Netzwerk- und System-Management-Projekt

Netzwerk- und Service-Struktur einer Fakultät

Tom Wegener, 18INM/TZ

18. März 2019

Inhaltsverzeichnis

Kapitel 1

Einleitung

Für das Modul Netzwerk- und System-Management (NSM) sollen die Studierenden des Studiengangs Informatik Master"der HTWK Leipzig die Infrastruktur einer Fakultät erstellen, die sich außerhalb des Universitäts-netzes befindet.
Das Projekt soll mit Hilfe von Netkit als virtuelle Infrastruktur realisiert werden und anschließend über Ansible konfiguriert werden. Zuletzt soll ein Bericht zu dem Netzwerk und der Umsetzung verfasst werden.

1.1 Umgebung

Das Projekt wurde nicht innerhalb der VM umgesetzt, sondern für bessere Performance direkt auf einem privaten Rechner. Auf dem Rechner ist eine Linux-Distribution, die auf Ubuntu 18.10 basiert, installiert. Dabei hat Ansible die Version 2.7.8 und nutzt die Python-Version 3.6.7. Anstatt der originalen Netkit-Version wurde Netkit-ng genutzt, welches ein neueres Filesystem nutzt, das auf Debian wheezy basiert. Das war notwendig, um die notwendige Version von Python zur Verfügung zu haben, da Ansible mindestens Python der Version 2.7 benötigt.
Die Verbindung zwischen dem Host bzw. Ansible und den Netkit-VMs wird über SSH realisiert in einer Agent-less Architektur.
Durch die trotzdem veraltete Version des Netkit-File-Systems können einige Sachen nicht wie im Konzept beschrieben umgesetzt werden. Durch ein Update des File-Systems auf eine neuere Debian-Version, kann dies ermöglicht werden. Für dieses Projekt wurde versucht, die bereits vorhandene Software so wenig wie möglich zu verändern. Dementsprechend sind auch nur relevante Applikationen auf den VMs aktuell, es wurde kein generelles Update ausgeführt.

Kapitel 2

Konzept

Es soll die Infrastruktur einer externen Fakultät realsiert werden.

2.1 Anforderungen

Die Fakultät ist in einem weit von der Universität entfernten Gebäudekomplex untergebracht, die Infrastruktur für die Fakultät muss dementsprechend als eigene, unabhängige Infrastruktur behandelt werden. Diese Infrastruktur soll alle notwendigen Dienste der Fakultät beinhalten, wie ein Web-Auftritt, ein Mail-Service und die AAA-Services beinhalten. Das Netzwerk der Fakultät erhält Internet und Anbindung an die Universität über eine sogenannte Dark Fiber-Leitung, diese ist eine bisher ungenutzte und angemietet Leitung eines bereits verlegten Netzes.
Außerdem sollen die einzelnen Server über SNMP über Icinga, Zabbix oder Ganglia überwachbar sein.

2.2 Konzeption

Für das Netzwerk-Konzept wurde eine Struktur mit mehreren getrennten Subnetzen gewählt, das eine einfache Administration gewährleistet, eine Erweiterung erleichtert und es erleichtert sicherheits-relevante Änderungen schnell umzusetzen.
Die Infrastruktur besteht grundlegend aus drei Subnetzen, sowie einem großen Netzwerk. Die Verbindung der Subnetze wird über das Kern-Netzwerk bzw. den Kern-Router ermöglicht. Zusätzlich zu dem Kern-Router hat jedes Subnetzwerk einen Router und der Anschluss über die Dark-Fiber-Leitung wird auch über einen Router realisiert. Die drei Subnetzwerke sind die demilitarisierte Zone (DMZ), das Server-Netzwerk und das Client-Netzwerk. Verbunden wird alles über das Kern-Netzwerk, welches für sich auch ein eigenes Subnetz darstellt. Über dieses Netzwerk werden die verschiedenen Netzwerke verbunden. Die gesamte Infrastruktur ist vereinfacht in der Abbildung 2.1 grafisch dargestellt.
In der Abbildung ist pro Netzwerk nur ein Router eingezeichnet, um die Übersichtlichkeit zu verbessern. Es sollte bei einer Umsetzung bedacht werden, dass es mindestens zwei gibt, um einerseits einen Ersatz bei einem Ausfall zu haben, aber auch, um ein Load-Balancing zu ermöglichen.
Die DMZ stellt alle Dienste bereit, die über das Internet erreichbar sein sollen, also einen Web-Server, einen Mail-Server und einen AAA-Server. Jedoch werden kritische Daten nicht auf Servern in der DMZ gespeichert, sondern sind auf Servern in dem Server-Netzwerk gespeichert, die jedoch über Server aus der DMZ erreichbar sind.
Das Server-Netzwerk ist für die Bereitstellung von Daten und Diensten innerhalb der Fakultät zuständig. Zur Sicherheit sollten keine Daten aus diesem Subnetz direkt den Dark-Fiber-Router passieren, sondern maximal über einen Server der DMZ abgefragt werden und dann weitergeleitet werden. Das Netzwerk enthält den für den AAA-Services benötigten Server, die benötigten Datenbanken, die Incinga-Instanz, sowie den Foreman-Server. Außerdem können spezifische weitere Services in dem Netz realisiert werden.
Die Rechner der Angestellten der Fakultät, sowie der Studierenden der Fakultät, sind alle über das Client-Netzwerk verbunden. Die Administration erfolgt ebenfalls über einen Rechner im Client-Netz oder über den Administrations-Rechner im Server-Netzwerk.
Generell soll das Netzwerk durch das Tool Foreman gemanaged werden. Foreman ermöglicht die Administration von Hosts und kann auch für die Administration von großen Netzwerken samt Routern, Clients und Servern genutzt werden. Über eine Web-Oberfläche wird es ermöglicht einen Überblick zu behalten,

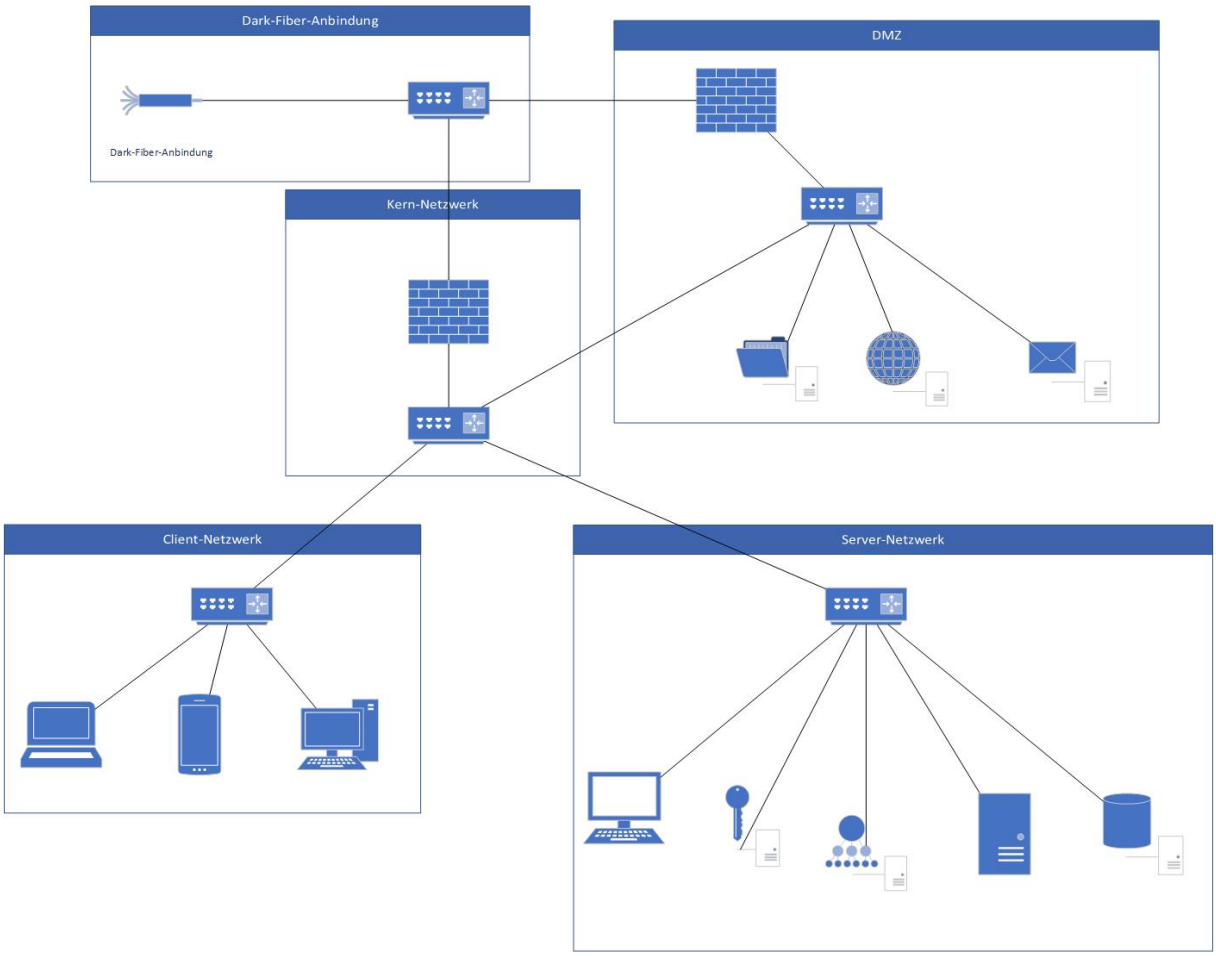

Abbildung 2.1: Modell der Infrastruktur

sowie die Provisionierung und die Konfiguration abzuwickeln. Das Administrationstool wickelt die Konfiguration eigentlich über Puppet ab, kann jedoch durch Plugins erweitert werden, wie dem Ansible-Plugin. Sollte die Software kein anderes Betriebssystem als Ubuntu-Server benötigen kann zusätzlich das kommerzielle Management-Tool Landscape von Canonical benutzt werden. Es ermöglicht eine einfache Administration verschiedener Instanzen und kann die Auslastung, Zustand der Hardware und den Sicherheitszustand anzeigen. Landscape basiert aus einer Agent-Architektur, erfordern also einen Client auf den zu verwaltenden Rechnern.
Außerdem können Foreman und Landscape auch bei der Realisierung von FCAPS helfen.

2.3 FCAPS

FCAPS ist ein Modell für das Management von Netzwerken bzw. Infrastrukturen, es ist ein Akronym für Fault-Management, Configuration-Management, Administration and Accounting Management, Performance Management und Security Management. FCAPS wird in diesem Fall über verschiedene Tools und mit Hilfe von Foreman realisiert.

2.3.1 Fault-Management

Fault-Management bedeutet das frühzeitige Erkennen und Beheben von Fehlern innerhalb des Netzwerkes, das kann durch z.B. eine Icinga-Instanz realisiert werden. Alternativ kann auch ein anderes Werkzeug, wie z.B. Foreman, genutzt werden, welches mehrere Teile von FCAPS in sich vereinigt.
Foreman überprüft die Anwesenheit und Funktionalität von Hosts durch puppet-nodes, außerdem kann durch ein Plugin zentralisiertes Logging umgesetzt werden. Sollte ein Fehler auftreten, der unter eine bestimmte Einstufung, wie z.B. "kritisch" fällt, kann eine Benachrichtigung gesendet werden, außerdem wird auch ein vereinfachtes Handeln unterstützt, solange eine Verbindung zum Host besteht, können Logs abgerufen werden, Konfigurationen erneut angewendet werden oder Updates gefahren werden.
Für ein übersichtliches Logging müssen die Logs in verschiedene Stufen eingeteilt werden. Es empfiehlt sich, diese einerseits nach Gefahr für die weitere Funktionalität einzuteilen, wie auch in die verschiedene Komponenten. So können Logs, wie "critical: infrastructure: lost connection to mail-server" schnell verstanden werden.

2.3.2 Configuration Management

Das Konfigurationsmanagement wird über Ansible abgewicklet. Dabei werden die einzelnen benötigten Dienste als Konfigurationen in playbooks angelegt, die einen entsprechenden Namen haben, sollte ein Host ausfallen, kann in der host-Datei ein neuer Host der entsprechenden Gruppe hinzugefügt werden. Theoretisch können die Konfigurationen der Router ebenfalls über playbooks abgespeichert werden.
Durch eine Integration von Ansible in Foreman über das dazugehörige Plugin kann die Ausführung von playbooks einfach umgesetzt werden, sowie die Ausführung überwacht werden. Die Ergebnisse der Ausführung werden bei Foreman je Host aufgelistet.

2.3.3 Administration and Accounting Management

Administration and Accounting Management

2.3.4 Performance Management

"Performance Management" bedeutet die Überwachung der Performance aller Komponenten des Netzwerkes. Dabei muss die Auslastung der Server, die Gesundheit und das Alter von Festplatten und anderen (Netzwerk-)Komponenten überwacht werden.
Grundlegendes Performanmces-Monitoring kann über Landscape abgewickelt werden, aber auch die Icinga-Instanz kann eine grundlegende Überwachung ermöglichen. Der Foreman-Server kann ähnliche Daten wie die Icinga-Instanz bereitstellen.

2.3.5 Security Management

Security Management bedeutet sich über die Sicherheit der Infrastruktur bewusst zu sein und diese so gut wie möglich zu verbessern. Das beinhaltet die physische, sowie die digitale Sicherheit.

Die physische Sicherheit wird unter Anderem durch eine Zugangskontrolle zu den Räumen in denen die Server stehen erreicht. Jedoch werden noch weitere Schritte benötigt.
Die digitale Sicherheit kann unter Anderem durch IPSec realisiert werden, außerdem muss ein Überblick über wichtige Sicherheits-Updates beibehalten werden und diese durch das Konfigurations-Management aufgespielt werden.
Die Authorisierung für die Dienste und das Netzwerk wird über den AAA-Server realisiert.
Alle über das Internet erreichbaren Dienste können nur über https erreicht werden, während bestimmte Dienste, wie ein File-Server, nur über ein VPN erreichbar sind.
Außerdem wird der Zugriff auf z.B. das Server-Netzwerk aus dem Internet eingeschränkt. Die es kann nur aus dem Client-Netzwerk und der DMZ auf Daten, die auf diesen Servern liegen zugegriffen werden.
Außerdem werden über die beiden Firewalls die Zugriffe zusätzlich beschränkt und verschiedenen IP-Adressen geblockt.
Über Landscape kann überwacht werden, welche Sicherheits-Updates die Software, die auf den Rechnern installiert ist, noch ausstehend sind.

Kapitel 3

Umsetzung

Für die Umsetzung musste statt dem originalen Netkit Netkit-ng genutzt werden, welches python2.7 unterstützt, das für Ansible benötigt wird. Ein Update der Netkit-Instanzen auf python2.7 war auf Grund des Alters des File-Systems nicht möglich.
Es wurde eine wie in 2.1 Topologie erzeugt und über statische Routen eine grundlegende Netzwerk-Kommunikation ermöglicht. Die virtuellen Maschine, die mit "r" enden, sind die Router, die Herzstücke des Netzwerkes bzw. der Subnetzwerke bilden. Außerdem fangen die Namen der Maschinen mit dem jeweiligen Subnetzwerk an, zu dem sie gehören. So ist "server-r" der Router des Server-Netzwerkes, während "server-foreman" der Foreman-Server im Server-Netzwerk ist.

3.1 Darkfiber

Über die VM "darkfiber-r" wird eine Internet-Anbindung realisiert, wie sie in den Anforderungen gefordert wird. Die VM hat drei Anschlüsse, einer ist die Verbindung zu dem Internet bzw. die Dark-Fiber-Anbindung, die zweite Leitung führt zu dem Kern-Subnetzwerk, während die dritte Leitung zu der demilitarisierten Zone führt.

3.2 Kern-Subnetz

Über das Kern-Subnetz werden für alle Subnetze eine Verbindung zu jeweils anderen Subnetzen zur Verfügung gestellt, sowie auch die Verbindung zum Internet.

3.3 DMZ

In der DMZ, also der demilitarisierten Zone, stehen die Server, die über das Internet erreichbar sein sollen. Dementsprechend ist der Web-Auftritt der Fakultät, sowie der Mail-Server und verschiedenen andere Dienste in der DMZ vertreten, aus Sicherheitsgründen werden jedoch personenbezogene Daten aus dem Server-Netzwerk nachgeladen.

3.4 Server-Subnetz

In dem Server-Subnetz sind die verschiedenen Server der Fakultät enthalten, die für Datenspeicherung und Datenverarbeitung benötigt werden. Außerdem sind die Server, die für die Administration des Netzwerkes benötigt werden, wie die Icinga-Instanz und der Foreman-Server, ebenfalls in diesem Netzwerk vertreten. Auf sie kann über den Computer in dem Subnetz zugegriffen werden oder über Computer aus den anderen Subnetzen, jedoch nicht direkt über den Darkfiber-Router.

3.5 Client-Subnetz

Das Client-Subnetz ist mit dem Kern-Subnetz verbunden und kann über den Kern-Router eine Verbindung zu den anderen Subnetzen und zu dem Server aufbauen. Zu dem Client-Subnetz gehören einerseits alle fest verbauten Computer der Computer-Pools, sowie die Computer der Lehrenden und der weiteren

Angestellten. Außerdem sind verschiedenen Wireless-Access-Points auch mit diesem Netzwerk verbunden, darüber können die Studierenden sich mit dem Internet verbinden.

3.6 Ausblick

Kapitel 4

Fazit

Kapitel 5

Anhang

5.1 Glossar

5.1.1 PXE

5.1.2 AAA-Services

"Authentication, Authorization and Accounting"