УТИЛИТА ALADDIN ENTERPRISE CA AGENT

Инструкция по использованию

1. НАЗНАЧЕНИЕ

Утилита Aladdin Enterprise CA Agent (далее — утилита) предназначена для получения и обновления сертификатов доменных пользователей и АРМ от Центра регистрации Aladdin eRA в среде Linux по протоколу MS-WSTEP с использованием Kerberos аутентификации.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ УТИЛИТЫ

Утилита поддерживает работу в операционных системах (ОС):

- Astra Linux Special Edition, версия 1.7 или 1.8, уровень защищённости «Смоленск», «Воронеж» и «Орел» (далее – Astra Linux).
- РЕД ОС версия 7.3, сертифицированная редакция, конфигурация «Рабочая станция» (далее – РЕД ОС 7.3).
- РЕД ОС версия 8, конфигурация «Рабочая станция» (далее – РЕД ОС 8).
- ОС Альт 8 СП, вариант исполнения «Рабочая станция» (далее – Альт 8 СП).
- ОС Альт СП релиз 10, вариант исполнения «Рабочая станция» (далее – Альт СП релиз 10).
- Platform V SberLinux OS Server, включая сертифицированные редакции.
- ОС РОСА «ХРОМ» 12, исполнение «Рабочая станция».

Для работы утилиты требуется:

- Не менее 150 МБ свободного дискового пространства.
- Не менее 1 ГБ RAM.
- Не менее одного процессорного ядра. Поддерживаемая процессорная архитектура: x64, x86.

Получение и обновление сертификатов возможно только для пользователей и компьютеров домена, к которому подключён используемый утилитой экземпляр Центра регистрации Aladdin eRA.

3. ПОДГОТОВКА К ИСПОЛЬЗОВАНИЮ УТИЛИТЫ

Для подготовки выполнения утилиты:

- Убедитесь, что компьютер соответствует требованиям, приведённым в разделе 2.

- Распакуйте утилиту на жёсткий диск компьютера.
- Перейдите в каталог с утилитой и выполните команду с правами суперпользователя:
  - `bash install.sh install_all` для полной установки утилиты, включая активацию функциональности автоматического выпуска сертификатов доменного пользователя;
  - `bash install.sh install` для установки утилиты без активации функциональности автоматического выпуска сертификатов доменного пользователя.
- В Центре сертификации Aladdin eCA настройте шаблон, являющийся копией шаблона Web-Client, с необходимым сроком действия (далее – Web-Client-XXm, где XX — количество минут).
- В Центре регистрации Aladdin eRA должно быть либо правило автоматического выпуска для доменного пользователя, под которым будет проверяться выпуск, и шаблона Web-Client-XXm, указанного выше, либо правило автоматического выпуска для всех субъектов по всем шаблонам.
- Выполните проверки, приведённые в подразделах 3.1 и 3.2.

3.1. Проверка доступных Центров сертификации

Для проверки доступных Центров сертификации выполните команду с правами суперпользователя:

```
getcert list-cas
```

В результате выполнения команды будет выведен список доступных Центров сертификации. В ходе установки утилиты Центр сертификации cepces устанавливается автоматически.

Убедитесь, что в выведенном списке Центров сертификации присутствуют сведения о Центре сертификации cepces:

```
CA 'cepces':
        is-default: no
        ca-type: EXTERNAL
        helper-location: /opt/cepces/ca_helpers/cepces-submit
CA 'ucepces':
        is-default: no
        ca-type: EXTERNAL
        helper-location:     /opt/cepces/ca_helpers/cepces-submit     --
principals=user
```

Для ручного добавление Центра сертификации cepces в список выполните команду с правами суперпользователя:

```
getcert add-ca -c cepces -e '/opt/cepces/ca_helpers/cepces-submit'
```

3.2. Проверка keytab-файла

Для проверки keytab-файла:

- Узнайте имя хоста при помощи команды: `hostname`.
- Выполните команду с правами суперпользователя: `klist -k /etc/krb5.keytab`
- Убедитесь, что при отклике на команду присутствует строка:

`{имя_хоста_в_верхнем_регистре}$@{имя_домена_в_верхнем_регистре}`

- Если в файле `/etc/krb5.keytab` отсутствует строка:

`{имя_хоста_в_верхнем_регистре}$@{имя_домена_в_верхнем_регистре}`,

выполните одно из следующих действий:

– укажите в файле `/etc/cepces/cepces.conf` строку `{HOSTNAME}$$@{DOMAIN}`, как показано в примере ниже (обратите внимание на символы $$ после имени хоста, имя хоста и имя домена укажите в верхнем регистре):

```
ini
principals=
  ${shortname}$$
  ${SHORTNAME}$$
  host/${SHORTNAME}
  host/${fqdn}
  {HOSTNAME}$$@{DOMAIN}
```

– измените имя хоста на имя, указанное в файле `krb5.keytab`.

- Перезагрузите компьютер.

3.3. Активация функциональности автоматического выпуска сертификатов доменного пользователя

Для активации функциональности автоматического выпуска сертификатов доменного пользователя выполните следующую команду с правами суперпользователя:

```
bash install.sh enable_for_user
```

3.4. Деактивация функциональности автоматического выпуска сертификатов доменного пользователя

Для деактивации функциональности автоматического выпуска сертификатов доменного пользователя выполните следующую команду с правами суперпользователя:

```
bash install.sh disable_for_user
```

4. ВЫПОЛНЕНИЕ УТИЛИТЫ

4.1. Получение сертификата доменного пользователя

Для получения сертификата доменного пользователя в автоматическом режиме выполните следующие действия:

- Под суперпользователем в файле `/etc/cepces/cepces.conf` укажите в параметре `server` адрес хоста Центра регистрации Aladdin eRA (он должен быть доступен с компьютера).
- Под суперпользователем в файле `/etc/cepces/ugetcert.conf` укажите в параметре `template` идентификатор шаблона Web-Client-XXm.
- Войдите в ОС под учетной записью доменного пользователя, для которого создано правило выпуска по шаблону Web-Client-XXm. Сертификат автоматически будет загружен в папку `/home/имя_пользователя/crt`.

Для проверки корректности получения сертификата убедитесь, что:

- В каталоге `/home/имя_пользователя/crt` появился файл `user.crt`, который является сертификатом доменного пользователя.
- Параметры сертификата соответствуют шаблону Web-Client-XXm.
- Срок действия сертификата составляет XX минут с момента входа пользователя в ОС.
- Не позднее чем через XX минут после истечения срока действия сертификата доменного пользователя, данный сертификат перевыпускается и сохраняется в каталоге `/home/имя-пользователя/crt`.

4.2. Удаление сертификата доменного пользователя

Для удаления сертификата выполните следующие действия:

- Остановите отслеживание заявки для доменного пользователя, выполнив следующую команду с правами суперпользователя: `getcert stop-tracking -i`

- Удалите в каталоге `/home/имя_пользователя/crt` файлы сертификата и закрытого ключа.

4.3. Получение сертификата доменного компьютера

Для получения сертификата выполните следущую команду с правами суперпользователя:

```
getcert request -c cepces -k /home/user/myhost.key -f /home/user/myhost.crt
 -T "template_id" -I host
```

где:

- `/home/user/myhost.key` – путь к файлу, в котором должен храниться закрытый ключ компьютера;
- `/home/user/myhost.crt` – путь к файлу, в котором должен храниться сертификат, выпущенный для компьютера;
- `template_id` – идентификатор шаблона, который должен использоваться для выпуска (перевыпуска) сертификата компьютера.

4.4. Проверка статуса сертификата

Для проверки статуса сертификата выполните следущую команду с правами суперпользователя:

```
getcert list
```

4.5. Логирование

Логи по умолчанию сохраняются в директорию `/var/log/cepces/cepces.log`.

Параметры логирования работы утилиты находятся в конфигурационном файле `/etc/cepces/logging.conf`.

По умолчанию включён режим логирования — `DEBUG`. Режимы `INFO` и `WARNING` — отображают минимальное количество информации в логах.

5. УДАЛЕНИЕ УТИЛИТЫ

Для удаления утилиты выполните следущую команду с правами суперпользователя:

```
bash install.sh uninstall
```