

Kubernetes: Обновление сертификатов кластера

Взял у Слерма.

Команды kubectl различных версий для продления сертификатов.

В зависимости от версии kubectl ключи и функционал по обновлению сертификатов менялись и расширялись, поэтому я приведу команды для разных версий kubectl.

Версия kubectl	Команда	Что делает
1.12	kubectl alpha phase certs renew all	продлевает все сертификаты в каталоге /etc/kubernetes/pki
1.13 и 1.14	kubectl alpha certs renew all	продлевает все сертификаты в каталоге /etc/kubernetes/pki
1.15 - 1.19	kubectl alpha certs renew all	продлевает все сертификаты в каталоге /etc/kubernetes/pki, а также сертификаты в файлах конфигурации controller-manager.conf, scheduler.conf, admin.conf
1.20 и выше	kubectl certs renew all	продлевает все сертификаты в каталоге /etc/kubernetes/pki, а также сертификаты в файлах конфигурации controller-manager.conf, scheduler.conf, admin.conf Игнорирует отсутствующие файлы сертификатов, без ошибки

До kubectl версии 1.15 для продления сертификатов в файлах конфигурации .conf надо использовать команду

```
kubectl alpha kubeconfig user --client-name --org
```

указывая client-name и org такие же, как в существующих сертификатах.

```
kubectl alpha kubeconfig user --client-name kubernetes-admin --org system:masters > /etc/kubernetes/admin.conf
kubectl alpha kubeconfig user --client-name system:kube-scheduler > /etc/kubernetes/scheduler.conf
kubectl alpha kubeconfig user --client-name system:kube-controller-manager > /etc/kubernetes/controller-manager.conf
```

Для продления сертификата в kubelet.conf на первом мастер узле до версии 1.16 также надо пользоваться командой

```
kubectl alpha kubeconfig user
```

но только надо не забыть указать актуальное название узла, для kubelet которого

продлевается сертификат

```
kubeadm alpha kubeconfig user --client-name system:node:kube.s000.slurm.io -  
-org system:nodes > /etc/kubernetes/kubelet.conf
```

Начиная с версии 1.17 на всех узлах кластера kubelet автоматически продлевает свой сертификат при необходимости, в том числе и на том узле, который был создан самым первым в кластере (командой `kubeadm init`). На этом узле сначала создается временный сертификат, а после запуска кластера он меняется на динамический, который хранится в файле `/var/lib/kubelet/pki/kubelet-client-current.pem`

[kubernetes](#), [k8s](#), [certificate](#), [renew](#), [обновление сертификатов](#)

From:

<https://wiki.rtzra.ru/> - RTzRa's hive

Permanent link:

<https://wiki.rtzra.ru/devops/k8s/k8s-certs-renew>

Last update: **2022/06/07 19:19**

