Universität Stuttgart
Technische Informations- und
Kommunikationsdienste (TIK)

All config models suck!

Choose the one that sucks least!

Kilian Krause
kilian.krause@tik.uni-stuttgart.de
BelWü TechDay, 2024-04-09

tik

Universität Stuttgart

Zahlen und Fakten

- 1829 gegründet, hat sich die frühere Technische Hochschule zu einer forschungsintensiven Universität mit überwiegend ingenieur- und naturwissenschaftlicher Orientierung entwickelt, zu deren besonderem Profil die Vernetzung dieser Fachrichtungen mit den Geistes- und Sozialwissenschaften gehört.
- 22.000 Studierende an 10 Fakultäten
- 270 Professoren und Professorinnen, 3.500 wissenschaftlich Beschäftigte, 1.800 nichtwiss. Beschäftigte
- 2 Campus-Standorte, 140 Gebäude 350.000 m^2 Hauptnutzfläche
- HLRS: Tier-1 HPC
- Starke Kooperation mit außer–universitären Forschungs–einrichtungen
- Im Herzen einer der stärksten High-Tech-Regionen Europas

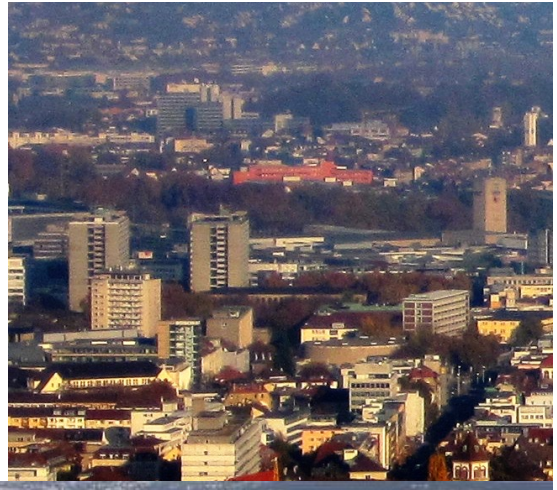


Foto: Universität Stuttgart / © Luftbild Elsässer

Status quo

- **Border/Core/Datacenter**
  - Vollständiges [selbst geschriebenes] Configuration-Management
  - Git Repository mit eigener Template Engine
  - ACLs separat verwaltet (anderes eigenes Tooling)
- **Access-Netz Gebietsrouter**
  - Analog zu DC voll standardisiert, Template-basierend
- **Access-Netz Aggregation/Access**
  - Reiner „Hand-am-Arm“ Modus
  - Keine einheitlichen Standards -> „gewachsene Konfiguration“
  - Templating für Standardconfig bei Switchtausch (neue Hardware-Generation)

Motivation

- Vermeidung Vendor-Lock in
- Steigerung der Compliance
- Vermeidung von “Experten-Wissen/Datenbank”
  → aktuell viel “gefühlte” Konfiguration
  - z.B. Drucker, Laborgeräte
  - Legacy-Trail wird immer länger!
  - Dokumentation schwierig, Wegfallbedingungen unklar
- Spezialfälle müssen individuell betrachtet werden → Reduzieren möglich?
- Größere Änderungen kaum strukturiert automatisierbar
- Onboarding neuer Mitarbeiter, Urlaubsvertretung schwierig

Motivation – Teil 2

- RZ eher ISP als IT-Abteilung → Schnittstelle?
- Compliance muss vom dezentralen Admin kommen (BYOD!)
- [regelmäßiges] Reporting an dezentrale Admins
  - Admins wechseln oft
  - Neue Admins erhalten nicht immer Doku
  - Automatische Wiedervorlage durch das TIK?
  - Aufforderung zur Nachdokumentation (z.B. neue Räume)
- Sonderfälle sauber zurückbauen, wenn nicht mehr benötigt

Bisheriger Ansatz

- Manuelle Konfiguration
- Wenig Unterschiede durch starke Homogenität der Hardware-Auswahl
- Viele Möglichkeiten der Switch-Soft-/Hardware, aber nicht intensiv genutzt (höchstens punktuell)
- Zentralisierung stark auf allgemeine Konfiguration (nicht pro Interface/Port)
- Nur wenige Spezialfälle pro Switchport/Nutzer (punktuell genutzt)
- Quasi keine dynamische Konfiguration (MAB, 802.1X nur in Ausnahmefällen)

Layer1 Infrastruktur Grundlagen

- Genauigkeit der Infrastrukturpläne nicht 100%
- Vollständige Automatisierung ohne Nutzerauthentifizierung technisch nicht umsetzbar
- Leitungsverfügbarkeit eher weniger problematisch
- Einzelne Nutzer dürfen aus historischen Gründen selbst rangieren
- Nicht überall dedizierte Verteiler exklusiv nur für Netz verfügbar
- Wanddosen direkt auf Switch rangiert, aber nicht überall Endgeräte direkt in Wanddose angeschlossen
- Teilweise Desktop-Switches hinter Wanddosen → nicht einheitlich

Umsetzungsoptionen

- Dynamische Switchportkonfiguration (User-/Machine-/MAC-Auth)
- Template Engine im IOS-XE
- Makros im IOS-XE
- Embedded event manager (Cisco EEM)
- Template Engine auf Management-Host
  - Ansible
  - Terraform
  - Selbst geschrieben
- Hersteller Management-Framework
  - z.B. Catalyst Center
  - DCNM

Template Engine IOS-XE

- ```
  template TIK
    storm-control broadcast level pps 100 10
    description RUS
  ```
- ```
  Switch#show run int gi1/0/6
  interface GigabitEthernet1/0/6
    description OVERRIDE-RUS
    storm-control broadcast level pps 5k 500
    source template TIK
  end
  ```
- ```
  evpn-test-a3-mgmt#show derived-config int gi1/0/6
  Building configuration...
  interface GigabitEthernet1/0/6
    description OVERRIDE-RUS
    storm-control broadcast level pps 5k 500
  end
  ```
  ```

Makro auf IOS-XE

- ```
  Switch(config)#macro name TIK
  Enter macro commands one per line. End with the character '@'.
  description ** NKS **
  switchport mode access
  switchport access vlan 123
  spanning-tree portfast
  @
  ```
- ```
  Switch(config)# interface TwentyFiveGigE1/0/2
  description ** NKS **
  switchport access vlan 123
  switchport mode access
  macro description TIK
  end
  ```
- ```
  Switch#show parse macro name TIK
  Macro name : TIK
  Macro type : customizable
  description ** NKS **
  switchport mode access
  switchport access vlan 123
  ```
  ```

EEM für Switchport-Config

https://community.cisco.com/t5/wireless-mobility-blogs/using-eem-and-cdp-for-ap-port-description-and-configuration/ba-p/3798247

```
event manager applet detect-AP-add-adress authorization bypass
event neighbor-discovery interface regexp Ethernet.* cdp add
action 1.0 regexp "(AIR-)" "$_nd_cdp_platform"
action 2.0 if $_regexp_result eq "1"
action 3.0 cli command "enable"
action 4.0 cli command "config t"
action 5.0 cli command "default interface $_nd_local_intf_name"
action 5.1 cli command "int $_nd_local_intf_name"
action 5.2 cli command "switch access vlan 255"
action 5.3 cli command "switchport mode access"
action 5.5 cli command "load-interval 30"
action 5.6 cli command "spanning-tree portfast"
action 5.7 cli command "spanning-tree link-type shared"
action 6.0 cli command "end"
action 6.1 cli command "write"
action 6.2 syslog msg "EEM script configured AP port and saved config"
action 7.0 end
```

Ansible für Switchport-Config

```yaml
- name: Configure top level configuration
  cisco.ios.ios_config:
    lines: hostname {{ inventory_hostname }}

- name: Configure interface settings
  cisco.ios.ios_config:
    lines:
      - description test interface
      - ip address 172.31.1.1 255.255.255.0
    parents: interface Ethernet1

- name: Configure ip helpers on multiple interfaces
  cisco.ios.ios_config:
    lines:
      - ip helper-address 172.26.1.10
      - ip helper-address 172.26.3.8
    parents: "{{ item }}"
  with_items:
    - interface Ethernet1
    - interface Ethernet2
    - interface GigabitEthernet1
```

Terraform Switchport Config

```
resource "iosxe_interface_ethernet" "example" {
  type                            = "GigabitEthernet"
  name                            = "3"
  bandwidth                       = 1000000
  description                     = "My Interface Description"
  shutdown                        = false
  ip_proxy_arp                    = false
  ip_redirects                    = false
  ip_unreachables                 = false
  ipv4_address                    = "15.1.1.1"
  ipv4_address_mask               = "255.255.255.252"
  ip_dhcp_relay_source_interface = "Loopback100"
  ip_access_group_in              = "1"
  ip_access_group_in_enable       = true
  ip_access_group_out             = "1"
  ip_access_group_out_enable      = true
  helper_addresses = [
    {
      address = "10.10.10.10"
      global  = false
      vrf     = "VRF1"
    }
  ]
  source_template = [
    {
      template_name = "TEMP1"
      merge         = false
    }
  ]
```

Selbstgeschriebene Template Engine

```
profiles:
  adminvpn-outside:
    cdp: false
    stp: false
    vlan: 122
  oob-maintenance:
    vlan: 123
  oob-maintenance-1g:
    vlan: 124
    speed_nonegotiate: true
  provision:
    vlan: 1

router1:
  managed_ports:
    1: TwentyFiveGigE1/0/{1-24}
    25: HundredGigE1/0/{25-28}
    201: TwentyFiveGigE2/0/{1-24}
    225: HundredGigE2/0/{25-28}
  virtual_stack:
    "on Switch 1":              TwentyFiveGigE1/0/{23-24}
    "on Switch 2":              TwentyFiveGigE2/0/{23-24}
    # keepalive: TwentyFiveGigE{1-2}/0/{19-20}
  network:
    "switch1":                  TwentyFiveGigE{1-2}/0/1
    "switch2":                  TwentyFiveGigE{1-2}/0/5
    "switch3":                  TwentyFiveGigE{1-2}/0/9
    "switch4":                  TwentyFiveGigE{1-2}/0/10
  oob-maintenance:
    "oob LR maintenance":
      channel:                  false
      members:                  TwentyFiveGigE1/0/14
  oob-maintenance-1g:
    "oob LX maintenance":
      channel:                  false
      members:                  TwentyFiveGigE2/0/14
  l3_uplinks:
    - "Up C1":
        members:                HundredGigE{1-2}/0/27
    - "Up C2":
        members:                HundredGigE{1-2}/0/28
```

```
$  ./manage diff --exec router1
Generating config for router1
On Host router1:
---
l2vpn evpn
 no default-gateway advertise
no l2vpn evpn instance 465 vlan-based
no vlan configuration 465
interface Port-channel33
 no switchport trunk allowed vlan 205,207,465,477,483-485,560,833-837
 switchport trunk allowed vlan 205,207,477,483-485,560-562,833-837
interface Port-channel93
 no switchport trunk allowed vlan 205,207,465,477,483-485,560,833-837
 switchport trunk allowed vlan 205,207,477,483-485,560-562,833-837
interface TwentyFiveGigE1/0/33
 no switchport trunk allowed vlan 205,207,465,477,483-485,560,833-837
 switchport trunk allowed vlan 205,207,477,483-485,560-562,833-837
interface TwentyFiveGigE1/0/34
 no switchport trunk allowed vlan 205,207,465,477,483-485,560,833-837
 switchport trunk allowed vlan 205,207,477,483-485,560-562,833-837
interface TwentyFiveGigE2/0/33
 no switchport trunk allowed vlan 205,207,465,477,483-485,560,833-837
 switchport trunk allowed vlan 205,207,477,483-485,560-562,833-837
interface TwentyFiveGigE2/0/34
 no switchport trunk allowed vlan 205,207,465,477,483-485,560,833-837
 switchport trunk allowed vlan 205,207,477,483-485,560-562,833-837
interface Vlan560
 no description WIRED-CAPTIVE-MGMT
 description WIRED-CAPTIVE-TEST-MGMT
$
```

VXLAN-EVPN anyone?

```
l2vpn evpn
 logging peer state
 replication-type ingress
 router-id Loopback1
!
l2vpn evpn instance 42 vlan-based
 encapsulation vxlan
!
vlan configuration 42
 member evpn-instance 42 vni 120042
!
interface nve1
 no ip address
 source-interface Loopback1
 host-reachability protocol bgp
 member vni 120042 ingress-replication
!
```

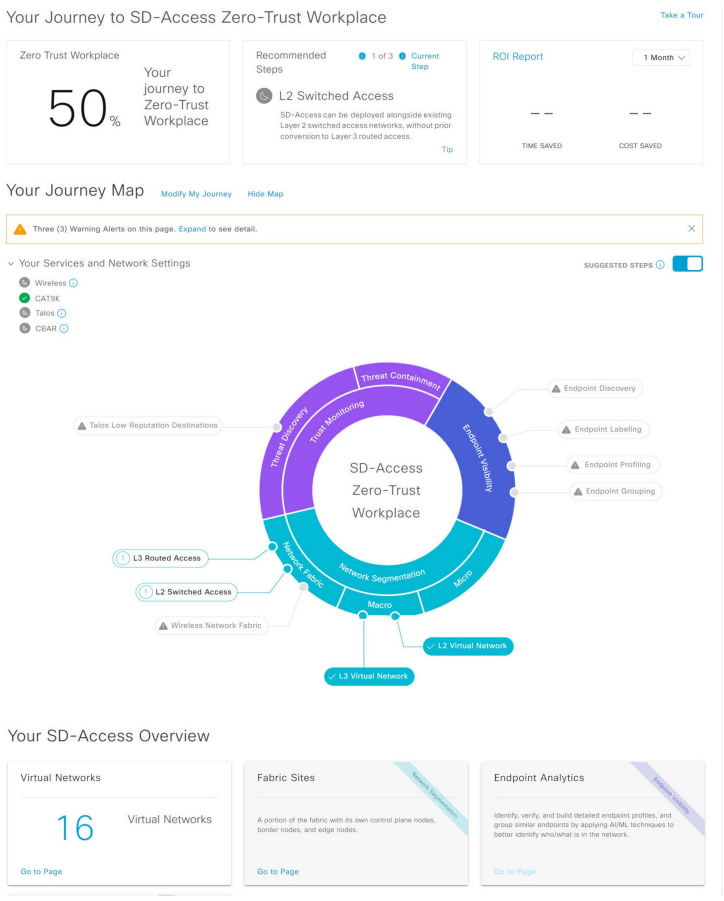
```
router bgp 65001
 bgp router-id 192.0.2.1
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 192.0.2.2 remote-as 65101
 neighbor 192.0.2.2 update-source Loopback1
 neighbor 192.0.2.3 remote-as 65101
 neighbor 192.0.2.3 update-source Loopback1
 !
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn evpn
  neighbor 192.0.2.2 activate
  neighbor 192.0.2.2 send-community both
  neighbor 192.0.2.3 activate
  neighbor 192.0.2.3 send-community both
 exit-address-family
```

VXLAN-EVPN anyone?

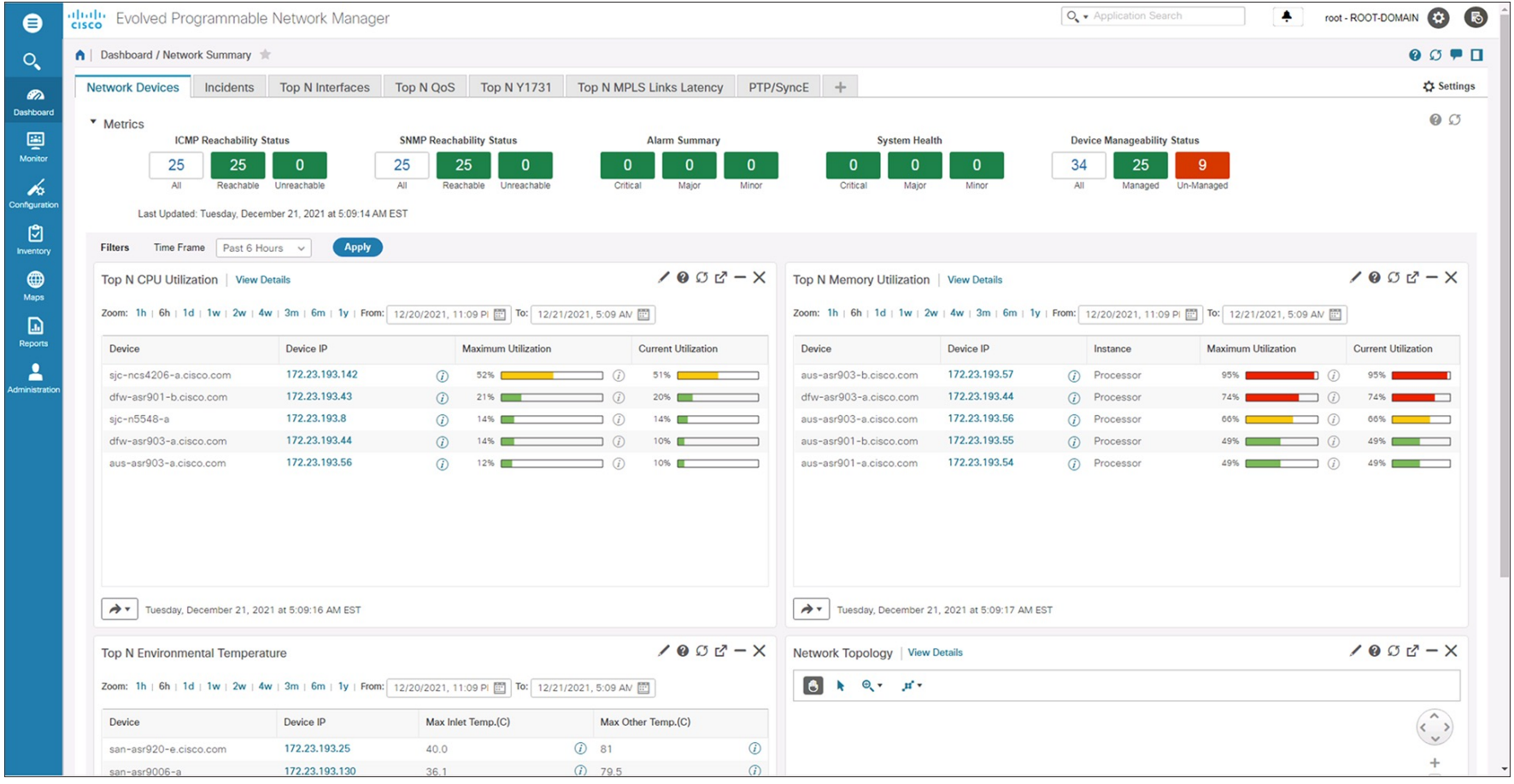
```
l2vpn evpn
 logging peer state
 replication-type ingress
 router-id Loopback1
!
l2vpn evpn instance {{ vlan }} vlan-based
 encapsulation vxlan
!
vlan configuration {{ vlan }}
 member evpn-instance {{ vlan }} vni {{ vni }}
!
interface nve1
 no ip address
 source-interface Loopback1
 host-reachability protocol bgp
 member vni {{ vni }} ingress-replication
!
```

```
router bgp {{ bgp_as }}
 bgp router-id {{ router_ip }}
 bgp log-neighbor-changes
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor {{ nei1 }} remote-as {{ bgp_as }}
 neighbor {{ nei1 }} update-source Loopback1
 neighbor {{ nei2 }} remote-as {{ bgp_as }}
 neighbor {{ nei2 }} update-source Loopback1
 !
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn evpn
  neighbor {{ nei1 }} activate
  neighbor {{ nei1 }} send-community both
  neighbor {{ nei2 }} activate
  neighbor {{ nei2 }} send-community both
 exit-address-family
```

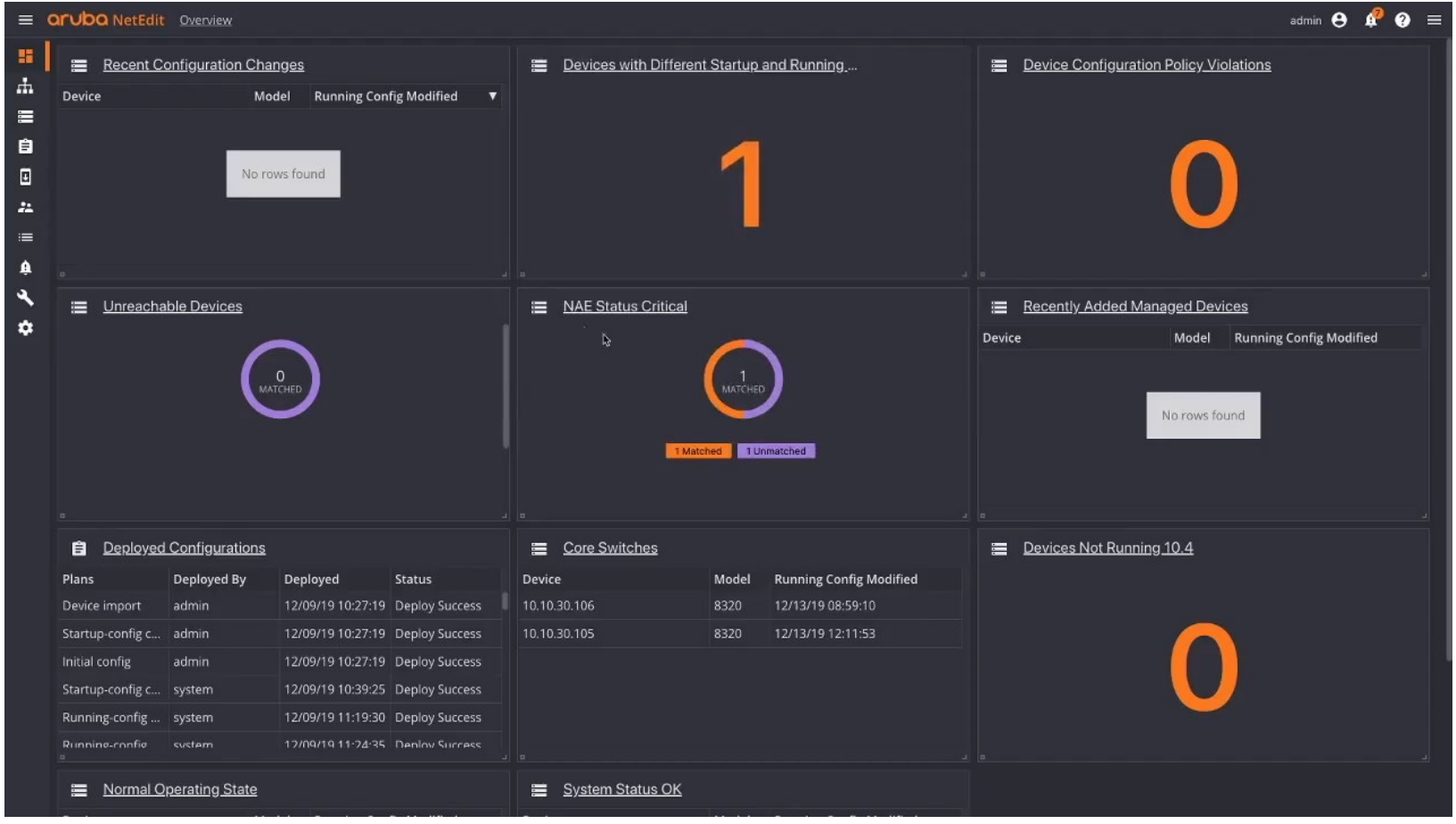
Catalyst Center



DCNM


Evolved Programmable Network Manager
Application Search
root - ROOT-DOMAIN
Dashboard / Network Summary
Network Devices
Incidents
Top N Interfaces
Top N QoS
Top N Y1731
Top N MPLS Links Latency
PTP/SyncE
Settings
Dashboard
Monitor
Configuration
Inventory
Maps
Reports
Administration
Metrics
ICMP Reachability Status
25 All
25 Reachable
0 Unreachable
SNMP Reachability Status
25 All
25 Reachable
0 Unreachable
Alarm Summary
0 Critical
0 Major
0 Minor
System Health
0 Critical
0 Major
0 Minor
Device Manageability Status
34 All
25 Managed
9 Un-Managed
Last Updated: Tuesday, December 21, 2021 at 5:09:14 AM EST
Filters
Time Frame
Past 6 Hours
Apply
Top N CPU Utilization
View Details
Zoom: 1h | 6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | From: 12/20/2021, 11:09 PM | To: 12/21/2021, 5:09 AM
Device
Device IP
Maximum Utilization
Current Utilization
sjc-ncs4206-a.cisco.com 172.23.193.142 52% 51%
dfw-asr901-b.cisco.com 172.23.193.43 21% 20%
sjc-n5548-a 172.23.193.8 14% 14%
dfw-asr903-a.cisco.com 172.23.193.44 14% 10%
aus-asr903-a.cisco.com 172.23.193.56 12% 10%
Tuesday, December 21, 2021 at 5:09:16 AM EST
Top N Memory Utilization
View Details
Zoom: 1h | 6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | From: 12/20/2021, 11:09 PM | To: 12/21/2021, 5:09 AM
Device
Device IP
Instance
Maximum Utilization
Current Utilization
aus-asr903-b.cisco.com 172.23.193.57 Processor 95% 95%
dfw-asr903-a.cisco.com 172.23.193.44 Processor 74% 74%
aus-asr903-a.cisco.com 172.23.193.56 Processor 66% 66%
aus-asr901-b.cisco.com 172.23.193.55 Processor 49% 49%
aus-asr901-a.cisco.com 172.23.193.54 Processor 49% 49%
Tuesday, December 21, 2021 at 5:09:17 AM EST
Top N Environmental Temperature
Zoom: 1h | 6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | From: 12/20/2021, 11:09 PM | To: 12/21/2021, 5:09 AM
Device
Device IP
Max Inlet Temp.(C)
Max Other Temp.(C)
san-asr920-e.cisco.com 172.23.193.25 40.0 81
san-asr9006-a 172.23.193.130 36.1 79.5
Network Topology
View Details

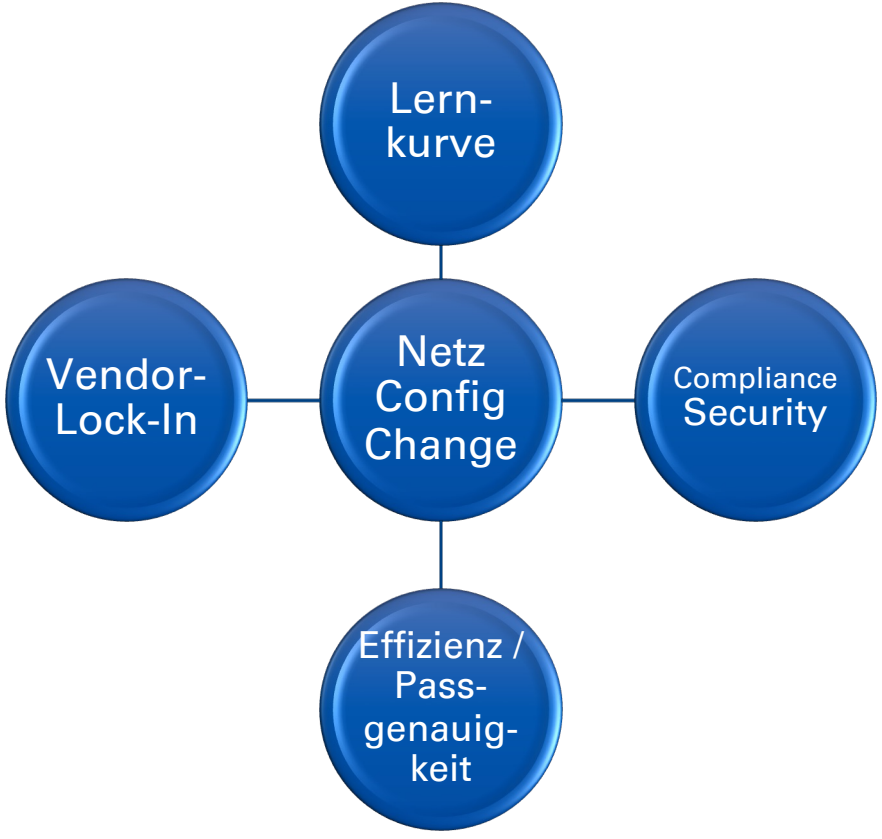
Aruba NetEdit



One Size Fits all?

- Nein, immer Kompromiss!
- Standard-Administrationspraxis muss berücksichtigt werden
- Abhängig von Verfügbarkeit externer Daten
- Dezentrale Zuständigkeiten vs. zentrale Prozesse

Lösungen anyone?



Zusammenfassung / Ausblick

- Konfigurationsänderungen sind Aufwand!
- Unwissenheit/Unklarheit verbessert nichts!
- Aufwände können minimiert werden, wenn Wildwuchs unter Kontrolle
- Änderungen kontrollierter Umgebungen sind einfacher!
- Beschreibung bekannter Zustände -> Compliance, Security, Servicability
- Proaktives Monitoring bzw. Unit-Test möglich!
- Standardisierung kommt auch nicht umsonst!

Universität Stuttgart
Technische Informations- und
Kommunikationsdienste (TIK)

Vielen Dank!

Kilian Krause

E-Mail kilian.krause@tik.uni-stuttgart.de
Telefon +49 (0) 711 685-64512
www.tik.uni-stuttgart.de

Universität Stuttgart
Technische Informations- und Kommunikationsdienste (TIK)
Allmandring 30A
70550 Stuttgart