MAGAZIN

07
2015

Sonderdruck für NetApp

NetApp

Rainer Huttenloher
Herausgeber
rhh@oberland.net

Einmal Voll-Backup und dann „incremental FOREVER“

Viele Vorteile zeichnen das Konzept „Backup as a Service“ (BaaS) aus. NetApp hat für seinen BaaS-Ansatz Partner zertifiziert, die diese Dienstleistung aus deutschen Rechenzentren heraus anbieten. Doch welche Aspekte sind beim Umstieg zu beachten und wie wird im Notfall verfahren. Uwe Jockel, Business Development Manager für den Bereich Service Provider & Cloud Services Deutschland, gibt Antworten auf die drängendsten Fragen.

Viele Unternehmen haben erkannt, dass ein Konzept wie „Backup as a Service“ mehr Sicherheit für ihre Daten bringt. Doch das ist nicht der einzige Vorteil: Dieses Konzept spart dazu noch die Kosten und löst Kapazitätsprobleme. Doch speziell im Mittelstand steht diesem Ansatz noch ein gewichtiger Grund entgegen: Viele Unternehmen müssen bei ihren Datenbeständen spezielle Anforderungen beachten – die kritischen Daten müssen im Inland gespeichert sein. Diese Forderungen bestehen seitens des Gesetzgebers aber auch aufgrund von bestimmten Vorgaben, die einzelne Branchen berücksichtigen müssen.

Hier setzt die Lösung „Backup as a Service“ (BaaS) an, für die NetApp einige seiner Partner zertifiziert hat. Sie übernehmen die externe Datensicherung auf NetApp-basierten Systemen in einem deutschen Rechenzentrum. Interessant ist zum einen die „On Demand“-Komponente: Es ist nur mehr für den Speicherplatz zu bezahlen, den eine Firma auch wirklich nutzt. Dabei kommen die effizienten Backup-Technologien von NetApp zum Einsatz. Experten bei den NetApp-Partnern übernehmen dabei den gesamten Backup-Workload und die damit verbundene Verantwortung. Ein Anwenderunternehmen kann sich komplett auf das eigene Kerngeschäft konzentrieren und das Thema Backup/Recovery vollständig auslagern. Dieser Backup-Service steht nicht nur für Unternehmen zur Verfügung, die bereits im eigenen Haus NetApp-Lösungen verwenden. Er kann auch in Verbindung mit Systemen anderer Hersteller genutzt werden.

Damit das Umschalten vom Backup/Recovery in den eigenen Räumen auf BaaS funktioniert, müssen zuerst die Daten komplett überspielt werden – die sogenannte Erstsicherung. Das kann Probleme bereiten, vor allem wenn ein Unternehmen nur über eine vergleichsweise geringe Bandbreite bei der Internet-Anbindung verfügt. Laut Uwe Jockel, Business Development Manager für den Bereich Service Provider & Cloud Services Deutschland, ist die Problemlösung im Falle von BaaS von Partner zu Partner unterschiedlich. Dabei können von sicheren Transportwegen eines dedizierten Storage Devices bis zur verschlüsselten externen Festplatte alle Optionen ins Spiel kommen. Auf jeden Fall haben alle zertifizierten Partner passende Angebote in ihrem Programm.

Bild 1. Made in Germany: NetApp-Partner bieten zertifizierten „Backup as a Service“. Quelle: NetApp

Wer bereits eine eigene Backup-/Recovery-Lösung betreibt, der steht vor der Frage, wie er seine Daten gesichert bekommt. Muss er dazu bei BaaS neue Software auf seinen Server installieren, und was kann er von seiner bestehenden Backup-Recovery-Umgebung nutzen? Hier gibt es laut Jockel diverse Alternativen. Ziel von allen Partnern sei es, die bestehende Backup-Umgebung zu nutzen. Hierzu muss die individuelle Umgebung betrachtet werden. Zum besseren Verständnis skizziert Jockel dazu drei Szenarien.

Der Anwender hat bereits NetApp im Einsatz und nutzt NetApp-Mechanismen, wie etwa SnapMirror und SnapVault, für seine Backup-Anforderungen. Dann wird im Grunde genommen nur das Ziel – also das entsprechende Rechenzentrum eines Serviceproviders – geändert und die Daten über den betreffenden NetApp-Mechanismus dorthin repliziert. Das hört sich sehr einfach an, ist aber natürlich technisch nicht so einfach. Hier gibt es Partner, wie zum Beispiel teamix aus Nürnberg (u. a. Star Reseller Partner), die aus ihrem NetApp-Know-how eine sehr intelligente Lösung entwickelt haben, erklärt Jockel. Sie spiegeln über eine gesicherte Verbindung eine NetApp-Instanz aus Ihrem eigenen Rechenzentrum in die Netzwerkumgebung des Anwenderunternehmens und dort lässt sich diese dann wie eine „eigene“ NetApp-Maschine verwenden.

Das Anwenderunternehmen hat keine NetApp-basierte Lösung im Einsatz und setzt dabei aber eine Backup-Software ein, die von NetApp unterstützt wird. Dann müssen beim Anwender vor Ort die entsprechenden Prozesse etabliert werden, um ein weiteres externes Ziel für die Backup-Daten festzulegen. Hierzu haben alle Serviceprovider die entsprechende Expertise und Lösungsangebote im Programm.

Das Anwenderunternehmen hat keine NetApp-Lösung im Einsatz und verfügt auch über keine Backup-Software, die mit NetApp Data ONTAP sprechen kann, die aber mit dem NetApp-Produkt AltaVault zusammenspielt. Dann lässt sich über diese Weise eine Beziehung auf den Cloud Storage des Serviceproviders herstellen. Als Zusatznutzen bekommt der Anwender dann noch alle Funktionalitäten von AltaVault: Verschlüsselung, Deduplizierung und Komprimierung, lokaler Cache von Backup Daten, sowie den automatisierten Datentransfer in die gewünschte Cloud.

Das Thema Sicherheit der Daten bei BaaS spielt in der Konzeption eine gewichtige Rolle: Bei den Übertragungen, sei es die erste Übertragung, oder die regelmäßigen Sicherungen oder auch beim Zurückspielen im Falle eines Recoverys, sind die Daten nach Aussage von Jockel absolut sicher. Wenn eine besonders hohe Sicherheitsstufe gewünscht ist, werden dies die BaaS-Anbieter mit dem Kunden besprechen und eine Lösung dafür anbieten.

Bei der Übertragung selbst kommt zudem Verschlüsselung zum Einsatz. Zum einen erfolgt das über die eingesetzte Backup-Software (sie bietet in den meisten Fällen bereits eine verschlüsselte Datenübertragung), zum anderen über vom BaaS Partner eigens dafür eingesetzte Softwarelösungen.

Ob für die jeweilige Sicherungssoftware zusätzliche Agenten nötig sind, hängt ebenfalls von der Lösung des jeweiligen Serviceproviders ab. NetApp gibt für das BaaS-Konzept grundsätzlich keine Architektur vor und prüft beim Backup Service vor allem die Datensicherheit, die nachgelagerte Storage-Architektur und Backup-Kompetenz. Allerdings ist zum Beispiel beim NetApp-Partner matrix technology eine Backup-Software von asigra in Einsatz. Sie gilt im internationalen SP Umfeld als sehr verbreitet und deckt ein breites Anwendungsfeld – bis zu mobilen Endgeräten – ab, arbeitet dabei noch zusätzlich agenten-

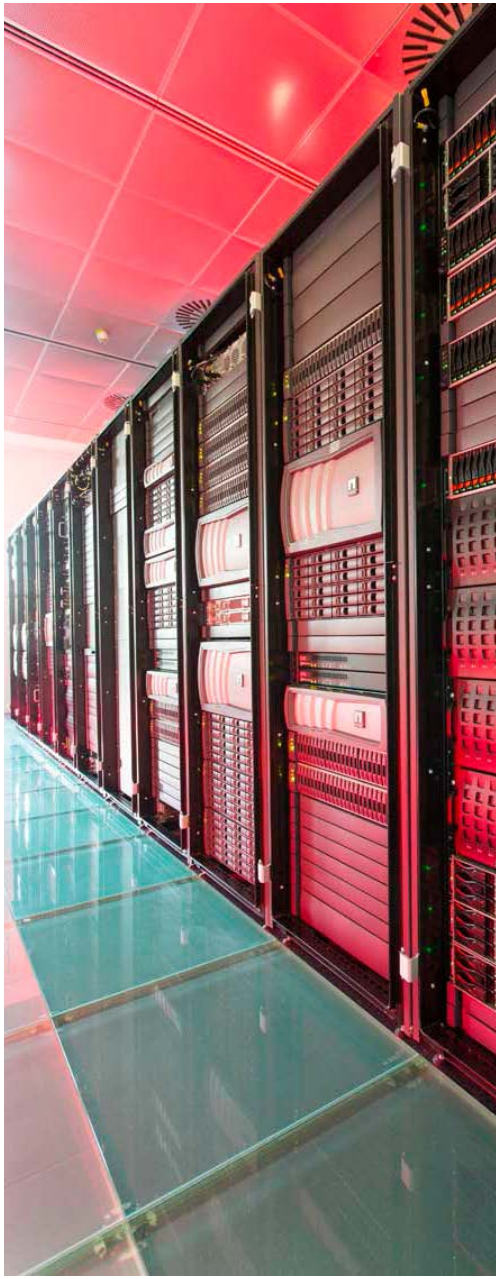

Bild 2. Umschalten aus BaaS. Quelle: NetApp

los. Zudem ist diese Software über einfache Mechanismen zu installieren. Es stellt sich, so Jockel, aber immer die Frage, ob ein Anwenderunternehmen an existenten Backup Strukturen etwas ändern möchte, oder man ein bestehendes Szenario um „die Cloud“ ergänzen möchte.

In Bezug auf die Spezifikationen (Betriebssystemversionen, Virtualisierungs-Plattformen, Applikationen wie ERP-Systeme, Datenbanken) an die zu sichernden Systeme (Windows, Linux, PowerLinux, andere Unix-Derivate) werden diese Parameter nicht durch NetApp, sondern durch die eingesetzte Backup-Software vorgegeben. Grundsätzlich gebe es dabei, so Jockel, nur wenig Einschränkungen. Denn „Backup“ erfüllt in aller Regel nur eine nachgelagerte Funktion, und die gängigen Backup-Softwareprodukte unterstützen alle Standardsysteme. Insbesondere in virtualisierten Umgebungen sollte dies kein Problem sein, da es im professionellem Bereich quasi zwei Defacto-Standards gibt: VMware mit vSphere und Microsoft mit der Plattform Hyper-V.

Sollte bereits NetApp Data ONTAP Technologie im Einsatz sein, können die bekannten NetApp-Replizierungsoptionen SnapVault und SnapMirror zum Einsatz kommen und somit alle Vorteile der NetApp Data ONTAP integrierten Datensicherung angewendet werden. Möchte ein Anwenderunternehmen seine eigenen, lokalen Medien wie etwa eigene Bandlaufwerke, Wechselmedien, Storage-Systeme oder externe Festplatten in das Konzept mit einbinden, dann steht auch diese Option offen. Bandlaufwerke und Wechselmedien sollten zwar mit dem Backup in die Cloud überflüssig sein, doch bei Unternehmen können andere Gründe dafür sprechen. Die Storage-Systeme und Festplatten bei einem Unternehmen sollten bereits in eine lokale Backup-Strategie eingebunden sein. Mit dem Cloud Backup gewinnt man den zweiten Standort hinzu und kann somit die Anforderung an ein ausgelagertes Backup erfüllen.

Hat ein Unternehmen bereits ein erprobtes Sicherheitskonzept in Betrieb ,wie etwa lokal installierte Backup-Software plus Agenten auf den Servern mit lokalen Bandlaufwerke oder Wechselmedien, dann kann all dies bestehen bleiben. „Backup in die Cloud“ ersetzt nicht unbedingt eine lokale Backup-Strategie. Sollte dies vom Kunden jedoch explizit gewünscht sein (sprich wenn er das Thema Backup/Recovery komplett auslagern möchte), kann natürlich ein neues Backup/Recovery-Konzept erstellt werden. Bandlaufwerke, Wechselmedien, etc. können dann bei einem reinen Backup in die Cloud entfallen.

Denn laut Jockel lohnt es sich immer, die bisherige, lokale Backup-Richtlinie parallel zu BaaS zu betreiben. In diesem Fall handelt es sich beim Cloud-Backup um eine zusätzliche Sicherung. In den meisten Fällen erweist es sich als nachlässig – wenn nicht sogar als absolut geschäftsgefährdend, die Daten an einem Standort zu sichern. Denn wenn an diesem Standort ein Brand, Wasserschaden oder anderes elementares Ereignis eintritt, ist der Fortbestand des Geschäftsbetriebes gefährdet. Sollte BaaS als primäres Backup-Ziel gewählt werden, muss der IT-Verantwortliche aber genau auf die Bandbreiten für Wiederherstellungszeiten achten.

Wenn bei einer BaaS-Konstruktion ein Anwender versehentlich Daten gelöscht hat, steht die Frage im Raum, ob die Anwender ihre Daten selbst wiederherstellen können. Das hängt, so Jockel, vom jeweiligen BaaS-Partner und seiner Lösung (Sicherungssoftware) ab. Sollte die Selbstwiederherstellung nicht möglich sein, würde dies über ein Serviceticket beim BaaS-Partner geregelt werden, da ein Backup eine Sicherung gegen Verlust und nicht ein „Use Medium“ für Anwenderfehler ist.

Nach einem eventuellen Datenverlust auf dem Server aufgrund von Hardwarefehlern beim Anwenderunternehmen wird die Wiederherstellung über den BaaS-Provider angestoßen. Einen Datenverlust aufgrund von Hardwarefehlern beim BaaS-Provider schließt Jockel aus, dazu gebe es entsprechende Vorgaben an die Ausfallsicherheit im Rechenzentrum des Serviceproviders.

Ein weiteres Problem bei der Wiederherstellung ist die Zeitdauer, bis die Daten wieder auf dem Produktivsystemen des Anwenderunternehmens liegen. Hier erweist sich Backup in die Cloud vom Prinzip her als nichts anderes als ein lokales Backup. Laut Herr Jockel ist die Vereinbarung der Servicelevel und Wiederherstellungszeiten mit dem BaaS-Partner der essentielle Bestandteil des Vertrages. Bei den Wiederherstellungszeiten ist die Bandbreite für die Anbindung an den BaaS-Provider zu beachten. Wenn es um die Frage nach den sinnvollen Backup-Konzepten geht, macht laut Jockel bei BaaS lediglich inkrementell Sinn: „Alles andere ist zu kostspielig und nicht Stand der Technik – ein Full Backup zu Beginn und dann immerzu inkrementell.“

Rainer Huttenloher