ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон/Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный комплекс С-Терра Шлюз. Версия 4.1

Руководство администратора

Копирование, клонирование и размножение образа «С-Терра Виртуальный Шлюз»

РЛКЕ.00009-01 90 03

07.12.2015

Содержание

Копирование, клонирование и размножение образа «С-Терра Виртуальный Шлюз» 3

Ограничения на копирование, клонирование и размножение образа «С-Терра Виртуальный Шлюз» до прохождения процедуры инициализации.....4

Ограничения на копирование, клонирование и размножение образа «С-Терра Виртуальный Шлюз» после прохождения процедуры инициализации 5

Настройка шлюза без использования скриптов «Программного продукта С-Терра КП» 5

Настройка шлюза с использованием скриптов «Программного продукта С-Терра КП» 9

 Copyright © S-Terra CSP 2003 -2015

Копирование, клонирование и размножение образа «С-Терра Виртуальный Шлюз»

Данный документ относится только к «Программному комплексу С-Терра Шлюз. Версия 4.1», работающему в виртуальной среде и описывает ограничения на действия пользователя при копировании, клонировании и размножении образа «С-Терра Виртуальный Шлюз».

«С-Терра Виртуальный Шлюз» распространяется в виде OVA-шаблона. Данный шаблон представляет собой виртуальную машину с образом «С-Терра Виртуальный Шлюз», на котором не пройдена процедура инициализации.

Клонирование виртуальной машины необходимо проводить стандартными средствами гипервизора, в общем случае это позволяет избежать одинаковых MAC-адресов сетевых интерфейсов.

Описание ограничений на копирование, клонирование и размножение образа зависит от стадии настройки шлюза:

- до прохождения процедуры инициализации (рекомендуемый вариант);
- после прохождения процедуры инициализации.

 Copyright © S-Terra CSP 2003 -2015

Ограничения на копирование, клонирование и размножение образа «С-Терра Виртуальный Шлюз» до прохождения процедуры инициализации

До прохождения процедуры инициализации данный образ разрешается клонировать, копировать и размножать аналогично дистрибутиву программного комплекса «С-Терра Клиент 4.1» – для получения требуемого количества дистрибутивов, подтвержденного лицензиями на право использования и регистрационными документами СКЗИ.

Данный вариант является наиболее предпочтительным.

Copyright © S-Terra CSP 2003 -2015

Ограничения на копирование, клонирование и размножение образа «С-Терра Виртуальный Шлюз» после прохождения процедуры инициализации

После прохождения инициализации необходимо задать новые лицензии, повторно инициализировать датчик случайных чисел, удалить контейнеры и сертификаты исходного шлюза и изменить, при необходимости, конфигурационный файл с локальной политикой безопасности (LSP).

Возможны два варианта:

- Настройка шлюза без использования скриптов «Программного продукта С-Терра КП».
- Настройка шлюза с использованием скриптов «Программного продукта С-Терра КП».

Настройка шлюза без использования скриптов «Программного продукта С-Терра КП»

Задание новых лицензий

Необходимо задать новую лицензию на «С-Терра Шлюз».

- Удалите старую лицензию на «С-Терра Шлюз»:

  ```
  rm /opt/VPNagent/bin/agent.lic
  ```

- Задайте новую лицензию с помощью утилиты `lic_mgr`. Например:

  ```
  lic_mgr set -p GATE1000 -c DEMO -n 1 -l 1234567890ABCDEF
  Active license:
  CustomerCode=DEMO
  ProductCode=GATE1000
  LicenseNumber=1
  LicenseCode=1234567890ABCDEF
  ```

Если используется СКЗИ «КриптоПро CSP», необходимо задать новую лицензию на «КриптоПро CSP».

- Для этого воспользуйтесь утилитой `cpconfig` (размещена в каталоге /opt/cprocsp/sbin/ia32/ или /opt/cprocsp/sbin/amd64/, в зависимости от разрядности операционной системы). Например:

  ```
  ./cpconfig -license -set 01234-56789-ABCDE-FGHIJ-KLMNO
  ```

Повторная инициализация датчика случайных чисел

Необходимо повторно пройти процедуру инициализации датчика случайных чисел.

- Если используется криптобиблиотека, разработанная компанией «С-Терра СиЭсПи», то необходимо запустить утилиту `rnd_mgr`:

  ```
  /opt/VPNagent/bin/rnd_mgr
  ```

 Copyright © S-Terra CSP 2003 -2015

```
Progress: [********* ]

Press key:

Successfully initialized RNG.
```

- Если используется СКЗИ «КриптоПро CSP», то необходимо запустить утилиту `csp_cprng_init`:

```
/opt/VPNagent/bin/csp_cprng_init

CSP (Type:75) v3.9.8000 KC1 Release Ver:3.9.8212 OS:Linux CPU:AMD64
FastCode:READY:AVX.

AcquireContext: OK. HCRYPTPROV: 13283043

GetProvParam(PP_NAME): Crypto-Pro GOST R 34.10-2001 KC1 CSP

Container name: "gDs3OgGR"

Signature key is not available.

Attempting to create a signature key...

Press keys...

[.....................................]

a signature key created.

Keys in container:

  signature key

Total:

[ErrorCode: 0x00000000]

Initialization SUCCESS.
```

Удаление контейнеров и сертификатов

Построение защищенного соединения происходит с аутентификацией абонентов при помощи ключевой пары (закрытого и открытого ключа). Закрытый ключ аутентификации является конфиденциальным и должен использоваться только одним абонентом. Если клонирование произведено после введения ключа аутентификации, то необходимо удалить клонированный ключ и ввести ключ, принадлежащий абоненту, для которого производится клонирование виртуального шлюза.

Порядок удаления ключа описан далее.

Для работы с сертификатами используется утилита `cert_mgr`.

- Вывод списка сертификатов:

```
cert_mgr show

Found 2 certificates. No CRLs found.

1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-
W2008SP1-X64-CA

2 Status: local   C=RU,OU=Research,CN=GW1
```

- Вывод пути до контейнера, относящегося к сертификату:

```
cert_mgr show -i 2 | grep "container"

  Private key container name: '\\.\HDIMAGE\HDIMAGE\\vpn5493fd98'
```

  где `-i 2` – номер сертификата.

- Удаление сертификата:

```
cert_mgr remove –i 2
```

 Copyright © S-Terra CSP 2003 -2015

```
2 OK   C=RU,OU=Research,CN=GW1
```

где `-i 2` – номер сертификата.

Описание работы утилиты `cert_mgr` представлено в документации на ПК «С-Терра Шлюз 4.1» (документ «Специализированные команды»).

Для работы с контейнерами применяются следующие утилиты:

- `cont_mgr`, если используется криптобиблиотека, разработанная компанией «С-Терра СиЭсПи»,
- `csptest`, если используется СКЗИ «КриптоПро CSP».

Утилита `cont_mgr`

- Вывод списка контейнеров:

  ```
  cont_mgr show
  file://ContName1
  ```

- Удаление контейнера:

  ```
  cont_mgr delete -cont file://ContName1 -PIN 1234
  ```

  где:

  `-cont file://ContName1` – путь до контейнера.

  `-PIN 1234` – пароль для доступа к контейнеру.

Описание работы утилиты `cont_mgr` представлено в документации на ПК «С-Терра Шлюз 4.1» (документ «Специализированные команды»).

Утилита `csptest` размещена в каталоге /opt/cprocsp/bin/ia32/ или /opt/cprocsp/bin/amd64/, в зависимости от разрядности операционной системы.

- Описание возможных ключей утилиты `csptest` можно вызвать, запустив утилиту с ключом --help:

  ```
  ./csptest --help
  ./csptest -keyset --help
  ```

- Вывод списка контейнеров:

  ```
  ./csptest -keyset -machinekeyset -verifycontext -enum_containers -fqcn –unique
  CSP (Type:75) v3.9.8000 KC1 Release Ver:3.9.8212 OS:Linux CPU:AMD64 FastCode:READY:AVX.
  AcquireContext: OK. HCRYPTPROV: 30670563
  \\.\HDIMAGE\HDIMAGE\\vpn5493fd98
  |\\.\HDIMAGE\HDIMAGE\\vpn5493fd98
  OK.
  Total:
  [ErrorCode: 0x00000000]
  ```

- Удаление контейнера:

  ```
  ./csptest -keyset -machinekeyset -deletekeyset -container '\\.\HDIMAGE\HDIMAGE\\vpn5493fd98' -password pass
  CSP (Type:75) v3.9.8000 KC1 Release Ver:3.9.8212 OS:Linux CPU:AMD64 FastCode:READY:AVX.
  ```

 Copyright © S-Terra CSP 2003 -2015

```
Container \\.\HDIMAGE\HDIMAGE\\vpn5493fd98 deleted.
Total:
[ErrorCode: 0x00000000]
```

где:

`-container '\\.\HDIMAGE\HDIMAGE\\vpn5493fd98'` – путь до контейнера.

`-password pass` – пароль для доступа к контейнеру.

Изменение LSP конфигурации

В LSP конфигурации могут присутствовать структуры с информацией об используемых сертификатах. Если они присутствуют, замените сертификаты и контейнеры на новые (раздел «Удаление контейнеров и сертификатов»), а также измените связанные с ними структуры в LSP.

Пример:

```
IdentityEntry local_auth_identity_01(
  DistinguishedName *= CertDescription(
    Subject *= COMPLETE,"C=RU,CN=base"
    )
)
CertDescription local_cert_dsc_01(
    FingerprintMD5 = "6B681CA341C8D7E8AE8DD4438DEAC243"
    Issuer *= COMPLETE,"CN=S-Terra Demo CA"
    SerialNumber = "612D03BE00000000000D"
    Subject *= COMPLETE,"C=RU,CN=base"
)
```

 Copyright © S-Terra CSP 2003 -2015

Настройка шлюза с использованием скриптов «Программного продукта С-Терра КП»

Чтобы избежать одинаково настроеных шлюзов, необходимо повторно установить предварительно подготовленные скрипты setup_product.sh и setup_upagent с новыми настройками. Настройки должны включать новые лицензии, контейнеры, сертификаты и конфигурацию.

На отдельном компьютере с ОС Windows Server 2003/2008/2008R2/2012 и установленным Сервером управления из состава «Программного продукта С-Терра КП. Версия 4.1» подготовьте два скрипта согласно Руководству администратора http://www.s-terra.com/documents/R41/KP/S-Terra_KP_Admin_Guide.pdf, используя раздел 5 «Настройка и управление центральным шлюзом». Скрипт setup_upagent.sh будет использован для инициализации Клиента управления на обновляемом устройстве, дистрибутив которого уже предустановлен на С-Терра Шлюз 4.1. Скрипт setup_product.sh будет применен для регистрации лицензий, выставления локальных настроек и политики безопасности продукта С-Терра Шлюз 4.1.

После успешного выполнения скриптов необходимо инициализировать датчик случайных чисел (раздел «Повторная инициализация датчика случайных чисел») и удалить старые контейнеры (раздел «Удаление контейнеров и сертификатов»).

 Copyright © S-Terra CSP 2003 -2015