

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.	Installation des EVault Agents	- 6 -
4.	Konfiguration des VMware Agenten	- 8 -
4.1.	Konfiguration des Agenten im Webfrontend	- 8 -
4.2.	Hinzufügen eines Vault Profils	- 8 -
4.3.	Anlegen von Aufbewahrungstypen	- 10 -
4.4.	Anlegen von Benachrichtigungen.....	- 12 -
4.5.	Anmeldung am vCenter	- 12 -
5.	Datensicherung	- 13 -
5.1.	Einrichten einer Datensicherung	- 13 -
6.	Restore einer Datensicherung	- 17 -
6.1.	Restore – Virtuelle Maschine	- 19 -
6.2.	Restore – Virtuelle Festplatte	- 22 -
6.3.	Restore – Dateien und Ordner	- 24 -



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 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. 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 Web Frontend 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 Web Frontend

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

URL:

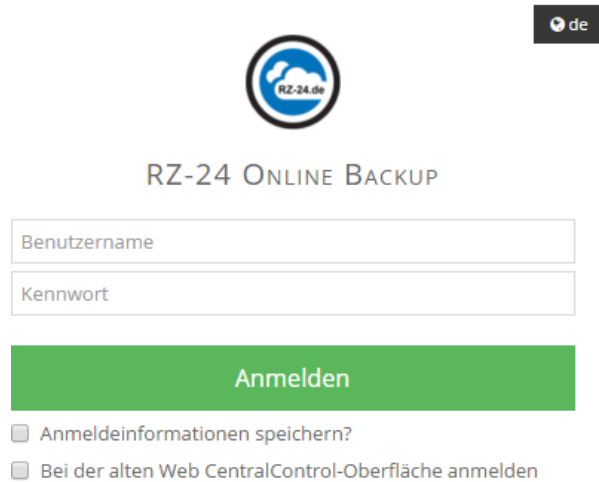
<https://backup.rz-24.de/>

Benutzername:

Ihr Benutzer

Kennwort:

Ihr Kennwort



Hinweis:

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

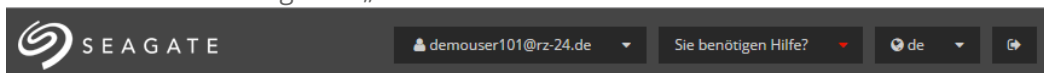
2.2. Anlegen von Benutzern

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



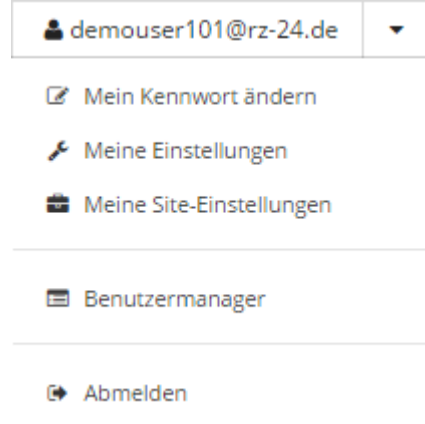
- Im erscheinenden Dropdown-Menü haben Sie nun die Möglichkeit, den „**Benutzermanager**“ aufzurufen

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)



demouser101@rz-24.de ▼

- Mein Kennwort ändern
- Meine Einstellungen
- Meine Site-Einstellungen
- Benutzermanager
- Abmelden

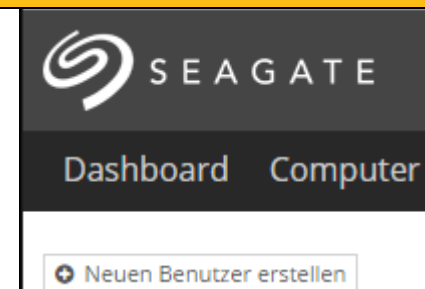
- Nachdem Sie den Benutzermanager aufgerufen haben, sehen Sie im oberen Teil der Webseiten den Menüpunkt „**Neuen Benutzer erstellen**“. Wählen Sie bitte diese Option um einen neuen Benutzer zu erstellen.

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.



SEAGATE

Dashboard Computer

+ Neuen Benutzer erstellen

- 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):
Kundenname@kd.microplan.de

Vorname:
Kunden

Nachname:
Name

Rolle:
Benutzer

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

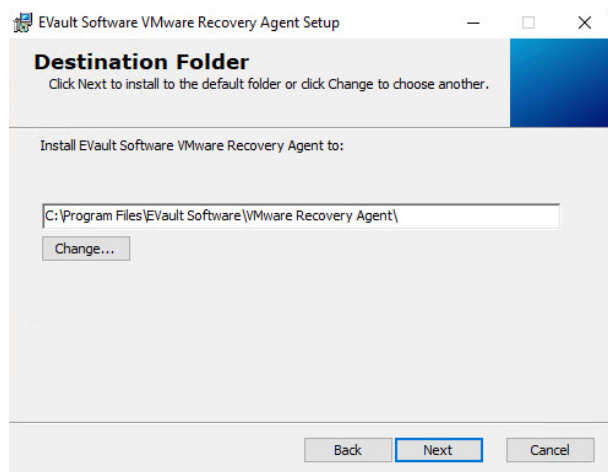
Um vollständige VMs sichern zu können, ist zwingend erforderlich, dass der Kunde über ein vCenter verfügt, da sich der Sicherungsagent nur hier anmelden kann. Des Weiteren sollte das vCenter am selben Standort wie der ESX laufen. Theoretisch ist es auch möglich über ein vCenter an einem anderen Standort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

Der Agent unterstützt als Basis aktuell nur Windows 10 und Windows Server 2012 R2. Laut Vorgabe des Softwareherstellers ist es verboten den Agenten auf einem Satelliten, dem Domain Controller, einem Mailserver, oder Datenbankserver zu installieren. Wir empfehlen für den Agenten eine eigene virtuelle Maschine zu erstellen. Minimalvoraussetzungen sind hier 2 vCPUs und 4 GB RAM.

3.1. Installation des EVault Agents

Gehen Sie dazu wie folgt vor: Die Installation starten, den Nutzungsbedingungen zustimmen und dem Dialog weiter folgen.

Im nächsten Schritt muss der Installationspfad gewählt werden.



Abschließend muss der Agent noch am Webportal registriert werden.

Netzwerkadresse:

- backup.rz-24.de

Port:

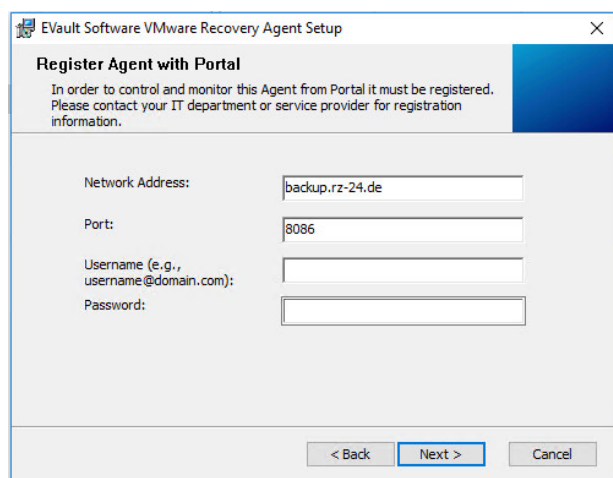
- 8086

Benutzername:

- Der Ihnen mitgeteilte Benutzername bzw. der von Ihnen angelegte Benutzer aus dem Webportal.

Kennwort:

- Das Ihnen mitgeteilte Kennwort bzw.



EVault Agent für Windows – VMware	22.11.2017
--------------------------------------	------------



Hinweis / Empfehlung:

- Legen Sie den entsprechenden Benutzer im Webportal an.
- Wird die Registrierung übersprungen, sind die weiteren Schritte nicht möglich.

4. Konfiguration des VMware Agenten

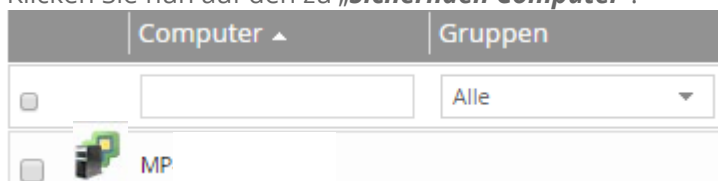
4.1. Konfiguration des Agenten im Web Frontend

Nach Abschluss der Installation erscheint der Agent automatisch im Web Frontend 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**“.



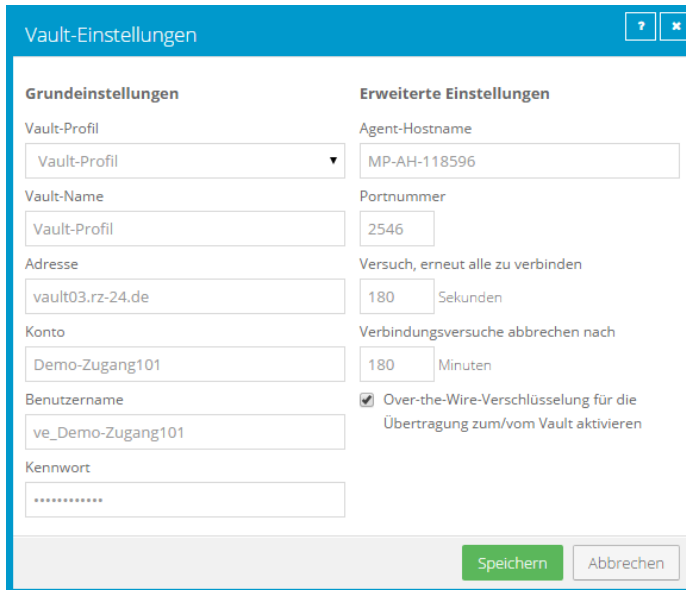
3. Wählen Sie in der folgenden Ansicht den entsprechenden Menüpunkt „**Manuelle Konfiguration**“.



4.2. 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 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 vergeben).
Benutzername	Der Anmeldeame Ihres Sicherungskontos (wird von der microPLAN vergeben).
Kennwort	Das Kennwort Ihres Sicherungskontos (wird von der microPLAN 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.

4.3. Anlegen von Aufbewahrungstypen

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

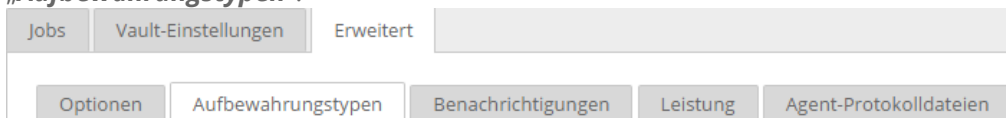
Standardmäßig sind drei Aufbewahrungstypen vorkonfiguriert.

Daily : es werden bis zu 7 Sicherungen 7 Tage aufbewahrt.
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	30	30	...
Monthly	365	11	...

3. 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

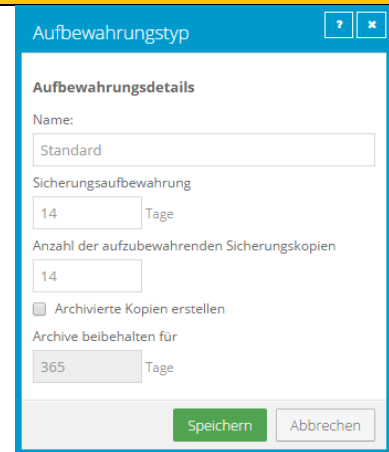
Hier haben Sie nun die Möglichkeit, einen neuen Aufbewahrungstypen zu erstellen.

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

Beispiel:

Es sollen 6 Sicherungen 6 Monate gespeichert werden.

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



Aufbewahrungstyp

Aufbewahrungsdetails

Name:
Standard

Sicherungsaufbewahrung
14 Tage

Anzahl der aufzubewahrenden Sicherungskopien
14

Archivierte Kopien erstellen

Archive beibehalten für
365 Tage

Speichern Abbrechen

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.

4.4. 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 gestellt.

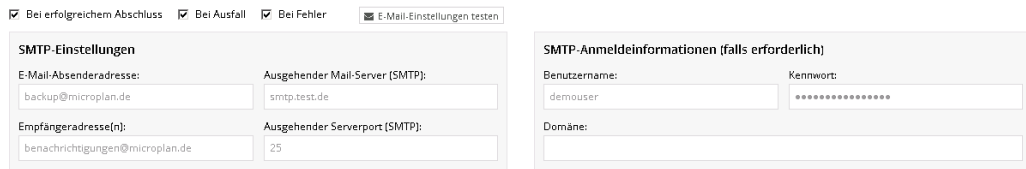
Um dem Agent eine Benachrichtigung hinzuzufügen gehen Sie bitte wie folgt vor:

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



The screenshot shows a navigation menu with 'Erweitert' selected. Below it, a sub-menu is open, highlighting 'Benachrichtigungen'.

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

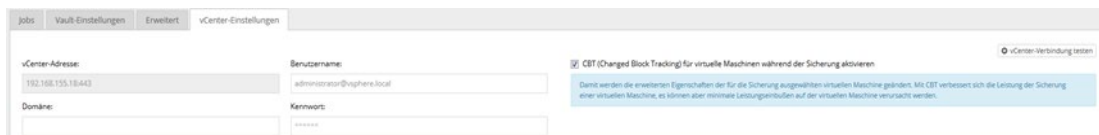


The screenshot shows the 'SMTP-Einstellungen' form. It includes checkboxes for 'Bei erfolgreichem Abschluss', 'Bei Ausfall', and 'Bei Fehler', and a checkbox for 'E-Mail-Einstellungen testen'. The form has fields for 'E-Mail-Absenderadresse', 'Ausgehender Mail-Server (SMTP)', 'Empfängeradresse(n)', and 'Ausgehender Serverport (SMTP)'. There is also a section for 'SMTP-Anmeldeinformationen (falls erforderlich)' with fields for 'Benutzername', 'Kennwort', and 'Domäne'.

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.

4.5. Anmeldung am vCenter



The screenshot shows the 'vCenter-Einstellungen' form. It includes fields for 'vCenter-Adresse', 'Benutzername', 'Domäne', and 'Kennwort'. There is a checkbox for 'CBT (Changed Block Tracking) für virtuelle Maschinen während der Sicherung aktivieren' and a button for 'vCenter-Verbindung testen'.

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

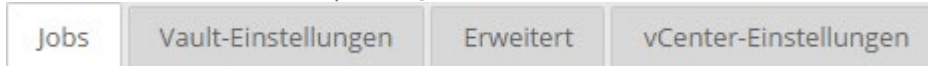
Hierzu müssen Sie unter dem Punkt „**vCenter-Einstellungen**“ die Zugangsdaten, mit denen Sie den vAgent bereits am vCenter registriert haben, noch mal hinterlegen.

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**“.

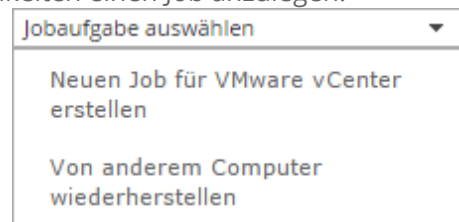


2. Wählen Sie im rechten Teil der Webseite den Menüpunkt „**Jobaufgabe auswählen**“.

Jobaufgabe im Detail

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

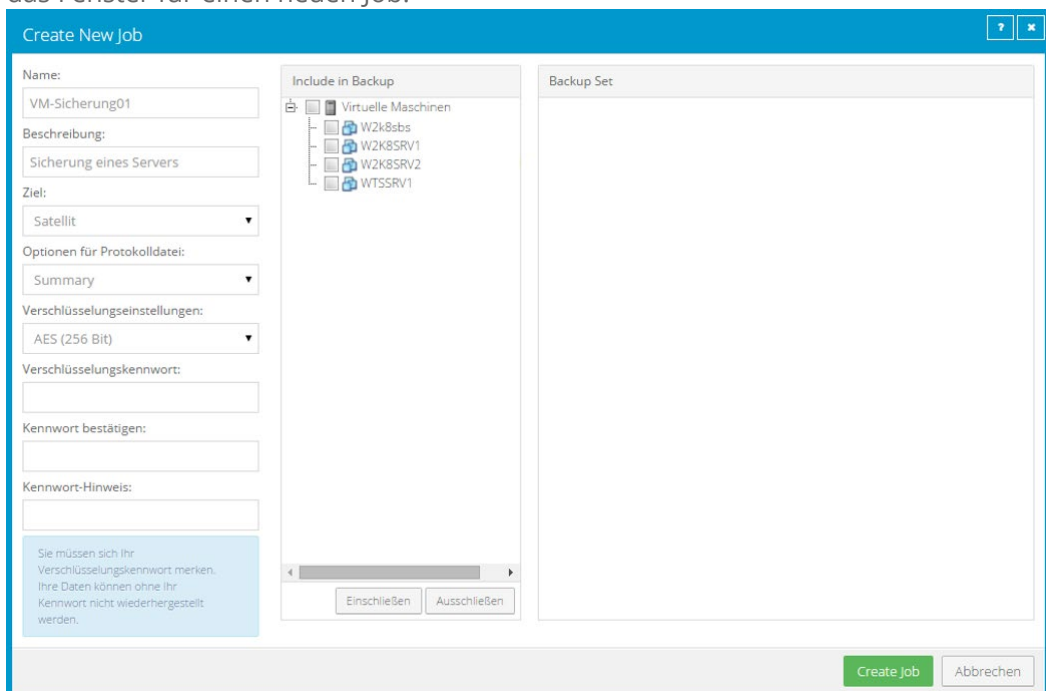
1. Neuen Job für VMware vCenter erstellen.
2. Von anderem Computer wiederherstellen.



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 auch die Möglichkeit geboten die Verschlüsselung abzuschalten. Die Sicherungsserver von microPLAN 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:

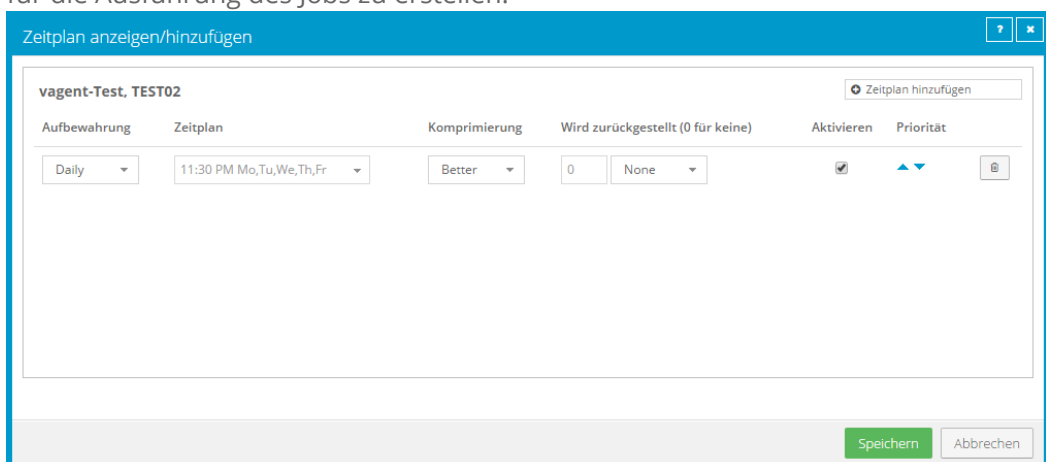
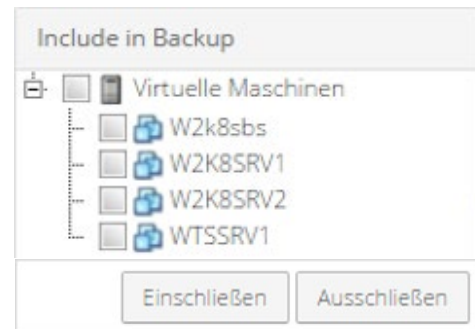
Nun können Sie in der mittleren Spalte festlegen, welche „Virtuellen Maschinen“ gesichert werden sollen.

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 abubrechen 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 Schedulingern, 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.

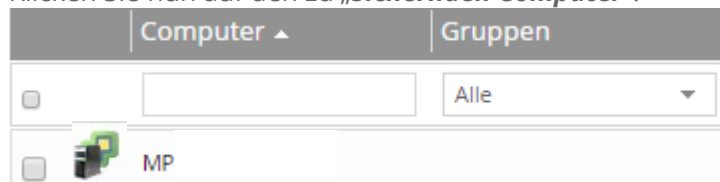
6. Restore einer Datensicherung

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

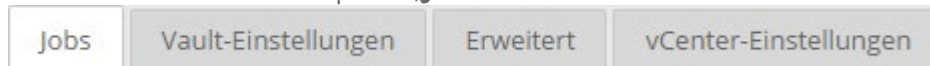
1. Klicken Sie in der Navigation auf den Menüpunkt „**Computer**“.

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.

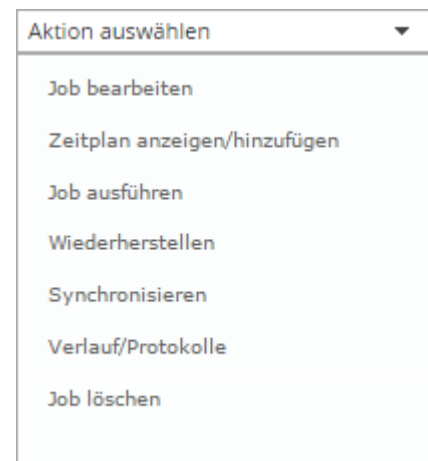
Name	Jobtyp	Beschreibung	Letzter Sicherungsstatus	Letzte Ausführung	Aktion
VM-Sicherung	vSphere		<input checked="" type="checkbox"/> Abgeschlossen	yesterday at 22:40	Aktion auswählen

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 neuste 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 Festplatten an welcher Stelle wiederhergestellt werden können.

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

Quellgerät
Vault (TestVaultDaKl)

Ziel-Datstore
Auswählen

Safeset
3 (23.02.2016 22:03)

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 (TestVaultDaKI)

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

Zielformat:

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 Dateien und Ordner 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 neuste 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.

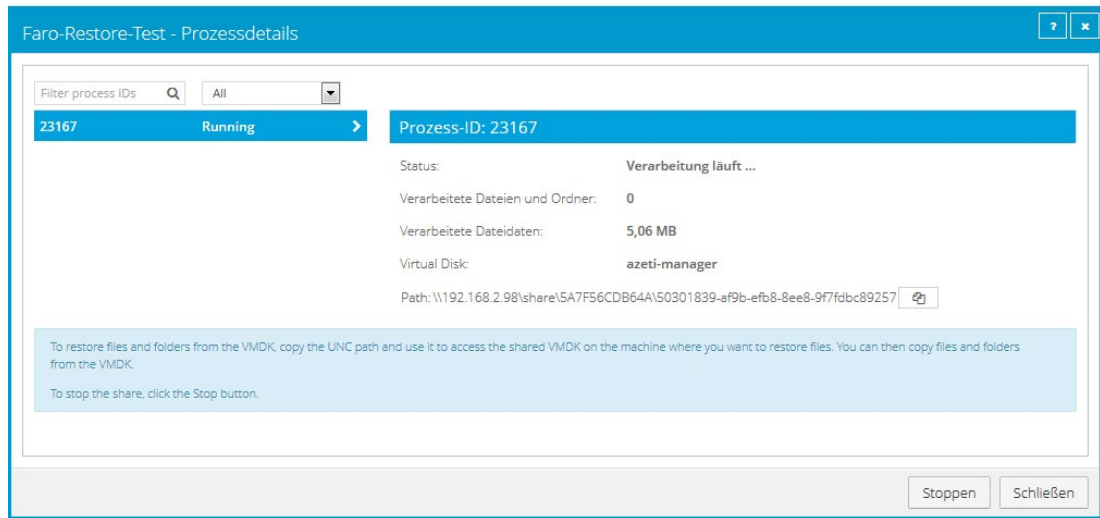
Idle Time

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

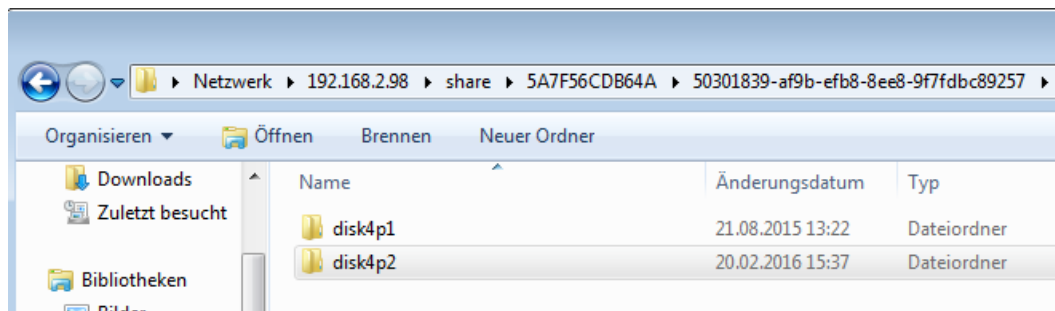
Idle Time

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 per „**Stop-Button**“ beendet werden. Alternativ hebt der Agent die Freigabe nach der eingestellten Idle-Time wieder auf.