vSphere замена истекшего сертификата

vSphere замена истекшего сертификата vCenter Appliance

18 января 2022 1 Maxim Zhukov

Недавно наш заказчик пришел с проблемой **потери управления виртуализированной инфраструктурой.**

356e0c6b-5b18-f0c2-3727-73a398523848?imagePreview=1

При попытке авторизации в консоль vSphere
An error occurred during authentication

```
Please configure certool.cfg file with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] : (Note: Value for Country should be
only 2 letters)
Enter proper value for 'Name' [Default value : CA] :
Enter proper value for 'Organization' [Default value : VMware] :
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] :
Enter proper value for 'State' [Default value : California] :
Enter proper value for 'Locality' [Default value : Palo Alto] :
Enter proper value for 'IPAddress' [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' [Enter valid Fully Qualified Domain Name(FQDN), For Example
: example.domain.com] :
Enter proper value for VMCA 'Name':
```

Ошибку следует диагностировать просмотром сертификата – который истек (видно из браузера).

При попытке входа в vCenter консоль (**Appliance Management**) для просмотра состояния сервисов

```
Exception in invoking authentication handler
[SSL.CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:719)
```

Проблема в том, что при истекшем сертификате не попасть в консоль управления так как не может аутентифицировать, где по процедуре можно заменить сертификат из web- консоли.

7e776b5c-520a-e13c-40ac-3c1aa9dfddb3?imagePreview=1

Причину подтвердим просмотром трейса ошибки:

```
javax.net.ssl.SSLHandshakeException:
com.vmware.vim.vmomi.client.exception.VlsiCertificateException:
Server certificate chain is not trusted and thumbprint verification is not configured
```

Ошибки при истекшем сертификате будут вида

Что **такая-то служба** не может соединиться (так как **не устанавливается защищенное соединение с vCenter Appliance** из-за невалидного сертификата)

```
Authentication failed, Update Manager server could not be contacted.


An unexpected error has occurred.
```

> В том числе **не будет работать и служба Аутентификации vSphere**, а это, сами понимаете, «привет» управлению инфраструктурой и работе служб vSphere.

Что делать?

Нужно заменить истекший сертификат в vCenter Appliance. Но есть ньюансы.

При отсутствии доступа в web-консоль **vCenter Appliance Management**

```
Exception in invoking authentication handler
[SSL.CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:719)
```

Остается доступ через коммандную строку в виртуальную машину.

В ситуации с истекшим сертификатом работоспособность запущенных виртуальных машин не затронута, и можно зайти на узлы гипервизора ESXi и временно поуправлять вручную запуском и выключением виртуальных машин.

Собственно этот путь (**через подключения к ESXi**) с вызовом консоли машины с vCenter Appliance и потребуется проделать для замены истекшего сертификата, если на машине выключен **SSH** в целях безопасности.

Но где лежит сертификат и как его правильно заменить?

Оказывается, что для генерации сертификата vCenter Server Appliance имеет утилиту **Certificate Manager.**

Для начала подключитесь к vCenter через ssh или через консоль виртуальной машины с vCenter через гипервизор ESXi где она функционирует.

Если у Вас много хостов в инфраструктуре, возможно придется поискать последовательно подключаясь на каждый пока не отыщите свой запущенный vCenter.

1. # Запустите /usr/lib/vmware-vmca/bin/certificate-manager

    1. # Если Вам приемлем Self-Signed Certificate и нужно быстро восстановить доступ

        1. Выбирите пункт **4 Regenerate a new VMCA Root Certificate and replace all certificates** и введите пароль для administrator@vsphere.local
        2. Далее последовательно заполните поля с учетом того, что **Name, Hostname и VMCA должны соответствовать Primary Network Identifier PNID** .
        3. Значение PNID можно посмотреть выполнив /usr/lib/vmware-vmafd/bin/vmafd-cli get-pnid --server-name localhost
        4.
        5. Нажмите Y (Yes) для продолжения.
        6. В случае неактуального сертификата в веб-консоли vCenter перезагрузите vCenter.

    2. # Если Вы хотите валидный сертификат полученный через центр сертификации

        1. В меню выберите пункт **1. Replace Machine SSL certificate with Custom Certificate** и введите пароль для administrator@vsphere.local
        2. Укажите директорию, где будут помещены запросы на выпуск, например /tmp/ssl/
        3. Далее последовательно заполните поля с учетом того, что **Name, Hostname и VMCA должны соответствовать Primary Network Identifier PNID** .
        4. Значение PNID можно посмотреть выполнив /usr/lib/vmware-vmafd/bin/vmafd-cli get-pnid --server-name localhost

5.
```
Country      : Two uppercase letters only (Eg. US), the country where your company is located.
Name         : FQDN of the vCenter Server(This will be your Certificate Subject Alternate Name)
Organization : Company Name
OrgUnit      : The name of your department within the organization. Example: "IT"
State        : The state/province where your company is located
Locality     : The city where your company is located.
IPAddress    : IP Address of vCenter Server, this field is Optional
Email        : Email Address
Hostname     : FQDN of vCenter Server(This field accepts multiple entries separated by comma.
```

6. Файл /tmp/ssl/vmca_issued_csr.csr передаем в центр сертификации для выпуска SSL сертификата.
7. Помещаем выпущенный сертификат на систему, например, в /tmp/ssl/ в отдельной сессии
8. Продолжаем импорт

```
Provide a valid custom certificate for Machine SSL.
File : /tmp/ssl/machine_name_ssl.cer

Provide a valid custom key for Machine SSL.
File : /tmp/ssl/machine_name_ssl.key

Provide the signing certificate of the Machine SSL certificate.
File : /tmp/ssl/Root64.cer
```

9. Нажмите Y (Yes) для продолжения.
10. В случае неактуального сертификата в веб-консоли vCenter перезагрузите vCenter.

Revision #3
Created 2023-04-10 11:06:19 UTC by yuzer
Updated 2023-09-11 22:28:14 UTC by yuzer