Active Directory / LDAP - Troubleshooting Authentication Integration

Article Number: 600 | Rating: Unrated | Last Updated: Thu, Mar 26, 2020 at 12:28 PM

Overview

This KB article explains how you can troubleshoot Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) authentication issues. The troubleshooting methods are simil Nagios Log Server, Network Analyzer and XI products, hence this guide applies to them all.

It is assumed that you have already followed the existing documentation and are facing issues in getting it to work. The existing documentation is as follows:

- Nagios Log Server
  - Updated documentation coming soon, the Network Analyzer documentation is very similar and can be used.
- Nagios Network Analyzer
  - Authenticating and Importing Users with AD and LDAP
  - Using SSL with AD and LDAP
- Nagios XI
  - How to Authenticate and Import Users with Active Directory or LDAP
  - Using SSL/TLS with Active Directory / LDAP

Editing Files

In many steps of this article you will be required to edit files. This documentation will use the **vi** text editor. When using the vi editor:

- To make changes press `i` on the keyboard first to enter insert mode
- Press **`Esc`** to exit insert mode
- When you have finished, save the changes in vi by typing **`:wq`** and press Enter

Enable Debug Logging

Enabling debug logging can provide a lot of information available about the connections being made and errors that can help identify the source of your problem.

Debug logging is enabled by adding the following line to the correct PHP file:

```
ldap_set_option(NULL, LDAP_OPT_DEBUG_LEVEL, 7);
```

The file that this line needs to be added to is different in each product.

Nagios Log Server

The file the line needs to be added to is `/var/www/html/nagioslogserver/application/helpers/ldap_ad_helper.php` after the `create_auth_connection` function oper bracket (line 82).

Open the file in vi by executing the following command:

```
vi /var/www/html/nagioslogserver/application/helpers/ldap_ad_helper.php
```

Make the change as per the following example:

```
function create_auth_connection()
{
    ldap_set_option(NULL, LDAP_OPT_DEBUG_LEVEL, 7);
    $ci =& get_instance();
```

Nagios Network Analyzer

The file the line needs to be added to is `/var/www/html/nagiosna/application/helpers/ldap_ad_helper.php` after the `create_auth_connection` function open curly bra 71).

Open the file in vi by executing the following command:

```
vi /var/www/html/nagiosna/application/helpers/ldap_ad_helper.php
```

Make the change as per the following example:

```
function create_auth_connection()
{
    ldap_set_option(NULL, LDAP_OPT_DEBUG_LEVEL, 7);
```

```
    $ci =& get_instance();
```

Nagios XI

The file the line needs to be added to is `/usr/local/nagiosxi/html/includes/components/ldap_ad_integration/ldap_ad_integration.inc.php` after the `create_auth_conn_obj` function open curly bracket (line 208).

Open the file in vi by executing the following command:

```
/usr/local/nagiosxi/html/includes/components/ldap_ad_integration/ldap_ad_integration.inc.php
```

Make the change as per the following example:

```
function create_auth_conn_obj($server_id='')
{
    ldap_set_option(NULL, LDAP_OPT_DEBUG_LEVEL, 7);
    // Get our settings
```

Once the line is added, debug logging will appear in the Apache `error_log` which is located in `/var/log/httpd/`. You can watch this log by executing the following command:

```
tail -f /var/log/httpd/error_log /var/log/httpd/ssl_error_log
```

The following troubleshooting techniques will use the debug logging to help diagnose your issue.

Credential Problems

In Nagios Log Server, Nagios Network Analyzer and Nagios XI you can import users from AD / LDAP. The first screen you are presented with is to select your authentication server an credentials to connect.

The account credentials you are providing are only required to authenticate against AD / LDAP to retrieve the directory contents. They are not saved or used in the actual user authent Make sure the account you provide has sufficient privileges to query the contents of AD / LDAP, this is a common cause of not being able to retrieve all the AD / LDAP objects.

If your credentials are incorrect or there is a configuration issue you will not be able to proceed past this step. To get further details about the problem:

- Enabling the debug logging and watch the Apache `error_log` as explained in the Enable Debug Logging section.
- Click the Next button to generate the error
- Review the debug logging generated

CA Certificate Not Loaded

If you have selected SSL or TLS for security / encryption then you will need to have the correct Certificate Authority (CA) certificate loaded into the Nagios server. The following DEBUG that the "Peer's Certificate issuer is not recognized".

```
attempting to connect:
connect success
TLS: certificate [CN=DC01.BOX293.local] is not valid - error -8179:Peer's Certificate issuer is not recognized..
TLS: error: connect - force handshake failure: errno 0 - moznss error -8179
TLS: can't connect: TLS error -8179:Peer's Certificate issuer is not recognized..
ldap_err2string
```

The "Peer" is the AD / LDAP server being contacted. This server will present the Nagios server with a certificate to validate it's authenticity. However in this case the Nagios server do the CA certificate that generated the peer certificate, so it has no way of validating the certificate.

The solution is to upload the CA certificate to the Nagios Server. Steps on how to do this as well as a detailed explanation are in the following documentation:

- Nagios Log Server
    - Updated documentation coming soon, the Network Analyzer documentation is very similar and can be used.
- Nagios Network Analyzer
    - Using SSL with AD and LDAP
- Nagios XI
    - Using SSL/TLS with Active Directory / LDAP

Here is output from the debug log when the CA certificate exists and the peer's certificate was validated:

```
attempting to connect:
connect success
TLS: certificate [CN=DC01.BOX293.local] is valid
TLS certificate verification: subject: CN=DC01.BOX293.local, issuer: CN=BOX293-DC02-CA,DC=BOX293,DC=local, cipher: AES-256, security le
```

```
secret key bits: 256, total key bits: 256, cache hits: 0, cache misses: 0, cache not reusable: 0
ldap_open_defconn: successful
```

Hostname Does Not Match Common Name (CN)

This problem applies if you have selected SSL or TLS for security / encryption.

The following DEBUG log reports that the "hostname (xxxx) does not match common name in certificate (yyyyy)".

```
attempting to connect:
connect success
TLS: certificate [CN=DC01.BOX293.local] is valid
TLS certificate verification: subject: CN=DC01.BOX293.local, issuer: CN=BOX293-DC02-CA,DC=BOX293,DC=local, cipher: AES-256, security le
secret key bits: 256, total key bits: 256, cache hits: 0, cache misses: 0, cache not reusable: 0
TLS: hostname (10.25.14.51) does not match common name in certificate (DC01.BOX293.local).
ldap_err2string
```

When you add your AD / LDAP servers to your Nagios server you will define them with an IP address or a DNS record. When the Nagios server contacts the AD / LDAP server, that ser present the Nagios server with a certificate to validate it's authenticity. The Nagios server checks the Common Name (CN) in that certificate against the address you configured in you settings.

In the error message above you can see that in Nagios the server address is `10.25.14.51` however the CN in the certificate is `DC01.BOX293.local`. It is important that these two otherwise authentication will fail.

The solution is to correctly configure your AD / LDAP server setting to match the CN in the certificate. This means that the Nagios server needs to be able to resolve that DNS record.

Steps on how to do this as well as a detailed explanation are in the following documentation:

- Nagios Log Server
  - Updated documentation coming soon, the Network Analyzer documentation is very similar and can be used.
- Nagios Network Analyzer
  - Authenticating and Importing Users with AD and LDAP
- Nagios XI
  - How to Authenticate and Import Users with Active Directory or LDAP

Here is output from the debug log when the CA certificate exists and the peer's certificate was validated:

```
attempting to connect:
connect success
TLS: certificate [CN=DC01.BOX293.local] is valid
TLS certificate verification: subject: CN=DC01.BOX293.local, issuer: CN=BOX293-DC02-CA,DC=BOX293,DC=local, cipher: AES-256, security le
secret key bits: 256, total key bits: 256, cache hits: 0, cache misses: 0, cache not reusable: 0
ldap_open_defconn: successful
```

No Users Returned

When you are on the **Select Users to Import** page there are no users displayed. This problem can be one of two issues.

1) Account does not have enough privileges to obtain a list of users

The first screen you are presented with is to select your authentication server and provide credentials to connect. The account credentials you are providing are required to authentic AD / LDAP to retrieve the directory contents. Make sure the account you provide has sufficient privileges to query the contents of AD / LDAP, this is a common cause of not being able all the AD / LDAP objects.

2) LDAP Account Type Not Detected

In some Nagios products the LDAP users are not correctly detected. Nagios XI does not exhibit this problem as it has a more recent and improved version of the integration compone Nagios Log Server and Network Analyzer there is a simple fix for this by modifying the code to include the addition user types.

Here is the code from Nagios XI, it is in the `/usr/local/nagiosxi/html/includes/components/ldap_ad_integration/index.php` file at line 700:

```
$units = array('person', 'inetorgperson', 'organizationalperson', 'shadowaccount', 'posixaccount');
```

In **Nagios Log Server** the file is `/var/www/html/nagioslogserver/application/helpers/ldap_ad_helper.php` and the change needs to be made to line 225:

```
if ($type == "person" || $type == "inetOrgPerson") {
```

Change it to:

```
if ($type == "person" || $type == "inetOrgPerson" || $type == "organizationalPerson" || $type == "shadowAccount" || $type == "posixAcco
```

Once the change has been made you should see the user accounts on the Import page and be able to select and add the users.

In **Nagios Network Analyzer** the file is `/var/www/html/nagiosna/application/helpers/ldap_ad_helper.php` and the change needs to be made to line 226:

```
if ($type == "person" || $type == "inetOrgPerson") {
```

Change it to:

Change it to:

```
if ($type == "person" || $type == "inetOrgPerson" || $type == "organizationalPerson" || $type == "shadowAccount" || $type == "posixAcco
```

Once the change has been made you should see the user accounts on the Import page and be able to select and add the users.

Not All Active Directory Users Are Listed

When you are on the **Select Users to Import** page, not all of your Active Directory users are displayed, most likely only `1000` are shown. This problem has to do with a hard limit de this limit defines how many results can be returned when performing a query. This problem does not affect authenticating users against AD, it simply limits the amount of users displa **Select Users to Import** page.

Solution 1

When you don't have many users to add, or your domain admins don't allow solution 2, you can manually define the directory settings for each user.

The first step is to manually add your users to the Nagios product. Using Nagios XI as an example please refer to the Understanding User Rights documentation.

After adding your users, you will need to edit each user individually and define the:

- Auth Type
- Auth Server
- Their full distinguished name (DN) in the User's Full DN field

Using Nagios XI as an example, refer to the How to Authenticate and Import Users with Active Directory or LDAP documentation, specifically the **Linking Existing Nagios XI Users Directory Users** section.

Solution 2

This solution is to increase this limit by performing the following steps. In the following example you will need to replace `dc01.box293.local` with the name of your domain controlle example will increase the limit to `5000`. This change only needs to be performed on one DC, it is a change to the domain policy and takes affect immediately against all DCs.

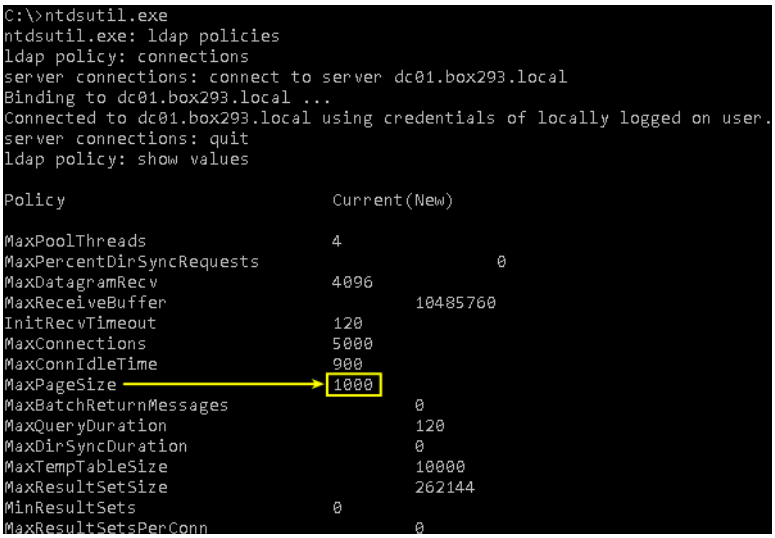
On your DC open a command prompt with Administrative rights and execute the following commands ... `[enter]` means to press the Enter key on your keyboard:

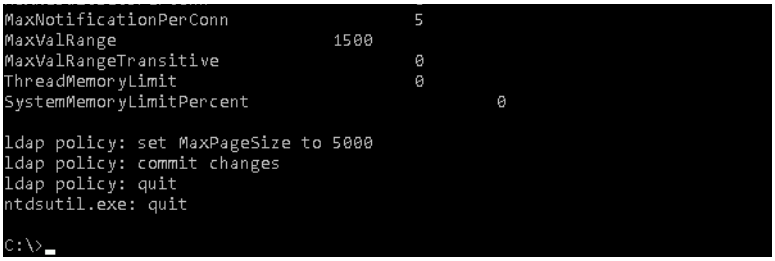
```
ntdsutil.exe [enter]
ldap policies [enter]
connections [enter]
connect to server dc01.box293.local [enter]
quit [enter]
show values [enter]
```

The setting you are interested in is the `MaxPageSize` setting, mine was set to `1000` so I ran this to change it to `5000`:

```
set maxpagesize to 5000 [enter]
commit changes [enter]
quit [enter]
quit [enter]
```

Here is a screenshot that shows all the commands above with output:





In addition to the changes above your Nagios server also requires changes to PHP to allow a large number of variables. Based on the number of `5000` used above the following char will also be applied to the PHP variables shown below. If the setting does not exist in `php.ini` then simply add it. To determine the location of your `php.ini` file execute the following

```
find /etc -name php.ini
```

If there are multiple results then the one in the `apache` directory is the one that needs changing.

Open the `php.ini` file in **`vi`** and make the changes as per the following example:

```
max_input_vars = 5000
suhosin.post.max_vars = 5000
suhosin.request.max_vars = 5000
```

These settings may also need to be changed in some circumstances:

```
max_execution_time
memory_limit
```

Save the `php.ini` file and then exit vi. Execute the following command to restart the Apache web server:

RHEL 6 | CentOS 6 | Oracle Linux 6

```
service httpd restart
```

RHEL 7 | CentOS 7 | Oracle Linux 7

```
systemctl restart httpd.service
```

Ubuntu 14

```
service apache2 restart
```

Debian | Ubuntu 16/18

```
systemctl restart apache2.service
```

Once these changes have been applied the Import Users page should correctly show all of the users in AD. If you are still having problems you may need to increase the limits as the `5000` may be too small for your environment.

Final Thoughts

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/

Posted by: **tlea** - Mon, Jun 26, 2017 at 9:59 PM. This article has been viewed 5042 times.

Online URL: https://support.nagios.com/kb/article/active-directory-ldap-troubleshooting-authentication-integration-600.html