Nagios XI - How To Use CA Certificates With check_ldaps Plugin

Article Number: 525 | Rating: 5/5 from 1 votes | Last Updated: Tue, Jul 26, 2016 at 3:16 AM

Overview

This KB article shows you how to use certificate authority (CA) certificates with the `check_ldaps` plugin.

Problem

When you try and execute the `check_ldaps` plugin:

```
/usr/local/nagios/libexec/check_ldaps -H dc01.domain.local -b '' -p 636
```

The following error is produced:

```
Could not bind to the LDAP server
```

If you enable the vebose mode `-v` for the plugin:

```
/usr/local/nagios/libexec/check_ldaps -H dc01.domain.local -b '' -p 636 -v
```

The following error is produced:

```
ldap_bind: Can't contact LDAP server (-1)
    additional info: TLS error -8179:Peer's Certificate issuer is not recognized.
Could not bind to the LDAP server
```

This verbose output has indicated that the plugin did not have a CA certificate to validate the certificate.

Resolution

You need to create the CA certificate on the Nagios server and configure `openldap` to use the certificate (`check_ldaps` plugin uses `openldap`).

You will need to obtain the CA certificate from your CA and open it in a text editor, you'll be copying the contents of the certificate into a file on the Nagios XI server.

Open an SSH session to your Nagios XI server.

Create Certificate

This example will create a certificate file called `/etc/openldap/certs/windows_ca.cer` and as you can imagine this is from a Microsoft Windows server.

Execute this command:

```
vi /etc/openldap/certs/windows_ca.cer
```

This opens the vi text editor.

Press **i** on the keyboard to go into insert mode.

Paste the contents of your CA certificate into the SSH session.

Press **Escape** on the keyboard to exit insert mode.

When you pasted the text, if a blank line was added after every line you'll need to delete all of these blank lines. Simply press **dd** on your keyboard to delete a blank line.

Type **:wq** and then press Enter (this will save the file and exit vi).

Update ldap.conf

Now you need to tell `openldap` to use this certificate.

Execute this command:

```
vi /etc/openldap/ldap.conf
```

This opens the vi text editor.

Press **i** on the keyboard to go into insert mode.

Down arrow until you reach the end of the file

On a new line type the following:

```
TLS_CACERT /etc/openldap/certs/windows_ca.cer
```

Press **Escape** on the keyboard to exit insert mode.

Type **:wq** and then press Enter (this will save the file and exit vi).

Test Plugin

The `check_ldaps` plugin should now work:

```
/usr/local/nagios/libexec/check_ldaps -H dc01.domain.local -b '' -p 636
```

The following message is produced:

```
LDAP OK - 0.043 seconds response time|time=0.042861s;;;0.000000
```

Final Thoughts

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

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