

vSphere Recovery Agent 9.1

Benutzerhandbuch

© Copyright-Inhaber 2022. Alle Rechte vorbehalten.

Für die Nutzungsbedingungen, siehe <https://s3.amazonaws.com/carbonite.com/docs-and-files/release+notes/License.pdf>.

Der Softwarehersteller übernimmt keine Gewährleistung für die Inhalte des vorliegenden Dokuments und lehnt insbesondere jegliche impliziten Gewährleistungen hinsichtlich der handelsüblichen Qualität oder der Eignung für einen bestimmten Zweck ab. Darüber hinaus behält sich der Softwarehersteller das Recht vor, diese Veröffentlichung zu revidieren und jederzeit Änderungen an dem Inhalt des vorliegenden Dokuments vorzunehmen, ohne dass eine Pflicht aufseiten des Softwareherstellers besteht, irgendeine Person über eine solche Revision oder Änderungen zu benachrichtigen. Alle Unternehmen, Namen und Daten, die in den hierin genannten Beispielen verwendet wurden, sind fiktiv, sofern nichts anderes angegeben ist.

Kein Teil des vorliegenden Dokuments darf ohne vorherige schriftliche Genehmigung auf irgendeine Weise oder mit irgendwelchen Mitteln, weder elektronisch, mechanisch, magnetisch, optisch, chemisch oder in sonstiger Weise reproduziert, übertragen, umgeschrieben, in einem Abrufsystem gespeichert oder in irgendeine Sprache einschließlich Computersprache übersetzt werden.

Alle anderen Produkte oder Namen von Unternehmen, die in diesem Dokument genannt werden, sind Marken oder eingetragene Marken der jeweiligen Inhaber.

Lizenzhinweise: Zwei Verschlüsselungsmethoden, DES und TripleDES, enthalten Verschlüsselungssoftware von Eric Young. Die Windows-Versionen dieser Algorithmen enthalten zusätzlich Software von Tim Hudson. Die Blowfish-Verschlüsselung wurde von Bruce Schneier entwickelt.

„Ein Teil der in dieses Produkt eingebetteten Software ist gSOAP-Software. Für die von gSOAP erstellten Teile gilt ein Copyright (C) 2001 - 2006 Robert A. van Engelen, Genivia Inc. Alle Rechte vorbehalten. DIE SOFTWARE IN DIESEM PRODUKT WURDE TEILWEISE VON GENIVIA INC BEREITGESTELLT UND SÄMTLICHE AUSDRÜCKLICHEN ODER IMPLIZITEN GEWÄHRLEISTUNGEN WERDEN AUSGESCHLOSSEN, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF GEWÄHRLEISTUNGEN DER HANDELSÜBLICHEN QUALITÄT UND DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. KEINESFALLS HAFTET DER AUTOR FÜR IRGENDWELCHE DIREKTEN, INDIREKTEN, ZUFÄLLIG ENTSTANDENEN, KONKRETEN SCHÄDEN, STRAFEEINSCHLIESSENDEN SCHADENERSATZ ODER FOLGESCHÄDEN (INSBESONDERE NICHT FÜR DIE BESCHAFFUNG VON ERSATZGÜTERN ODER -DIENSTLEISTUNGEN, FÜR NUTZUNGSAusFALL, DATENVERLUST, ENTGANGENE GEWINNE ODER BETRIEBSUNTERBRECHUNGEN), GANZ GLEICH IN WELCHER WEISE UND AUF WELCHER HAFTUNGSRECHTLICHEN ANSPRUCHSGRUNDLAGE, OB VERTRAGLICH, KAUSAL ODER DELIKTISCH (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER ANDERES), SIE IN VERBINDUNG MIT DER VERWENDUNG DIESER SOFTWARE AUCH ENTSTEHEN MÖGEN, SELBST WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.“

Die Anwendungen Agent, Agent Console und Vault verfügen über die zusätzliche Verschlüsselungsoption mit 128/256-Bit-AES (Advanced Encryption Standard). Der Advanced Encryption Standard-Algorithmus (namens Rijndael, ausgesprochen „Reyndoll“) wurde von den Kryptografen Dr. Joan Daemen und Dr. Vincent Rijmen entwickelt. Dieser Algorithmus wurde vom National Institute of Standards and Technology (NIST) des US-amerikanischen Handelsministeriums als neuer Standard für die Informationsverarbeitung (Federal Information Processing Standard, FIPS) festgelegt.

Die Agent- und Vault-Anwendungen bieten auch das zusätzliche Sicherheitsfeature einer Over-the-Wire-Verschlüsselungsmethode.

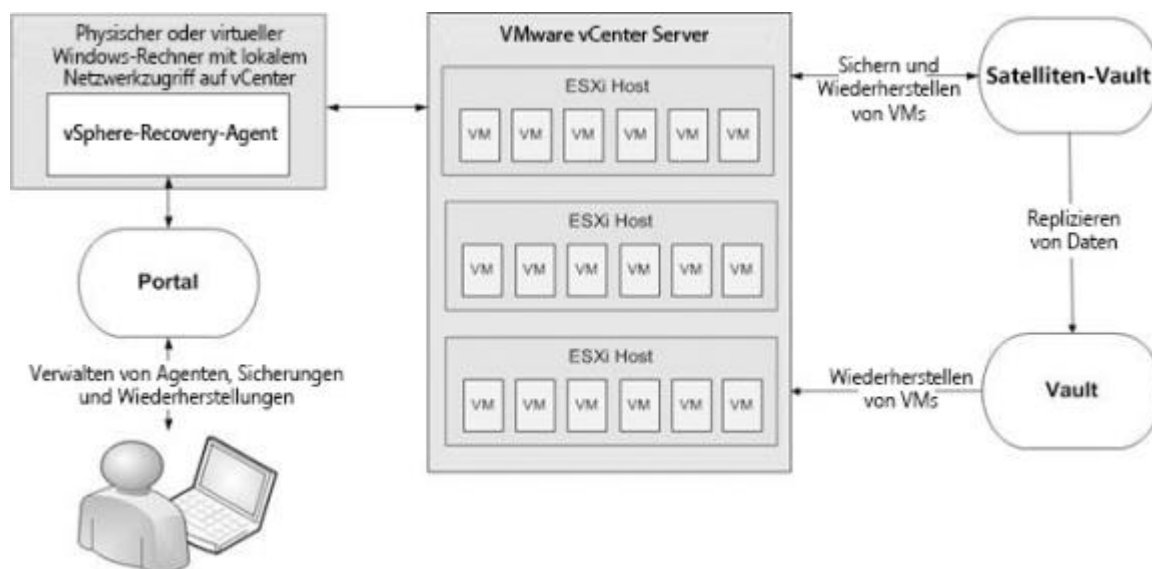
Inhalt

1 Einführung in den vSphere Recovery Agent	5
2 Vorbereiten der Installation des vSphere Recovery Agent.....	7
2.1 Portal zum Verwalten des vSphere-Recovery-Agenten.....	7
2.2 Vaults für Sicherungen des vSphere-Recovery-Agenten	7
2.3 Empfohlene Bereitstellung für vSphere-Recovery-Agent.....	7
2.4 Anforderungen für bestimmte Funktionen von vSphere Recovery-Agent	8
2.5 vSphere-Recovery-Agenten-Ports	11
2.6 Empfehlungen und Einschränkungen zu vSphere-Recovery-Agent	12
2.7 Installieren des vSphere-Recovery-Agenten im unbeaufsichtigten Modus.....	13
2.8 Upgraden des vSphere Recovery Agent.....	14
2.9 Upgraden des vSphere Recovery Agent im unbeaufsichtigten Modus	15
2.10 Deinstallieren des vSphere Recovery Agent	15
2.11 Deinstallieren des vSphere Recovery Agent im unbeaufsichtigten Modus	15
3 Konfigurieren des vSphere-Recovery-Agenten	16
3.1 Ändern der vCenter- oder ESXi-Host-Informationen für einen vSphere Recovery Agent	18
3.2 Ändern der CBT-Einstellung für den vSphere-Recovery-Agenten.....	19
3.3 Eingabe der Einstellungen für die Sicherungsüberprüfung für einen vSphere Recovery Agent.....	20
3.4 Ändern der Portal-Registrierung für den vSphere-Recovery-Agenten.....	20
3.5 Hinzufügen von Vault-Einstellungen.....	22
3.6 Hinzufügen einer Beschreibung	24
3.7 Hinzufügen von Aufbewahrungstypen	24
3.8 Konfigurieren der Bandbreitendrosselung.....	26
4 Hinzufügen von vSphere-Sicherungsjobs	28
4.1 Anwendungskonsistente Sicherungen auf vSphere-VMs	32
4.2 Sicherungsüberprüfung für vSphere-VMs.....	34
4.3 Protokolldateioptionen.....	35
4.4 Verschlüsselungseinstellungen	35
4.5 Planen von Sicherungen.....	36
4.6 Maximale Anzahl von Wiederherstellungspunkten für einen Job	40
4.7 Angeben, ob geplante Sicherungen nach einem Fehler wiederholt werden sollen.....	41

4.8	Ausführen einer Ad-hoc-Sicherung.....	42
4.9	Synchronisieren eines Jobs	43
5	Beheben von Zertifikatfehlern und möglichen Bedrohungen	44
5.1	Beheben von Zertifikatfehlern	44
5.2	Handhaben möglicher Ransomware-Bedrohungen	44
6	Wiederherstellen von vSphere-Daten.....	47
6.1	Wiederherstellen von vSphere-VMs.....	47
6.2	vSphere VM innerhalb von Minuten wiederherstellen mit Rapid VM Restore	50
6.3	Wiederherstellen von Dateien, Ordnern und Datenbankelementen mit einem vSphere Recovery Agent.....	56
6.4	Wiederherstellen von Daten auf einem Ersatzcomputer	59
6.5	Wiederherstellen von Daten von einem anderen Computer.....	60
6.6	Erweiterte Wiederherstellungsoptionen	61
7	Löschen von Jobs und Computern und Löschen von Daten aus Vaults	63
7.1	Löschen von Sicherungsjobs ohne Löschung der zugehörigen Daten aus den Vaults	63
7.2	Löschen von Sicherungsjobs und der zugehörigen Jobdaten aus Vaults.....	64
7.3	Abbrechen einer geplanten Jobdatenlöschung.....	66
7.4	Löschen von Computern ohne Löschung der zugehörigen Daten aus den Vaults ...	67
7.5	Löschen eines Computers und von Computerdaten aus Vaults.....	68
7.6	Abbrechen einer geplanten Computerdatenlöschung	70
7.7	Löschen von spezifischen Sicherungen aus Vaults	71
8	Überwachen von Computern, Jobs und Prozessen	73
8.1	Überwachen von Sicherungen und Computern mit der aktuellen Momentaufnahme	73
8.2	Anzeigen von Informationen zu Computer- und Jobstatus	74
8.3	Anzeigen von Protokollen zu nicht konfigurierten Computern.....	76
8.4	Anzeigen von aktuellen Prozessinformationen eines Jobs	77
8.5	Sicherungen mithilfe von E-Mail-Benachrichtigungen überwachen.	79
8.6	Anzeige des Sicherungsüberprüfungs-Berichts.....	84
8.7	Zeitliche Planung des täglichen Statusberichts	85
8.8	Anzeigen von Protokollen zu Jobprozessen und Informationen zu Sätzen	90
8.9	Anzeigen und Exportieren neuer Sicherungsstatus.....	91

1 Einführung in den vSphere Recovery Agent

Der vSphere Recovery Agent (VRA) bietet Datenschutz für Umgebungen mit VMware vSphere-Umgebungen. Wie in der folgenden Abbildung gezeigt, kann ein einzelner VRA virtuelle Maschinen (VMs) und Vorlagen auf allen Hosts sichern, die von einem vCenter Server verwaltet werden.



Ab Version 8.87 kann ein VRA auch virtuelle Maschinen (VMs) und Vorlagen auf einem ESXi-Host sichern, der nicht von vCenter Server verwaltet wird.

Hinweis: Für jeden ESXi-Host, der nicht von vCenter Server verwaltet wird, ist ein separater VRA erforderlich.

Der VRA muss auf einem physischen oder virtuellen Windows-Rechner installiert werden, der lokalen Netzwerkzugriff auf das vCenter oder den ESXi-Host hat, das bzw. den Sie schützen möchten. Sie können Portal verwenden, um den VRA zu konfigurieren und zu verwalten, VMs und Vorlagen in einem geschützten Vault zu sichern und Daten wiederherzustellen.

Um die Sicherungsdauer und die den benötigten Speicherplatz im Vault zu minimieren, liest und sichert der VRA nur Datenträgerblöcke, die auf den einzelnen VMs verwendet werden. Wenn ein Datenträger jedoch mit Bitlocker verschlüsselt ist, muss der VRA alle Sektoren des Datenträgers lesen. Mit dem VRA können VMs mit verschlüsselten Datenträgern gesichert werden, der Vorgang dauert jedoch möglicherweise länger als bei nicht verschlüsselten Datenträgern.

Um die Leistung von Delta-Sicherungen zu verbessern, kann der VRA Changed Block Tracking (CBT) verwenden – eine VMware-Funktion, mit der geänderte Datenträgersektoren nachverfolgt werden können.

Mit dem VRA können Sie die folgenden Komponenten sichern und wiederherstellen:

- VMs mit VMDKs mit einer Größe von bis zu 10 TB.
- VMs, die sich teilweise oder vollständig auf dem vSAN-Speicher befinden. Der VRA kann VMs auf dem vSAN-Speicher sichern und wiederherstellen, solange die für den vSAN-Cluster erforderliche Mindestanzahl von Knoten aktiviert ist.
- VMs in vSAN Stretched Clusters.

Die folgenden Optionen sind in vSphere-Sicherungsjobs verfügbar:

- **Anwendungskonsistente Sicherungen.** Ab Version 8.82 kann der VRA anwendungskonsistente Sicherungen von Microsoft SQL Server, Exchange, SharePoint und Active Directory auf Windows-VMs erstellen. Anwendungskonsistente Sicherungen minimieren den Arbeitsaufwand zum Wiederherstellen von Anwendungen aus Sicherungen. Weitere Informationen finden Sie unter *Anwendungskonsistente Sicherungen auf vSphere-VMs* auf Seite [32](#).
- **Ransomware-Bedrohungserkennung.** Ab Version 9.10 kann der VRA bei der Ausführung des Sicherungsjobs VMs auf mögliche Ransomware-Bedrohungen prüfen. Wenn der VRA eine mögliche Bedrohung auf einer VM erkennt, wird die VM-Sicherung im Portal als mögliche Bedrohung gekennzeichnet, damit Sie die Bedrohung untersuchen und beheben können. Siehe *Handhaben möglicher Ransomware-Bedrohungen* auf Seite [44](#).
- **Sicherungsüberprüfung.** Ab Version 9.00 kann der VRA prüfen, ob jede Windows VM aus der Sicherung wiederhergestellt werden kann. Sie können den Status der Sicherungsüberprüfung von Windows VMs im Sicherungsüberprüfungs-Bericht in Portal 9.00 oder höher anzeigen. Weitere Informationen finden Sie unter *Sicherungsüberprüfung für vSphere-VMs* auf Seite [34](#) und *Anzeige des Sicherungsüberprüfungs-Berichts* auf Seite [84](#).

Mit dem VRA können Sie entweder VMs vollständig wiederherstellen oder spezifische Dateien, Ordner und Datenbankelemente von Windows-VMs wiederherstellen. Siehe *Wiederherstellen von vSphere-Daten* auf Seite [47](#). Ab VRA 8.80 können Sie eine VM innerhalb von Minuten mit Rapid VM Restore wiederherstellen. In einem vCenter können Sie eine VM mithilfe von Rapid VM Restore wiederherstellen und dann in einen anderen Datenspeicher migrieren, um sie dauerhaft wiederherzustellen. Auf einem ESXi-Host, der nicht von vCenter Server verwaltet wird, können Sie eine VM vorübergehend mit Rapid VM Restore wiederherstellen. Weitere Informationen finden Sie unter *vSphere VM innerhalb von Minuten wiederherstellen mit Rapid VM Restore* auf Seite [50](#).

2 Vorbereiten der Installation des vSphere Recovery Agent

Vor der Installation eines vSphere-Recovery-Agenten (VRA) müssen Sie folgende Maßnahmen durchführen:

- Richten Sie ein Portal-Konto zum Verwalten des Agenten ein. Siehe *Portal zum Verwalten des vSphere-Recovery-Agenten* auf Seite 7.
- Bestimmen Sie die Ziel-Vaults für vSphere-Sicherungen. Siehe *Vaults für Sicherungen des vSphere-Recovery-Agenten* auf Seite 7.
- Bestimmen Sie den Installationsort für den Agenten. Siehe *Empfohlene Bereitstellung für vSphere-Recovery-Agent* auf Seite 7.

Sie sollten auch die Anforderungen für die VRA-Funktionen prüfen, die Sie verwenden möchten. Siehe *Anforderungen für bestimmte Funktionen von vSphere Recovery-Agent* auf Seite 8.

Empfehlungen für eine gesicherte VMware-vSphere-Umgebung finden Sie unter *Empfehlungen und Einschränkungen zu vSphere-Recovery-Agent* auf Seite 12.

2.1 Portal zum Verwalten des vSphere-Recovery-Agenten

vSphere Recovery Agents müssen über Portal verwaltet werden. vSphere Recovery Agents können nicht über die ältere Windows CentralControl-Schnittstelle verwaltet werden.

Sie müssen über ein Portal-Konto verfügen, bevor Sie den vSphere-Recovery-Agenten installieren. Das Konto kann sich auf einer Portal-Instanz befinden, die von Ihrem Dienstanbieter gehostet wird oder lokal installiert ist.

2.2 Vaults für Sicherungen des vSphere-Recovery-Agenten

Zur Bereitstellung eines schnellen, lokalen Vault-Zugriffs für Sicherungen und Wiederherstellungen sichern Sie vSphere-Daten in einem Satelliten-Vault. Ein lokaler Vault wird ebenfalls benötigt, um VMs innerhalb von Minuten mit Rapid VM Restore wiederherzustellen oder VM-Sicherungen zu prüfen. Siehe *Anforderungen für vSphere Rapid VM Restore und Sicherheitsüberprüfung* auf Seite 8.

Die Daten können dann in einem durch Ihren Dienstanbieter gehosteten Vault repliziert werden, um eine Offsite-Sicherung für den Katastrophenfall zu sichern.

Wenn Sie keinen Satelliten-Vault verwenden möchten, ziehen Sie die Nutzung eines eigenständigen Vaults zum Seeding und zur Wiederherstellung von umfangreichen Sicherungen in Erwägung.

Unterstützte Vault-Versionen finden Sie in den Versionshinweisen zu vSphere Recovery Agent.

2.3 Empfohlene Bereitstellung für vSphere-Recovery-Agent

Der vSphere Recovery Agent muss auf einem physischen oder virtuellen Windows-Rechner installiert werden, der Netzwerkzugriff auf das vCenter oder den ESXi-Host hat, das bzw. den Sie schützen möchten. Um beste Leistungen zu erzielen, installieren Sie den vSphere Recovery Agent auf einem Rechner im selben Subnetz wie das vCenter oder der ESXi-Host.

Zum Verteilen der Arbeitslast können bis zu fünf vSphere Recovery Agents (VRAs) VMs in einem einzelnen vCenter schützen.

In einem vSAN Stretched Cluster weist jede VM einen bevorzugten Standort auf. Idealerweise sollten Sie an jedem Standort, an dem bevorzugte VMs für diesen Standort gesichert werden, einen lokalen VRA haben. Wenn eine VM an einen anderen Standort umgezogen wird (z. B. wegen Wartung oder Ausfällen), kann sich die Sicherungsleistung verschlechtern. Sie bleibt aber im akzeptablen Bereich.

Für jeden ESXi-Host, der nicht von vCenter Server verwaltet wird, ist ein separater VRA erforderlich. Ein VRA kann nur dann VMs auf mehreren ESXi-Hosts schützen, wenn sich die Hosts im selben vCenter befinden.

Systemanforderungen und unterstützte Plattformen finden Sie in den Versionshinweisen zu vSphere Recovery Agent.

Wir empfehlen die Verwendung von Firewalls oder anderen Mechanismen, um VRAs und vSphere-Umgebungen vom Internet zu isolieren.

2.4 Anforderungen für bestimmte Funktionen von vSphere Recovery-Agent

Um bestimmte VRA-Funktionen zu nutzen, müssen folgende Voraussetzungen erfüllt sein:

- Zur Durchführung von anwendungskonsistenten Sicherungen finden Sie weitere Informationen unter *Anforderungen für anwendungskonsistente Sicherungen* auf Seite [8](#).
- Um VMs innerhalb weniger Minuten wiederherzustellen oder zu überprüfen, ob Windows VMs aus Backups wiederhergestellt werden können, siehe *Anforderungen für vSphere Rapid VM Restore und Sicherungsüberprüfung* auf Seite [8](#).
- Um Windows VMs auf mögliche Ransomware-Bedrohungen zu prüfen, siehe *Anforderungen an die Erkennung von Ransomware-Bedrohungen* auf Seite [11](#).

1.4.1 Anforderungen für anwendungskonsistente Sicherungen

Ab Version 8.82 kann VRA anwendungskonsistente Sicherungen von Microsoft SQL Server, Exchange, SharePoint und Active Directory auf Windows-VMs in vSphere-Umgebungen durchführen. Dazu müssen auf den VMs die VMware Tools ab Version 11 installiert sein.

Als Teil einer anwendungskonsistenten Sicherung kann der VRA SQL Server-, Exchange- und SharePoint-Transaktionsprotokolle auf VMs auf ESXi 7.0-, 6.7- und 6.5-Hosts abschneiden.

Anwendungskonsistente Sicherungen werden auf VMs mit Hardwareversion 8 oder höher unterstützt.

Hinweis: Anwendungskonsistente Sicherungen werden auf Linux-VMs nicht unterstützt.

1.4.2 Anforderungen für vSphere Rapid VM Restore und Sicherungsüberprüfung

Ab VRA 8.80 und Portal 8.84 können Sie eine virtuelle Maschine (VM) mit Rapid VM Restore innerhalb von Minuten in einer vSphere-Umgebung wiederherstellen. Siehe *vSphere VM innerhalb von Minuten wiederherstellen mit Rapid VM Restore* auf Seite [50](#).

Die folgende Tabelle enthält und beschreibt die Anforderungen für Rapid VM Restore. Wenn die Anforderungen für VRA, Portal und Vault nicht erfüllt sind, wird Rapid VM Restore nicht als Wiederherstellungsoption in Portal angezeigt. Wenn die vSphere-Umgebungsanforderungen nicht erfüllt sind, können Sie Rapid VM Restore zwar starten, jedoch nicht erfolgreich abschließen.

Komponente	Rapid VM Restore-Anforderung
VRA	<p>vSphere-Recovery-Agent Version 8.80 oder neuer, installiert auf einer Windows Server-Plattform.</p> <p>Windows Datei- und Speicherdienste müssen mit der Funktion „iSCSI-Zielserver“ auf dem Server installiert sein. Wenn Sie die Funktion „iSCSI-Zielserver“ nach der Installation von VRA installieren, müssen Sie die VRA-Dienste (BUAgent und VVAgent) neu starten, bevor Sie Rapid VM Restore ausführen können.</p>
Portal	Portal-Version 8.84 oder höher.
Vault	<p>Ein lokal installierter (also nicht auf einem Cloudserver oder in einem Remote-Rechenzentrum) Vault ab Version 8.50.</p> <p>Die Funktion „Rapid VM Restore“ muss im Vault aktiviert sein. Diese Funktion ist in Satelliten-Vaults standardmäßig aktiviert. Wenn Sie einen lokalen Basis-Vault verwenden, können Sie die Funktion „Rapid VM Restores“ mit einem Skript aktivieren. Siehe <i>Funktion „Rapid VM Restore“ in einem Vault aktivieren</i> auf Seite 11.</p>
vSphere-Umgebung	
ESXi-Hosts	<p>Auf allen ESXi-Hosts muss der Software-iSCSI-Adapter installiert und an eine Netzwerkportgruppe gebunden werden, die für den VRA erreichbar ist.</p> <p>Um die mit Rapid VM Restore wiederhergestellten VMs in den permanenten Speicher zu verschieben, muss jeder ESXi-Host auf zwei Datenspeicher zugreifen können: einen Datenspeicher für die Änderungen, während die VM mit Rapid VM Restore ausgeführt wird, und einen für die permanente Speicherung. Beide Datenspeicher benötigen genügend freien Speicherplatz für die wiederhergestellte VM.</p> <p><i>Hinweis:</i> Auf einem ESXi-Host, der nicht von vCenter Server verwaltet wird, kann mithilfe von Rapid VM Restore überprüft werden, ob VMs korrekt gesichert wurden; das Feature kann jedoch nicht verwendet werden, um VMs dauerhaft wiederherzustellen. Ein ESXi-Server, der nicht Teil eines vCenters ist, verfügt nicht über die erforderlichen Funktionen, um VMs in permanenten Speicher zu migrieren.</p>
Lizenz	Um VMs, die mit Rapid VM Restore wiederhergestellt wurden, auf einen permanenten Speicher zu migrieren, muss Ihre VMware-Lizenz die Speichermigration unterstützen.
Datenspeicher	<p>Wir empfehlen, einen der unterstützten Speicher aus der VMware-Hardwarekompatibilitätsanleitung zu verwenden: https://www.vmware.com/resources/compatibility/search.php</p> <p>Wenn Sie eine VM mit Rapid VM Restore wiederherstellen, müssen Sie einen Datenspeicher auswählen, in den die Änderungen geschrieben werden, während die VM mit Rapid VM Restore ausgeführt wird. Dieser Datenspeicher kann ein lokaler, iSCSI- oder vSAN-Speicher sein, jedoch kein NFS-Speicher.</p> <p>Wenn Sie eine VM in einen permanenten Speicher verschieben, können Sie einen lokalen, iSCSI-, vSAN- oder NFS-Speicher verwenden.</p>

Ab VRA 9.00 und Portal 9.00 kann der VRA überprüfen, ob Windows VMs aus vSphere-Sicherungen wiederhergestellt werden können. Siehe *Sicherungsüberprüfung für vSphere-VMs* auf Seite 34.

In der folgenden Tabelle sind die Anforderungen für die Sicherungsüberprüfung aufgeführt und beschrieben. Die Einstellungen für die Sicherungsüberprüfung werden für einen VRA nur angezeigt, wenn die Portal- und VRA-Anforderungen erfüllt sind.

Hinweis: Da der VRA automatisierte Rapid VM Restore-Prozesse zur Überprüfung von VM-Sicherungen verwendet, sind die Anforderungen an die Sicherungsüberprüfung ähnlich wie die Anforderungen an Rapid VM Restore.

Komponente	Anforderung für die Sicherungsüberprüfung
VRA	<p>vSphere-Recovery-Agent Version 9.00 oder neuer, installiert auf einer Windows Server-Plattform.</p> <p>Windows Datei- und Speicherdienste müssen mit der Funktion „iSCSI-Zielsever“ auf dem Server installiert sein. Wenn Sie die Funktion „iSCSI-Zielsever“ nach der Installation von VRA installieren, müssen Sie die VRA-Dienste (BUAgent und VVAgent) neu starten, bevor Sie Rapid VM Restore ausführen können.</p>
Portal	Portal-Version 9.00 oder höher.
Vault	<p>Ein lokal installierter (also nicht auf einem Cloudserver oder in einem Remote-Rechenzentrum) Vault ab Version 8.50.</p> <p>Die Funktion „Rapid VM Restore“ muss im Vault aktiviert sein. Diese Funktion ist in Satelliten-Vaults standardmäßig aktiviert. Wenn Sie einen lokalen Basis-Vault verwenden, können Sie die Funktion „Rapid VM Restores“ mit einem Skript aktivieren. Siehe <i>Funktion „Rapid VM Restore“ in einem Vault aktivieren</i> auf Seite 11.</p>
vSphere-Umgebung	
ESXi-Hosts	<p>Auf dem ESXi-Host, auf dem die Sicherungsüberprüfungen durchgeführt werden, muss der Software-iSCSI-Adapter installiert und an eine Netzwerkportgruppe gebunden sein, die für den VRA erreichbar ist.</p> <p>Der ESXi-Host muss in der Lage sein, die erwartete Last zu bewältigen. Während der Sicherungsüberprüfung startet der VRA jede VM mit einem automatisierten Rapid VM Restore-Prozess. In jedem Sicherungsjob wird jeweils eine VM überprüft, wobei die ursprünglichen Speichereinstellungen für jede VM verwendet werden. Wenn beispielsweise die Sicherungsüberprüfung für fünf Sicherungsjobs gleichzeitig ausgeführt wird und jede VM 256 GB RAM verwendet, kann die Sicherungsüberprüfung bis zu 1268 GB RAM auf dem Host verwenden.</p> <p><i>Hinweis:</i> Der ESXi-Host für die Durchführung von Sicherungsüberprüfungen wird in der Registerkarte „vSphere-Einstellungen“ für einen VRA ausgewählt. Siehe <i>Konfigurieren des vSphere-Recovery-Agenten</i> auf Seite 16.</p>

Komponente	Anforderung für die Sicherungsüberprüfung
Datenspeicher	Wir empfehlen, einen der unterstützten Speicher aus der VMware-Hardwarekompatibilitätsanleitung zu verwenden: https://www.vmware.com/resources/compatibility/search.php Bei der Eingabe der Einstellungen für die Sicherungsüberprüfung müssen Sie einen Datenspeicher für die Überprüfung von VMs auswählen. Dieser Datenspeicher kann ein lokaler, iSCSI- oder vSAN-Speicher sein, jedoch kein NFS-Speicher.
Virtuelle Maschinen	Die Sicherungsüberprüfung wird für Windows-VMs unterstützt. Die Sicherungsüberprüfung wird bei Nicht-Windows-Betriebssystemen (z. B. Linux) nicht unterstützt. VMware Tools Version 11 oder höher muss auf der VM installiert sein.

Funktion „Rapid VM Restore“ in einem Vault aktivieren

Um eine VM innerhalb von Minuten mit Rapid VM Restore wiederherstellen zu können, muss die VM-Sicherung in einem lokalen Vault mit Version 8.50 oder höher gespeichert werden, in dem die Funktion „Rapid VM Restore“ aktiviert ist.

Die Funktion „Rapid VM Restore“ ist in Satelliten-Vaults standardmäßig aktiviert. In lokal installierten Basis-Vaults müssen Sie die Funktion „Rapid VM Restore“ aktivieren, bevor Sie die folgenden Schritte ausführen können.

So aktivieren Sie die Funktion „Rapid VM Restore“ in einem Vault:

- Öffnen Sie auf dem Server, auf dem der Vault installiert ist, ein PowerShell-Fenster als Administrator, und navigieren Sie zum Unterordner „Scripts“ im Vault-Installationsverzeichnis.
- Führen Sie den folgenden Befehl aus:

```
.\VaultSettings.ps1 set IsRVMRAAllowed 1
```

1.4.3 Anforderungen an die Erkennung von Ransomware-Bedrohungen

Ab VRA 9.10 und Portal 9.10 kann der VRA bei der Ausführung eines Sicherungsjobs Windows VMs auf mögliche Ransomware-Bedrohungen prüfen. VMware Tools muss auf den VMs installiert sein. Wir empfehlen, die neueste Version der VMware Tools zu verwenden.

Der VRA kann nur auf VMs, die ausgeführt werden, auf Ransomware-Bedrohungen prüfen. Der VRA kann nicht auf VM-Vorlagen auf Ransomware-Bedrohungen prüfen.

2.5 vSphere-Recovery-Agenten-Ports

Die folgende Tabelle enthält die Ports, die geöffnet sein müssen, damit der vSphere-Recovery-Agent mit anderen Systemen kommunizieren kann:

Port	Kommunikation	Protokoll
Ausgehend: 8086, 8087	Mit dem Portal	TCP

Port	Kommunikation	Protokoll
Ausgehend: 2546	Mit dem Vault	TCP
Ausgehend: 443	Zu vCenter	TCP
Ausgehend: 902	Zu ESXi	TCP/UDP
Eingehend: 3260	iSCSI-Verbindungen (für Rapid VM Restore)	TCP

2.6 Empfehlungen und Einschränkungen zu vSphere-Recovery-Agent

Der VRA kann VMs mit VMDKs sichern und wiederherstellen, die 10 TB groß sind. Vermeiden Sie es, VMDKs zu verwenden, die größer als 10 TB sind.

Der VRA überspringt beim Sichern von VMs die physische Partitionsgerätauordnung (Physical Raw Device Mapping, pRDM) sowie freigegebene und unabhängige Datenträger, da VMware nicht zulässt, dass diese für Sicherungen auf VM-Ebene hinzugefügt werden. Um Daten auf diesen Datenträgern zu sichern, müssen Sie einen Agenten in der virtuellen Maschine installieren. Während der Sicherung überspringt der VRA diese Funktionen und gibt eine Warnmeldung aus. Wenn eine virtuelle Maschine einen oder mehrere Datenträger enthält, die geschützt werden können, wird die virtuelle Maschine dennoch gesichert.

Mit dem VRA können Sie VMs sichern und wiederherstellen, die über Volumes in Windows-Speicherplätzen verfügen. Der VRA unterstützt jedoch keine Datei- und Ordnerwiederherstellungen von Volumes aus Windows-Speicherplätzen.

Der vSphere Recovery Agent (VRA) ist eine Windows-Anwendung. Sie können den VRA auf einem physischen oder virtuellen Windows-Rechner installieren, der lokalen Netzwerkzugriff auf das vCenter oder den ESXi-Host hat, das bzw. den Sie schützen möchten.

Nach der VRA-Installation können Sie die vSphere Umgebung, den Vault und andere Einstellungen für den Agenten konfigurieren. Siehe *Konfigurieren des vSphere-Recovery-Agenten* auf Seite 16.

Um einen VRA zu upgraden, siehe *Upgraden des vSphere Recovery Agent* auf Seite 14.

Die VRA-Installation kann nicht geändert werden. Um die Portal-Adresse für einen VRA zu ändern, müssen Sie den VRA deinstallieren, mit der neuen Portal-Registrierung erneut installieren und anschließend den VRA mit dem Vault erneut registrieren.

Hinweis: Wir empfehlen die Verwendung von Firewalls oder anderen Mechanismen, um VRAs und vSphere-Umgebungen vom Internet zu isolieren.

Um eine VMware vSphere-Umgebung zu schützen, müssen Sie den vSphere Recovery Agent (VRA) auf einem physischen oder virtuellen Windows-Rechner installieren, der lokalen Netzwerkzugriff auf das vCenter oder den ESXi-Host hat, das bzw. den Sie schützen möchten.

Sie können den VRA nicht auf einem Rechner installieren, auf dem der Windows-Agent installiert ist.

Installieren Sie den VRA nicht auf einem Active Directory-Domänencontroller.

Stellen Sie sicher, dass auf dem Rechner, auf dem Sie den VRA installieren möchten, die Energieverwaltung deaktiviert ist.

So installieren Sie den vSphere-Recovery-Agenten:

1. Doppelklicken Sie auf einer physischen oder virtuellen Maschine mit unterstützter Windows-Plattform auf das VRA-Installationskit.
2. Lesen Sie die Lizenzvereinbarung auf der Seite „Vertragsbedingungen“. Klicken Sie auf **Ich stimme den Lizenzbedingungen zu**, und dann auf **Installieren**.
3. Klicken Sie auf der Begrüßungsseite auf **Weiter**.
4. Führen Sie auf der Seite „Zielordner“ eine der folgenden Aktionen aus:
 - Klicken Sie auf **Weiter**, um den VRA am Standardspeicherort zu installieren.
 - Klicken Sie auf **Ändern**, um den VRA an einem anderen Ort zu installieren. Navigieren Sie im Dialogfeld „Zielordner ändern“ zum neuen Installationsordner, oder geben Sie den Ordner in das Feld **Ordnername** ein. Klicken Sie auf **OK**. Klicken Sie auf der Seite „Zielordner“ auf **Weiter**.
5. Geben Sie auf der Seite „Agent beim Portal registrieren“ die folgenden Informationen an:
 - Geben Sie im Feld **Netzwerkadresse** den Hostnamen oder die IPV4-Adresse von Portal für die Verwaltung des VRA ein.

Hinweis: Wenn Sie einen Agent in Portal registrieren, empfehlen wir Ihnen, den Hostnamen von Portal anzugeben. Wenn sich die IP-Adresse von Portal in Zukunft ändert, können Sie mittels DNS die Änderung verwalten. Eine erneute manuelle Registrierung des Agenten in Portal ist nicht erforderlich.
 - Geben Sie im Feld **Port** die Portnummer für die Kommunikation mit dem Portal ein.
 - Geben Sie im Feld **Benutzername** den Namen des Portalbenutzers für die Verwaltung des VRA ein.

Nachdem der VRA installiert wurde, wird er diesem Benutzer und anderen Administratorbenutzern in der Site des Benutzers in Portal auf der Seite „Computer“ angezeigt.
 - Geben Sie im Feld **Kennwort** das Kennwort des angegebenen Portalbenutzers ein.
6. Klicken Sie auf **Weiter**.
7. Klicken Sie nach Abschluss der Installation auf **Fertigstellen**.
8. Klicken Sie auf **Schließen**.

2.7 Installieren des vSphere-Recovery-Agenten im unbeaufsichtigten Modus

Führen Sie den folgenden Befehl mit Administratorrechten im Verzeichnis aus, in dem sich das Installationskit befindet, um den vSphere-Recovery-Agenten im unbeaufsichtigten Modus zu installieren:

```
installKitName /install /quiet [AGENTDIR="installPath"]  
PORTAL_ADDRESS=PortalAddress [PORTAL_PORT=portNumber]  
PORTAL_USER=PortalUser PORTAL_PASSWORD=PortalPassword
```

Dabei gilt Folgendes: *installKitName* ist der Name des Installationskits für vSphere Recovery Agent.

Die folgende Tabelle führt Befehlsparameter auf und beschreibt diese:

Parameter	Beschreibung
AGENTDIR=" <i>installPath</i> "	Optional. Legt den Installationsort für den Agenten fest. Wenn Sie diesen Parameter nicht angeben, wird der standardmäßige Installationsort verwendet.
PORTAL_ADDRESS= <i>PortalAddress</i>	Gibt den Hostnamen oder die IPV4-Adresse von Portal zur Verwaltung des Agenten an. Beispiel: PORTAL_ADDRESS=portal.site.com Die Angabe des Hostnamens wird empfohlen. Auf diese Weise können IP-Adressänderungen per DNS verarbeitet werden.
PORTAL_PORT= <i>portNumber</i>	Optional. Gibt die Portnummer für die Kommunikation mit Portal an. Wenn Sie diesen Parameter nicht angeben, wird der Standardwert (8086) verwendet.
PORTAL_USER= <i>PortalUser</i>	Gibt den Namen des Portalbenutzers an, der zu dem Agenten gehört. Beispiel: PORTAL_USER=user@site.com
PORTAL_PASSWORD= <i>PortalPassword</i>	Gibt das Kennwort des Portalbenutzers an. Beispiel: PORTAL_PASSWORD=password1234

2.8 Upgraden des vSphere Recovery Agent

Sie können ein Upgrade für einen vSphere Recovery Agent (VRA) durchführen, indem Sie das Agent-Installationskit manuell ausführen. Informationen zu den unterstützten Upgrade-Pfaden und Systemanforderungen finden Sie in den Versionshinweisen zu VRA.

Hinweis: Bei der ersten Ausführung eines vorhandene VRA-Sicherungsjobs nach dem Upgrade von Version 8.80 oder niedriger auf Version 8.82 oder höher kann die Sicherung mehr Zeit als eine herkömmliche Delta-Sicherung in Anspruch nehmen. Wenn der VRA eine VM nach einem Upgrade zum ersten Mal sichert, liest der VRA alle VM-Daten.

Ab Version 8.82 kann der VRA anwendungskonsistente Sicherungen von Microsoft SQL Server, Exchange, SharePoint und Active Directory auf virtuellen Windows-Maschinen (VMs) erstellen. Siehe *Anwendungskonsistente Sicherungen auf vSphere-VMs* auf Seite 32. Wenn Sie einen VRA von Version 8.80 oder niedriger auf Version 8.82 oder höher upgraden, ist die Einstellung für anwendungskonsistente Sicherungen in vorhandenen Sicherungsjobs nicht aktiviert. Um Anwendungskonsistenz in einem Sicherungsjob zu aktivieren, bearbeiten Sie den Job.

So upgraden Sie den vSphere Recovery Agent:

1. Doppelklicken Sie auf dem Computer, auf dem eine frühere VRA-Version installiert ist, auf das VRA-Installationskit.

2. Lesen Sie die Lizenzvereinbarung auf der Seite „Vertragsbedingungen“. Klicken Sie auf **Ich stimme den Lizenzbedingungen zu**, und dann auf **Installieren**.
3. Klicken Sie auf der Bestätigungsseite auf **Ja**.
4. Klicken Sie auf der Begrüßungsseite auf **Weiter**.
5. Klicken Sie nach Abschluss des Upgrade auf **Fertigstellen**.
6. Klicken Sie auf **Schließen**.

2.9 Upgraden des vSphere Recovery Agent im unbeaufsichtigten Modus

Führen Sie den folgenden Befehl mit Administratorrechten im Verzeichnis aus, in dem sich das Installationskit befindet, um den vSphere Recovery Agent im unbeaufsichtigten Modus zu upgraden:

```
installKitName /install /quiet
```

2.10 Deinstallieren des vSphere Recovery Agent

Hinweis: Um die Portal-Adresse für einen VRA zu ändern, müssen Sie den VRA deinstallieren, mit der neuen Portal-Registrierung erneut installieren und anschließend den VRA mit dem Vault erneut registrieren. Siehe *Konfigurieren des vSphere-Recovery-Agenten* auf Seite 16. Die VRA-Installation kann nicht geändert werden.

Führen Sie stattdessen eine der folgenden Aktionen aus, um einen vSphere-Recovery-Agenten zu deinstallieren:

- Doppelklicken Sie auf das VRA-Installationsprogramm. Klicken Sie im Feld „Setup bearbeiten“ auf **Deinstallieren**. Warten Sie, bis der VRA deinstalliert wurde, und klicken Sie auf **Schließen**.
- Deinstallieren Sie den vSphere Recovery Agent über die Systemsteuerung.

2.11 Deinstallieren des vSphere Recovery Agent im unbeaufsichtigten Modus

Führen Sie den folgenden Befehl mit Administratorrechten im Verzeichnis aus, in dem sich das Installationskit befindet, um den vSphere-Recovery-Agenten im unbeaufsichtigten Modus zu deinstallieren:

```
installKitName /uninstall /quiet
```

3 Konfigurieren des vSphere-Recovery-Agenten

Nach Installation und Registrierung des vSphere Recovery Agenten (VRA) in Portal müssen Sie den Agenten wie folgt konfigurieren:

- Geben Sie Informationen und Anmeldeinformationen für das vCenter oder den ESXi-Host ein, das bzw. den Sie schützen möchten. Das angegebene Konto muss über Administratorrechte für die vSphere-Umgebung verfügen.
- Ändern Sie die CBT-Einstellung. CBT (Changed Block Tracking) ist ein VMware-Feature, mit dem geänderte Datenträgersektoren nachverfolgt und die Leistung von VM-Sicherungen verbessert werden kann. Beim vSphere-Agenten ist CBT (Changed Block Tracking) für virtuelle Maschinen standardmäßig aktiviert.
- Fügen Sie eine Vault-Verbindung hinzu. Vault-Verbindungen umfassen Vault-Informationen und Anmeldeinformationen, mit denen der Agent Daten im Vault sichern und aus dem Vault wiederherstellen kann.

Ab Version 9.00 können Sie auch Einstellungen für die Sicherungsüberprüfung für einen VRA eingeben. Wenn Einstellungen für die Sicherungsüberprüfung eingegeben werden und die Sicherungsüberprüfung für einen vSphere-Sicherungsjob aktiviert ist, prüft der VRA, ob jede Windows-VM aus der Sicherung wiederhergestellt werden kann. Siehe *Sicherungsüberprüfung für vSphere-VMs* auf Seite [34](#).

Um diese Einstellungen nach der Erstkonfiguration zu ändern, siehe *Ändern der vCenter- oder ESXi-Host-Informationen für einen vSphere Recovery Agent* auf Seite [18](#), *Ändern der CBT-Einstellung für den vSphere-Recovery-Agenten* auf Seite [19](#), *Eingabe der Einstellungen für die Sicherungsüberprüfung für einen vSphere Recovery Agent* auf Seite [20](#) und *Hinzufügen von Vault-Einstellungen* auf Seite [22](#).

Sie können auch Folgendes vornehmen:

- Fügen Sie eine Beschreibung für den Agent hinzu. Die Beschreibung wird für die vSphere-Umgebung auf der Seite „Computer“ angezeigt. Siehe *Hinzufügen einer Beschreibung* auf Seite [24](#).
- Fügen Sie Aufbewahrungstypen hinzu, die festlegen, wie lange die Sicherungen im Vault aufbewahrt werden. Siehe *Hinzufügen von Aufbewahrungstypen* auf Seite [24](#).
- Konfigurieren Sie E-Mail-Benachrichtigungen an Benutzer, wenn eine Sicherung abgeschlossen wurde, nicht ausgeführt werden kann oder wenn Fehler auftreten. Weitere Informationen finden Sie unter *Sicherungen mithilfe von E-Mail-Benachrichtigungen überwachen*. auf Seite [79](#).
- Geben Sie die für Sicherungen verwendete Bandbreite an. Siehe *Konfigurieren der Bandbreitendrosselung* auf Seite [26](#).

So konfigurieren Sie den vSphere Recovery Agent:

1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den nicht konfigurierten vSphere Recovery Agent und klicken Sie auf die entsprechende Zeile, um die Ansicht zu erweitern.

Wenn der Agent nicht konfiguriert wurde, werden die Felder „Automatisch konfigurieren“ und „Manuell konfigurieren“ angezeigt.



3. Wenn die Liste **Den Computer einer Site zuordnen** angezeigt wird, wählen Sie eine Site für den Agenten aus.

Die Site-Liste wird angezeigt, wenn Sie sich als Administratorbenutzer bei einer übergeordneten Site angemeldet haben, die untergeordnete Sites enthält. Die Liste enthält die übergeordnete Site, wenn ihr ein Vault-Profil zugewiesen ist und sich alle untergeordneten Sites in der übergeordneten Site befinden. Wenn der Name der übergeordneten Site in der Liste enthalten ist, wird er in Fettdruck, gefolgt von dem Wort „Übergeordnet“ in Klammern angezeigt.

4. Führen Sie zum Hinzufügen einer Vault-Verbindung für den Agent eine der folgenden Aktionen durch:

- Wählen Sie in der Liste **Vault auswählen** einen Vault aus und klicken Sie dann auf **Automatisch konfigurieren**. Wenn die Vault-Verbindung hinzugefügt werden konnte, wird eine Meldung angezeigt. Klicken Sie auf **Zu Agent wechseln**.
Wenn die Vault-Verbindung nicht hinzugefügt werden konnte, können Sie diese manuell hinzufügen.
- Klicken Sie auf **Manuell konfigurieren**. Klicken Sie auf der Registerkarte „Vault-Einstellungen“ auf **Vault hinzufügen**. Führen Sie im Dialogfeld „Vault-Einstellungen“ eine der folgenden Maßnahmen durch:

- Geben Sie im Feld **Vault-Name** einen Namen für die Vault-Verbindung ein.
- Geben Sie im Feld **Adresse** den Hostnamen oder die IPV4-Adresse des Vaults ein.
Die Angabe des Hostnamens wird empfohlen. Auf diese Weise können IP-Adressänderungen per DNS verarbeitet werden.
- Geben Sie in den Feldern **Konto**, **Benutzername** und **Kennwort** einen Kontonamen und die Anmeldeinformationen zum Sichern und Wiederherstellen von Daten aus dem Vault ein.

Klicken Sie auf **Speichern**.

5. Führen Sie auf der Registerkarte „vSphere-Einstellungen“ die folgenden Aktionen durch:
 - Geben Sie im Feld **Host** den Hostnamen oder die IPv4-Adresse des vCenter oder ESXi-Hosts ein, das bzw. den Sie schützen möchten. Die Angabe des Hostnamens wird empfohlen. Auf diese Weise können IP-Adressänderungen per DNS verarbeitet werden.

- Geben Sie im Feld **Domäne** die Domäne des Kontos zur Authentifizierung beim vCenter oder ESXi-Host ein. Die Domäne ist nicht erforderlich, wenn Sie die Domäne im Feld **Benutzername** angeben.
 - Geben Sie im Feld **Benutzername** das Konto ein, das zur Authentifizierung beim vCenter oder ESXi-Host verwendet wird. Sie können das Konto im Format *Benutzername*, *Domäne\Benutzername* oder *Benutzername@Domäne* eingeben.
Der Benutzer muss über Administratorrechte verfügen.
 - Geben Sie im Feld **Kennwort** das Kennwort des angegebenen Benutzers ein.
Hinweis: Wenn sich das Kennwort für den angegebenen Benutzer ändert, ändern Sie es so schnell wie möglich für den VRA.
6. Klicken Sie auf **Verifizieren und Speichern**. Wenn die Anmeldeinformationen gültig sind, wird eine Erfolgsmeldung angezeigt. Klicken Sie auf **OK**.
 7. Führen Sie eine der folgenden Aktionen aus:
 - Um CBT für virtuelle Maschinen zu aktivieren, für die CBT nicht aktiviert ist, wählen Sie „CBT (Changed Block Tracking) für virtuelle Maschinen während der Sicherung aktivieren“.
 - Wenn Sie nicht zulassen möchten, dass die VRA CBT für virtuelle Maschinen aktiviert, deaktivieren Sie die Option „CBT (Changed Block Tracking) für virtuelle Maschinen aktivieren“.
 8. Um die Einstellungen zur Sicherungsüberprüfung zu öffnen, führen Sie Folgendes aus:
 - a. Wählen Sie **Sicherungen nach Abschluss prüfen**.
 - b. Wählen Sie in der Liste **Temporärer Datenspeicher** einen Datenspeicher für während der Sicherungsüberprüfung ausgeführte VMs.
 - c. Wählen Sie in der Liste **Zielhost** einen Host aus, auf dem VMs während der Sicherungsüberprüfung ausgeführt werden.

Hinweis: Die Einstellungen für die Sicherungsüberprüfung werden nur angezeigt, wenn die Portal- und VRA-Anforderungen erfüllt sind. Siehe *Anforderungen für vSphere Rapid VM Restore und Sicherungsüberprüfung* auf Seite 8.
 9. Klicken Sie auf **Speichern**. Die Meldung „Erfolg“ wird angezeigt. Klicken Sie auf **OK**.
Die VRA kann nun zur Erstellung von Sicherungsjobs verwendet werden. Siehe *Hinzufügen von vSphere-Sicherungsjobs* auf Seite 28.

3.1 Ändern der vCenter- oder ESXi-Host-Informationen für einen vSphere Recovery Agent

Gehen Sie wie folgt vor, um Informationen zur vCenter- oder ESXi-Host-Umgebung für einen vSphere Recovery Agent zu ändern, einschließlich des Host-Namens oder der Adresse sowie des Kontos und des Kennworts für die Authentifizierung bei der vSphere-Umgebung.

Wenn Sie das Kennwort für das Konto ändern, das zur Authentifizierung bei einer vSphere-Umgebung verwendet wird, ändern Sie es so bald wie möglich für den VRA.

So ändern Sie vCenter- oder ESXi-Host-Informationen für einen vSphere Recovery Agent:

1. Klicken Sie in der Navigationsleiste in Portal auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den vSphere Recovery Agent, und klicken Sie auf die entsprechende Zeile, um die Ansicht zu erweitern.
3. Führen Sie auf der Registerkarte „vSphere-Einstellungen“ die folgenden Aktionen durch:
 - Geben Sie im Feld **Host** den Hostnamen oder die IP-Adresse des vCenter oder ESXi-Hosts ein, das bzw. den Sie schützen möchten. Die Angabe des Hostnamens wird empfohlen. Auf diese Weise können IP-Adressänderungen per DNS verarbeitet werden.
 - Geben Sie im Feld **Domäne** die Domäne des Kontos zur Authentifizierung beim vCenter oder ESXi-Host ein. Die Domäne ist nicht erforderlich, wenn Sie die Domäne im Feld **Benutzername** angeben.
 - Geben Sie im Feld **Benutzername** das Konto ein, das zur Authentifizierung beim vCenter oder ESXi-Host verwendet wird. Sie können das Konto im Format *Benutzername*, *Domäne\Benutzername* oder *Benutzername@Domäne* eingeben.
Der Benutzer muss über Administratorberechtigungen für das vCenter oder den ESXi-Host verfügen.
 - Geben Sie im Feld **Kennwort** das Kennwort des angegebenen Benutzers ein.
4. Klicken Sie auf **Speichern**. Die Meldung „Erfolg“ wird angezeigt. Klicken Sie auf **OK**.

3.2 Ändern der CBT-Einstellung für den vSphere-Recovery-Agenten

CBT (Changed Block Tracking) ist ein VMware-Feature, mit dem geänderte Datenträgersektoren nachverfolgt und die Leistung von VM-Sicherungen verbessert werden kann. Beim vSphere-Agenten ist CBT (Changed Block Tracking) für virtuelle Maschinen standardmäßig aktiviert.

Da CBT jedoch einigen Aufwand für die Verarbeitung virtueller Datenträger mit sich bringt, können Sie verhindern, dass der Agent CBT für virtuelle Maschinen aktiviert. Dabei wird CBT nicht für VMs deaktiviert, bei denen das Feature bereits über den Agenten oder einen anderen Mechanismus aktiviert wurde. Es wird lediglich verhindert, dass der Agent künftig CBT für virtuelle Maschinen aktiviert, bei denen das Feature noch nicht aktiviert wurde.

So ändern Sie die CBT-Einstellung für einen vSphere Recovery Agent:

1. Klicken Sie in der Navigationsleiste in Portal auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den vSphere Recovery Agent, und klicken Sie auf die entsprechende Zeile, um die Ansicht zu erweitern.
3. Führen Sie auf der Registerkarte „vSphere-Einstellungen“ eine der folgenden Aktionen durch:
 - Um CBT für virtuelle Maschinen zu aktivieren, für das Feature nicht aktiviert ist, wählen Sie **CBT (Changed Block Tracking) für virtuelle Maschinen während der Sicherung aktivieren** aus.
 - Wenn Sie nicht zulassen möchten, dass der VRA CBT für virtuelle Maschinen aktiviert, deaktivieren Sie die Option **CBT (Changed Block Tracking) für virtuelle Maschinen aktivieren**.

4. Klicken Sie auf **Speichern**.

3.3 Eingabe der Einstellungen für die Sicherungsüberprüfung für einen vSphere Recovery Agent

Ab Version 9.00 können Sie die Einstellungen für die Überprüfung von Sicherungen für einen VRA eingeben. Wenn Einstellungen für die Sicherungsüberprüfung eingegeben werden und die Sicherungsüberprüfung für einen vSphere-Sicherungsjob aktiviert ist, prüft der VRA, ob jede Windows VM im Job aus der Sicherung wiederhergestellt werden kann. Siehe *Sicherungsüberprüfung für vSphere-VMs* auf Seite 34.

So geben Sie die Einstellungen für die Sicherungsüberprüfung für einen vSphere Recovery-Agenten ein:

1. Klicken Sie in der Navigationsleiste in Portal auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den vSphere Recovery Agent, und klicken Sie auf die entsprechende Zeile, um die Ansicht zu erweitern.
3. Wählen Sie in der Registerkarte „vSphere-Einstellungen“ **Sicherungen nach Abschluss prüfen**.
Hinweis: Die Einstellungen für die Sicherungsüberprüfung werden nur angezeigt, wenn die Portal- und VRA-Anforderungen erfüllt sind. Siehe *Anforderungen für vSphere Rapid VM Restore und Sicherungsüberprüfung* auf Seite 8.
4. Wählen Sie in der Liste **Temporärer Datenspeicher** einen Datenspeicher für während der Sicherungsüberprüfung ausgeführte VMs.
5. Wählen Sie in der Liste **Zielhost** einen Host aus, auf dem VMs während der Sicherungsüberprüfung ausgeführt werden.
6. Klicken Sie auf **Speichern**. Die Meldung „Erfolg“ wird angezeigt. Klicken Sie auf **OK**.

3.4 Ändern der Portal-Registrierung für den vSphere-Recovery-Agenten

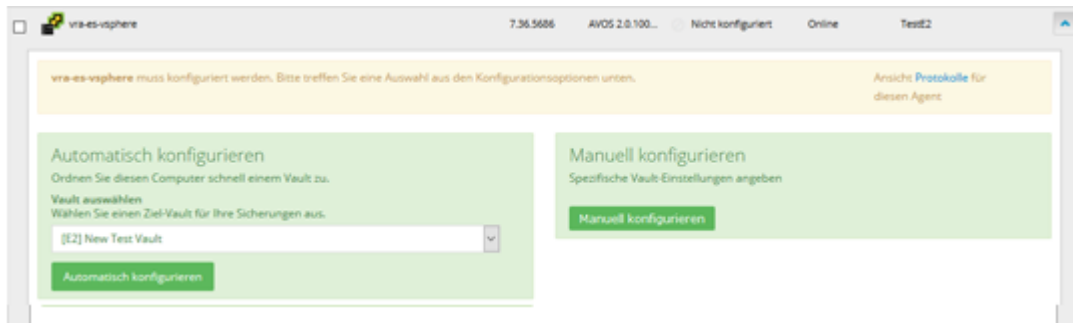
Sie können die Portal-Registrierung eines VRAs nicht durch Ausführen des Installationskits ändern. Um die Portal-Adresse oder die Benutzerinformationen für einen vSphere Recovery Agent zu ändern, müssen Sie den VRA deinstallieren, den VRA während der neuen Portal-Registrierung erneut installieren und anschließend den VRA mit dem Vault erneut registrieren.

So ändern Sie die Portal-Registrierung für den vSphere Recovery Agent:

1. Sichern Sie auf dem Rechner, auf dem der VRA installiert ist, die Protokolldateien im Ordner, in dem der Agent installiert ist.
2. Deinstallieren Sie den VRA.
3. Installieren Sie den VRA neu. Wenn Sie aufgefordert werden, den Agenten bei Portal zu registrieren, geben Sie die neuen Portal-Registrierungsinformationen ein. Siehe *Der vSphere Recovery Agent (VRA) ist eine Windows-Anwendung. Sie können den VRA auf einem physischen oder virtuellen Windows-Rechner installieren, der lokalen Netzwerkzugriff auf das vCenter oder den ESXi-Host hat, das bzw. den Sie schützen möchten.* auf Seite 12.

4. Klicken Sie in Portal in der Navigationsleiste auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
5. Suchen Sie den installierten VRA und klicken Sie auf die entsprechende Zeile, um die Ansicht zu erweitern.

Die Felder „Automatisch konfigurieren“ und „Manuell konfigurieren“ werden angezeigt.



6. Klicken Sie auf **Manuell konfigurieren**.
7. Klicken Sie auf der Registerkarte „Vault-Einstellungen“ auf **Erneut registrieren**.



8. Führen Sie im Dialogfeld „Vault-Einstellungen“ eine der folgenden Maßnahmen durch:
 - Wählen Sie in der Liste **Vault-Profil** den Vault aus, der Sicherungen vom ursprünglichen VRA enthält. Daraufhin werden die Vault-Einstellungen und Anmeldeinformationen im Dialogfeld ausgefüllt.
 - Geben Sie im Feld **Vault-Name** einen Namen für den Vault ein. Geben Sie im Feld **Adresse** den Hostnamen oder die IPV4-Adresse des Vaults ein, für den Sicherungen vom ursprünglichen VRA verfügbar sind. Geben Sie in den Feldern **Konto**, **Benutzername** und **Kennwort** ein Konto und die Anmeldeinformationen zum Sichern und Wiederherstellen von Daten aus dem Vault ein.

Geben Sie nach Möglichkeit den Hostnamen des Vaults an. Auf diese Weise können IP-Adressänderungen per DNS verarbeitet werden.
9. Klicken Sie auf **Computer laden**.
10. Klicken Sie in der Computerliste auf den Namen der ursprünglichen VRA. Klicken Sie auf **Speichern**.
11. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
12. Geben Sie auf der Registerkarte „vSphere-Einstellungen“ den Benutzernamen und das Kennwort zur Authentifizierung bei vCenter oder ESXi-Host ein.
13. Klicken Sie auf **Speichern**. Die Meldung „Erfolg“ wird angezeigt. Klicken Sie auf **OK**.
14. Führen Sie auf der Registerkarte „Jobs“ für jeden Sicherungsjob die folgenden Maßnahmen durch:

- a. Klicken Sie im Menü **Aktion auswählen** auf **Job bearbeiten**.
 - b. Geben Sie im Dialogfeld „Job bearbeiten“ erneut das Verschlüsselungskennwort für den Job in den Felder **Kennwort** und **Kennwort bestätigen** ein.
WICHTIG: Um ein erneutes Seeding des Jobs zu verhindern, müssen Sie das Verschlüsselungskennwort eingeben, das während der Ausführung des Sicherungsjobs durch den ursprünglichen VRA verwendet wurde.
 - c. Speichern Sie den Job.
 - d. Klicken Sie im Menü **Aktion auswählen** auf **Synchronisieren**.
15. Wenn auf der Registerkarte „Erweitert“ die Registerkarte „Benachrichtigungen“ angezeigt wird und Sie SMTP-Einstellungen bearbeiten können, geben Sie die SMTP-Anmeldeinformationen ein und speichern Sie sie. Klicken Sie auf **Speichern**.

3.5 Hinzufügen von Vault-Einstellungen

Bevor ein VRA Daten sichern oder aus einem Vault wiederherstellen kann, müssen Vault-Einstellungen für den VRA hinzugefügt werden. Die Vault-Einstellungen umfassen Vault-Informationen, Anmeldeinformationen und Verbindungsinformationen für den Zugriff auf einen Vault.

Beim Hinzufügen von Vault-Einstellungen für ein VRA können Administratorbenutzer und normale Benutzer manuell Vault-Informationen eingeben oder ein Vault-Profil mit Vault-Informationen und Anmeldedaten auswählen.

Wenn eine Richtlinie zu ein VRA zugewiesen ist, können Administratorbenutzer jedes beliebige Vault-Profil aus der Richtlinie auswählen. Normale Benutzer können nur diejenigen Vault-Profile aus der Richtlinie auswählen, die ihnen zugewiesen wurden.

Wenn keine Richtlinie zu ein VRA zugewiesen ist, können Administratorbenutzer jedes beliebige Vault-Profil in der Site auswählen. Normale Benutzer können nur diejenigen Vault-Profile auswählen, die ihnen zugewiesen wurden.

Die Over-the-Wire-Verschlüsselung (OTW) wird automatisch aktiviert, wenn Sie Vault-Einstellungen hinzufügen oder vorhandene Vault-Einstellungen ändern.

So fügen Sie Vault-Einstellungen hinzu:

1. Klicken Sie in Portal in der Navigationsleiste auf **Computer**.
2. Suchen Sie VRA, für das Sie Vault-Einstellungen hinzufügen möchten, und klicken Sie auf die VRA-Zeile, um seine Ansicht zu erweitern.

Wenn das Feld „Manuell konfigurieren“ angezeigt wird, klicken Sie auf **Manuell konfigurieren**. Das Feld „Manuell konfigurieren“ wird bei einigen Computern angezeigt, auf denen kein Sicherungsjob erstellt wurde.

3. Klicken Sie auf der Registerkarte „Vault-Einstellungen“ auf **Vault hinzufügen**.

Das Dialogfeld „Vault-Einstellungen“ wird angezeigt.

4. Führen Sie eine der folgenden Aktionen aus:

- Geben Sie im Feld **Vault-Name** einen Namen für den Vault ein. Geben Sie im Feld **Adresse** den Hostnamen oder die IPV4-Adresse des Vaults ein. Geben Sie in den Feldern **Konto**, **Benutzername** und **Kennwort** ein Konto und die Anmeldeinformationen zum Sichern und Wiederherstellen von Daten aus dem Vault ein.

Geben Sie nach Möglichkeit den Hostnamen des Vaults an. Auf diese Weise können IP-Adressänderungen per DNS verarbeitet werden.

- Klicken Sie auf das Feld **Vault-Profil**. Falls eines oder mehrere Vault-Profile angezeigt werden, klicken Sie auf das Vault-Profil, das Sie zum Computer hinzufügen möchten. Vault-Informationen und Anmeldeinformationen werden dann im Dialogfeld „Vault-Einstellungen“ gefüllt.

Wenn eine Richtlinie zugewiesen ist, werden in der Liste **Vault-Profil** die Vault-Profile aus der Richtlinie angezeigt. Wenn keine Richtlinie zugewiesen ist, werden in der Liste die Vault-Profile aus der Site angezeigt. Für normale Benutzer werden in der Liste nur diejenigen Vault-Profile angezeigt, die ihnen zugewiesen wurden.

5. (Optional) Ändern Sie bei Bedarf die folgenden erweiterten Einstellungen für die Vault-Verbindung:

- **Hostname des Agenten**. Name für den VRA im Vault.
- **Portnummer**. Der Port für die Verbindung mit dem Vault. Der Standardport ist 2546.
- **Alle x Sekunden versuchen, die Verbindung wiederherzustellen**. Legt fest, nach wie vielen Sekunden sich der Agent erneut mit dem Vault verbindet, wenn die Verbindung während einer Sicherung oder Wiederherstellung abbricht. Der Wert kann zwischen 30 und 1800 Sekunden betragen.
- **Verbindungsversuche abbrechen nach**. Geben Sie an, nach wie vielen Minuten sich der Agent nicht mehr erneut mit dem Vault verbinden soll, wenn die Verbindung während einer Sicherung oder Wiederherstellung abbricht. Der Wert kann 60 bis 720 Minuten betragen. Wenn sich der Agent innerhalb der angegebenen Zeit nicht mit dem Vault verbinden kann, schlägt die Sicherung bzw. Wiederherstellung fehl.

6. Klicken Sie auf **Speichern**.

3.6 Hinzufügen einer Beschreibung

Sie können eine Beschreibung für ein VRA in Portal hinzufügen. Die Beschreibung wird auf der Seite „Computer“ angezeigt. Sie unterstützt bei der Suche und Identifizierung eines bestimmten VRAs.

So fügen Sie eine Beschreibung hinzu:

1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den VRA, für den Sie eine Beschreibung hinzufügen möchten, und klicken Sie auf die Zeile, um ihre Ansicht zu erweitern.
Wenn das Feld „Manuell konfigurieren“ angezeigt wird, klicken Sie auf **Manuell konfigurieren**. Das Feld „Manuell konfigurieren“ wird bei einigen Computern angezeigt, auf denen kein Sicherungsjob erstellt wurde.
3. Klicken Sie in der Registerkarte „Erweitert“ auf die Registerkarte **Optionen**.
4. Geben Sie im Feld „Agent-Beschreibung“ eine Beschreibung für den VRA ein.



5. Klicken Sie auf **Speichern**.

3.7 Hinzufügen von Aufbewahrungstypen

Bei der Erstellung und Ausführung von Sicherungsjobs müssen Sie einen Aufbewahrungstyp für den resultierenden Sicherungssatz auswählen. Der Aufbewahrungstyp legt fest, für wie viele Tage eine Sicherung im Vault bleibt, wie viele Kopien der Sicherung online gespeichert werden und wie lange die Sicherungsdaten offline gespeichert werden.

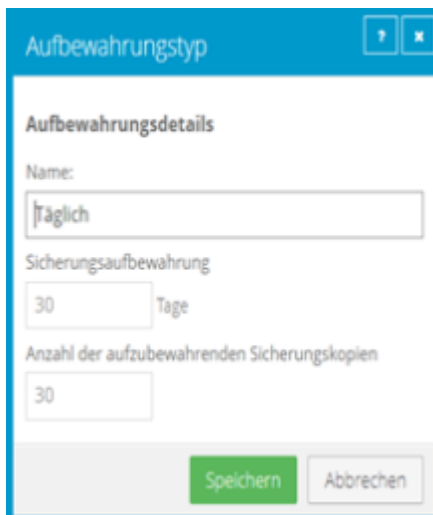
Administratorbenutzer und normale Benutzer können im Portal Aufbewahrungstypen für ein VRA hinzufügen, wenn keine Richtlinie zugewiesen ist.

Wenn eine Richtlinie zu ein VRA zugewiesen ist, können die Aufbewahrungstypen nicht auf der Seite „Computer“ hinzugefügt oder geändert werden. In diesem Fall können die Aufbewahrungstypen nur in der Richtlinie hinzugefügt oder geändert werden.

So können Sie einen Aufbewahrungstyp hinzufügen:

1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den VRA, für den Sie einen Aufbewahrungstyp hinzufügen möchten, und klicken Sie auf die Zeile, um die Ansicht zu erweitern.
Wenn das Feld „Manuell konfigurieren“ angezeigt wird, klicken Sie auf **Manuell konfigurieren**. Das Feld „Manuell konfigurieren“ wird bei einigen Computern angezeigt, auf denen kein Sicherungsjob erstellt wurde.

3. Klicken Sie in der Registerkarte „Erweitert“ auf die Registerkarte **Aufbewahrungstypen**.
Wenn eine Richtlinie zum VRA zugewiesen ist, können Sie in der Registerkarte „Aufbewahrungstypen“ keine Werte hinzufügen oder ändern. In diesem Fall können die Aufbewahrungstypen nur in der Richtlinie hinzugefügt oder geändert werden.
4. Klicken Sie auf **Aufbewahrungstyp erstellen**.
Das Dialogfeld „Aufbewahrungstyp“ wird geöffnet:



5. Füllen Sie die folgenden Felder aus:

Name	Gibt einen Namen für den Aufbewahrungstyp an.
Sicherungsaufbewahrung	Gibt an, wie viele Tage ein Sicherungssatz im Vault verbleibt. Wenn das Ablaufdatum erreicht ist, wird der Sicherungssatz gelöscht. <i>Hinweis:</i> Sicherungssätze werden nur dann gelöscht, wenn auch die angegebene Anzahl der Online-Kopien erreicht wurde.
Anzahl der aufzubewahrenden Sicherungskopien	Gibt an, wie viele Sicherungssätze eines Sicherungsjobs online gespeichert werden. Hierbei wird die Eingangsreihenfolge berücksichtigt. Wenn die maximale Anzahl der Sicherungssätze erreicht ist, werden die ältesten Sicherungssätze automatisch gelöscht, bis die tatsächliche Anzahl der Sicherungssätze den Angaben entspricht. <i>Hinweis:</i> Sicherungssätze werden erst dann gelöscht, wenn auch die angegebene Dauer der Onlinespeicherung (Tage) erreicht ist.
Archivierte Kopien erstellen	Markieren Sie dieses Kontrollkästchen, um archivierte Kopien von Sicherungssätzen zu erstellen.

Archive beibehalten für	<p><i>Hinweis:</i> Wenn die Datenarchivierung in Ihrer Portal-Instanz deaktiviert ist, wird dieser Wert nicht angezeigt.</p> <p>Gibt an, wie lange die Daten offline gespeichert werden. Die Archivspeicherung wird verwendet, um Daten über einen längeren Zeitraum offline zu speichern. Auf diese Daten kann nicht sofort zugegriffen werden, da sie an einem entfernten Standort gespeichert sind. Die Wiederherstellung von Archivdatenträgern ist zeitaufwändiger. In der Regel werden nur Langzeitdatenarchive offline gespeichert. Die Parameter für archivierte Daten liegen bei 365 bis 9999 Tagen.</p> <p>Wenn mindestens eine Sicherung erfolgreich für den Job abgeschlossen wurde, existiert mindestens eine Onlinekopie seiner Sicherung. Dies gilt auch, wenn alle Aufbewahrungseinstellungen auf null gesetzt sind, Ablaufbedingungen erfüllt sind und die Jobdefinition aus Ihrem System gelöscht wurde. Das Löschen des Jobs hat keine Auswirkung auf die Daten im Vault. Nur Ihr Dienstleister kann Jobs und die dazugehörigen Daten aus dem Vault entfernen. Dies dient als Vorsichtsmaßnahme, um zu verhindern, dass Daten versehentlich oder böswillig vernichtet werden.</p>
-------------------------	--

6. Klicken Sie auf **Speichern**.

3.8 Konfigurieren der Bandbreitendrosselung

Mögliche Bandbreiteneinstellungen:

- Maximale Bandbreite (obere Grenze) in MB pro Sekunde, die der Agent für Sicherungen und Wiederherstellungen verbrauchen darf.
- Zeitraum tagsüber, an dem die Drosselung aktiviert ist. Es kann nur ein Zeitfenster angegeben werden. Außerhalb des Zeitfensters findet keine Drosselung statt.
- Die Wochentage, an denen die Drosselung aktiviert ist.

Wenn das Zeitfenster für die Bandbreitendrosselung während einer laufenden Sicherung beginnt, wird die maximale Bandbreite dynamisch für die laufende Sicherung übernommen. Wenn das Zeitfenster für die Drosselung während einer laufenden Sicherung endet, wird die Bandbreitendrosselung für die Sicherung aufgehoben.

Wenn Sie die Bandbreiteneinstellungen eines ein VRAs während einer laufenden Sicherung ändern, wirken sich die neuen Einstellungen nicht auf die laufende Sicherung aus. Die Bandbreiteneinstellungen werden beim Start der Sicherung übernommen und nicht nachträglich für bereits laufende Sicherungen geändert.

Wenn eine Richtlinie zu einem ein VRA zugewiesen ist, können die Einstellungen für die Bandbreitendrosselung nicht auf der Seite „Computer“ geändert werden. In diesem Fall können die Einstellungen nur in der Richtlinie hinzugefügt oder geändert werden.

So können Sie die Bandbreitendrosselung konfigurieren:

1. Klicken Sie in der Navigationsleiste auf **Computer**.

- Suchen Sie den VRA, für den Sie die Bandbreitendrosselung konfigurieren möchten, und klicken Sie auf die Zeile, um die Ansicht zu erweitern.

Wenn das Feld „Manuell konfigurieren“ angezeigt wird, klicken Sie auf **Manuell konfigurieren**. Das Feld „Manuell konfigurieren“ wird bei einigen Computern angezeigt, auf denen kein Sicherungsjob erstellt wurde.

- Klicken Sie in der Registerkarte **Erweitert** auf die Registerkarte **Leistung** und bearbeiten Sie die Bandbreiteneinstellungen.

Wenn eine Richtlinie zum VRA zugewiesen ist, können Sie auf der Registerkarte Leistung keine Werte hinzufügen oder ändern. Stattdessen müssen die Bandbreiteneinstellungen in der Richtlinie geändert werden.

Hinweis: Je nach Internetgeschwindigkeit kann der empfohlene maximale Bandbreitenwert (1,5 Mbit/s), der in Portal angezeigt wird, niedrig sein. Dies ist lediglich eine Empfehlung. Sie können eine höhere maximale Bandbreite angeben, wenn diese von Ihrer Internetgeschwindigkeit unterstützt wird.



- Klicken Sie auf **Speichern**.

4 Hinzufügen von vSphere-Sicherungsjobs

Sie müssen Vault-Einstellungen und vSphere-Umgebungsinformationen hinzufügen, bevor Sie einen Sicherungsjob hinzufügen können. Siehe *Konfigurieren des vSphere-Recovery-Agenten* auf Seite 16.

Sie können die folgenden Optionen in einem vSphere-Sicherungsjob aktivieren:

- **Anwendungskonsistente Sicherungen.** Ab Version 8.82 kann der VRA anwendungskonsistente Sicherungen von Microsoft SQL Server, Exchange, SharePoint und Active Directory auf Windows-VMs erstellen. Anwendungskonsistente Sicherungen minimieren den Arbeitsaufwand zum Wiederherstellen von Anwendungen aus Sicherungen. Sie können auch angeben, ob Anwendungstransaktionsprotokolle während anwendungskonsistenter Sicherungen abgeschnitten werden sollten. Weitere Informationen finden Sie unter *Anwendungskonsistente Sicherungen auf vSphere-VMs* auf Seite 32.

Hinweis: Ein Sicherungs-Snapshot enthält nur VM-Daten, die auf die Festplatte geschrieben werden. Wenn sich Datei-Schreibvorgänge noch im Speicher befinden, wenn eine Sicherung ausgeführt wird, werden einige Daten möglicherweise nicht erfasst, selbst wenn die Sicherung anwendungskonsistent ist. Bei einer anwendungskonsistenten Sicherung werden ausstehende Transaktionen für einige Anwendungen auf die Festplatte geschrieben, jedoch nicht für das gesamte Dateisystem. Um das Betriebssystem zu zwingen, die Daten im Speicher auf die Festplatte zu schreiben, können Sie ein Drittanbieter-Dienstprogramm vor einer Sicherung ausführen.

- **Ransomware-Bedrohungserkennung.** Ab Version 9.10 kann der VRA bei der Ausführung des Sicherungsjobs Windows-VMs auf mögliche Ransomware-Bedrohungen prüfen. Wenn der VRA eine mögliche Bedrohung auf einer VM erkennt, wird die VM-Sicherung im Portal als mögliche Bedrohung gekennzeichnet, damit Sie die Bedrohung untersuchen und beheben können. Siehe *Handhaben möglicher Ransomware-Bedrohungen* auf Seite 44.


Hinweis: Der VRA prüft in einer Seed-Sicherung oder der ersten Sicherung nicht auf mögliche Ransomware-Bedrohungen, wenn die Bedrohungserkennung in einem Job aktiviert ist.

- **Sicherungsüberprüfung.** Ab Version 9.00 kann der VRA VMs im Job sichern und dann prüfen, ob jede Windows VM aus der Sicherung wiederhergestellt werden kann. Siehe *Sicherungsüberprüfung für vSphere-VMs* auf Seite 34. Die Einstellungen für die Sicherungsüberprüfung müssen auch für den VRA eingegeben werden. Siehe *Eingabe der Einstellungen für die Sicherungsüberprüfung für einen vSphere Recovery Agent* auf Seite 20.

So fügen Sie einen vSphere-Sicherungsjob hinzu:

1. Klicken Sie in der Navigationsleiste auf **Computer**.

Die Seite „Computer“ zeigt registrierte Computer und Umgebungen.

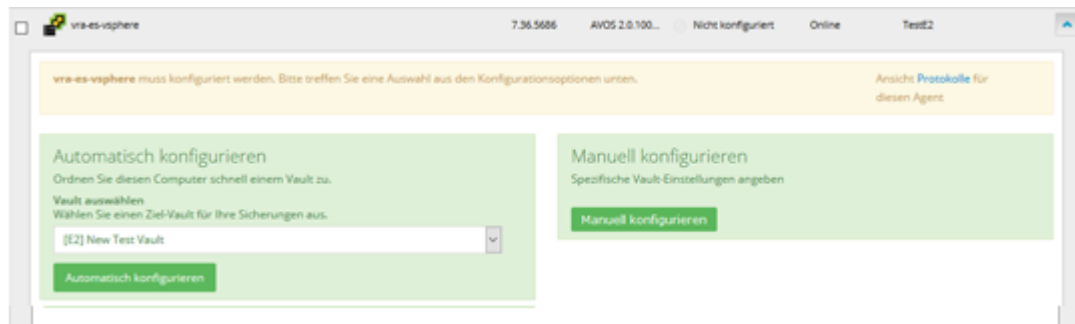
2. Klicken Sie auf die Zeile mit der vSphere-Umgebung. 

Wenn eine Meldung angezeigt wird, dass der Agent konfiguriert werden muss, müssen Sie Vault-Einstellungen und vSphere-Umgebungsinformationen hinzufügen, bevor Sie einen Sicherungsjob hinzufügen. Siehe *Konfigurieren des vSphere-Recovery-Agenten* auf Seite 16.

Wenn in der vSphere-Umgebung keine Vault-Einstellungen festgelegt sind, wird das Feld „Manuell konfigurieren“ angezeigt. Um Vault-Einstellungen manuell hinzuzufügen, klicken Sie

auf **Manuell konfigurieren** und fügen Sie auf der Registerkarte „Vault-Einstellungen“ einen Vault hinzu. Siehe *Hinzufügen von Vault-Einstellungen* auf Seite 22.

Wenn in der vSphere-Umgebung keine Vault-Einstellungen festgelegt sind, wird das Feld „Automatisch konfigurieren“ angezeigt. Wählen Sie zum Hinzufügen von Vault-Einstellungen einen Vault aus der Liste **Vault auswählen**. Wenn die Liste **Diesen Computer einer Site zuordnen** angezeigt wird, können Sie auch eine untergeordnete Site für den Computer auswählen. Klicken Sie auf **Automatisch konfigurieren**.



3. Klicken Sie auf die Registerkarte **Jobs**.
4. Klicken Sie im Menü **Jobaufgabe auswählen** auf **Neuen Job für VMware vSphere erstellen**.

Geben Sie im Dialogfeld „Mit vSphere verbinden“ folgende Informationen an:

- Geben Sie im Feld **Benutzername** den Benutzernamen für das Windows-Domänenkonto ein, das zur Authentifizierung des VRA beim vCenter oder ESXi-Host verwendet wird.
- Geben Sie im Feld **Kennwort** das Kennwort des angegebenen Benutzers ein.
- Geben Sie im Feld **Domäne** die Domäne des angegebenen Benutzerkontos ein. Die Domäne ist optional, wenn Sie die Domäne im Feld **Benutzername** eingeben (z. B. *Domäne\Benutzername*).

Hinweis: Die in diesem Dialogfeld eingegebenen vSphere-Umgebungseinstellungen werden auf der Registerkarte **vSphere-Einstellungen** des Agenten übernommen.

5. Geben Sie im Dialogfeld „Neuen Job erstellen“ folgende Informationen an:
 - Geben Sie im Feld **Name** einen Namen für den Sicherungsjob an.
 - Geben Sie im Feld **Beschreibung** eine optionale Beschreibung für den Sicherungsjob an.
 - Wählen Sie in der Liste **Ziel** den Vault aus, in dem die Sicherungsdaten gespeichert werden sollen.
In der Liste werden Vaults nur angezeigt, wenn sie dem Benutzer zugewiesen sind oder wenn der Benutzer sie auf der Registerkarte „Vault-Einstellungen“ des Computers hinzugefügt hat.
 - Wählen Sie in der Liste **Protokolldateioptionen** die Detailebene für die Protokollierung aus. Weitere Informationen finden Sie unter *Protokolldateioptionen* auf Seite 35.
 - Neue Sicherungsjobs verwenden die Verschlüsselungsmethode AES (256 Bit). Vorhandene Jobs können andere Verschlüsselungsmethoden nutzen. Siehe *Verschlüsselungseinstellungen* auf Seite 35.

- Geben Sie in die Felder **Kennwort** und **Kennwort bestätigen** ein Verschlüsselungskennwort ein. Sie können auch einen Kennworthinweis in das Feld **Kennworthinweis** eingeben.
6. Führen Sie im Dialogfeld „In Sicherung aufnehmen“ eine oder mehrere der folgenden Aktionen aus, bis im Feld **Sicherungssatz** alle VMs angezeigt werden, die Sie in den Sicherungsjob einschließen oder daraus ausschließen möchten:
- Um bestimmte VMs zum Sicherungsjob hinzuzufügen, aktivieren Sie das Kontrollkästchen für die jeweilige VM und klicken Sie anschließend auf **Einschließen**.
 - Um bestimmte VMs vom Sicherungsjob auszuschließen, aktivieren Sie das Kontrollkästchen für die jeweilige VM und klicken Sie anschließend auf **Ausschließen**.
 - Um bestimmte VMs anhand des Namens zum Sicherungsjob hinzuzufügen, aktivieren Sie das Kontrollkästchen **Virtuelle Maschinen** und klicken Sie anschließend auf **Einschließen**. Geben Sie im Feld **Filter** die Namen der VMs ein, die Sie einschließen möchten. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. Um beispielsweise VMs in einer Sicherung einzuschließen, deren Namen mit „x64“ enden oder mit „SQL“ beginnen, geben Sie folgenden Filter ein: *x64, SQL*
- Hinweis:* Das Sternchen (*) ist das einzige unterstützte Platzhalterzeichen in Filterfeldern.
- Um bestimmte VMs anhand des Namens vom Sicherungsjob auszuschließen, aktivieren Sie das Kontrollkästchen **Virtuelle Maschinen** und klicken Sie anschließend auf **Ausschließen**. Geben Sie im Feld **Filter** die Namen der VMs ein, die Sie ausschließen möchten. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. Um beispielsweise VMs von einer Sicherung auszuschließen, deren Namen mit „Testen“ enden oder mit „x32“ beginnen, geben Sie folgenden Filter ein: test*, *x32
 - Um einen Einschließen- oder Ausschließen-Datensatz im Feld **Sicherungssatz** zu entfernen, klicken Sie neben dem Datensatz auf die Schaltfläche „Löschen“.
7. Legen Sie fest, ob der VRA anwendungskonsistente Sicherungen durchführen soll, indem Sie eine der folgenden Optionen wählen:
- Um absturzkonsistente Sicherungen von VMs im Sicherungsjob durchzuführen, deaktivieren Sie das Kontrollkästchen **Anwendungskonsistente Sicherungen aktivieren**.
 - Um anwendungskonsistente Sicherungen von SQL Server, Exchange, SharePoint und Active Directory auf Windows VMs im Sicherungsjob durchzuführen, gehen Sie wie folgt vor:
 - a. Aktivieren Sie das Kontrollkästchen **Anwendungskonsistente Sicherungen**.
 - b. Führen Sie eine der folgenden Aktionen aus:
 - Um Anwendungstransaktionsprotokolle auf VMs im Job beizubehalten, deaktivieren Sie das Kontrollkästchen **Datenbanktransaktionsprotokolle abschneiden**.
 - Um Anwendungstransaktionsprotokolle auf VMs im Job abzuschneiden, aktivieren Sie das Kontrollkästchen **Datenbanktransaktionsprotokolle abschneiden**, und geben Sie die Anmeldeinformationen zur Herstellung einer Verbindung mit VMs im Job ein.

Um Anmeldeinformationen für mehrere VMs im Job einzugeben, geben Sie einen Benutzernamen und ein Passwort im Bereich **Gast-VM-Anmeldeinformationen** ein.

Um Anmeldeinformationen für eine spezifische VM im Job einzugeben, klicken Sie auf den Pfeil rechts neben dem VM-Namen im Bereich „Sicherungssatz“, und geben Sie einen Benutzernamen und ein Passwort im Bereich **Gast-VM-Anmeldeinformationen** für die VM ein.

Sie können einen Benutzernamen als *Benutzername* oder *Domäne\Benutzername* eingeben. Die angegebenen Benutzer benötigen Administratorzugriff auf VMs im Sicherungsjob; sie benötigen keine Administratorrechte für Anwendungen auf den VMs.

Hinweis: Wenn Sie Anmeldeinformationen für eine spezifische VM im Job eingeben, versucht der Agent nicht, eine Verbindung zur VM mit den für mehrere VMs im Job angegebenen Anmeldeinformationen herzustellen.

Hinweis: Wenn Sie außerdem die Datenbanken mit einem anderen Tool (z. B. native SQL Server-Sicherung) sichern, verwenden Sie nur ein Tool, um die Protokolle zu kürzen.

- Um eine anwendungskonsistente Sicherung eines Domänencontrollers mit Active Directory durchzuführen, aktivieren Sie die Option **Datenbanktransaktionsprotokolle abschneiden** und geben Sie die Domänenadministrator-Anmeldeinformationen für die VM im Format *Domäne\Benutzername* ein.

Hinweis: Es sind keine Protokolle zum Abschneiden vorhanden, wenn Sie anwendungskonsistente Sicherungen von Domänencontrollern mit Active Directory durchführen. Für anwendungskonsistente Sicherungen von Domänencontrollern sind jedoch Anmeldeinformationen mit Domänenadministratorrechten erforderlich. Wenn die Option zum Abschneiden von Protokollen aktiviert ist, können Sie die erforderlichen Anmeldedaten eingeben.

8. Legen Sie fest, ob der VRA auf mögliche Ransomware-Bedrohungen prüfen soll, indem Sie eine der folgenden Optionen wählen:

- Um VMs ohne Prüfung auf mögliche Ransomware-Bedrohungen zu sichern, deaktivieren Sie das Kontrollkästchen **Bedrohungserkennung aktivieren**.

WICHTIG: Wenn Sie die Bedrohungserkennung für einen Job deaktivieren, bei dem sie aktiviert war, werden alle möglichen Bedrohungskennzeichen für Sicherungen in diesem Job gelöscht. Deaktivieren Sie die Bedrohungserkennung für einen Job erst, wenn alle möglichen Bedrohungen beseitigt wurden. Siehe *Handhaben möglicher Ransomware-Bedrohungen* auf Seite [44](#).

- Um VMs zu sichern und auf mögliche Ransomware-Bedrohungen zu prüfen, aktivieren Sie das Kontrollkästchen **Bedrohungserkennung aktivieren**. Wenn Sie keine Anmeldeinformationen zum Abschneiden von Anwendungstransaktionsprotokollen in Schritt 7 angegeben haben, geben Sie die Anmeldeinformationen zur Herstellung einer Verbindung mit VMs im Job ein.

Um Anmeldeinformationen für mehrere VMs im Job einzugeben, geben Sie einen Benutzernamen und ein Passwort im Bereich **Gast-VM-Anmeldeinformationen** ein.

Um Anmeldeinformationen für eine spezifische VM im Job einzugeben, klicken Sie auf den Pfeil rechts neben dem VM-Namen im Bereich „Sicherungssatz“, und geben Sie einen Benutzernamen und ein Passwort im Bereich **Gast-VM-Anmeldeinformationen** für die VM ein.

Sie können einen Benutzernamen als *Benutzername* oder *Domäne\Benutzername* eingeben. Der angegebene Benutzer oder die Benutzer benötigt/benötigen Administratorzugriff auf VMs im Sicherungsjob.

Hinweis: Für das Abschneiden von Transaktionsprotokollen in anwendungskonsistenten Sicherungen und die Überprüfung auf mögliche Ransomware-Bedrohungen werden dieselben Anmeldeinformationen verwendet.

Hinweis: Wenn Sie Anmeldeinformationen für eine spezifische VM im Job eingeben, versucht der Agent nicht, eine Verbindung zur VM mit den für mehrere VMs im Job angegebenen Anmeldeinformationen herzustellen.

9. Legen Sie fest, ob der VRA prüfen soll, ob VMs wiederhergestellt werden können, indem Sie eine der folgenden Optionen wählen:

- Um VMs zu sichern und nicht zu prüfen, ob sie wiederhergestellt werden können, deaktivieren Sie das Kontrollkästchen **Diese Sicherung bei Abschluss überprüfen**.
- Um VMs zu sichern und zu prüfen, ob Windows VMs aus der Sicherung wiederhergestellt werden können, aktivieren Sie das Kontrollkästchen **Diese Sicherung bei Abschluss überprüfen**.

Hinweis: Sie können die Sicherungsüberprüfung nur aktivieren, wenn der gewählte Vault diese Funktion unterstützt und die Einstellungen für die Sicherungsüberprüfung für den VRA eingegeben wurden. Siehe *Anforderungen für vSphere Rapid VM Restore und Sicherungsüberprüfung* auf Seite 8 und *Eingabe der Einstellungen für die Sicherungsüberprüfung für einen vSphere Recovery Agent* auf Seite 20.

10. Klicken Sie auf **Job erstellen**.

Der Job wird erstellt und das Dialogfeld „Zeitplan anzeigen/hinzufügen“ wird angezeigt. Um einen Zeitplan für die Ausführung der Sicherung zu erstellen, siehe *Nach dem Erstellen eines Sicherungsjobs können Sie ihn jederzeit manuell (ad hoc) ausführen und ihn für bestimmte Tage in der Woche oder im Monat planen. Siehe Run an ad-hoc backup und Schedule a backup job to run daily or monthly.* auf Seite 36. Klicken Sie auf **Abbrechen**, wenn Sie aktuell keinen Zeitplan erstellen möchten.

4.1 Anwendungskonsistente Sicherungen auf vSphere-VMs

Ab Version 8.82 kann der vSphere-Recovery-Agent anwendungskonsistente Sicherungen von Microsoft SQL Server, Exchange, SharePoint und Active Directory auf virtuellen Windows-Maschinen (VMs) in vSphere-Umgebungen erstellen.

Hinweis: Eine VRA-Sicherung ist für eine autoritative Wiederherstellung von Active Directory-Objekten nicht ausreichend. Für eine autoritative Wiederherstellung ist eine Systemstatussicherung mit Windows Agent erforderlich.

In einer anwendungskonsistenten Sicherung werden ausstehende Anwendungstransaktionen vor dem Sichern der Daten auf Datenträger geschrieben. Dies minimiert den Arbeitsaufwand zum Wiederherstellen der Anwendung.

Wenn Anwendungskonsistenz nicht in einem Sicherungsjob aktiviert ist, sind die Sicherungen absturzkonsistent. In einer absturzkonsistenten Sicherung werden ausstehende Anwendungstransaktionen zurückgerollt. Es sind manuelle Schritte erforderlich, um sicherzustellen, dass Anwendungen komplett wiederhergestellt werden.

Wenn Sie anwendungskonsistente Sicherungen in einem Sicherungsjob aktivieren, aber keine anwendungskonsistente Sicherung für eine VM erstellt werden kann, erstellt der VRA eine absturzkonsistente Sicherung für die VM. Um zu prüfen, ob jede VM-Sicherung anwendungs- oder absturzkonsistent ist, sehen Sie sich das Sicherungsprotokoll an.

Anwendungskonsistente Sicherungen werden nur auf Windows-VMs unterstützt. Wenn Linux-VMs in Sicherungsjobs enthalten sind, bei denen die anwendungskonsistente Sicherungseinstellung aktiviert ist, werden Warnungen für die Linux-VMs in den Sicherungsprotokollen angezeigt.

Um eine anwendungskonsistente Sicherung auf einer VM zu erstellen, muss VMware Tools Version 11 oder höher auf der VM installiert sein.

Hinweis: Der vSphere Recovery Agent kann eine Anwendungsdatenbank auf einer physical Raw Device Mapping (pRDM)-, freigegebenen oder unabhängigen Festplatte nicht sichern oder wiederherstellen. VMware erlaubt nicht das Einfügen dieser Festplattentypen in Snapshots für VM-Sicherungen. Um eine Anwendung auf einer pRDM-, freigegebenen oder unabhängigen Festplatte zu sichern, installieren Sie das Windows Agent- und SQL Server- oder Exchange-Plug-in auf der VM.

Protokollabschneidung in anwendungskonsistenten Sicherungen

Bei anwendungskonsistenten Sicherungen kann der vSphere Recovery Agent SQL Server-, Exchange- und SharePoint-Transaktionsprotokolle auf VMs abschneiden. Dies verhindert, dass Transaktionsprotokolle eine große Menge an Festplattenplatz verbrauchen und die Systemleistung reduzieren. Es sind keine Protokolle zum Abschneiden vorhanden, wenn Sie anwendungskonsistente Sicherungen von Domänencontrollern mit Active Directory durchführen.

Hinweis: Der vSphere Recovery Agent kann Transaktionsprotokolle für die standardmäßige SQL Server-Instanz und für alle Exchange Server-Datenbanken abschneiden. Der VRA kann keine Protokolle für benannte SQL Server-Instanzen abschneiden.

Um Transaktionsprotokolle auf einer VM nach einer anwendungskonsistenten Sicherung abzuschneiden, müssen Sie die Protokollabschneidung im Sicherungsjob aktivieren und Anmeldeinformationen bereitstellen, die Administratorzugriff auf die VM haben. Der angegebene Benutzer benötigt keine Administratorrechte für Anwendungen auf der VM; er benötigt nur Zugriff auf die VM.

Sie können Gast-VM-Anmeldeinformationen mit Administratorzugriff auf mehrere VMs in einem Sicherungsjob und/oder Anmeldeinformationen für spezifische VMs bereitstellen. Wenn Sie Anmeldeinformationen für eine spezifische VM bereitstellen, werden die Anmeldeinformationen für die Gast-VM für mehrere VMs nie verwendet, um eine Verbindung zu dieser VM herzustellen.

Protokolle können nicht abgeschnitten werden, wenn eine anwendungskonsistente Sicherung aus einem bestimmten Grund nicht durchgeführt werden konnte (z. B. VMware-Tools nicht auf Gast-VM installiert).

Um zu prüfen, ob die Protokollabschneidung auf jeder VM nach einer Sicherung erfolgreich war, sehen Sie sich die Sicherungsprotokolle an.

Hinweis: Wenn Sie außerdem die Datenbanken mit einem anderen Tool (z. B. native SQL Server-Sicherung) sichern, verwenden Sie nur ein Tool, um die Protokolle zu kürzen.

4.2 Sicherungsüberprüfung für vSphere-VMs

Ab Version 9.00 kann der vSphere Recovery Agent prüfen, ob jede Windows VM in einer Sicherung wiederhergestellt werden kann. Sie können die Überprüfungsergebnisse im Sicherungsüberprüfungs-Bericht ab Portal Version 9.00 anzeigen. Siehe *Anzeige des Sicherungsüberprüfungs-Berichts* auf Seite [84](#).

Wenn Einstellungen für die Sicherungsüberprüfung für einen VRA eingegeben werden und die Sicherungsüberprüfung für einen vSphere-Sicherungsjob aktiviert ist, sichert der VRA die VMs im Job und prüft dann, ob jede Windows VM aus der Sicherung wiederhergestellt werden kann. Mithilfe automatisierter Rapid VM Restore-Prozesse versucht der VRA, jede VM aus der Sicherung zu starten und macht einen Screenshot des Anmeldebildschirms für jede Windows VM, die wiederhergestellt werden kann.

Die VMs in einem Sicherungsjob werden sequentiell, eine nach der anderen, überprüft. Der Überprüfungsprozess für jede VM kann bis zu 10 Minuten dauern. Wenn die VM nach 10 Minuten noch nicht gestartet ist, wird der Prozess abgebrochen und der VRA versucht, die nächste VM im Sicherungsjob zu überprüfen.

Wenn VMs in einem Sicherungsjob gerade überprüft werden und Sie den Sicherungsjob erneut starten, wird die Überprüfung für VMs, die noch nicht überprüft wurden, abgebrochen. Wenn VMs in einem Sicherungsjob in letzter Zeit nicht überprüft wurden, wurde der Job möglicherweise zu häufig geplant, um die Sicherungsüberprüfung abschließen zu können.

Es kann nur ein Rapid VM Restore-Prozess für eine VM in einem Sicherungsjob gleichzeitig ausgeführt werden, unabhängig davon, ob Rapid VM Restores von einem Benutzer oder von einem Sicherungsüberprüfungs-Prozess gestartet werden. Wenn der VRA versucht, eine VM-Sicherung zu überprüfen, während Sie die VM mit Rapid VM Restore wiederherstellen, kann der Überprüfungsprozess fehlschlagen. Ebenso kann, wenn ein Überprüfungsprozess für eine VM-Sicherung beginnt, während die vorherige VM-Sicherung überprüft wird, die Überprüfung der neuen Sicherung fehlschlagen.

Weitere Informationen finden Sie unter *Anforderungen für vSphere Rapid VM Restore und Sicherungsüberprüfung* auf Seite [8](#), *Eingabe der Einstellungen für die Sicherungsüberprüfung für einen vSphere Recovery Agent* auf Seite [20](#) und *Hinzufügen von vSphere-Sicherungsjobs* auf Seite [28](#).

4.3 Protokolldateioptionen

Beim Erstellen oder Bearbeiten eines Sicherungsjobs können Sie die Detailebene für die Protokollierung des Jobs festlegen. Wählen Sie in der Liste eine der folgenden Protokollierungsebenen aus:

- **Dateien:** Bietet ausführlichere Informationen und wird in der Regel zur Fehlerbehebung verwendet. Bietet Informationen zu Dateien, die gesichert werden.
- **Verzeichnis:** Bietet weniger detaillierte Informationen als die Protokollierungsebene „Dateien“. Bietet Informationen zu Ordnern, die gesichert werden.
- **Zusammenfassung:** Bietet Informationen der obersten Ebene, einschließlich der Vault-/Agent-Version und Sicherungsgröße.
- **Minimal:** Bietet Informationen der obersten Ebene, einschließlich der Vault-/Agent-Version.

Eine Änderung der Protokollierungsebene wirkt sich nur auf Protokolldateien aus, die danach erstellt werden. Bereits erstellte Protokolldateien sind von dieser Änderung nicht betroffen.

4.4 Verschlüsselungseinstellungen

In den Verschlüsselungseinstellungen wird der Verschlüsselungstyp für statische Sicherungsdaten auf dem Vault festgelegt. Für neue Sicherungsjobs ist nur der Verschlüsselungstyp „AES 256-Bit“ verfügbar.

Wenn für einen vorhandenen Job ein anderer Verschlüsselungstyp verwendet wird (z. B. AES 128-Bit, Blowfish, DES, Triple DES), können Sie den Job mit diesem Typ weiterhin verschlüsseln. Wenn Sie jedoch den Verschlüsselungstyp für einen vorhandenen Job ändern, können Sie nicht mehr zum ursprünglichen Verschlüsselungstyp wechseln. Nur der Verschlüsselungstyp „AES 256-Bit“ steht zur Verfügung.

Wenn Sie die Verschlüsselungsoptionen für einen vorhandenen Job ändern, wird eine neue vollständige Sicherung erzwungen (d. h. ein erneutes Seeding ausgeführt). Die nächste Sicherung dauert länger als vorherige Deltasicherungen und die auf dem Vault gespeicherte Datenmenge nimmt kurzzeitig in Abhängigkeit von Ihren Aufbewahrungseinstellungen zu.

Verschlüsselungskennwort

Sie müssen ein Kennwort für die verschlüsselten Sicherungsdaten eingeben. Bei dem Kennwort wird zwischen Groß- und Kleinschreibung unterschieden. Für die Wiederherstellung der Daten müssen Sie das Verschlüsselungskennwort eingeben, das bei der Sicherung der Dateien eingegeben wurde.

Sie können auch einen Kennworthinweis eingeben. Bei der Wiederherstellung von Daten können Sie den Kennworthinweis anzeigen, damit Sie an das Verschlüsselungskennwort für diesen Job erinnert werden. Der Passworthinweis kann Kleinbuchstaben (a-z), Großbuchstaben (A-Z), internationale Zeichen (Á-ÿ), Zahlen (0-9), Leerzeichen und die folgenden Sonderzeichen beinhalten: ! @ # \$ % ^ & * () _ - + = [] { } | ' " : ; , < . > ? ~ `

WICHTIG: Das Verschlüsselungskennwort ist für die Wiederherstellung der Daten erforderlich; achten Sie daher darauf, es an einem sicheren Ort aufzubewahren. Wenn Sie dieses Kennwort vergessen haben, können Sie Ihre Daten nicht wiederherstellen. Das Kennwort wird an keiner anderen Stelle aufbewahrt und kann nicht wiederhergestellt werden.

Nach dem Erstellen eines Sicherungsjobs können Sie ihn jederzeit manuell (ad hoc) ausführen und ihn für bestimmte Tage in der Woche oder im Monat planen. Siehe *Ausführen einer Ad-hoc-Sicherung* auf Seite 42 und *Planen von Sicherungen* auf Seite 36.

Beim Ausführen und Planen von Sicherungen können Sie die folgenden Einstellungen festlegen:

- **Aufbewahrungstyp.** Der Aufbewahrungstyp legt die Anzahl der Tage fest, die eine Sicherung im Vault bleibt, wie viele Kopien von einer Sicherung online gespeichert werden und wie lange Sicherungsdaten offline gespeichert werden.
- **Zurückstellung.** Mit der Zurückstellung können Sie verhindern, dass umfangreiche Sicherungen im Netzwerk zu Spitzenlastzeiten ausgeführt werden. Wenn die Zurückstellung aktiviert ist, sichert der Sicherungsjob nach dem festgelegten Zeitraum keine neuen Daten mehr und führt einen Commit für den Sicherungssatz im Vault aus, auch wenn die Daten noch nicht komplett gesichert wurden. Änderungen an zuvor gesicherten Daten werden unabhängig vom angegebenen Zeitraum gesichert.

Wenn der Job erneut ausgeführt wird, sucht der Agent zunächst nach Änderungen in den bereits gesicherten Daten, sichert diese Änderungen und anschließend die restlichen Daten.

Wenn ein Sicherungsjob zurückgestellt wird, während ein Element gesichert wird, dann ist die Sicherung für dieses Element unvollständig, und die Daten des Elements können nicht wiederhergestellt werden. Sie können jedoch alle Elemente im Job wiederherstellen, die vor dem Zurückstellen vollständig gesichert wurden.

Wenn Sie einen Job für die Ausführung planen, können Sie außerdem den Komprimierungsgrad für die Daten festlegen. Die Komprimierungsstufe optimiert die Menge der gespeicherten Daten im Verhältnis zur Sicherungsgeschwindigkeit. Der Standardwert für den Komprimierungsgrad ist normalerweise optimal eingestellt.

Bei der ersten Ausführung eines Sicherungsjobs werden alle im Job ausgewählten Daten an den Vault übertragen. Diese Ausgangssicherung nennt man auch Seeding-Sicherung. Bei nachfolgenden Sicherungen werden nur noch die geänderten Daten an den Vault übertragen, es sei denn, ein erneutes Seeding ist erforderlich (z. B. nachdem das Verschlüsselungskennwort für den Job geändert wurde). Beim erneuten Seeding werden alle im Job ausgewählten Daten erneut an den Vault übertragen, auch wenn diese Daten zuvor bereits gesichert wurden.

Nach der Sicherung können Sie in den Protokollen nachsehen, ob die Sicherung erfolgreich abgeschlossen wurde. Siehe *Anzeigen von Protokollen zu Jobprozessen und Informationen zu Sicherungssätzen* auf Seite 90.

Manchmal müssen Sie einen Sicherungsjob synchronisieren, bevor Sie ihn ausführen oder Daten aus dem Job wiederherstellen können. Bei der Synchronisierung prüft der Agent, welche Sicherungssätze für den Job online sind und für die Wiederherstellung verfügbar sind. Siehe *Synchronisieren eines Jobs* auf Seite 43.

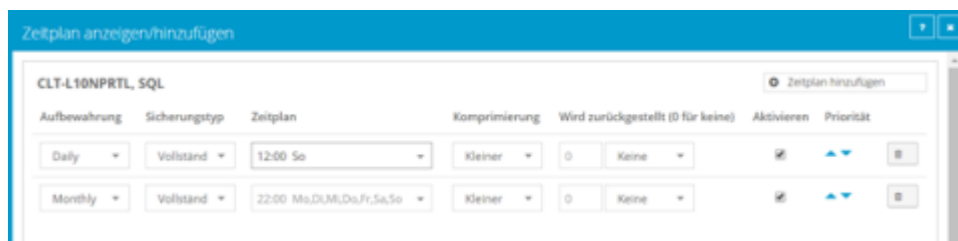
4.5 Planen von Sicherungen

Nachdem Sie einen Sicherungsjob erstellt haben, können Sie einen oder mehrere Zeitpläne für dessen Ausführung an bestimmten Tagen der Woche oder des Monats hinzufügen. Sie können mehrere Zeitpläne erstellen, um komplexe Ausführungspläne zu implementieren. Sie können zum

Beispiel einen Sicherungsjob planen, der jeden Freitag um Mitternacht und auch um 20:00 Uhr am ersten Tag eines Monats ausgeführt wird.

Wenn ein Job von mehreren Zeitplänen genau zur gleichen Zeit ausgeführt werden soll, wird der Job nur einmal zum geplanten Zeitpunkt ausgeführt. Der Aufbewahrungstyp des Zeitplans, der weiter oben in der Zeitplanliste steht, wird auf den resultierenden Sicherungssatz angewendet. Beispiel: In der folgenden Abbildung soll der Job laut zwei Zeitplänen samstags um Mitternacht ausgeführt werden. Samstags wird der Job nur einmal um Mitternacht ausgeführt. Da der Zeitplan mit dem Aufbewahrungstyp „Wöchentlich“ eine höhere Priorität in der Liste als der Zeitplan mit dem Aufbewahrungstyp „Täglich“ hat, wird der Aufbewahrungstyp „Wöchentlich“ für den resultierenden Sicherungssatz verwendet.

Hinweis: Wenn ein Job zu fast gleichen Zeiten geplant ist, versucht der Agent, jeden Zeitplan auszuführen. Wenn zum Beispiel ein Job für 23 Uhr und durch einen anderen Zeitplan für 23:01 Uhr geplant ist, versucht der Agent, den Job zweimal auszuführen. Versuchen Sie, sich überschneidende Zeitpläne zu vermeiden. Es können Probleme auftreten, wenn ein Job zweimal innerhalb kurzer Zeit ausgeführt werden soll.



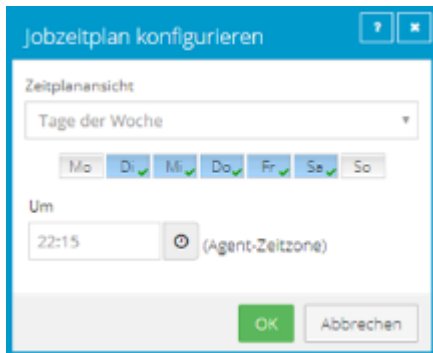
Beim Planen eines Sicherungsjobs wird im Dialogfeld „Zeitplan anzeigen/hinzufügen“ die maximale Anzahl von Wiederherstellungspunkten angezeigt, die sich aus den aktuellen Zeitplänen und Aufbewahrungstypen des Jobs ergeben können. Sie können dann Ihre Zeitpläne bei Bedarf ändern. Siehe *Maximale Anzahl von Wiederherstellungspunkten für einen Job* auf Seite 40.

So planen Sie einen Sicherungsjob, der täglich oder monatlich ausgeführt werden soll:

1. Führen Sie eine der folgenden Aktionen aus:
 - Klicken Sie in der Navigationsleiste auf **Computer**. Suchen Sie den VRA mit dem Sicherungsjob, den Sie planen möchten, und klicken Sie auf die Zeile, um ihre Ansicht zu erweitern. Suchen Sie auf der Registerkarte „Jobs“ den Job, den Sie zeitlich planen möchten. Klicken Sie im Menü **Aktion auswählen** auf **Zeitplan anzeigen/hinzufügen**.
 - Erstellen Sie einen neuen Sicherungsjob. Das Dialogfeld „Zeitplan anzeigen/hinzufügen“ wird angezeigt, wenn Sie den Job speichern.
2. Klicken Sie Dialogfeld „Zeitplan anzeigen/hinzufügen“ auf **Zeitplan hinzufügen**.
Im Dialogfeld wird eine neue Zeile hinzugefügt.
3. Klicken Sie in der neuen Zeile in der Liste **Aufbewahrung** auf einen Aufbewahrungstyp.
Der Aufbewahrungstyp legt die Anzahl der Tage fest, die eine Sicherung im Vault bleibt, wie viele Kopien von einer Sicherung online gespeichert werden und wie lange Sicherungsdaten offline gespeichert werden. Siehe *Hinzufügen von Aufbewahrungstypen* auf Seite 24.
6. Klicken Sie im Feld **Zeitplan** auf den Pfeil.
Das Dialogfeld „Jobzeitplan konfigurieren“ wird geöffnet.

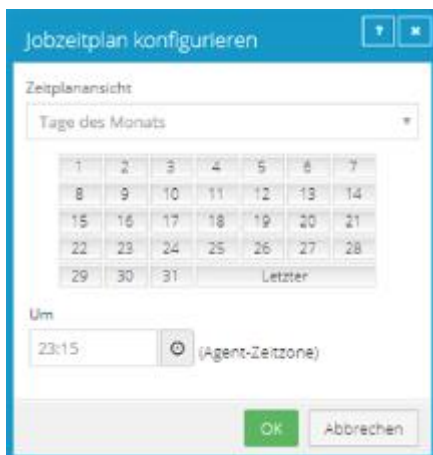
7. Gehen Sie im Dialogfeld „Jobzeitplan konfigurieren“ wie folgt vor:

- Um die Sicherung an bestimmten Wochentagen auszuführen, wählen Sie die Option **Tage der Woche** in der Liste **Zeitplanansicht** aus. Wählen Sie die Tage aus, an denen der Job ausgeführt werden soll. Geben Sie im Feld **Um** den Zeitpunkt an, an dem der Job ausgeführt werden soll.



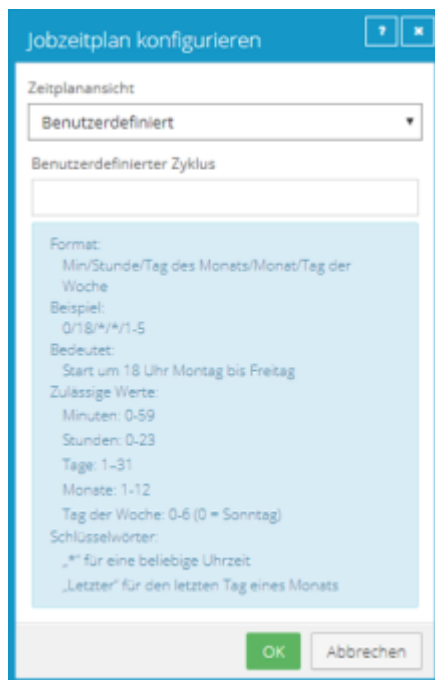
The screenshot shows the 'Jobzeitplan konfigurieren' dialog box. Under 'Zeitplanansicht', the 'Tage der Woche' dropdown is selected. Below it, a row of buttons for days of the week is shown: Mo, Di, Mi, Do, Fr, Sa, So. The 'Di', 'Mi', 'Do', and 'Sa' buttons have green checkmarks. The 'Um' field contains '22:15' and a clock icon with '(Agent-Zeitzone)' next to it. At the bottom are 'OK' and 'Abbrechen' buttons.

- Um die Sicherung an bestimmten Zeitpunkten im Monat auszuführen, wählen Sie die Option **Tage des Monats** in der Liste **Zeitplanansicht** aus. Wählen Sie im Kalender die Zeitpunkte aus, an denen der Job ausgeführt werden soll. Geben Sie im Feld **Um** den Zeitpunkt an, an dem der Job ausgeführt werden soll.



The screenshot shows the 'Jobzeitplan konfigurieren' dialog box. Under 'Zeitplanansicht', the 'Tage des Monats' dropdown is selected. Below it is a calendar grid with dates from 1 to 31, and 'Letzter' for the last day of the month. The 'Um' field contains '23:15' and a clock icon with '(Agent-Zeitzone)' next to it. At the bottom are 'OK' and 'Abbrechen' buttons.

- Um einen benutzerdefinierten Zeitplan zu erstellen, wählen Sie die Option **Benutzerdefiniert** in der Liste **Zeitplanansicht** aus. Geben Sie im Dialogfeld „Benutzerdefinierter Zyklus“ einen benutzerdefinierten Zeitplan ein. Befolgen Sie das beschriebene Format und die Notation.



8. Klicken Sie auf **OK**.

Der neue Zeitplan wird im Feld „Zeitplan“ angezeigt.

9. Klicken Sie in der Liste **Komprimierung** auf eine Komprimierungsstufe für die Sicherungsdaten. Komprimierungsstufen optimieren die Menge der gespeicherten Daten im Verhältnis zur Sicherungsgeschwindigkeit.
10. Führen Sie eine der folgenden Aktionen aus:
 - Wenn Sie möchten, dass der Sicherungsjob ohne Zeitlimit ausgeführt wird, klicken Sie auf **Keine** in der Liste **Zurückstellung**.
 - Um für die Ausführung des Sicherungsjobs eine maximale Zeitdauer festzulegen, klicken Sie auf **Minuten** oder **Stunden** in der Liste **Zurückstellung**. Geben Sie in das Feld daneben in Minuten oder Stunden ein, wie lange der Job maximal ausgeführt werden soll.

Hinweis: Wenn die Zurückstellung aktiviert ist, werden bei dem Sicherungsjob nach dem festgelegten Zeitraum keine neuen Daten mehr gesichert, auch wenn Daten vorhanden sind, die noch nicht gesichert wurden. Änderungen an zuvor gesicherten Daten werden unabhängig vom angegebenen Zeitraum gesichert.
11. Aktivieren Sie das Kontrollkästchen **Aktivieren** am Ende der Zeile, um den Job mit dem angegebenen Zeitplan auszuführen.
12. Wenn mehr als eine Zeitplanzeile existiert, können Sie mit den Pfeilen **Priorität** die Priorität der einzelnen Zeilen ändern. Zeitpläne, die weiter oben in der Liste stehen, haben eine höhere Priorität als weiter unten stehende Zeitpläne.

Wenn ein Job von mehreren Zeitplänen zur gleichen Zeit ausgeführt werden soll, wird der Job nur einmal zum geplanten Zeitpunkt ausgeführt. Wenn die Zeitpläne unterschiedliche Aufbewahrungstypen haben, wird der Aufbewahrungstyp des Zeitplans mit der höchsten Priorität in der Liste ausgeführt.

13. Überprüfen Sie die Anzahl der Wiederherstellungspunkte, die sich aus den Zeitplänen und Aufbewahrungsrichtlinien des Jobs ergeben könnten. Wenn Sie die Anzahl der Wiederherstellungspunkte erhöhen oder reduzieren möchten, ändern Sie die Zeitpläne oder Aufbewahrungstypen.
Die maximale Anzahl der Wiederherstellungspunkte wird unter den Zeitplänen im Dialogfeld „Zeitplan anzeigen/hinzufügen“ angezeigt. Weitere Informationen finden Sie unter *Maximale Anzahl von Wiederherstellungspunkten für einen Job* auf Seite 40.
14. Wenn der Bereich „Automatischer Neustart für zeitgesteuerte Sicherung“ unten im Dialogfeld „Zeitplan anzeigen/hinzufügen“ angezeigt wird, können Sie angeben, ob geplante Sicherungen nach fehlgeschlagenen Sicherungsversuchen wiederholt werden sollen. Siehe *Angeben, ob geplante Sicherungen nach einem Fehler wiederholt werden sollen* auf Seite 41.
15. Klicken Sie auf **Speichern**.

4.6 Maximale Anzahl von Wiederherstellungspunkten für einen Job

Ab Portal Version 8.88 wird beim Planen eines Sicherungsjobs im Dialogfeld „Zeitplan anzeigen/hinzufügen“ die maximale Anzahl von Wiederherstellungspunkten angezeigt, die sich aus den aktuellen Zeitplänen und Aufbewahrungstypen des Jobs ergeben können. Die maximale Anzahl von Wiederherstellungspunkten bzw. Sicherungen im Vault wird aktualisiert, wenn Sie eine Zeitplanzeile hinzufügen oder ändern, damit Sie die Auswirkungen Ihrer Zeitplanänderungen nachvollziehen und ggf. zusätzliche Änderungen vornehmen können.

Wenn Sie z. B. für eine Sicherung die tägliche Ausführung planen und den Standardaufbewahrungstyp „Monatlich“ auswählen (der angibt, dass jede Sicherung 365 Tage aufbewahrt wird), beträgt die maximale Anzahl von Wiederherstellungspunkten, die im Dialogfeld „Zeitplan anzeigen/hinzufügen“ angezeigt werden, 365. Wenn 365 Wiederherstellungspunkte zu viel Speicherplatz im Vault belegen würden, können Sie die Häufigkeit der Sicherungen reduzieren oder den Aufbewahrungstyp ändern. Sie können z. B. den Aufbewahrungstyp in den Standard-Aufbewahrungstyp „Täglich“ ändern, der angibt, dass jede Sicherung 30 Tage lang aufbewahrt wird.

Die maximale Anzahl von Wiederherstellungspunkten schließt Sicherungen ein, die auf Basis von Zeitplänen des Typs „Tagesintern“, „Tage der Woche“ und „Tage des Monats“ erstellt wurden. Die maximale Anzahl von Wiederherstellungspunkten enthält keine Wiederherstellungspunkte, die wie folgt erstellt wurden:

- Mit benutzerdefinierten Zeitplänen für den Job.
- Mit Aufbewahrungstypen, die nicht mehr verwendet werden. Wenn ein Zeitplan gelöscht oder die Aufbewahrung für einen Job geändert wurde, verbleiben möglicherweise weitere Sicherungen im Vault.

Wenn beispielsweise ein Job gemäß Zeitplan täglich mit dem standardmäßigen Aufbewahrungstyp „Täglich“ ausgeführt wurde, Sie diesen Zeitplan jedoch löschen und einen neuen Zeitplan mit einem anderen Aufbewahrungstyp erstellen, werden die Sicherungen aus dem ursprünglichen täglichen Zeitplan sowie die Sicherungen aus dem neuen Zeitplan im Vault gespeichert. Sicherungen aus dem ursprünglichen täglichen Zeitplan sind jedoch nicht in der maximalen Anzahl der Wiederherstellungspunkte enthalten, die im Dialogfeld „Zeitplan anzeigen/hinzufügen“ angezeigt werden.

4.7 Angeben, ob geplante Sicherungen nach einem Fehler wiederholt werden sollen

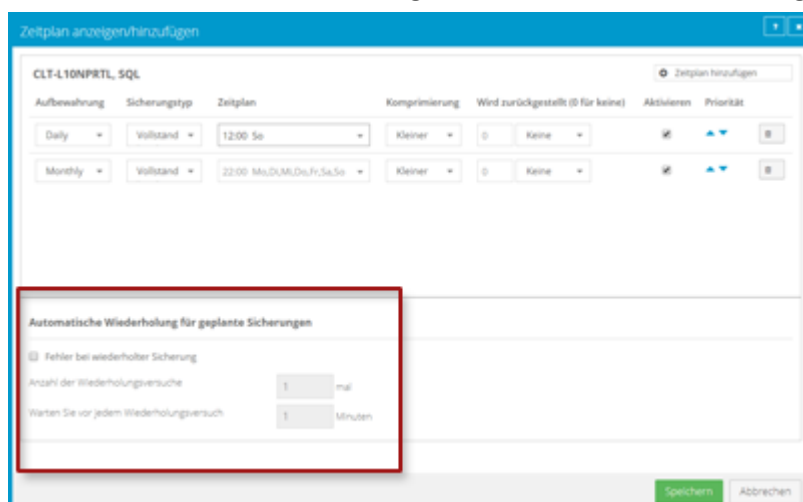
Sie können festlegen, ob geplante Sicherungen automatisch wiederholt werden sollen, wenn diese nicht erfolgreich ausgeführt werden können.

Sie können auch angeben, wie oft eine geplante Sicherung nach einem fehlgeschlagenen Versuch wiederholt werden soll, sowie die Zeitspanne zwischen den Wiederholungen.

Hinweis: Die Einstellungen für die automatische Wiederholung gelten nur für geplante Sicherungen. Eine Sicherung wird nach einer fehlgeschlagenen Ad-hoc-Sicherung nicht automatisch wiederholt.

So legen Sie fest, ob geplante Sicherungen nach einem Fehler wiederholt werden sollen:

- Führen Sie eine der folgenden Aktionen aus:
 - Klicken Sie in der Navigationsleiste auf **Computer**. Suchen Sie den VRA, für den Sie die Einstellungen für die automatische Wiederholung festlegen möchten, und klicken Sie auf die Zeile, um die entsprechende Ansicht zu erweitern. Klicken Sie auf der Registerkarte **Jobs** im Menü **Aktion auswählen** für den betreffenden Job auf **Zeitplan anzeigen/hinzufügen**.
 - Erstellen Sie einen neuen Sicherungsjob. Das Dialogfeld „Zeitplan anzeigen/hinzufügen“ wird angezeigt, wenn Sie den Job speichern.
- Führen Sie im Abschnitt „Automatische Wiederholung für geplante Sicherungen“ eine der folgenden Aktionen aus:
 - Wenn geplante Sicherungen nach einem fehlgeschlagenen Versuch nicht wiederholt werden sollen, deaktivieren Sie das Kontrollkästchen **Fehlgeschlagenen Job wiederholen**.
 - Wenn geplante Sicherungen nach einem fehlgeschlagenen Versuch wiederholt werden sollen, aktivieren Sie das Kontrollkästchen **Fehlgeschlagenen Job wiederholen**. Geben Sie im Feld **Anzahl der Wiederholungsversuche** ein, wie oft die Sicherung wiederholt werden soll. Geben Sie im Feld **Wartezeit vor jedem Wiederholungsversuch für [] Minuten** die Anzahl der Minuten ein, die der Agent vor dem nächsten Sicherungsversuch warten soll.



- Klicken Sie auf **Speichern**.

4.8 Ausführen einer Ad-hoc-Sicherung

Nach dem Erstellen eines Sicherungsjobs können Sie die Sicherung jederzeit ausführen, auch wenn für die Ausführung des Jobs ein bestimmter Zeitplan festgelegt wurde.

So führen Sie eine Ad-hoc-Sicherung aus:

1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die verfügbaren Computer werden in einem Raster aufgelistet.
2. Suchen Sie den VRA mit dem Sicherungsjob, den Sie ausführen möchten, und erweitern Sie durch Klicken auf die Computerzeile die Ansicht.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Suchen Sie den Job, den Sie ausführen möchten. Klicken Sie dann im Menü **Aktion auswählen** des Jobs auf **Job ausführen**.

Im Dialogfeld „Job ausführen“ werden die Standardeinstellungen für die Sicherung angezeigt.

Hinweis: An dieser Stelle können Sie auf **Sicherung starten** klicken, um den Job sofort zu starten. Bei Bedarf können Sie die Sicherungsoptionen vor der Ausführung des Jobs ändern.

5. Um die Daten auf dem Vault zu sichern, der für den Job festgelegt wurde, dürfen Sie das **Ziel** nicht ändern.

Um die Daten als SSI-Dateien (Sicherungssatz-Image-Dateien) auf einem Datenträger zu sichern, wählen Sie in der Liste **Ziel** die Option **Verzeichnis auf Datenträger**. Klicken Sie auf die Schaltfläche **Durchsuchen**. Wählen Sie im Dialogfeld „Ordner auswählen“ den Speicherort zum Speichern der SSI-Dateien und klicken Sie auf **OK**.

SSI-Dateien sind vollständige Sicherungen, die – statt auf einem Vault – auf einem Datenträger gespeichert werden. Wenn Sie die Sicherungsdateien auf physischen Medien speichern und sie dann zum Importieren auf einen Remote-Vault übertragen können Sie mehr Zeit sparen, als wenn Sie die Daten direkt auf einem Vault in einem externen Rechenzentrum sichern.

Hinweis: Sicherungen in SSI-Dateien auf einem Datenträger können nicht zurückgestellt werden.

6. Klicken Sie in der Liste **Aufbewahrungsschema** auf einen Aufbewahrungstyp.
Der Aufbewahrungstyp legt die Anzahl der Tage fest, die eine Sicherung im Vault bleibt, wie viele Kopien von einer Sicherung online gespeichert werden und wie lange Sicherungsdaten offline gespeichert werden.
7. Führen Sie eine der folgenden Aktionen aus:
 - Wenn Sie möchten, dass der Sicherungsjob ohne Zeitlimit ausgeführt wird, deaktivieren Sie das Kontrollkästchen **Zurückstellung verwenden**.
 - Um für die Ausführung des Sicherungsjobs eine maximale Zeitdauer festzulegen, markieren Sie das Kontrollkästchen **Zurückstellung verwenden**. Wählen Sie in der Liste **Zeitfenster für die Sicherung** die Option **Minuten** oder **Stunden** aus. Geben Sie in das Feld daneben in Minuten oder Stunden ein, wie lange der Job maximal ausgeführt werden soll.

Hinweis: Wenn die Zurückstellung aktiviert ist, werden bei dem Sicherungsjob nach dem festgelegten Zeitraum keine neuen Daten mehr gesichert, auch wenn Daten vorhanden

sind, die noch nicht gesichert wurden. Änderungen an den Daten, die zuvor gesichert wurden, werden unabhängig vom Sicherungszeitfenster gesichert.

8. Klicken Sie auf **Sicherung starten**.

Das Dialogfeld „Prozessdetails“ zeigt den Sicherungsfortschritt und gibt an, wann die Sicherung abgeschlossen ist. Es können weitere kürzlich abgeschlossene Jobprozesse im Dialogfeld angezeigt werden. Siehe *Anzeigen von aktuellen Prozessinformationen eines Jobs* auf Seite 77.

9. Wenn Sie den Sicherungsvorgang unterbrechen möchten, klicken Sie auf **Stoppen**.
10. Um das Dialogfeld „Prozessdetails“ zu schließen, klicken Sie auf **Schließen**.

4.9 Synchronisieren eines Jobs

Wenn ein Sicherungsjob synchronisiert wird, prüft der Agent, welche Sicherungssätze für den Job online sind und für die Wiederherstellung verfügbar sind.

Ein Job wird automatisch synchronisiert, wenn Sie die Daten des Jobs wiederherstellen. Sie können einen Job jederzeit auch manuell synchronisieren. Die manuelle Synchronisierung ist in den folgenden Fällen zu empfehlen bzw. erforderlich:

- Vor dem Ausführen von Sicherungsjobs auf neu registrierten Computern. Außerdem müssen Sie die Verschlüsselungskennwörter für vorhandene Sicherungsjobs auf dem Computer eingeben.
- Vor dem Wiederherstellen von Daten von Jobs, die auf einem Satelliten-Vault gesichert und in der Cloud oder einem anderen Vault repliziert werden
- Zum Neuerstellen einer DTA-Datei (Deltadatei) für einen Job. Wenn eine Fehlermeldung in einer Protokolldatei anzeigt, dass die Deltazuordnungsdatei beschädigt ist, löschen Sie die DTA-Datei (Deltadatei) aus dem Jobordner auf dem geschützten Computer. Synchronisieren Sie dann den Job, um die Deltadatei neu zu erstellen.

So synchronisieren Sie einen Job:

1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den VRA mit dem Job, den Sie synchronisieren möchten. Klicken Sie auf seine Zeile, um seine Ansicht zu erweitern.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Suchen Sie den Job, den Sie synchronisieren möchten. Klicken Sie dann im Menü **Aktion auswählen** des Jobs auf **Synchronisieren**.

Das Dialogfeld „Prozessdetails“ zeigt den Sicherungsfortschritt und gibt an, wann die Sicherung abgeschlossen ist. Es können weitere kürzlich abgeschlossene Jobprozesse im Dialogfeld angezeigt werden. Siehe *Anzeigen von aktuellen Prozessinformationen eines Jobs* auf Seite 77.

5. Wenn Sie den Sicherungsvorgang unterbrechen möchten, klicken Sie auf **Stoppen**.
Um das Dialogfeld „Prozessdetails“ zu schließen, klicken Sie auf **Schließen**.

5 Beheben von Zertifikatfehlern und möglichen Bedrohungen

5.1 Beheben von Zertifikatfehlern

Wenn ein Agent einen Zertifikatfehler meldet, müssen Sie den Fehler beheben, bevor Sicherungen und Wiederherstellungen fortgesetzt werden können. Zertifikatfehler werden unter „Aktuelle Momentaufnahme“ im Dashboard zusammengefasst und auf der Seite „Computer“ in Portal angezeigt. Siehe *Überwachen von Sicherungen und Computern mit der aktuellen Momentaufnahme* auf Seite 73 und *Anzeigen von Informationen zu Computer- und Jobstatus* auf Seite 74. Agenten können Zertifikatfehler melden, wenn sie das Anheften von Zertifikaten unterstützen, eine Sicherheitsfunktion, die sicherstellen soll, dass Agenten sich mit legitimen Vaults und Umgebungen verbinden.

Wenn ein Zertifikatfehler gemeldet wird, wenden Sie sich an das IT-Sicherheitspersonal oder einen Dienstleister, um festzustellen, ob die Zertifikatänderung erwartet wurde oder ob weitere Untersuchungen erforderlich sind.

Wenn die Zertifikatänderung erwartet wurde, führen Sie die folgenden Schritte aus, um das Zertifikat erneut anzuhängen. Wenn Sie ein Zertifikat neu anheften, zeichnet der Agent den neuen öffentlichen Schlüssel des Zertifikats sicher auf. Das gleiche Verfahren wird verwendet, um die Zertifikate des Vaults und der vSphere-Umgebung neu anzuhängen, so dass Sicherungen und Wiederherstellungen fortgesetzt werden können.

So beheben Sie Zertifikatfehler:

1. Klicken Sie in der Navigationsleiste auf **Computer**. Die Seite „Computer“ zeigt registrierte Computer an.
2. Aktivieren Sie das Kontrollkästchen für jeden Computer mit einem Zertifikatfehler, den Sie beheben möchten.

Hinweis: Wählen Sie nur Computer aus, für die der Status „Zertifikatfehler“ angezeigt wird, da ansonsten die Aktion „Zertifikat erneut anheften“ nicht verfügbar ist.

3. Klicken Sie in der Liste **Aktionen** auf **Zertifikat neu anheften**.
4. Klicken Sie im Bestätigungsdialoefeld auf **Ja**.
5. Klicken Sie im Fenster mit der Erfolgsmeldung auf **OK**.

5.2 Handhaben möglicher Ransomware-Bedrohungen

Wenn ein Agent eine mögliche Ransomware-Bedrohung erkennt, wird der Job in Portal gekennzeichnet. Mögliche Bedrohungen werden gekennzeichnet:

- In der aktuellen Momentaufnahme im Dashboard. Siehe *Überwachen von Sicherungen und Computern mit der aktuellen Momentaufnahme* auf Seite 73.
- Auf den Seiten „Computer“ und „Überwachung“. Siehe *Anzeigen von Informationen zu Computer- und Jobstatus* auf Seite 74 und *Anzeigen und Exportieren neuer Sicherungsstatus* auf Seite 91.

- In den täglichen Statusberichten. Siehe *Statusbericht für Sicherung* auf Seite 86 und *Zeitliche Planung des täglichen Statusberichts* auf Seite 85.
- In E-Mail-Benachrichtigungen an Administratoren, wenn E-Mail-Benachrichtigungen zentral in einer Portal-Instanz konfiguriert sind. Siehe *Einrichten von E-Mail-Benachrichtigungen für mögliche Ransomware-Bedrohungen* auf Seite 83 .
- Wenn Sie Daten wiederherstellen oder bestimmte Sicherungen aus einem vSphere-Sicherungsjob löschen. Siehe *Wiederherstellen von vSphere-Daten* auf Seite 47 und *Löschen von spezifischen Sicherungen aus Vaults* auf Seite 71.

Wenn eine VM eine mögliche Bedrohung aufweist, scannt der VRA die VM während der Sicherungen erst wieder, wenn die Warnung vor einer möglichen Bedrohung für den Job gelöscht wurde. Wenn eine VM eine mögliche Bedrohung aufweist, aber während der nächsten Sicherung nicht in der vSphere-Umgebung vorhanden ist, wird die Sicherung weiterhin als mögliche Bedrohung gekennzeichnet, bis ein Administrator die Warnung vor einer möglichen Bedrohung löscht.

Wenn eine mögliche Bedrohung auf einem Windows erkannt wird, können Sie sich bei dem in Ihrer Umgebung anmelden und untersuchen, ob er/sie mit Ransomware infiziert ist. Ein Administrator im Portal kann dann die Bedrohung handhaben:

- Wenn der nicht infiziert ist oder die Ransomware-Bedrohung beseitigt wurde, kann ein Administrator die Warnung vor der möglichen Bedrohung vom Job löschen.
- Wenn der mit Ransomware infiziert ist, kann ein Administrator eine vor dem Angriff erstellte Sicherung (auch als Sicherungssatz bezeichnet) wiederherstellen. Sicherungen mit möglichen Bedrohungen werden im Dialogfeld „Wiederherstellen“ gekennzeichnet, so dass Sie eine Sicherung ohne mögliche Bedrohung auswählen können. Nach der Wiederherstellung verbleiben Sicherungen mit möglichen Ransomware-Bedrohungen im Vault und stehen zur Wiederherstellung zur Verfügung. Um diese Sicherungen (Sicherungssätze) zu entfernen, löschen Sie sie aus dem Vault und synchronisieren Sie den Job. Siehe *Löschen von spezifischen Sicherungen aus Vaults* auf Seite 71 und *Synchronisieren eines Jobs* auf Seite 43. Ein Administrator kann dann das Kennzeichen für die mögliche Bedrohung aus dem Job löschen.

So handhaben Sie eine mögliche Ransomware-Bedrohung:

1. Klicken Sie nach erfolgter Anmeldung als Administrator in der Navigationsleiste auf **Computer**. Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den Computer oder die Umgebung mit der möglichen Bedrohung und erweitern Sie durch Klicken auf deren Zeile die Ansicht.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Suchen Sie den Job mit der möglichen Bedrohung und klicken Sie im Menü **Aktion auswählen** auf **Mögliche Bedrohung handhaben**.

Hinweis: Die Option „Mögliche Bedrohung handhaben“ wird für einen Job, der von einem anderen Computer wiederhergestellt wird, nicht angezeigt. Um eine mögliche Bedrohung für einen Job handzuhaben, müssen Sie den Job auf dem ursprünglichen Computer, falls vorhanden, suchen oder registrieren Sie einen neuen Computer im Vault als ursprünglichen Computer.

5. Führen Sie eine der folgenden Aktionen im Feld „Mögliche Bedrohung handhaben“ durch:

- *Hinweis:* Nach einer Wiederherstellung verbleiben Sicherungen mit möglichen Ransomware-Bedrohungen im Vault und stehen zur Wiederherstellung zur Verfügung. Um diese Sicherungen zu entfernen, löschen Sie sie aus dem Vault und synchronisieren Sie den Job. Siehe *Löschen von spezifischen Sicherungen aus Vaults* auf Seite [71](#) und *Synchronisieren eines Jobs* auf Seite [43](#). Ein Administrator kann das Kennzeichen für die mögliche Bedrohung aus dem Job löschen.
- Wenn Sie die mögliche Bedrohung untersucht oder beseitigt haben und sicher sind, dass der nicht von Ransomware betroffen ist, wählen Sie **Warnung vor potenzieller Bedrohung löschen** und klicken Sie dann auf **Fortfahren**. Klicken Sie im Warndialogfeld auf **Fortfahren**, um die mögliche Bedrohung vom Job und allen seinen Sicherungen (Sicherungssätzen) zu entfernen.

Hinweis: Wenn Sie mögliche Bedrohungswarnungen löschen, werden alle vorhandenen Bedrohungswarnungen aus dem Job und seinen Sicherungen (Sicherungssätzen) entfernt. Die Warninformationen sind jedoch weiterhin in den Protokolldateien verfügbar.

6 Wiederherstellen von vSphere-Daten

Wenn VMs in einer vSphere-Umgebung geschützt sind, können Sie:

- *Wiederherstellen von vSphere-VMs* auf Seite [47](#)
- *vSphere VM innerhalb von Minuten wiederherstellen mit Rapid VM Restore* auf Seite [50](#)
- *Wiederherstellen von Dateien, Ordnern und Datenbankelementen mit einem vSphere Recovery Agent* auf Seite [56](#)

6.1 Wiederherstellen von vSphere-VMs

Bevor Sie eine vSphere-VM wiederherstellen, prüft der vSphere Recovery Agent (VRA), ob ausreichend Speicherplatz verfügbar ist. Steht nicht genügend Speicherplatz zur Verfügung, schlägt die Wiederherstellung fehl und es wird eine Meldung in der Protokolldatei angezeigt.

Wenn Sie eine VM oder eine Vorlage in einer vSphere-Umgebung wiederherstellen und die ursprüngliche VM vorhanden ist, wird die VM als Kopie des Originals mit folgendem Namen wiederhergestellt: `<VMname>-vra-restored-<Date>`. Dieser Name wird für die Kopie sowohl in der vCenter-Umgebung als auch auf dem Datenspeicher angezeigt. Die virtuelle Maschine wird unabhängig vom Betriebszustand des ursprünglichen Rechners als Kopie wiederhergestellt; dieser kann aktiviert, deaktiviert oder angehalten sein. Der ursprüngliche VM-Name wird nicht geändert und seine Daten werden nicht überschrieben. Ab VRA 8.87 wird der wiederhergestellten VM eine neue MAC-Adresse zugewiesen. Ein IP-Adressenkonflikt tritt nicht auf, wenn die ursprüngliche und neu wiederhergestellte VM eingeschaltet werden.

Nach der Wiederherstellung einer VM aus einer absturzconsistenten Sicherung führt die VM beim ersten Start evtl. eine Festplattenprüfung durch.

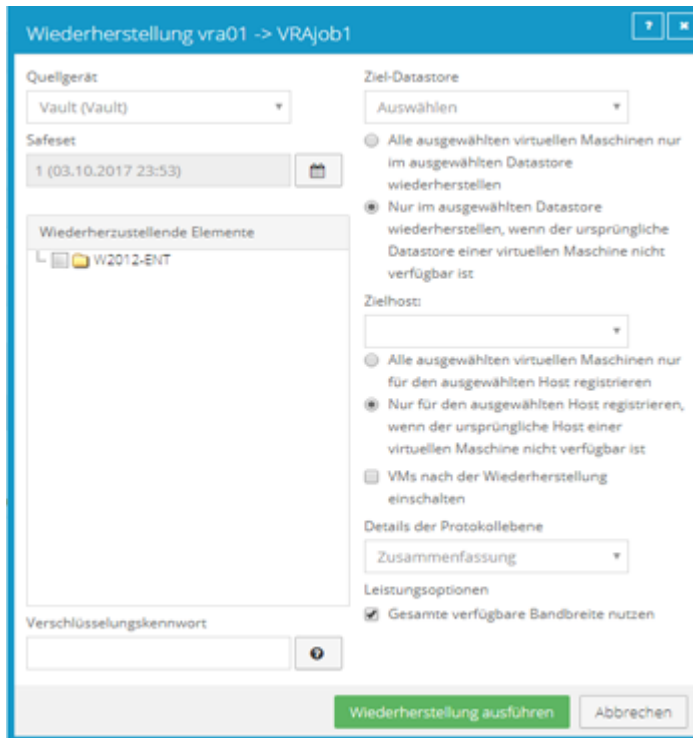
So stellen Sie vSphere-VMs wieder her:

1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die verfügbaren Computer werden in einem Raster aufgelistet.
2. Suchen Sie die vSphere-Umgebung mit der VM, die Sie wiederherstellen möchten, und erweitern Sie durch Klicken auf die Zeile ihre Ansicht.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Suchen Sie den Sicherungsjob für die VM, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellung** im Menü **Aktion auswählen** des Jobs.
5. Wählen Sie im Dialogfeld „Wiederherzustellende Elemente auswählen“ die Option **Virtuelle Maschinen**.





6. Klicken Sie auf **Weiter**.

Das Dialogfeld „Wiederherstellung“ wird angezeigt. Wenn im Job keine mögliche Ransomware-Bedrohung erkannt wurde, wird im Feld „Sicherungssatz“ der letzte Sicherungssatz für den Job angezeigt.



Wenn bei der Ausführung des Jobs eine mögliche Ransomware-Bedrohung erkannt wurde, wird ein Kalender mit einer Liste von Sicherungssätzen angezeigt. „Mögliche Bedrohung“ wird neben jedem Vault angezeigt, bei dem eine mögliche Ransomware-Bedrohung erkannt wurde.

Hinweis: Wenn Sie Daten wie in *Wiederherstellen von Daten auf einem Ersatzcomputer* auf Seite 59 oder *Wiederherstellen von Daten von einem anderen Computer* auf Seite 60 beschrieben wiederherstellen, wird für keinen Sicherungssatz „Mögliche Bedrohung“ angezeigt, selbst wenn eine mögliche Bedrohung während einer Sicherung in der ursprünglichen vSphere-Umgebung erkannt wurde.

7. Gehen Sie wie folgt vor, um Daten aus einem älteren Sicherungssatz oder von SSI-Dateien (Sicherungssatz-Image) auf dem Datenträger wiederherzustellen:
 - Um die Daten eines älteren Sicherungssatzes wiederherzustellen, klicken Sie auf die Schaltfläche **Sicherungssätze durchsuchen**, falls nicht bereits ein Kalender mit einer Liste von Sicherungen angezeigt wird.  Klicken Sie im Kalender auf das Datum des Sicherungssatzes, von dem Sie die Wiederherstellung durchführen möchten. Klicken Sie rechts neben dem Kalender auf den spezifischen Sicherungssatz, aus dem Sie wiederherstellen möchten.
 - Um Daten von SSI-Dateien (Sicherungssatz-Image) auf einem Datenträger wiederherzustellen, wählen Sie in der Liste **Quellgerät** die Option **Verzeichnis auf Datenträger** aus. Klicken Sie auf die Ordnerschaltfläche.  Wählen Sie im Dialogfeld


„Ordner auswählen“ das Verzeichnis aus, in dem sich die Dateien befinden, und klicken Sie auf **OK**.

SSI-Dateien sind vollständige Sicherungen, die aus dem Vault exportiert oder – anstatt auf einem Vault – auf einem Datenträger gesichert wurden. Sie können u. U. Zeit sparen, indem Sie Sicherungsdateien auf physischen Medien speichern und sie dann zur Wiederherstellung an einen anderen Speicherort übertragen, anstatt die Daten aus einem Vault in einem externen Rechenzentrum wiederherzustellen.

Hinweis: Wenn SSI-Dateien mittels einer Sicherung in einem Verzeichnis auf einem Datenträger erstellt wurden, können Sie eine Wiederherstellung von den SSI-Dateien erst durchführen, nachdem diese in den Vault importiert und der Agent mit dem Vault synchronisiert wurden.

8. Aktivieren Sie im Feld **Wiederherzustellende Elemente** das Kontrollkästchen für die einzelnen VM, die Sie wiederherstellen möchten.

Wenn eine VM eine mögliche Ransomware-Bedrohung aufweist, wird „Mögliche Bedrohung“ neben dem Namen der VM angezeigt.

9. Geben Sie im Feld **Verschlüsselungskennwort** das Verschlüsselungskennwort für die Daten ein. Um den Kennworthinweis anzuzeigen, klicken Sie auf die Schaltfläche **Hinweis**. 
10. Klicken Sie in der Liste **Zieldatenspeicher** auf den Datenspeicher für die wiederhergestellten VMs.
11. Wählen Sie eine der folgenden Optionen für die Wiederherstellung von VMs in den ausgewählten Datenspeicher:
 - **Alle ausgewählten virtuellen Maschinen nur im ausgewählten Datastore wiederherstellen**
 - **Nur im ausgewählten Datenspeicher wiederherstellen, wenn der ursprüngliche Datenspeicher eines virtuellen Rechners nicht verfügbar ist.** Wenn die wiederhergestellte virtuelle Maschine mehrere virtuelle Datenträger in mindestens zwei Datenspeichern enthält und mindestens einer der Datenspeicher nicht verfügbar ist, wird die gesamte virtuelle Maschine im ausgewählten Datenspeicher wiederhergestellt.
12. Wählen Sie in der Liste **Zielhost** den Host aus, bei dem Sie die virtuellen Maschinen registrieren möchten.

In der Liste werden nur Hosts angezeigt, die Zugriff auf den gewählten Datenspeicher haben. Wenn nur ein ESXi-Host verfügbar ist, wird dieser bei der Auswahl eines Datenspeichers als Zielhost angegeben.
13. Wenn VRA einen vCenter Server schützt, wählen Sie zum Registrieren der virtuellen Maschinen beim ausgewählten Host eine der folgenden Optionen aus:
 - **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.**

Hinweis: Wenn VRA einen einzelnen ESXi-Host schützt, der nicht von vCenter Server verwaltet wird, werden die Registrierungsoptionen nicht im Dialogfeld „Wiederherstellung“ angezeigt.

14. Um die VMs nach dem Wiederherstellen zu aktivieren, wählen Sie **VMs nach der Wiederherstellung einschalten**.
15. Klicken Sie in der Liste **Details der Protokollebene** auf die Detailebene für die Protokollierung. Siehe *Erweiterte Wiederherstellungsoptionen* auf Seite [61](#).
16. Um die gesamte verfügbare Bandbreite für die Wiederherstellung zu nutzen, wählen Sie **Gesamte verfügbare Bandbreite nutzen** aus.
Um die Leistung für Ihre Wiederherstellung zu optimieren, empfehlen wir, die Option **Gesamte verfügbare Bandbreite nutzen** zu aktivieren.
17. Klicken Sie auf **Wiederherstellung ausführen**.

6.2 vSphere VM innerhalb von Minuten wiederherstellen mit Rapid VM Restore

Mit Rapid VM Restore können Sie eine virtuelle Maschine (VM) innerhalb von Minuten auf einem vCenter oder ESXi-Host wiederherstellen.

In einem vCenter können Sie eine VM mithilfe von Rapid VM Restore wiederherstellen und dann in einen zweiten Datenspeicher migrieren, um sie dauerhaft wiederherzustellen. Dies kann bei einer Notfallwiederherstellung nützlich sein, wenn kritische Server schnellstmöglich wiederhergestellt und für Benutzer und Anwendungen bereitgestellt werden müssen. Sie können eine VM auch vorübergehend wiederherstellen, um schnell zu überprüfen, ob die VM-Sicherung wiederhergestellt werden kann.

Auf einem ESXi-Host, der nicht von vCenter Server verwaltet wird, können Sie eine VM vorübergehend mit Rapid VM Restore wiederherstellen. Das vorübergehende Wiederherstellen einer VM kann als Test nützlich sein, um schnell zu überprüfen, ob eine VM-Sicherung wiederhergestellt werden kann.

Wenn Sie eine vSphere-VM erstmals mit Rapid VM Restore wiederherstellen, werden die Datenträger aus der ausgewählten VM-Sicherung zunächst als Speichergeräte (virtuelle RDMS) auf einer VM bereitgestellt, damit sofort darauf zugegriffen werden kann. Während die VM ausgeführt wird, werden Änderungen in einen temporären Datenspeicher geschrieben. In dieser Phase benötigt die VM einen aktiven Rapid VM Restore-Prozess, muss mit dem VRA und dem Vault verbunden sein und kann nur vorübergehend eingesetzt werden. Je länger eine VM mit Rapid VM Restore ausgeführt wird, desto schlechter wird die Leistung und desto mehr Vault- und VRA-Ressourcen werden verwendet.

Nach der Migration einer wiederhergestellten VM in permanenten Speicher in einem vCenter benötigt die VM keinen aktiven Rapid VM Restore-Prozess mehr und ist unabhängig von VRA und Vault. Wir empfehlen, eine VM so bald wie möglich nach der Wiederherstellung mit Rapid VM Restore in permanenten Speicher zu migrieren. Siehe *Migrieren einer mit Rapid VM Restore wiederhergestellten vSphere VM in den permanenten Speicher* auf Seite [53](#). Wenn die Netzwerkverbindung zum VRA, Vault oder ESXi-Host unterbrochen wird, bevor eine VM in den permanenten Speicher migriert wird, können VM-Daten verloren gehen.

WICHTIG: Wenn der VRA einen einzelnen ESXi-Host schützt, der nicht von vCenter Server verwaltet wird, ist das dauerhafte Wiederherstellen einer VM mit Rapid VM Restore nicht möglich. Ein ESXi-

Server, der nicht Teil eines vCenters ist, verfügt nicht über die erforderlichen Funktionen, um VMs in permanenten Speicher zu migrieren.

Hinweise:

- Bevor eine VM mit Rapid VM Restore wiederhergestellt wird, überprüft der VRA, ob ausreichend Speicherplatz verfügbar ist. Steht nicht genügend Speicherplatz zur Verfügung, schlägt die Wiederherstellung fehl und es wird eine Meldung in der Protokolldatei angezeigt.
- Wenn Sie eine Vorlage mit Rapid VM Restore wiederherstellen, wird sie als aktive virtuelle Maschine wiederhergestellt, und nicht als Vorlage.
- Nach der Wiederherstellung einer VM aus einer absturzkonsistenten Sicherung führt die VM beim ersten Start evtl. eine Festplattenprüfung durch.
- Sie sollten die mit Rapid VM Restore wiederhergestellten virtuellen Maschinen (VMs) unbedingt sichern. Siehe *Best Practice: Sichern von vSphere VMs, die mit Rapid VM Restore wiederhergestellt wurden* auf Seite 55.
- Rapid VM Restore ist mit vSphere Recovery Agent (VRA) Version 8.80 oder höher verfügbar. Eine komplette Liste der Anforderungen finden Sie unter *Anforderungen für vSphere Rapid VM Restore und Sicherheitsüberprüfung* auf Seite 8.

So stellen Sie eine vSphere-VM innerhalb von Minuten mit Rapid VM Restore wieder her:

1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die verfügbaren Computer werden in einem Raster aufgelistet.
2. Suchen Sie die vSphere-Umgebung mit der VM, die Sie wiederherstellen möchten, und erweitern Sie durch Klicken auf die Zeile ihre Ansicht.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Suchen Sie den Sicherungsjob für die VM, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellung** im Menü **Aktion auswählen** des Jobs.
5. Wählen Sie im Dialogfeld „Wiederherzustellende Elemente auswählen“ die Option **Virtuelle Maschine mit Rapid VM Restore** aus.



Wenn die Option **Virtueller Computer mit Rapid VM Restore** nicht angezeigt wird, dann ist diese Wiederherstellungsmethode nicht verfügbar. Dies ist der Fall, wenn Sie eine ältere VRA-Version als 8.80 verwenden, wenn die Sicherungen nicht in einem lokalen Vault verfügbar sind, der Rapid VM Restores unterstützt, oder wenn andere Anforderungen nicht erfüllt sind. Eine komplette Liste der Anforderungen finden Sie unter *Anforderungen für vSphere Rapid VM Restore und Sicherheitsüberprüfung* auf Seite 8.

6. Klicken Sie auf **Weiter**.

Das Dialogfeld „Wiederherstellung“ wird angezeigt. Wenn im Job keine mögliche Ransomware-Bedrohung erkannt wurde, wird im Feld „Sicherungssatz“ der letzte Sicherungssatz für den Job angezeigt.

Wenn bei der Ausführung des Jobs eine mögliche Ransomware-Bedrohung erkannt wurde, wird ein Kalender mit einer Liste von Sicherungssätzen angezeigt. „Mögliche Bedrohung“ wird neben jedem Vault angezeigt, bei dem eine mögliche Ransomware-Bedrohung erkannt wurde.

Hinweis: Wenn Sie Daten wie in *Wiederherstellen von Daten auf einem Ersatzcomputer* auf Seite 59 oder *Wiederherstellen von Daten von einem anderen Computer* auf Seite 60 beschrieben wiederherstellen, wird für keinen Sicherungssatz „Mögliche Bedrohung“ angezeigt, selbst wenn eine mögliche Bedrohung während einer Sicherung in der ursprünglichen vSphere-Umgebung erkannt wurde.

7. Um die Daten eines älteren Sicherungssatzes wiederherzustellen, klicken Sie auf die Schaltfläche **Sicherungssätze durchsuchen**, falls nicht bereits ein Kalender mit einer Liste von Sicherungen angezeigt wird.  Klicken Sie im Kalender auf das Datum des Sicherungssatzes, von dem Sie die Wiederherstellung durchführen möchten. Klicken Sie rechts neben dem Kalender auf den spezifischen Sicherungssatz, aus dem Sie wiederherstellen möchten.
8. Wählen Sie in der Liste **Wiederherzustellende VM** die VM aus, die wiederhergestellt werden soll.
Wenn eine mögliche Ransomware-Bedrohung auf einer VM erkannt wurde, wird „Mögliche Bedrohung“ neben dem Namen der VM angezeigt.
9. Geben Sie im Feld **Verschlüsselungskennwort** das Verschlüsselungskennwort für die Daten ein. Um den Kennworthinweis anzuzeigen, klicken Sie auf die Schaltfläche  **Hinweis**.
10. Wählen Sie unter **Detailebene des Protokolls** die Detailebene für die Protokollierung aus. Weitere Informationen finden Sie unter *Protokolldateioptionen* auf Seite 35.
11. Führen Sie im Feld „Wiederherstellungseinstellungen“ die folgenden Schritte aus:

- Geben Sie im Feld **Name der wiederhergestellten VM** einen Namen für die wiederhergestellte VM an.
Wenn der eingegebene VM-Name in der vSphere-Umgebung bereits existiert (z. B. die VM, die gesichert wurde), erhält die wiederhergestellte VM den folgenden Namen: *VMname-rvmr-yyyy-Mon-dd--hh-mm-ss*, dabei ist *yyyy-Mon-dd--hh-mm-ss* der Zeitpunkt, an dem die VM wiederhergestellt wurde (z. B. VM-rvmr-2019-Nov-27--06-14-09).
- Wählen Sie in der Liste **Datenspeicher** einen Datenspeicher aus, in den die Änderungen geschrieben werden sollen, während die VM mit Rapid VM Restore wiederhergestellt wird (während die Laufwerke aus der ausgewählten Sicherung als Speichergeräte eingebunden sind).
Falls der VRA ein vCenter schützt und Sie die VM später in permanenten Speicher migrieren möchten, wählen Sie nicht den Datenspeicher aus, den Sie als permanenten Speicher verwenden möchten.
- Wählen Sie in der Liste **Zielhost** einen Host aus, auf dem die wiederhergestellte VM ausgeführt werden soll.
Wenn nur ein ESXi-Host verfügbar ist, wird dieser bei der Auswahl eines Datenspeichers als Zielhost angegeben.
Falls der VRA ein vCenter schützt und Sie die VM später in permanenten Speicher migrieren möchten, wählen Sie einen Host aus, der auf den permanenten Datenspeicher zugreifen kann.
- Führen Sie eine der folgenden Aktionen aus:

- Um die VM im eingeschalteten Zustand wiederherzustellen, wählen Sie die Option **VM einschalten** aus.
- Um die VM im ausgeschalteten Zustand wiederherzustellen, deaktivieren Sie die Option **VM einschalten**.

Sie können die VM beispielsweise im ausgeschalteten Zustand wiederherstellen, um die VM-Einstellungen vor dem Einschalten überprüfen oder ändern zu können.

- Führen Sie eine der folgenden Aktionen aus:
 - Um die VM mit dem Netzwerk zu verbinden, wählen Sie **Mit Netzwerk verbinden** aus.
 - Um die VM ohne Netzwerkkonnektivität wiederherzustellen, deaktivieren Sie die Option **Mit Netzwerk verbinden**.


Die Wiederherstellung ohne Netzwerkverbindung kann beispielsweise erforderlich sein, wenn Sie die VM in einem vCenter wiederherstellen, das nicht mit dem ursprünglichen Netzwerk verbunden ist. Auf diese Weise können Sie die VM-Einstellungen überprüfen, bevor Sie die VM mit dem Netzwerk verbinden.

12. Klicken Sie auf **Wiederherstellung ausführen**.

Das Dialogfeld „Prozessdetails“ wird angezeigt. Nach Abschluss der Wiederherstellung wird die folgende Statusmeldung angezeigt: *Rapid VM Restore wird ausgeführt*.

Die wiederhergestellte VM wird in der vSphere-Umgebung angezeigt. Die VM ist jetzt einsatzbereit.

13. Führen Sie eine oder mehrere der folgenden Aktionen aus:

- Um das Dialogfeld „Prozessdetails“ zu schließen, klicken Sie auf **Schließen**. Wenn Sie das Dialogfeld „Prozessdetails“ schließen, ohne Rapid VM Restore abzubrechen, wird die VM nicht aus der vSphere-Umgebung entfernt.
- Um das Dialogfeld „Prozessdetails“ erneut zu öffnen, suchen Sie den VRA-Sicherungsjob der VM auf der Seite „Computer“ oder „Überwachung“. Klicken Sie auf das Rapid VM Restore-Symbol, das neben dem VRA-Jobnamen angezeigt wird: 
- Informationen zum dauerhaften Wiederherstellen der VM durch Migration in permanenten Speicher finden Sie unter *Migrieren einer mit Rapid VM Restore wiederhergestellten vSphere VM in den permanenten Speicher* auf Seite 53.
WICHTIG: Das Migrieren der VM in permanenten Speicher ist nicht möglich, wenn der VRA einen einzelnen ESXi-Host schützt, der nicht von vCenter Server verwaltet wird.
- Um die VM aus der vSphere-Umgebung zu entfernen, klicken Sie im Dialogfeld „Prozessdetails“ auf **Schnelle VM-Wiederherstellung abbrechen**.

5.2.1 Migrieren einer mit Rapid VM Restore wiederhergestellten vSphere VM in den permanenten Speicher

Wenn Sie Rapid VM Restore zum ersten Mal verwenden, um eine vSphere-VM wiederherzustellen, ist die VM vom VRA und vom Vault abhängig und kann nur vorübergehend eingesetzt werden.

Um die VM permanent wiederherzustellen, müssen Sie sie in Portal in einen permanenten Speicher migrieren. Wenn die VM eingeschaltet ist, können Sie sie während der Migration weiterhin

verwenden. Nach der Migration ist die VM unabhängig von VRA und Vault, und ihre Laufwerke werden in ihrem Originalformat wiederhergestellt (thin- oder thick-Bereitstellung).

WICHTIG: Auf einem ESXi-Host, der nicht von vCenter Server verwaltet wird, kann mithilfe von Rapid VM Restore überprüft werden, ob VMs korrekt gesichert wurden; das Feature kann jedoch nicht verwendet werden, um VMs dauerhaft wiederherzustellen. Ein ESXi-Server, der nicht Teil eines vCenters ist, verfügt nicht über die erforderlichen Funktionen, um VMs in permanenten Speicher zu migrieren.

Wenn Sie eine Migration abbrechen, bevor die VM vollständig in den permanenten Datenspeicher migriert wurde, ist die wiederhergestellte VM weiterhin in der vSphere-Umgebung vorhanden und wird weiterhin mit dem Rapid VM Restore-Prozess ausgeführt. Wenn Sie den Rapid VM Restore-Prozess nicht abbrechen, können Sie erneut versuchen, die VM zu migrieren.

Für die Migration einer mit Rapid VM Restore wiederhergestellten VM in den permanenten Speicher empfehlen wir Folgendes:

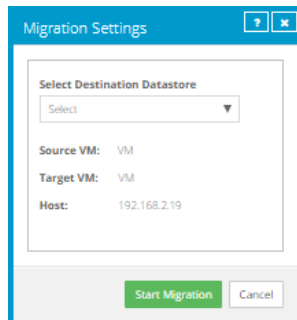
- Vor der Migration sollten Sie die VM sichern, die mit Rapid VM Restore wiederhergestellt wurde. Siehe *Best Practice: Sichern von vSphere VMs, die mit Rapid VM Restore wiederhergestellt wurden* auf Seite 55. Sie können eine VM nicht sichern, während sie migriert wird, oder eine VM migrieren, während sie gesichert wird.
- Verwenden Sie das Portal, um die VM in den permanenten Speicher zu verschieben, und nicht den vSphere-Client oder den Webclient. Wenn Sie eine VM in den permanenten Speicher verschieben, garantiert das Portal, dass alle Laufwerke migriert und in ihre Originalformate konvertiert werden. Wenn Sie versuchen, eine VM ohne das Portal in den permanenten Speicher zu verschieben, dabei jedoch nicht alle Laufwerke migrieren und in ihre Originalformate konvertieren, können Sie die VM nicht mehr mit dem Portal migrieren. Die VM wird unter Umständen gelöscht, wenn Sie den Rapid VM Restore-Prozess abbrechen.
- Führen Sie niemals mehr als sechs Migrationen gleichzeitig aus, selbst wenn die Migrationen auf mehrere Hosts in der vSphere-Umgebung verteilt sind.
- Schalten Sie die VM während der Migration nicht im Gastbetriebssystem aus. Andernfalls kann es passieren, dass Sie bis zum Abschluss der Migration aus der VM ausgesperrt werden. Während der Migration können Sie die VMs nicht mit dem vSphere-Client ein- oder ausschalten oder anhalten.

Gehen Sie wie folgt vor, um eine mit Rapid VM Restore wiederhergestellte VM in den permanenten Speicher zu migrieren:

1. Überprüfen Sie, ob die VM in dem für die Migration gewünschten Zustand ist: eingeschaltet, ausgeschaltet oder angehalten.
2. Falls das Dialogfeld „Prozessdetails“ für den Rapid VM Restore-Prozess der VM nicht geöffnet ist, suchen Sie den VRA-Sicherungsjob der VM auf der Seite „Computer“ oder „Überwachung“. Klicken Sie auf das Rapid VM Restore-Symbol neben dem VRA-Jobnamen: Im Dialogfeld „Prozessdetails“ werden Rapid VM Restore-Prozesse für den ausgewählten Sicherungsjob aufgelistet.
3. Wenn in der Liste „VM-Name“ mehr als eine VM angezeigt wird, wählen Sie die VM aus, die Sie migrieren möchten.
4. Klicken Sie auf **VM migrieren**.

WICHTIG: Die Schaltfläche „VM migrieren“ ist nicht verfügbar, wenn Sie die VM auf einem einzelnen ESXi-Host wiederherstellen, der nicht von vCenter Server verwaltet wird. Das permanente Wiederherstellen einer VM mit Rapid VM Restore ist nicht möglich, wenn der VRA einen einzelnen ESXi-Host schützt, der nicht von vCenter Server verwaltet wird.

Das Dialogfeld „Migrationseinstellungen“ wird angezeigt.



5. Wählen Sie in der Liste **Zieldatenspeicher auswählen** den permanenten Datenspeicher für die VM aus.

Diese Liste enthält die Datenspeicher, die für den Host verfügbar sind, den Sie für Rapid VM Restore ausgewählt haben, jedoch nicht den temporären Datenspeicher, den Sie für Rapid VM Restore ausgewählt haben.

6. Klicken Sie auf **Migration starten**.

Im Dialogfeld „Prozessdetails“ wird die folgende Statusmeldung angezeigt: *VM-Migration wird ausgeführt*.

Wenn Sie auf **Migration abbrechen** klicken, während die Migration ausgeführt wird, ist die wiederhergestellte VM weiterhin in vCenter vorhanden, und hängt weiterhin von VRA und Vault ab. Sie können die Migration bei Bedarf neu starten.

Nachdem die VM in den permanenten Datenspeicher migriert wurde, wird im Dialogfeld „Prozessdetails“ die folgende Statusmeldung angezeigt: *VM wurde migriert*. Zu diesem Zeitpunkt ist die VM vollständig wiederhergestellt und hängt nicht mehr von VRA und Vault ab. Der Rapid VM Restore-Prozess wird beendet, und das Rapid VM Restore-Symbol wird nicht mehr neben dem Jobnamen auf der Seite „Computer“ Oder „Überwachung“ angezeigt.

5.2.2 Best Practice: Sichern von vSphere VMs, die mit Rapid VM Restore wiederhergestellt wurden

Um Datenverluste zu vermeiden, sollten Sie die mit Rapid VM Restore wiederhergestellten vSphere virtuellen Computer (VMs) unbedingt sichern. Wenn Sie eine VM mit Rapid VM Restore wiederherstellen, hängt sie zunächst von einem aktiven Rapid VM Restore-Prozess und von Verbindungen zu VRA und Vault ab. Wenn die Verbindung zu VRA oder Vault unterbrochen wird, geht die VM unter Umständen verloren.

Daher sollten Sie die VM direkt vor der Migration sichern, falls bei der Migration ein Problem auftritt. Sie können eine VM nicht sichern, während sie migriert wird, oder eine VM migrieren, während sie gesichert wird.

Wenn Sie eine VM wiederherstellen und die ursprüngliche VM weiterhin in der vSphere-Umgebung existiert, wird die VM als Kopie der ursprünglichen VM wiederhergestellt. Sie müssen Ihren Sicherungsjob anpassen, um die wiederhergestellte VM einzubinden.

Wenn Sie eine VM wiederherstellen und die ursprüngliche VM nicht mehr in der vSphere-Umgebung existiert, wird die VM mit demselben eindeutigen Bezeichner (UUID) wie die ursprüngliche VM wiederhergestellt. Die wiederhergestellte VM wird durch den vorhandenen Job gesichert, obwohl die erste Sicherung länger als erwartet dauern kann.

Wenn bei einer Notfallwiederherstellung mehrere VMs aus demselben Sicherungsjob nicht mehr in der vSphere-Umgebung existieren, stellen Sie alle fehlenden VMs mit Rapid VM Restore wieder her, bevor Sie den Sicherungsjob ausführen. Wenn Sie den Job ausführen und nur ein Teil der VMs wiederhergestellt wurde, werden die fehlenden VMs bei der Sicherung übersprungen, und bei der nächsten Ausführung des Sicherungsjobs wird ein erneutes Seeding durchgeführt.

6.3 Wiederherstellen von Dateien, Ordnern und Datenbankelementen mit einem vSphere Recovery Agent

Sie können Dateien und Ordner von geschützten virtuellen Windows-VMs mithilfe des vSphere Recovery Agent (VRA) wiederherstellen.

Während der Wiederherstellung von Dateien und Ordnern werden Volumes von der ausgewählten virtuellen Maschine als Laufwerke auf der Maschine bereitgestellt, auf der der VRA ausgeführt wird. Anschließend können Sie folgende Aufgaben durchführen:

- Geben Sie einige oder alle bereitgestellten Laufwerke frei, damit Benutzer auf Dateien und Ordner von anderen Rechnern zugreifen können.
- Melden Sie sich bei der VRA-Maschine an und kopieren Sie Dateien und Ordner von den bereitgestellten Laufwerken.

Hinweis: Alle Benutzer des VRA-Systems können auf die Dateien und Ordner auf den bereitgestellten Laufwerken zugreifen, auch Benutzer ohne Administratorberechtigungen. Wenn Sie Bedenken hinsichtlich der Sicherheit haben, sichern Sie den Agent-Rechner und verhindern Sie, dass Benutzer sich lokal beim Rechner anmelden können.

Sie können Dateien und Ordner aus den bereitgestellten Laufwerken kopieren und ferner Elemente aus Exchange- und SQL Server-Datenbanken suchen und wiederherstellen. Verwenden Sie die Anwendung „Granular Restore for Microsoft Exchange and SQL“, um Exchange-Postfächer und -Nachrichten zu PST-Dateien oder Live-Datenbanken wiederherzustellen, SQL Server-Datenbankelemente zu Live-Datenbanken zu exportieren und SQL Server-Datenbankelemente als SQL-Skripte zu exportieren. Weitere Informationen finden Sie im *Benutzerhandbuch für Granular Restore for Microsoft Exchange and SQL*.

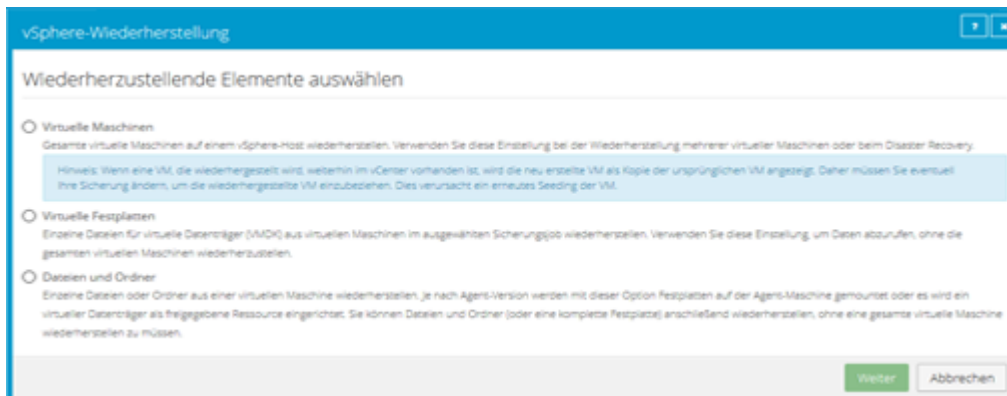
Hinweis: Sie können bestimmte Dateien und Ordner von Festplatten, die mit Bitlocker verschlüsselt sind, oder von Linux-VMs nicht wiederherstellen.

So stellen Sie Dateien, Ordner und Datenbankelemente mit einem vSphere Recovery Agent wieder her:

1. Klicken Sie in der Navigationsleiste auf **Computer**.

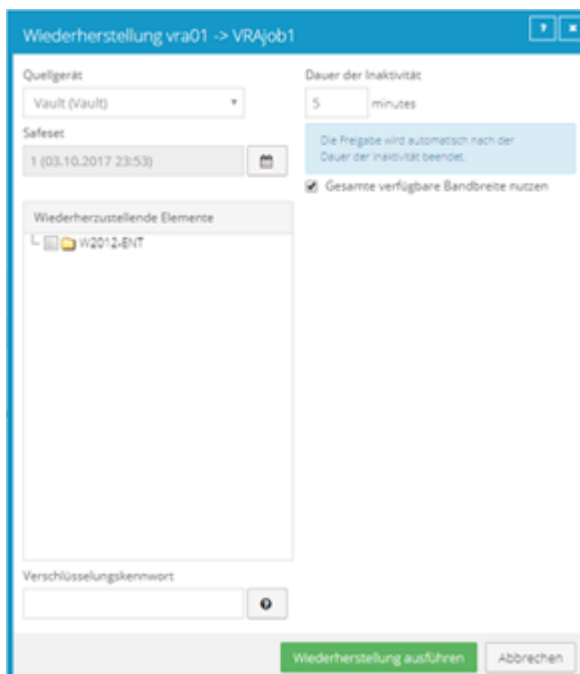
Die verfügbaren Computer werden in einem Raster aufgelistet.

2. Suchen Sie die vSphere-Umgebung mit der VM, die Sie wiederherstellen möchten, und erweitern Sie durch Klicken auf die Zeile ihre Ansicht.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Suchen Sie den Sicherungsjob für die VM, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellung** im Menü **Aktion auswählen** des Jobs.
5. Wählen Sie im Dialogfeld „Wiederherzustellende Elemente auswählen“ die Option **Dateien und Ordner**.




6. Klicken Sie auf **Weiter**.

Das Dialogfeld „Wiederherstellung“ wird angezeigt. Wenn bei der Ausführung des Sicherungsjobs keine mögliche Ransomware-Bedrohung erkannt wurde, wird im Feld „Sicherungssatz“ der letzte Sicherungssatz für den Job angezeigt.



Wenn bei der Ausführung des Sicherungsjobs eine mögliche Ransomware-Bedrohung erkannt wurde, wird ein Kalender mit einer Liste von Sicherungssätzen angezeigt. „Mögliche Bedrohung“ wird neben jedem Vault angezeigt, bei dem eine mögliche Ransomware-Bedrohung erkannt wurde.

Hinweis: Wenn Sie Daten wie in *Wiederherstellen von Daten auf einem Ersatzcomputer* auf Seite 59 oder *Wiederherstellen von Daten von einem anderen Computer* auf Seite 60 beschrieben wiederherstellen, wird für keinen Sicherungssatz „Mögliche Bedrohung“ angezeigt, selbst wenn eine mögliche Bedrohung während einer Sicherung in der ursprünglichen vSphere-Umgebung erkannt wurde.

7. Um die Daten eines älteren Sicherungssatzes wiederherzustellen, klicken Sie auf die Schaltfläche **Sicherungssätze durchsuchen**, falls nicht bereits ein Kalender mit einer Liste von Sicherungen angezeigt wird.  Klicken Sie im Kalender auf das Datum des Sicherungssatzes, von dem Sie die Wiederherstellung durchführen möchten. Klicken Sie rechts neben dem Kalender auf den spezifischen Sicherungssatz, aus dem Sie wiederherstellen möchten.
8. Aktivieren Sie im Feld **Wiederherzustellende Elemente** das Kontrollkästchen für die virtuellen Datenträger mit Dateien und Ordner, die Sie wiederherstellen möchten.
Wenn eine mögliche Ransomware-Bedrohung auf einer VM erkannt wurde, wird „Mögliche Bedrohung“ neben dem Namen der VM angezeigt.
9. Geben Sie im Feld **Verschlüsselungskennwort** das Verschlüsselungskennwort für die Daten ein. Um den Kennworthinweis anzuzeigen, klicken Sie auf die Schaltfläche **Hinweis**.
10. Geben Sie im Feld **Dauer der Inaktivität** die Anzahl der Minuten ein, die ohne Aktivität verstreichen sollen, bis die Bereitstellung des freigegebenen Laufwerks automatisch aufgehoben wird. Die **Leerlaufzeit** kann zwischen 2 und 180 Minuten liegen.

Hinweis: Das Laufwerk hebt die Freigabe nicht auf, solange neue Daten kopiert werden. Wenn Daten von einem freigegebenen Laufwerk mehrmals kopiert werden, kann dies zu einer Zeitüberschreitung des Systems führen, da fortlaufend neue Daten gelesen werden.

11. Um die gesamte verfügbare Bandbreite für die Wiederherstellung zu nutzen, wählen Sie **Gesamte verfügbare Bandbreite nutzen** aus.
Um die Leistung für Ihre Wiederherstellung zu optimieren, empfehlen wir, die Option **Gesamte verfügbare Bandbreite nutzen** zu aktivieren.
12. Klicken Sie auf **Wiederherstellung ausführen**.
Volumes von der ausgewählten VM werden als Laufwerke auf dem Rechner zugewiesen, auf dem der VRA ausgeführt wird, und sind im Ordner „RestoreMount“ auf dem VRA-Rechner verfügbar.
13. (Optional) Um Zugriff auf die Sicherungsdaten von anderen Servern zu erlauben, gehen Sie auf dem Rechner mit dem VRA wie folgt vor:
 - Geben Sie eines oder mehrere zugeordnete Laufwerke frei.
 - Geben Sie ein oder mehrere Verzeichnisse vom Ordner „RestoreMount“ frei.
14. Wählen Sie eine oder beide der folgenden Optionen:
 - Kopieren Sie die Dateien und Ordner, die Sie von den zugeordneten Laufwerken oder Freigaben wiederherstellen möchten.
 - Verwenden Sie die Anwendung „Granular Restore for Microsoft Exchange and SQL“, um Elemente aus Exchange- und SQL Server-Datenbanksicherungen auf den zugeordneten Laufwerken oder Freigaben zu finden und wiederherzustellen. Sie können Exchange-Postfächer und -Nachrichten zu PST-Dateien oder Live-Datenbanken wiederherstellen,

SQL Server-Datenbankelemente zu Live-Datenbanken exportieren und SQL Server-Datenbankelemente als SQL-Skripte exportieren. Siehe *Benutzerhandbuch für Granular Restore for Microsoft Exchange and SQL*.

6.4 Wiederherstellen von Daten auf einem Ersatzcomputer

Wenn Sie ein System ersetzen und alle Daten zu einem neuen Computer migrieren möchten (z. B. am Ende eines Leasingvertrags) oder bei einer Notfallwiederherstellung, können Sie den neuen Computer im Vault als den alten Computer erneut registrieren und Daten aus den Sicherungen auf dem alten Computer wiederherstellen. Wenn auf dem alten Computer Daten in mehreren Vaults gesichert wurden, können Sie den neuen Computer über Portal Version 8.50 oder höher erneut registrieren.

Nachdem Sie einen Computer in einem Vault erneut registriert haben, müssen Sie:

- Jeden vorhanden Sicherungsjob bearbeiten und das Verschlüsselungskennwort für den Sicherungsjob eingeben.
- Die Jobs synchronisieren, bevor sie erfolgreich ausgeführt werden. Siehe *Synchronisieren eines Jobs* auf Seite 43.

Falls Sie die Daten auf einem anderen Computer wiederherstellen möchten, ohne den vorhandenen Computer zu ersetzen, können Sie die Daten von einem anderen Computer wiederherstellen. Siehe *Wiederherstellen von Daten von einem anderen Computer* auf Seite 60.

So können Sie Daten auf einem Ersatzcomputer wiederherstellen:

1. Laden Sie einen Agenten herunter und installieren Sie ihn auf dem neuen bzw. neu aufgebauten Computer.
2. Klicken Sie in der Navigationsleiste auf **Computer**.
Die verfügbaren Computer werden in einem Raster aufgelistet.
3. Suchen Sie den Ersatzcomputer, auf dem Sie die Daten wiederherstellen möchten, und erweitern Sie durch Klicken auf die Computerzeile seine Ansicht.
4. Klicken Sie auf **Manuell konfigurieren**.
5. Klicken Sie auf die Registerkarte „Vault-Einstellungen“.
6. Klicken Sie auf **Erneut registrieren**.
6. Wählen Sie im Dialogfeld „Vault-Einstellungen“ in der Liste **Vault-Profil** den Vault aus, in dem die Sicherung des Originalcomputers gespeichert wurde.
7. Klicken Sie auf **Computer laden**.
8. Klicken Sie in der Liste der Computer auf den Namen des Computers, auf dem Sie die Daten gesichert haben. Klicken Sie auf **Speichern**.
9. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
10. Wenn der ursprüngliche Computer Daten in einem anderen Vault gesichert hat, wiederholen Sie Schritt 6 bis Schritt 9, um Jobinformationen aus dem anderen Vault herunterzuladen.
11. Nachdem die Jobinformationen heruntergeladen wurden, klicken Sie auf die Registerkarte **Jobs**.

Sie müssen alle für den Job erforderlichen Kennwörter eingeben, einschließlich des Verschlüsselungskennworts.

Für einen vSphere- Recovery Agent müssen Sie auch vCenter- oder ESXi-Hostinformationen auf der Registerkarte „vSphere-Einstellungen“ eingeben.

12. Suchen Sie den Job mit den Daten, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellung** im Menü **Aktion auswählen** des Jobs.

Die weiteren Schritte entsprechen dem Vorgehen bei normalen Wiederherstellungen.

Hinweis: Wenn Sie Daten aus einem vSphere-Job wiederherstellen, wird im Dialogfeld „Wiederherstellung“ für keinen Sicherungssatz „Potenzielle Bedrohung“ angezeigt, selbst wenn eine potenzielle Bedrohung während einer Sicherung in der ursprünglichen vSphere-Umgebung erkannt wurde.

WICHTIG: Nachdem Sie einen Computer im Vault erneut registriert haben, müssen Sie die Verschlüsselungskennwörter für die Sicherungsjobs auf dem Computer eingeben und die Jobs synchronisieren, bevor diese erfolgreich ausgeführt werden können. Siehe *Synchronisieren eines Jobs* auf Seite [43](#).

6.5 Wiederherstellen von Daten von einem anderen Computer

Sie können einige oder alle auf einem Computer gesicherten Daten auf einem anderen Computer mit gleichen Merkmalen wiederherstellen.

Um die Daten von einem anderen Computer wiederherzustellen, können Sie die Daten aus einem Sicherungsjob im Vault auf einen anderen Computer umleiten.

Anschließend lädt der neue Computer Informationen aus dem Vault herunter, um die Daten auf dem neuen Computer wiederherstellen zu können. Beispiel:

- Computer A sichert seine Daten mit Job A
- Computer B stellt die Daten von Job A (Daten von Computer A) auf Computer B wieder her.

Wenn Sie eine Notfallwiederherstellung auf demselben oder einem Ersatzcomputer durchführen möchten, können Sie einen neu konfigurierten Computer nach der Installation eines Betriebssystems und eines Agenten erneut registrieren. Informationen dazu finden Sie unter *Wiederherstellen von Daten auf einem Ersatzcomputer* auf Seite [59](#).

Wenn die Datenstreams kompatibel sind, können Sie auf einen anderen Computer mit einem ähnlichen (aber nicht genau gleichen) Betriebssystem wiederherstellen. Unterschiedliche Versionen desselben Betriebssystems sind oft kompatibel. Betriebssysteme, die die gleiche Abstammung haben, sind ebenfalls akzeptabel.

So stellen Sie Daten von einem anderen Computer wieder her

1. Klicken Sie in der Navigationsleiste auf **Computer**.

Die verfügbaren Computer werden in einem Raster aufgelistet.

2. Suchen Sie den Computer, auf dem Sie die Daten wiederherstellen möchten, und erweitern Sie durch Klicken auf die Computerzeile seine Ansicht.
3. Klicken Sie im Menü **Jobaufgaben** auf **Von einem anderen Computer wiederherstellen**.

Das Dialogfeld Von einem anderen Computer wiederherstellen wird geöffnet.

4. Wählen Sie in der Liste **Vaults** den Vault aus, in dem die Sicherung gespeichert wurde.
5. Wählen Sie in der Liste **Computer** den Computer mit der Sicherung aus, mit der die Wiederherstellung durchgeführt werden soll.
6. Wählen Sie in der Liste **Jobs** den Job aus, aus dem die Daten wiederhergestellt werden sollen.
7. Klicken Sie auf **OK**.

Das Portal versucht, Informationen zu dem ausgewählten Job herunterzuladen. Nachdem die Jobinformationen heruntergeladen wurden, wird der Job in der Registerkarte „Jobs“ für den Computer angezeigt. Anschließend können Sie wie bei einer normalen Wiederherstellung verfahren.

Hinweis: Wenn Sie Daten aus einem vSphere-Job wiederherstellen, wird im Dialogfeld „Wiederherstellung“ für keinen Sicherungssatz „Potenzielle Bedrohung“ angezeigt, selbst wenn eine potenzielle Bedrohung während einer Sicherung in der ursprünglichen vSphere-Umgebung erkannt wurde.

Falls beim Download der Informationen über den ausgewählten Job ein Fehler auftritt, kann die Wiederherstellung nicht fortgesetzt werden. Dies kann passieren, wenn der Vault nicht erreichbar ist, die Jobinformationen nicht abrufbar sind oder ein benötigtes Plug-in nicht auf dem Zielcomputer installiert ist. Vergewissern Sie sich, dass alle benötigten Plug-ins auf dem Zielcomputer installiert sind, bevor Sie den Vorgang wiederholen.

6.6 Erweiterte Wiederherstellungsoptionen

Protokolloptionen

Wählen Sie in der Liste eine der folgenden Protokollierungsebenen aus:

- **Dateien:** Bietet ausführlichere Informationen und wird in der Regel zur Fehlerbehebung verwendet. Bietet Informationen zu Dateien, die gesichert werden.
- **Verzeichnis:** Bietet weniger detaillierte Informationen als die Protokollierungsebene „Dateien“. Bietet Informationen zu Ordnern, die gesichert werden.
- **Zusammenfassung:** Bietet Informationen der obersten Ebene, einschließlich der Vault-/Agent-Version und Sicherungsgröße.
- **Minimal:** Bietet Informationen der obersten Ebene, einschließlich der Vault-/Agent-Version.

Eine Änderung der Protokollierungsebene wirkt sich nur auf Protokolldateien aus, die danach erstellt werden. Bereits erstellte Protokolldateien sind von dieser Änderung nicht betroffen.

Leistungsoptionen

Um die gesamte verfügbare Bandbreite für die Wiederherstellung zu nutzen, wählen Sie **Gesamte verfügbare Bandbreite nutzen** aus.

Die Bandbreitendrosselung legt fest, welche Bandbreite ein Agent für Sicherungen und Wiederherstellungen verbrauchen darf. Sie können zum Beispiel Sicherungen tagsüber so beschränken, dass Online-Benutzer nicht beeinträchtigt werden, und nachts die Nutzung

uneingeschränkt freigeben, damit geplante Sicherungen schnellstmöglich ausgeführt werden können.

7 Löschen von Jobs und Computern und Löschen von Daten aus Vaults

Reguläre Benutzer und Administratoren können Sicherungsjobs aus Portal löschen, ohne dass die zugehörigen Daten aus den Vaults gelöscht werden. Weitere Informationen finden Sie unter *Löschen von Sicherungsjobs ohne Löschung der zugehörigen Daten aus den Vaults* auf Seite [63](#).

Administratoren können Computer und geschützte Umgebungen aus Portal löschen, ohne dass die zugehörigen Daten aus den Vaults gelöscht werden. Weitere Informationen finden Sie unter *Löschen von Computern ohne Löschung der zugehörigen Daten aus den Vaults* auf Seite [67](#).

In einer Portal-Instanz, in der die Funktion zum Löschen von Daten aktiviert ist, können Administratoren darüber hinaus folgende Aktionen ausführen:

- Sicherungsjobs aus Portal löschen und Anforderungen zum Löschen der Jobdaten aus den Vaults senden. Weitere Informationen finden Sie unter *Löschen von Sicherungsjobs und der zugehörigen Jobdaten aus Vaults* auf Seite [64](#).

Beim Löschen von Jobdaten aus Vaults gibt es eine 72-stündige Wartezeit, bevor die Anforderung zum Löschen der Daten an die Vaults gesendet wird. Während dieser Wartezeit können Administratorbenutzer in der Site die Datenlöschung abbrechen. Siehe *Abbrechen einer geplanten Jobdatenlöschung* auf Seite [66](#).

- Computer aus Portal löschen und Anforderungen zum Löschen der Computerdaten aus den Vaults senden. Weitere Informationen finden Sie unter *Löschen eines Computers und von Computerdaten aus Vaults* auf Seite [68](#).

Hinweis: Ab Portal 8.90 können Administratoren Anforderungen zum Löschen von Daten aus Vaults für Online- oder Offline-Computer übermitteln. In früheren Portalversionen konnten Anforderungen zum Löschen von Daten aus Vaults nur für Online-Computer übermittelt werden.

Beim Löschen von Computerdaten aus Vaults gibt es eine 72-stündige Wartezeit, bevor die Anforderung zum Löschen der Daten an die Vaults gesendet wird. Während dieser Wartezeit können Administratorbenutzer in der Site die Datenlöschung abbrechen. Siehe *Abbrechen einer geplanten Computerdatenlöschung* auf Seite [70](#).

- Spezifische Sicherungen aus Vaults löschen. Diese Option ist ab Portal 8.90 verfügbar. Siehe *Löschen von spezifischen Sicherungen aus Vaults* auf Seite [71](#).

Anforderungen zum Löschen von Sicherungen werden sofort an die Vaults übermittelt; es gibt keine Wartezeit, bevor die Anforderung zum Löschen von Daten an die Vaults gesendet wird. Da Anforderungen zum Löschen von Sicherungen sofort übermittelt werden, können Löschanforderungen für Sicherungen nicht storniert werden.

7.1 Löschen von Sicherungsjobs ohne Löschung der zugehörigen Daten aus den Vaults

Reguläre Benutzer und Administratoren können Sicherungsjobs von Online-Computern löschen, ohne dass zugehörigen Jobdaten aus den Vaults gelöscht werden.

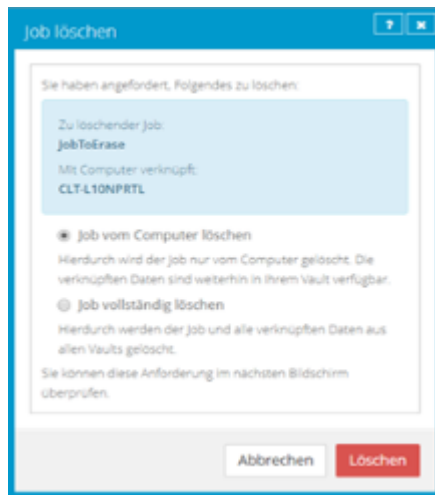
In einer Portal-Instanz, in der die Funktion zum Löschen von Daten aktiviert ist, können Administratorbenutzer Anforderungen zum Löschen von Jobdaten aus den Vaults senden, wenn sie

Jobs in Portal löschen. Weitere Informationen finden Sie unter *Löschen von Sicherungsjobs und der zugehörigen Jobdaten aus Vaults* auf Seite 64.

So löschen Sie einen Sicherungsjob, ohne die zugehörigen Daten aus den Vaults zu löschen.

1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den Online-Computer mit dem Job, den Sie löschen möchten und erweitern Sie die entsprechende Ansicht durch Klicken auf die jeweilige Zeile.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Klicken Sie im Menü **Aktion auswählen** des Jobs, den Sie löschen möchten, auf **Job löschen**.
5. Wenn Sie als Administrator in einer Portal-Instanz angemeldet sind, in der die Funktion zum Löschen von Daten aktiviert ist, wird das Dialogfeld „Job löschen“ angezeigt.

Um den Sicherungsjob zu löschen, ohne die zugehörigen Daten aus den Vaults zu löschen, klicken Sie auf **Job vom Computer löschen** und dann auf **Löschen**.



Hinweis: Das Dialogfeld „Job löschen“ wird nicht angezeigt, wenn Sie Sicherungsdaten in Vaults nicht löschen können. Das liegt daran, dass Ihre Portal-Instanz die Löschung von Vault-Daten nicht unterstützt oder Sie als regulärer Benutzer angemeldet sind.

6. Geben Sie im Bestätigungsdialogfeld **BESTÄTIGEN** ein.
Hinweis: Sie müssen den Text **BESTÄTIGEN** in Großbuchstaben eingeben.
7. Klicken Sie auf **Löschen bestätigen**.

7.2 Löschen von Sicherungsjobs und der zugehörigen Jobdaten aus Vaults

Wenn in einer Portal-Instanz die Funktion zum Löschen von Daten aktiviert ist, können Administratoren Sicherungsjobs löschen und die Löschung der zugehörigen Daten aus sämtlichen Vaults anfordern. Um zu verhindern, dass versehentlich die falschen Daten gelöscht werden, wird die Löschung der Daten auf einen Zeitpunkt von 72 Stunden nach Übermittlung der Anforderung angesetzt und es wird eine E-Mail-Benachrichtigung an die Administratoren der Site und an die Superuser gesendet.

Während der 72-stündigen Wartezeit vor der Durchführung des Löschvorgangs können Administratoren geplante Jobs zur Datenlöschung auf den ihnen zugewiesenen Sites abbrechen. Siehe *Abbrechen einer geplanten Jobdatenlöschung* auf Seite 66.

Wenn eine geplante Löschung von Jobdaten während der 72-stündigen Wartezeit nicht abgebrochen wird, wird der Job in Portal gelöscht. Die Löschanforderung wird anschließend an die Vaults gesendet und die Jobdaten in den entsprechenden Vaults werden automatisch gelöscht. Wenn die Daten zu einem Job aus irgendeinem Grund nicht gelöscht werden können, wird eine E-Mail-Benachrichtigung an einen Vault-Administrator gesendet. Der Vault-Administrator kann dann die Daten manuell löschen.

Hinweis: Da die Daten in der 72-stündigen Wartezeit zur Wiederherstellung verfügbar sind, werden sie weiterhin in den Kundenrechnungen berücksichtigt. Eine Nutzungsreduzierung zu Abrechnungszwecken erfolgt erst, wenn die Daten gelöscht werden.

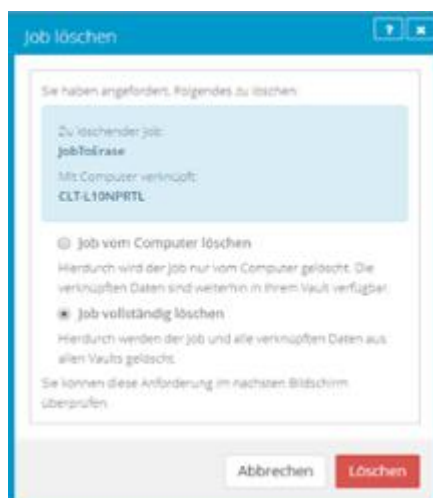
WARNUNG: Die Löschung von Jobdaten kann nicht rückgängig gemacht werden. Nachdem die Daten aus den Vaults gelöscht wurden, können sie nicht wiederhergestellt werden.

So löschen Sie einen Sicherungsjob und die zugehörigen Daten aus den Vaults:

1. Melden Sie sich als Administrator an und klicken Sie in der Navigationsleiste auf **Computer**. Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den Computer mit dem Job, den Sie löschen möchten, und erweitern Sie durch Klicken auf seine Zeile seine Ansicht.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Klicken Sie im Menü **Aktion auswählen** des Jobs, den Sie löschen möchten, auf **Job löschen**.

Wenn die Funktion zum Löschen von Daten in Ihrer Portal-Instanz aktiviert ist, wird das Dialogfeld „Job löschen“ angezeigt.

Hinweis: Wenn das Dialogfeld „Job löschen“ nicht angezeigt wird, können Sie die Löschung der zugehörigen Jobdaten aus den Vaults nicht anfordern. Sie können den Job nur über Portal löschen. Weitere Informationen finden Sie unter *Löschen von Sicherungsjobs ohne Löschung der zugehörigen Daten aus den Vaults* auf Seite 63.



5. Wählen Sie die Option **Job vollständig löschen** und klicken Sie dann auf **Löschen**.

WICHTIG: Um nicht mehr benötigte Daten dauerhaft aus den Vaults zu löschen und die Abrechnung zu reduzieren, müssen Sie **Job vollständig löschen** auswählen. Wenn Sie **Job löschen** auswählen, werden die Daten nicht aus den Vaults entfernt und Ihre Rechnung wird nicht beeinflusst.

WARNUNG: Die Löschung von Jobdaten kann nicht rückgängig gemacht werden. Nachdem die Daten aus den Vaults gelöscht wurden, können sie nicht wiederhergestellt werden.

6. Geben Sie im Bestätigungsdialogfeld **BESTÄTIGEN** ein.

Hinweis: Sie müssen den Text **BESTÄTIGEN** in Großbuchstaben eingeben.

7. Klicken Sie auf **Löschen bestätigen**.

Im Dialogfeld "Job gelöscht" wird angezeigt, dass der Job und die zugehörigen Daten in Ihren Vaults gelöscht werden.

8. Klicken Sie auf **Schließen**.

In der Spalte "Letzter Sicherungsstatus" wird für den Auftrag die Meldung **Zum Löschen vorgesehen** angezeigt. In der Spalte "Datum" wird das Datum angezeigt, an dem der Job aus Portal und die zugehörigen Jobdaten aus den Vaults gelöscht werden. Innerhalb eines Tages nach dem geplanten Löschvorgang wird in der Spalte "Datum" auch der Zeitpunkt angezeigt, zu dem der Job und die zugehörigen Daten gelöscht werden.

Ab Portal 9.10 wird der Status **Zum Löschen vorgesehen** für jede Instanz des Jobs in Portal angezeigt, wenn ein Job zur Löschung vorgesehen ist. Ein Job kann für mehrere Computer angezeigt werden, wenn ein Computer neu registriert wurde oder der Arbeitsablauf „Von einem anderen Computer wiederherstellen“ verwendet wurde. Wenn ein Job aus Vaults gelöscht wird, wird der Job von allen Computern gelöscht, auf denen er angezeigt wird.

Während der 72-stündigen Wartezeit, bevor die Daten gelöscht werden, können Sie die Anforderung zur Löschung widerrufen. Da die Daten in diesem Zeitraum zur Wiederherstellung verfügbar sind, werden sie weiterhin in den Kundenrechnungen berücksichtigt. Eine Nutzungsreduzierung zu Abrechnungszwecken erfolgt erst, wenn die Daten gelöscht werden.

Es wird eine E-Mail-Nachricht an die Administratoren der Site und die Superuser gesendet mit der Angabe, dass die Joblöschung geplant wurde.



7.3 Abbrechen einer geplanten Jobdatenlöschung

In einer Portal-Instanz, in der die Funktion zum Löschen von Daten aktiviert ist, können Administratoren Sicherungsjobs löschen und anfordern, dass die zugehörigen Jobdaten aus allen Vaults gelöscht werden. Die Löschung der Daten wird auf einen Zeitpunkt von 72 Stunden nach Übermittlung der Anforderung angesetzt und es wird eine E-Mail-Benachrichtigung an die Administratoren der Site und an die Superuser gesendet.

Während der 72-stündigen Wartezeit vor Löschung eines Jobs aus Portal und der zugehörigen Jobdaten aus den Vaults können die Administratoren der Site die Datenlöschung abbrechen. Wenn eine geplante Datenlöschung abgebrochen wird, wird eine E-Mail-Benachrichtigung an die Administratorbenutzer der Site und an die Superuser gesendet.

Ab Portal 9.10 wird der Status **Zum Löschen vorgesehen** für jede Instanz des Jobs in Portal angezeigt, wenn ein Job zur Löschung vorgesehen ist. Ein Job kann für mehrere Computer angezeigt werden, wenn ein Computer neu registriert wurde oder der Arbeitsablauf „Von einem anderen Computer wiederherstellen“ verwendet wurde. Ein Administrator kann die Löschung von jeder Instanz des Jobs abbrechen.

So brechen Sie eine geplante Jobdatenlöschung ab:

1. Melden Sie sich als Administrator an und klicken Sie in der Navigationsleiste auf **Computer**. Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den Computer, für den die Jobdatenlöschung geplant ist, und erweitern Sie die entsprechende Ansicht durch Klicken auf die jeweilige Zeile.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Klicken Sie im Menü „Aktion auswählen“ zum Job, den Sie löschen möchten, auf **Löschen abbrechen**.



Sie werden in einem Bestätigungsdialogfeld aufgefordert, den Abbruch der Löschung zu bestätigen.

5. Klicken Sie auf **Ja**.

Die Werte in den Spalten „Letzter Sicherungsstatus“ und „Datum“ zum jeweiligen Job werden auf die Werte zurückgesetzt, die angezeigt wurden, bevor der Job für die Löschung vorgesehen wurde.

Es wird eine E-Mail-Nachricht an die Administratoren der Site und die Superuser gesendet mit der Angabe, dass die geplante Joblöschung abgebrochen wurde.



7.4 Löschen von Computern ohne Löschung der zugehörigen Daten aus den Vaults

Administratoren können Computer aus Portal löschen, ohne dass die Computerdaten aus den Vaults gelöscht werden. Sie können sowohl Online- als auch Offline-Computer aus Portal löschen, ohne dass die zugehörigen Daten aus den Vaults gelöscht werden.

Wenn ein Computer auf diese Weise aus Portal gelöscht wird, können die Daten mit dem Verfahren *Von einem anderen Computer wiederherstellen* wiederhergestellt werden.

Hinweis: Wenn ein Computer aus Portal gelöscht wird, wird der Agent nicht von dem Computer entfernt, auf dem er installiert ist. Sie müssen den Agent manuell deinstallieren.

So löschen Sie einen Computer, ohne Daten aus den Vaults zu löschen:

1. Melden Sie sich als Administrator an und klicken Sie in der Navigationsleiste auf **Computer**. Die Seite „Computer“ zeigt registrierte Computer an.
2. Aktivieren Sie das Kontrollkästchen für jeden Computer, den Sie löschen möchten.

3. Klicken Sie in der Liste **Aktionen** auf **Ausgewählte(n) Computer löschen**.
4. Wenn die Funktion zum Löschen von Daten in Ihrer Portal-Instanz aktiviert ist, wird das Dialogfeld "Computer löschen" angezeigt.

Klicken Sie auf **Computer löschen** und dann auf **Löschen**, um den Computer ohne Löschung der zugehörigen Daten aus den Vaults zu löschen.



Hinweis: Das Dialogfeld "Computer löschen" wird nur angezeigt, wenn Ihre Portal-Instanz das Löschen von Vault-Daten unterstützt.

5. Geben Sie im Bestätigungsdialogfeld **BESTÄTIGEN** ein.

Hinweis: Sie müssen den Text **BESTÄTIGEN** in Großbuchstaben eingeben.

6. Klicken Sie auf **Löschen bestätigen**.
7. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
8. Klicken Sie im Dialogfeld „Erfolg“ auf **OK**.

7.5 Löschen eines Computers und von Computerdaten aus Vaults

In einer Portal-Instanz, in der die Funktion zum Löschen von Daten aktiviert ist, können Administratoren Computer löschen und anfordern, dass die zugehörigen Computerdaten aus allen Vaults gelöscht werden. Um zu verhindern, dass versehentlich die falschen Daten gelöscht werden, wird die Löschung der Daten auf einen Zeitpunkt von 72 Stunden nach Übermittlung der Anforderung angesetzt, es wird eine E-Mail-Benachrichtigung an die Administratoren der Site und an die Superuser gesendet und der Status des Computers in Portal wechselt zu *Zur Löschung geplant*.

Hinweis: Ab Portal 8.90 können Administratoren Anforderungen zum Löschen von Daten aus Vaults für Online- oder Offline-Computer übermitteln. In früheren Portalversionen konnten Anforderungen zum Löschen von Daten aus Vaults nur für Online-Computer übermittelt werden.

Während der 72-stündigen Wartezeit vor Senden der Anforderung zur Löschung von Computerdaten an die Vaults können Administratorbenutzer der Site die geplante Computerdatenlöschung abbrechen. Weitere Informationen finden Sie unter *Abbrechen einer geplanten Computerdatenlöschung* auf Seite 70.

Wenn eine geplante Löschung von Computerdaten während der 72-stündigen Wartezeit nicht abgebrochen wird, wird die Löschanforderung an die Vaults gesendet und die Jobdaten werden in den entsprechenden Vaults automatisch gelöscht. Wenn die Daten zu einem Computer aus irgendeinem Grund nicht gelöscht werden können, wird eine E-Mail-Benachrichtigung an einen Vault-Administrator gesendet. Der Vault-Administrator kann dann die Daten manuell löschen. Nach Löschung der Computerdaten aus den Vaults wird der Computer aus Portal gelöscht.

Hinweis: Da die Daten in der 72-stündigen Wartezeit zur Wiederherstellung verfügbar sind, werden sie weiterhin in den Kundenrechnungen berücksichtigt. Eine Nutzungsreduzierung zu Abrechnungszwecken erfolgt erst, wenn die Daten gelöscht werden.

Hinweis: Wenn ein Computer aus Portal gelöscht wird, wird der Agent nicht von dem Computer entfernt, auf dem er installiert ist. Sie müssen den Agent manuell deinstallieren.

WARNUNG: Die Löschung von Computerdaten kann nicht rückgängig gemacht werden. Nachdem die Daten aus den Vaults gelöscht wurden, können sie nicht wiederhergestellt werden.

So löschen Sie einen Computer und Computerdaten aus Vaults:

1. Melden Sie sich als Administrator an und klicken Sie in der Navigationsleiste auf **Computer**. Die Seite „Computer“ zeigt registrierte Computer an.
2. Aktivieren Sie das Kontrollkästchen für jeden Computer, den Sie löschen möchten.
3. Klicken Sie in der Liste **Aktionen** auf **Ausgewählte(n) Computer löschen**.

Wenn die Funktion zum Löschen von Daten in Ihrer Portal-Instanz aktiviert ist, wird das Dialogfeld „Computer löschen“ angezeigt.

Hinweis: Wenn das Dialogfeld „Computer löschen“ nicht angezeigt wird oder die Option **Computer vollständig löschen** nicht verfügbar ist, können Sie nicht anfordern, dass die Daten für die ausgewählten Computer aus den Vaults gelöscht werden. Sie können nur die ausgewählten Computer aus Portal löschen. Weitere Informationen finden Sie unter *Löschen von Computern ohne Löschung der zugehörigen Daten aus den Vaults* auf Seite [67](#).

4. Wählen Sie **Computer vollständig löschen**, und klicken Sie dann auf **Löschen**.

WICHTIG: Um nicht mehr benötigte Daten dauerhaft aus den Vaults zu löschen und die Abrechnung zu reduzieren, müssen Sie **Computer vollständig löschen** auswählen. Wenn Sie **Computer löschen** auswählen, werden die Daten nicht aus den Vaults entfernt und Ihre Rechnung wird nicht beeinflusst.

WARNUNG: Die Löschung von Computerdaten kann nicht rückgängig gemacht werden. Nachdem die Daten aus den Vaults gelöscht wurden, können sie nicht wiederhergestellt werden.

5. Geben Sie im Bestätigungsdialogfeld **BESTÄTIGEN** ein.

Hinweis: Sie müssen den Text **BESTÄTIGEN** in Großbuchstaben eingeben.

6. Klicken Sie auf **Löschen bestätigen**.

WARNUNG: Die Löschung von Computerdaten kann nicht rückgängig gemacht werden. Nachdem die Daten aus den Vaults gelöscht wurden, können sie nicht wiederhergestellt werden.

Im Dialogfeld "Computer gelöscht" wird angezeigt, dass die gewünschten Computer und die zugehörigen Daten in Ihren Vaults gelöscht werden.

7. Klicken Sie auf **Schließen**.

In der Spalte "Status" wird für die betreffenden Computer die Meldung *Zum Löschen vorgesehen* angezeigt. Wenn Sie die Ansicht zu einem Computer erweitern, wird in einer Meldung der Zeitpunkt der Löschung angezeigt.

Während der 72 Stunden können Sie die Anforderung zur Löschung abbrechen. Da die Daten in diesem Zeitraum zur Wiederherstellung verfügbar sind, werden sie weiterhin in den Kundenrechnungen berücksichtigt. Eine Nutzungsreduzierung zu Abrechnungszwecken erfolgt erst, wenn die Daten gelöscht werden.

Sie können für Computer, die zum Löschen vorgesehen sind, keine Jobs hinzufügen, bearbeiten, ausführen, planen oder löschen. Bestehende Sicherungsjobs werden wie geplant ausgeführt, bis der Computer gelöscht wird.

7.6 Abbrechen einer geplanten Computerdatenlöschung

In einer Portal-Instanz, in der die Funktion zum Löschen von Daten aktiviert ist, können Administratorbenutzer Online-Computer löschen und anfordern, dass die zugehörigen Computerdaten aus allen Vaults gelöscht werden. Die Datenlöschung wird für 72 Stunden nach der Anforderung angesetzt. Weitere Informationen finden Sie unter *Löschen eines Computers und von Computerdaten aus Vaults* auf Seite [68](#).

Während der 72-stündigen Wartezeit vor Senden der Anforderung zur Löschung von Computerdaten an die Vaults können die Administratorbenutzer der Site die Datenlöschung abbrechen. Wenn eine geplante Datenlöschung abgebrochen wird, wird eine E-Mail-Benachrichtigung an die Administratorbenutzer der Site und an die Superuser gesendet.

So brechen Sie eine geplante Computerdatenlöschung ab:

1. Melden Sie sich als Administratorbenutzer an und klicken Sie in der Navigationsleiste auf **Computer**.

Die Seite „Computer“ zeigt registrierte Computer an.

2. Aktivieren Sie das Kontrollkästchen für jeden Computer, für den Sie die geplante Datenlöschung abbrechen möchten.

In der Spalte „Status“ wird für die betreffenden Computer die Meldung *Zur Löschung geplant* angezeigt.

3. Klicken Sie in der Liste „Aktionen“ auf **Löschen ausgewählter Computer abbrechen**.

Hinweis: Wenn **Löschen ausgewählter Computer abbrechen** nicht verfügbar ist, wurde die Anforderung zum Löschen von Daten für den ausgewählten Computer möglicherweise bereits an die Vaults gesendet. Um zu sehen, wann ein Computer zur Löschung vorgesehen war, erweitern Sie die Computerzeile.

Sie werden in einem Bestätigungsdialogfeld aufgefordert, den Abbruch der Löschung zu bestätigen.

4. Klicken Sie auf **Ja**.

Das Dialogfeld "Erfolg" wird angezeigt.

5. Klicken Sie auf **OK**.

Der Wert in der Spalte "Status" zum jeweiligen Computer wird auf den Wert zurückgesetzt, der angezeigt wurde, bevor der Computer für die Löschung vorgesehen wurde.

Es wird eine E-Mail-Nachricht an die Administratoren der Site und die Superuser gesendet mit der Angabe, dass die geplante Computerlöschung abgebrochen wurde.

7.7 Löschen von spezifischen Sicherungen aus Vaults

In einer Portal-Instanz, in der die Datenlöschfunktion aktiviert ist, können Administratoren beantragen, dass bestimmte Sicherungen (auch als Sicherungssätze bezeichnet) aus allen Vaults gelöscht werden. Bei der Auswahl der zu löschenden Sicherungen können Administratoren Informationen zu jeder Sicherung anzeigen, darunter das Datum, die Aufbewahrungseinstellungen, die Größe und ob eine mögliche Ransomware-Bedrohung erkannt wurde.

Anforderungen zum Löschen von Sicherungen werden sofort an die Vaults übermittelt und die Daten werden automatisch aus den zugehörigen Vaults gelöscht. Da Anforderungen zum Löschen von Sicherungen sofort übermittelt werden, können Löschanforderungen für Sicherungen nicht storniert werden.

Wenn eine Anforderung zum Löschen von Sicherungen übermittelt wird, wird eine E-Mail-Benachrichtigung an die Administratoren für die Site und an die Superuser gesendet. Eine Benachrichtigung wird auch im Status-Feed angezeigt.

Wenn eine Anforderung zum Löschen von Sicherungen fehlschlägt, wird eine E-Mail-Benachrichtigung an einen Vault-Administrator gesendet, dessen E-Mail-Adresse in Portal angegeben ist. Der Vault-Administrator kann dann die Sicherung oder die Sicherungen manuell aus den Vaults löschen.

WARNUNG: Die Löschung von Sicherungsdaten kann nicht rückgängig gemacht werden. Nachdem die Daten aus den Vaults gelöscht wurden, können sie nicht wiederhergestellt werden.

So löschen Sie spezifische Sicherungen aus Vaults:

1. Melden Sie sich als Administrator an und klicken Sie in der Navigationsleiste auf **Computer**. Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den Computer mit den Sicherungen, die Sie löschen möchten, und erweitern Sie durch Klicken auf seine Zeile seine Ansicht.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Klicken Sie im Menü **Aktion auswählen** des Jobs mit Sicherungen, die Sie löschen möchten, auf **Sicherung löschen**.

Wenn die Option „Sicherung löschen“ nicht angezeigt wird oder eine Meldung angibt, dass der Job in einem Vault registriert ist, der das Löschen von Sicherungen nicht unterstützt, können Sie keine Anforderung zum automatischen Löschen von Sicherungen aus Vaults übermitteln.

Ein Dialogfeld zum Löschen der Sicherung wird angezeigt. Das Dialogfeld zeigt Informationen zu jeder Sicherung an, darunter die Aufbewahrungseinstellungen, die Größe und ob eine

mögliche Ransomware-Bedrohung erkannt wurde. Sicherungen, die nicht gelöscht werden können (z. B. weil für den Job oder Computer eine Löschanforderung geplant ist), können nicht ausgewählt werden.

5. Aktivieren Sie das Kontrollkästchen für jede Sicherung, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Sicherungen, die nicht gelöscht werden können (z. B. weil für den Job oder Computer eine Löschanforderung geplant ist), können nicht ausgewählt werden.

Sie können nicht alle verfügbaren Sicherungen für einen Job löschen. Löschen Sie stattdessen den gesamten Job. Siehe *Löschen von Sicherungsjobs und der zugehörigen Jobdaten aus Vaults* auf Seite [64](#).

WARNUNG: Die Löschung von Sicherungsdaten kann nicht rückgängig gemacht werden. Nachdem die Daten aus den Vaults gelöscht wurden, können sie nicht wiederhergestellt werden.

6. Geben Sie im Bestätigungsdialogfeld im Textfeld **BESTÄTIGEN** ein.

Hinweis: Sie müssen den Text **BESTÄTIGEN** in Großbuchstaben eingeben.

7. Klicken Sie auf **Löschen bestätigen**.

WARNUNG: Die Löschung von Sicherungsdaten kann nicht rückgängig gemacht werden. Nachdem die Daten aus den Vaults gelöscht wurden, können sie nicht wiederhergestellt werden.

Ein Dialogfeld weist darauf hin, dass die Sicherungsdaten aus den Vaults gelöscht werden.

8. Klicken Sie auf **Schließen**.

8 Überwachen von Computern, Jobs und Prozessen

Sie können Sicherungen, Wiederherstellungen und geschützte Computer mit den folgenden Funktionen in Portal überwachen:

- **Aktuelle Momentaufnahme.** Die aktuelle Momentaufnahme gibt die Gesamtzahl der Sicherungen und Computer an Ihrem Standort nach verschiedenen Kategorien geordnet an und ermöglicht Ihnen die Anzeige detaillierter Informationen. Siehe *Überwachen von Sicherungen und Computern mit der aktuellen Momentaufnahme* auf Seite [73](#).
- **Seite „Computer“.** Auf der Seite „Computer“ werden Statusinformationen zu Computern und der zugehörigen Jobs angezeigt. Siehe *Anzeigen von Informationen zu Computer- und Jobstatus* auf Seite [74](#). Zudem können Sie auf dieser Seite auf Protokolle für nicht konfigurierte Computer zugreifen. Siehe *Anzeigen von Protokollen zu nicht konfigurierten Computern* auf Seite [76](#).
- **Dialogfeld „Prozessdetails“.** In diesem Dialogfeld werden Informationen über alle ausgeführten, in der Warteschlange befindlichen und kürzlich abgeschlossenen Prozesse eines Jobs angezeigt. Siehe *Anzeigen von aktuellen Prozessinformationen eines Jobs* auf Seite [77](#).
- **E-Mail-Benachrichtigungen.** Damit Sicherungen leichter überwacht werden können, besteht die Möglichkeit, eine E-Mail zu versenden, sobald die Sicherung abgeschlossen bzw. fehlgeschlagen ist. Siehe *Sicherungen mithilfe von E-Mail-Benachrichtigungen überwachen* auf Seite [79](#).
- **Prozessprotokolle und Informationen aus Sicherungssätzen.** Prozessprotokolle geben an, ob Sicherungen und Wiederherstellungen erfolgreich durchgeführt wurden. Darüber hinaus enthalten sie Informationen über aufgetretene Probleme. Sie können auch Informationen über Sicherungen aus spezifischen Sicherungssätzen anzeigen. Siehe *Anzeigen von Protokollen zu Jobprozessen und Informationen zu Sicherungssätzen* auf Seite [90](#).
- **Seite „Überwachung“.** Auf der Seite „Überwachen“ wird der neueste Sicherungsstatus der einzelnen Jobs angezeigt. Sie haben die Möglichkeit, den Computer und die zugehörigen Jobs zu jeder Sicherung anzuzeigen. Siehe *Anzeigen und Exportieren neuer Sicherungsstatus* auf Seite [91](#).

8.1 Überwachen von Sicherungen und Computern mit der aktuellen Momentaufnahme

In der aktuellen Momentaufnahme auf dem Dashboard können Sie die Gesamtzahl der Sicherungsjobs und Computer auf Ihrer Website in verschiedenen Kategorien anzeigen. Sie können dann von diesen Anzahlen navigieren, um detailliertere Informationen über die Jobs und Computer anzuzeigen.

So überwachen Sie Sicherungen und Computern mit der aktuellen Momentaufnahme:

1. Klicken Sie in der Navigationsleiste auf **Dashboard**.

Die aktuelle Momentaufnahme auf der linken Seite des Dashboards zeigt die Anzahl der Sicherungsjobs und Computer in den folgenden Kategorien an:

- **Sicherungen, die Ihre Aufmerksamkeit erfordern** – Anzahl der Sicherungsjobs, bei denen der letzte Sicherungsversuch fehlgeschlagen ist, mit Fehlern abgeschlossen wurde, keine Dateien gesichert wurden, eine Lizenz einschränkung aufgetreten ist, abgebrochen wurde oder eine mögliche Ransomware-Bedrohung erkannt wurde.

- **Nicht durchgeführte Sicherungen** – Anzahl der Sicherungsjobs, die 7 Tage lang nicht durchgeführt wurden.
 - **Sicherungen mit Warnungen** – Anzahl der Sicherungsjobs, bei denen der letzte Sicherungsversuch mit Warnungen abgeschlossen wurde, zurückgestellt, mit Warnungen zurückgestellt oder übersprungen wurde. Diese Kategorie enthält auch die Sicherungsjobs, die noch nie ausgeführt wurden.
 - **Computer, die einen Neustart erfordern** – Anzahl der Computer, für die ein Neustart aussteht.
 - **Offline-Computer** – Anzahl der Computer, die aktuell nicht mit Portal verbunden sind. Computer können offline sein, wenn sie ausgeschaltet sind, wenn der Agent im System deinstalliert wurde oder das System nicht mehr vorhanden ist.
 - **Zur Löschung geplante Computer** – Anzahl der Computer, die zur Löschung aus dem Portal und aus Vaults vorgesehen sind. Diese Kategorie gilt nur für Portal-Instanzen, in denen die Funktion zum Löschen von Daten aktiviert ist.
 - **TresorComputer mit Zertifikatfehlern** – Anzahl der Computer, die einen Zertifikatfehler in der Vault- oder vSphere-Umgebung melden. Siehe *Beheben von Zertifikatfehlern* auf Seite 44.
 - **Gesamtanzahl Computer** – Gesamtanzahl der Computer auf der Site.
 - **Erfolgreiche Sicherungen** – Anzahl der Sicherungsjobs, bei denen der letzte Sicherungsversuch ohne Fehler, Warnungen oder Zurückstellungen abgeschlossen wurde.
 - **Zur Löschung geplante Jobs** – Anzahl der Jobs, die zur Löschung aus dem Portal und aus Vaults vorgesehen sind. Diese Kategorie gilt nur für Portal-Instanzen, in denen die Funktion zum Löschen von Daten aktiviert ist.
2. Um Computer auf einer bestimmten Site anzuzeigen, klicken Sie auf das Feld „Sites“ oben rechts im Feld „Aktuelle Momentaufnahme“. Suchen Sie im Menü die Site, die Sie anzeigen möchten.

Die Computer auf der ausgewählten Site werden auf der Seite „Computer“ angezeigt.

3. Um Informationen zu Sicherungsjobs oder Computern in einer der Kategorien anzuzeigen, klicken Sie auf die Kategorie.

Wenn Sie auf **Mögliche Bedrohungen, Sicherungen, die Ihre Aufmerksamkeit erfordern, Nicht durchgeführte Sicherungen, Sicherungen mit Warnungen** oder **Erfolgreiche Sicherungen** klicken, werden Sicherungsjobs in der Kategorie auf der Seite „Überwachung“ angezeigt.

Wenn Sie auf **Computer, die einen Neustart erfordern, Offline-Computer, Zur Löschung geplante Computer, Computer mit Zertifikatfehlern** oder **Gesamtanzahl Computer** klicken, werden die Computer der Kategorie auf der Seite „Computer“ angezeigt.

8.2 Anzeigen von Informationen zu Computer- und Jobstatus


Auf der Seite „Computer“ in Portal können Sie Statusinformationen zu Computern und den zugehörigen Jobs anzeigen.

So zeigen Sie Informationen zu Computer- und Jobstatus an:


1. Klicken Sie in der Navigationsleiste auf **Computer**.

Die Seite „Computer“ zeigt registrierte Computer an.

2. Suchen Sie den Computer, für den Sie Statusinformationen anzeigen möchten, und klicken Sie auf die Zeile, um die Ansicht zu erweitern.
3. Klicken Sie auf die Registerkarte **Jobs**.







Wenn eine Sicherung oder Wiederherstellung für einen Job ausgeführt wird, wird neben dem Jobnamen das Symbol „Prozessdetails“  zusammen mit der Anzahl der ausgeführten Prozesse angezeigt.






Name	Jobtyp	Beschreibung
 1 AppAware	Image	
 2 FilesAndFolders	Lokales System	

Wenn eine Rapid VM Restore-Prozess für einen vSphere Recovery Agent-Job (VRA) ausgeführt wird, wird neben dem Jobnamen das Symbol „Rapid VM Restore“  zusammen mit der Anzahl der ausgeführten Rapid VM Restore-Prozesse angezeigt.

Wenn Sie auf das Symbol „Prozessdetails“ bzw. „Rapid VM Restore“ klicken, wird das Dialogfeld „Prozessdetails“ mit Informationen über die Prozesse für den Job geöffnet. Siehe *Anzeigen von aktuellen Prozessinformationen eines Jobs* auf Seite 77.

In der Spalte **Letzter Sicherungsstatus** wird der letzte für jeden Job gemeldete Sicherungsstatus angezeigt. Ein Agent meldet dem Portal jedes Mal einen Sicherungsstatus, wenn er eine Sicherung startet, überspringt oder abschließt. Folgende Status sind möglich:

-  **Abgeschlossen:** Gibt an, dass die letzte Sicherung erfolgreich abgeschlossen und ein Sicherungssatz erstellt wurde.
-  **Mit Warnungen abgeschlossen:** Gibt an, dass die letzte Sicherung abgeschlossen und ein Sicherungssatz erstellt wurde, aber während der Sicherung Probleme aufgetreten sind. Beispiel: Eine Warnung kann angeben, dass eine Datei oder ein Volume, die bzw. das im Sicherungsjob ausgewählt wurde, für die Sicherung nicht verfügbar ist. Eine Warnung kann auch anzeigen, dass ein Ransomware-Scan nicht erfolgreich durchgeführt wurde.
-  **Zurückgestellt:** Gibt an, dass die letzte Sicherung zurückgestellt wurde. Ein Sicherungssatz wurde erstellt; es wurden jedoch nicht alle ausgewählten Daten gesichert. Die Zurückstellung verhindert, dass umfangreiche Sicherungen im Netzwerk zu Spitzenlastzeiten ausgeführt werden. Wenn die Zurückstellung aktiviert ist, werden bei einem Sicherungsjob nach einem bestimmten Zeitraum keine neuen Daten gesichert.
-  **Übersprungen:** Gibt an, dass eine Sicherung übersprungen wurde. Sicherungen werden manchmal übersprungen, wenn sie mehrmals am Tag ausgeführt werden sollen.
-  **Nie ausgeführt:** Gibt an, dass der Sicherungsjob nie ausgeführt wurde.
-  **Nicht ausgeführt:** Gibt an, dass der Job seit 7 Tagen nicht ausgeführt wurde.

-  **Mit Fehlern abgeschlossen:** Gibt an, dass die Sicherung abgeschlossen wurde und ein Sicherungssatz für die Wiederherstellung verfügbar ist, jedoch Probleme aufgetreten sind. In der Regel gibt dieser Status an, dass nicht alle Daten gesichert wurden. Dieser Status kann auch darauf hinweisen, dass eine mögliche Ransomware-Bedrohung erkannt wurde.
-  **Keine Dateien gesichert:** Gibt an, dass während des letzten Sicherungsversuchs keine Dateien gesichert wurden.
-  **Fehlgeschlagen:** Gibt an, dass die Sicherung fehlgeschlagen ist und kein Sicherungssatz erstellt wurde.
-  **Abgebrochen**
-  **Zum Löschen vorgesehen:** Gibt an, dass zu dem in der Spalte „Datum“ angegebenen Datum der Job in Portal und die Jobdaten aus allen Vaults gelöscht werden sollen. Dieser Sicherungsstatus ist nur in Portal-Instanzen möglich, in denen die Funktion zum Löschen von Daten aktiviert ist. Siehe *Löschen von Sicherungsjobs und der zugehörigen Jobdaten aus Vaults* auf Seite 64.

Wenn **Mögliche Bedrohung** nach dem Status in der Spalte „Letzter Sicherungsstatus“ angezeigt wird, wurde während der Ausführung des Sicherungsjobs eine mögliche Ransomware-Bedrohung erkannt. Siehe *Handhaben möglicher Ransomware-Bedrohungen* auf Seite 44.

Um Protokolle zu einem Job anzuzeigen, klicken Sie auf den Jobstatus. Weitere Informationen finden Sie unter *Anzeigen von Protokollen zu Jobprozessen und Informationen zu Sicherungssätzen* auf Seite 90.

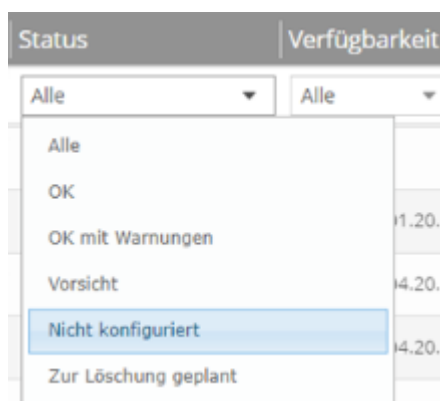
8.3 Anzeigen von Protokollen zu nicht konfigurierten Computern

Sie können Protokolle für nicht konfigurierte Online-Computer anzeigen. Auf nicht konfigurierten Computern befinden sich keine Sicherungsjobs.

So zeigen Sie Protokolle zu nicht konfigurierten Computern an:

1. Klicken Sie in der Navigationsleiste auf **Computer**.

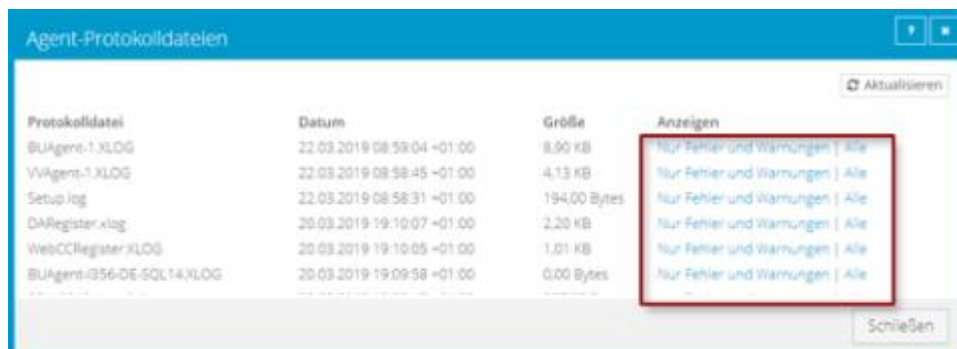
Die Seite „Computer“ zeigt registrierte Computer an. Klicken Sie im Filter **Status** auf „Nicht konfiguriert“, um nur unkonfigurierte Computer anzuzeigen.



2. Suchen Sie den nicht konfigurierten Computer und erweitern Sie die Ansicht durch Klicken auf die jeweilige Computerzeile.

3. Klicken Sie auf den Link **Protokolle** für den unkonfigurierten Computer.

Im Fenster „Agent-Protokolldateien“ wird eine Auflistung der Protokolle für die Computer angezeigt. Rechts im Fenster werden Links zu den Protokollen angezeigt.



Protokolldatei	Datum	Größe	Anzeigen
BUAgent-1.XLOG	22.03.2019 08:59:04 +01:00	8,90 KB	Nur Fehler und Warnungen Alle
VVAgent-1.XLOG	22.03.2019 08:58:45 +01:00	4,13 KB	Nur Fehler und Warnungen Alle
Setup log	22.03.2019 08:58:31 +01:00	194,00 Bytes	Nur Fehler und Warnungen Alle
DARRegister.xlog	20.03.2019 19:10:07 +01:00	2,20 KB	Nur Fehler und Warnungen Alle
WebCCRRegister.XLOG	20.03.2019 19:10:05 +01:00	1,01 KB	Nur Fehler und Warnungen Alle
BUAgent-056-DE-SQL14.XLOG	20.03.2019 19:09:58 +01:00	0,00 Bytes	Nur Fehler und Warnungen Alle

4. Führen Sie eine der folgenden Aktionen aus:

- Wenn im Protokoll nur Fehler und Warnungen angezeigt werden sollen, klicken Sie auf **Fehler und Warnungen**.
- Wenn ein vollständiges Protokoll angezeigt werden soll, wählen Sie **Alle**.



Das Protokoll wird auf einer neuen Registerkarte im Browser angezeigt.

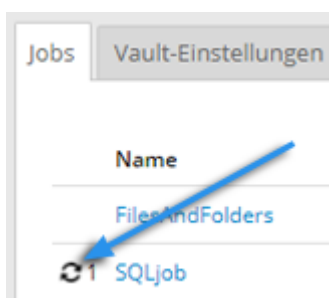
8.4 Anzeigen von aktuellen Prozessinformationen eines Jobs



In Dialogfeld „Prozessdetails“ können Sie Informationen über ausgeführte, in der Warteschlange befindliche und kürzlich abgeschlossene Prozesse eines Jobs anzeigen. Prozesse umfassen Sicherungen, Wiederherstellungen und Synchronisierungen, und werden normalerweise innerhalb von einer Stunde nach Prozessende gelöscht.

Sie können Informationen zu aktiven und kürzlich ausgeführten Rapid VM Restore- und Migrationsprozessen für einen vSphere-Recovery-Agent-Job (VRA) abrufen. Weitere Informationen finden Sie unter *vSphere VM innerhalb von Minuten wiederherstellen mit Rapid VM Restore* auf Seite 50.

So zeigen Sie aktuelle Prozessinformationen eines Jobs an:

1. Führen Sie eine der folgenden Aktionen aus, während eine Sicherung, Wiederherstellung, Synchronisierung oder ein Rapid VM Restore ausgeführt wird:
 - Klicken Sie auf der Seite „Computer“ auf der Registerkarte „Jobs“ auf das Symbol „Prozessdetails“  oder „Rapid VM Restore“  neben dem Jobnamen.



- Klicken Sie auf der Seite „Überwachung“ auf das Symbol „Prozessdetails“  oder „Rapid VM Restore“  neben dem Jobnamen.

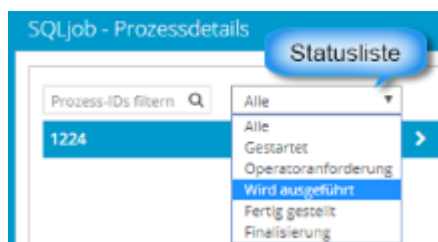


Falls Sie auf eines der „Prozessdetails“-Symbole geklickt haben, wird das Dialogfeld „Prozessdetails“ mit einer Liste der Sicherungs-, Wiederherstellungs- und Synchronisierungsprozesse geöffnet, die für den Job ausgeführt werden, sich in der Warteschlange befinden oder kürzlich abgeschlossen wurden. Links im Dialogfeld werden detaillierte Informationen zum ausgewählten Prozess angezeigt.



Falls Sie auf eines der „Rapid VM Restore“-Symbole geklickt haben, wird das Dialogfeld „Prozessdetails“ mit einer Liste der Rapid VM Restore- und Migrationsprozesse geöffnet, die für den Job ausgeführt werden oder kürzlich abgeschlossen wurden.

2. Um Informationen zu einem anderen Prozess oder Rapid VM Restore anzuzeigen, klicken Sie links im Dialogfeld auf den gewünschten Prozess oder VM-Namen. Rechts im Dialogfeld werden detaillierte Informationen angezeigt.
3. Wenn im Dialogfeld „Prozessdetails“ Sicherungs-, Wiederherstellungs- und Synchronisierungsprozesse für den Job angezeigt werden, können Sie die Statusliste wie folgt nach bestimmten Prozessen filtern:
 - Um nur in der Warteschlange befindliche Prozesse anzuzeigen, klicken Sie auf **Gestartet**.
 - Um nur Prozesse anzuzeigen, die eine Benutzeraktion erfordern, klicken Sie auf **Operatoranforderung**.
 - Um nur Prozesse anzuzeigen, die sich in Bearbeitung befinden, klicken Sie auf **Wird ausgeführt**.
 - Um nur abgeschlossene Prozesse anzuzeigen, klicken Sie auf **Abgeschlossen**.
 - Um nur Prozesse anzuzeigen, die fertig gestellt werden, klicken Sie auf **Finalisierung**.



8.5 Sicherungen mithilfe von E-Mail-Benachrichtigungen überwachen.

Damit Sicherungen leichter überwacht werden können, besteht die Möglichkeit, eine E-Mail zu versenden, sobald die Sicherung abgeschlossen bzw. fehlgeschlagen ist. Administratoren und reguläre Benutzer in Portal können E-Mail-Benachrichtigungen für einen Computer einrichten. Siehe *Einrichten von E-Mail-Benachrichtigungen für Sicherungen auf einem Computer* auf Seite 79.

Wenn E-Mail-Benachrichtigungen zentral in einer Portal-Instanz konfiguriert werden, können Administratoren auch E-Mail-Benachrichtigungen erhalten, wenn sich das Verschlüsselungspasswort für einen Sicherungsjob ändert. Siehe *Einrichten von E-Mail-Benachrichtigungen bei einer Änderung von Verschlüsselungskennwörtern* auf Seite 82.

7.5.1 Einrichten von E-Mail-Benachrichtigungen für Sicherungen auf einem Computer

So richten Sie E-Mail-Benachrichtigungen für einen Computer ein:

1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den Computer, für den Sie E-Mail-Benachrichtigungen konfigurieren möchten, und klicken Sie auf die Computerzeile, um die Ansicht zu erweitern.
3. Klicken Sie in der Registerkarte **Erweitert** auf die Registerkarte **Benachrichtigungen**.
Falls die Registerkarte „Benachrichtigungen“ nicht angezeigt wird, werden die E-Mail-Benachrichtigungen zu den Sicherungen des Computers zentral statt für jeden Computer einzeln konfiguriert. Siehe *Einrichten von E-Mail-Benachrichtigungen für Sicherungen auf mehreren Computern* auf Seite 81.

Hinweis: Wenn E-Mail-Benachrichtigungen für den Computer eingerichtet wurden, bevor E-Mail-Benachrichtigungen in der Portal Instanz aktiviert wurden, kann die Registerkarte „Benachrichtigungen“ für den Computer angezeigt werden.

Wenn die Registerkarte „Benachrichtigungen“ angezeigt wird, dem Computer jedoch eine Richtlinie zugewiesen wurde, können Sie die Werte auf der Registerkarte „Benachrichtigungen“ nicht ändern. In diesem Fall können die Benachrichtigungen nur in der Richtlinie geändert werden.

4. Aktivieren Sie eines oder mehrere der folgenden Kontrollkästchen:

- **Bei Fehlschlagen.** Mit dieser Option erhalten die Benutzer eine E-Mail-Benachrichtigung, wenn eine Sicherung oder Wiederherstellung fehlschlägt. Aus fehlgeschlagenen Sicherungen können keine Dateien wiederhergestellt werden.
- **Bei Fehler.** Mit dieser Option erhalten die Benutzer eine E-Mail-Benachrichtigung, wenn eine Sicherung oder Wiederherstellung mit Fehlern im Protokoll abgeschlossen wird. Dateien mit Fehlern können nicht wiederhergestellt werden. Andere Dateien aus dieser Sicherung (diesem Sicherungssatz) können jedoch wiederhergestellt werden.
- **Bei erfolgreichem Abschluss.** Mit dieser Option erhalten die Benutzer eine E-Mail-Benachrichtigung, wenn eine Sicherung oder Wiederherstellung erfolgreich abgeschlossen wurde. Die Dateien aus abgeschlossenen Sicherungen können wiederhergestellt werden, auch wenn die Protokolldatei Warnungen enthält.

Die E-Mail-Benachrichtigungen werden für jeden Sicherungs- und Wiederherstellungsvorgang separat verschickt. Wenn auf einem Computer beispielsweise drei Sicherungsjobs fehlschlagen und die Option **Bei Ausfall** für den Computer ausgewählt ist, werden drei Benachrichtigungs-E-Mails verschickt.

Geben Sie die folgenden Daten ein, falls die Benutzer E-Mail-Benachrichtigungen nach Sicherungen und Wiederherstellungen erhalten sollen:

E-Mail-Absenderadresse	Die Absenderadresse für die E-Mail-Benachrichtigungen.
Ausgehender Mail-Server (SMTP):	Die Netzwerkadresse des SMTP-Servers, der die E-Mail sendet.
Empfängeradresse(n):	Empfängeradressen für die E-Mail-Benachrichtigungen, mit Kommas getrennt. Geben Sie echte, gültige E-Mail-Adressen ein. Wenn eine oder mehrere Adressen nicht gültig sind, schlägt das Senden an diese Adressen fehl und in den Protokolldateien werden Fehler angezeigt.
Ausgehender Serverport (SMTP):	Die Portnummer für den Versand von E-Mail-Benachrichtigungen.
SMTP-Anmeldeinformationen	SMTP-Benutzername, -Domäne und -Kennwort, falls erforderlich.

5. Klicken Sie auf **Speichern**.

7.5.2 Einrichten von E-Mail-Benachrichtigungen für Sicherungen auf mehreren Computern

Administratoren erhalten in einigen Portal-Instanzen automatisch E-Mail-Benachrichtigungen, wenn Sicherungen fehlschlagen oder abgebrochen, verschoben, nicht ausgeführt, übersprungen oder abgeschlossen werden. Administratoren können die Sicherungsstatus auswählen, für die Sie Benachrichtigungen per E-Mail erhalten möchten.

Wenn E-Mail-Benachrichtigungen zentral in einer Portal-Instanz konfiguriert werden, können zusätzliche E-Mail-Adressen für Benachrichtigungen für jede untergeordnete Site angegeben werden.

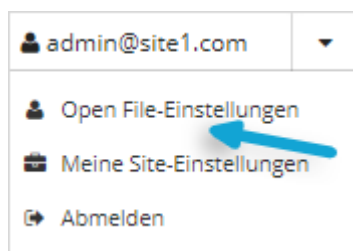
Hinweis: E-Mail-Benachrichtigungen, die in den Profileinstellungen des Administratorbenutzers ausgewählt werden, werden nur auf Englisch gesendet. E-Mail-Benachrichtigungen für E-Mail-Adressen auf untergeordneten Sites werden in mehreren Sprachen unterstützt.

In Portal-Instanzen, bei denen Administratoren nicht automatisch per E-Mail benachrichtigt werden, müssen die Benachrichtigungen separat für jeden Computer konfiguriert werden. Siehe *Einrichten von E-Mail-Benachrichtigungen für Sicherungen auf einem Computer* auf Seite 79.

So richten Sie E-Mail-Benachrichtigungen für Sicherungen auf mehreren Computern ein:

1. Melden Sie sich als Administratorbenutzer an und klicken Sie oben rechts auf der Portal-Seite auf Ihre E-Mail-Adresse.

Das Benutzermenü wird angezeigt.



2. Klicken Sie auf **Profileinstellungen**.

Ihr Benutzerprofil wird angezeigt. Wenn Ihr Profil einen Bereich für E-Mail-Benachrichtigungseinstellungen mit einer Liste von Sicherungsereignissen enthält (z. B. Sicherung abgebrochen, Sicherung abgeschlossen, Sicherung übersprungen), können Sie Ereignisse auswählen, für die Sie E-Mails erhalten möchten.

Falls die E-Mail-Benachrichtigungseinstellungen nicht angezeigt werden, müssen Sie Benachrichtigungen separat auf jedem Computer konfigurieren. Siehe *Einrichten von E-Mail-Benachrichtigungen für Sicherungen auf einem Computer* auf Seite 79.

Wenn die Option zum Ändern von Verschlüsselungskennwörtern angezeigt wird, können Sie festlegen, ob Sie per E-Mail benachrichtigt werden möchten, wenn sich die Verschlüsselungskennwörter auf Ihrer Site ändern.

3. Wählen Sie aus der Auflistung „Benachrichtigungseinstellungen“ die Ereignisse aus, bei denen E-Mails versendet werden sollen:

- Sicherung abgebrochen
- Sicherung abgeschlossen
- Sicherung mit Fehlern abgeschlossen
- Sicherung mit Warnungen abgeschlossen
- Sicherung wird zurückgestellt
- Sicherung fehlgeschlagen
- Sicherung verpasst
- Sicherung übersprungen

Hinweis: Sicherungen werden manchmal übersprungen, wenn sie stündlich oder mehrmals am Tag ausgeführt werden sollen.

4. Klicken Sie auf **Benachrichtigungen aktualisieren**.

7.5.3 Einrichten von E-Mail-Benachrichtigungen bei einer Änderung von Verschlüsselungskennwörtern

In einigen Sites können Administratoren angeben, ob sie darüber informiert werden möchten, wenn die Verschlüsselungskennwörter für einen Job geändert werden.

Administratoren in einer übergeordneten Site können E-Mail-Benachrichtigungen empfangen, wenn sich die Verschlüsselungskennwörter für einen Job in der übergeordneten Site und den zugehörigen untergeordneten Sites ändern. Administratoren in einer untergeordneten Site können E-Mail-Benachrichtigungen empfangen, wenn sich die Verschlüsselungskennwörter für einen Job nur in der untergeordneten Site ändern.

Superuser legen fest, ob Administratoren in einer Site bei einer Änderung von Verschlüsselungskennwörtern eine E-Mail-Benachrichtigung empfangen sollen.

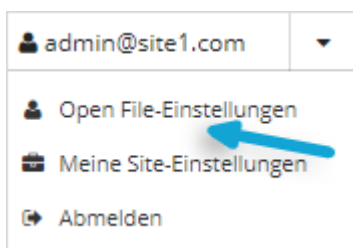
Wenn E-Mail-Benachrichtigungen zentral in einer Portal-Instanz konfiguriert werden, können zusätzliche E-Mail-Adressen für Benachrichtigungen für jede untergeordnete Site angegeben werden.

Hinweis: E-Mail-Benachrichtigungen, die in den Profileinstellungen des Administratorbenutzers ausgewählt werden, werden nur auf Englisch gesendet. E-Mail-Benachrichtigungen für E-Mail-Adressen auf untergeordneten Sites werden in mehreren Sprachen unterstützt.

So richten Sie E-Mail-Benachrichtigungen ein, die bei einer Änderung von Verschlüsselungskennwörtern gesendet werden:

1. Melden Sie sich als Administratorbenutzer an und klicken Sie oben rechts auf der Portal-Seite auf Ihre E-Mail-Adresse.

Das Benutzermenü wird angezeigt.



2. Klicken Sie auf **Profileinstellungen**.

Ihr Benutzerprofil wird angezeigt. Wenn Ihr Profil einen Bereich für E-Mail-Benachrichtigungseinstellungen mit der Option zum Ändern von Verschlüsselungskennwörtern enthält, können Sie angeben, ob sie darüber informiert werden möchten, wenn die Verschlüsselungskennwörter für einen Job geändert werden.

3. Wählen Sie in der Liste „Benachrichtigungseinstellungen“ die Option **Verschlüsselungskennwort geändert** aus.
4. Klicken Sie auf **Benachrichtigungen aktualisieren**.

7.5.4 Einrichten von E-Mail-Benachrichtigungen für mögliche Ransomware-Bedrohungen

Administratoren in einer übergeordneten Site können E-Mails erhalten, wenn mögliche Bedrohungen in der übergeordneten Site und in deren untergeordneten Sites erkannt werden. Administratoren in einer untergeordneten Site können E-Mails erhalten, wenn mögliche Bedrohungen in der untergeordneten Site erkannt werden.

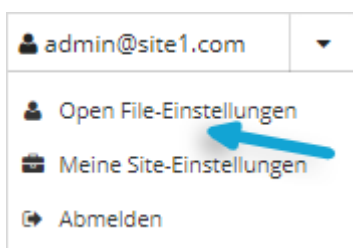
Wenn E-Mail-Benachrichtigungen zentral in einer Portal-Instanz konfiguriert werden, können zusätzliche E-Mail-Adressen für Benachrichtigungen für jede untergeordnete Site angegeben werden.

Hinweis: E-Mail-Benachrichtigungen, die in den Profileinstellungen des Administratorbenutzers ausgewählt werden, werden nur auf Englisch gesendet. E-Mail-Benachrichtigungen für E-Mail-Adressen auf untergeordneten Sites werden in mehreren Sprachen unterstützt.

So richten Sie E-Mail-Benachrichtigungen für mögliche Ransomware-Bedrohungen ein:

1. Melden Sie sich als Administratorbenutzer an und klicken Sie oben rechts auf der Portal-Seite auf Ihre E-Mail-Adresse.

Das Benutzermenü wird angezeigt.



2. Klicken Sie auf **Profileinstellungen**.
3. Wählen Sie in der Liste „Benachrichtigungseinstellungen“ die Option **Mögliche Bedrohungen** aus.

4. Klicken Sie auf **Benachrichtigungen aktualisieren**.

8.6 Anzeige des Sicherungsüberprüfungs-Berichts

Um festzustellen, ob Windows-VMs aus vSphere-Sicherungen wiederhergestellt werden können, können Administratoren und Support-Benutzer den Sicherungsüberprüfungs-Bericht im Portal anzeigen.

Der Bericht zeigt die Ergebnisse von Sicherungsüberprüfungs-Prozessen, die mit vSphere Recovery Agent (VRA) ab Version 9.00 verfügbar sind. Wenn Einstellungen für die Sicherungsüberprüfung für einen VRA eingegeben werden und die Sicherungsüberprüfung für einen vSphere-Sicherungsjob aktiviert ist, sichert der VRA die VMs im Job und prüft dann, ob jede Windows VM aus der Sicherung wiederhergestellt werden kann. Siehe *Sicherungsüberprüfung für vSphere-VMs* auf Seite 34 und *Anforderungen für vSphere Rapid VM Restore und Sicherungsüberprüfung* auf Seite 8.

Der Bericht zeigt nur den letzten Überprüfungsstatus für jede VM in einem Sicherungsjob an. Wenn eine VM in mehreren Sicherungsjobs enthalten ist, bei denen die Überprüfung aktiviert ist, kann die VM mehrfach im Bericht angezeigt werden. Wenn zwei VMs mit demselben Namen gesichert werden, können Sie im Bericht nicht zwischen den beiden VMs unterscheiden.

Hinweis: In vSphere können zwei oder mehr VMs in einer vSphere-Umgebung denselben Namen haben, wenn sich jede VM in einem eigenen Ordner befindet. Wenn mehrere VMs denselben Namen haben, können Sie die VMs weder im Portal noch im Sicherungsüberprüfungs-Bericht voneinander unterscheiden. Erwägen Sie in diesem Fall, die VMs umzubenennen.

So zeigen Sie den Sicherungsüberprüfungs-Bericht an:

1. Melden Sie sich als Administrator- oder Supportbenutzer an und klicken Sie auf der Navigationsleiste auf **Berichte**.

Auf der Seite **Berichte** werden die Standard- und benutzerdefinierten Berichtansichten aufgeführt.

Wenn Sie als Supportbenutzer angemeldet sind, müssen Sie im Support-Dashboard, das auf der Seite „Berichte“ angezeigt wird, eine Site auswählen.

2. Klicken Sie im Sicherungsüberprüfungs-Bericht auf **Tabellenansicht**.

Der Bericht zeigt Windows-VMs in Sicherungsjobs an, bei denen die Sicherungsüberprüfung aktiviert war. Der Site-Name wird in der Spalte „Name“ angezeigt. Wenn eine Site eine übergeordnete Site ist, wird das Symbol für übergeordnete Site (⚡) neben dem Site-Namen angezeigt.

Der Überprüfungsstatus für jede VM zeigt an, ob die VM überprüft wurde und von der Sicherung wiederhergestellt werden kann. Folgende Werte sind möglich:

- **Abgeschlossen:** Die VM wurde überprüft und kann von der Sicherung wiederhergestellt werden.

Um einen Screenshot des Anmeldebildschirms der wiederhergestellten VM anzuzeigen, klicken Sie in der Spalte „Screenshot“ auf **Ansicht**.

- **Erfolglos - Zeitüberschreitung** - Die VM-Sicherung konnte nicht innerhalb von 10 Minuten überprüft werden. Dies kann beispielsweise auftreten, wenn der in den Einstellungen für die VRA-Sicherungsüberprüfung angegebene Host nicht über ausreichend Arbeitsspeicher

oder Speicherplatz verfügt, wenn der Vault stark belastet ist, wenn der Start der VM lange dauert oder wenn die VMware Tools nicht auf der VM installiert sind.

- Erfolglos (siehe Protokolle) - Die VM-Sicherung konnte nicht überprüft werden. Weitere Informationen finden Sie im Sicherungsprotokoll.

Hinweis: In seltenen Fällen wird im Bericht der Status *Nicht geprüft* oder *Unbekannt* angezeigt. Diese Status zeigen auch an, dass die VM-Sicherung nicht überprüft werden konnte.

Wenn die VM-Sicherung nicht überprüft werden konnte, können Sie eine schnelle VM-Wiederherstellung durchführen, um festzustellen, ob die VM wiederhergestellt werden kann. Siehe *vSphere VM innerhalb von Minuten wiederherstellen mit Rapid VM Restore* auf Seite 50.

3. Um bei einer VM mit dem Überprüfungsstatus *Abgeschlossen* einen Screenshot des Anmeldebildschirms der wiederhergestellten VM anzuzeigen, klicken Sie in der Spalte „Screenshot“ auf **Ansicht**.
4. Wenn nur bestimmte Datensätze angezeigt werden sollen, geben Sie Kriterien ein, die die Datensätze erfüllen müssen. Gehen Sie in der Filterzeile unter den Spaltenüberschriften für jede Spalte, in der Sie einen Filter setzen möchten, auf eine der folgenden Weisen vor:
 - Geben Sie in das leere Feld den Text ein, mit dem die Datensätze übereinstimmen müssen.
 - Klicken Sie in der Auflistung auf den Wert, mit dem die Datensätze übereinstimmen müssen.

Datensätze erscheinen nur dann im Bericht, wenn sie alle angegebenen Kriterien erfüllen.

5. Beim Anzeigen des Berichts können Sie eine der folgenden Aktionen ausführen:
 - Exportieren Sie die Berichtsdaten im Adobe Acrobat-Format (.pdf).
 - Versenden Sie die Berichtsdaten per E-Mail an einen oder mehrere Empfänger. Daten können im Adobe Acrobat-Format (.pdf) per E-Mail versendet werden.
 - Erstellen Sie einen Zeitplan für das Versenden des Berichts an einen oder mehrere E-Mail-Empfänger. Daten können im Adobe Acrobat-Format (.pdf) per E-Mail versendet werden.

Hinweis: Sie können den Sicherungsüberprüfungs-Bericht nicht im Format Komma-getrennte Werte (.csv) oder Microsoft Excel (.xls) exportieren oder per E-Mail versenden.

8.7 Zeitliche Planung des täglichen Statusberichts

Der tägliche Statusbericht enthält Informationen zum Sicherungsstatus für die letzten 24 Stunden, einschließlich nicht ausgeführter und übersprungener Sicherungen und laufender Jobs für Computer, auf denen Agent Version 8.0 oder höher installiert ist. Der tägliche Statusbericht zeigt auch an, ob mögliche Ransomware-Bedrohungen während der Sicherungen erkannt wurden. Siehe *Statusbericht für Sicherung* auf Seite 86.

Dieser Bericht kann geplant und per E-Mail an Benutzer gesendet werden. Er kann jedoch nicht in Portal angezeigt werden. Jeder dieser geplanten täglichen Statusberichte wird auf der Seite „Berichte“ unter „Täglicher Statusbericht“ angezeigt.

So planen Sie den täglichen Statusbericht:

1. Melden Sie sich als Administrator- oder Supportbenutzer an und klicken Sie auf der Navigationsleiste auf **Berichte**.

Auf der Seite „Berichte“ werden die verfügbaren Berichte aufgelistet.

Wenn Sie als Supportbenutzer angemeldet sind, wählen Sie im Support-Dashboard, das auf der Seite „Berichte“ angezeigt wird, eine Site aus.

2. Klicken Sie im Bereich „Täglicher Statusbericht“ auf **Neuen Bericht hinzufügen**.
3. Gehen Sie im Dialogfeld „E-Mail/Zeitplan“ wie folgt vor:
 - Geben Sie in das Feld **An** eine oder mehr E-Mail-Adressen ein, die den Bericht per E-Mail erhalten sollen. Trennen Sie mehrere E-Mail-Adressen mithilfe von Kommas voneinander.
 - Geben Sie in das Feld **Betreff** die Überschrift für die Berichts-E-Mail ein.
 - Geben Sie in das Feld **Berichtsname** einen Namen für den geplanten Bericht ein. Dieser Name wird auf der Seite „Berichte“ unter „Täglicher Statusbericht“ angezeigt.
 - Geben Sie im Feld **Um** die Uhrzeit für die Ausführung des Berichts und dessen Versendung per E-Mail für jeden einzelnen Tag an. Klicken Sie in der Liste **Zeitzone** auf die Zeitzone der angegebenen Zeit.
 - Wenn Sie abgeschlossene Sicherungen von dem Bericht ausschließen möchten, aktivieren Sie das Kontrollkästchen **Erfolgreiche Ereignisse ausschließen**.

4. Wenn das Dialogfeld „E-Mail/Zeitplan“ einen Bereich für **Einzuschließende Sites für den Bericht** enthält, führen Sie einen der folgenden Schritte durch:
 - Wenn Sie zusätzlich zu Computern von der übergeordneten Site auch Computer von untergeordneten Sites in den Bericht einschließen möchten, aktivieren Sie das Kontrollkästchen für die entsprechenden untergeordneten Sites.
 - Wenn Sie nur Computer von der übergeordneten Site in den Bericht einschließen möchten, aktivieren Sie keines der Kontrollkästchen für untergeordnete Sites.

5. Klicken Sie auf **OK**.

7.7.1 Statusbericht für Sicherung

Die folgende Tabelle enthält und beschreibt Daten, die für den täglichen Statusbericht verfügbar sind.

Spalte für Daten des täglichen Statusberichts	Beschreibung
Übergeordnete Site	Übergeordnetes Unternehmen oder Dienstleister, der den Agenten besitzt oder verwaltet
Site	Untergeordnetes Unternehmen, das Eigentümer des Agenten ist (falls zutreffend)
Agent	Gesicherter Computer (oder Einheit, auf der die Sicherung ausgeführt wurde)
Job	Sicherungsjob
Ereignisstart	Datum und Uhrzeit des Starts der Sicherung
Ereignisende	Datum und Uhrzeit der Beendigung der Sicherung (sofern zutreffend)
Ereignissicherungssatz	Numerischer Wert des Sicherungssatzes, der bei der Sicherung versucht wurde. Wenn die Sicherung fehlgeschlagen ist, wurde dieser Sicherungssatz nicht in den Vault übertragen, und das nächste Ereignis erhält dieselbe Sicherungssatznummer. Die Sicherungssatznummer wird erst erhöht, wenn eine Sicherung übertragen wurde.
Agent-Typ	Zeigt an, ob die Sicherung geplant oder ad-hoc ausgeführt wurde.

Spalte für Daten des täglichen Statusberichts	Beschreibung
Ereignisstatus	<p>Status des Ereignisses. Folgende Werte sind möglich:</p> <ul style="list-style-type: none">• Abgebrochen – Die Sicherung wurde von einem Benutzer vor Abschluss abgebrochen.• Wird durchgeführt – Die Sicherung wurde beim Ausführen des Berichts ausgeführt.• Abgeschlossen – Die Sicherung wurde gestartet und erfolgreich abgeschlossen.• Mit Warnungen abgeschlossen – Die Sicherung wurde gestartet und mit Warnungen abgeschlossen.• Mit Fehlern abgeschlossen – Die Sicherung wurde gestartet und mit Fehlern abgeschlossen.• Zurückgestellt – Die Sicherung wurde erfolgreich übermittelt, es wurden aber einige Daten zurückgestellt.• Fehlgeschlagen – Die Sicherung wurde zwar gestartet, aber nicht abgeschlossen.• Lizenzobergrenze erreicht – Die Sicherung schlug fehl, weil im Vault keine Lizenzen verfügbar sind.• Keine Dateien gesichert – Die Sicherung schlug fehl, da keine Dateien für die Sicherung verfügbar waren.• Plan ist deaktiviert – Alle Zeitpläne für den Job wurden deaktiviert.• Offline – Der Agent des Jobs war zum Zeitpunkt der Ausführung des Berichts offline.• Nicht durchgeführt – Der Job war geplant, wurde aber nicht gemäß Zeitplan ausgeführt. Dies könnte auftreten, wenn das Agent-System heruntergefahren wurde oder die Sicherungsdienste auf dem Agent gestoppt wurden.• Übersprungen - Für den Job ist eine Ausführung mehrmals am Tag geplant, er wurde aber übersprungen.

Spalte für Daten des täglichen Statusberichts	Beschreibung
Mögliche Bedrohung	<p>Gibt an, ob während der Sicherung eine mögliche Ransomware-Bedrohung erkannt wurde. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • Nicht definiert - Der Agent unterstützt die Bedrohungserkennung nicht. „Nicht definiert“ ist der einzig mögliche Wert für eine mögliche Bedrohung für einen Agenten, der die Erkennung von Ransomware-Bedrohungen nicht unterstützt. • Deaktiviert - Ransomware-Bedrohungserkennung war im Sicherungsjob nicht aktiviert. • Nicht erkannt - Die Erkennung von Ransomware-Bedrohungen wurde im Sicherungsjob aktiviert, aber eine mögliche Ransomware-Bedrohung wurde während der Sicherung nicht erkannt. • Erkannt - Eine mögliche Ransomware-Bedrohung wurde während der Sicherung erkannt. Siehe <i>Handhaben möglicher Ransomware-Bedrohungen</i> auf Seite 44. • Nicht ausgeführt - Die Erkennung von Ransomware-Bedrohungen wurde während der Sicherung nicht durchgeführt, obwohl sie im Sicherungsjob aktiviert war. Dies kann z. B. vorkommen, wenn das Betriebssystem die Erkennung von Bedrohungen nicht unterstützt. Es ist keine weitere Aktion erforderlich. • Fehler - Bei der Erkennung von Ransomware-Bedrohungen während der Sicherung ist ein Fehler aufgetreten. Bitte prüfen Sie die Protokolle auf weitere Informationen und versuchen Sie, das Problem zu beheben. Bei einer vSphere-Sicherung kann ein Fehler auftreten, wenn die angegebenen VM-Anmeldeinformationen nicht korrekt sind, eine VM offline oder nicht ansprechbar ist oder die VMware Tools nicht installiert sind.
Aufbewahrung	Name des für die Sicherung verwendeten Aufbewahrungstyps.
Optionen	<p>Für die Sicherung verwendete Optionen. Dies gilt nur für einige SQL Server- und Exchange-Sicherungstypen.</p> <p>Bei SQL Server gibt dies die Art der Sicherung an: Vollständig, Vollständig mit Transaktionsprotokollen oder nur eine Zuwachssicherung.</p> <p>Bei Exchange gibt dies an, ob es sich um eine vollständige oder inkrementelle Sicherung handelte, sowie, ob die Sicherung auch die Datenbank überprüft hat.</p>
Originalgröße	Gesamtmenge der Quelldaten, die in der Sicherung enthalten waren
Geänderte Größe (Delta)	Anzahl der geänderten Daten, die mit dieser Sicherung gesichert werden
OTW-Datengröße (Komprimiert)	Menge der über das Netzwerk gesendeten Daten


Spalte für Daten des täglichen Statusberichts	Beschreibung
Zurückgestellte Datengröße	Ungefähre Datenmenge, die für die Sicherung ausgewählt wurde, aber nicht innerhalb des definierten Sicherungsfensters abgeschlossen werden konnte und daher auf eine folgende Sicherung verschoben wurde. Dies geschieht in der Regel nur bei der ersten Sicherung oder beim erneuten Seeding eines Jobs, wenn die zu schützende Datenmenge größer ist, als was in einem einzigen Sicherungsfenster verarbeitet und übertragen werden kann.
Status des aktuellsten Jobs	Aktuellster Status des Jobs. Bei Jobs, die mehrmals pro Tag ausgeführt werden, ist dies das aktuellste Ergebnis des Jobs.
Datum der letzten Sicherung	Datum und Uhrzeit des letzten Events für den Job
Datum des letzten übermittelten Sicherungssatzes	Datum und Uhrzeit der letzten abgeschlossenen Sicherung, die ein Sicherungssatz an den Vault übermittelt hat.
Aktueller Sicherungssatz	Numerischer Wert der letzten abgeschlossenen Sicherung, die ein Sicherungssatz an den Vault übermittelt hat.

8.8 Anzeigen von Protokollen zu Jobprozessen und Informationen zu Sicherungssätzen

Mit den Protokollen zu einem Jobprozess können Sie herausfinden, ob eine Sicherung oder eine Wiederherstellung erfolgreich abgeschlossen wurde oder warum ein Prozess fehlgeschlagen ist.

Außerdem können Sie Informationen über Sicherungssätze für einen Job abrufen. Ein Sicherungssatz ist eine Instanz von Sicherungsdaten im Vault.


So können Sie Protokolle zu Jobprozessen und Informationen zu Sicherungssätzen anzeigen:

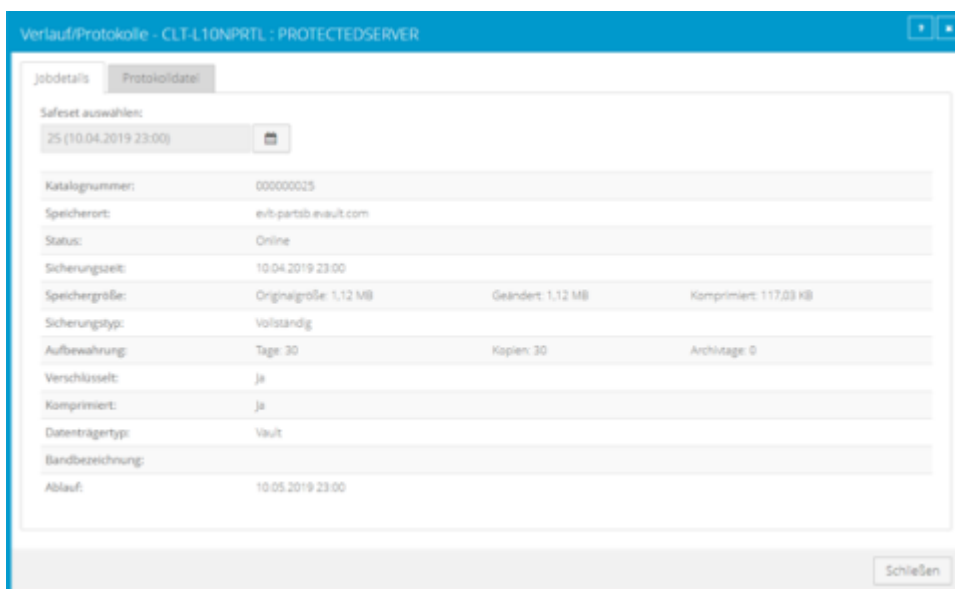
1. Klicken Sie in der Navigationsleiste auf **Computer**.
Die Seite „Computer“ zeigt registrierte Computer an.
2. Suchen Sie den Computer, für den Sie Protokolle anzeigen möchten, und erweitern Sie durch Klicken auf die jeweilige Computerzeile die Ansicht.
Auf der Registerkarte **Jobs** wird in der Spalte **Letzter Sicherungsstatus** der Status jedes Sicherungsjobs angezeigt.
3. Um Protokolldateien für einen Job anzuzeigen, führen Sie eine der folgenden Maßnahmen aus:
 - Klicken Sie in der Spalte **Letzter Sicherungsstatus** auf den Jobstatus.
4. Klicken Sie auf die Kalenderschaltfläche, um Prozesse für einen anderen Tag anzuzeigen. 
Klicken Sie im angezeigten Kalender auf das Datum des Protokolls, das Sie anzeigen möchten.

5. Klicken Sie in der Liste der Prozesse für das ausgewählte Datum auf den Prozess, für den Sie das Protokoll anzeigen möchten.

Das ausgewählte Protokoll wird im Fenster angezeigt.

6. Um Informationen zum Sicherungssatz für eine bestimmte Sicherung anzuzeigen, klicken Sie auf die Registerkarte **Jobdetails**. In der Registerkarte werden Informationen zum Sicherungssatz für die zuletzt ausgeführte Sicherung des Jobs angezeigt.

Klicken Sie auf die Kalenderschaltfläche, um Informationen für einen anderen Sicherungssatz anzuzeigen.  Klicken Sie im angezeigten Kalender auf das Datum der Sicherung, deren Informationen Sie anzeigen möchten. Klicken Sie in der Liste der Sicherungen für das ausgewählte Datum auf die Sicherung, deren Informationen Sie anzeigen möchten. In der Registerkarte werden Informationen zum Sicherungssatz für die ausgewählte Sicherung angezeigt.



8.9 Anzeigen und Exportieren neuer Sicherungsstatus

Sie können neue Sicherungsstatus für Computer in Portal auf der Seite „Überwachung“ anzeigen. Außerdem können Sie die Informationen in kommagetrennten Werten (.csv), im Microsoft Excel-Format (.xls) oder Adobe Acrobat-Format (.pdf) exportieren.

Hinweis: Wir empfehlen die Deaktivierung von Makros in Microsoft Excel bei Verwendung von Portal, insbesondere wenn Sie Informationen im XLS- oder CSV-Format exportieren und diese Berichte in Excel öffnen.

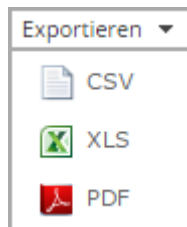
Sie können über die Seite „Überwachung“ zu verwandten Informationen auf der Seite „Computer“ oder im Fenster „Protokolle“ navigieren.

So zeigen Sie neue Sicherungsstatus an und exportieren diese:

1. Klicken Sie in der Navigationsleiste auf **Überwachung**.

Auf der Seite „Überwachung“ werden die letzten Sicherungsstatus für Jobs an Ihrem Standort angezeigt.

2. Um zu ändern, welche Sicherungsstatus auf der Seite angezeigt werden sollen, klicken Sie oben auf der Seite auf die Ansichtenliste und anschließend auf die Ansicht, die Sie anwenden möchten.
3. Um Informationen für einen Job oder Computer auf der Seite „Computer“ anzuzeigen, klicken Sie auf den Namen eines Online-Computers oder Jobs.
4. Um die Protokolle zum Job im Fenster „Verlauf/Protokolle“ anzuzeigen, klicken Sie auf den letzten Sicherungsstatus des Jobs.
5. Um Informationen zum Sicherungsstatus von der Seite zu exportieren, klicken Sie auf das Feld **Exportieren**. Klicken Sie in der angezeigten Liste auf eines der folgenden Formate für die exportierte Datendatei:
 - CSV (kommagetrennte Werte)
 - XLS (Microsoft Excel)
 - PDF (Adobe Acrobat)



Die Datendatei wird im angegebenen Format auf Ihren Computer heruntergeladen.