the **External Authentication** tab:
    - **Auth Type: Active Directory**
    - **AD Server:** Select the authentication server(s) you previously defined
    - **AD Username:**
        - Type the username for this user as it is configured in Active Directory
        - Example: `johndoe`

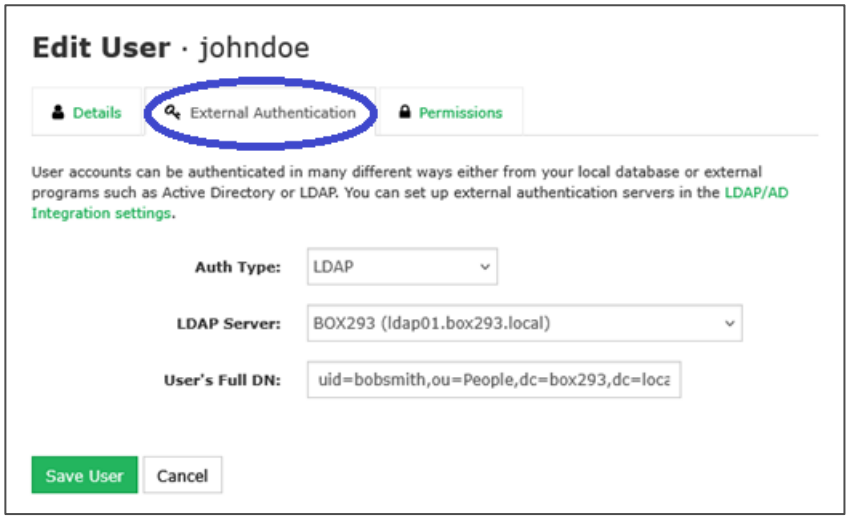


3. Click the **Save User** button to save the changes.
4. Once these changes have been made, the existing Nagios Log Server user will be able to log in using their Active Directory credentials.

Linking Existing Nagios Log Server Users to LDAP Users

If you already have Nagios Log Server users that have been created, you can easily link these local accounts to LDAP accounts.

1. Navigate to **Admin > Management > User Management**.
2. Click the **Edit** link for the user you want to update, the settings are on the **External Authentication** tab:
    - **Auth Type: LDAP**
    - **LDAP Server:** Select the authentication server you previously defined
    - **Users Full DN:**
        - Type the full distinguished name (DN) for this user as it is defined in LDAP
        - Example: `uid=bobsmith,ou=People,dc=box293,dc=local`



3. Click the **Save User** button to save the changes.
4. Once these changes have been made, the existing Nagios Log Server user will be able to log in using their LDAP credentials.

LDAP Account Requirements

The following details demonstrate the required object classes and attributes that need to exist for an LDAP user. If these attributes do not exist it is likely that they will not appear in the list of users when performing an import from your LDAP server.

```
dn: uid=bobsmith,ou=People,dc=box293,dc=local
givenName: Bob
sn: Smith
cn: Bob Smith
uidNumber: 10004
gidNumber: 10004
mail: bobsmith@box293.local
homeDirectory: /home/bobsmith
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
```

Finishing Up

This completes the documentation on using Active Directory and LDAP to authenticate users in Nagios Log Server. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library