

Dokumentation

Gruppe 9 (sdi09)

Software defined Infrastructure

Prof. Dr. Martin Goik
WS20/21

Autoren: **Fabian Ikizoglu (fi006)**
 Aydin Mirzaghayev (am180)

Datum: **01.03.2021**

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
1. DNS.....	4
1.1 Querying DNS data.....	4
1.2 Installing Bind.....	4
1.3 Reverse lookups.....	4
1.4 Forwarders.....	4
1.5 Mail exchange record.....	5
2. LDAP.....	6
2.1 Browse an existing LDAP Server.....	6
2.2 Set up an OpenLdap server.....	6
2.3 Populating your DIT.....	6
2.4 Testing a bind operation as non - admin user.....	6
2.5 Filter based search.....	7
2.6 Extending an existing entry.....	7
2.7 Accessing LDAP data by a mail client.....	7
2.8 LDAP configuration.....	7
2.9 LDAP based user login.....	8
2.10 Backup and recovery / restore.....	9
3. Apache web server.....	10
3.1 First Steps.....	10
3.1.1 sdi9b.mi.hdm-stuttgart.de.....	10
3.1.2 Apache Dokumentation umbenennen.....	10
3.1.3 Neue HTML-Datei einrichten.....	10
3.1.4 Apache Dokumentation installieren.....	11
3.1.5 sdi9b.mi.hdm-stuttgart.de/am180.....	11
3.2 Virtual hosts.....	11
3.3 SSL / TLS Support.....	13
3.4 LDAP authentication.....	14
3.5 Mysql™ database administration.....	15
3.5.1 Installation.....	15
3.5.2 Konfiguration.....	15
3.5.3 phpMyAdmin.....	16
3.6 Providing WEB based user management dto your LDAP Server.....	16
3.6.1 LDAP Account Manager installieren.....	16
3.6.2 Konfiguration http://sdi9b.mi.hdm-stuttgart.de/lam aufrufen.....	16
3.7 Publish your documentation.....	17
4. File cloud.....	18
4.1 Voraussetzungen.....	18
4.2 Installation.....	18
4.2.1 PHP upgraden.....	18
4.2.2 Nextcloud herunterladen.....	19
4.2.3 Apache konfigurieren.....	19
4.2.4 Datenbank.....	19
4.2.5 SSL Verschlüsselung.....	19
4.2.6 /etc/apache/apache.conf.....	20
4.2.7 Apache site configuration.....	20
4.2.8 Installationsoberfläche.....	21
4.3 LDAP Benutzerauthentifizierung.....	21

5. Icinga.....	25
5.1 Server anpassen: PHP.....	25
5.2 Datenbank.....	25
5.2.1 Datenbank-Schema installieren.....	25
5.3 Installation.....	25
5.3.1 Token erstellen.....	26

1. DNS

1.1 Querying DNS data.

```
dig +noall +answer -t NS hdm-stuttgart.de
dig +noall +answer learn.medieninformatik.hdm-stuttgart.de
dig +noall +answer -t MX hdm-stuttgart.de
dig +noall +answer -x 141.62.64.28
```

```
root@sdi9a:~# dig +noall +answer -t NS hdm-stuttgart.de
hdm-stuttgart.de.      3600    IN      NS      iz-net-2.hdm-stuttgart.de.
hdm-stuttgart.de.      3600    IN      NS      iz-net-4.hdm-stuttgart.de.
hdm-stuttgart.de.      3600    IN      NS      dns3.belwue.de.
hdm-stuttgart.de.      3600    IN      NS      iz-net-3.hdm-stuttgart.de.
hdm-stuttgart.de.      3600    IN      NS      dns1.belwue.de.
root@sdi9a:~#
```

1.2 Installing Bind

```
sudo apt install bind9 bind9utils bind9-doc
sudo cp /etc/bind/db.empty /etc/bind/db.sdi9a.mi.hdm-stuttgart.de
```

Die Syntax der Zone Files ist sehr gewöhnungsbedürftig.

1.3 Reverse lookups

in "/named.conf.local":

```
...109.75.in-addr.arpa...
...file "/etc/bind/zones/db.109.75"...
```

```
sudo cp /etc/bind/db.127 ./db.109.75
62.141    IN      PTR      sdi9a.mi.hdm-stuttgart.de.
```

Die Syntax kann man per Befehl kontrollieren:

```
sudo named-checkconf
```

1.4 Forwarders

Innerhalb "named.conf.options" im "options{" part folgendes einfügen:

```
recursion yes;
forwarders { 8.8.8.8; 8.8.4.4; }; //google dns server
```

```
forwarders {
    0.0.0.0;
};
```

1.5 Mail exchange record

Im Zone File muss man folgendes Einfügen:

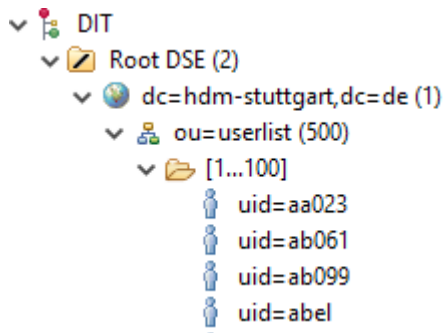
```
IN      MX      10      mx1.hdm-stuttgart.de.
```

2. LDAP

2.1 Browse an existing LDAP Server

Man Kann mit folgenden Daten den HDM LDAP Server durchforsten:

DN: uid=fi006,ou=userlist,dc=hdm-stuttgart,dc=de



2.2 Set up an OpenLdap server

apt install dialog && apt install slapd

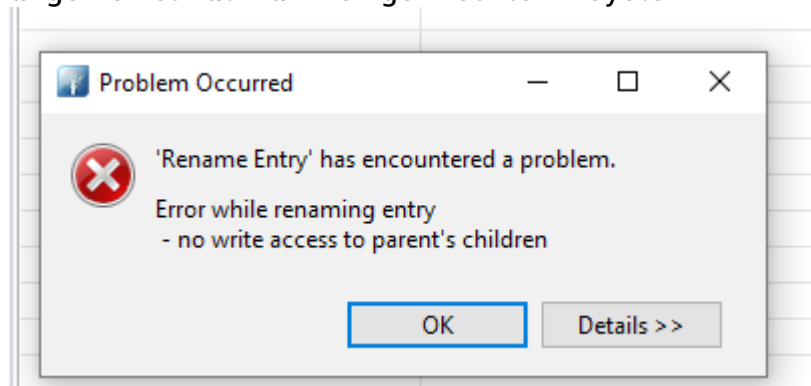
Und mit **dpkg-reconfigure slapd** den Server konfigurieren. Dies musste mehrere male wiederholt werden und die entsprechenden Ordner gelöscht, bevor es funktioniert.

2.3 Populating your DIT.

Mit **cn=admin,dc=betrayer,dc=com** als DN war es einfach den Server per UI zu füllen.

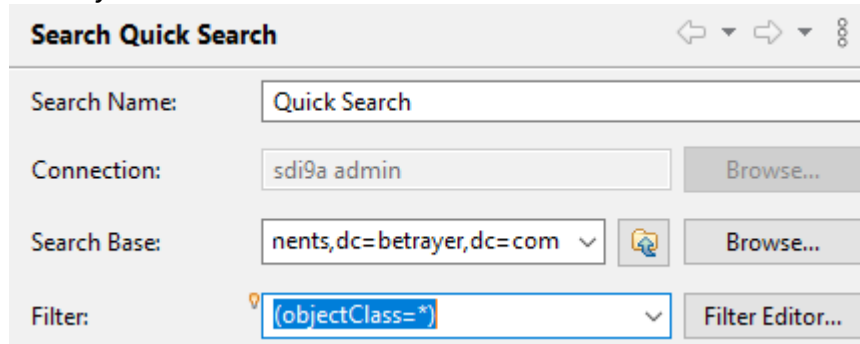
2.4 Testing a bind operation as non - admin user

Mit **uid=bean,ou=devel,ou=software,ou=departments,dc=betrayer;dc=com** angemeldet hat man weniger Rechte im System.



2.5 Filter based search

Mit `ldapsearch -x -b 'uid=b*'` über die CLI per Filter suchen, oder per Apache Directory UI.



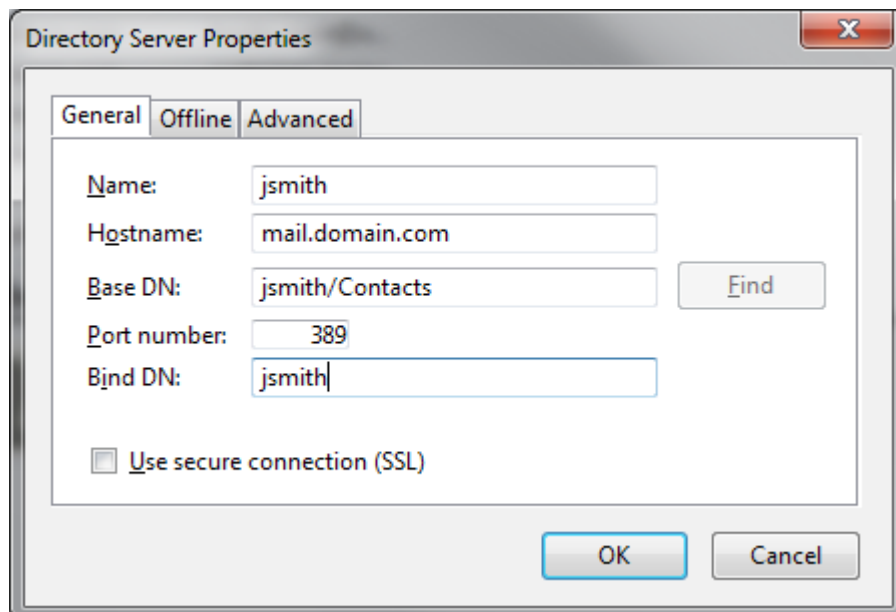
The screenshot shows the 'Search Quick Search' dialog box. It has a title bar with navigation icons. The fields are: 'Search Name' with the value 'Quick Search'; 'Connection' with 'sdi9a admin' and a 'Browse...' button; 'Search Base' with 'nents,dc=betrayer,dc=com' and a 'Browse...' button; and 'Filter' with '(objectClass=*)' and a 'Filter Editor...' button. There are also icons for undo, redo, and search.

2.6 Extending an existing entry

Ldif File mit gewünschten Änderungen (***objectClass =posixAccount, ...***) und **changetype: add** etwas hinzufügen, oder per **changetype: modify** etwas modifizieren.

2.7 Accessing LDAP data by a mail client

Es wird auf folgender seite gut erklärt: <https://answers.uillinois.edu/illinois/page.php?id=47790>



The screenshot shows the 'Directory Server Properties' dialog box, 'General' tab. It has fields for 'Name' (jsmith), 'Hostname' (mail.domain.com), 'Base DN' (jsmith/Contacts), 'Port number' (389), and 'Bind DN' (jsmith). There is a 'Find' button next to the 'Base DN' field. At the bottom, there is a checkbox for 'Use secure connection (SSL)' which is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

2.8 LDAP configuration

Ldapsearch per `ldapsearch -Y EXTERNAL -H ldapi:/// -b cn=config` zeigt 2 Datenbanken {0, 1}

```
# {0}config, config
dn: olcDatabase={0}config,cn=config
objectClass: olcDatabaseConfig
olcDatabase: {0}config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth manage by * break
olcRootDN: cn=admin,cn=config
olcRootPW: secret

# {1}mdb, config
dn: olcDatabase={1}mdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: {1}mdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=betrayer,dc=com
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to * by * read
olcLastMod: TRUE
olcRootDN: cn=admin,dc=betrayer,dc=com
olcRootPW: {SSHA}Sfp9WTFGDAP/KY9PVeYQFjyL4S5uG1N6
olcDbCheckpoint: 512 30
olcDbIndex: objectClass eq
olcDbIndex: cn,uid eq
```

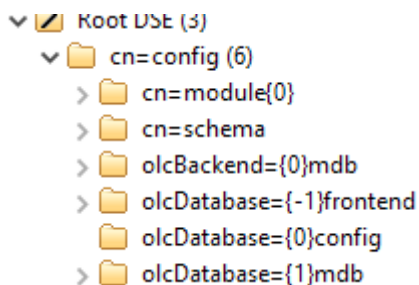
Mit einem Ldif File :

```
dn: olcDatabase={0}config,cn=config
```

```
add: olcRootPW
```

```
olcRootPW: {ssha}pHE+EPOG2gyRyOgjvFqsWOb5zGsG19CD
```

und `ldapmodify` kann man externen Zugriff erlangen.



2.9 LDAP based user login

Erst die Pam backupen per `tar zcf /root/pam.tgz pam.conf pam.d` und dann `apt install libpam-ldapd` installieren. Anschließend den Befehlen hier.

thomas-krenn.com/de/wiki/Passwort-Authentifizierung_mit_Active_Directory_unter_Debian_einrichten folgen.

Konfiguriere nslcd

Bitte geben Sie den Uniform Resource Identifier des benutzten LDAP-Servers ein. Das Format ist »ldap://<Rechnername oder IP-Adresse>:<Port>/«. Alternativ kann auch »ldaps://« oder »ldapi://« benutzt werden. Der Port muss nicht angegeben werden.

Wenn Sie »ldap« oder »ldaps« verwenden, sollten Sie eine IP-Adresse eingeben, um Ausfälle zu verhindern, falls die Namensauflösung einmal nicht verfügbar ist.

Mehrere URIs können, durch Leerzeichen getrennt, angegeben werden.

URI des LDAP-Servers:

ldapi:///

<Ok> <Abbrechen>

2.10 Backup and recovery / restore

Man kann per `slapcat -l ldif` ein Backup erstellen und per `slapadd -l ldif` ein Backup wieder einspielen.

3. Apache web server

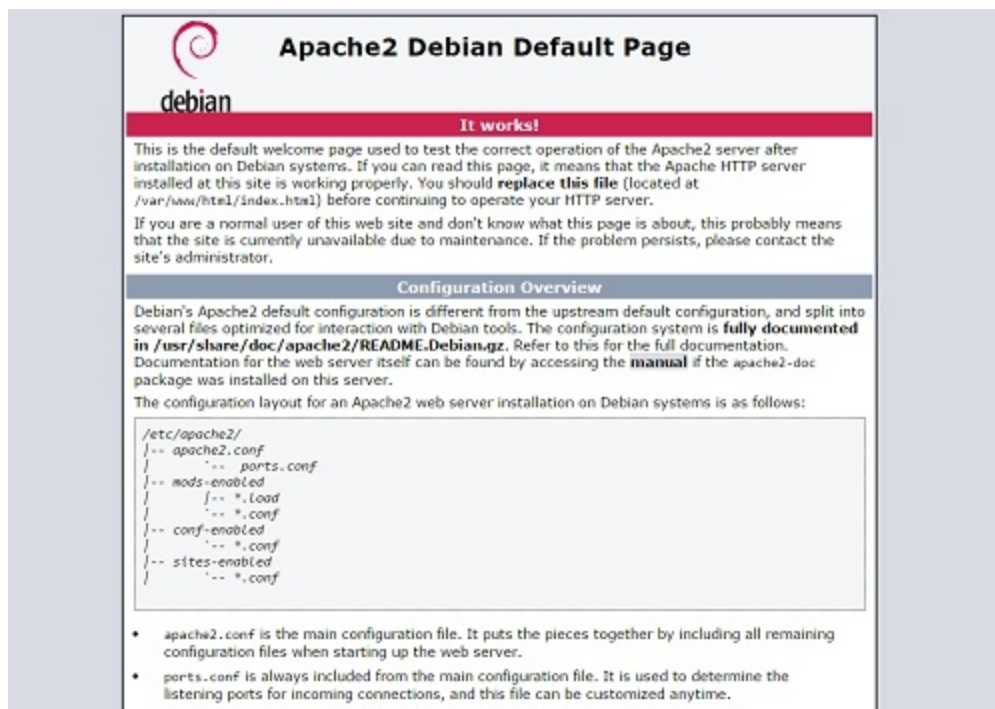
Install the Apache web server apache2 software package:

```
aptitude install apache2
```

3.1 First Steps

3.1.1 sdi9b.mi.hdm-stuttgart.de

Nach der Installation kann der WebServer über sdi9b.mi.hdm-stuttgart.de erreicht werden. Hier finden Sie hilfreiche Informationen zur Konfiguration des Servers.



3.1.2 Apache Dokumentation umbenennen

Apaches Startdokument wird von index.html in doc.html umbenannt.

```
mv index.html doc.html
```

3.1.3 Neue HTML-Datei einrichten

Da aktuell im Verzeichnis keine aufzurufende Index-Datei vorhanden ist, wird beim Aufruf des WebServers die Verzeichnisstruktur wiedergegeben. Im nächsten Schritt ist eine neue HTML-Datei zu erzeugen.

```
touch index.html
```

3.1.4 Apache Dokumentation installieren

apt-get install apache2-doc

3.1.5 sdi9b.mi.hdm-stuttgart.de/am180

Die Dokumentation auf den Server hochladen und mit /am180 erreichbar machen.

Neuen Ordner anlegen: **mkdir /var/www/html/home/sdidoc**

In den Verzeichnis wechseln: **cd /var/www/html/home/sdidoc**

Neue Datei anlegen: **touch index.html**

apache.conf bearbeiten: **nano /etc/apache2/apache2.conf**

Folgenden Skript einfügen:

```
Alias "/am180" "/var/www/html/home/am180"
<Directory /var/www/html/home/am180/>
    AllowOverride None
    Require all granted
</Directory>
```

3.2 Virtual hosts

<https://sdi9b.mi.hdm-stuttgart.de/am180>

<https://sdi9b.mi.hdm-stuttgart.de/manual>

Default-Konfigurationsdatei in /etc/apache2/sites-available/ duplizieren und umbenennen:

cp 000-default.conf am180.conf

cp 000-default.conf manual.conf

Skript am180.conf

```
NameVirtualHost *:80

<VirtualHost *:80>
    ServerName am180.mi.hdm-stuttgart.de

    ServerAdmin am180@hdm-stuttgart.de
    DocumentRoot /var/www/html/home/am180

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

BIND-Konfiguration anpassen, **am180** und **manual** als A records hinterlegen:

nano /etc/bind/db.sdi9b

```
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL      86400
@         IN      SOA      localhost. root.localhost. (
                        1      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200  ; Expire
                        86400 )  ; Negative Cache TTL
;

; main domain name servers
; name servers - NS records
@         IN      NS       sdi9b.mi.hdm-stuttgart.de.
@         IN      NS       am180.mi.hdm-stuttgart.de.
@         IN      NS       manual.mi.hdm-stuttgart.de.

; name servers - A records
sdi9b.mi.hdm-stuttgart.de.    IN      A       141.62.75.123
am180.mi.hdm-stuttgart.de.    IN      A       141.62.75.123
manual.mi.hdm-stuttgart.de.   IN      A       141.62.75.123
```

Für die beiden VirtualHosts muss die Konfiguration nur noch generiert werden und anschließend Apache neu starten.

```
a2ensite am180.conf
a2ensite manual.conf
service apache2 restart
```

Während den Übungen konnte mit Schwierigkeit die beiden VirtualHosts eingerichtet werden, leider sind diese wieder nicht zugänglich.

<https://am180.mi.hdm-stuttgart.de>
<https://manual.mi.hdm-stuttgart.de>

```
root@sdi9b:/etc/apache2# nslookup
> am180
Server:          141.62.64.21
Address:         141.62.64.21#53

** server can't find am180: NXDOMAIN
>
```

Ein Problem könnte die IP-Adresse sein in db.sdi9b.

3.3 SSL / TLS Support

Enable SSL:

a2enmod ssl

Zertifikat erzeugen:

openssl genrsa -des3 -out rootCA.key 2048

openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem

```
root@sdi9b:~# openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
Enter pass phrase for rootCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Baden-Württemberg
Locality Name (eg, city) []:Stuttgart
Organization Name (eg, company) [Internet Widgits Pty Ltd]:HdM
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:Aydin
Email Address []:am180@hdm-stuttgart.de
```

Es werden drei verschiedene Dateien erzeugt, diese müssen ausgelagert werden.

- device.key (private key)
- device.csr (certificate signing request)
- device.crt (signed certificate)

cp device.crt /etc/ssl/certs/sdi9bam180.crt

cp device.key /etc/ssl/private/sdi9bam180.key

Als letzten Schritt muss nur noch die jeweilige Apache-Konfiguration angepasst werden, indem auch auf die beiden oberen Dateien verlinkt wird:

```

GNU nano 2.7.4                                Datei: sites-available/am180.conf

NameVirtualHost *:443
NameVirtualHost *:80

<VirtualHost *:80>
    ServerName am180.mi.hdm-stuttgart.de

    ServerAdmin am180@hdm-stuttgart.de
    DocumentRoot /var/www/html/home/am180

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin am180@hdm-stuttgart.de
    ServerName am180.mi.hdm-stuttgart.de
    DocumentRoot /var/www/html/home/am180

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLOptions +StrictRequire
    SSLCertificateFile /etc/ssl/certs/sdi9bam180.crt
    SSLCertificateKeyFile /etc/ssl/private/sdi9bam180.key
</VirtualHost>

```

3.4 LDAP authentication

LDAP Konfiguration einrichten:

```
a2enmond ldap
```

```
a2enmond authnz_ldap
```

Neuen Datensatz (inetOrgPerson) in unserer Datenbank anlegen:

```
#!RESULT OK
```

```
#!CONNECTION ldap://sdi9b.mi.hdm-stuttgart.de:389
```

```
#!DATE 2021-01-18T08:24:33.679
```

```
dn:cn=tuser,ou=testing,ou=software,ou=departments,dc=betrayer,
dc=com
```

```
changetype:add
```

```
cn: tuser
```

```
sn: Testuser
```

```
objectClass: inetOrgPerson
```

```
objectClass: organizationalPerson
```

```
objectClass: person
```

```
objectClass: top
```

Dem Nutzer „tuser“ neues Attribut hinzufügen:

#!RESULT OK

#!CONNECTION ldap://sdi9b.mi.hdm-stuttgart.de:389

#!DATE 2021-01-18T08:33:23.103

dn: cn=tuser,ou=testing,ou=software,ou=departments,dc=betrayer,dc=com

changetype: modify

add: userPassword

userPassword: :e1NNRDV9NXdTZGdPV3JzZXRqRG1sY2cyM0xVN3FJOFloczhCM3A=

Nachdem Nutzer mit Passwort erzeugt worden ist, geht es in ApacheKonfiguration **/etc/apache2/apache.conf** weiter. Den bereits bestehenden „Directory“ erweitern:

```
<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    AuthName "Private"
    AuthType Basic
    AuthBasicProvider ldap
    AuthLDAPURL ldap://sdi9b.mi.hdm-stuttgart.de/ou=testing,ou=software,ou=departments,dc=betrayer,dc=com?uid
    Require valid-user
</Directory>
```

Apache neustarten und <https://sdi9b.mi.hdm-stuttgart.de/> aufrufen und sich einloggen

Benutzername: **tuser**

Passwort: **tusdi9b**

3.5 Mysql™ database administration

3.5.1 Installation

apt install mysql-server

3.5.2 Konfiguration

mysql_secure_installation

Dies führt Sie durch eine Reihe von Eingabeaufforderungen, in denen Sie einige Änderungen an den Sicherheitsoptionen Ihrer MySQL-Installation vornehmen können. Die erste Eingabeaufforderung fragt, ob Sie das validierte Passwort-Plugin einrichten möchten, mit dem Sie die Stärke Ihres MySQL-Passworts testen können. Unabhängig von Ihrer Wahl wird die nächste Eingabeaufforderung darin bestehen, ein Passwort für den MySQL-Root-Benutzer festzulegen.

Geben Sie ein sicheres Passwort Ihrer Wahl ein und bestätigen Sie es anschließend. Von dort aus können Sie Y und dann ENTER drücken, um die Standardwerte für alle folgenden Fragen zu übernehmen. Dadurch werden einige anonyme Benutzer und die Testdatenbank entfernt, Remote-Root-Logins deaktiviert und diese neuen Regeln geladen, so dass MySQL die von Ihnen vorgenommenen Änderungen sofort berücksichtigt.

Wenn die Konfiguration abgeschlossen ist, sollte folgende Meldung erscheinen:

"All done! If you've completed all of the above steps, your MariaDB installation should now be secure. Thanks for using MariaDB!"

3.5.3 phpMyAdmin

```
apt install phpmyadmin php-mbstring php-zip php-gd php-json php-curl
```

- Wählen Sie für die Serverauswahl apache2
- Wählen Sie Yes, wenn Sie gefragt werden, ob dbconfig-common zum Einrichten der Datenbank verwendet werden soll.
- Sie werden dann aufgefordert, ein MySQL-Anwendungspasswort für phpMyAdmin auszuwählen und zu bestätigen
- Der Installationsvorgang fügt die Apache-Konfigurationsdatei phpMyAdmin in das Verzeichnis /etc/apache2/conf-enabled/ ein, wo sie automatisch gelesen wird. Um die Konfiguration von Apache und PHP für die Arbeit mit phpMyAdmin abzuschließen, müssen Sie in diesem Abschnitt des Tutorials nur noch explizit die mbstring-PHP-Erweiterung aktivieren. Geben Sie dazu Folgendes ein:
 - **sudo phpenmod mbstring**
- Starten Sie anschließend Apache neu, damit Ihre Änderungen erkannt werden
 - **systemctl restart apache2**
- <http://sdi9b.mi.hdm-stuttgart.de/phpmyadmin/>

```
mysql -u root -> UPDATE mysql.user SET authentication_string =  
PASSWORD('sdi_9b') WHERE User = 'root' AND Host = 'localhost';
```

Datenbank neustarten:

```
systemctl start mariadb
```

3.6 Providing WEB based user management to your LDAP Server

3.6.1 LDAP Account Manager installieren

```
apt -y install ldap-account-manager
```

3.6.2 Konfiguration

<http://sdi9b.mi.hdm-stuttgart.de/lam> aufrufen

- Navigieren durch
 - [LAM configuration]
 - Edit server profiles -> Default password is lam

Zu Beginn das Kennwort unter „General Settings“ aktualisieren!

LDAP Server Adresse aktualisieren:

Server address **sdi9b.mi.hdm-stuttgart.de**
Tree suffix: **dc=betrayer,dc=com**
Security settings:
 List of valid users: **cn=admin,dc=betrayer,dc=com**

3.7 Publish your documentation

<https://sdi9b.mi.hdm-stuttgart.de/doc/>

PDF Dokumentation

4. File cloud

Nextcloud ist eine **Open-Source-Software**, die Cloud-Lösungen für private Personen und Unternehmen anbietet. Ehemalige Entwickler von ownCloud haben die Plattform entwickelt und sie im Juni 2016 auf den Markt gebracht. Sie ist für mehrere Betriebssysteme, wie Windows, MacOS, iOS, Linux und Android verfügbar.¹

Mit der Cloud-Software können Nutzer ihre Dateien auf eigenen Servern hinterlegen. Das heißt, es handelt sich entweder um einen privaten Server oder um einen Server bei einem Provider. Nextcloud setzt darauf, dass Anwender die Hoheit über ihre Dateien behalten. So können Nutzer immer selbst entscheiden, wo Dokumente oder Fotos abgelegt werden und wer darauf Zugriff hat.

4.1 Voraussetzungen

Betriebssystem	Ubuntu 20.04 LTS (empfohlen) Red Hat Enterprise Linux 8 (empfohlen) Debian 10 (Buster) SUSE Linux Enterprise Server 15 openSUSE Leap 42.1+ CentOS 8
Webserver	Apache 2.4 (empfohlen) nginx
Datenbank	MySQL 8.0+ or MariaDB 10.2+ (empfohlen) Oracle Database 11g PostgreSQL 9.6/10/11 SQLite
PHP	7.3, 7.4 (empfohlen)

4.2 Installation

4.2.1 PHP upgraden

Aufgrund vorheriger Übungen entspricht unsere aktuelle PHP-Version nicht den Mindestvoraussetzungen für die Installation von Nextcloud. Hierfür muss je nach System die PHP Version aktualisiert werden.

```
apt install software-properties-common
apt install apt-transport-https lsb-release ca-certificates curl -y
```

```
wget -O /etc/apt/trusted.gpg.d/php.gpg |
```

¹ <https://teamdrive.com/nextcloud-eine-komplett-kostenlose-cloud-loesung/>

<https://packages.sury.org/php/apt.gpg>

```
sh -c ,echo „deb https://packages.sury.org/php/ |  
$(lsb_release -sc) main“ > /etc/apt/sources.list.d/php.list'
```

```
apt update
```

```
apt install php7.4 php7.4-common php7.4-cli
```

4.2.2 Nextcloud herunterladen

In diesem Schritt wird die Cloud-Installation auf den Server heruntergeladen und in den für den WebServer ausgelegten Ordner verschoben.

```
wget https://download.nextcloud.com/server/releases/latest.zip  
unzip latest.zip  
mv nextcloud/ /var/www
```

4.2.3 Apache konfigurieren

Nextcloud Installation erfordert einige Serveranpassungen.

```
a2enmod rewrite  
a2enmod headers  
a2enmod env  
a2enmod dir  
a2enmod mime  
a2enmod proxy  
a2enmod proxy_http  
a2enmod proxy_wstunnel
```

4.2.4 Datenbank

Nachdem Mysql/MariaDB erfolgreich eingerichtet worden ist (siehe *mysql_secure_installation*) kann über die Konsole eine separate Datenbank für die Nextcloud-Umgebung eingerichtet werden.

```
mysql -u root -p
```

```
CREATE DATABASE nextcloud;  
GRANT ALL ON nextcloud.* to ,nextcloud'@'localhost'  
IDENTIFIED BY ,YOURdbPASSWORD';  
FLUSH PRIVILEGES;  
exit
```

4.2.5 SSL Verschlüsselung

Um sichere Datentransport gewährleisten zu können, ist ein SSL Zertifikat zu generieren.

```
apt install python-certbot-apache  
certbot
```

4.2.6 /etc/apache/apache.conf

Damit die Installationsumgebung über <http://sdi9b.mi.hdm-stuttgart.de/nextcloud> erreichbar ist, muss dieser noch in apache.conf konfiguriert werden.

```
Alias "/nextcloud" "/var/www/html/nextcloud"
<Directory /var/www/html/nextcloud/>
    Options +FollowSymlinks
    AllowOverride All
    SetEnv HOME /var/www/html/nextcloud
    SetEnv HTTP_HOME /var/www/html/nextcloud
    Satisfy Any
</Directory>
```

4.2.7 Apache site configuration

Desweiteren ist eine separate Konfigurationsdatei für Apache noch zu herunterladen und anschließend anzupassen.

```
cd /etc/apache2/sites-available/
wget https://raw.githubusercontent.com/dicenl/nextcloud/master/vhost.conf
mv vhost.conf nextcloud.conf
nano nextcloud.conf
```

```
GNU nano 2.7.4      Datei: sites-available/nextcloud.conf      Verändert
<IfModule mod_ssl.c>
    <VirtualHost *:80>
        ServerName sdi9b.mi.hdm-stuttgart.de
        Redirect permanent / https://sdi9b.mi.hdm-stuttgart.de/nextcloud/
    </VirtualHost>

    <VirtualHost *:443>
        DocumentRoot "/var/www/html/nextcloud"
        ServerName sdi9b.mi.hdm-stuttgart.de
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        Alias "/nextcloud" "/var/www/html/nextcloud"
        <Directory /var/www/html/nextcloud/>
            Options +FollowSymlinks
            AllowOverride All
            SetEnv HOME /var/www/html/nextcloud
            SetEnv HTTP_HOME /var/www/html/nextcloud
            Satisfy Any
        </Directory>

        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/apache.pem
        SSLCertificateKeyFile /etc/apache2/ssl/apache.key

        <IfModule mod_headers.c>
            Header always set Strict-Transport-Security "max-age=1555200$"
        </IfModule>
    </VirtualHost>
</IfModule>
```

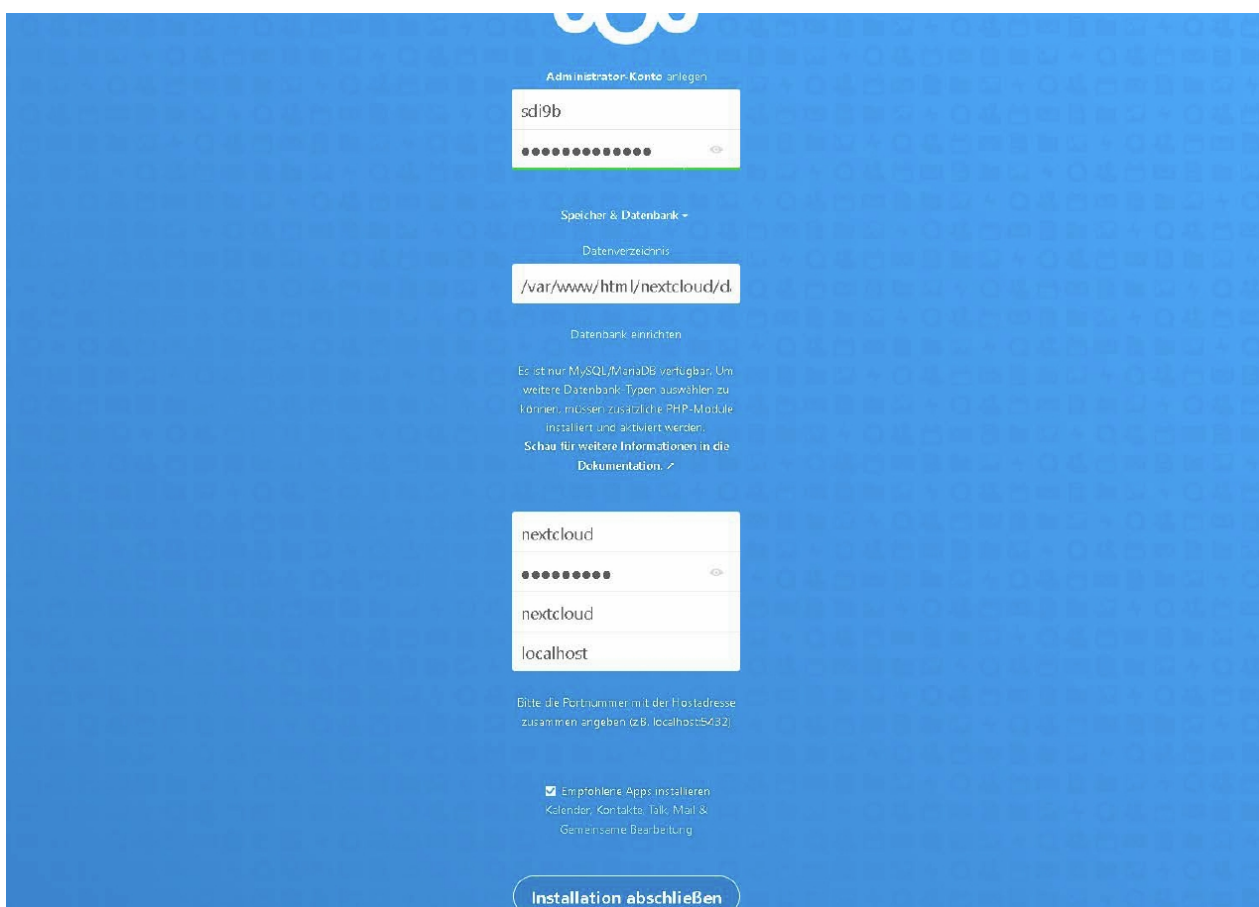
Anschließend muss die Konfiguration noch aktiviert werden und die involvierten Dienste neugestartet werden.

```
a2ensite nextcloud.conf
```

```
systemctl restart apache2
systemctl enable apache2
systemctl restart mariadb
systemctl enable mariadb
```

4.2.8 Installationsoberfläche

Nach Durchführen aller Schritte kann über den Nextcloud-Link die Oberfläche zum Installieren abgerufen werden. Zur weiteren Installation sind Zugangsdaten für die Nextcloud-Umgebung und die Datenbank einzutragen.

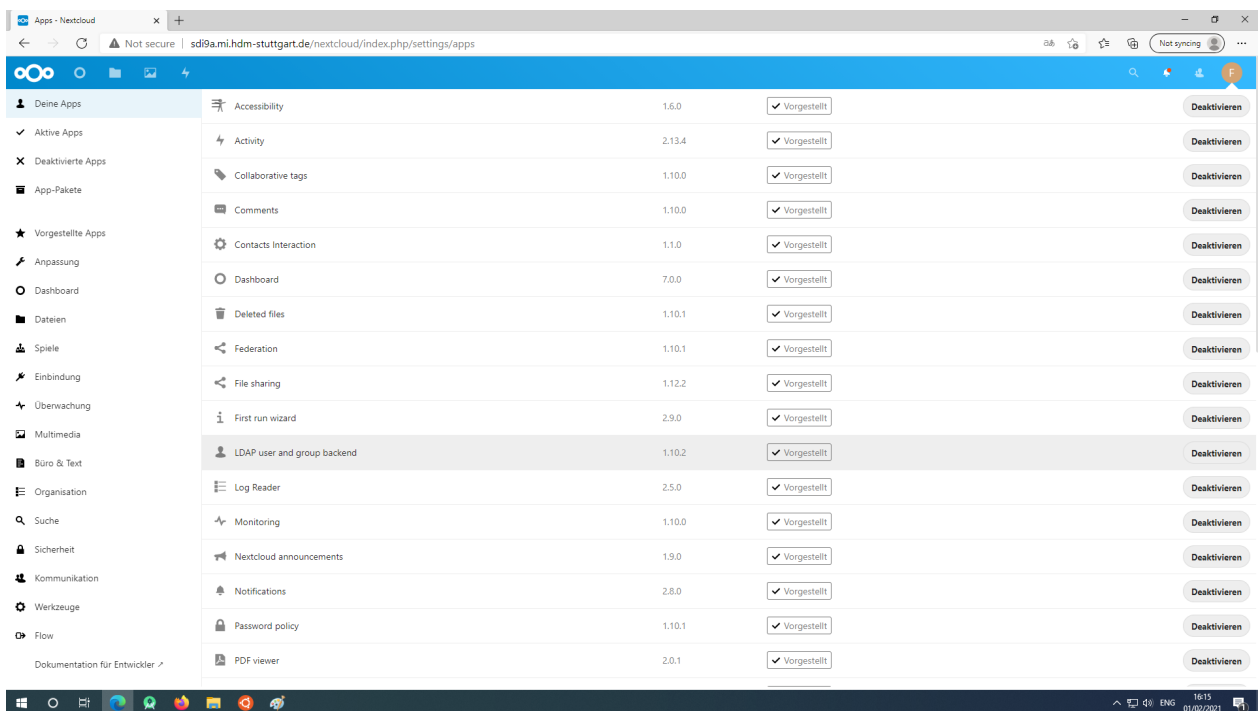
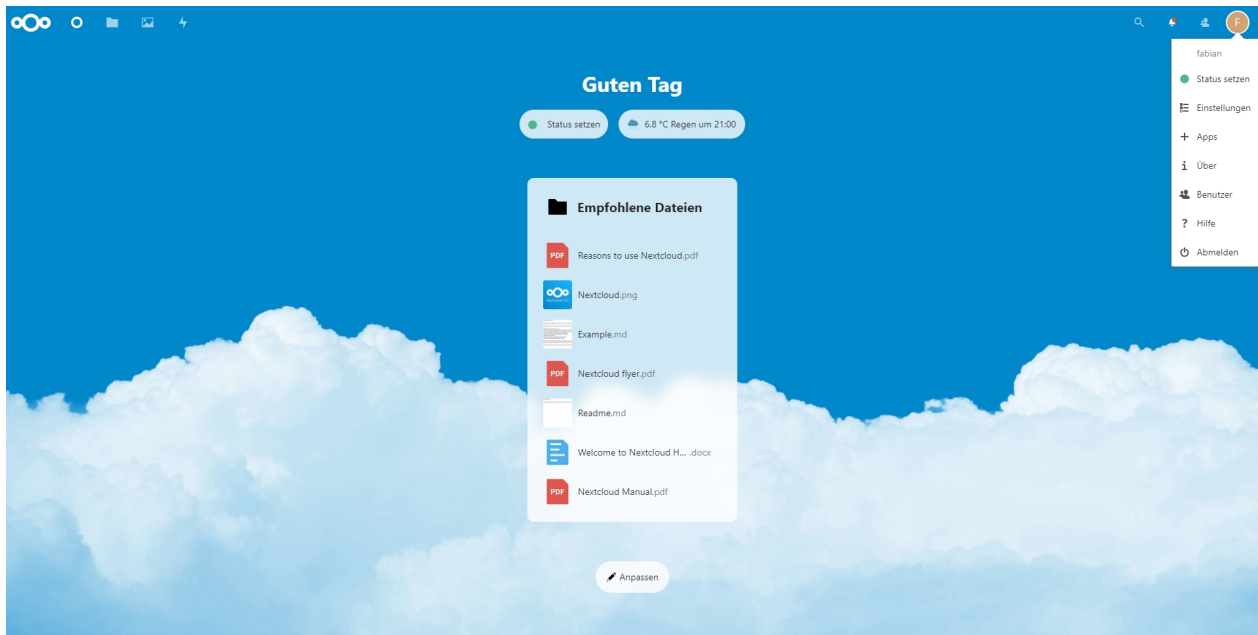


The screenshot shows the Nextcloud installation wizard on a blue background. The steps are as follows:

- Administrator-Konto anlegen**: A text input field contains 'sdl9b' and a password field with 10 dots and an eye icon.
- Speicher & Datenbank**:
 - Datenverzeichnis**: A text input field contains '/var/www/html/nextcloud/'.
 - Datenbank einrichten**: A message states: 'Es ist nur MySQL/MariaDB verfügbar. Um weitere Datenbank-Typen auswählen zu können, müssen zusätzlich die PHP-Module installiert und aktiviert werden. Schau für weitere Informationen in die Dokumentation.' Below this is a link 'Dokumentation' with a checkmark icon.
- nextcloud**: A text input field contains 'nextcloud', a password field with 10 dots and an eye icon, and a dropdown menu with 'nextcloud' and 'localhost' as options.
- A note: 'Bitte die Portnummern mit der Hostadresse zusammen angeben (z.B. localhost:5432)'.
- A checkbox labeled 'Empfohlene Apps installieren' (checked) with subtext 'Kalender, Kontakte, Talk, Mail & Gemeinsame Bearbeitung'.
- A button at the bottom: 'Installation abschließen'.

4.3 LDAP Benutzerauthentifizierung

Die Anforderung ist es, Nextcloud-Login mit den LDAP-Nutzern aus **ldap1.hdm-stuttgart.de** zu ermöglichen. Hierfür öffnen wir nach der Anmeldung die Einstellungen für Nextcloud und aktivieren die App „**LDAP user and group backend**“.



Nachdem Aktivieren der App öffnen wir die Anwendung zum Bearbeiten und tragen unsere Eckdaten zur Verbindungsherstellung ein:

The screenshot shows the 'LDAP / AD Integration' setup page in a web browser. The left sidebar contains navigation links under 'Persönlich' and 'Verwaltung'. The main content area is titled 'LDAP / AD Integration' and has tabs for 'Server', 'Benutzer', 'Anmelde-Attribute', and 'Gruppen'. The 'Server' tab is active. It shows a list of servers with one entry: '1. Server: ldap1.hdm-stuttgart.de'. Below this, there are input fields for 'ldap1.hdm-stuttgart.de', '389', 'uid=foo6, ou=userlist, dc=hdm-stuttgart, dc=de', and a password field. There are buttons for 'Port ermitteln', 'Zugangsdaten speichern', 'Base DN ermitteln', and 'Base DN testen'. A checkbox for 'LDAP-Filter manuell eingeben' is present. At the bottom, it says 'Konfiguration OK' and has a 'Fortsetzen' button.

The screenshot shows the 'LDAP / AD Integration' setup page, now on the 'Benutzer' (Users) tab. It displays configuration options for user listing and search. A dropdown menu shows 'Nur diese Objektklassen: hdmStudent, inetOrgPerson'. Below this, there is a text box explaining that these are the most common object classes for users. Another dropdown menu shows 'Nur aus diesen Gruppen: Gruppen auswählen'. There is a link to 'LDAP-Abfrage bearbeiten'. The LDAP-Filter is set to '(&(objectclass=hdmStudent)(objectclass=inetOrgPerson))'. At the bottom, there is a button 'Einstellungen überprüfen und Benutzer zählen' and a status '500 Benutzer gefunden'. The 'Konfiguration OK' message and 'Fortsetzen' button are also present.

Server

Benutzer

Anmelde-Attribute

Gruppen

Fortgeschritten

Exportieren

Beim Anmelden wird Nextcloud den Benutzer basierend auf folgenden Attributen finden:

LDAP-/AD-Benutzernamen: ☒

LDAP-/AD-E-Mail-Adresse: ☒

Andere Attribute: **Attribute auswählen**

[LDAP-Abfrage bearbeiten](#)

LDAP-Filter: (&(((objectclass=hdnStudent)(objectclass=inetOrgPerson)))(uid=%uid)(mailPrimaryAddress=%uid)(mail=%uid)))

Anmeldenamen testen

Einstellungen überprüfen

Konfiguration OK

Zurück

Fortsetzen

Hilfe

5. Icinga

5.1 Server anpassen: PHP

```
nano /etc/php/7.4/apache2/php.ini

    php_value max_execution_time 300
    php_value memory_limit 128M
    php_value max_input_time 300
    date.timezone = Europe/London
    opcache.enable=1
    opcache.enable_cli=1
    opcache.interned_strings_buffer=8
    opcache.max_accelerated_files=10000
    opcache.memory_consumption=128
    opcache.save_comments=1
    opcache.revalidate_freq=1
```

```
systemctl restart apache2
```

5.2 Datenbank

```
mysql -u root -p

    create database icingadb;
    grant all privileges on icingadb.* to      'icinga_user'@'local-
host' identified by 'icinga_pass';
    flush privileges
    exit
```

5.2.1 Datenbank-Schema installieren

```
mysql -u root icingadb -p < /usr/share/icinga2-ido-mysql/schema/
mysql.sql
```

5.3 Installation

```
apt install icinga2 icinga2-ido-mysql
```

```
systemctl start icinga2.service
icinga2 feature enable ido-mysql
icinga2 feature enable command
systemctl restart icinga2
```

```
apt install icingaweb2 icingacli
apt install icingaweb2 libapache2-mod-php icingacli
```

```
apt install python3-software-properties
add-apt-repository ppa:ondrej/php
```

5.3.1 Token erstellen

```
icingacli setup token create
```

Token kann leider nicht erstellt werden:

```
PHP Fatal error:  Uncaught Exception: "continue" targeting switch is equivalent
to "break". Did you mean to use "continue 2"? in /usr/share/php/Icinga/Application/Mo
dules/Module.php:689
Stack trace:
#0 /usr/share/php/Icinga/Application/ClassLoader.php(306): Icinga\Application\Applika
tionBootstrap->Icinga\Application\{closure}()
#1 /usr/share/php/Icinga/Application/ClassLoader.php(306): require()
#2 [internal function]: Icinga\Application\ClassLoader->loadClass()
#3 /usr/share/php/Icinga/Application/Modules/Manager.php(225): spl_autoload_call()
#4 /usr/share/php/Icinga/Application/ApplicationBootstrap.php(407): Icinga\Applcatio
n\Modules\Manager->loadModule()
#5 /usr/share/php/Icinga/Application/Cli.php(46): Icinga\Application\ApplicationBoots
trap->loadSetupModuleIfNecessary()
#6 /usr/share/php/Icinga/Application/ApplicationBootstrap.php(336): Icinga\Applcatio
n\Cli->bootstrap()
#7 /usr/bin/icingacli(7): Icinga\Application\ApplicationBootstrap::start()
#8 {main}
   thrown in /usr/share/php/Icinga/Application/Modules/Module.php on line 689

Fatal error: Uncaught Exception: "continue" targeting switch is equivalent to "b
reak". Did you mean to use "continue 2"? in /usr/share/php/Icinga/Application/Modules
/Module.php:689
Stack trace:
#0 /usr/share/php/Icinga/Application/ClassLoader.php(306): Icinga\Application\Applika
tionBootstrap->Icinga\Application\{closure}()
#1 /usr/share/php/Icinga/Application/ClassLoader.php(306): require()
#2 [internal function]: Icinga\Application\ClassLoader->loadClass()
#3 /usr/share/php/Icinga/Application/Modules/Manager.php(225): spl_autoload_call()
#4 /usr/share/php/Icinga/Application/ApplicationBootstrap.php(407): Icinga\Applcatio
n\Modules\Manager->loadModule()
#5 /usr/share/php/Icinga/Application/Cli.php(46): Icinga\Application\ApplicationBoots
trap->loadSetupModuleIfNecessary()
#6 /usr/share/php/Icinga/Application/ApplicationBootstrap.php(336): Icinga\Applcatio
n\Cli->bootstrap()
#7 /usr/bin/icingacli(7): Icinga\Application\ApplicationBootstrap::start()
#8 {main}
   thrown in /usr/share/php/Icinga/Application/Modules/Module.php on line 689
```

Unsere Recherche hat ergeben, dass die aktuelle PHP Version 7.4 eventuell mit icinga Probleme hat. Aus diesem Grund ist auch die Oberfläche nicht abrufbar.

<https://sdi9b.mi.hdm-stuttgart.de/icingaweb2/setup>

```
Deprecated: array_key_exists(): Using array_key_exists() on ob-
jects is deprecated. Use isset() or property_exists() instead
in /usr/share/icingaweb2/library/vendor/Zend/Registry.php on line
201
```

Deprecated: array_key_exists(): Using array_key_exists() on objects is deprecated. Use isset() or property_exists() instead in /usr/share/icingaweb2/library/vendor/Zend/Registry.php on line 201

Fatal error: Uncaught RuntimeException: session_name(): Cannot change session name when session is active in /usr/share/php/Icinga/Web/Session/PhpSession.php:97 Stack trace: #0 [internal function]: Icinga\Application\ApplicationBootstrap->Icinga\Application\{closure}() #1 /usr/share/php/Icinga/Web/Session/PhpSession.php(97): session_name() #2 /usr/share/php/Icinga/Web/Session/PhpSession.php(152): Icinga\Web\Session\PhpSession->open() #3 /usr/share/php/Icinga/Web/Controller/ActionController.php(544): Icinga\Web\Session\PhpSession->write() #4 /usr/share/php/Icinga/Web/Controller/ActionController.php(489): Icinga\Web\Controller\ActionController->shutdownSession() #5 /usr/share/icingaweb2/library/vendor/Zend/Controller/Action.php(512): Icinga\Web\Controller\ActionController->postDispatch() #6 /usr/share/php/Icinga/Web/Controller/Dispatcher.php(76): Zend_Controller_Action->dispatch() #7 /usr/share/icingaweb2/library/vendor/Zend/Controller/Front.php(937): Icinga\Web\Controller\Dispatcher->dispatch() #8 /usr/share/php/Icinga/Apply in /usr/share/icingaweb2/library/vendor/Zend/Controller/Plugin/Broker.php on line 332

Wahrscheinlich müssten wir PHP downgraden, jedoch kann es zu Konflikten mit anderen Installationen kommen. Deswegen haben wir die Aufgabe bis hierhin durchgeführt.