MightyCare white paper

we care for IT

vCenter Orchestrator and ldaps

author: Christian Johannsen <christian.johannsen@mightycare.de>

initial date: 01.11.10

last change: 01.11.10

MightyCare Solutions GmbH
Philipp-Reis-Str. 15a
D-61130 Nidderau

Fon: +49 (0) 6187 900 156
Fax: +49 (0) 6187 900 157

http://www.mightycare.de

history:

version	changes
0.1	inital release
0.2	integration of the screenshots
0.3	description change
0.4	pre-final
0.5	final

table of contents

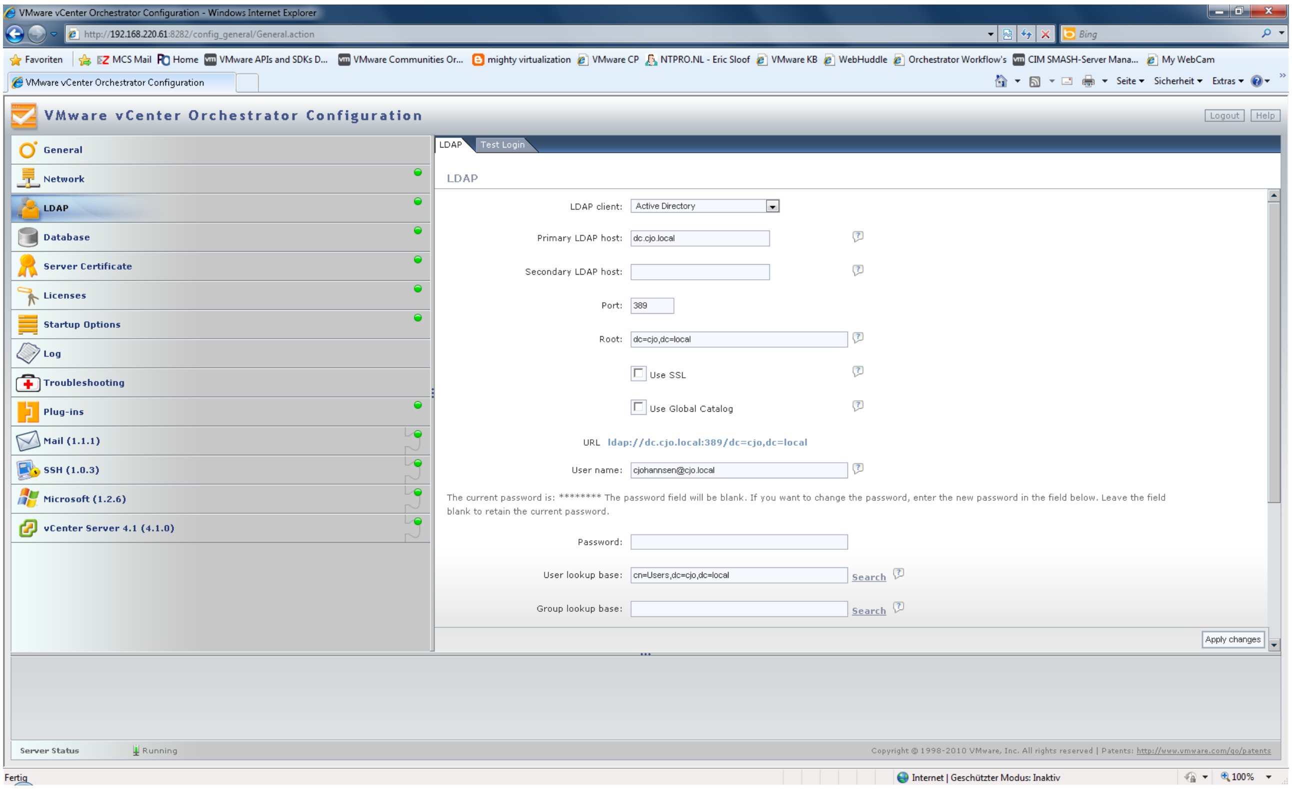
1 summary

The following white paper describes how to implement the ldap directory service with vCenter Orchestrator 4.1 build 581. Because the vCenter Orchestrator configuration does not support NTLMv2 authentication, like it does in the database configuration tab it is necessary to do a workaround. Based on my experience it is best to implement this workaround in close collaboration with the Active-Directory (in Windows environments) team because sometimes there are different approaches for security implementations.

The following workaround is bases on the vCenter Orchestrator 4.1 build 581 on a Windows Server 2008 R2 x64 and a Windows-Active-Directory on Windows Server 2003 and Windows Server 2008. For the implementation it is not necessary to install any optional applications or components.

2 vCO configuration

When installing and configuring vCenter Orchestrator you have to define the ldap settings for authentication (see screenshot 1). In most environments it is easily done by adding the Active-Directory domain controller and entering the credentials for an administrative account. There is also the need to define the user and group lookup base and define the vCO administration group.


VMware vCenter Orchestrator Configuration - Windows Internet Explorer
http://192.168.220.61:8282/config_general/General.action
VMware vCenter Orchestrator Configuration
Logout
Help
General
Network
LDAP
Database
Server Certificate
Licenses
Startup Options
Log
Troubleshooting
Plug-ins
Mail (1.1.1)
SSH (1.0.3)
Microsoft (1.2.6)
vCenter Server 4.1 (4.1.0)
LDAP
Test Login
Apply changes
Server Status
Running
Internet | Geschützter Modus: Inaktiv
100%

LDAP

LDAP client: Active Directory

Primary LDAP host: dc.cjo.local

Secondary LDAP host:

Port: 389

Root: dc=cjo,dc=local

☐ Use SSL

☐ Use Global Catalog

URL ldap://dc.cjo.local:389/dc=cjo,dc=local

User name: cjohannsen@cjo.local

The current password is: ******** The password field will be blank. If you want to change the password, enter the new password in the field below. Leave the field blank to retain the current password.

Password:

User lookup base: cn=Users,dc=cjo,dc=local Search

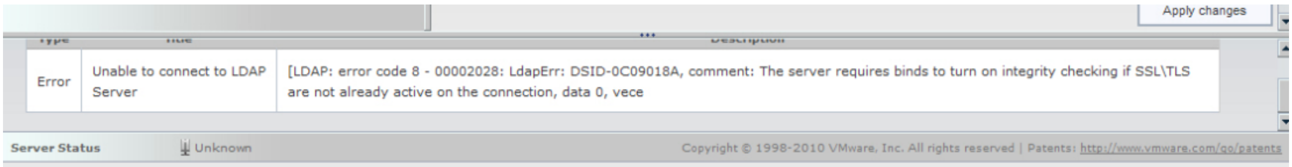
Group lookup base: Search

screenshot 1 – ldap configuration

Instead of using the Windows Active Directory it is also possible to use Novell eDirectory or SUN Java System Directory Server.

2.1 error messages

When using an ldaps domain the vCO ldap configuration could fail with the following error message:

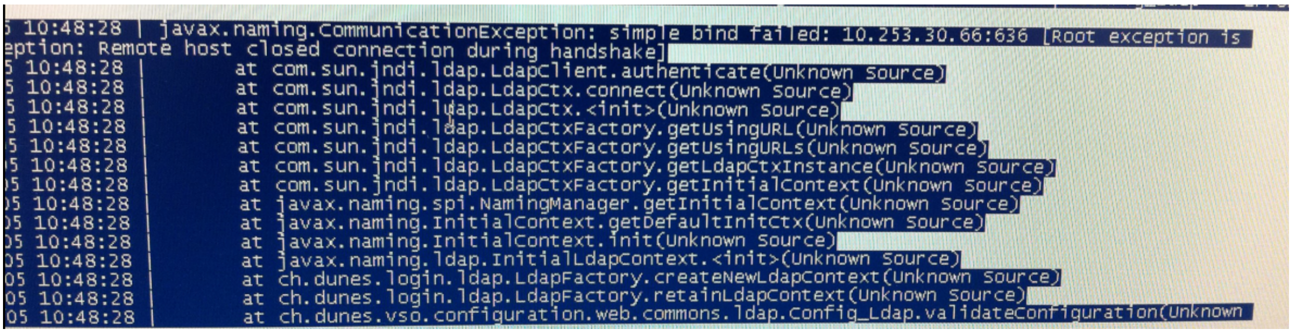


Error	Unable to connect to LDAP Server	[LDAP: error code 8 - 00002028: LdapErr: DSID-0C09018A, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, vece

Server Status
Unknown
Copyright © 1998-2010 VMware, Inc. All rights reserved | Patents: http://www.vmware.com/go/patents

screenshot 2 – error message

By searching this ldap error it seems that SSL integration is needed and the solution is to turn on the SSL option "Use SSL". When activating the SSL usage a certificate is needed and with this a PKI in the Active-Directory. Also the port changes into 636 which is standard for SSL connections. But, if there is no SSL active you get another error:



```
5 10:48:28 | javax.naming.CommunicationException: simple bind failed: 10.253.30.66:636 [Root exception is
eption: Remote host closed connection during handshake]
5 10:48:28 |          at com.sun.jndi.ldap.LdapClient.authenticate(Unknown Source)
5 10:48:28 |          at com.sun.jndi.ldap.LdapCtx.connect(Unknown Source)
5 10:48:28 |          at com.sun.jndi.ldap.LdapCtx.<init>(Unknown Source)
5 10:48:28 |          at com.sun.jndi.ldap.LdapCtxFactory.getUsingURL(Unknown Source)
5 10:48:28 |          at com.sun.jndi.ldap.LdapCtxFactory.getUsingURLs(Unknown Source)
5 10:48:28 |          at com.sun.jndi.ldap.LdapCtxFactory.getLdapCtxInstance(Unknown Source)
5 10:48:28 |          at com.sun.jndi.ldap.LdapCtxFactory.getInitialContext(Unknown Source)
05 10:48:28 |          at javax.naming.spi.NamingManager.getInitialContext(Unknown Source)
05 10:48:28 |          at javax.naming.InitialContext.getDefaultInitCtx(Unknown Source)
05 10:48:28 |          at javax.naming.InitialContext.init(Unknown Source)
05 10:48:28 |          at javax.naming.ldap.InitialLdapContext.<init>(Unknown Source)
05 10:48:28 |          at ch.dunes.login.ldap.LdapFactory.createNewLdapContext(Unknown Source)
05 10:48:28 |          at ch.dunes.login.ldap.LdapFactory.retainLdapContext(Unknown Source)
05 10:48:28 |          at ch.dunes.vso.configuration.web.commons.ldap.Config_Ldap.validateConfiguration(Unknown
```

screenshot 3 – java error message

The error message that you are getting: "javax.naming.communicationException: simple bind failed: (Root exception is: Remote host closed connection during handshake" indicates that it is the remote machine (the AD server) that terminated the connection.

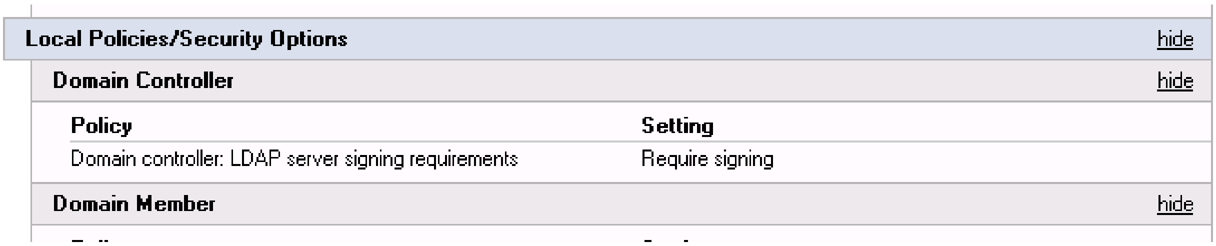
3 solution

In high secure environments the simple bind mechanism isn´t allowed because of the clear-text password in the transmission. If there is no PKI available and the error is displayed the problem is another one:

With Windows Server 2003 and Active Directory (AD), a new group policy security option configures AD to only respond to binds that have requested LDAP integrity. The GPO is: Active Directory Group Policy Security Setting "LDAP Server Signing Requirements".

3.1 the GPO deactivation

The simplest way to get the vCenter Orchestrator running with the Active-Directory is to change the group policy at the domain controller from: "Require Signing" or "Negotiate Signing" to "None". After this change run a `gpupdate /force` to activate the new rule.



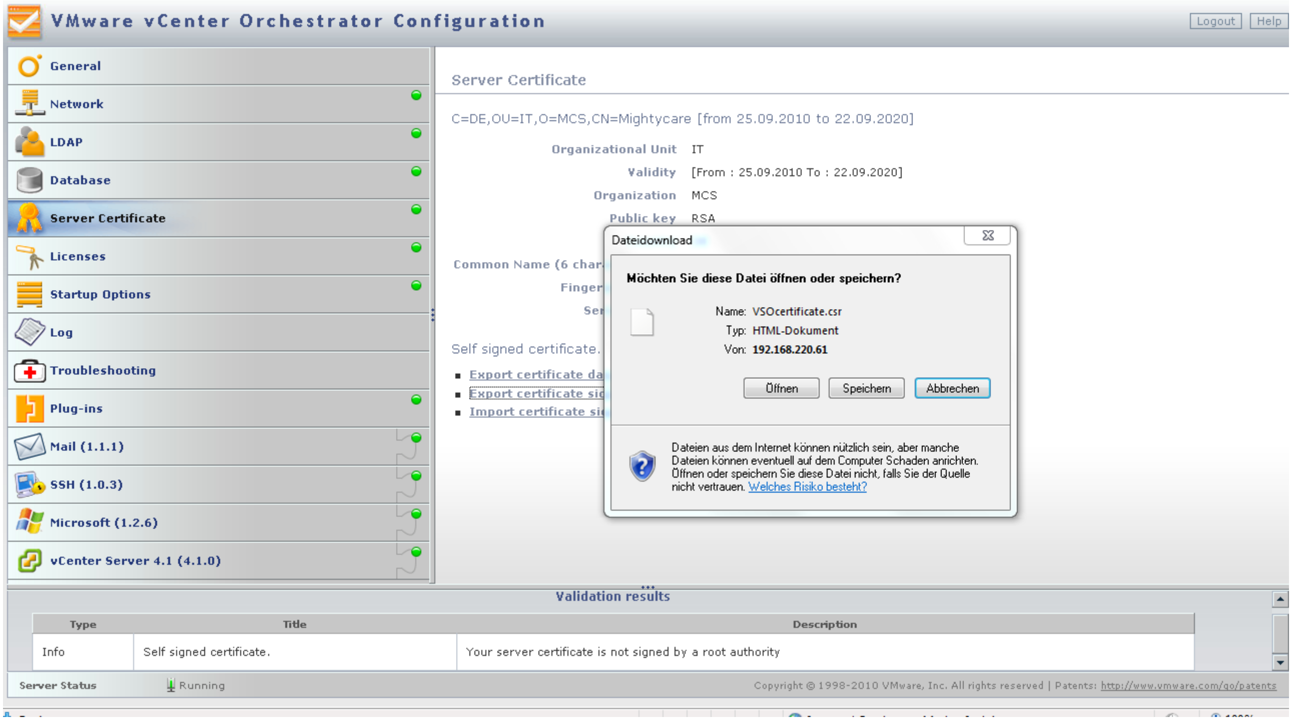
Local Policies/Security Options	hide
Domain Controller	hide
Policy	**Setting**
Domain controller: LDAP server signing requirements	Require signing
Domain Member	hide

screenshot 4 – GPO rule

This way is as said before the simplest solution but it is also not really secure because of the clear-text password transmission.

3.2 the SSL activation

The alternative to establish a secure connect between the vCenter Orchestrator and a Windows-Active-Directory is to create an certificate authority and enable the SSL authentification for ldap clients on port 636. Based on the certificate authority it is possible to create an CA signed certificate for the vCenter Orchestrator Server. The certificate signing request can be created in the vCenter Orchestrator configuration interface and after signing through the CA the .crt certificate can be imported.



Server Certificate

C=DE,OU=IT,O=MCS,CN=Mightycare [from 25.09.2010 to 22.09.2020]

Organizational Unit IT
Validity [From : 25.09.2010 To : 22.09.2020]
Organization MCS
Public key RSA
Common Name (6 char
Finger
Ser

Self signed certificate.

- Export certificate da
- Export certificate si
- Import certificate si

Dateidownload

Möchten Sie diese Datei öffnen oder speichern?

Name: VSOcertificate.csr
Typ: HTML-Dokument
Von: 192.168.220.61

Dateien aus dem Internet können nützlich sein, aber manche Dateien können eventuell auf dem Computer Schaden anrichten. Öffnen oder speichern Sie diese Datei nicht, falls Sie der Quelle nicht vertrauen. Welches Risiko besteht?

Validation results

Type	Title	Description
Info	Self signed certificate.	Your server certificate is not signed by a root authority

Server Status Running

Copyright © 1998-2010 VMware, Inc. All rights reserved | Patents: http://www.vmware.com/go/patents

screenshot 5 – certificate signing request

As is said before: this way is the most secure, but in some environments the effort is to high for internal server communication.

4 hints and proofs

vCenter Orchestrator Community:
http://communities.vmware.com/community/vmtn/mgmt/orchestrator

mighty virtualization Blog:
http://mighty-virtualization.blogspot.com

vCO Team Blog:
http://www.vcoteam.info/

5 used Abbreviations

vCO	vCenter Orchestrator
AD	Active-Directory
ldap	lightweight directory access protocol
SSL	secure sockets layer
NTLMv2	NT Lan Manager version 2
PKI	Public Key Infrastructure
simple bind	Authentication with a simple plaintext password
.csr	File: certificate signing request
.crt	File: