

Open Source Videokonferenzlösung von der Ostfalia Hochschule für angewandte Wissenschaften

Vom Bericht zum campusSOURCE Online-Workshop „Hochschul-IT in Corona Zeiten“ hin zum „Best Practice“ einer fest in die Hochschul-IT integrierten Lösung

Das Best-Practice Beispiel zum Einsatz der Open Source Videokonferenzlösungen Jitsi und Big Blue Button (BBB) im Rahmen eines Hochschulkontextes mit rund 30.000 aktiven User ist bereits in der fünften Iterationsstufe optimiert. In dieser kurzen Dokumentation wird der Weg bis zur aktuellen Ausbaustufe aufgezeigt – warum wurde welche Veränderung / Optimierung vorgenommen?

Adressaten dieses Dokumentes sind „grundsätzlich Interessierte“ sowie die mit der Evaluation von Videokonferenzlösungen betrauten „Hochschul-Task-Forces“ (Manager / Techniker). Bei letzterer Gruppe geht es primär um die Abschätzung zu der Fragestellung „könnte das hier aufgezeigte System eventuell in unseren Kontext passen?“ ohne dabei in die ganz tiefen Details zu Technik und Kosten zu gehen. Bei Interesse an der hier aufgezeigten Lösung können weitergehende Informationen bei einer persönlichen Kontaktaufnahme ausgetauscht werden.

Die zu dieser Lösung führenden Auswahlkriterien hatten „Datenschutz“ und „Digitale Souveränität“ als äußerst starke Gewichtung. Aufgrund eines seitens des Ostfalia Rechenzentrums (RZ) mitversorgten Instituts, ist das Ostfalia RZ im Punkt „Informationssicherheit“ [TISAX zertifiziert](#). Eine Verwendung von populären VC Systemen wie Office 365, Zoom, etc., bei denen keine direkte Kontrolle über die Kommunikationswege und deren Abhörsicherheit geben ist, schied daher von Anfang an aus.

Diese Entscheidung nahm auch quasi die auf dem aus dem Juli 2020 stammenden EUGH Urteil in der Sache EuGH C-311/18 basierende Strategieempfehlung der EU vom 29.10.2020 voraus „**the EDPS (European Data Protection Supervisor) strongly encourages EUIs to avoid transfers of personal data towards the United States for new processing operations or new contracts with service providers**“ https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en

Die „Eckdaten“ zu den eingesetzten Open Source Systemen finden sich hier:

System	Homepage	About
Jitsi	https://desktop.jitsi.org/	https://de.wikipedia.org/wiki/Jitsi
BigBlueButton	https://bigbluebutton.org/	https://en.wikipedia.org/wiki/BigBlueButton

Ergänzende aktuelle Informationen (Auswahl)

- [Aktuelle Open Source Strategie der EU](#)
- [joinup News zum Thema Videokonferenz](#)
- [Frankreich setzt auf Open Source](#)
- [Strategie der EU als Antwort auf „Schrems II“ \(EuGH C-311/18\)](#)

Bedeutung von Open Source für Open Science

- [Reflektionen zur Europäischen Vision der 3 O's – Open Innovation, Open Science, Open to the world](#)

Stichworte: Datensicherheit, Digitale Souveränität, Open Science, Open Source, Schrems II (EuGH C-311/18), Vendor Lock-In

Bericht

Im Folgenden werden die einzelnen Phasen mit Netzwerk-, Systemkonfiguration und der jeweils verwendeten Hardware aufgelistet und die damit möglichen Leistung in Anzahl von Benutzern, Konferenzen oder auch maximaler Teilnehmerzahl pro Konferenz dokumentiert.

Im Betrieb seit März 2020 haben die ca. 30.150 aktiven User indirekt über den spezifischen Einsatz der zwei Open Source Systeme im Hochschulkontext „abgestimmt“: Big Blue Button wird aufgrund der guten Integration in die Open Source Lehr-/Lernplattformen Stud.IP und moodle intensiv für den strukturierten Austausch im Bereich Lehre und Studium genutzt, Jitsi wird verstärkt für „mal eben“ Meetings genutzt. Interessanter Nebenaspekt: Aufgrund der Jitsi App wird Jitsi gerne durch das Baudezernat der Hochschule genutzt, da ein Mitarbeiter mit seinem Smartphone – welches quasi als tragbare Kamera zum Einsatz kommt – innerhalb der zu betreuenden Liegenschaften vor Ort das zu diskutierende Objekt allen Konferenzteilnehmern vor Auge führen kann – „es müssen nicht alle raus fahren“.

Grundsätzlich existiert im Rechenzentrum an der Ostfalia Hochschule die Devise Open Source Systeme immer bei der Evaluierung von Software mit einzubeziehen und diesen Systemen bei positiver Evaluation Vorrang zu gewähren.

Die Sicherheit der Systeme ist in der jeweils aktuellen Konfiguration gewährleistet. Hier, so sagt Dr. Thorsten Ludewig, wurde von Anfang an ein besonderes Augenmerk darauf gelegt. Aufgezeigte Sicherheitslücken, wie zum Beispiel "[Sicherheitslücke Big Blue Button - Dateien exfiltrieren mit Libreoffice](#)", waren und sind bei der Ostfalia aufgrund der überlegten Installation basierend auf dem vorhandenen Know-How kein Thema.

Phase 1 – März 2020:

Start / Evaluation:

„Ich hatte ein Gespräch mit meinem Präsidium: In zwei Tagen machen wir den Lockdown. Ich hab mir zwei aus meiner Truppe geschnappt und dem einen Jitsi und dem anderen BBB an die Hand gegeben. Erst mal auf uralter Hardware installiert und getestet.“

Dr. Thorsten Ludewig, Leiter des Rechenzentrums an der Ostfalia Hochschule

Die Installation erfolgte nach den Standardanleitungen für „manuelle Installation“, die auf den jeweiligen Projektseiten zu finden sind:

Jitsi: <https://jitsi.github.io/handbook/docs/devops-guide/devops-guide-manual>

Big Blue Button: <https://docs.bigbluebutton.org/2.2/install.html>

Tip: Es ist sehr praktisch sich für alle Fälle ein Wildcard Zertifikat für eine Subdomain auszustellen, sonst „wird man irre wenn man für Alles und Jedes“ ein eigenes Zertifikat beim DFN beantragen muss.

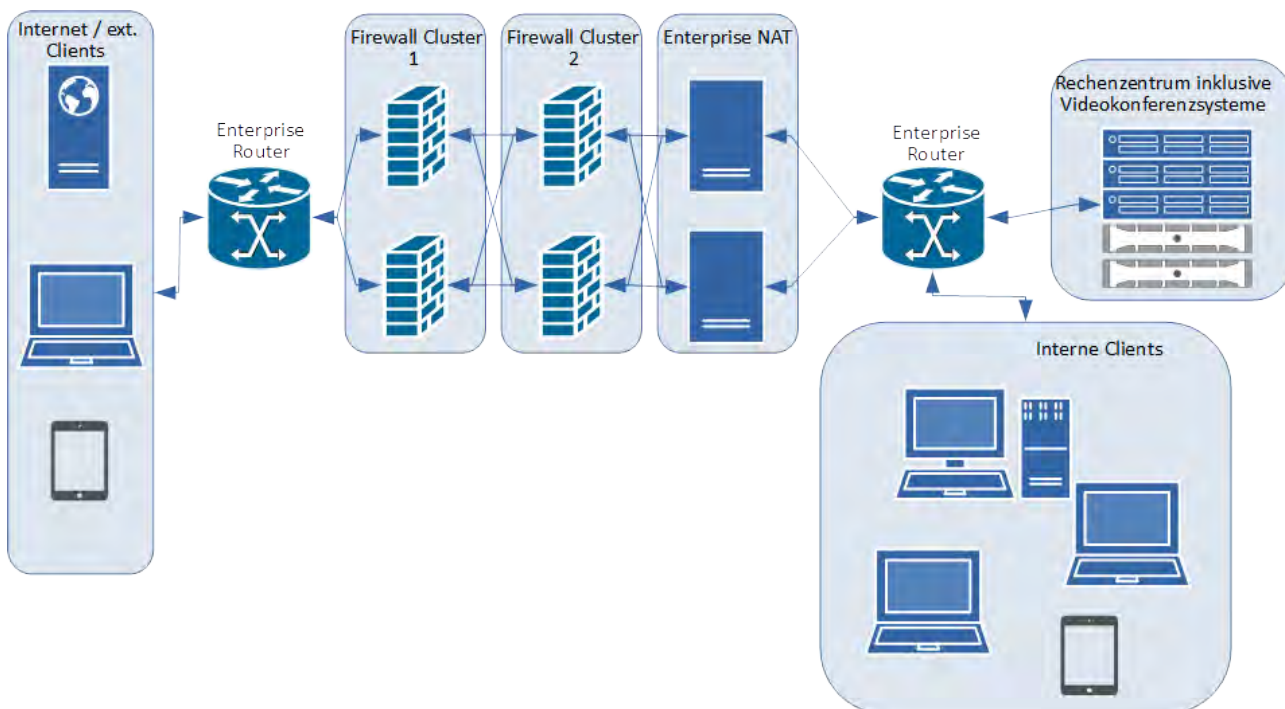
Tipp: „Das als Systemvoraussetzung für BBB genannte Ubuntu 16.04 ist nun wirklich in die Jahre gekommen und die NFS Performance von 16.04 ist nicht sehr gut“. Die Kommunikation mit dem NFS Storage sollte über eine 18.04er Version, besser 20.04er realisiert werden.

Wichtig: Auf jeden Fall sollten eigene STUN / TURN Server verwendet werden, ansonsten wird Google Standardmäßig genutzt und das Thema „Datenschutz“ ist wieder aufgeweicht – um es vorsichtig zu formulieren. (STUN/TURN, siehe z.B. [Artikel auf Wikipedia](#) oder die [Installationsanleitung](#) auf den BBB Seiten)

Unterstützung bei der BigBlueButton Umsetzung kam auch vom [ELAN e.V.](#)

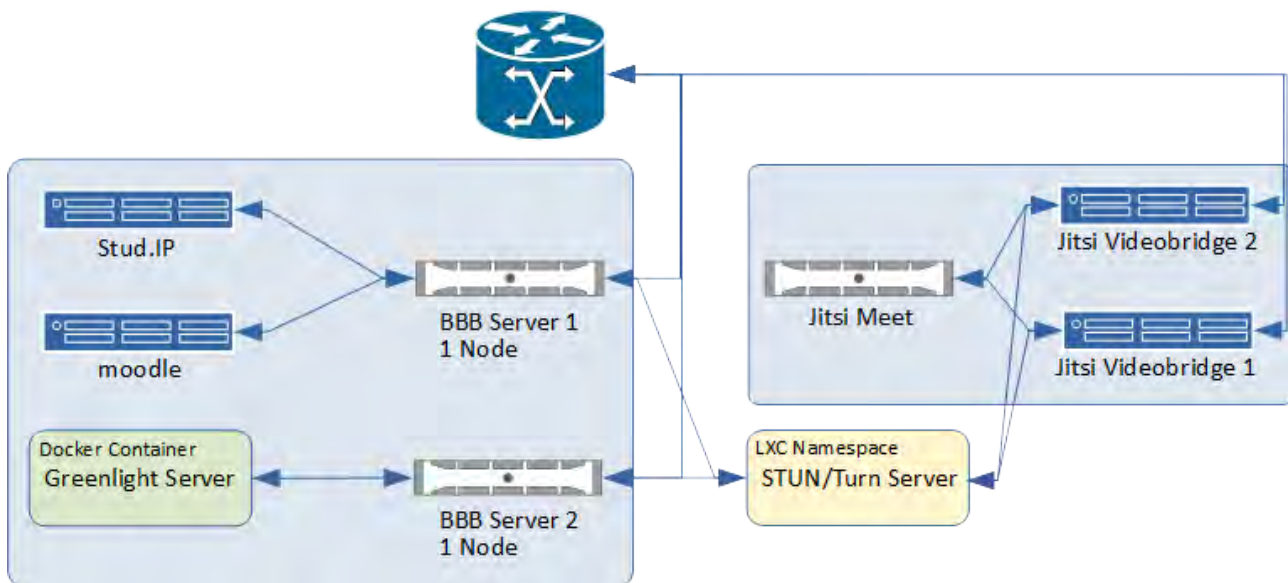
Nach der ersten Evaluation wurde nachfolgende Konfiguration für den Start gewählt:

Konfiguration März 2020 - Netzwerk



Die Enterprise NAT Systeme dienen der breiten Anwendung größerer privater Netzwerksegmente innerhalb der durch das Ostfalia Rechenzentrum angebundenen Institutionen. Es lassen sich aus der Sicht des Internets hinter diesen Systemen sehr viele IP Adressen verstecken.

Konfiguration März 2020 - Videokonferenzsysteme



Die Instanzen der einzelnen Systeme wurden dabei in LXC Containern virtualisiert (<https://de.wikipedia.org/wiki/LXC> oder <https://linuxcontainers.org/lxc/introduction/>). Diese Art der Virtualisierung ist deutlich performanter als virtuelle Maschinen. Denn im Gegensatz zu virtuellen Maschinen erzeugt LXC eine virtuelle Umgebung, die zwar ihre eigenen Prozesse besitzt, doch für diese gemeinschaftlich den Kernel des Hostsystems nutzt. In den LXC Containern wurden bei den Ubuntu 16.04 Systeme alle unnötigen Services in Host und Nodes abgeschaltet – auch die Firewall. Die SSH des jeweiligen LXC ist ausschließlich über die Admin-Ethernet-Schnittstelle des jeweiligen BBB Servers erreichbar.

Der [Greenlight](#) Server („Big Blue Button Oberfläche“) dient zur Benutzung von Big Blue Button unabhängig von einem führenden System wie Stud.IP oder moodle, er läuft in einem [Docker-Container](#) auf dem [Kubernetes](#) Cluster des Ostfalia Rechenzentrums und benötigt kaum Ressourcen. Er ermöglicht:

- Authentifizierung, hier Anbindung an lokalen [LDAP](#)
- Erstellen und Verwalten von Videokonferenzräumen
- „Warteraumfunktionalität“
- Einladung anderer Teilnehmer durch Benutzung einfacher URLs

Die Hardware-Konfiguration der BBB & Jitsi Server war zu der Zeit wie folgt: Ca. 5 Jahre alte DELL 730 Maschinen mit 56 Cores und 128 GB Hauptspeicher. Die Greenlight Instanz lief in einem Docker Container, der eine TURN Server mit auf der BBB Maschine.

In Phase 1 war damit folgende Auslastung möglich - Werte erfasst am 12.05.2020 (Siehe Grafik):

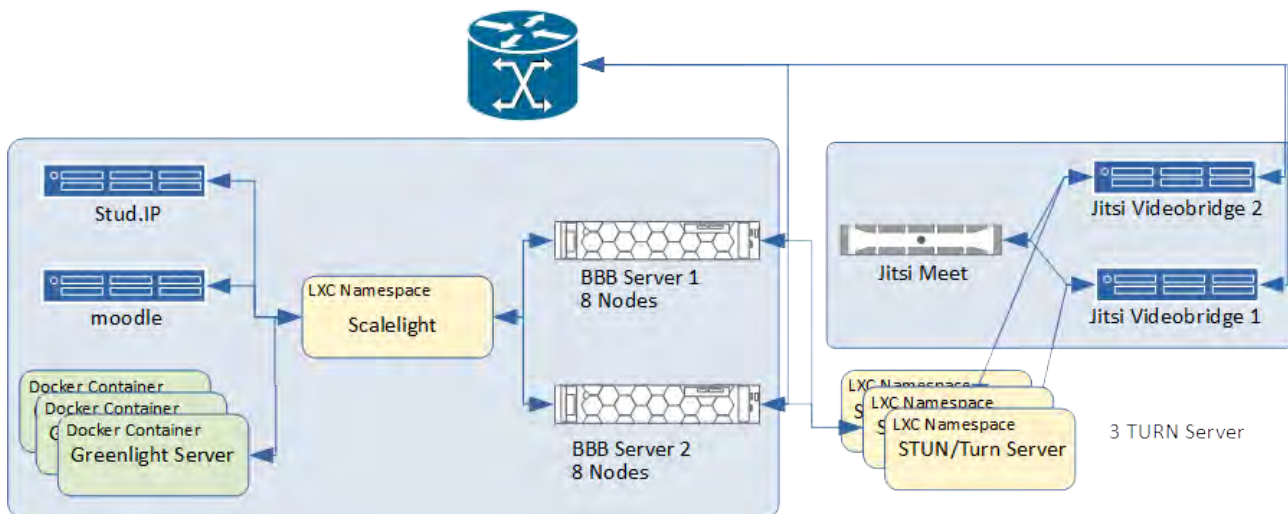
- In Summe 4.591 Unique Users an dem Tag
- In Summe 142 Meetings an dem Tag (Jitsi & BBB)
- Größte Konferenz an dem Tag mit 65 Usern
- In der Spitze 697 User gleichzeitig auf BBB Server 1

Anm.: Das Open Source Skript zur Erfassung der statistischen Daten (<https://github.com/thorsten-l/sonia-app-bbb2influxdb>) arbeitet mit Grafana (<https://de.wikipedia.org/wiki/Grafana>), einer plattformübergreifende Open-Source-Anwendung zur grafischen Darstellung, zusammen.



Das Videokonferenzsystem lief (fast) stabil mit bis zu 4.591 eindeutigen Benutzern pro Tag (Erfasster Spitzenwert). Immer Mittwochs um 11:00 Uhr gab es einen Ausfall – warum? Als Ursache wurden die Cisco Catalysts identifiziert. Der Grund konnte jedoch nicht tiefer analysiert werden.

Insgesamt konnte die Leistungsfähigkeit der aufgesetzten Systeme - in Verbindung mit dem vor Ort vorhandenen Know-How - den Anwenderkreis überzeugen und es wurde entschieden diese Systeme aufgrund der weiteren Entwicklung der COVID-19 Epidemie und der weiter steigenden Anforderungen auszubauen.

Ausbaustufe 2 – Ende Mai 2020:

Hier wurde die Hardware aufgestockt und es kamen für Big Blue Button zwei Systeme mit jeweils 1 TB RAM und 128 Threads zum Einsatz. Die Hardwarekonfiguration der BBB Server (64 Cores, 128 Threads) war dabei folgendermaßen ausgelegt (Weitere Details zu dem Server finden sich im Anhang):

Dell Server 1024GB 2 HE Chassis mit 12x 3.5" HDD-Slots,

- 4 x 8HLPCIe-Slots,
- 2 x AMD EPYC 7542 (2.9GHz/32-Core/64-Threads/128MBCache) CPU,
- 32x 32GB RDIMM, 2300MHz,
- 8 x 8TB NLSAS-HDD (12Gb/s, 7200UPM),
- 2 x 480TB SAS-SSD (MU, PM5-V),
- 2 x 240TB SATA-SSD (MU, S4610),
- 1x RAID-Controller,
- 1x 1GBaseT onBoard,
- 2x SFP+ OPC NIC,(2 x 10 Gigabit NIC) - werden per Trunking zusammengefasst
- 1x iDRAC9 Enterprise-Service-Prozessor

Inklusive eines 5 Jahre „vor Ort Service“ liegen die Kosten pro Maschine bei rund 30.000 €.

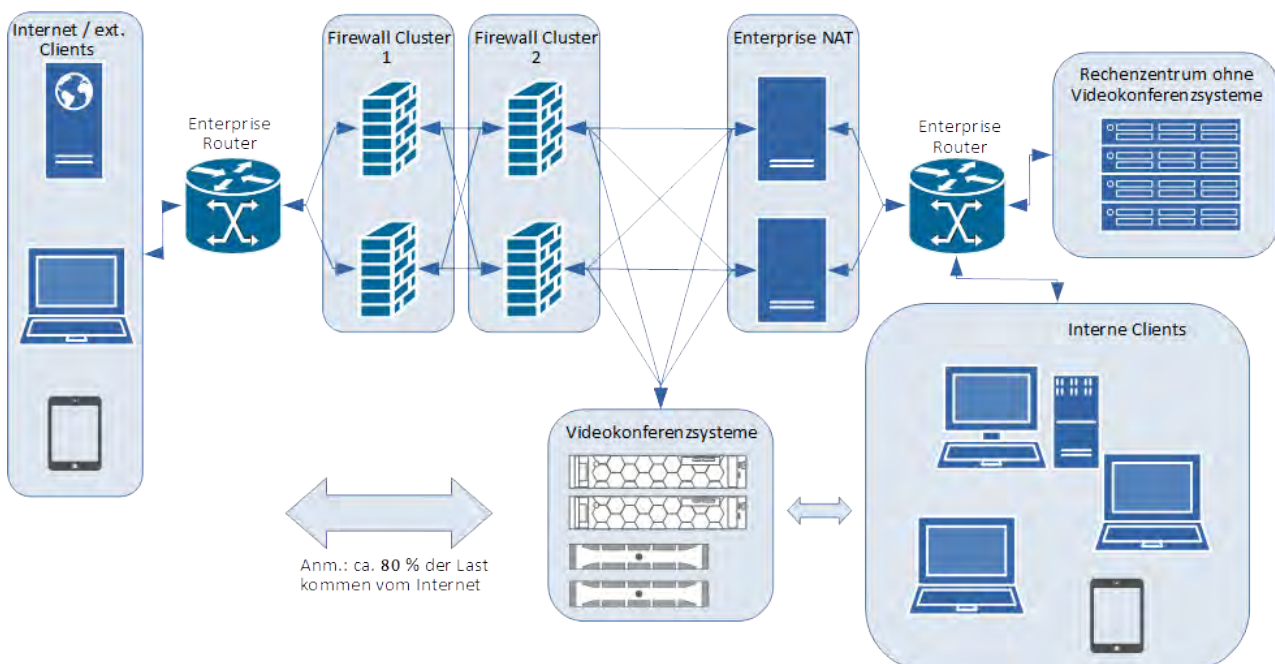
Die TURN Server liefen innerhalb eines LXC Namespace auf den Maschinen. [Scalelite](#) ist ein Open Source Loadbalancer welcher ebenso in einem LXC Container auf einem der DELL Server installiert wurde.

Es wurden mehrere Greenlight Server für unterschiedliche Benutzergruppen aufgesetzt. Unter anderem ein dedizierter Server auf dem Studierende ihre eigenen Konferenzen einrichten und durchführen können. Letzterer ist quasi durch Zufall entstanden: Die Adresse des anfänglichen Testsystems hat sich „wie ein Lauffeuer“ an der Hochschule verbreitet. Es wurde entschieden das Testsystem nicht abzuschalten, sondern für alle Benutzer offen zu lassen. Die Anwenderkreise der anderen Greenlight Server (Dozierende, Verwaltung, etc.) wurden dediziert frei gegeben.

Ausbaustufe 3 – August 2020:

„Jede Nanosekunde zählt“

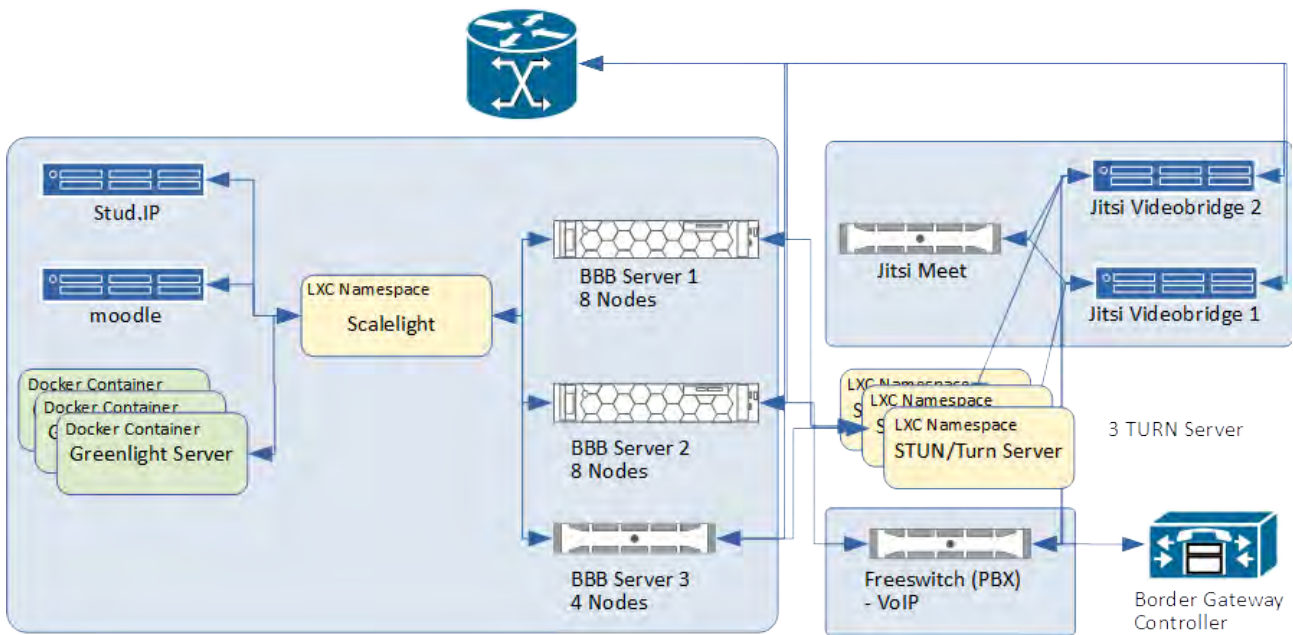
Die bis dato gemachten Erfahrungen führten zu nachfolgender Konfiguration – „wir arbeiten an jeder Nanosekunde“. Das Videokonferenzsystem wurde netzwerktechnisch zur Verringerung von Latenzen direkt hinter die Firewall gelegt. Die Firewall besteht dabei aus der Sicht des Internets aus zwei hintereinander gelagerten Firewall-Clustern. Der zweite Cluster wurde hierzu zusätzlich mit 2x 10 Gigabit Karten erweitert. Der Effekt dieser Maßnahme war deutlich und es gab viele positive Rückmeldungen durch die Anwender: „Was habt ihr gemacht? Die Konferenzqualität ist noch einmal besser geworden“



Ausbaustufe 4 – Videokonferenzarchitektur Oktober 2020

Die Konfiguration der VC Systeme wurde wie folgt weiter entwickelt: Noch ein zusätzlicher BBB Server (BBB 3), sowie die Integration in die VoIP Telefonanlage. Jeder BBB Node hat dabei eine eigene Rufnummer aus einem im [Border Gateway Controller](#) reservierten Rufnummernband zugewiesen bekommen. Alle VoIP-Verbindungen laufen dabei über den FreeSWITCH (<https://en.wikipedia.org/wiki/FreeSWITCH>) und sind vollständig unabhängig von der CISCO Telefonanlage der Hochschule.

Ein Richtwert, basierend auf den Erfahrungen der Ostfalia, ist ca. 10-12GB Hauptspeicher pro LXC BBB-Knoten (Hierzu später mehr, siehe weiter unten). Deshalb werden auf dem kleinen 64GB Server (Dell 730) nur 4 Knoten zur Verfügung gestellt.



In der Leistungsübersicht sieht das für die BBB Systeme in Ausbaustufe 4 so aus: Werte erfasst innerhalb eines 7 Tage Intervalls:

- In Summe 14.452 Meetings über 7 Tage, in der Spitze 2.406 Meetings an einem Tag
- In Summe 105.666 Users, in der Spitze 19.438 Benutzer am Tag, bzw. 17.126 Unique am Tag
- Im Mittel 7,3 Benutzer pro Meeting, bei 14.452 Meetings und 105.666 Benutzer im betrachteten Zeitraum, das größte Meeting im betrachteten Zeitraum lag bei 272 Teilnehmern
- Es gab maximal 208 Meetings gleichzeitig im betrachteten Zeitraum



Verbesserungen Stand November / Dezember 2020:

Aus den ersten Erfahrungen mit den single BBB Servern aus März 2020 wurde es für eine gute Idee gehalten, die CPU Ressourcen für die einzelnen LXC Nodes im Server zu begrenzen. Die Einstellung war 16 Threads pro BBB LXC Node, bei 128 Threads sind dies 8 BBB Nodes pro Maschine. Anfang diesen Winter-Semesters (WS 20/21) mit der 5fachen Last gegenüber dem letzten Semester zeigte es sich, dass dieses eine „suboptimale“ Entscheidung war: Einzelne Knoten mit vielen Nutzern hatten eine extrem hohe Last mit hohen IOWAIT-States, während andere Knoten auf dem selben Server ohne Last waren. Zuerst wurden jegliche Ressourcen-Begrenzungen für die LXC-Container auf den Servern entfernt. **Danach ging die Gesamtlast des Systems soweit runter, dass nun die doppelte Zahl an Knoten**, also 16, auf einem Server mit 128 Threads und 1024 GB RAM bereitgestellt werden können. Seit dem stehen $2 * 16 + 4 = 36$ BBB-Nodes den Nutzern zur Verfügung.

Eine weiter steigende Anforderung und auch das Thema „Ausfallsicherheit“ bedeuten natürlich auch wachsenden Hardware-Bedarf: Es wurde ein weiterer großer Server gekauft. In Sachen Optimierung soll diesmal der Installationsprozess so lange optimiert werden, bis er zu 100% per ANSIBLE-Skript durchführbar ist (<https://de.wikipedia.org/wiki/Ansible> & <https://www.ansible.com/>). Ganz im Sinne des Open Source Gedankens wird das „fertige“ & getestete Ansible-Skript durch die Ostfalia Hochschule veröffentlicht.

Ein weiteres Thema zur Anforderungsanpassung ist die Durchführung von Konferenzen bzw. Vorlesungen mit großen Teilnehmerzahlen. Hier ist ein so genannter „Fernseher Modus“ vorgesehen: Ein in einem Docker Container laufender Headless [Chrome](#) verbindet sich dabei mit dem BBB Node und streamt die Veranstaltung über youtube. Hier gibt es zwei Varianten: Einmal „nur zuschauen“ und einmal „zuschauen & Chat“ ([RocketChat](#)). Erste Veranstaltungen mit dieser technischen Variante liefen problemlos. Für beide Varianten hat die Ostfalia Open Source Tools zur Verfügung gestellt:

- Präsentation ohne Chat - <https://github.com/alpapado/bbb-download>
- Präsentation mit Rückkanal - <https://github.com/jibon57/bbb-recorder>

Benutzersupport

Die Ostfalia Hochschule hat in Absprache mit der TU Chemnitz die dortige Anleitung - ganz im Sinne des „Openness“ Prinzips - übernehmen dürfen:

<https://www.tu-chemnitz.de/urz/vidcon/bbb/>
<https://wiki.sonia.de/display/anonymous/BigBlueButton>

Kostenbetrachtungen

Insgesamt liegen die Kosten für die VC Lösung bei ca. 200.000 € für 5 Jahre. Die Kosten setzen sich im wesentlichen aus Hardwarekosten und deren Support zusammen. Die eingesetzte Software steht unter Open Source Lizenzen und hier fallen somit keine Lizenzkosten an.

Frage: Lassen sich die Kosten nach „Jitsi“ und „BBB“ aufteilen? In Anbetracht der Tatsache, dass im Falle der konkreten Anwendungsszenarien der Ostfalia Hochschule die BBB Systeme deutlich

stärker nachgefragt wurden und werden, sind diese dementsprechend stärker ausgebaut worden. Eine allgemein gültige Aufteilung oder ein Vergleich der Kosten für das eine oder andere System kann an dieser Stelle somit nicht gegeben werden.

Die Betreuung der Systeme erfolgt im Regelbetrieb durch einen Mitarbeiter. Aufgrund der Stabilität der Systeme ist dies im Normalbetrieb völlig ausreichend. Dieser Mitarbeiter betreut ebenso die Stud.IP und moodle Systeme.

Als Beispiel für Kostenbetrachtungen kommerzieller Systeme seien hier die Kosten für [Zoom](#) und [Adobe® Connect](#) exemplarisch abgeschätzt (Institutionsgröße: ca. 1.800 Verwaltungsmitarbeiter / 30.000 Studierende; nicht alle gleichzeitig Online sondern Online im Rahmen des „normalen Corona online“ Studienbetriebes): Bei Adobe Connect liegen die geschätzten Kosten bei ca. 80.000 € jährlich, bei zoom, ausgelegt als Backup-System bei ca. 35.000 € jährlich. Grob abgeschätzt könnten die Kosten für diese beiden Systeme in Kombination somit ca. 100.000 € bis 120.000 € pro Jahr an Lizenzkosten betragen, d.h. bei 5 Jahren liegen die geschätzten Lizenz-Kosten zwischen rund 500.000 € und 600.000 €, wobei zusätzliche Betriebskosten und Betreuungskosten i.d.R. nicht anfallen. Für ein konkretes Angebot, welches – je nach Verhandlungsgeschick – natürlich von den hier abgeschätzten Größenordnungen abweichen kann, sind die jeweiligen Unternehmen zu kontaktieren.

Ansprechpartner

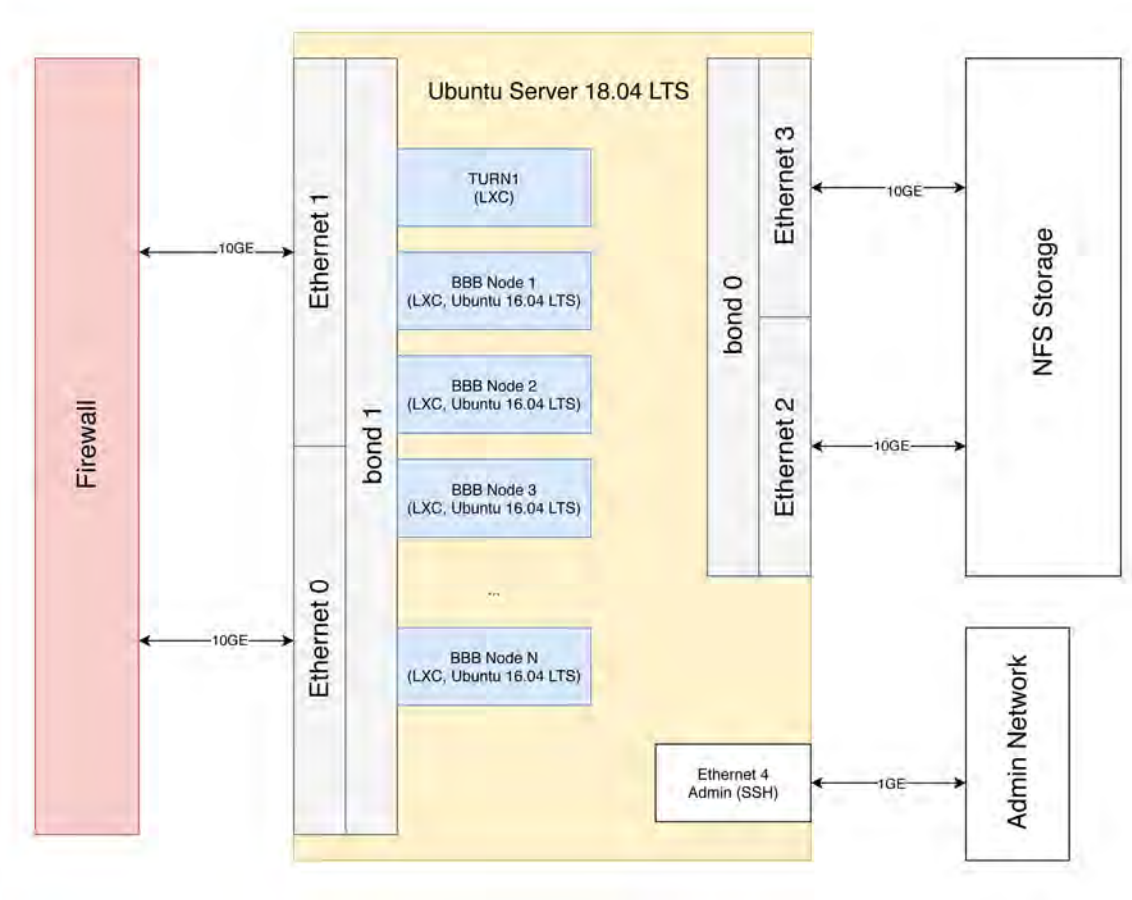
Dr. Thorsten Ludewig
Leiter des Rechenzentrums
Ostfalia Hochschule für angewandte Wissenschaften

Oder die campusSOURCE Geschäftsstelle

Anhang - Hardwareaufbau BBB Server mit 128 Threads und 1024 GB RAM:

Auf dem Server und auf den einzelnen Nodes läuft **KEINE Firewall**: Es wird – wie erwähnt - um jede Nanosekunde Latenz gefeilscht. Die Externe Firewall ist für den Schutz der Systeme verantwortlich. Es ist **wichtig z.B. Port 5060 zu blocken**, dieser wird sofort von Draußen kompromittiert. Alle unnötigen Services sind in Host und Nodes abgeschaltet. Die SSH ist ausschließlich über die Admin-Ethernet-Schnittstelle erreichbar.

Wie erwähnt erfolgt die Virtualisierung nicht mittels virtueller Maschinen sondern per LXC, was deutlich effizienter ist (<https://linuxcontainers.org/lxc/introduction/>). Die Consolen der Nodes erreicht man nur über den Host per "lxc exec". Nochmal erwähnt sei hier die Big Blue Button Systemvoraussetzung: Ubuntu 16.04 64-bit OS running Linux kernel 4.x und der Eingangs erwähnte **Tipp**: „Ubuntu 16.04 ist nun wirklich in die Jahre gekommen und die NFS Performance von 16.04 ist nicht sehr gut“. Die Kommunikation mit dem NFS Storage sollte über eine 18.04er Version, besser 20.04er realisiert werden. Der jeweilige TURN Service steht allen Nodes im Cluster zur Verfügung, nicht nur denjenigen auf dessen Hosts er läuft.



Konfiguration der Hardware

Server 1024GB 2 HE Chassis mit 12x 3.5" HDD-Slots,

- 4 x 8HLPCIe-Slots, inkl. Rackschienen,
 - 2 x AMD EPYC 7542 (2.9GHz/32-Core/64-Threads/128MBCache) CPU,
 - 32x 32GB RDIMM, 2300MHz,
 - 8 x 8TB NLSAS-HDD (12Gb/s, 7200UPM),
 - 2 x 480TB SAS-SSD (MU, PM5-V),
 - 2 x 240TB SATA-SSD (MU, S4610),
 - 1 x RAID-Controller,
 - 1 x 1GBaseT onBoard,
 - 2 x SFP+ OPC NIC,(2 x 10 GB NIC) werden per Trunking zusammengefasst
 - 2 x 1400W Netzteil,
 - 2 x 2m Netzkabel,
 - 1 x iDRAC9 Enterprise-Service-Prozessor,
- 5 Jahre ProSupport mit NBD Reaktion