

Installationsleitfaden

EVault Agent für Windows – VMware –



Inhalt

| | | |
|-----------|---|---------------|
| 1. | Technische Informationen | - 1 - |
| 1.1. | Firewall – Ports | - 1 - |
| 1.2. | Hinweis zur Dokumentation | - 1 - |
| 1.3. | Hintergrundwissen | - 1 - |
| 1.4. | Ihr Zugang | - 2 - |
| 1.5. | Support | - 2 - |
| 2. | Erste Schritte im Webinterface | - 3 - |
| 2.1. | Anmelden am Webfrontend | - 3 - |
| 2.2. | Anlegen von Benutzern | - 3 - |
| 3. | Installation des VMware Agenten | - 6 - |
| 3.1. | Einbinden des VMware Agenten in das vCenter | - 6 - |
| 4. | Konfiguration des VMware Agenten | - 9 - |
| 4.1. | Grundkonfiguration | - 9 - |
| 4.2. | Erweiterte Konfiguration | - 10 - |
| 4.3. | Konfiguration des Agenten im Webfrontend | - 11 - |
| 4.4. | Hinzufügen eines Vault Profils | - 11 - |
| 4.5. | Anlegen von Aufbewahrungstypen | - 12 - |
| 4.6. | Anlegen von Benachrichtigungen | - 14 - |
| 4.7. | Anmeldung am vCenter | - 14 - |
| 5. | Datensicherung | - 15 - |
| 5.1. | Einrichten einer Datensicherung | - 15 - |
| 6. | Restore einer Datensicherung | - 19 - |
| 6.1. | Restore – Virtuelle Maschine | - 21 - |
| 6.2. | Restore – Virtuelle Festplatte | - 24 - |
| 6.3. | Restore – Dateien und Ordner | - 26 - |
| 7. | vAgent Konsolenbefehle | - 29 - |
| 7.1. | agent | - 29 - |
| 7.2. | config | - 29 - |
| 7.3. | mount | - 29 - |
| 7.4. | net | - 29 - |
| 7.5. | ntp | - 30 - |
| 7.6. | ssh | - 30 - |
| 7.7. | support | - 30 - |
| 7.8. | system | - 30 - |
| 7.9. | vcenter | - 30 - |
| 7.10. | webcc | - 30 - |

| | |
|--------------------------------------|------------|
| EVault Agent für Windows – VMware | 06.01.2017 |
|--------------------------------------|------------|

1. Technische Informationen

1.1. Firewall – Ports

Die folgenden Ports sind „**Ausgehend**“ an Ihrer Firewall freizuschalten.

| Port | Verwendung | Protokoll | Ziel |
|-------|--|-----------|---|
| 8086 | Anbindung des Agents an das Webportal. | TCP | 89.251.128.130 |
| 8087 | Anbindung des Agents an das Webportal. | TCP | 89.251.128.140 |
| 2546 | Datenverbindung vom Agent zum Sicherungsserver. | TCP | 89.251.128.0/24 89.251.131.80/28 |
| 2547 | Datenverbindung vom Satelliten zum Sicherungsserver (wird nur beim Einsatz eines Satelliten benötigt). | TCP | 89.251.128.0/24 89.251.131.80/28 |
| 12547 | Datenverbindung vom Satelliten zum Sicherungsserver (wird nur beim Einsatz eines Satelliten benötigt). | TCP | 89.251.128.0/24 89.251.131.80/28 |
| 25 | Mailbenachrichtigung durch den Agent. | TCP | In der Mailkonfiguration des Agents angegebenen Mailserver. |

1.2. Hinweis zur Dokumentation

Bitte lesen Sie diese Dokumentation sehr sorgfältig durch. Bei einigen Konfigurationspunkten sind Arbeiten vorab zu erledigen.

1.3. Hintergrundwissen

Bei der Sicherung mit dem Produkt EVault handelt es sich um eine Online-Backup. Die Sicherung Ihrer Computer sowie die Konfiguration der Sicherungsjobs erfolgt „**online**“. Eine Internetverbindung ist daher zwingend notwendig.

Je nach Sicherungsgröße und Bandbreite Ihrer Internetverbindung empfiehlt sich der Einsatz eines sogenannten „**Backup-Satelliten**“. Hierbei handelt es sich um einen weiteren Sicherungsserver, der am Standort Ihrer zu sichernden Server aufgestellt wird. Die Sicherung erfolgt dann in zwei Schritten: Die eigentliche Sicherung erfolgt standortintern auf den Satelliten. Anschließend werden die auf den Satelliten gesicherten Daten auf die Sicherungsserver im Rechenzentrum der microPLAN GmbH repliziert.

Zusätzlich gibt es die Möglichkeit das Initialbackup bei größeren Sicherungen mittels einer „**Starterbox**“ ins Rechenzentrum zu liefern. Hierbei handelt es sich um einen Sicherungsserver, der für den Zeitraum der Erstsicherung am Standort Ihrer Server aufgestellt wird. Nach dem Abschluss der Erstsicherung wird diese Starterbox ans Rechenzentrum geliefert und die Erstsicherung hier importiert. Anschließend kann die normale Sicherung über die Internetverbindung in Betrieb genommen werden.

| | |
|--------------------------------------|------------|
| EVault Agent für Windows – VMware | 06.01.2017 |
|--------------------------------------|------------|

Abhängig von der Menge der zu sichernden Daten und der Bandbreite Ihrer Internetverbindung kann es sonst dazu kommen, dass das Initialbackup mehrere Tage dauern kann.

1.4. Ihr Zugang

Nach der Bestellung eines Demozugangs bzw. der Beauftragung einer Onlinesicherung, erhalten Sie von uns eine E-Mail mit Zugangsdaten. Mit diesen Zugangsdaten erhalten Sie Zugriff auf das Webfrontend der Onlinesicherung. Loggen Sie sich unter <https://backup.rz-24.de/> mit Ihren Zugangsdaten ein.

1.5. Support

Sollte es weitergehende Fragen oder Probleme geben, stehen wir Ihnen selbstverständlich gerne zur Verfügung. Wenden Sie sich einfach an unseren Support:

E-Mail: technik@microPLAN.de

Wir sind telefonisch für Sie erreichbar:

Mo-Fr 07:30 Uhr – 17:30 Uhr

Tel.: 02572 / 93 65 400

2. Erste Schritte im Webinterface

Hier soll Ihnen erläutert werden, wie Sie Schritt für Schritt zu Ihrer Datensicherung kommen.

2.1. Anmelden am Webfrontend

Das Webfrontend ist das zentrale Tool zur Verwaltung Ihrer Sicherung. Die komplette Sicherung inklusive Benachrichtigungen, Protokolle und Co. wird hiermit verwaltet.

URL:

<https://backup.rz-24.de/>

Benutzername:

Ihr Benutzer

Kennwort:

Ihr Kennwort



Hinweis:

Bitte verwenden Sie nicht die alte „**Web CentralControl-Oberfläche**“. Dieses Portal bietet nur einen eingeschränkten Funktionsumfang.

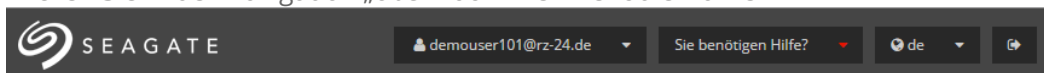
2.2. Anlegen von Benutzern

Wir empfehlen einen gesonderten Benutzer anzulegen, mit dem die Sicherungsagents bei der Installation am Webportal registriert werden. Dies hat den Hintergrund, dass Sie, wenn Sie die Agents mit Ihrem „**normalen**“ Benutzer registrieren, diese neu registrieren müssen, sollten Sie das Kennwort Ihres Benutzers ändern.

Für die Registrierung eines neuen Agenten reicht es, wenn der verwendete Benutzer der Rolle „Benutzer“ angehört.

Um einen Benutzer anzulegen, gehen Sie bitte wie folgt vor.

1. Klicken Sie in der Navigation „**oben**“ auf ihren Benutzernamen



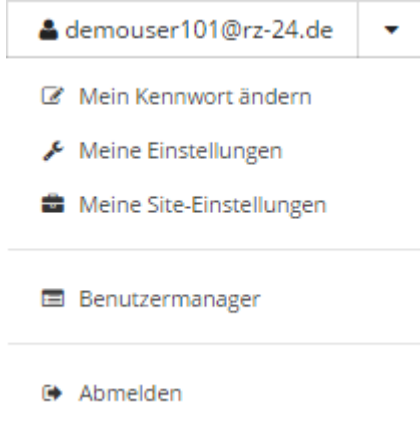
2. Im erscheinenden Dropdown-Menü haben Sie nun die Möglichkeit, den „**Benutzermanager**“ aufzurufen

Kontext Menü im Detail

Folgende Optionen werden angeboten:

1. Mein Kennwort ändern
2. Meine Einstellungen
3. Meine Site-Einstellungen
4. Benutzermanager
5. Abmelden

Zum Anlegen eines neuen Benutzers verwenden Sie den Punkt 4 (Benutzermanager)



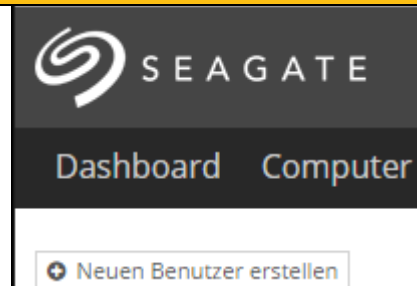
3. Nachdem Sie den Benutzermanager aufgerufen haben, sehen Sie im oberen Teil der Webseiten den Menüpunkt „**Neuen Benutzer erstellen**“. Wählen Sie bitte diese Option um einen neuen Benutzer zu erstellen.

Kontext Menü im Detail

Folgende Optionen werden angeboten:

1. „+ **Neuen Benutzer erstellen**“

Dieser Menüpunkt ruft die Option „Seite“ auf mit deren Hilfe Sie einen neuen Benutzer für die Agenten Installation erstellen können.



4. Zum Anlegen eines Benutzers müssen alle Felder ausgefüllt sein.
- Füllen Sie die Felder aus.
 - Beachten Sie die Kennwort-Hinweise.
 - Sobald alle Felder gefüllt sind, können Sie unten rechts auf „**Erstellen**“ klicken.

Allgemeine Informationen

E-Mail-Adresse (Benutzername):

Vorname:

Nachname:

Rolle:

Kennwort

Kennwort:

Kennwort bestätigen:

Benutzer muss das Kennwort ändern:

Benutzer-Rollen

Administrator:

Ein Benutzer vom Typ „Administrator“ darf Agents registrieren und konfigurieren, Jobs anlegen und ausführen und Benutzer anlegen.

Benutzer:

Ein Benutzer der Rolle „Benutzer“ darf Agents registrieren, von ihm registrierte oder ihm zugewiesene Agents konfigurieren sowie bei diesen Agents Jobs anlegen und ausführen.

Nur ausführen:

Ein Benutzer der Rolle „Nur ausführen“ darf bereits angelegte Jobs und die jeweiligen zugewiesenen Agents ausführen und Restore-Jobs auf diesen Server konfigurieren und starten.

Nur lesen:

Ein Benutzer der Rolle „Nur lesen“ darf nur den Status der von ihm zugewiesenen Agents und Jobs sehen.

3. Installation des VMware Agenten

Um vollständige VMs sichern zu können ist zwingend erforderlich, dass der Kunde über ein vCenter verfügt, da sich der Sicherungsagent nur hier anmelden kann. Des Weiteren sollte das vCenter am selben Standort wie der ESX laufen. Theoretisch ist es auch möglich über ein vCenter an einem anderen Standort zu sichern. Dies führt aber immer wieder Problemen mit Timeouts und ist daher nicht zu empfehlen.

Die Sicherung erfolgt über einen virtuellen Agent. Dieser muss aus einer OVA-Vorlage erstellt werden.

3.1. Einbinden des VMware Agenten in das vCenter

1. Starten Sie den vSphere Client und melden sie sich an dem vCenter an in das der vAgent eingebunden werden soll
2. Wählen Sie **„Datei / OVF Vorlage bereitstellen“**

OVF-Vorlage bereitstellen im vCenter

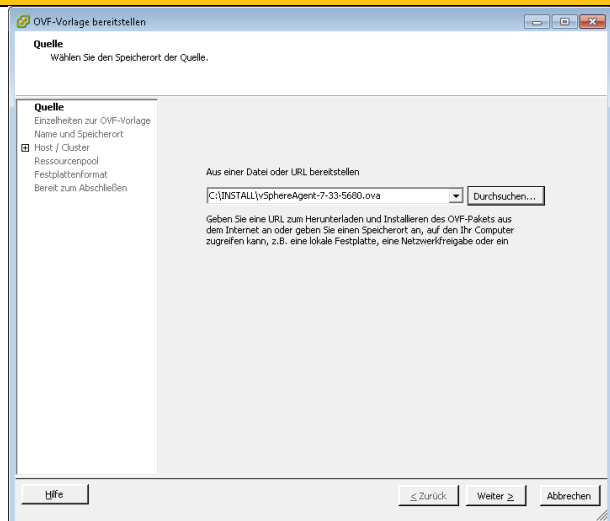
1. Klicken Sie auf „Datei“
2. OVF-Vorlage bereitstellen



3. Im folgenden Fenster die Vorlagedatei auswählen und dem Dialog weiter folgen.

OVF-Vorlage bereitstellen im vCenter

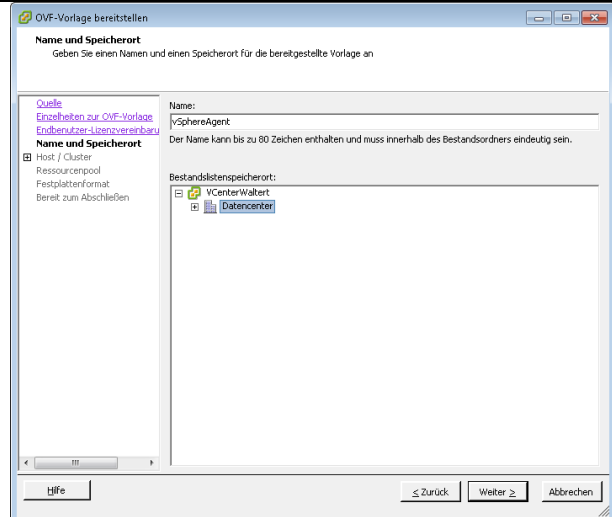
Wählen Sie die OVA-Dateien mit Hilfe von Durchsuchen. Klicken Sie anschließend auf „weiter“.



- Nachdem die Lizenzbedingungen akzeptiert wurden, müssen Name und Speicherort ausgewählt werden.

OVF-Vorlage bereitstellen im vCenter

Vergeben Sie einen Namen und wählen Sie aus welchem Datacenter der vAgent zugeordnet werden soll.



The screenshot shows the 'OVF-Vorlage bereitstellen' wizard in the vSphere Client. The current step is 'Name und Speicherort'. The 'Name' field contains 'vSphereAgent'. The 'Bestandslisten Speicherort' section shows a tree view with 'vCenter-Wallert' expanded and 'Datacenter' selected. The wizard includes navigation buttons: 'Hilfe', '< Zurück', 'Weiter >', and 'Abbrechen'.

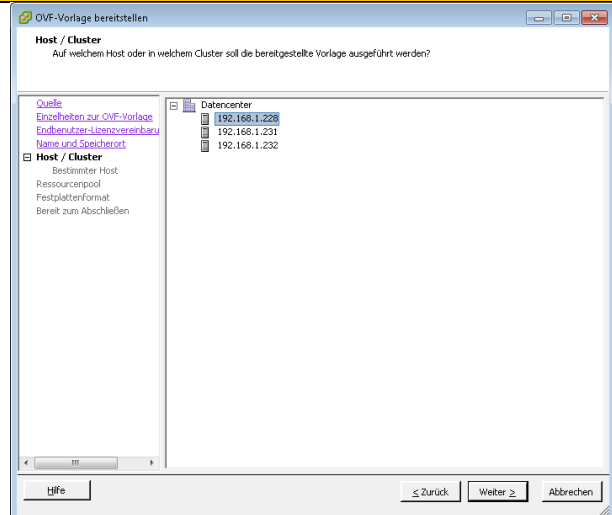
Der Name sollte auf die Funktion verweisen, zum Beispiel vAgent.

- Auf den folgenden Seiten wird ausgewählt auf welchem ESX der Agent läuft und in welche Datastore er liegen soll.

OVF-Vorlage bereitstellen im vCenter

Wählen Sie an dieser Stelle den entsprechenden ESX-Server des gewählten Datacenters aus, auf dem der vAgent bereitgestellt werden soll.

Anschließend müssen Sie noch auswählen in welche Datastore der vAgent abgelegt werden soll.

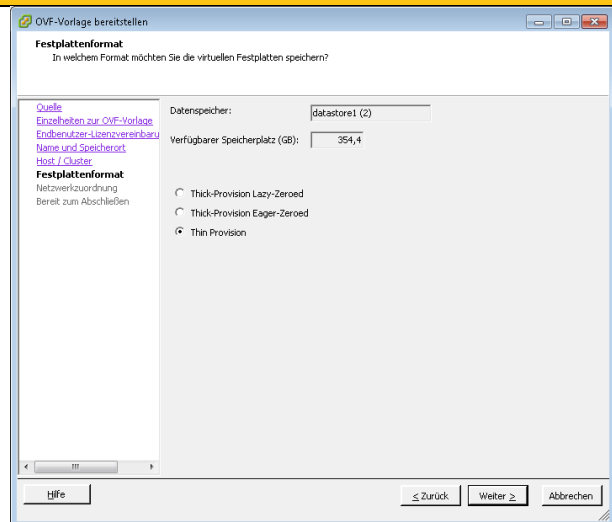


The screenshot shows the 'OVF-Vorlage bereitstellen' wizard in the vSphere Client. The current step is 'Host / Cluster'. The 'Datacenter' section is expanded, showing a list of ESX hosts with IP addresses: 192.168.1.228, 192.168.1.231, and 192.168.1.232. The wizard includes navigation buttons: 'Hilfe', '< Zurück', 'Weiter >', and 'Abbrechen'.

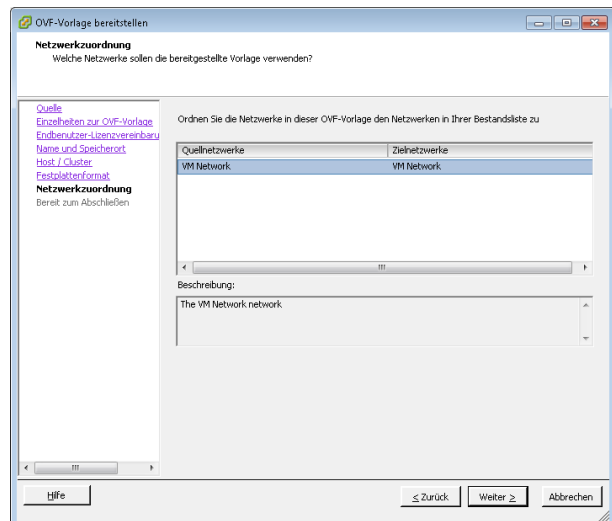
6. Als nächstes muss das Festplattenformat ausgewählt werden. Hierbei empfiehlt es sich „**Thin-Provision**“ auszuwählen, da der vAgent bei Thin-Provision in den seltensten Fällen die Größe von 160 GB erreicht wie es beim Thick-Provisioning der Fall ist. Abschließend ist noch das virtuelle Netzwerk auszuwählen in das der vAgent eingehängt werden soll. Starten Sie danach die Bereitstellung.

OVF-Vorlage bereitstellen im vCenter

Die Provision-Art der Festplatte auswählen.



Wählen Sie das entsprechende „**Virtuelle Netzwerk**“ und fahren Sie damit weiter fort.



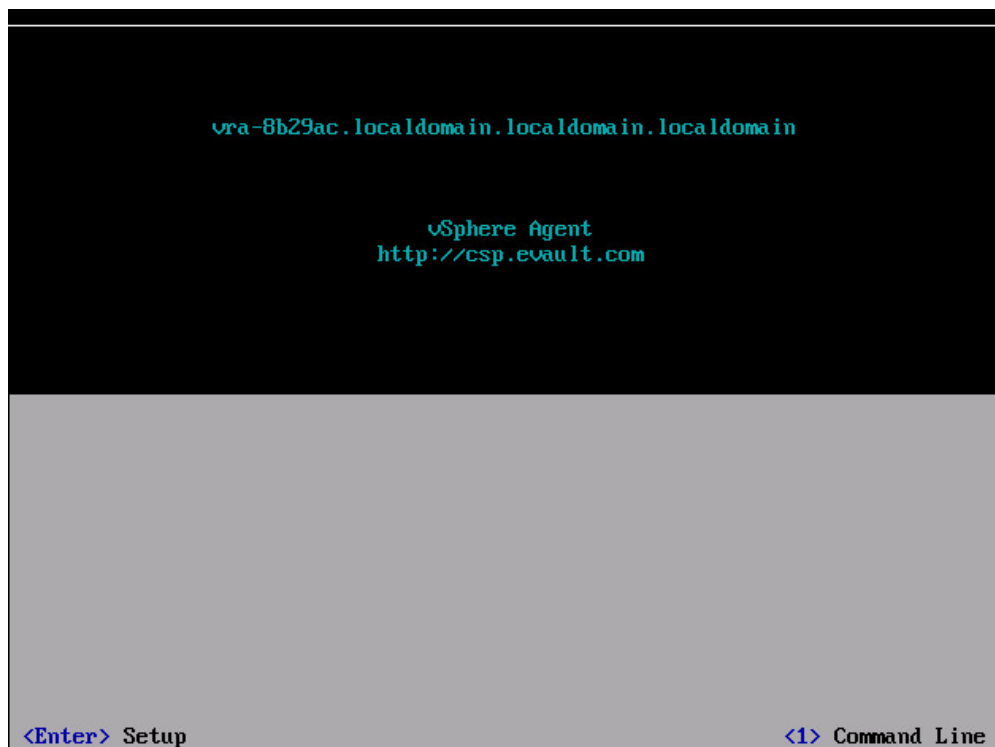
Hinweis:

Sobald die Bereitstellung abgeschlossen ist, kann der vAgent gestartet werden. Die Konfiguration erfolgt über das Konsolenfenster. Hierbei ist zu beachten, dass der Agent das „**US Tastaturlayout**“ verwendet.

4. Konfiguration des VMware Agenten

4.1. Grundkonfiguration

1. Die erste Grundkonfiguration startet man über „Enter“ und muss sich dann mit dem Benutzer „**sysadmin**“ und dem Kennwort „**sysadmin**“ anmelden. Hierbei bitte beachten, dass beim „**US Tastaturlayout**“ y und z vertauscht sind.



2. Als erstes sollte der „**Hostname**“ geändert werden. Der Hostname ist gleichzeitig der Name unter dem Sie den vAgent später im Webfrontend wiederfindet.
3. Ob Sie dem vAgent eine feste IP geben oder dieser eine IP per DHCP bezieht, ist für die Funktion und Verwaltbarkeit des vAgent unerheblich.

Hinweis:

Bei der Verwendung einer festen IP muss auch ein DNS eingetragen werden.

4. Nachdem alle Einstellungen gesetzt sind, kann man das Setup-Menü über ESC wieder verlassen. Die Einstellungen werden automatisch gespeichert.

4.2. Erweiterte Konfiguration

1. Diese wird über die Eingabe 1 geöffnet. Auch hier ist wieder die Anmeldung über den Benutzernamen „sysadmin“ und das Kennwort „sysadmin“ nötig.

```
Welcome to vSphere Agent 7.33.5680  
  
The default username/password is sysadmin/sysadmin  
vra-8b29ac login:
```

Der Befehlssatz auf der Konsole ist extrem eingeschränkt und weicht vollständig vom normalen Linux Befehlssatz ab. Über „help“ werden alle Grundbefehle aufgelistet. Um die Parameter des gewünschten Befehls aufgeführt zu bekommen, können Sie einfach den Befehl ohne Parameter eingeben.

2. Als erstes muss über den Befehl „**config set timezone Europe/Berlin**“ die Uhrzeit eingestellt werden.
3. Als nächstes muss der vAgent am vCenter angemeldet werden. Die Anmeldung erfolgt über den Befehl „**vCenter register [VCentername oder IP] Benutzername**“. Beim Benutzer muss es sich um einen Benutzer handeln, der im vCenter über Administratorrechte verfügt.

z.B: **vCenter register 192.168.1.230 root**

Nun werden die für die Kommunikation nötigen Ports abgefragt. Diese werden die Standard-Ports „**443**“ als Communication Port und „**902**“ als Data Port vorschlagen. Abschließend wird noch das Kennwort des Benutzers, mit dem die Registrierung durchgeführt wird, abgefragt.

4. Nachdem die Registrierung am vCenter abgeschlossen ist, muss der vAgent noch am Frontend angemeldet werden. Dies geschieht über den Befehl „**webcc register backup.rz-24.de 8086 Benutzer Kennwort**“. Beim Benutzer handelt es sich um den unter Ihnen mitgeteilten bzw. den von Ihnen angelegten Benutzer.
5. Hiermit ist die Einrichtung des Agents abgeschlossen und die Konsole kann per „Exit“ verlassen werden.

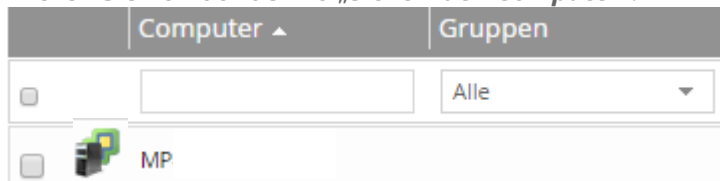
4.3. Konfiguration des Agenten im Webfrontend

Nach Abschluss der Installation erscheint der Agent automatisch im Webfrontend und kann nun hierüber konfiguriert werden.

1. Klicken Sie in der Navigation auf den Menüpunkt „**Computer**“.

Dashboard Computer Überwachung Berichte Richtlinien

2. Klicken Sie nun auf den zu „**Sichernden Computer**“.



3. Wählen Sie in der folgenden Ansicht den entsprechenden Menüpunkt „**Manuelle Konfiguration**“.

Manuell konfigurieren durch Bereitstellen von bestimmten Agent- und Vault-Einstellungen.

4.4. Hinzufügen eines Vault Profils

Als erstes muss dem Agent ein Vault-Profil zugewiesen werden. Das Vault Profil beschreibt das Sicherungsziel.

1. Klicken Sie dazu bitte auf den Button „**+Vault hinzufügen**“ im rechten Teil der Ansicht.
2. Hier wird Ihnen im Dropdown-Menü das entsprechende Profil zur Auswahl angeboten. Sollten Sie einen Satelliten einsetzen muss die Adresse ggf. von der URL auf die IP-Adresse des Satelliten umgestellt werden. Sollte das gewünschte Profil nicht vorhanden sein, können Sie die Daten auch händisch eingeben.

Vault-Einstellungen ? ✕

| | |
|--|--|
| <p>Grundeinstellungen</p> <p>Vault-Profil <input type="text" value="Vault-Profil"/></p> <p>Vault-Name <input type="text" value="Vault-Profil"/></p> <p>Adresse <input type="text" value="vault03.rz-24.de"/></p> <p>Konto <input type="text" value="Demo-Zugang101"/></p> <p>Benutzername <input type="text" value="ve_Demo-Zugang101"/></p> <p>Kennwort <input type="password" value="....."/></p> | <p>Erweiterte Einstellungen</p> <p>Agent-Hostname <input type="text" value="MP-AH-118596"/></p> <p>Portnummer <input type="text" value="2546"/></p> <p>Versuch, erneut alle zu verbinden <input type="text" value="180"/> Sekunden</p> <p>Verbindungsversuche abbrechen nach <input type="text" value="180"/> Minuten</p> <p><input checked="" type="checkbox"/> Over-the-Wire-Verschlüsselung für die Übertragung zum/vom Vault aktivieren</p> |
|--|--|

Vault Einstellungen im Detail

Diese Ansicht erläutert die entsprechenden Punkte, die Sie im vorherigen Schaubild sehen können.

| | |
|---|---|
| Vault Profile | Auswahl der hinterlegten Profile. |
| Vault Name | Name des Vault (kann frei vergeben werden). |
| Adresse | Adresse des Sicherungsziels. |
| Konto | Der Name Ihres Sicherungskontos (wird von der microPLAN GmbH vergeben). |
| Benutzername | Der Anmeldename Ihres Sicherungskontos (wird von der microPLAN GmbH vergeben). |
| Kennwort | Das Kennwort Ihres Sicherungskontos (wird von der microPLAN GmbH vergeben). |
| Agenten Hostname | Definiert den Namen, unter dem der Agent in den Reports angezeigt wird. Dieser Name kann nachträglich nicht mehr geändert werden. |
| Portnummer | 2546: Der Port für die Datenverbindung. |
| Versuch erneut alle zu verbinden | Definiert die Zeit zwischen zwei Verbindungsversuchen zum Sicherungsserver, wenn der Verbindungsaufbau fehlschlägt. |
| Verbindungsversuche Abbrechen nach | Definiert den Zeitraum, nachdem die Verbindungsversuche abgebrochen werden. |

4.5. Anlegen von Aufbewahrungstypen

Mit Hilfe von „**Aufbewahrungstypen**“ wird festgelegt, wie lange eine Sicherung auf dem Vault gespeichert wird.

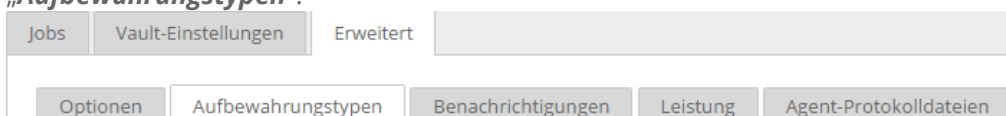
Standardmäßig sind drei Aufbewahrungstypen vorkonfiguriert.

- Daily : es werden bis zu 7 Sicherungen 7 Tage aufbewahrt.
- Weekly : es werden bis zu 5 Sicherungen 31 Tage aufbewahrt.
- Monthly : es werden bis zu 12 Sicherungen 365 Tage aufbewahrt.

Darüber hinaus können Sie beliebig individuelle Aufbewahrungstypen erstellen.

Um einen individuellen Aufbewahrungsplan zu erstellen, gehen Sie bitte wie folgt vor:

1. Wählen Sie nun den Menüpunkt „**Erweitert**“ und im unteren Teil den Punkt „**Aufbewahrungstypen**“.



2. Ihnen wird nun eine Listung mit aller vorhandenen Aufbewahrungstypen angezeigt.

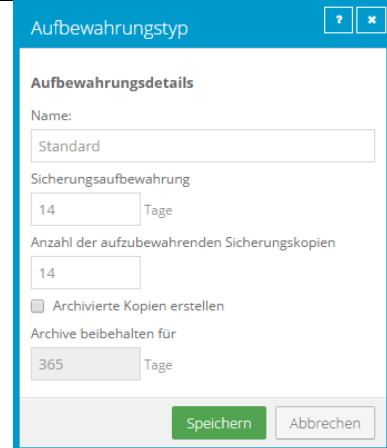
| Aufbewahrungsname | Onlinespeicherung (Tage) | Onlinekopien | Archivierungsdauer (Tage) | |
|-------------------|--------------------------|--------------|---------------------------|---|
| Daily | 7 | 7 | --- |   |
| Monthly | 365 | 12 | --- |   |
| Weekly | 31 | 5 | --- |   |

- Sie haben hier nun die Möglichkeit eigene „**Aufbewahrungstypen**“ anzulegen. Klicken Sie dazu im oberen Teil auf den Button „**+Aufbewahrungstypen erstellen**“. Es öffnet sich nun ein Fenster in dem Sie einen „**Aufbewahrungstypen**“ erstellen können.

Aufbewahrungstypen erstellen im Detail

Hier haben Sie nun die Möglichkeit, einen neuen Aufbewahrungstypen zu erstellen.

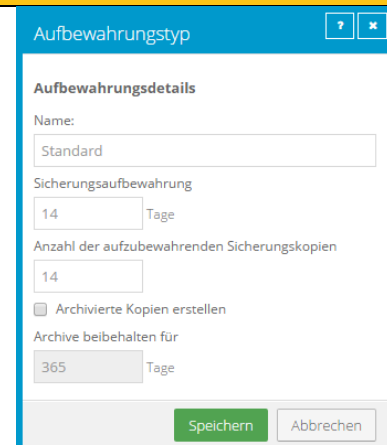
- Vergeben Sie einen beliebigen Namen.
- Definieren Sie, wie lange eine Sicherung dieses Aufbewahrungstyps gespeichert werden soll.
- Legen Sie die Anzahl der Kopien fest, die gespeichert werden sollen.
- Speichern Sie.



Beispiel:

Es sollen 6 Sicherungen 6 Monate gespeichert werden.

- Vergeben Sie einen Namen.
- Stellen Sie die „**Sicherungsaufbewahrung**“ auf 186 Tage ein.
- Stellen Sie die „**Anzahl der aufzubewahrenden Sicherungskopien**“ auf 6 ein.



Achtung: Beide Bedingungen müssen erfüllt sein, damit ein Safeset gelöscht wird. Wird eine Sicherung, wie in unseren Beispiel Aufbewahrungstyp verwendet, innerhalb der 186 ein 7. Mal ausgeführt, wird das älteste Safeset erst gelöscht, wenn es 186 Tage alt ist. Ebenso würde ein Safeset das zwar 186 Tage alt ist, aber von dem es nur 5 Versionen gibt, solange nicht gelöscht, bis die Anzahl von 6 Safesets erreicht ist.

4.6. Anlegen von Benachrichtigungen

Benachrichtigungen dienen der Information. Wird diese Funktion aktiviert, versendet der Agent -bei Abschluss jeder Sicherung die dieser Agent ausführt- eine Benachrichtigung.

Hinweis: Die Benachrichtigungen werden per E-Mail an einen Empfänger geschickt. Sie benötigen hierzu einen Mailserver, der vom Agent aus per SMTP erreichbar ist. Es wird kein Mailserver durch die microPLAN GmbH gestellt.

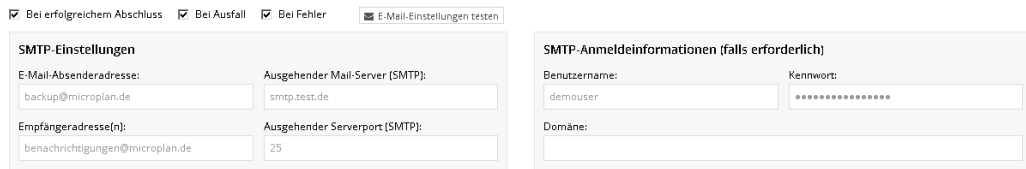
Um dem Agent eine Benachrichtigung hinzuzufügen gehen Sie bitte wie folgt vor:

1. Wählen Sie den Menüpunkt „**Erweitert**“ und im unteren Teil den Punkt „**Benachrichtigungen**“.



The screenshot shows a navigation bar with tabs: 'Jobs', 'Vault-Einstellungen', 'Erweitert', and an unlabeled tab. Below the 'Erweitert' tab, there is a sub-menu with buttons for 'Optionen', 'Aufbewahrungstypen', 'Benachrichtigungen', 'Leistung', and 'Agent-Protokolldateien'. The 'Benachrichtigungen' button is highlighted.

2. Sie müssen nun eine Absenderadresse, einen erreichbaren Mail-Server sowie eine Zieladresse angeben. Zusätzlich haben Sie die Möglichkeit Authentifikationsdaten zu hinterlegen.



The screenshot shows the 'SMTP-Einstellungen' form. It includes checkboxes for 'Bei erfolgreichem Abschluss', 'Bei Ausfall', and 'Bei Fehler', along with an 'E-Mail-Einstellungen testen' button. The form fields are:

- SMTP-Einstellungen:**
 - E-Mail-Absenderadresse: backup@microplan.de
 - Ausgehender Mail-Server (SMTP): smtp.test.de
 - Empfängeradresse(n): benachrichtigungen@microplan.de
 - Ausgehender Serverport (SMTP): 25
- SMTP-Anmeldeinformationen (falls erforderlich):**
 - Benutzername: demouser
 - Kennwort: [masked]
 - Domäne: [empty]

Folgende Optionen zur Benachrichtigung stehen Ihnen zur Verfügung:

- Bei einem erfolgreichem Abschluss: Nach erfolgreicher Sicherung.
- Bei Ausfall: Wenn ein Ausführzeitpunkt verpasst wurde.
- Bei Fehler: Bei fehlgeschlagenen Sicherungen.

4.7. Anmeldung am vCenter



The screenshot shows the 'vCenter-Einstellungen' form. It includes fields for 'vCenter-Adresse' (192.168.155.18443), 'Benutzername' (administrator@vghere.local), and 'Kennwort' (password). There is a checkbox for 'CBT (Changed Block Tracking) für virtuelle Maschinen während der Sicherung aktivieren' and a 'vCenter-Verbindung testen' button. A blue information box states: 'Dabei werden die erweiterten Eigenschaften der für die Sicherung ausgewählten virtuellen Maschine geändert. Mit CBT verbessert sich die Leistung der Sicherung einer virtuellen Maschine, es können aber monatliche Leistungsberichte auf der virtuellen Maschine verursacht werden.'

Nun muss der Agent noch zum Auslesen der virtuellen Maschinen am vCenter angemeldet werden.

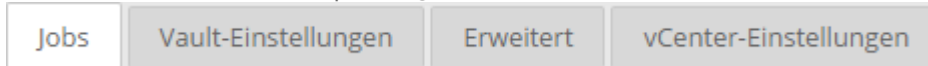
Hierzu müssen Sie unter dem Punkt „vCenter-Einstellungen“ die Zugangsdaten, mit denen Sie den vAgent bereits am vCenter registriert haben, noch mal hinterlegen.

Hinweis: Die Angabe der Domain ist nur nötig, wenn ein Benutzer außerhalb der Benutzerverwaltung des vCenters verwendet wird.

5. Datensicherung

Nun da der Agent konfiguriert ist, können die Sicherungen angelegt werden.

1. Wählen Sie nun den Menüpunkt „**Jobs**“.

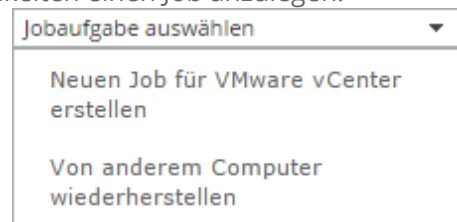


2. Wählen Sie im rechten Teil der Webseite den Menüpunkt „**Jobaufgabe auswählen**“.

Jobaufgabe im Detail

Im Dropdown-Menü haben Sie diverse Möglichkeiten einen Job anzulegen.

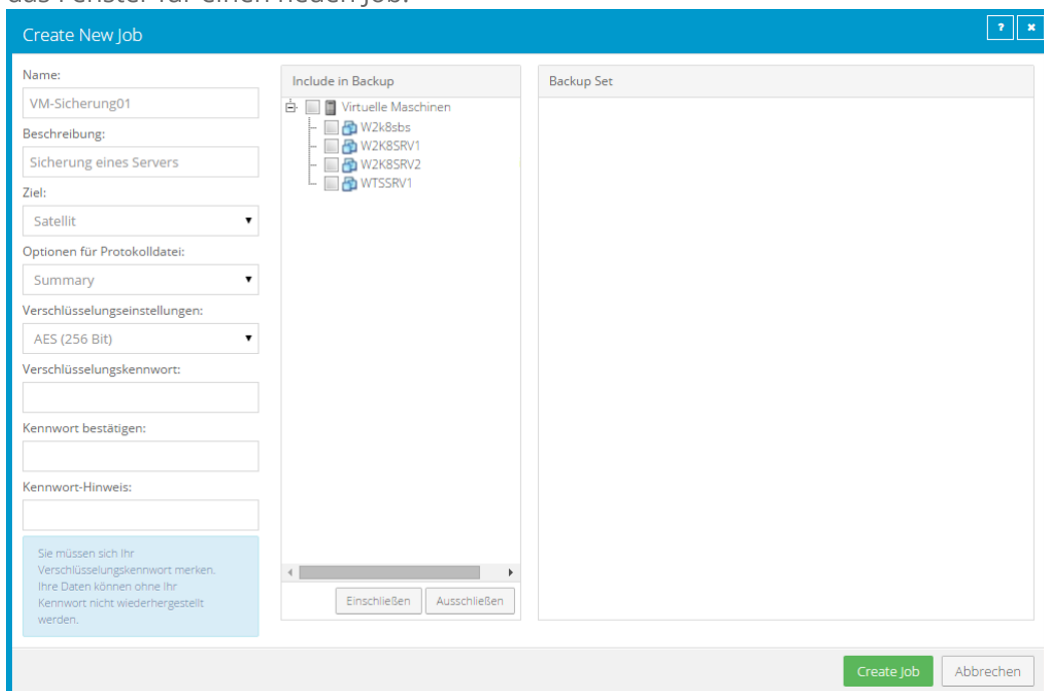
1. Neuen Job für VMware vCenter erstellen.
2. Von anderem Computer wiederherstellen.



Wählen Sie an dieser Stelle bitte „**Neuen Job für VMware vCenter erstellen**“.

5.1. Einrichten einer Datensicherung

1. Um eine Sicherung von „**Virtuellen Maschinen**“ anzulegen, wählen Sie den Menüpunkt „**Neuen Job für VMware vCenter erstellen**“.
2. Nachdem Sie „**Neuen Job für VMware vCenter erstellen**“ gewählt haben, öffnet sich das Fenster für einen neuen Job.



Neuen Job erstellen im Detail

Um einen neuen Job zu erstellen, bedarf es gewisser Einstellungen.

1. Es muss ein Name für den Sicherungsjob vergeben werden.

Name:

Sicherung

2. Es kann eine Beschreibung hinzugefügt werden.

Beschreibung:

Sicherung von Daten

3. Das Sicherungsziel muss zugewiesen werden. (Hier können nur die vorher dem Agent zugewiesenen Vault Profile ausgewählt werden.)

Ziel:

Vault-Profil

4. Hier wird die Art der Protokollierung des Jobs festgelegt. Im normalen Betrieb sollte „Summary“ vollkommen ausreichen.

Optionen für Protokolldatei:

Summary

5. Hier kann die Verschlüsselungsart ausgewählt werden. Standardmäßig ist „AES“ ausgewählt. Alternativ wird hier zwar auch die Möglichkeit geboten die Verschlüsselung abzuschalten. Die Sicherungsserver der microPLAN GmbH nehmen unverschlüsselte Sicherungen nicht an.

Verschlüsselungseinstellungen:

AES (256 Bit)

6. Abschließend wird noch das Verschlüsselungskennwort vergeben.

Kennwort:

Hinweis zum Verschlüsseln:

1. Bewahren Sie das Verschlüsselungskennwort gut auf. Ohne das Verschlüsselungskennwort ist kein Zugriff und somit auch keine Wiederherstellung Ihrer gesicherten Daten möglich.

Kennwort bestätigen:

2. Wenn das Verschlüsselungskennwort geändert wird, wird automatisch eine neue Vollsicherung durchgeführt.

Kennwort-Hinweis:

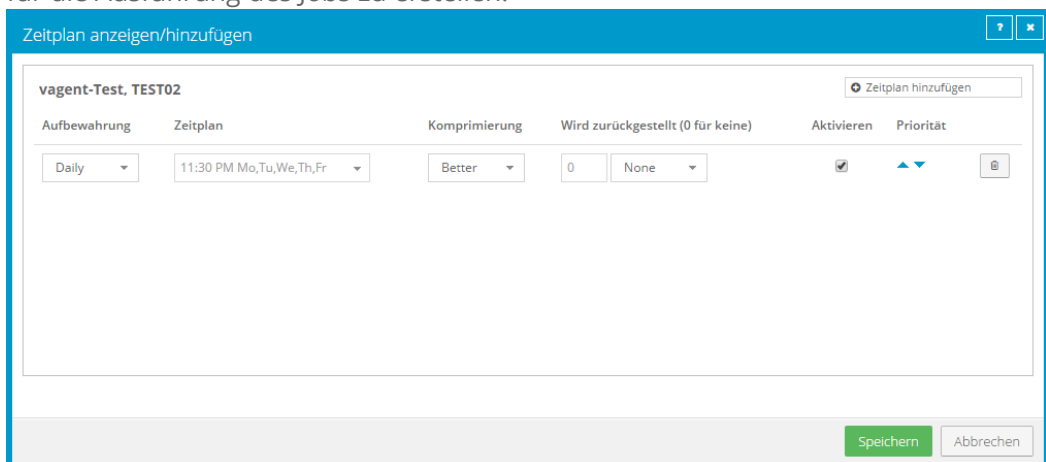
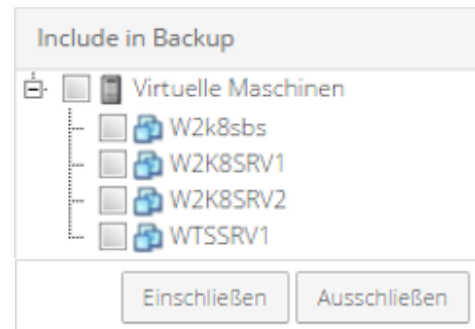
Nun können Sie in der mittleren Spalte festlegen, welche „Virtuellen Maschinen“ gesichert werden sollen.

Empfehlung: Pro Job möglichst nicht mehr als 5 Server sichern, da es sonst vorkommen kann, dass es zu Lesefehlern beim Sichern einzelner Maschinen des Jobs kommen kann, die Sicherung des betroffenen Servers abgebrochen und der Snapshot des Servers zurückgelassen wird.

Beispiel:

Sie wollen den „w2k8srv1“ sichern.

1. Wählen Sie „w2k8srv1“.
2. Klicken Sie auf „**Einschließen**“.
3. Nachdem Sie den Job erstellt haben, haben Sie noch die Möglichkeit einen Zeitplan für die Ausführung des Jobs zu erstellen.



Anlegen eines Zeitplans im Detail

| | |
|----------------------------|---|
| Aufbewahrung | Hier müssen Sie einen Aufbewahrungstyp auswählen, der das Aufbewahrungsmuster Ihrer Sicherung bestimmt. |
| Zeitplan | Hier stellen Sie ein, wann und wie spät Ihre Sicherung ausgeführt wird. Zur Auswahl stehen Tage der Woche, Tage des Monats sowie die Möglichkeit eigene Startzeitpunkte zu definieren. Achtung: Das US Zeitformat AM / PM beachten! |
| Komprimierung | Hier kann der Grad der Komprimierung eingestellt werden. Den besten Kompromiss zwischen Rechenlast und Komprimierungsgrad bietet „Better“. |
| Wird zurückgestellt | Diese Option bietet die Möglichkeit, nach einem bestimmten Zeitfenster die Sicherung abzubrechen und die noch nicht gesicherten Daten bis zur nächsten Sicherung zurückzustellen. Achtung: Da bei der nächsten Sicherung die Prüfung der Dateien auf Änderungen von vorne beginnt, kann dies dazu führen, dass wenn die Menge der geänderten Daten dauerhaft zu groß für das Sicherungszeitfenster ist, Daten am Ende der Auswahl nie gesichert werden. |
| Aktivieren | Diese Option aktiviert und deaktiviert den Zeitplan. |
| Priorität | In Zeitplänen mit mehreren Schemulern, können diese über die Prioritätspfeile sortiert werden. Achtung: Bei mehreren Zeitplänen wird immer der erste zutreffende verwendet. |

- Vom System wird bei der Konfiguration automatisch ein Zeitplan angelegt. Weitere Zeitpläne können Sie oben rechts über den Button „**+Zeitplan Hinzufügen**“ hinzufügen. Hierbei ist zu beachten, dass der Zeitplan, der am seltensten ausgeführt wird, an oberster Stelle steht.

Möchten Sie also eine Sicherung erstellen, die täglich läuft und zusätzlich eine Wochen- und Monatssicherung durchführt, müsste als oberstes die Monatssicherung aufgeführt werden, dann die Wochensicherung und als unterstes die Tagessicherung. Wenn mehrere Zeitpläne gleichzeitig zutreffen, die Sicherung aber nur einmal durchgeführt werden soll (zum Beispiel bei einer Tagessicherung, die jeden Tag läuft und einer Monatssicherung, die an jedem ersten des Monats ausgeführt wird), muss der Startzeitpunkt gleich sein.

Sobald alle Einstellungen getroffen wurden, beenden Sie die Konfiguration des Jobs, indem Sie auf „Speichern“ klicken.

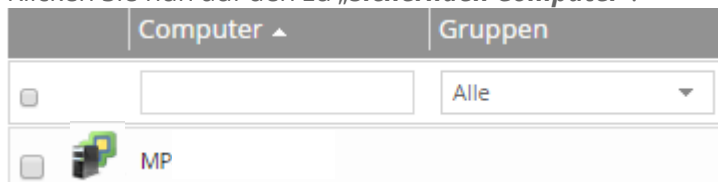
6. Restore einer Datensicherung

Im Fall des Falles ist es nötig, Daten aus einer Datensicherung wiederherzustellen. Damit Daten wiederhergestellt werden können, gehen Sie bitte wie folgt vor.

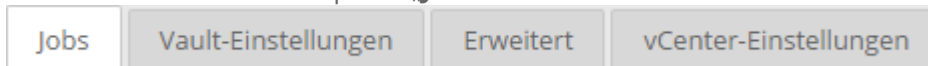
1. Klicken Sie in der Navigation auf den Menüpunkt „**Computer**“.

Dashboard **Computer** Überwachung Berichte Richtlinien

2. Klicken Sie nun auf den zu „**Sichernden Computer**“.



3. Wählen Sie nun den Menüpunkt „**Jobs**“.



4. Es öffnet sich nun die Übersicht mit allen „**Jobs**“ die zum Computer vorhanden sind.

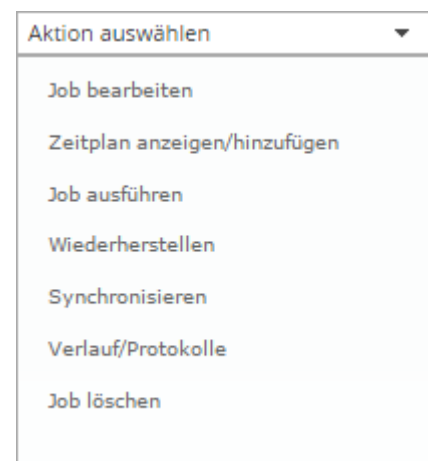
| Name | Jobtyp | Beschreibung | Letzter Sicherungsstatus | Letzte Ausführung | Aktion |
|--------------|---------|--------------|--------------------------|--------------------|------------------|
| VM-Sicherung | vSphere | | ✓ Abgeschlossen | yesterday at 22:40 | Aktion auswählen |

5. Wählen Sie nun unter „**Aktion auswählen**“ den Punkt „**Wiederherstellen**“.

Aktion im Detail

Um eine Aktion zum Job zu hinterlegen ist es nötig, auf „**Aktion auswählen**“ zu klicken.

1. Job bearbeiten
2. Zeitplan anzeigen/hinzufügen
3. Job ausführen
4. Wiederherstellen
5. Synchronisieren
6. Verlauf/Protokolle
7. Job löschen



6. Nachdem Sie „**Wiederherstellen**“ gewählt haben, bekommen Sie ein Auswahlmenü mit drei Optionen.

vSphere-Wiederherstellung

Wiederherzustellende Elemente auswählen

Virtuelle Maschinen
Gesamte virtuelle Maschinen auf einem vSphere-Host wiederherstellen: Verwenden Sie diese Einstellung bei der Wiederherstellung mehrerer virtueller Maschinen oder beim Disaster Recovery.

Hinweis: Wenn eine VM, die wiederhergestellt wird, weiterhin im vCenter vorhanden ist, wird die neu erstellte VM als Kopie der ursprünglichen VM angezeigt. Daher müssen Sie eventuell Ihre Sicherung ändern, um die wiederhergestellte VM einzubeziehen. Dies verursacht ein erneutes Seeding der VM.

Virtuelle Festplatten
Einzelne VMDK-Dateien von virtuellen Maschinen im ausgewählten Sicherungsjob wiederherstellen: Verwenden Sie diese Einstellung zum Abrufen von Daten, ohne gesamte virtuelle Maschinen wiederherzustellen.

Dateien und Ordner
Einzelne Dateien oder Ordner von einem virtuellen Datenträger wiederherstellen: Mit dieser Option wird der virtuelle Datenträger als freigegebene Ressource festgelegt. Anschließend kann er zur Wiederherstellung von Dateien und Ordnern (oder des gesamten Datenträgers) bereitgestellt werden, ohne die gesamte virtuelle Maschine wiederherzustellen.

Weiter Abbrechen

vSphere-Wiederherstellung im Detail

Um eine Aktion zum Job zu hinterlegen ist es nötig, auf „**Aktion auswählen**“ zu klicken.

- | | | |
|----|-----------------------|---|
| 1. | Virtuelle Maschine | Bietet die Möglichkeit, die vollständige virtuelle Maschine wiederherzustellen und wenn gewünscht am vCenter zu registrieren. |
| 2. | Virtuelle Festplatten | Bietet die Möglichkeit, einzelne vmdk-Dateien wiederherzustellen. |
| 3. | Dateien und Ordner | Bietet die Möglichkeit, einzelne Dateien aus einer virtuellen Festplatte wiederherzustellen. |

6.1. Restore – Virtuelle Maschine

Es öffnet sich nun das Fenster mit dessen Hilfe Sie wählen können, welche virtuellen Maschinen an welcher Stelle wiederhergestellt werden können.

?
✕
Wiederherstellung vra-9c3b3c -> Faro-Restore-Test

Quellgerät

Vault (TestVaultDaKl) ▼

Safeset

3 (23.02.2016 22:03) 📅

Wiederherzustellende Elemente

- azeti-manager
- z_mptest-vSphereAgent

Verschlüsselungskennwort

?

Ziel-Datastore

Auswählen ▼

- Alle ausgewählten virtuellen Maschinen nur im ausgewählten Datastore wiederherstellen
- Nur im ausgewählten Datastore wiederherstellen, wenn der ursprüngliche Datastore einer virtuellen Maschine nicht verfügbar ist

Zielhost:

▼

- Alle ausgewählten virtuellen Maschinen nur für den ausgewählten Host registrieren
- Nur für den ausgewählten Host registrieren, wenn der ursprüngliche Host einer virtuellen Maschine nicht verfügbar ist
- VMs nach der Wiederherstellung einschalten

Details der Protokollebene

Summary ▼

Leistungsoptionen

- Gesamte verfügbare Bandbreite nutzen

Wiederherstellung ausführen

Abbrechen

Wiederherstellen im Detail

Safeset:

Hier legen Sie fest, von welchem Zeitpunkt Sie die Daten wiederherstellen möchten. Automatisch wird immer das neueste Backup vorgeschlagen.

Safeset

3 (23.02.2016 22:03)



Quellgerät:

Als nächstes wählen Sie aus, von wo Sie wiederherstellen wollen. Im Normalfall ist dies immer Ihr Vault Profil.

Wenn sehr große Datenmengen wiederhergestellt werden müssen ist es aber auch möglich, diese auf einen Datenträger exportieren zu lassen, der Ihnen dann zugesandt wird und bei der Wiederherstellung als Quelle dient. Bei dem Export handelt es sich weiterhin um verschlüsselte Dateien, die bei der Wiederherstellung entschlüsselt werden.

Quellgerät

Vault (TestVaultDaKI)



Wiederherzustellende Elemente

Hier kann ausgewählt werden, welche virtuellen Maschinen wiederhergestellt werden sollen. Zur Auswahl stehen alle im ausgewählten Safeset vorhandenen virtuellen Maschinen.

Wiederherzustellende Elemente

- azeti-manager
- z_mptest-vSphereAgent

Verschlüsselungskennwort:

Hier müssen sie das Verschlüsselungskennwort, das Sie bei der Einrichtung der Sicherung vergeben haben, eingeben.

Hinweis: Ohne das Kennwort ist keine Wiederherstellung möglich.

Verschlüsselungskennwort



Zieldatastore

Hier können Sie aus einer Liste aller Datastores, auf die der vAgent Zugriff hat, auswählen.

Des Weiteren kann hier festgelegt werden, ob noch vorhandene alte virtuelle Maschinen überschrieben werden sollen oder nicht.

Ziel-Datastore

Auswählen



- Alle ausgewählten virtuellen Maschinen nur im ausgewählten Datastore wiederherstellen
- Nur im ausgewählten Datastore wiederherstellen, wenn der ursprüngliche Datastore einer virtuellen Maschine nicht verfügbar ist

Zielhost

Hier kann ausgewählt werden, auf welchem ESX die virtuelle Maschine registriert werden soll. Hier werden nur die ESX angeboten, die Zugriff auf den ausgewählten Datastore haben. Zusätzlich wird auch hier wieder festgelegt, ob vorhandene Registrierungen von alten virtuellen Maschinen überschrieben werden sollen und ob die virtuelle Maschine nach der Wiederherstellung automatisch eingeschaltet werden soll.

Details der Protokollebene

Hier wird die Art der Protokollierung des Jobs festgelegt. Im Normalfall sollte „Summary“ vollkommen ausreichen.

Zielhost:

- Alle ausgewählten virtuellen Maschinen nur für den ausgewählten Host registrieren
- Nur für den ausgewählten Host registrieren, wenn der ursprüngliche Host einer virtuellen Maschine nicht verfügbar ist
- VMs nach der Wiederherstellung einschalten

Details der Protokollebene

Abschließend starten Sie mit „**Wiederherstellungen ausführen**“ die gewünschte Wiederherstellung.

6.2. Restore – Virtuelle Festplatte

Es öffnet sich das Fenster mit dessen Hilfe Sie wählen können, welche virtuellen Maschinen an welcher Stelle wiederhergestellt werden können.

?
✕
Wiederherstellung vra-9c3b3c -> Faro-Restore-Test

Quellgerät

Vault (TestVaultDaKl) ▼

Safeset

3 (23.02.2016 22:03) 📅

Ziel-Datastore

Auswählen ▼

Ordner

▼

Neuen Ordner erstellen

✓

Details der Protokollebene

Summary ▼

Leistungsoptionen

Gesamte verfügbare Bandbreite nutzen

Wiederherzustellende Elemente

- 📁 azeti-manager
- 📁 z_mptest-vSphereAgent

Verschlüsselungskennwort

?

Wiederherstellung ausführen

Abbrechen

Wiederherstellen im Detail

Quellgerät:

Wählen Sie aus, von wo Sie wiederherstellen wollen. Im Normalfall ist dies immer ihr Vault Profil. Wenn sehr große Datenmengen wiederhergestellt werden müssen, ist es aber auch möglich diese auf einen Datenträger exportieren zu lassen, der Ihnen dann zugesandt wird und bei der Wiederherstellung als Quelle dient. Bei dem Export handelt es sich weiterhin um verschlüsselte Dateien, die bei der Wiederherstellung entschlüsselt werden.

Quellgerät

Vault (TestVaultDaKl)

Safeset:

Hier legen Sie fest, von welchem Zeitpunkt Sie die Daten wiederherstellen möchten. Automatisch wird immer das neuste Backup vorgeschlagen.

Safeset

3 (23.02.2016 22:03)

Wiederherzustellende Elemente

Hier kann ausgewählt werden, welche vmdk-Dateien wiederhergestellt werden sollen. Zur Auswahl stehen alle Dateien der im ausgewählten Safeset vorhandenen virtuellen Maschinen.

Wiederherzustellende Elemente

- azeti-manager
- z_mptest-vSphereAgent
 - [datastore1] mptest-vSphereAgent
 - [datastore1] mptest-vSphereAgent

Verschlüsselungskennwort:

Hier müssen Sie das Verschlüsselungskennwort, das Sie bei der Einrichtung der Sicherung vergeben haben, eingeben. **Hinweis:** Ohne das Kennwort ist keine Wiederherstellung möglich.

Verschlüsselungskennwort

Zielfatadastore

Hier wählen Sie, in welchem Datastore und welchem Ordner die wiederherzustellenden Dateien abgespeichert werden sollen. Alternativ haben Sie die Möglichkeit einen neuen Ordner im ausgewählten Datastore anzulegen.

Ziel-Datastore

Auswählen

Ordner

Neuen Ordner erstellen

Details der Protokollebene

Hier wird die Art der Protokollierung des Jobs festgelegt. Im Normalfall sollte „Summary“ vollkommen ausreichen

Details der Protokollebene

Summary

Abschließend starten Sie mit „**Wiederherstellungen ausführen**“ die gewünschte Wiederherstellung.

6.3. Restore – Dateien und Ordner

Es öffnet sich nun das Fenster mit dessen Hilfe Sie wählen können, welche virtuellen Maschinen an welcher Stelle wiederhergestellt werden können.

Wiederherstellung vra-9c3b3c -> Faro-Restore-Test
?
✕

Quellgerät

Vault (TestVaultDaKl)
▼

Idle Time

minutes

Safeset

3 (23.02.2016 22:03)
📅

Wiederherzustellende Elemente

- 📁 [datastore1] mptest-vSphereAgent/mpt
- 📁 [datastore1] mptest-vSphereAgent/mpt
- 📁 [VVol15-MR-LUN15] azeti-manager/azet

Verschlüsselungskennwort

🔑

Freigeben

Abbrechen

Die Freigabe wird automatisch nach der Dauer der Inaktivität beendet.

Gesamte verfügbare Bandbreite nutzen

Wiederherstellen im Detail

Quellgerät:

Als nächstes wählen Sie aus, von wo Sie wiederherstellen wollen. Im Normalfall ist dies immer Ihr Vault Profil.

Wenn sehr große Datenmengen wiederhergestellt werden müssen, ist es aber auch möglich diese auf einen Datenträger exportieren zu lassen, der Ihnen dann zugesandt wird und bei der Wiederherstellung als Quelle dient. Bei dem Export handelt es sich weiterhin um verschlüsselte Dateien die bei der Wiederherstellung entschlüsselt werden.

Quellgerät

Vault (TestVaultDaKl)

Safeset:

Hier legen Sie fest, von welchem Zeitpunkt Sie die Daten wiederherstellen möchten. Automatisch wird immer das neueste Backup vorgeschlagen.

Safeset

3 (23.02.2016 22:03)

Wiederherzustellende Elemente

Hier wählen Sie aus, von welcher der im Safeset vorhandenen Festplatten Sie Daten wiederherstellen wollen.

Wiederherzustellende Elemente

- [datastore1] mptest-vSphereAgent/mpt
- [datastore1] mptest-vSphereAgent/mpt
- [Vol15-MR-LUN15] azeti-manager/azet

Verschlüsselungskennwort:

Hier müssen Sie das Verschlüsselungskennwort, das Sie bei der Einrichtung der Sicherung vergeben haben, eingeben.

Verschlüsselungskennwort

Hinweis: Ohne das Kennwort ist keine Wiederherstellung möglich.

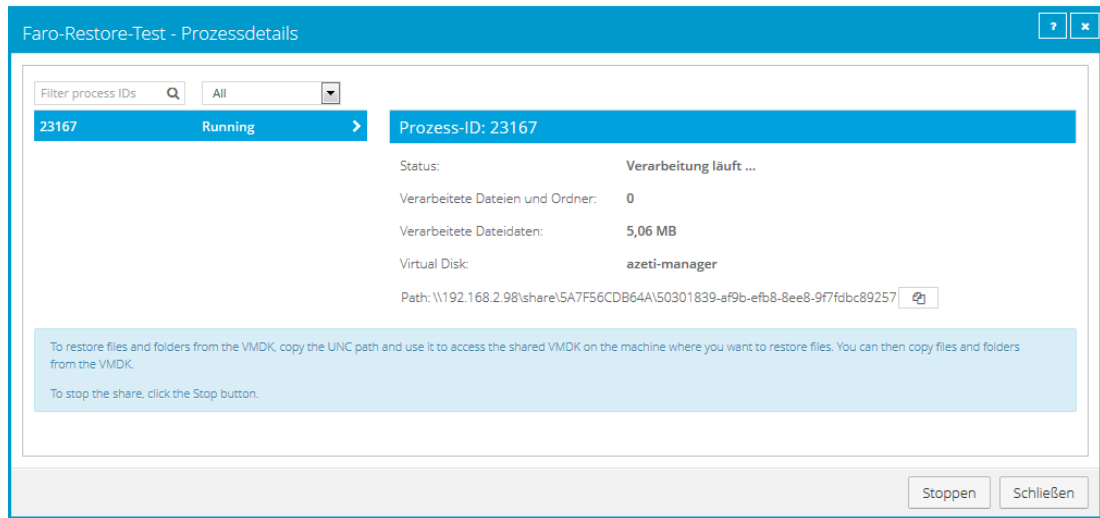
Idle Time

Hier stellen Sie ein, nach welcher Zeit ohne Zugriff, die Bereitstellung der Festplatte aufgehoben wird.

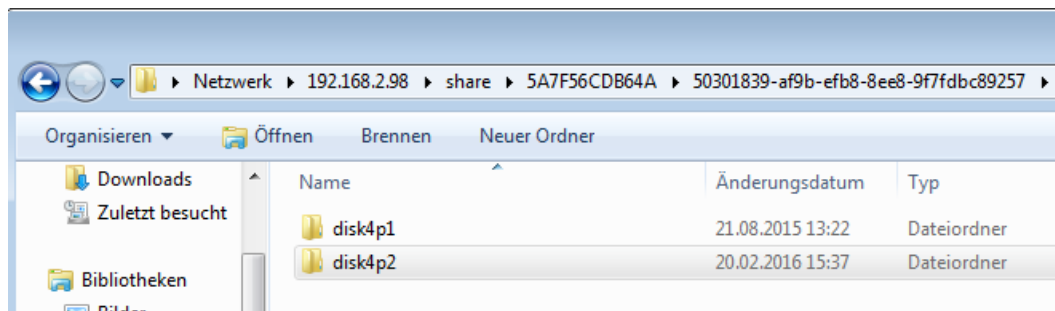
Idle Time

5 minutes

Sobald Sie die Auswahl über „Freigeben“ bestätigen, wird die ausgewählte Festplatte am vAgent gemountet und als Freigabe bereitgestellt.



Um auf die Daten der Festplatte zugreifen zu können, kopieren Sie den Freigabepfad in den Explorer eines Rechners, der den vAgent erreichen kann. Hier können Sie nun die gewünschten Dateien oder Ordner heraussuchen und an den gewünschten Ort kopieren.



Nachdem alle gewünschten Order/Dateien wiederhergestellt sind, kann die Freigabe der Festplatte entweder per „Stop-Button“ beendet werden. Alternativ hebt der Agent die Freigabe nach der eingestellten Idle-Time wieder auf.

7. vAgent Konsolenbefehle

7.1. agent

| | |
|---------------|---|
| agent start | Startet die Agent Dienste. |
| agent stop | Stoppt die Agent Dienste. |
| agent restart | Startet die Agent Dienste neu. |
| agent status | Zeigt den Ausführstatus der Agent Dienste an. |

7.2. config

| | |
|---|--|
| config set date MM/DD/YYYY HH:MM[:SS] | Setzt manuell Uhrzeit und Datum auf dem vAgent. |
| config set timezone <timezone> | Setzt die Zeitzone des vAgent auf den gewünschten Wert. |
| config show timezones [help regions all] [list <region-name>] | Listet alle Zeitzonen auf. Wahlweise kann die Auflistung auch auf eine Region z.B. Europa beschränkt werden. |

7.3. mount

| | |
|---|--|
| mount add [//host/share [[domain/]username guest]] | Mountet ein beliebiges Netzlaufwerk (z.B. als „Backup to Disk“-Verzeichnis). |
| mount remove [all] | Trennt alle verbundenen Netzlaufwerke. |
| mount list | Listet alle verbundenen Netzlaufwerke auf. |

7.4. net

| | |
|-----------------------------------|--|
| net hosts add <ipaddr> <hostname> | Fügt den angegebenen Host der hosts-Datei des vAgents hinzu. |
| net hosts del <ipaddr> | Entfernt den angegebenen Host aus der hosts-Datei des vAgent. |
| net hosts show | Gibt die hosts-Datei des vAgent aus. |
| net hosts reset | Setzt die hosts-Datei zurück. |
| net nslookup <hostname ipaddr> | Findet den Namen des gewünschten Hosts. |
| net ping <host> | Sende „pings“ an den angegebenen Host. |
| net reset | Setzt die gesamte Netzwerkkonfiguration auf die Default-Einstellungen zurück. |
| net set hostname <hostname> | Setzt den Hostname des vAgents. |
| net show config [all] | Zeigt die Netzwerkkonfiguration des vAgents. |
| net show dhcp | Zeigt, ob die IP-Adresse des vAgents per DHCP zugewiesen oder fest vergeben wurde. |
| net show hostname | Zeigt den Hostnamen des vAgents. |
| net show routes | Zeigt die Routingtabelle des vAgents. |
| net show status | Zeigt den aktuellen Netzwerkverbindungsstatus sowie offene Ports. |

7.5. ntp

| | |
|------------------|---|
| ntp add <server> | Fügt einen Zeitserver hinzu. |
| ntp del <server> | Entfernt einen Zeitserver. |
| ntp show | Zeigt den aktuell verwendeten Zeitserver. |
| ntp sync | Startet manuell den Sync mit dem Zeitserver. |
| ntp reset | Setzt den Zeitserver auf pool.ntp.org zurück. |

7.6. ssh

| | |
|-------------|---|
| ssh enable | Aktiviert den ssh-Zugriff auf den vAgent. |
| ssh disable | Deaktiviert den ssh-Zugriff auf den vAgent. |
| ssh status | Zeigt den Status des ssh-Zugriffs. |

7.7. support

| | |
|---|---|
| support logs scp [[user@]host[:path]] copy guest]] | Erstellt aus den Logs und Einstellung des [/hostname/share/path[[domain/]usernamevAgents angegebenen Netzwerkpfad ab. |
|---|---|

7.8. system

| | |
|--|--|
| system reboot [force] | Startet den vAgent neu. |
| system show date | Zeigt das aktuelle Datum und die Uhrzeit des vAgents. |
| system password | Ermöglicht das neue Setzen des sysadmin Kennwortes. |
| system show uptime | Zeigt wie lange der vAgent läuft. |
| system shutdown [force] | Führt den vAgent herunter. |
| system upgrade [manual username password] | Prüft, ob Updates für den vAgent verfügbar sind und bietet diese zur Installation an. |

7.9. vcenter

| | |
|---|--|
| vcenter register [<vCenter> [<backup username>]] | Registriert den vAgent an einem vCenter. |
| vcenter change login [<backup username>] | Setzt die Logindaten für das vCenter neu. |
| vcenter show | Zeigt mit welchem vCenter der vAgent verbunden ist. |
| vcenter unregister [<backup username>] | Hebt die Registrierung am vCenter auf. |

7.10. webcc

| | |
|--|--|
| webcc register <WebCCAddress> <port> <login> <password> | Registriert den vAgent am Backup Portal. |
|--|--|