Network Campus Controller

Secure Device Provisioning Using SZTP

Students

Vanessa Gyger

Patrick Lenherr

Initial Situation: Managing many network devices takes a lot of effort and poses risks of inconsistency in configuration. Furthermore, time is needed to plug the device in, attach your computer and connect to the console for configuration. With automation, this process can be made much more efficient and reliable. The classical approach for this is called Zero Touch Provisioning (ZTP), meaning the device doesn't have to be touched to configure it. Instead, it is registered in an inventory and can load a predefined configuration automatically.

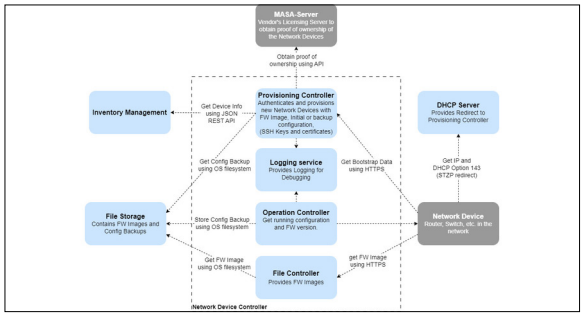
Objective: The objective of our term project is to lay the groundworks for a network controller that handles zero touch provisioning of newly installed devices, as well as transferring configuration in case of 1-to-1 device replacement. The scope of the controller is limited to Cisco devices for this project, but it should be extendable to support various other devices. Furthermore, the controller should also be open for future extension, providing more functionality like ongoing configuration after the provisioning process.

Result: We developed a controller that bridges between inventory management and network device. On one end Netbox is used to manage device parameters and context-dependent configuration. Both are rendered into the target devices configuration using a template. On the other end the devices use DHCP to get SZTP redirect information for the controller.
Our provisioning controller provides an endpoint for SZTP-compliant devices to securely get the data needed to bootstrap themselves via HTTPS. The bootstrapping data includes firmware target version, download source and integrity hash as well as the configuration itself.
During the devices lifetime our backup controller is used to automatically retrieve configuration backups. In the event of a hardware failure, a replacement device can quickly be set up. By simply setting the configuration source device in Netbox the provisioning controller will automatically load the backup configuration.

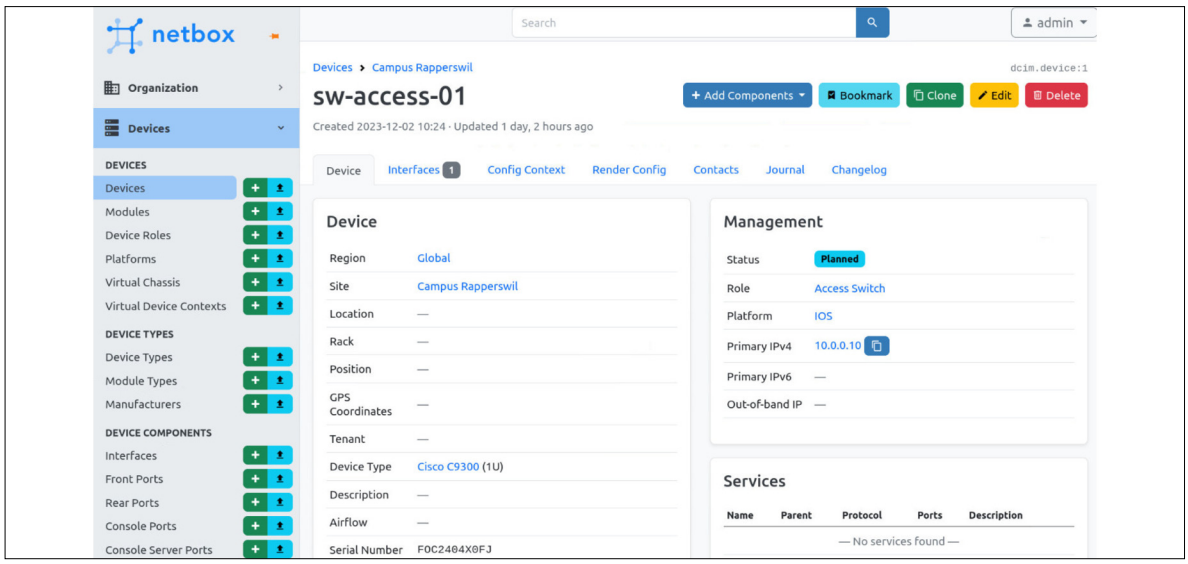
Cisco device certificate
Own presentment

```
Certificate
  Status: Available
  Certificate Serial Number (hex): 01FCCFBD
  Certificate Usage: General Purpose
  Issuer:
    o=Cisco
    cn=High Assurance SUDI CA
  Subject:
    Name: C9300-24P
    Serial Number: PID:C9300-24P SN:FOC2404X0FJ
    cn=C9300-24P
    ou=ACT-2 Lite SUDI
    o=Cisco
    serialNumber=PID:C9300-24P SN:FOC2404X0FJ
```

Network device controller component
Own presentment



Device inventory
Own presentment



Advisor
Urs Baumann

Subject Area
Networks, Security & Cloud Infrastructure