

Обновление/Установка KUMA версии до 2.0.X (распределенная инсталляция)

1. Создайте резервную копию ресурсов и сертификатов, см. советующий раздел в этой книге.

2. Распакуйте архив (операции выполняются на ядре системы KUMA):

```
tar -xvf kuma-ansible-installer-(БЕПСИЯ).tar.gz
```

3. Перейдите в распакованную папку:

```
cd kuma-ansible-installer
```

4. Добавить файл лицензии в папку `kuma-ansible-installer/roles/kuma/files` и переименовать на `license.key`:

```
cp ПУТЬ_ДО_КЛЮЧА*.key roles/kuma/files/license.key
```

5. Выполните команду копирования шаблона (либо подставьте ранее использованный файл при обновлении):

```
cp distributed.inventory.yml.template distributed.inventory.yml
```

6. Добавьте публичный ключ SSH на все удаленные хосты в том числе и для хоста с которого происходит развертывание:

1. На ВСЕХ хостах в конфигурации сервиса SSH должна быть включена опция удаленного входа от суперпользователя!

2. На хосте с которого происходит развертывание сгенерируйте ключ командой (без указания пароля и доп. параметров):

```
ssh-keygen -t rsa
```

3. Добавьте ключ по ssh на удаленные хосты и на сам хост развертывания:

```
ssh-copy-id login@remote_host_fqdn
```

7. Отредактируйте файл инвентаря с командой:

```
nano distributed.inventory.yml
```

В случае ручной правки файла старайтесь не добавлять лишних пробелов.

Количество keeper (ZooKeeper) должно быть нечетным (минимум 3). Если, например, хранилища два, то в файле инвентаря укажите в `storage: hosts: <полное_доменное_имя_машины> :` (этом может быть `core`, `collector`) с его IP адресом и значением keeper, по аналогии с другими записями. Например, если используется два хранилища, то конфигурация `storage` будет выглядеть следующим образом:

```
storage:
  hosts:
    kuma-maybe-collector.example.com:
      ip: 1.1.1.1
      keeper: 1
    kuma-storage-1.example.com:
      ip: 0.0.0.0
      shard: 1
      replica: 1
      keeper: 2
    kuma-storage-2.example.com:
      ip: 0.0.0.0
      shard: 1
      replica: 2
      keeper: 3
```

Для развертывания отдельного одного хранилища без кластера используйте следующие настройки в `distributed.inventory.yml`:

```
hosts:
  [REDACTED]-siem-app-01.[REDACTED].ru:
    ip: 0.0.0.0
    mongo_log_archives_number: 14
    mongo_log_frequency_rotation: daily
    mongo_log_file_size: 1G
collector:
  hosts:
    [REDACTED]-siem-app-01.[REDACTED].ru:
      ip: 0.0.0.0
correlator:
  hosts:
    [REDACTED]-siem-app-01.[REDACTED].ru:
      ip: 0.0.0.0
storage:
  hosts:
    [REDACTED]-siem-db-01.[REDACTED].ru:
      ip: 0.0.0.0
      shard: 1
      replica: 1
      keeper: 1
```

Демонстрационные сервисы

Если Вы хотите, чтобы инсталлятор развернул демонстрационные сервисы, присвойте параметру `deploy_example_services` значение `true` (Только для новых инсталляций).

Генерация содержимого файла `/etc/hosts`

Если целевые машины НЕ зарегистрированы в DNS-зоне вашей организации, то присвойте параметру `generate_etc_hosts` значение `true` и для каждой машины в инвентаре, замените значения параметра `ip` `0.0.0.0` на актуальные IP-адреса.

Список целевых машин

В файле определены 4 группы, именованные аналогично ключевым компонентам KUMA: `core`, `collector`, `correlator`, `storage`. Помещая целевую машину в одну из групп, вы инструктируете инсталлятор установить на нее соответствующий компонент KUMA. В каждой группе замените строки с суффиксом `*.example.com` на актуальные имена хостов целевых машин.

- Группа `core`. Может содержать только одну целевую машину.
- Группа `collector`. Может содержать одну или несколько целевых машин.
- Группа `correlator`. Может содержать одну или несколько целевых машин.
- Группа `storage`. Может содержать одну или несколько целевых машин. Каждая машина должна иметь одну из следующих комбинаций параметров:
 - `shard + replica + keeper`
 - `shard + replica`
 - `keeper`

Про устройство кластера хранилища можно почитать [тут](#).

Если хранилище одно, то оставьте параметры shard + replica + keeper, как у kuma-storage-1.example.com

Перед началом установки инсталлятор KUMA выполнит валидацию инвентаря и укажет на ошибки, если таковые были допущены.

8. Входим в ОС из-под суперпользователя (root):







```
sudo -i
```

9. Запустите процесс инсталляции:

```
./install.sh distributed.inventory.yml
```

10. Выполните настройку storage на использование двух хранилищ. В точках назначения нужно добавить URL второго хранилища, (если используются отдельные keeper, то их не нужно указывать в точках назначения) пример ниже:

Изменить точку назначения

Основные параметры	Дополнительные параметры
*Название	<input type="text" value="[Example] Storage"/>
*Тенант	<div>Main </div>
	<div><input type="checkbox"/> Выключено</div>
*Тип	<div>storage </div>
*URL	<div>kuma-storage-1.example.com:7230 </div>
URL	<div>kuma-storage-2.example.com:7230 </div>
	<div><div>Копировать URL сервиса</div><div>+ URL</div><div></div></div>
Описание	<div>Описание </div>

Корректность работы можно проверить, перейдя во вкладку События и нажав на значок увеличительного стекла (Поиск), должны появиться события, поступающие KUMA или Сообщение «События не найдены». Если при поиске возникает ошибка, то необходимо проверить статусы сервисов в веб интерфейсе KUMA. Провести первичный траблшутинг по этому документу и сообщить ответственному инженеру Лаборатории Касперского в случае неуспеха.

Revision #7

Created 10 August 2023 13:40:49 by Boris RZR

Updated 7 July 2024 08:30:24 by Koala