

Beratung und Support
Technische Plattform
Support-Netz-Portal



paedML® – stabil und zuverlässig vernetzen

Update-Anleitung

Bald ablaufende oder bereits abgelaufene Zertifikate erneuern im GServer03 der paedML Novell 4.2

Stand 05.01.2018

paedML® Novell

Version: 4.2

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111
70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Hubert Bechtold
Holger Dzeik
Stefan Falk
Ulrich Frei
Carl Heinz Gutjahr
Friedrich Heckmann
Uwe Labs
Alfred Wackler

Endredaktion

Wird von der Redaktion eingetragen.

Bildnachweis Titelbilder:

Thinkstock

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2017

Die Nutzung dieses Handbuches ist ausschließlich für eigene Zwecke zulässig. Die Nutzung sowie die Weitergabe dieses Handbuches zu kommerziellen Zwecken wie z.B. Schulungen ist nur nach ausdrücklicher Einwilligung durch das LMZ erlaubt.

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1.	Server-Zertifikat (GServer03)	4
1.1	Ablaufdatum feststellen	4
2.	eDirectory-Zertifikat	4
2.1	Ablaufdatum feststellen	4
2.2	ZCM-Zonenzertifikat (ZServer)	6
2.3	Vorbereitung auf dem ZServer	6
2.4	eDirectory-Zertifikat erneuern	8
3.	Nacharbeiten im ZServer	12
4.	Schluss	16

Vorwort

Auf dem GServer03 der paedML Novell 4.2 müssen ggf. Zertifikate erneuert werden.

Das Server-Zertifikat sollte noch bis zum 5.5.2024 gültig sein, das eDirectory-Zertifikat läuft möglicherweise am 7.1.2018 ab. In dieser Anleitung wird beschrieben, wie diese Zertifikate zu erneuern sind.

1. Server-Zertifikat (GServer03)

1.1 Ablaufdatum feststellen

Sicher fragen Sie sich: Habe ich noch Zeit oder muss ich sofort tätig werden? Um diese Frage zu beantworten, können Sie nachschauen, wann Ihre Zertifikate ablaufen:

Für die YaST_Default_CA können Sie dies an der Kommandozeile des GServer03 folgendermaßen feststellen:

```
openssl x509 -enddate -noout -in /var/lib/CAM/YaST_Default_CA/cacert.pem
```

Die Ausgabe sollte in der paedML Novell 4.2 so aussehen:

```
notAfter=May 5 14:51:55 2024 GMT
```

also noch gültig bis zum 5. May 2024. (Wir gehen davon aus, dass Sie dies z.B. beim Umstieg auf die paedML Novell 4.1 oder 4.2 erledigt hatten.)

Sollte bei Ihnen der Ablauf bald bevorstehen, so können Sie, wie im Dokument *paedML-Novell-41-Server-eDir-Zertifikat-erneuern.pdf* in Kapitel 2 beschrieben, auf der LMZ Support-Netz Seite unter *Updates und Patches*, [Ablaufende Zertifikate erneuern](#), vorgehen.

Falls Sie ein gekauftes vertrauenswürdigen Zertifikat einsetzen, sollten Sie dieses auch überprüfen. Dies geht ebenfalls mit dem obigen Befehl. Stellen Sie fest, wo Ihr Zertifikat liegt (z.B. in */etc/ssl/servercerts/* oder in */etc/apache2/ssl.crt*). Der Befehl lautet dann so:

```
openssl x509 -enddate -noout -in <Pfad>/<Zertifikatsname>.pem oder .crt
```

2. eDirectory-Zertifikat

2.1 Ablaufdatum feststellen

Öffnen Sie den iManager (egal, ob auf der graphischen Oberfläche des GServer03 oder auf einer Arbeitsstation) und melden sich als *admin* an. Navigieren Sie zu *NetIQ Certificate Access / Server Certificates* und klicken Sie auf *SSL CertificateIP* (oder *SSL CertificateDNS*). Dort können Sie das Ablaufdatum einsehen:

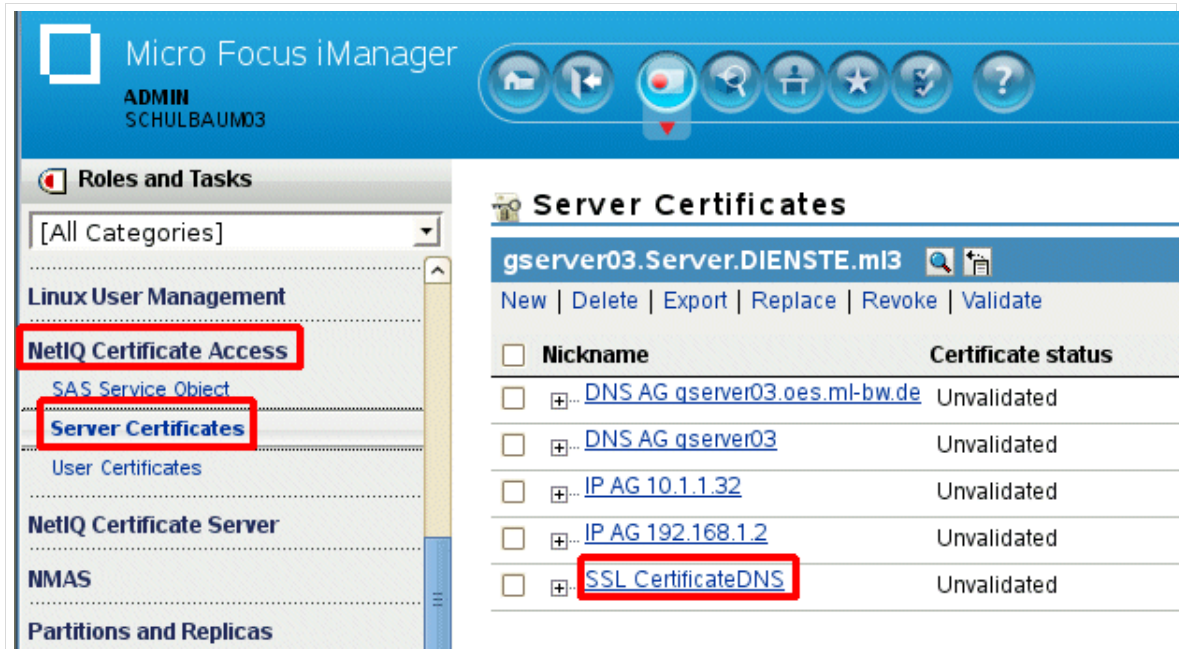


Abb. 1:

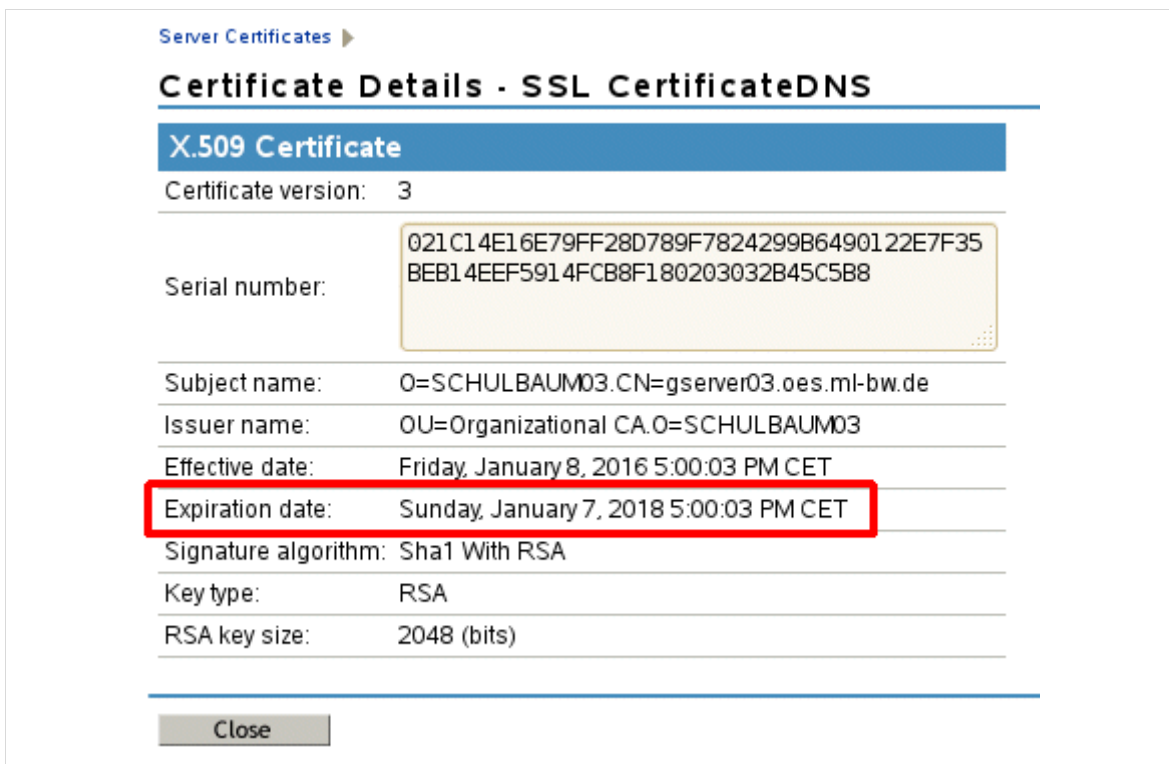


Abb. 2:

Sofern nicht Sie oder Ihr Händler etwas verändert haben, sollte hier das Ablaufdatum der **7.1.2018** sein.



Es ist auf jeden Fall wichtig, Zertifikate vor deren Ablauf zu erneuern, da sonst schwerwiegende Störungen in der paedML Novell auftreten können.

Wir empfehlen Ihnen, das Zertifikat jetzt zu erneuern.

2.2 ZCM-Zonenzertifikat (ZServer)

Beim Einloggen ins ZCC wird eine Warnung angezeigt, wenn die Restlaufzeit des **eDirectory**-Zertifikats kleiner als 90 Tage ist.

Das **ZCM-Zonenzertifikat** der vom LMZ ausgelieferten ZServer hat aber noch eine Laufzeit bis mindestens 27. Januar 2021. Hier besteht also z.Z. kein Bedarf, ein neues Zertifikat zu erzeugen. Deshalb verzichten wir hier auf eine Anleitung.

Wollen Sie trotzdem das Ablaufdatum nachprüfen. Ok, so geht's:

Loggen Sie sich als *admin* auf einer Arbeitsstation ein und öffnen Sie eine DOS-Box oder stellen Sie eine PuTTY-Sitzung mit dem ZServer her. Geben Sie dort folgenden Befehl ein:

```
zac cert-info      (oder auch zac ci)
```

Sie erhalten dann etwa folgende Ausgabe:

```
10.1.1.33 - PuTTY
ZServer:~ # zac ci

Processing Command: ci

Certificate Details for host zserver.oes.ml-bw.de.

Subject:      CN=zserver.oes.ml-bw.de,OU=ZENworks
Issued by:    CN=zserver.oes.ml-bw.de,OU=ZENworks,O=Internal Certificate Authority
Serial number: 01:2D:D7:77:98:5A
Not valid before: 1/28/11 4:08 PM
Not valid after: 1/27/21 4:08 PM
Thumbprint:   48:77:A4:CE:44:CA:A9:B5:48:4D:A9:74:18:F0:14:FB:68:B5:0B:0D

Certificate Details for host localhost
```

Abb. 3:

2.3 Vorbereitung auf dem ZServer

Starten Sie auf einer Arbeitsstation (oder auf der graphischen Oberfläche des GServer03) einen Browser und loggen sich im ZCC als *Administrator* ein.



Spätestens bevor Sie das eDirectory-Zertifikat erneuern (Kap.2.4), führen Sie die folgenden Schritte unbedingt und sorgfältig durch. Andernfalls riskieren Sie den Verlust aller Beziehungen in Bundles, Richtlinien,...!

Um ganz sicherzugehen, legen Sie bitte vom ZServer unbedingt ein Snapshot im *vSphere-Client* an. Auch ein Backup des ZServer (z.B. mit Veeam) ist sinnvoll.

Navigieren Sie zu *Konfiguration* und scrollen Sie im rechten Fenster etwas herunter zum Abschnitt Benutzerquellen. Klicken Sie dort auf *SCHULBAUM03* und dann im Abschnitt *Verbindungen* auf *Schulbaum03*:

Verbindungsdetails bearbeiten

Verbindungsname:* Schulbaum03

Adresse:* 10.1.1.32

SSL verwenden: Ja

Port: 636

Zertifikat:

Ausgestellt an: CN=gserver03.oes.ml-bw.de, O=SCHULBAUM03
 Ausgestellt von: O=SCHULBAUM03, OU=Organizational CA
 Gültig ab: Fr Jan 08 17:00:03 MEZ 2016
 Gültig bis: So Jan 07 17:00:03 MEZ 2018

Aktualisieren

OK Abbrechen

Abb. 4:

Klicken Sie dort auf *Aktualisieren* (es kann sein, dass eine Meldung erscheint, dass sich nichts geändert hat → Ok). In jedem Fall sehen Sie unter *Gültig bis* das Ablaufdatum des eDirectory-Zertifikats. → OK.

Klicken Sie nun weiter oben im Abschnitt *Allgemein* bei *SSL verwenden* auf *Nein*:

Das Ergebnis muss so aussehen:

[Konfiguration](#) > SCHULBAUM03


Allgemein	
Name:	SCHULBAUM03
Verzeichnistyp:	eDirectory
Kommunikationsstatus:	
Benutzername und Passwort: (Bearbeiten)	cn=ldapuserzcm,ou=server,ou=dienste,o=ml3
Authentifizierungsmethode: (Bearbeiten)	Benutzername/Passwort
SSL verwenden:	Nein (Ja)
Dynamische Gruppen in eDirectory ignorieren:	Nein (Ja)
Root-Kontext: (Bearbeiten)	
Beschreibung: (Bearbeiten)	

Abb. 5:

Vergewissern Sie sich, dass alles korrekt ist!

Nach der Erneuerung der eDirectory-Zertifikate werden wir diese Einstellung wieder rückgängig machen (siehe Kap.3).

2.4 eDirectory-Zertifikat erneuern



Vergewissern Sie sich, dass Sie die Arbeiten, die in Kap. 2.3 beschrieben wurden, ausgeführt haben!

Öffnen Sie den iManager (egal, ob auf der graphischen Oberfläche des GServer03 oder auf einer Arbeitsstation) und melden sich als *admin* an. Navigieren Sie zu *NetIQ Certificate Server / Repair Default Certificates* und wählen Sie das Objekt *gserver03* aus der OU *Server.DIENSTE.ml3*:

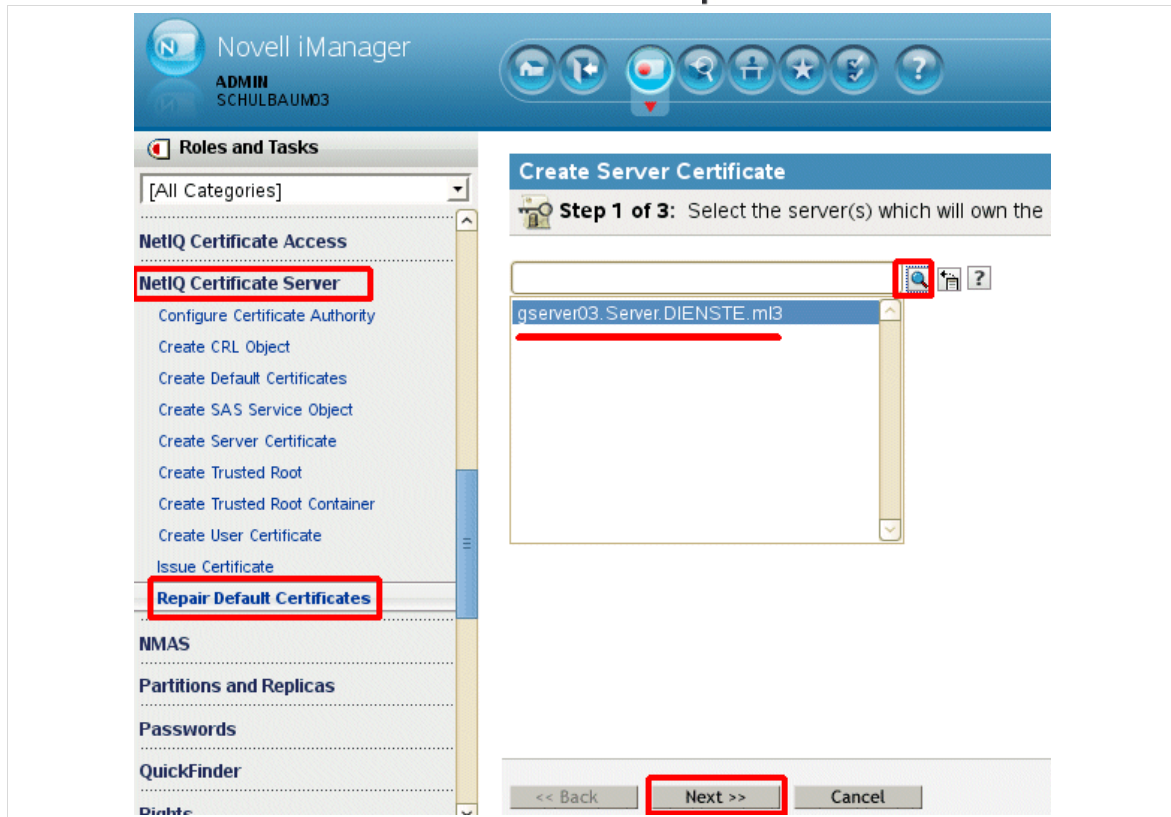


Abb. 6:

→ Next.

Wählen Sie dann *Yes All Default Certificates will be overwritten*:

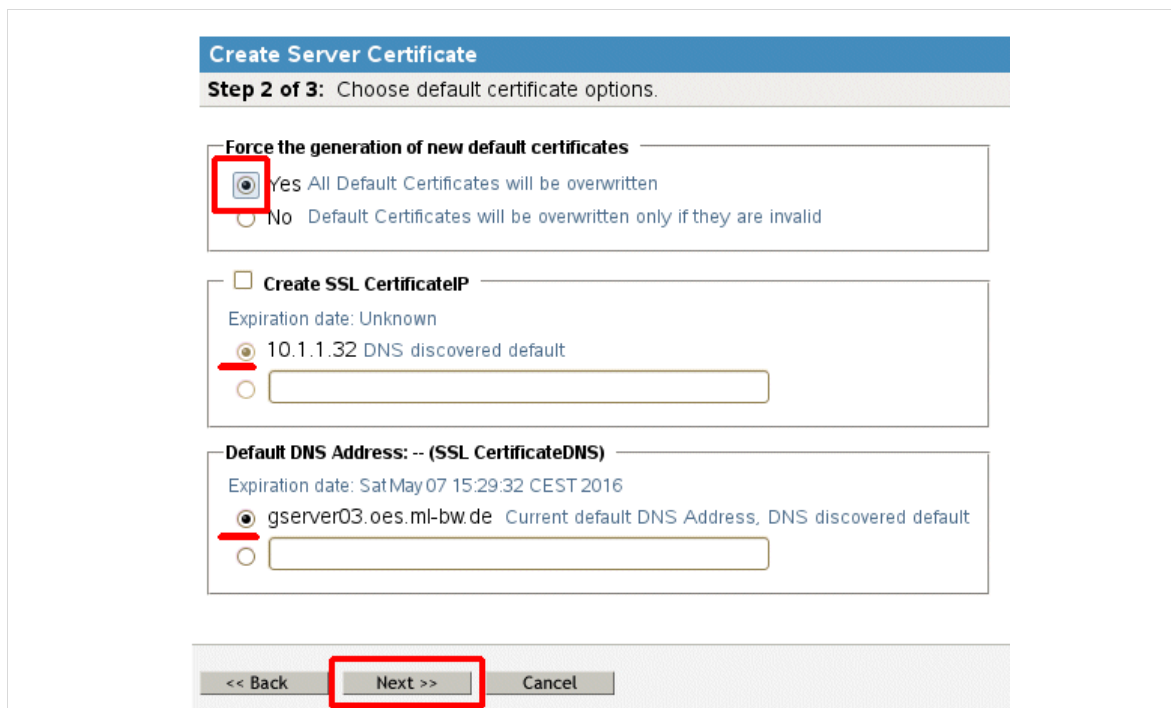


Abb. 7:

→ Next.

Es erfolgt eine Zusammenfassung:

Name	Value
Server:	.O=ml3.OU=DIENSTE.OU=Server.CN=gserver03
Default IP Address:	10.1.1.32
Default DNS Address:	gserver03.oes.ml-bw.de
Force replacement:	Yes

<< Back **Finish** Cancel

Abb. 8:

→ *Finish*,

gefolgt von einer Erfolgsmeldung:

Name	Result
SSL CertificateDNS	Success
IP AG 10.1.1.1\32	Success
DNS AG gserver03\oes\ml-bw\de	Success

Close

Abb. 9:

→ Close.

Überprüfen können Sie das neue Ablaufdatum, das nun wieder in zwei Jahren erreicht wird, unter *NetIQ Certificate Access / Server Certificates*. Klicken Sie dort z.B. auf *SSL CertificateIP* (oder/und eines der anderen):

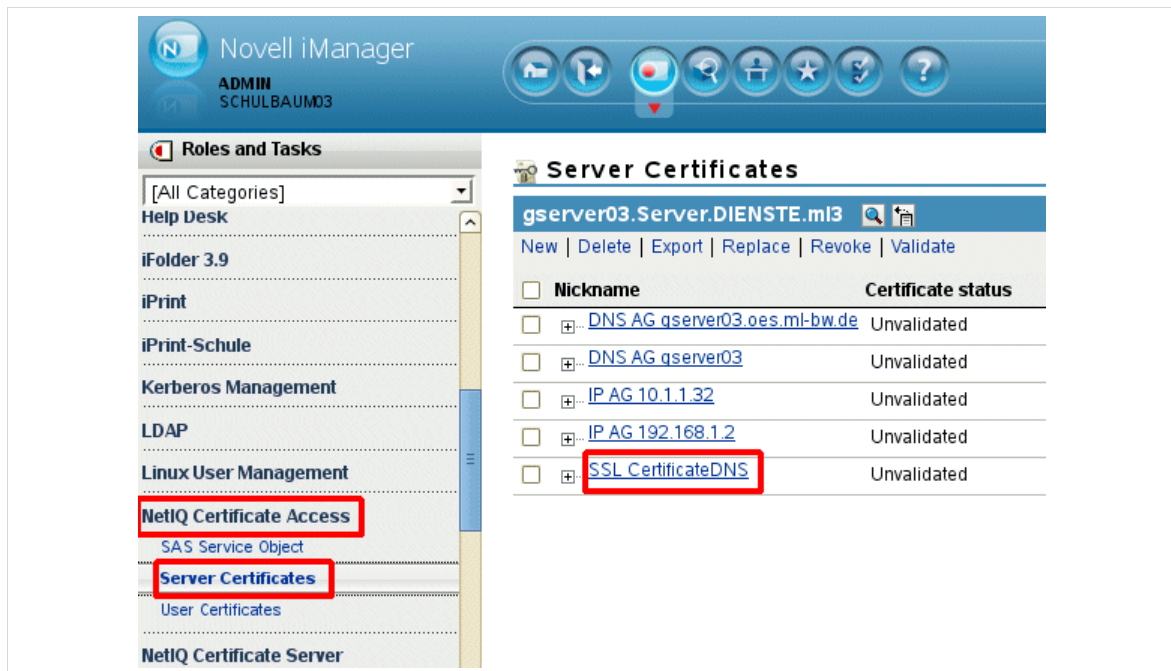


Abb. 10:

Certificate Details - SSL CertificateDNS

X.509 Certificate

Certificate version: 3

Serial number: 73B5CA4E762A502E35C6D14262A53E984B394F05

Subject name: O=SCHULBAUM03.CN=gserver03.oes.ml-bw.de

Issuer name: OU=Organizational CA.O=SCHULBAUM03

Effective date: Friday, December 8, 2017 10:48:08 AM CET

Expiration date: Sunday, December 8, 2019 10:48:08 AM CET

Signature algorithm: Sha1 With RSA

Key type: RSA

RSA key size: 2048 (bits)

Exponent: 010001 (hex)

Modulus: 00D896E49878722A59F4DD787C337F0375A1448
646185024C00BFD45151F685CBF8F8C39D0842C
9AEDDAC097EE07418F3BC7B72E9CB1F8A2EF2E7
CEB487EBA242328DEBC412E27AEA22B4783612B

Extensions

Close

Abb. 11:

(Bei Ihnen natürlich mit einem aktuellen Datum.)

Öffnen Sie jetzt noch ein Terminal-Fenster und geben ein:

```
namconfig -k      (geben Sie Ihr admin-Passwort ein)
nldap -u
nldap -l
```

Damit ist der Prozess abgeschlossen.

Starten Sie den GServer03 neu!!

3. Nacharbeiten im ZServer

Das neue eDirectory-Zertifikat muss nun noch dem ZCM bekannt gemacht werden und die Verbindung zum eDirectory muss wieder auf SSL gesetzt werden.

Starten Sie auf einer Arbeitsstation einen Browser und loggen sich im ZCC als *Administrator* ein. Falls Sie ZCC noch von vorher offen haben, loggen Sie sich aus und melden Sie sich erneut an. Navigieren Sie nun wieder zu *Konfiguration* und scrollen Sie im rechten Fenster etwas herunter zum Abschnitt Benutzerquellen. Klicken Sie dort auf *SCHULBAUM03*:

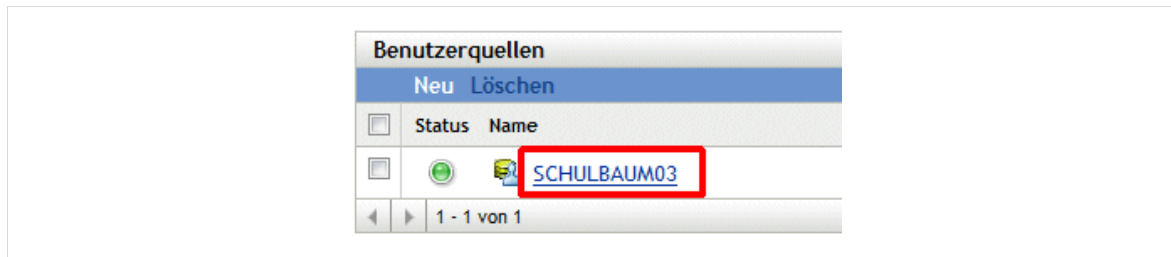


Abb. 12:

Klicken Sie nun im Abschnitt *Allgemein* bei *SSL verwenden* auf *Ja*:

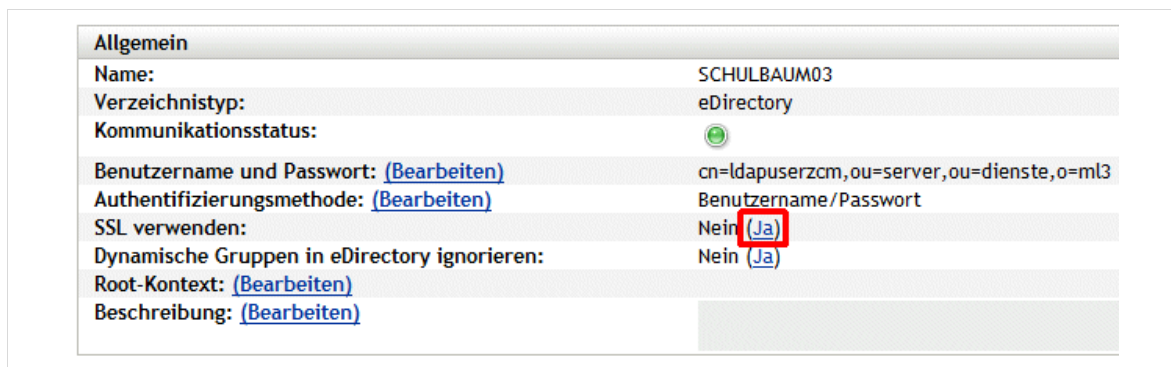


Abb. 13:

Es erscheint ein Fenster, das mit → OK bestätigt werden muss.

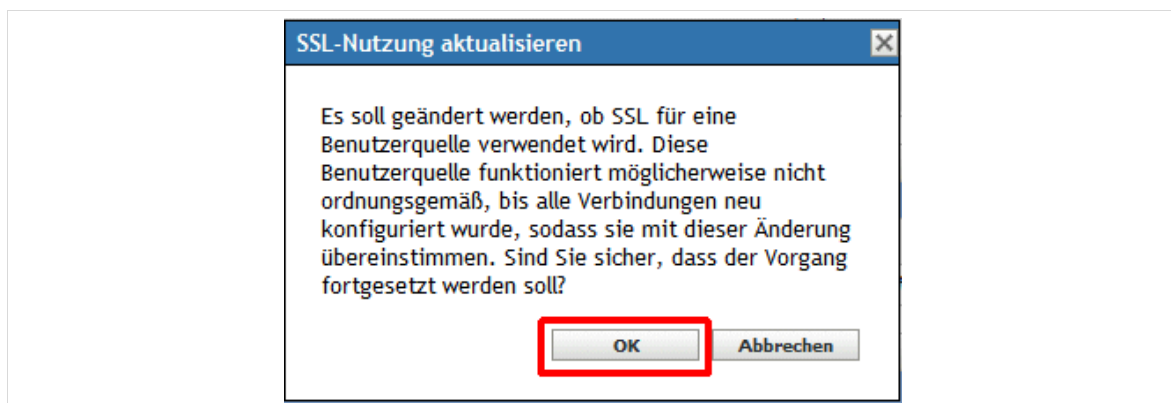


Abb. 14:

Gehen Sie danach in den Abschnitt *Verbindungen* und klicken auf *SCHULBAUM03*:

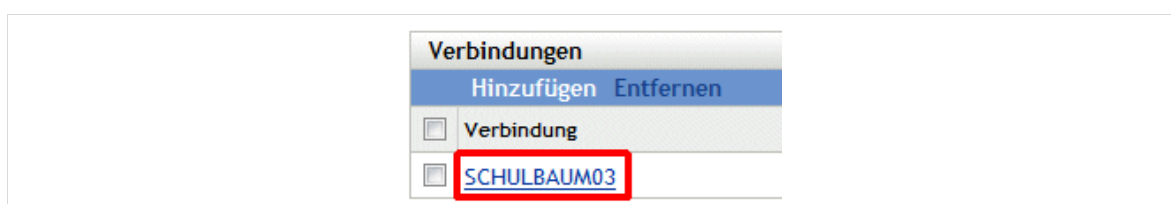


Abb. 15:

Dabei erscheint ein Fenster, in dem jetzt das neue Zertifikat bestätigt werden muss. Klicken Sie dazu auf den Button *Aktualisieren* (bis die Umstellung wirksam wird, kann ein Augenblick vergehen):

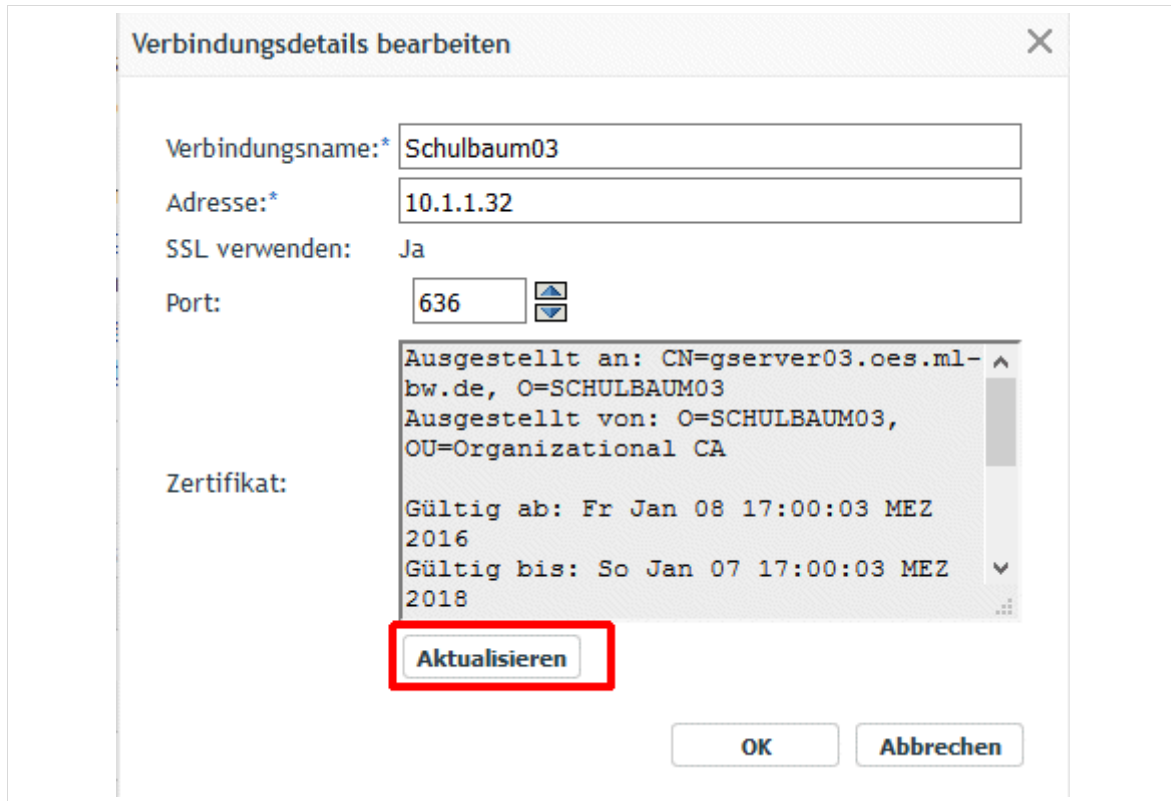


Abb. 16:

(Die Zertifikatsdaten im Bild sind nur beispielhaft zu verstehen und sehen bei Ihnen etwas anders aus.)

Daraufhin erscheint ein Fenster mit Ihren neuen Zertifikatsdaten:

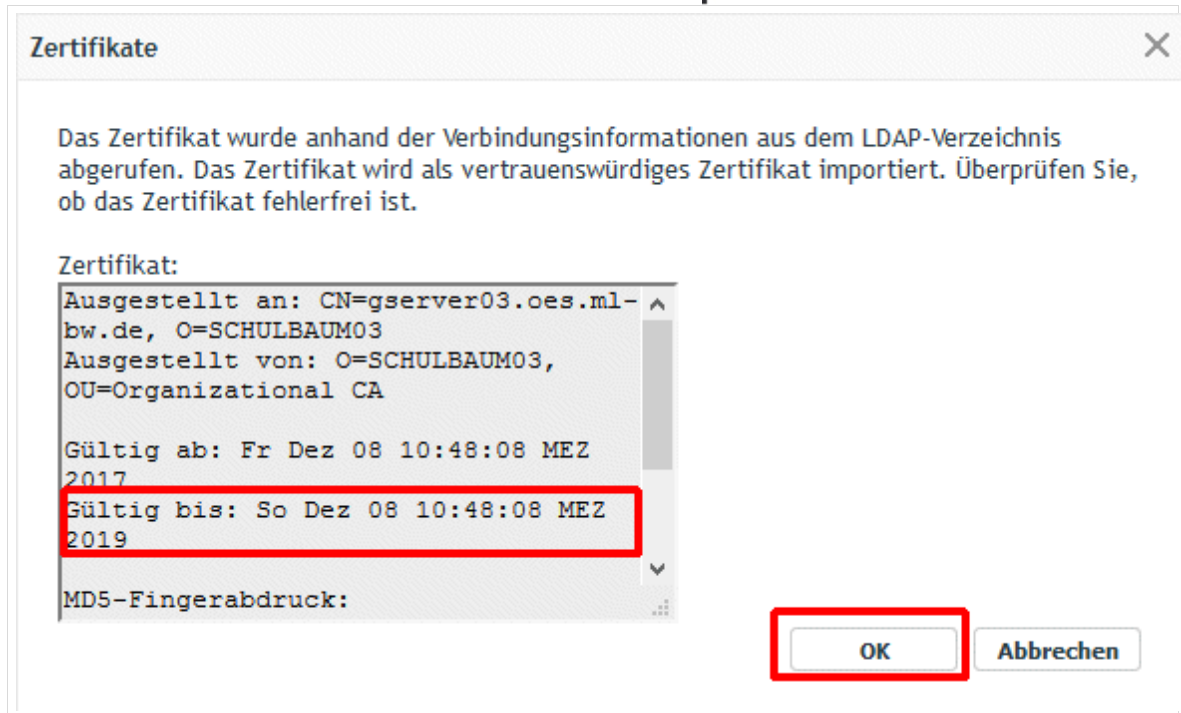


Abb. 17:

→ OK → OK.

Überprüfen Sie nun, ob die Verbindung zur Benutzerquelle erhalten geblieben ist. Dies können Sie z.B. bei einem Bundle prüfen, bei dem in den Beziehungen eine Benutzerzuweisung eingetragen ist. Folgendes Bild zeigt dies beispielhaft für das Bundle *SchulkonsoleW7* in Ihrer Schule.

Unter Benutzerzuweisung muss, wie in der folgenden Abbildung zu sehen, bei diesem Bundle *Lehrer* eingetragen sein. Dann sind Benutzerquelle und die damit verbundenen Benutzerzuweisungen korrekt erhalten geblieben.

(Im Fehlerfall würde hier *unbekannte externe Referenz* stehen).

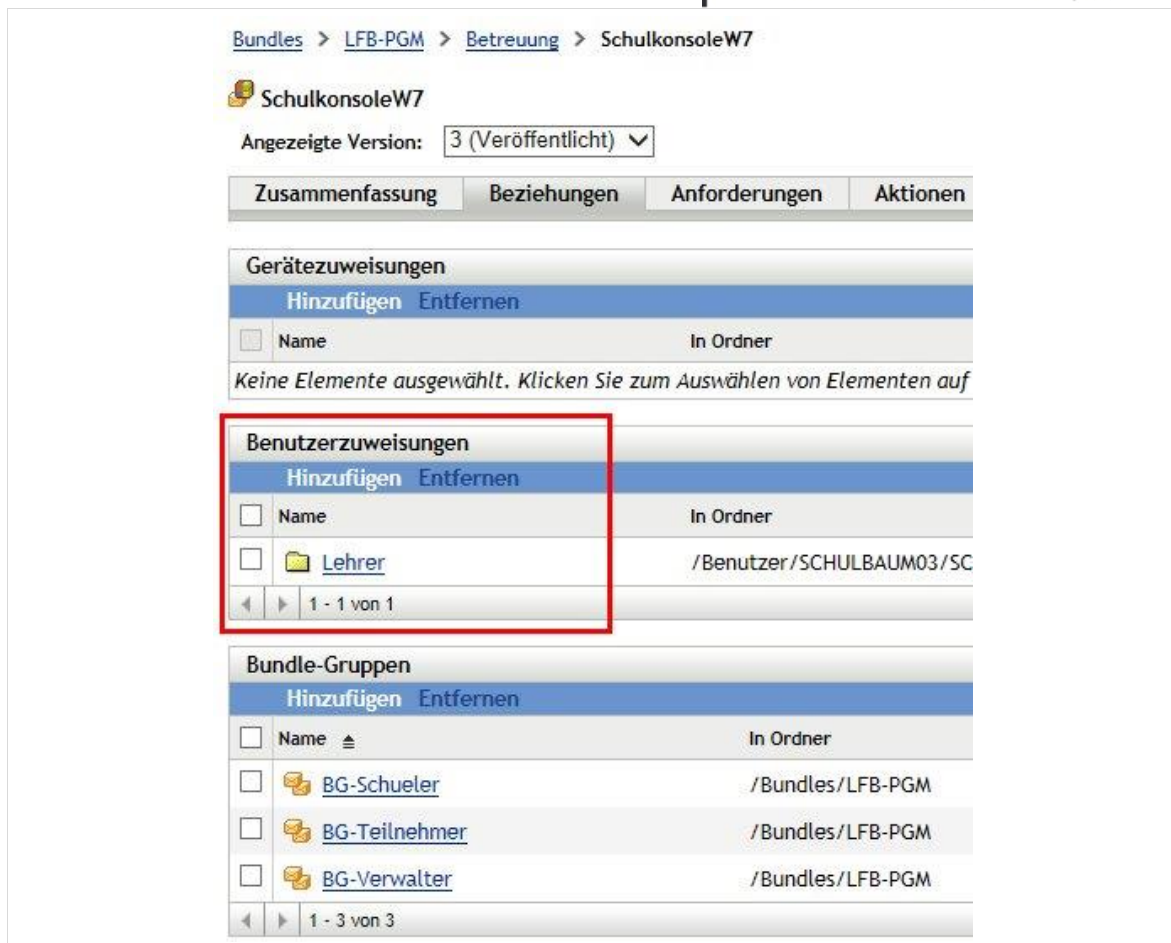


Abb. 18:

4. Schluss

Die Snapshots von GServer03 und ZServer sollten Sie zeitnah wieder löschen.

Erfreuen Sie sich nun an Ihren neuen Zertifikaten.

Viel Erfolg mit der *paedML Novell 4.2* wünscht Ihnen

Ihre ZEN-Novell.

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111
70190 Stuttgart

© Landesmedienzentrum Baden-Württemberg, 2017