Vollständige Backup-Lösung aus einer Hand

Dr. Götz Güttich

Mit seinen Backup-Appliances bietet Arcserve Backup-Lösungen der Enterprise-Klasse für Disaster Recovery und Anwendungsverfügbarkeit. Die Produkte bringen nicht nur eine über ein Web-Interface steuerbare, leistungsfähige Backup-Software, sondern auch die Hardware mit, die nötig ist, um effizient Sicherungen durchzuführen. Das schließt den nötigen Speicher mit ein, so dass Administratoren nach der Anschaffung der Appliance und ihrem Einbau ins Rack keine weiteren Komponenten besorgen müssen, um ihre Backup-Strategien umzusetzen. Im Test konnte das Produkt zeigen, was in ihm steckt.

Backup-Appliances eignen sich vor allem für den Einsatz in dezentralen Umgebungen, Niederlassungen oder kleineren Unternehmen. Sie sind aber auch als Primärbackup in größeren Netzen nutzbar. Zu den Deployment-Möglichkeiten der Arcserve Appliances gehören Single-Site-, Primary-Site-, Cross-Site- und Central-Appliance-Site-Szenarien.

Die Appliances arbeiten mit der Backup Software Unified Data Protection (UDP) von Arcserve, die uns zum Testzeitpunkt in der Version 7 vorlag und unter anderem Technologien wie Datenkompression und Deduplizierung unterstützt. Hardwareseitig setzen die Systeme auf Servern von einem Marktführer im Server-Hardwarebereich auf, die Flash-beschleunigten Speicher, große Rechenleistung, Gigabit-Ethernet-Anbindungen und redundante Hardware mitbringen.

Laut Hersteller sollen sich die Appliances in 15 Minuten in Betrieb nehmen lassen. Sie sind nicht nur dazu in der Lage, Sicherungen von physikalischen Maschinen unter Linux und Windows anzulegen, sondern können auch virtuelle Maschinen (VMs) aus den Virtualisierungsumgebungen von Microsoft und Vmware sichern. Darüber hinaus erstellen die Nutzer mit den Produkten unter anderem Backups von Office 365-Umgebungen, Exchange-Servern, SQL-Servern und Oracle-Installationen sowie von Workloads von Amazon AWS und Microsoft Azure. Unterstützt wird auch Nutanix sowie die von der zusätzlich installierbaren Teillösung Arcserve Backup unterstützten Betriebssysteme Solaris, AIX, HP-UX, FreeBSD und IBM System Z Mainframes. Die Datensicherungen selbst erfolgen entweder lokal auf der Appliance oder auf externen Speichern sowie in privaten oder öffentlichen Clouds. Dabei unterstützen die Lösungen die Cloud-Dienste Amazon AWS, Arcserve Cloud (in der sich die

Kunden Speicherplatz für ihre Backups anmieten können), Eucalyptus, Microsoft Azure und Rackspace. Cloud-Speicher sind für die Zusammenarbeit mit der Arcserve-Appliance besonders geeignet, da die dazugehörige Backup-Software eine eigene, sehr effiziente Deduplizierungstechnologie mitbringt, die quellseitig arbeitet und damit den Bedarf an Bandbreite und Cloud-Speicher reduziert.

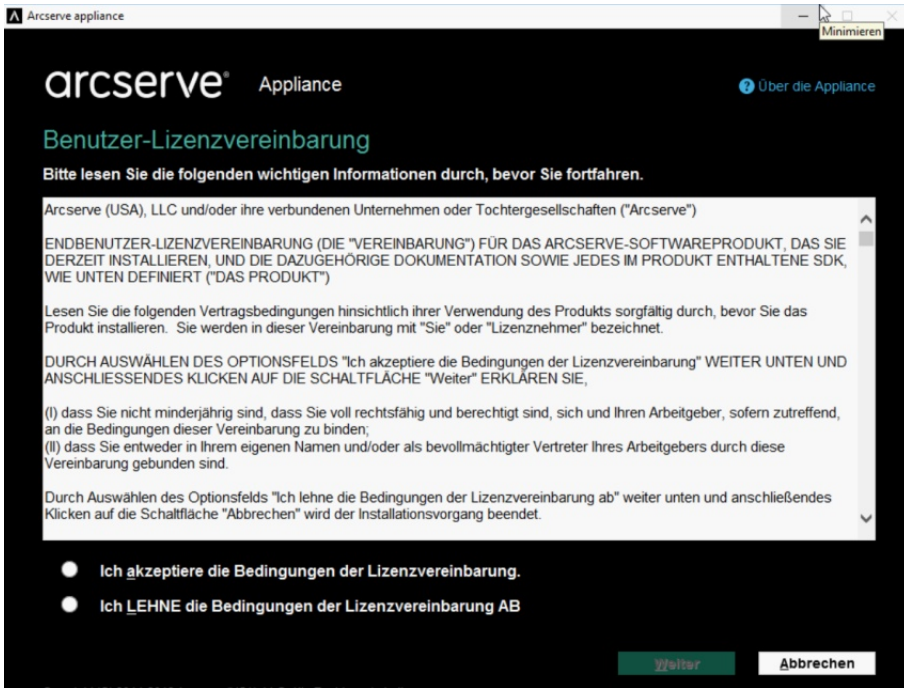
Abgesehen davon gehören Bare Metal-Restores (BMR), Replikationen und granulare Restores mit zum Leistungsumfang der Appliances. Die Lösungen unterstützen zudem Hardware-Snapshots, Hochverfügbarkeit und die Zusammenarbeit mit Bandlaufwerken.

Bei Bedarf lassen sich den Produkten zusätzliche Festplatten hinzufügen, um den Speicherplatz zu erhöhen. Maximal stehen auf einer Appliance bis zu 504 Terabyte Speicher zur Verfügung. Über das zentrale Management-Interface besteht die Möglichkeit, insgesamt bis zu sechs Petabyte an Backup-Daten an einer Stelle zu verwalten. In der Praxis sollen die Appliance eine „Set and Forget"-Strategie ermöglichen. Deswegen erfolgt ihre Konfiguration über Wizards, die ihre Inbetriebnahme und Erstkonfiguration abdecken.

Der Test

Für den Test stellte uns Arcserve eine 9240DR-Appliance mit zwei Intel Xeon Silver 4114 2.2G-CPUs, 192 GByte RAM und einem PERC H730P-RAID-Controller zur Verfügung. Diese kam in zwei Höheneinheiten und bot uns vier Gbit-Ethernet-Schnittstellen für Verbindungen in die zu sichernden Netze und eine zusätzliche Schnittstelle für den Remote-Zugriff auf den Server. Die Speicherkapazität unserer Appliance betrug 72 Terabyte binär, Geräte dieser Bauart lassen sich aber auf bis zu 168 Terabyte Kapazität ausbauen. Der Speicher wurde als RAID-6-Array konfiguriert und es gehörten noch zwei zusätzliche 1,9 Terabyte große SSDs als Cache zum Leistungsumfang, die als RAID-1-Array konfiguriert waren.

Im Test nahmen wir das System in Betrieb, erstellten damit Backups von Linux- und Windows-Systemen, sicherten VMs von Hyper-V-Hosts sowie Vmware ESXi-Hypervisoren und führten eine Datensicherung eines Office 365-Kontos aus. Darüber hinaus ließen wir Restore-Vorgänge laufen und lagerten die Backup-Daten auf externe Devices aus.



Die Erstkonfiguration der Appliance erfolgt über einen Wizard auf der lokalen Konsole des Betriebssystems

Inbetriebnahme

Um die Lösung in Betrieb zu nehmen, verbanden wir die Appliance über ihre regulären Schnittstellen und über das Appliance-Interface mit unserem LAN. Danach versorgten wir sie mit Strom und fuhren sie hoch. Dabei erhielt die Appliance-Schnittstelle eine IP-Adresse von unserem DHCP-Server, die auf einem Display auf der Vorderseite des Geräts angezeigt wurde. Anschließend konnten wir uns über unseren Browser mit dieser IP-Adresse verbinden und auf die Konsole des Systems zugreifen.

Alternativ besteht – da es sich ja um eine Standard Server-Hardware handelt – auch die Option, Tastatur, Maus und Bildschirm direkt an die Appliance anzuschließen und die Erstkonfiguration lokal durchzuführen. Als Betriebssystem kommt auf der Appliance Windows Server 2016 zum Einsatz.

Dieses System fragte nach dem ersten Boot-Vorgang zunächst einmal auf der Konsole nach den zu verwendenden Spracheinstellungen und verlangte von uns, die

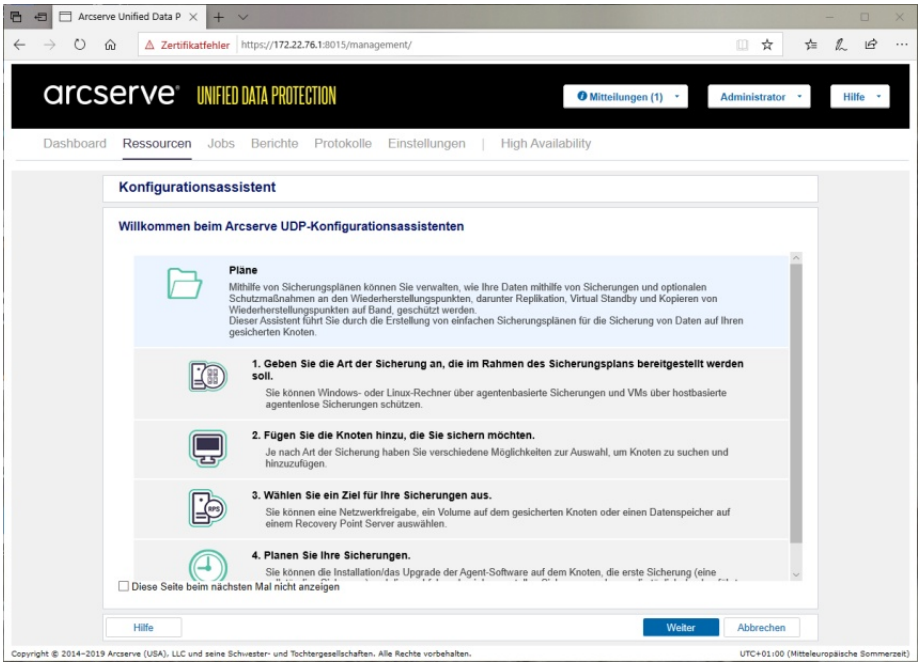
Lizenzbedingungen zu akzeptieren. Danach wurde ein Neustart fällig.

Nach dem Abschluss des zweiten Boot-Vorgangs mussten wir zunächst einmal ein Administratorpasswort festlegen und uns beim System anmelden. Danach startete automatisch der so genannte Arcserve Appliance Wizard.

Dieser zeigt zunächst einmal Lizenzinformationen an und bietet den Administratoren dann die Möglichkeit, den Hostnamen zu ändern und einer Domäne beizutreten. Danach wird wieder ein Neustart fällig.

Nach diesem Reboot konfigurierten wir – ebenfalls mit dem Wizard – die lokalen Schnittstellen des Systems so, dass sie mit einer festen IP-Adresse arbeiteten. Anschließend war die Appliance über die URL https://{IP-Adresse des Systems}:8015 via Browser erreichbar.

Dieser ganze Vorgang zeigt bereits, dass es sich bei der Arcserve Appliance nicht – wie bei vielen anderen Appliance-Angeboten – um ein geschlossenes System handelt, sondern um eine – wie der Hersteller sagt – offene Appliance, bei der die Anwender Zugriff auf das zugrundeliegende Betriebssystem haben. Das eröffnet umfassende Möglichkeiten, das System an die eigenen Anforderungen anzupassen, so sind die Kunden beispielsweise bei Bedarf dazu in der Lage, auf dem Backup-System eine eigene Antivirus-Lösung einzuspielen.



Der UDP-Konfigurationsassistent hilft beim Erstellen eines Backup-Plans

Sicherungspläne

Zum Abschluss der Inbetriebnahme ging es im Test daran, die Backup-Umgebung mit Hilfe des UDP Plan-Konfigurationsassistenten einzurichten. Dieser will zunächst einmal wissen, ob es sich bei der Appliance um eine eigenständige Instanz handelt, oder ob das Produkt von einer anderen Konsole verwaltet werden soll. Da es sich bei uns im Test um das einzige Gerät handelte, wählten wir hier die erste Option. Danach zeigte der Wizard die Speicherkonfiguration an und wollte das Passwort wissen, dass für die Verschlüsselung der Backup-Daten zum Einsatz kommen sollte. Im nächsten Schritt hatten wir dann die Möglichkeit, E-Mail-Benachrichtigungen zu konfigurieren. Das geht entweder für erfolgreiche Jobs, für fehlgeschlagene Jobs oder beides. Anschließend fragt der Assistent nach dem remote Wiederherstellungspunkt-Server. Ein solcher kann beispielsweise Verwendung finden, wenn im Netz bereits ein Backup-Server von Arcserve existiert. Diesen Punkt überprangen wir im Test, da wir ja mit einem Standalone-System arbeiteten.

Jetzt ging es daran, unseren ersten Backup-Plan zu erstellen. Dazu mussten wir zunächst ein Session Passwort angeben, um den Zugriff auf die Session abzusichern. Auf diese Weise ist es unter anderem möglich, nur bestimmten Administratoren zu erlauben, auf bestimmte Backup-Sitzungen zuzugreifen.

Anschließend konnten wir einen oder mehrere zu sichernde Knoten aus unserem Netz auswählen. Das geht – bei Windows-Geräten – über Hostname und beziehungsweise oder IP-Adresse, über die Auswahl der Knoten aus dem Active Directory und über den Import aus vCenter/ESXi- beziehungsweise Hyper-V-Installationen. Im Test wählten wir zu diesem Zeitpunkt zunächst einmal einen physischen Windows 10-Client (Version 1903) aus unserem Active Directory aus, den die Appliance komplett sichern sollte. Der letzte Schritt der Plan-Definition bestand dann aus dem Anlegen eines Zeitplans. Dabei richteten wir das System so ein, dass es zunächst einmal an einem

Dienstag um 12:30 den Backup-Agenten auf dem Zielsystem installierte. In den Folgewochen kam dieser Job dann zum Einsatz, um den genannten Agenten – falls erforderlich – zu aktualisieren.

Darüber hinaus legten wir auch noch fest, dass die täglich durchzuführende Sicherung um 13:00 Uhr starten sollte. Beim ersten Mal sichert das System in diesem Fall den Rechner komplett, die nächsten Sicherungen erfolgen dann inkrementell. Die Benutzer können in diesem Zusammenhang festlegen, wie viele Sicherungspunkte das System vorzuhalten hat. Wird die maximale Zahl der aufzubewahrenden Sicherungspunkte erreicht, so verschmilzt das System automatisch den letzten Sicherungspunkt mit dem Vollbackup. Die Administratoren müssen sich darum nicht kümmern und es ist im Betrieb auch nicht erforderlich, neue Vollbackups anzulegen.

Mit der Definition des Plans ist die Erstkonfiguration abgeschlossen und die Appliance nimmt die Arbeit auf. Anschließend verhielt sich das System im Test wie erwartet, brachte den Agenten zum genannten Zeitpunkt auf unseren Client aus und führte eine halbe Stunde später das Backup durch. Insgesamt nahm die Inbetriebnahme der Appliance mehr Zeit als die versprochenen 15 Minuten in Anspruch, das lag aber hauptsächlich an den mehreren erforderlichen Boot-Vorgängen, die auf der Server-Hardware einige Zeit in Anspruch nahmen. Was die wirkliche effektive Arbeitszeit angeht, dürfte die Aussage des Herstellers mit den 15 Minuten im Prinzip recht genau hinkommen.

Die nächsten Sicherungen

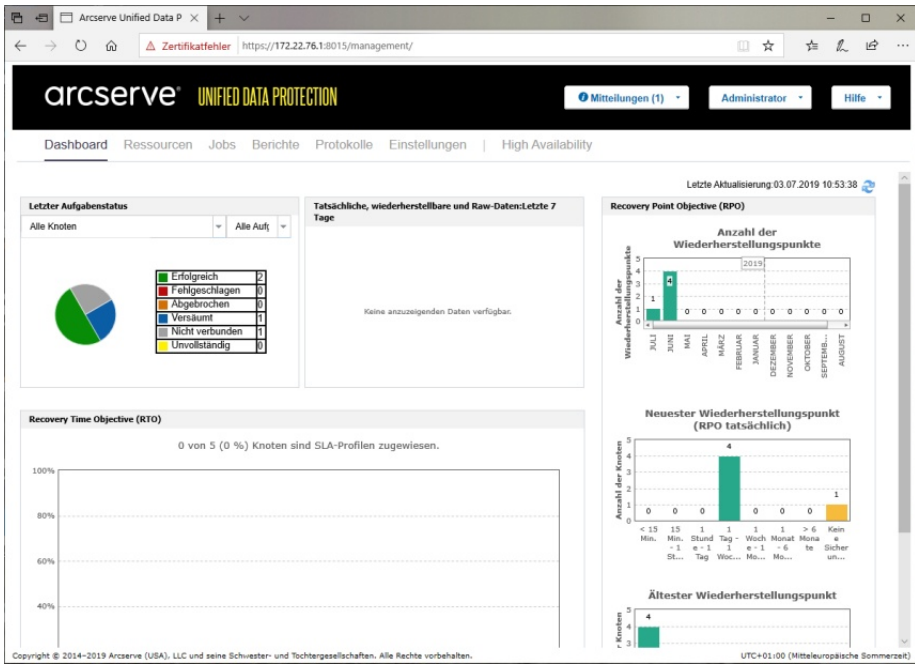
Der Sicherungsplan unseres Windows 10-Clients blieb während des gesamten Tests in Betrieb und erstellte zuverlässig nach der ersten Komplettsicherung jeden Tag differentielle Sicherungen des betroffenen Systems. Im nächsten Schritt des Tests machten wir uns nun daran, einen Windows Server zu sichern, der unter Windows Server 2019 lief.

Dazu fügten wir den Server als Sicherungsknoten aus unserem Active Directory zu unserer Arcserve-Umgebung hinzu und richteten einen entsprechenden Sicherungsplan ein. Daraufhin installierte die Appliance, wie schon bei dem Windows 10 Client, zunächst den Agenten auf dem zu schützenden Rechner und führte dann das Backup aus. Das Sichern von Windows-Rechnern stellt damit offensichtlich kein Problem dar.

Datenwiederherstellung

Mindestens genauso wichtig wie eine erfolgreiche Sicherung ist aber auch die Wiederherstellung der Daten. Arcserve bietet in diesem Zusammenhang an, alle Daten komplett wiederherzustellen, einzelne Daten auszuwählen und die Wiederherstellung an die Orginalorte oder an ein alternatives Ziel durchzuführen.

Im Test entschieden wir uns zu diesem Zeitpunkt, das komplette "Users"-Verzeichnis des Servers an einem alternativen Ort wiederherzustellen. Als Ziel bot uns die Appliance dazu sämtliche lokalen Laufwerke auf der Appliance selbst an, dazu gehörten auch zuvor über Windows verbundene Shares. Damit stellte der Restore-Vorgang auf ein Netzwerk-Share, auf das alle zugreifen konnten, kein Problem dar.



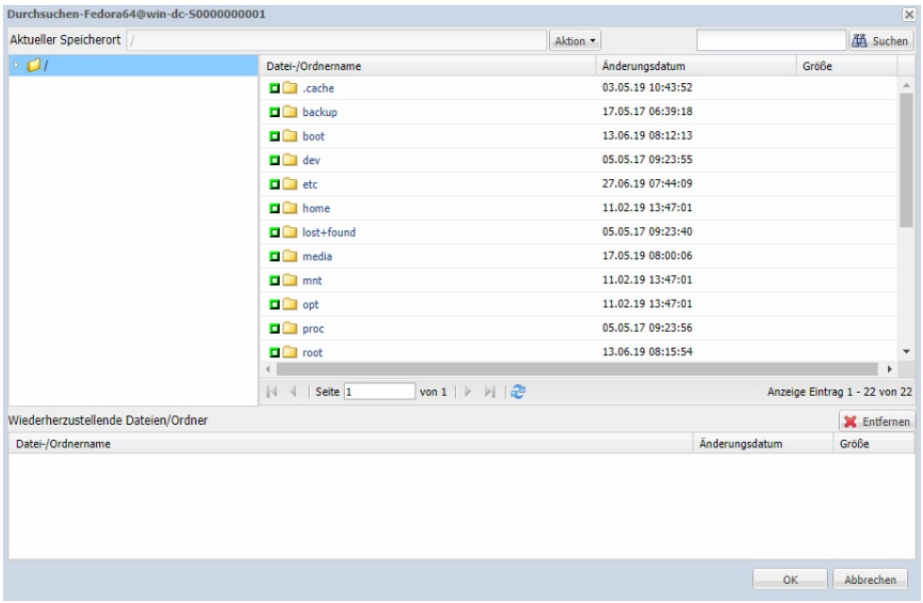
Das Dashboard gibt Aufschluss über den Gesamtzustand des Systems

Backup eines Linux-Systems

Das Backup eines Linux-Rechners funktioniert ähnlich wie bei Windows-Systemen. Man muss der Appliance beim Einfügen des Linux-Knotens neben dem Rechnernamen oder der IP-Adresse die SSH-Zugangsdaten angeben, danach lassen sich die Daten auf Linux-Systemen sichern. Damit

das funktioniert, benötigt die Backup-Software übrigens noch einen so genannten Linux-Sicherungsserver. Dieser wurde als virtuelle Maschine unter Centos 7 auf Hyper-V-Basis direkt auf der Appliance eingerichtet, die Nutzer müssen sich damit also nicht extra befassen.

Nach der Definition eines Linux-Sicherungsknotens läuft die Datensicherung dann genau wie bei Windows über Pläne ab. Im Test sicherten wir auf diese Weise erfolgreich Maschinen unter Centos 7.



Datenwiederherstellung von einem Linux-Rechner

Das Sichern virtueller Umgebungen

Als nächstes nahmen wir das Backup von virtuellen Maschinen unter die Lupe, die in Microsoft Hyper-V und Vmware ESXi-Umgebungen arbeiteten. Dazu mussten wir zunächst unsere Hypervisoren, die bei Hyper-V unter Windows Server 2019 und Windows Server 2016 liefen und bei Vmware den ESXi 6.7 Update 2 verwendeten, als Knoten zu unserer Sicherungsumgebung mit den entsprechenden Zugangsdaten hinzufügen.

Danach nahm die Appliance Verbindung zu den entsprechenden Systemen auf und zeigte an, welche VMs auf ihnen vorhanden waren. Diese konnten wir dann einfach auswählen und die Sicherung starten oder planen.

In diesem Zusammenhang spielt es noch eine Rolle zu wissen, dass die VMs unter Hyper-V während des Backup-Vorgangs laufen sollten, da das System sonst nicht dazu in der Lage ist, auf den Volume Shadow Copy Service (VSS) der betroffenen virtuellen Maschine zuzugreifen, beispielsweise um über Snapshots konsistente Sicherungen von SQL-Server-Installationen durchzuführen. Spielt diese Funktionalität keine Rolle, so lassen sich die Backups auch von ausgeschalteten Maschinen erstellen, der eigentliche Backup-Vorgang wird davon nicht betroffen.

Generell war es unproblematisch, die Backups der VMs anzulegen. Auch der Restore-Vorgang verlief wie erwartet. Auch hier ist es wieder möglich, die ganze VM oder einzelne Dateien und Ordner zurückzuspielen.

In Vmware-Umgebungen sollte man noch wissen, dass die kostenlose ESXi-Lizenz generell mit keiner Lösung keine Backups ermöglicht. Setzt man einen kostenlosen Vmware-Hypervisor ein, so kann man die darauf befindlichen VMs aber immer noch agentenbasiert wie physikalische Rechner sichern.

Backups von Office 365

Arcserve bietet auch an, Backups von Office 365-Konten zu erstellen. Dabei unterscheidet das System zwischen Backups von OneDrive, dem Exchange Server und SharePoint. Im Test sicherten wir OneDrive von einem normalen Office 365 Business-Account. Dazu mussten wir die entsprechende Funktionalität aber erst einmal aktivieren.

Dazu ist es zunächst erforderlich, über den Befehl "Install-Module AzureAD" über die Powershell das dazugehörige Modul einzuspielen. Außerdem mussten wir auch (ebenfalls über die Powershell) die Execution-Policy auf "Remote Signed" umstellen: "Set-ExecutionPolicy RemoteSigned".

Als das erledigt war, legten wir einen Backup-Plan für eine Office 365 OneDrive-Sicherung an, gaben die Appliance als Sicherungs-Proxy an und trugen die Credentials unseres Office 365-Abonements ein. Danach öffnete sich ein Browserfenster, über das wir der Arcserve UDP-Anwendung das Recht erteilen konnten, auf die Graph-API unseres Office 365-Kontos zuzugreifen.

Anschließend war der Sicherungsknoten verfügbar und wir konnten ihn in unseren Backup-Plan integrieren. Im Betrieb lief

das Backup dann genauso wie geplant ab.

Das Auslagern von Backup-Daten auf externe Speichermedien

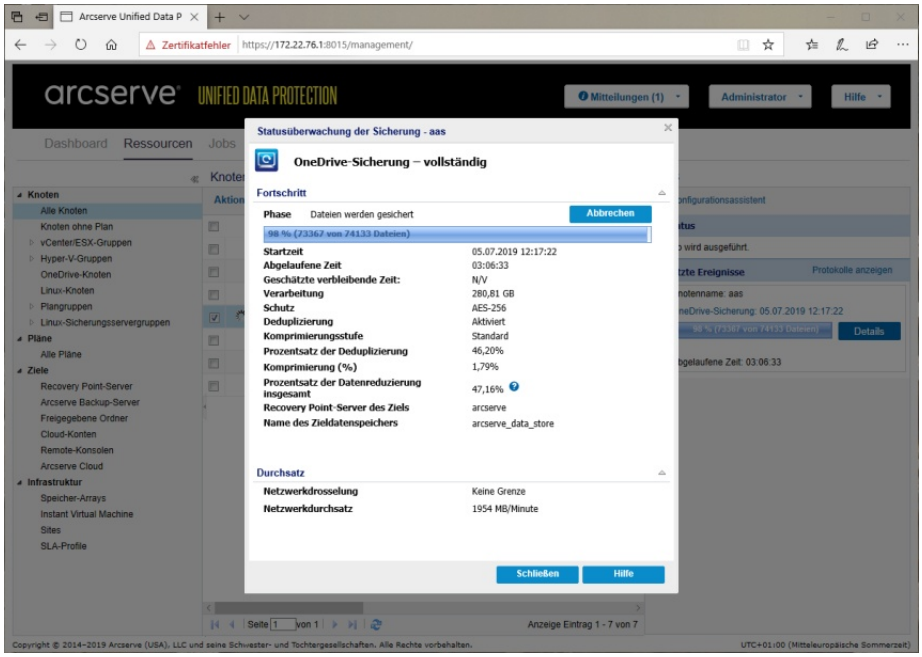
In der Praxis ergibt es keinen Sinn, Backups nur an einem Ort vorzuhalten. Deswegen ermöglich es die Arcserve Appliance, die Daten erstellter Backups automatisch auf andere Speichermedien zu kopieren. Dazu müssen die Administratoren lediglich auf den Sicherungs-Plan gehen, dessen Daten sie kopieren wollen und innerhalb der Plan-Konfiguration auf der linken Seite einen neuen Task hinzufügen.

Der Task-Typ lautet in diesem Fall "Wiederherstellungspunkte kopieren" und ermöglicht es, einen lokalen Datenträger, beispielsweise ein USB-Speichermedium, oder ein Netzwerk-Share beziehungsweise einen Cloud-Speicher als Kopierziel anzugeben. Im Test verwendeten wir zu diesem Zweck ein über einen UNC-Pfad definiertes Netzwerk-Share. Dabei traten keine Probleme auf. Über die Tasks lassen sich im Betrieb auch andere Aktionen durchführen, beispielsweise das Speichern der Backup-Daten auf Bandlaufwerken.

Dashboard, Analysen und Reports

Eine Backup-Lösung wäre wenig wert, wenn die Administratoren über ihre Aktionen im Unklaren blieben. Deswegen bietet die Arcserve Appliance nicht nur ein Dashboard mit aktuellen Informationen zum Status der Aufgaben, zur Zahl der Wiederherstellungspunkte und ähnlichem, sondern auch leistungsfähige Analyse- und Reportwerkzeuge. Letztere geben beispielsweise Aufschluss über den Trend bezüglich der Sicherungsgrößen, damit die zuständigen Mitarbeiter sehen, wie lange der vorhandene Backup-Speicher ausreicht.

Außerdem gibt es grafisch illustrierte Berichte, die zeigen, wie der Sicherungsstatus der im Netz vorhandenen Knoten aussieht und beispielsweise darauf hinweisen, wenn Sicherungen versäumt oder abgebrochen wurden. Genauso sind die Verantwortlichen unter anderem dazu in der Lage, den belegten Speicherplatz einzusehen oder auf die Systemprotokolle zuzugreifen.



Während der Sicherung können die IT-Verantwortlichen umfassende Informationen über Deduplizierung und Komprimierung einsehen

Fazit

Die Backup-Appliance von Arcserve konnte uns im Test voll überzeugen. Die Lösung lässt sich einfach einrichten und stellt out-of-the-box eine komplette Backup-Umgebung mit allen erforderlichen Komponenten und einer leistungsfähigen Deduplizierungsfunktion bereit. Diese kann aufgrund des zentralen Management-Interfaces im Betrieb einfach verwaltet werden und es ist auch problemlos möglich sie um externe Assets zu erweitern.

So lassen sich jederzeit andere Windows Server im Netz als zusätzliche Recovery Point-Server nutzen. In diesem Fall kommen die genannten Systeme als zweiter Backup Server zum Einsatz. Dazu sind keine zusätzlichen Lizenzen erforderlich.

Bei der Lizensierung verfolgt Arcserve die Politik, dass lediglich eine Lizenz vorhanden sein muss, um das ursprüngliche Backup zu erstellen. Danach können die Benutzer die Sicherungsdaten so oft von der Appliance exportieren, wie sie wollen. Aufgrund des großen Leistungsumfangs und der guten Bedienbarkeit verleihen wir dem Produkt, an dem es wenig auszusetzen gibt (lediglich die Dokumentation könnte übersichtlicher sein) das Prädikat "IAITested and recommended".

Dr. Götz Güttich leitet das Institut zur Analyse von IT-Komponenten (IAIT) in Korschenbroich. Sein Blog findet sich unter www.sysbus.eu.