

Datensicherung für heterogene Netze

Dr. Götz Güttich

Arkeia Network Backup unterstützt nach Angaben des Herstellers 150 verschiedene Plattformen und bringt Agenten für die gängigsten Datenbanken, Applikationen sowie virtuellen Umgebungen mit. Zu den neuen Funktionen der Version 9 gehört unter anderem die so genannte progressive Deduplizierung, die redundante Daten bei der Datensicherung eliminieren soll, um so Zeit und Speicherplatz zu sparen. IAIT hat den Funktionsumfang der Backuplösung und das Deduplizierungsfeature im Testlabor genau unter die Lupe genommen.

Das Backupprodukt von Arkeia besteht aus mehreren Komponenten: Auf den zu sichernden Rechnern laufen Agenten, die die gesicherten Daten an den Backup-Server weiter geben, welcher sie wiederum an den Medienserver weiterreicht, der sie dann auf Speichermedien wie Bandlaufwerken, virtuellen Bandlaufwerken oder Festplatten ablegt. Es ist auch möglich, Backup-Daten über das LAN oder das WAN automatisch auf Replikationsserver zu übertragen. Alle Daten lassen sich jederzeit über eine AES-256-Verschlüsselung absichern. Verwaltet wird das Produkt über ein Browser-basiertes Interface.

Dieser modulare Ansatz sorgt dafür, dass Arkeia Network Backup sich problemlos an Umgebungen unterschiedlicher Art und Größe anpasst. Kleinere Organisationen richten einen Backup Server mit dem Konfigurationsinterface ein, der auch gleich als Medienserver zum Einsatz kommt und installieren dann auf ihrer Rechnern im LAN die Agenten. Danach ist die Backupumgebung bereit für die tägliche Arbeit. Bei großen Unternehmen kann es im Gegensatz dazu Sinn ergeben, einen zentralen Administrationsserver und mehrere Backup- sowie Replication-Ser-



ver aufzusetzen und dann über Agenten tausende von Client-Systemen zu sichern.

Beim Planen der Umgebung ist es lediglich wichtig zu wissen, dass die Serversoftware nur für Linux zur Verfügung steht. Die Windows-Komponente der Arkeia-Lösung lässt sich lediglich als Agent und als Medienserver nutzen. Für Datenbanken und Anwendungen stehen gesonderte Hot-

Backup-Agenten zur Verfügung und die Sicherung virtueller Installationen läuft über einen separaten Agenten für virtuelle Umgebungen.

Die progressive Deduplizierung, die Arkeia Network Backup seit der Version 9 unterstützt, hilft darüber hinaus beim Reduzieren der Datenbestände – und zwar nach Angaben des Herstellers um bis zu 40 Prozent.

Hintergründe zur progressiven Deduplizierung

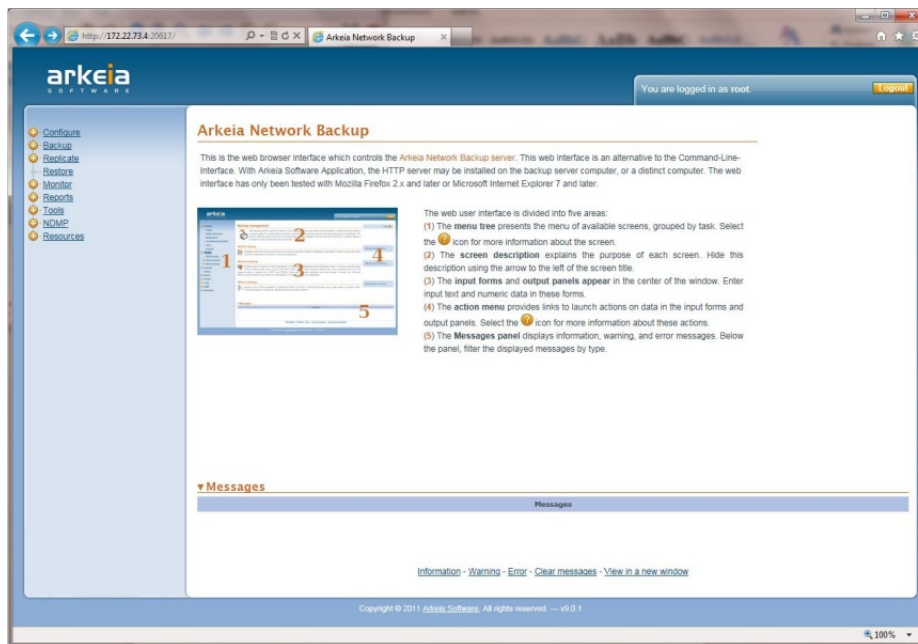
Die eben genannte progressive Deduplizierungsfunktion setzt zum Verringern der zu sichernden Datenmenge zwei unterschiedliche Techniken ein. Zuerst scannt die Software alle Blöcke einer bestimmten Größe in einer Datei und rückt dabei immer um ein Byte vor. Danach kommt ein Algorithmus zum Einsatz, um die Blöcke zu identifizieren, die mit bereits bekannten Blöcken übereinstimmen. Zum

arbeit mit der Community mehrerer Millionen Dateien untersucht und aufgrund der dabei gewonnenen Erkenntnisse für hunderte von Dateitypen die optimale Blockgröße ermittelt.

Die genannte Funktion eignet sich besonders gut für den Einsatz in virtuellen Umgebungen: In Installationen mit Hypervisor fallen immer viele redundante Dateien an, da jede virtuelle Maschine ihre eigene Betriebssystemkopie und ihre eigenen Anwen-

zen. Da die zu sichernden Files dem System nach dem ersten Backup-Lauf bekannt sind, verringert sich die Zahl der neu zu speichernden Informationen mit jedem zusätzlichen Backup-Zyklus, so dass das Verhältnis zwischen den tatsächlich vorhandenen und den gesicherten Bytes immer günstiger wird. Das spart ebenfalls Speicherplatz und Zeit.

Im Gegensatz zu klassischen Deduplizierungsmethoden – wie beispielsweise der Fixed-Block-Deduplizierung – ermöglicht die progressive Deduplizierung auch das Hinzufügen von Daten, Datenanhängen und Datenänderungen zu einzelnen Dateien und arbeitet deswegen sehr effizient. Die neue Funktion bringt dann besonders viel, wenn die Backupsoftware die Deduplizierung auf Clientseite durchführt. In diesem Fall verringert sich die Datenmenge vor der Übertragung der zu sichernden Informationen über das Netz, was das Backupfenster verkleinert und die Netzlast senkt.



Das Web-basierte Konfigurationswerkzeug von Arkeia Network Backup begrüßt die Anwender mit einer umfassenden Hilfeseite

Schluss bildet ein weiterer Algorithmus einen Hash-Wert über die möglicherweise übereinstimmenden Daten, um die Übereinstimmung zu verifizieren. Die Größe der Deduplikationsblöcke spielt also eine entscheidende Rolle für die Effizienz der Deduplizierung. Deswegen verwendet Arkeia unterschiedliche Blockgrößen für verschiedene Dateitypen. Eine Textdatei wird mit anderen Blockgrößen dedupliziert als eine Datenbank, ein Image einer virtuellen Maschine oder ein Anwendungsfile. Um hier die größtmögliche Effizienz sicher zu stellen, hat Arkeia in Zusammen-

hängungen vorhält. Das gleiche gilt natürlich auch für Netzwerke mit vielen identischen Clients. Durch die Eliminierung dieser Redundanzen beim Backup – die Software sichert die vorhandenen Daten nur einmal und setzt bei Clients, die die gleichen Informationen vorhalten, lediglich Pointer – laufen die Datensicherungen schneller durch und benötigen weniger Speicherplatz auf den Zielmedien.

Die progressive Deduplizierung bringt auch in Umgebungen, in denen häufig dieselben Daten gesichert werden, einen großen Nut-

Eine weitere wichtige Neuerung von Arkeia Network Backup 9 spielt ebenfalls noch eine Rolle: das zweiphasige Backup. Dieser Ansatz bringt den größten Vorteil in Umgebungen mit vielen kleinen Dateien. In einem solchen Umfeld ist die Zeitspanne zum Übertragen der Files viel geringer als die Zeit, die benötigt wird, um den Katalog auf den aktuellen Stand zu bringen. Das zweiphasige Backup reduziert das Backupfenster nun dadurch, dass es zuerst die zu sichernden Informationen überträgt und dann erst (nach dem Abschluss des eigentlichen Backuplaufs) im Hintergrund den Katalog aktualisiert. Hierbei müssen die Anwender lediglich beachten, dass

Restorevorgänge erst nach dem Abschluss der Anpassung des Katalogs möglich sind, also nicht sofort nach dem Ende des Kopiervorgangs.

Der Test

Im Test installierten wir unseren Backup- und Medienserver auf einem Server unter Centos 5.6, der mit einem AIT-3-Ex-Laufwerk von Sony bestückt war. Auf diesem Server kam auch das Webinterface von Arkeia Network Backup zum Einsatz.

Installation

Vor der Installation des Backup-servers, sind einige Grundvoraussetzungen zu erfüllen. Der Hersteller empfiehlt für Umgebungen, in denen die Deduplizierungsfunktion zum Einsatz kommen soll, eine verhältnismäßig starke Serverhardware, da dieses Feature relativ viel Speicher und Rechenleistung benötigt. Nach Möglichkeit sollte ein Rechner mit einem 64-Bit-Linux, sechs GByte RAM und vier Prozessorkernen Verwendung finden. Zu-

tig, vor der Arkeia-Installation die iptables-Firewall zu stoppen und SELinux in den passiven Modus zu versetzen.

Sobald wir diese vorbereitenden Schritte durchgeführt hatten, installierten wir die Backup-Software und das Webinterface unter Centos mit Hilfe folgender Befehle:

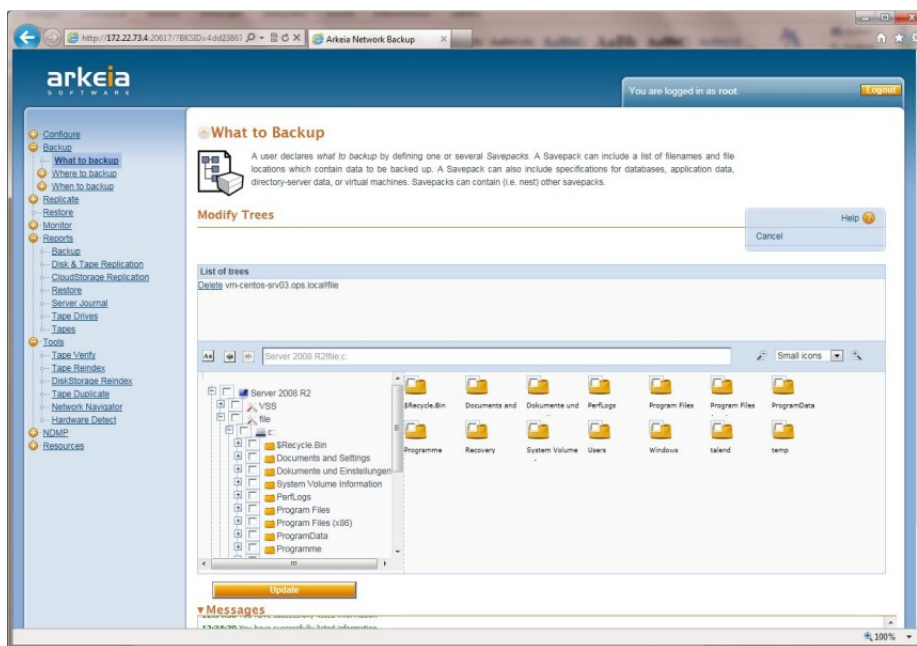
```
rpm -Uvh arkeia.9.0.1_master_ -  
linux.rhel5.0_x86-64.rpm  
rpm -Uvh arkeia.9.0.1_arkwui_ -  
linux.rhel5.0_x86-64.rpm
```

Das Web-Interface

Sofort nach der Installation ist es möglich, über die URL `http://{IP-Adresse oder Name des Backup-Servers}:20617` auf das Web-Interface der Software zuzugreifen. Dieses steht auf Englisch und Französisch zur Verfügung und umfasst neben einem Login-Prompt diverse Links zu Ressourcen, Dokumentation, Support, Knowledge Base, User Forum und ähnlichem.

Der erste Login erfolgt nun über das Default Konto "root" ohne Passwort. Nachdem wir uns angemeldet hatten, landeten wir in einem übersichtlichen Konfigurationswerkzeug, das uns mit einem Willkommensbildschirm begrüßte, der das Interface mit seinem Verwaltungsmenü erklärte.

Generell gilt, dass der Anwender immer wenn er einen Hauptmenüpunkt aus der Menüstruktur selektiert, auf einer Übersichtsseite landet, die ihn darüber informiert, welchen Zweck die darunter liegenden Befehle erfüllen. Im Test empfanden wir diesen Ansatz als sehr positiv, da er einen separaten Blick in die Dokumentation wohl in den meisten Fällen überflüssig macht.



Die Auswahl der zu sichernden Dateien läuft über einen übersichtlichen Browser ab

Danach fügten wir unserer Backupumgebung diverse Clients unter Linux, MacOS X, Solaris 10 sowie Windows XP, Windows Server 2003 R2, Windows 7 und Windows Server 2008 R2 hinzu und sicherten Daten aus diesen Umgebungen auf Band beziehungsweise auf ein Festplattenstora in unserem Server.

Dabei führten wir die Sicherungen jeweils einmal mit und einmal ohne die progressive Deduplizierung durch und überprüften dann die Unterschiede bei der Dateigröße auf den Zielmedien.

sätzlich müssen die Administratoren vor dem Aufruf des Setups unter Linux die IPC-Parameter anpassen, genügend Shared Memory bereitstellen, die Tapedrives oder Libraries einrichten und sicherstellen, dass der Hostname in der richtigen Form in der Datei `/etc/hosts` eingetragen wurde. Alle dafür erforderlichen Schritte werden genau im Getting-Started-Guide der Software unter `http://wiki.arkeia.com/mediawiki/index.php/Arkeia_Network_Backup_Version_9.0_Quick_Start_Guide_-_English` erklärt, so dass wir uns hier nicht weiter damit befassen müssen. Genauso ist es wich-

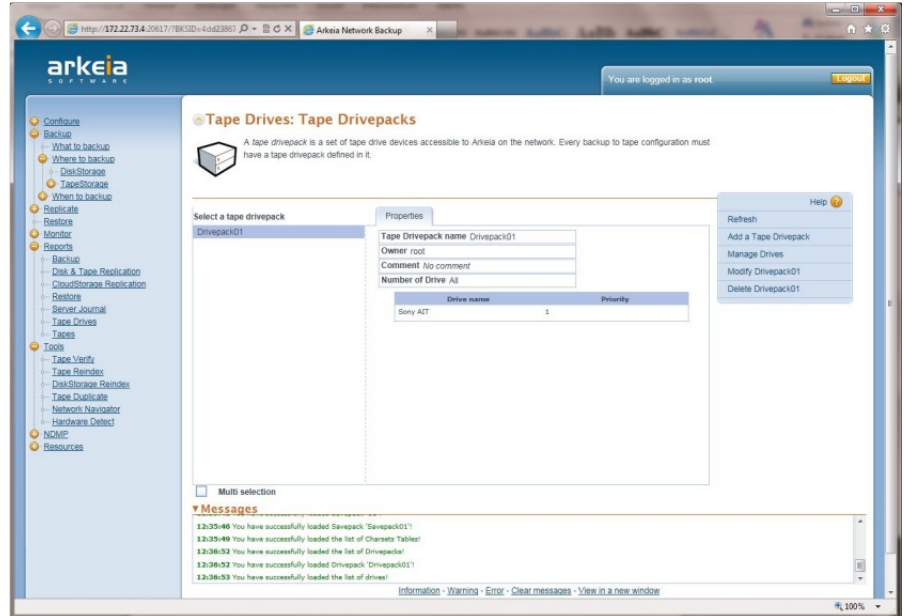
Der Funktionsumfang

Gehen wir jetzt erst einmal auf den Funktionsumfang der Software ein, die sich bei Bedarf übrigens nicht nur über das hier vorgestellte Konfigurationsinterface, sondern auch über die Kommandozeile bedienen lässt. Unter "Configure" haben die zuständigen Mitarbeiter die Option, die im Netz vorhandenen Clients in die Backupumgebung aufzunehmen, um die dort vorhandenen Daten oder bestimmte Anwendungen (wie Datenbanken) sichern zu können. An gleicher Stelle ist es auch möglich, die Verschlüsselung zu konfigurieren, Agenten neu zu starten oder zu entfernen, Ports für die Datenkommunikation zwischen Server und Clients festzulegen und die Log-Konfiguration mit maximaler Log-Größe und Syslog-Level vorzunehmen. Auf ähnliche Weise lassen sich auch Vmware-Server in die Backup-Umgebung aufnehmen und Medienserver einrichten. In unserer Testumgebung ergaben sich dabei keine Probleme. Zusätzlich finden sich innerhalb des Configure-Menüs noch die Benutzerverwaltung und die Cloud Storage Replication. Letztere dient zum Angeben entfernter Backup-Server für Replikationsläufe, während erstere zum Einsatz kommt, um Benutzerkonten für die Backup-Software anzulegen. Diese umfassen nicht nur den Usernamen und das Kennwort, sondern auch E-Mail-Adressen für Alertmeldungen und die Benutzerrechte. Bei den Rechten unterscheidet Arkeia zwischen Administratoren, die alles dürfen, Operatoren, die die lediglich Backups starten und Usern, die nur auf die Restore-Funktion zugreifen können. Die Lizenzverwaltung schließt den Konfigurationspunkt ab. An dieser Stelle trugen wir im Test per Cut-and-Paste unsere Lizen-

zen ein. Dazu müssen die Benutzer bei jeder Lizenz die Felder für Kundenname, Lizenzname, Seriennummer und Checksumme ausfüllen. Wir hatten insgesamt zwölf Lizenzen für verschiedene Funktionen der Lösung wie Exchange-Sicherungen, Active-Directory-Backups, Verschlüsse-

zur Deduplizierung, zum Mediaserver, zu den vorher beziehungsweise nachher auszuführenden Befehlen und ähnlichem.

"Where to Backup" legt im Gegensatz dazu die Speicherziele, also die Bandlaufwerke und Festplattenbereiche fest, die für das



Das Einrichten von Tape Drivepacks stellt über das Management Tool von Arkeia Network Backup kein Problem dar

lung, Disaster Recovery und ähnliches, deswegen nahm die Lizenzierung durchaus etwas Zeit in Anspruch. Es stimmt zwar, dass die zuständigen Mitarbeiter diesen Schritt in der Regel nur einmal durchführen müssen, trotzdem wäre ein einfacherer Weg zum Eintragen der Lizenzen vorzuziehen. Eine Seriennummer pro Teillizenz sollte genügen.

Der nächste Menüpunkt des Web-Interfaces geht gleich "in medias res" und befasst sich mit der Backup-Konfiguration. Unter "What to backup" legen die Anwender so genannte Savepacks an, die die zu sichernden Dateien und Systeminformationen umfassen. Dabei ist es auch möglich, einzelne Ordner oder Files zu selektieren. Die Savepacks enthalten auch Zusatzoptionen, beispielsweise zur Verschlüsselung,

Backup zum Einsatz kommen. Neben Bandlaufwerken unterstützt Arkeia Network Backup auch Direct Attached Storage, SANs und Netzwerkspeicher. Datenreplikationen können über LAN- und WAN-Verbindungen ablaufen. Um Diskspeicher einzusetzen, müssen die Administratoren zunächst das gewünschte Zielverzeichnis mit dem dahin führenden Pfad definieren. Danach legen sie noch weitere Parameter fest, wie beispielsweise die Speicherkapazität, die maximal möglichen gleichzeitigen Zugriffe, die Deduplizierung und die automatische Replikation. Der fertig angelegte Diskspeicher lässt sich dann so genannten Disk Drivepacks hinzufügen, die ihrerseits beim Erstellen der Backup-Jobs als Zielangabe nutzbar sind. Die Definition der Speichermedien läuft also sehr

flexibel ab und es lassen sich Ordner auf verschiedenen Festplatten in einem Disk Drivepack zusammenfassen.

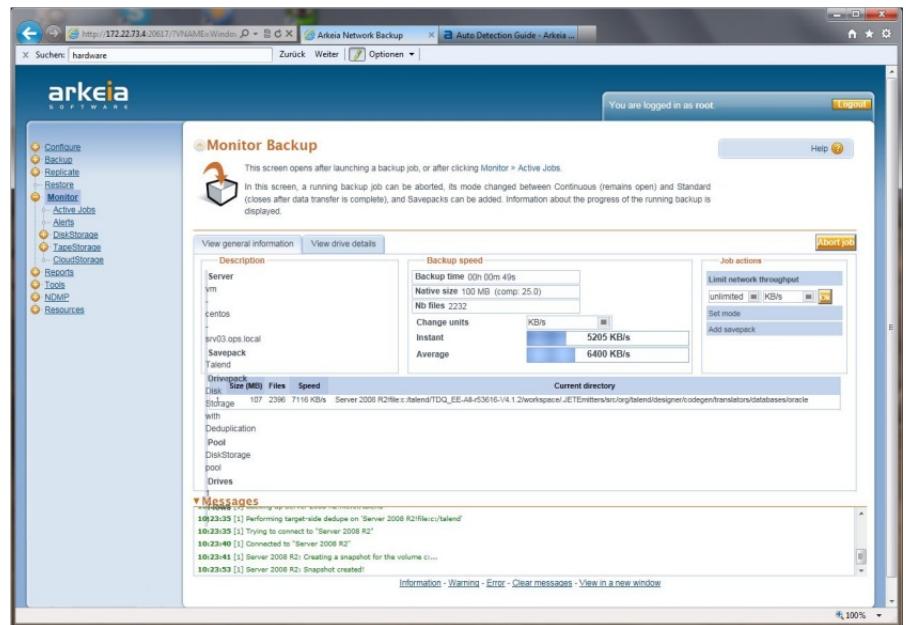
Ähnlich funktioniert die Definition der Bandlaufwerke. Hier stehen Tape Drives und Tape Libraries mit Bändern zur Verfügung, die die IT-Verantwortlichen zu Tape Pools und Tape Drivepacks zusammenfassen können. Die Tape Pools enthalten die Tapes (von denen sich auch mehrere in einem Arbeitsschritt anlegen lassen, was in großen Umgebungen von nicht zu vernachlässigender Bedeutung ist) und die Tape Drivepacks umfassen die zu verwendenden Laufwerke. Alle Elemente kommen dann bei der Definition des Backup-Jobs zum Einsatz, um das Ziel der Datensicherung festzulegen. Im Test ergaben sich dabei keine Probleme.

Der nächste Punkt der Backup-Konfiguration nennt sich "When to Backup". Hier lassen sich sofortige Backup-Läufe starten oder Backups mit einem Zeitplaner automatisch zu bestimmten Terminen einrichten. Es sind auch periodisch wiederkehrende Datensicherungen möglich, die je nach Bedarf als volles, differentielles oder inkrementelles Backup arbeiten.

Entscheidet sich ein Benutzer beispielsweise, ein sofortiges Backup auf Festplatte durchzuführen, so gibt er das zu sichernde Savepack und das als Ziel zu verwendende Disk Drivepack an und legt den Typ des Backups fest (Standard, Continuous). Danach definiert er die Gültigkeitsdauer des Backups (nach deren Ablauf es überschrieben werden kann) und konfiguriert das Alerting. Bei Bedarf ist es nämlich mög-

lich, die Administratoren mit Hilfe von E-Mails über den Backup-Erfolg zu informieren. Zusätzlich lassen sich mit den Backups auch noch andere Funktionen ver-

Unter "Replicate" läuft die Datenreplikation ab. Im Bereich "Where to Replicate" geben die Administratoren das Replikationsziel (Disk, Band oder einen



Die laufenden Jobs lassen sich ohne Probleme im Betrieb überwachen

binden wie beispielsweise automatische Replikationen oder auch VSS-Backups (Volume Shadow Copy Service) unter Windows.

Die Konfiguration der Tape Backups läuft vergleichbar ab, hier geben die zuständigen Mitarbeiter aber zusätzlich noch die Strategie an. Dabei ist es einerseits möglich, die Bänder in Benutzung zunächst vollzuschreiben, andererseits besteht auch die Option, priorisiert neue oder recycelte Tapes einzusetzen. Bei den Backups mit Zeitplaner hilft auf Wunsch ein Wizard beim Anlegen der Jobs, der nach allen relevanten Kriterien wie Zeitpunkt, Drivepack, Savepack und ähnlichem fragt. Im Test empfanden wir diesen Assistenten als sehr hilfreich und konnten ohne Schwierigkeiten binnen kürzester Frist die von uns gewünschten Jobs anlegen. Eine Kalenderübersicht verschafft den Benutzern im Betrieb einen Überblick darüber, wann welche Backup-Jobs geplant sind.

Server in der Cloud – also in LAN oder WAN) an. "When to Replicate" bietet dann die Wahl zwischen sofortiger Disk-, Cloud- oder Tape-Replikation. Alternativ lassen sich Replikationsvorgänge auf andere Server auch mit einem Zeitplaner steuern, dabei existiert wieder ein Wizard, der die Konfiguration der dazu erforderlichen Schritte vereinfacht.

Auch die Datenwiederherstellung läuft über Assistenten ab. Insgesamt stehen vier Wizards zur Verfügung, und zwar erstens zum Zurückspielen von Dateien, Systeminformationen, Datenbanken und Anwendungsdaten, zweitens für Windows VSS Applikationen, drittens für VMware vStorage und viertens für Cloud Replikationen. Die wiederherzustellenden Files lassen sich über eine Navigations- und eine Suchfunktion lokalisieren. Für die Restorevorgänge bietet die Software eine Vielzahl von Optionen: So ist es unter anderem

möglich, Zugriffsrechte oder Linux Extended Attributes wiederherzustellen und eine Overwrite Policy festzulegen. Letztere kann zum Beispiel besagen, dass das System keine Dateien wiederherstellen soll, die im Zielverzeichnis bereits existieren. Alternativ stellt die Software nur die Files wieder her, die seit dem Backup-Datum verändert wurden. In größeren Umgebungen führen die Administratoren die Wiederherstellungsvorgänge sogar unter Angabe bestimmter Medienserver durch. Die zuständigen Mitarbeiter können Restoreläufe bei Bedarf auch mit einer Überprüfung der Checksummenintegrität simulieren, etwa um zu klären, ob die zuvor gesicherten Daten auch lesbar sind. Die Redirection schließlich realisiert die Wiederherstellung der Files an einem anderen Ort. Im Test ergaben sich dabei keine Probleme.

Mit Hilfe der Monitor-Funktionen lassen sich nicht nur die aktiven Backup-, Restore- und Replikations-Jobs überwachen, sondern auch Alarmmeldungen einsehen und konfigurieren, beispielsweise bei Hardwarefehlern, ausgehendem Speicherplatz, Temperaturproblemen und ähnlichem. Der Bereich "Disk Storage" liefert den IT-Verantwortlichen Informationen über die Aktivität der einzelnen Komponenten und umfasst zusätzlich eine Liste der Backup Sets sowie Statistiken zur Deduplizierung. Vergleichbare Übersichten existieren auch zu der Cloud Storage, dem Tapespeicher, dem Tape Status und der Nutzung von Bändern sowie Cleaning Tapes.

Über die Reports-Sektion sehen die Benutzer nicht nur die Berichte ein, sondern mailen bei Bedarf auch Reports an den Eigentümer

des jeweils dazugehörigen Jobs. Es stehen viele unterschiedliche Reporttypen zur Verfügung. In diesem Zusammenhang spielen zuerst einmal die Backup-Reports eine wichtige Rolle. Diese umfassen die verwendeten Medien, die Leistung, die eingesetzten Backup-Typen (Archive, Differential, etc.) und vieles mehr. Die Administratoren sind auch dazu in der Lage, eigene Profile mit Filtern wie "Backup Typ", "Backup Name" oder "Pool used by Backup" anzulegen. Weitere Reports befassen sich mit der Disk- und Tapereplikation, dem Cloud-Speicher, den Restores, den Tape Drives, den Tapes und den Serverereignissen. Es ist also im Betrieb kein Problem, stets über die aktuellen und vergangenen Aktionen des Backup-Systems auf dem Laufenden zu bleiben.

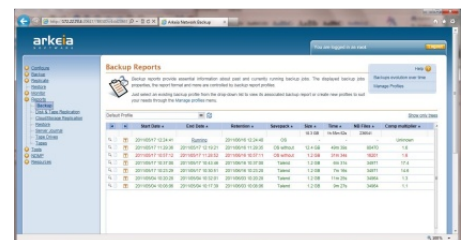
Ebenfalls von Interesse ist die Sektion "Tools". Hier haben die zuständigen Mitarbeiter die Möglichkeit, Bänder zu reindizieren und auf ihre Lesbarkeit hin zu überprüfen. Außerdem lassen sich Bändern duplizieren, die Hardware konfigurieren (diese Funktion wurde zur Inbetriebnahme der Bandlaufwerke, Libraries sowie SAN- und Netzwerkspeicher gedacht) und mit Hilfe des so genannten Network Navigators die im Netz vorhandenen Client Systeme anzeigen. Eine Funktion zum erneuten Indizieren des Festplattenspeichers schließt den Leistungsumfang der Tools ab.

Die letzten beiden Punkte des Konfigurationsmenüs sind schnell erklärt: Unter "NDMP" (Network Data Management Protocol) haben die Administratoren Gelegenheit, Backup- und Restore-Vorgänge ohne Agenten von beziehungsweise zu NDMP-kom-

patiblen NAS-Servern zu konfigurieren (mit NAS-Savepacks, Drivepacks und ähnlichem). Sollten die NAS-Server im LAN kein NDMP unterstützen, so müssen sie als Shares in das Backup-System eingebunden werden. "Resources" umfasst im Gegensatz dazu eine Liste der unterstützten Bandlaufwerke und -typen sowie Links zur Arkeia Download Site, zur Dokumentation, zum Support, zur Knowledge Base, zum Benutzerforum und ähnliches.

Das Einbinden der Clients

Die Client-Systeme lassen sich durch eine manuelle Installation der Agentensoftware auf den betroffenen Rechnern in die Backupumgebung integrieren. Im Test installierten wir den Agenten auf den bereits genannten Rechnern



Arkeia Network Backup generiert umfassende Reports für alle Anwendungsbereiche

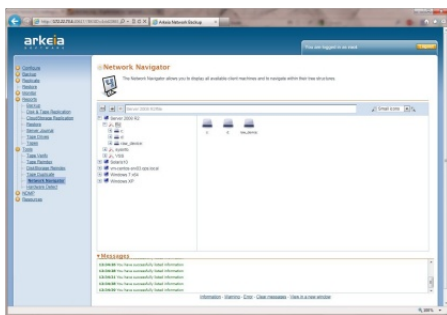
unter Unix und Windows. Unter Windows reicht es dazu, die Installationsdatei zu entpacken, das Setup zu starten und Parameter wie die IP-Adresse oder den Hostnamen des Arkeia-Servers anzugeben. Dazu kommen dann der Name, unter dem der Client auf dem Server geführt werden soll und die Verbindungsmethode (mit Hilfe der IP-Adresse oder des Hostnamens).

Danach läuft die Installation durch und der Client erscheint im Netzwerknavigator des Network Backup Konfigurationsinterfaces und lässt sich auch gleich sichern. Unter Unix ent-

packten wir die Installationsdatei ebenfalls und gaben auf der Kommandozeile vergleichbare Parameter an wie bei der Windows Software, woraufhin die betroffenen Systeme genau wie die Windows-Computer in unserer Backupumgebung erschienen und sofort für Datensicherungen nutzbar waren.

Testergebnisse

Für unseren Test führten wir erst einmal eine Datensicherung eines Windows Clients auf eines unserer AIT-Bandlaufwerke aus



Der "Network Navigator" zeigt die im Netz vorhandenen Systeme mit ihren Ressourcen

und stellten die Daten danach an einem anderen Ort wieder her. Dabei kam es zu keinen Problemen.

Im nächsten Schritt nahmen wir der Deduplizierung unter die Lupe. Dazu erstellten wir verschiedene Backup-Sets mit Nutzerdaten, Betriebssystemdaten und Mediendaten und sicherten diese jeweils in einen Festplattenspeicher mit und einen Festplattenspeicher ohne Deduplizierung. Da wir die Deduplizierung auf dem Server durchführten, konnten wir auch gleich die Last, die der Deduplizierungsvorgang erzeugt, im Auge behalten.

Dabei kamen wir zu folgenden Ergebnissen: Die CPU-Last eines Deduplizierungsjobs ist auf einem 2,4-GHz-Quad-Core-Prozessor etwa drei Mal so hoch, wie die eines Backup Tasks ohne De-

duplizierung. Der Hersteller hat also völlig Recht, wenn er eine leistungsstarke Maschine als Backup-Server empfiehlt. Was die Datenersparnis betrifft, so reduzierte die Deduplizierung das Volumen der Nutzerdaten (die sich selbst nicht ähnlich waren) im ersten Durchlauf um mehr als 26 Prozent. Bei den Mediendaten (die sich auch nicht ähnlich, aber schon hoch komprimiert waren), lag die Reduktion bei null Prozent. Hier wurde der Datenbestand sogar größer, wohl weil das System zusätzliche Informationen in das Backup-Set integrierte. Bei den Betriebssystemdaten schließlich (die auf den einzelnen gesicherten Testrechnern größtenteils identisch waren) betrug die Reduktion im ersten Durchlauf mehr als 54 Prozent.

Nachdem diese Testphase abgeschlossen war, führten wir mit den gleichen Daten noch einen zweiten und dritten Backup-Lauf durch. Dabei kamen wir zu folgenden Ergebnissen: Bei den Nutzerdaten reduzierte Arkeia Network Backup das Volumen im zweiten Durchlauf um mehr als 93 Prozent, im dritten Durchlauf waren es sogar mehr als 94 Prozent. Diese Ergebnisse sind durchaus beeindruckend, man muss aber im Hinterkopf behalten, dass es sich dabei um ideale Laborwerte handelt, da die Quelldaten nach den jeweiligen Backups nicht modifiziert wurden. Der Vollständigkeit halber noch die übrigen Ergebnisse: Bei den Betriebssystemdaten betrug die Reduktion des Datenvolumens im zweiten Backup Lauf 85 Prozent und im dritten 90 Prozent, während bei den Mediendaten im zweiten und dritten Lauf eine Reduktion von 98 Prozent herauskam. Bei diesen Daten veränderte sich allerdings zwischen den

Sicherungen auch kein einziges Bit. Bildet man einen Querschnitt über diese Ergebnisse, so liegen die Angaben des Herstellers, der eine Datenreduktion von 40 Prozent in Aussicht stellt, in manchen Umgebungen durchaus im Bereich des Möglichen.

Zusammenfassung und Fazit

Arkeia Network Backup 9 lässt sich problemlos einrichten und auf einfache Art und Weise benutzen, um in heterogenen Umgebungen Datensicherungen zu erstellen. Die Software bringt alle Funktionen mit, die ein Administrator im Backup-Umfeld benötigt. Das Konfigurationsinterface wurde übersichtlich gestaltet, verfügt über umfassende Hilfestellungen, lässt sich von überall aus bedienen und diverse Assistenten helfen den Benutzern beim Durchführen komplizierterer Aufgaben. Wer sich etwas mit Datensicherung auskennt, wird mit der Arkeia-Lösung sofort klar kommen. Auch die Alerting-, Monitoring- und Reportingfunktionen konnten überzeugen, sorgen sie doch dafür, dass alle betroffenen Mitarbeiter stets über die aktuellen oder auch vergangenen Aktionen der Backup-Umgebung informiert sind. Was die Deduplizierung angeht, so bietet Arkeia ein hocheffizientes Werkzeug zum Reduzieren des zu sichernden Datenvolumens an, das sich nicht nur für Umgebungen mit vielen ähnlichen Clients, sondern auch für Netze eignet, in denen oft die gleichen Daten gesichert werden. Damit gilt das Produkt unter dem Strich als sehr empfehlenswert.

Dr. Götz Güttich leitet das Institut zur Analyse von IT-Komponenten in Korschensbroich. Sein Blog: www.iait.eu.