Вход в Active Directory на рабочей станции Linux, используя сертификат MS CA на JaCarta

Версия ПО: GNU Linux, MS Windows Server

Токены: JaCarta PKI

Проблема:

Решение:

- Необходимо осуществить присоединение к домену рабочей станции. Воспользуйтесь, например, мануалом: <u>http://help.ubuntu.ru/wiki/ввод_в_домен_windows</u>
- Установите пакет libpam_pkcs11
- Установите драйвер для JaCarta PKI: <u>JaCarta PKI для Linux</u>
- Настройте модуль **pam_pkcs11**: sudo mkdir /etc/pam_pkcs11 . В указанном каталоге создайте файл конфигурации **pam_pkcs11.conf** (исправьте адреса и имя домена на свои):
- pam_pkcs11 { nullok = true;

```
debug = false;
use_first_pass = false;
try_first_pass = false;
use_authtok = false;
use_pkcs11_module = jacarta;
pkcs11_
```

```
module aladdin {
  module = /usr/lib/libjcPKCS11-2.so;
  description = "ARDS JaCarta pkcs#11 module";
  slot_num = 0;
  ca_dir = /etc/pam_pkcs11/cacerts;
  crl_dir = /etc/pam_pkcs11/crls; crl_policy = none;
  }
  use_mappers = subject, ads, ms, null;
  mapper_search_path = /lib/pam_pkcs11;
```

mapper subject {

```
debug = false;
# module = /usr/lib/pam_pkcs11/subject_mapper.so;
module = internal;
ignorecase = false;
mapfile = file:///etc/pam_pkcs11/subject_mapping;
}
mapper null {
debug = false;
module = internal;
```

}

```
mapper ads {
```

```
debug = false;
```

module = /lib/pam_pkcs11/ldap_mapper.so;

where base directory resides

```
basedir = /etc/pam_pkcs11/mapdir;
```

Здесь указываем адрес нашего контроллера домена

```
ldaphost = "192.168.0.1";
```

Port on ldap server to connect

ldapport = 389;

Scope of search: 0 = x, 1 = y, 2 = z scope = 0;

Указываем DN-имя пользователя, который имеет право на чтение каталога

```
binddn = "cn=Administrator,cn=Users,dc=domain,dc=ru" passwd = 1234567890
```

Searchbase for user entries

```
base = "dc=domain,dc=ru";
```

 $\ensuremath{\texttt{\#}}$ Attribute of user entry which contains the certificate

```
attribute = "userCertificate:";
```

Searchfilter for user entry. Must only let pass user entry for the login user.

#filter = "(&(cn=%s) (objectClass=inetOrgPerson))";

#filter = "(&(objectClass=posixAccount)(uid=%s))"

```
filter = "(msSFU30Name=%s)";
```

```
}
```

```
mapper ms {
```

```
debug = false;
```

```
module = internal;
```

```
ignorecase = true;
```

```
ignoredomain = true;
```

```
domain = "domain.ru"; }
```

```
}
```

- Настройте корневой сертификат и список отозванных сертификатов CRL. Скачайте эти файлы с расширениями соответственно CER и CRL с нашего сервера сертификации <u>http://server/certsrv.</u> Создайте каталоги:
- sudo mkdir /etc/pam_pkcs11/cacerts
- sudo mkdir /etc/pam_pkcs11/crls
- Скопируйте файлы: cer в /etc/pam_pkcs11/cacerts, crl в /etc/pam_pkcs11/crls. Необходимо захешировать эти файлы скриптом make_hash_link.sh. Загрузить его можно по ссылке: <u>https://github.com/OpenSC/pam_pkcs11/tree/master/tools</u>. Сделайте скрипт исполняемым:
- sudo chmod +x make_hash_link.sh
- Далее последовательно зайдите в каталоги /etc/pam_pkcs11/cacerts и /etc/pam_pkcs11/crls и выполните там этот скрипт.

Теперь можно настраивать pam.d для входа по смарт-карте. Внимание! Для экспериментов и начальной отладки используйте /etc/pam.d/su. В начало файла /etc/pam.d/su добавьте строку:

auth sufficient pam_pkcs11.so

Подключите токен с пользовательским сертификатом. Выполните команду:

su <имя доменного пользователя>

Будет запрошен ПИН-код и осуществлен вход под данным пользователем. Если всё прошло успешно, можно добавить эту строку в **gdm**, **kdm** и т.д.

ID статьи: 245

Последнее обновление: 16 Nov, 2017

Ревизия: 1

JaCarta -> Вход в Active Directory на рабочей станции Linux, используя сертификат MS CA на JaCarta

https://kbp-6.aladdin-rd.ru/index.php?View=entry&EntryID=245