HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Software-Defined Netzwerk im Campus Bereich

Studienarbeit

Abteilung Informatik
Hochschule für Technik Rapperswil

Frühjahrssemester 2018

Autoren:	Sandro Kaspar, Philipp Albrecht, Jessica Kalberer
Betreuer:	Laurent Metzger
Projektpartner:	Führungsunterstützungsbasis (FUB) der Schweizer Armee
Experte:	Laurent Billas
Gegenleser:	Beat Stettler

Inhaltsverzeichnis

1 Aufgabenstellung

Dies ist die initiale Aufgabenstellung, welche zu Beginn der Studienarbeit vorlag.

Software-Defined Netzwerk im Campus Bereich

Studiengang:	Informatik (I)
Semester:	FS 2018 (19.02.2018-16.09.2018)
Durchführung:	Bachelorarbeit, Studienarbeit
Fachrichtung:	Network Design and Security
Institut:	INS: Institut für vernetzte Systeme
Gruppengrösse:	2-3 Studierende
Status:	zugewiesen
Verantwortlicher:	Metzger, Laurent
Betreuer:	Metzger, Laurent
Gegenleser:	Beat Stettler
Experte:	Laurent Billas
Industriepartner:	Führungsunterstützungsbasis (FUB) der Schweizer Armee
Ausschreibung:	Das Netzwerk einer völlig neuen Ära. Da Software-Defined Access Neuland im Campus Bereich ist, wollen wir die SD-Access Lösung von Hersteller Cisco ausarbeiten. Aufgaben: - Installation von DNA-Center und Integration vom bestehenden Campus Labor-Netzwerk. - Definierung von Benutzer- und Geräteprofile, um basierend auf Geschäftsanforderungen die Zugriffsrechte und Netzwerksegmentierung zu verwalten und so das Netzwerk sicher zu halten. - Verwendung von Erkenntnisse von DNA Analytics and Assurance für eine proaktive Überwachung, Fehlerbehebung und Optimierung des Netzwerks. - Integration vom bestehenden IP Address Management Tool im DNA Center. - Durch APIs, Erstellung von Wochentlichen Reports über Campus Netzwerk-Status in einem E-Mail und in einem Slack Message.
Voraussetzungen:	Routing & Switching, Python, REST APIs, JSON/XML, git/GitHub, Linux Skills

Abbildung 1.1: Aufgabenstellung aus AVT [26]

Die Zielsetzungen der initialen Aufgabenstellung wurden nach Absprache mit dem Betreuer anhand der Erkentnisse im Verlauf der Studienarbeit angepasst. Die aktualisierte Aufgabenstellung mit den dazugehörigen Zielsetzungen sind im Abstract ersichtlich (Siehe: 2.1 Aufgabenstellung).

2 Abstract

2.1 Aufgabenstellung

Ziel dieser Studienarbeit war die Evaluation des Cisco Digital Network Architecture (DNA) Center, der Software-Defined Network (SDN) Lösung von Cisco, für die Führungsunterstützungsbasis (FUB) der Schweizer Armee. Das DNA Center ist eine Softwarelösung zur Netzwerkautomatisierung. Diese vereinfacht und automatisiert das Deployment und Management einer Campus Netzwerk Umgebung mit Hilfe von Technologien wie Virtual Extensible LAN (VXLAN) und Locator/ID Separation Protocol (LISP). Dank der zentralen Verwaltung der Infrastruktur wird die Qualität, sowie die Sicherheit der Netzwerkumgebung, stark erhöht.
Für die FUB sollte die Lösung unter anderem folgende Anforderungen abdecken:

- Definition von Benutzerprofilen
- Reporting der Netzwerkaktivitäten
- Benutzermobilität
- Degradation der Infrastruktur
- Backup und Restore
- Anbindung an externe Systeme wie die Identity Services Engine (ISE) und Infoblox

2.2 Vorgehen

Der erste Teil der Arbeit beinhaltete die Installation und Konfiguration des DNA Centers, die Anbindung an externe Systeme und das Deployment einer Fabric in einer Testumgebung. Die erste Inbetriebnahme hat einigen Aufwand gekostet, konnte aber schlussendlich erfolgreich abgeschlossen werden. Viele Schritte auf diesem Weg waren nur teilweise automatisiert und im aktuellen Release ist noch manueller Aufwand nötig. Auf diesem Weg konnten aber viele neue Erkenntnisse gewonnen werden, die ohne manuellen Aufwand nicht möglich gewesen wären. Als Beispiel kann hier die LAN Automation aufgeführt werden. Mit Hilfe dieser sollten sich Netzwerkgeräte automatisiert mittels Plug and Play (PnP) in Betrieb nehmen und konfigurieren lassen. Dieser Prozess erwies sich als komplex, war aber mehrheitlich dokumentiert.
In einem zweiten Schritt ging es darum, Benutzer- und Geräteprofile zu definieren, sowie deren Zugriffe zentral zu verwalten. Des Weiteren sollte mit DNA Assurance eine proaktive Überwachung, Fehlerbehebung und Optimierung des Netzwerkes sichergestellt werden. Mit diesen Informationen sollen wöchentliche Reports über den Status des Netzwerks per E-Mail versendet werden.

2.3 Fazit

Abschliessend kann gesagt werden, dass für die Installation und Konfiguration des DNA Centers genug Zeit eingerechnet werden muss. Zudem sollte im optimalen Fall ein Green Field vorliegen, da zur Zeit kein bestehendes Netzwerk ohne Unterbrüche migriert werden kann. Bei der Installation sollten die empfohlenen Softwareversionen vom ISE und auch der Switches genauestens eingehalten werden, da sonst die volle Funktionalität des DNA Centers nicht gewährleistet werden kann. Das DNA Center hat grosses Potenzial. Es vereinfacht die Umsetzung und Inbetriebnahme des Campus Netzwerkes enorm und macht es sicherer. Insbesondere duch die API kann vieles automatisiert werden und die Anbindung an bestehende Systeme gestaltet sich einfach.

3 Management Summary

3.1 Ausgangslage

Diese Arbeit beschäftigt sich mit Software Defined Networking (SDN) im Campus LAN für die Führungsunterstützungsbasis (FUB) der Schweizer Armee. Die Lösung soll den Netzwerkzugriff der Mitarbeiter der FUB sicherstellen und die Zugriffsrechte der einzelnen Mitarbeiter oder Teams regeln können. Zentrale Bestandteile der Arbeit sind dabei eine Produktevaluation und ausführliches Testing. Des Weiteren müssen Reportingfunktionen und eine proaktive Überwachung erstellt werden, um allfällige Fehler schnellstmöglich zu erkennen, das Netzwerk stets zu optimieren und dessen Funktion jederzeit sicherzustellen. Zusätzlich wird ein bestehendes IP Adress Management (IPAM) Tool in die Lösung integriert.
Da die Anforderungen an Campus Netzwerke aus verschiedenen Gründen, wie zum Beispiel neuen modernen Arbeitsmodellen oder neuen Sicherheitsanforderungen ständig steigen, ist es äusserst schwierig und aufwändig, diese Anforderungen mit traditionellen Methoden zu erfüllen.
Um dies zu erreichen, wird in dieser Arbeit ein SDN erstellt, dass diesen neuen Anforderungen gerecht werden soll. Vorteile zeigen sich insbesondere dadurch, dass eine derartige Lösung flexibler ist, also einfacher und schneller an neue Gegebenheiten angepasst werden kann und durch Schnittstellen einfach an bestehende Systeme anzubinden ist. Durch das zentrale Management und Monitoring der Komponenten sinkt zudem das Risiko für Fehler massiv und viele Aufgaben lassen sich einfach und schnell automatisieren. Schlussendlich kann durch diese Vorteile sehr viel Aufwand und damit Kosten eingespart werden.
Ziel ist es, die Vorteile dieser Lösung gegenüber einer traditionellen Netzwerkinfrastruktur aufzuzeigen, allfällige Risiken und mögliche Probleme früh zu erkennen und Lösungen für diese zu finden.

3.2 Vorgehen und Technologien

Die Lösung wird mit dem Produkt Software-Defined Access (SDA) von Cisco erstellt, welche aus mehreren Komponenten besteht. Dies ist zum einem das Digital Network Architecture (DNA) Center, welches die grundsätzliche Funktion des Netzwerks sicherstellt, sowie eine Identity Services Engine (ISE), welche die Benutzeridentitäten und Profile verwaltet. Zusätzlich muss das bestehende IPAM in die Lösung integriert und Reporting Funktionen mittels Slack und E-Mail implementiert werden. Diese Zusatzfunktionalitäten werden in Python implementiert und nutzen die in Ciscos SDA enthaltenen Application Programming Interfaces (APIs).

3.3 Ergebnisse

Am Ende dieser Arbeit wird ein funktionierender Prototyp eines SDN im Access Bereich zur Verfügung stehen, der alle Anforderungen des Industriepartners abdeckt. Der Prototyp besteht aus den Cisco Komponenten, sowie Eigenentwicklungen, die zusätzliche Features implementieren. Zudem steht eine Dokumentation des Systems zur Verfügung, die den Installationsprozess und die Handhabung des Systems erklärt. Des Weiteren zeigt die Dokumentation Vorteile, aber auch Risiken und mögliche Probleme im Vergleich zu einer traditionellen Netzwerklösung auf.

3.4 Ausblick

Die Resultate dieser Arbeit können dazu dienen, SDA in einer produktiven Umgebung in Betrieb zu nehmen. Zudem kann der Prototyp um zusätzliche Funktionen erweitert, an zusätzliche bestehende oder neue Systeme angebunden oder mit alternativen Lösungen verglichen werden.

4 Problembeschreibung

Wer den heutigen Anforderungen der Campus Netzwerke in Bezug auf Sicherheit, Wartbarkeit und Skalierbarkeit gerecht werden möchte, steht mit der isolierten Konfiguration einzelner Komponenten schnell vor verschiedenen Problemen. In erster Linie ist es extrem aufwändig, alle Konfigurationen manuell zu erstellen. Selbst das Hinzufügen von einfachen Richtlinien oder neuen Firmenabteilungen kann zu gewaltigem Aufwand führen. Des Weiteren kann die Übersicht schnell verloren werden und eine umfangreiche Dokumentation zu erstellen ist unumgänglich. Häufig kommen selbstgeschriebene Scripts, zum Beispiel mithilfe von NAPALM [20] zur automatisierten Konfiguration zum Einsatz. Für das Monitoring des Netzwerkes sind zusätzlich Tools wie icinga2 [21] oder ähnliches nötig.

Typische Herausforderungen bei den klassischen Campus Netzwerken:

- Zu wenig VLANs
- Mobilität von Endgeräten
- Mobilität von Benutzern
- Durchsetzen von Sicherheitsregeln mithilfe von Firewalls
- Direkte Abhängigkeit von Berechtigungen und IP Subnetzen
- Mehrere unabhängige Tools mit Informationsredundanz
- Komplexe Fehlersuche über verschiedene Komponenten/Geräte hinweg

Genau hier setzt das Cisco DNA Center an. Es fasst alle diese Tools unter einem Dach zusammen und bietet eine übergreifende Plattform.

5 Technologien

5.1 Software-Defined Access (SDA)

Cisco bietet mit SDA eine automatisierte End-to-End-Segmentierung um den Benutzer-, Geräte- und Anwendungsverkehr zu trennen, ohne das Netzwerk neu zu gestalten. Durch diesen automatisierten Benutzerzugriff ermöglicht SDA Einrichtungen innert kürzester Zeit. Durch diese enorme Vereinfachung wird eine zusätzliche Sicherheit und Skalierung des Betriebs gewonnen. Ebenso wird die Transparenz deutlich erhöht und die schnelle Bereitstellung neuer Dienste gewährleistet. Durch die Automatisierung von täglichen Aufgaben wie Konfiguration, Bereitstellung und Troubleshooting reduziert SDA die Zeit für Netzwerkanpassungen, verbessert die Problemlösungszeit und reduziert die Auswirkungen von Sicherheitsverletzungen.

So können Organisationen sicherstellen, dass für jeden Benutzer oder jedes Gerät mit jeder Anwendung innerhalb des Netzwerkes die richtigen Richtlinien angewendet werden. Dies wird mit einer einzigen Netzwerkstruktur über LAN und WLAN erreicht, wodurch ein konsistente Benutzererfahrung überall ohne Kompromisse bei der Sicherheit möglich ist.

SDA wird aus mehreren Komponenten zusammengesetzt. Dazu gehört das DNA Center, welches die grundsätzliche Funktion des Netzwerks sicherstellt, sowie eine ISE, welches die Benutzeridentitäten und Profile verwaltet. [5]

5.1.1 Campus Fabric

Um eine konsistente Benutzererfahrung zu erreichen, ist eine Switching-Infrastruktur nötig, mit der sich der Zugang zu bestimmten IP-Subnetzen ortsunabhängig realisieren lässt. [6]

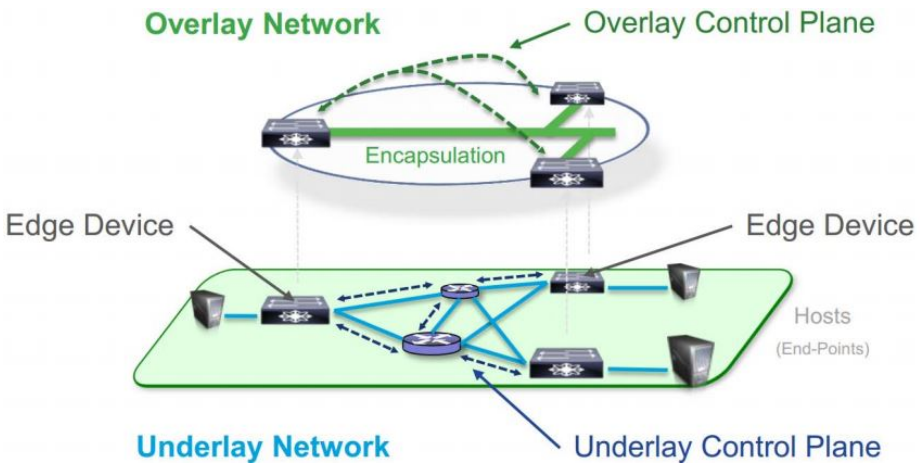


Abbildung 5.1: Aufteilung des Campus Fabric in Underlay und Overlay Netzwerk [22]

Die SDA Architektur wird durch die für den Campus implementierte Fabric Technologie unterstützt, welche die Verwendung virtueller Netzwerke (Overlay Network) in einem physischen Netzwerk (Underlay Network) ermöglicht, um alternative Topologien für die Verbindung von Geräten zu erstellen. Overlay Netzwerke werden in Data Center häufig

verwendet, um die Mobilität von virtuellen Maschinen über Layer 2 (L2) und Layer 3 (L3) bereitzustellen. Dies wird beispielsweise mit Application Centric Infrastructure (ACI), VXLAN und Fabric Path realisiert. Overlay Netzwerke werden auch in Wide Area Netzwerken (WAN) verwendet, um sicheres Tunneling von Remote-Standorten aus zu ermöglichen. Beispiele dafür sind die Protokolle Multiprotocol Label Switching (MPLS), Dynamic Multipoint VPN (DMVPN) und Generic Routing Encapsulation (GRE). [4]

Overlay Network Die Fabric bildet ein Overlay Netz. Das Overlay Netz bildet eine virtuelle Topologie, um Geräte miteinander zu verbinden, welches auf einer beliebigen physischen Underlay Topologie aufgebaut ist. Das Overlay Netzwerk verwendet oft alternative Weiterleitungsattribute, um zusätzliche Dienste bereitzustellen, die nicht vom Underlay Netzwerk bereitgestellt werden. Der Data Plane Traffic und die Control Plane Signalisierung sind in jedem virtualisierten Netzwerk enthalten, wobei zusätzlich zu der Isolation von dem Underlay Netzwerk eine Isolation zwischen den Netzwerken aufrechterhalten wird. Die SDA Fabric implementiert die Virtualisierung, indem sie den Benutzerdatenverkehr über IP-Pakete einkapselt, die an den Grenzen des Fabrics bereitgestellt und abgeschlossen werden. Overlay Netzwerke können über alle oder eine Teilmenge der Underlay Netzwerkgeräte hinweg ausgeführt werden. Mehrere Overlay Netzwerke können aber auch über das gleiche Underlay Netzwerk laufen, um Multi-Tenancy durch Virtualisierung zu unterstützen. Die Netzwerkvirtualisierung, welche sich ausserhalb der Fabric erstreckt, wird mithilfe herkömmlicher Virtualisierungstechnologien wie Virtual Routing and Forwarding (VRF)-Lite und MPLS VPN beibehalten. Der IPv4 Multicast wird gekapselt und an interessierte Fabric Edge Switches gesendet, welche den Multicast wiederum entkapseln und an die Empfänger weiterleiten. Ist der Empfänger ein drahtloser Client, so wird der Multicast (genau wie ein Unicast) durch den Fabric Edge in Richtung des Access Point (AP) mit dem Multicast-Empfänger gekapselt. Die Multicast Quelle kann entweder innerhalb oder ausserhalb eines Overlay Netzwerkes vorhanden sein. [4]

Underlay Network Das Underlay Netzwerk wird durch die physischen Switches und Router definiert, die Teil des SDA Netzwerks sind. Jegliche Geräte, die dem Underlay Netzwerk angehören, müssen über ein Routing Protokoll eine IP Konnektivität herstellen. Obwohl auf dem Underlay beliebige Topologie- und Routing-Protokolle verwendet werden können, wird von Cisco die Implementierung einer gut überlegten L3 Grundlage bis zum Campus Edge empfohlen, um die hohe Leistung, sowie Skalierbarkeit und Verfügbarkeit des Netzwerkes zu gewährleisten. Um dieses Ziel für die Underlay Deployments zu erreichen, welche nicht manuell erstellt werden, werden bei der DNA Center LAN-Automatisierung neue Netzwerke mit einem Intermediate System to Intermediate System (IS-IS)-Routing Access Design bereitgestellt. Obwohl es viele Alternativen gibt, bietet diese Auswahl betriebliche Vorteile wie zum Beispiel dem Nachbarschaftsaufbau ohne IP-Protokollabhängigkeiten, Peering-Fähigkeit unter Verwendung von Loopback-Adressen und agnostische Behandlung von IPv4-, IPv6- und Nicht-IP-Verkehr. [4]

Fabric Data Plane and Control Plane SDA konfiguriert das Overlay Netzwerk mit einer Fabric Data Plane mithilfe der VXLAN Technologie. VXLAN kapselt und durchtunnelt komplette L2 Frames über das Underlay Netzwerk, wobei jedes Overlay Netzwerk durch eine Virtual Extensible LAN Network Identifier (VNI) identifiziert wird. Der VXLAN Header enthält auch die Security Group Tags (SGTs), die für die Mikrosegmentierung erforderlich sind.

Das Mapping und Auflösen von Endpunkten, die VXLAN-Tunnelendpunkten (VTEPs) zugeordnet sind, erfordert ein Control Plane Protokoll, und SD Access verwendet LISP für diese Aufgabe. LISP bietet den Vorteil, dass das Routing nicht nur auf der IP-Adresse als Endpunktkennung (EID) für ein Gerät basiert, sondern auch eine zusätzliche IP-Adresse als Routing Locator (RLOC) zur Verfügung stellt, um den Netzwerkstandort dieses Geräts darzustellen. Die EID- und RLOC-Kombination bietet alle erforderlichen Informationen für die Weiterleitung von Datenverkehr, selbst wenn ein Endpunkt eine unveränderte IP-Adresse verwendet, wenn er an einem anderen Netzwerkstandort angezeigt wird. Gleichzeitig ermöglicht die Entkopplung der Endpunktidentität von ihrem Standort, dass Adressen in demselben IP-Teilnetzwerk hinter mehreren L3 Gateways (GW) verfügbar sind, gegenüber der Eins-zu-eins-Kopplung von IP-Teilnetzwerk mit Netzwerk GW in herkömmlichen Netzwerken Beispiel für zwei Subnetze, die Teil des Overlay Netzwerks sind. Die Subnetze erstrecken sich über physisch getrennte L3 Geräte. Die RLOC-Schnittstelle ist die einzige routbare Adresse, die zum Herstellen der Verbindung zwischen Endpunkten desselben oder eines anderen Subnetzes erforderlich ist. Weitere detailliertere Informationen zu LISP und VXLAN folgen in den nächsten Kapiteln. [4]

In der nachfolgenden Abbildung ist der Aufbau eines Campus Fabric mit allen Komponenten etwas detaillierter aufgezeigt.

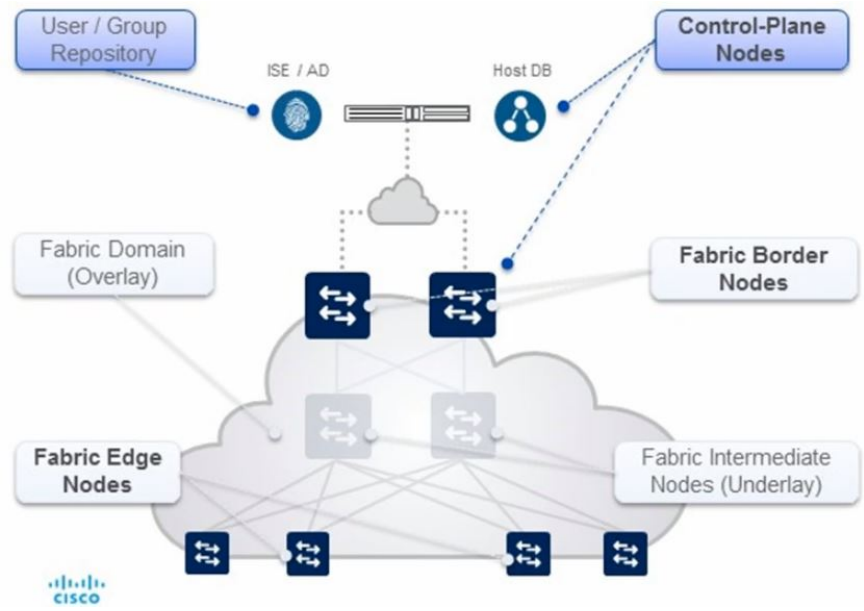


Abbildung 5.2: Fabric Rollen und Terminologie [23]

Dieses Campus Fabric besteht aus folgenden Elementen: [23]

- User/Group Repository: Ein externes ID-Speichergerät (z. B. ISE oder AD) kann verwendet werden, um eine dynamische Zuordnung von Benutzer/Gerät zu Gruppen bereitzustellen
- Control Plane Nodes: Ein Map System, das die Beziehung eines Endpoints zu einem GW (Edge oder Border) verwaltet
- Border Nodes: Das L3 GW Gerät (Core), das externe L3-Netzwerke mit dem Fabric verbindet
- Edge Nodes: Das L3 GW Gerät (Access oder Distribution), welches Endpoints mit Fabric verbindet

- Intermediate Nodes: Normale L3 (IP) Forwarder im Underlay Netzwerk

Control-Plane Nodes Der SDA Fabric Control Plane basiert auf der LISP Map Server (MS) und LISP Map Resolver (MR), welche auf demselben Node kombiniert sind. Die Funktion des Control Planes wird am Border Node oder Dedicated Node instanziiert. Der Control Plane Node ermöglicht folgende Funktionen: [4]

- Host Tracking Database (HTDB): Die HTDB ist ein zentrales Repository von EID zu Fabric Edge Nodes Verbindungen.
- Map Server (MS): Der LISP MS wird verwendet, um die HTDB mit Registrierungsnachrichten von Fabric Edge Geräten zu füllen.
- Map Resolver (MR): Der LISP MR wird verwendet, um auf Map Abfragen von Fabric Edge Geräten zu reagieren, die RLOC Mapping Informationen für Ziel EIDs anfordern.

Fabric Border Nodes Die Fabric Border Nodes dienen als GW zwischen der SDA Fabric Domäne und dem Netzwerk ausserhalb der Fabric. Der Fabric Border Node ist für die Netzwerkvirtualisierung und die SGT Propagierung vom Fabric zum Rest des Netzwerks verantwortlich. Die Fabric Border Nodes können entweder als GW für bestimmte Netzwerkadressen, zum Beispiel ein Netzwerk für gemeinsam genutzte Dienste, oder in einer Standard Border Rolle, die für das Internet oder einen gemeinsamen Austrittspunkt aus einer Fabric nützlich ist. Border Nodes implementieren die folgenden Funktionen: [4]

- Advertisement von EID Subnetzen: SDA konfiguriert das Border Gateway Protocol (BGP) als bevorzugtes Routing Protokoll zum Anbieten der EID Präfixe ausserhalb der Fabric und der für EID Subnetze von ausserhalb der Fabric bestimmte Verkehr durchläuft die Border Nodes. Diese EID Präfixe werden nur in den Routingtabellen am Border angezeigt. Im gesamten Fabric werden die EID Informationen über den Fabric Control Plane abgerufen.
- Fabric Domain Exit Point: Der Standard Fabric Border ist der GW für den letzten Exit Point für die Fabric Edge Nodes. Dies wird mithilfe der LISP Proxy Tunnel Funktionalität implementiert.
- Mapping von LISP Instanzen zu VRF: Der Fabric Border kann die Netzwerkvirtualisierung von innerhalb des Fabrics nach ausserhalb des Fabrics erweitern, indem externe VRF Instanzen verwendet werden, um die Virtualisierung beizubehalten.
- Policy Mapping: Der Fabric Border Node bildet auch SGT Informationen aus dem Fabric ab, die beim Verlassen des Fabric entsprechend gepflegt werden. Tags aus dem VXLAN Header werden Cisco Meta Data (CMD) zugeordnet, wenn Inline-Tagging-Funktionen verwendet werden, oder alternativ werden die Tags über das SGT Austauschprotokoll (SXP) transportiert, sodass eine nahtlose Integration in die Cisco TrustSec Lösung möglich ist.

Fabric Edge Nodes Die SDA Fabric Edge Nodes entsprechen einem Access Layer Switch in einem herkömmlichen Campus Design. Die Edge Nodes implementieren ein L3 Access Design mit den folgenden Fabric Funtkionen: [4]

- Endpunktregistrierung: Nachdem ein Endpunkt von der Fabric Edge erkannt wurde, wird er einer lokalen HTDB hinzugefügt. Das Edge Gerät gibt auch eine LISP Map Register Nachricht aus, um den Control Plane Node über den erkannten Endpunkt zu informieren, damit dieser die Informationen in die HTDB einfügen kann.

- Zuordnung von Benutzer zu virtuellem Netzwerk: Endpunkte werden in virtuellen Netzwerken platziert, indem der Endpunkt einem VLAN zugewiesen wird, das einer LISP Instanz zugeordnet ist. Die Zuordnung von Endpunkten zu VLANs kann statisch oder dynamisch mit 802.1X erfolgen. Eine SGT wird ebenfalls zugewiesen, und eine SGT kann verwendet werden, um Segmentierung und Richtliniendurchsetzung an der Fabric Edge bereitzustellen.
- Anycast L3 GW: Ein gemeinsamer GW (IP- und MAC-Adressen) kann an jedem Knoten verwendet werden, der sich ein gemeinsames EID Subnetz teilt, um eine optimale Weiterleitung und Mobilität zwischen verschiedenen RLOCs zu gewährleisten.
- LISP Forwarding und VXLAN Encapsulation/De-Encapsulation: Anstelle einer typischen routingbasierten Entscheidung fragen die Fabric Edge Nodes den MS an, um den der Ziel IP zugeordneten RLOC zu ermitteln und den Verkehr mit VXLAN Headern zu kapseln. Schlägt die Abfrage fehl, so wird der Traffic an einen Default Fabric Border gesendet, auf dem die globale Routing Tabelle für das Weiterleiten verwendet wird. Die von MS empfangene Antwort wird im LISP Map Cache gespeichert.

Fabric Intermediate Nodes (Underlay) Die Fabric Intermediate Nodes sind Teil des L3 Netzwerkes, das für Verbindungen zwischen den Edge Nodes zu den Border Nodes verwendet wird. Falls ein drei Tier Campus Design mit einem Core, Distribution und Access Layer verwendet wird, sind die Intermediate Nodes äquivalent zu Distribution Switches. Intermediate Nodes routen nur den IP Verkehr innerhalb der Fabric. [4]

5.1.2 Architektur

Cisco SDA kann grob in fünf Layer aufgeteilt werden.

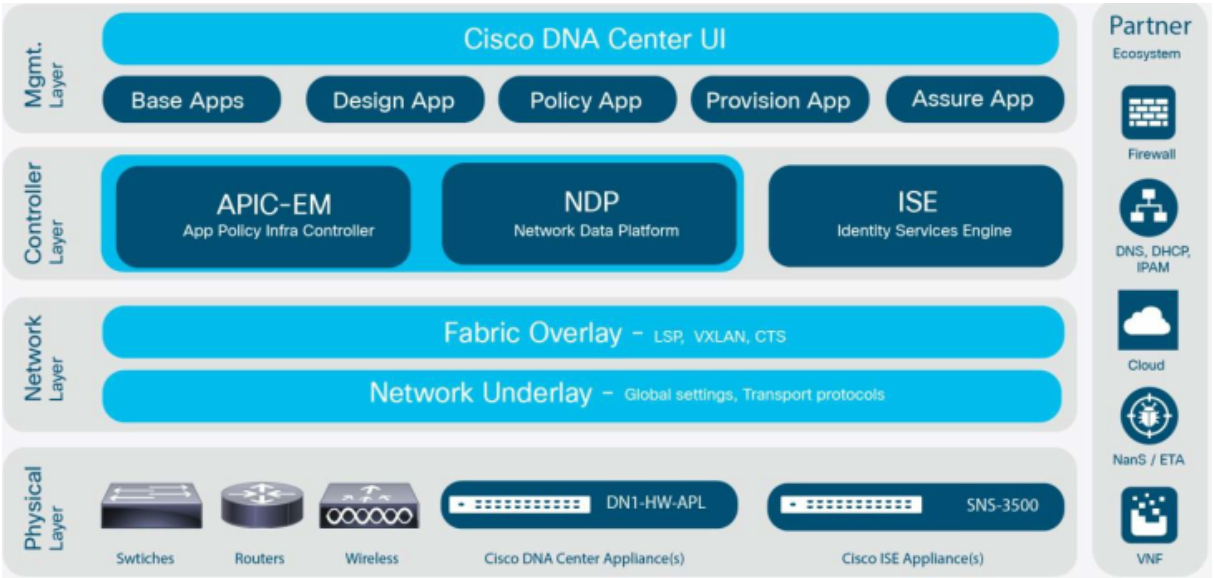


Abbildung 5.3: SDA Architektur [3]

5.2 Cisco Digital Network Architecture Center (Cisco DNA-Center)

Im Zentrum der Automatisierung der SDA Lösung steht das Cisco DNA Center. DNA Center ist ein Controller für die Planung und Vorbereitung, Installation und Integration eines SDN. SDA ist eines der vielen Softwarepakete, die auf dem DNA Center laufen und ist die Grundlage des Cisco DNA. Es ermöglicht den Netzwerkzugriff in Minuten für jeden Benutzer oder jedes Gerät für jede Anwendung, ohne Kompromisse. Bei SDA folgen die festgelegten Richtlinien automatisch dem Benutzer über alle Netzwerkdomänen hinweg. DNA Center ist das zentrale Überwachungs-Dashboard für Netzwerke, mit dem alle Cisco DNA-Produkte und -Lösungen verwaltet werden können.
Das DNA Center gibt die Möglichkeit unter einem Grafischen Nutzer Interface direkt mit Application Policy Infrastructure Controller (APIC)-EM 2.x Applikationen mit der ISE und mit Network Data Plattform (NDP) der Assurance und Analytics Plattform zu sprechen. Alle Parameter die angezeigt oder konfiguriert werden müssen, können im DNA Center ausgeführt werden und es muss nicht zwischen den einzelnen Modulen und Oberflächen hin und her gesprungen werden.

Abbildung 5.4: DNA Solution [24]

Der APIC-EM 2.x automatisiert dann die notwendigen Konfigurationen und spricht mit dem Netzwerk. Auch die Integration von IPAM Lösungen, wie zum Beispiel Infoblox, werden nur über die DNA Center Oberfläche konfiguriert. Dies geschieht über verschiedene API-basierte Datenaustauschmechanismen, sowie einen automatisierten Zertifikataustausch für Partnersysteme (zum Beispiel ISE). [3]

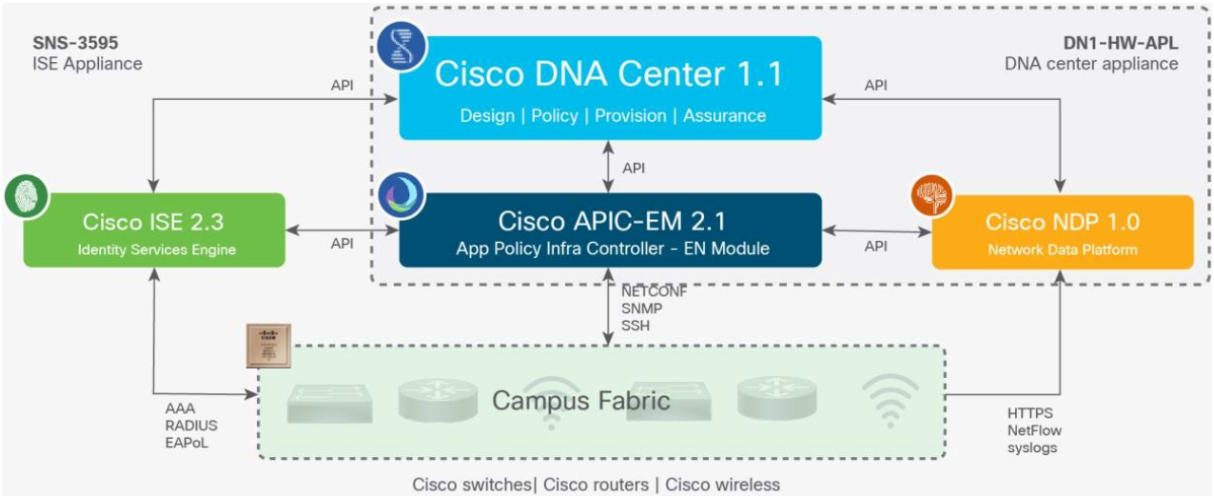


Abbildung 5.5: SDA Architektur [3]

Das DNA Center verwaltet zentral folgende vier Hauptbereiche: [4]

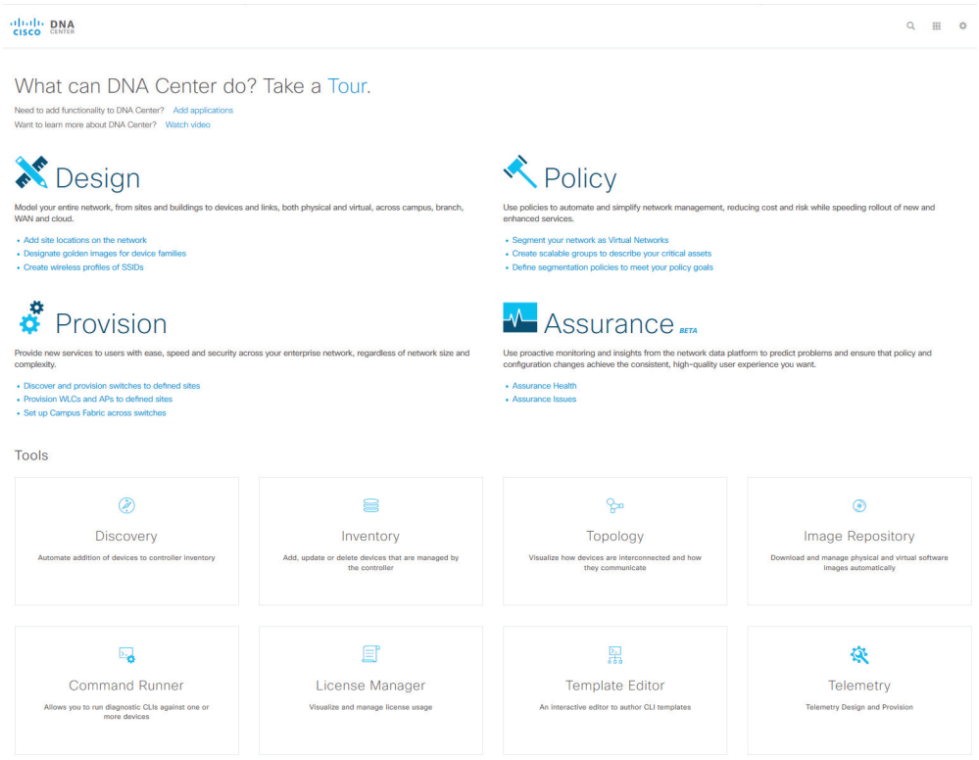


Abbildung 5.6: DNA Dashboard

Design Konfiguriert globale Geräteeinstellungen, Netzwerkstandortprofile für die physische Geräteinventur, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), IP-Adressierung, Software-Image-Verwaltung, PnP und Benutzerzugriff.

Policy Definiert die Geschäftsabsicht für die Bereitstellung im Netzwerk, einschliesslich der Erstellung virtueller Netzwerke, der Zuweisung von Endpunkten zu virtuellen Netzwerken und der Definition von Richtlinienverträgen für Gruppen.

Provision Stellt Geräte für das Management bereit und erstellt Fabric Domänen, Control Plane Nodes, Border Nodes, Edge Nodes, Fabric Wireless und externe Konnektivität.

Assurance Aktiviert das Health-Score-Dashboard, Client/Gerät-360 Grad-Ansichten, Knoten-, Client- und Pfad-Traces. DNA Center unterstützt die Integration mithilfe von APIs. Zum Beispiel ist die Integration von IP-Adressen von Infoblox und die Integration von Policy Enforcement mit ISE über das DNA Center verfügbar. Ein umfassendes Set von Northbound-REST-APIs ermöglicht Automatisierung, Integration und Innovation.

5.3 Identity Service Engine (ISE)

Cisco ISE ist ein wesentlicher Bestandteil für die Richtlinienimplementierung von SDA. Mit der ISE können Benutzer und Geräte, die mit dem Unternehmensnetzwerk verbunden sind, angezeigt und gesteuert werden. Dies alles von einer zentralen Stelle aus. Die ISE ermöglicht es einem Netzwerkadministrator, Zugriffsrichtlinien für kabelgebundene und drahtlose Endpunkte basierend auf Informationen zentral zu steuern, die über Remote Authentication Dial-In User Service (RADIUS)-Nachrichten gesammelt werden, die zwischen dem Gerät und dem ISE Knoten übertragen werden. Dies wird auch als Profiling bezeichnet. Die Profiling-Datenbank wird regelmäßig aktualisiert, um mit den neuesten und besten Geräten Schritt zu halten, so dass keine Lücken in der Gerätesichtbarkeit bestehen.

Im Wesentlichen hängt ISE eine Identität an ein Gerät an, basierend auf Benutzer-, Funktions- oder anderen Attributen, um Richtliniendurchsetzung und Sicherheitskonformität bereitzustellen, bevor das Gerät autorisiert wird, auf das Netzwerk zuzugreifen. Basierend auf den Ergebnissen einer Vielzahl von Variablen kann ein Endpunkt mit bestimmten Zugriffsregeln auf das Netzwerk zugelassen werden, die auf die Schnittstelle angewendet werden, mit der er verbunden ist. Andernfalls kann er vollständig verweigert oder basierend auf den spezifischen Unternehmensrichtlinien gewährt werden.

DNA Center bietet einen Mechanismus zum Erstellen einer vertrauenswürdigen Kommunikationsverbindung mit Cisco ISE und ermöglicht den beiden Anwendungen, Daten auf sichere Weise miteinander zu teilen. ISE integriert sich in DNA Center mit Hilfe von Cisco Platform Exchange Grid (pxGrid) und REST APIs zum Austausch von Client Informationen und zur Automatisierung von Fabric bezogenen Konfigurationen auf ISE. Sobald die ISE beim DNA Center registriert ist, wird jedes Gerät, das ISE entdeckt, zusammen mit der entsprechenden Konfiguration und anderen Daten an das DNA Center weitergeleitet. Benutzer können beide Anwendungen verwenden, um Geräte zu erkennen und dann sowohl DNA Center als auch ISE Funktionen auf sie anzuwenden, da diese Geräte in beiden Anwendungen verfügbar sind. DNA Center und ISE Geräte werden alle durch ihre Gerätenamen eindeutig identifiziert.

In ähnlicher Weise werden DNA Center Geräte, sobald sie bereitgestellt werden und zu einer bestimmten Seite in der DNA Center Standorthierarchie gehören, an die ISE übergeben. Alle Aktualisierungen an einem DNA Center Gerät (zum Beispiel Änderungen an der IP-Adresse, Simple Network Management Protocol (SNMP)- oder Command-Line Interface (CLI)-Anmeldeinformationen, gemeinsamer ISE Schlüssel und weitere) werden automatisch an die entsprechende Geräteinstanz auf der ISE weitergeleitet. Wenn ein

DNA Center Gerät gelöscht wird, wird es ebenfalls aus der ISE entfernt. [4]

5.4 Locator ID Separation Protocol (LISP)

LISP ist das Produkt einer Arbeitsgruppe in der Internet Engineering Taskforce (IETF), um das wachsende Problem des doppelten Verwendungszwecks der IP-Adressen zu bereinigen. Zur Zeit wird die IP-Adresse benutzt um die Identität eines Hosts festzulegen und auch den Ort zu bestimmen, an dem er sich im Internet befindet. Dies hat zur Folge das sich bei einem Aufenthalsortwechsel auch die IP-Adresse des Hosts ändert, was bedeutet das die Identität verloren geht und die alten IP-Verbindungen verfallen.

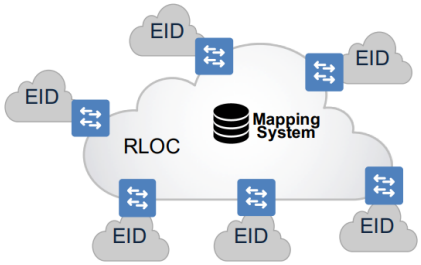


Abbildung 5.7: LISP Aufbau [6]

Dies soll nun durch LISP geändert werden, in dem es die Identität eines Gerätes, von seinem Aufenthaltsort, in zwei separate Adressräume unterteilt. Das bedeutet, dass die Router in einer LISP Architektur nur Routing Informationen von RLOCs speichern müssen. Um Pfadinformationen eines Hosts abzurufen, kann der Router diese beim LISP MS Abfragen, was analog wie das DNS-Mapping funktioniert.

LISP verwendet für die SDA Fabric eine VXLAN Kapselung. Um die VXLAN Kapselung für LISP zu aktivieren, muss auf dem Router der LISP Konfigurationsmodus, der Befehl für die VXLAN Enkapsulierung verwendet werden. Dieser Befehl muss auf allen LISP Edge Geräten im Enterprise Fabric konfiguriert werden: Ingress Tunnel Router (ITR), Egress Tunnel Router (ETR), Proxy Ingress Tunnel Router (PITR), Proxy Egress Tunnel Router (PETR). Wenn dieser Befehl nicht auf einem der LISP Edge Geräte konfiguriert wird, führt dies zu einem Verlust der Kontrolle und des Datenverkehrs. [2]

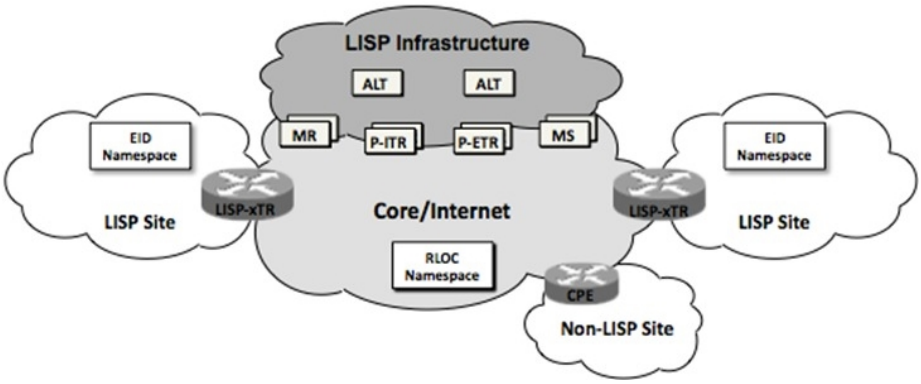


Abbildung 5.8: LISP Infrastruktur [25]

LISP Gerät	Funktion
Alternative Logical Topology (ALT)	Sammelt EID Daten von MS und wirbt mit einem aggregierten EID Präfix. Bei einem Einsatz von mehreren MS werden alle synchronisiert.
Egress Tunnel Router(ETR) und Proxy ETR(PETR)	Verbindet ein LISP-fähiges Kernnetzwerk. Registriert EID Präfixe bei MS. Entkapselt LISP Pakete, die vom LISP Kern empfangen werden. Reagiert auf Map Request Meldungen mit einem Map Reply durch Angabe eines entsprechenden EID Präfixes. Typischerweise ist dies ein Customer Premise Equipment (CPE)-Router. PETR arbeitet im Auftrag von Nicht-LISP-Domains und bietet LISP-Nicht-LISP-Konnektivität.
Ingress Tunnel Router(ITR) und Proxy Ingress Tunnel Router(PITR)	Verantwortlich für die Weiterleitung des lokalen Verkehrs an externe Ziele. Löst RLOC für ein bestimmtes Ziel auf, indem es einen Map Request an den MR sendet. Kapselt (VXLAN) Datenverkehr mit LISP Header. Typischerweise ist dies ein Access Layer Switch. PITR arbeitet im Auftrag von Nicht-LISP-Domains und bietet LISP-Nicht-LISP-Konnektivität.
x Tunnel Router(xTR)	Wenn sowohl ITR als auch ETR Funktionen von einem Router verarbeitet werden, heißt das xTR. Das ist typisch für die Praxis.
Map Resolver(MR)	Reagiert auf Map Requests vom ITR. Map Requests werden mit einer negativen Map Antwort beantwortet oder an die entsprechende ETR oder ALT weitergeleitet.
Map Server(MS)	Registriert EID Speicherplatz beim Empfang von Map Registernachrichten vom ETR. Aktualisiert ALT und MR mit EID und RLOC Daten.
Map Server Map Resolver(MSMR)	Wenn ein Gerät sowohl als MS als auch als MR fungiert, wird es MSMR genannt. Das ist typisch für die Praxis.
Endpoint ID(EID)	IP-Adressen, die in der Routingtabelle des Kernnetzwerks versteckt sind. RLOC agiert im nächsten Schritt, um den EID Raum zu erreichen.
Routing Locator(RLOC)	Existiert in globalen Routing-Tabellen. Verbindlich, um den EID Raum zu erreichen.

Tabelle 5.1: LISP Elemente [25]

5.4.1 Campus Fabric und LISP

Im Einzug mit dem Campus Fabric wurden für bestehende LISP Namenskonzepte neue Begriffsdefinitionen zugewiesen:

- Control Plane Node ≈ LISP MS
- Edge Node ≈ LISP xTR
- Border Node ≈ LISP PxTR
- Intermediate Node ≈ Nicht-LISP IP Forwarder

Fabric Control Plane Node basiert auf einem LISP MS / MR. Führt die LISP HTDB aus, um Overlay Erreichbarkeitsinformationen bereitzustellen.

- Eine einfache Host Datenbank, die die Endpunkt-ID zu Edge-Knoten-Bindungen zusammen mit anderen Attributen verfolgt
- Host-Datenbank unterstützt mehrere EID Lookup Schlüssel (IPv4 / 32, IPv6 / 128 oder MAC)
- Empfängt Präfix Registrierungen von Edge Nodes mit lokalen Endpunkten
- Beheben von Suchanforderungen von Remote Edge Knoten, um lokale Endpunkte zu finden

Fabric Edge Node basiert auf einem LISP xTR. Bietet Konnektivität für Benutzer und Geräte, die mit dem Fabric verbunden sind.

- Verantwortlich für das Identifizieren und Authentifizieren von Endpunkten
- Registrieren von EID mit dem Control Plane Node(s)
- Bietet Anycast L3 GW für verbundene Endpunkte
- Host Datenverkehr von und zu Endpunkten, die mit dem Fabric verbunden sind, verkapseln/entkapseln

Fabric Border Node basiert auf einem LISP PxTR. Der gesamte Verkehr, der das Fabric betritt oder verlässt, durchläuft diesen Knotentyp.

- Verbindet traditionelle L3 Netzwerke und / oder verschiedene Fabric Domänen mit der lokalen Domäne
- Wo zwei Domänen Endpunkte Erreichbarkeit und Richtlinieninformationen austauschen
- Verantwortlich für die Übersetzung von Kontexten (VRF und SGT) von einer Domäne in eine andere
- Stellt einen Domänenexitpunkt für alle Edge Knoten bereit

5.5 Virtual Extensible LAN (VXLAN)

VXLAN ist ein Encapsulation Protokoll, um ein Overlay Netzwerk auf einer existierenden L3 Infrastruktur laufen zu lassen. VXLAN wurde ursprünglich von Cisco Systems, VMware und Arista Network entwickelt und ist einer der IETF festgelegten Standards (RFC 7348). [1]

Technisch gesehen erzeugt ein VXLAN logische L2 Netzwerke, die dann in standardmässige L3 Pakete eingepackt werden. VXLAN dient dazu, in sehr grossen Netzwerkumgebung die Probleme zu lösen, die durch beschränkte Anzahl von VLANs betroffen sind. Mit VXLAN

sind insgesamt 16'777'215 (24 Bit) L2 Umgebungen möglich, die ihrerseits wieder jeweils 4096 VLANs beinhalten können.

5.5.1 VXLAN Encapsulation

Die Data Plane basiert auf VXLAN, im Gegensatz zur Control Plane, welche auf LISP basiert. Die VXLAN Kapselung ist IP/UDP-basiert, was bedeutet, dass sie von jedem IP-basierten Netzwerk (Legacy- oder nicht-Cisco-Netzwerk) weitergeleitet werden kann und effektiv den Overlay Aspekt der SDA Fabric erzeugt. Die VXLAN Kapselung wird (statt der LISP Kapselung) aus zwei Hauptgründen verwendet. VXLAN umfasst den Source L2 (Ethernet) -Header (LISP nicht) und bietet auch spezielle Felder für zusätzliche Informationen, wie die ID des virtuellen Netzwerks (VNs) und die ID der Gruppe (Segment). [3]

Diese Technologie bietet mehrere Vorteile für SDA, zum Beispiel die Unterstützung für virtuelle L2 und L3 Topologien (Overlays) und die Möglichkeit, über jedes IP-basierte Netzwerk mit integrierter Netzwerksegmentierung (VRF/VN) und gruppenbasierter Richtlinie zu arbeiten.

In SDA wurden einige Verbesserungen der ursprünglichen VXLAN Spezifikationen hinzugefügt, insbesondere die Verwendung von SGTs. Dieses neue VXLAN Format ist derzeit ein IETF Entwurf, der als Gruppenrichtlinienoption (oder VXLAN-GPO) bekannt ist.

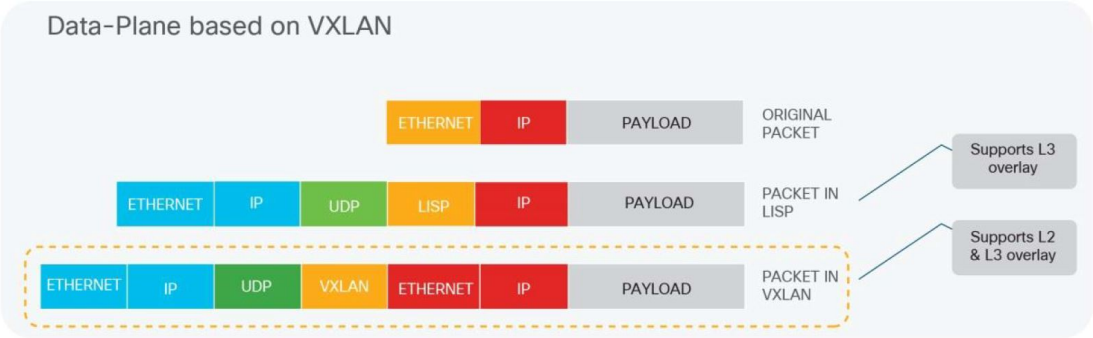


Abbildung 5.9: Fabric Data Plane basierend auf VXLAN [3]

Die Fabric Data Plane bietet folgendes:

- Underlay Adressanzeige und -zuordnung
- Automatischer Tunnelaufbau (Virtuelle Tunnelendpunkte)
- Frame-Kapselung zwischen RLOCs

Unterstützung für das LISP- oder VXLAN-Header Format

- Fast gleich, mit verschiedenen Feldern und Nutzlast
- LISP-Header trägt IP-Payload (IP in IP)
- VXLAN-Header trägt MAC-Payload (MAC in IP)

Ausgelöst durch LISP Control Plane Ereignisse

- ARP oder NDP Learning auf L3 GW
- Map Reply oder Cache auf RLOCs

5.5.2 Fabric Data Plane

RFC 7348 definiert die Verwendung von VXLAN als eine Möglichkeit, ein L2 Netzwerk über einem L3 Netzwerk zu überlagern. Mit VXLAN wird ein ursprünglichen L2 Frame

mit UDP/IP über das L3 Netzwerk getunnelt. Die Tunnelschnittstelle an jedem Knoten wird VTEP genannt. VTEPs beruhen auf dem Lernen der Data- oder Control-Plane, um den entfernten Endpunkt für das VTEP-Mapping für die Verkapselung des Datenverkehrs zu bestimmen. Jedes Overlay Netzwerk wird als VXLAN Segment bezeichnet und mithilfe einer 24-Bit VXLAN Netzwerk-ID identifiziert, die bis zu 16 Millionen VXLAN Segmente unterstützt. [1]

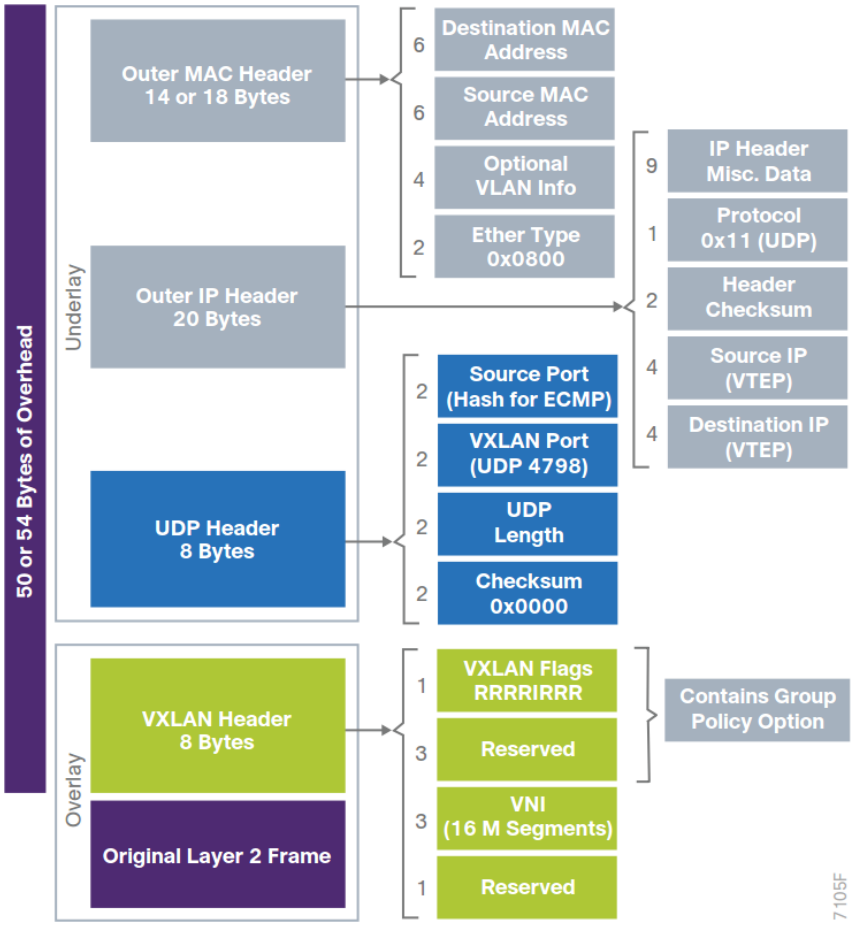


Abbildung 5.10: RFC7348 VXLAN Header [4]

Das SDA Fabric verwendet die VXLAN Data Plane, um das vollständige, ursprüngliche L2 Frame bereitzustellen und verwendet zusätzlich LISP als Control Plane, um die Endpunkt zu VTEP Zuordnungen aufzulösen. Das SDA Fabric ersetzt 16 der reservierten Bits im VXLAN Header, um bis zu 64'000 SGTs zu transportieren. Dabei wird ein modifiziertes VXLAN-GPO-Format verwendet.
Der VNI wird einer virtuellen Routing- und Weiterleitungsinstanz für L3 Overlays zugeordnet, während ein L2 VNI einer VLAN Broadcastdomäne zugeordnet wird. Beide bieten den Mechanismus zur Isolierung von Data und Control Plane für jedes einzelne virtuelle Netzwerk. Die SGT trägt Gruppenmitgliedschaftsinformationen von Benutzern und stellt eine Data Plane Segmentierung innerhalb des virtualisierten Netzwerks bereit. [4]

5.6 Infoblox

Infoblox ist einer der führenden Hersteller für DNS, DHCP, Trivial File Transfer Protocol (TFTP) und IPAM. Die Integration von Infoblox ermöglicht dem DNA Center die IPAM Funktionen von Infoblox zu nutzen. Dafür werden beispielsweise die IP-Adresspools zwischen dem DNA Center und Infoblox synchronisiert. Mit dieser Integration können IP-Adresszuweisungen automatisiert werden, was eine richtlinienbasierte Bereitstellung in einer einzigen Operation ermöglicht und so die betriebliche Effizienz verbessert.
Infoblox ermöglicht die automatische Überprüfung der Netzwerkinfrastrukturen, die Konfiguration sowie Anpassung an die jeweiligen Compliance-Vorgaben. Mittels DNS, DHCP, TFTP und IPAM werden wichtige Kontrollfunktionen für Endgeräte und Anwendungen bereitgestellt. Dank der DNS Management Software Appliance kann stets der Überblick über die IP-Adressbereiche behalten und die Verteilung der DNS- und DHCP-Daten überprüft und automatisiert werden. Reportings älterer sowie aktueller Daten können dank einer zuverlässigen Netzwerkdatenbank sowie Grid-Technologie erstellt werden.[17]

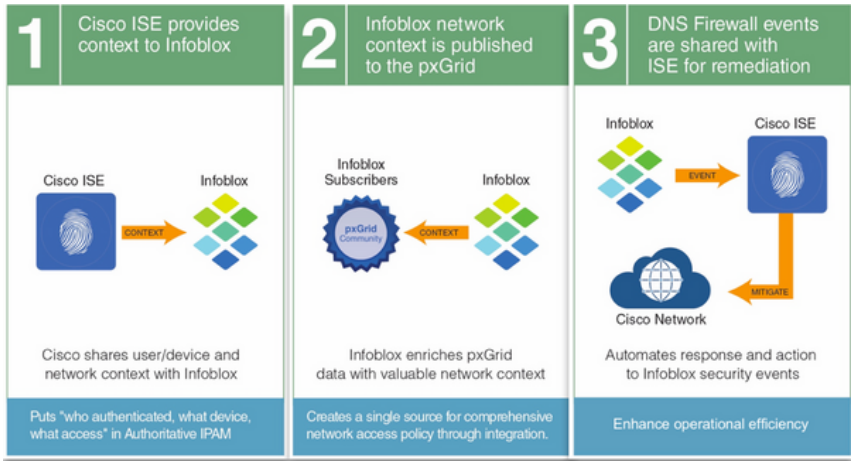


Abbildung 5.11: Zusammenspiel Infoblox und ISE [18]

Die gemeinsame Lösung von Infoblox ActiveTrust und Cisco ISE verbessert die Genauigkeit und Aktualität von Sicherheitsmaßnahmen, erhöht die Sichtbarkeit und erleichtert den Austausch von Informationen zwischen Netzwerk- und Sicherheitsteams. Cisco teilt den Gerätekontext mit Infoblox, während der Infoblox Netzwerkkontext in pxGrid veröffentlicht wird, sodass Netzwerkadministratoren die Reaktionszeit für die Sicherheit automatisieren und verkürzen können.[18]

5.7 SDA Mechanismus Beispiel

Zum besseren Verständnis des ganzen Ablaufes einer Kommunikation zwischen zwei Clients, wird von folgender Ausgangslage ausgegangen: Wenn ein IP Paket über SD-A von PC1 172.16.1.1/24 nach PC2 10.0.2.34/24 geschickt wird, was passiert mit dem Paket?

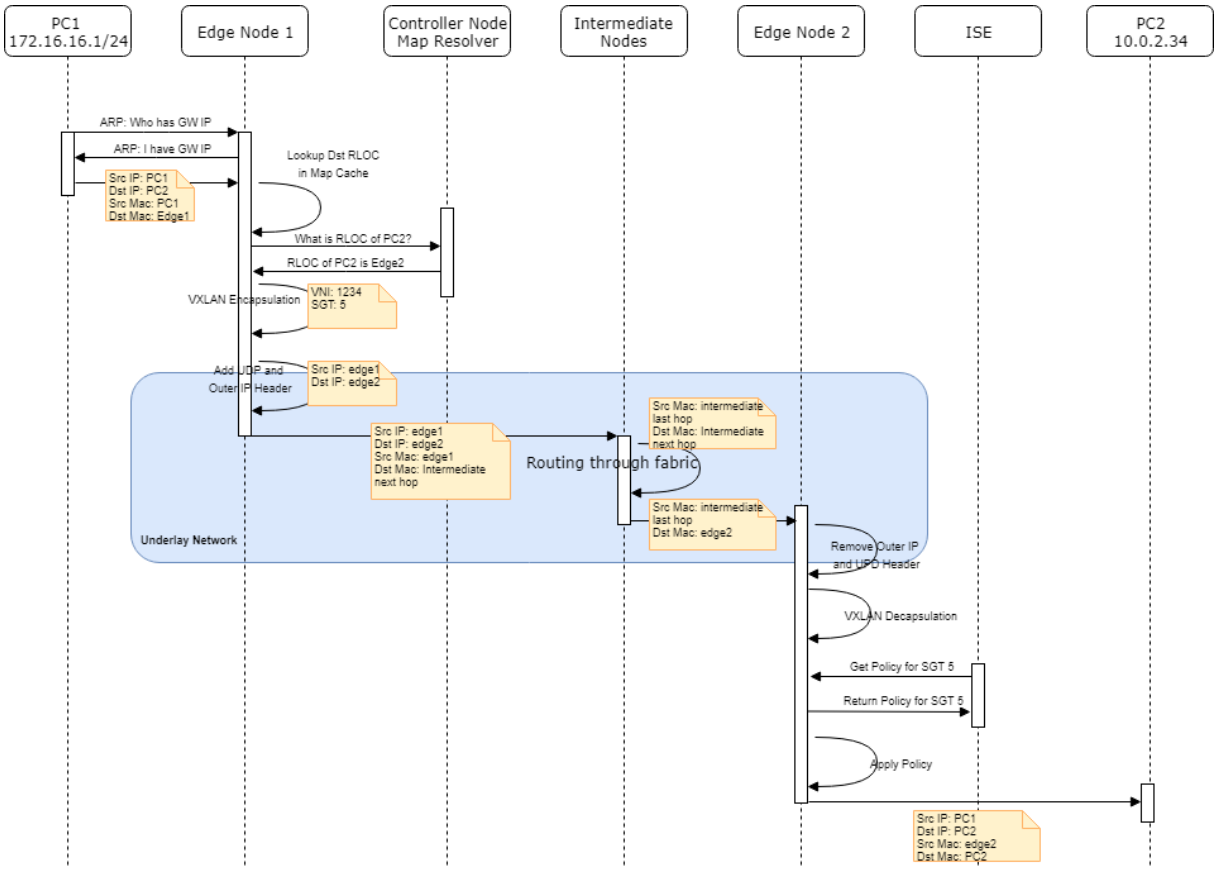


Abbildung 5.12: SDA Mechanismus

Als erstes wird vom PC1 ein Address Resolution Protocol (ARP) Lookup an den default GW gesendet. Dieser erhält eine Antwort vom Edge Node 1 (GW ist Anycast Adresse und wird von jedem Edge Node beantwortet). Nachfolgend sendet der PC1 sein Paket an den GW. Der Edge Node 1 führt ein RLOC Lookup im lokalen Map Cache aus. Falls kein Eintrag im lokalen Cache vorhanden ist, sendet er ein RLOC Lookup an den MR. Von diesem MR erhält der Edge Node 1 den RLOC von PC2, falls vorhanden. Ist dieser nicht bekannt, wird der Border Node verwendet. Nun erfolgt die VXLAN Encapsulation (SGT 5, VNI1234) und es wird der UDP und Outer IP Header hinzugefügt (Underlay Network). Das Paket wird nun an die RLOC IP (Destination Edge Node) weitergesendet. Sollten Intermediate Nodes vorhanden sein, wird das Paket durch diese geroutet, bis der Edge Node 2 das Paket erhält. Nun werden der UDP und Outer IP Header wieder entfernt (Underlay Netowork) und es geschieht die VXLAN Decapsulation. Nun wird die Policy für SGT 5 beim ISE angefragt. Dieser gibt die dazugehörigen Policies zurück und wendet diese auf das Paket an. Je nach Policy wird das Paket weitergesendet oder verworfen. In diesem Fall wird die Policy angewendet und an das Ziel, den PC2 weitergeleitet.

6 Use Cases

6.1 Use Cases Brief

6.1.1 UC01: Definierung von Benutzerprofilen

Ein Administrator definiert die Profile für Benutzer, Gruppen oder Geräte, sodass diese auf alle nötigen Ressourcen zugreifen können, unberechtigter Zugriff aber verhindert wird.

6.1.2 UC02: Backup and Restore DNA Center

Auf Grund eines Problems des DNA Centers muss die Appliance ausgetauscht oder auf einen vorherigen Konfigurationsstand zurückgesetzt werden. Um eine Neukonfiguration des Systems zu verhindern, wird eine zuvor gesicherte Konfiguration wiederhergestellt.

6.1.3 UC03: Reporting

Es werden regelmässig Reports über relevante Netzwerkaktivitäten erstellt und den zuständigen Personen via Mail zugestellt.

6.1.4 UC04: Hardware Ersatz

Ein Switch muss auf Grund eines Hardwaredefekts oder anderen Gründen ausgetauscht werden.

6.1.5 UC05: Benutzermobilität

Ein User ändert seinen Arbeitsplatz, das Gebäude oder den Arbeitsort. Er muss an allen Standorten dieselben Policies erhalten und auf dieselben Ressourcen zugreifen können.

6.1.6 UC06: Degradation

Bearbeitung von möglichen Degradations-Szenarien mit entsprechenden Degradations-Tests.

6.1.7 UC07: Integration von nicht Fabric Komponenten

Netzintegration von „nicht Campus Fabric Netzkomponenten“ (zum Beispiel traditionelle Access und Distribution Switches).

6.1.8 UC08: Migration von bestehendem klassichen Campus

Migrationskonzept einer bestehenden Campus LAN Lösung zu einer Campus Fabric Lösung mit dem DNA Center.

6.1.9 UC09: Einsatz von SGT

Einsatz von SGTs zusammen mit VXLAN (Netzdesign, Design-Rules, Transport innerhalb und ausserhalb der Fabrics, Schnittstelle L2/L3 und Überführung der IP-Konnektivität an ein IP-Backbone wie zum Beispiel MPLS VPN).

6.1.10 UC10: Infoblox

Integration Infoblox DNS, DHCP und IPAM (DDI) mit dem DNA Center für die Provisionierung von IP-Adressen für das Management von neuen Netzkomponenten in die Fabric (beispielsweise Access Switches).

6.2 Use Cases Fully Dressed

6.2.1 UC01: Definierung von Benutzer und Geräteprofilen

Primary Actor	Administrator
Beschreibung	Ein Administrator definiert die Profile für Benutzer, Gruppen oder Geräte, sodass diese auf alle nötigen Ressourcen zugreifen können, unberechtigter Zugriff aber verhindert wird.
Stakeholders	• Administrator • User
Preconditions	• DNA Center komplett konfiguriert • ISE konfiguriert und mit DNA Center verbunden
Postconditions	• User kann auf all nötigen Ressourcen zugreifen • Zugriffe auf nicht berechtige Ressourcen werden blockiert
Main Success Story	1. Profil wird definiert 2. Profil wird Usern oder Geräten zugewiesen 3. Entsprechende Geräte und Benutzer haben Zugriff auf benötigte Ressourcen (und keine zusätzlichen)

Alternative Flows	1a. Definitionen fehlen
	  1. Netzwerksegmente oder Ressourcen definieren
	  2. Profil definieren
	2a. User oder Geräte fehlen
	  1. User oder Geräte erfassen
	  2. Profil wird Usern oder Geräten zugewiesen

Tabelle 6.1: UC01 Fully Dressed

6.2.2 UC02: Backup and Restore DNA Center

Primary Actor	Netzwerkadministrator
Beschreibung	Auf Grund eines Problems des DNA Centers muss die Appliance ausgetauscht oder auf einen vorherigen Konfigurationsstand zurückgesetzt werden. Um eine Neukonfiguration des Systems zu verhindern, wird eine zuvor gesicherte Konfiguration wiederhergestellt.
Stakeholders	Alle Netzwerkbenutzer
Preconditions	• Ein Backup der DNA Center Konfiguration existiert
Postconditions	• Appliance läuft mit einer zuvor gesicherten Konfiguration
Main Success Story	1. Passendes Backup wählen 2. Appliance auf den Stand des Backups zurücksetzen
Alternative Flows	-

Tabelle 6.2: UC02 Fully Dressed

6.2.3 UC03: Reporting

Primary Actor	Netzwerkadministrator
Beschreibung	Es werden regelmässig Reports über relevante Netzwerkaktivitäten erstellt und den zuständigen Personen via Mail zugestellt
Stakeholders	• Netzwerkadministratoren • Management
Preconditions	• Alle nötigen Daten zur Erstellung der Reports stehen im DNA Center zur Verfügung.
Postconditions	• Definierte Benutzer erhalten regelmässige Reports
Main Success Story	1. Relevante Informationen aus dem DNA Center werden erfasst 2. Informationen werden aufbereitet, Report wird generiert 3. Report wird per Mail an alle definierten Personen
Alternative Flows	3a. Alternativer Messenger 1. Report wird via Slack an alle definierten Personen gesendet

Tabelle 6.3: UC03 Fully Dressed

6.2.4 UC04: Hardware Ersatz

Primary Actor	Netzwerkadministrator
Beschreibung	Ein Switch muss auf Grund eines Hardwaredefekts oder ähnlichen Gründen ausgetauscht werden.
Stakeholders	• Netzwerkadministratoren • User am betroffenen Switch
Preconditions	• Ersatzhardware verfügbar
Postconditions	• Ersatzhardware hat die Funktionalität des auszutauschenden Geräts vollständig übernommen
Main Success Story	1. Auszutauschendes Gerät wird entfernt 2. Neues Gerät wird installiert 3. Neues Gerät wird verkabelt 4. Neues Gerät wird im DNA Center erfasst 5. DNA Center installiert Konfiguration des alten Geräts auf das neue 6. Neues Gerät übernimmt Funktion des alten Geräts 7. Altes Gerät im DNA Center entfernen
Alternative Flows	4a. Andere Hardware 1. Ersatzhardware ist nicht identisch mit dem alten Gerät 2. Konfiguration wird im DNA Center angepasst

Tabelle 6.4: UC04 Fully Dressed

6.2.5 UC05: Benutzermobilität

Primary Actor	Mobiler Benutzer
Beschreibung	Ein User ändert seinen Arbeitsplatz, das Gebäude oder den Arbeitsort. Er muss an allen Standorten dieselben Policies erhalten und auf dieselben Ressourcen zugreifen können.
Stakeholders	• User
Preconditions	• User / Gerät erfasst und entsprechende Policies definiert
Postconditions	• User kann nach einem Standortwechsel alle Ressourcen verwenden, die ihm auch vor dem Wechsel zur Verfügung standen
Main Success Story	1. User trennt Verbindung am alten Standort 2. User verbindet sich am neuen Standort 3. User authentifiziert sich 4. Die SDA Lösung gewährt dem User Rechte gemäss Policies 5. User kann auf dieselben Ressourcen zugreifen wie am alten Standort
Alternative Flows	4a. Während des Standortwechsels wurden die Policies angepasst 1. User erhält Rechte gemäss aktualisierten Policies

Tabelle 6.5: UC05 Fully Dressed

6.2.6 UC06: Degradation

Primary Actor	Netzwerkadministrator
Beschreibung	Es soll aufgezeigt werden, wie sich das System beim Ausfall von verschiedenen Komponenten verhält, wo Single Point of Failures liegen und wie diese allenfalls eliminiert werden können.
Stakeholders	• Netzwerkadministrator • Netzwerkbenutzer
Preconditions	• Netzwerkinfrastruktur läuft einwandfrei
Postconditions	• Ausfall/Probleme bei einer oder mehrerer Komponenten
Main Success Story	1. Netzwerk funktioniert einwandfrei 2. Eine oder mehrere Komponenten fallen aus oder weisen sonstige Probleme auf 3. Netzwerkfunktionalität ist durch den Ausfall nicht beeinträchtigt 4. Fehler wird behoben, System wieder im Sollzustand
Alternative Flows	3a. Durch den Ausfall kommt es zu einer Störung im Netzwerk 1. Was sind die genauen Auswirkungen? Wer ist betroffen? 2. Wie kann die Funktionalität wiederhergestellt werden? 3. Kann die Fehlerursache verhindert werden? 3b. Es kommt zum kompletten Ausfall des Netzwerks 1. Was sind die genauen Auswirkungen? 2. Wie kann die Funktionalität wiederhergestellt werden? 3. Kann die Fehlerursache verhindert werden?
Mögliche Szenarien	• Ausfall eines Edge-, Intermediate- oder Border/Controller-Nodes Wenn 1 Node vorhanden ist Wenn 2 Nodes vorhanden sind • Ausfall DNA Center Appliance, ISE, Infoblox, WLC oder einer physischen Netzwerkleitung

Tabelle 6.6: UC06 Fully Dressed

6.2.7 UC07: Integration von nicht Fabric Komponenten

Primary Actor	Netzwerkadministrator
Beschreibung	Die Fabric muss mit Komponenten, die nicht der Fabric angehören kommunizieren können.
Stakeholders	• Netzwerkadministrator • Benutzer
Preconditions	• Fabric funktioniert • Es sind Komponenten oder Teile des Netzwerks vorhanden, die nicht zu einer Fabric gehören.
Postconditions	• Kommunikation funktioniert auch über nicht-Fabric Komponenten hinweg • Policies können auch bei Kommunikation über nicht-Fabric Komponenten angewendet werden
Main Success Story	1. Ein User kommuniziert mit Ressourcen ausserhalb der Fabric 2. Kommunikation funktioniert einwandfrei 3. Policies können wie bei der Kommunikation innerhalb der Fabric angewendet werden
Alternative Flows	1a. Ein User ausserhalb der Fabric will mit Ressourcen innerhalb der Fabric kommunizieren 2a. Kommunikation funktioniert einwandfrei 3a. Policies können wie bei der Kommunikation innerhalb der Fabric angewendet werden

Tabelle 6.7: UC07 Fully Dressed

6.2.8 UC08: Migration von bestehenden klassichen Campus

Primary Actor	Netzwerkadministrator
Beschreibung	Ein bestehendes Netzwerk nach klassischem Campus Design soll zu einer modernen Fabric migriert werden
Stakeholders	• Netzwerkadministrator • Netzwerkbenutzer
Preconditions	• Netzwerk nach klassischem Campus Design existiert und funktioniert einwandfrei • DNA Center Appliance inklusive aller Abhängigkeiten ist vorhanden • Netzwerkkomponenten sind fähig in einer Fabric verwendet zu werden
Postconditions	• Fabric ist erstellt • DNA Center läuft und verwaltet Fabric(s) • Policies, die in der traditionellen Infrastruktur vorhanden waren funktionieren weiterhin
Main Success Story	1. Bestehende Infrastruktur wird analysiert und inventarisiert 2. DNA Center wird aufgesetzt (inkl. aller Abhängigkeiten) 3. User, Gruppen und Policies werden in DNA Center übernommen 4. Falls nötig wird das Netzwerkdesign angepasst 5. Downtime wird geschätzt und organisatorische Massnahmen werden getroffen 6. Bestehende Netzwerkgeräte werden in die Fabric übernommen 7. Benutzer können Fabric analog der traditionellen Infrastruktur nutzen
Alternative Flows	-

Tabelle 6.8: UC08 Fully Dressed

6.2.9 UC09: Einsatz von SGT

Primary Actor	Administrator
Beschreibung	Im DNA Center können über das ISE Panel definierte SGT Gruppen hinzugefügt und angepasst werden.
Stakeholders	• Administrator
Preconditions	• DNA Center muss mit dem ISE verbunden sein und alle ISE SGT-Gruppen und -Geräte müssen im DNA Center vorhanden sein
Postconditions	• SGT Gruppen ersichtlich
Main Success Story	1. Login auf DNA Center 2. Unter Systemeinstellungen Cisco ISE Panel auswählen 3. Unter *Policy* → *Registry* → *Scalable Groups* können neue SGT Gruppen hinzugefügt werden
Alternative Flows	-

Tabelle 6.9: UC09 Fully Dressed

6.2.10 UC10: Infoblox

Primary Actor	Administrator
Beschreibung	Infoblox ist die IP-Adressmanagement-Lösung (IPAM) für das Cisco Digital Network Architecture (DNA) Center. IP-Adresspools werden zwischen DNA Center und Infoblox synchronisiert. Mit dieser Integration kann die Zuweisung von IP-Adressen automatisiert werden, was eine richtlinienbasierte Bereitstellung in einem einzigen Vorgang ermöglicht und so die Betriebseffizienz verbessert.
Stakeholders	• Administrator
Preconditions	• Infoblox Server ist eingerichtet
Postconditions	• Unter *Design* → *Network Settings* → *IP Address Pools* sind nun die IP-Adressen ersichtlich. • Anpassungen an Addresspool werden zwischen DNA Center und Infoblox synchronisiert • Infoblox verwendet die im DNA Center erstellten Infos für weitere Dienste wie DNS oder DHCP
Main Success Story	1. Login auf DNA Center 2. Unter *Settings* → *IP Adress Manager* kann ein Infoblox Server hinterlegt werden. 3. Unter *Design* → *Network Settings* → *IP Address Pools* können nun die IP-Adressen angezeigt werden

Alternative Flows	1a. Direkt nach der Installation des DNA Centers, Infoblox Server bei erstem Konfigurations-Wizard hinzufügen
	  1. Login auf DNA Center
	  2. IPAM angeben (Server Name, Server URL, Username, Password, Provider)
	1b. Schritt in erstem Konfigurations-Wizard überspringen und Infoblox mit nachfolgenden Schritten hinzufügen.

Tabelle 6.10: UC10 Fully Dressed

7 Testprotokolle

7.1 UC01-1: Anlegen von Benutzern

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login in ISE	Eingelogged in ISE	Eingelogged in ISE	OK
2	Benutzer anlegen via *Work Centers* → *Network Access* → *Identities* → *Network Access Users*	User ist erstellt	User ist erstellt	OK
3	Benutzer einer Gruppe zuweisen via *Work Centers* → *Network Access* → *Identities* → *Network Access Users*	User ist in Gruppe	User ist in Gruppe	OK

Tabelle 7.1: UC01-1: Anlegen von Benutzern

Die Benutzer sind nun angelegt, ein Login ist aber noch nicht möglich, da noch keine Authentication Policy für diese erstellt wurde. Dies wird daher im nächsten Schritt erledigt.

7.2 UC01-2: Anlegen von Authentication Policies

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login in ISE	Eingelogged in ISE	Eingelogged in ISE	OK
2	Authentication Policy anlegen via *Work Centers* → *Network Access* → *Policy Sets* → *Default* für 802.1x Wired	Policy ist erstellt	Policy ist erstellt	OK
3	User logged sich ein	User ist eingelogged	User ist eingelogged	OK

Tabelle 7.2: UC01-2: Anlegen von Authentication Policies

Nun kann sich der Benutzer einloggen, wird aber noch nicht einer Scalable Group zugewiesen. Somit hat er keine für ihn gültige Policy und somit keine Zugriffe im Netzwerk. Damit der Benutzer die korrekten Policies erhält, muss eine Authorization Policy erstellt werden.

7.3 UC01-3: Anlegen von Authorization Policies

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login in ISE	Eingelogged in ISE	Eingelogged in ISE	OK
2	Authorization Policy anlegen via *Work Centers* → *Network Access* → *Policy Sets* → *Default* für 802.1x Wired und Gruppe des Users	Authorization Policy ist erstellt	Authorization Policy ist erstellt	OK
3	User wird beim Login der korrekten SG zugewiesen	User ist der korrekten Gruppe zugewiesen	User ist der korrekten Gruppe zugewiesen	OK

Tabelle 7.3: UC01-3: Anlegen von Authorization Policies

7.4 UC01-4: Einrichten einer Policy

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login auf DNA Center	DNA Center Dashboard wird angezeigt	DNA Center Dashboard wird angezeigt	OK
2	Policy einrichten unter *Policy* → *Policy Administration* → *Group Based Access Control*	Policy wird angelegt	Policy wird angelegt	OK
3	DNA Center synchronisiert Policy mit dem ISE	Policy ist auf ISE	Policy ist auf ISE	OK

4	ISE pushed Policy auf Border und Edge Nodes	Policy ist auf Nodes vorhanden	Policy ist auf Nodes vorhanden	OK
5	Die Nodes enforcen die Policy für die korrekten Clients	Policy wird enforced	Policy wird enforced	OK

Tabelle 7.4: UC01-4: Einrichten einer Policy

Die Policy ist nun auf allen nötigen Geräten deployed und wird von diesen enforced. Die Clients dürfen also nur auf die Ressourcen zugreifen, die gemäss der definierten Policy erlaubt sind.

7.5 UC02-1 Backup DNA Center

Sämtliche Konfigurationen des DNA Centers sollen gesichert werden, sodass diese im Notfall wiederhergestellt werden können.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login auf DNA Center	DNA Center Dashboard wird angezeigt	DNA Center Dashboard erscheint	OK
2	Zu den Backup Einstellungen navigieren *Settings* → *System Settings* → *Backup and Restore*	Backup Einstellungen anzeigen	Backup Einstellungen erscheinen	OK
3a	Backup Server hinzufügen via *Add* → SSH IP Address: 217.26.58.9, SSH Port: 22, Server Path: /home/dnacenter/backup, Username: dnacenter, Password: xxx, Encryption Passphrase: xxx. Mittels Apply die Eingaben bestätigen.	Eingaben werden angenommen.	Eingaben werden meist nicht angenommen und führen zu Absturz des DNA Centers	NOT OK
3b	Backup Server hinzufügen via *Add* → SSH IP Address: 217.26.58.9, SSH Port: 22, Server Path: /home/dnacenter/backup, Username: dnacenter, Password: xxx, Encryption Passphrase: xxx. Mittels Apply die Eingaben bestätigen.	Eingaben werden angenommen.	Eingaben werden angenommen.	OK
4b	Regelmässiges Backup einrichten via *Schedule* → *Add* Schedule Later, Weekday: Wednesday, Time: 10:30 AM. Mittels Schedule die Eingaben bestätigen.	Eingaben werden angenommen.	Eingaben werden angenommen.	OK
5b	Backup wird regelmässig zum definierten Zeitpunkt ausgeführt.	Backup wird zum definierten Zeitpunkt ausgeführt	Backup wird nicht ausgeführt	NOT OK

Tabelle 7.5: UC02-1 Backup DNA Center

7.6 UC02-2 Restore DNA Center

Sämtliche Konfigurationen des DNA Centers sollen aus einem zuvor erstellten Backup wiederhergestellt werden.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login auf DNA Center	DNA Center Dashboard wird angezeigt	DNA Center Dashboard erscheint	OK
2	Zu den Backup Einstellungen navigieren *Settings* → *System Settings* → *Backup and Restore*	Zuvor erstellte Backups werden angezeigt	Backups werden angezeigt	OK
3	Restore erstellen via *Restore* neben dem gewünschten Backup	DNA Center wird auf den Stand vom gewählten Backup zurückgesetzt	DNA Center wurde auf den gewünschten Stand zurückgesetzt	OK

Tabelle 7.6: UC02-2 Restore DNA Center

Es kann ein Backup erstellt werden und auch ein Restore eines zuvor erstellten Backups ist möglich. Leider ist das Erfassen, Bearbeiten und Löschen eines Backup Servers enorm unzuverlässig und hat mehrfach zu kompletten Abstürzen des DNA Centers geführt.
Zudem funktioniert der Backup Schedule nicht. Backups werden nicht automatisch ausgeführt, sind also nur manuell möglich. Auch ein Restore einzelner Komponenten des DNA Centers ist nicht vorgesehen und es gibt kein komplettes Backup des DNA Centers. Einzelne Teile wie zum Beispiel Assurance werden nicht gesichert.
Da die Backup Funktionalität des DNA Centers sehr eingeschränkt ist und nur unzuverlässig funktioniert, wird der Use Case "Backup und Restore" nicht vollständig erfüllt.

7.7 UC03 Reporting

Mit Hilfe der DNA Center API können regelmässige Reports über den Zustand der Netzwerkumgebung per E-Mail oder Slack versendet werden. Damit dieser Use Case ausgeführt werden kann, muss ein Mailserver und ein Benutzer zur Verfügung stehen, der E-Mails versenden kann. Des weiteren wird ein System benötigt, welches das Script ausführt. Auf diesem muss Python installiert sein.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Reporting Script aus GIT Repository auschecken (auf dem System, das die Reports versenden soll)	Code ist ausgecheckt	Code ist ausgecheckt	OK
2	config.py mit Texteditor öffnen und anpassen	Reporting Config ist komplett	Reporting Config ist komplett	OK
3	Cronjob einrichten, der das Script in regelmässigen Abständen ausführt	Script wird regelmässig ausgeführt	Script wird regelmässig ausgeführt	OK
4a	Cronjob wird ausgeführt und versendet Report per E-Mail	Report wird per E-Mail versendet.	Report wird per E-Mail versendet	OK
4b	Cronjob wird ausgeführt und versendet Report per Slack	Report wird per Slack versendet.	Nicht implementiert	NOT OK

Tabelle 7.7: UC03 Reporting

Mit dieser Lösung ist ein sehr rudimentäres Reporting implementiert worden. Es wird lediglich eine Liste aller Netzwerkgeräte, sowie eine Liste aller Hosts mit den wichtigsten Informationen und dem Zustand der Geräte ausgegeben. Wünschenswert wären natürlich wesentlich mehr Informationen, insbesondere aus dem Bereich Assurance. Leider unterstützt die API des aktuellen Release 1.1.6 diese Funktionien nicht. Im Release 1.2 ist einiges mehr vorhanden, aber nach wie vor als Early Field Trial (EFT) gekennzeichnet. Eine sinnvolle Reporting Funktion ist daher mit den aktuell verfügbaren APIs des DNA Centers nicht realisierbar.

7.8 UC04: Hardware Ersatz

Wenn ein Device in der Fabric ausfällt, ist folgendermassen vorzugehen, um dieses auszutauschen und den alten Stand der Fabric wiederherzustellen.

- Altes Gerät durch neues ersetzen
- Neues Gerät identisch verkabeln
- Das Gerät mittels LAN Automation wieder in Betrieb nehmen
- Device Provisioning ausführen
- Device der ursprünglichen Fabric hinzufügen
- Device Provisioning erneut ausführen
  Sofern der Gerättyp zwischen altem und neuen Device identisch ist, sollte die Access Portkonfiguration übernommen werden
  Sind es unterschiedliche Gerätetypen müssen die Access Ports manuell konfiguriert werden
- Der neue Switch sollte nun die komplette Funktion des alten übernommen haben

Die obigen Informationen sind nur theoretisch und konnten in der Testumgebung nicht getestet werden.

7.9 UC05 Benutzermobilität

Ein User ändert seinen Arbeitsplatz, das Gebäude oder den Arbeitsort. Er muss an allen Standorten dieselben Policies erhalten und auf dieselben Ressourcen zugreifen können.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	User ist in Gebäude 1 mit dem Netzwerk verbunden	User ist mit dem Netzwerk verbunden	User ist mit dem Netzwerk verbunden	OK
2	User authentifiziert sich und erhält die korrekten Policies	User erreicht nur die Ressourcen, die per Policy erlaubt sind	User erreicht nur die Ressourcen, die per Policy erlaubt sind	OK
3	User trennt Verbindung in Gebäude 1	Verbindung ist getrennt	Verbindung ist getrennt	OK
4	User verbindet sich im Gebäude 2	User ist mit dem Netzwerk verbunden	User ist mit dem Netzwerk verbunden	OK
5	User authentifiziert sich	User ist authentifiziert	User ist authentifiziert	OK
6	User erhält die korrekten Policies	User erreicht dieselben Ressourcen wie zuvor in Gebäude 1	User erreicht dieselben Ressourcen wie zuvor n Gebäude 1	OK

Tabelle 7.8: UC05 Benutzermobilität

Benutzermobilität funktioniert in einer vom DNA Center verwalteten Umgebung sehr gut. In unseren Tests wurden sogar bestehende SSH Sessions vom alten an den neuen Standort übernommen.

7.10 UC06: Degradation

In diesem Use Case wird beschrieben, wie sich das Netzwerk verhält, wenn einzelne Komponenten ausfallen. In untenstehender Tabelle ist zu sehen, was für einen Impact der Ausfall der einzelnen Komponenten hat. Die Informationen sind allerdings nur theoretisch und konnten in der Lab Umbegung nicht getestet werden.

Ausfall Gerät	**Impact**
Edge Node	Alle Clients an diesem Device verlieren die Konnektivität.
Intermediate Node	Kein Impact solange alle Edge Devices noch einen Pfad zum Border und somit zu den anderen Edge Nodes haben
Border Node	Kein Impact, solange ein weiterer Border verhanden ist. Falls nicht, verliert die Fabric die Kommunikation zu Geräten ausserhalb der Fabric
Control Plane	Kein Impact, solange eine weitere Control Plane vorhanden ist. Falls nicht, können die Edge Nodes den RLOC von Clients nicht mehr ermitteln und müssen auf den eigenen Cache zurückgreifen. Die Kommunikation innerhalb und ausserhalb der Fabric ist also eingeschränkt. Sobald die TTL der Cache Einträge abgelaufen ist, ist nur noch Kommunikation zwischen Clients am gleichen Edge Node möglich.
DNA Center	Ein Ausfall des DNA Centers hat keinen direkten Einfluss auf das Netzwerk. Es können allerdings keine Anpassungen mehr gemacht werden, die Assurance Daten stehen nicht zur Verfügung und werden nicht mehr erfasst.
ISE	Fällt der ISE aus und es ist kein weiterer ISE vorhanden, können sich Benutzer nicht mehr am Netzwerk authentifizieren und die Policies sind nicht mehr verfügbar. Das heisst, der Netzwerkbetrieb ist stark eingeschränkt oder gar komplett unterbrochen. Es gibt daher die Möglichkeit, ein "Notfall VLAN" zu definieren, über welches die Clients in diesem Fall weiterhin kommunizieren könnten.
Infoblox	Fällt Infoblox aus, können keine neuen IP Pools angelegt werden. Des Weiteren funktioniert DNS nicht mehr, sofern Infoblox der einzige DNS Server war. Dasselbe gilt auch für DHCP.

Kabelunterbruch	Ein Kabelunterbruch zwischen zwei Netzwerkkomponenten in der Fabric hat keinen Impact auf den Betrieb, sofern alle Edge Nodes über Pfade zu den anderen Edge Nodes und dem Border verfügen.

Tabelle 7.9: UC06: Testprotokoll Degradation

7.11 UC07: Integration von nicht Fabric Komponenten

Der Einsatz von nicht Fabric Komponenten ist im aktuellen Release nicht unterstützt. Es ist aber vorgesehen, dass im Release 1.2 die "SD Access Extension for IoT" eingeführt wird, mit der die Fabric mit Hilfe von Geräten wie zum Beispiel dem C3650CX erweitert werden kann.

7.12 UC08: Migration von bestehendem klassischen Campus

Es gibt derzeit keinen definierten Migrationspfad von einem klassischen Campus Netzwerk. Die Empfehlung von Cisco ist allerdings wie folgt:

- Parallel zu bestehendem Netzwerk einen Border Node aufsetzen
- Mit Hilfe der LAN Automation einen Intermediate Node in Betrieb nehmen
- Mit Hilfe der LAN Automation einen ersten Edge Node in Betrieb nehmen
- Fabric erstellen
- User, Policies usw. definieren
- Schrittweise Clients migrieren
- Schrittweise weitere Nodes (Border, Intermediate, Edge) hinzufügen

Werden Devices aus einem klassischen Netz in die Fabric übernommen, sollten die Konfiguration zuerst gelöscht werden. Dieses Vorgehen wird von Cisco so empfohlen, konnte aber in unserer Testumgebung nicht getestet werden, da ein Parallelbetrieb einer klassischen Umgebung und der Fabric zu aufwändig gewesen wäre.

7.13 UC09: Einsatz von SGT

Erstellen einer neuen Scalable Group.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login auf DNA Center	DNA Center Dashboard wird angezeigt	DNA Center Dashbaord erscheint	OK
2	Zu den Einstellungen navigieren *Policy* → *Registry* → *Scalable Groups*	Liste der *Scalable Groups* wird angezeigt, inklusive der *Add Group* Schaltfläche.	Liste der *Scalable Groups* wird angezeigt, inklusive der *Add Group* Schaltfläche.	OK
2	Hinzufügen einer neuer Gruppe mithilfe der Schaltfläche *Add Group*	Neuer Dialog erscheint zum Anlegen einer *Scalable Group.*	Weiterleitung zum Cisco ISE zur Ansicht *Components* → *Security Groups.* (Eventuell muss man sich zuvor beim ISE zusätzlich einloggen.) Dort muss *Add* ausgewählt werden. Es erscheint ein Dialog zum Hinzufügen einer *Security Group.*	NOT OK
3	Neue Gruppe anlegen mit einem Namen	Im Dialog kann ein neuer Name für die *Scalable Group* eingegeben werden. Der Dialog wird mit *Speichern* geschlossen.	Ein neuer Name, ein Symbol und eine Beschreibung kann hinterlegt werden. Zusätzlich muss *Propagate to ACI* angewählt werden. Der Dialog wird mit *Anlegen* geschlossen	OK

4	Die Scalable Group ist erstellt.	In der Liste der Scalable Groups wird die neu erstellte Gruppe angezeigt.	Da man immernoch in der ISE Ansicht ist, muss zuerst zum alten Tab des DNA Centers gewechselt werden. Anschliessend muss die Seite neu geladen werden. Die neue erstellte Gruppe wird angezeigt.	OK

Tabelle 7.10: UC09: Einsatz von SGT

Noch nicht alle Funktionen können komplett im DNA Center erledigt werden. Ein Teil der Funktionen erfolgt weiterhin über die GUI der anderen Komponenten.

7.14 UC10-1: Infoblox verknüpfen

Durch die Integration des Infoblox DDI im DNA Center soll das IP-Adressen Management für neue Netzwerkkomponenten vereinfacht werden.

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	Login auf DNA Center	DNA Center Dashboard wird angezeigt	DNA Center Dashboard erscheint	OK
2	Zu IP Adress Manager Einstellungen navigieren über *Settings* → *System Settings* → *Settings* → *IP Adress Manager*	IP Adress Manager Einstellungen anzeigen	IP Adress Manager Einstellungen erscheinen	OK
3	Infoblox Informationen hinterlegen → Server Name: Infoblox, Server Url: https://10.22.0.21, Username: admin, Password: xxx, Provider: INFOBLOX). Mittels Apply die Eingaben bestätigen.	Eingaben werden angenommen.	Eingaben wurden angenommen und Verbindung zu Infoblox Server erfolgreich hergestellt.	OK

Tabelle 7.11: UC10-1: Infoblox verknüpfen

7.15 UC10-2: IP Adress Pool erstellen

IP Adress Pools auf dem Infoblox erstellen und mit DNA Center synchronisieren

Nr	Beschreibung	Erwartetes Ergebnis	Tatsächliches Ergebnis	Status
1	IP Adress Pools anzeigen über *Design* → *Network Settings* → *IP Adress Pools*.	IP Adress Pools sollten angezeigt werden.	Es werden vorhandene IP Adress Pools angezeigt.	OK

2	Mit einem Klick auf *Add IP Pool* kann ein neuer IP Pool hinzugefügt werden. Hierfür werden folgende Angaben benötigt: IP Pool Name, CIDR Prefix, IP Subnetz, Gateway IP Adresse, DHCP Server (optional), DNS Server (optional)	Fenster um IP Adress Pool hinzuzufügen erscheint	Fenster um IP Adress Pool hinzuzufügen ist erschienen	OK
3	Mit einem Klick auf Save wird der IP Adress Pool hinzugefügt und mit dem Infoblox Server synchronisiert	Übersicht über vorhandene IP Adress Pools wird angezeigt	Übersicht über vorhandene IP Adress Pools wird angezeigt mit vorher hinzugefügtem IP Adress Pool	OK

Tabelle 7.12: UC10-2: IP Adress Pool erstellen

Der Infoblox konnte im DNA Center relativ einfach hinterlegt werden. Das Erstellen eines IP Adress Pools auf dem DNA Center funktioniert gut und wird auch schnell mit dem Infoblox synchronisiert. Wird jedoch ein IP Adress Pool auf dem Infoblox erstellt, so ist es eher mühsam diesen neuen IP Adress Pool auf dem DNA Center anzuzeigen. Diese Synchronisation erfolgt nicht sauber. Es ist auf dem DNA Center zwar eine Import Funktion vorhanden, welche die IP Adress Pools vom Infoblox importieren sollte, aber nur mässig gut funktioniert. Jedes Netz welches importiert werden soll, muss einzeln erstellt und genaustens angegeben werden. Aus diesem Grunde sollte generell alles was im DNA Center erstellt werden kann, auf diesem erstellt werden und nicht manuell auf dem Infoblox.

8 Umsetzung

8.1 Labor Netzwerk Architektur

Mit der zur Verfügung gestellten Hardware ist die folgende Netzwerk Architektur entstanden.
Folgende zentrale Überlegungen sind eingeflossen:

- Campus Netzwerk mit mehreren Gebäuden, um das Wandern von Geräten zu simulieren.
- Mischung der zur Verfügung stehenden Switches (Catalyst 9300 & 3850) in der Fabric Edge Nodes, um Verhalten zu vergleichen.
- Management Netzwerk ist inbound. Kabelführung zu jedem Switch ist meistens von den Gegebenheiten in typischen Gebäuden nicht möglich.

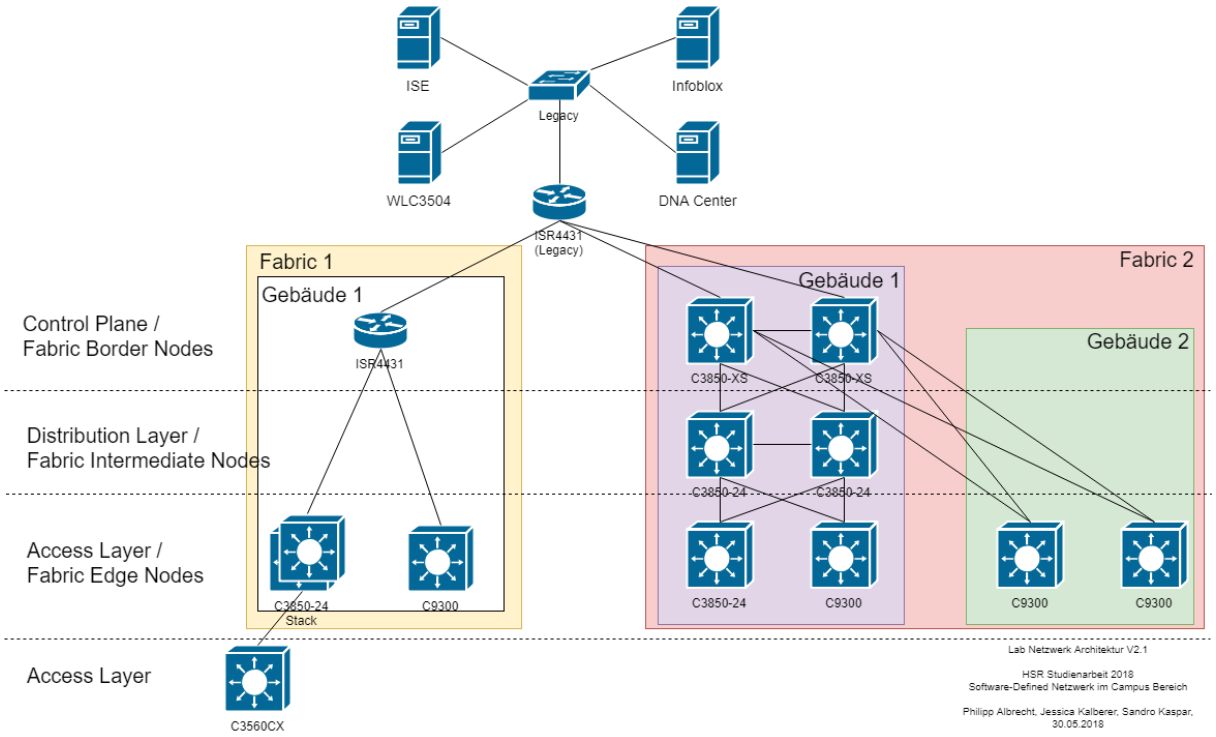


Abbildung 8.1: SDN Netzwerk Architektur

Unsere Netzwerk Architektur besteht aus drei Layer. Weitere Informationen über die Funktion des Fabric Border, Fabric Intermediate und Fabric Edge sind im Kapitel der Technologien beschrieben (siehe Kapitel 5.1.1 Campus Fabric).

8.1.1 Empfehlungen von Cisco

Die ursprüngliche Architektur wurde an die Empfehlungen von Cisco angepasst. Die Border sind wie in der Abbildung oben ersichtlich nun Catalyst 3850 und die Catalyst 9300 kommen erst als Edge zum Zug, anstatt schon als Border.

Platform	Supported supervisor	Supported fabric-facing interfaces	Edge node	Border node	Control plane node
Catalyst 3850 and 3650 Series	–	Onboard ports and 10G/40G network module ports	Yes–CVD verified	Yes–3850XS 10G fiber versions CVD verified (small scale deployments)	Yes–3850XS 10G fiber versions CVD verified (small scale deployments)
Catalyst 4500-E Series	Supervisor 8-E	Supervisor uplink ports	Yes–CVD verified	No	No
Catalyst 4500-E Series	Supervisor 9-E	Supervisor Uplink ports	Yes	No	No
Catalyst 9300 Series	–	Onboard ports and network module ports	Yes–CVD verified	Capable	Capable
Catalyst 9400 Series	Supervisor Engine-1	Supervisor and line card ports	Yes	No	No
Catalyst 6807-XL Switch and Catalyst 6500-E Series	Supervisor 6T and Supervisor 2T	Supervisor uplink ports (Supervisor 6T only) C6800 10G Series WS-X6900 Series	No	Yes–CVD verified	Yes–wired only
Catalyst 6880-X and 6840-X Series	–	Onboard ports and port card ports	No	Yes–CVD verified	Yes–wired only
Nexus 7700 Series	Supervisor 2E	M3 Series	No	Yes–CVD verified (For large scale 40G/100G deployments)	No (requires adding and manually configuring dedicated external control plane node)
Catalyst 9500 Series	–	Onboard ports and network module ports	Capable	Yes–CVD verified	Yes–CVD verified

Abbildung 8.2: SDA Switching Platform and Deployment Capabilities [4]

8.2 Verkabelungsplan

Auf nachfolgendem Verkabelungsplan sind die genauen Ports zwischen den Geräten ersichtlich, so dass für Konfigurationen die richtigen Interfaces schnell gefunden werden können.

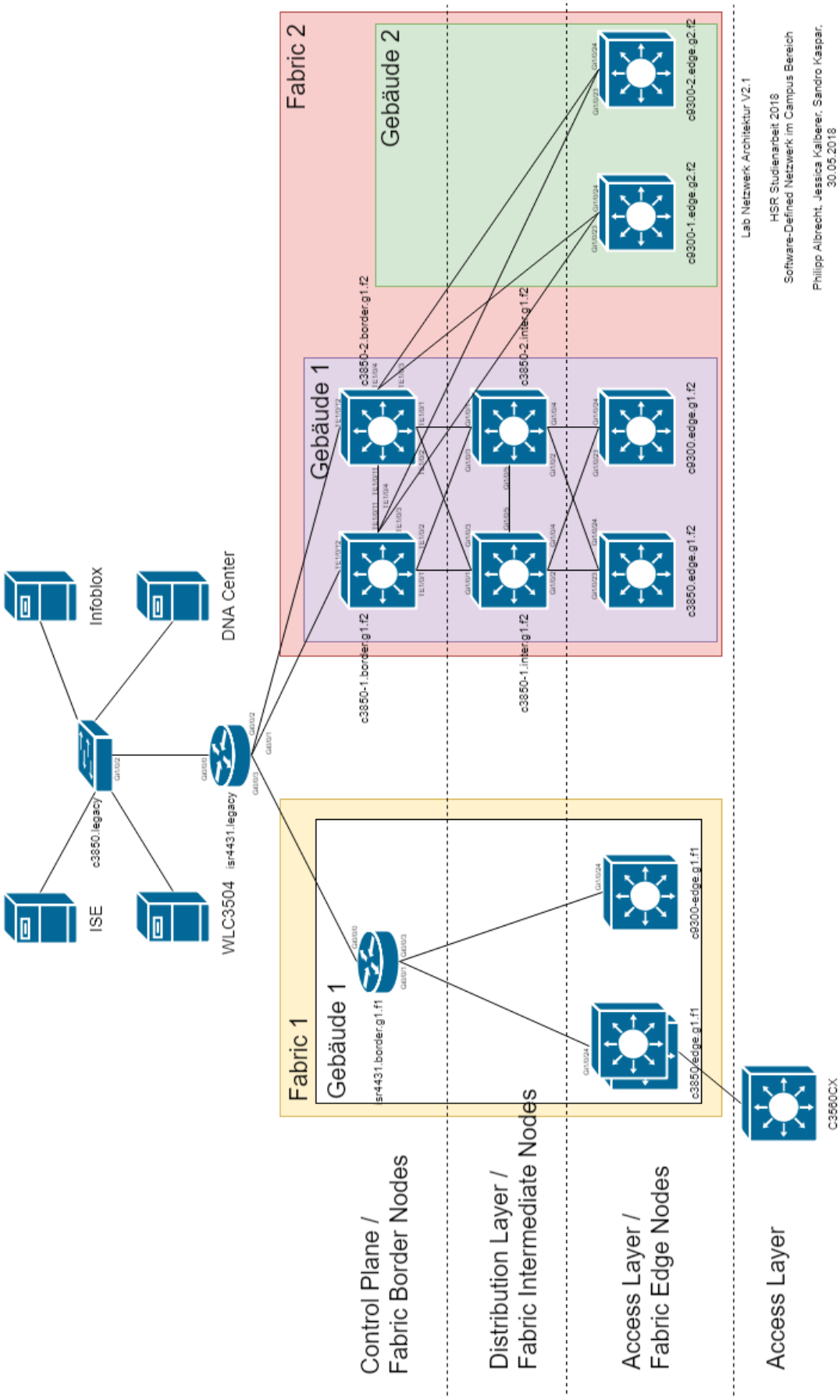


Abbildung 8.3: Lab Architecture with physical Interfaces

8.3 Netzwerkarchitekturen Vergleich

Hauptunterschiede zwischen der klassischen Netzwerkarchitektur und der "Modernen" Software-Defined Access Architektur.

- Bis zur Fabric Edge Nodes (Vergleichbar mit dem Access Layer) unterliegt ein L3 Netzwerk.
- Kein Einsatz von Spanning Tree Protocol (STP) oder Virtual Switching Systems (VSS) auf Distribution Layer notwendig, da das Underlay Netzwerk rein L3 ist und Routing Protokolle (BGP oder Open Shortest Path First (OSPF)) zum Einsatz kommen.
- Der Distribution Layer nimmt neu als Fabric Intermediate Nodes nur noch die Funktion als L3 Brücke beziehungsweise VXLAN Transporteur ein, anstatt die Grenze zwischen L3 und L2 zu sein. Die Fabric Intermediate Nodes sind optional.
- Während beim klassischen Design die logische Netzwerkarchitektur direkt Abhängig ist von der physikalischen Architektur, wird bei SDN die physikalische Netzwerkarchitektur von der logischen Architektur getrennt. Dabei wird von der Physical Fabric Topology oder auch dem Underlay und den entsprechenden L2 und L3 Overlay Network gesprochen.

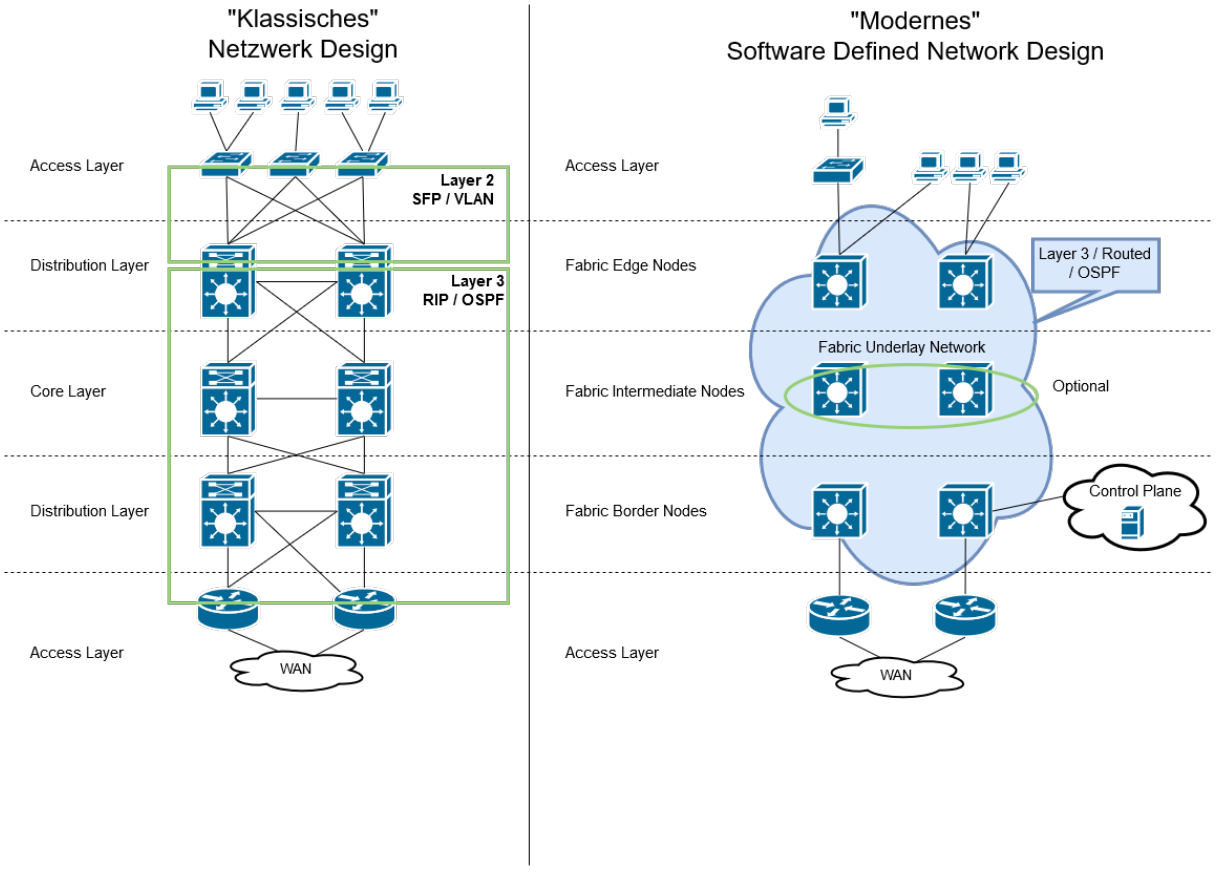


Abbildung 8.4: Netzwerk Architektur Vergleich

8.4 Maximale Skalierungen

Nachfolgend werden die aktuell maximalen Skalierungen des DNA Centers, sowie der Border und Edge Nodes aufgelistet. Diese Skalierungen sind vor allem in einer ersten

Evaluationsphase von Bedeutung, um zu entscheiden ob die Produkte mit den aktuellen maximalen Skalierungen überhaupt in Betracht gezogen werden können.

SD-Access construct	Maximum for single DNA Center cluster
Endpoints (wired+APs, excluding wireless clients)–across all fabric domains	25,000
Fabric nodes–across all fabric domains (routers, switches/switch stacks, WLCs)	2,500
Non-Fabric Nodes (Intermediate, Extension)	10,000
Access points–across all fabric domains (each AP counts as an endpoint)	4,000
IP pools–across all fabric domains	500
Sites	500
Fabric domains	20
Scalable group tags–across all fabric domains	1,000
Policies–across all fabric domains	1,000
Contracts–across all fabric domains	500

Abbildung 8.5: DNA Center Maximum Scale Constraints HA Cluster [4]

SD-Access construct	Maximum per fabric domain
Control plane nodes	2
Default border nodes	4

Abbildung 8.6: DNA Center Maximum Scale Constraints Fabric [4]

	Catalyst 3850/3650	Catalyst 9300	Catalyst 4500 Supervisor 8-E and 9-E	Catalyst 9400 Supervisor Engine-1
Virtual Networks (limited fabric-wide by deployed devices having lowest capability)	64	256	64	256
Scalable group tags	4,000	8,000	2,000	8,000
Security group ACLs	1,500	5,000	32,000	18,000

Abbildung 8.7: SDA Edge Node Scale Constraints [4]

	Catalyst 3850 (Fiber)	Catalyst 9300	Catalyst 9500	Catalyst 6800	Nexus 7700 Supervisor 2E	ASR 1000 and ISR 4000	CSR1000v
Virtual networks (limited fabric-wide by deployed devices having lowest capability)	64	256	256	512	500	4,000	–
Scalable group tags	4,000	8,000	8,000	30,000	64,000	64,000	–
Security group ACLs	1,500	5,000	18,000	30,000	64,000	64,000	–
Fabric control plane entries	4,000	4,000	96,000	25,000	Unsupported	200,000	200,000
IPv4 routes	8,000	8,000	48,000	1,000,000 (XL) 256,000 (non-XL)	1,000,000	4,000,000 (16GB) 1,000,000 (8GB)	–
IPv4 host entries	16,000	24,000	96,000	1,000,000 (XL) 256,000 (non-XL)	1,000,000	4,000,000 (16GB) 1,000,000 (8GB)	–

Abbildung 8.8: SDA Border Node Scale Constraints [4]

8.5 Anwendung und Vorgehen

Bei der Architektur und Planung der Konfiguration wurden die vorgegebenen maximalen Skalierungen berücksichtigt. Es ist aber wichtig zu erwähnen, dass sich diese maximalen Skalierungen in jedem neuen Release des DNA Centers wieder ändern können.
Im nächsten Kapitel wird der genaue Vorgang der Installation, sowie auch der Konfiguration des DNA Centers und des Campus Netzwerkes erläutert (Siehe: Kapitel 9 Vorgang 1 und Kapitel 10 Vorgang 2)

9 Vorgehen Versuch 1

Nachfolgend wird das Vorgehen des ersten Versuches in einer Grafik übersichtlich dargestellt. Die Blitze deuten dabei auf ein Hindernis bei welchem mehr Aufwand benötigt wurde hin und das rote X als einen fehlgeschlagenen Versuch, welcher abgebrochen werden musste.

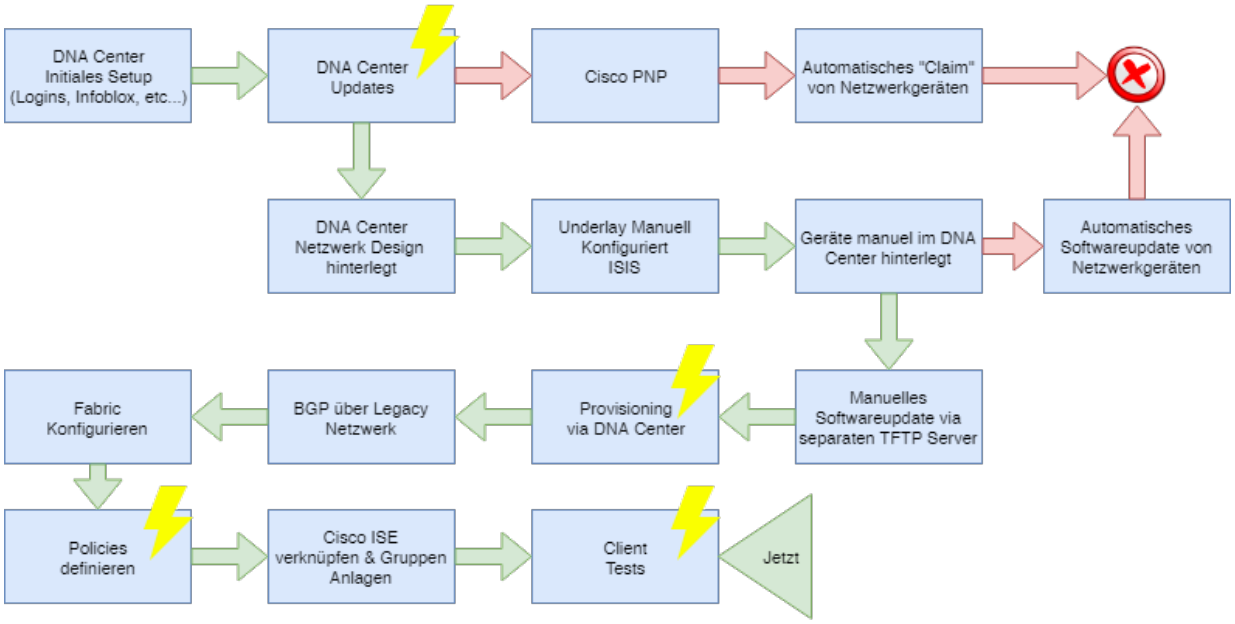


Abbildung 9.1: Grafische Übersicht über das Vorgehen beim ersten Versuch

9.1 DNA Center Initiales Setup

9.1.1 Installation

Die Installation des DNA Centers erfolgt direkt an der Konsole oder über die Cisco IMC. Dabei wird der maglev-config-wizard ausgeführt. Dieser Befehl sollte zu einem späteren Zeitpunkt nicht erneut ausgeführt werden, da er die Appliance unbrauchbar macht.
Wie in Kapitel 2[7] beschrieben werden folgende Angaben benötigt:

- Host IP Adresse
- Netmask
- Default Gateway IP adress
- DNS Servers
- Static Routes
- HTTPS Proxy
- Maglev Master Node IP
- Username, Passwort und Linux Passwort
- Administration Passphrase für das Web-Interface
- NTP Server
- Service Subnets

Im ersten Schritt 9.2 wird gewählt, ob ein neuer Cluster erstellt werden soll oder einem beigetreten werden soll. Bei der Testumgebung dieser Arbeit war nur eine Appliance verfügbar, weshalb schliesslich "Start a DNA-C Cluster" ausgewählt wurde.

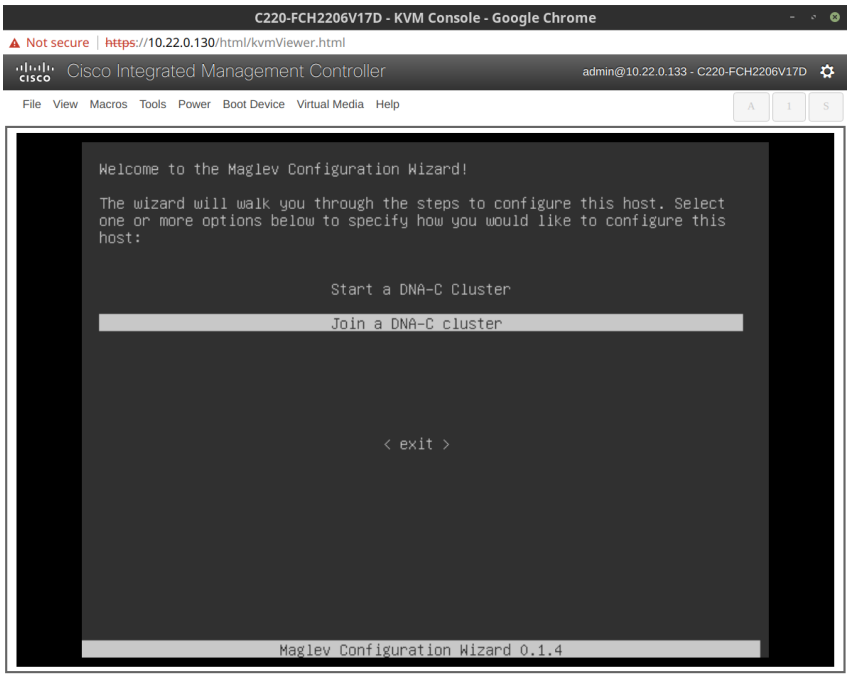


Abbildung 9.2: DNA Center Configuration Wizard - Start

Im nächsten Schritt muss die IP Konfiguration für die DNA Center Appliance angegeben werden. Es muss mindestens ein Interface konfiguriert werden und als Cluster Link definiert sein. Statische Routen können definiert werden, sind aber optional.

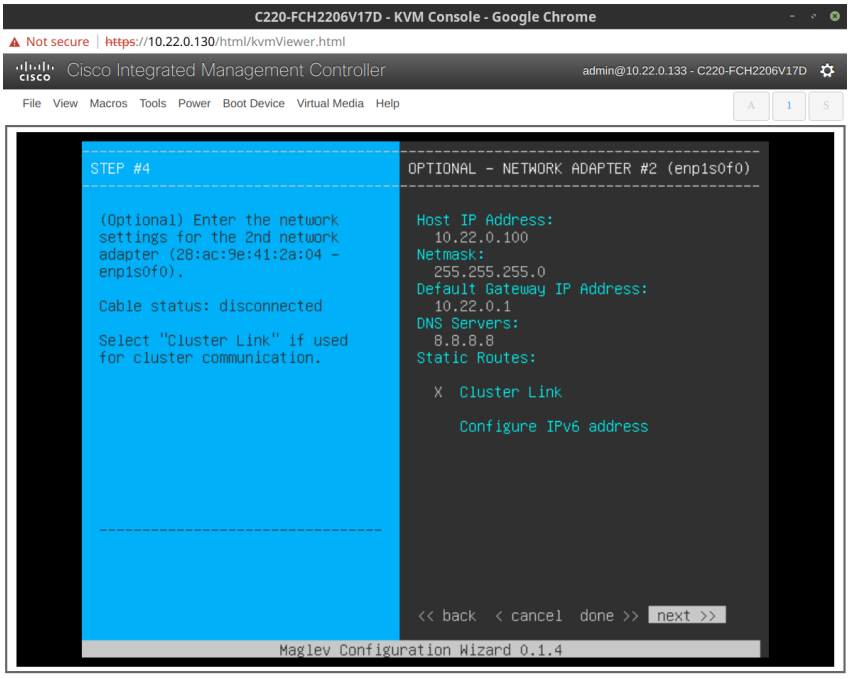


Abbildung 9.3: DNA Center Configuration Wizard - Entering Management IP

Im letzten Schritt des Wizards werden alle User Account Einstellungen festgelegt. Hier bei ist zu beachten, dass das "Linux Password" für den SSH Zugriff benötigt wird und die "Administrator Passphrase" für den Zugang zum Web Interface.

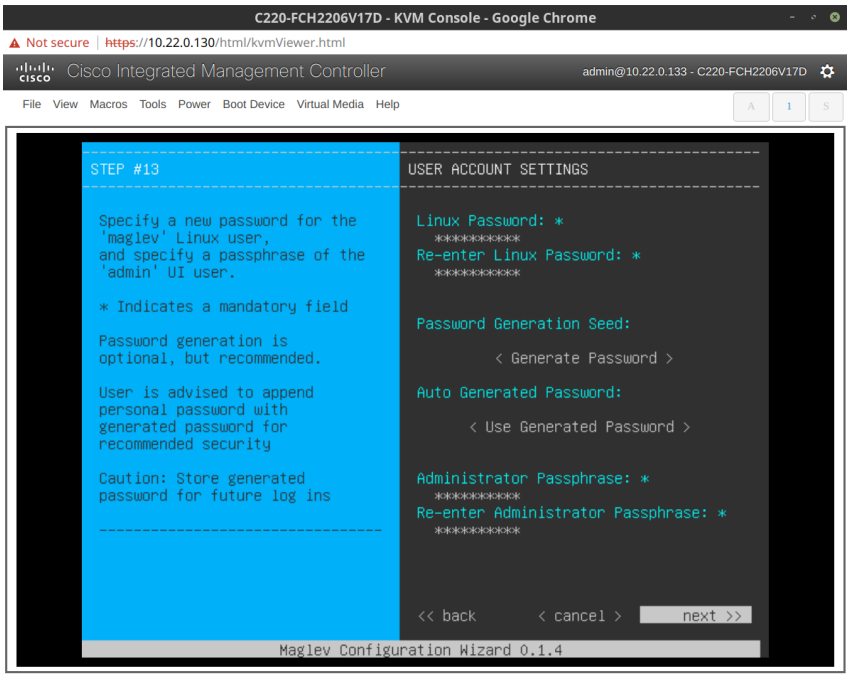


Abbildung 9.4: DNA Center Configuration Wizard - Entering Authentification Data

Nun wird das DNA Center aufgesetzt. Dieser Prozess dauert mehrere Stunden.

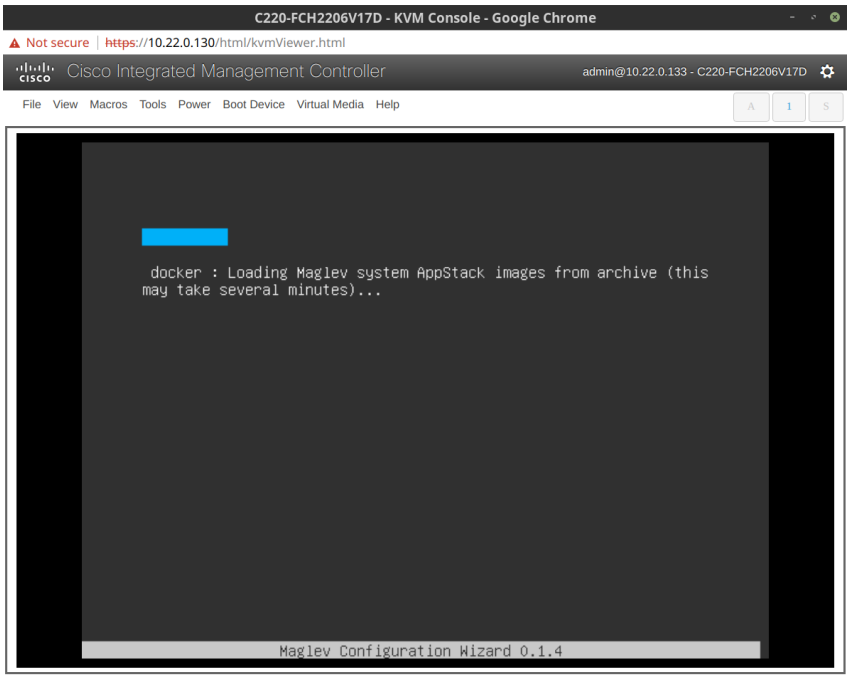


Abbildung 9.5: DNA Center Configuration Wizard - DNA Center uses docker

9.1.2 Setup Accounts

Nach dem der Wizard die Installation vollständig ausgeführt hat, ist das DNA Center Web-GUI verfügbar. Die Konfiguration kann nun über dieses weitergeführt werden.

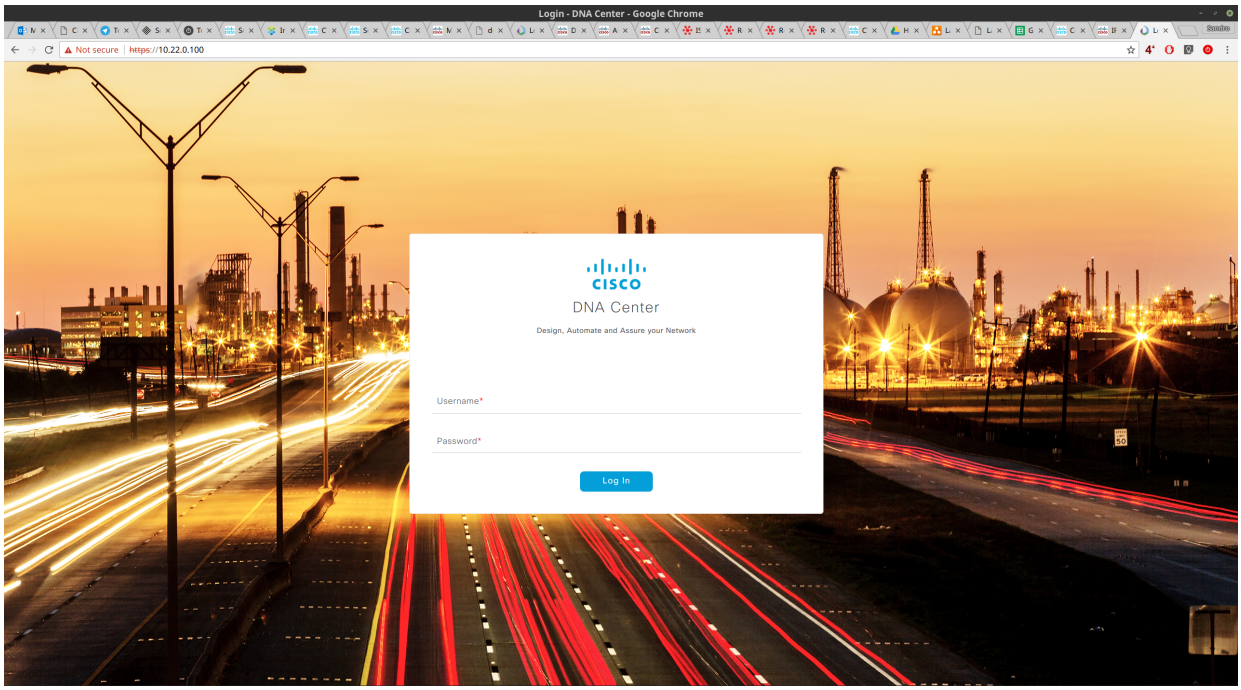


Abbildung 9.6: DNA Center Web GUI - Login Page

Gleich zu Beginn verlangt das DNA Center die Cisco Credentials die mit dem Smart Account verknüpft sind, in welchem die Lizenzen verwaltet werden. Diese Informationen können auch zu einem späteren Zeitpunkt noch eingetragen werden.

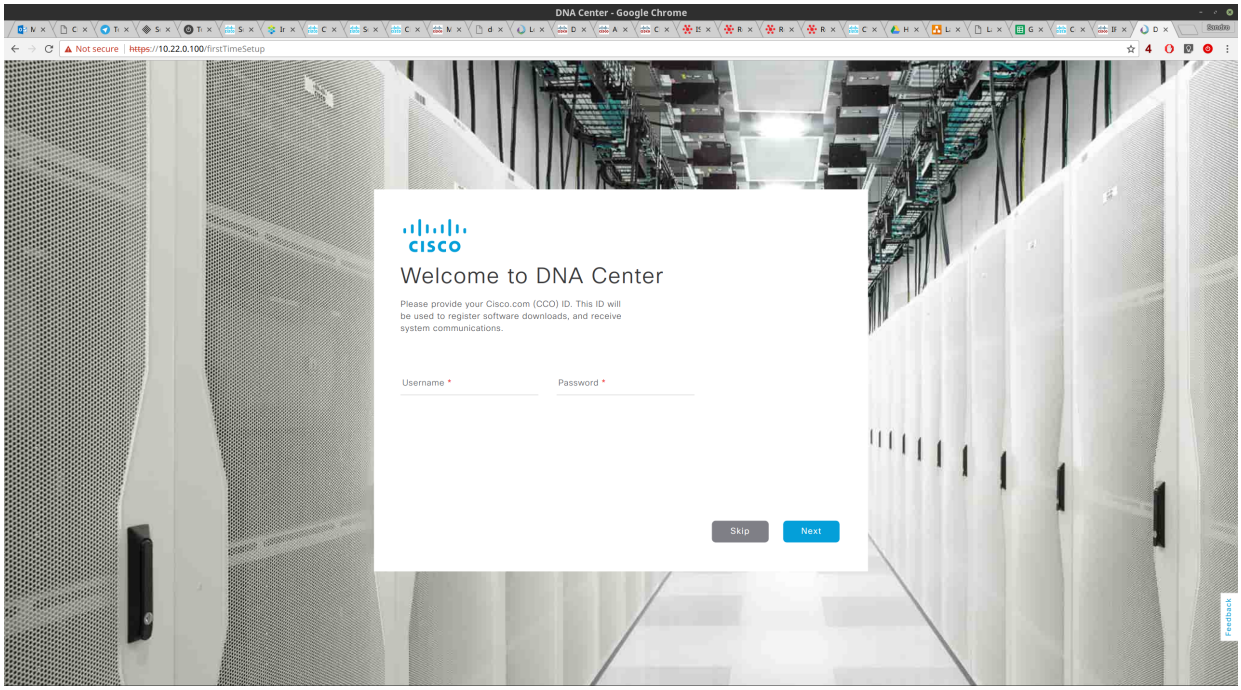


Abbildung 9.7: DNA Center Web GUI - Cisco Credentials for Licences

Im nächsten Schritt kann ein IPAM Server angegeben werden. Diese Einstellung kann ebenfalls später angepasst werden, weshalb wir diesen Schritt zu Beginn übersprungen haben.

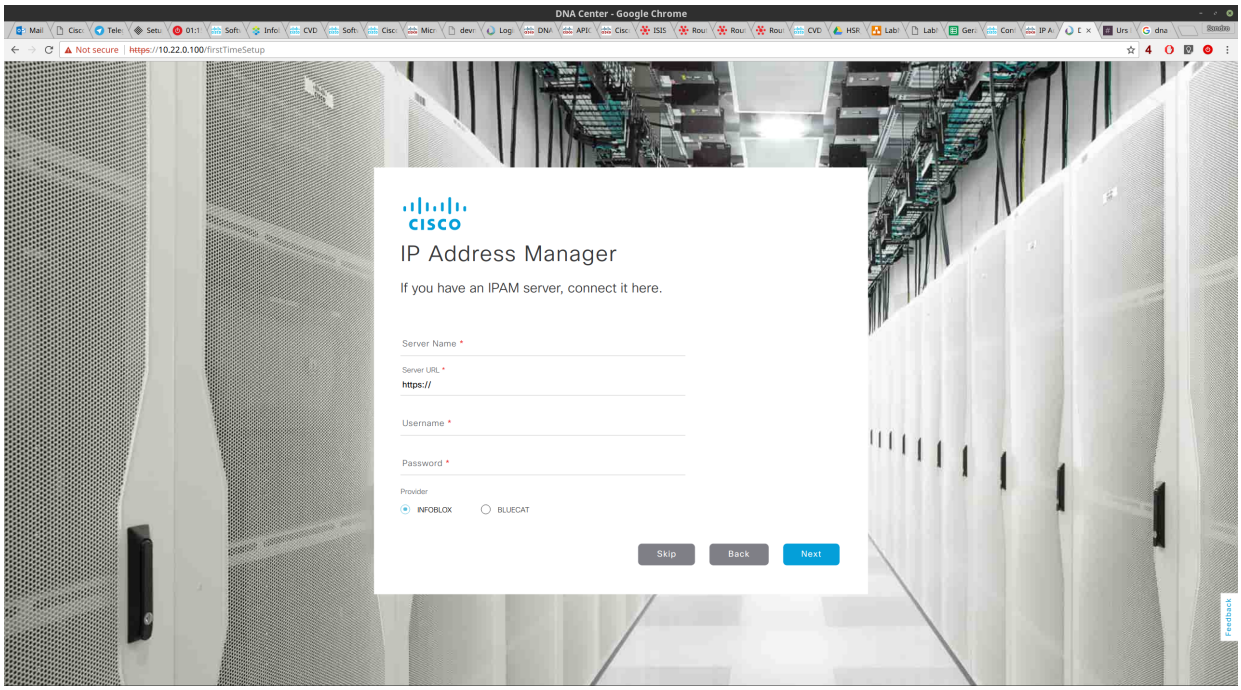


Abbildung 9.8: DNA Center Web GUI - Cisco IPAM

Danach ist die initiale Konfiguration beendet und das DNA Center Dashboard wird angezeigt.

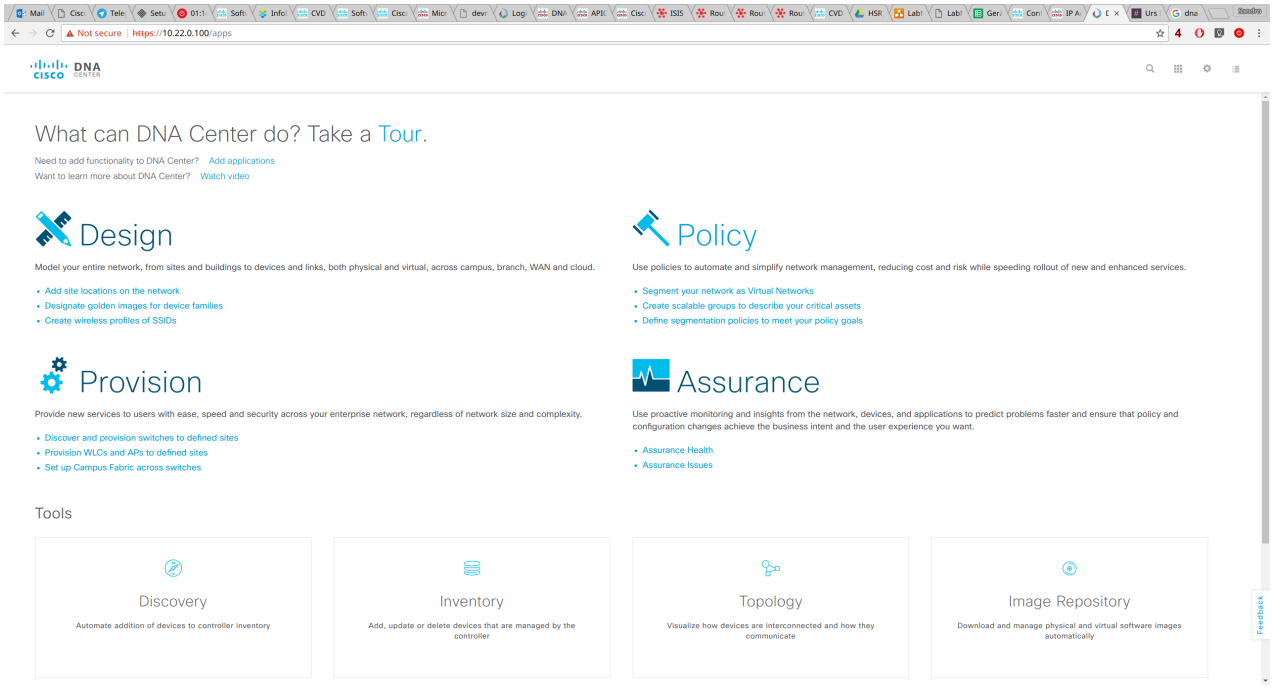


Abbildung 9.9: DNA Center Web GUI - Dashboard

9.2 DNA Center Updates

Da sich das DNA Center während dem Setup Prozess nicht automatisch aktualisiert und die DNA Center Versionen in relativ kurzen Intervallen released werden, ist es ratsam, gleich zu Beginn die aktuellsten Updates zu installieren.

Der Updateprozess birgt jedoch einige Hürden:

- System Updates müssen vor den Package Updates heruntergeladen und installiert werden.

  Werden die Package Updates vor dem System Update ausgeführt, können diese blockieren.
- Die Package Updates müssen in der richten Reihenfolge installiert werden.
- Die oben genannte Reihenfolge ist nicht direkt ersichtlich.
- Der Updatevorgang dauert mehrere Stunden.
- Der Updatefortschritt wird nicht angezeigt.
- Während dem Updateprozess können Teile des Web-GUIs Fehlermeldungen anzeigen oder überhaupt nicht mehr erreichbar sein.

Die Update Ansicht ist unter *Einstellungen (Zahnrad-Symbol)* → *System Settings* → *App Management* zu finden:

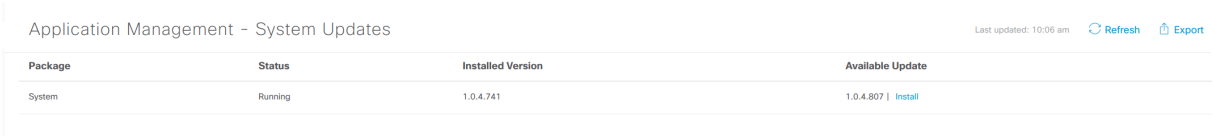


Abbildung 9.10: DNA Center App Management

9.2.1 Fehlgeschlagene Updates reparieren

Falls Updates in der falschen Reihenfolge installiert wurden oder aus anderen Gründen blockiert sind, können bereits heruntergeladene oder installierte Updates mit folgenden Befehlen entfernt und bereinigt werden. (am Beispiel von main-system-package:1.0.4.779):

```
$ maglev package status | awk '$3 ~ /[0-9]+/ {print $1":"$3}' |
grep -v "^system" | while read pkg;
do maglev catalog package delete $pkg;done
$ maglev system_update_package install main-system-package:1.0.4.779
```

9.2.2 Update Reihenfolge

Nach einem Update wurde die Reihenfolge von System und Package Updates angepasst. Vermutlich um den Administrator dazu zu bringen zuerst die System Updates zu installieren.

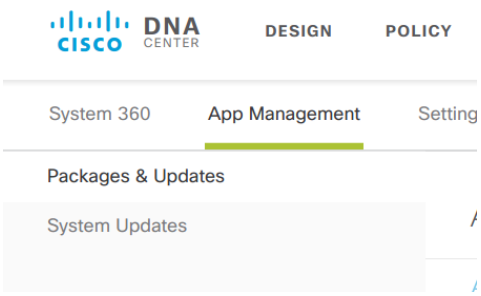


Abbildung 9.11: DNA Center App Management - Alte Menü Anordnung

9.2.3 Schwierigkeit: CCO Credentials für Updates notwendig

Application Packages und System Updates können nur installiert werden, wenn die CCO Credentials hinterlegt sind.

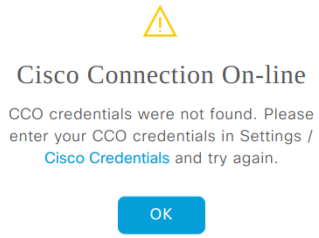


Abbildung 9.12: DNA Center Upgrade - Cisco Credentials required

9.2.4 Schwierigkeit: Unterschiedliche Versionsangabe

Beim Updatevorgang kann es zu Verwirrungen kommen, weil die Versionangabe von der Funktion *About* von der Version des System Packages abweicht.

Abbildung 9.13: DNA Center - About - Version

Oben wurde bei *About* die richtige Version 1.1.4 angegeben. Nachfolgend die Anzeige unter *System Updates*, welche eine andere Version anzeigt.

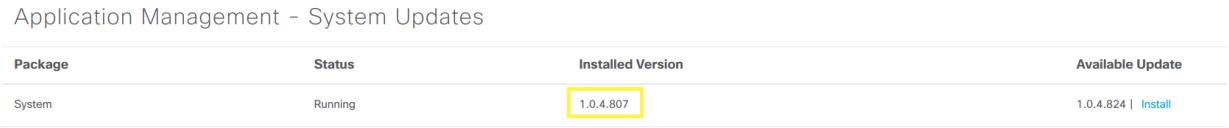


Abbildung 9.14: DNA Center - System Upgrade - Version

9.3 DNA Center Netzwerk Design

9.3.1 Network Hierarchy

Gemäss unserer Netzwerk Architektur wie in Kapitel 8.1 beschrieben, haben wir zwei Standorte. Rapperswil mit zwei Gebäuden und Jona mit einem Gebäude. In DNA Center können diese sehr einfach im Abschnitt *Design* → *Network Hierarchy* hinzugefügt werden.

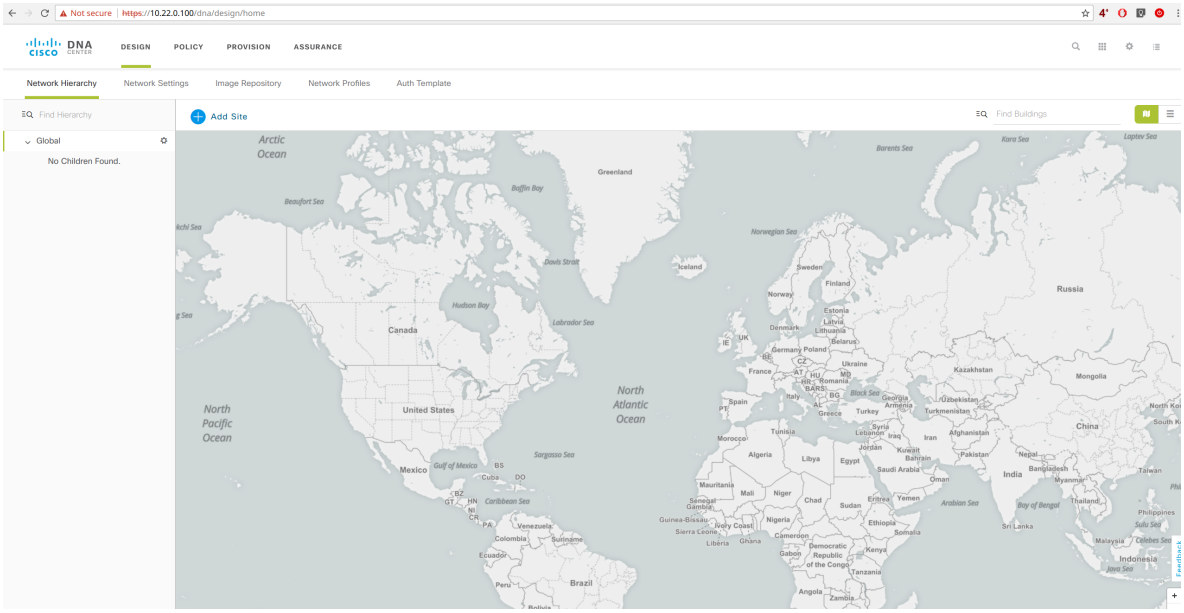


Abbildung 9.15: DNA Center Design Map

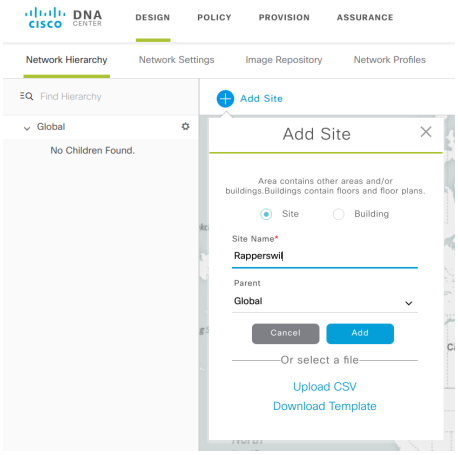


Abbildung 9.16: DNA Center Design - Standort hinzufügen

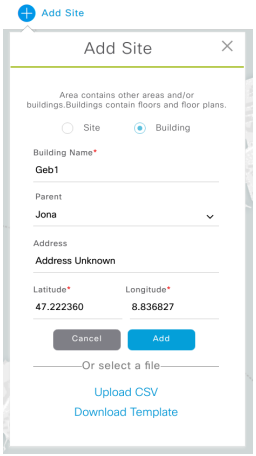


Abbildung 9.17: DNA Center Design - Gebäude können mit Koordinaten hinzugefügt werden.

Abbildung 9.18: DNA Center Design - Übersicht über alle Standorte und Gebäude

9.4 LAN Automation

Das DNA Center nutzt Plug and Play um automatisch Netzwerkgeräte in Betrieb zu nehmen und initial zu konfigurieren.

9.4.1 DHCP Konfiguration

Bei unserem ersten Versuch ein Seed-Device festzulegen, wurde vom DNA Center kein DHCP Server konfiguriert, weshalb wir diesen manuell auf Infoblox eingerichtet haben.

Cisco PnP kann über die DHCP Optionen 43 und 60 konfiguriert werden ([12]). In unserem Fall haben wir diese Optionen wie nachfolgend auf der Grafik erischtlich auf dem Infoblox Server konfiguriert. Diese sind nötig, damit das Netzwerkgerät den PnP Server findet.

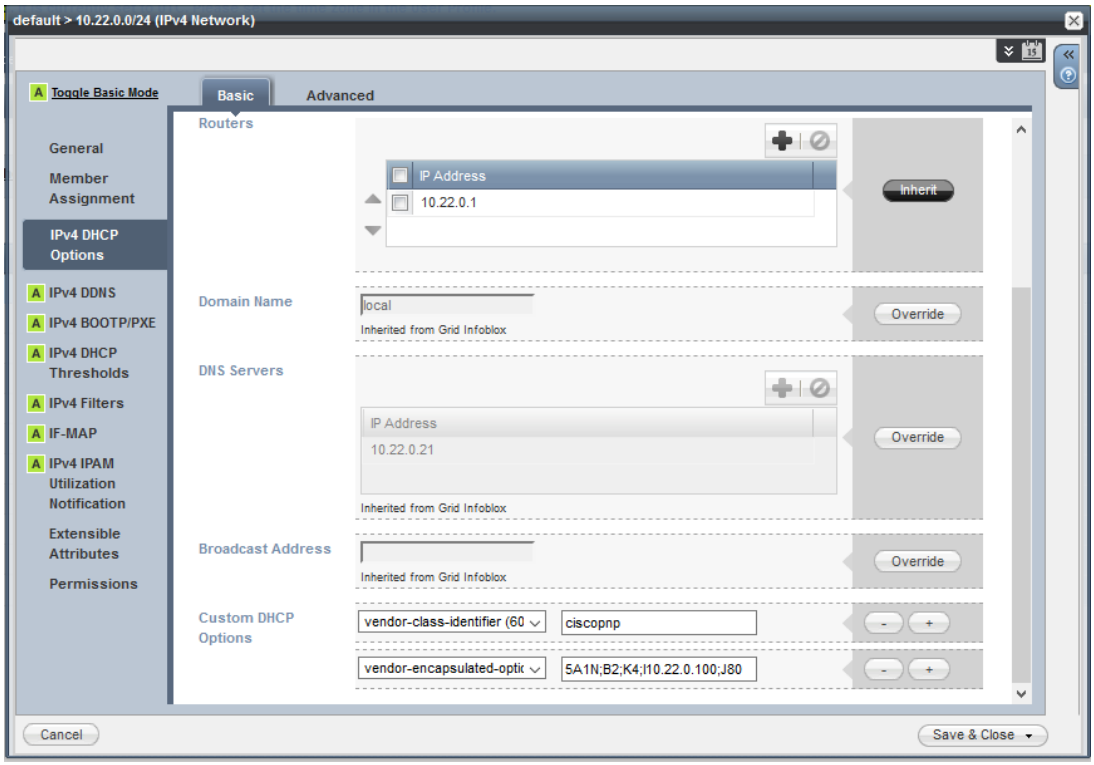


Abbildung 9.19: Infoblox Cisco PNP DHCP Option Konfiguration

Mit diesen Einstellungen hat PnP funktioniert. Allerdings nur sehr unzuverlässig und es kam oft zu Problemen, weshalb dies für viele Geräte mehrmals wiederholt werden musste. Hier ist zu empfehlen, nie mehr als ein Gerät gleichzeitig in Betrieb zu nehmen, damit es möglichst wenig Probleme gibt.

Uptime	First Seen	Status
2018-04-18 20:59:17.000382	2018-04-18 20:58:09.000507	UNCLAIMED
2018-04-18 21:10:11.000468	2018-04-18 21:10:04.000342	CERTIFICATE_INSTALL_REQUESTED
2018-04-18 21:00:21.000283	2018-04-18 20:59:12.000378	UNCLAIMED
2018-04-18 20:54:07.000560	2018-04-18 20:47:48.000666	ERROR_DURING_CERTIFICATE_INSTALL

Abbildung 9.20: DNA Center Provision - Fehlermeldungen in der "Unclaimed List"

9.5 Underlay Konfiguration

Das ISIS Routing im Underlay sollte vom DNA Center automatisch konfiguriert werden können. Da die entsprechende Funktion LAN Automation in unserem Versuch aber nicht funktionierte, wurde der Underlay manuell konfiguriert. Dazu wurden auf den Geräten IP Addressen auf den Loopback Interfaces und den P2P Links konfiguriert und entsprechende Router eingerichtet. Am Border wurde BGP verwendet, damit die Devices auch aus dem Legacy Netz erreichbar sind.
Dabei ist uns aufgefallen, dass die Geräte nur über eine IP-Base Lizenz verfügen. Für die Verwendung von BGP und VRF-lite ist aber die IP-Services Lizenz nötig.

Functions	LAN Base	IP Base	IP Services
Layer 2+	Enterprise access Layer 2 Wide range of Layer 2 access features for enterprise deployments supports Cisco StackPower technology	Complete Access Layer 2 Supports all Cisco Catalyst 2000 and Cisco Catalyst 3000 Layer 2 features, including hot standby protocols	
Layer 3	Static IP routing support Support for SVI	Enterprise access Layer 3 RIP, EIGRP stub, OSPF for routed access, PBR, IPv4 & IPv6 EIGRP stub routing, WCCP, IPV6 uRPF, IPV6 PBR, VRRPv3, Policy Classification Engine, HSRP v6	Complete access Layer 3 OSPF, EIGRP, BGP, IS-IS VRF-lite
Multicast	IGMP	IPV4 & IPV6 PIM routing	
Mobility	Supports Cisco Unified Wireless Networking mobility architecture	Supports Cisco Converged Access mobility architecture with CAPWAP termination at the access	
Manageability	Basic manageability Support for a wide range of MIBs, IPSLA Responder, and RSPAN, PnP, Autoconf, Interface Templates, Secure CDP	Enterprise access Layer 3, Flexible NetFlow for wired and wireless traffic EEM, GOLD-Lite, and Smart Install Director	
Security	Enterprise access security DHCP Snooping, IPSG, DAI, PACLs, Cisco Identity 4.0, NAC and 802.1x features	Complete access security Router and VLAN ACLs, private VLANs, complete identity and security; Cisco TrustSec® SXP and IEEE 802.1AE capable in hardware, Device Sensor	
QoS	Enterprise access QoS Ingress policing, Trust Boundary, AutoQoS, and DSCP mapping	Complete access QoS Support for all Cisco Catalyst 2000 and Cisco Catalyst 3000 QoS features, including per-VLAN policies	
Interoperability	Prime 2.1	Identity Services Engine (ISE 1.2/1.3), Mobility Services Engine (MSE 8.0), Improved WebUI	

Abbildung 9.21: IP Base and Services

Mit folgenden Befehlen war es möglich, eine IP-Services Test Lizenz zu aktivieren und somit die benötigten Features zu nutzen.

```
sh license right-to-use activate ipservices all acceptEULA
reload
show license right-to-use
```

9.6 "Claim" von Netzwerkgeräten

9.6.1 DNA Center Provision - Unclaimed Devices

Nachdem die Geräte via PnP eine initiale Konfiguration erhalten haben und die Konnektivität via ISIS und BGP sichergestellt war, wurden diese im Device Inventory als Unclaimed Devices angezeigt.

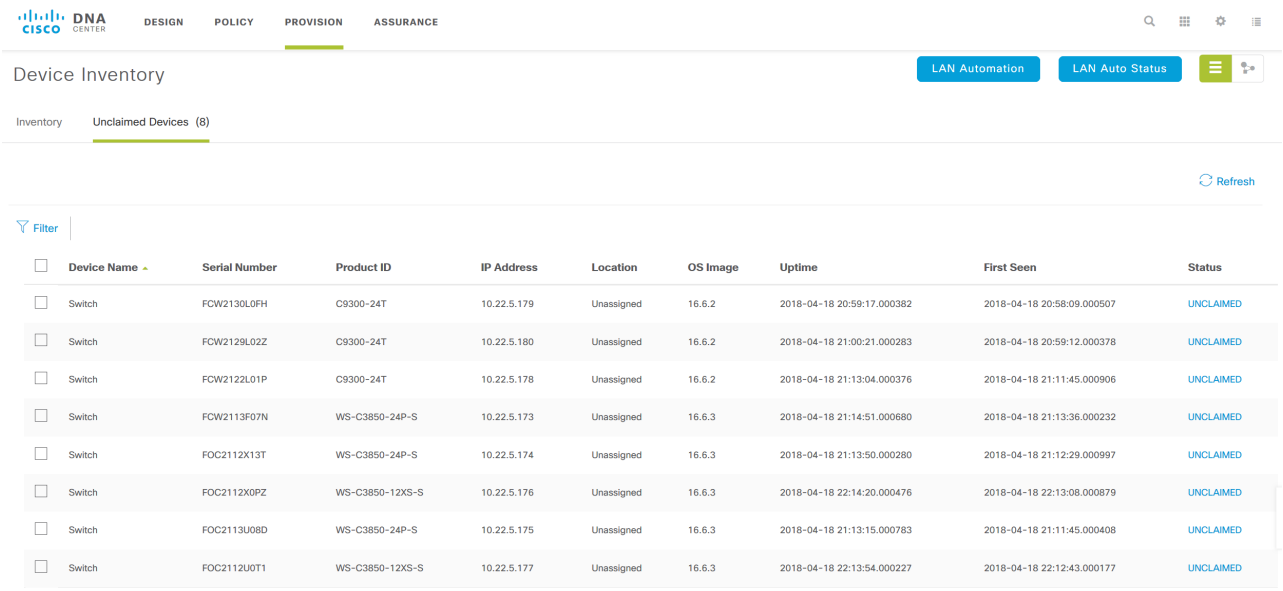


Abbildung 9.22: DNA Center Provision - Alle Geräte erfolgreich in der "Unclaimed List"

9.7 Netzwerkgeräte zu Inventory hinzufügen

Der nächste Schritt wäre nun, die Devices zu "Claimen". Dies bedeutet, dass die Geräte einem Standort zugewiesen werden und somit erste Konfigurationen erhalten können. Der Claim Prozess hat leider gar nie funktioniert. Das DNA Center reagierte einfach nicht auf die Eingabe.

9.7.1 Manuell Geräte im DNA Center hinzufügen

Da alle Versuche die Geräte automatisch hinzuzufügen gescheitert sind, entschieden wir uns den Vorgang manuell durchzuführen.
Im Dashboard klickt man dazu auf *Inventory* (siehe 9.23)

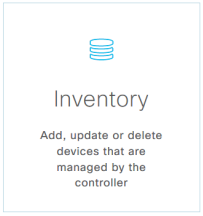


Abbildung 9.23: DNA Center Dashboard - Inventory Knopf

Anschliessend wählt man *Add* (siehe 9.24)

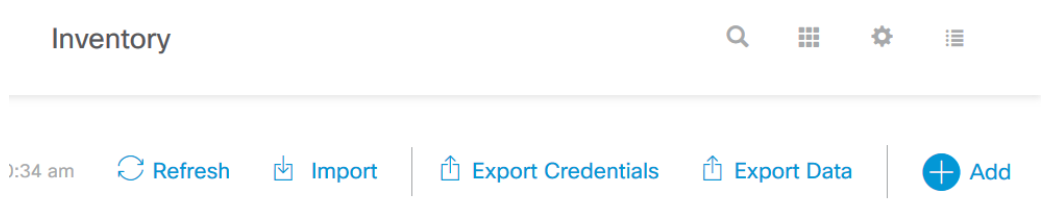


Abbildung 9.24: DNA Center Inventory - Gerät hinzufügen

Danach müssen folgende Informationen eingegeben werden:

- Device Type
- Device IP Name
- SNMP (Version, Read und Write Community)
- CLI (via SSH oder Telnet) *oder*
- NETCONF

Wir entschieden uns hier CLI via SSH zu wählen.

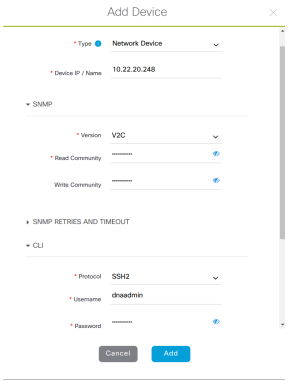


Abbildung 9.25: DNA Center Inventory - Formular Gerät hinzufügen

Danach erscheint das Gerät im Inventory. (siehe 9.26)

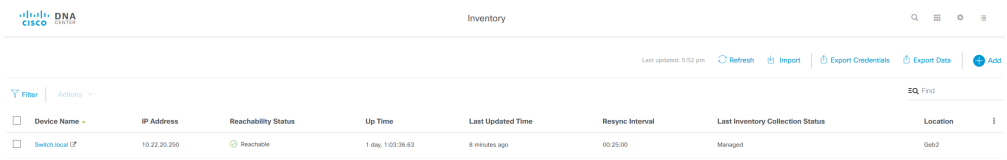


Abbildung 9.26: DNA Center Inventory - Neue Geräte in der Liste

9.8 Image Repository

Im DNA Center können Netzwerkgeräte automatisch aktualisiert werden. Sobald ein Gerät im Inventory erfolgreich hinzugefügt worden ist, sucht das DNA Center automatisch nach Updates. Allerdings nur, wenn ein CCO Account konfiguriert ist. Die verfügbaren Images sind unter *Desing* → *Global* → *Image Repository* zu finden.

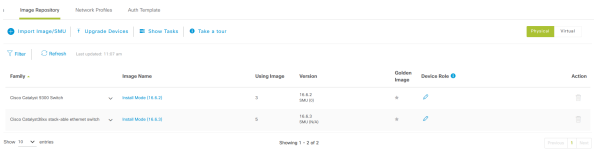


Abbildung 9.27: DNA Center Design - Image Respository

In diesem Image Repository kann das gewünschte Image mit einem "Golden Tag" versehen werden, worauf dieses heruntergeladen wird.

9.9 Automatisches Softwareupdate von Netzwerkgeräten

Die Softwareupdates von Netzwerkgeräten können im DNA Center unter *Provision* → *Devices* → *Inventory* durchgeführt werden. Ebenfalls wird hier angezeigt, welche Softwareversion zur Zeit auf dem Gerät installiert ist und ob diese aktuell ist.

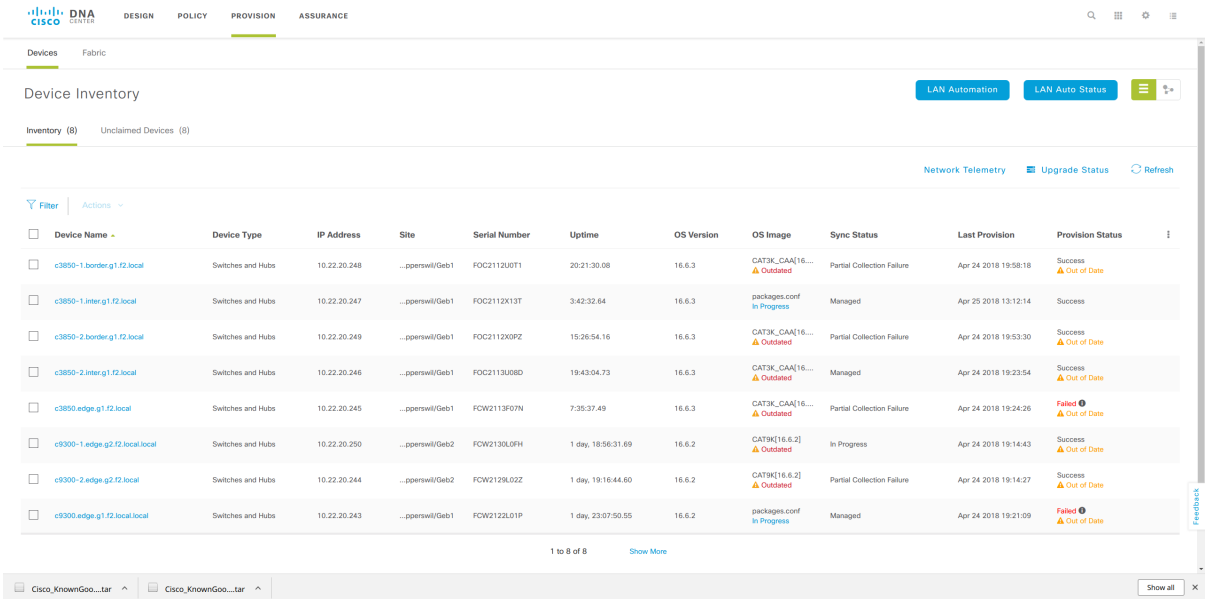


Abbildung 9.28: DNA Center Provision - Die OS Versionen sind outdated.

Das automatische Softwareupdate hat bei keinem von unseren Switches oder Routern geklappt. Nachfolgend eine kleine Übersicht über die verschiedenen Update Methoden und ausgeführten Versuche.

Methode	**Resultat**
DNA Center über HTTP und SFTP	Fehlgeschlagen (siehe 9.29)
CLI - HTTPS	Fehlgeschlagen (siehe 9.30)
CLI - SCP	Fehlgeschlagen (siehe 9.30)
CLI - TFTP	Erfolgreich (siehe 9.31)

Tabelle 9.1: Softwareupdate - Übersicht Methoden und ausgeführten Versuche

Beim Versuch die Softwareupdates im DNA Center über HTTP oder SFTP durchzuführen, wurden folgende Fehlermeldungen angezeigt.

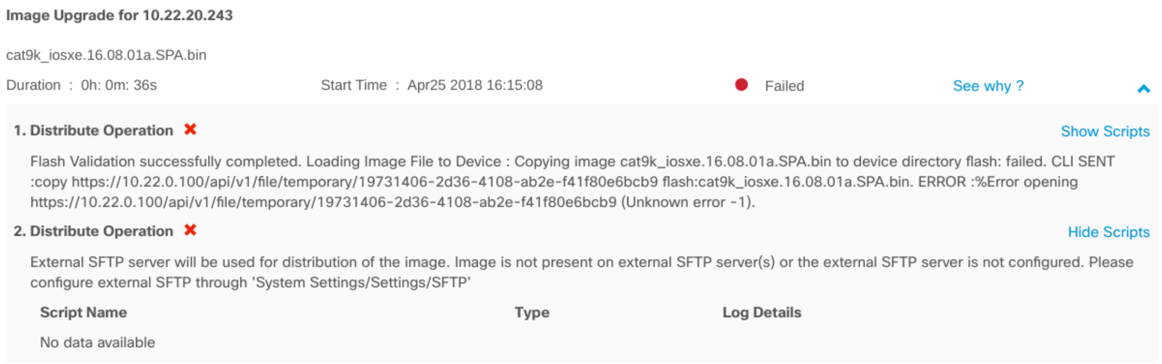


Abbildung 9.29: Fehlermeldung Updatevorgang via DNA Center

Die Upgrade Prozesse wurden schon beim Kopieren der einzelnen Images nach unterschiedlicher Dauer immer abgebrochen.

9.10 Manuelles Softwareupdate

Da wie oben beschrieben das automatische Update nicht funktionierte, wurde in einem nächsten Schritt versucht, die Updates manuell auf die Netzwerkgeräte zu installieren.

Abbildung 9.30: Firmwareupdate Switch via CLI HTTPs

Das Kopieren via HTTPS und SCP war sehr unzuverlässig und wurde nach einer gewissen Dauer abgebrochen.

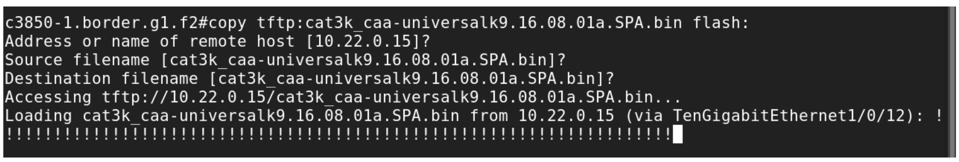


Abbildung 9.31: Firmwareupdate Switch via CLI TFTP

Mittels TFTP Server konnten die Devices schlussendlich erfolgreich aktualisiert werden.

9.11 Lizenzen

Die Lizenzen bezieht das DNA Center vom konfigurierten CCO Account.

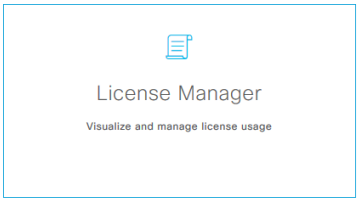


Abbildung 9.32: Der Licence Manager ist über das Dashboard erreichbar.

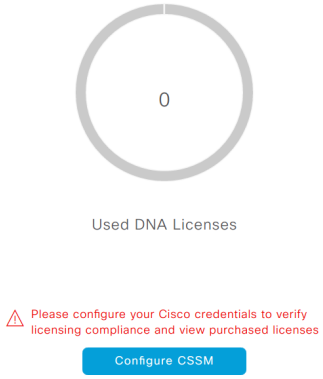


Abbildung 9.33: Ohne verlinkten CSSM Account können keine Lizenzen zugewiesen werden.

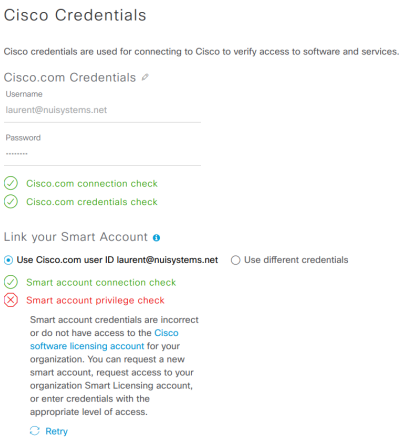


Abbildung 9.34: Der im DNA Center hinterlegte Cisco Account muss Zugriff zum entsprechenden Smart Account haben.

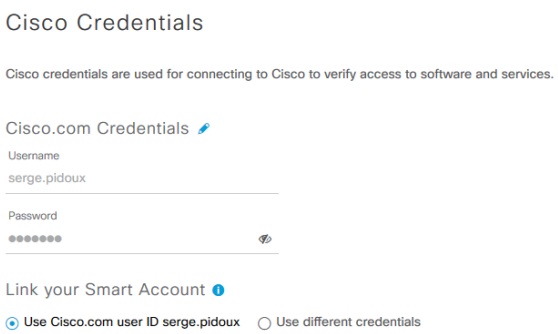


Abbildung 9.35: Der korrekt hinterlegte Account

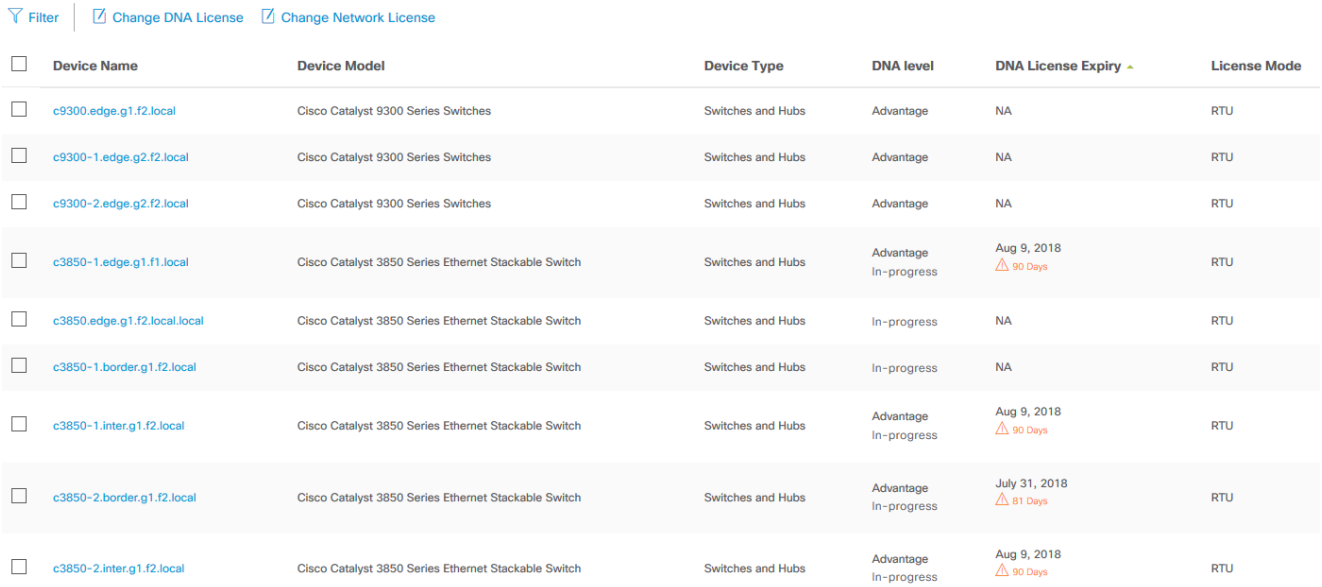


Abbildung 9.36: Übersicht über die den Netzwerkkomponenten zugewiesenen Lizenzen

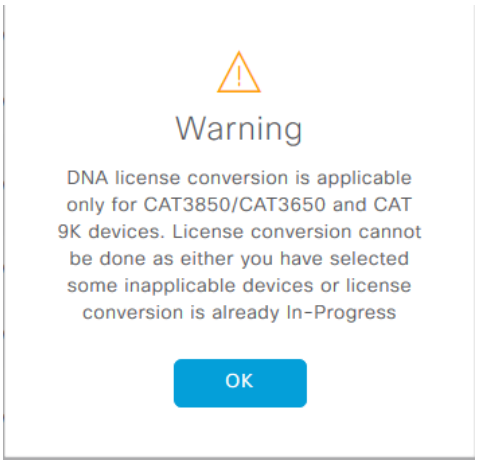


Abbildung 9.37: Nicht jedem Gerät kann eine Lizenz zugewiesen werden (Siehe Tabelle)

Geräteserie	Lizenzzuweisung möglich
Cisco Catalyst 9300 Series Switches	Ja
Cisco Catalyst 3850 Series Ethernet Stackable Switch	Ja
Cisco 4400 Series Integrated Services Routers	Nein

Tabelle 9.2: Netzwerkgeräte Lizenzzuweisung

9.12 Device Provisioning via DNA Center

Um den einzelnen Netzwerkgeräten einen Namen und die Basis Konfiguration zu geben, werden im DNA Center unter *Provision* → *Devices* die zu provisionierenden Geräte ausgewählt. Danach wird *Action* → *Provision Device* der Provision Vorgang gestartet.
Dabei wird die komplette Konfiguration, die das DNA Center für ein Device vorsieht auf dem Gerät konfiguriert. Sind Templates für den entsprechende Devicetyp konfiguriert worden, werden diese ebenfalls angewendet. Templates können im Template Editor erstellt und entsprechenden Gerätetypen zugewiesen werden.

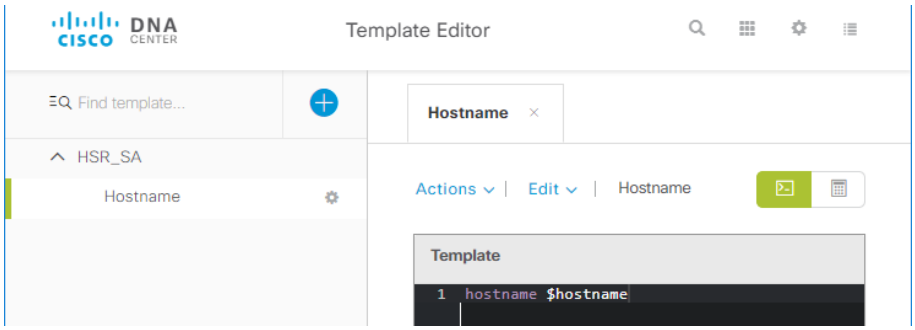


Abbildung 9.38: DNA Center - Template Editor

9.13 Fabric Konfigurieren

Nach der manuellen Konfiguration des Underlays, dem hinzufügen der Geräte, dem Update und dem Provisionieren, konnten wir endlich die Fabric konfigurieren.
Erreichbar ist das unter *Provision* → *Fabric*. Nachfolgend wird die Fabric des entsprechenden Standortes ausgewählt.
Den einzelnen Netzwerkgeräten werden nun mit Rechtsklick folgende Rollen zugeteilt:

- Border
- Border + CP (Control Plane)
- Edge

Nachdem alle Geräte der entsprechenden Fabric zugeteilt worden sind, kann die Konfiguration gespeichert werden und wird auf die Geräte geschrieben.

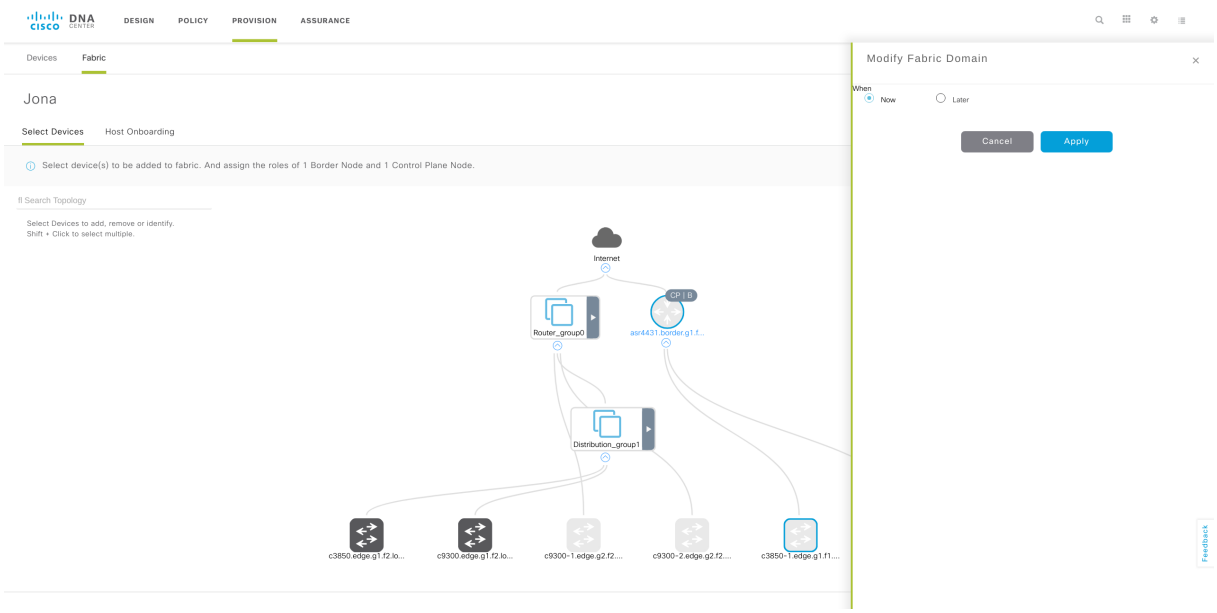


Abbildung 9.39: DNA Center Provision - Fabric - Nach der Zuteilung wird die Konfiguration auf die Geräte geschrieben.

Darstellung	Teil einer Fabric	Änderung ausstehend	Provisioniert	Bemerkung
Dunkelgrau	Ja	Nein	Nein	fremde Fabric
Hellgrau	Nein	Nein	Nein	
Grau mit blauem Rand	Ja	Ja	Nein	nicht deployed
Blau	Ja	Nein	Ja	aktuelle Fabric
Umrandung mit Pfeil	-	-	-	Gruppierte Geräte

Tabelle 9.3: DNA Center Provision - Fabric - Darstellung

9.14 DNA Center Reset

Da das Overlay Provisioning auch nach mehreren Versuchen nur teilweise funktioniert hatte, haben wir entschlossen, die Switches zusätzlich über das Out-of-Band Management zu verbinden, da dies in mehreren Videos von Cisco so erwähnt wird und im ersten Release zwingend nötig war.
Dazu benötigt das DNA Center ein zusätzliches Interface im Out-of-Band Management Netz. Um dieses einzurichten, muss der initiale Wizard erneut gestartet werden.

```
$ maglev-config-wizard #DO NOT EXECUTE THIS COMMAND
```

Als Folge dieses Befehls, nachdem alle Parameter eingegeben wurden, kam die folgende Meldung:

Abbildung 9.40: DNA Center - maglev-config-wizard - Fehlermeldung

Nach einem Neustart der Appliance erschien die folgende Meldung und das System bootete nicht mehr.

Abbildung 9.41: DNA Center - Boot Fehlermeldung

Es stellte sich heraus, dass wir den falschen Wizard gestartet hatten. Korrekt wäre der folgende Befehl gewesen:

```
$ sudo maglev-config update
```

Allerdings hätte auch der erste Befehl nicht dazu führen sollen, dass das System nicht mehr startet.

Neuinstallation

In der Folge war es nötig, dass DNA Center komplett neu zu installieren. Dazu ist ein entsprechendes ISO nötig, welches leider nicht mitgeliefert wird. Dieses kann bei Cisco via TAC Case angefordert werden. Mit dem ISO muss dann ein bootbarer USB Stick erstellt werden.

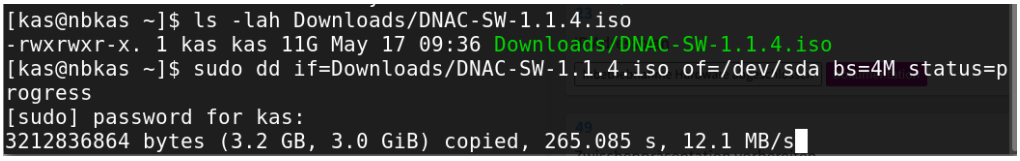


Abbildung 9.42: DNA Center - Neuinstallation - Installations ISO wird auf USB Drive kopiert

Anschliessend kann der USB-Stick in die Appliance gesteckt und diese gestartet werden. Die initiale Installation ist in Abschnitt 9.1.1 gezeigt.

Nach der Neuinstallation sind alle Daten und die Konfiguration gelöscht. Eine Option die Konfiguration beizubehalten gibt es nicht.

10 Vorgehen Versuch 2

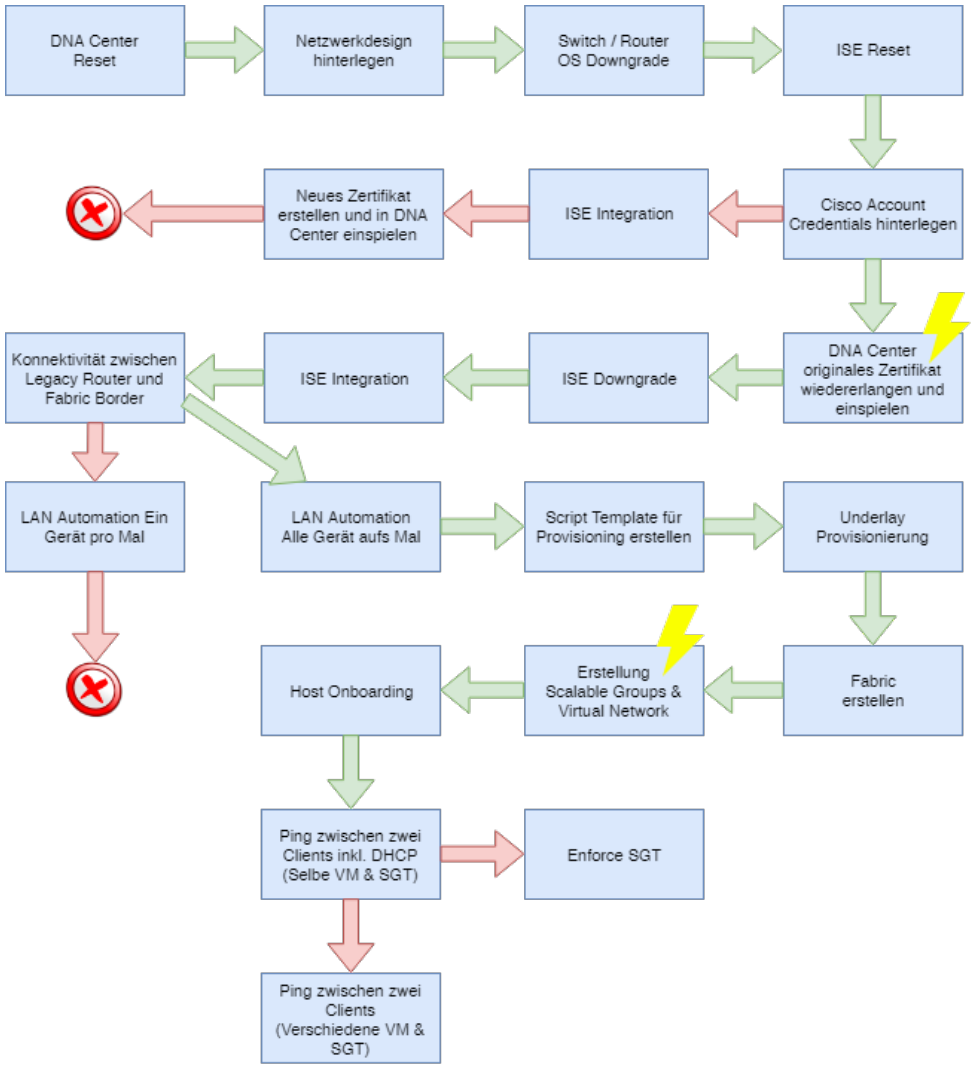


Abbildung 10.1: Grafische Übersicht über das Vorgehen beim zweiten Versuch

10.1 Vorarbeiten

Damit im zweiten Versuch keine Probleme mit bestehenden Konfigurationen entstehen, haben wir den alle Konfigurationen in Infoblox gelöscht und ISE auf den Werkszustand zurückgesetzt.
Des Weiteren wurde auf allen Netzwerkdevices die IOS-XE Version 16.6.3 installiert, da gemäss Patrick Mosimann von Cisco nur diese Version mit dem aktuellen DNA Center kompatibel ist.

10.1.1 ISE reset

Um die Störungen durch alte Konfigurationen zu vermeiden, wurde das Cisco ISE Center ebenfalls zurückgesetzt. Dies kann einfach mittels eines Befehls durchgeführt werden.

ISE/admin# *applicaiton reset-config ise*

```
ISE/admin# application reset-config ise
Initialize your Application configuration to factory defaults? (y/n): y
Leaving currently connected AD domains if any...
Please rejoin to AD domains from the administrative GUI
Retain existing Application server certificates? (y/n): y
Reinitializing local configuration to factory defaults...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping PassiveID WMI Service...
Stopping PassiveID Syslog Service...
Stopping PassiveID API Service...
Stopping PassiveID Agent Service...
Stopping PassiveID Endpoint Service...
Stopping PassiveID SPAN Service...
Stopping ISE pxGrid processes...
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
Stopping ISE Sxp Engine Service...
Stopping TC-NAC Service ...
Error: No such container: irf-core-engine-runtime
irf-core-engine-runtime is not running
```

Abbildung 10.2: Cisco ISE Reset

10.2 DNA Center Update

Wie im ersten Versuch, haben wir das DNA Center nach der Installation auf den aktuellsten Stand geupdated. Dieser Vorgang wurde im Abschnitt 9.2 gezeigt. Dies war mittlerweile die Version 1.1.6. Im ersten Versuch arbeiteten wir mit den Versionen 1.1.4 und 1.1.5.

10.3 DNA Center Netzwerk Design

Das Netzwerkdesign wurde analog unserem ersten Versuch in Abschnitt 9.3 erstellt.

10.4 ISE Integration

Bei der Integration des ISE wollten wir gleich vorgehen, wie im ersten Versuch. Es stellt sich aber heraus, dass im Release 1.1.6 in Kombination mit ISE 2.4 geprüft wird, ob das DNA Center über ein Zertifikat verfügt, das den Hostname oder die IP des DNA Centers im Common Name hat. Aus diesem Grund haben wir das Zertifikat des DNA Centers durch eines ersetzt, dass diese Bedingung erfüllt.

Before You Begin

Before attempting to integrate ISE with Cisco DNA Center, be sure you have met the following pre-requisites:

- You have deployed one or more ISE version 2.3 hosts on your network. If you have a multi-host ISE deployment, integrating with the ISE admin node is recommended.

  For information on installing ISE, see the Cisco Identity Services Engine Installation Guide, Release 2.3.
- The PxGrid service must be enabled on the ISE host with which you plan to integrate DNA Center. The procedure below explains how to enable this service.
- The ISE admin node on which PxGrid is enabled must be reachable on the IP address of the eth0 interface of ISE from DNA Center.
- The ISE node can reach the fabric underlay network via the appliance NIC.
- The ISE node has SSH enabled
- The ISE CLI and GUI user accounts must use the same username and password
- The ISE admin node certificate must contain the ISE IP address or fully-qualified domain name (FQDN) in either the certificate subject name or the SAN.
- The DNA Center system certificate must contain the DNA Center appliance IP or FQDN in either the certificate subject name or the SAN.

Abbildung 10.3: ISE Integration Prerequirements [7]

Das Zertifikat kann unter *Settings* → *Settings* → *Certificate* → *Replace Certificate* ausgetauscht werden. Es ist möglich Zertifikate im PEM Format oder als PKCS Datei hochzuladen.

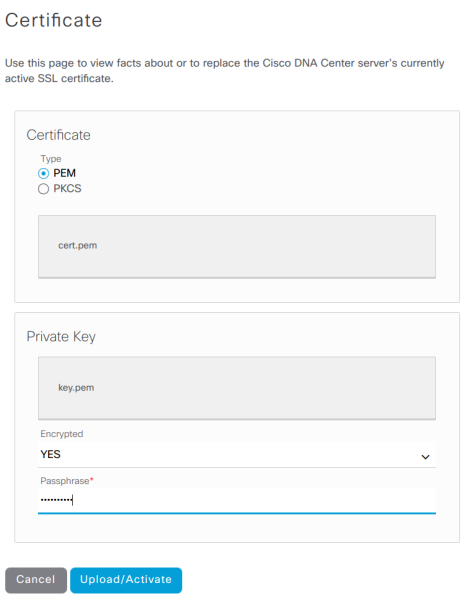


Abbildung 10.4: DNA Center Certificate Replacement

Nachdem das Zertifikat durch ein self-signed Zertifikat ausgetauscht wurde, welches die Bedingung erfüllt, dass die IP oder der Hostname im Common Name sein muss, funktionierte die ISE Integration ohne weitere Probleme.

10.5 LAN Automation

Bevor die LAN Automation gestartet werden kann, müssen folgende Bedinungen für das Seed Device erfüllt sein:

- Aktives SSH
- IP Konnektivität

10.5.1 Verbindung zwischen Legacy Router und Border Switch

Damit die LAN Automation gestartet werden kann, muss zuerst ein Seed Device eingerichtet werden, dass vom DNA Center aus erreichbar ist. Dies kann mit untenstehenden Befehlen über ein temporäres VLAN erreicht werden.

```
# interface lo0
#   ip address 10.22.30.1 255.255.255.255
#
# interface Te1/0/12
#   switchport trunk native vlan 100
#   switchport mode trunk
#
# interface vlan 100
#   ip adress 10.22.31.1 255.255.255.252
```

```
#
# ip route 10.22.0.0 255.255.255.0 10.22.31.2


# interface GigabitEthernet0/0/1.100
#  encapsulation dot1Q 100
#  ip address 10.22.31.2 255.255.255.252
#
# ip route 10.22.30.1 255.255.255.255 10.22.31.1
```

10.5.2 Discovery

Da der oben konfigurierte Border Router als Seed Device genutzt werden soll um die restlichen Geräte zu finden und zu deployen, muss dieses im DNA Center bekannt gemacht werden. Am einfachsten geht dies über die Discovery Funktion. Diese kann mittels *Discovery → New Discovery* eingerichtet werden. Die Discovery kann gemäss untenstehender Grafik konfiguriert werden.

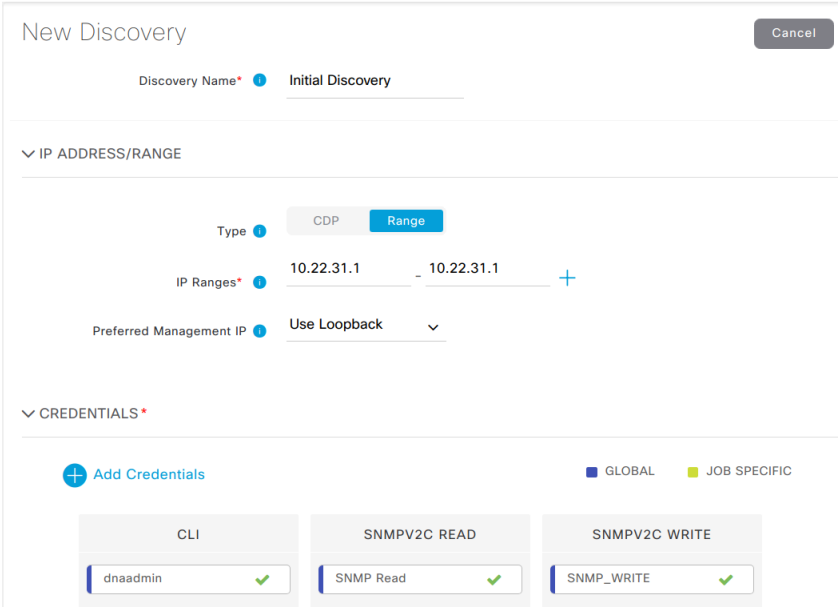


Abbildung 10.5: DNA Center Discovery

Sobald das Device gefunden wurde, erscheint dieses im Inventory. Damit dieses als Seed Device verwendet werden kann, ist zuerst ein Provisioning wie in 9.12 beschrieben nötig und das Device muss einer Fabric hinzugefügt werden 9.13.
Beim Provisioning ist aber aufgefallen, dass es Probleme mit der Verbindung zwischen dem Border Switch und dem ISE gibt. Patrick Mosimann hat uns dann erklärt, dass das DNA Center in den aktuell verfügbaren Versionen ausschliesslich mit ISE in der Version 2.3 kompatibel ist.
Unglücklicherweise war in unserer Lab Umgebung die Version 2.4 installiert. Ein Downgrade ist leider nicht möglich, weshalb die virtuelle Maschine ausgetauscht werden musste und der ISE erneut ins DNA Center integriert werden musste.

10.5.3 LAN Automation PnP

Nun konnte die eigentliche LAN Automation gestartet werden. Dabei wird, wie in untenstehender Grafik gezeigt ein Seed Device ausgewählt und definiert, auf welchen Interfaces DHCP Requests der anderen Devices beantwortet werden. Zudem muss ein IP Pool angegeben werden, der für folgende Zwecke verwendet wird:

- DHCP Pool während dem PnP Vorgang
- Loopback Interfaces der Devices
- Netze für Point to Point Links

Dabei ist zu beachten, dass die Unterteilung des IP Pools nicht optimal ist. Unabhänig von der Grösse des Pools werden beispielsweise nur 30 Adressen für den DHCP Pool reserviert, was in einer grossen Umgebung ein Problem darstellen könnte.

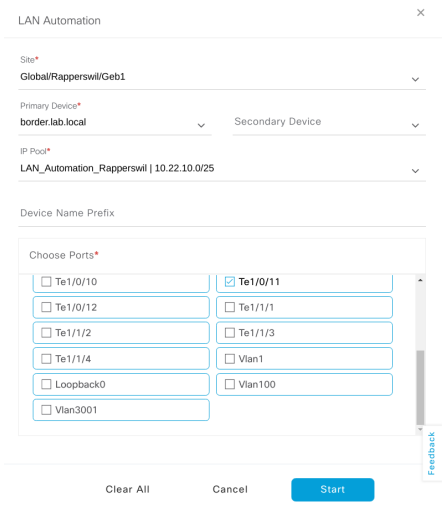


Abbildung 10.6: DNA Center - LAN Automation

Wir haben dann die LAN Automation gestartet. Dies konfiguriert auf dem Seed Device einen DHCP Server. Werden nun die Konfiguration auf anderen Netzwerkgeräten gelöscht und diese neu gestartet, senden diese DHCP Request, die vom Seed Device beantwortet werden. Die Antworten verweisen auf das DNA Center als PnP Server. Die Geräte senden nur DHCP Requests, wenn Sie im Zustand sind, der auf untenstehendem Bild ersichtlich ist.

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

Abbildung 10.7: Cisco Switch - Initial Config - Versucht DHCP und PnP zu machen, solange der Dialog aktiv ist.

Während des PnP Prozesses wird das Zertifikat, sowie die CA (Certificate Authority) des DNA Centers auf die Netzwerkgeräte kopiert. Dies ist nötig, damit die Verbindung auf HTTPS umgestellt werden kann. Nach diesem Schritt blieb der Setup Prozess jeweils mit folgender Meldung stehen:

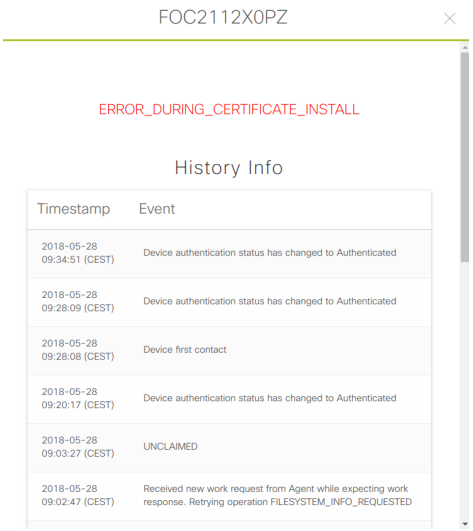


Abbildung 10.8: LAN Automation - PnP Error

Es stellte sich heraus, dass das Problem war, dass unser self-signed Zertifikat nicht von der DNA Center CA signiert war und die Netzwerkgeräte daher nicht validiern konnten ob dieses gültig ist. Leider konnte uns auch Patrick Mosimann von Cisco nicht sagen, wie wir dieses Zertifikat signieren können, das ursprüngliche Zertifikat wiederherstellen können oder das Problem anderweitig lösen können. Gemäss dem Installation Guide von Cisco [7] kann hier auch ein Zertifikat verwendet werden, dass von einer "Well-Known Certificate Authority" signiert ist. Aus diesem Grund haben wir das Zertifikat auch durch ein korrekt von Lets Encrypt signiertes Zertifikat ausgetauscht. Patrick konnte uns aber nicht sagen, ob diese Authority auf dem Gerät bekannt ist. Auch das korrekt signierte Zertifikat wurde nicht akzeptiert und der PnP Prozess konnte nicht weitergeführt werden. Aus diesem Grund haben wir uns via SSH auf die Appliance eingelogged und dort nach dem ursprünglichen Zertifikat oder der CA gesucht. Nach einer Weile wurden wir fündig und fanden das alte Zertifikat und die CA:

```
# $ sudo ls -lah /etc/maglev/.pki/
# [sudo] password for maglev:
# total 140K
# drwxr-xr-x 2 4.0K May 21 06:20 .
# drwxr-xr-x 4 4.0K May 21 06:20 ..
# -rw-r--r-- 1 1.3K May 17 09:09 apiserver.crt
# -rw------- 1 1.7K May 17 09:09 apiserver.key
# -rw-r--r-- 1 1.2K May 17 09:09 apiserver-kubelet-client.crt
# -rw------- 1 1.7K May 17 09:09 apiserver-kubelet-client.key
# -r--r--r-- 1 1.1K May 17 08:49 ca.crt
# -rw-r--r-- 1 1.7K May 17 08:49 ca.key
# lrwxrwxrwx 1   23 May 17 08:49 ca-key.pem -> /etc/maglev/.pki/ca.crt
# lrwxrwxrwx 1   23 May 17 09:09 ca.pem -> /etc/maglev/.pki/ca.crt
# -r-------- 1 1.7K May 17 08:49 credentialmanager-key.pem
# -r-------- 1  307 May 21 06:20 credentialmanager-openssl.cnf
# -r--r--r-- 1 1.1K May 17 08:49 credentialmanager.pem
# -r-------- 1 1.7K May 17 08:49 encryptionmanager-key.pem
# -r-------- 1  307 May 21 06:20 encryptionmanager-openssl.cnf
```

```
# -r--r--r--  1  1.1K May 17 08:49 encryptionmanager.pem
# -r--------  1  1.7K May 17 08:49 encryption_seed-key.pem
# -r--r--r--  1   981 May 17 08:49 encryption_seed.pem
# -rw-r--r--  1  1.1K May 17 09:09 front-proxy-ca.crt
# -rw--------  1  1.7K May 17 09:09 front-proxy-ca.key
# -rw-r--r--  1  1.1K May 17 09:09 front-proxy-client.crt
# -rw--------  1  1.7K May 17 09:09 front-proxy-client.key
# -r--------  1  1.7K May 17 08:49 kong-key.pem
# -r--------  1   299 May 21 06:20 kong-openssl.cnf
# -r--r--r--  1  1.1K May 17 08:49 kong.pem
# -r--------  1  1.7K May 17 08:49 kube-admin-key.pem
# -r--r--r--  1   977 May 17 08:49 kube-admin.pem
# -r--------  1  1.7K May 17 08:49 kube-worker-1-key.pem
# -r--------  1   336 May 21 06:20 kube-worker-1-openssl.cnf
# -r--r--r--  1  1.1K May 17 08:49 kube-worker-1.pem
# -r--------  1  1.7K May 17 08:49 maglev-registry-key.pem
# -r--------  1   472 May 21 06:20 maglev-registry-openssl.cnf
# -r--r--r--  1  1.3K May 17 08:49 maglev-registry.pem
# -r--------  1    36 May 17 08:49 passphrase.txt
# -rw-r--r--  1  1.1K May 21 06:20 registry-ca.pem
# -rw--------  1  1.7K May 17 09:09 sa.key
# -rw--------  1   451 May 17 09:09 sa.pub
```

So konnten wir das alte Zertifikat wiederherstellen (sh. 10.4). Dies war kein Problem, da mit ISE Version 2.3 der Hostname und die IP nicht im Common Name sein müssen. Es wäre aber auch möglich gewesen, mit der CA ein neues zu signieren, da die Passphrase für den Private Key der CA in einem Textfile abgelegt ist.

Durch das erneute des Zertifikats wurde leider die Trust Verbindung zum ISE gebrochen, weshalb der ISE erneut ins DNA Center integriert werden musste.
Nun konnten wir die LAN Automation starten und der PnP Prozess auf den Netzwerkgeräten schien zu funktionieren.
Wir haben dann, wie von Patrick Mosimann vorgeschlagen, die ersten zwei Devices am Standort Rapperswil mit der LAN Automation konfiguriert, was einwandfrei funktioniert hat. Damit die Konfiguration auf die Geräte geschrieben wird, muss die LAN Automation beendet werden. Anschliessend wiederholten wir diesen Vorgang für die nächsten zwei Geräte. Dabei stellte sich heraus, dass die generierte Konfiguration unbrauchbar ist, da nur einzelne Point to Point Links konfiguriert wurden, aber nicht alle die nötig gewesen wären.
Da es sich bei der LAN Automation um ein Basisfeature handelt, wollten wir die Underlay Konfiguration nicht manuell erstellen und versuchten die Ursache für diesen Fehler zu finden. Schlussendlich hat uns folgendes Vorgehen zum Erfolg geführt:

- LAN Automation starten
- Ein Gerät nach dem anderen via PnP aufsetzen
  Wenn mehrere Geräte gleichzeitig konfiguriert werden, bricht PnP meistens ab
- Erst wenn alle Devices via PnP aufgesetzt sind, die LAN Automation stoppen

So wurden alle Konfigurationen korrekt erstellt und der Underlay mit ISIS war korrekt konfiguriert. Ebenfalls waren nun alle Geräte im Inventory sichtbar.
Dieses Vorgehen verhindert aber natürlich das Hinzufügen weiterer Geräte zu einem

späteren Zeitpunkt, da damit zu rechnen ist, dass es wieder zu Problemen kommt, wenn für denselben Underlay erneut eine LAN Automation gestartet wird.

10.6 Provisioning

10.6.1 Templates

Damit der Hostname der Switches und Router via Provisioning gesetzt werden kann, muss ein Template angelegt werden.
Über das Hauptmenü *Tools* → *Template Editor* kann mit *Add (Pluszeichen)* → *Create Project* ein neues Projekt anlegt werden. (Siehe: 10.9)

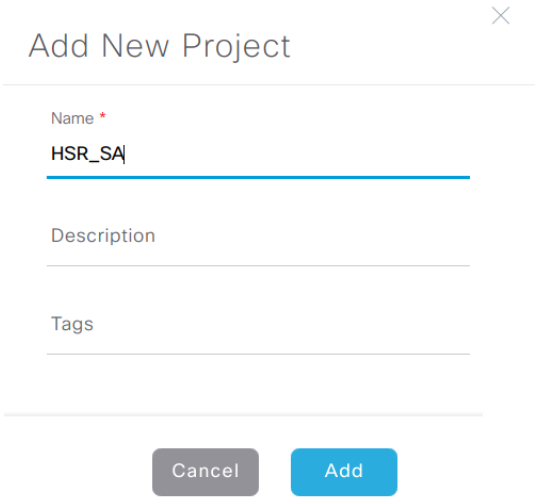


Abbildung 10.9: DNA Center - Templateeditor - Add Project

Weiter kann mit *Add (Pluszeichen)* → *Add Template* ein neues Template angelegt werden. (Siehe 10.10)

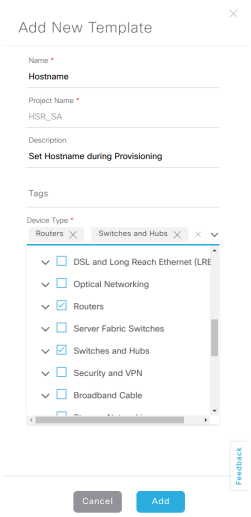


Abbildung 10.10: DNA Center - Templateeditor - Add Template

Wie in Abbilung 10.10 sind folgende Einstellungen festzulegen:

- Name des Templates
- Zugehörige Projekt
- Beschreibung
- Tags
- Für welche *Device Types* das Template verwendet werden soll.

Anschliessend wurde das Template befüllt. Hier kann die Script Sprache "velocity" verwendet werden. Da wir aber nur den Hostnamen setzen wollten, reicht das CLI Kommando und eine entsprechende Variable.

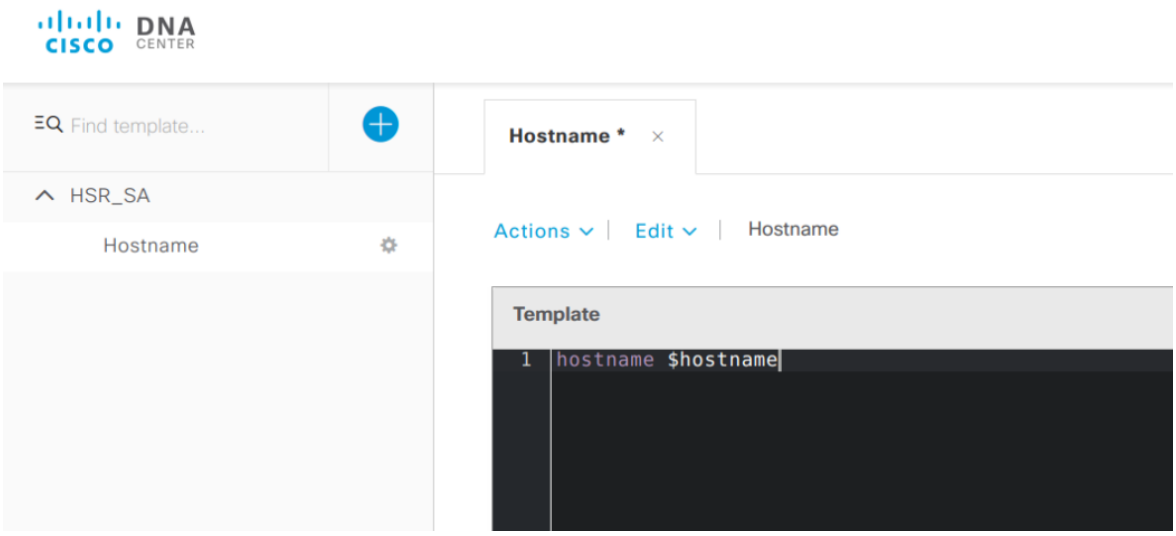


Abbildung 10.11: DNA Center - Templateeditor - Template um den Hostname bei der Provisionierung zu setzen.

10.6.2 Network Profile anlegen

Unter *Design* → *Network Profiles* → *Add Profile* konnte ein neues Profil angelegt werden. Dieses Profil wird während des Provisionierungsvorgang verwendet. Das Profil stellt das Bindeglied zwischen Site, Device Type, und Template dar.

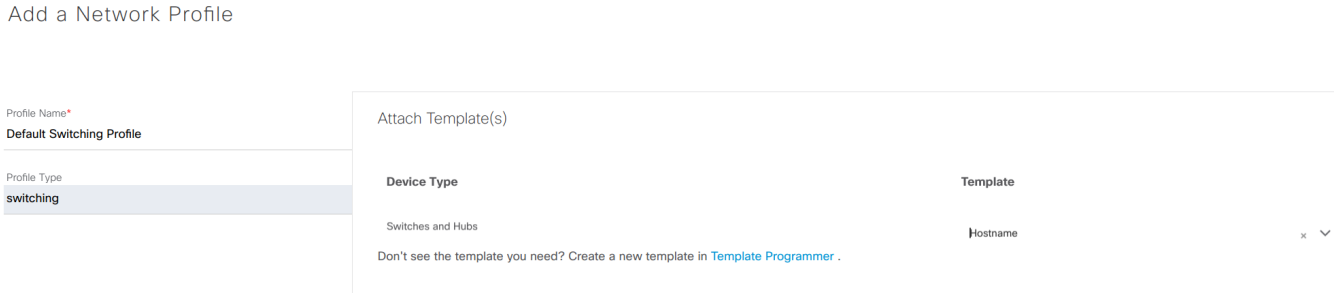


Abbildung 10.12: DNA Center - Network Profile - New Profile

Weiter wird festgelegt für welche *Sites* das Netzwerkprofil verwendet werden soll.

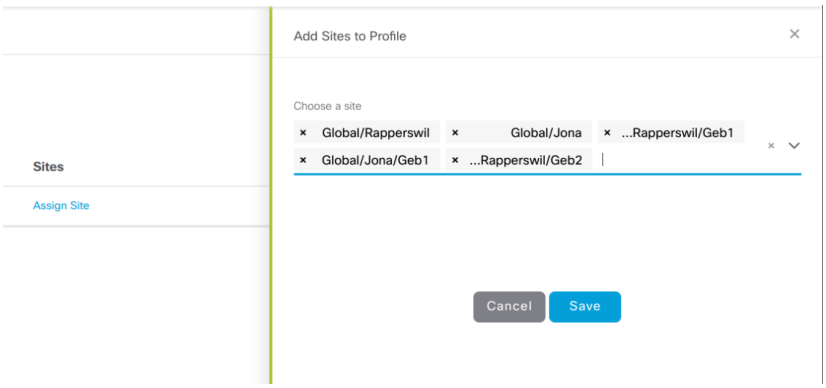


Abbildung 10.13: DNA Center - Network Profile - Assign Sites

10.6.3 Virtual Networks anlegen

Damit die Virtual Networks später in einer Fabric verwendet werden können, mussten diese zuerst angelegt werden. Wir haben die folgenden VNs angelegt:

- Mitarbeiter
- Gebäudemgmt
- Guest

Diese wurden im DNA Center unter *Policy* → *Virtual Network* → *Add (Plus Symbol)* angelegt.
Es musste ein Name, sowie die Scalable Groups, die im VN verfügbar sind angegeben werden. Dies kann aber auch später gemacht werden.

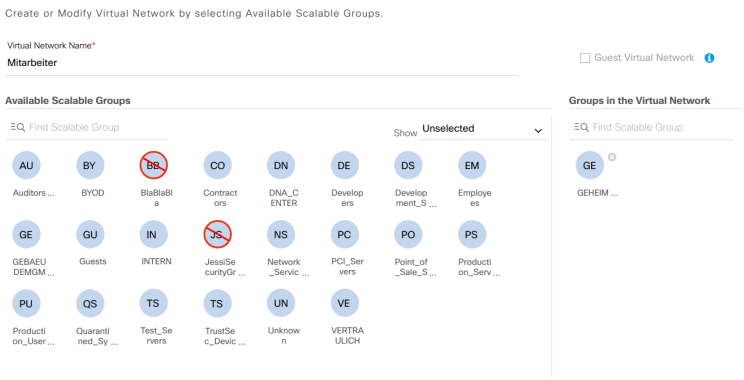


Abbildung 10.14: DNA Center - Add Virtual Network

10.6.4 Initial Provisioning

Nun kann ein initales Provisioning der neuen Netzwerkgeräte durchgeführt werden. Dies ist im Modul *Provision* → *Devices* → *Inventory* zu finden. Das zu provisionierende Gerät wird in der Liste ausgewählt. Über *Action* → *Provision* wird das Provisioning gestartet.

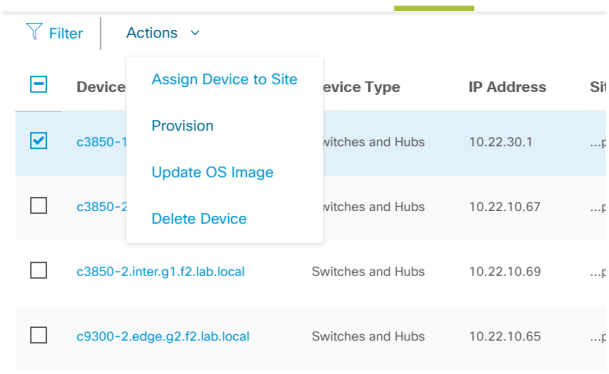


Abbildung 10.15: DNA Center - Device Provisioning

Es folgt ein Wizard, der durch das Provisioning führt. Im ersten Schritt (Siehe: 10.16) wird die entsprechende *Site* ausgewählt.

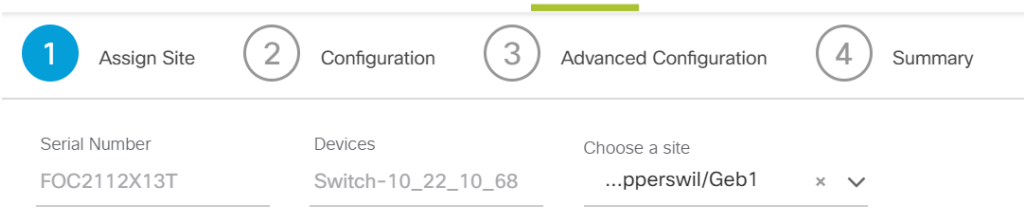


Abbildung 10.16: DNA Center - Provision Step 1

Im zweiten Schritt gibt es keine wählbaren Optionen.
Im dritten Schritt kann das im Abschnitt 10.6.1 definierte Template ausgefüllt werden. Die Variablen (im Falle 10.17), in unserem Fall der Hostname des Geräts mussten angegeben werden.

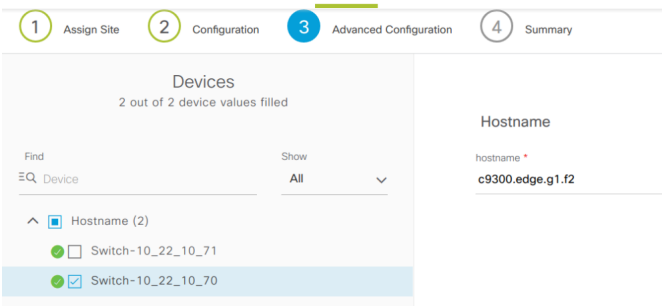


Abbildung 10.17: DNA Center - Provision Step 3

Im letzte Schritt erscheint eine Übersicht. Mit einem Klick auf *Deploy* wird das Device provisioniert. Die dabei automatisch ausgeführten Befehle durch das DNA Center sind untenstehend 1 ersichtlich.

Listing 1: Befehle automatisch ausgeführt durch das DNA Center während der Provisionierung

```
enable
no ip domain-lookup
ip access-list extended ACL_WEBAUTH_REDIRECT
```

```
180 permit tcp any any eq www
190 permit tcp any any eq 443
200 permit tcp any any eq 8443
210 permit udp any any eq domain
220 permit udp any eq bootpc  any eq bootps
170 deny ip any host 10.22.0.22
exit
ip tacacs source-interface Loopback0
ip radius source-interface Loopback0
aaa new-model
ip radius source-interface Loopback 0
exit
aaa group server radius dnac-network-radius-group
server name dnac-radius_10.22.0.22
ip radius source-interface Loopback 0
exit
aaa accounting dot1x default start-stop group dnac-client-radius-group
aaa accounting update newinfo periodic 600
aaa accounting exec default start-stop group dnac-network-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa authorization exec VTY_author group dnac-network-radius-group local \
    if-authenticated
aaa authorization exec VTY_author group dnac-network-radius-group local
aaa authentication login default local
aaa authentication dot1x default group dnac-client-radius-group
aaa authentication login VTY_authen group dnac-network-radius-group \
    local
dot1x system-auth-control
radius server dnac-radius_10.22.0.22
address ipv4 10.22.0.22 auth-port 1812 acct-port 1813
pac key *
retransmit 1
radius-server deadtime 30
radius-server attribute 25 access-request include
radius-server attribute 8 include-in-access-req
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
cts authorization list dnac-cts-list
line vty 0 97
login authentication VTY_authen
authorization exec VTY_author
transport input all
banner motd #\"Welcome to our SA Lab!\"#
hostname c9300-2.edge.g2.f2
```

10.6.5 Geräte zur Fabric hinzufügen

Im nächsten Schritt mussten die neuen Devices zu einer Fabric hinzugefügt werden. Dies wird unter *Provision* → *Fabric* → *Rapperswil* gemacht. Das Vorgehen ist in Abschnitt 9.13 beschrieben. Bei allen Nodes, ausser den Border und Control Plane Nodes, musste lediglich die Rolle definiert werden. Für den Border und Control Plane Node war etwas mehr Konfiguration nötig.

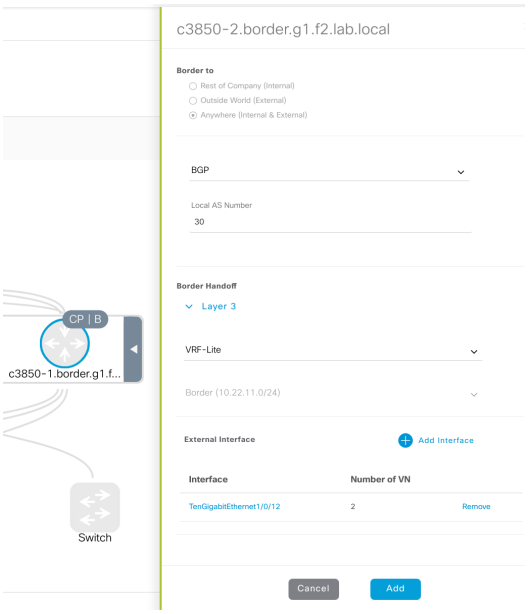


Abbildung 10.18: DNA Center - Border Konfiguration

Wie in obiger Grafik ersichtlich ist, müssen folgende Informationen für den Border angegeben werden:

- Routing Protokoll (derzeit nur BGP möglich)
  - AS-Number
- IP Pool für den Border
- Externes Interface
  - Remote AS-Number
  - Virtual Networks

Sobald die Rollen aller Devices definiert sind und der Border konfiguriert wurde, kann die Konfiguration mittels *Save* Button auf die Geräte verteilt werden. Was dabei genau auf dem Gerät gemacht wird, ist nachfolgend 2 am Beispiel eines Edge Devices ersichtlich.

Listing 2: Befehle automatisch ausgeführt durch das DNA Center während dem hinzufügen zur Fabric

```
!exec: enable
ip dhcp snooping
cts role-based enforcement
vrf definition DEFAULT_VN
address-family ipv4
vlan 4000
name VOICE_VLAN
exit
vlan 3999
```

```
name CRITICAL_VLAN
exit
interface GigabitEthernet1/0/3
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/4
no load-interval
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/7
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/10
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
interface GigabitEthernet1/0/12
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/13
no load-interval
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/15
```

```
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/18
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
interface GigabitEthernet1/0/21
no load-interval
no spanning-tree portfast
no switchport trunk native vlan
switchport
switchport mode dynamic auto
switchport access vlan 1
exit
switchport access vlan 1
exit
router lisp
ipv4 source-locator Loopback0
locator-set rloc_def9f1a7-9572-4e74-afaf-44215f0fbbde
IPv4-interface Loopback0 priority 10 weight 10
exit
locator-table default
locator default-set rloc_def9f1a7-9572-4e74-afaf-44215f0fbbde
service ipv4
etr map-server 10.22.10.67 proxy-reply
etr
sgt
use-petr 10.22.10.67
use-petr 10.22.30.1
exit
service ethernet
database-mapping limit dynamic 5000
map-cache-limit 25000
itr map-resolver 10.22.30.1
ipv4 locator reachability exclude-default
ip dhcp relay information option
banner motd #\"Welcome to our SA Lab!\"#
ip sla 1
```

```
icmp-echo 10.22.0.22 source-ip 10.22.10.65
frequency 60
threshold 3
timeout 5000
ip sla schedule 1 life forever start-time now
banner motd #\"Welcome to our SA Lab!\"#
ip sla 2
icmp-echo 10.22.10.67 source-ip 10.22.10.65
frequency 60
threshold 3
timeout 5000
ip sla schedule 2 life forever start-time now
banner motd #\"Welcome to our SA Lab!\"#
ip sla 3
icmp-echo 10.22.30.1 source-ip 10.22.10.65
frequency 60
threshold 3
timeout 5000
ip sla schedule 3 life forever start-time now
banner motd #\"Welcome to our SA Lab!\"#
```

10.7 Border BGP Konfiguration

Auf den Border Nodes wurde nun die BGP Konfiguration erstellt, damit die Fabric mit der Aussenwelt kommunizieren kann. Die Konfiguration der Gegenseite kann das DNA Center leider nicht übernehmen. Diese muss daher manuell erstellt werden.
Hier ein Beispiel einer Konfiguration, die vom DNA Center erstellt wurde:

```
c3850-1.border.g1.f2#sh run | sec router bgp
router bgp 30
bgp router-id interface Loopback0
bgp log-neighbor-changes
neighbor 10.22.11.2 remote-as 10
neighbor 10.22.11.2 update-source Vlan3001
!
address-family ipv4
network 10.22.30.1 mask 255.255.255.255
redistribute connected
redistribute lisp metric 10
redistribute isis level-1-2
neighbor 10.22.11.2 activate
neighbor 10.22.11.2 weight 65535
exit-address-family
!
address-family ipv4 vrf Mitarbeiter
bgp aggregate-timer 0
network 10.22.100.1 mask 255.255.255.255
aggregate-address 10.22.100.0 255.255.254.0 summary-only
```

```
redistribute lisp metric 10
neighbor 10.22.11.30 remote-as 10
neighbor 10.22.11.30 update-source Vlan3008
neighbor 10.22.11.30 activate
neighbor 10.22.11.30 weight 65535
exit-address-family
```

Nun musste auf dem Legacy Router die passende Konfiguration erstellt werden. Diese kann wie folgt aussehen:

```
isr4431.legacy#sh run int Gi0/0/1.3008
Building configuration...

Current configuration : 109 bytes
!
interface GigabitEthernet0/0/1.3008
encapsulation dot1Q 3008
ip address 10.22.11.30 255.255.255.252
end
isr4431.legacy#sh run | sec router bgp
router bgp 10
bgp log-neighbor-changes
neighbor 10.22.11.1 remote-as 30
neighbor 10.22.11.29 remote-as 30
!
address-family ipv4
network 0.0.0.0
redistribute connected
redistribute static
neighbor 10.22.11.1 activate
neighbor 10.22.11.29 activate
```

Je nach Anzahl VNs wird diese Konfiguration natürlich wesentlich grösser. Es ist zu beachten, dass jedes Mal wenn ein VN erstellt wird, die Konfiguration auf dem Legacy Router angepasst werden muss, sofern Kommunikation zwischen dem VN und der Aussenwelt möglich sein soll.

10.8 IP Pools für Clients definieren

Damit sich Clients am Netzwerk anmelden können, mussten IP Pools für die verschiedenen VNs definiert werden. Diese können unter *Design* → *Network Settings* → *Global* → *IP Address Pools* → *Add IP Pool* hinzugefügt werden.

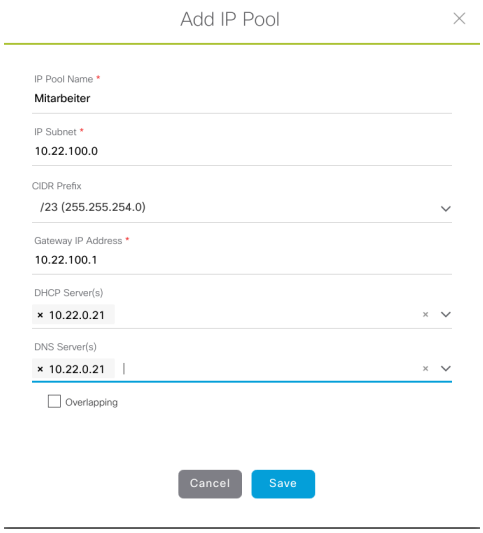


Abbildung 10.19: DNA Center - Add IP Pool

Der IP Pool wurde dann vom DNA Center in Infoblox erstellt. Leider wurde dabei kein DHCP Server für den Pool auf Infoblox erstellt. Dies musste also manuell gemacht werden. In Infoblox sind folgende Schritte nötig, damit der DHCP Server den neuen Pool bedient. *Data Management → IPAM → 10.22.0.100/23 → Edit → Member Assignment*

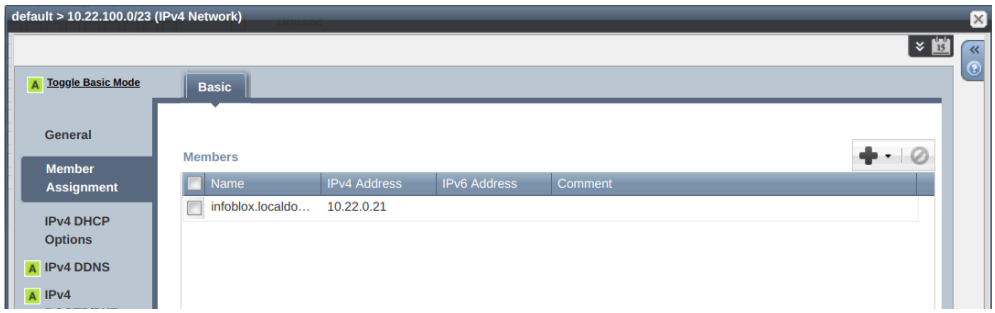


Abbildung 10.20: Infoblox - Member Assignment

Wie in der obenstehenden Grafik zu sehen ist, musste ein Member für den neuen Pool assigned werden. In unserer Lab Umbegung gibt es nur einen Infoblox Server, weshalb dieser ausgewählt werden muss. Anschliessend muss eine DHCP Range erstellt werden, aus der die Clients Adressen erhalten können. Das Vorgehen dazu ist In Infoblox sind folgende Schritte nötig, damit der DHCP Server den neuen Pool bedient. *Data Management → DHCP → Networks → 10.22.100.0/23 → Add (Plus Symbol)* Es startet ein Wizard, mit dem die Range definiert werden kann. Dabei müssen die Start- und Endadresse der IP Range angegeben werden.

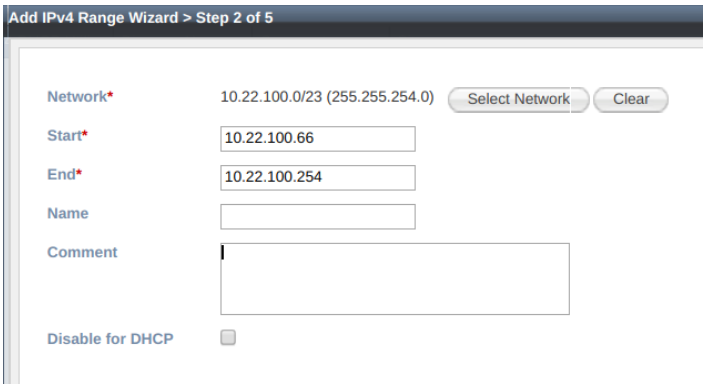


Abbildung 10.21: Infoblox - Add IP Range

Im zweiten Schritt des Wizards muss definiert werden, welcher Member die Range bedient. Da zuvor nur einer zugewiesen wurde, konnte einfach dieser ausgewählt werden.

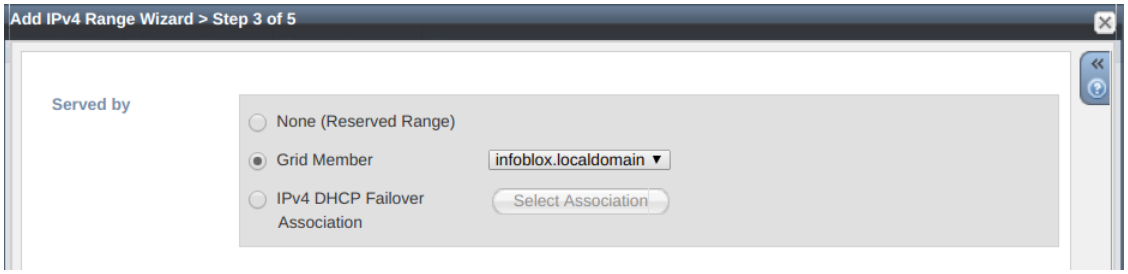


Abbildung 10.22: Infoblox - Assign Grid Memger

Zum Schluss muss diese Konfiguration gespeichert werden. Damit diese auch aktiviert wird, muss der DHCP Service auf dem Infoblox Server neu gestartet werden. Infoblox weist jeweils darauf hin, wenn Änderungen einen Neustart der Services benötigen, das DNA Center leider nicht.

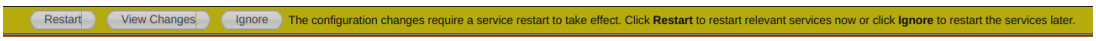


Abbildung 10.23: Infoblox - Restart Services

10.9 Benutzerprofile und Policies

10.9.1 SGTs erstellen

Damit Benutzern Policies zugewiesen werden können, müssen zu Beginn Scalable Groups erstellt werden, denen die Benutzer später zugewiesen werden können. Zwischen den Scalable Groups werden die Zugriffe dann mittels Policies geregelt. Scalable Groups müssen im ISE erstellt werden und können nicht direkt im DNA Center angelegt werden. Das DNA Center verweist aber under *Policy* → *Registry* → *Scalable Groups* → *Add Groups* auf die korrekte Seite im ISE und sieht alle bereits vorhandenen Groups.

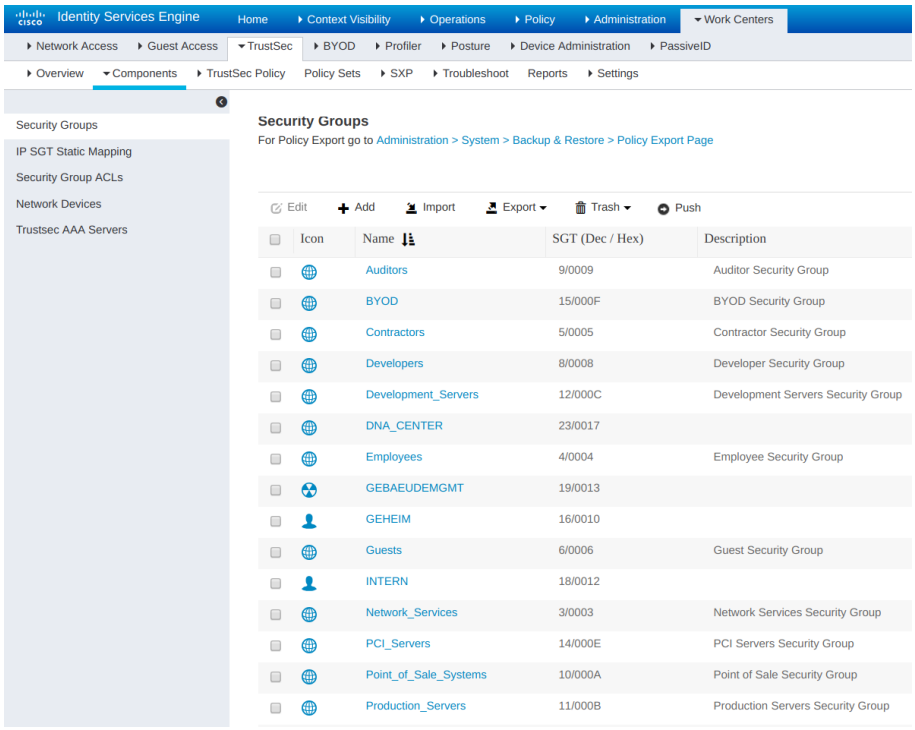


Abbildung 10.24: ISE - Scalable Groups

Mit dem *Add* Button können weitere Gruppen hinzugefügt werden.

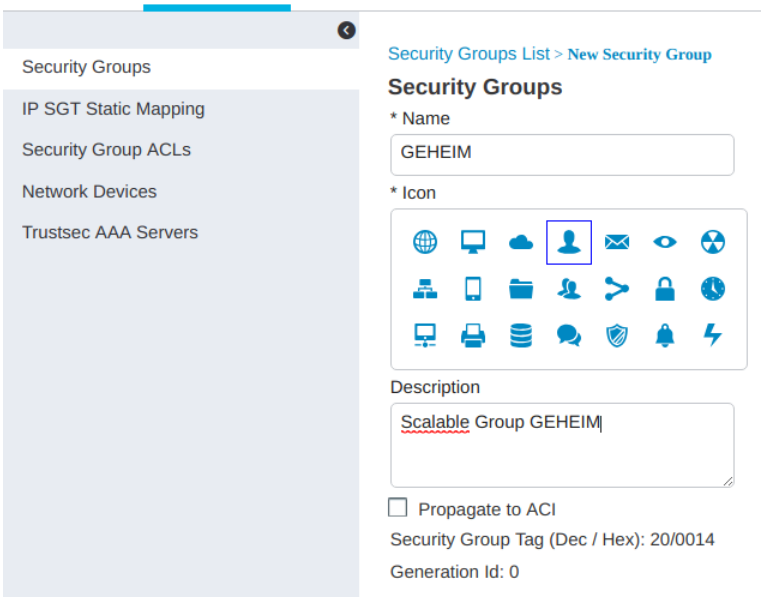


Abbildung 10.25: ISE - Add Scalable Group

10.9.2 Contracts erstellen

Um schlussendlich Policies zwischen den Scalable Groups erstellen zu können, waren sogenannte Contracts nötig. Dies sind im Prinzip Access Control Lists (ACLs), die dann

mittels Policy zwischen zwei Gruppen angewandt werden kann. Zu Beginn waren zwei Contacts vorhanden:

- permit
- deny

Diese entsprechen einer ACL die alles erlaubt oder verbietet. Zusätzlich können weitere Contracts erstellt werden, die einzelne Protokolle erlauben.
Untenstehend ein Contract, der lediglich SSH erlaubt.

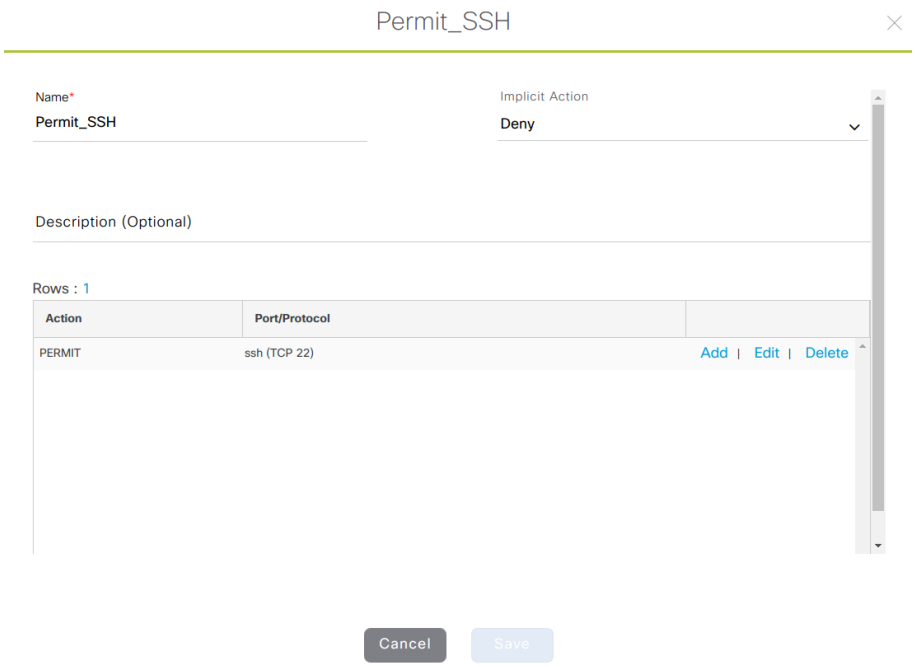


Abbildung 10.26: DNA Center - Add Contract

10.9.3 Policies erstellen

Die zuvor erstellten Contracts konnten nun genutzt werden, um Policies zwischen den Scalable Groups zu erstellen. Die Policies sind im DNA Center unter *Policy* → *Policy Administration* → *Group-Based Access Control* zu finden.
Hier kann die Kommunikation zwischen den Scalable Groups geregelt werden. Mit Hilfe des *Add Policy* Buttons können zusätzliche Policies erstellt werden. Die folgende Policy verbietet Traffic aus der Scalable Group "INTERN" zu den Gruppen "VERTRAULICH" und "GEHEIM".

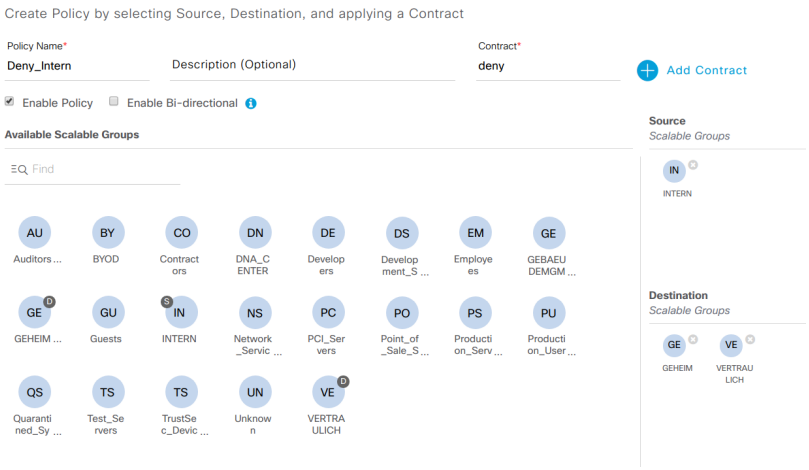


Abbildung 10.27: DNA Center - Add Policy

So konnten alle Policies erstellt werden, die nötig waren, um die Kommunikation innerhalb der Fabric zu regeln.

10.10 Host Onboarding

Im Bereich Host Onboarding wird geregelt, was geschieht, wenn sich ein Client mit dem Netzwerk verbindet. Dies kann global pro Fabric, aber auch pro Port geregelt werden.

10.10.1 Authentifizierungsmethoden

Typ	Beschreibung
Closed Authentication	Basiert auf 802.1x. Kein Netzwerkzugriff möglich, bevor sich der Client mittels 802.1x authentifiziert.
Open Authentication	Basiert auf 802.1x. Temporärer Zugriff (PXE, DHCP) ist erlaubt bevor sich der Client mittels 802.1x authentifiziert.
Easy Connect	Basiert auf LDAP kombiniert mit MAC Address Bypass (MAB).
No Authentication	Statische Portkonfiguration. Dies ist geeignet für Geräte, die 802.1x nicht unterstützen.

Tabelle 10.1: Host Onboarding Methoden

In der LAB Umgebung haben wir eine Kombination aus "No Authentication" und "Open Authentication gewählt. An Ports, die für das Gebäudemanagement vorgesehen sind, ist "No Authentication" konfiguriert und das VN "Gebaeudemgmt" ist statisch konfiguriert. Dies aus dem Grund, da solche Geräte 802.1x wahrscheinlich nicht unterstützen. Alle anderen Ports sind mit "Open Authentication" konfiguriert. Ein Client der sich mit dem Netzwerk verbindet, kann also nur DHCP und PXE nutzen, bis er sich erfolgreich authentifiziert hat und anschliessend ins entsprechende VN verschoben wird.

Die Portkonfiguration kann im DNA Center unter *Provision* → *Fabric* → *Host Onboarding* vorgenommen werden.

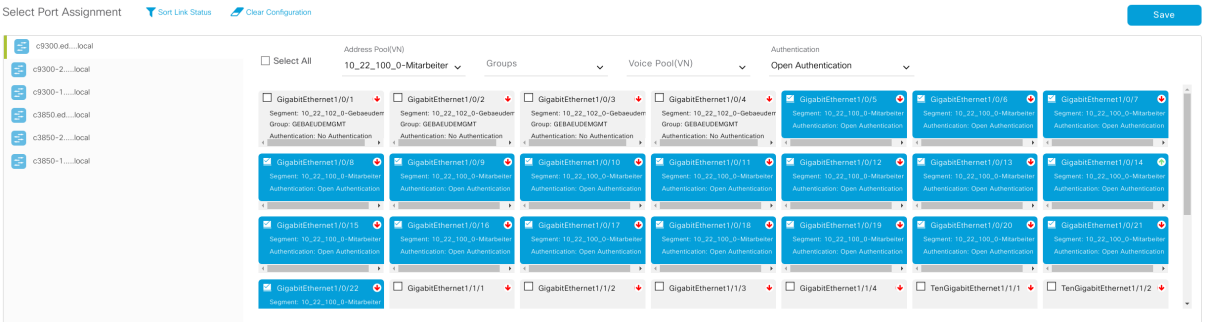


Abbildung 10.28: DNA Center - Host Onboarding

Auf dem Netzwerk Device sah die Port Konfiguration dann wie folgt aus:

No Authentication

```
interface GigabitEthernet1/0/1
  switchport access vlan 1021
  switchport mode access
  device-tracking attach-policy IPDT_MAX_10
  load-interval 30
  cts manual
  policy static sgt 19
  no propagate sgt
  spanning-tree portfast
end
```

Open Authentication

```
interface GigabitEthernet1/0/5
  switchport access vlan 1022
  switchport mode access
  device-tracking attach-policy IPDT_MAX_10
  load-interval 30
  authentication control-direction in
  authentication event server dead action authorize vlan 3999
  authentication event server dead action authorize voice
  authentication host-mode multi-auth
  authentication open
  authentication order dot1x mab
  authentication priority dot1x mab
  authentication port-control auto
  authentication periodic
```

```
  authentication timer reauthenticate server
  authentication timer inactivity server dynamic
  mab
  dot1x pae authenticator
  dot1x timeout tx-period 10
  spanning-tree portfast
end
```

10.10.2 802.1x Client Config

Ubuntu

Unter Ubuntu sind zwei Konfigurationen nötig. Zum einen eine "wpa_supplicant" Konfiguration, sowie die passende Interface Config. Die wpa_supplicant.conf sieht so aus:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
eapol_version=2
ap_scan=0

network={
        key_mgmt=IEEE8021X
        eap=PEAP
        identity="jessica"
        password="MYPASSWORD"
        eapol_flags=0
}
```

In der Interface Konfiguration unter "/etc/network/interfaces" muss das gewünschte Interface folgendermassen konfiguriert werden:

```
auto enxc0742bfff8af
iface enxc0742bfff8af inet dhcp
  wpa-driver wired
  wpa-conf /root/wpa_supplicant.conf
```

Fedora / RedHat

In Red Hat basierten Linux Distributionen kann die Datei "/etc/sysconfig/network-scripts/ifcfg-INTERFACE_NAME" angepasst werden. Folgende Zeilen müssen hinzugefügt werden:

```
KEY_MGMT=IEEE8021X
IEEE_8021X_EAP_METHODS=PEAP
IEEE_8021X_IDENTITY=sandro
IEEE_8021X_INNER_AUTH_METHODS=MSCHAPV2
```

Windows

Unter Windows sind mehrere Schritte notwendig.

Service Starten

Unter Services muss der Service *Wired AutoConfig* gestartet werden.

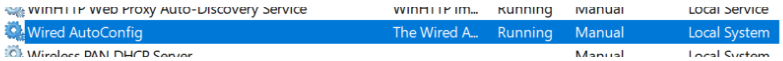


Abbildung 10.29: Windows Service Wired AutoConfig aktivieren

Credentials hinterlegen

Beim entsprechenden Interface müssen nun die entsprechenden Credentials hinterlegt werden. Dazu wählt man mit rechter Maustaste auf den entsprechenden Netzwerkadapter *Properties* → *Authentication* → *Additional Settings*, setzt einen Haken bei *Specify authentication mode*, wählt im Dropdown *User authentication*, klickt auf *Replace credentials* (oder ähnlich) und gibt im im neuen Fenster die Benutzerauthentifizierungsdaten ein.

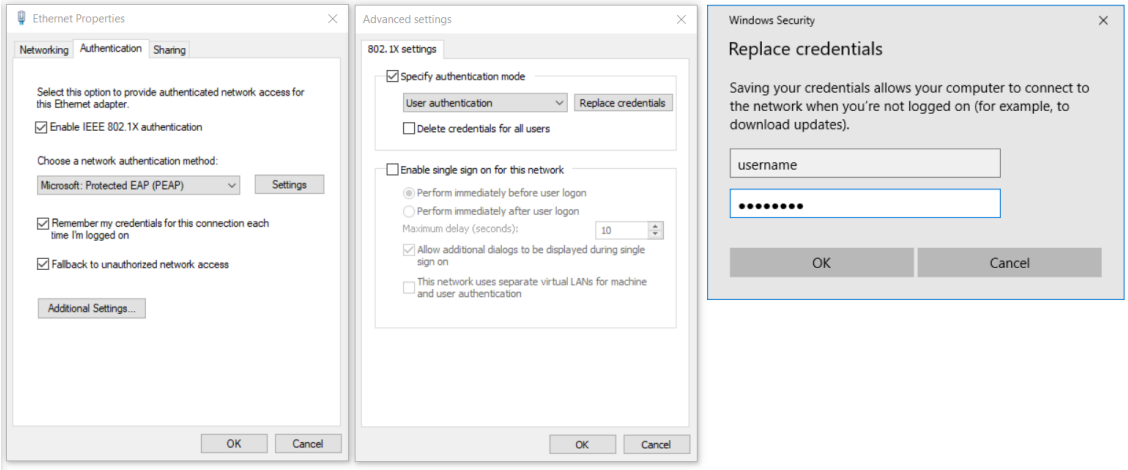


Abbildung 10.30: Windows Netzwerkadapter - Benutzerauthentifizierungsdaten hinterlegen - Übersicht über alle Fenster

Wireshark Capture des Authentifizierungsvorganges

Nachfolgend sind zwei Screenshots eines Wireshark Capture von einer erfolgreichen und einer nicht erfolgreichen Authentifizierung.

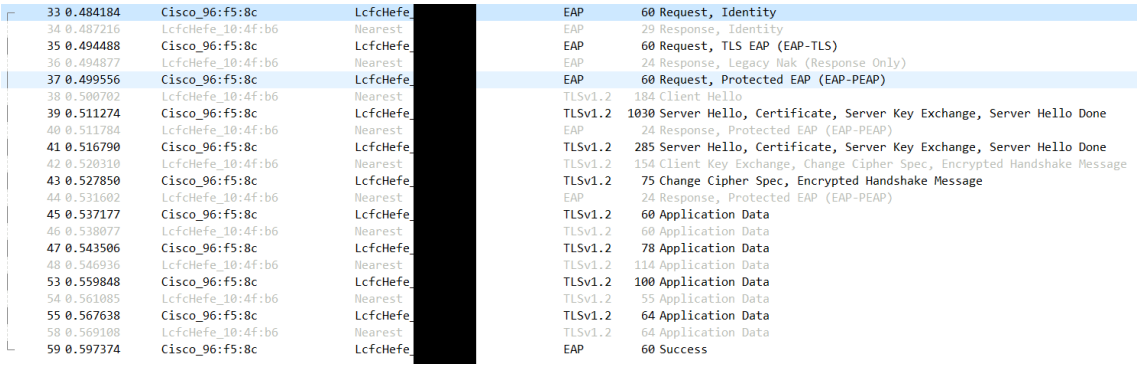
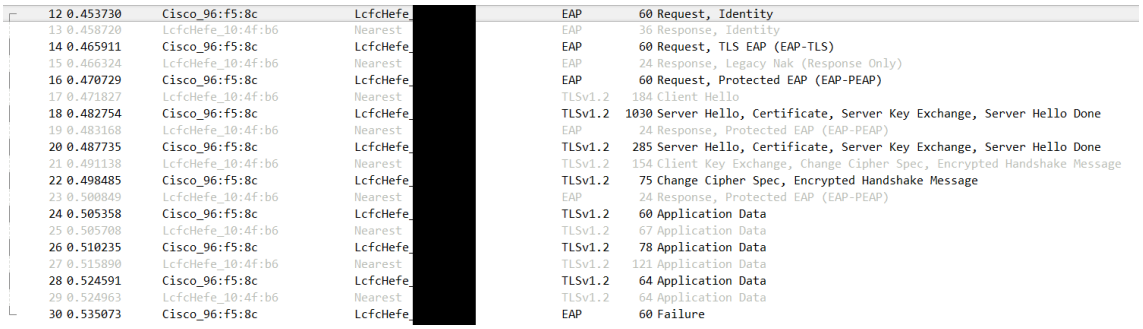


Abbildung 10.31: Wireshark Capture - Erfolgreiches EAP



12	0.453730	Cisco_96:f5:8c	LcfcHefe_	EAP	60	Request, Identity
13	0.458720	LcfcHefe_10:4f:b6	Nearest	EAP	36	Response, Identity
14	0.465911	Cisco_96:f5:8c	LcfcHefe_	EAP	60	Request, TLS EAP (EAP-TLS)
15	0.466324	LcfcHefe_10:4f:b6	Nearest	EAP	24	Response, Legacy Nak (Response Only)
16	0.470729	Cisco_96:f5:8c	LcfcHefe_	EAP	60	Request, Protected EAP (EAP-PEAP)
17	0.471827	LcfcHefe_10:4f:b6	Nearest	TLSv1.2	184	Client Hello
18	0.482754	Cisco_96:f5:8c	LcfcHefe_	TLSv1.2	1030	Server Hello, Certificate, Server Key Exchange, Server Hello Done
19	0.483168	LcfcHefe_10:4f:b6	Nearest	EAP	24	Response, Protected EAP (EAP-PEAP)
20	0.487735	Cisco_96:f5:8c	LcfcHefe_	TLSv1.2	285	Server Hello, Certificate, Server Key Exchange, Server Hello Done
21	0.491138	LcfcHefe_10:4f:b6	Nearest	TLSv1.2	154	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
22	0.498485	Cisco_96:f5:8c	LcfcHefe_	TLSv1.2	75	Change Cipher Spec, Encrypted Handshake Message
23	0.500849	LcfcHefe_10:4f:b6	Nearest	EAP	24	Response, Protected EAP (EAP-PEAP)
24	0.505358	Cisco_96:f5:8c	LcfcHefe_	TLSv1.2	60	Application Data
25	0.505708	LcfcHefe_10:4f:b6	Nearest	TLSv1.2	67	Application Data
26	0.510235	Cisco_96:f5:8c	LcfcHefe_	TLSv1.2	78	Application Data
27	0.515890	LcfcHefe_10:4f:b6	Nearest	TLSv1.2	121	Application Data
28	0.524591	Cisco_96:f5:8c	LcfcHefe_	TLSv1.2	64	Application Data
29	0.524963	LcfcHefe_10:4f:b6	Nearest	TLSv1.2	64	Application Data
30	0.535073	Cisco_96:f5:8c	LcfcHefe_	EAP	60	Failure

Abbildung 10.32: Wireshark Capture - Fehlgeschlagenes EAP

10.11 Policies ausserhalb der Fabric

Damit auch Policies für Ressourcen ausserhalb der Fabric erstellt werden können, sind SGT Mappings nötig, sowie das Protokoll SXP, dass die vom ISE mit den Border Nodes synchronisiert.

10.11.1 SGT Mapping

Um ein Mapping zwischen IP Adressen ausserhalb der Fabric und Security Groups zu erstellen, mussten in einem ersten Schritt die SGs erstellt werden, die später für das Mapping verwendet werden. SGs können im ISE unter *Workcenters* → *Trustsec* → *Components* → *Security Groups* → *Add*, wie in Abschnitt 10.9.1 beschrieben, erstellt werden.
Anschliessend mussten unter *Workcenters* → *Trustsec* → *Components* → *IP SGT Static Mapping* → *Add* die entsprechenden Mappings erfasst werden.

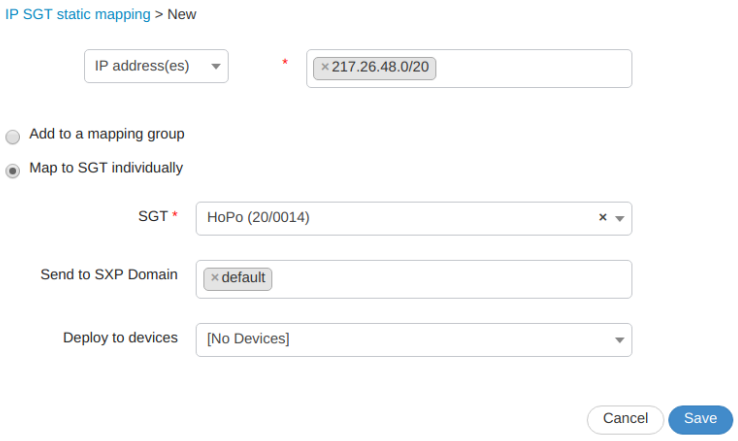


Abbildung 10.33: ISE - IP SGT Mapping

10.11.2 SXP

Damit die manuell im ISE erstellten Security Groups und IP SGT Mappings am Border bekannt werden, muss das SGT Exchange Protocol (SXP) zwischen ISE und den Border Nodes eingerichtet werden. Dies musste manuell gemacht werden. Im ISE ist SXP unter *Workcenters* → *Trustsec* → *SXP* zu finden. Mit dem Add Button konnten Devices hinzugefügt werden, mit denen die SGs synchronisiert werden.

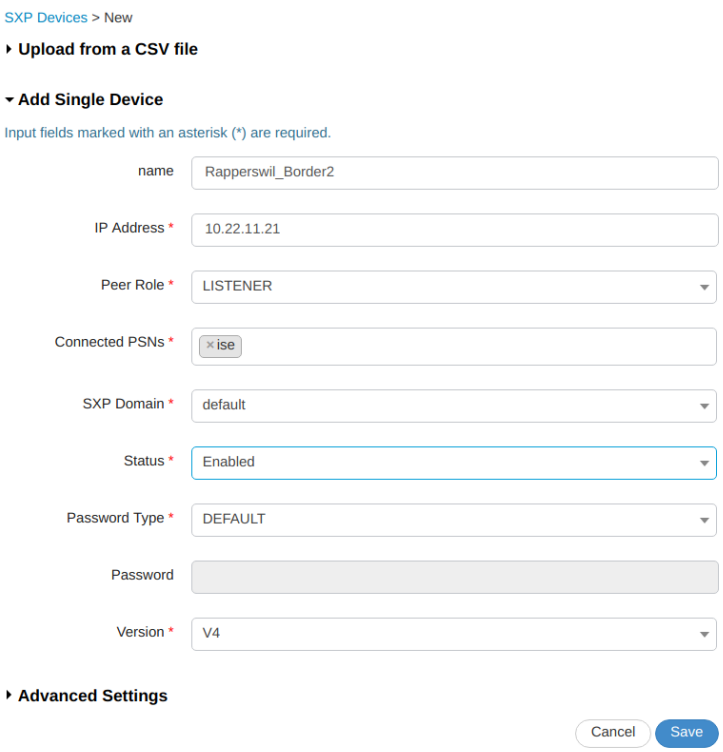


Abbildung 10.34: ISE - SXP

Auf den Border Nodes musste SXP dann ebenfalls konfiguriert werden. Dies konnte mit folgenden Befehlen erreicht werden:

```
cts sxp enable
cts sxp default password 7 09444F05150A3743595F50
cts sxp connection peer 10.22.0.22 source 10.22.11.21 password default \
    mode local listener hold-time 0 0 vrf Mitarbeiter
cts role-based enforcement
cts role-based enforcement vlan-list all
```

Wichtig dabei war, dass als Source die IP Adresse des VLAN Interfaces gewählt wird, das mit dem VN Mitarbeiter assoziiert ist. Falls in anderen VNs ebenfalls Policies für Ressourcen ausserhalb der Fabric nötig sind, müssen die obigen Schritte für dieses VN wiederholt werden.
Sobald die Verbindung zwischen ISE und Border Node aktiv ist, sieht man die zuvor erstellten Mappings:

```
#sh cts role-based sgt-map vrf Mitarbeiter all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.22.0.100             23      SXP
10.22.100.253           17      SXP
217.26.48.0/20          20      SXP

IP-SGT Active Bindings Summary
```

```
Total number of SXP bindings = 3
Total number of active bindings = 3
```

10.11.3 Policies

Nun konnten für Ressourcen ausserhalb der Fabric die Policies genau gleich wie in Abschnitt 10.9.3 beschrieben erstellt werden.
In der LAB Umbebung haben wir die Policies gemäss untenstehender Matrix definiert:

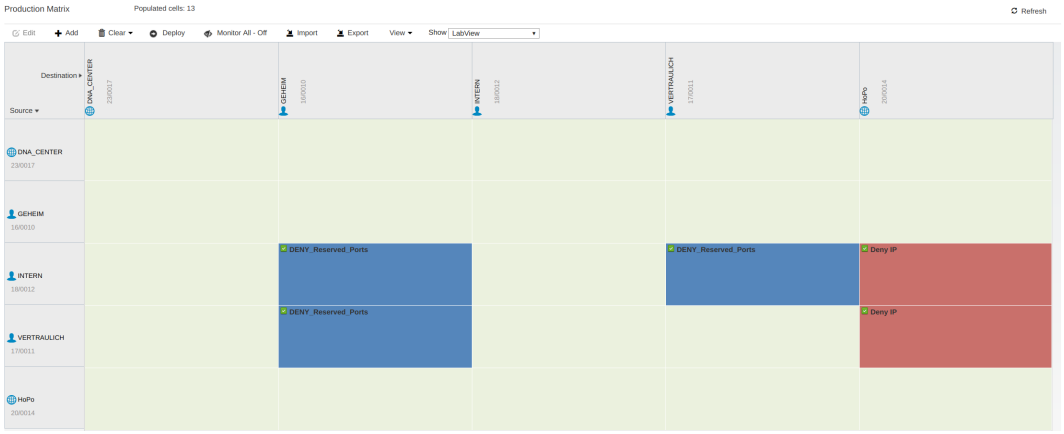


Abbildung 10.35: ISE - Policy Matrix

Clients den Gruppen "Intern" und "Vertraulich" dürfen also nicht mit Clients in der Gruppe "Geheim" kommunizieren. Des Weiteren dürfen diese nicht auf die Gruppe "HoPo" zugreifen. Dies ist eine externe Gruppe, die wie in Abschnitt 10.11.1 beschrieben, erstellt wurde. Die Gruppe "Geheim" hingegegen darf Verbindungen zu allen anderen Gruppen aufbauen.

10.11.4 Policies testen

Um die verschiedenen Policies zu testen, haben wir Clients in den verschiedenen Gruppen mit dem Netzwerk verbunden und die verschiedenen Verbindungen ausprobiert. Zu den einzelnen Verbindungsversuchen sind diesem Dokument tcpdumps beigelegt, die den Verkehr zwischen den Edge Nodes aufzeichnen.

Intern Auf dem folgenden Screenshot ist zu sehen, wie der Client in der Gruppe "Intern" versucht auf die Gruppe "Geheim zuzugreifen.

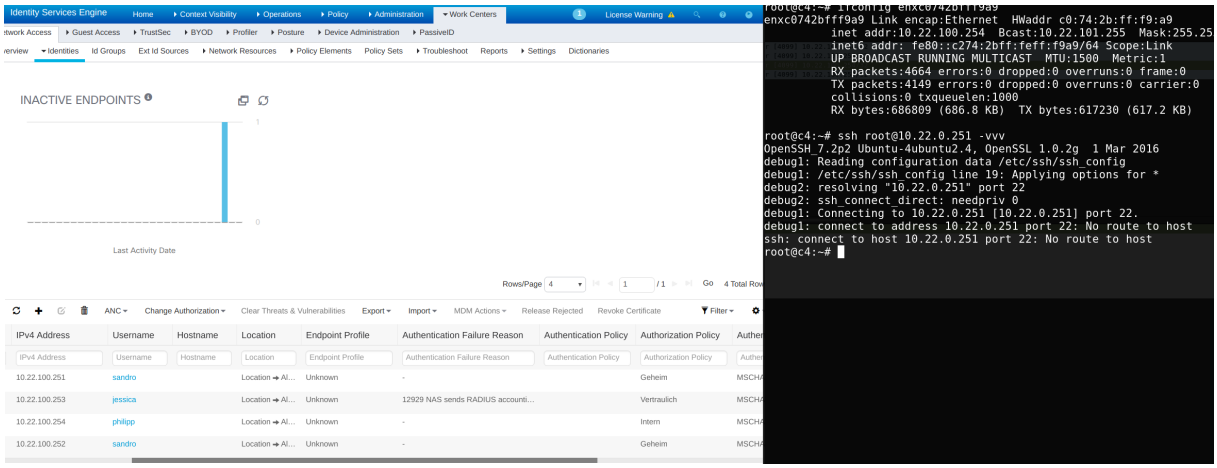


Abbildung 10.36: SSH - Intern - Geheim

Im nachfolgenden Screenshot ist der Verbindungsversuch in die Gruppe "HoPo" zu sehen.

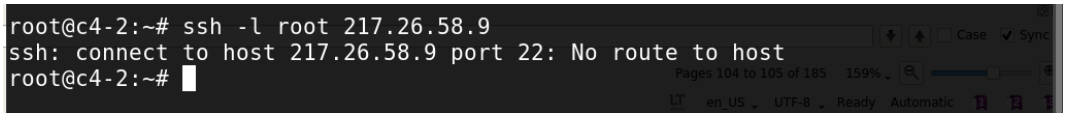


Abbildung 10.37: SSH - Intern - HoPo

Das die Policy funktioniert sieht man auf den Edge Nodes an den entsprechenden Counters.

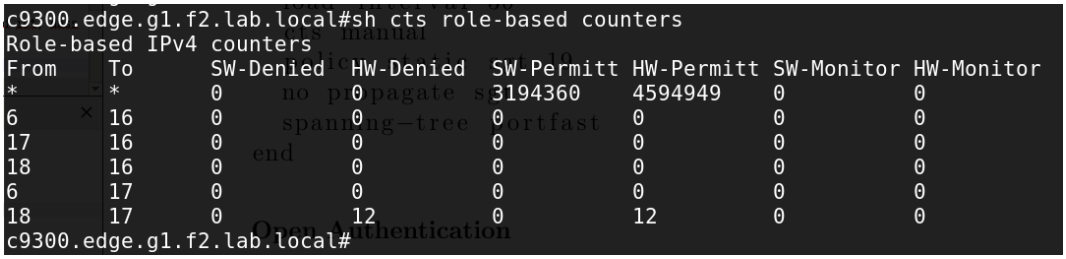


Abbildung 10.38: CTS - Counters

Das Enforcement der Policy findet jeweils auf dem Destination Edge Node statt. Dies erkennt man am einfachsten daran, dass die entsprechende Policy nur dort vorhanden ist. Der Edge Node bezieht also nur die Policies für die Security Groups, in denen Clients verbunden sind.

Vertraulich Aus der Gruppe "Vertraulich sehen die Verbindungsversuche gleich aus wie bei der Gruppe Intern. Der einzige Unterschied liegt darin, dass hier eine Verbindung von "Vertraulich" nach "Intern", also in der Gegenrichtung, erlaubt ist.

Geheim Diese Gruppe darf auf alle anderen Gruppen zugreifen. Dass dies funktioniert ist im folgenden Bild ersichtlich.

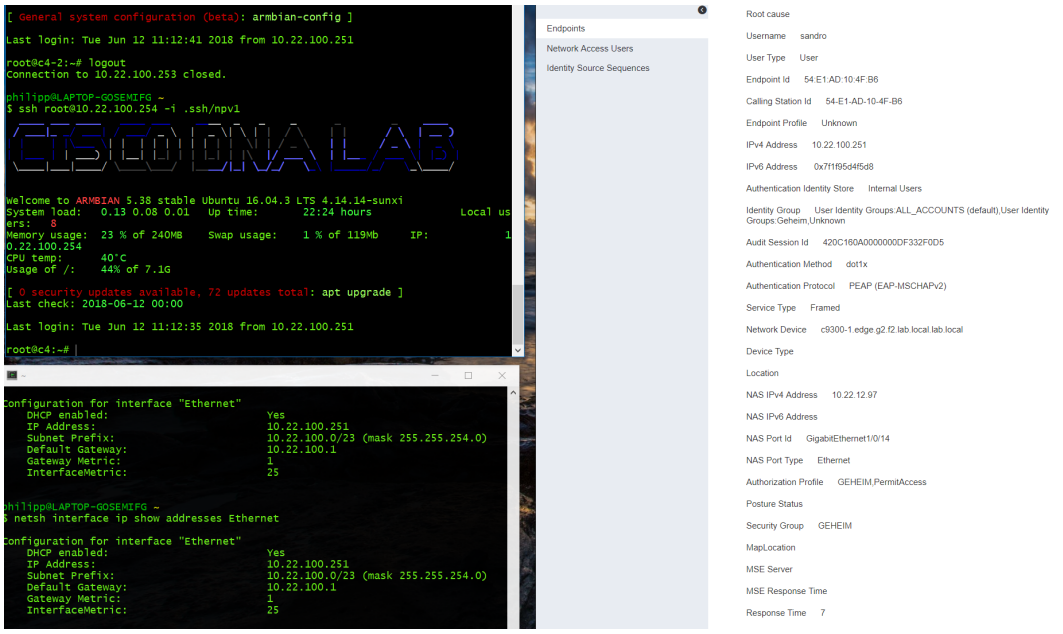


Abbildung 10.39: SSH - Geheim - Intern

10.11.5 Benutzermobilität testen

Um die Benutzermobilität zu testen, haben wir einen Client an einem Edge Node im Gebäude zwei angeschlossen. Dieser hat sich als User authentifiziert, hat alle benötigten Policies erhalten und konnte auf alle nótigen Ressourcen zugreifen. Wir haben dann eine SSH Session auf einen Host im Internet gestartet. Anschliessend wurde der Client vom Switch getrennt und an einem anderen Edge Device im Gebäude eins angeschlossen. Er hat sich umgehend authentifiziert und wieder die korrekten Policies erhalten. Die SSH Session wurde dabei nicht getrennt und hat weiterhin funktioniert. In der folgenden Grafik ist der LISP Traffic des neuen Edge Nodes zu sehen, nachdem sich der Client verbunden hat.

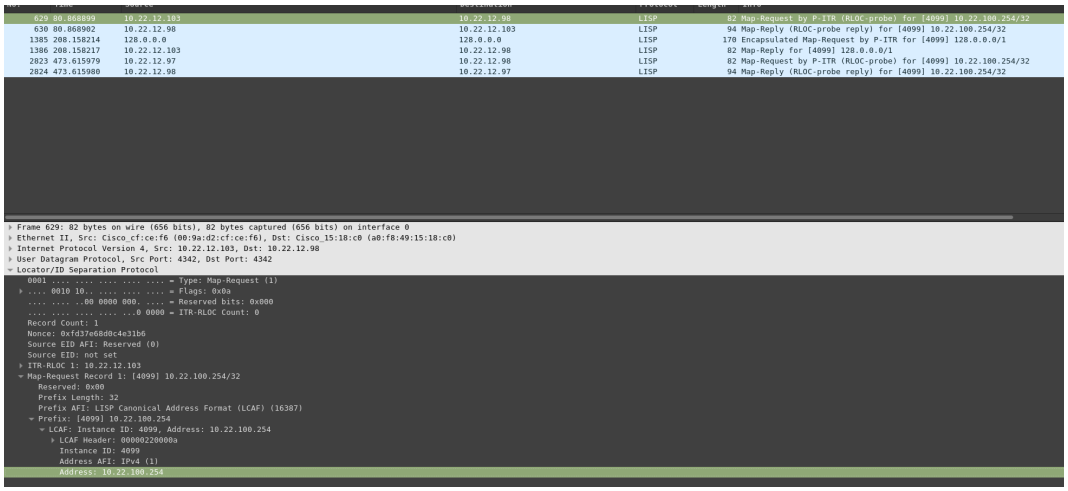


Abbildung 10.40: LISP - Client Mobility

10.12 Reporting einrichten

Die Reporting Funktionalität besteht aus einigen python Scripts. Im ersten Schritt mussten diese auf ein System kopiert werden, welches die regelmässigen Reports versenden kann. Am einfachsten mittels GIT Checkout. Anschliessend muss die Datei "config.py" angepasst werden. Folgende Informationen müssen angegeben werden:

- DNA Center IP Adresse
- DNA Center Port
- DNA Center Benutzername
- DNA Center Password
- Mailserver Hostname
- Mailserver Port
- E-Mail Benutzer
- E-Mail Passwort
- Empfänger der Reports

In unserer Lab Umgebung sah die Konfiguration dann folgendermassen aus:

```
# DNA Center Settings

DNAC_IP = "10.22.0.100"
DNAC_PORT = 443
USERNAME = "admin"
PASSWORD = "********"
VERSION = "v1"

# Mail Server Settings
MAIL_SERVER = "asmtp.mail.******.ch"
MAIL_PORT = 587
MAIL_USER = "dnacenter@XYZ.ch"
MAIL_PASSWORD = "********"
MAIL_RECIPIENTS = ['********@gmail.com', '******@hsr.ch']
```

Sobald die Konfiguration angepasst ist, kann das Script "gen_config.py" entweder manuell ausgeführt werden oder regelmässig via Cronjob gestartet werden. Dieser sah bei uns für einen täglichen Versand so aus:

```
30 0 * * * /usr/bin/python2 /opt/dnacenter_reporting/gen_report.py \
    > /dev/null 2>&1
```

Der erstellte Report ist in untenstehender Grafik ersichtlich:

All Hosts connected to the Network

Number	Host IP	Mac Address	Host Type	Connected to Network Device
1	10.22.0.15	02:42:c2:2e:69:49	wired	Switch
2	10.22.100.253	02:42:f3:ac:fd:88	wired	c9300.edge.g1.f2.lab.local
3	10.22.0.66	0e:d4:aa:d1:e5:19	wired	Switch
4	10.22.0.67	28:ac:9e:41:29:fe	wired	Switch
5	10.22.0.100	28:ac:9e:41:2a:04	wired	Switch
7	10.22.100.254	c0:74:2b:ff:f9:a9	wired	c9300-2.edge.g2.f2.lab.local.lab.local
8	10.22.0.14	cc:2d:e0:31:38:43	wired	Switch

All Network Devices

Number	Hostname	Reachability	Collection Status	IP Address	type	Mac Address	Boot Time
1	c3850-1.border.g1.f2.lab.local.lab.local	Reachable	Managed	10.22.30.1	Cisco Catalyst38xx stack-able ethernet switch	00:f8:2c:59:41:00	2018-05-23 08:18:30
2	c3850-1.inter.g1.f2.lab.local	Reachable	Managed	10.22.12.99	Cisco Catalyst38xx stack-able ethernet switch	00:9a:d2:f3:8d:00	2018-05-28 22:33:36
3	c3850-2.border.g1.f2.lab.local.lab.local	Reachable	In Progress	10.22.12.103	Cisco Catalyst38xx stack-able ethernet switch	00:9a:d2:cf:ce:80	2018-05-29 09:04:11
4	c3850-2.inter.g1.f2.lab.local	Reachable	Managed	10.22.12.102	Cisco Catalyst38xx stack-able ethernet switch	00:f8:2c:96:d6:80	2018-05-29 08:51:05
5	c3850.edge.g1.f2.lab.local.lab.local	Reachable	Managed	10.22.12.101	Cisco Catalyst38xx stack-able ethernet switch	00:f8:2c:96:f5:80	2018-05-29 07:26:27
6	c9300-1.edge.g2.f2.lab.local.lab.local	Reachable	Managed	10.22.12.97	Cisco Catalyst 9300 Switch	70:6b:b9:c8:36:80	2018-05-28 21:02:18
7	c9300-2.edge.g2.f2.lab.local.lab.local	Reachable	Managed	10.22.12.98	Cisco Catalyst 9300 Switch	a0:f8:49:15:18:80	2018-05-28 21:26:12
8	c9300.edge.g1.f2.lab.local.lab.local	Reachable	Managed	10.22.12.100	Cisco Catalyst 9300 Switch	04:6c:9d:1f:42:80	2018-05-28 21:44:12
9	isr4431.legacy.local	Reachable	Managed	10.22.0.254	Cisco 4431 Integrated Services Router	00:27:e3:1f:f5:e0	2018-04-18 14:10:57
10	Switch	Reachable	In Progress	10.22.0.10	Cisco Catalyst38xx stack-able ethernet switch	00:9a:d2:7c:e7:80	2018-04-14 13:04:28

Abbildung 10.41: DNA Center - Report

11 Ergebnisdiskussion

11.1 Zielsetzungen

Wie in der Architektur 8.1 ersichtlich, wurden zwei Standorte geplant. Auf Grund der aufgetretenen Probleme und Bugs, wurde entschieden sich nur auf die Seite Rapperswil mit mehreren Devices und zwei Gebäuden zu konzentrieren. Hier konnte eine funktionierende Fabric erstellt und Policies implementiert werden. Nachfolgend werden die Ergebnisse der einzelnen Zielsetzungen genauer erläutert. Genauere Informationen zu den dazugehörigen Use Cases, können dem Kapitel Use Cases 6 entnommen werden.

11.1.1 Definition von Benutzerprofilen

Die Definition von Benutzerprofilen wurde umgesetzt, hat aber einiges mehr Aufwand gekostet, als geplant war. Mit dem ISE für die Verwaltung der Benutzeridentitäten und Profile, war einiges notwendig, um den ganzen Ablauf des Policy Enforcements zu verstehen.

11.1.2 Benutzermobilität

Nach dem erfolgreichen Umsetzen der Definition von Benutzerprofilen, konnte in einem weiteren Schritt auch die Benutzermobilität getestet werden. Diese Benutzermobilität funktionierte bei einem Test reibungslos und unglaublich schnell. Nach dem Standortwechsel des Benutzers erhielt er wieder die korrekten Policies und eine bestehende SSH Verbindung überstand den Wechsel.

11.1.3 Reporting der Netzwerkaktivitäten

Mit Hilfe der DNA Center API können regelmässige Reports über den Zustand der Netzwerkumgebung per E-Mail versendet werden. Es konnte in der Arbeit ein sehr rudimentäres Reporting implementiert werden, mit dem lediglich eine Liste aller Netzwerkgeräte, sowie eine Liste aller Hosts mit den wichtigsten Informationen, per E-Mail versendet wird. Leider unterstützt die API des aktuellen Release 1.1.6 noch keine Reportingfunktionen im Assurance Bereich. Diese Erweiterung ist erst im Release 1.2 implementiert, wird aber nach wie vor als EFT gekennzeichnet.

11.1.4 Degradation der Infrastruktur

Die Degradation konnte aus Zeitgründen leider nicht mehr umgesetzt und getestet werden. Es sind aber Informationen von Cisco Experten vorhanden, welche das DNA Center ausgiebig getestet und teilweise schon bei einigen Kunden implementiert haben, mit welchen ein guter Einblick gewonnen werden kann. Die Switches, sowie Server sollten in einem Netzwerk auf jeden Fall redundant vorhanden sein, damit ein Ausfall keine weiterreichenden Probleme verursacht. Der Ausfall des DNA Centers sollte keinen direkten Einfluss auf das Netzwerk haben. Es können allerdings keine zentralen Konfiguration mehr gemacht werden und die Assurance Daten stehen nicht mehr zur Verfügung. Fällt eine ISE aus und es ist keine weiterere mehr vorhanden, können sich die Benutzer nicht mehr am Netzwerk authentifizieren und die Policies sind nicht mehr verfügbar, da diese allesamt nicht im DNA Center, sondern auf der ISE gespeichert sind.

11.1.5 Backup und Restore

Das Backup und Restore funktionierte. Jedoch haben wir beim Lesen der Release Notes 1.2 des DNA Center gemerkt, das vorher anscheinend der Assurance Teil noch gar nicht im Backup inkludiert war. In einer früheren Version des DNA Centers funktionierte das Backup aus unerfindlichen Gründen nicht und brachte das gesamte DNA Center zum Absturz. Dies zeigte sich, in dem nach und nach immer mehr Docker Container abgestürzt sind und aus diesem Grund auch Teile des DNA Centers nur noch teilweise bis gar nicht mehr reagiert haben. Das Abstürzen der Docker Container ging weiter, bis das DNA Center gar nicht mehr erreichbar war. In dem Release 1.1.6 funktionierte das Backup nach mehrmaligem Hinzufügen eines Backup Servers. Auch ein Restore war möglich, jedoch war die Backup Funktionalität nicht zuverlässig.

11.1.6 Anbindung an externe Systeme wie die Identity Services Engine (ISE) und Infoblox

Die externen Systeme, welche in dieser Arbeit verwendet wurden, konnten grösstenteils gut an das DNA Center angebunden werden. Dies war aber auch nur möglich, wenn die genauen empfohlenen Versionen von Cisco eingehalten wurden. So musste beispielsweise die ISE bei einer Neuinstallation eine Version heruntergestuft werden, um die volle Funktionalität und Synchronisation mit dem DNA Center sicherzustellen. Die Anbindung des Infoblox hat ohne Probleme funktioniert, jedoch funktioniert die Kommunikation einzelner Elemente, wie zum Beispiel der IP Adress Pools nur vom DNA Center zum Infoblox. Umgekehrt funktioniert die Synchronisation der IP Adress Pools gar nicht.

11.2 Bugs

Wie bei neuerer Software üblich, sind auch in DNA Center noch verhältnismässig viele Bugs vorhanden. Die Bugs wurden in dieser Arbeit dokumentiert und jeweils an die Cisco Experten weitergeleitet. Teilweise konnten die Bugs mit neuen Releases behoben werden. Bei einzelnen Bugs sind Antworten oder Verbesserungen noch ausstehend.

12 Schlussfolgerungen

12.1 Erreichte Ziele

Zusätzlich zum Ziel das Netzwerk mit Underlay und Overlay aufzusetzen, konnten alle Use Cases praktisch oder theoretisch in der Arbeit abgedeckt werden.

12.2 Mögliche Verbesserungen

Um noch mehr Netzwerkorchestrierung über Programmierschnittstellen zu erreichen sind die kommenden Erweiterungen der API des Cisco DNA Centers unabdingbar. Die in dieser Arbeit bisher aufgetretenen Bugs, sind für eine neue und moderne Software nicht ungewöhnlich, müssen in zukünftigen Releases aber behoben werden.

12.3 Zukunft

Die Verwaltung des Netzwerkes durch einen zentralen Controller, wie das Cisco DNA Center, schafft viel Vorteile. In der Zukunft können sich Netzwerkingenieure mehr auf ertragreiche Aufgaben, wie das Netzwerkdesign und die Überwachung, konzentrieren. Dank des vereinfachten und zentralen Troubleshootings mit der Cisco DNA Center Assurance sind Netzwerkprobleme im Handumdrehen gelöst. Des Weiteren bietet die API in den kommenden Versionen des Cisco DNA Centers die Möglichkeit alle Netzwerkgeräte über eine einzige Schnittstelle zu programmieren und an externe Systeme anzubinden. Der komplexe und aufwändige Zugriff auf jedes einzelne Gerät entfällt.

13 Abkürzungsverzeichnis

AAA Authentication, Authorization, and Accounting

ACI Application Centric Infrastructure

ACL Access Control List

ALT Alternative Logical Topology

AP Access Point

API Application Programming Interface

APIC Application Policy Infrastructure Controller

ARP Address Resolution Protocol

BGP Border Gateway Protocol

CAPWAP Control and Provisioning of Wireless Access Points

CCO Cisco Connection On-line

CIMC Cisco Integrated Management Controller

CLI Command-Line Interface

CMD Cisco Meta Data

CPE Customer Premise Equipment

DDI DNS, DHCP und IPAM

DHCP Dynamic Host Configuration Protocol

DMVPN Dynamic Multipoint VPN

DNA Cisco Digital Network Architecture

DNS Domain Name System

EID Endpoint Identifier

ETR Egress Tunnel Router

GRE Generic Routing Encapsulation

GUI Graphical User Interface

GW Gateway

HTDB Host Tracking Database

IETF Internet Engineering Taskforce

IGP Interior Gateway Protocol

IOS	Internetworking Operating System
IP	Internet Protocol
IPAM	IP-Adress-Management
ISE	Cisco Identity Services Engine
IS-IS	Intermediate System to Intermediate System
ITR	Ingress Tunnel Router
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LISP	Locator/ID Separation Protocol
MPLS	Multiprotocol Label Switching
MR	Map Resolver
MS	Map Server
MSMR	Map Server Map Resolver
MTU	Maximum Transmission Unit
NDP	Network Data Plattform
OSPF	Open Shortest Path First
PETR	Proxy Egress Tunnel Router
PITR	Proxy Ingress Tunnel Router
PnP	Plug and Play
pxGrid	Platform Exchange Grid
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
RLOC	Routing locator
SDA	Software-Defined Access
SDN	Software-Defined Networking
SGACL	Scalable Group Access Control List
SGT	Security Group Tags
SNMP	Simple Network Management Protocol

STP Spanning Tree Protocol

SXP Security Group Tag Exchange Protocol

TFTP Trivial File Transfer Protocol

UDP User Datagram Protocol

URL Uniform Resource Locator

VLAN Virtual Local Area Network

VN Virtual Network

VNI Virtual Extensible LAN Network Identifier

VPN Virtual Private Network

VRF Virtual Routing and Forwarding

VSS Virtual Switching Systems

VTEP Virtual Extensible LAN Tunnel Endpoint

VXLAN Virtual Extensible LAN

VXLAN-GPO Virtual Extensible LAN Group Policy Option

WAN Wide Area Network

WLAN Wireless Local Area Network

xTR x Tunnel Router

A Installationsanleitung

A.1 DNA Center Installation

Teile der nachfolgenden Installationsanleitung wurden aus den Anleitungen [9], [7], [8] entnommen. Informationen die für die Installation nicht relevant sind, wurden weggelassen.
Das DNA Center kann auf zwei verschiedene Modi aufgesetzt werden. Einerseits als Standalone Version oder als Cluster. Beim Cluster werden mehrere DNA Center Instanzen beziehungsweise Appliances benötigt. Diese Installationsanleitung behandelt nur die Variante *Standalone*.

A.2 CIMC Zugang aktivieren

Schritt 1
Um die Installation über KVM durchzuführen zu können, muss zuerst Cisco IMC aktiviert werden. In unserem Fall macht das Cisco IMC DHCP. Die IP Adresse wird über die Leases auf dem DHCP Server ermittelt. (Siehe: [8], *Figure 2. DNA Center Rear Panel LEDs*).

Schritt 2
Anschliessend kann mit folgendem Link (`https://CIMC_IP_ADDRESS`) auf die CIMC zugegriffen werden. Auf diesem muss mit den Standard Anmeldedaten (Benutzername: admin, Passwort: password) eingeloggt werden.

A.3 Konfiguration des Master Nodes

Schritt 1
Nachdem wie im vorherigen Abschnitt beschrieben im DNA Center eingeloggt wurde, kann im Cisco IMC *Host Power* → *Power Cycle* gewählt und bestätigt werden.

Schritt 2
Im Cisco IMC *Launch KVM* → *Java based KVM* auswählen.

Schritt 3
Nun wird der *Maglev Configuration Wizard* angezeigt und es kann *Start a DNA-C Cluster* ausgewählt werden.

Schritt 4
Im nächsten Schritt muss die IP Konfiguration für die DNA Center Appliance angegeben werden. Es muss mindestens ein Interface konfiguriert und als Cluster Link definiert sein. Statische Routen können definiert werden, sind aber optional. Mit einem Klick auf Next erscheint der nächste Konfigurationsschritt im Wizard.

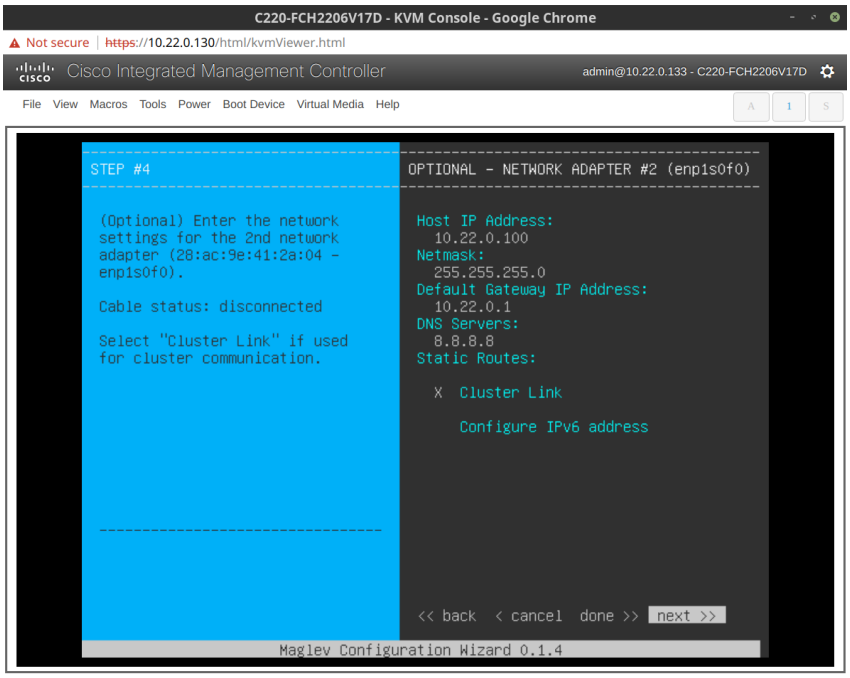


Abbildung A.1: DNA Center Configuration Wizard - Entering Management IP

Schritt 5

Anschliessend kann die virtuelle Cluster IP Adresse hinterlegt werden. Da es sich in diesem Fall um eine Standalone Installation handelt, kann dieser Schritt übersprungen werden.

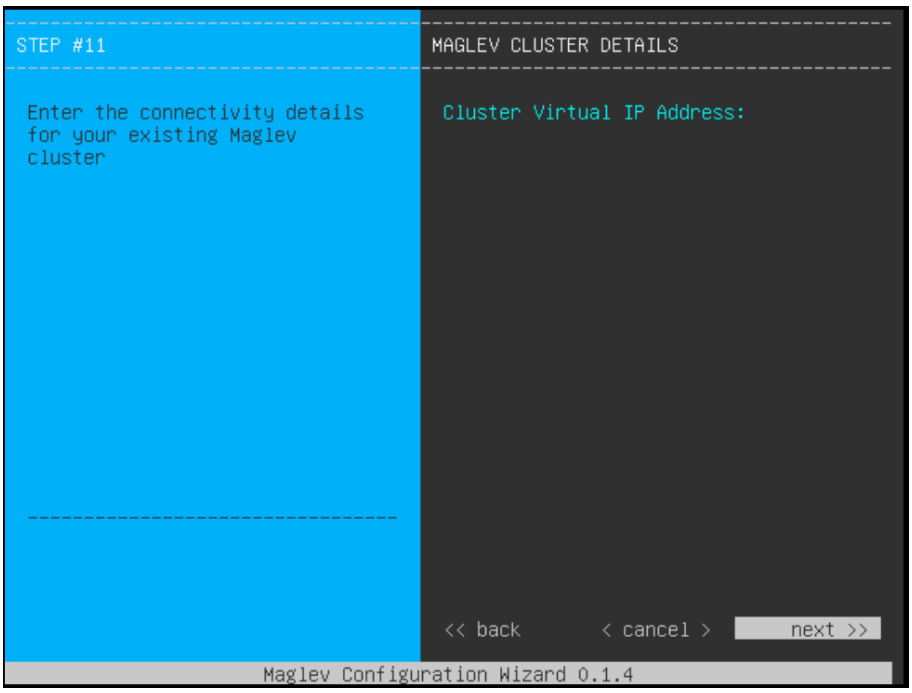


Abbildung A.2: Cisco - Maglev Configuration Wizard - Cluster Virtual IP Address

Schritt 6

In diesem Schritt des Wizards werden alle User Account Einstellungen festgelegt. Hierbei

ist zu beachten, dass das "Linux Password" für den SSH Zugriff benötigt wird und die "Administrator Passphrase" für den Zugang zum Web Interface.

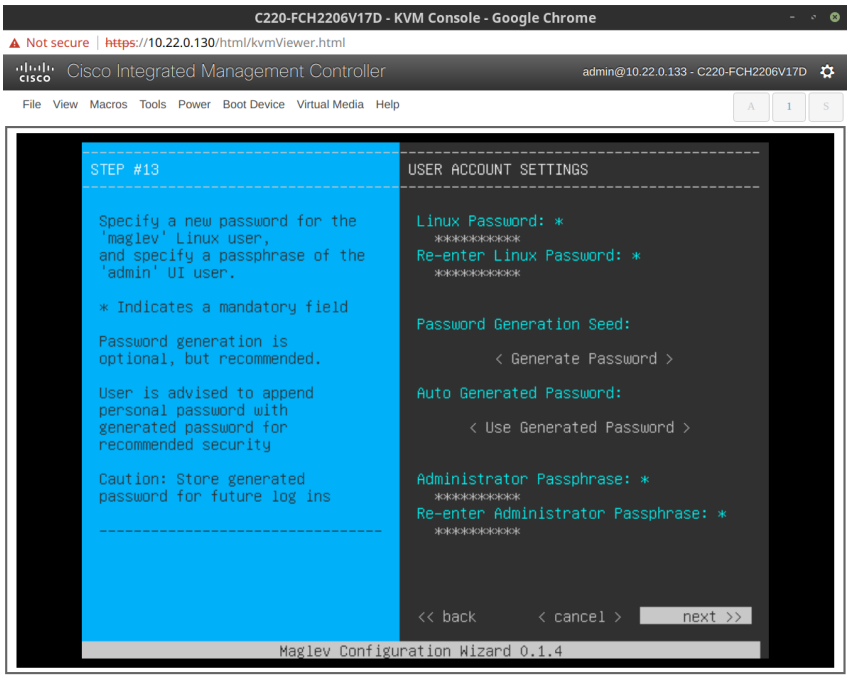


Abbildung A.3: DNA Center Configuration Wizard - Entering Authentification Data

Schritt 7
In diesem Schritt wird der gewünschte NTP Server eingegeben. Im vorliegenden Fall `pool.ntp.org`.

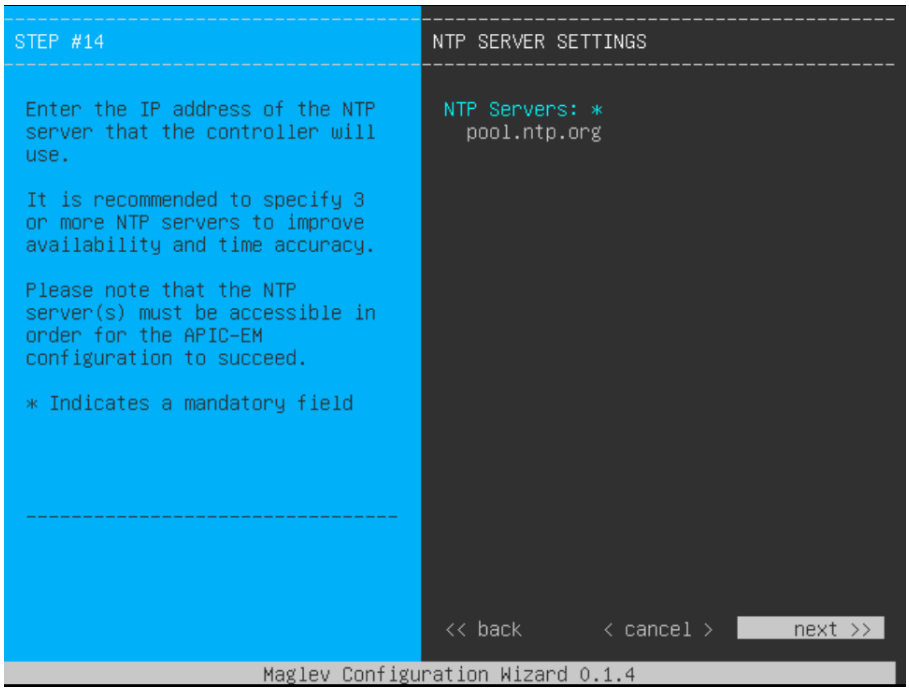


Abbildung A.4: Cisco - Maglev Configuration Wizard - NTP Server

Schritt 8
Das DNA Center benötigt für das interne Netzwerk zwei Subnetze. Dazu müssen die entsprechenden Subnetze eingegeben werden, welche mindestens aus einem /21 bestehen. Diese Netzwerke müssen nicht von ausserhalb erreichbar sein.

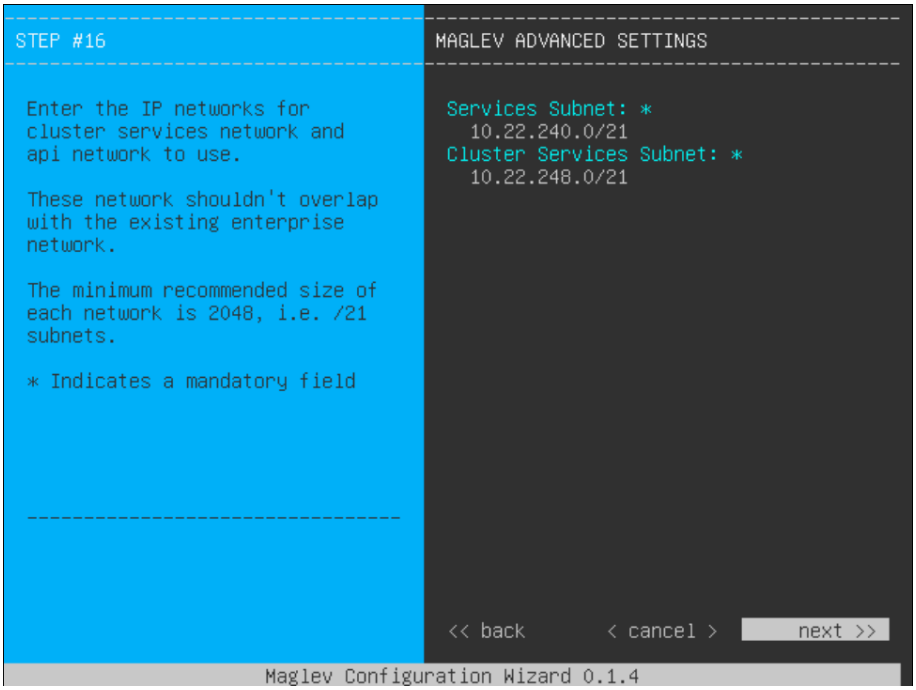


Abbildung A.5: Cisco - Maglev Configuration Wizard - Service Subnet

Schritt 9
Der Wizard wird mit einem Klick auf *next* oder *proceed* abgeschlossen.

Schritt 10
Nun wird das DNA Center aufgesetzt. **Achtung:** Dieser Prozess dauert mehrere Stunden.

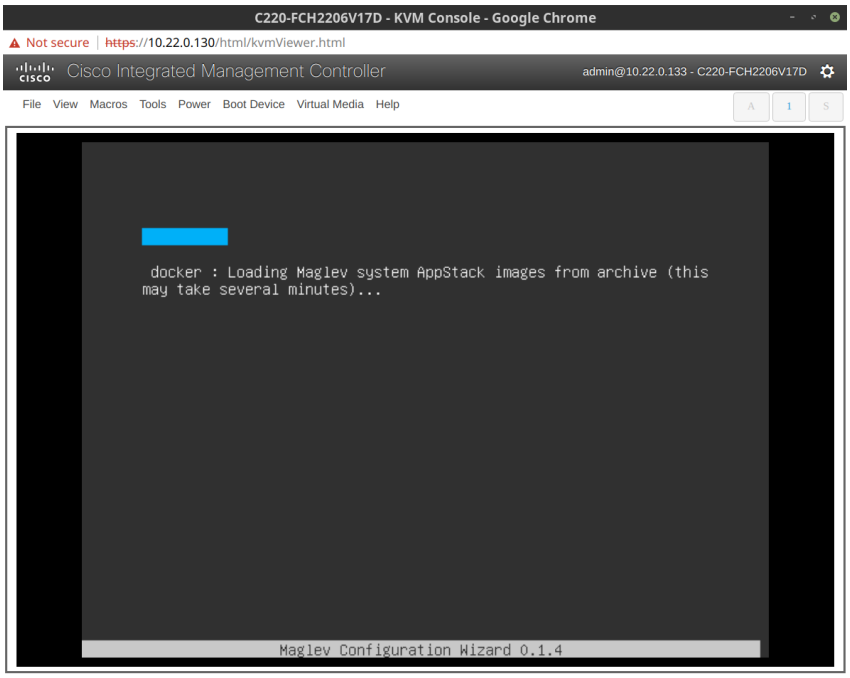


Abbildung A.6: DNA Center Configuration Wizard - DNA Center uses docker

A.4 Einloggen im Web GUI

Nachdem der *Maglev Configuration Wizard* die Installation abgeschlossen hat, kann das DNA Center über das Webinterface aufgerufen werden.
Dazu wird mit einem gängigen Webbrowser die zuvor definierte IP-Adresse aufgerufen. In folgendem Fall `https://10.22.0.100`.
Anschliessend erfolgt das Login mit den im vorhergehenden Schritt definierten Anmeldedaten.

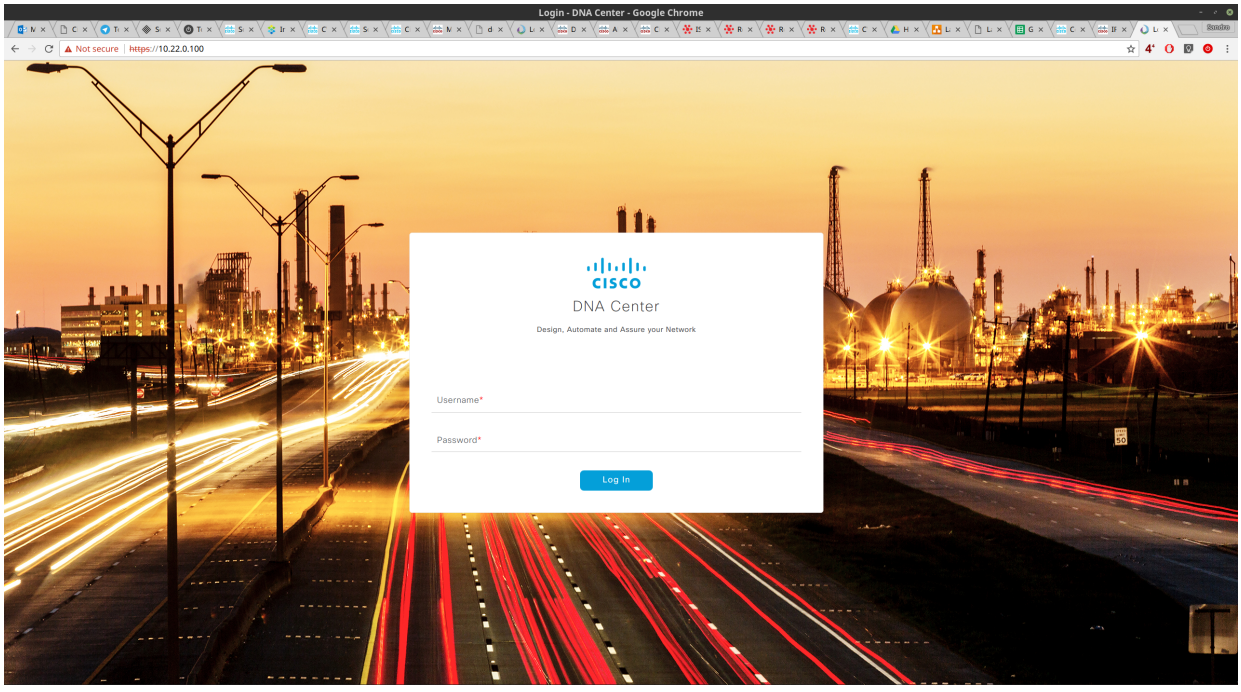


Abbildung A.7: DNA Center Web GUI - Login Seite im Webbrowser

A.5 Cisco Credentials

Gleich zu Beginn verlangt das DNA Center die Cisco Credentials, die mit dem Smart Account verknüpft sind, in welchem die Lizenzen verwaltet werden. Diese Informationen können auch zu einem späteren Zeitpunkt noch eingetragen werden.

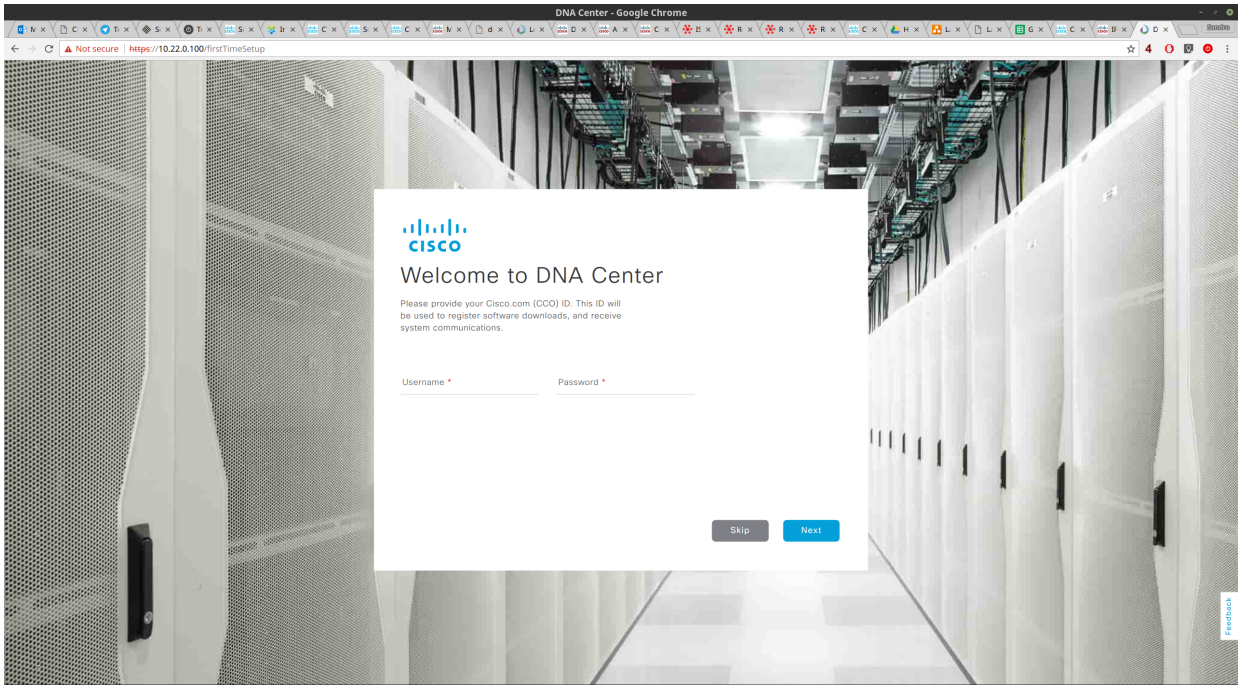


Abbildung A.8: DNA Center Web GUI - Cisco Credentials for Licences

A.6 IP Address Manager - IPAM Server

Im nächsten Schritt kann ein IPAM Server angegeben werden. Diese Einstellung ist optional und kann ebenfalls später angepasst werden.

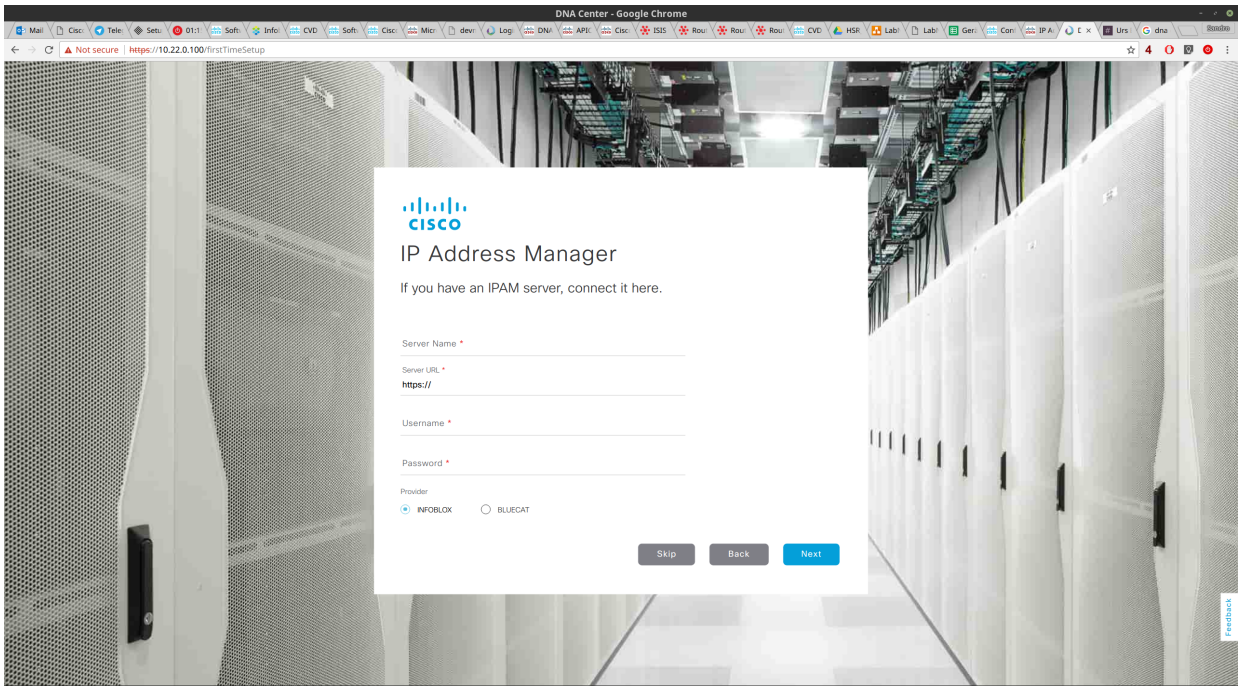


Abbildung A.9: DNA Center Web GUI - Cisco IPAM - Enter Infoblox Credentials

A.7 Terms and Conditions

Im folgenden Abschnitt sind das *Cisco End User Licence Agreement (EULA)* und alle weiteren relevanten *Terms* aufmerksam zu lesen und mit *Next* zu akzeptieren.

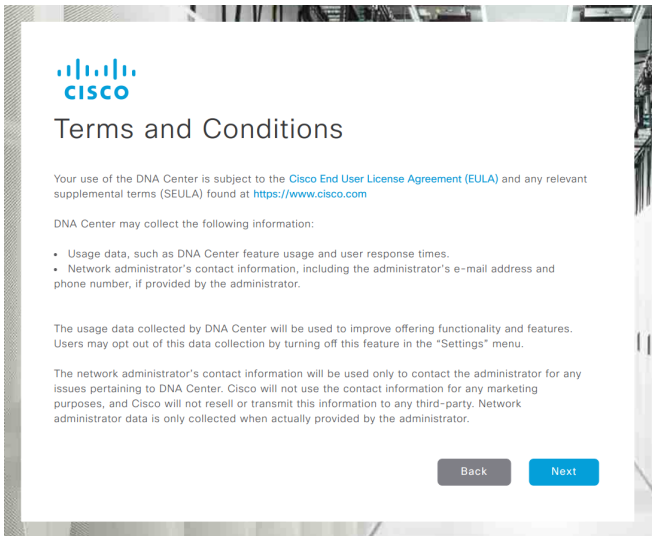


Abbildung A.10: DNA Center Web GUI - Terms and Conditions

A.8 Abschluss

Danach ist die initiale Konfiguration beendet und das DNA Center Dashboard wird angezeigt.

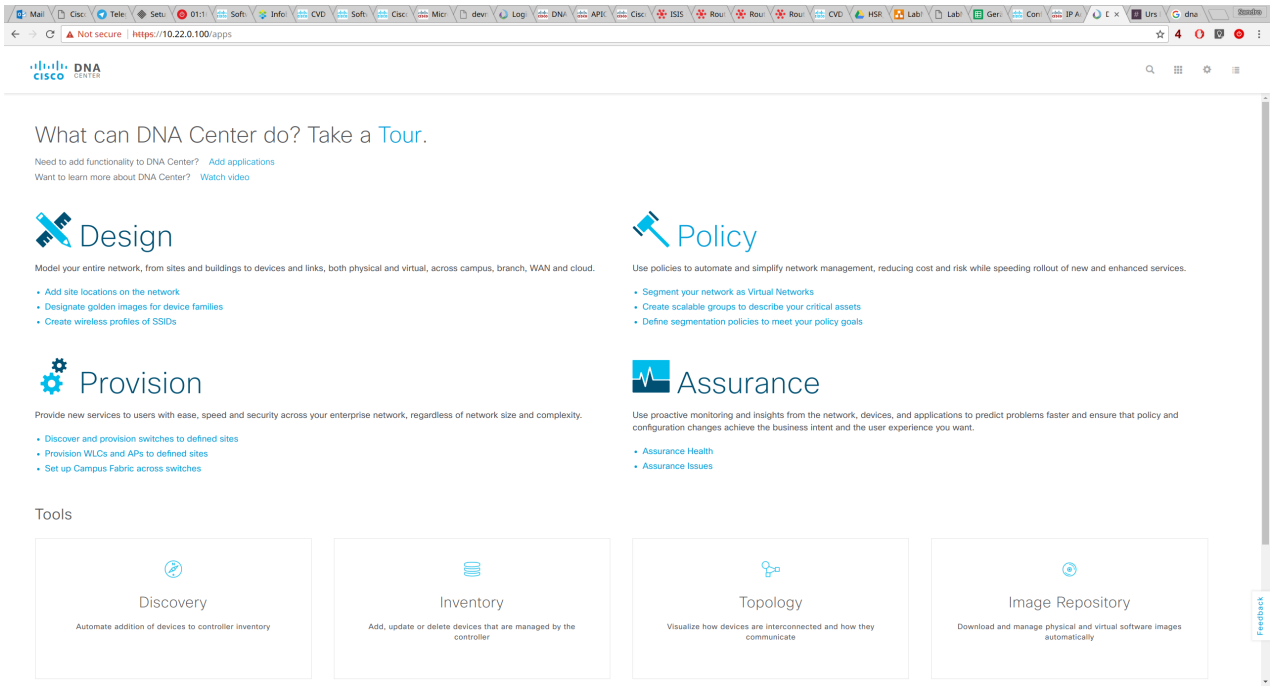


Abbildung A.11: DNA Center Web GUI - Dashboard

A.9 ISE Integration

Für das Identity und Policy Management muss eine Cisco ISE integriert werden. Es gilt dabei zu beachten, dass die Cisco ISE in der richtigen Version vorliegen muss. Genauere Details dazu müssen der aktuellsten offiziellen Installationsanleitung von Cisco entnommen werden, da sich dies bei jedem Release ändern kann. Damit eine Verknüpfung zwischen dem Cisco DNA Center und der Cisco ISE hergestellt werden kann, müssen im Cisco ISE zuerst einige Einstellungen vorgenommen werden. Die genauen Einstellungen für die ISE Integration können der folgenden Anleitung entnommen werden (Siehe: [16]).

A.9.1 ISE Vorbereiten

1. In Cisco ISE einloggen.
2. *Administration* → *Deployment* auswählen.
3. Gewünschten ISE Node auswählen und in der nachfolgenden Ansicht *Enable SXP Service*, *Enable Passive Identity Service* und *pxGrid* mit einem Haken anwählen
4. Speichern drücken
5. Im *Profiling Configuration* Tab muss mindestens *RADIUS* und *SNMPQUERY* ausgewählt sein
6. Unter *Administration* → *Settings* → *ERS Settings Enable ERS for Read/Write* auswählen und mit *OK* bestätigen

A.9.2 Cisco ISE im DNA Center hinterlegen

1. In Cisco DNA Center Web GUI einloggen
2. System Settings auswählen (Zahnrad oben rechts)
3. Cisco ISE Panel auswählen
4. *Configure Setting* wählen

5. Unter *Settings- Auhentication and Policy Servers* auf das grosse Plus (+) drücken
6. Im neuen Dialog Management IP Adresse, Shared Secret, Username, Password, FQDN und Subscriber Name eingeben
7. Update wählen

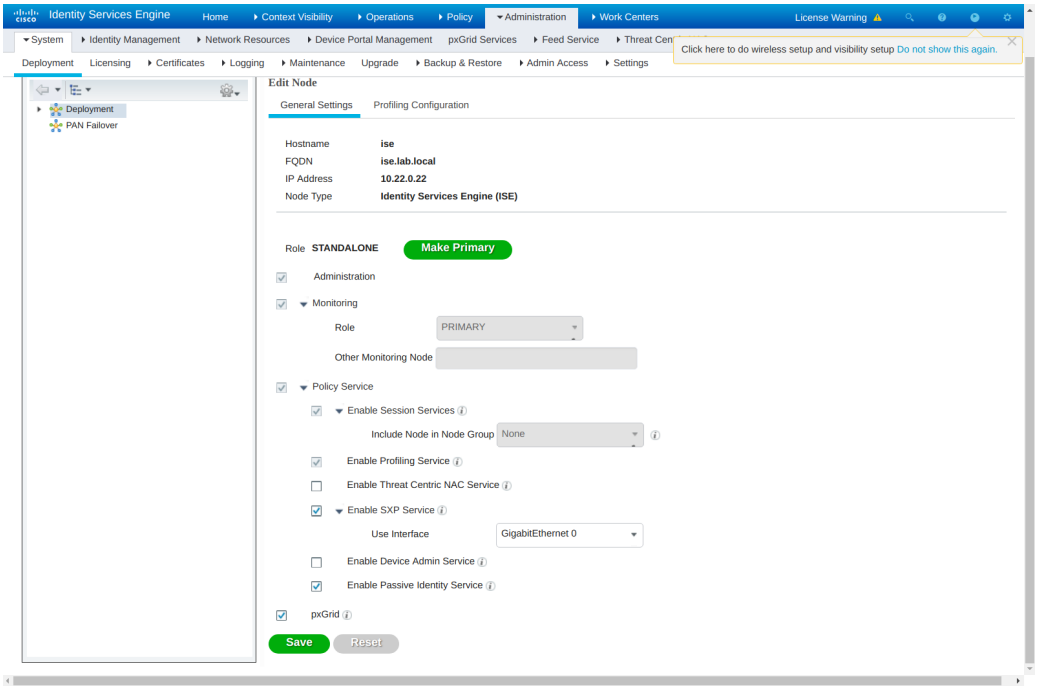


Abbildung A.12: Cisco ISE benötigte Konfigurationen für die DNA Center Verknüpfung

B Benutzerhandbuch

B.1 Updates

Es ist wichtig das DNA Center auf einem aktuellen Stand zu halten, da sehr häufig neue Updates publiziert werden.
Auf folgender Webseite veröffentlicht Cisco die Sicherheitslücken und erklärt gleich zu welcher Version das DNA Center geupdatet werden muss: `https://tools.cisco.com/security/center/publicationListing.x?resourceIDs=233151&apply=1&totalbox=1&pt0=Cisco&cp0=233151#~FilterByProduct`

B.1.1 Updates installieren

1. Ausgehend vom DNA Center Dashboard nach *Settings* → *System Settings* → *App Management* navigieren
2. Das gewünschte System Update oder Package markieren und mittels *Action* → *Download* herunterladen
3. Das heruntergeladene Update markieren und mittels *Action* → *Install* installieren

Es ist zu beachten, dass System Updates immer vor den Package Updates installiert werden müssen. Des Weiteren sollen die restlichen Funktionen des DNA Centers während dem Update nicht verwendet werden.

B.2 Design

Mit dem Design wird die physische Struktur bis auf Gebäudeebene hinterlegt. Zusätzlich werden Konfigurationen hinterlegt, die das DNA Center während der Provisionierung auf die Netzwerkkomponenten schreibt.

B.2.1 Site hinzufügen

1. Ausgehend vom DNA Center Dashboard nach *Design* → *Network Hierarchy* navigieren
2. *Add Site* wählen
3. Im neuen Popup den gewünschten Namen eingeben
4. *Add* anwählen

B.2.2 Gebäude zur Site hinzufügen

1. Ausgehend vom DNA Center Dashboard nach *Design* → *Network Hierarchy* navigieren
2. *Add Site* wählen
3. Im neuen Popup den gewünschten Namen eingeben
4. *Building* anwählen
5. Adresse und/oder Koordinaten eingeben
6. *Add* anwählen.

B.2.3 Netzwerkdienste Konfigurieren

1. Ausgehend vom DNA Center Dashboard nach *Design* → *Network Settings* navigieren.
2. *Global* wählen
3. Bei *AAA Server Network* und *Client/Endpoint* anwählen
4. Bei *Network* → *ISE* wählen und entsprechende IP Adresse eingeben

5. Bei *Network* → *RADIUS* wählen und entsprechende IP Adresse eingeben
6. Bei *Client/Endpoint* → *Servers* → *ISE* wählen und entsprechende IP Adresse eingeben
7. Bei *Client/Endpoint* → *Protocol* → *RADIUS* wählen und entsprechende IP Adresse eingeben
8. Bei *DHCP Server* das **PLUS**-Zeichen anklicken und die IP Adresse des DHCP Servers hinterlegen
9. *SYSLOG Server*, *SNMP Server* und *Netflow Collector Server* können leer gelassen werden
10. Mit einem Klick auf *Save* ist alles abzuspeichern

B.2.4 Device Credentials hinterlegen

1. Ausgehend vom DNA Center Dashboard nach *Design* → *Network Settings* → *Device Credentials* navigieren
2. *Add* wählen
3. *Name*, *Username*, *Password* und *Enable Password* eingeben
4. Mit einem Klick auf *Save* alles abspeichern

B.2.5 IP Address Pools hinzufügen

Das DNA Center benötigt verschiedene IP Adressen Pools. Die Grösse der Pools ist entsprechend der Anforderungen in der Umgebung zu wählen.

- Ein Pool für die LAN Automation (P2P Links, Loopback Adressen)
- Ein Pool für die Border Konfiguration
- Für jedes VN einen Pool

Weitere Pools können jederzeit hinzugefügt werden.

1. Ausgehend vom DNA Center Dashboard nach *Design* → *Network Settings* → *IP Address Pools* navigieren
2. *Add IP Pool* wählen
3. Nun gilt es einen IP Pool Name, ein IP Subnet, ein CIDR Präfix, eine Gateway IP Adresse einzugeben
4. Der korrekte DHCP Server und DNS Server ist per Dropdown auszuwählen
5. Mit einem Klick auf *Save* die Eingaben speichern

B.2.6 Templates erstellen

Um Konfigurationen auf den Geräten vorzunehmen, die nicht vom DNA Center abgedeckt sind, können Templates definiert werden.

1. Ausgehend vom DNA Center Dashboard nach *Template Editor navigieren*
2. **PLUS** Zeichen anwählen und *Add Project* wählen
   Einen Namen für das Projekt angeben und speichern
3. **PLUS** Zeichen anwählen und *Add Template* wählen
4. *Name, Projekt, Device Type und Software Type* wählen und speichern
5. Im Editor die gewünschte Konfiguration eingeben
6. Template mittels *Actions* → *Save* und *Actions* → *Save* speichern

B.2.7 Netzwerkprofile

Netzwerkprofile erstellen Um die erstellten Templates anwenden zu können, müssen Netzwerkprofile erstellt werden.

1. Ausgehend vom DNA Center Dashboard nach *Design* → *Network Profiles* navigieren
2. *Add Profile* klicken und *Switching Profile* wählen
3. *Name* definieren
4. Mittels *Add* die gewünschten Templates hinzufügen

Netzwerkprofile zuweisen Damit die Netzwerkprofile angewendet werden, müssen diese noch den nötigen Sites zugewiesen werden.

1. Ausgehend vom DNA Center Dashboard nach *Design* → *Network Profiles* navigieren
2. In der Zeile des gewünschten Profils auf *Sites* klicken
3. Im neuen Popup alle nötigen Sites über das Multidropdown-Menü hinzufügen
4. Mit *Save* das Netzwerkprofil speichern

B.3 Policies

B.3.1 Virtual Network

Virtuelle Netzwerke dienen der Isolierung der Netzwerkbenutzer und dienen somit der Sicherheit. Standardmässig können Hosts in unterschiedlichen virtuellen Netzwerken nicht miteinander kommunizieren. Mit Hilfe von virtuellen Netzwerken kann das physische Netzwerk in mehrere logische Netzwerk geteilt werden. Ein typischer Anwendungsfall ist die Segmentierung von Gästen, Mitarbeitern und Kontraktor in getrennte Gruppen, so dass der Zugriff nur auf Teile des Netzwerkes erlaubt oder eingeschränkt werden kann. Die verschiedenen Arten von Netzwerken sind:

- Gast-Netzwerk: Netzwerkverbindungen, die von einem Unternehmen zur Verfügung gestellt werden, um seinen Gästen den Zugang zum Internet und zum eigenen Unternehmen zu ermöglichen, ohne die Sicherheit der Unternehmens Infrastruktur zu beeinträchtigen. Gäste können auf das Internet zugreifen, aber nicht auf interne Anwendungen.
- Mitarbeiter-Netzwerk: Netzwerkverbindungen, die den Zugriff auf das Internet und interne Anwendungen ermöglichen. Diese Gruppe kann weiter segmentiert werden, um Zugriffe innerhalb des Firmennetzwerks zu regeln und für spezifische Benutzer und Gruppen einzuschränken.
- Kontraktor-Netzwerk: Netzwerkverbindung, die es den Benutzern ermöglicht, auf das Internet und auf unternehmensspezifische Anwendungen innerhalb des Unternehmensnetzwerks zuzugreifen.

Virtual Network hinzufügen

1. Ausgehend vom DNA Center Dashboard nach *Policy* → *Virtual Network* navigieren.
2. **PLUS** Zeichen anwählen
3. *Virtual Network Name* eingeben
4. Scalable Groups per Drap&Drop in das Virtual Network ziehen
5. Mit *Save* speichern

B.3.2 Scalable Group

Scalable Groups umfassen eine Gruppierung von Benutzern, Endgeräten oder Ressourcen, die dieselben Anforderungen an die Zugriffskontrolle stellen. Diese Gruppen, in Cisco ISE als Sicherheitsgruppen oder SGs bekannt, werden auf dem Cisco ISE definiert.

Scalable Group hinzufügen

1. Ausgehend vom DNA Center Dashboard nach *Policy* → *Registry* → *Scalable Groups* navigieren
2. *Add Groups* wählen
3. In Cisco ISE einloggen
4. *+ Add* anklicken
5. *Name, Icon und Beschreibung* eingeben
6. Mit *Submit* speichern

Die erstellte Scalable Group ist nun auch im DNA Center verfügbar und kann verwendet werden um Policies zu definieren.

B.3.3 Group-based Access Control Policy

Group-based Access Control Policies regeln die Kommunikation zwischen Scalable Groups. Diese Policies können im DNA Center definiert werden und werden mit dem ISE synchronisiert, damit diese den Netzwerkgeräten zur Verfügung stehen.
Das folgende Beispiel zeigt den Prozess der Authentifizierung und Zugriffskontrolle, den ein Benutzer durchläuft, wenn er sich in das Netzwerk einloggt:

1. Ein Benutzer verbindet sich mit dem Netzwerk.
2. Der Benutzer authentifiziert sich am ISE.
3. Der Switch lädt alle relevanten SGTs und SGACLs vom ISE.
4. Dem Benutzer wird der Zugang zu bestimmten Benutzern oder Geräten auf Grundlage der definierten Policies gewährt.

Workflow
Workflow zur Konfiguration einer gruppenbasierten Zugriffskontrollrichtlinie.

Schritt	Aktion
1	Erstellen eines virtuellen Netzwerkes. Abhängig von der Konfiguration des Unternehmens und seinen Zugriffsanforderungen und -beschränkungen können die Gruppen in verschiedene virtuelle Netzwerke unterteilt werden, um eine weitere Segmentierung zu ermöglichen.
2	Erstellen einer skalierbaren Gruppe. Nach der Integration von Cisco ISE werden die in ISE vorhandenen skalierbaren Gruppen in das DNA Center übertragen. Wenn eine skalierbare Gruppe nicht besteht, kann diese direkt angelegt werden.
3	Erstellen eines Contracts. Ein Contract definiert eine Reihe von Regeln, die eine Aktion (erlauben oder verweigern), die Netzwerkgeräte basierend auf dem Datenverkehr durchführen, der bestimmten Protokollen oder Ports entspricht.
4	Erstellen einer *Group-based Access Control Policy*. Die Policy definiert den Zugriffskontrollvertrag, der den Verkehr zwischen den skalierbaren Quell- und Zielgruppen regelt.

Tabelle B.1: Workflow zur Erstellung der Access Control Policies

Erstellen eines Contracts

1. Ausgehend vom DNA Center Dashboard nach *Policy* → *Contracts* → *Access Contracts* navigieren
2. *Add Contract* klicken
3. Im Dialogfenster des *Contract Editor* kann ein Name und eine Beschreibung für den Contract erfasst werden
4. *Implicit Action Deny* oder *Permit* wählen
5. *Port/Protocol* wählen
6. Mit *Save* speichern

Erstellen einer Group-Based Access Control Policy

1. Ausgehend vom DNA Center Dashboard nach *Policy* → *Policy Administration* → *Group-Baed Access Control* navigieren
2. *Add Policy* klicken
3. *Name* und *Contract* angeben
4. *Scalable Groups* für Source und Destination in die gewünschten Felder ziehen
5. Mit *Save* speichern

B.4 LAN Automation

Die LAN Automation nimmt die Netzwerkgeräte mittels PnP in Betrieb und konfiguriert das Underlay Netzwerk für die Fabric und stellt somit das Routing innerhalb des Netzwerks sicher.

B.4.1 Seed Device manuell konfigurieren

Ein Seed Device ist nötig, damit die restlichen Geräte automatisch in Betrieb genommen werden können.

1. VLAN Interface definieren, welches das *Seed Device* mit dem Legacy Netzwerk verbindet und sicherstellt, dass das *Seed Device* vom DNA Center aus erreichbar ist
2. IP Adresse auf dem Loopback Interface konfigurieren (muss für das DNA Center erreichbar sein)
3. Die im DNA Center konfigurierten Device Credentials setzen
4. Ausgehend vom DNA Center Dashboard nach *Discovery* navigieren
   Discovery Name definieren
   Range wählen und eine Range angeben in der sich die Loopback Adresse des Seed Devices befindet
   Preferred Management IP auf *Use Loopback* setzen
5. Discovery mittels *Start* starten

Das Seed Device wird nach dem erfolgreichen Discovery im Inventory auftauchen und kann nun zur LAN Automation verwendet werden.

B.4.2 LAN Automation durchführen

1. Ausgehend vom DNA Center Dashboard nach *Provision* → *Devices* → *Inventory* navigieren
2. *LAN Automation* klicken

3. *Site, Seed Device, IP Pool* wählen
4. Alle Ports wählen, über die weitere Netzwerkgeräte verbunden sind, die mittels *LAN Automation* konfiguriert werden sollen
5. *LAN Automation* mittels Klick auf *Start* starten

Nun wird automatisch ein DHCP Server auf dem Seed Device konfiguriert, der den Geräten mitteilt wo sich der PnP Server befindet.

1. Konfiguration eines Devices mittels *write erase* löschen
2. Gerät mittels *reload* neu starten
   Das Gerät wird während dem Start den PnP Server erkennen und sich automatisch konfigurieren
3. Die Schritte 1 und 2 wiederholen, bis alle Geräte konfiguriert sind

Die Geräte sollten nacheinander in Betrieb genommen werden. Wird dies parallel gemacht, kann es zu Problemen mit PnP kommen. Sobald die LAN Automation auf den Geräten erfolgreich durchgeführt wurde, erscheinen diese im Inventar.

B.5 Provisioning

B.5.1 Fabric erstellen

Im ersten Schritt des Provisionings muss eine Fabric erstellt werden.

1. Ausgehend vom DNA Center Dashboard nach *Provision* → *Fabric* navigieren
2. *Add* klicken
3. *Campus* wählen und einen Namen für die Fabric angeben
4. *Add* klicken um die Fabric zu speichern

B.5.2 Devices zur Fabric hinzufügen

Border + CP Nodes definieren

1. Ausgehend vom DNA Center Dashboard nach *Provision* → *Fabric* navigieren
2. Die gewünschte Fabric wählen
3. Klick auf den gewünschten Border und *Add as Border + CP* wählen
4. *Local AS Number* angeben
5. *Layer 3 Handoff* anklicken und das Interface zum Legacy Netzwerk definieren
   Remote AS und *VNs* angeben
   Save klicken um zu speichern
6. *Add* klicken um den Border Node zu speichern
7. Schritte 3 bis 5 wiederholen falls mehrere Border definiert werden

Auf den Border Nodes wurde nun BGP für die Anbindung an das Legacy Netzwerk konfiguriert. Daher muss auf dem Legacy Device, das mit den Border Nodes verbunden ist, die Gegenseite für das BGP Routing konfiguriert werden.

Intermediate und Edge Nodes definieren

1. Ausgehend vom DNA Center Dashboard nach *Provision* → *Fabric* navigieren
2. Die gewünschte Fabric wählen
3. Klick auf den gewünschten Node und *Add to Fabric* wählen
4. Klick auf den gewünschten Node und *Device Role* definieren

Sobald alle Geräte zur Fabric hinzugefügt sind, kann die Fabric mittels *Save* gespeichert werden.

B.5.3 Netzwerkkomponenten Provisionieren

Damit die definierten Konfigurationen auf die Geräte geschrieben werden, muss das Provisioning ausgeführt werden.

1. Ausgehend vom DNA Center Dashboard nach *Provision* → *Devices* → *Inventory* navigieren
2. Gewünschtes Device markieren
3. Provisioning mittels *Actions* → *Provision* ausführen

B.5.4 Host Onboarding

Virtual Networks auswählen
Um ein Virtual Network verwenden zu können, muss dieses in der entsprechenden Fabric zuerst aktiviert und ein IP Pool zugewiesen werden.

1. Ausgehend vom DNA Center Dashboard nach *Provision* → *Fabric* → *FABRIC_NAME* → *Host Onboarding* navigieren
2. Im Abschnitt *Virtual Networks* werden nun alle gewünschten *Virtual Networks* ausgewählt
3. Im neuen Popup wird der gewünschte IP Pool ausgewählt
4. Der Dialog wird mit einem Klick auf *Update* geschlossen

Ports konfigurieren
Für jeden Port, der nicht bereits für die Konnektivität zwischen den Fabric Nodes verwendet wird, kann ein Addresspool, eine Gruppe und eine Authentifizierungsmethode (Siehe: 10.10.1) definiert werden.

1. Ausgehend vom DNA Center Dashboard nach *Provision* → *Fabric* → *FABRIC_NAME* → *Host Onboarding* navigieren
2. Im *Select Port Assignment* werden für die zu konfigurierenden Ports *Virtual Networks* ausgewählt
3. Für die ausgewählten Ports wird nun ein *Address Pool*, *Scalable Group*, *Voice Pool* und eine Authentifizierungsmethode gewählt
4. Die Änderungen werden mit einem Klick auf *Save* gespeichert

B.6 Debugging

Untenstehend sind die wichtigsten Befehle für das Debugging innerhalb der Fabric aufgeführt.

B.6.1 Policies / Authentication

```
sh cts role-based permissions # Policies anzeigen
sh cts role-based sgt-map vrf VRF_NAME all # Zuweisungen von IPs \
    zu SGTs anzeigen
sh cts role-based counters # Counter der Policies anzeigen
sh cts rbacl # Role Based ACLs anzeigen
sh cts server-list # CTS Server anzeigen
sh AAA servers # AAA Server anzeigen
```

B.6.2 Connectivity / LISP

```
sh ip lisp eid-table sum # EID VRFs anzeigen
sh ip cef vrf VRF_NAME DESTINATION  # Next Hop zu \
    einer Destination anzeigen
sh ip lisp eid-table vrf VRF_NAME map-cache # LISP Map Cache anzeigen
sh ip lisp eid-table vrf Mitarbeiter database # LISP Database anzeigen
sh isis neighbors detail # IS-IS Neighbors anzeigen
sh ip route vrf Mitarbeiter # Routing Table eines VN anzeigen
```

C Projektmanagement

C.1 Projektübersicht

Das Hauptziel dieser Studienarbeit ist die Installation des DNA Centers und Integration eines Campus Labor Netzwerkes.

C.1.1 Ziele der Projektes

Da SDN im Campus Bereich Neuland ist, soll die SDA Lösung vom Hersteller Cisco ausgearbeitet werden. Dazu gehören folgende Ziele:

- Installation von DNA Center und Integration vom Campus Labor Netzwerk
- Definition von Benutzer- und Geräteprofilen, um basierend auf Geschäftsanforderungen die Zugriffsrechte und Netzwerksegmentierung zu verwalten und so das Netzwerk sicher zu halten
- Verwendung von Erkenntnissen von DNA Analytics and Assurance für eine proaktive Überwachung, Fehlerbehebung und Optimierung des Netzwerks
- Integration vom bestehendem IPAM Tool im DNA Center
- Erstellung von wöchentlichen Reports über den Campus Netzwerk Status in einem E-Mail

C.2 Projektorganisation

Diese Studienarbeit wird von drei Personen umgesetzt und durch zwei Betreuer überwacht.

C.2.1 Organisationsstruktur

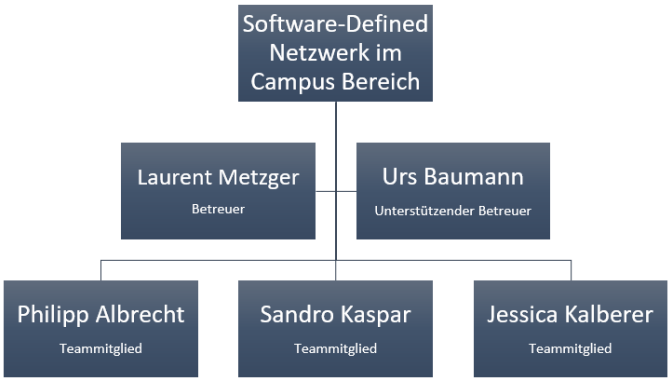


Abbildung C.1: Organisationsstruktur

C.3 Management Abläufe

Für die Umsetzung der Studienarbeit stehen insgesamt 15 Wochen und pro Person 240 Stunden zur Verfügung. In einer Woche liegt das Arbeitspensum von 16 Stunden pro Person vor. Das Projekt startet am 19. Februar 2018 und endet am 15. Juni 2018.

C.3.1 Zeitliche Planung

Die zeitliche Planung, sowie die Verwaltung der Arbeitspakete erfolgte auf Waffle.io. Die Planung wird während dem Projekt laufend aktualisiert und angepasst. Die Arbeitszeiten werden während der Arbeitsausführung mit Toggle erfasst.

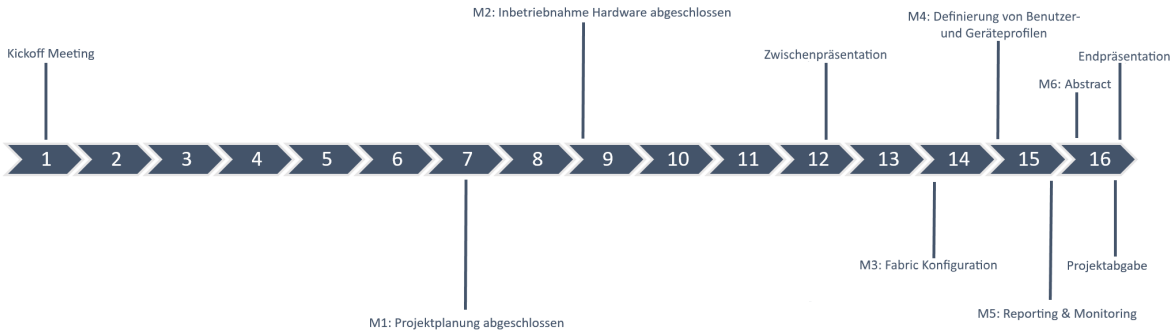


Abbildung C.2: Projektplanung

C.3.2 Meilensteine

Folgende Meilensteine sind für das Projekt definiert:

Nr	Datum	Meilenstein
M0	27.02.2018	Kickoff Meeting
M1	10.04.2018	Projektplanung abgeschlossen
M2	24.04.2018	Inbetriebnahme Hardware abgeschlossen
	16.05.2018	Zwischenpräsentation
M3	01.06.2018	Fabric Konfiguration
M4	10.06.2018	Definierung von Benutzer- und Geräteprofilen
M5	12.06.2018	Reporting und Monitoring
M6	13.06.2018	Freigabe des Abstracts
M7	13.06.2018	Abgabe Projekt
	15.06.2018	Endpräsentation

Tabelle C.1: Meilensteine

C.3.3 Arbeitspakete

Alle Arbeitspakete werden in Waffle.io erfasst und sind unter folgendem Link ersichtlich: https://waffle.io/night28/HSR_SA

C.3.4 Besprechungen

Die Besprechungen mit dem Betreuer finden an den nachfolgend aufgelisteten Tagen statt:

- jeden Dienstag zwischen 15.10 - 16.10 Uhr

Offene Traktanden und Probleme werden mit dem Betreuer diskutiert. Nach dieser Besprechung wird jeweils in einem Team-Meeting das weitere Vorgehen geplant.

C.4 Infrastruktur

Die Organisation der Arbeit und Teammitglieder wird durch folgende Werkzeuge unterstützt:

Abbildung C.3: Übersicht über die Verknüpfung der eingesetzten Werkzeuge zur internen Organisation.

Unsere Tools sind unter folgenden Links einsehbar:

GitHub https://github.com/night28/HSR_SA

Waffle.io https://waffle.io/night28/HSR_SA

Toggl https://toggl.com/

C.5 Risiko Management

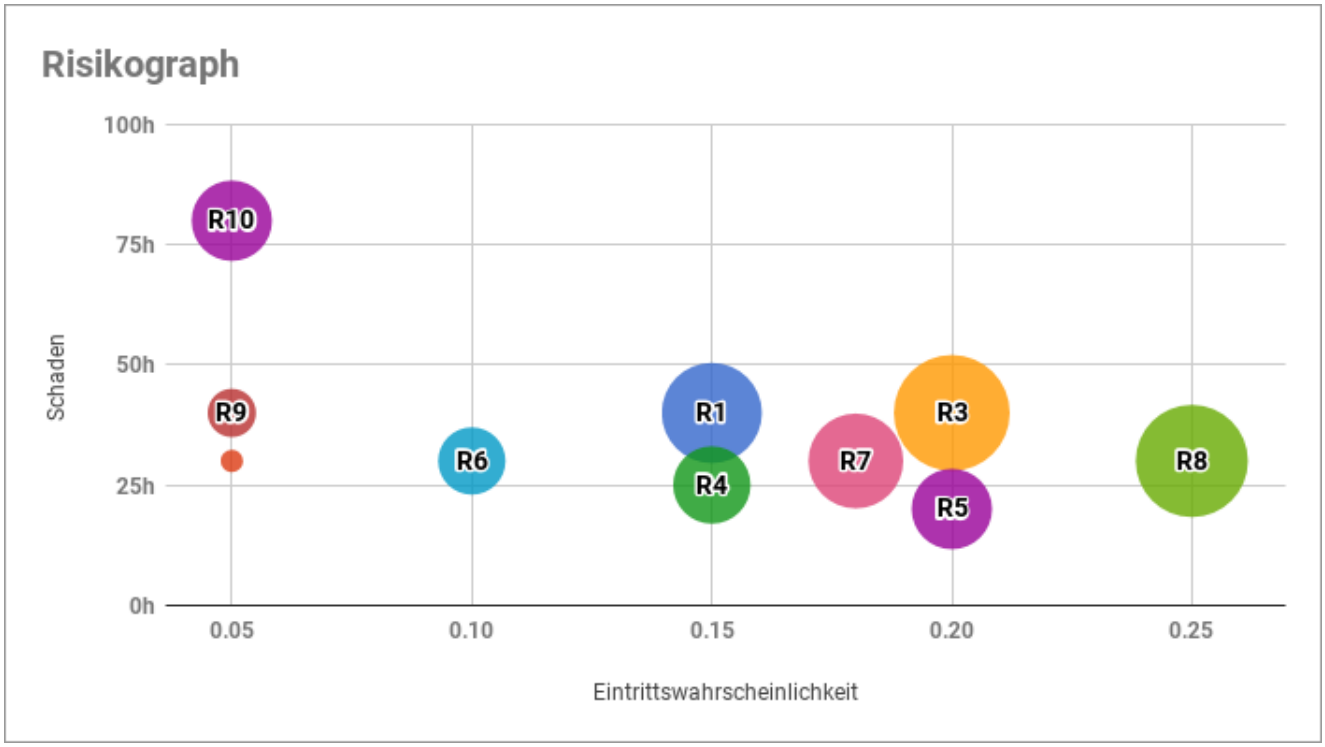
C.5.1 Umgang mit Risiken

Risiken lassen sich nicht vermeiden. Aus diesem Grund sind nachfolgend mögliche Risiken aufgeführt. Des Weiteren wurden vorbeugende Massnahmen definiert, um die Eintrittswahrscheinlichkeit von Risiken mit schwerwiegenden Konsequenzen zu reduzieren. Für den Fall, dass ein Risiko dennoch eintreten sollte, sind entsprechende Massnahmen definiert, um den Schaden möglichst gering zu halten. Sollten sich während dem Projekt neue potenzielle Risiken zeigen, wird dieses Dokument laufend aktualisiert.

C.5.2 Risiken

Nummer	Titel	Beschreibung	maximaler Schaden [h]	Eintritts-wahrscheinlichkeit	Gewichteter Schaden [h]	Vorbeugung	Verhalten beim Eintreten
1	Ausfall eines Teammitglieds	Ausfall auf Grund unvorhergesehener Ereignisse wie Krankheit, Unfall etc.	40	15%	6	Reserven einplanen, Kommunikation sicherstellen, damit andere Teammitglieder die Aufgaben übernehmen können	Tasks des ausgefallen Mitglieds möglichst auf die anderen Teammitglieder aufteilen.
2	Hardwareausfall DNA-Center	DNA-Center Appliance fällt durch Hardwaredefekt aus	30	5%	1.5	keine vorbeugenden Massnahmen möglich	Austausch im Rahmen der Garantie veranlassen
3	Fehlendes Know-How	Da viele der Themen neu sind, kann entsprechendes Wissen fehlen	40	20%	8	Zeit einplanen, um sich in neue Themen einzuarbeiten	Fehlendes Wissen sobald wie möglich aneignen. Bei Bedarf Rat der Betreuer einholen
4	Konflikte oder Missverständnisse im Team	Das Team ist sich bezüglich wichtigen Entscheidungen uneinig	25	15%	3.75	Entscheidungen stets mit Begründung dokumentieren	Kann auch mit Hilfe der Dokumentation keine Einigung gefunden werden, fachlichen Rat des Betreuers einholen
5	Missverständnisse im Team	Im Team herrscht Uneinigkeit über bereits getroffene Entscheidungen	20	20%	4	Protokolle führen und Entscheidungen klar dokumentieren	Protokolle und Dokumentationen beiziehen

6	Ausfall Server / Netzwerkinfrastruktur	Ausfall der von der HSR zur Verfügung gestellten Infrastrukturkomponenten	30	10%	3	Keine Vorbeugenden Massnahmen möglich	Sobald die Infrastruktur wieder verfügbar ist, Systeme erneut in Betrieb nehmen
7	Lieferverzögerung Hardware	Die von Cisco bestellte Hardware kommt später als angekündigt	30	18%	5.4	Keine Vorbeugenden Massnahmen möglich	Projektplanung an neue Gegebenheiten anpassen, notfalls Projektumfang in Absprache mit Betreuer anpassen
8	Zeitaufwände falsch geschätzt	Auf Grund falscher Schätzungen kommt es zu Verzögerungen im Projekt	30	25%	7.5	Laufende Kontrolle des Projektfortschritts um Probleme frühzeitig zu erkennen, Reserven einplanen	Verbleibende Schätzungen korrigieren, Planung anpassen
9	Datenverlust	Verlust von projektbezogenen Daten wie Dokumentationen, Konfigurationen etc.	40	5%	2	Regelmässige und verteilte Backups aller Daten erstellen	Verlorenen Daten aus Backups wiederherstellen, fehlende Daten neu erarbeiten
10	Unausgereifte Software	Verzögerung des Projektes durch unvorhergesehene Hürden, da Software nicht genügend auf Funktionalität getestet und Dokumentiert. Software steht noch in einem frühen Release.	80	5%	4	Über aktuelle Funktionalitäten und Bugs informieren	Bugs reporten und bei Möglichkeit diese umgehen. Falls nötig Unterstützung beim Hersteller suchen.


Risikograph
100h
75h
50h
25h
0h
Schaden
0.05
0.10
0.15
0.20
0.25
Eintrittswahrscheinlichkeit
R10
R9
R6
R1
R4
R7
R3
R5
R8

C.5.3 Eingetretene Risiken

Nachfolgend werden die eingetretenen Risiken genauer erläutert.

Lieferverzögerung Hardware
Leider wurde die Hardware nicht zum geplanten Zeitpunkt geliefert. Deshalb wurde die Projektplanung an die neuen Gegebenheiten angepasst.
Nachfolgend die alte Projektplanung:

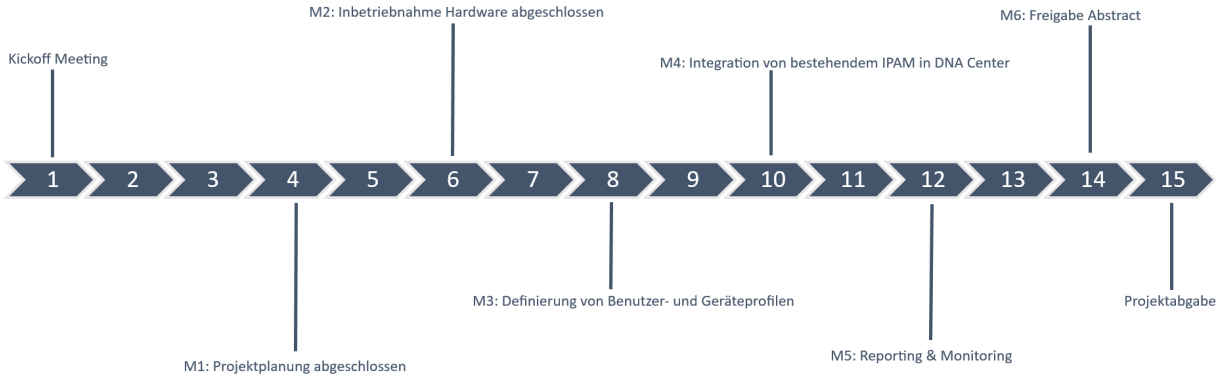


Abbildung C.4: alte Projektplanung

Folgende Meilensteine waren für das Projekt definiert:

Nr	Datum	Meilenstein
M0	27.02.2018	Kickoff Meeting
M1	20.03.2018	Projektplanung abgeschlossen
M2	03.04.2018	Inbetriebnahme Hardware abgeschlossen
M3	17.04.2018	Definierung von Benutzer- und Geräteprofilen
M4	01.05.2018	Integration von bestehenden IPAM in DNA Center
M5	15.05.2018	Reporting & Monitoring
M6	28.05.2018	Freigabe des Abstracts
M7	01.06.2018	Abgabe Projekt

Tabelle C.3: alte Meilensteine

Die neue Projektplanung sieht nun folgendermassen aus:

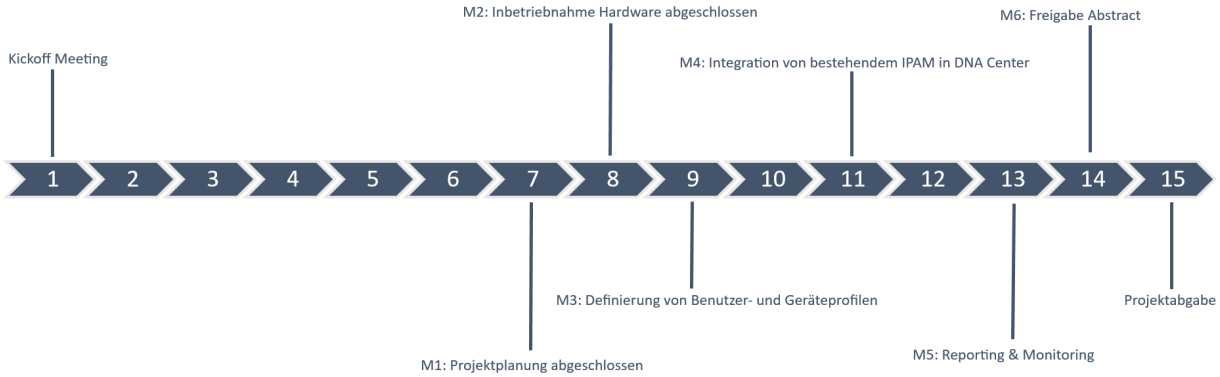


Abbildung C.5: neue Projektplanung

Folgende Meilensteine sind nun aufgrund der Lieferverzögerung für das Projekt definiert:

Nr	Datum	Meilenstein
M0	27.02.2018	Kickoff Meeting
M1	10.04.2018	Projektplanung abgeschlossen
M2	17.04.2018	Inbetriebnahme Hardware abgeschlossen
M3	24.04.2018	Definierung von Benutzer- und Geräteprofilen
M4	08.05.2018	Integration von bestehenden IPAM in DNA Center
M5	22.05.2018	Reporting & Monitoring
M6	28.05.2018	Freigabe des Abstracts
M7	01.06.2018	Abgabe Projekt

Tabelle C.4: neue Meilensteine

Unausgereifte Software und fehlendes Know-How
Das DNA Center befand sich beim Beginn unserer Studienarbeit noch in der Version 1.1.3. Bis zur Abgabe wurde die Version 1.1.6 veröffentlicht, auf welche wir unser DNA Center auch aktualisiert hatten.

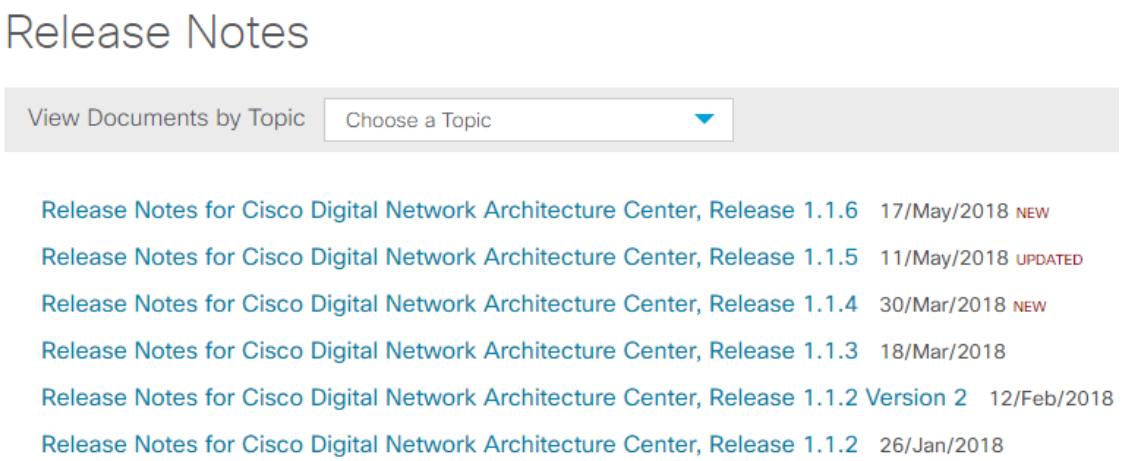


Abbildung C.6: Release Notes

Das DNA Center enthält in diesen frühen Versionen noch viele Bugs und auch Beta Features, welche oft zu Problemen führen können. Die Funktionalitäten sind teilweise nur beschränkt so umsetzbar, wie sie angekündigt und beschrieben wurden. Bei unserem ersten Versuch mit der Version 1.1.3 stiessen wir auf das Problem, dass wir die Geräte über die LAN Automation nicht in Betrieb nehmen konnten, da nicht einmal ein DHCP Server auf dem Seed Device konfiguriert wurde. Weitere Probleme kamen auch beim Provisionierungsprozess hinzu. Geräte welche vorher verwaltet werden konnten, waren auf einmal nicht mehr erreichbar im DNA Center, obwohl dies manuell per SSH kein Problem darstellte. Ein Versuch das DNA Center per Backup zu sichern, brachte das ganze DNA Center zum Absturz. Nachdem viele solche Hürden und Probleme aufgetaucht waren, entschieden wir uns es mit einem Out of Band Management zu versuchen. Hierzu musste der Konfigurations-Wizard des DNA Centers nochmal gestartet werden, um das zweite Netzwerkinterface zu definieren. Das erneute Durchführen dieses Konfigurations-Wizard führte zum kompletten Absturz, so dass die ganze DNA Center Appliance gar nicht mehr startete.
Nach einer zweiten Installation des DNA Centers versuchten wir erneut die LAN Automation auszuführen, um ein Underlay bereitzustellen. Diesmal funktionierte das Hinzufügen eines Seed-Devices. Die LAN Automation soll nach der Konfiguration eines Seed-Devices so oft wie nötig gestartet und gestoppt werden können. Sollte später ein weiterer Switch hinzu kommen, so könnte diese erneut für dieses Device gestartet werden. In unserem Fall führe dies zu Problemen mit der Konfiguration des IS-IS Protokolls. Es wurden nur einzelne Point to Point Interfaces konfiguriert. Aus diesem Grund war für einzelne Geräte keine Kommunikation zum DNA Center möglich. Dies führte bei einigen Konfigurationen zu Verwirrung, da wir teilweise nicht verifizieren konnten, ob es sich um ein falsches Verhalten der Software oder einen Fehler unsererseits handelte. Aus diesem Grund wurde beschlossen, uns für einen Tag einen Cisco Experten zur Verfügung zu stellen. Wir konnten mit ihm die Konfiguration noch einmal von Grund auf durchführen und kamen bis zur Konfiguration eines Seed-Devices für die LAN Automation. An diesem Punkt stiessen wir aber wieder auf diverse Hindernisse, bei welchen uns auch der Cisco Experte zu dieser Zeit nicht weiterhelfen konnte. Nach eigenen weiteren Versuchen gelang es uns jedoch das Problem zu beheben und die LAN Automation auf einem weiteren Gerät durchzuführen. Des Weiteren fehlen Dokumentationen zu der Verwendung von Policies oder der genauen Verwendung der *Authentication Templates* für das *Host Onboarding*. Zur Bedeutung der verschiedenen Authentication Templates konnte uns jedoch der Experte von Cisco

Auskunft geben.
Da bei uns bereits zwei eher schwerwiegende Risiken eingetreten waren, wurde entschieden, dass der Abgabetermin um knapp zwei Wochen, auf den 13. Juni 2018 verschoben wird. Das hatte folgende Anpassungen in der Projektplanung zur Folge:

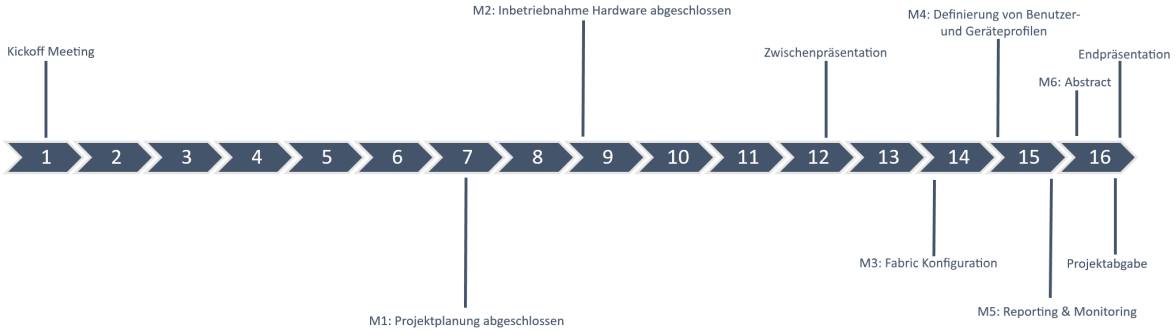


Abbildung C.7: Erweiterte Anpassung der Projektplanung

Folgende Meilensteine sind nun auf Grund der Lieferverzögerung für das Projekt definiert:

Nr	Datum	Meilenstein
M0	27.02.2018	Kickoff Meeting
M1	10.04.2018	Projektplanung abgeschlossen
M2	24.04.2018	Inbetriebnahme Hardware abgeschlossen
	16.05.2018	Zwischenpräsentation
M3	01.06.2018	Fabric Konfiguration
M4	10.06.2018	Definierung von Benutzer- und Geräteprofilen
M5	12.06.2018	Reporting und Monitoring
M6	13.06.2018	Freigabe des Abstracts
M7	13.06.2018	Abgabe Projekt
	15.06.2018	Endpräsentation

Tabelle C.5: Erweiterte Anpassung der Meilensteine

In der Grafik ist ersichtlich, dass die komplette Konfiguration des DNA Centers nach der Zwischenpräsentation stattfand. Geplant war die Fabric Konfiguration schon in der zehnten Woche, jedoch funktionierte zu diesem Zeitpunkt die LAN Automation nicht und die Geräte wurden manuell zum DNA Center hinzugefügt, sodass eine Fabric konfiguriert werden konnte. Kurz vor der Zwischenpräsentation war die Definierung der Benutzer- und Geräteprofile wichtig, da an der Präsentation unter Anderem die Konnektivität zwischen zwei Clients vorgeführt werden sollte. Dies war jedoch wegen mehreren aufgetretenen Fehlern und Problemen nicht möglich. Der Versuch das DNA Center nochmals komplett mit einem Out of Band Management zu konfigurieren scheiterte leider. Der Maglev Configuration Wizard brach am Schluss der Konfigurationen mit einem Fehler ab und brachte das ganze DNA Center in einen "not bootable" Zustand.

Dies war ein guter Zeitpunkt um die komplette Installation des DNA Center von vorne zu beginnen. Durch die vielen aufgetretenen Probleme wurde uns, wie schon oben erwähnt, für einen Tag ein Experte von Cisco zur Seite gestellt. Mit ihm konnten wir die Konfiguration des Underlay Netzwerkes bis zum Definieren eines ersten Seed-Devices durchführen.

D Zeitmanagement

D.1 Zeitaufwand pro Person und Kategorie

Die untenstehende Tabelle zeigt auf, wer wie viel Arbeit pro Kategorie aufgewendet hat.

	Dokumentation	Inbetriebnahme Labumgebung	Meetings	Research	UseCases	**Total pro Person**
Philipp Albrecht	64 h	51 h	48 h	36 h	16 h	**215 h**
Jessica Kalberer	89 h	71 h	62 h	17 h	9 h	**248 h**
Sandro Kaspar	60 h	121 h	56 h	10 h	40 h	**286 h**
Total pro Kategorie	**213 h**	**243 h**	**166 h**	**62 h**	**65 h**	**749 h**

Abbildung D.1: Zeitaufwand pro Person und Kategorie

D.2 Verteilung pro Kategorie

Die nachfolgende Grafik beschreibt die Aufteilung der kompletten Arbeitsleistung in die einzelnen Kategorien.

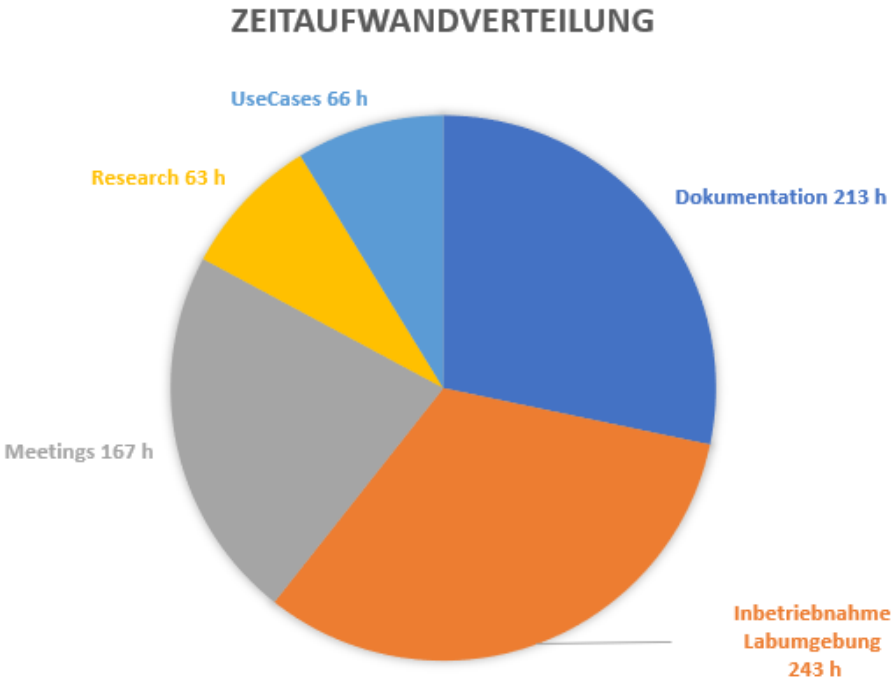


Abbildung D.2: Prozentuale Verteilung nach Kategorie

D.3 Zeitaufwand pro Woche

Im nächsten Bild ist der Zeitaufwand pro Woche ersichtlich. Besonders hervorzuheben ist der Anstieg ab Woche 16, da zu diesem Zeitpunkt die Hardware eingetroffen ist.

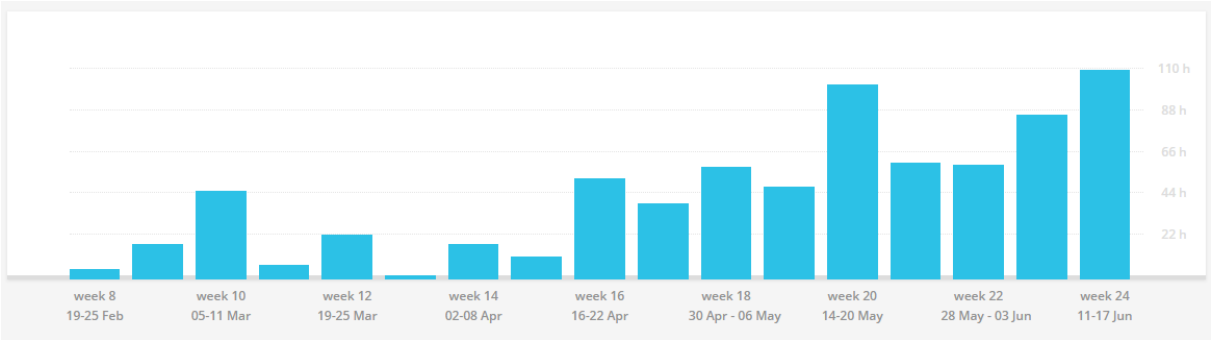


Abbildung D.3: Zeitaufwand pro Woche

E Bugs

Im Folgenden werden Bugs aufgeführt, die während dieser Arbeit aufgetreten sind. Die hier erwähnten Bugs wurden auch via Slack an Cisco gemeldet. Alle erwähnten Bugs beziehen sich auf das DNA Center in Version 1.1.6 und ISE in Version 2.3.

E.1 Backup Server hinzufügen

Komponente	*Einstellungen → System Settings → Backup & Restore*
Priorität	Hoch
Beschreibung	Nach der Eingabe der Backup Server Einstellungen und dem Klick auf *Apply* geschieht nichts. Nach einer Weile stürzen immer mehr Docker Container ab, bis das DNA Center nicht mehr gebraucht werden kann. Ein Neustart des DNA Centers ist erforderlich. **Nachtrag:** Nach mehreren Versuchen mit verschiedenen SSH Servern hat es geklappt. Über die genaue Ursache kann keine Aussage gemacht werden.
Konsequenzen	Beim Ausfall der Appliance können die Einstellungen nicht wiederhergestellt werden.
Workaround	Keiner
Reproduzieren	1. *Settings → System Settings → Backup & Restore* 2. Im Popup *Configure* wählen. 3. SSH Servereinstellungen eingeben 4. *Apply* drücken.
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.1: Bug: Backup Server hinzufügen

E.2 Netzwerkgerät OS Update

Komponente	*Provision → Devices → Inventory*
Priorität	Mittel
Beschreibung	Im DNA Center können OS Images der Netzwerkgeräte aktualisiert werden. Dieser Funktion hat bei allen Versuchen immer zu Fehlern geführt und konnte nicht fertiggestellt werden. **Wichtig:** Im Image Repository muss das Image verfügbar sein.
Konsequenzen	OS Updates müssen manuell durchgeführt werden.
Workaround	Update manuell via CLI mit Hilfe eines TFTP Servers auf dem Netzwerkgerät ausführen.
Reproduzieren	1. *Provision → Devices → Inventory* 2. Gewünschtes Gerät anwählen 3. *Action → Update OS Image* 4. *Im Popup Gerät auswählen → Update*
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.2: Bug: Netzwerkgerät OS Update

E.3 DNA Center Update - Appliance nicht nutzbar während Update

Komponente	*Einstellungen → App Management*
Priorität	Mittel
Beschreibung	Wenn ein *System Update* oder ein *Package Update* durchgeführt wird, kann das GUI des DNA Center nicht verwendet werden. Problematisch: Der Zugriff ist trotzdem möglich. Jedoch sind dann zufällig Funktionen nicht vorhanden oder benutzbar.
Konsequenzen	Appliance nicht nutzbar während Update
Workaround	Während Update GUI nicht verwenden
Reproduzieren	Bedingung: Updates sind verfügbar 1. *Einstellungen → App Management* 2. *System Update* oder *Package Update* wählen 3. Packages auswählen 4. *Install* oder *Update* wählen
Reporter	Philipp Albrecht
Feedback Cisco	Die Empfehlung von Cisco lautet, das DNA Center während Updates nicht zu verwenden.

Tabelle E.3: Bug: DNA Center Update - Appliance nicht nutzbar während Update

E.4 Devices mit Namen "NULL" können nicht gelöscht werden

Komponente	*Provision* → *Devices* → *Inventory*
Priorität	Niedrig
Beschreibung	Nach der LAN Automation kommt es vor, dass Devices mit dem Namen "NULL" erscheinen. Diese können nicht über das Action Menü gelöscht werden, da der entsprechende Button deaktiviert ist.
Konsequenzen	Wenn die Synchronisation nicht funktioniert und das Device neu hinzugefügt werden muss, kann es nicht entfernt werden.
Workaround	"NULL-Device" zusammen mit einem funktionierendem Netzwerkgerät markieren. Die *Action* Schaltfläche wird dann klickbar. Das funktionierende Device deselektieren. Die Schaltfläche bleibt danach weiterhin klickbar und das "NULL-Device" kann über *Action* → *Delete* gelöscht werden.
Reproduzieren	Bedingung: "NULL-Device" in *Inventory* vorhanden 1. *Provision* → *Devices* → *Inventory* 2. "NULL-Device" anwählen 3. Versuchen *Action* Schaltfläche anzuwählen
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.4: Bug: Devices mit Namen "NULL" können nicht gelöscht werden

E.5 https://dnacenter/mypnp *Configurations* nicht löschbar

Komponente	`https://dnacenter/mypnp` → *Configurations*
Priorität	Mittel
Beschreibung	Im myPNP können Konfigurationen nicht gelöscht werden.
Konsequenzen	Annahme: Von dort kommen veraltete Informationen die auf die Netzwerkgeräte geschrieben wird.
Workaround	Nicht vorhanden
Reproduzieren	Bedingung: In myPNP sind Konfigurationen vorhanden. 1. *https://dnacenter/mypnp* → *Configurations* 2. Beliebige Konfiguration anwählen 3. *Delete* klicken
Reporter	Sandro Kaspar
Feedback Cisco	Dieses Feature ist noch in der Beta Phase und offiziell noch nicht verfügbar.

Tabelle E.5: Bug: https://dnacenter/mypnp *Configurations* nicht löschbar

E.6 9xxx Series Lizenzzuordnung

Komponente	*Licence Manager* → *Switches*
Priorität	Mittel
Beschreibung	In der Tabelle *Switch Licence Usage* werden redundante Einträge für Switches der 9xxx Series angezeigt. Einerseits gibt es den Eintrag *Cisco Catalyst 9300 Series Switches* andererseits *Cisco Catalyst 9xxx Series Switches* Ein Gerät mit der Version 9300 fällt demnach in zwei verschiedene *Model*.
Konsequenzen	Die Lizenzen können nicht zugewiesen werden.
Workaround	Nicht vorhanden
Reproduzieren	Siehe Beschreibung
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.6: Bug: 9xxx Series Lizenzzuordnung

E.7 Lizenzanzeige

Komponente	*Licence Manager → Switches*
Priorität	Niedrig
Beschreibung	In der Tabelle *Switch Licence Usage* werden Lizenzen als *Available* angezeigt, die erst in der Zukunft gültig werden.
Konsequenzen	Die Lizenzen können zum aktuellen Zeitpunkt nicht verwendet werden. Die Zahl der *Available Licences* ist nicht korrekt.
Workaround	Nicht vorhanden
Reproduzieren	Siehe Beschreibung
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.7: Bug: Lizenzanzeige

E.8 PNP

Komponente	*Provision → LAN Automation*
Priorität	Mittel
Beschreibung	Während der LAN Automation machen die Switches und Router PNP auf das DNA Center. Dies klappt teilweise nicht und der Switch muss zurückgesetzt und neu gestartet werden. Insbesondere wenn mehrere Geräte gleichzeitig aufgesetzt werden sollen funktioniert dies kaum.
Konsequenzen	Die LAN Automation braucht viel manuelle Eingriffe und ist sehr aufwändig.
Workaround	Nicht vorhanden
Reproduzieren	Mehrere Netzwerkgeräte gleichzeitig via PNP in Betrieb nehmen.
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.8: Bug: PNP

E.9 LAN Automation IP Vergabe

Komponente	*Provision → Devices → Inventory*
Priorität	Mittel
Beschreibung	Wir haben die LAN Automation ein zweites Mal mit einem grösseren IP Pool gestartet. Bei einzelnen Geräten wird aber im DNA Center weiterhin die alte IP angezeigt nachdem diese PNP versucht haben.
Konsequenzen	Die IP Adresse ist ungültig und die Geräte nicht erreichbar.
Workaround	Geräte löschen und Vorgang wiederholen bis die IP Adresse stimmt.
Reproduzieren	Siehe Beschreibung
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.9: Bug: LAN Automation IP Vergabe

E.10 Manuelle Eingriffe Infoblox

Komponente	*Design → Network Settings → IP Address Pool*
Priorität	Niedrig
Beschreibung	Wenn etwas an den IP Pools geändert wird, zum Beispiel das Hinzufügen oder Löschen von IP Pools werden diese Änderungen nicht aktiv, da auf dem Infoblox die entsprechenden Services nicht neu gestartet werden.
Konsequenzen	Die Anzeige im DNA Center zeigt nicht die Realität. DHCP und DNS funktionieren nur eingeschränkt.
Workaround	Die entsprechenden Services auf dem Infoblox Server neu starten
Reproduzieren	Siehe Beschreibung
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.10: Bug: Manuelle Eingriffe Infoblox

E.11 Cisco ISE - TrustSec - Monitor

Komponente	*Work Center* → *TrustSec* → *TrustSec Policy* → *Matrix* → *Monitor All - Off*
Priorität	Hoch
Beschreibung	Wird das Monitoring bei den TrustSec Policy aktiviert/deaktiviert, wird diese Änderung nicht immer auf die Switches geschrieben. Ein zusätzlicher Klick auf *Deploy* hilft nicht. Der ISE meldet, es seien bereits alle Änderungen deployed.
Konsequenzen	Monitoring wird nicht aktiviert oder deaktiviert. Das kann bedeuten, dass auf einzelnen Edge Nodes Policies nicht enforced werden.
Workaround	Auf dem Switch die entsprechende Ports down und wieder up nehmen, sodass dieser die Policies vom ISE pulled.
Reproduzieren	Siehe Beschreibung
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.11: Bug: Cisco ISE - TrustSec - Monitor

E.12 Policies - Contracts - Access Contract

Komponente	*Policy* → *Contracts* → *Access Contract*
Priorität	Niedrig
Beschreibung	Wird ein zuvor erstellter Contract bearbeitet, dauert es mehrere Sekunden bis die Rows mit den Actions angezeigt werden.
Konsequenzen	Kann zu Missverständnissen führen, wenn ein Benutzer davon ausgeht, ein Contract sei leer.
Workaround	Warten
Reproduzieren	Unter *Policy* → *Contracts* einen bestehenden Contract bearbeiten.
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.12: Bug: Policies - Contracts - Access Contract

E.13 Policies - Contracts - Traffic Copy Destination

Komponente	*Policy* → *Contracts* → *Traffic Copy Destination* → *Add Traffic Copy Destination*
Priorität	Mittel
Beschreibung	Wird mittels Policy → *Contracts* → *Traffic Copy Destination* → *Add Traffic Copy Destination* eine neue Destination hinzugefügt und der *Save* Butten geklickt, speichert dies die Eingabe nicht.
Konsequenzen	Es ist nicht möglich Traffic Copy Destinations anzulegen und somit auch keine Traffic Copy Contracts, da die Destinations dafür benötigt werden.
Workaround	Nicht vorhanden
Reproduzieren	Unter → *Contracts* → *Traffic Copy Destination* → *Add Traffic Copy Destination* eine neue Destination hinzufügen und speichern.
Reporter	Sandro Kaspar
Feedback Cisco	

Tabelle E.13: Bug: Policies - Contracts - Traffic Copy Destination

F Persönliche Summaries

F.1 Sandro Kaspar

Ich habe mich schon immer sehr stark für Netzwerktechnologien interessiert und war daher sehr erfreut, dass wir diese Arbeit erhalten haben. Mein Erwartungen an das DNA Center waren hoch, da ich die Verwaltung von traditionellen Netzwerken aus meiner beruflichen Erfahrung kenne und die Vereinfachung, die durch das DNA Center erreicht werden soll sehr vielversprechend ist. Ähnliche Technolgien werden schon länger erfolgreich in Data Center Netzwerken eingesetzt. Daher ist der Ansatz, diese Technologien auch im Campus anzuwenden, die Netzwerke zentral zu verwalten und mit Hilfe von Overlay Netzwerken viel mehr Flexibilität zu schaffen, sicherlich sinnvoll.
Zu Beginn der Arbeit gab es sehr viel Neues zu lernen, was ich als sehr interessant empfand. Als die Appliance dann mit einigen Wochen Verspätung endlich eintraf, wollte ich das gelernte natürlich gleich anwenden und das Produkt ausgiebig testen. Relativ schnell musste ich aber feststellen, dass das DNA Center nicht ist, was ich mir vorgestellt hatte. Es ist ein Produkt, dass noch in den Kinderschuhen steckt und bei dem die einfachsten Funktionen teilweise nicht funktionieren. Es mussten also häufig Workarounds gesucht oder Konfigurationen manuell erstellt werden, die das DNA Center eigentlich beherschen sollte.
Die Arbeit im Team funktionierte meiner Meinung nach gut. Etwas schwierig war sicherlich die Tatsache, dass die Appliance zu spät eingetroffen ist und wir dadurch Zeit aufholen mussten. Zudem kam es öfters zu kleineren Problemen wenn mehrere Personen gleichzeitig mit dem DNA Center arbeiteten.
Zusammenfassend kann ich sagen, dass die Arbeit für mich sehr spannend und lehrreich war. Mit dem Ergebnis bin ich jedoch nicht ganz zufrieden, da ich mir vom DNA Center wesentlich mehr erhofft hatte. Meiner Meinung nach ist dieses Produkt noch nicht bereit für den produktiven Einsatz, bietet aber grosses Potential.

F.2 Philipp Albrecht

Mit der Vorstellung wie klassische Netzwerke konfiguriert werden, bin ich an das DNA Center mit grossen Erwartungen herangetreten. Network Orchestration mit zentralen Kontrollern habe ich bisher nur von Ubiquiti und Cisco Meraki gekannt. Als wir nach langem Warten endlich die Hardware Mitte April bekommen haben, merkte ich, dass meine Erwartungen viel zu hoch waren. Während ich mir wie bei Cisco Meraki eine einfache intuitive "Clicki-Bunti" Lösung vorgestellt habe, stiess ich an ein unintuitives "Etwas", mit komplizierten Lizenzen und haufenweise Bugs. Alle Operationen und Versuche waren geprägt vom langen Warten bis irgendwelche Geräte ihren Reboot durchgeführt hatten und durchstöbern von, als Marketingunterlagen strukturierten, Bedienungsanleitungen. Schnell merkte ich zwei Dinge. Einerseits den Mangel an Erfahrungen und Wissen mit Cisco ISE, LISP, VXLAN und andererseits, dass das effektive Erlebnis mit dem DNA Center weit von den farb-freudigen Marketing Videos auf der Webseite von Cisco abweicht.
Im persönlichen Zeitmanagement kam mit dem späten Eintreffen der Appliance noch ein weiteren Problem. Seit Beginn der Arbeit waren nun schon fast zwei Monate vergangen und plötzlich musste ich viel mehr Zeit in die Semesterarbeit investieren. Da ich Teilzeit studiere, nebenbei arbeite und jeweils von Zürich nach Rapperswil pendle, konnte ich leider nicht einfach plötzlich mehr Zeit für die Semesterarbeit aufbringen.

Alles in Allem fand ich unsere Arbeit sehr spannend. Das Ergebnis hingegen ist ernüchternd. Das DNA Center ist nicht wie erwartet ein fertiges ausgereiftes Produkt, sondern hat noch einige offene Baustellen. Zum Glück hatten wir gegen Ende der Arbeit immer mehr Erfolgserlebnisse. Deshalb habe ich nun gegen Ende der Arbeit eine positive Einstellung gegenüber dieser zukunftsweisenden Lösung.

F.3 Jessica Kalberer

Das Themengebiet Network Design and Security hat mich schon seit Anfang des Studiums interessiert und mich nun in der Studienarbeit vor neue Herausforderungen gestellt. Als ich zum ersten mal vom Cisco DNA Center hörte, war ich fasziniert von der ganzen Appliance. Der Gedanke, dass nun alles zentral über eine einzige Appliance konfiguriert und verwaltet werden könnte, war einfach traumhaft. Am Anfang dieser Arbeit musste ich mich einige Stunden in die Technologien einlesen, da vieles für mich neu war. Bisher kannte ich nur die traditionellen Netzwerk Designs die aus einem Access, Distribution und Core Layer bestanden.
Ende März trat leider ein erstes Problem auf, da die Hardware nicht wie geplant geliefert wurde. Dadurch verschob sich unsere ganze Zeitplanung, da die Hardware schlussendlich erst drei Wochen später bei uns ankam. Gegen Ende April konnten wir dann mit der ganzen Installation und Konfiguration starten. Die Konfiguration des DNA Center war relativ ernüchternd, da vieles noch nicht fehlerfrei funktionierte und darum einiges manuell konfiguriert werden musste. Die anschliessende Zeit war sehr herausfordernd und arbeitsintensiv, aber vor allem auch lehrreich. Durch die aufgetreten Stolpersteine habe ich erneut gelernt, wie fordernd die Arbeit im Netzwerkbereich sein kann. Auch wenn es teilweise etwas mühsam war, verlor es durch die aufgetretenen Hindernisse nie seinen Reiz. Vor allem das Troubleshooting in dieser Tiefe war für mich völlig neu und hat enorm zum besseren Verständnis beigetragen.
Die Arbeit in einem dreier Team empfand ich als angenehm. Es war jedoch teilweise etwas schwierig, wenn Konfigurationen im DNA Center oder auf der ISE gemacht wurden und nicht alle in einem Raum sassen, sodass nicht jeder wusste was gerade gemacht wird. Da das DNA Center fehleranfällig ist, musste immer genau abgesprochen werden, wer was konfiguriert und wann etwas neu gestartet wird. Teilweise funktionierten Ansichten nicht mehr wie vorgesehen oder der ISE wurde wahllos nicht mehr angezeigt. Die Arbeit im Team hatte aber zum Vorteil, dass viele Probleme besprochen werden konnten und immer jemand wusste wie man es anders angehen könnte.
Zum Schluss kann ich sagen, dass es für mich eine sehr spannende, herausfordernde und lehrreiche Arbeit war. Ich bin gespannt was die Bachelor Arbeit für neue Überraschungen bereit hält und freue mich auf die erneute Zusammenarbeit.

Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

[1] RFC7348 *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*, RFC 7348, 2014 (URL: https://tools.ietf.org/html/rfc7348), 07.03.2018

[2] RFC6830 *The Locator/ID Separation Protocol (LISP)*, RFC 6830, 2014 (URL: https://tools.ietf.org/html/rfc6830), 07.03.2018

[3] SDA White Paper *Software-Defined Access 1.0 Solution White Paper*, 2017 (URL: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/white-paper-c11-739642.html), 07.03.2018

[4] SDA Design Guide *Software-Defined Access Design Guide*, 2018 (URL: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Guide-2018JAN.pdf), 07.03.2018

[5] SDA Cisco Definition *Software Defined Access Cisco Definition*, 2018 (URL: https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/index.html), 07.03.2018

[6] Campus Fabric *Cisco Campus Fabric Introduction*, 2017 (URL: https://www.cisco.com/c/dam/m/hr_hr/training-events/2017/cisco-connect/pdf/Cisco-Campus-Fabric-Introduction.pdf), 07.03.2018

[7] *Cisco Digital Network Architecture Center Appliance Installation PDF*, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/install/b_dnac_install_1_1_0P2.pdf)

[8] *Cisco Digital Network Architecture Center Installation Guide, Release 1.2 - Chapter: Install the Appliance* , 2018 (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2/install/b_dnac_install_1_2/b_dnac_install_1_2_chapter_00.html)

[9] *Cisco Digital Network Architecture Center Installation Guide, Release 1.2 - Chapter: Configure the Appliance*, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2/install/b_dnac_install_1_2/b_dnac_install_1_2_chapter_01.html)

[10] *Cisco Digital Network Architecture Center User Guide, Release 1.1*, 2018 (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/user_guide/b_dnac_ug_1_1.pdf)

[11] *Release Notes for Cisco Digital Network Architecture Center, Release 1.1.3* (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/rn_release_1_1_3/b_dnac_release_notes_1_1_3.html), 2018

[12] *Cisco Open Plug-n-Play Agent Configuration Guide - DHCP Option-based Discovery* (URL: https://www.cisco.com/c/en/us/td/docs/

ios-xml/ios/pnp/configuration/xe-3e/pnp-xe-3e-book.html#concept_4A3D8AD59EAE4339B5E7FC7DA73C3594), 10.05.2018

[13] *Cisco Digital Network Architecture Center Appliance Installation Guide, Release 1.0 - Install a New ISO on the Appliance* (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-0-x/app_install_guide/b_dnac_install_1_0/b_dnac_install_1_0_chapter_010.html#concept_dxd_tfy_k1b), 19.05.2018

[14] *Cisco Catalyst 3850 Series Switches FAQ* (URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/qa_c67-722110.html), 22.05.2018

[15] *Cisco Digital Network Architecture Center Appliance Installation Guide, Release 1.1* (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/install/b_dnac_install_1_1_0P2/b_dnac_install_1_1_0P2_chapter_010.html), 28.05.2018

[16] *Cisco Digital Network Architecture Center Appliance Installation Guide, Release 1.0, Chapter: Perform Post-Installation Tasks* (URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-0-x/app_install_guide/b_dnac_install_1_0/b_dnac_install_1_0_chapter_010.html), 11.06.2018

[17] *Infoblox Information* (URL: https://www.infoblox.com/), 04.06.2018

[18] *Infoblox Community Blog about Cisco Integrations* (URL: https://community.infoblox.com/t5/Community-Blog/Infoblox-Cisco-integrations-will-make-you-a-Networking-and/ba-p/12264), 04.06.2018

[19] *Ivan Caduff via Slack, 01.06.2018*

[20] *NAPALM (Network Automation and Programmability Abstraction Layer with Multivendor support) Python Library* (URL: https://napalm.readthedocs.io/en/latest/index.html)

[21] *icinga2 - Icinga Open Source Monitoring* (URL: https://www.icinga.com/products/icinga-2/)

[22] *Software-Defined Access 1.0 White Paper* (URL: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/software-defined-access/white-paper-c11-740585.pdf), 11.06.2018

[23] *Webinar SDA Troubleshooting LISP and Fabric Fundamentals Video* (URL: https://drive.google.com/file/d/1EEa9rdTJwo1WwL0Eyx26pTmh4NzMGzTg/view), 12.06.2018

[24] *Cisco Blog Deutschland - Was ist DNA Center?* (URL: https://gblogs.cisco.com/de/was-ist-dna-center/), 12.06.2018

[25] *Locator ID Separation Protocol (LISP) Overview* (URL: `https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/15-mt/irl-15-mt-book/irl-overview.html`), 12.06.2018

[26] *AVT Tool Archiv* (URL: `https://avt-archiv.hsr.ch`), 12.06.2018