это to do, тему нужно разобрать глубже, используется для командной разработки.

**docker create secret secretName fileWithPasswords.txt**

https://docs.docker.com/engine/swarm/secrets/

<https://docs.docker.com/compose/how-tos/use-secrets/>

В docker хорошей практикой является не хранить пароли в образах во избежания их утечки при коммитах.

Именно docker secret предназначены для хранения паролей во многонодовых проектах. Должен быть инициалезироват docker sworm(рой) init для возможности создания secret. Насколько я понял, docker sworm предназначен для объединения нескольких компьютеров(нод) с подчененными docker под руководство головного компьютера с управляющим docker. Тогда возможно распределить нагрузку между машинами путем запуска копийодного одного образа на разных нодах. И тогда каждая копия образа на разных нодах будет иметь доступ к secret не храня пароли в себе. Так-же secret применяется и в kubernetes.

При создании srcret docker создает что-то похожее на volume но с шифрованием, в котором хранится файл с паролями или непосредственно пароль. Монтирование происходит как volume и тогда в контейнере становится доступен файл с паролем уже без шифрования. Шифрует каждый docker своим индивидуальным ключем, поэтому secret нельзя перенести с машины на машину. В образе вместо пароля указывается ссылка на secret.

Если разработка происходит в «одно рыло» и docker sworm не инициализирован, то secret создать нельзя, однако рекомендуется использовать bind mounts с файлом с паролями, а в образе вместо паролей использовать ссылки на пароли.

Так-же не рекомендуется использовать для хранения паролей переменные окружения docker (ARG, ENV), так-как, насколько я понял, их значения остаются в логах сборки образа.

Docker secrets ограничены размером в 500 КБ.