Authenticating and Importing Users with Active Directory and LDAP



Purpose

This document describes how to integrate Nagios Network Analyzer with Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) to allow user authentication and validation with an AD or LDAP infrastructure through the Nagios Network Analyzer interface. This is

helpful for system administrators by simplifying user management of large infrastructures and standardizing credentials needed for Network Analyzer by allowing users to authenticate with their AD or LDAP credentials.

Target Audience

This is intended for Nagios administrators who want to allow users to authenticate with their Windows AD or LDAP credentials when logging into Nagios Network Analyzer.

Prerequisites

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

- A separate Microsoft Windows-based AD infrastructure that is accessible to the Nagios Network Analyzer machine
 - o OR
- A separate LDAP infrastructure (like OpenLDAP) that is accessible to the Nagios Network Analyzer machine

Nagios Network Analyzer Server DNS Resolution

It is assumed that the DNS settings for your Nagios Network Analyzer server use DNS servers that are:

- Domain Controllers (DC) in your AD domain
 - o 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

Authenticating and Importing Users with Active Directory and LDAP

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:
 - o 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:

RHEL7 + | CentOS 7 + | Oracle Linux 7 +

systemctl restart httpd.service

Debian | Ubuntu 16/18/20

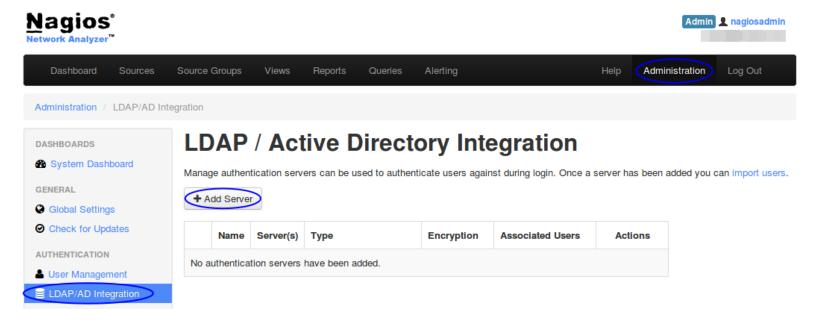
systemctl restart apache2.service

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

Configuring The Authentication Servers

First you must define the Authentication Server(s) that Nagios Network Analyzer will use. Navigate to **Administration > Authentication** and click **LDAP/AD Integration**.

Authenticating and Importing Users with Active Directory and LDAP



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

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:

Authenticating and Importing Users with Active Directory and LDAP

A comma separated list of DC servers that Nagios Network Analyzer 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 Network Analyzer server.

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: <u>Using SSL with AD and LDAP</u>.

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

Authenticating and Importing Users with Active Directory and 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 Network Analyzer can use to authenticate against. This can be an IP address, short name or fully qualified domain name.

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 Network Analyzer server.

Example: ldap01.box293.local

LDAP Port:

The TCP network port used to communicate with the LDAP server.

Example: 389

Encryption Method:

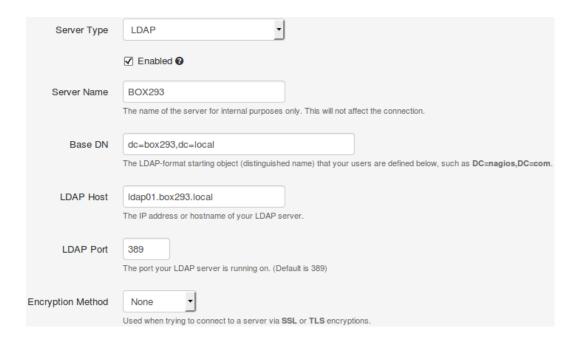
Select the security method (or not) to use. This guide will choose **None**.

If SSL or TLS is required then please refer to the <u>Using SSL with AD and LDAP</u> documentation.

Authenticating and Importing Users with Active Directory and LDAP

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

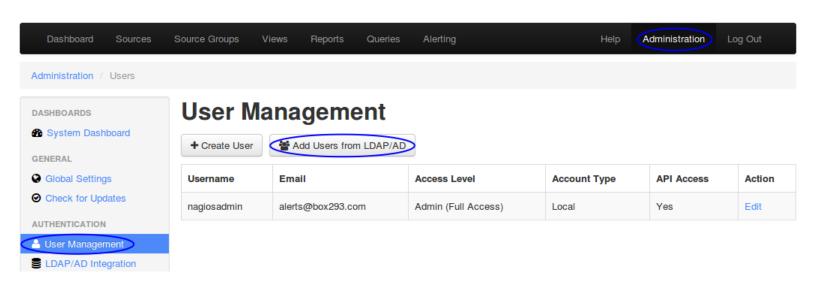
You can now proceed to the Importing Users section.



Importing Users

The next step is to import users from Active Directory or LDAP. Once the user has been imported, Nagios Network Analyzer 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.

Navigate to Administration > Authentication > User Management and click Add users from LDAP/AD.



Authenticating and Importing Users with Active Directory and LDAP

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.

LDAP / Active Directory Import Users

Log into your LDAP / Active Directory administrator or privileged account to be able to import users directly into Network Analyzer.

Administrator	
•••••	
Active Directory - dc01.box293.loca	•
Next >	

Click Next.

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 to the right you can see the Users node has been selected.

The user **John Smith** has been selected to import and you can see it summarizes this at the top of the screen.

When you've chosen all the users to import, click the **Add Selected**Users button.

LDAP / Active Directory Import Users

Select the users you would like to give access to Network Analyzer via LDAP / Active Directory authentication. You will be able to set user-specific permissions on the next page.

Select Users to Import 1 users selected for import Company □ 🚨 001 Admin User (admin user 001) Œ Computers ☐ Administrator (Administrator) ⊞ Domain Controllers □ 🚨 backup user (backup user) ⊞ □ A DefaultAccount (DefaultAccount) ⊕ Microsoft Exchange Security Groups Microsoft Exchange System Objects (SM_f464c3ac561b49529) Allowed RODC Password Replication Group ☐ A FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042 (SM bca34b6b3b6840718) ⊕ A Cert Publishers A Cloneable Domain Controllers A Denied RODC Password Replication Group △ DnsAdmins DnsUpdateProxy □ A Nagios Alerts (nagios alerts) ⊕ Admins Domain Admins □ A snapshot user (snapshot user) ⊕ A Domain Computers SystemMailbox{1f05a927-9d44-4d09-8eb2-f69e9857f89f} (SM_2e6ef0ad63fb41be8) ⊕ A Domain Controllers SystemMailbox{2CE34405-31BE-455D-89D7-A7C7DA7A0DAA} A Domain Guests (SM_c57260936d894caeb) A Domain Users A Enterprise Admins SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9} (SM_a5018e92238e419eb) A Enterprise Key Admins SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c} (SM 9d257a9a28ba4ad79) A Enterprise Read-only Domain Controllers A Group Policy Creator Owners SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201} A Key Admins (SM c7a415d502bb4584a) A Protected Users SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9} (SM_5ebd7f446a964e04a) A RAS and IAS Servers A Read-only Domain Controllers ☐ Section Test User (testuser) ☐ A Schema Admins ☐ Select All

1295 Bandana Blvd N, St. Paul, MN 55108 sales@nagios.com US: 1-888-624-4671 INTL: 1-651-204-9102

Add Selected Users >

Authenticating and Importing Users with Active Directory and LDAP

On the next screen you are presented with a list of the users you are going to import and the summary of how they are going to be imported (see screenshot below).

LDAP / Active Directory Import Users

Set up the new users. Add missing information and update the account.

Fill Out New User Information

	Full Name		Username *	Email *	User Type *		API Access	Auth Type	Auth Identifier
~	John	Smith	john.smith		User	•	No •	Active Directory	john.smith@BOX293.loca

Create Users

Every user will need the required fields (marked by an *) defined before you can click the Create Users button.

Click the **Create Users** button to continue. The user accounts will now be imported into Nagios Network Analyzer. When finished you will be returned to the User Management screen.

User Management



This completes importing users into Nagios Network Analyzer from Active Directory or LDAP.

Authenticating and Importing Users with Active Directory and LDAP

Linking Existing Nagios Network Analyzer Users to Active Directory Users

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

Navigate to **Administration > Authentication > User Management**.

Click the **Edit** link for the user you want to update, the settings are under the **Authentications Setting** section:

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: jane.doe

Click the Save User button to save the changes.

Here is a screenshot of the user settings described above:

Once these changes have been made, the existing Nagios Network Analyzer user will be able to login using their Active Directory credentials.

Authentication Settings

User accounts can be authenticated in many different ways either from your local database or external programs such as Active Directory or LDAP. You can set up external authentication servers in the LDAP/AD Integration settings.

Auth Type:	Active Directory	•	
AD Server:	BOX293 (dc01.box293.local)		-
AD Username:	jane.doe		

Authenticating and Importing Users with Active Directory and LDAP

Linking Existing Nagios Network Analyzer Users to LDAP Users

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

Navigate to **Administration > Authentication > User Management**.

Click the **Edit** link for the user you want to update, the settings are under the **Authentications Setting** section:

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

Click the Save User button to save the changes.

Here is a screenshot of the user settings described above:

Once these changes have been made, the existing Nagios Network Analyzer user will be able to login using their LDAP credentials.

Authentication Settings

User accounts can be authenticated in many different ways either from your local database or external programs such as Active Directory or LDAP. You can set up external authentication servers in the LDAP/AD Integration settings.

Auth Type:	LDAP	
LDAP Server:	BOX293 (Idap01.box293.local)	•
User's Full DN:	uid=bobsmith,ou=People,dc=box293,dc=local	

Authenticating and Importing Users with Active Directory and LDAP

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 how to integrate Nagios Network Analyzer with Active Directory or LDAP to allow user authentication and validation with the Nagios Network Analyzer interface.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb