ComConsult Research

Der Netzwerk Insider

Februar 2011

Systematische Weiterbildung für Netzwerk- und IT-Professionals

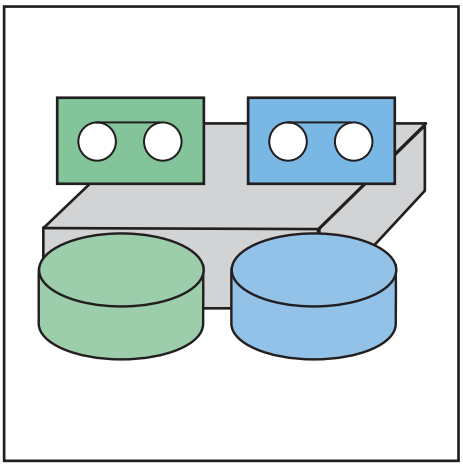
Schwerpunktthema

Storage: Backup von SAP-Umgebungen mit virtuellen Tape Libraries

von Dipl.-Inform. Matthias Egerland

Das Volumen der Daten, die innerhalb eines Unternehmens anfallen, wächst exponentiell. Wachstumsraten von 50% pro Jahr sind hier keine Seltenheit, auch bei unternehmenskritischen Daten. Hier spielt SAP eine zunehmend wichtige Rolle.

Unternehmen, die seit Jahren auf SAP setzen, sind genauso von der Frage nach der Datensicherheit betroffen, wie Unternehmen, die die Einführung von SAP erst planen. Über mehrere Standorte verteilte Cluster-Lösungen können zwar den aktiven Datenstand sicherstellen, doch für logische Fehler ist die Verfügbarkeit von Datensicherungen essentiell. Da auch in einer



Multi-Site-Umgebung der Ausfall eines beliebigen Standorts vom Backup-Konzept abgebildet werden muss, stellt sich gleichzeitig die Frage, wie Datensicherungen simultan auf mehrere Standorte verteilt werden können. Die hierfür relevanten sowohl organisatorischen als auch technologischen Überlegungen werden im Folgenden analysiert.

weiter auf Seite 11

Zweitthema

Shortest Path Bridging vs. TRILL

Ein Vergleich

von Markus Geller, Dipl.-Math. Cornelius Höchel-Winter

Seit Monaten wird im Netzwerkmarkt über zwei neue, konkurrierende Technologie-Standards diskutiert: „Shortest Path Bridging“ und „TRILL“. Die Aussagen, die dabei über beide Technologien gemacht werden, sind äußerst vielfältig: Von „Ablösung des Spanning Trees“ über „optimiertes Netzwerkdesign für Rechenzentren“ und „enorme Durchsatzsteigerungen“ bis „Provider-Technik“ wird nahezu jedes Schlagwort bemüht, das heutzutage Aufmerksamkeit verspricht.

Worum geht es tatsächlich? Wir werden im folgenden Artikel die drei standardisierten bzw. sich im Standardisierungsprozess befindenden Verfahren in ihren Grundzügen vorstellen und gegeneinander abwägen.

weiter auf Seite 23

Standpunkt Sicherheit

Stuxnet: Machtdemonstration und Armutszeugnis

auf Seite 8

Aktueller Kongress

IPv6-Forum 2011

ab Seite 4

Geleit

Migration zu IPv6: Wie aufwendig ist der Wechsel wirklich? Blockieren die Provider die Migration?

ab Seite 2

Neuer Termin

ComConsult Storage-Forum 2011 jetzt 13. - 15.07.11 in Bonn

ab Seite 20

Zum Geleit

Migration zu IPv6: Wie aufwendig ist der Wechsel wirklich? Blockieren die Provider die Migration?

In vielen Artikeln zu IPv6 wird die Migration geradezu als unterhaltsamer und kurzfristiger Spaziergang dargestellt. Unsere aktuellen Tests, die auch der Vorbereitung auf unser großes ComConsult IPv6-Forum dienen, zeigen klar auf, dass dies nicht so sein wird. Der Übergang wird mehr Zeit erfordern und er wird mit einer ganzen Reihe von Herausforderungen verbunden sein. Auch die fehlenden IPv6-Zugänge fast aller namhaften Provider deuten auf nicht unerhebliche technische Probleme hin. Zwar kann man mit Recht die Frage stellen, was die Provider eigentlich in den letzten Jahren getrieben haben, aber es ist offensichtlich, dass die Technik verfügbar wäre, wenn sie wirklich so trivial wäre.

Was bedeutet das konkret für ein aktuelles IPv6-Projekt? Welche Empfehlungen können gegeben werden?

- Das Projekt zur Migration sollte jetzt begonnen werden. Für die Vorbereitungen sollte das ganze Jahr 2011 eingeplant werden und die eigentliche Migration sollte in 2012 erfolgen. Entsprechende Geldmittel und Personal-Kapazitäten für die Vorbereitung sollten bereitgestellt werden.

- Die Idee, dass eine triviale Migration auf Basis Dual-Stack für Endgeräte, Layer-3-Switches und Router sowie Server erfolgen kann, sollte sofort gleich wieder vergessen werden. Die üblichen Trivialtests mit Windows-Clients und Windows-Servern decken zwar viele der Endgeräte, aber nur einen Teil der Problembereiche ab.

- Die Empfehlung, eine Liste aller betroffenen Geräte aufzustellen, sollte sehr ernst genommen werden. Unser ComConsult IPv6-Forum 2011 widmet sich bewusst in einem Vortrag dem Thema mobiler Endgeräte und deren Wireless-Zugang. Es ist erkennbar, dass hier einige Herausforderungen liegen.

- Weitere Gerätetypen müssen analysiert werden, um eine saubere Integration zu erreichen. Denken Sie an Drucker, Videoüberwachung, Zugangssysteme, Zeiterfassung, Gebäudeautomatisierung und den Fertigungsbereich.

- Auch sollte nicht übersehen werden, dass es Endgeräte gibt, die direkt miteinander kommunizieren. Hier ist es erforderlich, dass IPv6 auf beiden Seiten gesprochen wird. Dies betrifft IP-Telefonie, Video inkl. Raumkonferenzsysteme und die Integration von Fax und sonstigen Gateways. Hier stellt sich die Frage, ob eine stufenweise Migration für solche Welten überhaupt Sinn macht oder ob derartige Lösungen komplett auf einmal migriert werden müssen. Das generiert eine ganze Reihe von Folgeproblemen, da viele Hersteller Geräte von Drittherstellern in ihre TK und UC-Lösungen integriert haben. Nicht alle Dritthersteller werden bereit sein, der Roadmap des jeweiligen TK-Herstellers zu folgen.

- Auch müssen Protokolle berücksichtigt werden, die IP-Adressen als Parameter transportieren. Herausragend ist ohne Frage SIP. Es hat seinen Grund, dass selbst Microsoft zum Lync-Server, obwohl der keine Bestandskunden mit alter Technik berücksichtigen muss, keine Angaben zur Verfügbarkeit von IPv6 macht. Auch alle anderen TK-Hersteller haben zwar Roadmaps vorgestellt, sind aber von der eigentlichen Bereitstellung noch weit entfernt (Innovaphone hat die Verfügbarkeit für Mitte 2011 angekündigt).

- In jedem Fall muss davon ausgegangen werden, dass ein Parallelbetrieb von IPv4 und IPv6 unvermeidbar sein wird. Es werden zu viele Geräte existieren, die in absehbarer Zeit nicht IPv6 unterstützen werden.

- Es muss mit Herstellern gerechnet werden, die ihrer Verpflichtung, IPv6 bereit zu stellen, nicht ausreichend schnell nachkommen. Gerade Firewalls sind ein tückischer Bereich, da alle Regeln geändert werden müssen. Der Übergang nach IPv6 geht für Firewalls tief ins Eingemachte. Trotzdem ist es nicht akzeptabel, dass Hersteller wie Watchguard noch nicht einmal einen Termin nennen können. Dual-Stack-Betrieb für eine Firewall wird, soweit überhaupt durch den jeweiligen Hersteller unterstützt, erhebliche Anforderungen an Hauptspeicher und Rechenleistung stellen.

- Sorgen Sie dafür, dass Ihr Trouble-Shooting einsetzfähig bleibt. Hier werden eine ganze Reihe von Änderungen und auch Umgewöhnungen erforderlich sein.

- Gleiches gilt für System-Management-Lösungen und alle darum herum angeordneten Management-Bereiche, die IP-Adressen als Basis der Identifikation benutzen. Prüfen Sie, was der Umstieg auf IPv6 für Ihre Management-Lösungen bedeutet.

Wo liegen auf der Basis der bisherigen Untersuchungen mögliche Probleme:

- Wie auch schon die ct in einer kurzen Darstellung berichtet hat, muss die Nutzung von Tunneln egal welcher Art sicher sehr sorgfältig getestet werden. Nach dem Bericht der ct geht es dabei vor allem auch um einen Dauertest, da aus unerklärlichen Gründen in 10 bis 15 Prozent der Übertragungen Probleme auftraten. Betrachtet man die mit IPv6 vorgesehenen Tunnel-Mechanismen näher, dann wundert das nicht.

- Layer-3-Switches und Router müssen genau geprüft werden. Hier geht es ja nicht nur um den Speicher- und Rechen-Mehrbedarf des reinen IPv6-Stacks, es geht auch um Dual-Stack, Tunnel und Gateway-Einsatz. Der benötigte Hauptspeicher kann so schnell in den Bereich des 2 bis 3-fachen des heute vorhandenen kommen. Auch der Bedarf an Rechenleistung kann deutlich steigen.

- Die Nutzung von DNS und DHCP in Kombination mit einer gemischten IPv4 und IPv6-Umgebung muss sorgfältig getestet werden. Es gibt eine Reihe von Tücken im Detail.

Migration zu IPv6: Wie aufwendig ist der Wechsel wirklich? Blockieren die Provider die Migration?

- Mobile Endgeräte in Kombination mit Wireless-Zugängen stellen auf jeden Fall einen eigenen Bereich dar, der sorgfältig geprüft werden muss.

Sie haben sicher die Diskussion der häufig zitierten Autokonfiguration vermisst. Aus meiner Sicht stellt das den kleineren Problembereich dar, wenn eine harmonische Integration mit DHCP und DNS gelingt. Aber gerade die Nutzung des Namensdienstes wird zur Schaffung der erforderlichen Transparenz unverzichtbar sein. Die klare Forderung nach einer eindeutigen Identifizierbarkeit eines Endgeräts für Trouble-Shooting und CMDB-Zwecke ist dabei elementar. Es muss sicher geprüft werden, ob die Möglichkeit temporärer Adressen wie in der Autokonfiguration vorgesehen, innerhalb eines Unternehmens wirklich Sinn macht.

Zum Abschluss bleibt die Frage, wie glaubwürdig angesichts der Vielzahl von Optionen und Alternativen die seitens eines Herstellers zugesicherte „IPv6-Readyness ist“? Tatsächlich wird das in den nächsten Monaten zu prüfen sein. Das IPv6-Forum wird eine Schlüsselrolle übernehmen. Dieses hat das IPv6 Ready Logo Committee eingerichtet und führt entsprechende Tests durch und vergibt das IPv6-Ready-Logo. Wie gut und wie zuverlässig dieser Prüfprozess ist, wird sich herausstellen. Ihm kommt ein zentraler Stellenwert zu.

Wie Sie sehen, gibt es unzählige Fragezeichen und Varianten, die mit der Migration nach IPv6 verbunden sind. Wir analysieren für Sie diese Fragen und stellen auf dem ComConsult IPv6-Forum unsere Empfehlungen exklusiv für die Teilnehmer vor.

Die wichtigsten Punkte noch einmal zum Abschluss:

- Machen Sie sich klar, dass die Migration unvermeidbar ist. Die letzten IPv4-Adressbereiche sind letzte Woche an die Regional Internet Providers übergeben worden. Damit sind zwar noch Restbestände von IPv4-Adressen im Markt verfügbar, aber das Ende ist jetzt sehr nahe. Der Einstieg in IPv6 rollt jetzt weltweit an.

- SAAS als Teil von Cloud Computing ist ein ernstzunehmender Trend. Es gibt gute Gründe, einer ganzen Reihe von Cloud-Services mit großer Skepsis zu begegnen, doch der Zug in Richtung SAAS ist nicht mehr aufzuhalten. Die Vorteile für Software Hersteller sind zu groß. Neue Lösungen werden auf Dauer als IPv6-Angebote ins Netz gehen.

- NAT ist keine Dauerlösung, um dem Problem aus dem Wege zu gehen. Damit würde der Übergang zum öffentlichen Netzwerk zu einem Gateway werden. Firewall-Regeln würden auf Dauer sehr unübersichtlich.

- Jeder langfristig angelegte Parallelbetrieb vieler Endgeräte mit IPv4 und IPv6 sollte vermieden werden.

- Unterschätzen Sie die Migration nicht. Zu viele Varianten sind zu prüfen. Zu viele Sonderfälle werden existieren.

- Geben Sie dem Projekt ausreichend Zeit, Geld und Personal.

- Nutzen Sie 2011 für die Tests und planen Sie den Übergang für 2012.

- Die Verzögerungen auf der Providerseite sind zwar ärgerlich, aber nicht tragisch. Es gibt zu viele hausinterne Baustellen, als dass das Ihr Projekt behindern sollte. Natürlich würde man gerne mal die IPv6-Konnektivität nach Außen testen. Tatsächlich wird es vermutlich diese Möglichkeit im Laufe des Jahres geben.

Bei allem Aufwand bietet der Umstieg auf IPv6 eine gute Gelegenheit, in seinem IP-Netzwerke einmal richtig aufzuräumen. Viele Kunden haben historisch gewachsene IPv4-Adressstrukturen und Betriebsverfahren, die dringend einer Konsolidierung bedürfen. Nun ist der ideale Zeitpunkt gekommen, hier ein sauberes Betriebs-Fundament zu schaffen.

Auf jeden Fall wünsche ich Ihnen viel Erfolg mit diesem herausragenden Projekt.

Ihr
Dr. Jürgen Suppan

Frühbucher-phase nur noch bis zum 15.02.2011

Kongress

ComConsult IPv6-Forum 2011
09. - 11.05.11 in Königswinter

Der Wechsel von IPv4 auf IPv6 ist unvermeidbar und wird in 2011 weltweit im großen Stil beginnen. Dabei liefert IPv6 nicht nur einen neuen Adressraum sondern ein völlig verändertes Betriebsszenario. DNS, DHCP und wesentliche Teile der vorhandenen Sicherheits-Lösungen müssen neu durchdacht und angepasst werden. Speziell Firewall- und NAT-Installationen sind betroffen.

Moderator: Markus Schaub
Preis: € 1.790,--* zzgl. MwSt. - gültig bis 15.02.2011 dann € 1.990,-- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Neuer Kongress

ComConsult IPv6-Forum 2011

Die ComConsult Akademie veranstaltet vom 09.05. - 11.05.11 ihren neuen Kongress „ComConsult IPv6-Forum 2011“ in Königswinter.

Der Wechsel von IPv4 auf IPv6 ist unvermeidbar und wird in 2011 weltweit im großen Stil beginnen. Dabei liefert IPv6 nicht nur einen neuen Adressraum, sondern ein völlig verändertes Betriebsszenario. DNS, DHCP und wesentliche Teile der vorhandenen Sicherheits-Lösungen müssen neu durchdacht und angepasst werden. Speziell Firewall- und NAT-Installationen sind betroffen.

Der Wechsel von IPv4 auf IPv6 ist aus mehreren Gründen komplex und bedarf einer sorgfältigen Planung:

- Es sind Applikationen, Endgeräte, Server, Drucker, Netzwerk-Komponenten betroffen. Der Wechsel muss so erfolgen, dass er über alle diese Komponenten hinweg funktioniert
- Viele Applikationen und Komponenten sind IPv6-ready, aber nicht alle und nicht in allen Firmware-Versionen. Hier muss eine Inventur erfolgen, ggf. müssen Beschaffungen ausgelöst werden
- Ein Sofortumstieg wird selten machbar sein, ein sinnvoller Migrationsweg muss gefunden werden, der alle Anwendungen und Gerätetypen sowie ihre Eigenarten berücksichtigt

- Externe Dienste werden in Kürze auf der Basis von IPv6 angeboten werden. Das betrifft Cloud-Services, Email-Dienste und Kollaboration im weitesten Sinne. In jedem Fall muss geklärt werden, wie diese Dienste in eine vorhandene IPv4-Umgebung eingebunden werden
- Da IPv6 ein neues und anderes Betriebs-Szenario mitbringt, ist zu klären wie dieses genutzt wird. Tatsächlich bestehen erhebliche Optionen, deren Tragweite auf den ersten Blick nicht klar ist

Hier setzt unser ComConsult IPv6-Forum 2011 an. Es greift diese Fragen strukturiert auf und zeigt den optimalen Weg nach IPv6 auf. Im Einzelnen leistet das IPv6 Forum 2011:

- IPv6 und seine technische Konzeption wird erklärt und diskutiert
- Die verschiedenen Betriebsszenarien werden verglichen
- Migrationswege werden analysiert und bewertet
- Die technische Situation der verschiedenen Komponenten vom Endgerät über den Server bis zum Netzwerk wird erläutert
- Beispielprojekte und Laboranalysen werden vorgestellt
- Empfehlungen für den besten Weg nach IPv6 werden von ausgewählten Experten vorgestellt

Das ComConsult IPv6-Forum ist ein Muss für alle Betreiber und Planer von Netzwerken, Endgeräten, Servern, Speichersystemen und Applikationen im Netzwerk. Versäumen Sie nicht, sich rechtzeitig einen Platz auf dieser herausragenden Veranstaltung zu sichern.

Die Moderation des Forums übernimmt Markus Schaub von ComConsult-Study.tv.

Frühbucherrabatt bis 15.02.11

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult IPv6-Forum 2011

Ich buche den Kongress
ComConsult IPv6-Forum 2011

☐ 09.05. - 11.05.11 in Königswinter
zum Preis von € 1.790,--* zzgl. MwSt.

*Preis gültig bis zum 15.02.2011

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Aktueller Kongress

Netzwerk-Redesign-Forum 2011

Die ComConsult Akademie veranstaltet vom 04.04. - 07.04.11 ihren Kongress „Netzwerk-Redesign Forum 2011“ in Königswinter.

Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, das Campus-Netzwerk, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Neue Standards zur Gestaltung von Netzwerken im Rechenzentrum und im Backbone sind gute Beispiele dafür. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen.

Die Entwicklung geht einher mit einem neuen Kampf um den Markt. Neue Standards erfordern neue Produkte, die technische Entwicklung führt zu neuen Leistungsmaßstäben bei Produkten und damit öffnet sich die Tür für einen neuen Wettbewerb in einem bisher aufgeteilten Markt. Standard-Leistung wird zunehmend durch Standard-Chips erbracht werden. Unterschiede zwischen Herstellern werden verschwimmen. Der Preis als Kaufargument wird noch wichtiger werden als bisher. Was bedeutet das für die bekannten Anbieter? Kann Cisco seine Position verteidigen, gelingt HP der großangelegte Angriff, wie verhalten sich die anderen Hersteller und welche Chancen haben sie? Leisten Netzwerke in Zukunft mehr und kosten weniger?

Das ComConsult Netzwerk Redesign Forum 2011 analysiert und diskutiert diese Änderungen und ihre Auswirkungen speziell auf die Netzwerk-Infrastrukturen.

Im Mittelpunkt des Forums stehen dementsprechend die Themenbereiche:

- Was ändert sich im Umfeld von Netzwerken? Welche neuen Architekturen und Anforderungen müssen Netzwerke konkret erfüllen?
- Wie verändern sich demgegenüber Netzwerke selber? Welche neuen Technologien und Standards kommen auf uns zu?
- Wie passen Anforderungen aus IT-Architekturen, Clients, Applikationen und Speicher mit den neuen Netzwerk-Standards zusammen? Wann und wie können die Anforderungen erfüllt werden?
- Wie verändern neue Anforderungen, neue Standards, neue Technologien und neue Produkte den Markt? Wie positionieren sich die Hersteller für den neuen und noch intensiveren Wettbewerb?

Das ComConsult Netzwerk-Redesign Forum 2011 ist ein Muss für alle Betreiber und Planer von Netzwerken. Wie immer wird sich auch 2011 hier die Branche treffen. Top-Experten, kontroverse Diskussionen, Projektbeispiele stehen auf der einen Seite. Die Hersteller stellen sich einem Musterprojekt auf der anderen Seite. Wohin geht der Netzwerk-Markt und was ist wirklich wichtig? Das ComConsult Netzwerk-Redesign Forum 2011 ist unsere Top-Veranstaltung des Jahres 2011. Versäumen Sie nicht, sich rechtzeitig einen Platz auf dieser herausragenden Veranstaltung zu sichern.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign-Forum 2011

Ich buche den Kongress
Netzwerk-Redesign-Forum 2011

inkl. Workshops am letzten Tag
☐ 04.04. - 07.04.11 in Königswinter
zum Preis von € 2.390,-- zzgl. MwSt.

Workshopauswahl
☐ Workshop 1: Ultra Low Latency (ULL) Networks und DCB
☐ Workshop 2: Wireless LAN und Co

ohne Workshops am letzten Tag
☐ 04.04. - 06.04.11 in Königswinter
zum Preis von € 1.990,-- zzgl. MwSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Programmübersicht - Netzwerk-Redesign Forum 2011

Montag, den 04.04.2011 - Moderation: Dr. Kauffels, Dr. Moayeri

9:30 bis 11:00 Uhr

Was sich im Netz verändert

- Wo werden 40/100 Gbit Ethernet benötigt: im RZ, im Campus, im WAN? • Was ist im Access-Bereich nötig?
- Auswirkungen von Virtualisierung auf die Netze
- Konvergenz: ein Netz für Client-Server-Verkehr, Storage, Voice und Video?
- Mandantenfähige Netze und warum sie benötigt werden
- Warum IPv6 nicht mehr aufzuhalten ist

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:45 Uhr

Entwicklung der IT-Architekturen und Auswirkungen auf Netzwerke

- Web-Architekturen und Virtualisierung
- Konvergenz und Konzentration
- Anforderungen an das Netz als Systembus: Leistung und Latenzarmut • Unterschiede zwischen RZ und Campus
- 10, 40 oder 100 GbE?

Dr. Franz-Joachim Kauffels, Unternehmensberater

12:45 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr

Netzstruktur: Layer 2 versus Layer 3

- Neue Verfahren für die Netzstrukturierung: TRILL und Shortest Path Bridging • Sind klassische Layer-3-Strukturen überhaupt noch erforderlich?
- Können neue Layer-2-Mechanismen den Übergang zu IPv6 erleichtern?

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

15:00 bis 15:45 Uhr

Verkabelung im Backbone- und Access-Bereich

- Singlemode im Backbone-Bereich, werden die Standardfasern den zukünftigen Anforderungen noch gerecht, welche Typen sind sinnvoll?
- Macht die Multimodefaser im Backbone-Bereich noch Sinn, wenn ja, welchen? • Steckertechniken im Glasfaserbereich, gibt es qualitative Unterschiede? Welche sind sinnvoll, lohnt sich ein Umstieg auf neue Typen, wenn ja auf welche?
- Innovationen im Tertiärbereich, welche lohnen sich?
- Ist die Zeit gekommen für Kategorie-7 oder genügt auch weniger, was bringt das „Mehr“ und welche Planungskonsequenzen haben die verschiedenen Alternativen? Wie sieht die aktuelle Marktsituation aus?

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

15:45 bis 16:15 Uhr - Kaffeepause

16:15 bis 17:00 Uhr

Neue Entwicklungen im WAN-Bereich

- Macht Carrier Ethernet MPLS überflüssig?
- Was ist von Microsoft Direct Access zu halten?
- WAN Acceleration: wo ist diese Technologie sinnvoll?

Dipl.-Inform. Andreas Meder, ComConsult Beratung und Planung GmbH

17:00 bis 17:45 Uhr

Provider-Technik im Unternehmensnetz: ist das die Zukunft?

- Private Cloud: Unfug oder die Zukunft der Unternehmens-IT?
- Sollte und kann die Unternehmens-IT so organisiert und betrieben werden wie eine Provider-Infrastruktur?
- Wavelength Division Multiplexing (WDM): Varianten und Nutzbarkeit in Unternehmensnetzen
- Über WDM hinaus: Optical Transport Network (OTN) gemäß G.709 und Perspektiven eines Einsatzes im Campus

Dr. Franz-Joachim Kauffels, Unternehmensberater

ab 18:00 Uhr - Happy Hour

Dienstag, den 05.04.2011 Vormittag - Moderation: Frau Borowka-Gatzweiler, Dr. Kauffels

9:00 bis 9:45 Uhr

Anforderungen von Voice und Video an Netze

- Unterschiede zwischen Voice und Video
- Anforderungen neuer Video Codecs
- Welche Bandbreite ist erforderlich?
- Wo ist QoS einzusetzen?
- Hat die die traditionelle Videokonferenz ausgedient? Welche Rolle spielen neue Verfahren wie SVC?
- PoE flächendeckend oder bei Bedarf?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

9:45 bis 10:45 Uhr

Desktop-Virtualisierung: was bedeutet das für das Netz?

- Architektur aktueller Virtueller Desktop Infrastrukturen (VDI)
- Welche Aufgaben haben die einzelnen Architekturbestandteile und welche Auswirkungen hat dies auf das Datennetz?
- Zusammenspiel mit Servervirtualisierungstechniken: Anforderungen an das logische Netzdesign
- Leistungsanforderungen an Server, Netzwerk, Speicher
- Welche Rolle spielen die Übertragungsprotokolle (z.B. RDP, ICA, PCoIP, ALP, SPICE etc.)?
- USB-Redirection: neben der technischen Herausforderung, was bedeutet das für die erforderliche Bandbreite?
- Thin Client, Zero Clients: welche Anforderungen bringen Endgeräte in den Access-Bereich?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

10:45 bis 11:15 Uhr - Kaffeepause

11:15 bis 12:15 Uhr

Data Center Bridging oder IEEE 802.1BA als neue QoS-Architektur?

- Was bedeutet DCB? • Ersetzt DCB klassische QoS-Architekturen? • Ist der Einsatz von DCB außerhalb der Rechenzentren sinnvoll?
- Welche Rolle kommt Audio Video Bridging (AVB) Systems gemäß IEEE 802.1BA zu?

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

12:15 bis 13:30 Uhr - Mittagspause

Programmübersicht - Netzwerk-Redesign Forum 2011

Dienstag, den 05.04.2011 Nachmittag- Moderation: Frau Borowka-Gatzweiler, Dr. Kauffels

13:30 bis 14:15 Uhr

Mandantenfähige Netze

- Warum werden mandantenfähige Netzstrukturen benötigt?
- Gastnetz über LAN, WLAN oder LTE/GSM?
- Tücken bei Network Access Control
- Anforderungen an Firewalls, Intrusion-Prevention-Systeme und Security Gateways
- Was wird durch MACsec und 802.1X-2010 geändert?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:15 bis 15:00 Uhr

Zukunft der Netzanalyse

- Vorratsdatenspeicherung im Netz?
- Infrastruktur für forensische Untersuchungen im Netz
- Kommt die Vorratsdatenspeicherung der Fehlersuche und der IT-Sicherheit zugute?
- Paketanalyse oder intelligente Expertensysteme?
- Paketanalyse - ein Mehrwert für das Netzwerkmanagement?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:45 Uhr

IPv6-Migration

- Konstellationen
- Grundlegende Ansätze
- Beiträge der Kommunikations-Endpunkte (Clients, Server, ...)
- Konkretisierung aus Sicht der Kommunikations-Endpunkte
  - Windows • Unix • Drucker?! • Drucker und Multifunktionsgeräte? • IP-Telefone, MDAs etc.?

Dipl.-Inform. Oliver Flüs, ComConsult Beratung und Planung GmbH

Mittwoch, den 06.04.2011 - Moderation: Frau Borowka-Gatzweiler, Dr. Moayeri

9:00 bis 9:45 Uhr

Anforderungen an die Netzkomponenten: virtuelle Ausschreibung

- Performance-Anforderungen
- Unterstützung neuer Verfahren und Standards: DCB, TRIIL, SPB, …
- Energie-Effizienz
- Netzmanagement

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

9:45 bis 15:00 Uhr

Hersteller stellen sich der virtuellen Ausschreibung

12:45 bis 14:00 Uhr - Mittagspause

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:00 Uhr

Diskussionsrunde: Frau Borowka-Gatzweiler, Dr. Moayeri, Dr. Kauffels und die Hersteller

Donnerstag, den 07.04.2011 - Ein-Tages-Intensiv-Trainings/Workshops - 9:00 - 15:30 Uhr

Workshop 1:

Ultra Low Latency (ULL) Networks und DCB

- Allgemeine Anwendungsbereiche für ULL-Networks, z.B. Finanznetze
- Das ULL Network als Systembus Virtualisierter Gesamtlösungen
- Sind vollständige, skalierbare Netze mit einer Ende-zu-Ende Verzögerung im Bereich weniger Mikrosekunden machbar?
- Wie sieht das Chipdesign für Switches aus, die mit Latenzen im Bereich einiger Hundert Nanosekunden arbeiten?
- Die tragende Rolle der DCB-Funktionen
- Wie sind die Kosten dafür zu beurteilen? Ist das Ganze unerschwinglich?
- Reichen Designansätze wie Clos-Netze mit TRILL oder PLSB aus oder müssen noch weiter optimierte Konstruktionen betrachtet werden?
- Integration von ULL-Networks in Virtualisierungskonzepte
- Die Rolle etablierter Hersteller ist hier noch bescheiden. Wer sind die Herausforderer und wie ist deren Gesamtstrategie?

Dr. Franz-Joachim Kauffels, Unternehmensberater

Workshop 2:

Wireless LAN und Co.

- WLAN-Design mit IEEE 802.11n
- Herausforderung an Planungstools und Messtechnik durch neue WAN-Technologien
- Controller-basiertes WLAN-Design: Architekturvarianten und Herstellerlösungen im Vergleich
- Long-Term Evolution: Wohin steuert der Mobilfunk?
- Frequenzmanagement und Regulierung
- Sichere WLANs: Entsorgung von Altlasten und Umgang mit neuen Techniken

Dr. Simon Hoff, Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

10:30 bis 11:00 Uhr - Kaffeepause

12:30 bis 14:00 Uhr - Mittagspause

15:30 Uhr - Ende der Veranstaltung

Standpunkt Sicherheit

Stuxnet: Machtdemonstration und Armutszeugnis

Der Standpunkt Sicherheit von Dr. Simon Hoff greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Der Wurm Stuxnet hat letztes Jahr Furore gemacht, da er höchstwahrscheinlich mit der Absicht, das iranische Atomprogramm zu sabotieren, entwickelt worden ist. Hierzu greift er zielgerichtet spezielle Anlagen des Herstellers Siemens an. Über den Erfolg gibt es unterschiedliche Aussagen, es gibt jedoch deutliche Anzeichen, dass durch Stuxnet die höchstempfindliche Steuerung der Zentrifugen zur Anreicherung von Uran so gestört worden ist, dass das Atomprogramm erheblichen Schaden genommen hat. Inzwischen wird befürchtet, dass Stuxnet bereits als Vorbild für andere Angriffe dient, und es wurden schon Vorstellungen von Katastrophen bis hin zur Kernschmelze geweckt.

Stuxnet war eine gezielte Sabotageaktion, die einen erheblichen Aufwand an Expertenwissen (und Kosten für den Einkauf von Exploits) erfordert hat. Stuxnet war aber noch mehr.

Stuxnet war eine Machtdemonstration!

Stuxnet hat zunächst bewusst gemacht, dass schadenstiftende Software in Abläufe kontrollierend eingreifen, reale Dinge bewegen, physikalische Systeme steuern kann. Stuxnet hat aber insbesondere sehr laut und deutlich gezeigt, wie effektiv und effizient Angriffe ablaufen können, die auf der einfachen Tatsache beruhen, dass im modernen Anlagenbau massiv Standard-IT eingesetzt wird.

Vernetzte Anlagen, die Standard-IT-Komponenten und -Protokolle verwenden, erben zunächst automatisch die gesamte Last der Gefährdungen der Standard-IT. Würmer, die sich über den Anschluss eines infizierten PCs (z.B. einer Service-Technikers) an das Netz in der Produktion über nicht gepatchte Windows PCs in Anlagen hermachen und die Produktion lahmlegen, hat es daher schon früher gegeben. Nur war dies eher ein Sicherheitsvorfall durch Unachtsamkeit und kein zielgerichteter Angriff wie bei Stuxnet.

Nun könnte man vielleicht meinen, dass es doch ein Leichtes sein müsste, die im Office-IT-Bereich seit langem etablierten Standardsicherheitsmaßnahmen wie Virenschutz, Patch-Management und Härtung auf den Anlagenbereich zu portieren. Weit gefehlt! Nachdem eine Anlage in Betrieb genommen ist, möchte man die Elemente der Anlage am liebsten nicht mehr verändern. Wie kann beispielsweise bei einem Patch sichergestellt werden, dass die Anlage noch wie gewünscht funktioniert? Jeder Patch verursacht also einen (im Vergleich zu Office-Anwendungen) erheblichen Aufwand durch Analysen und Tests der Auswirkungen eines Patches. Wenn PCs im Anlagenbereich überhaupt gepatcht werden, dann ist oft zumindest das Zeitraster um ein Vielfaches gröber als im Office-Bereich.

Der Trend des Einsatzes von Standard-IT für Spezialsysteme verbunden mit der Konvergenz zu IP-basierter Vernetzung der Komponenten und Nutzung von Standard-Protokollen und -Middleware findet sich in vielen anderen Bereichen. Zu nennen ist beispielsweise neben der Medzintechnik die Gebäudetechnik. Die Idee, als vorbereitende Maßnahme für einen Einbruch durch eine schadenstiftende Software eine Überwachungsanlage zu manipulieren, ist nicht abwegig.

Die Verwendung von Standard-IT in der Automatisierungstechnik und in verwandten Bereichen erzwingt konsequente Sicherheitsmaßnahmen. Der Schutz vor schadenstiftender Software muss mindestens die Qualität aufweisen, die im Office-IT-Bereich möglich ist. Wenn hierzu PCs in Maschinen und Steuerungen nicht angemessen gehärtet und mit einem soliden Virenschutz und Patch-Management gesichert werden können, muss mit anderen Mitteln ein vergleichbarer Schutz geschaffen werden. Hier müssen dann Maßnahmen der Netztrennung kritischer Bereiche in Verbindung mit Firewall- und Intrusion-Prevention-Techniken greifen.

Stuxnet hat auch gezeigt, dass in kritischen Bereichen damit zu rechnen ist, dass neue bzw. noch nicht in Umlauf befindliche Exploits zum Einsatz kommen und es durchaus gefährlich lange dauern kann, bis ein Patch für die entsprechende Verwundbarkeit zur Verfügung steht. In kritischen Bereichen (und dies sind selbstverständlich auch alle Bereiche, in denen ein Angriff erheblichen wirtschaftlichen Schaden bedeuten kann) müssen daher auch Konzepte zur Begrenzung der Angriffsfläche und zur Verkleinerung des Wirkungskreises einer Schadsoftware umgesetzt werden.

Die Produkte der IT-Sicherheitsbranche schützen primär vor historischen Viren und Würmern. Solche Produkte sind daher gegen Szenarien, wie wir sie im Fall von Stuxnet erlebt haben, wertlos. Das ist ein Armutszeugnis für die gesamte IT-Industrie. Wie konnte es dazu kommen, dass das Einstecken eines USB-Sticks eine Industrieanlage des Weltmarktführers so empfindlich stören konnte? Machen wir uns nichts vor: Die verständliche Freude darüber, dass ohne militärische Maßnahmen der Griff eines unliebsamen Regimes nach der Atombombe erschwert wurde, täuscht darüber hinweg, dass Stuxnet eigentlich ein sehr besorgniserregendes Armutszeugnis darstellt.

Wir machen mittlerweile Leib und Leben von Menschen davon abhängig, dass reichlich vorhandene Sicherheitslücken der IT nicht missbraucht werden. Ein Armutszeugnis für die Automatisierungsbranche. Stuxnet ist auch ein Armutszeugnis für den Ansatz „Security by Obscurity“. Hersteller wollen suggerieren, dass die Geheimhaltung der Interna von Hardware und Software auch der Sicherheit dient. Das ist ein Trugschluss. Sicherheit erfordert Offenheit. Nur ein offengelegter Quellcode stellt sicher, dass Sicherheitslücken auch bekannt werden können, bevor sie ausgenutzt werden.

Ein Prozess des Umdenkens muss beginnen. Nicht nur in der IT-Branche.

Sonderveranstaltung

Weiterer Zusatztermin:
UC - Cisco versus Microsoft
Wer hat die bessere Unified-Communications-Lösung?

Die ComConsult Akademie veranstaltet aufgrund der hohen Nachfrage am 24.03.11 eine dritte Durchführung ihrer Sonderveranstaltung „UC - Cisco versus Microsoft“ in Düsseldorf.

Die Sonderveranstaltung „ UC - Cisco versus Microsoft“ analysiert die bestehenden UC-Lösungen von Cisco und Microsoft und stellt die spannende Frage, wer die bessere Lösung hat. Auch die erkennbaren Weiterentwicklungen der nächsten Jahre werden dabei berücksichtigt. Bewertet wird nicht nur die rein technische Funktionalität, sondern die Veranstaltung gibt auch Einschätzungen zum strategischen Einsatz sowie zur Zukunftssicherheit der Produkte ab.

Übersicht über Unified Communications
- Was heißt Unified Communications?
- Kontakte / Verzeichnisdienst
- Presence / Erreichbarkeitsdienst
- Instant Messaging (IM)
- Voice / TK / Video
- Konferenzen: Audio-, Video- Web-, IM-Konferenz
- E-Mail Integration
- Unified Messaging
- Integration mobiler Benutzer
- Verschiedene Architekturen von UC-Lösungen
- Typische Einsatzszenarien für UC

Vergleich: Die UC-Lösungen von Cisco und Microsoft
- Architektur, Redundanzmöglichkeiten, Integration der non-IP Welt

- Lösung eines vorgegebenen Einsatzszenarios
- Endgeräte / Clients
- Kontakte / Verzeichnisdienst, Erreichbarkeits-Dienste (Presence)
- Kommunikationsfunktionen: IM, Voice, Video, Konferenz, E-Mail-Integration
- Integration mobiler Benutzer
- Management und Administration
- Schnittstellen, 3rd Party Integration, Zertifizierung
- Lizenzmodell, Partner, Referenzen
- Typischer UC-Arbeitsablauf unter Nutzung verschiedenster Funktionen

Live Demo: Die UC-Lösungen von Cisco und Microsoft
- Instant Messaging (IM)
- Eskalation zur Audiokonferenz
- IM Nebenkonferenz
- Eskalation zur Videokonferenz
- Eskalation zur Webkonferenz
- Hinzunahme von Shared Application mit Excel und Word
- Hinzunahme eines weiteren Teilnehmers per Namensmarkierung aus Word
- Nutzung eines Flipchart während der Konferenz
- Aufzeichnung
- Neue Konferenz
- Einspielung der Aufzeichnung
- Fragen an die Hersteller

Kriterienliste zur Evaluierung der UC-Lösungen von Cisco und Microsoft
- Vorstellung der bewerteten Bereiche und ihrer Gewichtung
- Zusammenfassender Vergleich der Lösungen von Cisco und Microsoft
- Stärken und Schwächen von Cisco und Microsoft
- Fazit und Ausblick

Eine derartige Gegenüberstellung der UC-Lösungen dieser beiden Hersteller hat es bisher noch nicht gegeben, sie ist einzigartig und kontrovers. Diese Sonderveranstaltung der ComConsult Akademie ist ein elementares Hilfsmittel für jede Evaluierung des UC-Marktes. Der Kriterien-Katalog ist zudem so aufgebaut, dass er auch auf andere Hersteller übertragen werden kann.

Referentin und Moderatorin dieser Sonderveranstaltung ist Petra Borowka-Gatzweiler, vergent Aachen und UBN.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
UC - Cisco versus Microsoft

Ich buche die Sonderveranstaltung
UC - Cisco versus Microsoft

☐ 24.03.11 in Düsseldorf
zum Preis von € 890,-- zzgl. MwSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

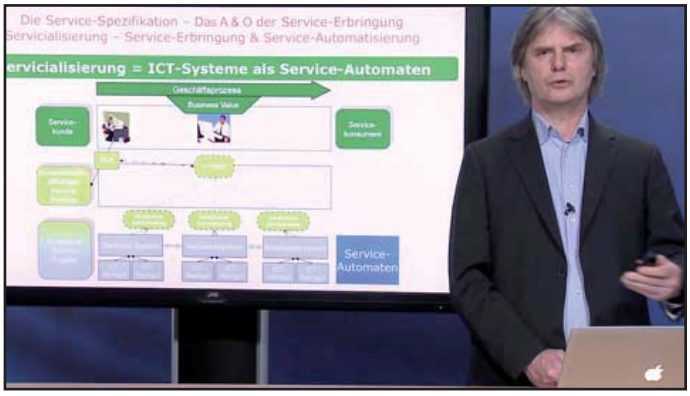
_____ Unterschrift

ComConsult-Study.tv

Aktuelle Neuerscheinungen bei ComConsult-Study.tv

Themenbereich: Betrieb und Architekturen

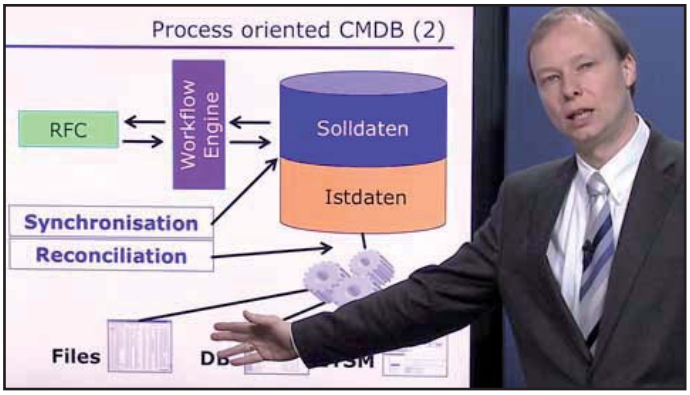
Service-Spezifikation
Referent: **Dipl.-Ing. Paul G. Huppertz**
Zeit: 00:37:21
Preis: Kostenlos mit Abo



Die Service-Spezifikation ist das Fundament jeder erfolgreichen Service-Erbringung. Dieses Video erklärt, wie eine Service-Spezifikation entsteht und wie sie stufenweise die Basis für alle Bausteine eines erfolgreichen Service-Betriebs legt.

Themenbereich: Betrieb und Architekturen

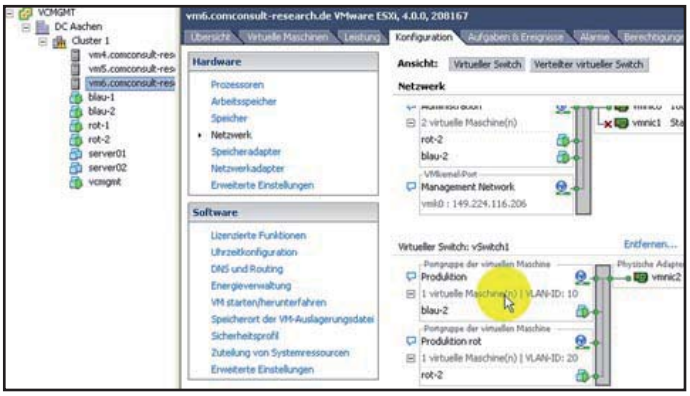
CMDB im CMS-Umfeld
Referent: **Dipl.-Ing. Ingo Voßkötter**
Zeit: 00:20:47
Preis: Kostenlos



Configuration Management Data Base Lösungen stehen theoretisch im Zentrum jeder System-Management-Lösung. Doch die Spannbreite der Lösungen ist groß. Lernen Sie in diesem Video, was eine richtige CMDB-Lösung ausmacht und welche Alternativen der Einbindung bestehen.

Themenbereich: Software

Seminar: Netzwerke mit VMware vSphere konfigurieren: Theorie und Praxis - Teil 6
Referent: **Dipl.-Math. Cornelius Höchel-Winter**
Zeit: 00:23:13 gesamtes Seminar 02:33:10
Preis: Kostenlos mit Abo



Dieses mehrteilige Seminar führt ausgehend von der Konzeption bis hin zur konkreten Administration in die optimale Konfiguration von Netzwerken unter VMware vSphere ein. Dabei geht jedem Praxisteil eine Einführung und Erklärung der Technologie voran, so dass die Konzepte verstanden werden können bevor die Praxis angegangen wird. Dieses Seminar erklärt nicht nur wie Sie vSphere/ESXi konfigurieren, sondern auch was dahinter steckt und welche Alternativen Sie haben.

Themenbereich: Netzwerke

Seminar: Siemens Open Scape Suite - Teil 3
Referent: **Markus Geller**
Zeit: 00:17:55 gesamtes Seminar 00:54:39
Preis: Kostenlos mit Abo

Dieses 3-teilige Seminar gibt einen kompakten Überblick über die Siemens OpenScape UC-Lösung, angefangen bei den Modulen und der Architektur und endend bei der Client-Applikation. In diesem Seminar werden Praxis- und Theorie-Module gemischt, so dass neben der Vorstellung der Architektur auch die Nutzung in der Praxis diskutiert werden kann. Der ideale Start für eine Evaluierung des Produkts.

Schwerpunktthema

Storage:

Backup von SAP-Umgebungen mit virtuellen Tape Libraries

Fortsetzung von Seite 1

Dipl.-Inform. Matthias Egerland hat an der RWTH Aachen Informatik studiert und ist seit 2005 Mitarbeiter der ComConsult Beratung und Planung GmbH. Er ist Leiter des Competence Center Data Center und unterstützt die Competence Center IT-Sicherheit und Netze. Neben den Schwerpunkten Desktop-, Server- und Infrastruktur-Virtualisierung beschäftigt sich Herr Egerland insbesondere mit Speicherlösungen in virtualisierten Umgebungen. In Projekten erstellt er Konzepte und Ausschreibungen von IT-Infrastruktur-Lösungen gemäß UfAB in den Bereichen Lokale Netze (LAN) für mehrere tausend Teilnehmer, aktive Rechenzentrumskomponenten – insbesondere Server, Speicher, Netzwerk und Firewalls – sowie Virtuelle Informationstechnologie.

1. Datensicherung und -wiederherstellung im SAP-Umfeld

In diesem Kapitel werden grundlegende Verfahrensweisen zur Datensicherung und -wiederherstellung dargestellt. Nach den allgemeinen Aspekten und Datensicherungsverfahren inkrementeller, differentieller und block-basiert inkrementeller Backups wird auf das Konzept virtueller Tape Libraries (VTL) eingegangen. Nach der exemplarischen Darstellung des Aufbaus einer SAP-Umgebung werden die verschiedenen Software-Komponenten dargestellt, die für die Durchführung einer Datensicherung ineinander greifen. Da SAP auf Oracle-Datenbanken aufbaut, wird anschließend die Struktur näher beleuchtet, die Oracle zur Durchführung von Datensicherungen bereitstellt.

1.1 Allgemeines

Völlig unabhängig von den Redundanzen in der Speicherumgebung oder in den Teilkomponenten der Speicherumgebung sind Datensicherungen unabdingbar für die Erhaltung der Verfügbarkeit von Daten. Während Redundanzen im Wesentlichen vor Hardware-Fehlern schützen, bewahrt die Datensicherung vor dem Datenverlust bei logischen und operationellen Fehlern sowie Software-Schäden. Selbst beim Einsatz von Clusterlösungen auf Server-Speicherebene hat daher eine regelmäßige Datensicherung zu erfolgen. Zu sichern sind die Daten, die für den Fortbestand und die Aufrechterhaltung des produktiven Betriebes notwendig sind.

Eingesetzt werden die durchgeführten Datensicherungen für die Wiederherstellung von zerstörten, gelöschten oder aus sonstigen Gründen nicht mehr zugänglichen Daten.

Für ein genaues Begriffsverständnis werden die folgenden Definitionen festgehalten:

- Unter einer Sicherung oder Backup wird die Speicherung von aktiven Daten verstanden. Aktive Daten sind die Daten, die auf den Servern und/oder auf den Speichersystemen für den produktiven Betrieb der Systeme und Applikationen benötigt werden.

- Unter einer Wiederherstellung oder einem Recovery wird der Wiederherstellungsprozess von Daten verstanden, die zuvor gesichert worden sind. Wenn z.B. ein Verzeichnis gelöscht wurde, dann ist dieses Verzeichnis wiederherzustellen. Unter Recovery fällt auch die Wiederherstellung eines Serversystems mit den Betriebssystemdaten und den Applikationsdaten.

- Das Zurückholen von archivierten oder bereits ausgelagerten Daten wird als Restore bezeichnet.

Für die Konzipierung einer Datensicherung sind sowohl technische als auch organisatorische Aspekte zu beachten. Die technischen Aspekte dienen der Auswahl der einzusetzenden Technik, welche als Basis für eine Technologieauswahl die folgenden Punkte berücksichtigen sollte:

- Verfügbarkeit der Datensicherungslösung,

- Datenvolumen, welches zu sichern ist,

- Performance, die notwendig ist, um eine Sicherung innerhalb von definierten Zeiten durchführen zu können bzw. Daten wiederherstellen zu können (maximale Wiederherstellungszeit),

- Applikationen, die in Abhängigkeit der eingesetzten Sicherungssoftware entsprechende Unterstützung durch Agenten und/oder Optionen erfordern, und

- Sicherungsverfahren.

Ein wichtiges Ziel bei der Datensicherung ist die Minimierung der Zeit, die zwischen folgenden Punkten verstreicht:

- Recovery Point Objective (RPO): Zeitpunkt, von dem die letzten konsistenten und korrekten Daten vorliegen und auf den zurückgesetzt werden kann

- Recovery Time Objective (RTO): Zeitpunkt, von dem an die Informations- und Kommunikationsdienstleistungen wieder verfügbar sind mit dem Stand des letzten konsistenten und korrekten Sicherungspunktes

Der Zusammenhang zwischen RPO, Zeitpunkt des Katastropheneintritts, Wiederherstellungszeit und RTO ist in Abbildung 1 dargestellt.

Zwischen dem Eintritt der Katastrophe und dem RTO verstreicht die Wiederherstellungszeit. Im Katastrophenfall (zum Beispiel Ausfall eines Rechenzentrums) entspricht der Zeitpunkt des Eintritts der Katastrophe dem Konsistenzpunkt, wenn die Daten gespiegelt sind.

Die organisatorischen Aspekte einer Konzipierung berücksichtigen den Standort der Datensicherungsmedien und deren Lagerung bzw. Auslagerung. Ebenso ist eine Sicherungsstrategie notwendig, die besonders im Falle der Wiederherstellung einen ausschlaggebenden Zeitfaktor darstellen kann. So ist eine inkremen-

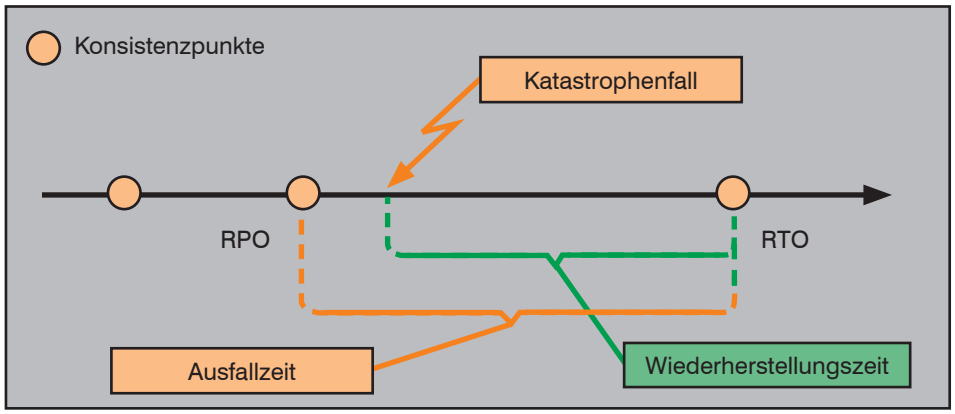


Abbildung 1: K-Fall-Vorsorge durch Datensicherung

telle Sicherung bei der Wiederherstellung organisatorisch zeitaufwendiger als eine differentielle oder volle Sicherung. Ein weiterer Aspekt ist die Aufteilung der Verantwortungsbereiche nach Sicherungsdurchführung und Wiederherstellung bzw. Restore.

Grundsätzlich sind die Anforderungen an die Durchführung eines zeitgemäßen Backups in den letzten Jahren gestiegen. Die Erstellung von Duplikaten von Sicherungen und eine sichere Auslagerung werden im Kontext eines Disaster-Recovery-Konzeptes immer wichtiger. Im Folgenden werden Lösungen und Techniken für die Datensicherung dargestellt.

1.2 Sicherungsverfahren

Von marktüblicher Datensicherungs-Software werden mindestens die nachfolgend aufgeführten Sicherungsverfahren unterstützt:

- Bei einer Vollsicherung werden mit jeder Ausführung alle Daten im vollen Umfang gesichert.

- Bei einer inkrementellen Sicherung werden die hinzugefügten oder geänderten Daten seit der letzten inkrementellen Sicherung in die Sicherung aufgenommen, wie aus Abbildung 2 hervorgeht. In Verbindung mit einer initialen Vollsicherung kann so über mehrere Jobs und in der Regel auch Medien eine komplette Sicherung aufgebaut werden. Zu beachten ist, dass hierbei längere Recovery-Zeiten aufgrund der höheren Anzahl von Jobs und Medien, die zu diesem Zweck eingesetzt werden, einzuplanen sind.

- Bei einer differentiellen Sicherung werden die hinzugefügten oder geänderten Dateien seit der letzen Vollsicherung in die Sicherung aufgenommen, wie in Abbildung 3 dargestellt. In Verbindung mit einer Vollsicherung kann hier mittels zwei Jobs eine Komplettsicherung aufgebaut werden. Dies hat zur Folge, dass die differentiellen Sicherungen von Tag zu Tag größer und damit zeitlich länger werden. Für die Wiederherstellungszeit ist dies jedoch positiv, da hier nur zwei Jobs zu berücksichtigen sind.

1.2.1 Block Level Incremental Backups (BLIB)

Die Möglichkeit, inkrementelle Datensicherungen auf Blockebene durchzuführen, wird als Block Level Incremental Backup (BLIB) bezeichnet. Hierbei werden zunächst nur alle belegten Blöcke einer zu sichernden Partition übertragen. Bei jedem inkrementellen Sicherungsvorgang werden anschließend nur die Blöcke gesichert, die sich gegenüber dem letzten Vorgang geändert haben. Dies hat i.W. drei Vorteile:

1. Das Volumen der zu sichernden Daten kann auf Blockebene deutlich kleiner ausfallen als auf Dateiebene, da nur die veränderten Daten einer Datei (blockbasiert) gesichert werden.

2. Da die Datensicherung selbst stets aus einem blockbasierten Abbild der Festplatten-Partition besteht, kann dieses Abbild z.B. per iSCSI an einem neuen Server gemounted werden. Dies gilt auch für die inkrementellen Backups im Zusammenhang mit den vorangegangenen Teilsicherungen und der letzten Vollsicherung. Damit ist ein System in Desaster-Recovery-Fällen nahezu ohne Zeitverlust wieder lauffähig. Dieser Vorgang wird typischerweise „Instant Availability Mapping“ genannt.

3. Einzelne Dateien können aus dem blockbasierten Gesamtabbild restauriert werden, ohne die gesamte Datensicherung zunächst vollständig zurückspielen zu müssen. Nach dem Mounten des blockbasierten Abbilds wird hierfür auf die zu restaurierenden Daten dateibasiert zugegriffen.

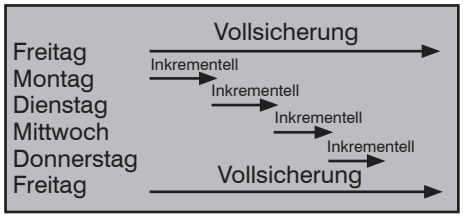


Abbildung 2: Inkrementelle Sicherung

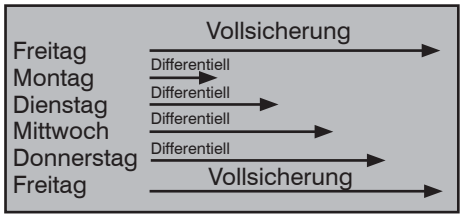


Abbildung 3: Differentielle Sicherung

Diese Vorteile sprechen für einen BLIB-Ansatz zur Datensicherung. Allerdings wird dieser nicht von jeder Backup-Software und für alle zu sichernden Umgebungen unterstützt, da er Snapshot-basiert arbeitet und zur Erzeugung von applikationskonsistenten Snapshots ein entsprechender Agent erforderlich ist.

1.2.2 Synthetische Backups

Anstelle in regelmäßigen Abständen den kompletten Datenbestand für eine aktuelle Vollsicherung über das Netzwerk zu transportieren, können neue Full-Backups auch auf Basis der letzten Vollsicherung und einer Reihe von inkrementellen Sicherungen neu berechnet werden. Allerdings kann der Ressourcenaufwand für eine solche Konsolidierung von Datensicherungen beträchtlich sein und bei unzureichender Auslegung der hierfür verantwortlichen Server-Hardware die Backup-Zeit um ein Vielfaches übersteigen. Außerdem zeigt die Praxis, dass es dennoch ratsam ist, in regelmäßigen Abständen eine neue Vollsicherung zu erzeugen. Damit wird verhindert, dass sich aufgrund von Übertragungs- oder Software-Fehlern Inkonsistenzen in die synthetischen Backups einschleichen, die erst im Recovery-Fall offensichtlich werden.

1.3 Virtuelle Tape Library (VTL)

Eine virtuelle Tape Library ist ein Festplattenspeichersystem, das sich mittels einer entsprechenden Software gegenüber den Servern als physische Bandbibliothek darstellt. Hierbei wird der Bandlaufwerks-Typ eines speziellen Herstellers so perfekt emuliert, dass aus Sicht der zu sichernden Server und der Backup-Software kein Unterschied zwischen einer physischen Bandbibliothek und der virtuellen Tape Library erkannt werden kann.

Storage: Backup von SAP-Umgebungen mit virtuellen Tape Libraries

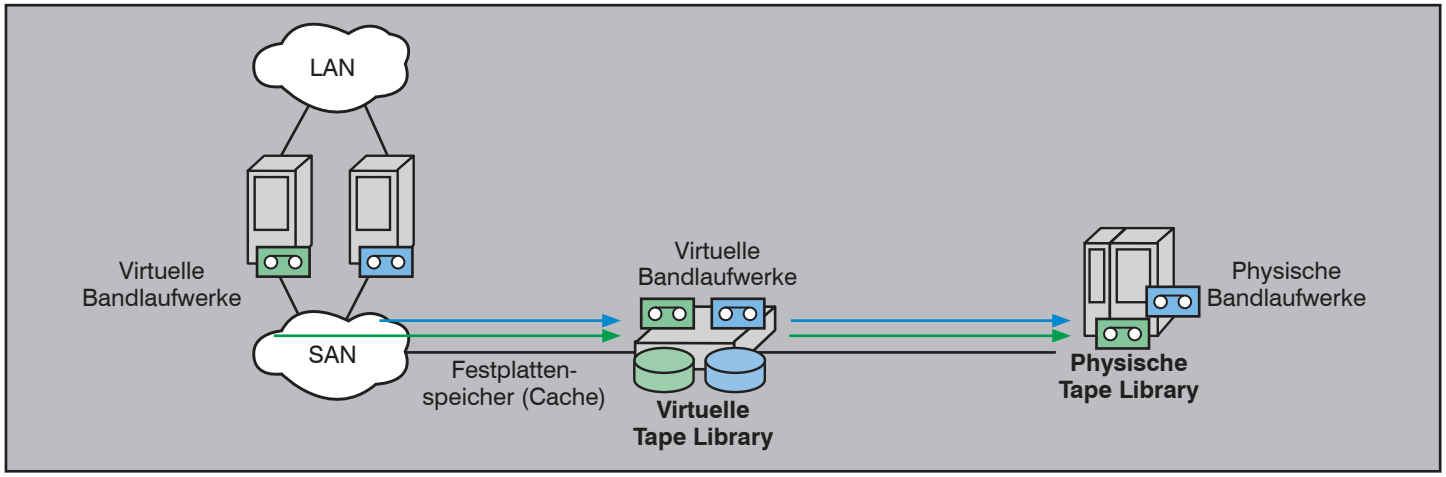


Abbildung 4: Anbindung Virtuelle Tape Library

Virtuelle Tape Libraries nutzen den Geschwindigkeitsvorteil durch die Sicherung auf Festplatten im ersten Schritt des gesamten Datensicherungsprozesses aus. Dieser Geschwindigkeitsvorteil besteht nicht nur in den höheren Schreib- und Leseraten auf das virtuelle Band. Insbesondere das Verteilen von Backup-Datenströmen und der anschließende Zugriff auf verteilt vorliegende Datensicherungen werden durch eine VTL massiv beschleunigt, da sämtliche Start- / Stoppvorgänge und das Spulen eines physischen Bandes entfallen.

Die VTLs können über das SAN angebunden werden und den Serversystemen über dieses SAN virtuelle Bandlaufwerke zur Verfügung stellen. Diese Laufwerke emulieren unterschiedliche Bandtechnologien. Der Zugriff erfolgt durch das Serversystem wie auf ein physikalisches Bandlaufwerk. Tatsächlich jedoch beinhaltet die VTL keine Bandlaufwerke, sondern über RAID-Technologie abgesicherte Festplatten in einem Verbund. Eine Software stellt jeweils Teile dieses Festplattenverbundes für die Serversysteme als Bandlaufwerk dar. Die Sicherung erfolgt somit tatsächlich auf Festplatten mit dem damit verbundenen Performancevorteil gegenüber physikalischen Bandlaufwerken. Der Start-Stopp-Betrieb entfällt bei dieser Technik, ebenso wie die mechanischen Beanspruchungen von Bändern. Mittels dieser Technik kann jedem Serversystem, das über das SAN angebunden ist, von zentraler Stelle aus ein Bandlaufwerk zur Verfügung gestellt werden.

Bei Einsatz von VTL wird die gleichzeitige Durchführung von Datensicherungsjobs von mehreren Serversystemen unterstützt. Unterschiedliche Bandtechnologien für die Jobs können emuliert werden.

Optional können entweder durch einen Algorithmus der VTL oder mittels einer Regel der Backup-Software die auf den Festplatten vorgehaltenen Daten auf tatsächliche physikalische Bandlaufwerke ausgelagert werden, die entweder direkt an die VTL oder über das SAN angebunden sind. Diese physikalischen Tape Libraries besitzen wiederum mehrere physikalische Bandlaufwerke und ausreichend Platz für die Aufnahme von Bandmedien. Die auf dem Markt zu diesem Zweck allgemein eingesetzten Tape Libraries sind in Bezug auf die Anzahl der Laufwerke und die Anzahl der Medienslots äußerst skalierbar (siehe auch Abbildung 4).

Mittels VTL ist nicht nur eine schnellere Sicherung realisierbar, sondern auch eine schnellere Wiederherstellung, solange die Daten noch auf den Festplatten innerhalb der virtuellen Tape Libraries vorgehalten werden. Ansonsten werden die Daten vom Bandmedium in die virtuelle Tape Library zurückgeholt und mittels der Emulation auf das Serversystem zurückgespielt.

Die Daten, die auf einem zentralen Speichersystem abgelegt sind, können über die Serversysteme und das SAN ggf. unter Einsatz von separaten HBAs für die Datensicherung auf die Festplatten der virtuellen Library und von dort auf die physikalische Tape-Library gesichert werden.

Zusammengefasst bestehen die Vorteile einer VTL in den folgenden Aspekten:

- Sie kann das Backup beschleunigen weil die Daten nicht auf Band, sondern auf ein schnelles Disk-System geschrieben werden.
- Besonders bei der Wiederherstellung von vielen kleinen Dateien bietet eine VTL einen Geschwindigkeitsvorteil gegenüber Bandbibliotheken.
- Eine VTL bietet erhebliche Geschwindigkeitsvorteile bei auf mehrere Laufwerke gestreuten Lesevorgängen.
- Der Datenfluss unterliegt nicht den Kontinuitätsanforderungen eines physischen Bandlaufwerks.
- Physische Bandmedien können eingespart werden oder werden weniger beansprucht.
- Backups können unabhängig von den Zeitfenstern für physische Laufwerke geschrieben werden.
- VTLs können nahtlos in die vorhandene Infrastruktur integriert werden. Da sie eine Bandbibliothek emulieren, sind keine Änderungen an der vorhandenen Backup-Struktur erforderlich. Die Server verwenden wie bisher ihren Backup-Client.
- Zugewinn an Flexibilität: zusätzliche (virtuelle) Laufwerke können „auf Knopfdruck“ als Backup-Ziele definiert werden.

Dem gegenüber stehen die folgenden Nachteile einer VTL:

- Zusätzliche Investitionskosten
- Zusätzlicher Betriebsaufwand
- Erhöhte Komplexität in der SAN Infrastruktur
- Mangelnde Transparenz der VTL-Funktionalitäten gegenüber der Backup-Software
  - Beispiel: Datensicherungen, die von der VTL dupliziert werden, sind der Backup-Software nicht bekannt.

- Zu hohe Transparenz der VTL gegenüber der Backup-Software
  - Die Backup-Software kann zwischen virtuellen und physischen Medien nicht unterscheiden. Besteht der Bedarf zur Auslagerung des Backups auf ein physisches Band, muss ein solches Laufwerk besonders kenntlich gemacht werden.
- Einfachere Transportierbarkeit von physischen Bändern, z.B. zur Archivierung entfällt
- Geringere Schutzmöglichkeiten der Daten im Vergleich zu ausgelagerten Bändern

1.4 Aufbau einer SAP-Umgebung

In einer SAP-Umgebung sind in der Regel die Applikations-Server im Sinne einer Multi-Tiering-Architektur von den Datenbanken getrennt. D.h., dass ein Server die SAP-Applikation beinhaltet, während ein anderer Server die von der Applikation genutzte Datenbank betreibt.

Da SAP zu den unternehmenskritischen Diensten gehört, wird dieser Dienst aus Verfügbarkeitsgründen in der Regel über zwei Rechenzentren verteilt. Die geclusterten SAP-Applikations-Server verwenden die "Enqueue-Replication" zur zentralen Verwaltung von logischen Sperren. Auf der Oracle-Seite sorgt der Real Application Cluster (RAC) für die synchrone Replikation der Daten. Abbildung 5 verdeutlicht diesen Aufbau.

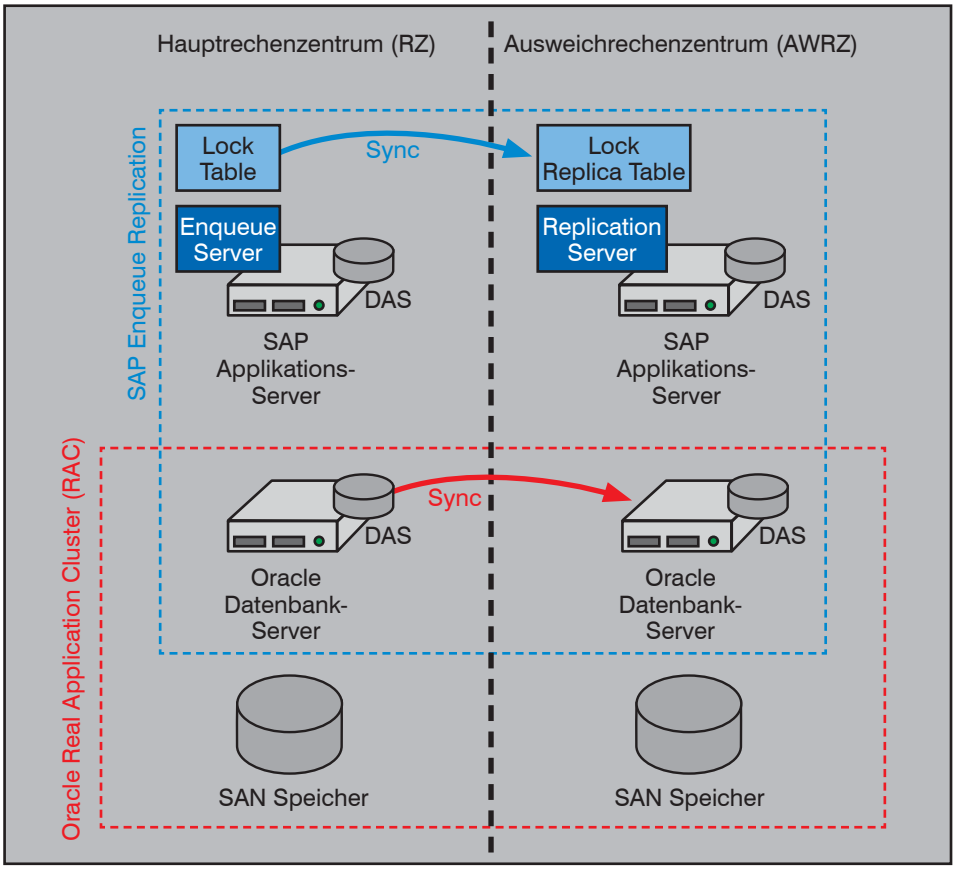


Abbildung 5: Redundante SAP-Umgebungen durch Oracle Real Application Cluster (RAC) und SAP Enqueue Replication

1.5 Datensicherungen im SAP-Umfeld

1.5.1 Backup-Software

Im SAP-Umfeld besteht häufig die Anforderung, Datensicherung direkt aus der eigenen Oberfläche heraus auslösen zu können. Dies wird über die Einbettung von entsprechenden Skripts in Schaltflächen oder Menüeinträge des SAP-GUI realisiert. Ein solches Skript generiert eine Kommandozeile für die SAP Backup & Recovery Tools (BRTOOLS). Die BRTOOLS wiederum erzeugen Kommandos für den Oracle Recovery Manager (RMAN). RMAN ist in der Lage, per „Block Change Tracking“ nur die veränderten Blöcke der Datenbank lesen zu müssen. Dies entspricht dem weiter oben beschriebenen Block Level Incremental Ansatz.

Der Backup-Job wird letztlich an die Dritthersteller Backup-Software übertragen und von dort auf die Ziel-Laufwerke geschrieben. Die Dritthersteller-Software übernimmt dabei die Steuerung und Verwaltung der Bandlaufwerke und –roboter.

Abbildung 6 zeigt dieses Ineinandergreifen der unterschiedlichen Backup-Produkte im SAP-Umfeld.

Problematisch wird diese Konstellation, wenn insbesondere RMAN und die Dritthersteller-Software nur begrenzt miteinander harmonieren. Ist z.B. nicht klar geregelt, wer die „führende Rolle“ übernimmt, kann es zu Inkonsistenzen in den jeweiligen Backup-Katalogen kommen oder es muss mit entsprechenden Aufwänden für Konsistenz gesorgt werden.

Um veraltete Backups beispielsweise zu löschen, muss in der Dritthersteller-Software eine „Retention Period“ von „Unendlich“ eingetragen werden. Unter RMAN bzw. über die BRTOOLS wird dann die Lebenszeit der Backups definiert. Durch einen täglichen „Delete Obsolete“-Lauf von RMAN werden die überflüssigen Backups schließlich gelöscht.

1.5.2 Backup von Oracle-Datenbanken

SAP setzt als Datenbanksystem Produkte des Herstellers Oracle ein. Insofern sind für Datensicherungen im SAP-Umfeld die Mechanismen für das Backup von Oracle Datenbanken zu betrachten.

Der gültige Ausgangszustand einer Oracle Datenbank enthält alle Einträge, Relationen und Schlüssel in konsistenter Form. Alle Änderungen und Ergänzungen, die im

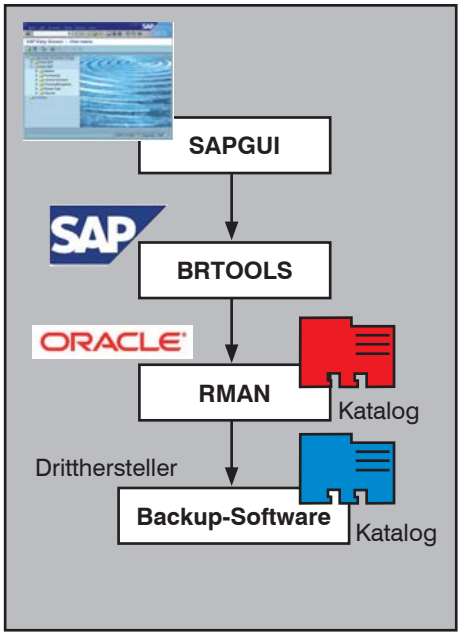


Abbildung 6: Ineinandergreifen unterschiedlicher Backup-Software im SAP-Umfeld

Laufe der Zeit an der Datenbank durchgeführt werden, werden in so genannte „Online Redo Logs“ gespeichert. Wird ein Fehler oder eine Inkonsistenz in der Datenbank entdeckt, kann sie mit Hilfe der Redo-Logs schrittweise wieder rekonstruiert werden. Um den Speicherplatzbedarf zu reduzieren, werden die Redo-Logs in zyklischer Abfolge überschrieben. Dabei wird in der Regel eine zeitliche Abfolge definiert.

Wird beispielsweise alle 6 Stunden ein neues Online Redo Log geschrieben und nach 4 Online Redo Logs das erste wieder überschrieben, steht stets Restaurierungsmaterial für die letzten 24 Stunden zur Verfügung. Dabei macht jedes Online Redo Log im Schnitt ein Viertel des gesamten Änderungsvolumens dieses Zeitraums aus.

Die Datensicherung von Oracle-Datenbanken betrifft insofern 2 unterschiedliche Aspekte. Zum einen ist dies das Backup der gesamten Datenbank, das zur Reduktion der zu übertragenenden Gesamtmenge blockweise inkrementell oder differentiell erfolgen kann. Dabei lautet die Bezeichnung für differentielle Backups unter RMAN „incremental level 0“.

Zum Anderen sind es die Online Redo Logs, die archiviert werden sollten, um möglichst schnell fehlerhafte Änderungen korrigieren zu können. Das Sichern der Online Redo Logs wird bei SAP über den ARCHIVELOG-Modus im SAPDBA-Menü eingestellt.

Abbildung 7 veranschaulicht diese Vorgehensweise.

Durch diese kombinierten Datensicherungsverfahren - Vollsicherung der Datenbank einerseits, Archivierung der Redo Logs andererseits - können folgende Aspekte in der Backup-Strategie berücksichtigt werden:

- Häufiges Archivieren der - vom Datenvolumen her relativ kleinen - Redo Logs, um beliebige Zwischenstände der an der Datenbank vorgenommenen Änderungsvorgänge rekonstruieren zu können.
- Selteneres Sichern der vollständigen Datenbank - gegegbenenfalls kombiniert mit inkrementellen oder differentiellen Zwischenschritten.

2. Synchrone Backups an unterschiedlichen Standorten

In der Praxis besteht häufig die Anforderung, Datensicherungen nicht nur an einem Standort vorzuhalten, sondern auch auf einen zweiten Standort zu schreiben.

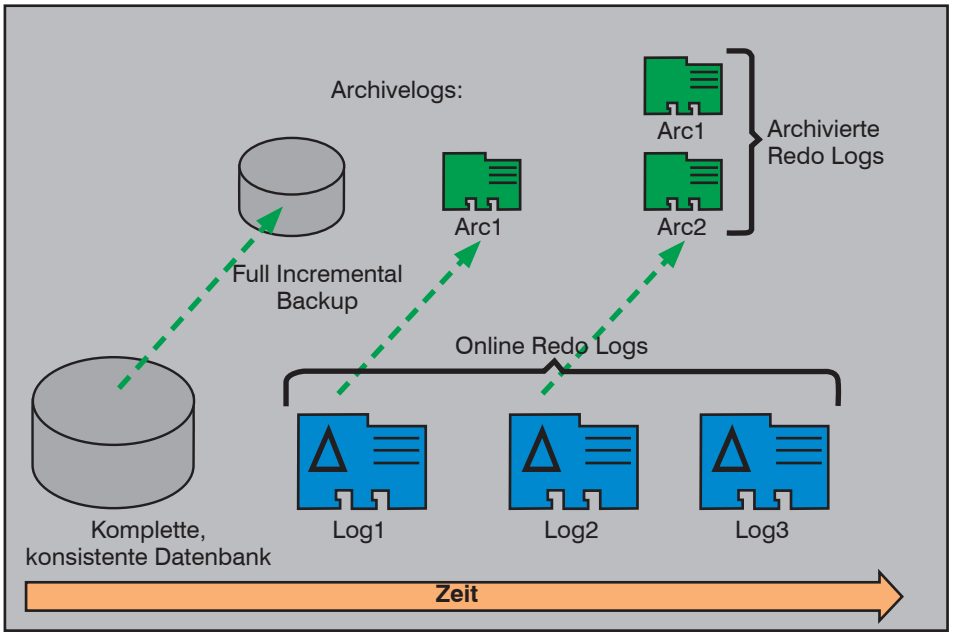


Abbildung 7: Datensicherung von Oracle-Datenbanken

Dabei gebietet es ein Desaster Recovery Konzept, dass diese Datensicherungen möglichst zeitgleich und möglichst identisch an beiden Standorten vorliegen. Im Folgenden werden mögliche Lösungsvarianten für das Verteilen von Datensicherungen auf verschiedene Backup-Ziele aufgezeigt und bewertet.

2.1 Variante 1: Parallele Sicherungsjobs

Die einfachste Methode, eine Datensicherung an unterschiedliche Backup-Ziele zu übertragen, besteht darin, auf dem zu sichernden Server zwei parallele Backup-Jobs zu starten. Diese lesen allerdings die Daten unabhängig voneinander, so dass es zu doppelten Zugriffen auf die - gegegbenenfalls im SAN platzierten - Plattenspeicher des Servers kommt. Außerdem verbrauchen die simultanen Backup-Jobs 2x die Systemressourcen auf dem zu sichernden Server. Des Weiteren werden die Backup-Daten 2x über die Server-Schnittstelle über das SAN in Richtung der Backup-Ziele geschrieben. Da die Backup-Jobs letztlich unabhängig voneinander sind, werden sie auch separat inventarisiert und besitzen unterschiedliche Zeitstempel.

Dem gegenüber besteht ein Vorteil in der Einfachheit dieser Lösung: Bei manchen am Markt befindlichen Backup-Produkten ist dies außerdem die einzige Möglichkeit, Datensicherungen auf zwei Backup-Ziele zu verteilen.

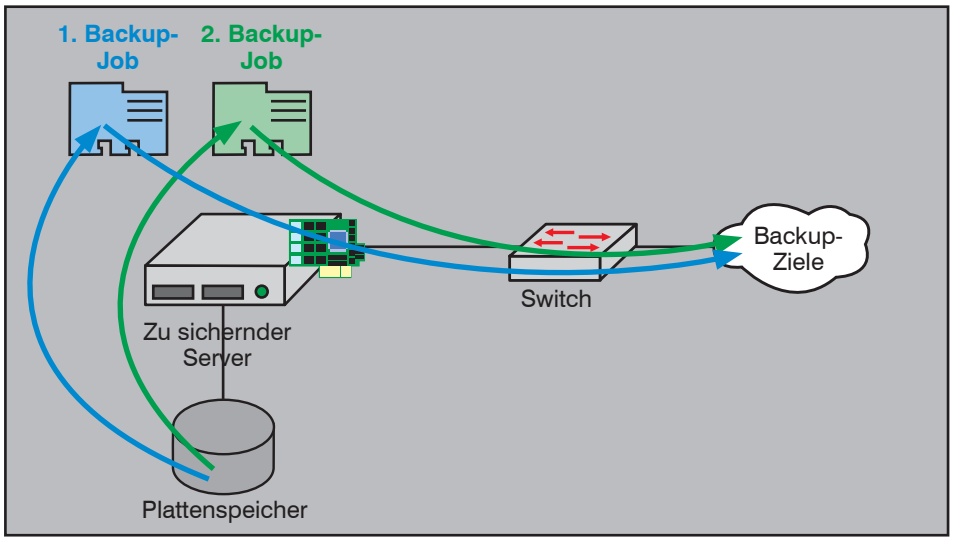


Abbildung 8: Replikation von Datensicherungen durch parallele Backup-Jobs

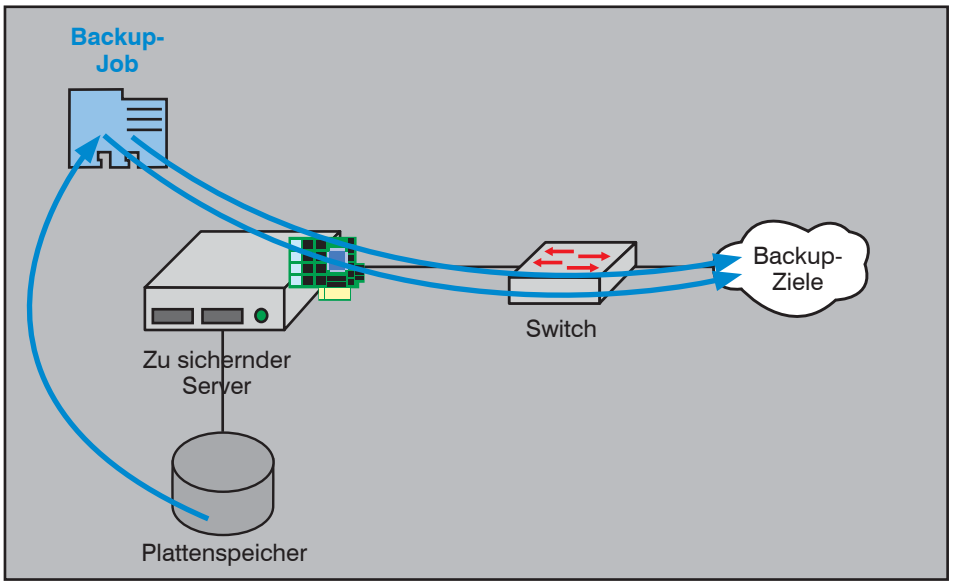


Abbildung 9: Replikation von Datensicherungen durch Adressierung mehrerer Backup-Ziele

Abbildung 8 veranschaulicht diesen Ansatz.

2.2 Variante 2: Adressierung mehrerer Backup-Ziele

Einige Backup-Produkte gestatten es, mehrere Backup-Ziele von ein und demselben Backup-Job aus zu adressieren. Dies führt zu dem Vorteil, dass die zu sichernden Daten zur 1x von Platte gelesen werden müssen und nur ein Backup-Job das zu sichernde System belastet. Da die Backups den gleichen Ursprung haben, besitzen sie außerdem den gleichen Zeitstempel.

In Richtung der Backup-Ziele muss die Datensicherung jedoch weiterhin mehrfach transportiert werden, was zu einer entsprechenden Belastung der Server-Schnittstellen und des Speichernetzes in dieser Richtung führt. Der Backup-Job wird erst dann abgeschlossen, wenn auch das langsamere der beiden Backup-Ziele fertig ist (typischerweise das an einem Remote-Standort).

Abbildung 9 veranschaulicht diesen Ansatz.

2.3 Variante 3: Verteilung des Datenstroms

Soll der zu sichernde Server noch weiter entlastet werden von den zu verteilenden Datensicherungen, kann der Medien-Server – der die Backup-Ziele anbindet – zur Verteilung des Datenstroms genutzt werden. Dieser Ansatz ist mit dem im IP-Netz bekannten Multicasting vergleichbar. Ein einzelner Datenstrom wird von einer nachgelagerten Komponente in Richtung mehrerer Ziele verteilt.

Der Medien-Server kann einerseits im IP-Netz stehen, was allerdings eine LAN-seitige Datensicherung zur Basis hätte. Steht hierfür kein vom Produktivnetz getrenntes Backup-Netz zur Verfügung, ist dieser Ansatz unbedingt zu vermeiden.

Auch in einem Fibre Channel SAN kann der Medien-Server zur Verteilung eines Backup-Stroms herangezogen werden. In diesem Fall kommen so genannte „Fibre Channel Transport Services“ auf dem Medien-Server zum Einsatz, die den Datenstrom aufsplitten und auf mehrere Ziele verteilen. Zu beachten ist in diesem Szenario, ob die Backup-Software auf ihrem Medien-Server diese Dienste anbietet und ob das Betriebssystem auf dem Medien-Server diese unterstützt.

Abbildung 10 veranschaulicht diesen Ansatz.

2.4 Verteilung der Datensicherungen über VTLs

Eine VTL kann nicht nur eingesetzt werden, um den Datensicherungsvorgang zu beschleunigen. Sie kann auch ein Hilfsmittel zur Verteilung der Datensicherungen auf mehrere Backup-Ziele darstellen. Dabei stehen einerseits Bordmittel der VTL zur Verfügung, die ein Backup auf eine zweite VTL replizieren können und dabei gegebenenfalls von VTL-spezifischen Deduplizierungsmechanismen profitieren können. Andererseits ist eine solche über die VTLs ausgeführte Kopie der Datensicherung für die Backup-Software intransparent, so dass sie nicht in ihrer Katalogdatei geführt werden kann und für einen Restore-Vorgang manuell eingebunden werden müsste.

Insofern ist ein Replizierungsverfahren vorzuziehen, das als Speicherplattform zwei VTLs nutzt, jedoch über die zentrale Datensicherungs-Software gesteuert wird. Über so genannte „Backup-Policies“ kann bei einigen Backup-Produkten definiert werden, wie mit einer Datensicherung weiter verfahren werden soll. So kann z.B. eine nachgelagerte Replikation einer Datensicherung auf einen oder mehrere andere Datenträger vorgenommen werden. Dabei behält die Backup-Datei nicht nur den gleichen Inhalt, sondern auch den gleichen Zeitstempel. Da auch die replizierten Backup-Dateien in der Katalogdatei der Backup-Software geführt werden, stehen sie für eine unmittelbare Restaurierung zur Verfügung.

Abbildung 11 veranschaulicht diesen Ansatz.

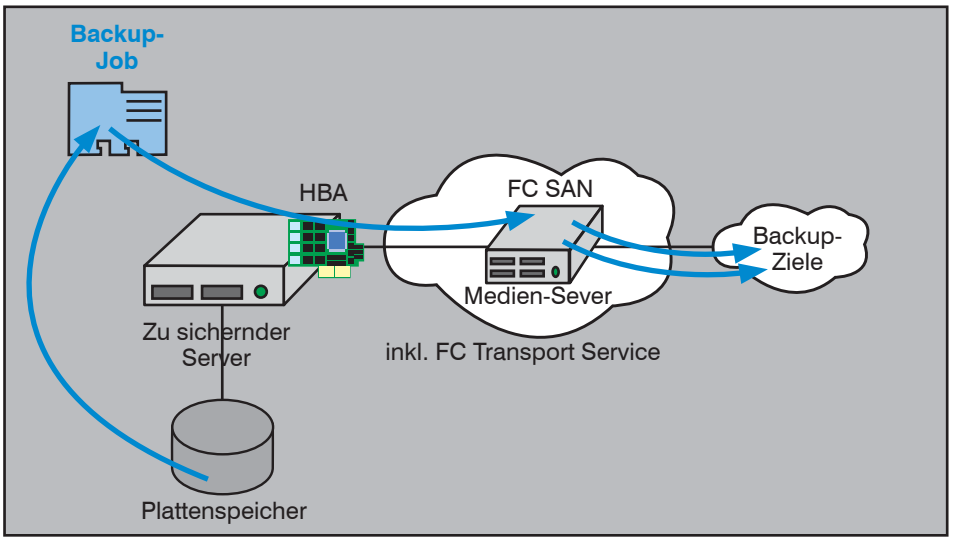


Abbildung 10: Replikation von Datensicherungen durch Nutzung eines Fibre Channel Transport Services

3. Backup-Szenarien mittels VTL

Im Folgenden werden drei aus den in Kapitel 2 dargestellten Varianten abgeleitete Szenarien einer Standort-übergreifenden Replizierung von Backups mittels VTLs diskutiert.

3.1 Szenario 1: Sequentiell auf VTL

In diesem ersten Szenario werden die Daten von dem zu sichernden Server zunächst auf die VTL des eigenen Standorts geschrieben. In einem nachgelagerten Prozess repliziert die Backup-Software (nicht die VTL) diese Datensicherung in das Ausweichrechenzentrum. In beiden Rechenzentren können die Datensicherungen optional noch auf physische Bänder ausgelagert werden, wenn dies z.B. zur Archivierung erforderlich ist. Dieses Szenario basiert auf der in Abschnitt 2.4 dargestellten Variante.

Anforderungen

- Die Backup-Software muss in der Lage sein, die Datensicherungen über die VTLs zu duplizieren, um diese Datensicherungen für den Wiederherstellungsfall zentral verwalten können.

Vorteile

- Nach Abschluss des Sicherungsvorgangs liegen an beiden RZ-Standorten identische Datensicherungen mit gleichem Zeitstempel vor.
- Durch die Nutzung einer VTL als Ziel für die zu sichernden Server werden die Leistungsanforderungen an das Netzwerk auf dieser Strecke entschärft.
- Das für die Durchführung der Datensicherung erforderliche Zeitfenster hängt von der Geschwindigkeit der lokalen VTL ab und liegt in der Regel unter dem eines physischen Bandlaufwerks.

Nachteile

- Da die Datensicherungen in einem nachgelagerten Prozess über die VTLs auf den Remote-Standort dupliziert werden, liegen die zwei identischen Datensicherungen nicht simultan an den beiden Standorten vor.

Abbildung 12 veranschaulicht dieses Szenario.

3.2 Szenario 2: Parallel auf VTL

Szenario 2 basiert auf einer Datensicherungs-Software, die in der Lage ist, innerhalb eines Backup-Jobs zwei verschiedene Backup Ziele gleichzeitig zu adressieren. Einerseits ist dies die VTL des eigenen Rechenzentrums, andererseits wird die VTL des Ausweichrechen-

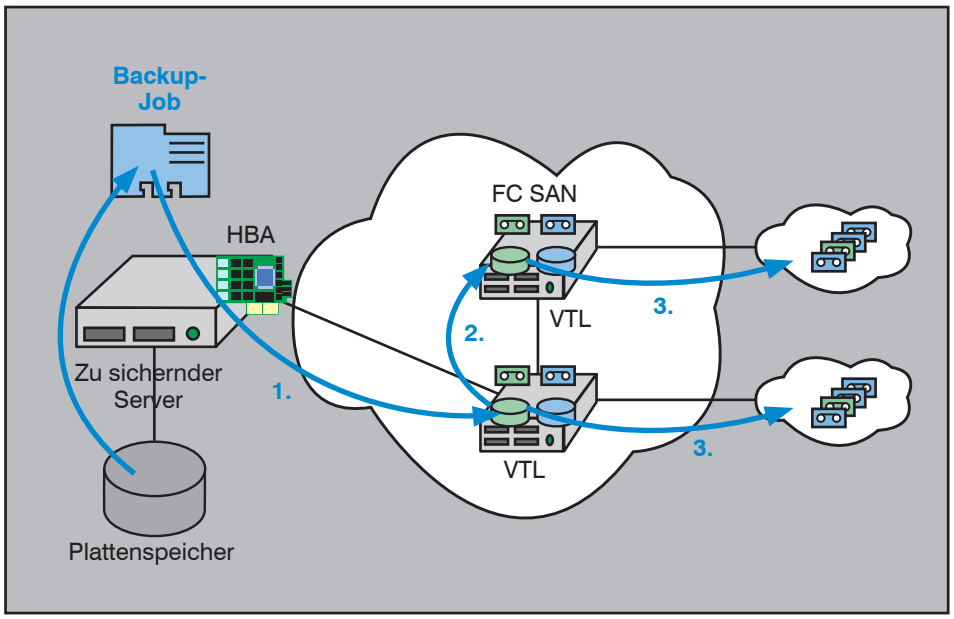


Abbildung 11: Replizierung von Datensicherungen über VTLs

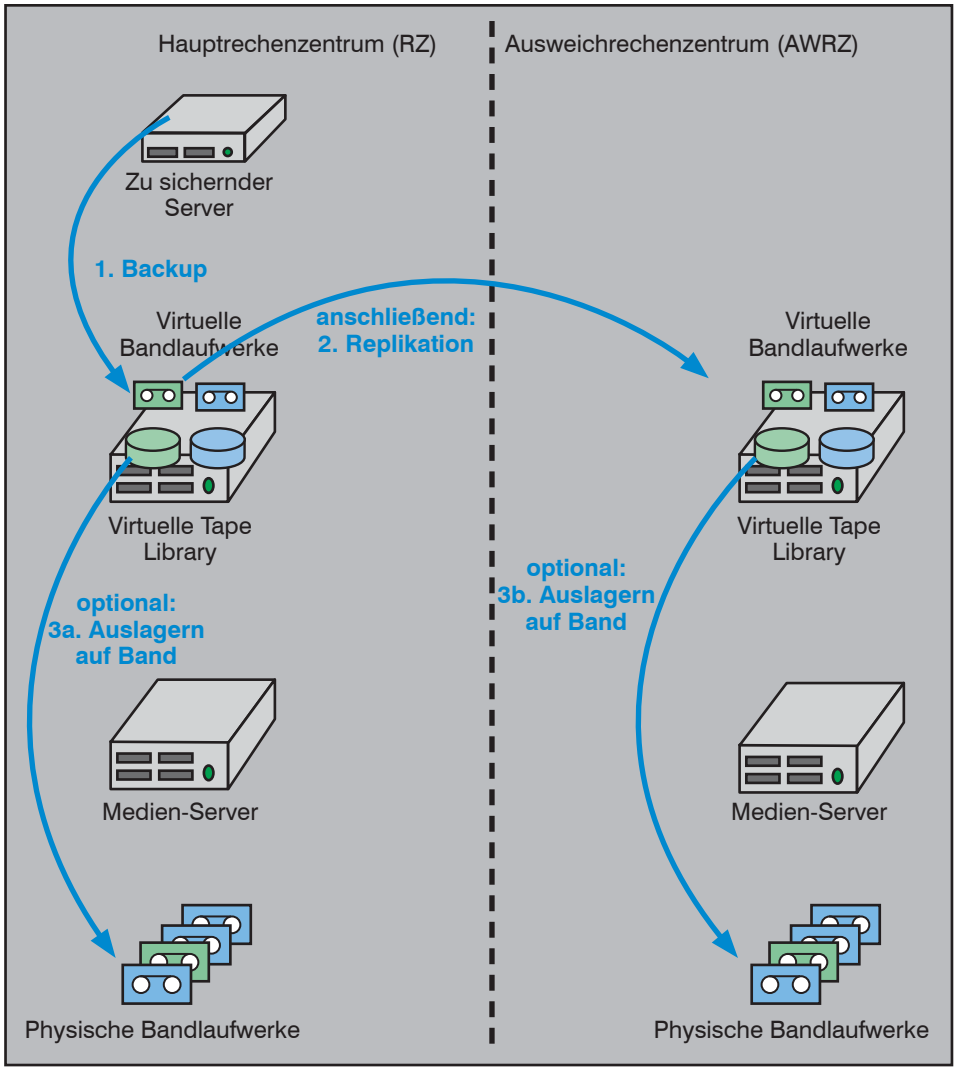


Abbildung 12: Szenario 1, sequentielle Datensicherung mittels VTLs

zentrums adressiert. Auch hier können bei Bedarf die virtuellen Bänder in einem nachgelagerten Prozess über einen Medien-Server auf physische Bandlaufwerke am gleichen Standort ausgelagert werden. Dieses Szenario basiert auf der in Abschnitt 2.2 dargestellten Variante.

Anforderungen

- Die Netzverbindung zwischen den RZ-Standorten muss eine der Server- und Laufwerksgeschwindigkeit angepasste Datenübertragungsrate gewährleisten.
- Die Netzwerkschnittstellen der Server müssen für die simultanen Datensicherungen die erforderlichen Netzwerk-IOs sowie eine der Laufwerksgeschwindigkeit angepasste Datenübertragungsrate gewährleisten.

Vorteile

- Durch die Nutzung einer VTL als Ziel für die zu sichernden Server besteht keine Anforderung hinsichtlich einer gleichmäßigen Datenübertragungsrate an das Netzwerk auf dieser Strecke.
- Da die simultanen Datensicherungen ihren Ursprung im gleichen Backup-Job haben, besitzen sie den gleichen Zeitstempel.

Nachteile

- Durch die simultane Durchführung der Datensicherungen werden die Anforderungen an Netzwerk-IOs und Datenübertragungsrate auf Seiten der Server-Schnittstelle verdoppelt.
- Die Größe des erforderlichen Backup-Fensters hängt von der Dauer des langsamsten der beiden simultanen Datensicherungen ab. Dies wird aufgrund der Weitverkehrsübertragung in der Regel die Sicherung in den Remote-Standort sein.

Abbildung 13 veranschaulicht dieses Szenario.

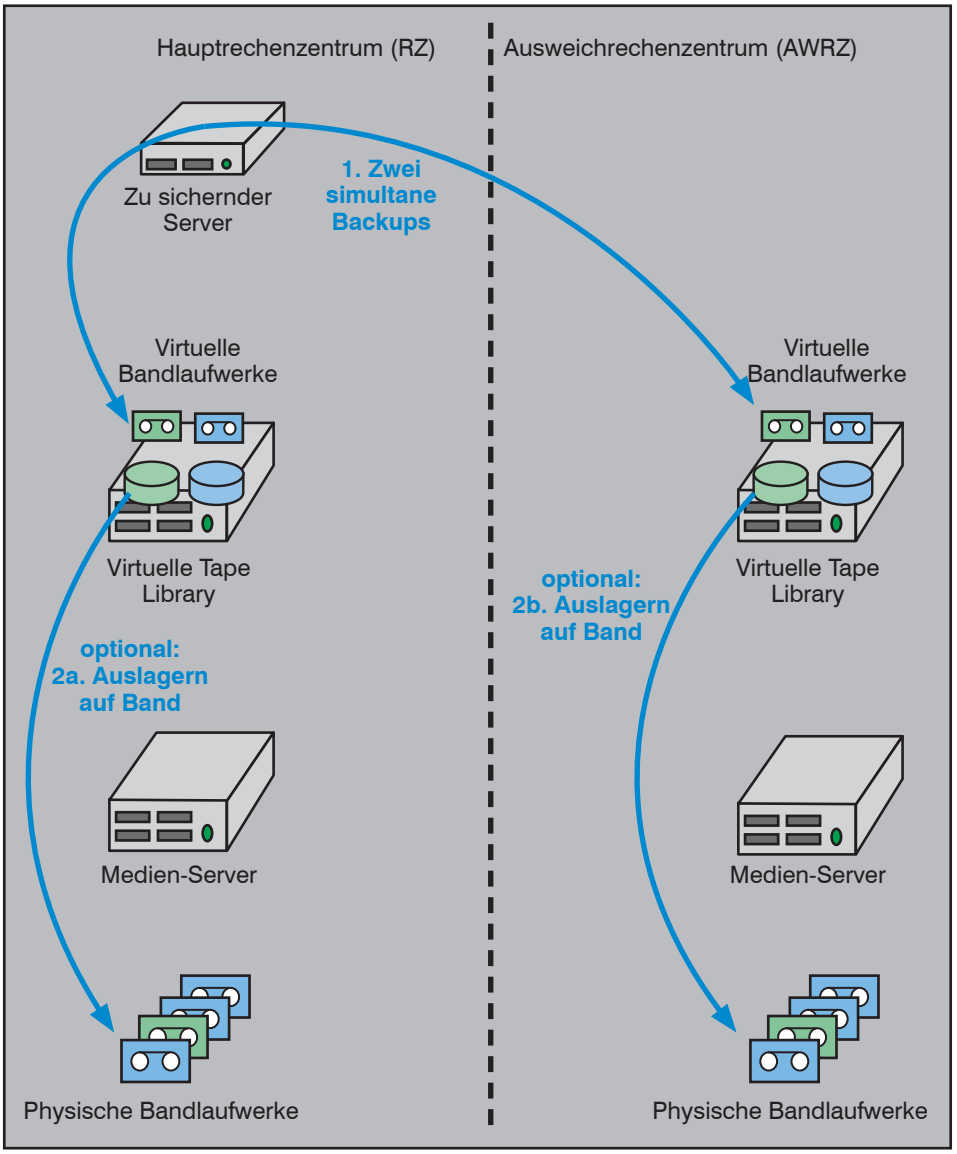


Abbildung 13: Szenario 2, parallele Datensicherung mittels VTLs

3.3 Szenario 3: Kombination aus Szenario 1 und 2

Szenario 3 kombiniert die Vorteile der Szenarien 1 und 2, um insbesondere im SAP-Umfeld den Charakter von Oracle-Datenbanken für eine möglichst effiziente Form der Datensicherung zu nutzen. Zunächst wird die vollständige Datenbank gemäß Variante 1 in regelmäßigen Abständen als Full-Backup auf die lokale VTL gesichert und von dort in einem nachgelagerten Prozess in das Ausweichrechenzentrum repliziert.

Dem gegenüber werden die Archive-Logs gemäß Variante 2 auf die beiden VTLs simultan geschrieben. Da die Archive-Logs von der Größe her deutlich kleiner sind als die Datenbank, ist dieses Verfahren sehr effizient. Gleichzeitig haben die Archive-Logs eine sehr hohe Bedeutung, was die Verfügbarkeit der Daten angeht, da mit ihrer Hilfe sämtliche Zwischenstände seit der letzten Datenbanksicherung rekonstruiert werden können.

Anforderungen

- Die zu sichernden Daten müssen wie im Fall von SAP-/Oracle-Datenbanken unterscheidbar sein in „vollständige Datenbank“ und „Archive-Logs“, um unterschiedliche Backup-Strategien definieren zu können.
- Alternativ müsste die Backup-Software unterschiedliche Varianten für „Full-Backups“ und „Incremental Backups“ unterstützen.

Vorteile

- Für die großen Datenvolumen der Full-Backups wird die asynchrone Replikation eingesetzt.
- Für die kleinen Datenvolumen der Archive-Logs wird die synchrone Replikation eingesetzt.

Nachteile

- Die Backup-Strategie wird komplexer, da unterschiedliche Varianten in Abhängigkeit vom Datensicherungstyp verwendet werden.

Abbildung 14 veranschaulicht dieses Szenario.

4. Fazit

Da neben den allgemeinen Daten auch das Wachstum unternehmenskritischer Daten exponentiell zunimmt, kommt dem Datensicherungskonzept im Rahmen eines Disaster Recovery Plans eine sehr hohe Bedeutung zu. Immer mehr Unternehmen setzen auf SAP in Kombination mit Oracle Datenbanken als Kern für ihre „Business Critical Applications“.

Insofern ist es von enormer Bedeutung, frühzeitig - idealerweise schon in der Planungsphase - die richtige Kombination aus organisatorischen sowie technischen Maßnahmen zu wählen, um im Rahmen einer Backup-Strategie die hohen Verfügbarkeitsanforderungen an diese Daten zu gewährleisten.

Hier bietet die Kombination einer zeitlich nachgelagerten Verteilung der Vollsicherung einer Datenbank mit der parallelen Sicherung der Archive-Logs mit den Veränderungen an dieser Datenbank ein hohes Effizienzpotential. Ist gleichzeitig das Ziel der Datensicherungen eine virtuelle Tape Library, wird jede einzelne Datensicherung nicht nur beschleunigt, sondern insbesondere flexibilisiert.

Da für die Datensicherungen letztlich auf Bordmittel von SAP und Oracle in Form der BRTOOLS und RMAN zurückgegriffen wird (gesteuert von einer Drittherstellerlier-Software), sollten die folgenden Ansätze verfolgt werden:

- Regelmäßige Vollsicherungen der Datenbank, optimiert durch „Block Change Tracking“
- Regelmäßige Sicherung der Änderungen in Form der Archive-Logs

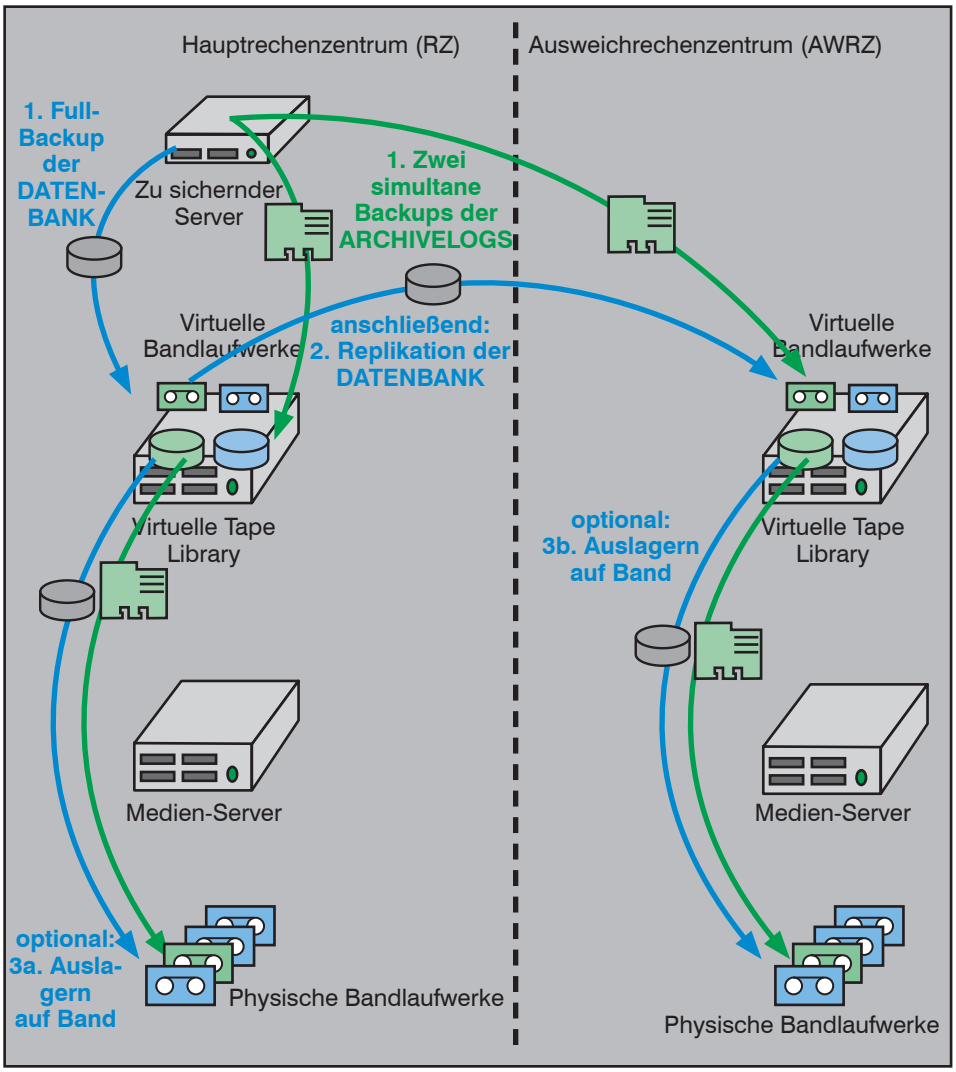


Abbildung 14: Szenario 3, Full-Backup per sequentieller Datensicherung, ARCHIVELOGS per paralleler Datensicherung

Die Häufigkeiten für diese beiden Backup-Aspekte hängen letztlich einerseits vom Datenvolumen, andererseits vom zur Verfügung stehenden Backup-Zeitfenster sowie den Anforderungen der jeweiligen Fachbereiche ab.

Kongress

ComConsult Storage-Forum 2011
13.07. - 15.07.11 in Bonn

Zentraler, im Netzwerk zugreifbarer Speicher steht im Mittelpunkt aller zukünftigen IT-Architekturen. Die technologische Spannweite ist riesig, permanent kommen neue Entwicklungen und Produkte hinzu. Das ComConsult Storage-Forum 2011 analysiert die aktuellen Entwicklungen im Speichermarkt, vergleicht Alternativen und zeigt auf, wo der Weg hingeht.

Moderatoren: Dipl.-Inform. Matthias Egerland, Dr. Franz-Joachim Kauffels
Preis: € 1.990,-- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Neuer Kongress

ComConsult Storage-Forum 2011 13.07. - 15.07.11 in Bonn

Die ComConsult Akademie veranstaltet vom 13.07. - 15.07.11 ihren neuen Kongress „ComConsult Storage-Forum 2011“ in Bonn. Das Forum war ursprünglich im März geplant und wurde auf den Juli-Termin verschoben.

Zentraler, im Netzwerk zugreifbarer Speicher steht im Mittelpunkt aller zukünftigen IT-Architekturen. Die technologische Spannweite ist riesig, permanent kommen neue Entwicklungen und Produkte hinzu. Das ComConsult Storage-Forum 2011 analysiert die aktuellen Entwicklungen im Speichermarkt, vergleicht Alternativen und zeigt auf, wo der Weg hingeht.

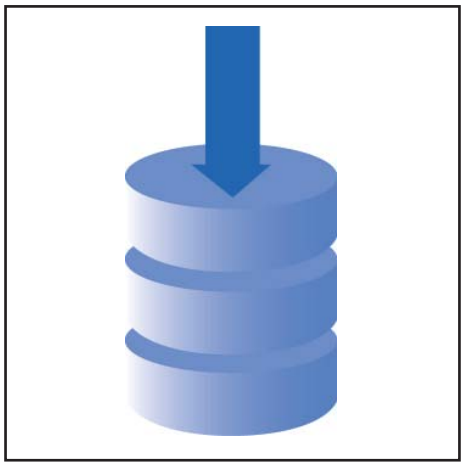
Alle wesentlichen IT-Architekturen werden sich in Zukunft auf zentrale, im Netzwerk zugreifbare Speicher-Lösungen abstützen. Die Bandbreite technologischer Entwicklungen in diesem Bereich, angefangen von neuen IT-Architekturen und hin zu neuen Speicher-Lösungen ist gewaltig. Kombiniert man das mit einem immer weiter wachsenden Datenbestand, dann ergibt dies ein explosives Gemisch:

- Immer mehr Daten müssen beherrscht werden.
- Immer mehr Applikationen hängen von zentralen Speicher-Systemen ab.
- Basis-Funktionen wie Backup/Restore werden zu einem echten Problem.

Die Gründe für den weiter wachsenden Bedarf sind vielfältig:

- Mehr Rechenleistung gestattet die Verarbeitung von immer mehr Daten.
- Auch neue Applikationen und Applikationstypen (Video, Web 2.0/3.0) erzeugen erhebliche Datenmengen.
- Zunehmende Automatisierung (RFID) stellt immer mehr Daten bereit.
- Eine veränderte Risiko- und Rechtssituation erfordert mehr Detail-Daten für eine verbesserte Prognose-Sicherheit.
- Neue Formen der Vermarktung erzeugen neue Daten (Internet).
- Verändertes Kundenverhalten schafft neue Daten zu Kunden-Bedürfnissen und Erwartungen.
- Virtualisierung und Konsolidierung von Servern zentralisiert Daten.

Dies erfolgt parallel zu wesentlichen Änderungen in IT-Technologien und Architek-



turen, die neue Anforderungen an die Leistung und Qualität von Speicher erzeugen:

- Virtualisierung geht immer mehr weg von der simplen Konsolidierung und hin zur Schaffung neuer Architekturen für Webanwendungen.
- Neue Virtualisierungsverfahen wie vMotion, HA, Desaster Recovery generieren erhebliche Anforderungen an Speicher-Performance.
- Traditionell wurde die Leistung von SAN-Systemen in I/O-Transaktionen pro Se--kunde gemessen, mit den neuen Architekturen kommen erhebliche Anforderungen an Bandbreite hinzu.
- Mit Desktop-Virtualisierung entsteht ein erheblicher Mehrbedarf an Speicher.
- Neue Netzwerk-Technologien geben dem Netzwerk Systembus-Charakter und ermöglichen eine Speicher-Einbindung mit bisher unbekannter Leistung.
- Die Entwicklung von SSD-Speicher muss als sehr kritisch angesehen werden, stellt sie doch die traditionelle Formel Lokale Leistung = Zentrale Leistung in Frage. SSD muss zwangsläufig auch im SAN eine Rolle spielen oder es entsteht ein Performance-Loch zur Server-Leistung. Dies generiert neue Probleme im Netzwerk.

Im Gegensatz zur Vergangenheit ist zentraler Speicher als SAN damit nicht mehr nur auf den Datenbank-Bereich beschränkt. Vielmehr muss in Leistung und Bedarf mindestens unterschieden werden nach den Anwendungsbereichen:

- Datenbank- und Mainframe
- File-Services
- Virtualisierung
- Webarchitekturen
- Datensicherung

Das führt direkt zu der Frage, wie sich Anforderungen an Speicher-Technik in Zukunft quantifizieren und messen lassen. Tatsächlich kommen sehr unterschiedliche Kriterien zusammen:

- I/O-Transaktionsrate
- Bandbreite
- Verfügbarkeit
- Speichermenge
- Preis pro TB

Die Kombination sehr unterschiedlicher Anforderungen an den zentralen Speicher aus den verschiedenen Nutzungsbereichen generiert eine Reihe von Problemen oder auch Fragen:

- Handhabung immer größerer Datenmengen • Aufbau von Hierarchien
- Nutzbarkeit von Bändern
- Backup- und Restore
- Verfügbarkeit
- Performance kontra Preis
- Betrieb zentraler Speicher über Layer-2-Grenzen hinweg
- Umsetzung von Desaster Recovery Konzepten mit großen Datenmengen

Natürlich stehen diesen Problemen und Fragen auch Lösungsansätze gegenüber:

- LifeCycle Management
- Speicher-Virtualisierung
- Deduplizierung • VTL
- Thin Provisioning
- iSCSI/NFS

Diese scheinbar wegweisenden Lösungen generieren aber wieder neue Probleme. Herausragend sind dabei Herstellerabhängigkeit und die Komplexität des Betriebs zu nennen.

Hier setzt unser Forum zur Speicherinfrastruktur 2011 an. Wir analysieren:

- wie sich der Bedarf verändert
- welche Lösungsmöglichkeiten bestehen
- was die verschiedenen Lösungsansätze wirklich bringen
- wie sich die Lösungen in einen handhabbaren Betrieb einbinden lassen

Programmübersicht - ComConsult Storage-Forum 2011

Mittwoch, den 13.07.2011

9:30 bis 11:00 Uhr
Keynote: Vom traditionellen RZ zur Private Cloud
- Cloud Computing: Funktion, Chancen, Risiken
- Entwicklung der Web-Architekturen
- Server-, Speicher- und Netzwerkvirtualisierung
- Entwicklungen bei Netzwerken (Leistung, Latenz, Scale-Out)
- Strukturwandel des RZs
- Hochkonzentrierte Blade-Server: der Host-Phönix?

Dr. Franz-Joachim Kauffels, Unternehmensberater

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:30 Uhr
Erfahrungen von Unternehmen mit ihrer Speicherinfrastruktur
- Datenwachstum: wie schnell wachsen die Datenbestände?
- Wie ist dem Problem des Datenwachstums beizukommen: mit organisatorischen oder technischen Mitteln?
- Was wird mehr benötigt: Volumen oder Performance?
- Welche neuen Verfahren können genutzt werden, um dem Bedarf an mehr Volumen und Performance gerecht zu werden?
- Abgrenzung zwischen verschiedenen Datenklassen und Speichertypen
- Hochverfügbarkeit der Speicherinfrastruktur
- Herausforderung Datensicherung
- Sinn und Zweck der Speichervirtualisierung
- Wie viel Speichervirtualisierung braucht ein Unternehmen?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr
iSCSI im Rechenzentrum - ein Erfahrungsbericht
- Wie sieht die Grobstruktur des betrachteten RZs aus?
- Welche Anforderungen bestehen seitens der Server beim Zugriff auf den Speicher?
- Welche Aspekte haben die Entscheidung in Richtung iSCSI begünstigt?
- Welche (negativen) Erfahrungen wurden seitens Vattenfall gemacht, als das iSCSI-Netz noch als VLAN über eine gemeinsame Infrastruktur geführt wurde?
- Welche Verbesserungen haben sich ergeben durch die Separierung des iSCSI-Netzes auf dedizierte Hardware?
- Welche Leistungswerte (Durchsatz, IOs, Latenzen) liefert das aktuelle iSCSI-Netz?
- Welche Gründe sprechen aus Sicht von Vattenfall für einen Wechsel auf NFS?

Michael Witschke, Vattenfall IT

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:30 Uhr
Dateibasierter Speicherzugriff - Erfahrungen aus aktuellen Speicherprojekten
- Wofür eignen sich dateibasierte Verfahren wie NFS, CIFS?
- Was ist neu an NFSv4 und wie wirkt sich das auf die Nutzbarkeit dieses Protokolls als Ersatz von blockbasiertem Speicherzugriff aus?
- Welche Vorteile ergeben sich im Umfeld von NFS bei der Nutzung für Datenbanken oder virtuelle Umgebungen?
- Welche Einschränkungen ergeben sich hierbei?
- In der Praxis erzielbare Leistungswerte: Durchsatz, IOPS, Latenzen
- Wie skaliert eine NFS-Umgebung für Datenbanken und virtuelle Maschinen?
- Gibt es eine Größenordnung (Anzahl Hosts / Anzahl VMs), ab der eine NFS-Umgebung nicht mehr effizient ist?
- Wie gestalten sich Disaster Recovery Szenarien mit NFS?

Michael Albers, Hellweg Data

16:30 bis 17:30 Uhr
Technologische Entwicklungen bei Speichersystemen
- Dauerhaftigkeit von Back-End-Systemen
- Masselose SSDs als neue Speicherklasse
- Weiterentwicklung 3D-SSDs
- Das Netz als Systembus der Virtualisierten Umgebung
- Enterprise Storage Management

Dr. Franz-Joachim Kauffels, Unternehmensberater

Happy Hour ab 18:00 Uhr

Donnerstag, den 14.07.2011

9:00 bis 10:00 Uhr
Konstruktive Sicherheitsaspekte virtualisierter Storage Networks
- Sicherheit in SAN und NAS
- Welche Gefährdungen sind in SAN und NAS relevant?
- Maßnahmen zur Absicherung von SAN und NAS - Elemente einer SAN-Sicherheitsrichtlinie
- Konzepte für eine Zonierung im SAN
- Wann sollte verschlüsselt werden?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:00 bis 11:00 Uhr
Speichervirtualisierung: Steigerung der Flexibilität und Funktionalität oder nur der Komplexität?
- Konzept der Speichervirtualisierung
- Implementierungsvarianten: Inband, Split-Path, Netzwerk-basiert
- Leistungsmerkmale aktueller Lösungen
- Nutzung zur Datenspiegelung zwischen entfernten Standorten

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:30 Uhr
Möglichkeiten und Grenzen von Thin Provisioning und Deduplizierung
- Funktionsweise von Thin Provisioning
- Mögliche Ansatzpunkte für Thin Provisioning (VM, SAN, Speichersystem)
- Grenzen des Thin Provisioning durch blockbasierte Übertragung und Dateisysteme
- Deduplizierung vs. Kompression: Unterschiede und Gemeinsamkeiten
- Deduplizierung: Implementierungsvarianten out-of-band vs. inband
- Wann sind in der Praxis welche Effizienzraten zu erwarten?
- An welcher Stelle der Infrastruktur kann und sollte Deduplizierung eingesetzt werden?

N.N.

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr
Moderne Datensicherung mit VTLs und Disk-2-Disk-Verfahren
- Funktionsweise einer VTL
- Wann ist eine VTL einem allgemeinen Disk-2-Disk-Datensicherungsverfahren vorzuziehen?
- Wie kann eine VTL dabei helfen, aktuelle SLAs gerade im Bereich der Wiederherstellungszeiten einzuhalten?
- Einsatz von Snapshots im Umfeld der Datensicherung
- Datensicherung in virtuellen Umgebungen: LAN-basiert oder LAN-free?
- Möglichkeiten und Grenzen Image- und Datei-basierter Datensicherungen in virtuellen Umgebungen
- Datensicherung mit Bordmitteln der Virtualisierungshersteller und aktuellen Produkten von Drittherstellern

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:15 Uhr
Troubleshooting im Fibre Channel

Sebastian Schröder, MEN@NET GmbH

16:15 bis 17:00 Uhr
Herstellervortrag: „Tape: Probleme, Herausforderungen und Lösungsansätze bei der Tape-Verarbeitung“

Bernd Krieger,Crossroads GmbH

Programmübersicht - ComConsult Storage-Forum 2011

Freitag, den 15.07.2011

9:00 bis 15:00 Uhr
Strategien und Produkte der führenden Hersteller
- Wie sieht die Architektur der Speicherlösung aus?
- Wie skaliert die Leistung des Speichersystems?
- Welche Hochverfügbarkeitsmechanismen besitzt das Speichersystem?
- Wie können Multi-Site Desaster Recovery Szenarien mit dem Speichersystem gelöst werden?
- Welche Vorteile bringt das Speichersystem insbesondere in virtualisierten Umgebungen?

9:00 bis 09:45 Uhr
EMC Symmetrix vMax *Carsten Haak, EMC Deutschland GmbH*

9:45 bis 10:30 Uhr
Fujitsu Eternus
Wolfgang Schenk, Fujitsu Technology Solutions GmbH

10:30 bis 11:00 Uhr - Kaffeepause

11:00 bis 11:45 Uhr
HP Lefthand *Ingo Kraft, Hewlett-Packard Deutschland GmbH*

11:45 bis 12:30 Uhr
IBM XIV *Dirk Vogelsang, IBM Deutschland GmbH*

12:30 bis 13:30 Uhr - Mittagspause

13:30 bis 14:15 Uhr
NetApp FAS/V-Serie *Roger Zink, NetApp Deutschland GmbH*

Anschließende Diskussion mit den Herstellern:
- Wie sieht die Speicherarchitektur der Zukunft aus?
- Welches Speicherzugriffsverfahren wird sich durchsetzen?
- Gehört die Zukunft den SSDs?

15:00 Uhr Ende der Veranstaltung

NEUER TERMIN UND ORT

ComConsult Storage-Forum 2011
13.07. - 15.07.11 in Bonn

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult Storage-Forum 2011

Ich buche den Kongress
ComConsult Storage-Forum 2011

☐ 13.07. - 15.07.11 in Bonn
zum Preis von € 1.790,--* zzgl. MwSt.
* gültig bis zum 31.05.2011

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Zweitthema

Shortest Path Bridging vs. TRILL

Ein Vergleich

Fortsetzung von Seite 1

Dipl-Math. Cornelius Höchel-Winter ist Leiter des Testlabors der ComConsult Technologie Information GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungstests neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von Windows- und Unixnetzen; so hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben.

Markus Geller verfügt über langjährige Erfahrung in Forschung, Entwicklung und Betrieb von Lokalen Netzen, IP-TV, Wireless Local Area Networks sowie Sicherheits-Technologien. Als Mitarbeiter der ComConsult Technologie Information GmbH ist er verantwortlich für Produkttests und Marktbeobachtung. Zu diesen Themengebieten ist er zudem als Referent bei der ComConsult Akademie tätig

Die hauptsächlichen Merkmale und Ziele aller drei Verfahren lassen sich schnell aus der Bezeichnung „Shortest Path Bridging“ ableiten:

1. Es handelt sich um Layer-2-Verfahren.

2. Es geht darum, zwischen Endknoten die schnellste („kürzeste“) Verbindung
   a. zu finden und
   b. zu nutzen.

Wo diese Anforderungen herkommen, liegt auf der Hand: Mit dem verstärkten Einzug von Virtualisierungstechniken in die Rechenzentren und insbesondere deren Evolution (Stichwort Hochverfügbarkeit) wächst der Bedarf an größeren Layer-2-Bereichen. Praktisch alle Hochverfügbarkeits-, Fail-over- und Lastverteilungsverfahren der bekannten Server-Virtualisierungsprodukte setzen eine Layer-2-Verbindung voraus. Ähnliches gilt für das Provisioning, also die Bereitstellung neuer Server, durch modere Technologie im Rahmen von Cloud Computing.

Viele Cluster-Techniken, die eventuell sogar zwischen virtuellen Maschinen eingesetzt werden, oder auch FCoE (Fibre Channel over Ethernet) sind weitere Bereiche, die ebenfalls eine Layer-2-Verbindung voraussetzen.

Darüber hinaus hat die IEEE in den letzten Jahren mit 802.1ad, 802.1ah und 802.1Qay wichtige Standards für den Provider-Markt entwickelt, die klar darauf zielen, MPLS als Transportprotokoll abzulösen und stattdessen Ethernet auch in Weitverkehrsnetzen einzusetzen.

Layer-2-Bereiche, insbesondere große Layer-2-Bereiche, haben aber zumindest zwei Nachteile:

1. Natürlich die Multicasts, die offensichtlich mit der Anzahl der Knoten im Netz zunehmen.

2. Etablierte Verfahren zur optimierten Nutzung der vorhandenen Wege im Netzwerk können nicht genutzt werden.

Punkt 1 ist heutzutage gar nicht mehr so gravierend, Multicasts hat man in modernen Netzen im Wesentlichen im Griff. Viel wichtiger ist aber Punkt 2: Alle bis dato eingesetzten Verfahren zur Wegewahl setzen auf Layer 3 auf. Auf Layer 2 gibt es im Wesentlichen nur ein einziges Verfahren: den Spanning Tree - wenn auch in mehreren Varianten.

Die Spanning-Tree-Protokolle haben aber nicht die optimale Wegewahl als Ziel, ihre Aufgabe ist einzig und allein dafür zu sorgen, dass sich im Netz keine Schleifen bilden. Das Ergebnis ist daher immer eine schleifenfreie Baumstruktur, vorhandene alternative Wege werden zur Verhinderung von Schleifen stillgelegt und nicht genutzt. Dies führt aber gerade in stark vernetzten Strukturen zu vielen brachliegenden Netzwerkressourcen und je nach Topologie zu mitunter verheerend schlechten Kommunikationspfaden (siehe Abbildung 1).

Die Art und Weise, wie wir heutzutage Netze aufbauen, ist wesentlich von solchen Baumstrukturen geprägt und damit zu einem guten Teil ineffektiv. Baum- oder sternförmige Topologien produzieren praktisch zwangsweise Engstellen, denen in „modernen“ Designs mit Overprovisioning entgegen gewirkt wird. Besser geeignete Designs wie Ringtopologien oder voll- oder teilvermaschte Topologien sind aber bislang nur auf Layer 3 realisierbar.

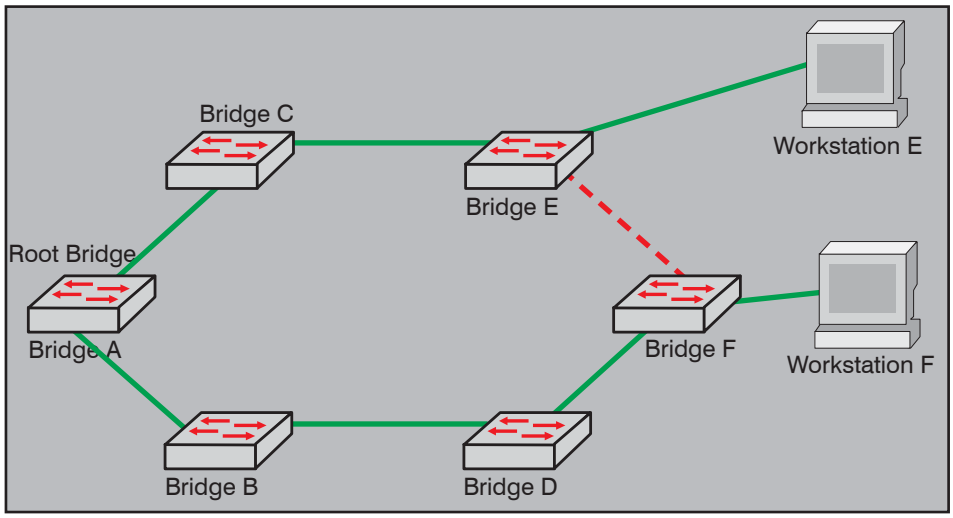


Abbildung 1: Spanning Tree bei Ringtopologie

Wünschenswert ist daher eine Technik, die es erlaubt, dass auch auf Layer 2 alle Verbindungen aktiv genutzt werden können und so eine Wegewahl möglich wird, ähnlich wie wir es aus Layer-3-Netzen kennen.

Anforderungen

Damit sind also die wichtigsten Anforderungen an die neuen Layer-2-Protokolle motiviert. Weitere Anforderungen ergeben sich aus den Tatsachen, dass gleichzeitig auch die Bandbreitenansprüche an die Netze wachsen und die neuen Protokolle natürlich in bestehende Netze integriert werden müssen.

Wir formulieren daher folgenden Anforderungskatalog:

1. Alle verfügbaren Netzwerkverbindungen sollen gleichzeitig aktiv genutzt werden können.

2. Zwischen jeweils zwei Endknoten soll ein optimaler („kürzester") Weg ausgewählt werden.

3. Falls mehrere gleichwertige (equal cost) Wege zwischen zwei Knoten gefunden werden, sollen gegebenenfalls mehrere dieser Wege gleichzeitig genutzt werden können, um so die Gesamtlast im Netzwerk gleichmäßig verteilen zu können.

4. Geräte, die die neuen Protokolle unterstützen, müssen zusammen mit herkömmlichen Brücken, die die neuen Protokolle nicht unterstützen, funktionieren (Abwärtskompatibilität).

5. Vorhandene Management- und Fehlersuche-Tools müssen weiter funktionieren und genutzt werden können.

Zwei sind besser als keiner?

Wie beschrieben gibt es also einen deutlichen Bedarf an neuen Netzwerktechniken, die die genannten Anforderungen erfüllen. Wie so oft hat aber niemand diesen Bedarf rechtzeitig vorhergesehen, oder genauer gesagt, niemand hat in vernünftiger Zeit einen entsprechenden Standard zu Wege gebracht. Mit „niemand" ist an dieser Stelle natürlich in erster Linie die IEEE gemeint, die ja bislang praktisch alle wichtigen Layer-1- und Layer-2-Protokolle standardisiert hat. Man kann sich also durchaus auf den Standpunkt stellen, dass die Entwicklung eines passenden Layer-2-Protokolls in den Aufgabenbereich der IEEE fällt. Und tatsächlich ist ja die IEEE seit einigen Jahren dabei, in der Arbeitsgruppe 802.1aq unter der Bezeichnung ***„Shortest Path Bridging"*** (SPB) einen entsprechenden Standard zu entwickeln. Der erste Draft hierzu stammt aus dem Jahr 2006, aktuell ist der Draft 3.2 vom Oktober 2010, auf den wir uns in diesem Artikel beziehen.

Trotz der in der vergangenen Zeit durchaus erfolgreichen Arbeitsteilung zwischen IEEE und IETF beschäftigt sich aber auch die IETF schon seit circa 2005 (die ersten Dokumente zu RBridges stammen sogar aus dem Jahr 2004) mit der Entwicklung einer konkurrierenden Lösung unter der Bezeichnung ***„Transparent Interconnection of Lots of Links"***, kurz TRILL. Die offizielle Begründung für dieses ja tatsächlich etwas befremdliche Vorgehen ist, dass die IEEE mit ihrer Arbeit nicht schnell genug vorankomme. Wie dem auch sei, auch die IETF ist mit ihrer Arbeit noch nicht am Ende. Lediglich eine so genannte „Base Protocol Specification" ist mittlerweile verabschiedet, aber auch dieses Dokument hat noch keine RFC-Nummer und keinen Standardstatus, da das referenzierte IS-IS-Verfahren seinerseits noch nicht verabschiedet ist.

TRILL: Grundlagen und Begriffe

TRILL liegt die Idee zugrunde, Layer-3-Routing-Verfahren auf Layer-2-Netze zu übertragen. Hierzu wird ein neuer Typ von Netzwerkkomponenten eingeführt, die so genannte RBridge (Routing Bridge). Eine RBridge ist diejenige Komponente, die TRILL im Netzwerk verfügbar macht.

Die Grundzüge des Verfahrens sind:

- Die Frames werden „Hop by Hop" von RBridge zu RBridge durch das Netzwerk weitergereicht. Die erste RBridge auf dieser Abfolge von RBridges, die also den Original-Frame entgegennimmt, wird als „Ingress RBridge" bezeichnet und entsprechend die letzte RBridge, die den Original-Frame ausliefert, als „Egress RBridge".

- Solange die „Ingress RBridge" noch nicht gelernt hat, über welche „Egress RBridge" eine bestimmte Ziel-MAC-Adresse (inkl. VLAN) zu erreichen ist, werden Multicasts zur Weiterleitung verwendet.

- Außerdem lernt jede RBridge über IS-IS als „Routing"-Protokoll, über welche „Next-Hop"-RBridges die „Egress RBridges" zu erreichen sind.

- Zur Weiterleitung wird der Original-Frame durch ein MAC-in-MAC-Verfahren eingekapselt. Als neue (äußere) Ziel-MAC-Adresse dient dabei die MAC-Adresse der „Next-Hop"-RBridge. Außerdem erhält der Frame einen zusätzlichen „TRILL-Header", in dem außer der letztendlichen „Egress RBridge" auch ein Hop-Count zur Schleifen-Vermeidung kodiert ist (Details weiter unten).

- An der „Next-Hop"-RBridge wird dann ähnlich bei einem Router der äußere MAC-Header ausgetauscht, der Hop-Count reduziert und der Frame weitergeschickt.

- Dies wird solange fortgeführt, bis die „Egress RBridge" erreicht ist (oder der Hop-Count auf Null steht). Auf der „Egress RBridge" wird dann der Original-Frame wiederhergestellt und zugestellt.

IS-IS wurde dabei als Topologie-Protokoll (Routing-Protokoll) ausgewählt, da IS-IS einige Vorteile bietet:

- IS-IS läuft direkt auf Layer 2. Es werden keine IP-Adressen benötigt wie etwa bei OSPF.
- IS-IS kann ohne Konfiguration (Zero Configuration) betrieben werden.
- IS-IS verwendet eine TLV-Kodierung (Typ, Length, Value); dieses vereinfacht die Definition und den Transport von neuen Arten von Daten.

Das skizzierte Verfahren hat offensichtlich folgende Vorteile:

- So genannte „Transit RBridges“, also RBridges, die innerhalb des Pfades Frames lediglich weiterleiten, müssen keine MAC-Adressen von Endgeräten, sondern lediglich die MAC-Adressen anderer RBridges lernen. Dies reduziert den Umfang der Weiterleitungstabelle, der so genannten „Forwarding Information Base“, deutlich.
- Mit Hilfe des Hop-by-Hop-Verfahrens unterstützen RBridges so genanntes „Multi-Pathing“, das ist die gleichzeitige Nutzung paralleler, kostengleicher Wege. Wie oben erwähnt, ermöglicht dies eine bessere Auslastung der Netzwerkknoten und so gegebenenfalls einen höheren Datendurchsatz. (siehe Abbildung 2)

TRILL: Aufbau der Header

Wie oben erwähnt nutzt TRILL zum Transport von Daten-Frames einen MAC-in-MAC-Einkapselungsmechanismus. Hierbei erhalten die Frames zum einen einen neuen äußeren Transport-Header und zum anderen einen so genannten „TRILL Header“. (siehe Abbildung 3)

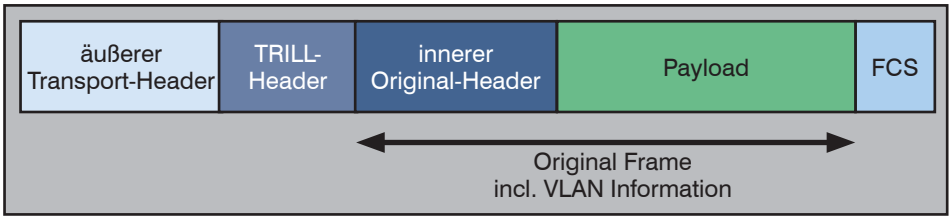


Abbildung 3: Format eines TRILL-Daten-Frames

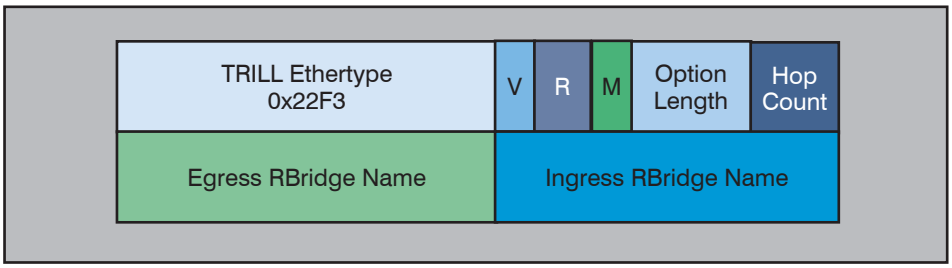


Abbildung 4: Format des „TRILL Headers“

Der TRILL-Header wird ausschließlich von der „Ingress RBridge“ gesetzt und bleibt bis auf den Hop Count während des gesamten Transports durch die TRILL-Domäne unverändert. Er hat folgendes Format (siehe Abbildung 4):

- 16 Bit Ethertype (0x22F3)
- 2 Bit Protokollversion (V)
- 2 Bit reserviert (R)
- 1 Bit Multi-Destination-Bit (M)
- 5 Bit Option Length
- 6 Bit Hop Count
- 16 Bit Egress RBridge Name
- 16 Bit Ingress RBridge Name

Über das Ethertype-Feld wird der gesamte Frame als TRILL-Daten-Frame gekennzeichnet.

Ingress und Egress RBridge Namen sind eindeutige Kennungen für die beiden Systeme, die automatisch für jede RBridge erzeugt werden, sobald die RBridge einer TRILL-Domäne beitritt. RBridge Namen sind jeweils 16 Bit lang.

Die „Egress RBridge“ bzw. deren Name wird für Unicast-Frames mit bereits gelernter Zieladresse aus der Weiterleitungstabelle (Forwarding Information Base) bestimmt.

Für Unicast-Frames mit unbekannter Zieladresse sowie für Multicast- und Broadcast-Frames wird dagegen ein spezielles Konzept genutzt, das auf so genannte „Distribution Trees“ aufsetzt. „Distribution Trees“ sind speziell für diesen Zweck berechnete VLAN-übergreifende Baumstrukturen, die jede RBridge mit jeder anderen schleifenfrei verbindet. Ein „Distribution Tree“ ist also vergleichbar mit dem Spanning Tree. Prinzipiell reicht daher ein einziger „Distribution Tree“, zur besseren Nutzung der vorhandenen Topologie können aber auch mehrere „Distribution Trees“ berechnet werden, von denen dann einer von der „Ingress Bridge“ ausgewählt wird.

Im Falle von Unicast-Frames lernt die letztliche erreichte „Egress RBridge“ über den TRILL-Header, von welcher „Ingress RBridge“ die Absenderadresse ursprünglich kam und kann mit einem Unicast-TRILL-Frame antworten. Sobald diese Antwort bei der ursprünglichen „Ingress RBridge“ eingetroffen ist, kennt auch diese RBridge die zuständige „Egress RBridge“ und ist ab dann nicht mehr auf Multicasts und „Distribution Trees“ angewiesen.

Der äußere Transport-Header besteht wie üblich aus

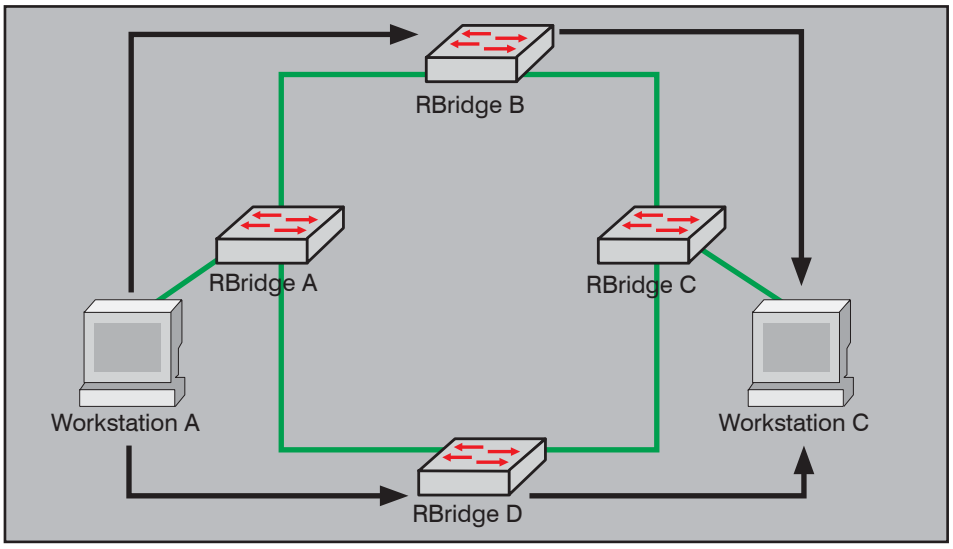


Abbildung 2: Multi-Pathing

- Zieladresse,
- Absenderadresse und
- VLAN-Tag

und wird an jeder RBridge für die nachfolgende Übertragung jeweils neu gesetzt. Absenderadresse ist dabei stets die MAC-Adresse der lokalen RBridge. Die Zieladresse wird anhand des „Egress RBridge Name“-Eintrags im TRILL-Header bestimmt. Wird dort auf eine „Egress RBridge“ verwiesen, dann der Frame über einen Unicast weitergeleitet und als Zieladresse wird die „Next-Hop“-RBridge eingetragen. Wird im „Egress RBridge Name“-Eintrag auf einen „Distribution Tree“ verwiesen, dann wird der Frame über eine entsprechende Multicast-Adresse weitergeleitet.

Der VLAN-Eintrag im äußeren Header wird nur dann benötigt, wenn die lokale RBridge und die nachfolgende RBridge nicht unmittelbar benachbart, sondern über ein herkömmliches, nicht TRILL-fähiges, LAN-Segment verbunden sind (siehe Bild) und der Transport über dieses LAN-Segment VLANs erfordert. Auch dieses Feld wird RBridge für RBridge neu gesetzt.

Damit sind wir bei einer Besonderheit des TRILL-Protokolls: Die Verbindung zwischen zwei RBridges muss nicht ein direkter Link sein, es können auch lokale Inseln aus herkömmlichen Brücken überquert werden. Diese Inseln werden dann natürlich durch Standardmechanismen, sprich Spanning-Tree-Protokolle gesteuert. Die Spanning Tree BPDUs werden von den RBridges terminiert, so dass die Wirkung der Spanning-Tree-Protokolle tatsächlich auf solche Bereiche beschränkt bleiben. (siehe Abbildung 5)

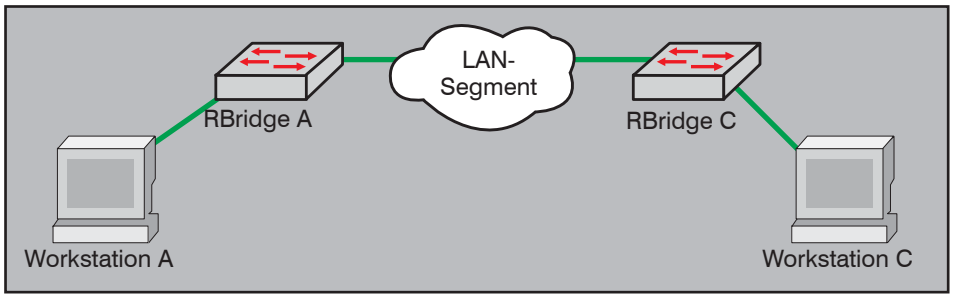


Abbildung 5: TRILL über herkömmliches LAN-Segment

SPB: Grundlagen und Begriffe

Shortest Path Bridging (SPB) wird von der IEEE in der Arbeitsgruppe 802.1aq als Erweiterung des VLAN-Standards 802.1Q entwickelt und schon damit ist klar, dass sich SPB mehr oder weniger nahtlos in bestehende Netze nach IEEE 802.1D („MAC Bridges“) und IEEE 802.1Q („VLANs“) integrieren wird.

Damit diese Integration in die vorhandenen 802.1-Strukturen funktionieren kann, müssen einige Grundvoraussetzungen, die in diesen Netzen gelten, berücksichtigt werden:

1. Unicasts, Multicasts und Broadcasts zwischen einem bestimmten Sender und einem bestimmten Ziel müssen über dieselben Wege transportiert werden (eine stabile Netzwerksituation vorausgesetzt).

2. Hinweg und Rückweg müssen symmetrisch sein, das heißt über dieselben Brücken führen.

Die grundlegende Konzeption von SPB ist es daher, den Spanning-Tree-Protokollen einen besser und schneller skalierenden Mechanismus zur Seite zu stellen, der zwar die eingangs formulierten Ziele wie die aktive Nutzung aller Links durch die Bestimmung optimaler Wege unterstützt, gleichzeitig aber an der Idee vollständiger (d. h. es gibt zu jedem Ziel einen Weg) und einfacher (d. h. es gibt keine Schleifen bzw. es gibt zu jedem Ziel nur einen einzigen Weg) Baumstrukturen festzuhalten.

Die Grundzüge von Shortest Path Bridging sind also:

- Über IS-IS werden pro VLAN von jeder Brücke optimale Wege durch das Netzwerk berechnet.

- Über geeignete (im Grunde sehr einfache) Algorithmen (ECT algorithms) wird sichergestellt,

  - dass bei kostengleichen Wegen deterministisch ein eindeutiger Weg ausgewählt wird;

  - dass Brücken, die auf diesem Weg liegen, denselben (Rest-)Weg zu demselben Ziel berechnen;

  - dass die Rückwege symmetrisch zu den Hinwegen berechnet werden.

- Diesen auf diese Weise berechneten, so genannten „Shortest Path Trees“ (SPTs) werden innerhalb einer SPB-Region eindeutige VLANs (Details siehe unten) zugeordnet.

- Alle diese Informationen werden über IS-IS im Netzwerk propagiert.

- Eingehende Frames werden am Rand der SPB-Region (also an der „Ingress Bridge“) dem entsprechenden SPT zugeordnet und dann unverändert durch die SPB-Region bis zur Ausgangsbrücke transportiert.

- Unicast-, Multicast- und Broadcast-Frames werden auf diese Weise gleich behandelt.

SPBV

In den ersten Entwürfen von Shortest Path Bridging war nur ein Verfahren vorgesehen, um SPTs zu kennzeichnen und Frames durch eine SPB-Region zu transportieren, nämlich mittels VLANs. Dieses ursprüngliche Verfahren wird immer noch unterstützt und wird im aktuellen Draft als ***SPBV*** bezeichnet.

SPBV-Bridges verwalten je eine so genannte „Translation Table“, die am Rand der SPB-Region die außerhalb genutzten Original-VLAN-IDs in nur innerhalb der Region genutzte Transport-VLANs übersetzt und umgekehrt. Die für diesen Zweck verwendeten VLAN-IDs werden netzwerkweit dynamisch reserviert und den jeweiligen Transportbäumen (SPTs) zugeordnet.

Die Koordination dieser netzwerkweiten Reservierung und Zuordnung übernimmt dabei ebenfalls IS-IS. Aufgrund der vollständigen Automatisierung dieser Vorgänge kann SPBV ohne Konfiguration „Plug-and-Play“ betrieben werden.

Dieser auf den ersten Blick überflüssig erscheinende Schritt der Übersetzung von externen in interne VLANs und umgekehrt geschieht, weil diese Zuordnung keineswegs umgekehrt eindeutig sein muss. Auf diese Weise kann man beispielsweise Multi-Pathing unterstützen – man ordnet einfach ein und demselben externen VLAN mehrere Transport-VLANs zu, die ihrerseits zu unterschiedlichen SPTs gehören.

Mit SPBV erwartet die IEEE, dass Topologien mit bis zu 100 Brücken in einer SPB-Region unterstützt werden können.

SPBM

Im Laufe der Jahre seit der Gründung der SPB-Arbeitsgruppe wurde dann mindestens ein sehr wichtiger Standard bei der IEEE verabschiedet, nämlich Provider Backbone Bridging (IEEE 802.1ah-2008) und spätestens seitdem kann man sagen, dass für die IEEE der Carrier-Markt wesentlich stärker in den Vordergrund gerückt ist. Daher beschreibt der SPB-Draft mittlerweile ein zweites Verfahren, welches auf das MAC-in-MAC-Verfahren aus 802.1ah zurückgreift: SPBM.

SPBM ist aus Sicht der IEEE Provider-Technik. So erwartet die IEEE beispielsweise mit SPBM Topologien mit bis zu 1.000 Brücken in einer SPB-Region unterstützen zu können. Aber SPBM hat auch im Enterprise- und Rechenzentrumsumfeld einige Vorteile.

Zu den Details:

- Die Original-Frames werden gemäß IEEE 802.1ah (siehe Abbildung 6) eingekapselt.
- Als Zieladresse (B-DA) wird von der Ingress Bridge die MAC-Adresse der Egress Bridge gesetzt, falls die originale Zieladresse (C-DA) (inkl. VLAN) in der lokalen Weiterleitungstabelle bereits bekannt ist. Ansonsten wird eine Multicast-Adresse genutzt. In jedem Fall bleibt der eingekapselte Frame auf dem gesamten Weg durch die SPB-Region unverändert.
- Durch die Einkapselung bleibt insbesondere das VLAN des Original-Frames erhalten. Das kann bei einer Fehlersuche hilfreich sein.
- Den Shortest Path Trees (SPTs) kann – wie in PBBNs (Provider Backbone Bridged Networks) üblich – an den Eingangsports ein zusätzlicher Service (I-SID, innerhalb des I-TAG) zugeordnet werden. Damit können deutlich mehr VLANs durch das SPB-PBBN transportiert werden als bei SPBV. (siehe Abbildung 7)
- Das Verfahren unterstützt damit alle typischen Carrier Ethernet Services wie E-Line, E-LAN, E-Tree.
- Durch die Einkapselung kommen im Innern der SPB-Region nur die MAC-Adressen der teilnehmenden SPB-Brücken vor, was deren Weiterleitungstabellen deutlich verkleinert. Die MAC-Adressen von Endgeräten müssen nur an den Randports der SPB-Region gelernt werden.
- Da die MAC-Adressen der SPB-Brücken durch IS-IS während der Pfadberechnung publiziert werden, ist das Lernen von MAC-Adressen an allen Ports, die mit anderen SPB-Brücken verbunden sind, unnötig und daher abgeschaltet.
- Angrenzende 802.1ah-Netze können durch die Bildung spezieller MAC-Multicasts, in denen die I-SID und die Adresse der Egress-Bridge kodiert sind, ebenfalls durch die SPB-Region transportiert werden.

SPB: Multi-Pathing

Wie oben erwähnt, wird zum Transport eines bestimmten Frames durch die SPB-Region von der „Ingress Bridge“ genau ein kürzester (kostengünstigster) Pfad ausgewählt. Die Bestimmung dieses Pfads erfolgt durch IS-IS. IS-IS unterscheidet jedoch nicht zwischen kostengleichen Pfaden! Daher muss ein zusätzlicher Algorithmus (ein so genannter ECT (Equal Cost Tree) Algorithm) für eine deterministische Entscheidung sorgen.

Im aktuellen Draft von SPB sind beispielhaft 16 solcher Algorithmen verpflichtend vorgeschrieben. Der Sinn dieser Algorithmen ist es, andere Shortest Path Trees auswählen zu können und so beispiels-

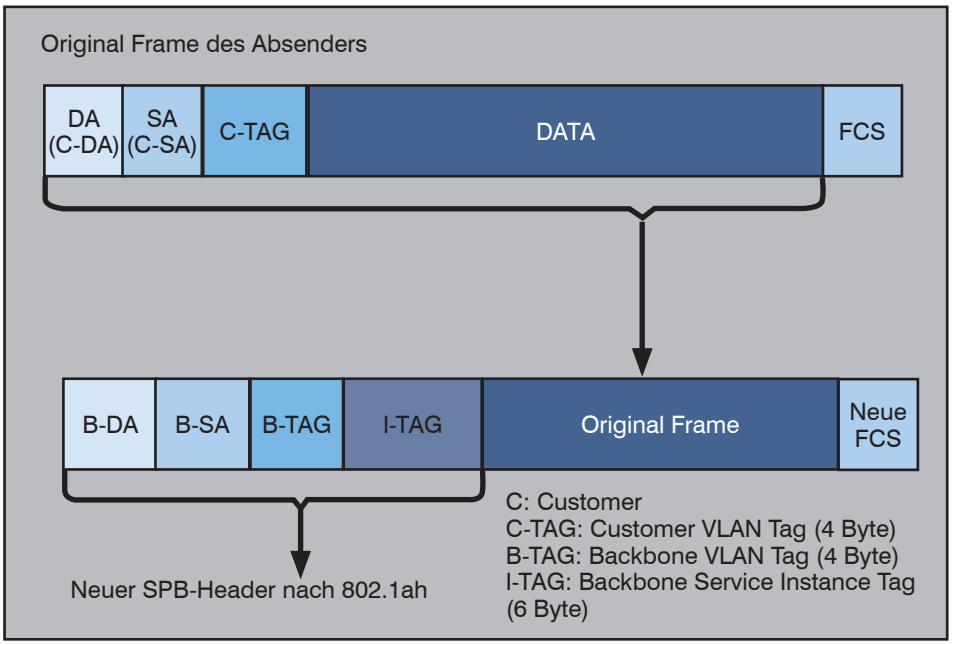


Abbildung 6: Encapsulation und Frame-Format nach IEEE 802.1ah

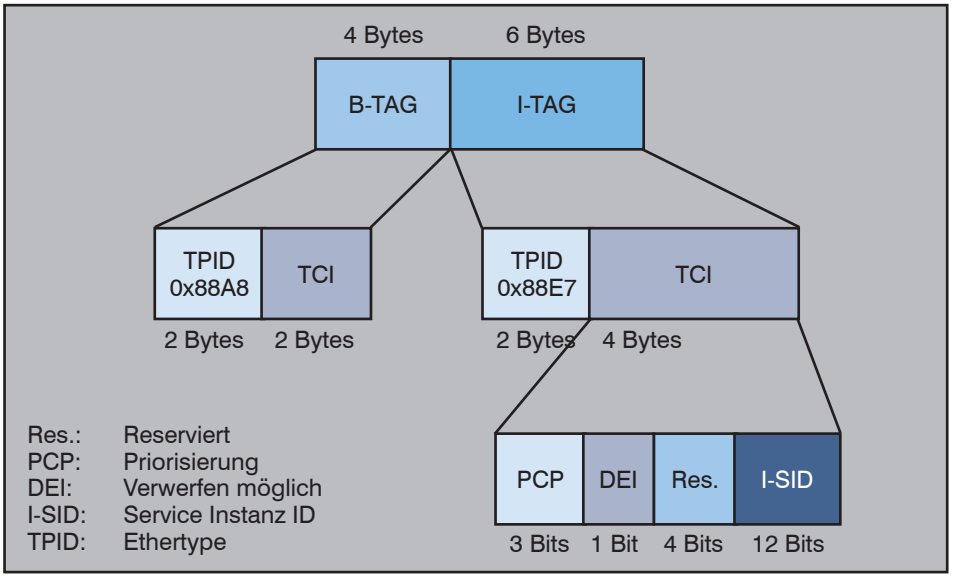


Abbildung 7: TAG-Formate bei 802.1ah

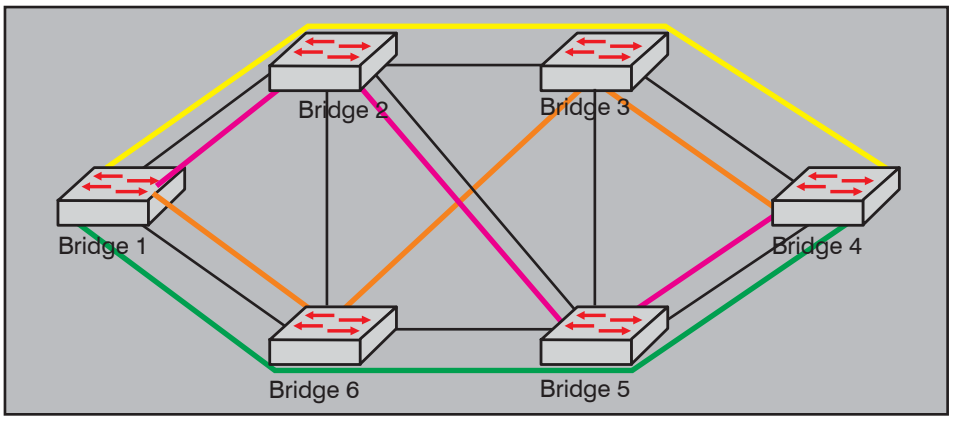


Abbildung 8: Vier kostengleiche Pfade von Bridge 1 zu Bridge 4

wiese verschiedene VLANs mittels verschiedener ECT-Algorithmen über verschiedene kostengleiche Pfade zu leiten. Weitere Algorithmen sind herstellerspezifisch möglich.

TRILL vs. SPB: Ein Vergleich

Auf den ersten Blick könnte man zu dem Ergebnis kommen, dass TRILL und SPB einander sehr ähnlich sind:

- Beide liefern kostengünstigste Pfade durch ein Netzwerk.
- Beide nutzen IS-IS zur Pfadbestimmung.
- Beide unterstützen Multi-Pathing bei kostengleichen Pfaden.
- Beide (wenn wir uns mal auf SPBM konzentrieren) nutzen ein MAC-in-MAC-Verfahren zum Transport der Daten-Frames.
- Beide nutzen VLANs zur Kennzeichnung der Datenpfade durch das Netzwerk.

Damit erfüllen beide Protokolle insbesondere die Punkte 1 bis 3 aus unserem Anforderungskatalog vom Anfang dieses Artikels.

Andererseits gibt es aber auch gravierende Unterschiede! Insbesondere die Entscheidung der IETF, TRILL ein Hop-by-Hop-Verfahren zugrunde zu legen, ist im Layer-2-Umfeld ein absolutes Novum und macht es äußerst schwer, wenn nicht unmöglich, dieses Protokoll kompatibel auf Layer-2-Switche zu implementieren. Im Grunde wird mit dem RBridge-Konzept eine neue Geräteklasse eingeführt, man könnte sagen Layer-2 ½ -Geräte.

Und dies ist keine rein akademische Feststellung. RBridges verhalten sich definitiv anders als „normale“ Switche nach IEEE 802.1, was durchaus Auswirkungen auf den Betrieb solcher Netze haben wird. So gehen beispielsweise praktisch alle Statistik- und Fehlersuche-Tools davon aus, dass man anhand der ersten Bytes eines Frames erkennen kann, von wo nach wo die Datenströme fließen – 802.1-Brücken ändern nun mal den Frame-Header beim Weiterleiten nicht (daher die Bezeichnung „Switch“), RBridges machen das aber, RBridge sind daher in dem Sinne keine Switches. Und dass an jeder RBridge damit die FCS (Frame Check Sequence) für jedes Paket neu berechnet werden muss, muss man nicht extra erwähnen.

Apropos Fehlersuche: Ganz allgemein muss man sicherlich davon ausgehen, dass Management und Fehlersuche in Shortest-Path-Netzen schwieriger und anspruchsvoller werden. Das liegt schon allein daran, dass diese Netze deutlich dynamischer sein werden als herkömmliche Netze, aber eben auch dezentraler, vermaschter. So ohne weiteres wird es dann nicht mehr klar sein, wie und wo sich die Datenströme im Netzwerk verteilen.

Da ist es durchaus von Vorteil, dass SPB vollständig kompatibel zu dem OAM-Standard (OAM = Operations, Administrations and Maintenance) IEEE 802.1ag (Connectivity Fault Management) ist, welcher seinerseits in weiten Teilen identisch ist mit der ITU-Empfehlung Y.1731. Für TRILL trifft das nicht zu, die TRILL-Arbeitsgruppe bei der IETF hat angekündigt, eigene OAM-Vorschläge zu entwickeln – das kann aber dauern.

Aber TRILL bringt auch mit seinem Weiterleitungskonzept für Broadcasts und Multicasts (über „Distribution Trees“) und seiner Multi-Pathing-Lösung weitere Dynamik ins Spiel. Denn einerseits werden Broadcasts und Multicasts über andere Wege geleitet als Unicasts (und haben damit andere Laufzeiten) und andererseits verteilt TRILL Datenpakete zufällig (Hash-basierend) über gegebenenfalls vorhandene, kostengleiche Pfade. SPB hält sich an diesem Punkt streng an die Erfordernisse der 802.1-Protokollsuite. Das hat Vorteile beim Monitoring und Trouble-Shooting: Wenn Sie wissen, wie ein konkreter Datenfluss verläuft, können Sie diesen dann auch an einem passend platziertem TAP oder an einem passenden Monitor-Port vollständig überwachen.

Auf der anderen Seite muss man der TRILL-Lösung zugutehalten, dass ihr Multi-Pathing-Konzept die Netzwerkressourcen vermutlich besser nutzt, da die Daten gleichförmiger über vorhandene Pfade verteilt werden. Der Nachteil einer solchen Auffächerung des Datenstroms ist allerdings wiederrum: Die Reihenfolge der Frames kann nicht garantiert werden. SPB bringt mit seinen ECT-Algorithmen zwar ein gewisses Maß an Flexibilität, dies muss allerdings administrativ konfiguriert werden. Der standardmäßig ausgewählte Algorithmus wird immer bestimmte Pfade und damit bestimmte Brücken bevorzugen.

Ein weiterer Unterschied zwischen TRILL und SPB ist das Frame-Format. TRILL führt mit seinem neuen Header ein neues Format ein (neue Data Plane), während SPB auf bereits eingeführte Formate aus 802.1ad und 802.1ah setzt. Dies führt dazu, dass SPB zumindest auf modernen Switchen mit vorhandenen ASICs auskommt und per Software-Update nachgerüstet werden kann. TRILL benötigt im Gegensatz dazu in jedem Fall neue Hardware – und das kostet.

Die Tabelle fasst die wesentlichen Merkmale von TRILL und SPB nochmals zusammen.

Fazit: Zwei sind einer zu viel

Schaut man sich einige Unterschiede zwischen TRILL und SPBM an:

- ca. 4000 VLANs bei TRILL gegenüber 16 Millionen Service-Tags bei SPB,
- Auffächerung des Datenstroms über verfügbare Pfade bei TRILL gegen die strikte Zuordnung von Verkehrs- bzw. Service-Klassen zu einzelnen SPTs bei SPB,
- die explizite Unterstützung von OAM-Standards bei SPB gegen keine Unterstützung bei TRILL

Shortest Path Bridging vs. TRILL - Ein Vergleich

	TRILL	SPB (802.1aq)
Wegewahl	Shortest Path nur für Unicasts	ein symmetrischer Shortest Path für alle Frame-Typen
Transportebene	MAC-in-MAC mit zusätzlichem TRILL-Header	SPBV: VLANs SPBM: 802.1ah (MAC-in-MAC)
Steuerungsebene (Link State Protocol)	IS-IS	IS-IS
Klassifizierung der Datenströme	VLANs (4.095)	SPBV: VLANs (4.095) SPBM: I-SID (> 16 Millionen)
Schleifenverhinderung	Unicasts: Hop Count (TTL) , Multicasts: RPF Check	RPF Check
Multi-Pathing	ja, Verteilung Hash-basierend	ja, ein Pfad pro VLAN/Service
Lastverteilung	ja	teilweise
Kompatibilität	teilweise: STP, RSTP, MSTP, VLANs (802.1D), DCB (802.1Qbb, 802.1Qaz, 802.1Qau)	alle 802.1D- und 802.1Q-Protokolle, insbesondere DCB und Provider Bridging
Operations, Administration and Maintenance	nicht vorhanden	802.1ag und Y.1731
Herstellerunterstützung	Brocade, Cisco, HP (3Com), Intel, Juniper	Avaya (Nortel), Alcatel-Lucent, Cisco, Huawei
Anwendungsgebiet	Rechenzentrum	Rechenzentrum, Carrier Markt, Metro Ethernet

Abbildung 9: Vergleich TRILL vs. SPB

erkennt man doch gewisse Tendenzen zu unterschiedlichen Zielmärkten: SPBM Richtung Carrier Markt, TRILL Richtung Data Center.

Das heißt keineswegs, dass sich SPB oder speziell SPBM nicht für Rechenzentrumsnetze eignet, im Gegenteil: Gerade um virtuelle Strukturen, wie sie in virtualisierten Rechenzentrum (oder in der neuen Bezeichnung Cloud Computing) zunehmend vorkommen, von der physikalischen Ebene zu abstrahieren, ist IEEE 802.1ah mit seinem I-TAG und damit auch SPB hervorragend geeignet. Aber SPBM ist offensichtlich für große, gemanagete Netze entworfen. Wie einfach oder komplex SPBM im Einzelfall zu konfigurieren sein wird, muss sich mit der Verfügbarkeit konkreter Produkte noch zeigen.

Damit kommen wir zum Schluss: Für SPB spricht eine Menge, insbesondere die höhere Kompatibilität sowohl mit existierenden Protokollen als auch mit existierender Hardware. Für TRILL spricht an erster Stelle die derzeit umfangreichere Herstellerunterstützung. Es bleibt abzuwarten, ob das so bleibt. Sobald der IEEE-Standard verabschiedet ist - und das könnte noch in diesem Jahr sein - können die Hersteller auf vorhandenen und gegebenenfalls sogar schon verbauten Chips implementieren. Avaya hat schon Ende letzten Jahres Prä-Standard-Implementierungen für einige ihrer großen Switche vorgestellt. Ciscos FabricPath wird zwar von vielen Kommentatoren als Prä-Standard-Implementation von TRILL angesehen, das Protokoll hat aber im Grunde viel mehr Ähnlichkeit mit SPB (so ändert FabricPath beispielsweise nicht den MAC-Header auf jedem Hop).

Ärgerlich bleibt die Entwicklung und letztlich auch Markteinführung zweier so ähnlicher Standards allemal. Die Unternehmen müssen sich auf absehbare Zeit zwischen beiden Verfahren entscheiden – und gehen damit letztlich eine Herstellerbindung ein, die eigentlich durch Standards vermieden werden sollte. Was bleibt, ist viel Beratungsbedarf, wenn solche Netze später einmal zusammengeführt oder umgestellt werden sollen.

Daher schließen wir mit einem Appell: IEEE und IETF mögen sich umgehend zusammensetzen und eine gemeinsame Lösung entwickeln.

Kongress

Netzwerk-Redesign Forum 2011
04.04. - 07.04.11 in Königswinter

Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, das Campus-Netzwerk, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Neue Standards zur Gestaltung von Netzwerken im Rechenzentrum und im Backbone sind gute Beispiele dafür.

Moderatoren: Dipl.-Inform. Petra Borowka-Gatzweiler, Dr. Franz-Joachim Kauffels
Dr.-Ing. Behrooz Moayeri
Preis: € 1.990,-- zzgl. MwSt. bzw. € 2.390,-- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

TCP/IP und SNMP, 14.02. - 18.02.11 in Berlin

LAN-, WLAN- und WAN-Netzwerke sind heutzutage IP-Netze, und ein Verzicht auf Nutzung des IP-basierten Internet undenkbar. Auch für früher nur mit herstellerspezifischen Protokollen in Verbindung gebrachte Anwendungsgebiete wie Telefonie oder Produktionsumgebungen gibt es mittlerweile geeignete IP-basierte Lösungen. Hersteller und Dienstanbieter versuchen den Eindruck zu vermitteln, die Nutzung sei kinderleicht, fast schon plug and play - man trägt ein paar Adressen ein (wenn überhaupt), und es kann losgehen. Falsch!

Preis: € 2.490,-- zzgl. MwSt.

Interne Absicherung der IT-Infrastruktur, 21.02. - 23.02.11 in Bonn

Bedingt durch Netzkonvergenz, Mobilität und Virtualisierung hat die interne Absicherung der IT-Infrastruktur in den letzten Jahren enorm an Bedeutung gewonnen. Heterogene Nutzergruppen mit unterschiedlichstem Sicherheitsniveau teilen sich eine gemeinsame IP-basierte Infrastruktur und in vielen Fällen ist der Aufbau sicherer, mandantenfähiger Netze notwendig. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Alle wichtigen Bausteine zur Absicherung von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN werden detailliert erklärt und anhand konkreter Projektbeispiele wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt. Preis: € 1.890,-- zzgl. MwSt.

IP-Wissen für TK-Mitarbeiter, 28.02. - 01.03.11 in Aachen

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das TK-Mitarbeiter ohne Vorkenntnisse zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen. Alle Seminarinhalte werden von einem Referenten mit hoher Praxiserfahrung betreut. Ziel ist dabei bewusst, statt einer umfassenden Theorieschulung gezielt die Aspekte vorzustellen und unter Praxis-relevanten Gesichtspunkten zu beleuchten, die erfahrungsgemäß aus Sicht einer IP-basierten Telefonielösung wichtig sind.

Preis: € 1.490,-- zzgl. MwSt.

Trouble Shooting für Netzwerk-Anwendungen, 01.03. - 04.03.11 in Aachen

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzte Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.190,-- zzgl. MwSt.

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 14.03. - 16.03.11 in München

Dieses Seminar behandelt die Projektschritte, Einsatz- und Migrations-Szenarien, einsetzbare Basis-Technologien, Komponenten und erweiterte TK-Anwendungen, Bewertungskriterien für eine TK-Lösung und gibt eine Übersicht über den bestehenden TK-Markt etablierter Hersteller wie Alcatel-Lucent, Avaya, Cisco, Nortel und Siemens aber auch des Newcomers Microsoft.

Preis: € 1.890,-- zzgl. MwSt.

Microsoft Unified Infrastructure 2010 - Produktivität pur und Tod der TK-Anlage?, 14.03. - 15.03.11 in München

In diesem 2-tägigen Seminar informieren wir Sie über die zahlreichen Neuerungen von Sharepoint 2010, Exchange 2010 und Lync Server 2010, gehen auf die Voraussetzungen und Abhängigkeiten ein und zeigen Migrationswege auf. Dazu gehören die unterschiedlichen Leistungsmerkmale, die Anbindung an bestehende Telefonanlagen oder Trunk-Lösungen ebenso wie Sicherheitsaspekte, Erweiterungsmöglichkeiten, Lizenz-Modelle und vieles andere mehr. Wir bieten Ihnen einen Einblick in den Nutzen dieser umfassend überarbeiteten Lösungen für Ihre IT-Strategie.

Preis: € 1.490,-- zzgl. MwSt.

WAN: Aktuelle Technologie und Erfahrungen aus Ausschreibungen, 14.03. - 15.03.11 in München

Das Programm des Seminars „WAN: Neue Verfahren und Erfahrungen aus Ausschreibungen“ bietet wertvolle Tipps und Empfehlungen sowohl zu technischen als auch zu organisatorischen Aspekten der Konzeption, der Planung, der Ausschreibung und des Betriebs von Wide Area Networks. Die Referenten des Seminars blicken auf langjährige Erfahrungen im WAN-Bereich zurück und vermitteln im Seminar Erkenntnisse aus Dutzenden von Projekten, in denen Wide Area Networks entworfen, ausgeschrieben und optimiert wurden. Der große Erfahrungsschatz von ComConsult bei der Lösung von Problemen und der Lokalisierung von Fehlern in standortübergreifenden Netzen fließt ebenso in das Seminarprogramm ein wie die Expertise der Referenten bei der Gestaltung sinnvoller Service Level Agreements (SLA) im WAN-Betrieb.

Preis: € 1.490,-- zzgl. MwSt.

Wireless LAN professionell, 14.03. - 16.03.11 in München

Dieses Seminar vermittelt den aktuellen Stand der WLAN-Technik und zeigt die in der Praxis verwendeten Methoden für Aufbau, LAN-Integration, Betrieb und Optimierung von WLANs im Enterprise-Bereich auf. Die verschiedenen WLAN-Varianten werden analysiert, Markt- und Produktsituation werden bewertet, und Empfehlungen für eine optimale Auswahl werden gegeben.

Preis: € 1.890,-- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
11.04. - 15.04.11 in Aachen
12.09. - 16.09.11 in Aachen
05.12. - 09.12.11 in Aachen

TCP/IP und SNMP
14.02. - 18.02.11 in Berlin
09.05. - 13.05.11 in Königswinter
26.09. - 30.09.11 in Stuttgart

Internetworking
21.02. - 25.02.11 in Aachen
16.05. - 20.05.11 in Aachen
17.10. - 21.10.11 in Aachen

Paketpreis für alle drei Seminare € 6.720,-- zzgl. MwSt. (Einzelpreise: je € 2.490,--)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
17.05. - 20.05.11 in Aachen
20.09. - 23.09.11 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
01.03. - 04.03.11 in Aachen
28.06. - 01.07.11 in Aachen
18.10. - 21.10.11 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- zzgl. MwSt.
(Seminar-Einzelpreis € 2.290,--, mit Prüfung € 2.470,--)

ComConsult Certified Voice Engineer

Session Initiation Protocol-Basis-Technologie der IP-Telefonie
28.03. - 30.03.11 in Bonn
27.06. - 29.06.11 in Hamburg
14.11. -16.11.11 in Bonn

Sicherheitsmechanismen für Voice over IP
21.03. - 22.03.11 in Stuttgart
04.07. - 05.07.11 in Nürnberg
17.11. - 18.11.11 in Aachen

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
14.03. - 16.03.11 in München
06.06. - 08.06.11 in Nürnberg
26.09. - 28.09.11 in Stuttgart
28.11. - 30.11.11 in Köln

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.740,-- zzgl. MwSt. statt € 5.270,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 1.090,-- zzgl. MwSt. statt € 1.490,-- zzgl. MwSt.

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
28.02. - 01.03.11 in Aachen
23.05. - 24.05.11 in Königswinter
10.10. - 11.10.11 in Berlin

ComConsult Zertifizierter Projektleiter

Projektmanagement I: Projekte aus IT und Kommunikationstechnik leiten und organisieren
28.03. - 01.04.11 in Aachen
17.10. - 21.10.11 in Aachen

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Teams führen
02.05. - 06.05.11 in Köln
14.11. - 18.11.11 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.480,-- zzgl. MwSt. (Einzelpreise: € 2.490,--)

Impressum

Verlag:
ComConsult Technology Information Ltd.
ComConsult Research
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research