

SAN Grundlagen / Design

Joachim Meurer Brocade
Ralf Szczepanski EMC

Presse

- ⇒ 2 Artikel aus der Computer Zeitung Nr. 40 vom 30. September 2003 Seite 21

Geräteinteroperabilität ist weitgehend hergestellt – Security-Themen geraten in den Blickpunkt

Das Storage Networking ist gereift

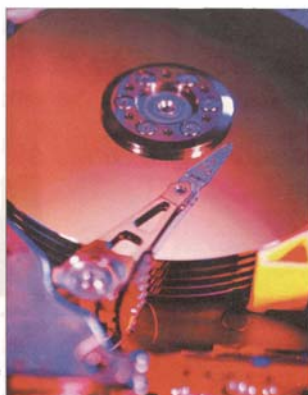
Auf Hardwareebene ist die Speicher-Netzwerk-Infrastruktur erwachsen geworden. Damit sich wirtschaftliche Vorteile daraus ziehen lassen, sind jetzt Fragen wie die Sicherheit und zentrales Management zu lösen. Vor der Investitionsrückhaltung der Unternehmen sind im vergangenen Jahr auch die wachstumsverwöhnten Speichernetzspezialisten nicht verschont geblieben: Weltweit ließen die Umsätze mit SAN-Infrastruktur laut IDC nur um moderate 6,9 Prozent. Erfolgreich seien vorrangig Konsolidierungssysteme wie Brocades

Highend-Switch Silkwood 12000 gewesen, während die Fabric-Switches sogar rückläufige Verkaufszahlen geliefert hätten. Dennoch erwarten die Analysten ein Anziehen der Investitionen in SAN-Equipment, vor allem im unteren Preissegment. Die kostensensitiven Midrange- und Lowend-Bereiche werden einen zunehmenden Anteil an SAN-Neuinstallationen haben“, schätzt IDC-Mann Eric Sheppard. Dazu trägt sicher die Tatsache bei, dass die viel diskutierten Interoperabilitätsprobleme bei Fibre-Channel-Equipment ausgeräumt sind – zumindest was

die Hardware- und Protokollebene betrifft. Auch die Diskussion um Konkurrenztechnologien wie IP-Storage, die kleineren und mittelständischen Anwendern die Entscheidung pro Fibre-Channel-SAN auch nicht unbedingt leichter gemacht hat, ist etwas abgeflaut. Allerdings sind weitere Standardisierungsprozesse nötig. Das gilt für die Managementsoftware – mit dem Bluefin-Projekt sind Schritte in diese Richtung eingeleitet worden – und vor allem für den Security-Bereich. Denn bei weitergehenden Techniken zur Zugriffskontrolle oder Verschlüsselung sind einheitliche Standards noch längst nicht geschaffen.

Virtualisierung hat viele Gesichter

Dennoch rufen Branchenvertreter schon die dritte Phase der SAN-Entwicklung aus, in der es geht, die entsprechende Wertschöpfung aus der Speichernetzung herauszuholen. Einen Schlüssel dafür stellt die Virtualisierung dar. Sie fasst die unternehmensweiten Speicherressourcen zu einem Pool zusammen und ermöglicht erst ein zentrales Management mit dem Ziel effizienter Nutzung der Hardware. Eine Patentlösung ist jedoch nicht in Sicht: Je nach vorliegender Infrastruktur und vorherrschender Speicherdenkweise sind unterschiedliche Wege zu beschreiben –



Wachsende Datenmengen im Unternehmen lassen sich ohne Netzschlüssel auf lange Sicht nicht mehr verwalten. Foto: IBM

oder auch eine Kombination davon: Blockbasierte Virtualisierung à la Datacore und Falconstor oder File-basierte Virtualisierung auf Basis paralleler Dateisysteme wie bei SGI, Adic oder IBMs StorageTank-Projekt. Mit dem Aufkommen intelligenter Switches nach Brocades-Muster stellt sich zudem die Plattformfrage neu.

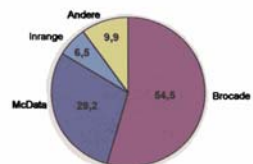
Impulse könnten indes aus dem Wissenschaftsbereich kommen: Projekte wie der Mega-Ring beschleuniger UHC am europäischen Kernforschungszentrum Cern führen zwangsläufig zur Entwicklung entsprechender Infrastrukturkonzepte, ohne die entsprechende Datenmengen schlicht nicht mehr zu behandeln sein werden. fm

KOMMENTAR

Normierung geht in Phase 3

Nach Jahren des Hypes ist die Speichernetzhardware gereift. Die Fibre-Channel-Technik steht als De-facto-Standard da, in den man ruhigen Gewissens investieren kann. Alternativen wie iSCSI – praktisch, ohne Zweifel – lassen den ersten Verheißungen noch keine Taten folgen. Interoperabilitätsprobleme der Switches bereiten den IT-Verantwortlichen kaum noch schlaflose Nächte; ein Blick auf die Marktverteilung relativiert diese Problematik ohnehin. Statt dessen treten die Gespenster des Netzwerkadministrators auf den Plan: Sicherheit im SAN dürfte mit Basistechniken wie Zoning oder LUN-Masking allein kaum zu gewährleisten sein. Spätbestens bei über IP-Bereichen verlinkten Speichernetzinstallationen tun weitergehende Security-Mechanismen Not, sei es nun über Zugriffskontroll-Listen oder kryptografische Methoden. Hier aber kochen die Anbieter oft noch ihr eigenes Süppchen. So wird es darauf ankommen, dass die Normierung in Phase 3 der SAN-Standardisierung ähnlich erfolgreich arbeiten wie sie es bei den Protokollen getan haben und – hoffentlich – bei den Managemententscheidungen tun werden. Frank-Michael Keß

Weltmarkt für Fibre-Channel-Hubs und -Switches nach Umsätzen 2002 (Marktanteile in Prozent)



Quelle: IDC

COMPUTER ZEITUNG 402003hd

Klare Verhältnisse kennzeichnen den Markt für Speichernetze (SAN)-Infrastruktur: Brocade und McData dominieren. Die meisten Spezialisten Inrange, inzwischen Teil von CNT, rangiert auf Rang 3. Den Rest teilen sich Hersteller wie Qlogic, Vixel und Gdataox. /fm

Sicherheit als oberste Speichernetzpflicht

where information lives

Ein ungeschütztes Speichernetz (SAN) ist einer Vielzahl von Bedrohungen ausgesetzt. Sicherheitslösungen umfassen nicht nur technische, sondern auch organisatorische und rechtliche Aspekte. Da in SANs sensitive Daten vorgehalten werden, ist deren Absicherung eine Aufgabe mit erster Priorität. Die größten Gefahren bestehen im unbefugten Serverzugriff, Angriffen über Netzwerke, Missbrauch von Managementapplikationen, fehlerhafter Konfiguration oder Diebstahl von Speichermedien (siehe Kästen). Gegen unbefugten Zugriff eines Servers sind Sicherheitsfunktionen verfügbar, die mithilfe von Access Control Lists den Zugriff auf Speicher- und Switch-Ports oder Logical Devices überwachen. Dies wird als Zoning, Port-Binding be-

wehungsweise LUN-Masking bezeichnet. Zu beachten ist, dass diese Funktionen wiederum anfällig gegen Spoofing – das heißt Adressfälschung – der verwendeten Kennung des Servers ist, etwa eines World Wide Name. Neuentwicklungen für den Zugriffsschutz sind kryptografischer Natur und beinhalten die Authentisierung unterschiedlicher Objekte oder die Verschlüsselung des gesamten Speichermediums auf Blockebene. Switches oder Ports von Switches, Servern und Storage-Geräten können sich gegenseitig authentisieren. Ein zufällig falsch verkabelter Switch kann durch eine Authentisierung rechtzeitig erkannt werden, ebenso wie manipulierte SAN eingefügte Switches oder Server. Sol der Schutz auf jeden Fibre-Channel-FC-Frame oder jedes IP-Paket ausgedeh-

werden, muss die Authentisierung dieser Einheiten erfolgen. Die komplette Verschlüsselung der Logical Devices ist unter Sicherheitsaspekten dem LUN-Masking überlegen. Sie wird durch Hardware in der FC-Fabric realisiert, und alle verwendeten Schlüssel werden dort gespeichert. Auch gegen Diebstahl ist die Verschlüsselung des Speichermediums ein probates Mittel – solange das Kryptografieren selbst nicht ebenfalls gestohlen wird.

Kryptostandards sind in Arbeit

Ein einheitliches Verschlüsselungsstandards wird erfrischend gearbeitet. Für das FC-Protokoll wurde vom T11.3-Forum (www.t11.org) des INCITS-Gremiums vorgeschlagen, das Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) als Standard zu verwenden. Optional kann FCAP (Fibre Channel Authentication Protocol) eingesetzt werden. Führende Switch-Hersteller bieten entsprechende Funktionen an oder arbeiten an ihrer Implementierung. Für IP-Block-Storage-Protokolle hat der IETF-Sicherheitsstandard die Verwendung von ESP (Encap-

sulation Security Payload) vorgeschrieben (ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-ips-security-19.txt), ist einer ähnlichen Lösung für FC wird gearbeitet. Ein IP-Link zwischen zwei SANs kann mit dem Sicherheitsprotokoll IPsec wirkungsvoll abgesichert werden. Technische Herausforderungen stellen jedoch die hohe Übertragungsgeschwindigkeit der Daten und die Anforderungen an eine geringe Verzögerung dar. Für das sichere Management der SAN-Geräte unter Verwendung des Protokolls IP stehen ebenfalls kryptografische Funktionen im Mittelpunkt. Die Nutzerauthentisierung, mit Hilfe der Hardware, schützt vor Missbrauch der Managementanwendung. Die unterschiedlichen Komponenten des Managementsystems (Client, Server, Agent) müssen sich ebenfalls gegenseitig authentisieren, zum Beispiel via SSL-Verschlüsselung. Das Managementprotokoll SNMP sollte in der Version 3 verwendet und Telnet durch SSH ersetzt werden. Die Absicherung von SANs ist eine sehr anspruchsvolle Aufgabe, die über die hier behandelten technischen Aspekte hinaus auch zahlreiche orga-

nisatorische und rechtliche Fragen aufwirft. Externe Dienstleister können hier wertvolle Hilfe leisten. Unterstützung kommt auch von der Industrievereinigung SNA (www.sna.org), die ein Modell für die Klassifizierung von SAN-Bedrohungen erarbeitet hat. Das SSF (Storage Security Industry Forum; www.sna.org/ssf), ein

ne Gruppe innerhalb der SNA, vereinigt Hersteller, die Sicherheitsfunktionen im Bereich Storage Networking anbieten, und unterstützt deren Lösungen. Die SNA Europe (www.snaeurope.org) bietet zudem ein Tutorial über Storage Network Security an. Christina Heibig, Beraterin, Secures Networks AG/fm

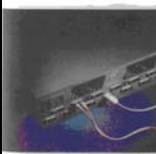
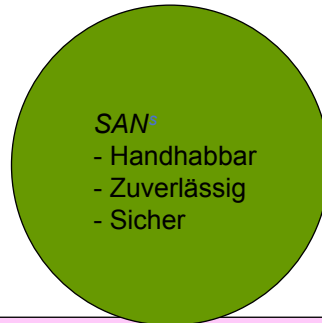
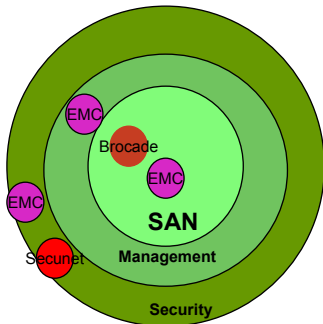


Foto: Qlogic

SAN^s aus Kundensicht

Herstellersicht

Systemintegrator- und Kundensicht



EMC und secunet bieten dem Systemintegrator bzw. dem Kunden ein sicheres SAN

EMC²
where information lives