IN&OUT AG

Huawei OptiXrans DC908 DWDM Benchmark

Andreas Zallmann
CEO, In&Out AG

Version:	1.0
Datum:	10.10.2020
Klassifikation:	Öffentlich

In&Out AG IT Consulting & Engineering
Seestrasse 353, CH-8038 Zürich
Phone +41 44 485 60 60

info@inout.ch, www.inout.ch

Vorbemerkung

Das vorliegende Whitepaper wurde im Auftrag der Firma Huawei unabhängig und neutral von der In&Out AG erstellt. Die Testumgebung wurde von Huawei Schweiz bereitgestellt.

In&Out AG

Die In&Out AG aus Zürich begleitet ihre Kunden als unabhängiges und herstellerneutrales Beratungsunternehmen seit Jahren in den Bereichen IT Infrastruktur und Datacenter. In&Out über ausgewiesene jahrelange Erfahrung in Performance Messungen und Optimierungen und hat das Benchmark Tool IOgen™ entwickelt.

Huawei

Huawei wurde 1987 gegründet und ist ein weltweit führender Anbieter von Informations- und Kommunikationstechnologie (ICT) Infrastruktur und intelligenten Geräten mit aktuell 194'000 Mitarbeitern. Huawei wird von Analysten als einer der Leader im Bereich der optischen Geräte für Provider eingestuft. Nach eigenen Angaben hat Huawei bis Ende 2019 in diesem Segment einen Marktanteil von knapp 30% erreicht und ist damit mit deutlichem Abstand Marktführer.

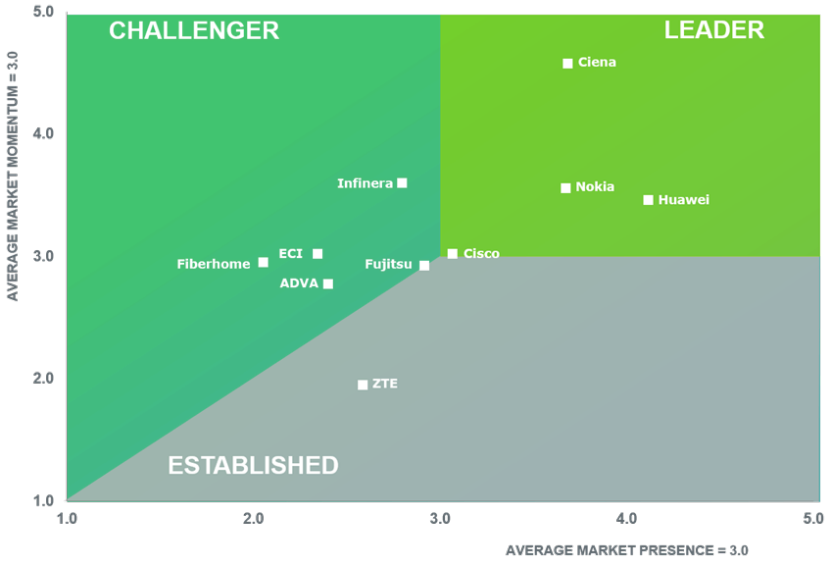

Abbildung 1 – Service provider optical leadership landscape graph 2019, source: IHS Markit

Huawei OptiXtrans DC908 DWDM Datacenter Interconnect

Die Huawei OptiXtrans DC908 Datacenter Interconnects sind DWDMs (Dense Wavelength Division Multiplexer), die über ein oder mehrere Darkfiber Verbindungen mehrere Fiber Channel und Gigabit Ethernet Kanäle zwischen Datacentern über grosse Entfernungen übertragen können.

Abbildung 2 – Huawei OptiXtrans DC 908

Das 2U hohe Gerät verfügt über 8 Slots und verfügt über eine interne Bandbreite von bis zu 12.8 Tbps. Über Interfacekarten können 10,40,100 und 400 GbE sowie 16 und 32 Gbit FC Kanale verbunden werden und über den Dark Fiber übertragen werden. Durch redundante Netzteile, Ventilatoren und Controller weisen die Systeme eine hohe Ausfallsicherheit auf.

Die Systeme verfügen über eine zuschaltbare AES256 Verschlüsselung über die Dark Fiber Verbindungen und sind laut Huawei besonders einfach zu administrieren und zu konfigurieren, sodass diese Aufgabe von den Kunden problemlos selbst übernommen werden kann.

Zielsetzung

Huawei hat In&Out als unabhängige Beratungsfirma gebeten, die neuen DC908 DCI Systeme einem intensiven Test zu unterziehen. Dabei sollten insbesondere folgende Punkte geprüft werden:

I. Einfluss auf die Latenz und Performance beim Storagezugriff in einer DCI Konstellation mit zwei DC908 Systemen im Vergleich zu einem lokalen Storagezugriff ohne DWDM Verbindung
II. Einfluss auf die Latenz und Performance beim Storagezugriff in einer verschlüsselten DCI Konstellation mit zwei DC908 Systemen im Vergleich zu einer unverschlüsselten DWDM Verbindung
III. Stabilität und konstante Performance sowie Latenz über eine DCI Verbindung mit zwei DC908 Systemen über einen Zeitraum von 24h
IV. Verfügbarkeit von DC908 Systemen bei Ausfall eines Netzteils, Ventilators oder einzelner Fiber Channel Verbindungen
V. Benutzung des End-to-End webbasierten GUIs zum zentralen Management der gesamten DCI Infrastruktur
VI. Überprüfung der Auto-Konfiguration der DCI Komponenten

Management Summary

Die Resultate unsere Messungen und Prüfungen können wir wie folgt zusammenfassen:

I. Die zusätzliche **Latenz** beim Storagezugriff via DWDM und weiteren Fiber Channel SAN Switches im DC2 beträgt **55-69 µs beim Lesen und 134-138 µs beim Schreiben**. Diese zusätzliche Latenz ist unabhängig von der verwendeten Blockgrösse, d.h. der Impact auf die Performance ist bei 1 KB genauso gross wie bei 256 KB. Ebenso verringert sich der Unterschied in der Latenz auf dem Server unter steigender Last schrittweise an, da die Latenz einzelner IOs bei hoher Parallelität eine immer geringere Rolle spielt. Bei Zugriff auf den Remote Storage über die DWDMs kann der gleiche Durchsatz und die gleichen IOPS erreicht werden wir beim lokalen Zugriff.
II. Die **AES-256 Verschlüsselung** über die DWDMs hat **keinen messbaren Einfluss** auf die Latenz und Bandbreite
III. Im 24h Stunden Dauer Belastungstests haben die Systeme **fehlerfrei eine stabile Performance** liefern können
IV. Die **Verfügbarkeit** der DC908 Systeme war in verschiedenen Ausfallszenarien **nie beeinträchtigt**.
V. Durch die **End-to-End Konfiguration** kann man einfacher den Überblick über alle Systeme behalten und schnell zwischen einzelnen Systemen wechseln.
VI. Das **Auto-Configuration** Feature ermöglicht eine sehr viel einfachere erste Inbetriebnahme oder eine komplette Neukonfiguration und ist zudem weniger fehleranfällig.

Die Stabilität und das Verhalten der Systeme war im Test immer einwandfrei. Wir konnten keine Ausfälle oder unerklärlichen Performanceschwankungen feststellen. Die Bedienung der Systeme war insbesondere für die relativ komplexen DWDMs vergleichsweise intuitiv und selbst für Benutzer, die mit dem System nicht vertraut waren, relativ einfach möglich, vor allem durch die automatische Konfiguration.

Testsetup

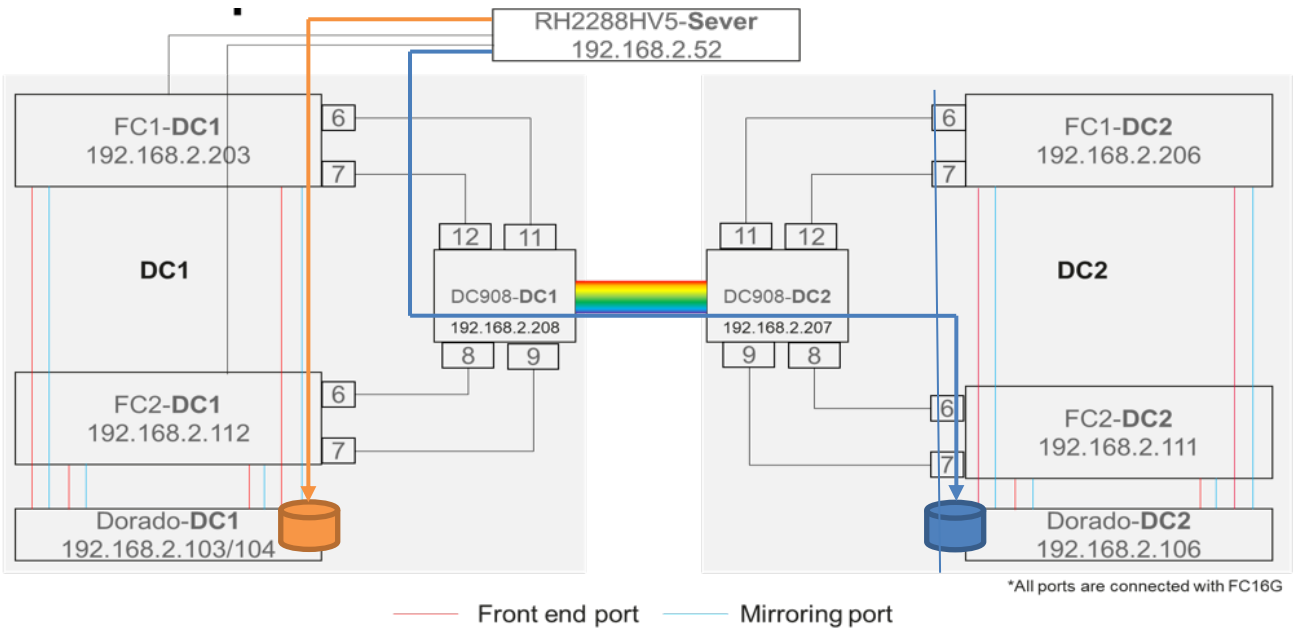

Abbildung 3 – Testsetup (Lokal und Remote Zugriff)

Huawei OptiXtrans DC908 Konfiguration

Getestet wurden zwei DC908 OptiXtrans DCI (Data Center Interconnect) DWDMs (Dense Wavelength Division Multiplexing), die über einen Dark Fiber pro Richtung miteinander verbunden waren. Wir bezeichnen diese als DC1 und DC2, auch wenn diese physisch im Testsetup am gleichen Standort platziert waren. Die Dark Fiber Verbindungen zwischen den DWDMs sind sehr kurz, da es hier nicht um das Messen des Einflusses der Entfernung geht, sondern nur um den Einfluss der DWDMs.

Die beiden DWDMs sind jeweils über 4 x 16 Gbit Links an zwei Huawei SNS2224 16 Gbit SAN Switches angeschlossen. An den SAN Switches ist in DC1 und DC2 jeweils ein Dorado 8000 V6 Storagesystem angeschlossen. Der Testserver ist an den DC1 Switches angeschlossen. Beim Zugriff auf die Dorado in DC1 (orange) wird ein lokaler Zugriff vom Testserver über die DC1 FC Switches gemessen, ohne Transfer per DWDM. Bei Zugriff auf die Dorado in DC2 (blau) erfolgt hingegen ein Remote Zugriff vom Server über die DC1 FC Switches, über die DWDMs und DC2 Switches auf die Dorado.

Huawei OceanStor Dorado 8000 V6 Konfiguration

Die beiden Storagesysteme sind mit 4 x 32 Gbit FC an zwei Huawei SNS2224 SAN 16 Gbit Switches verbunden. Somit ist die nutzbare Geschwindigkeit 4 x 16 GBit = 8 GB/s pro Storagesystem.

Pro Storagesystem sind 4 lokale (ungespiegelte) LUNs mit je 1 TB konfiguriert.

Die beiden Dorado 8000 V6 wurden in der folgenden Konfiguration genutzt:

	Getestete Konfiguration	Maximale Konfiguration
Storage	Huawei OceanStor Dorado V6 6.0.0.SPH7	
Firmware	7.60.03.011	
Controller	4 Controller (A-D) x Kunpeng920 128 Cores	16 Controller x Kunpeng920 128 Cores
Cache	1'024 GB insgesamt Read und Write	16'384 GB total (1'024 GB pro Controller)
FC	8 x 32 Gbit, effektiv 16 Gbit (4 für Server, 4 für Storagespiegelung)	448 x 32 Gbit (112 IO Slots oder 28 pro Controller Enclosure mit je 4 x 32 Gbit Ports)
Disks	1 NVMe Disk Enclosure mit 22 NVMe SSD x 3.84 TB	Bis zu 23 NVMe Disks Enclosures mit bis zu 3'200 SAS oder NVMe SSD
Raid-Konfiguration	Virtual Raid 2.0+ mit Raid-6 Dualprotection	
LUN Konfiguration	4 LUNs lokal (ungespiegelt) x 1 TB = 4 TB Deduplication und Compression aktiviert Diskverschlüsselung deaktiviert	

Tabelle 1 – Systemkonfiguration je Storage

Test Server

Als Test Server wurde ein Huawei RH2288HV5 Server mit 192 GB Memory und 2 CPUs Intel Xeon Gold 6114 @ 3.5 Ghz benutzt. Jede CPU hat 8 Cores oder 16 Threads, somit hat der Server insgesamt 16 Cores und 32 Threads. Hyperthreading war aktiviert, somit stehen dem Betriebssystem 32 logische CPUs zur Verfügung. Der Test Server ist an den FC Switches von «Datacenter 1» angeschlossen und somit effektiv mit 2 x 16 Gbit FC.

Als Betriebssystem wurde Red Hat Enterprise Linux (RHEL) Version 7.6 genutzt.

IOgen™

Die Messungen erfolgen mit IOgen™ 6.3.3 der In&Out AG. IOgen wurde auf RHEL 7.6 installiert. Das integrierte Multipathing von RedHat wurde benutzt, also die `/dev/mapper/mpath` Devices, um einen Failover bei Verlust von einzelnen Fiber Channel Verbindungen zu testen.

I. Einfluss DWDM

In den folgenden Tests wird der Einfluss der DWDM Übertragung dargestellt. Dabei wird der Zugriff auf die lokalen LUNs auf den lokalen Dorado Storage (orange) mit dem Zugriff auf die remote LUNs auf dem remote Dorado Storage (blau) verglichen. Der Zugriff auf die remote LUNs erfolgt dabei über die DWDMs und über zwei weitere Fiber Channel Switches auf die Dorado.

Die Tests wurden sowohl im Frontend (100% Cache Hit) sowie im Backend durchgeführt. Wir zeigen hier exemplarisch jeweils die Ergebnisse von Frontend Random Read und Backend Random Write.

Ia. Random 1 KB

Bei einer Blockgrösse von 1 KB ergibt sich im Vergleich zum lokalen Zugriff eine zusätzliche Latenz von **67 µs beim Lesen und 138 µs beim Schreiben**. Dieses Delta gleicht sich mit zunehmender Last auf dem Server immer mehr an und ist bei hoher Parallelität nicht mehr messbar. Auch mit DWDM Übertragung kann die identische Anzahl von IOPS erreicht werden.

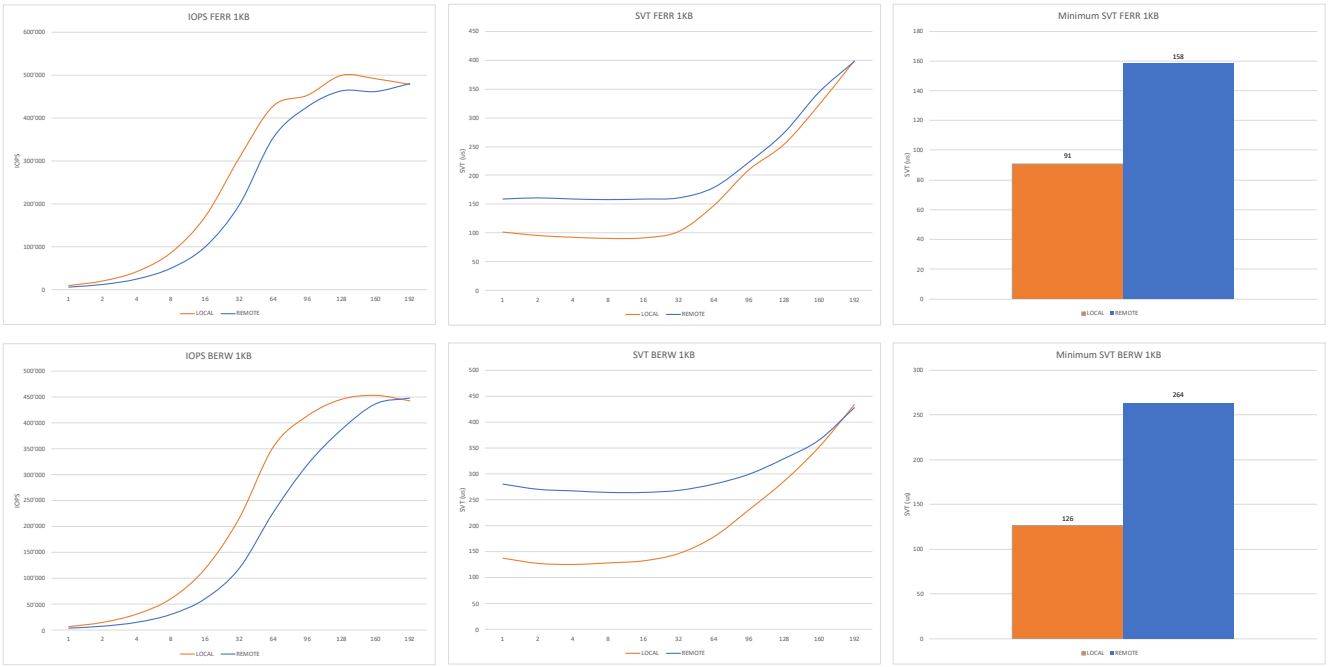

Abbildung 4 – Einfluss DWDM 1 KB Random Read (oben) und Random Write (unten)

Ib. Random 8 KB

Bei einer Blockgrösse von 8 KB ergibt sich im Vergleich zum lokalen Zugriff eine zusätzliche Latenz von **69 µs beim Lesen und 134 µs beim Schreiben**. Dieses Delta gleicht sich mit zunehmender Last auf dem Server immer mehr an und ist bei hoher Parallelität nicht mehr messbar. Auch mit DWDM Übertragung kann die identische Anzahl von IOPS erreicht werden.

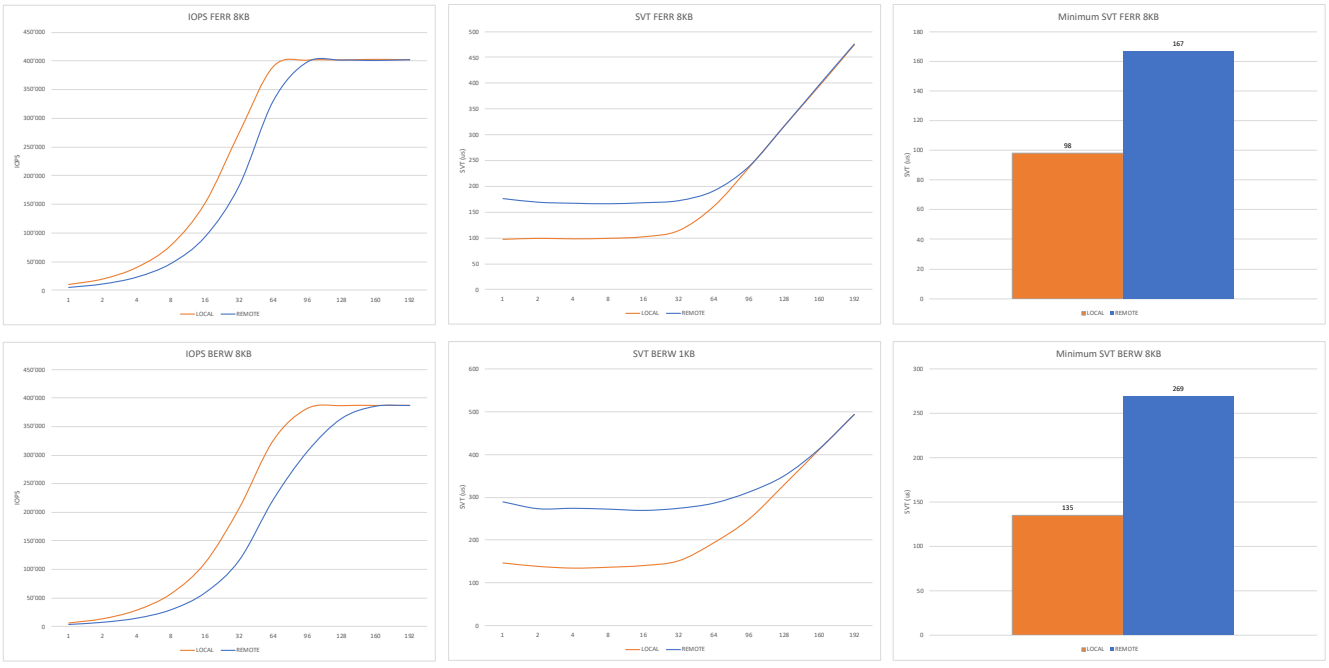

Abbildung 5 – Einfluss DWDM 8 KB Random Read (oben) und Random Write (unten)

Ic. Random 256 KB

Bei einer Blockgrösse von 256 KB ergibt sich im Vergleich zum lokalen Zugriff eine zusätzliche Latenz von **55 µs beim Lesen und 137 µs beim Schreiben**. Dieses Delta gleicht sich mit zunehmender Last auf dem Server immer mehr an und ist bei hoher Parallelität nicht mehr messbar. Auch mit DWDM Übertragung kann die identische Anzahl von IOPS erreicht werden.

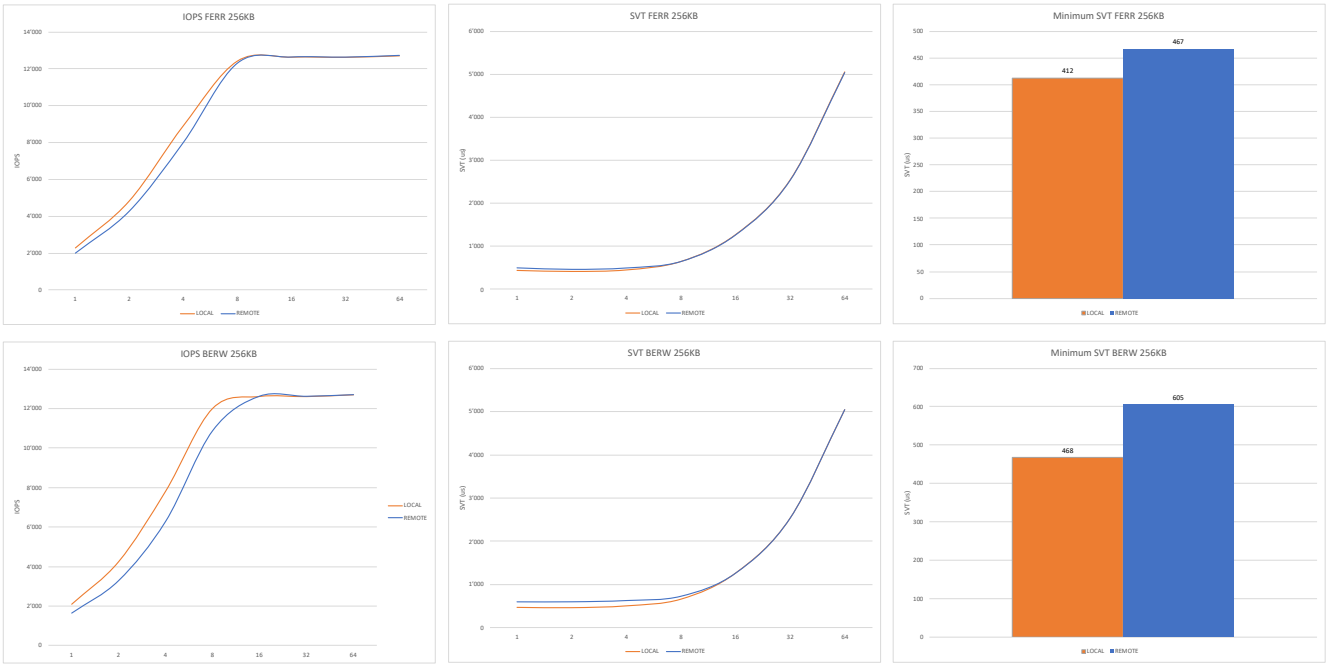

Abbildung 6 – Einfluss DWDM 256 KB Random Read (oben) und Random Write (unten)

Id. Zusammenfassung DWDM

Die folgende Tabelle zeigt den Einfluss mit und ohne DWDM Übertragung. Die zusätzliche Latenz beim Storagezugriff via DWDM und weiteren Fiber Channel SAN Switches im DC2 beträgt **55-69 µs beim Lesen und 134-138 µs beim Schreiben**. Diese zusätzliche Latenz ist unabhängig von der verwendeten Blockgrösse, d.h. der Impact auf die Performance ist beim 1 KB ähnlich gross wie bei 256 KB. Ebenso gleicht sich der Unterschied in der Latenz auf dem Server unter steigender Last schrittweise an, da die Latenz einzelner IOs bei hoher Parallelität eine zunehmend geringere Rolle spielt. Bei Zugriff auf den Remote Storage über die DWDMs kann der gleiche Durchsatz und die gleichen IOPS erreicht werden wir beim lokalen Zugriff.

Test	Lokaler Zugriff (ohne DWDM)	Remote Zugriff (mit DWDM)	Einfluss DWDM
1 KB Random Read	91 µs	158 µs	+67 µs
1 KB Random Write	126 µs	264 µs	+138 µs
8 KB Random Read	98 µs	167 µs	+69 µs
8 KB Random Write	135 µs	269 µs	+134 µs
256 KB Read	412 µs	467 µs	+55 µs
256 KB Write	468 µs	605 µs	+137 µs

Tabelle 2 – Einfluss DWDM

Zusätzlich muss zu der Latenz durch die DWDMs noch die Roundtrip Zeit auf dem Weg zwischen den Rechenzentren berücksichtigt werden. Hier kann als Faustregel pro Kilometer Distanz mit einer zusätzlichen Latenz von 10µs gerechnet werden.

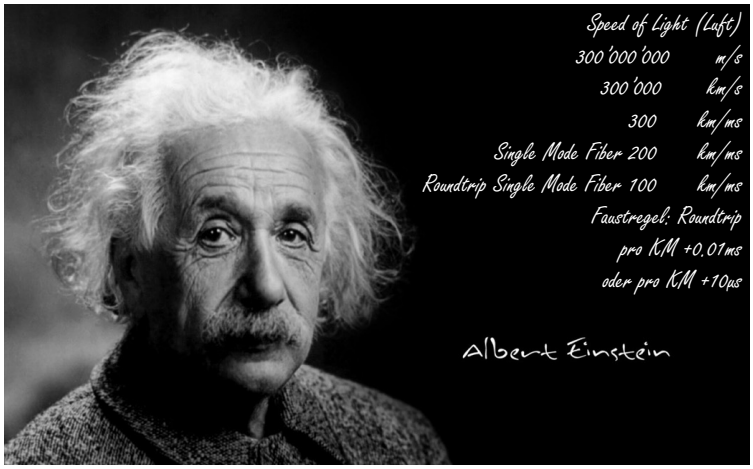

Abbildung 7 – Faustregel für die Roundtrip Zeit zwischen Rechenzentren (Dark Fiber)

II. Einfluss Verschlüsselung

In den folgenden Tests wird der Einfluss der DWDM Verschlüsselung dargestellt. Dabei wird auf Remote LUNs über DWDMs zugegriffen und die AES-256 Verschlüsselung deaktiviert und aktiviert (gestrichelt dargestellt). Die Tests wurden im Frontend (100% Cache Hit) und im Backend durchgeführt. Wir zeigen hier exemplarisch die Ergebnisse von Frontend Random Read und Backend Random Write. In allen Tests zeigt die Verschlüsselung keinen Einfluss auf Zugriffsgeschwindigkeit oder Bandbreite. Teilweise waren Zugriffe über verschlüsselten Leitungen im Rahmen der Messungenauigkeit sogar minimal schneller.

IIa. Random 1 KB

Bei einer Blockgrösse von 1 KB zeigt sich keinerlei negativer Einfluss der Verschlüsselung.

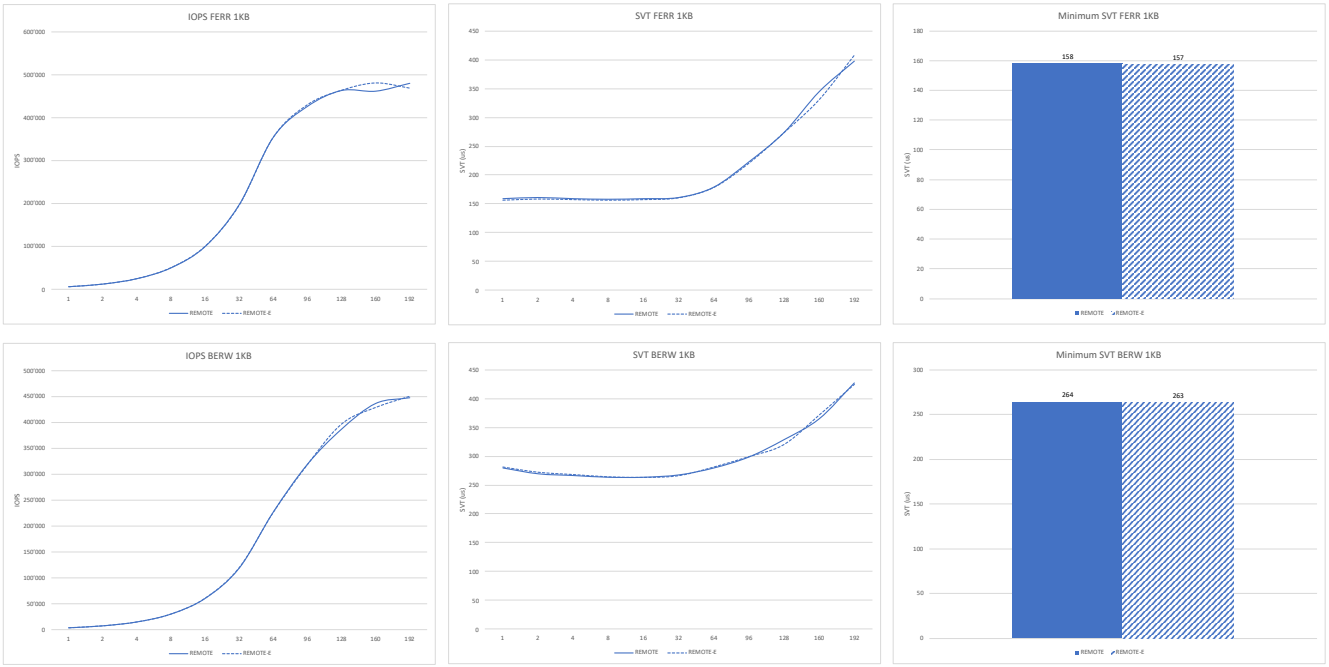

Abbildung 8 – Einfluss Verschlüsselung 1 KB Random Read (oben) und Random Write (unten)

IIb. Random 8 KB

Bei einer Blockgrösse von 8 KB zeigt sich keinerlei negativer Einfluss der Verschlüsselung.

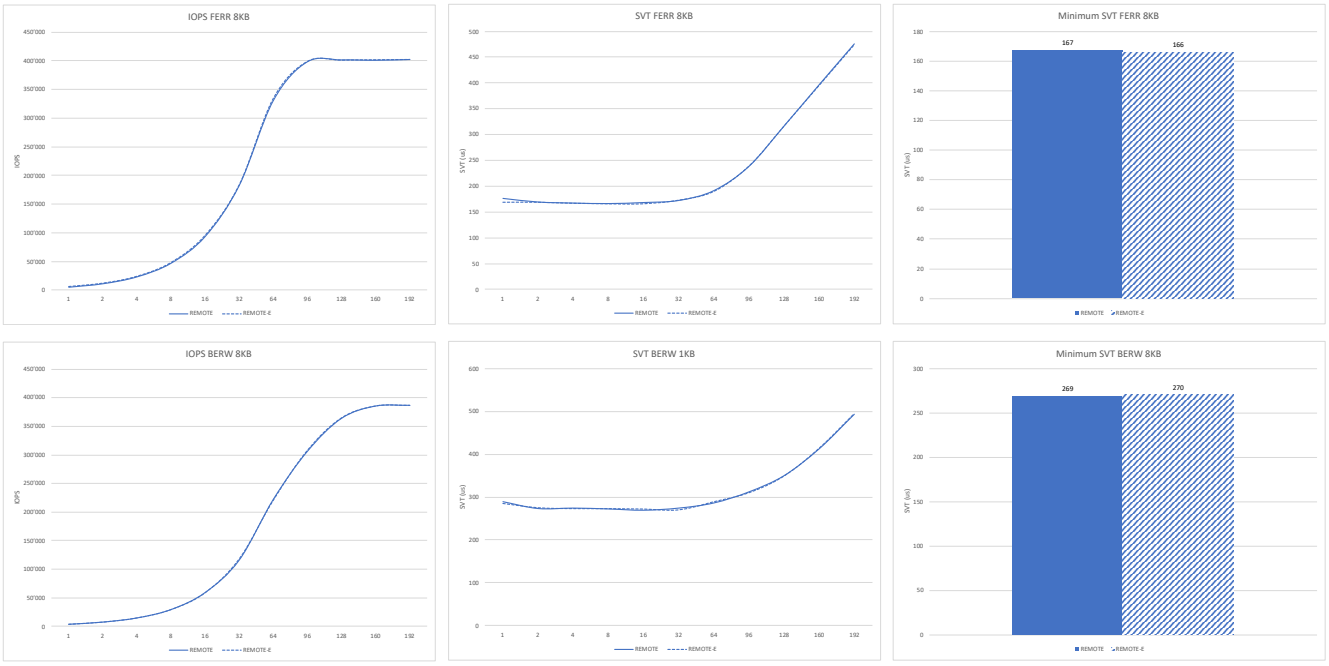

Abbildung 9 – Einfluss Verschlüsselung 8 KB Random Read (oben) und Random Write (unten)

IIc. Random 256 KB

Bei einer Blockgrösse von 256 KB zeigt sich keinerlei negativer Einfluss der Verschlüsselung. Sowohl die Latenz als auch der Durchsatz ist absolut identisch.

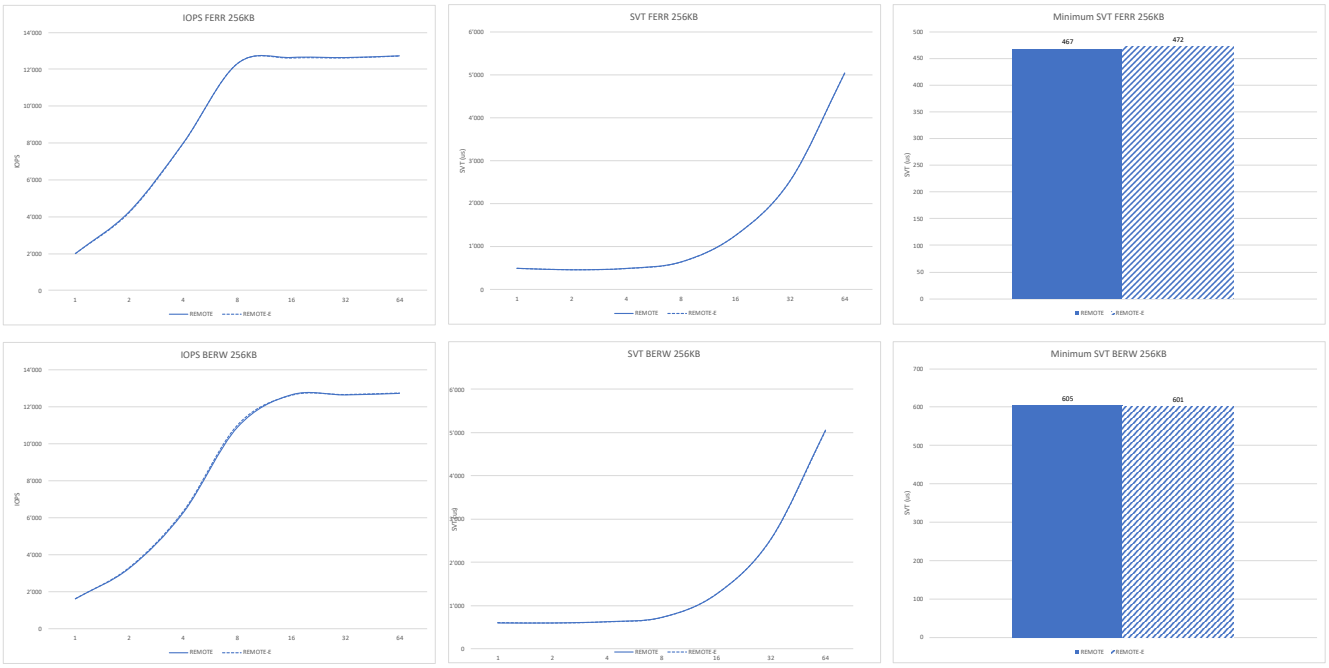

Abbildung 10 – Einfluss Verschlüsselung 256 KB Random Read (oben) und Random Write (unten)

IId. Zusammenfassung Verschlüsselung

Die folgende Tabelle zeigt den Einfluss der Verschlüsselung. Die Aktivierung der Verschlüsselung hat keinen signifikanten Einfluss auf die Latenz und den Durchsatz.

Test	Verschlüsselung nicht aktiv	Verschlüsselung aktiv (AES256)	Einfluss Verschlüsselung
1 KB Random Read	158 µs	157 µs Latenz	-1 µs
1 KB Random Write	264 µs	Min. 263 µs	-1 µs
8 KB Random Read	167 µs	166 µs	-1 µs
8 KB Random Write	269 µs	270 µs	+1 µs
256 KB Read	467 µs	472 µs	+5 µs
256 KB Write	605 µs	601 µs	-4 µs

Tabelle 3 – Einfluss Verschlüsselung

III. 24 Stunden Dauertest

Über 24h wurde mit IOgen permanent Last auf den Remote Devices und damit über die DWDMs generiert. Dabei wurden 8KB Random IOPS generiert, davon 50% Reads und 50% Writes sowie 50% Frontend (Cache Hit) und 50% Backend. Die Leistung blieb konstant bei bei ca. 300'000 bis 320'000 IOPS, die Servicezeit bei konstant 400µs.

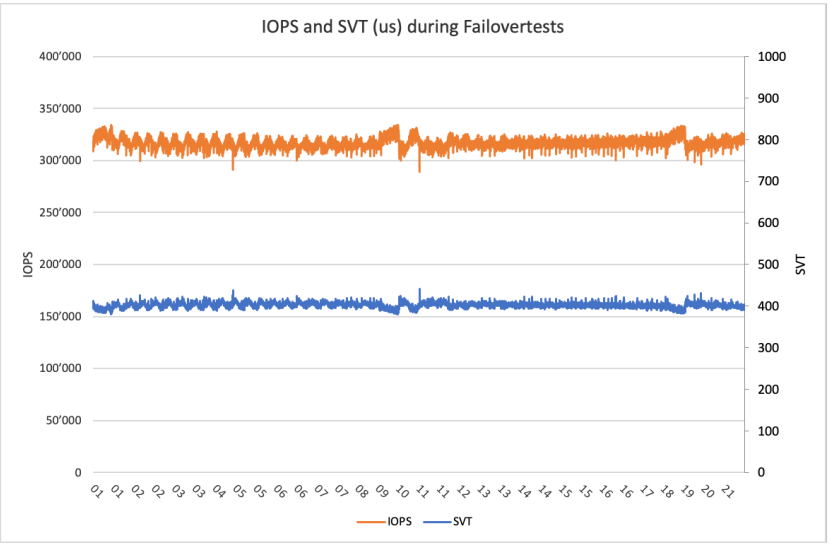

Abbildung 11 - 24h Dauertest IOPS und Servicezeit

Es wurden während den 24h keinerlei Fehler oder Übertragungsverzögerungen festgestellt, in den 86'400 einsekündigen Messintervallen sind immer 400µs Latenz mit einer maximalen Abweichung von 10% gemessen worden.

IV. Test Verfügbarkeit

Es wurden verschiedene Verfügbarkeitstests durchgeführt, mit der die unterbrechungsfreie Redundanz der DC908 Systeme überprüft wurde:

- Lüfter entfernen
- Netzteil entfernen
- Fiber Channel Links entfernen

IVa. Lüfter entfernen

Im folgenden Bild ist die Rückansicht mit den drei Lüftern in der Mitte dargestellt. Alle drei Lüfter sind funktionsfähig und laufen (grüne LED).

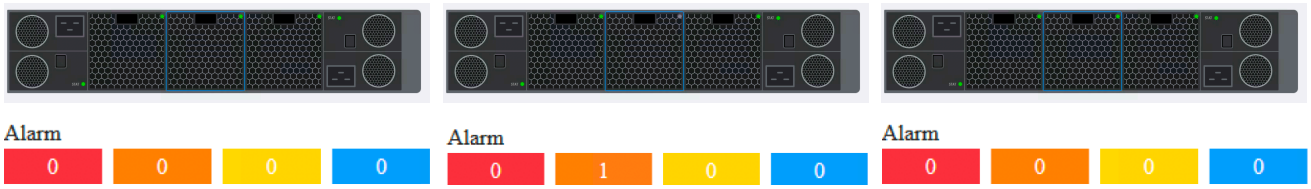

Abbildung 12 – Entfernen des Lüfters blau umrahmt (Links: Ausgangslage, Mitte: Fanmodul entfernt, Rechts: Fanmodul wieder gesteckt)

Nach Entfernen des Lüfters wird dieser grau dargestellt und die vormals grüne Status LED wird grau (mittleres Bild oben). Ausserdem wird ein «Major Alarm» generiert (orange). Der Alarm ist nicht «Critical» (rot), da das System mit zwei Lüftern einwandfrei funktioniert.

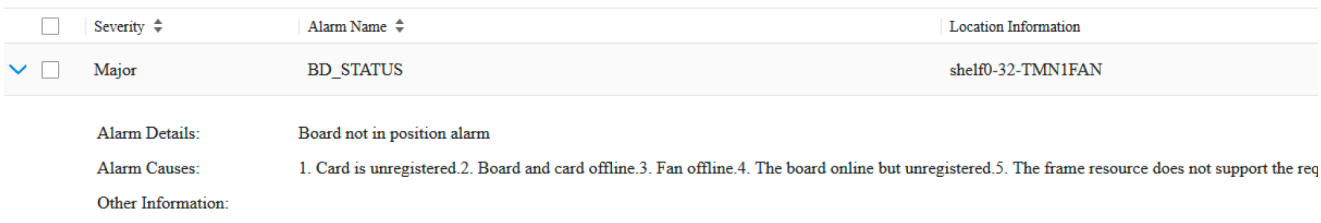

Abbildung 13 – Major Alarm nach Entfernen des Lüfters

Nach dem der mittlere Lüfter wieder eingeschoben wurde, leuchtet die Status LED wieder grün und der Alarm verschwindet.

IVb. Netzteil entfernen

Im folgenden Bild ist die Rückansicht mit den beiden Netzteilen links (Primary Power) und rechts (Backup Power) dargestellt. Beide Netzteile sind funktionsfähig und laufen (grüne LED).

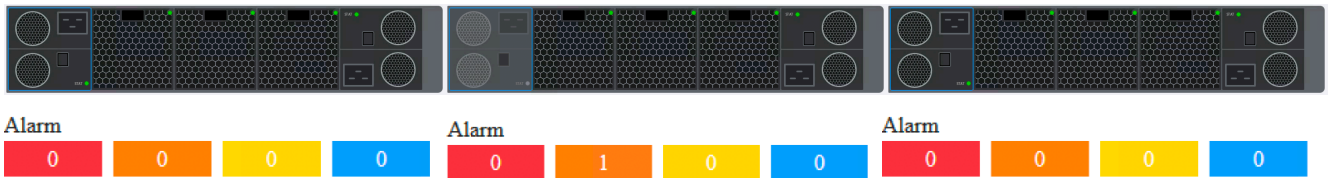

Abbildung 14 – Entfernen des Powermoduls blau umrahmt (Links: Ausgangslage, Mitte: Powermodul entfernt, Rechts Powermodul wieder gesteckt)

Nach Entfernen des primären Netzteils wird dieses grau dargestellt und die vormals grüne Status LED wird grau (mittleres Bild oben). Ausserdem wird ein «Major Alarm» generiert (orange). Der Alarm ist nicht «Critical» (rot), da das System mit dem Backup Netzteil einwandfrei funktioniert.

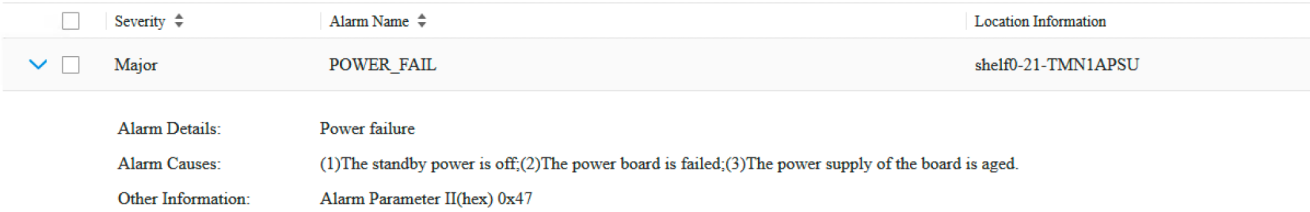

Abbildung 15 – Major Alarm nach Entfernen des Netzteils

Nach dem das primäre Netzteil wieder eingeschoben wurde, leuchtet die Status LED wieder grün und der Alarm verschwindet.

IVc. Fiber Channel Links entfernen

Das folgende Bild zeigt die aktuelle Benutzung und Konfiguration der DC908 Systeme. Die Channel C8, C9, C11 und C12 sind für Fiber Channel verwendet (vergleiche auch Abbildung 3). Im Test wurden nun die Fiberchannel Kabel an Kanl C8 und C12 entfernt und damit auf beiden SAN Fabrics einer der beiden Pfade deaktiviert.

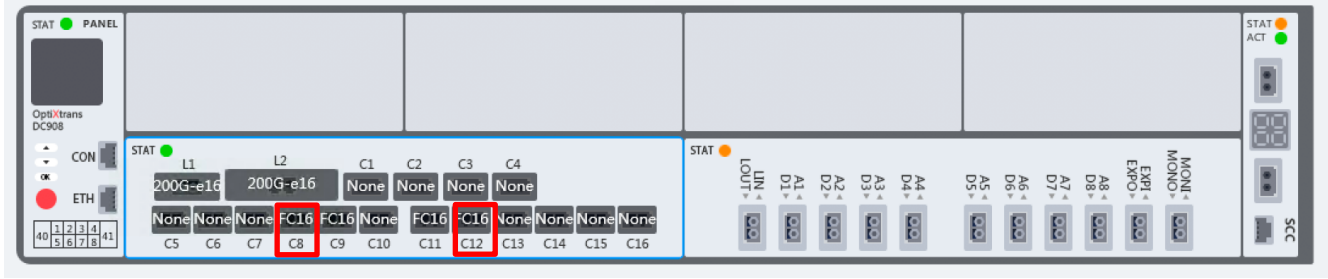

Abbildung 16 – Konfiguration DC908 Systeme

Das folgende Bild zeigt die Port Information beispielhaft für Channel C8 vor und nach dem Entfernen des FC Links. Man sieht, dass die «Input Power» von -2.7 auf -60 dBm (Dezibel Milliwatt) fällt, da der Port nicht gesteckt ist.

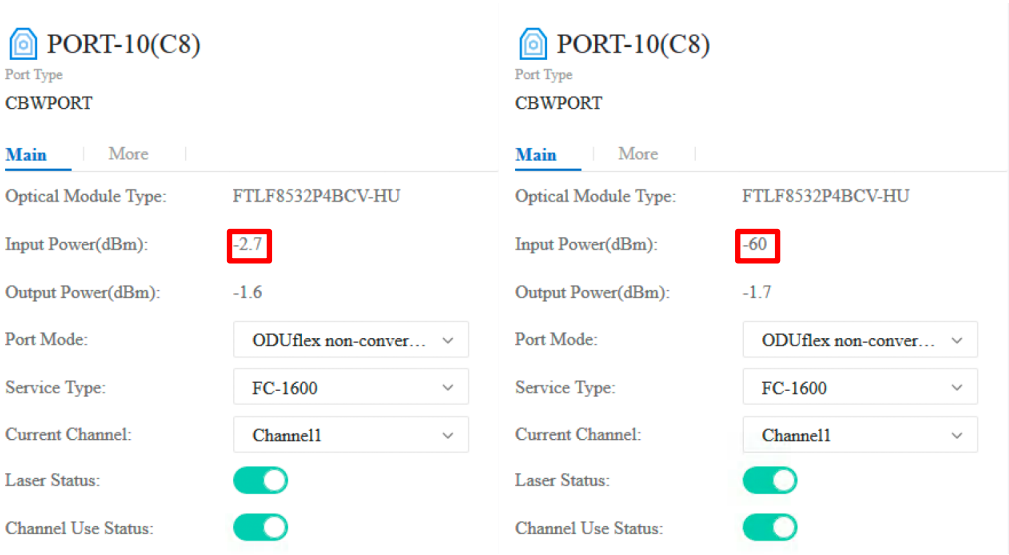

Abbildung 17 – Input Power bei Fiber Channel Loss of Signal (LOS)

Ausserdem wird für die beiden Ports jeweils ein kritischer Alarm generiert:

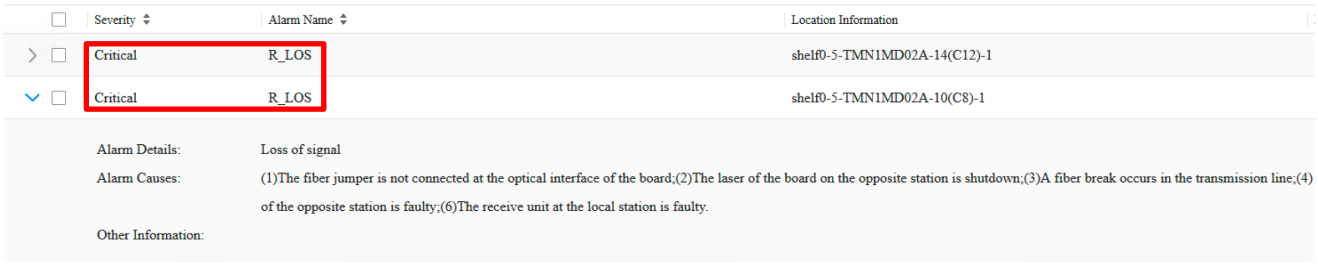

Abbildung 18 – Kritische Alarme (Loss of Signal) für die beiden entfernten FC Kabel

Nach dem Stecken der FC Kabel, werden die FC Ports automatisch wieder Online genommen. Der Verlust und die Wiederinbetriebnahme generiert ca. 10 Sekunden lange Wartezeiten bei IOs, ohne das es zu Fehlern gekommen wäre (siehe Folgeabschnitt).

IVd. Lastgeneration während Verfügbarkeitstests

Während der Verfügbarkeitstests wurde mit IOgen permanent Last auf den Remote Devices und damit über die DWDMs generiert. Dabei wurden 8KB Random IOPS generiert, davon 50% Reads und 50% Writes sowie 50% Frontend (Cache Hit) und 50% Backend. Die Leistung blieb bei allen simulierten Ausfällen konstant bei ca. 300'000 bis 320'000 IOPS, die Servicezeit bei konstant 400µs.

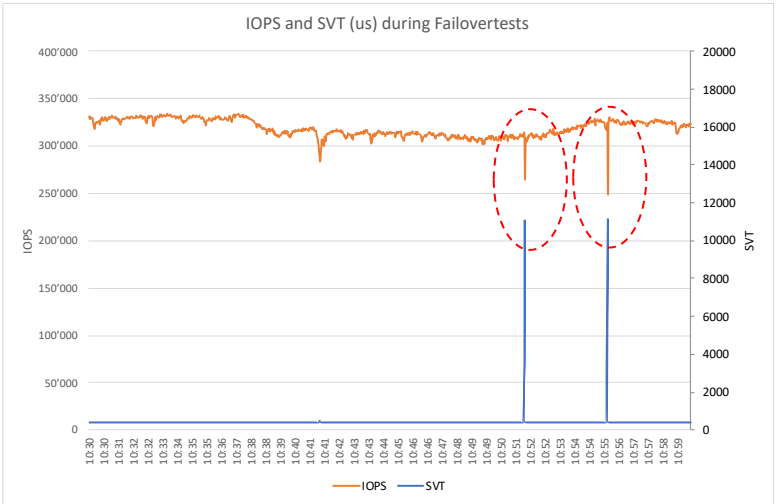

Abbildung 19 – IOPS und Latenz während der Failovertests

Allerdings sieht man auf dem Bild genau zwei Ausnahmen. Dabei wurde um 10:51 Uhr zwei Fiberchannel Kanäle am DWDM Switch entfernt und um 10:55 wieder gesteckt. In beiden Fällen kam es zu IO Wartezeiten von ca. 10s (rot eingerahmt). Dies ist ein normales Verhalten, da dies System erst nach einem Timeout die betroffenen IO Kanäle deaktiviert.

IVe. Zusammenfassung

Die Verfügbarkeit der Systeme ist auch bei Ausfall einzelner Lüfter, FANS oder FC Links vollumfänglich gegeben. Nicht testen konnten wir die redundante Anbindung der beiden DC 908 Systeme via redundantem Dark Fiber, da im der Testkonfiguration die Systeme nur mit einem Dark Fiber verbunden waren.

V. End-to-End Configuration

Huawei bietet mit den DC 908 Systemen eine End-to-End Sichtweise aller DWDMs an und die Konfiguration aller Systeme in einem browserbasierten GUI. Wie üblich loggt man sich auf einem beliebigem DWDM per Browser ein, kann dann aber mit einem Klick auf das «World» Symbol in den End-to-End Modus wechseln.

Figure 1 – Starting End-to-End Konfiguration

In der “Topology View” werden alle Systeme und deren Verbindungen dargestellt (in unserer Testumgebung mit nur zwei Systemen nicht sehr spannend, aber bei Einsatz von Duzenden DWDMs sehr hilfreich).

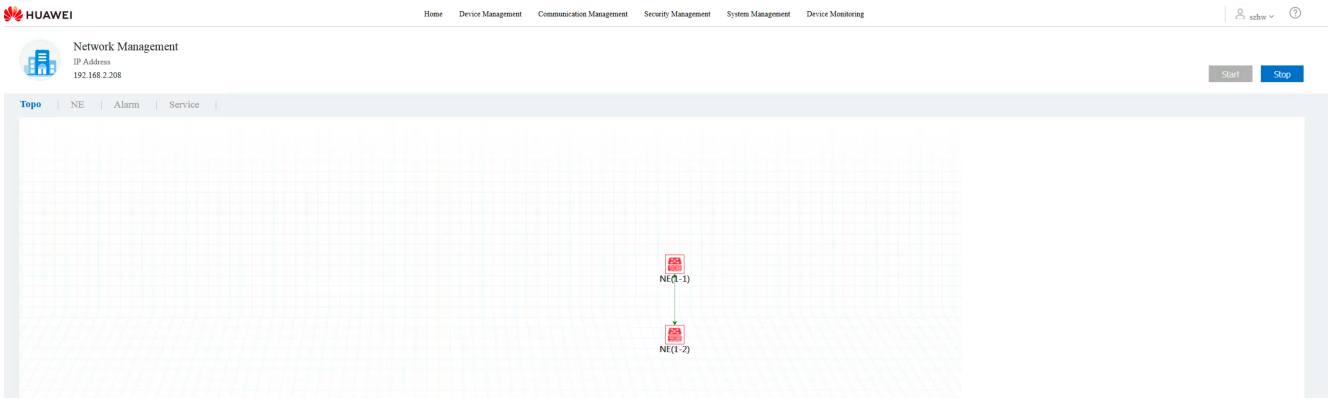

Abbildung 20 –End-to-End Topology View

Weiterhin ist eine Listendarstellung verfügbar in der alle «Network Elements» entsprechend aufgelistet werden. Wichtig ist hier, dass man mit dem Klick auf «Link» direkt auf die Konfigurationsoberfläche des jeweiligen Systems wechselt.

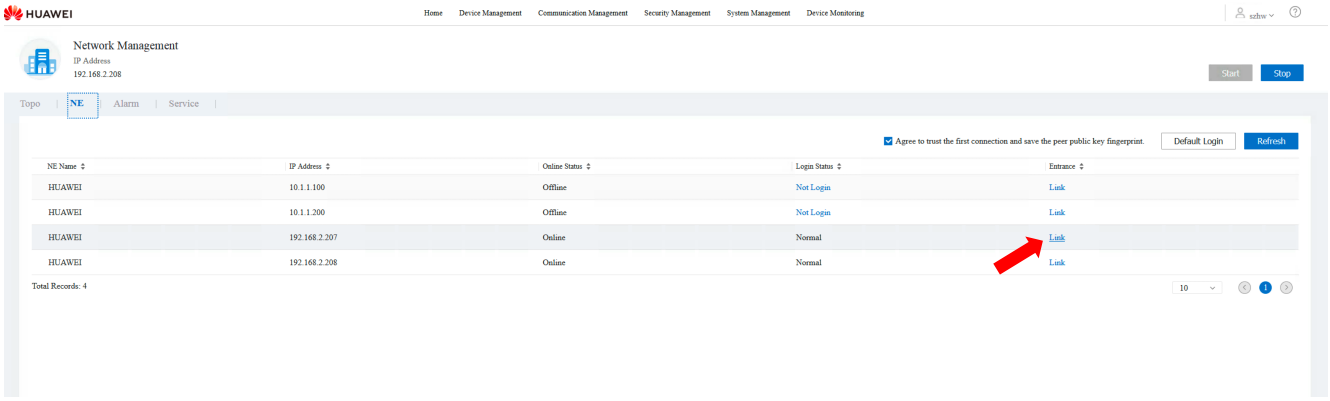

Abbildung 21 –End-to-End Network Element List View

Sehr hilfreich ist auch die konsolidierte Darstellung aller Warnungen, Fehler und Alarme über alle DWDMs. Obwohl wir über den DWDM mit IP 192.168.2.208 eingeloggt sind, sehen wir alle Fehler (hier dargestellt Alarme vom DWDM mit IP 192.168.2.207).

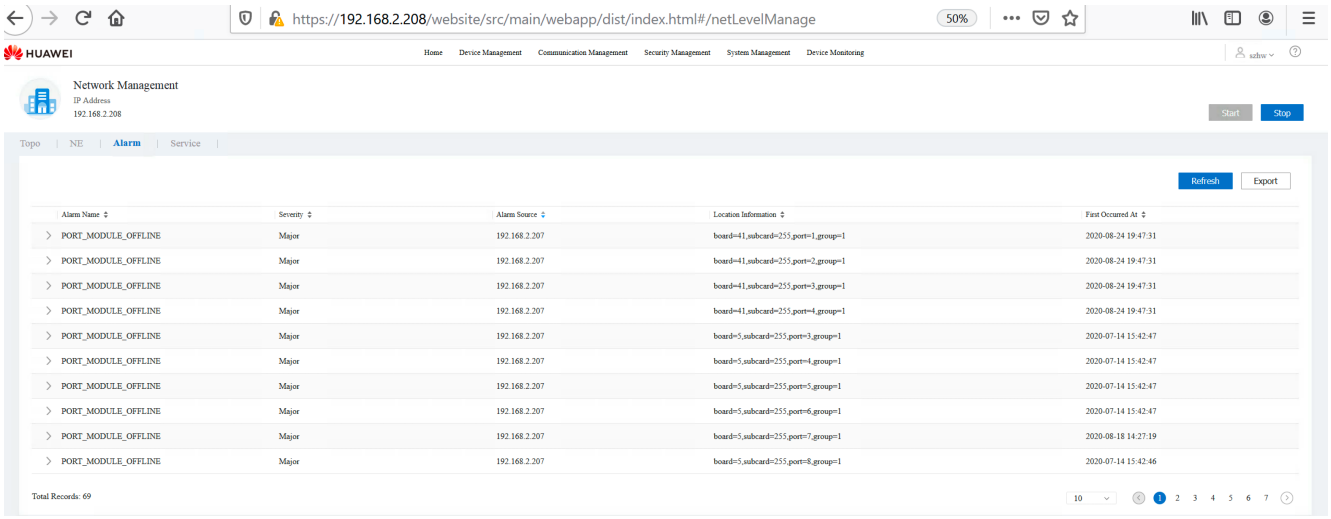

Abbildung 22 – Global Alarm View

Schlussendlich kann man auch den Status der Verbindungen über alle DWDMs in einer Status View gesamthaft darstellen.

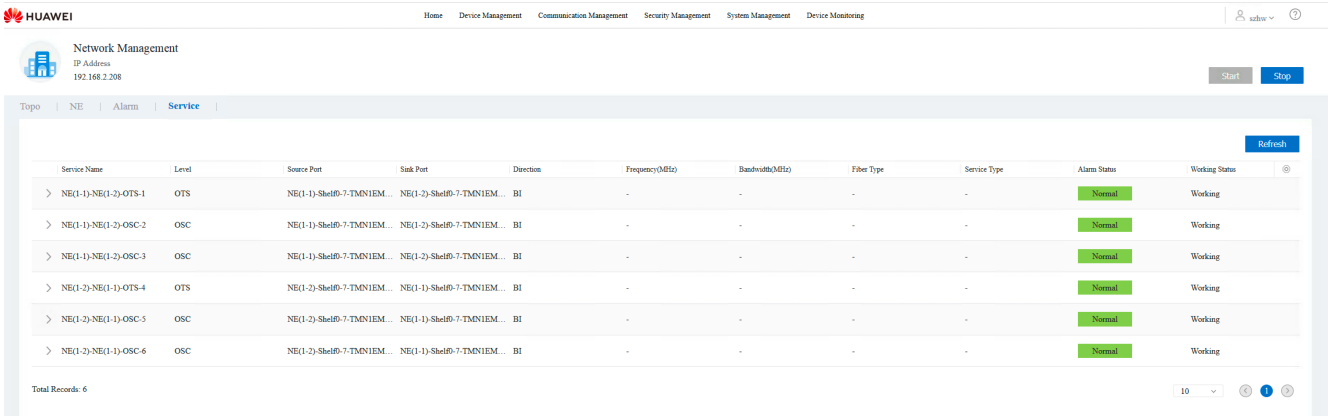

Abbildung 23 – Global Status View

Insgesamt kann man durch die End-to-End Konfiguration einfacher den Überblick über alle Systeme behalten und schnell zwischen einzelnen Systemen wechseln. Noch etwas besser wäre es, wenn man direkt mit dieser globalen Sichtweise startet, wenn man auf einem der DWDMs einlogged und dann über einen Dropdown Menü oder einen Hierarchiebaum das entsprechende System selektieren könnte. Möchte man die einzelnen Systeme konfigurieren, muss man über die Übersichtsseite mit dem Link auf das GUI des entsprechenden Systems wechseln.

VI. Auto-Configuration

Huawei bietet mit den DC 908 Systemen eine Auto-Configuration Mode an. Die Auto-Configuration wird mit einem Klick auf das «Config» Symbol gestartet.

Abbildung 24 – Aufruf Auto Konfiguration

Bei den meisten DWDMs müssen alle Links zwischen den DWDMs und die Wellenlängen manuell konfiguriert werden. Dazu muss man genau wissen, welches Interfaces mit welchem verbunden ist und auf beiden Seiten die gleiche Wellenlänge konfigurieren, damit sich die Systeme sehen. Ebenso müssen die Frontend Ports (z.B. Fiber Channel, Gigabit Ethernet, etc.) ebenfalls manuell konfiguriert werden.

Mit dem Auto-Configuration Mode der Huawei DC908 Systeme kann dies mit wenigen Klicks vollkommen automatisch erfolgen. Man wählt den Auto-Config Mode an (per Symbol in der Startzeile) und kann auswählen, welche Einheiten man konfigurieren möchte:

- Fiber Connection Discovery: Erkennt und konfiguriert alle verbundenen Interfaces (FC, GE, etc.) automatisch
- Optical Layer commisioning: Erkennt und konfiguriert alle Links zwischen zwei DWDMs automatisch

Im letzten Fall muss man diesen Vorgang auf den beiden verbundenen DWDMs gleichzeitig starten. Der Vorgang dauert bei der hier verwendeten Konfiguration ungefähr 10 Minuten, danach sind beide DWDMs vollständig konfiguriert.

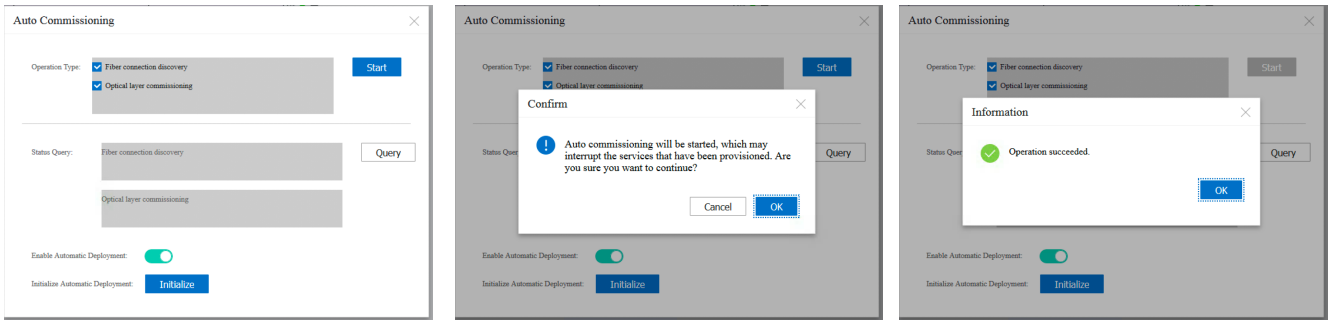

Abbildung 25 – Auto Commisioning

Das Auto-Configuration Feature ermöglicht eine sehr viel einfache erste Inbetriebnahme oder eine komplette Neukonfiguration und ist zudem viel weniger fehleranfällig.

Fazit

Die Resultate unsere Messungen können wir wie folgt zusammenfassen:

I. Die zusätzliche **Latenz** beim Storagezugriff via DWDM und weiteren Fiber Channel SAN Switches im DC2 beträgt **55-69 µs beim Lesen und 134-138 µs beim Schreiben**. Diese zusätzliche Latenz ist unabhängig von der verwendeten Blockgrösse, d.h. der Impact auf die Performance ist bei 1 KB genauso gross wie bei 256 KB. Ebenso gleicht sich der Unterschied in der Latenz auf dem Server unter steigender Last schrittweise an, da die Latenz einzelner IOs bei hoher Parallelität eine zunehmend geringere Rolle spielt. Bei Zugriff auf den Remote Storage über die DWDMs kann der gleiche Durchsatz und die gleichen IOPS erreicht werden wir beim lokalen Zugriff.

II. Die **AES-256 Verschlüsselung** über die DWDMs hat **keinen messbaren Einfluss** auf die Latenz und Bandbreite

III. Im 24h Stunden Dauer Belastungstests haben die Systeme **fehlerfrei eine stabile Performance** liefern können

IV. Die **Verfügbarkeit** der DC908 Systeme war in verschiedenen Ausfallszenarien **nie beeinträchtigt**.

V. Durch die **End-to-End Konfiguration** kann man einfacher den Überblick über alle Systeme behalten und schnell zwischen einzelnen Systemen wechseln.

VI. Das **Auto-Configuration** Feature ermöglicht eine sehr viel einfachere erste Inbetriebnahme oder eine komplette Neukonfiguration und ist zudem weniger fehleranfällig.

Die Stabilität und das Verhalten der Systeme war im Test immer einwandfrei. Wir konnten keine Ausfälle oder unerklärlichen Performanceschwankungen feststellen. Die Bedienung der Systeme war insbesondere für die relativ komplexen DWDMs vergleichsweise intuitiv und selbst für Benutzer, die mit dem System nicht vertraut waren, relativ einfach möglich, vor allem durch die automatische Konfiguration.

Über den Autor

Andreas Zallmann,
andreas.zallmann@inout.ch
In&Out AG,
Seestrasse 353, 8038 Zürich
www.inout.ch

Andreas Zallmann hat Informatik an der Universität Karlsruhe studiert und ist seit dem Jahr 2000 bei der In&Out AG. Er ist verantwortlich für den Geschäftsbereich Technology und seit 2016 CEO der In&Out AG.

Die In&Out verfügt über jahrelange Praxis-Erfahrung in Architektur, Konzeption, Benchmarking und Tuning von Storage- und Systemplattformen insbesondere für Core Applikationen für Banken und Versicherungen.

Andreas Zallmann ist der Entwickler des In&Out Performance Benchmarking Tool IOgen™ und hat in den letzten Jahren sehr viele Kunden- und Hersteller-Benchmarks durchgeführt.