

Re: LDAP authentication security ?

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-12/msg00038.html>

- *From:* Pascal <pascal_t@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 10 Dec 2007 10:44:29 +0100
-

Thank you for all these informations Joe !

I'm actually a big fan of external SSL certs for DCs simply because they are trusted by most clients by default. Using an internally rooted CA can be less expensive, but it is less easy to get all of the clients to trust your certs issued by this CA, especially in an environment that includes non-Windows machines that can't take advantage of auto enrollment or GPO for distributing trusted roots.

The biggest downside of external certs for DCs is that they expire and you need to renew them manually. Nothing is going to warn you that the certs are expiring, so you have to remember this (which can be hard a year or two after you bought them). There are ways to deal with this, but I've seen lots of temporary application failures due to unexpected expiration of DC certs. With a Windows CA, they are typically renewed automatically.

There is also more manual effort with external certs, but I don't think that's a huge big deal.

Joe K.

—
Joe Kaplan—MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"
<http://www.directoryprogramming.net>
—

"Pascal" <pascal_t@xxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:mn.3b907d7c29bbe267.70874@xxxxxxxxxxxxxxxxxxxxxx>

Hi Joe,

thank you for your answer.
It is very clear (as most of your interventions here :D).

Actually we don't have any PKI so we will buy a commercial SSL certificates.

You said that both solutions have pros and cons.

Why ? And do you know where I can find the pros and cons of each one ?

Re: LDAP authentication security ?

Thank you again.

This depends on the application. If the application only supports LDAP simple bind, then you will need an additional security mechanism like SSL/LDAP in order for the credential validation to be secure.

If the application supports SASL bind with either GSS-SPNEGO or DIGEST authentication, then you can use that directly with AD without needing to secure the channel as those authentication mechanisms are already secure without channel encryption.

Simple bind is the authentication mechanism in the LDAP V3 spec and is supported by all LDAP directories. SASL is a mechanism used in LDAP and other places of adding in additional authentication protocols. Not all LDAP servers and clients support all SASL mechanisms, so whether or not you can use SASL depends a great deal on the capabilities of the LDAP client (the application).

If you need SSL, AD supports SSL LDAP just fine, assuming you get a certificate for your domain controllers. You can either use a Windows CA or procure SSL certificates from an external CA. Either work and both have their pros and cons.

Joe K.

--

Joe Kaplan-MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"

<http://www.directoryprogramming.net>

--

"Pascal" <pascal_t@xxxxxxxxxxxxxxxxxxxx> wrote in message

<news:mn.1c157d7ca0336b3b.70874@xxxxxxxxxxxxxxxxxxxx>

Hi,
(First, sorry for my english ;-))

I would like to use an LDAP authentication with my application (Quality Center). So, the user will have to type his Active Directory username and password BUT the LDAP authentication secured is it secured ?

Re: LDAP authentication security ?

By default, there is no encryption so the password is transmitted in clear text ?

Do I need to use LDAP Over SSL ?

What is SASL ?

Thank you

-- Pascal

-- Pascal

--
Pascal

.