# **OPENID Keycloak Anbindung Proxmox**



Spenden

Zum frei verfügbaren Apt-Repository



Die folgende Dokumentation zeigt die Keycloakanbindung von Proxmox inkl. Login berechtigten Gruppen. Als Backend wird LDAP von UCS (Univention) verwendet. Für das ganze Vorhaben wird eine ähnlich funktionierende Umgebung voraus gesetzt.

Verwendete Systeme/Software:

- Proxmox 8.1.4
- UCS 5.0-6 errata993
- Keycloak installiert am Primary Directory Node (ohne verteilter Datenbank) 23.0.7

Proxmoxclusternodes:

- pve01.tux.lan
- pve02.tux.lan
- pve03.tux.lan

Primary Directory Node: dc1.tux.lan

## **OpenID Client in Keycloak hinzufügen**

Unter dem Realm "ucs" wird ein neuer Client names "proxmox-cluster01" hinzugefügt. Die Basiseinrichtung erfolgt in 3 Schritten:

1. Erstellen eines neuen Clients



Last update: 2025/05/18 virtualisierung:proxmox\_kvm\_und\_lxc:openid\_keycloak\_anbindung\_proxmox https://deepdoc.at/dokuwiki/doku.php?id=virtualisierung:proxmox\_kvm\_und\_lxc:openid\_keycloak\_anbindung\_proxmox 09:02

2.	Setzen	des	"Client	type"	und	der	"Client-ID"
----	--------	-----	---------	-------	-----	-----	-------------

Clients > Create client

#### Create client

Clients are applications and services that can request authentication of a user.

<ol> <li>General settings</li> </ol>	Client type ①	OpenID Connect
2 Capability config	1	
3 Login settings	Client-ID * 🗇	proxmax-cluster01
	Name 💮	
	Beschreibung 🕤	
	Always display in UI	Off Off
	Next Back	Abbrechen
Clients > Create client		
Create client		
Clients are applications and	services that can request authentication of	of a user.

General settings     Capability config     Jucgin settings	Client authentication	Off Off	
	Authentication flow	🛃 Standard flow	🗸 Direct access grants 🖱
		Implicit flow (5)	Service accounts roles @
		OAuth 2.0 Device Authoriza	ation Grant @
		OIDC CIBA Grant®	
	Next Back	Abbrechen	

3. Setzen der "Vaild redirect URI's

025/08/26 09:13		3/10	OPENID Keycloa
Create client Clients are applications and service	ces that can request authen	tication of a user.	
1 General settings	Root URL		
<ol> <li>Capability config</li> <li>Login settings</li> </ol>	Home URL		-
	Valid redirect URIs ③	https://pve01.tux.larc8006	_
		https://pve02.tux.lan:8006 https://pve03.tux.lan:8006	
		Add valid redirect URIs	
	Valid post logout redirect URIs ③	Add valid past logout redirect LIRIs	_
	Web Origins ①		-
		Q Add web origins	
	Speichern Bo	ck Abbrechen	

Für unser späteres Vorhaben "nur bestimmte Gruppen zu zulasssen", müssen nach dem "Speichern" noch zwei weitere Optionen unter **"Einstellungen"** aktiviert werden. Dies schaltet weitere Funktionen frei.

Anbindung Proxmox

Capability config	1	
Client authentication	On On	
Authorization ⑦		
Authentication flow	✓ Standard flow ⊚	🗸 Direct access grants 🔊
	Implicit flow	Service accounts roles 🔊
	OAuth 2.0 Device Authorization Gra	ant 🔊
	OIDC CIBA Grant 🔊	

Damit wäre die Basiseinrichtung abgeschlossen.

## Konfiguration OpenID auf Proxmox

Hier bedient man sich am besten der CMD. Bevor man dies tut muss man sich aber noch das **"Client** Secret" kopieren.

Last update: 2025/05/18 09:02

ad .
Clerits > Olerit datal     proximon-cluster(O) OpenD Cannot Cherts are applications and services that can request extendication of a case.      Clerit are applications and services that can request extendication of a case.      Clerit Autoentication     Clerit Id and Secret      Clerit Id and Secre
Jaacad I

Danach wird folgender Befehl auf der Rootshell von Proxmox abgesetzt:

```
pveum realm add tux.lan-SSO --type openid --issuer-url
https://ucs-sso-ng.tux.lan/realms/ucs --client-id proxmox-cluster01 --
client-key XXXXX --username-claim username
```

 -autocreate wäre optional. Damit werden Benutzer beim Ersten Login automatisch angelegt. Ab dem Zeitpunkt ist der Login mittels SSO/SAML möglich. Man hat aber noch keine Rechte.
 Berechtiungen müssen manuell im Proxmox Webinterface für den/die Benutzer hinzugefügt werden.
 Berechtigungen werden "on the fly" übernommen.

Die Empfehlung ist hier eine Gruppe im Proxmox Webinterface zu erstellen und den Benutzer dort einfach hinzuzufügen.

Datacenter → Permissions → Groups Gruppe anlegen, z.B. "admin" Datacenter → Permissions → Users Gewünschten Benutzer bearbeiten und die Gruppe "admin" zuweisen.

## Einschränkung auf Gruppen

Um überhaupt zu den LDAP-Gruppen zu kommen, muss ein **"group-Idap-mapper"** hinzugefügt werden. Hierzu wechselt man im Menü von Keycloak auf **"User federation"** und bearbeitet den **"Idap-provider"**. Im TAB Mappers, fügt man nun den **"group-Idap-mapper"** hinzu.

5/10

User federation > Einstellungen

#### LDAP

Einstellungen Mappers	
Q Search for mapper → Add mapper	
Name	Тур
creation date	user-attribute-Idap-mapper
displayName	user-attribute-Idap-mapper
email	user-attribute-Idap-mapper
entryUUID	user-attribute-Idap-mapper
first name	user-attribute-Idap-mapper
group-Idap-mapper	group-Idap-mapper
last name	user-attribute-Idap-mapper
modify date	user-attribute-Idap-mapper
second-mail	user-attribute-Idap-mapper
uid	user-attribute-Idap-mapper
Univention Idap mapper	univention-Idap-mapper
username	user-attribute-Idap-mapper

### Der Inhalt wurde auf einen Default UCS-LDAP angepasst.

Attributbeschreibung	Attributname	Info
ID	auto generiert	
Name	group-ldap-mapper	
Mapper type	group-ldap-mapper	
LDAP Groups DN	cn=tux-groups,cn=groups,dc=tux,dc=lan	Beispiel
Group Name LDAP Attribute	cn	
Group Object Classes	posixGroup	
Preserve Group Inheritance	OFF	
Ignore Missing Groups	OFF	
Membership LDAP Attribute	memberUid	
Membership Attribute Type	UID	
Membership User LDAP Attribute	uid	
LDAP Filter	(&(uid=%s)(memberof=cn=proximoxi,cn=tux-groups,cn=groups,dc=tux,dc=lan))	Kann verwendet werden um noch granularer zu werden.
Mode	READ_ONLY	
User Groups Retrieve Strategy	LOAD_GROUPS_BY_MEMBER_ATTRIBUTE	
Member-Of LDAP Attribute	memberOf	

Last update: 2025/05/18 09:02

Attributbeschreibung	Attributname	Info
Mapped Group Attributes		
Drop non-existing groups during sync	OFF	
Groups Path	/	Dies zu Ändern macht bei vielen Gruppen vielleicht Sinn.

Danach **"Speichern"**, nochmal einsteigen und rechts oben auf **"Aktion → Sync LDAP groups to Keycloak"** anklicken. Damit sollte eine grüne Infomeldung aufpoppen wo die gesyncten Gruppen angezeigt werden. Damit sind unter **"Gruppen"** nun auch alle Gruppen und Groupmembers in Keycloak ersichtlich.

<b>WIKEYCLOAK</b>		
	Q, Gruppen suchen →	< Gruppen
Venuiten	Exact search	Eine Gruppe ist eine Sammlung von Attributen und R bearbeiten und löschen sowie deren Hierarchie von K
Client scopes Resim-Rollen	backuppc-web	Q, Filter groups   Gruppe en
Benutzer Gruppen	benno-mailarchiv I bilderarchiv I	Gruppername
Sessions	steve steation	benno-malachiv
Kasha share	torium de É	bidenetiv
Realm-Einstellungen	eranakee rigevaa i	destances
Authentiftplerung Identity providers	Len I	
User federation	ye linder only was 1	1100 1100 VA2

### Userimport und automatischer Sync in Echtzeit (optional)

Dieser Schritt muss nicht durchgeführt werden. Keycloak schaut auch jedes mal gerne am LDAP Live nach welche Benutzer es gibt. Aus Performancegründe macht es bei größeren Installationen Sinn die Benutzer direkt in die lokal MariaDB zu syncen. Hier zu bearbeitet man wieder den **"Idap-provider"** und aktiviert bei **"Synchronization settings"** das Flag bei **Import users**. Danach einmal abspeichern.



Jetzt hat man in der rechten oberen Ecke unter **"Aktion"** eine neue freigechaltete Funktion: **"Sync all users"**. Hier sollte wiedermals eine grüne Infomeldung aufpoppen wo die gesyncten Benutzer angezeigt werden. Nach dieser Aktion möchte man auch noch den Livesync der User und Gruppenmitgliedschaften aktivieren. Hierzu noch das folgende Flag auf "On" schalten.

Synchronization settings				
Import users 💿	On On			
Sync Registrations ①	Off			
Batch size 💿	1000			
Periodic full sync 🛞	Off			
Periodic changed users sync 💿	On On			
Changed users sync period ⑦	-1			

Beim Speichern der Einstellungen deaktiviert sich dieses Flag wieder. ...scheint aber zu funktionieren, weil die richtigen Info's in Keycloak angezeigt werden.

×

## Einrichtung der Authorization im proxmox-cluster01 Client

Als erstes muss im Client die "Default Policy gelöscht werden".

Clents > Clent details	OpenID Connect			Aktiv 🕲 Aktion 🕶
Clients are applications and se	vices that can n	equest authentication of a user.		_
Einstellungen Keys	Passwörter	Rollen Client scopes Authorization	Service accounts roles Sessions Advanced	
Einstellungen Resour	ces Scopes	Policies Berechtigungen Evaluate	Export	
Search for permission		Create client policy		1-1 + (-
Name	Тур	Dependent permission	Beachreibung	
Default Policy	al.	Default Permission	A policy that grants access only for users within this realm	

### Nun fügen wir eine neue Group-Policy hinzu.

#### Choose a policy type

Choose one policy type from the list below and then you can configure a new policy for authorization. There are some types and description.

Name	Beschreibung
Client	Define conditions for your permissions where a set of one or more clients is permitted to access an object.
Client Scope	Define conditions for your permissions where a set of one or more client scopes is permitted to access an object.
Group	Define conditions for your permissions where a set of one or more groups (and their hierarchies) is
	permitted to access an object.
Regex	Define regex conditions for your permissions.
Regex Role	Define regex conditions for your permissions. Define conditions for your permissions where a set of one or more roles is permitted to access an object.
Regex Role Time	permitted to access an object.         Define regex conditions for your permissions.         Define conditions for your permissions where a set of one or more roles is permitted to access an object.         Define time conditions for your permissions.

Last update: 2025/05/12 virtualisierung:proxmox\_kvm\_und\_lxc:openid\_keycloak\_anbindung\_proxmox https://deepdoc.at/dokuwiki/doku.php?id=virtualisierung:proxmox\_kvm\_und\_lxc:openid\_keycloak\_anbindung\_proxmox 09:02

Clients > Client details > Create client policy

#### Create group policy

Name * 🗇	proxmox-zugang01				
Beschreibung 💮	Gruppeneinschraenkung fuer den Clusterzugang				
Groups claim 💿					
Gruppen * 💿	Add groups				
	Gruppen	Extend to children			
	/testgruppebla		٥		
	/gitlab		٥		
Logic 💿	Positive				
	O Negative				
	Speichern Abbrechen				
	Die folgender sollen also be können.	n zwei Gruppen "testgrup rechtigt sein sich auf der	pebla" und "gitl n Cluster einlog		

Im nächsten Schritt fügen wir nun noch die Berechtigungen hinzu.



9/10

Clients > Client details > Create permission

#### Create resource-based permission

Name * 🕲	proxmax-permission0	1	
Beschreibung 💮			é
Apply to resource type ⑦	Off		
Resources * ①	Default Resource K	0	•
Policies	proximox-zugang01 🗙	0	•
Decision strategy ①	<ul> <li>Affirmative</li> </ul>		
	Unanimous		
	<ul> <li>Consensus</li> </ul>		
	/		
	Speichern Abbre	chen	

### **Benutzer Evaluierung**

Ein ganz bequemes Werkzeug ist die Benutzer Evaluierung. Dies befindet sich auch in der Clientkonfiguration direkt neben Berechtigungen. Damit ist es möglich Benutzerrechte live zu testen. Da Keycloak einen Cache betreibt, ist das Werzeug nicht mehr weg zu denken.

		- asserver ber	Hoten	Client scopes	Authorizatio	Dervice a	scourres rolles	Dessions	Advanced	
Einstellungen	Resources	s Scopes	Policies	s Berechtigun	gen Evalu	ite Export				
identity inform	ation									
Client	proxm	ox-cluster01								•
Benutzer * 🛞	harald								,	•
Rollen	Select	t a role								•
Identity Inform	ation									
Identity Inform Apply to Resource Type ©	ation	Off								
Identity Inform Apply to Resource Type © Resources and	ation C Schlüss	Off			We	t				
Identity Inform Apply to Resource Type ① Resources and Scopes ①	ation Schlüss Select	Off el			we v S	<b>t</b> Hector type a ko	29		·	0
Identity Inform Apply to Resource Type ① Resources and Scopes ①	ation C Schlüss Select O Attrib	Off el tor type a key but hinzufüge	n		We • S	<b>t</b> Hector type a k	29		•	0

Hier kann man sehr gut erkennen das der Benutzer "harald" nicht darf. Sehr gut. Wie sieht es nun aus wenn wir den Benutzer Harald in die Gruppe "gitlab" werfen?

Last update: 2025/05/18 09:02

oxmox-ciu	ster01	OpenID Conne	:t					
ents are application	ins and serv	vices that can re	quest authe	ntication of a user.				
Einstellungen	Keys	Passwörter	Rollen	Client scopes	Authorization	Service accounts roles	Sessions	Advanced
Einstellungen	Resour	ces Scoper	Policies	Berechtigung	en Evaluate	Export		
uche		Q. All res	ults		•			
Resour	æ						0	verall Results
✓ Default	Resource						P	firma
	Permi	ssion		1		Results	/	Decision strategy
	proxn	nox-permission/	01			Permit		Unanimous

Und schon darf er sich einloggen.

Wie man sieht ist mit Keycloak/UCS/Proxmox schon einiges möglich. Und damit wäre die Konfiguration auch schon abgeschlossen.

## Automatisch delegierte Berechtigungen über eine LDAP-Gruppe

Damit müssen keine Berechtigungen mehr dem Benutzern in Proxmox manuell zugewiesen werden.



https://lists.proxmox.com/pipermail/pve-devel/2024-February/061760.html

Fix Me! Workaround für Gruppenrechte:

https://docs.software-univention.de/keycloak-app/latest/configuration.html#restrict-access-to-applicat



From: https://deepdoc.at/dokuwiki/ - DEEPDOC.AT - enjoy your brain

Permanent link:

https://deepdoc.at/dokuwiki/doku.php?id=virtualisierung:proxmox\_kvm\_und\_lxc:openid\_keycloak\_anbindung\_proxmox\_

Last update: 2025/05/18 09:02

