Einleitung

Ausgangspunkt ist ein Univention Server Version 4.4-3, auf dem über das App Center die Anwendungen *Active Directory-kompatibler Domänen-Controller, KVM Virtualisierungsserver* und *UCS Virtual Machine Manager* installiert wurden.

KIX ist ein vollwertiges Ticketsystem, das auf der etablieterten Lösung OTRS basiert. Da KIX ein Fork von OTRS ist, bietet es denselben Funktionsumfang, sowie zusätzliche Module und Services.

Der UCS hat in dieser Dokumentation die IP-Adresse 192.168.0.242, die virtuelle Maschine hat die IP-Adresse 192.168.0.223, die LDAP-Base des UCS lautet *dc=lab,dc=laptop* .

Ziel

Der Univention Server stellt eine ideale Grundlage für das Identity Management für verschiedene Anwendungen dar.

Daher soll der UCS auch für Anmeldung der Agenten und Kunden am KIX-Webinterface genutzt werden, so dass die zusätzliche Benutzerverwaltung in KIX entfällt. Die Überprüfung der Anmeldedaten soll KIX durch einen direkten Zugriff auf den LDAP-Server des UCS durchführen. Dabei sollen nicht nur Benutzername und Passwort geprüft werden, sondern auch anhand der Gruppenzugehörigkeit, ob es sich um einen Agent oder einen Kunden handelt.

Kurze Steig 31
75179 Pforzheim
http://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

Konfiguration des Univention Corporate Servers

Anpassen der Firewall-Konfiguration

Damit das KIX-System eine Verbindung zum LDAP-Server des UCS herstellen kann, muss der Port 7389 geöffnet werden:

iptables -I INPUT 1 -p tcp --dport 7389 -s 192.168.0.223/32 -j ACCEPT

Damit diese Regel auch nach einem Neustart des UCS Bestand hat, trägt man sie in die Datei */etc/security/packetfilter.d/50_local.sh* ein.

Für die Überprüfung der Anmeldedaten der Benutzer muss sich KIX am LDAP-Server anmelden und benötigt dazu eigene Anmeldedaten. Dafür verwendet man keinen vollständigen Benutzeraccount, sondern legt ein so genanntes „Einfaches Authentisierungskonto“ an. Dies geschieht im Webinterface des UCS unter **Domäne** -> **LDAP-Verzeichnis.** In dem sich öffnenden LDAP-Baum wählt man den Ordner **users** und danach die Funktion **Hinzufügen**. Den Typ wechselt man nun von Benutzer zu „Einfaches Authentisierungskonto“ und vergibt im Anschluss einen Benutzernamen (z.B. „ldap4kix“) und ein Passwort („ldappw4KIX“)

Im nächsten Schritt legt man unter **Benutzer** -> **Gruppen** die beiden Gruppen *kix-agents* und *kix-customers* an. Danach unter **Benutzer** -> **Benutzer** den Benutzer *mitarbeiter*, der Mitglied der Gruppe *kix-agents* wird und den Benutzer *kunde*, der Mitglied der Gruppe *kix-customers* wird.

Kurze Steig 31
75179 Pforzheim
http://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

Installation der virtuellen Maschine

Grundlage des KIX Systems ist ein Ubuntu 18.04. LTS, dessen ISO-Datei auf dem UCS im Verzeichnis */var/lib/libvirt/images* abgelegt wird.

Im *UCS Virtual Machine Manager* wählt man den Menüpunkt **Erstellen** und wählt danach **Erstellen einer neuen virtuellen Instanz** auf dem lokalen UCS.

Als Profil für die virtuelle Maschine wählt man die folgenden Einstellungen:

- Profil: Other (64 Bit)
- Name: KIX2017
- Größe des Arbeitsspeichers: 4096 MiB
- Anzahl der CPUs: 1
- Direktzugriff (VNC): aktiviert

Im nächsten Schritt wählt man **Hinzufügen -> Festplatte** und bestätigt die Vorgaben. Danach fügt man mittels **Hinzufügen -> CD-ROM-Laufwerk** das Installationsmedium hinzu und wählt im DropDown-Menü Laufwerk Image-Datei das Ubuntu ISO-Image aus.

Nachdem man die Konfiguration abgeschlossen hat, kann die Installation der virtuellen Maschine starten und über das Monitor Icon eine VNC Verbindung zur VM herstellen.

Nachdem die Grundinstallation des Ubuntu-Systems abgeschlossen ist und alle anstehenden Updates eingespielt wurden, erfolgt die Installation von KIX mit PostgreSQL gemäß der Anleitung aus dem Forum:

https://forum.kixdesk.com/index.php?topic=3364.0

Kurze Steig 31
75179 Pforzheim
http://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

Konfiguration der virtuellen Maschine

KIX basiert auf der Programmiersprache Perl und benötigt für den Zugriff auf den LDAP-Server des UCS die passende Bibliothek:

```
apt-get -y install libnet-ldap-perl
```

Nach der Installation sieht die zentrale Konfigurationsdatei */opt/kix17/Kernel/Config.pm* von KIX wie folgt aus:

```
package Kernel::Config;
use strict;
use warnings;
use utf8;
sub Load {
   my $Self = shift;
   $Self->{DatabaseHost} = 'localhost';
   $Self->{Database} = 'kix17';
   $Self->{DatabaseUser} = 'kix';
   $Self->{DatabasePw} = 'xxxxxxx';
   $Self->{DatabaseDSN} = "DBI:Pg:dbame=$Self->{Database};host=$Self->{DatabaseHost};";
   $Self->{CheckMXRecord} = 0;
   $Self->{FQDN} = 'kix.in-put.de';
}
use strict;
use warnings;
use vars qw(@ISA);
use Kernel::Config::Defaults;
push (@ISA, 'Kernel::Config::Defaults');
1;
```

Damit KIX die Anmeldung gegen den LDAP des UCS durchführt, sind an der Datei einige Änderungen erforderlich, die den Umfang der Konfigurationsdatei deutlich erhöhen. Die fett hervorgehobenen Stellen sind anzupassen, wenn man die Konfiguration für ein eigenes System übernehmen will.

```
package Kernel::Config;
use strict;
use warnings;
use utf8;
sub Load {
    my $Self = shift;
    $Self->{'DatabaseHost'} = '127.0.0.1';
    $Self->{'Database'} = "kix17";
    $Self->{'DatabaseUser'} = "kix";
    $Self->{'DatabasePw'} = 'xxxxx';
    $Self->{'DatabaseDSN'} = "DBI:Pg:dbname=$Self->{Database};host=$Self->{DatabaseHost}";
    $Self->{Home} = '/opt/kix17';
    # $Self->{SessionUseCookie} = 0;
    # $Self->{CheckMXRecord} = 0;
```


Kurze Steig 31 http://www.in-put.de/ fon +49 (0) 72 31 / 44 07 85 - 0
75179 Pforzheim kontakt@in-put.de fax +49 (0) 72 31 / 44 07 85 - 9

```
$Self->{'AuthModule1'} = 'Kernel::System::Auth::DB';

#
# Beginn Konfiguration LDAP Anbindung an UCS
#

# Anmeldung als Agent
#
$Self->{'AuthModule2'} = 'Kernel::System::Auth::LDAP';
$Self->{'AuthModule::LDAP::Host2'} = '192.168.0.242';
$Self->{'AuthModule::LDAP::BaseDN2'} = 'dc=lab,dc=laptop';
$Self->{'AuthModule::LDAP::UID2'} = 'uid';
$Self->{'AuthModule::LDAP::SearchUserDN2'} = 'uid=ldap4kix,cn=users,dc=lab,dc=laptop';
$Self->{'AuthModule::LDAP::SearchUserPw2'} = 'ldappw4KIX';
$Self->{'AuthModule::LDAP::SSCOPE2'} = 'sub';
$Self->{'AuthModule::LDAP::GroupDN2'} = 'cn=kix-agents,cn=groups,dc=lab,dc=laptop';
$Self->{'AuthModule::LDAP::AccessAttr2'} = 'memberUid';
$Self->{'AuthModule::LDAP::UserAttr2'} = 'UID';
$Self->{'AuthModule::LDAP::Params2'} = { port => 7389, version => 3, };

#
#  Synchronisation der Daten der Agents
#
$Self->{'AuthSyncModule'} = 'Kernel::System::Auth::Sync::LDAP';
$Self->{'AuthSyncModule::LDAP::Host'} = '192.168.0.242';
$Self->{'AuthSyncModule::LDAP::BaseDN'} = 'dc=lab,dc=laptop';
$Self->{'AuthSyncModule::LDAP::UID'} = 'uid';
$Self->{'AuthSyncModule::LDAP::UserAttr'} = 'DN';
$Self->{'AuthSyncModule::LDAP::AccessAttr'} = 'member';
$Self->{'AuthSyncModule::LDAP::SearchUserDN'} = 'uid=ldap4kix,cn=users,dc=lab,dc=laptop';
$Self->{'AuthSyncModule::LDAP::SearchUserPw'} = 'ldappw4KIX';
$Self->{'AuthSyncModule::LDAP::Params'} = { port => 7389, version => 3, };
$Self->{'AuthSyncModule::LDAP::UserSyncMap'} = {
    UserFirstname => 'gecos',
    UserLastname => 'sn',
    UserEmail => 'mailPrimaryAddress',
};
$Self->{'AuthSyncModule::LDAP::UserSyncGroupsDefinition'} = {
    'cn=kix-agents,cn=groups,dc=lab,dc=laptop' => {
        'admin' => { rw => 1, ro => 1, },
        'faq' => { rw => 1, ro => 1, },
    },
};

#
#  Anmeldung als Kunde
#
$Self->{'Customer::AuthModule3'} = 'Kernel::System::CustomerAuth::LDAP';
$Self->{'Customer::AuthModule::LDAP::Host3'} = '192.168.0.242';
$Self->{'Customer::AuthModule::LDAP::BaseDN3'} = 'dc=lab,dc=laptop';
$Self->{'Customer::AuthModule::LDAP::UID3'} = 'uid';
$Self->{'Customer::AuthModule::LDAP::SearchUserDN3'} =
'uid=ldap4kix,cn=users,dc=lab,dc=laptop';
$Self->{'Customer::AuthModule::LDAP::SearchUserPw3'} = 'ldappw4KIX';
$Self->{'Customer::AuthModule::LDAP::GroupDN3'} = 'cn=kix-
customers,cn=groups,,dc=lab,dc=laptop';
```

```
$Self->{'Customer::AuthModule::LDAP::AccessAttr3'} = 'memberUid';
$Self->{'Customer::AuthModule::LDAP::UserAttr3'} = 'UID';
$Self->{'Customer::AuthModule::LDAP::Params3'} = {port => 7389, version => 3,};
$Self->{'UserSyncLDAPMap1'} =  {
        'UserEmail' => 'mailPrimaryAddress',
        'UserFirstname' => 'givenName',
        'UserLastname' => 'sn',
        'UserLogin' => 'uid'
        };

 #
 #  Synchronisation der Daten der Agents
 #
$Self->{CustomerUser1} = {
   Module => 'Kernel::System::CustomerUser::LDAP',
   Params => {
          #
          # Der LDAP des UCS nimmt Verbindung nur auf Port 7389 an. In obigen Konfigurationsblöcken
          # wurde der Port über einen eigenen Parameter übergeben. Dies ist in diesem Konfigurations
          # block nicht möglich, hier muss der Port, getrennt durch einen Doppelpunkt, hinter der IP-
          # Adresse des UCS übergeben werden.
          #
          Host => '192.168.0.242:7389',
          BaseDN => 'dc=lab,dc=laptop',
          SSCOPE => 'sub',
          UserDN => 'uid=ldap4kix,cn=users,dc=lab,dc=laptop',
          UserPw => 'ldap4KIX',
          #
          # Ohne einen Filter würden in der Kundenverwaltung von KIX alle Accounts angezeigt, also auch
          # Systemkonten
          #
          AlwaysFilter => '(&(objectClass=posixAccount)(mailPrimaryAddress=*@*))',
          #
          # Ohne die beiden folgenden Parameter werden Umlaute in den Namen falsch dargestellt
          #
          SourceCharset => 'utf-8',
          DestCharset => 'utf-8',
          },
   CustomerKey => 'uid',
   CustomerID => 'mail',
   CustomerUserListFields => ['uid', 'sn', 'mailPrimaryAddress'],
   CustomerUserSearchFields => ['uid', 'sn', 'mailPrimaryAddress'],
   CustomerUserPostMasterSearchFields => ['mailPrimaryAddress'],
   CustomerUserNameFields => ['givenName', 'sn'],
   Map => [
          [ 'UserFirstname', 'Firstname', 'givenname', 1, 1, 'var' ],
          [ 'UserLastname', 'Lastname', 'sn', 1, 1, 'var' ],
          [ 'UserLogin', 'Login', 'uid', 1, 1, 'var' ],
          [ 'UserEmail', 'Email', 'mailPrimaryAddress', 1, 1, 'var' ],
          [ 'UserCustomerID', 'CustomerID', 'mailPrimaryAddress', 0, 1, 'var' ],
   ],
};
# Ende
return 1;
}
```


Kurze Steig 31
75179 Pforzheim
http://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

```
use strict;
use warnings;
use vars qw(@ISA);
use Kernel::Config::Defaults;
push (@ISA, 'Kernel::Config::Defaults');
1;
```

Nun sind 3 Anmeldungen an KIX möglich:

1. Mit dem Account root@localhost als Agent an http://192.168.0.223/kix/index.pl
2. Mit dem Account „mitarbeiter“ als Agent an http://192.168.0.223/kix/index.pl
3. Mit dem Account „kunde“ als Kunde an http://192.168.0.223/kix/customer.pl

Kurze Steig 31
75179 Pforzheim
http://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9