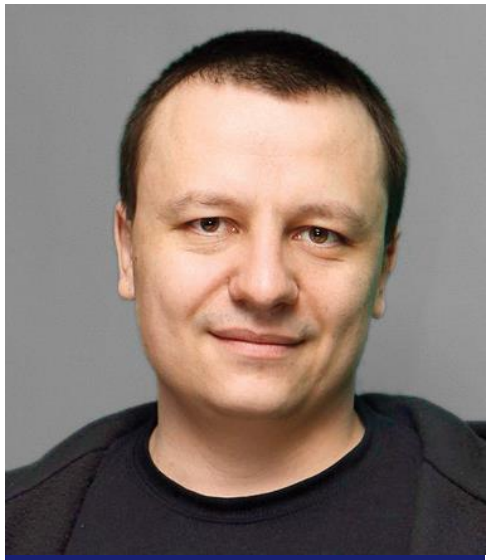
28 ОКТЯБРЯ 2022

Установка SUSE Rancher в среде с воздушным зазором

Не от всего можно укрыться за высоким забором.



Павел Жуков

SUSE Enterprise Architect

pavel.zhukov@suse.com

Содержание

1. Обеспечение безопасности контейнеров
2. Реализация «Воздушного зазора»
3. Демонстрация

Главные проблемы безопасности контейнеров

Быстрый рост популярности контейнерных решений

Традиционные средства ИБ не приспособлены к такой среде

Абстракция Kubernetes снижает сложность, но скрывает важные детали работы.

Уровни безопасности: эшелонированная оборона

Безопасность цепочки поставок

- Сканирование уязвимостей
- Проверка соответствия
- Разрешение запуска контейнера

Безопасность среды выполнения

- Сканирование при выполнении
- Оценка угроз в реальном времени
- Среда нулевого доверия

Варианты решения

Zero-Trust подход в реализации решения

- Использование специализированных решений
  - NeuVector
- Реализация «классических» методов
  - Автоматизация и уменьшение человеческого фактора
  - Контроль среды исполнения
  - Обновление программного обеспечения
  - Воздушный зазор

NeuVector и жизненный цикл контейнеров

Сборка | **Тестирование** | **Испытания** | **Производственная среда**

Обнаружение уязвимостей и проверка соответствия требованиям при сборке

Сканирование при сборке

Сканирование реестра

Проверка настроек Kubernetes и аудит

Проверка соответствия требованиям PCI, GDPR, NIST

Сканирование при работе контейнеры, хосты, платформы

Защита при выполнении

Развертывание

Политики безопасности как код

Автоматизация настройки Анализ поведения

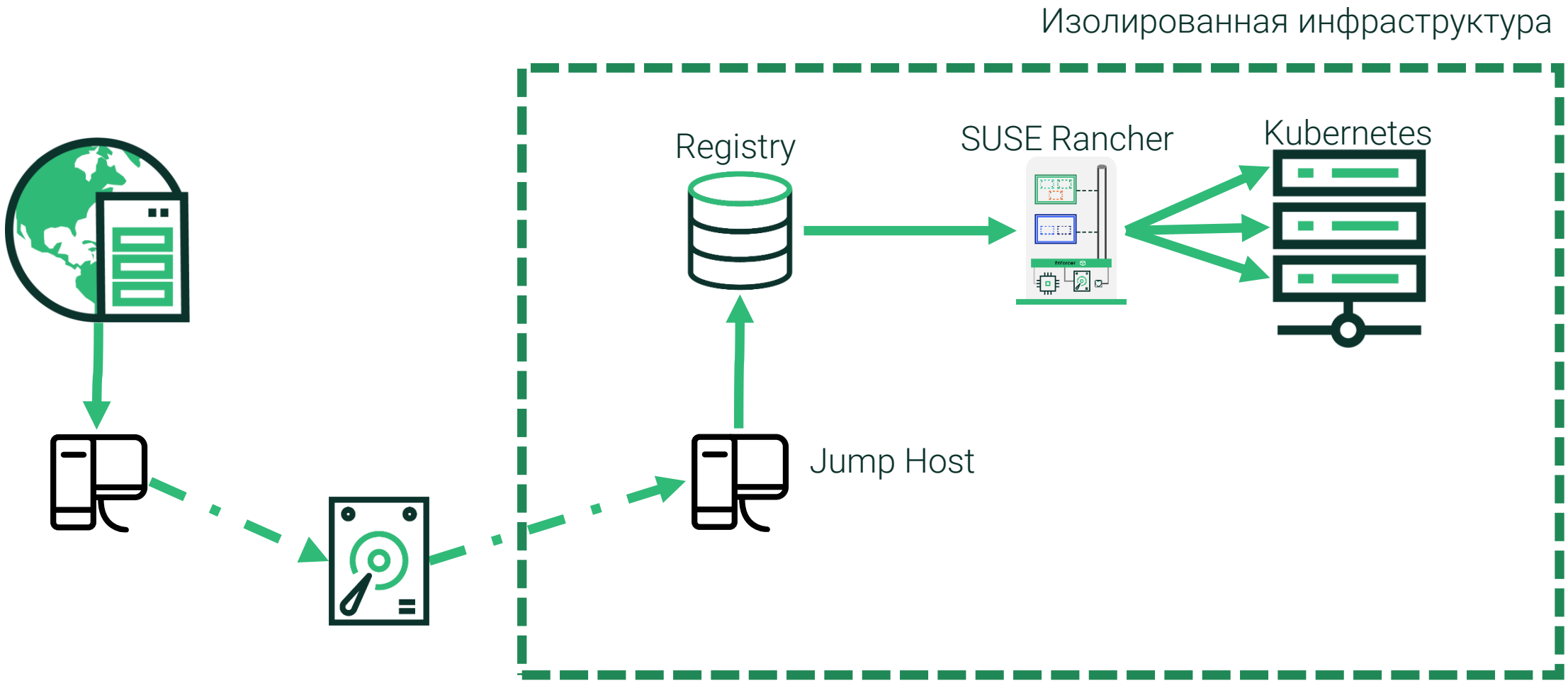
Разрешение или запрет запуска

Межсетевой экран уровня 7 DPI/DLP/WAF

Контроль доступа Блокировка процессов и попыток доступа к файлам

Оповещение Журналы

Воздушный зазор



Реализация

Данные для загрузки

- Скрипты загрузки образов в Registry
- Список образов
  - Rancher
  - RKE2
  - Cert manager
- Данные Helm
  - Render шаблона Rancher
  - Render шаблона Cert Manager
- CRD Cert Manager

Описание Демо-стенда
https://github.com/ppzhukov/airgap-10.2022

Реализация

Согласование версий

Требуется согласовать версии

- Для SUSE Rancher версии 2.6.8 требуется Kubernetes не выше 1.25
- RKE2 для этого соответствует версии v1.24.X
- Для работы с ним требуется Helm версии не выше 3.9.X

Описание Демо-стенда
https://github.com/ppzhukov/airgap-10.2022

Реализация

Данные для загрузки (Список образов)

- Rancher
  страница с данными releases на github https://github.com/rancher/rancher/releases
- RKE2
  страница с данными releases на github https://github.com/rancher/rke2/releases
  - если планируете использовать Registry для первичной установки, удалите в начале строк файла “docker.io/”
- Cert manager
  требуется получить из данных helm chart

Описание Демо-стенда
https://github.com/ppzhukov/airgap-10.2022

Реализация

Порядок действий

1. Загрузить нужные данные на подключенный к интернет узел
2. Перенести данные в изолированный сегмент
3. Установить
    1. RKE2
    2. Cert manager
    3. Rancher
4. Установить управляемые кластера Kubernetes

Описание Демо-стенда
https://github.com/ppzhukov/airgap-10.2022

Реализация

Локальный Registry

- Можно использовать Docker Registry
  - В описании демо-стенда используется R/W – для загрузки и R/O – анонимный
- Для загрузки образов в Registry Docker должен доверять сертификату Registry
- Если совмещаются роли Jump Host и Registry потребуется дополнительное место (с системой всего порядка 200 GB)
  - архив образов
  - место для разжатых образов в Docker
  - место в Registry

Описание Демо-стенда
https://github.com/ppzhukov/airgap-10.2022

Реализация

Установка RKE2

- Два варианта установки (https://docs.rke2.io/install/airgap/)
  - Tarball Method
    Вам потребуется скачать образы и разместить их на системе
  - Private Registry Method
    - Вам потребуется добавить файл настройки с параметром:
      system-default-registry
      Пример /etc/rancher/rke2/config.yaml:
      system-default-registry: "192.168.0.10.sslip.io:5000"
    - Для систем RKE2 Версий < v1.20 нужно добавить сертификат Registry в доверенные

Описание Демо-стенда
https://github.com/ppzhukov/airgap-10.2022

Реализация

Установка cert-manager

- Создайте Name Space для cert-manager
- Установите CRD
  Используйте ранее загруженный файл для установки в K8S CRD для cert-manager
- Установите cert-manager
  Используйте полученный ранее render шаблона для установки cert manager

Описание Демо-стенда
https://github.com/ppzhukov/airgap-10.2022

Реализация

Установка Rancher

- Создайте Name Space для SUSE Rancher (cattle-system)
- Установите SUSE Rancher
  Используйте полученный ранее render шаблона для установки SUSE Rancher

Описание Демо-стенда
https://github.com/ppzhukov/airgap-10.2022

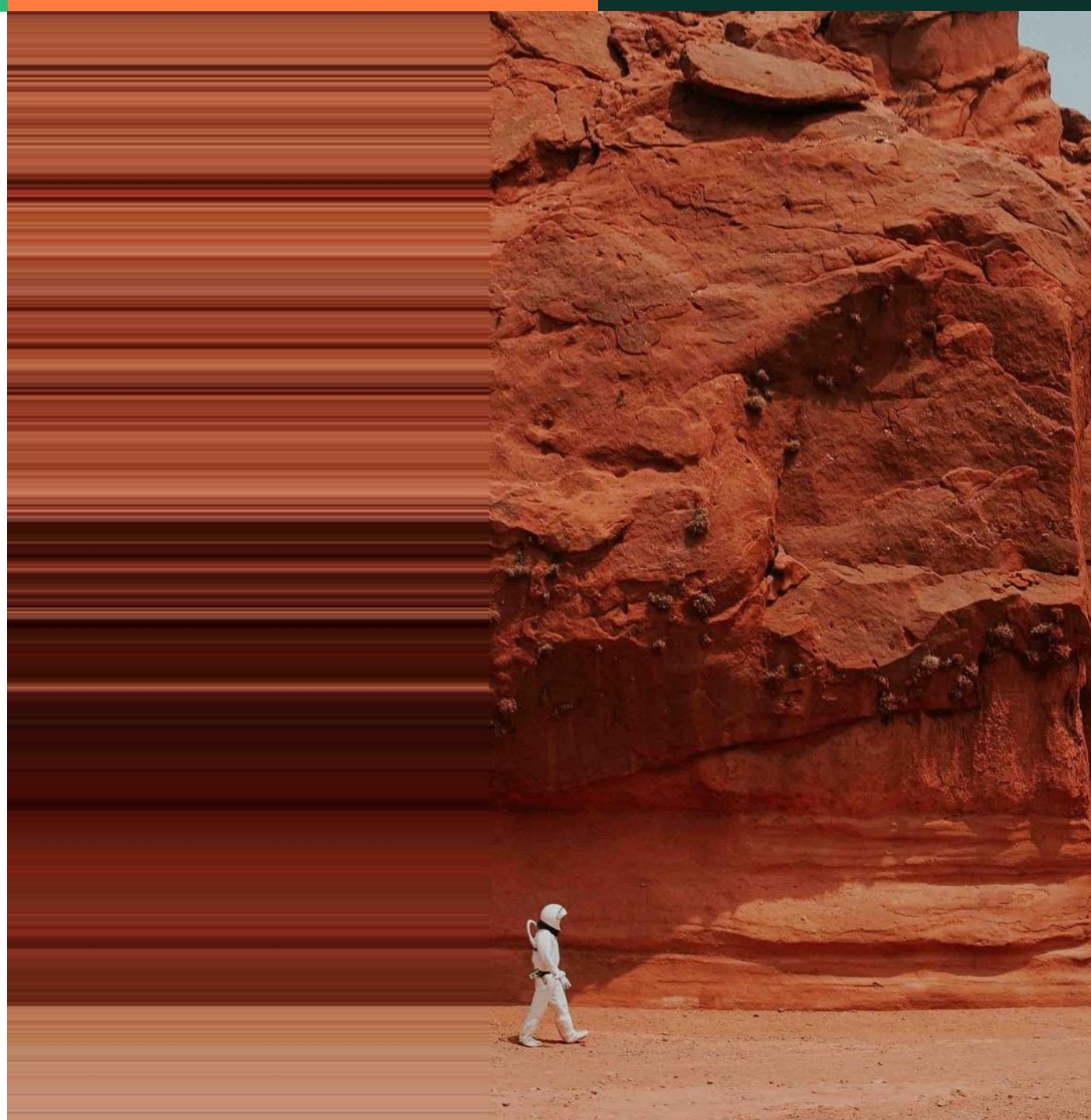
Реализация

Установка управляемых кластеров Kubernetes

- RKE
  Производится штатно
  Все нужные образы загружаются вместе с образами Rancher
- RKE2
  Производится штатно
  Все нужные образы добавляются из данными releases RKE2
- В обоих случаях используется локальный (приватный) Registry

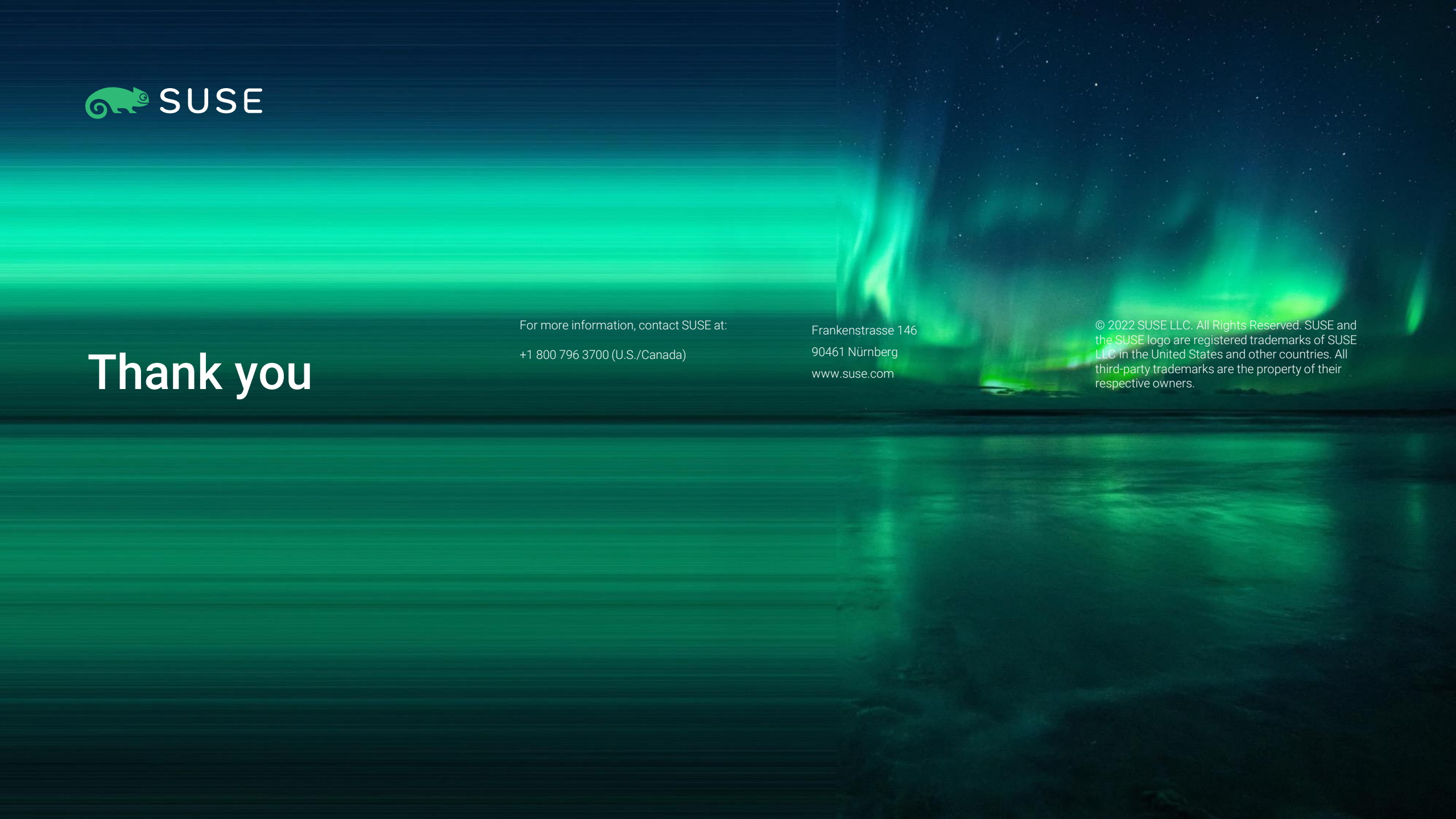
Описание Демо-стенда
https://github.com/ppzhukov/airgap-10.2022

Демонстрация



Полезные ссылки

- Установка Rancher Air-Gap
  https://docs.ranchermanager.rancher.io/pages-for-subheaders/air-gapped-helm-cli-install
- Установка RKE2 Air-Gap
  https://docs.rke2.io/install/airgap/
- Установка K3S Air-Gap
  https://docs.k3s.io/installation/airgap
- Инструкция для демо-стенда этого вебинара
  https://github.com/ppzhukov/airgap-10.2022



Thank you

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

Frankenstrasse 146

90461 Nürnberg

www.suse.com