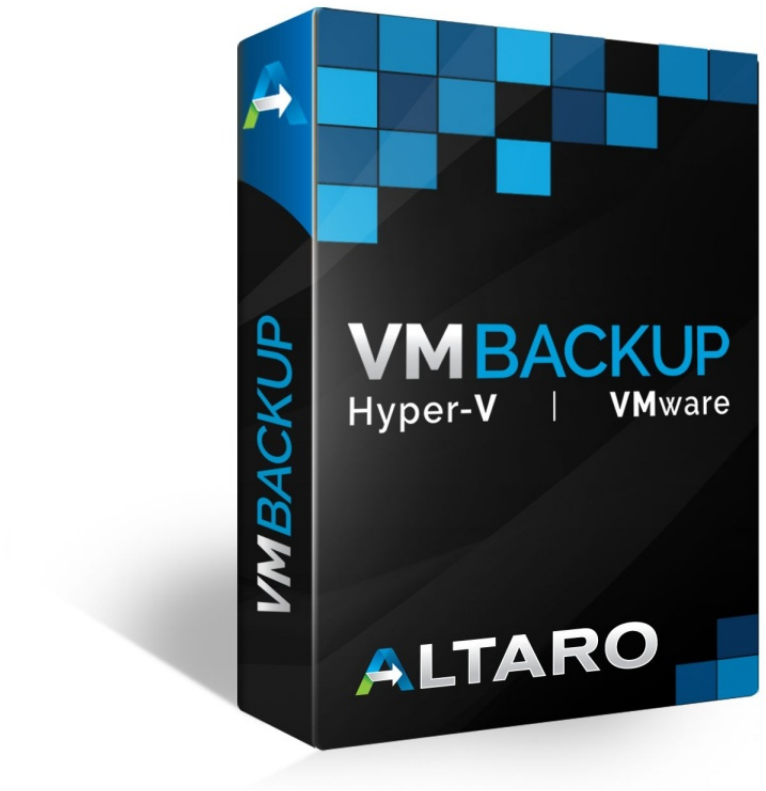
Backup schnell und einfach

Dr. Götz Güttich

Mit "VM Backup" bietet Altaro eine Backup Software an, die virtuelle Maschinen in Hyper-V- und VMware-Umgebungen sichern kann. Sie ist einfach zu bedienen und wendet sich an mittelgroße Unternehmen mit bis zu 50 Virtualisierungs-Hosts. Die Lösung konnte bei uns im Testlabor zeigen, was in ihr steckt.

Altaro nimmt für sich in Anspruch, dass es weniger als 15 Minuten dauert, um "VM Backup" zu installieren und die erste Sicherung zu starten. Ein besonderes Highlight des Produkts ist dabei das einfach zu bedienende, praktisch selbsterklärende Benutzerinterface, das die Anwender beim Implementieren ihrer Backup-Strategie an die Hand nimmt. Die zuständigen Mitarbeiter müssen dazu lediglich ihre Virtualisierungs-Hosts und Backup-Ziele angeben, danach lassen sich die Datensicherungen einfach durch das Ziehen des Icons der zu sichernden Virtuellen Maschine (VM) auf das gewünschte Backup-Ziel konfigurieren.



VM Backup ist im Betrieb dazu in der Lage, parallel auf mehrere Virtualisierungs-Hosts zuzugreifen, und die darauf laufenden VMs auf unterschiedliche Speichermedien zu sichern, sowohl on-premise als auch über das Netz an entfernten Orten. Die Verwaltung der Software und das Überwachen der Backups läuft dabei über eine zentrale Konsole ab.

Sichert das System VMs über das WAN auf entfernte Rechner, so kommen bei Bedarf WAN-Beschleunigungstechniken zum Einsatz. Abgesehen davon führt VM Backup auf Wunsch auch automatische Backup-Verifizierungen durch.

Darüber hinaus ist die Software dazu in der Lage, über eine granulare Restore-Option einzelne Dateien oder Exchange-Inhalte aus einem VM-Backup zu extrahieren und getrennt wiederherzustellen. Ein Zeitplaner sorgt dafür, dass die Backups bei Bedarf ohne Benutzerinteraktion regelmäßig im Hintergrund durchgeführt werden. Die dabei zum Einsatz kommenden Schedules lassen sich ebenfalls per Drag and Drop konfigurieren. Für kleine Umgebungen – beispielsweise zu Hause oder in Testlaboren – steht eine Freeware-Version von VM Backup zur Verfügung, die pro Host zwei VMs sichern kann.

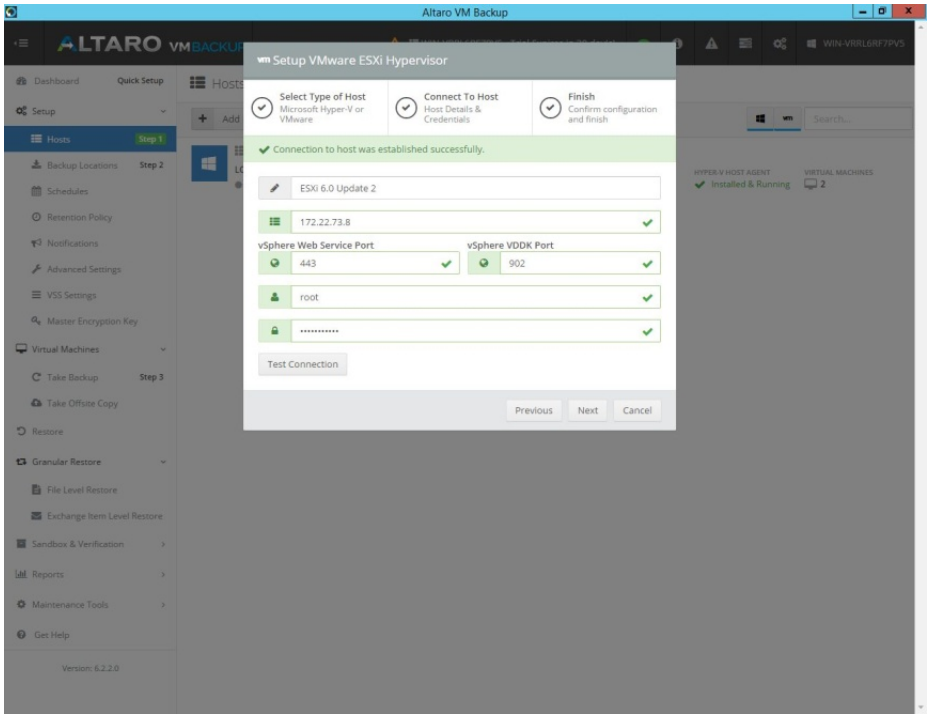
Altaro bietet für VM Backup sowohl Telefon-Support an, der in weniger als einer Minute antworten soll, als auch Unterstützung per E-Mail mit einer Antwortzeit von maximal einer Stunde. Für dringende Fälle existiert auch ein Live Chat, der praktisch sofort erreichbar ist.

Praktisch alle Funktionen, die zum Leistungsumfang des Produkts gehören, funktionieren sowohl in Hyper-V- als auch in Vmware-Umgebungen. Abgesehen von den bereits genannten Features unterstützt VM Backup das Sichern von laufenden VMs (auch unter Linux), Cluster Shared Volumes (CSVs) und die Zusammenarbeit mit Vmware vCenter. Die zu sichernden Daten lassen sich darüber hinaus jederzeit verschlüsseln und komprimieren.

Datenwiederherstellungen auf andere Hosts als das Originalsystem, von dem die VM ursprünglich kam, sind genauso möglich, wie die Wiederherstellung von unterschiedlichen Backup-Versionen, die zu verschiedenen Zeitpunkten erstellt wurden. Dabei lässt sich für jede VM genau festlegen, wie lang das System die Backups vorhalten soll.

Zusätzlich existiert auch die Option, Clones zu erzeugen, also Backups auf dem Original-Host wiederherzustellen, dabei aber einen unterschiedlichen Namen zu verwenden, so dass die Original-VM weiterlaufen kann. Für erweiterte Automatisierungs- und Reporting-Ansprüche bietet die Lösung das so genannte RESTful API. Möchte ein Administrator unter realen Bedingungen überprüfen, ob ein Backup voll funktionsfähig ist, so steht außerdem eine Funktion zum Wiederherstellen und Testen der jeweiligen Sicherheitskopie in einer Sandbox zur Verfügung.

Die Backups können auf USB-Medien, externe eSATA-Laufwerke, Netzwerk-Shares, NAS-Geräte, RDX-Cartridges und interne Festplatten erfolgen. Im Betrieb arbeitet die Software mit Windows Server 2008 R2 und neuer, dem Microsoft Hyper-V-Server (Core) sowie VMware ESXi, vSphere und vCenter, jeweils ab Version 5.0, zusammen. Die freie ESXi-Lizenz wird dabei allerdings nicht unterstützt, da sie das nötige API nicht zur Verfügung stellt.



Verbindungsaufbau zu einem Host unter ESXi 6.0 Update 2

Der Test

Für unseren Test installierten wir die Version 6.2.2.0 von Altaro VM Backup sowohl auf einer Workstation unter Windows 10, als auch auf einem Windows Server 2012 R2. Die Workstation kam zum Einsatz, um das Produkt im laufenden Betrieb zu testen, der Server führte jede Nacht mit Hilfe des Schedulers planmäßige Sicherungen der VMs in unserer Testumgebung durch. Diese VMs liefen sowohl auf zwei VMware ESXi-Hosts mit ESXi 6.0 Update 2, als auch auf einem unter Windows Server 2012 R2 laufenden Hyper-V-System. Innerhalb der VMs arbeiteten die Betriebssysteme Centos Linux 6 und 7 sowie Windows 7, Windows 10 und Windows Server 2012 R2.

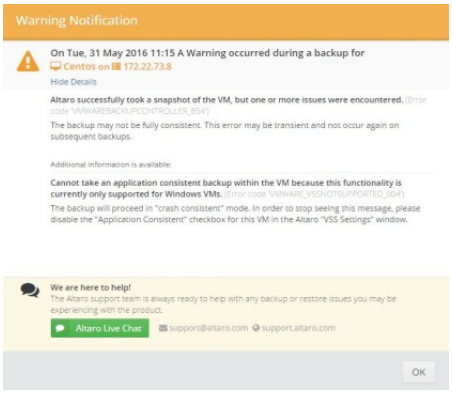
Nach der Installation machten wir uns zunächst mit dem Leistungsumfang der Backup-Lösung vertraut, erstellten einige Backups und richteten dann die automatischen Backups mit Hilfe des Zeitplaners ein. Anschließend stellten wir diverse VMs wieder her – auch auf unterschiedliche Zielsysteme – und testeten die granularen Restore-Optionen. Zum Schluss nahmen wir noch die Sandbox-Funktion unter die Lupe.

Installation

Um Altaros VM Backup zu installieren, genügt es, die von der Webseite des Herstellers heruntergeladene Setup-Datei auszuführen und den Installationspfad anzugeben. Danach läuft das Setup durch.

Anschließend startet die Management Console. Zu diesem Zeitpunkt hat der Installations-Wizard seine Arbeit allerdings noch

nicht beendet, sondern verlangt einen weiteren Klick auf "OK", um das Setup abzuschließen. Das verwirrt zwar etwas, stört aber nicht wirklich, da die Installationsroutine ein paar Sekunden



Kommt es während der Arbeit zu Problemen, so meldet VM Backup diese sofort

später fertig ist. Danach steht dem Login beim Altaro Backup-Dienst nichts mehr im Wege.

Die Standard-Setup-Datei, die wir in diesem Test verwendet haben, installiert übrigens immer alle drei Komponenten von Altaro VM Backup: den Backup-Dienst, den Altaro Offline-Server für WAN-Backups und die Management-Console. Möchte ein IT-Verantwortlicher nur eine Komponente – wie etwa die Management-Console auf einer zentralen Verwaltungsworkstation – einspielen, so stellt Altaro zu diesem Zweck separate Setup-Files bereit. Das Verwaltungswerkzeug muss folglich nicht auf dem gleichen System laufen, wie der Backup-Service.

Erstkonfiguration

Hat sich der Administrator mit Hilfe der Management Console mit der VM Backup-Instanz verbunden, so landet er in einer Dashboard-Übersicht, die eine Quick Setup-Seite anzeigt. Diese weist die Benutzer darauf hin, auf welche Weise sie die Software in Betrieb nehmen können. Zu diesem Zweck müssen sie zunächst ihre Hyper-V- beziehungsweise Vmware-Hosts zur Backup-Umgebung hinzufügen. Danach geht es an die Definition eines Backup-Ziels. Im dritten Schritt erfolgt dann das erste Backup.

Die Quick Setup-Seite zeigt den Anwendern für alle drei Schritte jeweils, wo sie hin klicken müssen, um die jeweilige Aufgabe zu erledigen. Wurden alle drei Aufgaben durchgeführt, so verschwindet die Seite und wird durch eine Dashboard-Übersicht ersetzt.

Im Test ergaben sich bei der Erstkonfiguration keine Probleme. Beim Hinzufügen eines Backup-Hosts muss der Administrator lediglich angeben, ob es sich um einen Hyper-V- oder einen ESXi-Hypervisor handelt. Alternativ kann – wie angesprochen – auch ein vCenter Server zum Einsatz kommen.

Bei einem Hyper-V-Host verlangt das System im nächsten Schritt die Angabe eines Namens, der Host-Adresse und der Credentials. Danach gibt es die Möglichkeit, die Verbindung zu testen. Fällt der Test positiv aus, so steht der Nutzung des Hypervisors nichts mehr im Wege.

Die Einrichtung eines ESXi-Hypervisors oder eines vCenter Servers läuft im Prinzip genauso ab. Die zuständigen Mitarbeiter haben hier aber zusätzlich die Option, die Ports für den vSphere Web Service und vSphere VDDK zu modifizieren.

Für die Definition des Backup-Ziels bietet das Produkt viele unterschiedliche Möglichkeiten. Zunächst einmal muss der IT-Verantwortliche entscheiden, ob er eine lokale oder eine Offsite Backup-Location einrichten will. Bei lokalen Backups offeriert die Software zunächst einmal physikalische Laufwerke wie USB-Datenträger, interne Festplatten oder iSCSI-Speicher. Alternativ lassen sich die Backups auch auf einem Netzwerk-Share sichern. Dazu müssen die Administratoren den Pfad zum Share sowie die Credentials angeben, danach richtet das System die Freigabe als Backup-Ziel ein.

Beim Anlegen einer Offsite-Location für die Backups bietet die Software den Usern neben den physikalischen Laufwerken und den Netzwerk-Shares noch zusätzliche Möglichkeiten an. Dazu gehören zunächst einmal austauschbare Laufwerke, zum Beispiel Sets externer USB- oder eSATA-Festplatten, RDX-Drives oder Netzwerkshares. Entscheidet sich der zuständige Mitarbeiter für ein Set, so muss er zunächst einmal Speicherkomponenten definieren, die dazu gehören sollen. Anschließend kann er das Set ganz normal als Drag and Drop-Ziel nutzen.

Eine weitere Alternative für ein Offline Backup-Ziel ist der Altaro Offline-Server mit WAN-Beschleunigung. Soll er zum Einsatz kommen, so müssen die Verantwortlichen in der Altaro Offsite Server Management-Console einen Benutzer-Account anlegen und diesem ein Speicherziel zuweisen.

Anschließend rufen sie den Konfigurationsdialog für Offsite-Backupziele auf und geben die Serveradresse und die gerade zuvor festgelegten Credentials ein.

Danach steht auch dieses Backup-Ziel zur Verfügung. Für Offsite-Backups muss allerdings zwingend eine Datenverschlüsselung aktiviert sein.

Nach der Definition des Backup-Ziels geht es daran, die auf den Hosts vorhandenen VMs per Drag and Drop zu Backup-Zielen zuzuweisen. Sobald das erledigt ist, können die IT-Mitarbeiter das erste Backup starten. Dazu müssen sie lediglich in der Übersicht unter "Take Backup" die zu sichernde VM auswählen und den Sicherungsvorgang anstoßen. Anschließend läuft die Datensicherung durch.

Im Test hatten wir VM Backup tatsächlich in wenigen Minuten eingespielt und mit einem lokalen Backupziel in Betrieb genommen. Der Hersteller hat hier mit seiner Angabe, dass es maximal 15 Minuten dauern würde, nicht übertrieben. Es kam weder bei der Kommunikation mit Hyper-V- noch beim Zugriff auf ESXi-Hosts zu irgendwelchen Problemen. Das Gleiche gilt für das Einrichten der Backup-Locations.

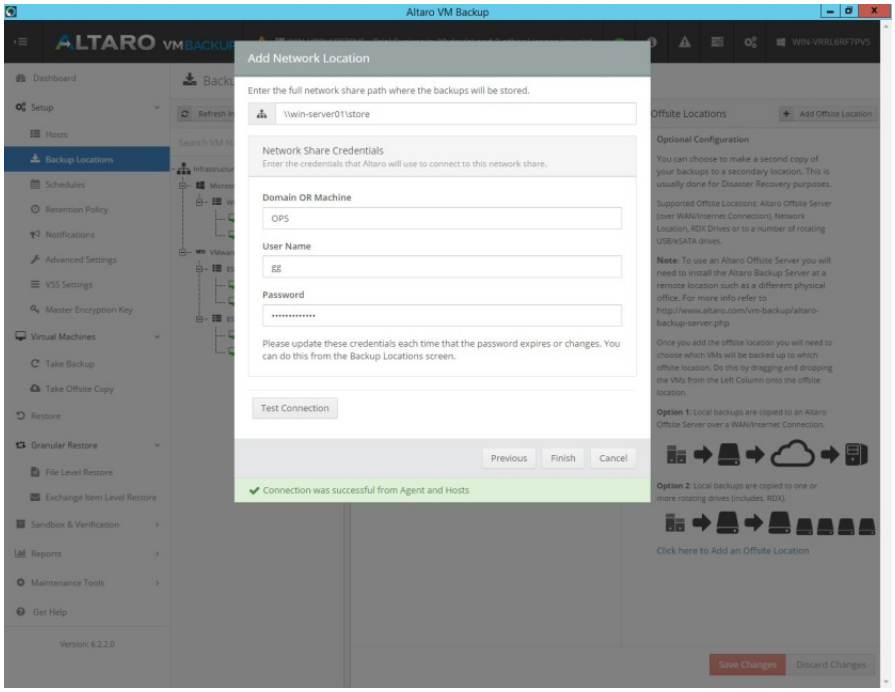
Der weitere Funktionsumfang der Lösung

Gehen wir nun genauer auf den sonstigen Funktionsumfang des Produkts ein. In diesem Zusammenhang ist zunächst einmal die Dashboard-Seite zu erwähnen, die im Betrieb anstelle des Quick Setups erscheint. Diese umfasst neben einer Tortengrafik, die die Administratoren über den Status der Backup-Laufwerke informiert (freier Speicherplatz und ähnliches) auch eine grafische Darstellung der Größe der täglich angelegten Backups. Darüber hinaus gibt es auch noch Listen mit den gerade aktiven Aktionen, den letzten Backups, den letzten Offsite-Kopien sowie der Restore- und der Verification-History.

Eines der wichtigsten Features neben dem eigentlichen Durchführen von Backups ist mit Sicherheit der Scheduler, der automatische Backup-Läufe zu bestimmten Zeiten durchführt. Standardmäßig wurden bereits Zeitpläne für nächtliche Backups unter der Woche und abendliche Sicherungen am Wochenende vordefiniert. Auch hier genügt es, die zu sichernden VMs per Drag and Drop auf die Icons der Zeitpläne zu ziehen, um automatische Backups zu aktivieren.

Möchten die Administratoren eigene Zeitpläne anlegen, so definieren sie zunächst, ob die Datensicherungen wöchentlich oder monatlich ablaufen sollen. Bei wöchentlichen Plänen geben sie danach die Uhrzeit und die Wochentage an, an denen der Schedule Gültigkeit besitzt. Die Wochentage lassen sich dabei für On- und Offsite-Backups getrennt festlegen. Bei monatlichen Plänen definieren die zuständigen Mitarbeiter die Backup-Tage anhand ihres Datums (zum Beispiel fünfter Tag des Monats) oder ihrer Lage (zweiter Montag des Monats).

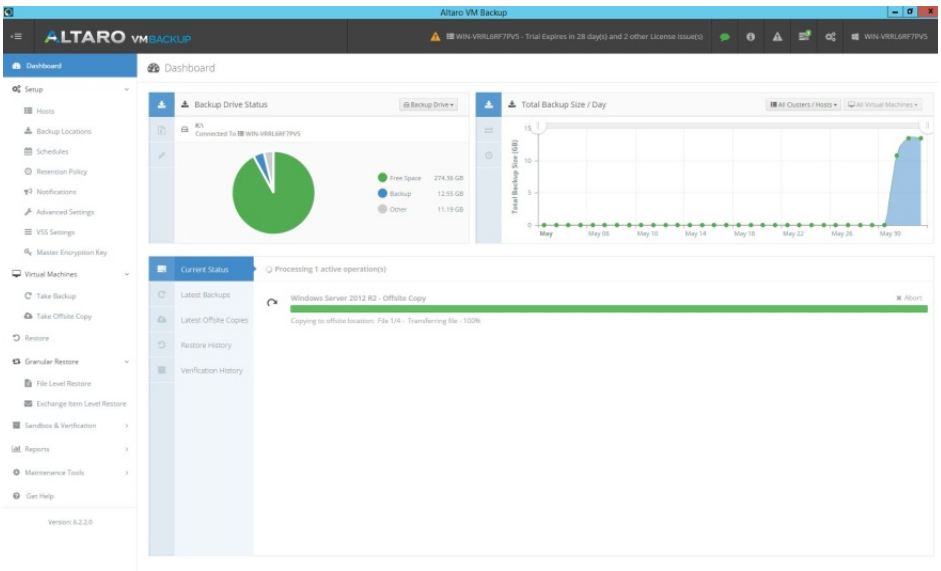
Letzteres ist sehr sinnvoll, beispielsweise wenn es darum geht, alle Windows-VMs vor dem monatlichen Patch-Day von Microsoft nochmal zu sichern. Auch bei monatlichen Backups steht eine Option zum zusätzlichen Sichern auf Offsite-Speicher zur Verfügung. Eine Preview, die die nächsten anstehenden Sicherungsläufe auf der rechten Fensterseite in Listenform anzeigt, schließt den Konfigurationsbereich der Zeitpläne ab.



Die Verbindung mit einem Netzwerk-Share als Backup-Ziel

Ebenfalls von Interesse sind die "Retention Policies" die festlegen, wie lange das System einzelne Backup-Kopien aufbewahrt. Standardmäßig löscht VM Backup alte Sicherungen nach zwei Wochen, es wurden aber auch Retention Policies für einen Monat, sechs Monate und Nie

(also gar keine Löschung) vordefiniert. Beim Anlegen einer neuen Policy geben die IT-Mitarbeiter lediglich die Zahl der Tage an, die die Software die Backups aufbewahren soll, danach ist die Regel nutzbar. Auch hier erfolgt die Zuweisung der VMs zu den



Das Dashboard beim Anlegen einer Offsite-Copy

Policies per Drag and Drop. Die Retention Policies existieren sowohl für On-, als auch für Offsite-Kopien.

Was die Benachrichtigungen angeht, so ist VM Backup auf Wunsch dazu in der Lage, bei erfolgreichen Sicherungen, fehlgeschlagenen Sicherungen und komplett durchgeführten Restore-Vorgängen E-Mails an die Administratoren zu verschicken oder Log-Einträge zu generieren. Die "Advanced Settings" lassen sich nutzen, um für die einzelnen VMs genau festzulegen, wie das Backup ablaufen soll.

So können die Administratoren hier die Komprimierung und Verschlüsselung ein- und ausschalten sowie festlegen, ob ISO-Images, die mit der jeweiligen VM verbunden sind, mit gesichert werden. Darüber hinaus definieren sie, nach wie vielen Backups die "Reverse Delta"-Funktion eine komplette Sicherung anstelle einer inkrementellen anlegt. Standardmäßig sind das 30 Tage, dieser Wert lässt sich aber auf VM- und Host-Ebene sowie auf Ebene der ganzen Backup-Umgebung ändern. Abgesehen davon existiert auch noch die Möglichkeit, bestimmte Laufwerke von den Datensicherungen auszunehmen und die Unterstützung von Vmwares Changed Block Tracking (CBT) zu aktivieren.

Die VSS-Einstellungen ermöglichen es den Benutzern im Gegensatz dazu, festzulegen, ob die Software "Application Consistent"- oder "File Consistent"-Backups erzeugt. Application Consistent bedeutet, dass sie Sicherungskopie im laufenden Betrieb aus einer Shadow Copy heraus angelegt wird.

Bei Betriebssystemen, die keine Shadow Copyies unterstützen, hält das System die VM an, erzeugt den Snapshot und startet die VM wieder. Dieses Vorgehen bezeichnet der Hersteller als File Consistent. Applicatation Consistent Backups lassen sich nur auf Windows Servern erzeugen, auf Windows Clients und Linux-Systemen kommen File Consistent Backups zum Einsatz. Die nächsten Punkte der Management Console ermöglichen das Setzen des Verschlüsselungs-Keys, der für die Encryption der Backups zum Einsatz kommt und das manuelle Erzeugen von On- oder Offsite-Sicherungen.

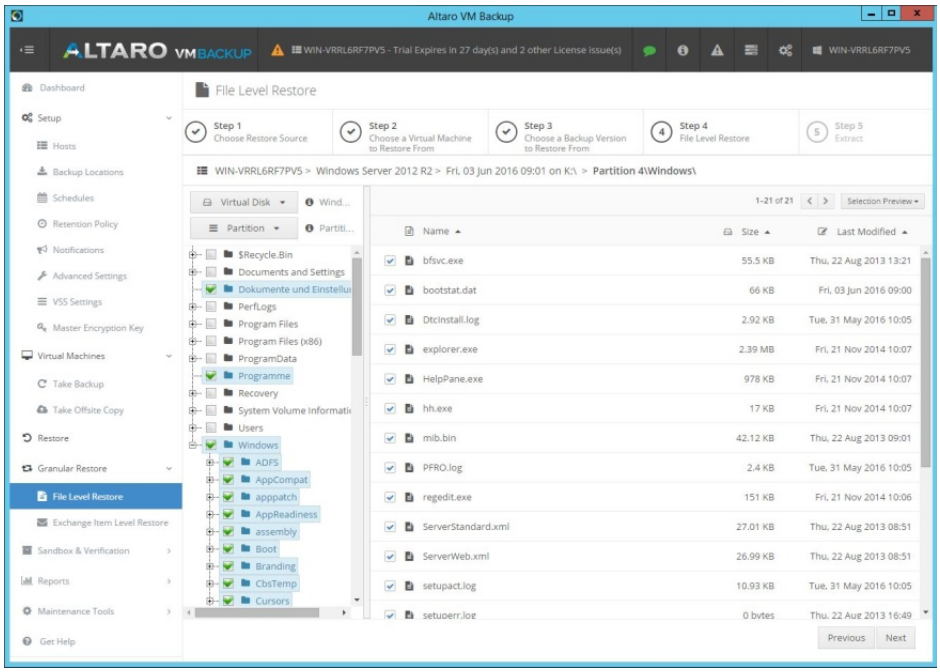
Datenwiederherstellung

Um Daten aus einmal generierten Backups wiederherzustellen, stehen mehrere Wege offen. Über den "Virtual Machine Restore Wizard" lassen sich ganze VMs zurückspielen. Dazu müssen die zuständigen Mitarbeiter zunächst den Data Store auswählen, in dem die wiederherzustellende VM liegt. Danach selektieren sie die betroffene VM selbst und zum Schluss geben sie an, wohin die Wiederherstellung erfolgen soll. Nach dem Abschluss des Restore-Vorgangs erscheint die VM dann in der Übersicht des Hypervisors.

Interessanter ist das "Granular Restore". Diese Funktion steht sowohl für Wiederherstellungen auf Dateiebene, als auch zum Zurückrückspielen von Exchange Items zur Verfügung. Wollen die IT-Mitarbeiter eine einzelne Datei aus dem Backup extrahieren, so müssen sie zuerst die Datenquelle und die betroffene VM auswählen.

Danach bietet ihnen VM Backup die vorhandenen Backup-Versionen der VM zur Selektion an. Nachdem sie sich für eine Version entschieden haben, können sie die gewünschte virtuelle Disk und die Partition selektieren. Da-

nach zeigt das Tool die vorhandenen Inhalte an und es besteht die



Die granulare Restore-Option erlaubt das Zurückspielen einzelner Dateien und Ordner aus einem Backup

Option, die benötigten Dateien und Ordner auszuwählen. Zum Schluss benötigt das Tool noch die Angabe eines Restore-Ziels, danach läuft die Wiederherstellung durch. Die Granular Restore-Funktion steht momentan übrigens nur für Windows-Backups zur Verfügung, für Linux-Systeme soll sie später dieses Jahr folgen.

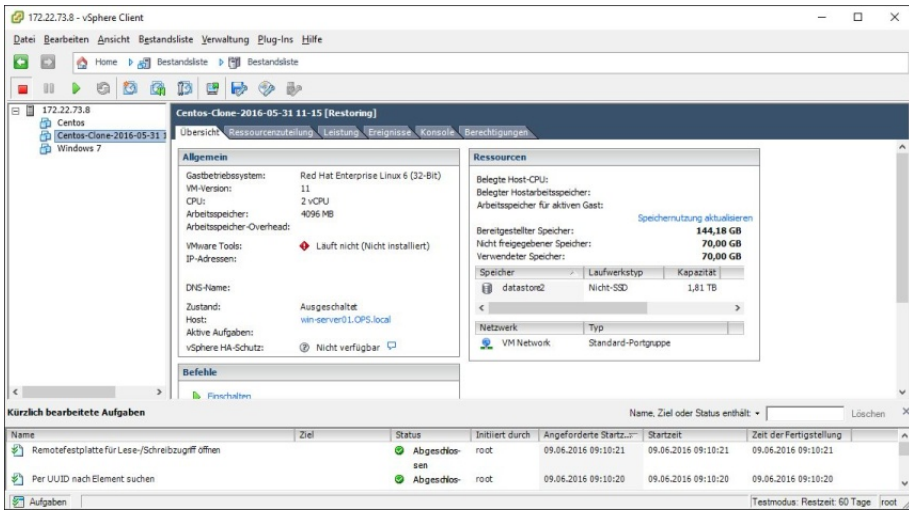
Bei der Exchange Item-Wiederherstellung läuft alles genauso ab, nach der Auswahl der virtuellen Disk und Partition wählen die Administratoren aber ein EDB-File aus, um den Restore-Vorgang auf Item-Level anzustoßen.

Sicherheit

Wenden wir uns nun der Sandbox-Funktion und der Verifizierung der Backups zu. Möchten die IT-Verantwortlichen überprüfen, ob eine Sicherungskopie erfolgreich war, so können sie unter "Test & Verify Backups" den zu verwendenden Sandbox Restore Type auswählen. Zunächst einmal steht an dieser Stelle "Verify Backup Folders" zur Verfügung. Dabei untersucht das System die Datenintegrität der gesicherten Informationen, ohne die VMs mit einem Hypervisor zu verbinden. Der "Full Test Restore" stellt die VM-Kopie als Clone wieder her, verbindet sie mit dem Hypervisor und prüft, ob das VM-System hochfährt. Die laufenden VMs werden davon nicht beeinträchtigt, es kommt aber kurzzeitig zu einer Belastung der CPU- und Speicherressourcen des Hosts. Im Test ließen wir zunächst die "Verify Backup Folders"-Funktion ablaufen. Dazu selektierten wir zunächst die Datenspeicher, die zu testende VM und die Backup-Version. Danach konnten wir den Test starten und im Dashboard verfolgen, wie der Job ablief.

Bei einem "Full Test Restore" erfolgt auch wieder die Auswahl der VM und der zu testenden Backup-Version, anschließend lässt sich der Test auch hier starten und im Dashboard verfolgen. Während des Tests konnten wir keine nennenswerte Zusatzlast auf dem Hypervisor feststellen und die Arbeit ging ganz normal weiter.

Die Sandbox-VM erschien allerdings in der Übersicht des Hypervisors als zusätzliche VM und verblieb dort auch. Das ist so gewünscht, da die Anwender bei manuellen Tests auf diese Weise

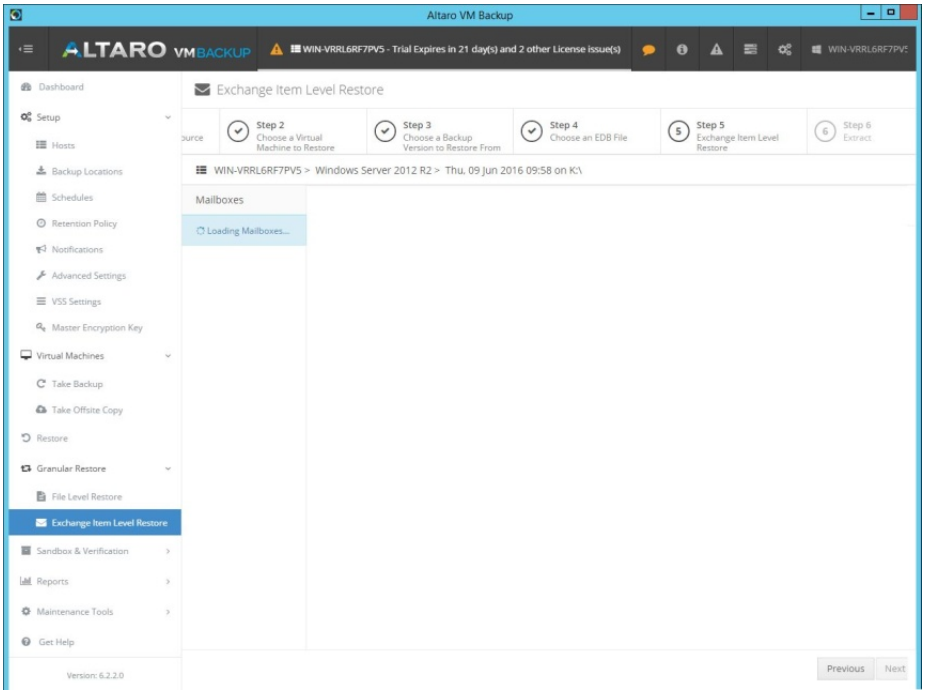


Mit VM Backup angelegte Clones erscheinen genau wie alle andere VMs auch in der Übersicht des jeweiligen Hypervisors

die Möglichkeit haben, die VM zu nutzen und so zu prüfen, ob das Backup wirklich allen Anforderungen entspricht.

Über die Funktion "Schedule Test Drills" haben die zuständigen

Mitarbeiter jederzeit die Möglichkeit, Zeitpläne für Testläufe



VM Backup beim Einlesen der Mailboxen aus einer EDB-Datei

anzulegen und diese automatisch im Hintergrund durchzuführen. Das Testen der Backups muss also keineswegs manuell erfolgen. Die Ergebnisse der Testläufe finden sich dann wie gewohnt im Dashboard.

Bei den zeitplangesteuerten Testdrills ist es übrigens möglich, die Full Test Restore-Drills so zu konfigurieren, dass sie nach dem Test automatisch vom Hypervisor gelöscht werden. Das ergibt Sinn, da sonst ständig neue VM-Einträge erzeugt würden.

Reporting und Speicherpflege

Was die Reports angeht, so liefert das System sowohl eine "Operation History", die zeigt, zu welchen Zeiten auf welchen Hosts Aktionen wie Backups, Restores, Verifications und ähnliches durchgeführt wurden, als auch eine reine Fehlerübersicht. Unter "Maintenance Tools" findet sich schließlich eine Funktion zum Löschen nicht mehr benötigter Backups. Damit können die Administratoren Speicherplatz freimachen und Überflüssiges entfernen bevor die jeweilige Retention Policy greift.

Abgeschlossen wird der Leistungsumfang von VM Backup durch eine Hilfefunktion, die einen Fehlerreport erzeugt, einen Remote Support Client bereitstellt, nach Updates sucht und Links zum Handbuch und zur Knowledge Base sowie den FAQs anbietet. Die Hilfeseite informiert die Benutzer auch über die Support-E-Mail sowie die Hotline und ermöglicht zudem auch den Start eines Support Live-Chats.

Am oberen Fensterrand der Management Console stehen noch diverse Icons zur Verfügung, mit denen sich ebenfalls der Live Chat starten lässt. Außerdem zeigt die Software darüber Statusmeldungen und Alarme an, präsentiert aktive Operationen und ermöglicht das Erzeugen eines Fehlerreports, das Durchführen von Updates, das Setzen des Verschlüsselungs-Keys und das Aufrufen des Handbuchs.

Fazit

Altaros VM Backup konnte uns im Test überzeugen. Die Software wird schnell eingerichtet, verfügt über alle Funktionen, die für Backups in kleinen und mittelgroßen virtuellen Umgebungen nötig sind und versah im Test zuverlässig ihre Arbeit. Der eigentliche Clou des Produkts ist aber das durchdachte und sehr übersichtliche Benutzer-Interface, über das sich alle wichtigen Funktionen per Drag and Drop konfigurieren lassen.

Dieses Management-Tool lässt sich so einfach bedienen, dass auch Administratoren ohne Erfahrung mit der Sicherung virtueller Maschinen ohne Schulung sofort dazu in der Lage sein sollten, mit der Lösung zu arbeiten. Wir verleihen dem Produkt deshalb die Auszeichnung "IAIT Tested and Recommended".

Altaro VM Backup 6.2.2.0

Backup- und Restore-Lösung für virtuelle Umgebungen auf Basis von Microsofts Hyper-V und Vmwares ESXi-Hypervisor beziehungsweise vCenter-Server.

Vorteile:
- Einfache Installation
- Übersichtliches Administrationsinterface
- Sehr einfache Bedienung
- Großer Funktionsumfang

Hersteller:
Altaro
www.altarosoftware.de