Umstellung auf Keycloak in UCS

Mit UCS 5.2 ist Keycloak die neue Authendifizierungsschnittstelle. Deswegen müssen UCS Systeme vor dem Upgrade umgebaut werden. Die Dokumentation ist von Univention sehr ausführlich vorhanden.

- Keycloak Appdokumentation
- Migrationsleitfaden
- Umstellung Nextcloud
- Failsafemode HA
- Multible Installationen (beißt sich mit oben)

Befehlsketten für die Installation und Konfiguration

Falls OpenID installiert sein sollte, ist dies vorher zu desintegrieren. Installation auf dem Primary Directory Node. Wichtig dabei ist das alle UCS Server im Cluster laufen und erreichbar sind. Dabei kann es passieren dass, das gesamte Schema von OpenID entfernt wird. Sollte dies passieren muss es wieder registriert werden. Daher vor der Deinstallation das Schema sichern. Dann wenn notwendig neu registrieren:

regopenid.sh

```
#!/bin/bash
. /usr/share/univention-lib/ldap.sh
ucs_registerLDAPExtension --packagename openid-connect-provider --
packageversion 1.0 --schema /var/lib/univention-ldap/local-
schema/openid-connect-provider.schema
```

```
univention-app install keycloak
```

Ab dem Zeitpunkt gibt es eine neue Kachel auf dem Dashboard. Login unter `https://ucs-sso-ng.$domainname/admin/` als Domänenadmin. Sowohl OIDC als auch SAML bieten den Diensten, die die Authentifizierungsdienste in Keycloak nutzen wollen, maschinenlesbare Informationen. Diese Informationen sind die Metadaten-Ermittlungsdokumente.

In der Keycloak Admin Console finden Sie diese unter Realm-Einstellungen ▸ UCS ▸ Endpunkte. Bei den Endpunkten sehen Sie OpenID Endpoint Configuration und SAML 2.0 Identity Provider Metadata. Um die Metadaten-Ermittlungsdokumente anzuzeigen, klicken Sie auf die Endpunkteinträge.

Mit den folgenden Befehlen können Sie die URLs zu den Metadateninformationen abrufen. Einige Dienste übernehmen bequem die URL und konfigurieren die Authentifizierung automatisch.

```
wget "https://$(ucr get keycloak/server/sso/fqdn)/realms/ucs/.well-
known/openid-configuration"
```

Dieser Befehl zeigt nun noch auf den alten simple Saml PHP:

```
ucr get umc/saml/idp-server
https://ucs-sso.domain.foo/simplesamlphp/saml2/idp/metadata.php
```

Die Umstellung global auf Keycloak manuell mittel UCR:

```
ucr set umc/saml/idp-
server="https://ucs-sso-ng.domain.foo/realms/ucs/protocol/saml/descriptor"
```

Grundsätzlich wird dies über eine Policy im LDAP ausgerollt. Im nächsten Schritt wird das Portal hierfür modifiziert:

```
udm portals/entry modify \
--dn "cn=login-saml,cn=entry,cn=portals,cn=univention,$(ucr get ldap/base)"
\
--set activated=TRUE
```

Danach müssen alle LDAP Server neu gestartet werden:

```
systemctl restart slapd.service
```

Standardmäßig erstellt die Keycloak-App einen SAML SP (Client) für jeden UCS Portal-Server. Sie können die Liste der vorhandenen SAML SP-Clients mit dem folgenden Befehl einsehen:

```
univention-keycloak saml/sp get --json
```

Sollte hier ein Server fehlen, kann dieser sehr einfach über die Konsole hinzugefügt werden:

```
FQDN="the fqdn of the UCS Portal server"
univention-keycloak saml/sp create \
  --metadata-url="https://$FQDN/univention/saml/metadata" \
  --umc-uid-mapper
```

Beim Login wird Default das lokale Kerberosticket dem Keycloak mit übergeben. Nachdem sich der SSO geändert hat, muss von „ucs-sso“ auf ucs-sso-ng„ nachkonfiguriert werden. Außer man hat das ganze für die Domäne schon als Wildcard (Default ITEAS Pakete) hinterlegt. Siehe auch diesen Forenbeitrag.

Migration von Diensten

https://docs.software-univention.de/keycloak-migration/migration-procedure/saml.html

```
udm saml/serviceprovider list
```

Public Cert abfragen:

```
univention-keycloak saml/idp/cert get \
   --as-pem \
```

```
   --output "/tmp/keycloak.cert"
```

Nextcloud auf Keycloak migrieren:

Neuen Client auf Keycloak erstellen:

```
univention-keycloak saml/sp create --
metadata-url="https://cloud.domain.foo/nextcloud/apps/user_saml/saml/metadat
a" --role-mapping-single-value
```

Danach am Nextcloudserver einloggen und auf das neue SAML von Keycloak umkonfigurieren:

```
univention-keycloak saml/idp/cert get \
   --as-pem \
   --output "/tmp/keycloak.cert"

SSO_URL="https://ucs-sso-ng.domain.foo"

univention-app shell nextcloud sudo -u www-data /var/www/html/occ
saml:config:set \
  --idp-x509cert="$(cat /tmp/keycloak.cert)" \
  --general-uid_mapping="uid" \
  --idp-singleLogoutService.url="$SSO_URL/realms/ucs/protocol/saml" \
  --idp-singleSignOnService.url="$SSO_URL/realms/ucs/protocol/saml" \
  --idp-entityId="$SSO_URL/realms/ucs" 1
```

Fragen und Antworten

Kann die vom Selbstcheck generierte Fehlermeldung von Simple Saml php Certs ignoriert werden? → JA
Dürfen die alten LDAPdaten/Schema von der OpenID App gelöscht werden? → NEIN
Dürfen noch vorhandene Serviceprovider von Simple Saml PHP in der UMC gelöscht werden? → JA, sofern sie nicht mehr benötigt werden.
Wenn ich die Keycloakapp auf mehreren UCSnodes installiere, spreche ich dann von einer HA-Installation? → NEIN, hierzu muss MariaDB im Cluster außerhalb von UCS installiert werden.

Debug

Befehlssammlung UCS

Zeit prüfen:

```
root@backup:~# ntpq
ntpq> pe
     remote           refid      st t when poll reach   delay   offset
jitter
```

```
==============================================================================
 LOCAL(0)        .LOCL.           9 l   8h   64    0    0.000    0.000
0.000
*master.multi.uc LOCAL(0)         6 u  916 1024  377    0.250    0.013
0.032
```