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
 - o 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
 - 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 as the primary name server.

• Edit the resolv.conf file in a text editor:

vi /etc/resolv.conf





Page 1 of 10

• 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**.

<u>N</u> agios' LS	Home Da	ashboards	Reports	Alerting	Configure	Help	Admin	s	Search logs		/ •	占 nagiosadmin	🖒 Logout
Home / Admin / Auth Servers													
Reports													
 Audit Log Unique Hosts 	LDAP /	AD In ntication server	rs can be used	on to authenticate	e users agains	t during login	Once a serve	er has bee	en added you can in	port users.			
System	+ Add Serv	er											
S Cluster Status	Name	Servers	Туре		Encryption	Associated	Users	Actions					
Instance Status	No LDAP/AD	auth servers h	ave been added	d.									
 Snapshots & Maintenance System Status Command Subsystem 	Certificate /	Authority Ma	anagement										
Management	If you are usin	ıg self-signed o	ertificates to co	onnect over SS	L/TLS, you wil	I need to add	the domain c	controllers'	certificates to the	local certificate	authority.		
Liser Management	+ Add Certi	ificate											
LDAP/AD Integration													
Contraction Bandward (mePA)	Hostname	1	Issuer (CA)		Expiration D	ate		Actions					
 Custom Includes 	No certificate	es have been ar	dded.										

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

www.nagios.com



Page 2 of 10

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:
 - \circ $\,$ An LDAP formatted string where the users are located.
 - Example: DC=B0X293, DC=local
- Account Suffix:
 - An @your-domain.suffix (the part of the full user identification after the username).
 - o Example @B0X293.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: <u>Using SSL with AD and LDAP</u>.
 - If SSL or TLS is required, then please refer to the same guide.





Page 3 of 10

Server Type	Active Directory v
	✓ Enabled Ø
Server Name	BOX293
	The name of the server for internal purposes only. This will not affect the connection.
Base DN	DC=BOX293,DC=local
	The LDAP-format starting object (distinguished name) that your users are defined below, such as DC=nagios,DC=com.
Account Suffix	@BOX293 local
Account SumA	The part of the full user identification after the username, such as @nagios.com.
Domain Controllers	dc01 box293 local
Domain Controllers	A comma-separated list of domain controllers.
Encryption Method	None
Енстурион менной	The type of security (if any) to use for the connection to the server(s). The STARTTLS option may use a plain text
	connection if the server does not upgrade the connection to TLS.

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:
 - o 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

www.nagios.com



Page 4 of 10

• 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:
 - \circ $\;$ The TCP network port used to communicate with the LDAP server.
 - o 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.

Server Type	LDAP ~
Server Name	BOX293
	The name of the server for internal purposes only. This will not affect the connection.
Base DN	DC=BOX293,DC=local
	The LDAP-format starting object (distinguished name) that your users are defined below, such as DC=nagios,DC=com.
LDAP Host	ldap01.box293.local
	The IP address or hostname of your LDAP server.
LDAP Port	389
	The port your LDAP server is running on. (Default is 389)
Encryption Method	None v
	The type of secunty (if any) to use for the connection to the server(s). The STARTTLS option may use a plain text connection if the server does not upgrade the connection to TLS.

Once completed, click the Create Server button.

You can now proceed to the Importing Users section.

www.nagios.com



Page 5 of 10

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.

<u>N</u> agios' LS	✓ Navigation		Sear	rch logs	•	🛓 nagiosadmin 🛛 Logout
Home / Admin / Users						
Reports	Harr Management					
 Audit Log Unique Hosts 	+ Create User	DAP/AD				
System						
🚯 Cluster Status	Username	Email	Access Level	Account Type	API Access	Action
 Instance Status Index Status 	nagiosadmin (Nagios Administrator)	root@localhost	Admin	Local	Yes	Sedit
Snapshots & Maintenance						
System Status Command Subsystem						
Management						
User Management						
LDAP/AD Integration						

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.

LDAP / AD Import Users
Log into your LDAP / Active Directory administrator or privileged account to be able to import users directly into Log Server.
Username
Password
Active Directory - BOX293 - dc01.box293.local v
Next >

www.nagios.com



Page 6 of 10

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.

LDAP / AD Impo	rt Users
Select the users you would like to gi user-specific permissions on the nex	ive access to Log Server via LDAP / Active Directory authentication. You will be able to set t page.
Select Users to Import 1 users selected for import	t
Computers SysAdmin Users DA Test OU	 Select All Between the start of the start o
Add Selected Users >	

- 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.

LD	AP / AD Import l	Jsers					
Set u	o the new users. Add missing informa	ation and update the acco	unt.				
Fill	Out New User Informa	tion					
	Full Name	Username *	Email Address *	User Type *	API Access	Auth Type	Auth Identifier
	John Doe	johndoe		User v	No v	Active Directory	johndoe@nagios.com
Cre	ate Users Cancel						

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

User Management					
+ Create User					
Username	Email	Access Level	Account Type	API Access	Action
johndoe (John Doe)	johndoe@box293.local	User (Limited Access)	Active Directory - BOX293	No	🖋 Edit 🗎 Delete
nagiosadmin (Nagios Administrator)	root@localhost	Admin	Local	Yes	Sedit

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

www.nagios.com



Page 7 of 10

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

La Details (
ser accounts can be authenticated in many different ways either f external programs such as Active Directory or LDAP. You can set athentication servers in the LDAP/AD Integration settings.	rom your local database up external
Active Directory	
AD Server:	
AD Server: BOX293 (winserv1a.nagios.internal)	
AD Server: BOX293 (winserv1a.nagios.internal)	

- 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

Edit User · johndo	e
Letails C External Authe	ntication Permissions
User accounts can be authenticated in programs such as Active Directory or Integration settings.	n many different ways either from your local database or external LDAP. You can set up external authentication servers in the LDAP/AD
Auth Type:	LDAP ~
LDAP Server:	BOX293 (ldap01.box293.local) v
User's Full DN:	uid=bobsmith,ou=People,dc=box293,dc=loca
Save User Cancel	

- 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.

www.nagios.com



Page 9 of 10

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

www.nagios.com



Page 10 of 10