Kubernetes: Обновление сертификатов кластера

Взял у Слерма.

Команды kubeadm различных версий для продления сертификатов.

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

Версия kubeadm	**Команда**	**Что делает**
1.12	kubeadm alpha phase certs renew all	продлевает все сертификаты в каталоге /etc/kubernetes/pki
1.13 и 1.14	kubeadm alpha certs renew all	продлевает все сертификаты в каталоге /etc/kubernetes/pki
1.15 - 1.19	kubeadm 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	kubeadm 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 остутствующие файлы сертификатов, без ошибки

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

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

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

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

```
kubeadm 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**