

Folge den Bildern:

RED HAT IDENTITY MANAGEMENT

Identity Policy Authentication Network Services IPA Server

Users Hosts Services Groups ID Views Automember Subordinate IDs

Services

Search

Principal name

DNS{idm.lab.local}@LAB.LOCAL

DNS{idm2.lab.local}@LAB.LOCAL

HTTP{idm.lab.local}@LAB.LOCAL

HTTP{idm2.lab.local}@LAB.LOCAL

dogtag{idm.lab.local}@LAB.LOCAL

dogtag{idm2.lab.local}@LAB.LOCAL

ipa-dskeysyncd{idm.lab.local}@LAB.LOCAL

ipa-dskeysyncd{idm2.lab.local}@LAB.LOCAL

ldap{idm.lab.local}@LAB.LOCAL

ldap{idm2.lab.local}@LAB.LOCAL

Show 1 to 10 of 10 entries.

Refresh Delete + Add

Wähle aus was für eine Art von Service du hast (meist HTTP) und auf welchem Server der Service läuft. Wenn der Host Name nicht in der Liste ist, musst du «Skip host check» anwählen.

Add service X

Service *

Host Name *

Force

Skip host check

* Required field

Verbinde dich jetzt per SSH auf «idm.lab.local» oder «idm2.lab.local»

```
[boeschja@idm ~]$ openssl req -new -newkey rsa:2048 -nodes -keyout nas.key -out nas.csr -subj "/CN=nas.lab.local"
openssl req -new -newkey rsa:2048 -nodes -keyout <short-hostname>.key -out <short-hostname>.csr -subj "/CN=<short-hostname>.amalab.arpa"
```

```
[boeschja@idm ~]$ ipa cert-request nas.csr
Principal: HTTP/nas.lab.local@LAB.LOCAL
ipa cert-request <short-hostname>.csr
```

Man Sollte im GUI das Zertifikat sehen:

Service Certificate

Certificates	nas.lab.local	Actions
Serial Number:	15	<input type="button" value="Actions"/>
Issued By:	Certificate Authority	
Valid from:	Mon Aug 12 08:47:16 2024 UTC	
Valid to:	Thu Aug 13 08:47:16 2026 UTC	