Linux-Agent und Oracle Plug-in 9.2

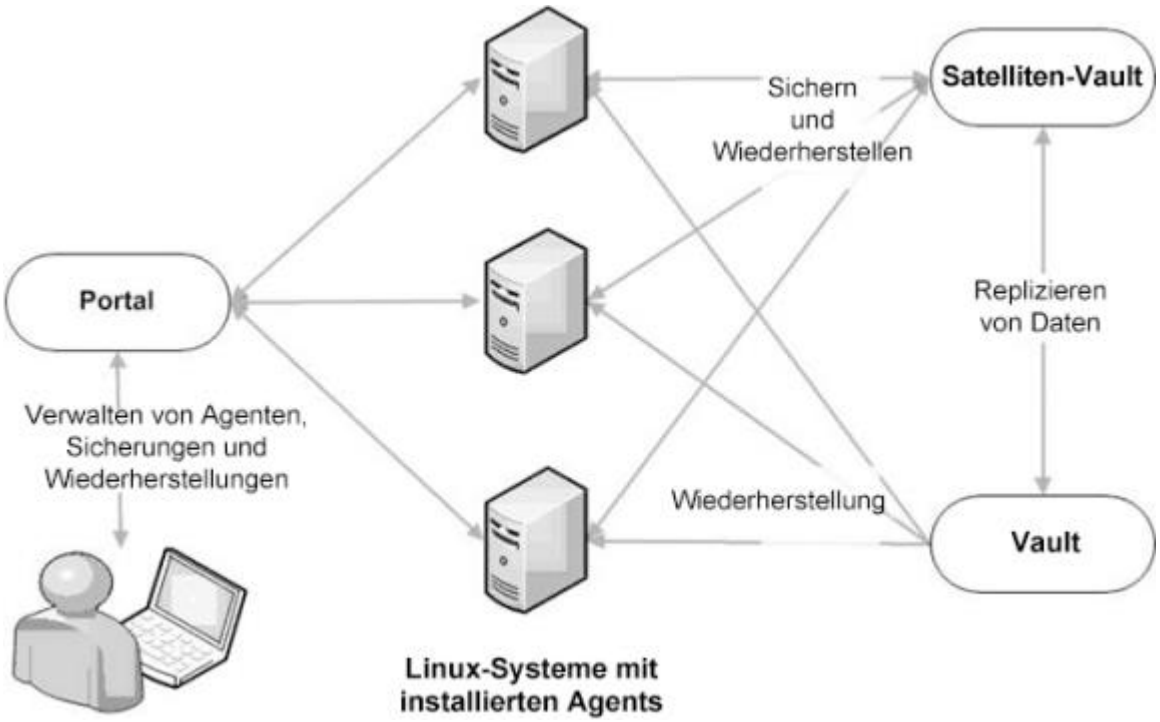
Benutzerhandbuch

Inhalt

1 Einführung in den Linux-Agenten

Der Linux-Agent sichert Daten auf Linux-Systemen und stellt Daten aus den Sicherungen wieder her.

Der Agent wird auf Linux-Systemen installiert, in denen Daten gesichert und wiederhergestellt werden sollen. Wie Sie im folgenden Diagramm sehen, können Sie Portal verwenden, um den Agenten und Jobs zu verwalten, um Daten in einem sicheren Remote-Vault zu sichern und um Daten aus den Sicherungen wiederherzustellen.



Mit dem Linux-Agenten können Sie Folgendes sichern:

- Dateien und Ordner auf einem Linux-System.
- Systemdateien für die Wiederherstellung des Betriebssystems, inklusive Registrierung und Bootdateien.
- Dateien und Ordner, die auf bereitgestellten NFS-Freigaben gespeichert sind.

Ab Linux-Agent 8.90 können Sie eine Sicherung planen, die mehrmals am Tag und sogar stündlich ausgeführt wird, wenn der Agent Daten in einem Vault der Version 8.60 sichert. Um einen Sicherungsjob zu planen, der mehrmals am Tag ausgeführt wird, erstellen Sie ab Portal 8.88 einen tagesinternen Zeitplan. Siehe *Planung eines Sicherungsjobs, der mehrmals am Tag ausgeführt wird* auf Seite 37.

Der Linux-Agent kann Bare Metal Restore (BMR)-Sicherungen zur Wiederherstellung ganzer Linux-Systeme erstellen. Eine Linux-BMR-Sicherung enthält eine ISO-Datei zum Starten des Zielsystems und zum Ausführen der Wiederherstellung sowie eine Sicherung im Vault, die standardmäßig alle Systemdaten enthält. Siehe *Wiederherstellen eines Linux-Systems aus einer BMR-Sicherung* auf Seite 54.

Ein Oracle Plug-in dient zur Sicherung und Wiederherstellung von Oracle-Datenbanken und kann mit dem Linux-Agenten installiert werden. Für das Oracle-Plug-in für Linux steht ein separates Installationskit zur Verfügung.

2 Installieren des Linux-Agenten

Ab Version 9.20 ist der Linux-Agent nur noch als 64-Bit-Anwendung verfügbar; es gibt keine 32-Bit-Version des Agenten mehr. Informationen zu den unterstützten Plattformen und Systemanforderungen finden Sie in den Versionshinweisen zum Linux-Agenten.

Der Linux-Agent kann Bare Metal Restore (BMR)-Sicherungen zur Wiederherstellung ganzer Linux-Systeme erstellen. Eine Linux-BMR-Sicherung enthält eine ISO-Datei zum Starten des Zielsystems und zum Ausführen der Wiederherstellung sowie eine Sicherung im Vault, die standardmäßig alle Systemdaten enthält. Wenn Sie Linux-BMR-Sicherungen aktivieren möchten, muss das Tool Relax-and-Recover auf dem System installiert sein. Siehe *Installieren und Verifizieren von Relax-and-Recover für Linux-BMR-Sicherungen* auf Seite 9. Sie können Linux-BMR-Sicherungen aktivieren, wenn Sie den Agenten installieren oder nachdem der Agent installiert wurde. Siehe *Registrieren des Linux-Agenten mit Relax-and-Recover und Aktivieren von BMR-Sicherungen* auf Seite 12.

Hinweis: Beim Installationsprozess des Linux-Agenten wird Relax-and-Recover für die Verwendung mit dem Agenten konfiguriert. Wenn Relax-and-Recover auf dem Server für andere Verwendungszwecke installiert ist, können Sie eine zweite Kopie des Tools an einem anderen Ort installieren, um ein Überschreiben Ihrer Einstellungen zu vermeiden. Geben Sie bei der Installation des Linux-Agenten den Relax-and-Recover-Speicherort an, den der Agent verwenden soll.

Das Installationskit des Linux-Agenten wird als Datei tar.gz bereitgestellt. Entpacken Sie diese Datei nur auf dem Rechner, auf dem er installiert wird. Wenn Sie die Datei auf einem anderen Rechner entpacken, kann das unvorhersehbare Ergebnisse zur Folge haben.

Für die Installation des Linux-Agenten sind Root-Privilegien für das Zielsystem erforderlich.

Das Installationsprogramm überprüft, ob ausreichend Speicherplatz für die Installation zur Verfügung steht. Wenn der verfügbare Speicherplatz nicht ausreicht, wird das Installationsverzeichnis im Originalzustand wiederhergestellt.

So installieren Sie den Linux-Agenten:

1. Wenn Sie die Unterstützung für BMR-Sicherungen aktivieren möchten, muss die richtige Version des Tools Relax-and-Recover auf dem Linux-System installiert sein. Siehe *Installieren und Verifizieren von Relax-and-Recover für Linux-BMR-Sicherungen* auf Seite 9.
2. Laden Sie das Installationspaket zum Linux-Agenten (tar.gz) auf dem Rechner herunter, auf dem Sie den Agenten installieren möchten.
3. Führen Sie den folgenden Befehl aus, um die Dateien aus dem Installationspaket zu extrahieren:

   ```
   tar -zxf packageName.tar.gz
   ```

   packageName ist der Name des Installationskits für den Agenten.
4. Führen Sie den folgenden Befehl aus, um das Verzeichnis für das Installationskit des Agenten zu ändern:

   ```
   cd packageName
   ```

5. Führen Sie den folgenden Befehl aus, um die Installation zu starten:

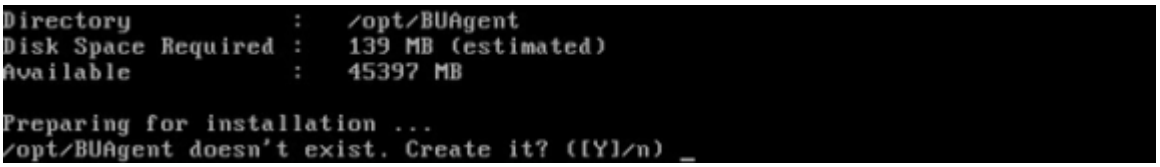
   ```
   ./install.sh
   ```

Eine Liste der verfügbaren Befehle finden Sie unter *Installieren oder Aktualisieren des Linux-Agenten im unbeaufsichtigten Modus* auf Seite 10.

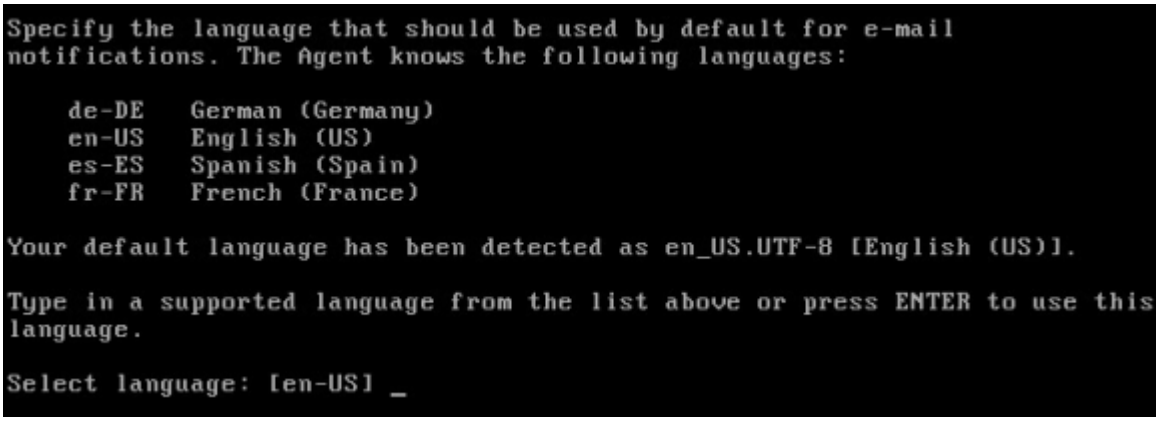
6. Drücken Sie die **Eingabetaste**, um die Softwarelizenzvereinbarung zu lesen. Wenn Sie die Vereinbarung akzeptieren, geben Sie **Y** ein.

7. Führen Sie in der Eingabeaufforderung des Installationsverzeichnisses eine der folgenden Aktionen aus:
   - Drücken Sie die **Eingabetaste**, um das Standardinstallationsverzeichnis (/opt/BUAgent) zu akzeptieren.
   - Geben Sie ein Installationsverzeichnis an und drücken Sie die **Eingabetaste**.

   Verzeichnis, erforderlicher Speicherplatz und verfügbarer Speicherplatz werden angezeigt.



8. Geben Sie **Y** ein, um das Verzeichnis „BUAgent“ zu erstellen.
9. Wenn Sie aufgefordert werden, die Sprache auszuwählen, geben Sie die Sprache ein, in der die Meldungen des Agenten angezeigt werden sollen. Die Standardeinstellung ist Englisch [en-US].

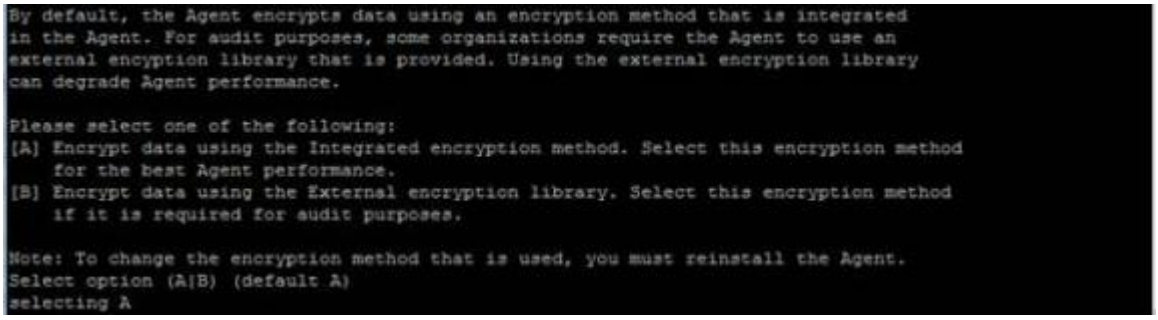


Anschließend werden Sie dazu aufgefordert, die Datenverschlüsselungsmethode auszuwählen.

Der Agent verschlüsselt die ruhenden Daten standardmäßig mithilfe der Verschlüsselungsmethode, die im Agenten integriert ist. In manchen Organisationen ist es erforderlich, dass der Agent zu Auditingzwecken die externe Verschlüsselungsbibliothek verwendet, die zusammen mit dem

Agenten bereitgestellt wird. Wenn eine externe Verschlüsselungsbibliothek verwendet wird, kann die Leistung des Agenten beeinträchtigt werden.

WICHTIG: Der Agent kann nur mit der vom Agent bereitgestellten externen Verschlüsselungsbibliothek verwendet werden. Es wurden keine anderen Verschlüsselungsbibliotheken getestet.



10. Führen Sie eine der folgenden Aktionen aus:
    - Geben Sie **A** ein, wenn Sie die integrierte Verschlüsselungsmethode verwenden möchten. Dies ist der Standardwert.
    - Geben Sie **B** ein, wenn Sie die mit dem Agenten bereitgestellte externe Verschlüsselungsbibliothek verwenden möchten.
11. Führen Sie in der Eingabeaufforderung für BMR-Sicherungen eine der folgenden Aktionen aus:
    - Um BMR-Sicherungen zu aktivieren, geben Sie **J** ein. Geben Sie den Pfad zum Relax-and-Recover-Tool ein, wenn Sie dazu aufgefordert werden.

      Standardmäßig ist das Tool im Verzeichnis „/usr/sbin/rear“ installiert. Das Relax-and-Recover-Tool muss bereits auf dem Linux-Server installiert sein. Siehe *Installieren und Verifizieren von Relax-and-Recover für Linux-BMR-Sicherungen* auf Seite 9.
    - Wenn Sie keine BMR-Sicherungen aktivieren möchten, geben Sie **N** ein.
12. Wenn Sie aufgefordert werden, sich bei Portal anzumelden, geben Sie **Y** ein.
13. Wenn Sie zur Eingabe der Portal-Adresse aufgefordert werden, geben Sie den Hostnamen von Portal oder die IPV4-Adresse 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.
14. Wenn Sie zur Eingabe des Portal-Verbindungsports aufgefordert werden, geben Sie den Verbindungsport ein. Der Standardwert ist 8086.
15. Sie werden zur Eingabe des Benutzernamens für das Portal aufgefordert. Geben Sie den Portalbenutzernamen ein, den Sie zur Registrierung des Agenten verwenden möchten.
16. Wenn Sie zur Eingabe des Kennworts für Portal aufgefordert werden, geben Sie das Kennwort für den im vorherigen Schritt angegebenen Portal-Benutzer ein.

Die Installation wird fortgesetzt. Nach Abschluss der Installation wird eine entsprechende Meldung angezeigt, und der Agent wird gestartet.

Das Installationsprotokoll (Install.log) befindet sich im Installationsverzeichnis.

2.1 Installieren und Verifizieren von Relax-and-Recover für Linux-BMR-Sicherungen

Der Linux-Agent kann Bare Metal Restore (BMR)-Sicherungen zur Wiederherstellung ganzer Linux-Systeme erstellen.

Für BMR-Sicherungen mit dem Linux-Agenten muss Relax-and-Recover (rear) Version 2.6 auf dem Linux-System installiert sein. In diesem Abschnitt wird die Installation und die Verifizierung der Installation dieses Open-Source-Tools beschrieben. Weitere Informationen finden Sie auf der Relax-and-Recover-Website: http://relax-and-recover.org/

Hinweis: Für BMR-Sicherungen mit dem Linux-Agenten 8.83 war die Relax-and-Recover Version 2.5 erforderlich. Vor einem Upgrade des Linux-Agenten von Version 8.83 auf Version wird empfohlen, wie hier beschrieben die Relax-and-Recover Version 2.5 zu deinstallieren und eine Neuinstallation der Relax-and-Recover Version 2.6 durchzuführen.

Wenn Relax-and-Recover auf einem Linux-System installiert ist, können Sie BMR-Sicherungen aktivieren, wenn Sie den Agenten installieren. Siehe *Installieren des Linux-Agenten* auf Seite 6. Sie können BMR-Sicherungen auch aktivieren, indem Sie ein Skript ausführen, nachdem der Agent installiert wurde. Die Ausführung dieses Skripts ist auch erforderlich, wenn Sie Relax-and-Recover neu installieren oder den Installationspfad ändern, nachdem Sie BMR-Sicherungen mit dem Linux-Agenten aktiviert haben. Siehe *Registrieren des Linux-Agenten mit Relax-and-Recover und Aktivieren von BMR-Sicherungen* auf Seite 12.

Wenn Sie BMR-Sicherungen für den Linux-Agenten aktivieren, wird Relax-and-Recover für die Verwendung mit dem Agenten konfiguriert. Wenn Relax-and-Recover auf einem Server für andere Verwendungszwecke installiert ist, können Sie eine zweite Kopie des Tools an einem anderen Ort installieren, um ein Überschreiben der vorhandenen Einstellungen zu vermeiden. Geben Sie bei der Installation des Linux-Agenten den Relax-and-Recover-Speicherort an, den der Agent verwenden soll.

Wenn Sie Relax-and-Recover deinstallieren, nachdem Sie BMR-Sicherungen für einen Linux-Agenten aktiviert haben, werden Nicht-BMR-Sicherungen weiterhin erstellt.

So installieren und verifizieren Sie Relax-and-Recover für Linux-BMR-Sicherungen:

1. Stellen Sie sicher, dass die folgenden für Relax-and-Recover erforderlichen Komponenten auf dem Linux-System installiert sind:
   - bash
   - mkisofs oder genisoimage
   - mingetty

   Auf der Relax-and-Recover-Website werden auch nfs-utils und cifs-utils als Anforderungen aufgeführt. Diese Pakete sind nicht für die Verwendung mit dem Linux-Agenten erforderlich.

   Hinweis: Einige Linux-Distributionen können zusätzliche Anforderungen aufweisen (z. B. binutils und isolinux für Ubuntu 18.04). Alle fehlenden Pakete werden in Schritt 6 dieses Verfahrens identifiziert.
2. Wenn Relax-and-Recover Version 2.5 auf dem System zur Verwendung mit dem Linux-Agenten 8.83 installiert ist, sichern Sie alle für Relax-and-Recover angepassten Dateien und deinstallieren Sie anschließend die Relax-and-Recover Version 2.5.
3. Laden Sie Relax-and-Recover herunter und installieren Sie es gemäß den Anweisungen auf der Relax-and-Recover-Website: http://relax-and-recover.org/documentation/installation

4. Wechseln Sie in den Ordner, in dem Relax-and-Recover (rear) installiert ist (standardmäßig /usr/sbin/rear). Überprüfen Sie die installierte rear-Version, indem Sie den folgenden Befehl ausführen:
   ```
   rear -V
   ```
   Wenn eine frühere Relax-and-Recover Version als 2.6 installiert ist, rufen Sie die Downloadseite für Relax-and-Recover auf und laden Sie die stabile Version 2.6 oder höher von Relax-and-Recover herunter. Installieren Sie die Relax-and-Recover Version 2.6 und stellen Sie sicher, dass sie durch erneutes Ausführen des Befehls `rear -V` installiert wird.
5. Wenn Sie angepasste Dateien für Relax-and-Recover in Schritt 2 dieses Verfahrens gesichert haben, stellen Sie diese angepassten Dateien wieder her.
6. Vergewissern Sie sich, dass die Installation erfolgreich war, indem Sie den folgenden Befehl ausführen:
   ```
   rear -D -v mkrescue
   ```
   Wenn die Installation erfolgreich war, wird eine ISO-Wiederherstellungsdatei unter /var/lib/rear/output erstellt.

   Wenn keine ISO-Wiederherstellungsdatei erstellt wurde, überprüfen Sie im Protokoll, ob eine Abhängigkeit fehlt. Standardmäßig befindet sich das Protokoll im Verzeichnis „/var/log/rear“. Gehen Sie zur Seite http://relax-and-recover.org/support/, um Support zu erhalten.

2.2 Installieren oder Aktualisieren des Linux-Agenten im unbeaufsichtigten Modus

Führen Sie den folgenden Befehl im Verzeichnis aus, in dem sich das Installationskit befindet, um den Linux-Agenten im unbeaufsichtigten Modus zu installieren oder zu aktualisieren:

```
install.sh [Optionen]
```

Wobei *Optionen* optionale Parameter für die Ausführung des Installationskits im unbeaufsichtigten Modus sind. Eine Liste der verfügbaren Parameter finden Sie unter *Installationsparameter für den Linux-Agenten* auf Seite 10.

Installationsparameter für den Linux-Agenten

Parameter	Beschreibung
`-shutdown | -s`	Erzwingt ein Herunterfahren des Agenten, wenn dieser läuft.
`-force | -F`	Erzwingt die Installation; überspringt die anfängliche Prüfung auf freien Speicherplatz.
`-defaults | -D`	Verwendet die Standardwerte für die Installation.
`-force-defaults`	Erzwingt die Installation mit den Standardwerten (nimmt -s und -F an).
`-web-registration=off -W-`	Deaktiviert die Portal-Registrierung.

Parameter	Beschreibung
`-web-registration=`*`file`* `-W=`*`file`*	Versucht eine Registrierung in Portal mit den in der *Datei* gefundenen Werten. Siehe *Registrierungsoptionen für den Linux-Agenten* auf Seite 11.
`-quiet | -Q`	Automatische Installation, gibt keine Ausgaben auf dem Bildschirm aus. Wenn Benutzerinteraktionen im automatischen Modus erforderlich sind, schlägt die Installation fehl, wenn „-force-defaults“ nicht angegeben ist.
`-log=`*`NAME`* `|` `-L=`*`NAME`*	Schreibt das Installationsprotokoll in die angegebene Datei *NAME*.
`-lang=`*`NAME`* `|` `-l=`*`NAME`*	Wählt *NAME* als Sprache aus. Muss mit einem ISO-Sprachcode beginnen. Kann optional ergänzt werden um einen Bindestrich oder Unterstrich und einem ISO-Ländercode (z. B. sind fr, fr-FR und fr_FR möglich). Zeichensatzmarkierungen (z. B. UTF-8) werden ignoriert. Sprachen, die nicht gefunden werden, führen zu einem Fehler, und die Sprache wird auf den Standard en-US [Englisch (US)] gesetzt. Wenn nicht angegeben, wird auf die Sprache anhand Ihres Systemwerts für „en_US.UTF-8“ geschlossen.
`-backup=`*`DIR`* `|` `-B=`*`DIR`*	Sichert die aktuelle Installation des Agenten in das angegebene Verzeichnis.
`-verify | -V`	Überprüft die Integrität des Installationskits.
`-enable-bmr=Y` `-rear-path=[`*`path`*`]`	Aktiviert die Unterstützung für Bare Metal Restore (BMR)-Sicherungsjobs. *path* gibt den Speicherort des Relax-and-Recover-Tools, das der Agent verwenden soll (z. B. /user/sbin/rear), um eine ISO-Datei zur Wiederherstellung des Systems zu erstellen. Das Relax-and-Recover-Tool (https://relax-and-recover.org/) muss auf dem Linux-System installiert sein, bevor Sie den Agenten installieren. Siehe *Installieren und Verifizieren von Relax-and-Recover für Linux-BMR-Sicherungen* auf Seite 9. *Hinweis:* Wenn Sie den Linux-Agenten installieren, wird das Relax-and-Recover-Tool für die Verwendung mit dem Linux-Agenten konfiguriert. Wenn Sie das Relax-and-Recover-Tool für andere Zwecke verwenden, können Sie das Überschreiben Ihrer Einstellungen des Relax-and-Recover-Tools vermeiden, indem Sie eine zweite Kopie des Tools an einem anderen Ort installieren.
`-enable-bmr=N`	Deaktiviert die Unterstützung für Bare Metal Restore (BMR)-Sicherungsjobs. *Hinweis:* Wenn Sie den Parameter „-enable-bmr=Y -rear-path=*[path*]“ nicht angeben, ist „-enable-bmr=N“ der Standardwert.
`-help`	Zeigt „install.sh“-Befehle an.

Registrierungsoptionen für den Linux-Agenten

Für den Befehl „-web-registration=*FILE*“ können Sie eine separate Datei erstellen, die folgende Werte als Antworten bereitstellt:

`wccAddress=`*`ADDRESS_OF_AMP_SERVER`*

```
wccPort=PORT_OF_AMP_SERVER # Defaults to 8086
```

```
wccLogin=PortalUserName
```

```
wccPassword=PortalPassword
```

Verwenden Sie in den Zeilen für die Adresse (address), den Port (port), den Anmeldenamen (login) und das Kennwort (password) die Angaben, die Ihnen der Administrator zur Verfügung gestellt hat.

Hinweis: Dieser Befehl kann nur während der Installation angewendet werden. Er kann mit dem Skript install.sh, nicht jedoch mit dem Skript register verwendet werden.

2.3 Registrieren des Linux-Agenten mit Relax-and-Recover und Aktivieren von BMR-Sicherungen

Das Relax-and-Recover-Tool muss auf dem Linux-System installiert sein, bevor Sie BMR-Sicherungen aktivieren können. Siehe *Installieren und Verifizieren von Relax-and-Recover für Linux-BMR-Sicherungen* auf Seite 9. Sie können anschließend Linux-BMR-Sicherungen aktivieren, wenn Sie den Agenten installieren. Siehe *Installieren des Linux-Agenten* auf Seite 6.

Sobald der Linux-Agent installiert wurde, können Sie Linux-BMR-Sicherungen mit diesem Verfahren aktivieren. Sie müssen dieses Verfahren auch befolgen, wenn Sie das Relax-and-Recover-Tool neu installieren oder den Installationspfad ändern, nachdem Sie Linux-BMR-Sicherungen aktiviert haben.

Sie können Linux-BMR-Sicherungen auf einem Agenten, auf dem sie aktiviert sind, deaktivieren. Siehe *Deaktivieren von BMR-Sicherungen* auf Seite 12.

So registrieren Sie den Linux-Agenten mit Relax-and-Recover und aktivieren BMR-Sicherungen:

1. Führen Sie im Installationsverzeichnis des Agenten (standardmäßig /opt/BUAgent) den folgenden Befehl aus:

   ```
   ./bmrregister
   ```

2. Geben Sie in der Eingabeaufforderung zum Aktivieren der Bare-Metal-Wiederherstellung **Y** ein.
3. Geben Sie den Pfad zum Relax-and-Recover-Tool ein, wenn Sie dazu aufgefordert werden.

   Standardmäßig ist das Tool im Verzeichnis „/usr/sbin/rear“ installiert. Das Relax-and-Recover-Tool muss bereits auf dem Linux-Server installiert sein. Siehe *Installieren und Verifizieren von Relax-and-Recover für Linux-BMR-Sicherungen* auf Seite 9.

1.3.1 Deaktivieren von BMR-Sicherungen

Sie können Linux-BMR-Sicherungen auf einem Linux-Agenten, auf dem sie aktiviert sind, deaktivieren.

Informationen zum Aktivieren von Linux-BMR-Sicherungen finden Sie unter *Registrieren des Linux-Agenten mit Relax-and-Recover und Aktivieren von BMR-Sicherungen* auf Seite 12.

So deaktivieren Sie Linux-BMR-Sicherungen:

1. Führen Sie im Installationsverzeichnis des Agenten (standardmäßig /opt/BUAgent) den folgenden Befehl aus:

   ```
   ./bmrregister
   ```

2. Geben Sie in der Eingabeaufforderung zum Aktivieren der Bare-Metal-Wiederherstellung **N** ein.

2.4 Aktualisieren des Linux-Agenten

Sie können einen Linux-Agenten aktualisieren, indem Sie das Installationskit für den Agenten manuell ausführen. Stellen Sie vor dem Upgrade des Agenten sicher, dass Ihr System die Mindestanforderungen für die neue Agenten-Version erfüllt, wie in den Linux-Agenten-Versionshinweisen beschrieben.

Geben Sie während des Upgrades das Installationsverzeichnis des Linux-Agenten an, der derzeit installiert ist. Andernfalls wird das Upgrade wie bei einer Neuinstallation fortgesetzt.

Für BMR-Sicherungen mit dem Linux-Agenten 8.83 war die Relax-and-Recover Version 2.5 erforderlich. Vor einem Upgrade des Linux-Agenten von Version 8.83 auf Version wird empfohlen, die Relax-and-Recover-Version 2.5 zu deinstallieren und eine Neuinstallation der Relax-and-Recover-Version 2.6 durchzuführen. Siehe *Installieren und Verifizieren von Relax-and-Recover für Linux-BMR-Sicherungen* auf Seite 9.

Hinweis: Wenn Sie Linux-BMR-Sicherungen aktivieren, wird Relax-and-Recover für die Verwendung mit dem Agenten konfiguriert. Wenn Sie Relax-and-Recover für andere Zwecke verwenden, können Sie das Überschreiben Ihrer Einstellungen vermeiden, indem Sie eine zweite Kopie des Tools an einem anderen Ort installieren. Wenn Sie ein Upgrade für den Agenten durchführen, werden Sie aufgefordert, den Speicherort des Tools einzugeben, das der Agent verwenden soll.

Hinweis: Nach dem Upgrade des Agenten wird empfohlen, die einzelnen Sicherungsjobs des Agenten auszuführen. So kann der Agent neue Konfigurationsinformationen in den Vault hochladen.

So aktualisieren Sie den Linux-Agenten:

1. Laden Sie das Installationskit zum Linux-Agenten (tar.gz) auf dem Rechner herunter, auf dem Sie den Agenten installieren möchten.
2. Führen Sie den folgenden Befehl aus, um die Dateien aus dem Installationspaket zu extrahieren:

   ```
   tar -zxf packageName.tar.gz
   ```

   packageName ist der Name des Installationskits für den Agenten.

3. Führen Sie den folgenden Befehl aus, um das Verzeichnis für das Installationskit des Agenten zu ändern:

   ```
   cd packageName
   ```

4. Führen Sie den folgenden Befehl aus, um das Upgrade zu starten:

   ```
   ./install.sh
   ```

5. Drücken Sie die Eingabetaste, um die Softwarelizenzvereinbarung zu lesen. Wenn Sie die Vereinbarung akzeptieren, geben Sie **Y** ein.

6. Wenn eine Meldung erscheint, dass VVAgent ausgeführt wird, geben Sie **Y** ein, um den Agenten zu stoppen.
7. Geben Sie in der Eingabeaufforderung des Installationsverzeichnisses das Installationsverzeichnis des Agenten ein. Das Standardinstallationsverzeichnis für den Agenten ist /opt/BUAgent.

   WICHTIG: Geben Sie das Installationsverzeichnis des Linux-Agenten an, der derzeit installiert ist. Andernfalls wird das Upgrade wie bei einer Neuinstallation fortgesetzt.
8. Wenn Sie aufgefordert werden, die Sprache auszuwählen, geben Sie die Sprache ein, in der die Meldungen des Agenten angezeigt werden sollen. Die Standardeinstellung ist Englisch [en-US].
9. Führen Sie, wenn Sie aufgefordert werden, eine Verschlüsselungsoption auszuwählen, eine der folgenden Aktionen aus:
   - Geben Sie **A** ein, wenn Sie die integrierte Verschlüsselungsmethode verwenden möchten. Dies ist der Standardwert.
   - Geben Sie **B** ein, wenn Sie die mit dem Agenten bereitgestellte externe Verschlüsselungsbibliothek verwenden möchten.

   Der Agent verschlüsselt die ruhenden Daten standardmäßig mithilfe der Verschlüsselungsmethode, die im Agenten integriert ist. In manchen Organisationen ist es erforderlich, dass der Agent zu Auditingzwecken die externe Verschlüsselungsbibliothek verwendet, die zusammen mit dem Agenten bereitgestellt wird. Wenn eine externe Verschlüsselungsbibliothek verwendet wird, kann die Leistung des Agenten beeinträchtigt werden.

   WICHTIG: Der Agent kann nur mit der vom Agent bereitgestellten externen Verschlüsselungsbibliothek verwendet werden. Es wurden keine anderen Verschlüsselungsbibliotheken getestet.
10. Führen Sie in der Eingabeaufforderung für BMR-Sicherungen eine der folgenden Aktionen aus:
    - Um BMR-Sicherungen zu aktivieren, geben Sie **J** ein. Geben Sie den Pfad zum Relax-and-Recover-Tool ein, wenn Sie dazu aufgefordert werden. Das Standardinstallationsverzeichnis lautet /usr/sbin/rear.

      Das Relax-and-Recover-Tool muss bereits auf dem Linux-Server installiert sein. Siehe *Installieren und Verifizieren von Relax-and-Recover für Linux-BMR-Sicherungen* auf Seite 9.
    - Wenn Sie BMR-Sicherungen nicht aktivieren möchten, geben Sie **N** ein.
11. Wenn eine Meldung angezeigt wird, dass Sie bereits in Portal registriert sind, und Sie gefragt werden, ob Sie sich als neuer Computer registrieren möchten, führen Sie einen der folgenden Schritte aus:
    - Um die Portal-Registrierung zu ändern, geben Sie **Y** und dann die neuen Portal-Informationen ein.
    - Um dieselbe Portal-Registrierung beizubehalten, geben Sie **N** ein.

Das Upgrade wird fortgesetzt. Nach Abschluss der Installation wird eine entsprechende Meldung angezeigt und der Agent wird gestartet.

2.5 Ändern der Portalregistrierung für einen Linux-Agenten

Wenn Sie einen Linux-Agenten installieren, können Sie den Agenten beim Portal registrieren. Sie können die Portalregistrierung jederzeit ändern.

Der Agent wird neu gestartet, wenn Sie die Portalregistrierung ändern.

So ändern Sie die Portalregistrierung für einen Linux-Agenten:

1. Führen Sie in dem Verzeichnis, in dem der Agent installiert ist, den folgenden Befehl aus:

   ```
   ./register
   ```

2. Geben Sie **Y** ein, wenn Sie dazu aufgefordert werden, eine Registrierung als neuen Computer vorzunehmen.
3. Wenn Sie zur Registrierung beim webbasierten Agent Console-Server aufgefordert werden, geben Sie **Y** ein.
4. Wenn Sie zur Eingabe der Portal-Adresse aufgefordert werden, geben Sie den Hostnamen von Portal oder die IPV4-Adresse 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.
5. Wenn Sie zur Eingabe des Portal-Verbindungsports aufgefordert werden, geben Sie den Verbindungsport ein. Der Standardwert ist 8086.
6. Sie werden zur Eingabe des Benutzernamens für das Portal aufgefordert. Geben Sie den Portalbenutzernamen ein, den Sie zur Registrierung des Agenten verwenden möchten.
7. Wenn Sie zur Eingabe des Kennworts für Portal aufgefordert werden, geben Sie das Kennwort für den im vorherigen Schritt angegebenen Portal-Benutzer ein.

Der Agent wird neu gestartet und die Portal-Registrierung wird geändert.

2.6 Deinstallieren des Linux-Agenten

So deinstallieren Sie den Linux-Agenten:

1. Führen Sie in dem Verzeichnis, in dem der Agent installiert ist, den folgenden Befehl aus:

   ```
   ./uninstall.sh
   ```

   Das Standardinstallationsverzeichnis für den Agenten ist /opt/BUAgent.
2. Wenn eine Meldung erscheint, dass VVAgent ausgeführt wird, geben Sie **Y** ein, um den Agenten zu stoppen.
3. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **Y** ein.

3 Konfigurieren des Linux-Agenten

Nachdem Sie einen Linux-Agenten installiert und im Portal registriert haben, können Sie die Einstellungen für den Agenten konfigurieren. Mögliche Einstellungen:

- Vault-Verbindungen. Vault-Verbindungen umfassen Vault-Informationen und Anmeldeinformationen, mit denen der Agent Daten im Vault sichern und aus dem Vault wiederherstellen kann. Siehe *Hinzufügen von Vault-Einstellungen* auf Seite 16.
- Beschreibung des geschützten Computers. Die Beschreibung wird für den Agenten auf der Seite „Computer“ im Portal angezeigt. Siehe *Hinzufügen einer Beschreibung* auf Seite 18.
- Aufbewahrungstypen. Aufbewahrungstypen legen fest, wie lange die Sicherungen im Vault aufbewahrt werden. Siehe *Hinzufügen von Aufbewahrungstypen* auf Seite 18.
- Die für Wiederherstellungen verwendete Bandbreite. Siehe *Konfigurieren der Bandbreitendrosselung* auf Seite 20.
- E-Mail-Benachrichtigungen an Benutzer, wenn eine Sicherung abgeschlossen wurde, nicht ausgeführt werden kann oder wenn Fehler auftreten. Siehe *Sicherungen mithilfe von E-Mail-Benachrichtigungen überwachen.* auf Seite 86.

Wenn ein Agent einen Zertifikatfehler meldet, müssen Sie den Zertifikatfehler beheben, bevor Sicherungen und Wiederherstellungen fortgesetzt werden können. Siehe *Beheben von Zertifikatfehlern* auf Seite 21.

3.1 Hinzufügen von Vault-Einstellungen

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

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

Wenn eine Richtlinie zu ein Agent 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 Agent 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:

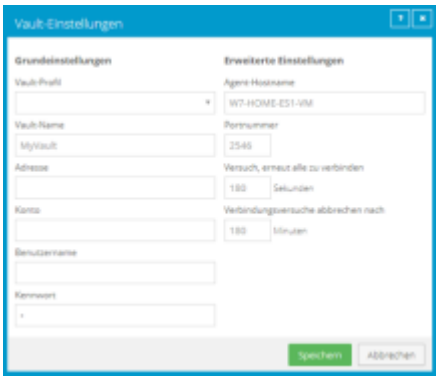
1. Klicken Sie in Portal in der Navigationsleiste auf **Computer**.

2. Suchen Sie Agent, für das Sie Vault-Einstellungen hinzufügen möchten, und klicken Sie auf die Agent-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-Profile** 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 Agent 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**.

3.2 Hinzufügen einer Beschreibung

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

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 Agent, 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 Agent ein.

5. Klicken Sie auf **Speichern**.

3.3 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 Agent hinzufügen, wenn keine Richtlinie zugewiesen ist.

Sie können keine Aufbewahrungstypen für tagesinterne Zeitpläne hinzufügen, ändern oder löschen. Für tagesaktuelle Zeitpläne müssen Sie einen der beiden tagesaktuellen Aufbewahrungstypen wählen, die ab Portal 8.88 verfügbar sind. Siehe *Planung eines Sicherungsjobs, der mehrmals am Tag ausgeführt wird* auf Seite 37.

Wenn eine Richtlinie zu ein Agent 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 Agent, für den Sie einen Aufbewahrungstyp hinzufügen möchten, und klicken Sie auf die Zeile, um die Ansicht zu erweitern.

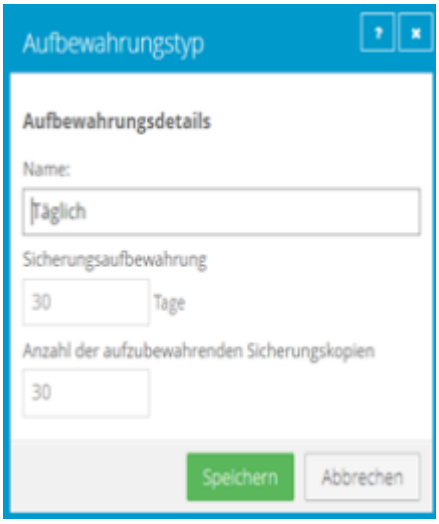
Wenn das Feld „Manuell konfigurieren“ angezeigt wird, klicken Sie auf **Manuell konfigurieren**. Das Feld “Manuell konfigurieren” wird bei einigen Computern angezeigt, auf denen kein Sicherungsjob erstellt wurde.

3. Klicken Sie in der Registerkarte „Erweitert“ auf die Registerkarte **Aufbewahrungstypen**.

   Wenn eine Richtlinie zum Agent 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. *Hinweis:* 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. *Hinweis:* 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	*Hinweis:* Wenn die Datenarchivierung in Ihrer Portal-Instanz deaktiviert ist, wird dieser Wert nicht angezeigt. 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. 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 Dienstanbieter kann Jobs und die dazugehörigen Daten aus dem Vault entfernen. Dies dient als Vorsichtmaßnahme, um zu verhindern, dass Daten versehentlich oder böswillig vernichtet werden.

6. Klicken Sie auf **Speichern**.

3.4 Konfigurieren der Bandbreitendrosselung

Mögliche Bandbreiteneinstellungen:

- Maximale Bandbreite (obere Grenze) in MB pro Sekunde, die der Agent für Sicherungen und Wiederherstellungen verbrauchen darf. Wenn beispielsweise drei Jobs gleichzeitig auf einem Computer ausgeführt werden, erhält jeder Job 1/3 der angegebenen maximalen Bandbreite.
- 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 Agents 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 Agent 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**.

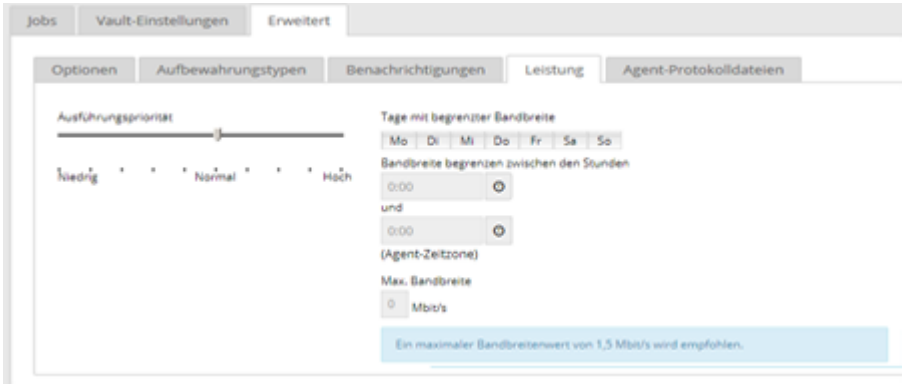
2. Suchen Sie den Agent, für den Sie die Bandbreitendrosselung konfigurieren möchten, und klicken Sie auf die Zeile, um die Ansicht zu erweitern.

   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.

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

   Wenn eine Richtlinie zum Agent 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.



4. Klicken Sie auf **Speichern**.

3.5 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 78 und *Anzeigen von Informationen zu Computer- und Jobstatus* auf Seite 79. Agenten können Zertifikatfehler melden, wenn sie das Anheften von Zertifikaten unterstützen, eine Sicherheitsfunktion, die sicherstellen soll, dass Agenten sich mit legitimen Vaultsverbinden.

Wenn ein Zertifikatfehler gemeldet wird, wenden Sie sich an das IT-Sicherheitspersonal oder einen Dienstanbieter, 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 anzuheften. Wenn Sie ein Zertifikat neu anheften, zeichnet der Agent den neuen öffentlichen Schlüssel des Zertifikats sicher auf.

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 Bestätigungsdialogfeld auf **Ja**.
5. Klicken Sie im Fenster mit der Erfolgsmeldung auf **OK**.

4 Hinzufügen von Linux-Sicherungsjobs

Nachdem ein Linux-System in Portal hinzugefügt wurde, können Sie Sicherungsjobs für das System erstellen.

Sie können Sicherungsjobs für Dateien und Ordner erstellen, die lokal auf dem Computer gespeichert sind. Der Sicherungsjob legt fest, welche Dateien und Ordner gesichert und an welchem Ort die Daten gespeichert werden. Sie können auch einen Sicherungsjob für Dateien und Ordner erstellen, die auf bereitgestellten NFS-Freigaben gespeichert sind. Siehe *Hinzufügen von NFS-Sicherungsjobs* auf Seite 27.

Sie können Bare Metal Restore (BMR)-Sicherungsjobs erstellen, die zur Wiederherstellung ganzer Linux-Systeme verwendet werden können. Eine Linux-BMR-Sicherung enthält eine ISO-Datei zum Starten des Zielsystems und zum Ausführen einer Wiederherstellung sowie eine Sicherung im Vault, die alle erforderlichen Systemvolumes und -dateien enthält.

WICHTIG: Es wird empfohlen, für jedes Linux-System nur einen BMR-Sicherungsjob zu erstellen. Wenn Sie mehrere BMR-Sicherungsjobs erstellen und ausführen, ist die resultierende ISO-Datei möglicherweise nicht verwendbar.

Hinweis: Standardmäßig sichert ein Linux-BMR-Job alle Systemdaten. Sie können Ordner von der BMR-Sicherung ausschließen. Wenn Sie jedoch einen der folgenden erforderlichen Ordner ausschließen, wird der Ausschluss bei der Ausführung des Sicherungsjobs ignoriert: /bin; /boot; /etc; /lib; /lib64; /root; /usr/bin; /usr/lib; /usr/lib64; /usr/share; /usr/sbin

Hinweis: Auf einem Server, auf dem Oracle oder eine andere Datenbank ausgeführt wird, wird empfohlen, die Datenbankdienste herunterzufahren, wenn Sie einen BMR-Job ausführen. Alternativ können Sie auf einem Server, auf dem Oracle ausgeführt wird, Datenbankverzeichnisse aus dem BMR-Job ausschließen und einen separaten Oracle Plug-in-Job für die Datenbank einrichten. Andernfalls sind die Datenbankdaten nach der Wiederherstellung möglicherweise inkonsistent.

Eine symbolische Verknüpfung (auch als Symlink oder Softlink bezeichnet) besteht aus einer besonderen Art von Datei, die als Referenz für eine andere Datei oder ein Verzeichnis dient. Während einer Sicherung wird eine symbolische Verknüpfung mit dem Zeitstempel der Verknüpfung gesichert. Bei der Wiederherstellung einer symbolischen Verknüpfung werden ihr Änderungsdatum und -uhrzeit auf das Datum und die Uhrzeit der Wiederherstellung festgelegt (statt des Datums und der Uhrzeit der Sicherung).

Um die Daten zu sichern, können Sie den Sicherungsjob manuell ausführen oder einen geplanten Sicherungsjob einrichten. 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 32.

So fügen Sie einen Linux-Sicherungsjob hinzu:

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

   Die Seite „Computer“ zeigt registrierte Computer an.

2. Suchen Sie das gewünschte Linux-System und erweitern Sie die Ansicht durch Klicken auf die jeweilige Computerzeile.

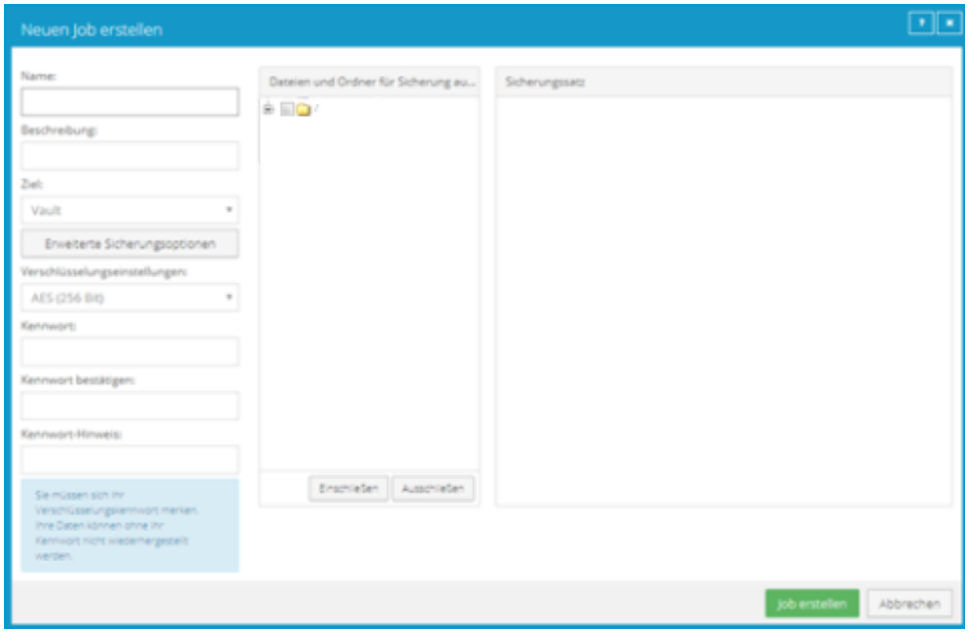
   Wenn für den Linux-Computer kein Sicherungsjob erstellt wurde, kann das System versuchen, einen Sicherungsjob automatisch zu erstellen. Siehe *Hinzufügen des ersten Sicherungsjobs für einen Linux-Server* auf Seite 26.

3. Klicken Sie auf die Registerkarte **Jobs**.

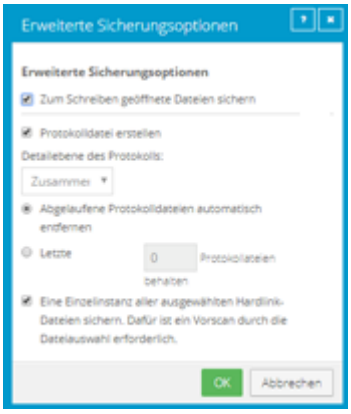
Wenn keine gültige Vault-Verbindung für den Computer verfügbar ist, können Sie nicht auf die Registerkarte mit den Jobs zugreifen. Siehe *Hinzufügen von Vault-Einstellungen* auf Seite 16.

4. Klicken Sie im Menü **Jobaufgabe auswählen** auf **Neuen lokalen Systemjob erstellen**.
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.
   - Neue Sicherungsjobs verwenden die Verschlüsselungsmethode AES (256 Bit). Vorhandene Jobs können andere Verschlüsselungsmethoden nutzen. Siehe *Verschlüsselungseinstellungen* auf Seite 30.
   - Geben Sie in die Felder **Kennwort** und **Kennwort bestätigen** ein Verschlüsselungskennwort ein. Sie können auch einen Kennworthinweis in das Feld **Kennworthinweis** eingeben.



6. Klicken Sie auf **Erweiterte Sicherungsoptionen**, um die Einstellungen für die Protokolldateien oder andere Sicherungsoptionen zu ändern. Legen Sie die gewünschten Optionen im Dialogfeld „Erweiterte Sicherungsoptionen“ fest und klicken Sie auf **OK**. Weitere Informationen finden Sie unter *Protokolldateioptionen* auf Seite 29 und *Erweiterte Sicherungsoptionen* auf Seite 30.



7. Führen Sie im Feld **Dateien und Ordner für die Sicherung auswählen** so oft die folgenden Aktionen aus, bis im Feld **Sicherungssatz** alle Ordner und Dateien angezeigt werden, die Sie bei der Sicherung berücksichtigen oder ausschließen möchten:

   - Um eine ISO-Datei mit Volumes und Dateien, die zum Starten des Systems und zum Sichern aller Systemdaten erforderlich sind, zu erstellen, wählen Sie **Bare-Metal-Wiederherstellung** aus und klicken Sie dann auf **Einschließen**.

     Standardmäßig sichert ein Linux-BMR-Job alle Systemdaten. Sie können Ordner von der Sicherung ausschließen. Wenn Sie jedoch einen erforderlichen Ordner ausschließen, wird der Ausschluss bei der Ausführung des Sicherungsjobs ignoriert und es wird eine Meldung in der Protokolldatei aufgeführt.

     Wenn ein Linux-BMR-Job ausgeführt wird, wird eine Boot-ISO-Datei namens „Bare_Metal_Restore_Image.iso“ im Stammverzeichnis (/) erstellt. Die Datei wird jedes Mal überschrieben, wenn ein BMR-Job ausgeführt wird. Es wird empfohlen, mindestens 1 GB Speicherplatz im Root-Dateisystem für die ISO-Datei zu reservieren, wenn Sie zum ersten Mal einen BMR-Sicherungsjob ausführen.

   - Um Dateien oder Ordner zum Sicherungsjob hinzuzufügen, aktivieren Sie die Kontrollkästchen für die jeweiligen Elemente und klicken Sie auf **Einschließen**. Die eingeschlossenen Dateien und Ordner werden im Feld **Sicherungssatz** angezeigt. Wenn Sie einen Ordner einschließen, umfasst der Sicherungsjob standardmäßig alle enthaltenen Unterordner und Dateien. Sie können Filter hinzufügen, falls Sie nicht alle Unterordner und Dateien sichern möchten. Siehe *Filtern von Unterverzeichnissen und Dateien in Sicherungsjobs* auf Seite 31.

   - Um Dateien oder Ordner vom Sicherungsjob auszuschließen, aktivieren Sie die Kontrollkästchen für die jeweiligen Elemente und klicken Sie auf **Ausschließen**. Die ausgeschlossenen Dateien und Ordner werden im Feld **Sicherungssatz** angezeigt. Wenn Sie einen Ordner ausschließen, werden standardmäßig alle enthaltenen Unterordner und Dateien vom Sicherungsjob ausgeschlossen. Sie können Filter hinzufügen, falls Sie nicht alle Unterordner und Dateien ausschließen möchten. Siehe *Filtern von Unterverzeichnissen und Dateien in Sicherungsjobs* auf Seite 31.

   - Um einen Einschließen- oder Ausschließen-Datensatz aus dem Feld **Sicherungssatz** zu entfernen, klicken Sie neben dem Datensatz auf die Schaltfläche „Löschen“.

8. Klicken Sie auf **Job erstellen**.

   Der Job wird erstellt und das Dialogfeld „Zeitplan anzeigen/hinzufügen“ wird angezeigt. Sie können nun einen Zeitplan zum Ausführen der Sicherung erstellen. Klicken Sie auf **Abbrechen**, wenn Sie aktuell keinen Zeitplan erstellen möchten.

Weitere Informationen zum Ausführen und Planen von Sicherungsjobs finden Sie unter *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 32.

4.1 Hinzufügen des ersten Sicherungsjobs für einen Linux-Server

Portal kann automatisch einen Sicherungsjob für einen Linux-Computer erstellen, der noch keinen Sicherungsjob hat. Bei automatisch erstellten Jobs wird das gesamte Root-Verzeichnis gesichert. Die automatisch erstellten Jobs werden jede Nacht ausgeführt.

Nach der automatischen Erstellung können Sie die Jobeinstellungen bei Bedarf ändern. Sie können beispielsweise andere Verzeichnisse für die Sicherung auswählen oder den Zeitplan für die Ausführung ändern.

Damit Portal Sicherungsjobs automatisch erstellen kann, muss ein gültiges Vault-Profil verfügbar sein.

Nach der Erstellung können Sie die Jobeinstellungen bei Bedarf ändern. Sie können beispielsweise andere Ordner für die Sicherung auswählen oder den Zeitplan für die Ausführung ändern.

So fügen Sie den ersten Sicherungsjob für einen Linux-Server hinzu:

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

   Die Seite „Computer“ zeigt registrierte Computer an.

2. Suchen Sie den gewünschten Linux-Computer und erweitern Sie die Ansicht durch Klicken auf die jeweilige Computerzeile.

   Wenn für den Computer kein Sicherungsjob erstellt wurde, wird das Feld „Manuell konfigurieren“ angezeigt. Wenn für den Computer kein Sicherungsjob erstellt wurde und mindestens ein Vault-Profil verfügbar ist, wird ebenfalls das Feld „Automatisch konfigurieren“ angezeigt.

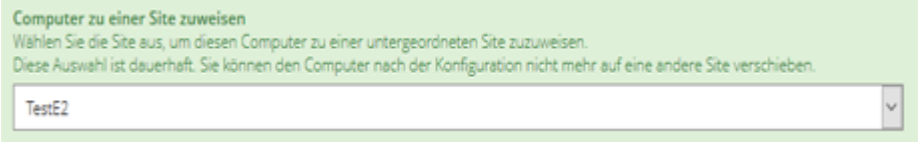
3. Führen Sie eine der folgenden Aktionen aus:
   - Um einen Sicherungsjob manuell zu erstellen, klicken Sie auf **Manuell konfigurieren**. Siehe *Hinzufügen von Linux-Sicherungsjobs* auf Seite 23.
   - Um automatisch einen Sicherungsjob für den Computer zu erstellen, führen Sie die folgenden Schritte aus:
     a. Geben Sie ein Verschlüsselungskennwort in die Felder **Kennwort erstellen** und **Kennwort bestätigen** ein.

WICHTIG: Sie benötigen das Verschlüsselungskennwort zur Wiederherstellung der Daten. Bewahren Sie es daher an einem sicheren Ort auf. Wenn Sie das Kennwort vergessen haben, können Sie Ihre Daten nicht wiederherstellen. Das Kennwort wird an keiner anderen Stelle aufbewahrt und kann nicht wiederhergestellt werden.

b. Geben Sie im Feld **Kennwort-Hinweis** einen Hinweis ein, damit Sie sich leichter an das Verschlüsselungskennwort erinnern können.

c. Wenn die Liste **Diesen Computer einer Site zuordnen** angezeigt wird, wählen Sie eine Site für den Computer aus.

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



d. Wenn mehrere Vaults verfügbar sind, wählen Sie den Vault aus der Liste **Vault auswählen** aus.

e. Klicken Sie auf **Automatisch konfigurieren**.

Wenn die Konfiguration erfolgreich angewendet wurde, wird ein Sicherungsjob für den Computer angezeigt.

Wenn die automatische Konfiguration von Jobs fehlschlägt, führen Sie die folgenden Schritte aus:

i. Klicken Sie auf **Manuell konfigurieren**.

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

iii. Geben Sie Vault-Informationen und Anmeldeinformationen im Dialogfeld „Vault-Einstellungen“ ein.

iv. Erstellen Sie einen Sicherungsjob manuell. Siehe *Hinzufügen von Linux-Sicherungsjobs* auf Seite 23.

4.2 Hinzufügen von NFS-Sicherungsjobs

Nachdem ein Linux-System in Portal hinzugefügt wurde, können Sie einen Sicherungsjob für Dateien und Ordner erstellen, die lokal auf bereitgestellten NFS-Freigaben gemountet sind. Der Sicherungsjob legt fest, welche Dateien und Ordner gesichert und an welchem Ort die Daten gespeichert werden.

NFS-Server müssen ihre Exporte freigeben, damit diese für Clientsysteme verfügbar sind. Wenn Sie an einem Bereitstellungspunkt eine Sicherung oder Wiederherstellung durchführen möchten, muss der NFS-Server verfügbar sein und Ihrem Clientsystem ausreichende Privilegien bereitstellen. Außerdem muss das NFS zum Zeitpunkt der Sicherung oder Wiederherstellung auf Ihrem Clientsystem gemountet sein.

Hinweis: Wenn Sie eine NFS-Sicherung wiederherstellen und der NFS-Mount nicht vorhanden ist, wird die Wiederherstellung wie eine lokale Wiederherstellung ausgeführt. Dabei werden die Daten auf dem lokalen

Datenträger (mit einem ähnlichen, lokalen Pfad) abgelegt, ohne dass ein Pfad mit einem Bereitstellungspunkt (NFS) verwendet wird. Es wird kein Fehler gemeldet.

NFS exportiert keine erweiterten Attribute aus Remote-Dateisystemen. Auf Linux NFSv3-Clients werden Remotedateisystem-ACLs soweit möglich als standardmäßige Linux-ACLs dargestellt. Auf NFSv4-Clients werden Remotedateisystem-ACLs als systemeigene NFSv4-ACLs dargestellt; sie werden jedoch vom Agenten als erweiterte Attribute geschützt.

Um die Daten zu sichern, können Sie den Sicherungsjob manuell ausführen oder einen geplanten Sicherungsjob einrichten. 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 32.

So fügen Sie NFS-Sicherungsjobs hinzu:

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

   Die Seite „Computer“ zeigt registrierte Computer an.

2. Suchen Sie das gewünschte Linux-System und erweitern Sie die Ansicht durch Klicken auf die jeweilige Computerzeile.

   In einigen Portal-Instanzen kann das System versuchen, einen Sicherungsjob automatisch zu erstellen, wenn für den Linux-Computer kein Sicherungsjob erstellt wurde.

3. Klicken Sie auf die Registerkarte **Jobs**.

   Wenn keine gültige Vault-Verbindung für den Computer verfügbar ist, können Sie nicht auf die Registerkarte mit den **Jobs** zugreifen.

4. Klicken Sie im Menü **Jobaufgabe auswählen** auf **Neuen Job für NFS-Dateien erstellen**.
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 29.
   - Neue Sicherungsjobs verwenden die Verschlüsselungsmethode AES (256 Bit). Vorhandene Jobs können andere Verschlüsselungsmethoden nutzen. Siehe *Verschlüsselungseinstellungen* auf Seite 30.
   - 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 Feld **Dateien und Ordner für die Sicherung auswählen** so oft die folgenden Aktionen aus, bis im Feld **Sicherungssatz** alle Ordner und Dateien angezeigt werden, die Sie bei der Sicherung berücksichtigen oder ausschließen möchten:
   - Um Dateien oder Ordner zum Sicherungsjob hinzuzufügen, aktivieren Sie die Kontrollkästchen für die jeweiligen Elemente und klicken Sie auf **Einschließen**. Die eingeschlossenen Dateien und

Ordner werden im Feld **Sicherungssatz** angezeigt. Wenn Sie einen Ordner einschließen, umfasst der Sicherungsjob standardmäßig alle enthaltenen Unterordner und Dateien. Sie können Filter hinzufügen, falls Sie nicht alle Unterordner und Dateien sichern möchten. Siehe *Filtern von Unterverzeichnissen und Dateien in Sicherungsjobs* auf Seite 31.

- Um Dateien oder Ordner vom Sicherungsjob auszuschließen, aktivieren Sie die Kontrollkästchen für die jeweiligen Elemente und klicken Sie auf **Ausschließen**. Die ausgeschlossenen Dateien und Ordner werden im Feld **Sicherungssatz** angezeigt. Wenn Sie einen Ordner ausschließen, werden standardmäßig alle enthaltenen Unterordner und Dateien vom Sicherungsjob ausgeschlossen. Sie können Filter hinzufügen, falls Sie nicht alle Unterordner und Dateien ausschließen möchten. Siehe *Filtern von Unterverzeichnissen und Dateien in Sicherungsjobs* auf Seite 31.
- Um einen Einschließen- oder Ausschließen-Datensatz aus dem Feld **Sicherungssatz** zu entfernen, klicken Sie neben dem Datensatz auf die Schaltfläche „Löschen“.

7. Klicken Sie auf **Job erstellen**.

   Der Job wird erstellt und das Dialogfeld „Zeitplan anzeigen/hinzufügen“ wird angezeigt. Sie können nun einen Zeitplan zum Ausführen der Sicherung erstellen. Klicken Sie auf **Abbrechen**, wenn Sie aktuell keinen Zeitplan erstellen möchten.

   Weitere Informationen zum Ausführen und Planen von Sicherungsjobs finden Sie unter *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 32.

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.

- **Protokolldatei erstellen**. Bei Aktivierung dieses Kontrollkästchens erstellt das System Protokolldateien für jeden Job. Protokolldateien können die Uhrzeit für Aufbau und Trennung der Verbindung, Dateinamen (d. h. die Namen der Dateien, die bei der Sicherung kopiert wurden) sowie Verarbeitungsfehler enthalten.
- **Abgelaufene Protokolldateien automatisch entfernen**. Bei Aktivierung dieses Kontrollkästchens wird die einer Sicherung zugeordnete Protokolldatei beim Löschen der Sicherung im Vault automatisch entfernt. Sicherungen werden in der Regel gemäß den Aufbewahrungstypen vom Vault gelöscht. Siehe *Hinzufügen von Aufbewahrungstypen* auf Seite 18.

- **Letzte** *<Anzahl der>* **Protokolldateien behalten**. Gibt die Anzahl beizubehaltender Protokolldateien für den Sicherungsjob an. Wenn die angegebene Anzahl erreicht ist, wird die älteste Protokolldatei eines Sicherungsjobs gelöscht, um Speicherplatz für die neueste Datei freizugeben.

Hinweis: Sie müssen entweder die Option **Abgelaufene Protokolldateien automatisch entfernen** oder **Letzte** *<Anzahl der>* **Protokolldateien behalten** auswählen. Beim Ausführen von Sicherungsjobs werden Protokolldateien gemäß der angegebenen Option entfernt. Protokolldateien werden beim Synchronisieren von Sicherungsjobs nicht entfernt.

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.

4.5 Erweiterte Sicherungsoptionen

Eine Einzelinstanz aller ausgewählten Hardlink-Dateien sichern

Ein Hardlink ist ein Verweis oder Zeiger auf Daten auf einem Speichervolume. Es kann denselben Daten mehr als ein Hardlink zugeordnet werden. Dateien mit Hardlinks können nicht auf anderen Datenträgern vorhanden sein und müssen sich auf demselben Datenträger befinden.

Wenn die Option **Eine Einzelinstanz aller ausgewählten Hardlink-Dateien sichern** ausgewählt ist, wird nur eine Kopie der Daten zusammen mit allen Hardlinks gesichert. Bei einer Wiederherstellung werden die

Daten (mit einem neuen Inode) zusammen mit ihren Hardlinks wiederhergestellt. Wenn diese Option ausgewählt ist, ist ein Vorscan-Prozess erforderlich. Bei Vorscans wird das gesamte Dateisystem gelesen, jeder Inode wird erfasst und in einer Zuordnung gespeichert. Je größer das Dateisystem ist, umso mehr Arbeitsspeicher erfordert diese Zuordnung, und umso mehr Zeit dauert ihre Verarbeitung. Allerdings ist dann die Sicherungsgröße kleiner.

Wenn die Option **Eine Einzelinstanz aller ausgewählten Hardlink-Dateien sichern** nicht ausgewählt ist, werden die Daten separat für die einzelnen Hardlinks gesichert. Bei der Wiederherstellung wird die Hardlinkbeziehung nicht wieder eingerichtet. Jede Datei wird einzeln wiederhergestellt, und Anwendungen, für die Hardlinks erforderlich sind, werden möglicherweise nicht automatisch wiederhergestellt. Wenn diese Option nicht ausgewählt ist, ist die Sicherung schneller, aber die gesamte Sicherungsgröße ist auch größer.

4.6 Filtern von Unterverzeichnissen und Dateien in Sicherungsjobs

Wenn Sie Ordner in einem Sicherungsjob ein- und ausschließen, sind die Unterverzeichnisse und Dateien dieser Ordner ebenfalls standardmäßig ein- bzw. ausgeschlossen.

Wenn Sie nur einige Unterverzeichnisse oder Dateien in einem Ordner sichern möchten, können Sie dem Einschließen-Datensatz Filter hinzufügen. Sie können beispielsweise einen Filter hinzufügen, damit Dateien in einem Ordner nur gesichert werden, wenn sie die .pl-Erweiterung haben.

Wenn Sie nur einige Unterverzeichnisse oder Dateien in einem Ordner vom Sicherungsjob ausschließen möchten, können Sie dem Ausschließen-Datensatz Filter hinzufügen. Sie können beispielsweise einen Filter hinzufügen, damit Dateien in einem Ordner nur gesichert werden, wenn sie die .mpg-Erweiterung haben.

Wenn einem Computer eine Richtlinie zugewiesen ist, können Sie Filter aus der Richtlinie zu einem Ordner-Einschließen- oder Ausschließen-Datensatz hinzufügen.

Die Filter in einem Sicherungsjob werden aktiviert, wenn der Job ausgeführt wird. Neue Unterverzeichnisse und Dateien, die von den Filtern ausgefiltert werden, werden bei der Ausführung des Jobs automatisch gesichert oder ausgeschlossen.

So filtern Sie Unterverzeichnisse und Dateien in einem Sicherungsjob:

1. Beachten Sie beim Erstellen oder Bearbeiten eines Sicherungsjobs das Feld **Sicherungssatz**.
2. Wenn keine bearbeitbaren Felder für einen Ordner-Einschließen- oder Ausschließen-Datensatz, in dem Sie Unterverzeichnisse und Dateien filtern möchten, angezeigt werden, klicken Sie in der Ordnerzeile auf die Schaltfläche **Bearbeiten**. 
3. Führen Sie im Feld **Sicherungssatz** für jeden eingeschlossenen Ordner, in dem bestimmte Unterverzeichnisse oder Dateien eingeschlossen werden sollen, eines oder mehrere der folgenden Verfahren durch:
   - Um bestimmte Unterverzeichnisse in den Sicherungsjob einzuschließen, geben Sie im Feld **Ordnerfilter** die Namen der entsprechenden Unterverzeichnisse ein. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. Um beispielsweise Unterverzeichnisse in einer Sicherung einzuschließen, deren Namen mit „-aktuell“ enden oder mit „2015“ beginnen, geben Sie folgenden Filter ein: *-aktuell, 2015*

     Hinweis: Das Sternchen (*) ist das einzige unterstützte Platzhalterzeichen in Filterfeldern.

- Um bestimmte Dateien im Sicherungsjob einzuschließen, geben Sie im Feld **Dateienfilter** die Namen der entsprechenden Dateien ein. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. Um beispielsweise nur Dateien in eine Sicherung einzuschließen, die eine .pl- oder .sh-Erweiterung haben, geben Sie folgenden Filter ein: *.pl, *.sh

  Hinweis: Das Sternchen (*) ist das einzige unterstützte Platzhalterzeichen in Filterfeldern.

- Wenn einem Computer eine Richtlinie zugewiesen ist, klicken Sie auf die Schaltfläche **Richtlinienfilter anwenden**, um Filter aus der Richtlinie für den Einschließen-Datensatz zu aktivieren. 

- Um den angegebenen Ordner ohne seine Unterverzeichnisse zu sichern, deaktivieren Sie das Kontrollkästchen **Rekursiv**.

- Um die Unterverzeichnisse des Ordners zu sichern, markieren Sie das Kontrollkästchen **Rekursiv**.

4. Führen Sie im Feld **Sicherungssatz** für jeden ausgeschlossenen Ordner, in dem bestimmte Unterverzeichnisse oder Dateien ausgeschlossen werden sollen, eines oder mehrere der folgenden Verfahren durch:

   - Um bestimmte Unterverzeichnisse aus dem Sicherungsjob auszuschließen, geben Sie im Feld **Ordnerfilter** die Namen der entsprechenden Unterverzeichnisse ein. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. Um beispielsweise Unterverzeichnisse aus einer Sicherung auszuschließen, deren Namen mit „-alt“ enden oder mit „2001“ beginnen, geben Sie folgenden Filter ein: *-alt, 2001*

     Hinweis: Das Sternchen (*) ist das einzige unterstützte Platzhalterzeichen in Filterfeldern.

   - Um bestimmte Dateien aus dem Sicherungsjob auszuschließen, geben Sie im Feld **Ordnerfilter** die Namen der entsprechenden Dateien ein. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. Um beispielsweise nur Dateien aus einer Sicherung auszuschließen, die eine .mpg- oder .gif-Erweiterung haben, geben Sie folgenden Filter ein: *.mpg, *.gif

     Hinweis: Das Sternchen (*) ist das einzige unterstützte Platzhalterzeichen in Filterfeldern.

   - Wenn einem Computer eine Richtlinie zugewiesen ist, klicken Sie auf die Schaltfläche **Richtlinienfilter anwenden**, um Filter aus der Richtlinie für den Ausschließen-Datensatz zu aktivieren. 

   - Um den angegebenen Ordner ohne seine Unterverzeichnisse auszuschließen, deaktivieren Sie das Kontrollkästchen **Rekursiv**.

   - Um die Unterverzeichnisse des Ordners auszuschließen, markieren Sie das Kontrollkästchen **Rekursiv**.

5. Klicken Sie auf **Job erstellen** oder **Speichern**.

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 33.

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.

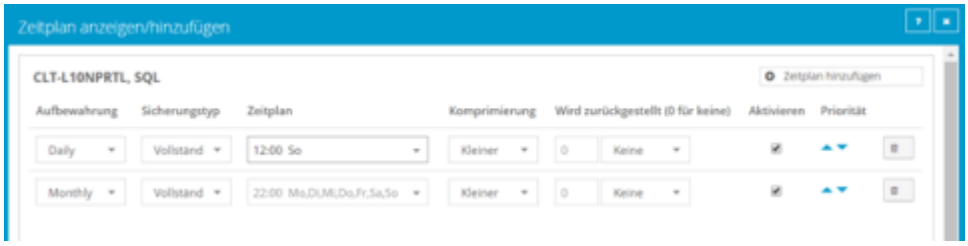
4.7 Planen von Sicherungen

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 Agent 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**.

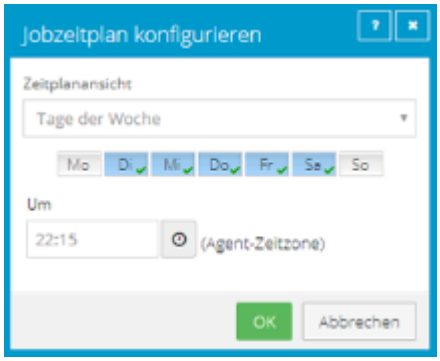
   Im Dialogfeld wird eine neue Zeile hinzugefügt.
3. Klicken Sie in der neuen Zeile in der Liste **Aufbewahrung** auf einen Aufbewahrungstyp.

   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 18.

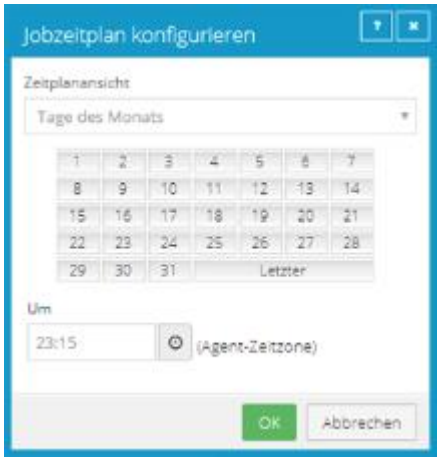
   Die Aufbewahrungstypen 24 und 48 Stunden stehen nur für tagesaktuelle Zeitpläne zur Verfügung. Siehe *Planung eines Sicherungsjobs, der mehrmals am Tag ausgeführt wird* auf Seite 37.

6. Klicken Sie im Feld **Zeitplan** auf den Pfeil.

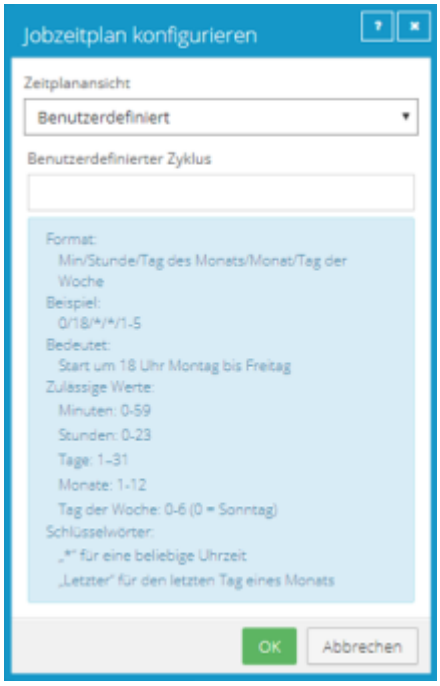
   Das Dialogfeld „Jobzeitplan konfigurieren“ wird geöffnet.
7. Gehen Sie im Dialogfeld „Jobzeitplan konfigurieren“ wie folgt vor:
   - Um die Sicherung an bestimmten Wochentagen auszuführen, wählen Sie die Option **Tage der Woche** in der Liste **Zeitplanansicht** aus. Wählen Sie die Tage aus, an denen der Job ausgeführt werden soll. Geben Sie im Feld **Um** den Zeitpunkt an, an dem der Job ausgeführt werden soll.



- 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.



- 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.



Hinweis: Wenn in der Liste **Zeitplanansicht Tagesaktuell** angezeigt wird, können Sie die Sicherung auch so planen, dass sie mehrmals am Tag ausgeführt wird. Siehe *Planung eines Sicherungsjobs, der mehrmals am Tag ausgeführt wird* auf Seite 37.

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**.

4.8 Planung eines Sicherungsjobs, der mehrmals am Tag ausgeführt wird

Hinweis: Um einen Sicherungsjob zu planen, der an bestimmten Tagen der Woche oder des Monats ausgeführt wird, finden Sie weitere Informationen unter *Planen von Sicherungen* auf Seite 33.

Jeder Sicherungsjob kann einen tagesinternen Zeitplan haben. Wenn der Job über andere Zeitpläne verfügt, hat der tagesinterne Zeitplan die niedrigste Priorität und steht am Ende der Zeitplanliste Wenn ein Job durch einen tagesinternen Zeitplan und einen anderen Zeitplan genau zur gleichen Zeit gestartet wird, wird der Job nur einmal ausgeführt und der Aufbewahrungstyp des anderen Zeitplans (z. B. täglich oder monatlich) wird auf den resultierenden Sicherungssatz angewendet.

Wenn Sie einen tagesinternen Zeitplan für einen Sicherungsjob erstellen, können Sie einen von zwei Aufbewahrungstypen wählen:

- 24-Stunden. Bei diesem Aufbewahrungstyp wird jede Sicherung mindestens 24 Stunden lang aufbewahrt und mindestens eine Sicherung mit dieser Aufbewahrungsart wird online gespeichert.
- 48-Stunden. Bei diesem Aufbewahrungstyp wird jede Sicherung mindestens 48 Stunden lang aufbewahrt und mindestens eine Sicherung mit dieser Aufbewahrungsart wird online gespeichert.

Andere Aufbewahrungstypen sind für tagesinterne Zeitpläne nicht verfügbar. Sie können keine Aufbewahrungstypen für tagesinterne Zeitpläne hinzufügen, ändern oder löschen.

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.

Um eine Zeitplan-Überlastung zu vermeiden, werden in einigen Fällen Sicherungen, die durch tagesinterne Zeitpläne geplant werden, übersprungen. Siehe *Übersprungene Sicherungen* auf Seite 39.

So planen Sie einen Sicherungsjobs, der mehrmals am Tag ausgeführt wird:

1. Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie in der Navigationsleiste auf **Computer**. Suchen Sie den Computer mit dem Sicherungsjob, den Sie planen möchten, und erweitern Sie die Ansicht, indem Sie auf die Zeile klicken. 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 Zeitplanzeile auf den Pfeil im Feld **Zeitplan**.

   WICHTIG: Um einen tagesinternen Zeitplan zu erstellen, müssen Sie im Feld Zeitplan die Option **Tagesintern** wählen, bevor Sie einen Aufbewahrungstyp auswählen.

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

   a. Wählen Sie in der Liste **Zeitplanansicht** die Option **Tagesintern** aus.

   b. Klicken Sie in der Liste **Alle *x* Stunden** auf die Häufigkeit, mit der der Job ausgeführt werden soll. Sie können den Job so planen, dass er alle 1, 2, 3, 4, 6, 8 oder 12 Stunden ausgeführt wird.

   c. Geben Sie in das Feld **um *y* Minuten nach der vollen Stunde** die Anzahl der Minuten nach der vollen Stunde ein, nach denen der Job ausgeführt werden soll. Geben Sie z. B. 15 ein, um den Job 15 Minuten nach jeder vollen Stunde auszuführen.

   d. Führen Sie im Bereich „Aktiver Zeitraum“ eine der folgenden Aktionen aus:

      - Wenn der Job mit der angegebenen Häufigkeit für den gesamten 24-Stunden-Zeitraum ausgeführt werden soll, klicken Sie auf **Sicherungen den ganzen Tag ausführen**.
      - Wenn der Job gemäß dem tagesinternen Zeitplan nur für einen Teil jedes 24-Stunden-Zeitraums ausgeführt werden soll, klicken Sie auf **Nur ausführen zwischen**. Klicken Sie auf das erste Uhrensymbol und geben Sie den Beginn des Zeitraums an, in dem Sicherungen mit der angegebenen Häufigkeit ausgeführt werden sollen. Klicken Sie auf das zweite Uhrensymbol und geben Sie das Ende des Zeitraums an, zu dem Sicherungen mit der angegebenen Häufigkeit ausgeführt werden sollen.

   e. Klicken Sie auf **OK**.

      Wenn der Job über andere Zeitpläne verfügt, wird der tagesinterne Zeitplan am Ende der Zeitplanliste angezeigt und hat die niedrigste Priorität. Die Priorität des Zeitplans für die tagesinterne Sicherung kann nicht geändert werden.

5. Klicken Sie in der Liste **Aufbewahrung** auf einen der folgenden Aufbewahrungstypen.

   - **24-Stunden**. Bei diesem Aufbewahrungstyp wird jede Sicherung mindestens 24 Stunden lang aufbewahrt und mindestens eine Sicherung mit dieser Aufbewahrungsart wird online gespeichert.
   - **48-Stunden**. Bei diesem Aufbewahrungstyp wird jede Sicherung mindestens 48 Stunden lang aufbewahrt und mindestens eine Sicherung mit dieser Aufbewahrungsart wird online gespeichert.

   Andere Aufbewahrungstypen sind für tagesinterne Zeitpläne nicht verfügbar.

6. Klicken Sie im Feld **Zeitplan** auf den Pfeil.

   Das Dialogfeld „Jobzeitplan konfigurieren“ wird geöffnet.

7. Klicken Sie auf **OK**.

   Der neue Zeitplan wird im Feld „Zeitplan“ angezeigt.

8. Klicken Sie in der Liste **Komprimierung** auf eine Komprimierungsstufe für die Sicherungsdaten. Die Komprimierungsstufen optimieren die Menge der gespeicherten Daten im Verhältnis zur Sicherungsgeschwindigkeit.
9. 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. Zum Aufschubverhalten für bestimmte Sicherungstypen finden Sie weitere Informationen unter *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 32.
10. Aktivieren Sie das Kontrollkästchen **Aktivieren** am Ende der Zeile, um den Job mit dem angegebenen Zeitplan auszuführen.
11. Überprüfen Sie die Anzahl der Wiederherstellungspunkte, die sich aus den Zeitplänen und Aufbewahrungsrichtlinien des Jobs ergeben können. 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.
12. Legen Sie im Bereich „Automatische Wiederholung für geplante Sicherungen“ in der Ansicht bzw. im Dialogfeld „Zeitplan hinzufügen“ fest, ob geplante Sicherungen nach einer fehlgeschlagenen Sicherung wiederholt werden sollen. Siehe *Angeben, ob geplante Sicherungen nach einem Fehler wiederholt werden sollen* auf Seite 41.
13. Klicken Sie auf **Speichern**.

3.8.1 Übersprungene Sicherungen

Um eine Zeitplanüberlastung zu vermeiden, wenn ein Sicherungsjob mehrmals am Tag ausgeführt wird, werden Sicherungen übersprungen, wenn:

- Ein Agent eine Sicherung startet, die nach einem tagesinternen Zeitplan geplant ist, und bereits eine Sicherung für den Job ausgeführt wird.
- Ein Agent ein Director Vault ab Version 8.60 kontaktiert, um eine Sicherung zu starten, die nach einem tagesinternen Zeitplan geplant ist, und der Vault mit Wartungsarbeiten von hoher Priorität für die Jobdaten beschäftigt ist.

Wenn E-Mail-Benachrichtigungen zentral in einer Portalinstanz konfiguriert sind, können Administratoren eine E-Mail erhalten, wenn eine Sicherung übersprungen wird. Siehe *Einrichten von E-Mail-Benachrichtigungen für Sicherungen auf mehreren Computern* auf Seite 88. Wenn der letzte für einen Job gemeldete Sicherungsstatus „Übersprungen“ war, wird dieser letzte Sicherungsstatus für den Job auf der Seite „Computer“ und der Seite „Überwachung“ angezeigt. Siehe *Anzeigen von Informationen zu Computer- und Jobstatus* auf Seite 79 und *Anzeigen und Exportieren neuer Sicherungsstatus* auf Seite 91. Der tägliche Statusbericht zeigt auch übersprungene Sicherungen an.

In einigen Portalinstanzen können Benutzer auch die Übersprungen-Rate und die 48-Stunden-Historie des Sicherungsstatus für Jobs anzeigen. Siehe *Anzeige der Übersprungen-Rate und der Sicherungsstatus-Historie* auf Seite 81.

Empfehlungen: Verringerung der Anzahl der übersprungenen Sicherungen

Wenn Sie feststellen, dass einige Sicherungen häufig übersprungen werden, können Sie Änderungen am Sicherungsjob, am Sicherungsplan oder an den Servern vornehmen, um zuverlässige Sicherungen zu gewährleisten. Beispielsweise können Sie Folgendes vornehmen:

- Die Häufigkeit von geplanten Sicherungen reduzieren.
- Die Größe von Jobs verringern.
- Systemressourcen (z. B. RAM, CPU, Storage IO) auf dem Server, auf dem der Agent ausgeführt wird, hinzufügen. Während die Ressourcen eines Servers für die regelmäßige Sicherung und Wiederherstellung von Daten ausreichen, reichen sie für die mehrfache Ausführung von Sicherungen pro Tag möglicherweise nicht aus.
- Systemressourcen zu dem Vault-Server hinzufügen.

4.9 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 Widerherstellungspunkten 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.

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

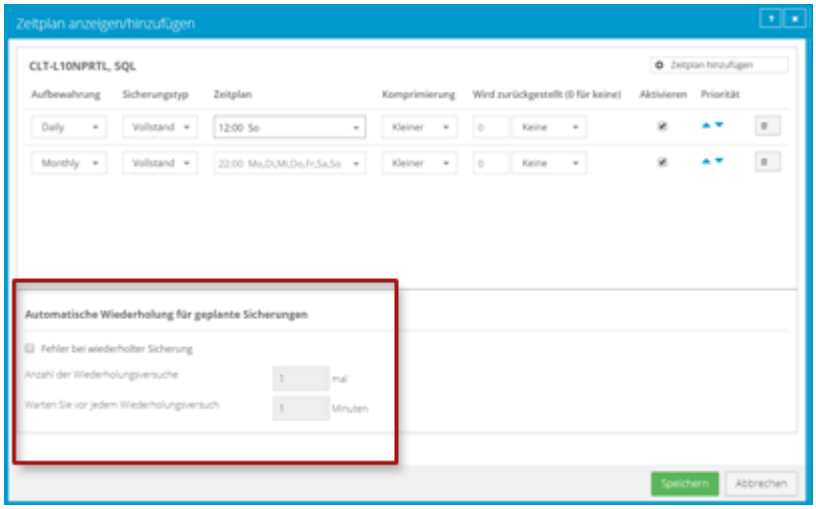
Sie können festlegen, ob geplante Sicherungen automatisch wiederholt werden sollen, wenn diese nicht erfolgreich ausgeführt werden können.

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:

1. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie in der Navigationsleiste auf **Computer**. Suchen Sie den Agent, 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.
2. 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.



3. Klicken Sie auf **Speichern**.

4.11 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 Agent 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.
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 84.

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

4.12 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 Agent 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 84.

5. Wenn Sie den Sicherungsvorgang unterbrechen möchten, klicken Sie auf **Stoppen**.

   Um das Dialogfeld „Prozessdetails“ zu schließen, klicken Sie auf **Schließen**.

5 Wiederherstellen von Linux-Dateien und -Ordnern

Nach dem Sichern von Daten von einem Linux-Computer können Sie Dateien und Ordner aus der Sicherung wiederherstellen.

Sie können auch Linux-Systeme aus BMR-Sicherungen wiederherstellen. Siehe *Wiederherstellen eines Linux-Systems aus einer BMR-Sicherung* auf Seite 54.

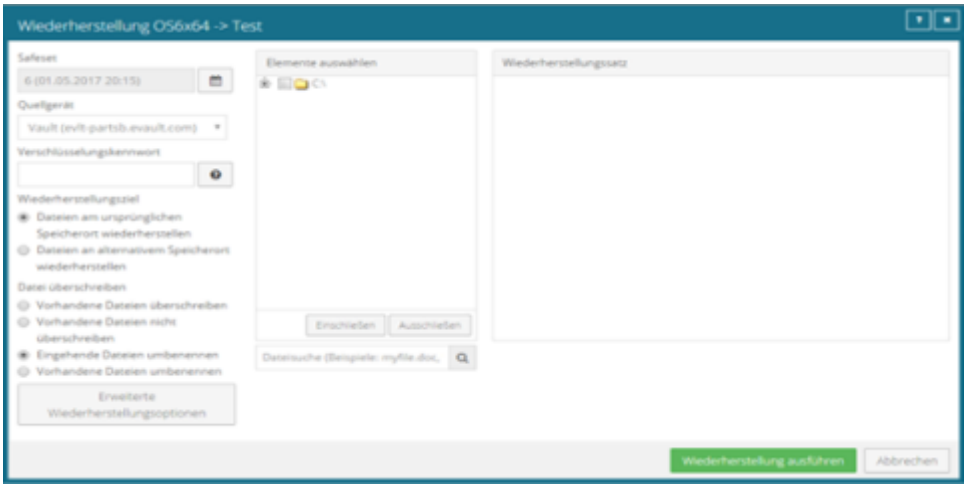
So stellen Sie Linux-Dateien und -Ordner wieder her:

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

   Die verfügbaren Computer werden in einem Raster aufgelistet.

2. Suchen Sie den Linux-Computer mit den Daten, die Sie wiederherstellen möchten, und erweitern Sie durch Klicken auf die Computerzeile seine Ansicht.
3. Klicken Sie auf die Registerkarte **Jobs**.
4. Suchen Sie den Job mit den Daten, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellung** im Menü **Aktion auswählen** des Jobs.

   Im Dialogfeld „Wiederherstellung“ wird der neueste Sicherungssatz zum Job angezeigt.



5. Gehen Sie wie folgt vor, um Daten aus einem älteren Sicherungssatz oder von SSI-Dateien (Sicherungssatz-Image) wiederherzustellen:

   - Um Daten aus einem älteren Sicherungssatz wiederherzustellen, klicken Sie auf die Kalenderschaltfläche. Klicken Sie im angezeigten Kalender auf das Datum des Sicherungssatzes, den Sie für die Wiederherstellung verwenden möchten. Klicken Sie rechts neben dem Kalender auf den spezifischen Sicherungssatz, den Sie verwenden 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.

6. Geben Sie im Feld **Verschlüsselungskennwort** das Verschlüsselungskennwort für die Daten ein. Um den Kennworthinweis anzuzeigen, klicken Sie auf die Schaltfläche **Hinweis**.
7. Wählen Sie die Option Wiederherstellungsziel.
   - Um Dateien und Ordner an dem Speicherort wiederherzustellen, an dem sie gesichert wurden, wählen Sie **Dateien am ursprünglichen Speicherort wiederherstellen** aus.
   - Um Dateien und Ordner an einem anderen Speicherort wiederherzustellen, wählen Sie **Dateien an alternativem Speicherort wiederherstellen** aus. Klicken Sie auf die Ordnerschaltfläche. Wählen Sie im Dialogfeld „Ordner auswählen“ den Speicherort für die Wiederherstellung aus und klicken Sie auf **OK**.
8. Wählen Sie eine Option zum Überschreiben. Diese Option legt fest, wie eine Datei, ein Ordner oder eine symbolische Verknüpfung an einem Speicherort wiederhergestellt wird, an dem sich eine Datei, ein Ordner oder eine symbolische Verknüpfung mit demselben Namen befindet.
   - Um ein vorhandenes Element durch ein wiederhergestelltes Element zu überschreiben, wählen Sie **Vorhandene Elemente überschreiben**.

     Hinweis: Wenn Sie versuchen, mehrere Dateien mit dem gleichen Namen an einem alternativen Speicherort wiederherzustellen und die Option **Vorhandene Elemente überschreiben** wählen, wird nur die letzte wiederhergestellte Datei beibehalten. Andere Dateien mit demselben Namen werden überschrieben.

     WICHTIG: Wenn Sie mit Agent Version 8.70 die Option **Vorhandene Elemente überschreiben** auswählen und eine Datei wiederherstellen, die den gleichen Namen wie ein Ordner am Wiederherstellungsort hat, wird der Ordner durch die Datei überschrieben. Der Ordner und sämtliche Inhalte werden entfernt.
   - Um die Wiederherstellung des Elements zu überspringen, das den gleichen Namen wie ein Element am Zielort hat, wählen Sie **Vorhandene Elemente nicht überschreiben**.
   - Um eine numerische Erweiterung (z. B. .0001) zum Namen eines *wiederhergestellten* Elements hinzuzufügen, wählen Sie **Eingehende Elemente umbenennen**. Wenn Sie beispielsweise eine Datei mit dem Namen „filename.txt“ an einem Speicherort wiederherstellen, an dem sich eine Datei mit demselben Namen befindet, wird dem **wiederhergestellten** Dateinamen eine Erweiterung hinzugefügt (z. B. „filename.txt.0001“).
   - Um eine numerische Erweiterung (z. B. .0001) zum Namen eines *wiederhergestellten* Elements hinzuzufügen, wählen Sie **Vorhandene Elemente umbenennen**. Wenn Sie beispielsweise eine Datei mit dem Namen „filename.txt“ an einem Speicherort wiederherstellen, an dem sich eine Datei mit demselben Namen befindet, wird dem *bestehenden* Dateinamen eine Erweiterung hinzugefügt (z. B. „filename.txt.0001“). Der Name der wiederhergestellten Datei ist „filename.txt“.
9. Wenn Sie die Optionen für gesperrte Dateien, Protokolldetails und Bandbreite ändern möchten, klicken Sie auf **Erweiterte Wiederherstellungsoptionen**. Legen Sie die Einstellungen im Dialogfeld

„Erweiterte Wiederherstellungsoptionen“ fest, und klicken Sie auf **OK**. Siehe *Erweiterte Wiederherstellungsoptionen* auf Seite 49.

10. Führen Sie im Feld **Elemente auswählen** eines oder mehrere der folgenden Verfahren aus, bis im Feld **Wiederherstellungssatz** die Ordner und Dateien angezeigt werden, die Sie wiederherstellen möchten:
    - Wählen Sie das Kontrollkästchen für die einzelnen Ordner und Dateien aus, die wiederhergestellt werden sollen, und klicken Sie auf **Einschließen**. Das Feld **Wiederherstellungssatz** zeigt die eingeschlossenen Ordner und Dateien. Wenn Sie einen Ordner einschließen, werden standardmäßig alle enthaltenen Unterordner und Dateien wiederhergestellt. Sie können Filter hinzufügen, falls Sie nicht alle Unterordner und Dateien wiederherstellen möchten. Siehe *Filtern von Unterverzeichnissen und Dateien beim Wiederherstellen von Daten* auf Seite 50.
    - Um Dateien oder Ordner von der Wiederherstellung auszuschließen, aktivieren Sie die Kontrollkästchen für die jeweiligen Elemente und klicken Sie auf **Ausschließen**. Das Feld **Wiederherstellungssatz** zeigt die ausgeschlossenen Ordner und Dateien. Wenn Sie einen Ordner ausschließen, werden standardmäßig alle enthaltenen Unterordner und Dateien von der Wiederherstellung ausgeschlossen. Sie können Filter hinzufügen, falls Sie nicht alle Unterordner und Dateien ausschließen möchten. Siehe *Filtern von Unterverzeichnissen und Dateien beim Wiederherstellen von Daten* auf Seite 50.
    - Um Dateien zu suchen, die wiederhergestellt oder von der Wiederherstellung ausgeschlossen werden sollen, klicken Sie auf die Schaltfläche **Suchen**. Geben Sie in das Feld **Nach Dateien suchen** die Suchkriterien ein und wählen Sie die Dateien aus. Siehe *Suchen nach wiederherzustellenden Dateien* auf Seite 52. Klicken Sie auf **Ausgewählte einschließen** oder **Ausgewählte ausschließen**. Das Feld **Wiederherstellungssatz** zeigt die eingeschlossenen oder ausgeschlossenen Dateien.
    - Um einen Einschließen- oder Ausschließen-Datensatz aus dem Feld **Wiederherstellungssatz** zu entfernen, klicken Sie neben dem Datensatz auf die Schaltfläche „Löschen“.
11. Klicken Sie auf **Wiederherstellung ausführen**.

    Im Dialogfeld „Prozessdetails“ werden der Verlauf und Fertigstellungszeitpunkt der Wiederherstellung angezeigt. Es können weitere kürzlich abgeschlossene Jobprozesse im Dialogfeld angezeigt werden. Siehe *Anzeigen von aktuellen Prozessinformationen eines Jobs* auf Seite 84.
12. Um das Dialogfeld „Prozessdetails“ zu schließen, klicken Sie auf **Schließen**. Wenn der Wiederherstellungsprozess bereits gestartet wurde, wird er weiterhin ausgeführt.

5.1 Wiederherstellen von Zugriffssteuerungslisten

Sie können Zugriffssteuerungslisten (Access Control Lists, ACLs) sichern und wiederherstellen. Bei der Wiederherstellung von ACLs auf einem Linux-Server können folgende Verhaltensweisen auftreten.

Mit ACLs wird der Zugriff von Benutzern oder Gruppen auf bestimmte Dateien gesteuert. Ähnlich wie gewöhnliche Dateiberechtigungen (z. B. „Owner“, „Group“, „World“) werden ACLs nach der ID des Benutzers/der Gruppe protokolliert. ACLs bieten eine höhere Granularität für die Zugriffssteuerung als gewöhnliche Dateiberechtigungen, und anders als gewöhnliche Berechtigungen sind sie nicht immer aktiviert.

Implementierungen von ACLs unterscheiden sich möglicherweise nach der Linux-Variante und nach dem Typ des Dateisystems. Nicht alle ACL-Implementierungen sind „portabel“ (d. h. ACLs auf einem Betriebs-

/Dateisystem sind möglicherweise nicht mit ACLs auf einem anderen Betriebs-/Dateisystem kompatibel). Außerdem müssen Sie möglicherweise die ACL-Unterstützung für eine Partition aktivieren, bevor Sie sie konfigurieren können.

Wenn Sie eine Wiederherstellung von ACLs auf einem nicht kompatiblen System versuchen (beispielsweise einem Dateisystem, das keine Unterstützung für ACLs bietet), werden die ACLs nicht wiederhergestellt. In das Sicherungsprotokoll wird eine entsprechende Fehlermeldung geschrieben.

Wenn Sie eine Wiederherstellung auf einem kompatiblen System durchführen (beispielsweise auf dem ursprünglichen System oder einem anderen System mit derselben Linux-Variante), werden auch ACLs wiederhergestellt.

Da ACLs mit Benutzer- und Gruppen-IDs verknüpft sind, können Sie Folgendes auf einem kompatiblen System beobachten:

- Wenn die Gruppe, Benutzernamen und IDs auf dem wiederhergestellten System mit denen des ursprünglichen Systems übereinstimmen, werden die ACLs mit dem gleichen Benutzernamen wie auf dem ursprünglichen System verknüpft.
- Wenn die Gruppe, Benutzernamen und IDs auf dem wiederhergestellten System nicht mit denen des ursprünglichen Systems übereinstimmen, werden die ACLs mit einem anderen Benutzer- oder Gruppennamen als auf dem ursprünglichen System verknüpft.
- Wenn die ID der Gruppe oder des Benutzernamens auf dem wiederhergestellten System nicht existiert, werden die ACLs mit der entsprechenden Benutzer- bzw. Gruppen-ID verknüpft. Wenn Sie in diesen Dateien nach ACLs suchen, werden folglich Benutzer-/Gruppen-IDs statt Benutzer-/Gruppennamen angezeigt.

5.2 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 48.

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.
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.

    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.

5.3 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 47.

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, wie beispielsweise Linux und Solaris, 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.

   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.

5.4 Erweiterte Wiederherstellungsoptionen

Beim Wiederherstellen von Daten können Sie die folgenden Optionen angeben:

Optionen für gesperrte Dateien

Beim Wiederherstellen von Daten aus einem lokalen können Sie angeben, ob gesperrte Dateien durch wiederhergestellte Dateien mit demselben Namen überschrieben werden sollen. Wählen Sie dazu eine der folgenden Optionen aus:

- **Ja, gesperrte Dateien überschreiben** – Dateien im System, die während der Wiederherstellung gesperrt sind, werden beim Neustart mit den wiederhergestellten Dateien überschrieben. Diese Option muss für Wiederherstellungen des Systemstatus oder von Systemvolumes aktiviert sein.
- **Nein, gesperrte Dateien nicht überschreiben** – Dateien im System, die während der Wiederherstellung gesperrt sind, werden beim Neustart nicht mit den wiederhergestellten Dateien mit gleichem Namen überschrieben.

Streams

Bei der Ausführung von Sicherungen werden Informationen aus Ihren Dateien in verschiedenen Streams erfasst. Die ursprünglichen, von einem Benutzer erstellten Daten werden als Datenstream bezeichnet.

Andere Informationen wie die Sicherheitseinstellungen, Daten für andere Betriebssysteme, Dateiverweise und Attribute werden in separaten Streams gespeichert.

Beim Wiederherstellen von Daten haben Sie die folgenden Optionen zur Auswahl:

- **Alle Streams wiederherstellen** – Stellt alle Informationsstreams wieder her. Verwenden Sie diese Option, wenn Sie Dateien auf einem System mit identischer Plattform wiederherstellen.
- **Nur Datenstreams wiederherstellen** – Wählen Sie diese Option für plattformübergreifende Wiederherstellungen aus. Mit dieser Option entstehen keine Konflikte aufgrund systemspezifischer Datenströme.

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.

5.5 Filtern von Unterverzeichnissen und Dateien beim Wiederherstellen von Daten

Wenn Sie die Daten wiederherstellen möchten, können Sie Order und Dateien festlegen, die aus der Sicherung wiederhergestellt werden sollen.

Wenn Sie einen Ordner in eine Wiederherstellung einschließen, sind die Unterverzeichnisse und Dateien in diesem Ordner ebenfalls standardmäßig eingeschlossen. Wenn Sie nur einen Teil der Unterverzeichnisse oder Dateien in einem Ordner wiederherstellen möchten, können Sie Filter zum Einschließen-Datensatz hinzufügen. Sie können beispielsweise einen Filter hinzufügen, damit Dateien in einem Ordner nur wiederhergestellt werden, wenn sie die .pl-Erweiterung haben.

Wenn Sie einen Ordner aus einer Wiederherstellung ausschließen, sind die Unterverzeichnisse und Dateien in diesem Ordner ebenfalls standardmäßig ausgeschlossen. Wenn Sie einen Teil der Unterverzeichnisse

oder Dateien in einem Ordner ausschließen möchten, können Sie Filter zum Ausschließen-Datensatz hinzufügen.

So können Sie Unterverzeichnisse und Dateien beim Wiederherstellen von Daten filtern:

1. Beachten Sie beim Wiederherstellen von Daten das Feld **Wiederherstellungssatz**.
2. Wenn keine bearbeitbaren Felder für einen Ordner-Einschließen- oder Ausschließen-Datensatz, in dem Sie Unterverzeichnisse und Felder filtern möchten, angezeigt werden, klicken Sie in der Ordnerzeile auf die Schaltfläche **Bearbeiten**. 
3. Führen Sie im Feld **Wiederherstellungssatz** für jeden eingeschlossenen Ordner, in dem bestimmte Unterverzeichnisse oder Dateien eingeschlossen werden sollen, eine oder mehrere der folgenden Aktionen aus:
   - Um bestimmte Unterverzeichnisse in die Wiederherstellung einzuschließen, geben Sie im Feld **Ordnerfilter** die Namen der entsprechenden Unterverzeichnisse ein. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. Um beispielsweise nur Unterverzeichnisse in einer Wiederherstellung einzuschließen, deren Namen mit „-aktuell“ enden oder mit „2015“ beginnen, geben Sie folgenden Filter ein: *-aktuell, 2015*

     Hinweis: Das Sternchen (*) ist das einzige unterstützte Platzhalterzeichen in Filterfeldern.
   - Um bestimmte Dateien wiederherzustellen, geben Sie im Feld **Dateifilter** die Namen der entsprechenden Dateien ein. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. Um beispielsweise nur Dateien mit .pl-Erweiterung wiederherzustellen, geben Sie folgenden Filter ein: *.pl

     Hinweis: Das Sternchen (*) ist das einzige unterstützte Platzhalterzeichen in Filterfeldern.
   - Um den angegebenen Ordner ohne seine Unterverzeichnisse wiederherzustellen, deaktivieren Sie das Kontrollkästchen **Rekursiv**.
   - Um die Unterverzeichnisse des Ordners wiederherzustellen, markieren Sie das Kontrollkästchen **Rekursiv**.
4. Führen Sie im Feld **Wiederherstellungssatz** für jeden ausgeschlossenen Ordner, in dem bestimmte Unterverzeichnisse oder Dateien ausgeschlossen werden sollen, eine oder mehrere der folgenden Aktionen aus:
   - Um bestimmte Unterverzeichnisse aus der Wiederherstellung auszuschließen, geben Sie im Feld **Ordnerfilter** die Namen der entsprechenden Unterverzeichnisse ein. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. Um beispielsweise Unterverzeichnisse aus einer Wiederherstellung auszuschließen, deren Namen mit „-alt“ enden oder mit „2001“ beginnen, geben Sie folgenden Filter ein: *-alt, 2001*

     Hinweis: Das Sternchen (*) ist das einzige unterstützte Platzhalterzeichen in Filterfeldern.
   - Um bestimmte Dateien von der Wiederherstellung auszuschließen, geben Sie im Feld **Dateifilter** die Namen der entsprechenden Dateien ein. Trennen Sie mehrere Namen mit Kommas, und verwenden Sie das Sternchen (*) als Platzhalterzeichen. beispielsweise nur Dateien aus einer Wiederherstellung auszuschließen, die eine .pl-Erweiterung haben, geben Sie folgenden Filter ein: *.pl

     Hinweis: Das Sternchen (*) ist das einzige unterstützte Platzhalterzeichen in Filterfeldern.

- Um den angegebenen Ordner ohne seine Unterverzeichnisse auszuschließen, deaktivieren Sie das Kontrollkästchen **Rekursiv**.
- Um die Unterverzeichnisse des Ordners auszuschließen, markieren Sie das Kontrollkästchen **Rekursiv**.

5. Klicken Sie auf **Wiederherstellung ausführen**.

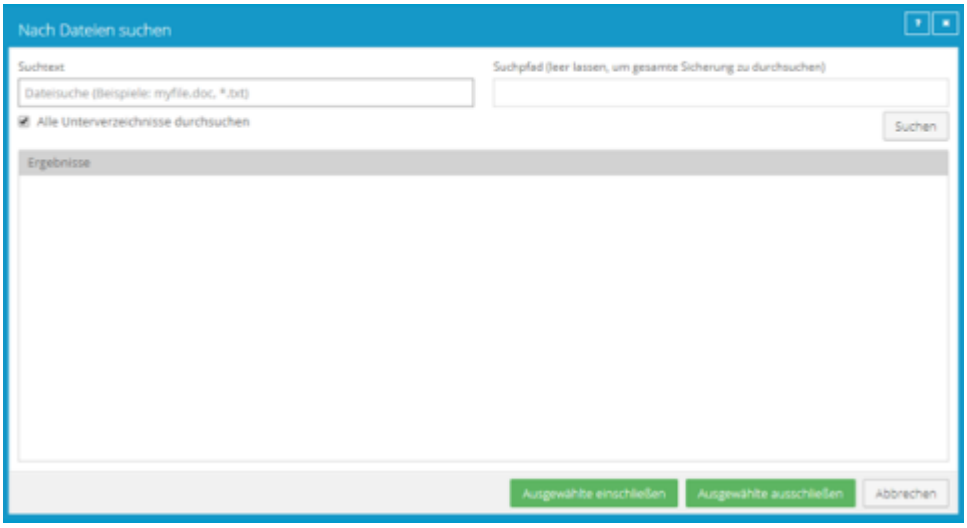
5.6 Suchen nach wiederherzustellenden Dateien

Wenn Sie die Daten wiederherstellen möchten, können Sie nach den wiederherzustellenden Dateien suchen oder diese von der Wiederherstellung ausschließen.

So suchen Sie nach wiederherzustellenden Dateien:

1. Klicken Sie im Dialogfeld „Wiederherstellung“ auf die Schaltfläche **Suchen**.

   Das Dialogfeld „Nach Dateien suchen“ wird angezeigt.



2. Geben Sie in das Feld **Suchtext** den gesuchten Dateinamen ein. Sie können das Sternchen (*) als Platzhalterzeichen verwenden.
3. Um nach Dateien in einem bestimmten Ordner der Sicherung zu suchen, geben Sie in das Feld **Suchpfad** den gewünschten Pfad ein.
4. Um nur nach den Dateien im angegebenen Ordner zu suchen, deaktivieren Sie das Kontrollkästchen **Alle Unterverzeichnisse durchsuchen**.
5. Klicken Sie auf **Suchen**.

   Im Feld „Ergebnisse“ werden die Dateien aufgeführt, die die Suchkriterien erfüllen.
6. Wählen Sie im Feld **Ergebnisse** die Dateien aus, die berücksichtigt und ausgeschlossen werden sollen. Um mehrere aufeinanderfolgende Elemente auszuwählen, halten Sie die Umschalttaste gedrückt und klicken Sie auf das erste und letzte Element in der Liste. Um mehrere Elemente auszuwählen, halten Sie die Strg-Taste gedrückt und klicken Sie auf die gewünschten Elemente.
7. Führen Sie eine der folgenden Aktionen aus:
   - Um die ausgewählten Dateien wiederherzustellen, klicken Sie auf **Ausgewählte einschließen**.

- Um die ausgewählten Dateien von der Wiederherstellung auszuschließen, klicken Sie auf **Ausgewählte ausschließen**.

6 Wiederherstellen eines Linux-Systems aus einer BMR-Sicherung

Sie können gesamte Linux-Server aus Bare Metal Restore (BMR)-Sicherungen wiederherstellen. Eine BMR-Sicherung umfasst Folgendes:

- Eine ISO-Datei zum Starten des Zielsystems und zum Ausführen der Wiederherstellung. Die ISO-Datei wird während einer BMR-Sicherung auf dem Quellsystem erstellt und im Vault gesichert.
- Eine Sicherung aller für das System erforderlicher Ordner und Dateien im Vault. Standardmäßig umfasst eine Linux-BMR-Sicherung alle Ordner und Dateien aus dem Stammverzeichnis (/), wobei einige Dateien ausgeschlossen werden können.

Wenn Sie einen Linux-Server aus einer BMR-Sicherung wiederherstellen, muss der Zielrechner Folgendes aufweisen:

- Mindestens 4 GB RAM.
- Denselben Boot-Typ (BIOS oder UEFI) wie das Quellsystem und kompatible Hardware.
- Festplatten, die gleich groß oder größer sind als die Laufwerke des Quellsystems.
- Eine Verbindung zum Netzwerk, damit der Rechner mit dem Vault kommunizieren kann.

Hinweis: Wiederherstellungen auf Systemen mit unterschiedlichen Firmwaretypen werden nicht unterstützt.

So stellen Sie ein Linux-System aus einer BMR-Sicherung wieder her:

1. Führen Sie eine der folgenden Aktionen aus:
   - Wenn das Quellsystem noch verfügbar ist, kopieren Sie die Datei „/Bare_Metal_Restore_Image.iso“ aus dem Stammverzeichnis (/) des Quellsystems auf einen anderen Rechner.
   - Befolgen Sie das Verfahren *Von anderem Computer wiederherstellen*, um die Datei „/Bare_Metal_Restore_Image.iso“ aus der Linux-BMR-Sicherung auf einem anderen Rechner wiederherzustellen. Siehe *Wiederherstellen von Daten von einem anderen Computer* auf Seite 48.
2. Erstellen Sie ein automatisch startendes USB-Gerät, eine CD oder DVD aus der Datei „Bare_Metal_Restore_Image.iso“ und stellen Sie es bzw. sie auf dem Zielsystem bereit.
3. Starten Sie das Zielsystem über die startbare Datei.
4. Führen Sie eine der folgenden Aktionen aus:
   - Wenn der Bildschirm „Relax-and-Recover“ angezeigt wird, wählen Sie *sourceSystemName* **wiederherstellen** und drücken Sie dann die Eingabetaste. Dieser Bildschirm wird angezeigt, wenn das geschützte System BIOS-basiert ist.

     Wählen Sie nicht die Option für die automatische Wiederherstellung von *sourceSystemName* aus, da das System sonst nicht erfolgreich gestartet werden kann.
   - Wenn der folgende Bildschirm angezeigt wird, wählen Sie **Relax-and-Recover (Kein sicherer Start)** aus und drücken Sie dann die Eingabetaste. Dieser Bildschirm wird angezeigt, wenn das geschützte System UEFI-basiert ist.
5. Melden Sie bei Aufforderung zur Anmeldung als root-Benutzer an.

Hinweis: Wenn zunächst keine Aufforderung zur Anmeldung angezeigt wird, drücken Sie die Eingabetaste.

6. (Optional) Um sicherzustellen, dass die Verbindung zum Vault aktiv ist, pingen Sie die IP-Adresse des Vaults an. Wenn Probleme mit der Netzwerkverbindung bestehen, ändern Sie die Netzwerkeinstellungen.
7. Geben Sie den folgenden Befehl ein:

   ```
   ./bmragent
   ```

8. Geben Sie im Bildschirm „Vault-Anmeldung“ die Informationen für die Verbindung mit dem Vault ein, in dem die BMR-Sicherung gespeichert ist.

   Geben Sie im Feld „Adresse“ die IP-Adresse oder den vollständig qualifizierten Domänennamen des Vaults ein. Geben Sie im Feld „Port“ die Portnummer für die Verbindung zum Vault ein (standardmäßig 2546). Geben Sie in den Feldern „Konto“, „Benutzername“ und „Kennwort“ ein Konto und die Anmeldeinformationen für die Sicherung ein.
9. Verwenden Sie im Bildschirm „Geschützte Server“ die Nach-oben- und Nach-unten-Tasten, um den wiederherzustellenden geschützten Server auszuwählen, und drücken Sie dann die Eingabetaste.
10. Verwenden Sie im Bildschirm „Jobliste“ die Nach-oben- und Nach-unten-Tasten, um den wiederherzustellenden BMR-Job auszuwählen, und drücken Sie dann die Eingabetaste.
11. Verwenden Sie im Bildschirm „Sicherungssatz“ die Nach-oben- und Nach-unten-Tasten, um die wiederherzustellende Sicherung auszuwählen, und drücken Sie dann die Eingabetaste.
12. Geben Sie im Bildschirm „Wiederherstellung starten“ das Verschlüsselungskennwort für den BMR-Sicherungsjob ein.

    Drücken Sie in der Zeile BESTÄTIGEN die rechte Pfeiltaste, um „Ja“ auszuwählen, und drücken Sie dann die Eingabetaste.
13. Wenn das Zielsystem größer als das geschützte System ist, wird die Aufforderung *Layout des neu erstellten Datenträgers bestätigen oder zum vorherigen Schritt zurückkehren* angezeigt. Drücken Sie die Eingabetaste, um die Standardoption auszuwählen.

    Wenn in dieser Phase ein Fehler auftritt, rufen Sie bitte http://relax-and-recover.org/support/ auf, um Relax-and-Recover-Support zu erhalten.
14. Wenn das Zielsystem eine größere Festplatte als das geschützte System hat, wir die Aufforderung *Bestätigen, dass wiederhergestellte Konfigurationsdateien in Ordnung sind, oder sie bei Bedarf anpassen* angezeigt. Drücken Sie die Eingabetaste und drücken Sie sie dann erneut, um die Standardoptionen auszuwählen.

    Die Systemwiederherstellung beginnt. Die Wiederherstellungsdauer hängt von der Größe der Sicherung ab.

    Wenn die Wiederherstellung sehr lange dauert, wird möglicherweise ein leerer Bildschirm angezeigt. Drücken Sie zum Aktualisieren die Eingabetaste.

    Sobald die Wiederherstellung abgeschlossen ist, wird die Meldung *Bare-Metal-Wiederherstellung abgeschlossen* angezeigt, gefolgt von der RESCUE-Eingabeaufforderung.
15. Führen Sie den folgenden Befehl aus, um das Wiederherstellungsprotokoll anzuzeigen:
    `./xlogcat jobName/RSTyyyymmdd-hhmmss.XLOG | tail -n 25`

Dabei steht *jobName* für den Namen des BMR-Jobs, aus dem Sie das System wiederhergestellt haben, und *yyyymmdd-hhmmss* ist das Datum und die Uhrzeit der Wiederherstellung.

Überprüfen Sie die Angaben im Wiederherstellungsprotokoll. Prüfen Sie, ob die Wiederherstellung ohne Fehler abgeschlossen wurde, und vergewissern Sie sich, dass die wiederhergestellte Systemgröße richtig ist.

16. Starten Sie das System neu.

    Je nach Plattform und Konfiguration des Quellsystems wird das System automatisch einmal oder zweimal neu gestartet.

17. Melden Sie sich am wiederhergestellten System mit den Anmeldeinformationen des geschützten Systems an und vergewissern Sie sich, dass das System funktioniert.

7 Wiederherstellen eines Linux-Systems ohne BMR-Sicherung

Sie können ganze Linux-Systeme aus BMR-Sicherungen wiederherstellen. Siehe *Wiederherstellen eines Linux-Systems aus einer BMR-Sicherung* auf Seite 54.

Wenn ein Linux-System nicht durch eine BMR-Sicherung geschützt ist, müssen Sie das System mit den in diesem Abschnitt beschriebenen Verfahren wiederherstellen. In diesem Abschnitt werden die Ressourcen beschrieben, die mindestens erforderlich sind, um ein Dateisystem in dem Zustand wiederherzustellen, den es bei der letzten Systemsicherung aufwies.

Das grundlegende Wiederherstellungsverfahren lautet wie folgt:

1. Installieren Sie das minimale Betriebssystem, einschließlich Netzwerk.
2. Installieren und konfigurieren Sie den Agenten.
3. Stellen Sie den gesicherten Systemzustand sowie die Programme und Daten mithilfe des Agenten wieder her.
4. Führen Sie Wartungsaufgaben für die M-Wiederherstellung durch.
5. Überprüfen Sie die Wiederherstellung.

Stellen Sie vor der Durchführung einer Wiederherstellung sicher, dass Ihre Hardwarekonfiguration für die Programme, die Daten und den Systemzustand des geschützten Systems ausreicht.

7.1 Hardwareanforderungen

Der lokale Speicher auf dem System muss unbedingt für eine vollständige Wiederherstellung der Programme, des Systemstatus und der Daten ausreichen. Andernfalls schlägt die Wiederherstellung fehl, und das System verbleibt möglicherweise in einem undefinierten Zustand.

Wenn Konfigurationsdateien für das Betriebssystem von bestimmten IDs der installierten Hardware abhängen (wie der MAC-Adresse der Netzwerkkarte), stellen Sie sicher, dass diese Informationen bekannt sind, da die Werte möglicherweise von denen abweichen, die bei der Sicherung des Systems durch den Agenten galten.

Hinweis: Bei Durchführung einer vollständigen Systemwiederherstellung (DR) müssen Sie sicherstellen, dass genügend Speicherplatz für die Erstellung großer Wiederherstellungsprotokolle durch den Agenten sowie potenzieller anderer Protokolle oder Überwachungsdaten des Betriebssystems verfügbar ist. Bei der Protokollierung auf Dateiebene für ein System, das ein großes Dateisystem umfasst, kann ein großes Protokoll generiert werden, das potenziell den verfügbaren oder zugewiesenen Speicherplatz ausfüllt. Wenn sich die Protokolle auf derselben Partition befinden wie das Root-Dateisystem, kann dies den Start des Betriebssystems verhindern.

7.2 Softwareanforderungen

Stellen Sie sicher, dass die entsprechenden Installationsmedien verfügbar sind. Die Systemsoftware umfasst mindestens Folgendes:

- Installationsmedien, die mit denen für das ursprüngliche System identisch sind.
- Ggf. alle erforderlichen Betriebssystem-Patches zum Installieren des Agenten, wie in den Installationsanweisungen für den Agenten und das Betriebssystem beschrieben.

- Installationsmedien für den Agenten, die mit denen für das ursprüngliche System identisch sind.

7.3 Wiederherstellungsschritte

In diesem Abschnitt werden die Schritte für die Durchführung einer Systemwiederherstellung beschrieben.

Installieren des minimalen Betriebssystems

Befolgen Sie die Anweisungen im Handbuch Ihres Betriebssystems und auf den Installationsmedien, um ein minimales Betriebssystem zu installieren.

- Wenn Sie zum Partitionieren des Laufwerks/der Laufwerke aufgefordert werden, stellen Sie sicher, dass die Partitionen groß genug für die Wiederherstellung sind. Sie müssen mindestens so groß sein wie die ursprünglichen Partitionen.
- Bei einer Wiederherstellung über das Netzwerk müssen TCP/IP-Netzwerkdienste installiert und entsprechend konfiguriert sein und es muss eine Verbindung zwischen dem System und dem Sicherungs-Vault bestehen.
- Bei einer Wiederherstellung von einem Verzeichnis auf einem Datenträger muss ausreichender Speicherplatz für alle wiederhergestellten Daten vorhanden sein.

Installieren und Konfigurieren des Agenten

1. Installieren Sie den Agenten für Ihr Betriebssystem.
2. Konfigurieren Sie den Agenten. Registrieren Sie den Agenten erneut im Vault, auf dem die Daten gesichert wurden.
3. Synchronisieren Sie den Job, um sicherzustellen, dass lokale Kopien der Jobkataloge erstellt werden.

Wiederherstellen des gesicherten Systems

1. Starten Sie eine Wiederherstellung.
2. Wählen Sie die Dateien aus, die wiederhergestellt werden sollen. Der Agent stellt die meisten Dateien an ihren ursprünglichen Speicherorten wieder her und schützt sie vor zahlreichen bekannten Wiederherstellungsproblemen (für Dateisysteme, die an ihren Standardorten gemountet sind). Einige Dateien können jedoch nach einer Wiederherstellung zu unvorhersehbaren Ergebnissen führen. Diese Dateien variieren und können im Allgemeinen problemlos an alternativen Speicherorten wiederhergestellt werden.
3. Stellen Sie sicher, dass die Dateien nicht in einem Dateisystem wiederhergestellt werden, das schreibgeschützt gemountet ist.

Hinweis: Der Agent verhindert Wiederherstellungen von Dateien an kritischen Orten, aber nicht alle kritischen Orte werden immer erkannt.

Nach Abschluss des Wiederherstellungsverfahrens kann die Integrität der Wiederherstellung überprüft werden.

Durchführen von Wartungsaufgaben nach der Wiederherstellung

Wenn nach der Wiederherstellung Änderungen an der Konfiguration des wiederhergestellten Systems erforderlich sind, sollten sie jetzt durchgeführt werden. Bekannte Wartungsschritte nach der Wiederherstellung sind im Folgenden aufgeführt.

Überprüfen der Wiederherstellung

Überprüfen Sie nach Abschluss des Wiederherstellungsverfahrens, ob die Wiederherstellung vollständig und korrekt durchgeführt wurde. Bei der Planung der Systemwiederherstellung sollten Sie alle Jobs auflisten und testen. Welche Jobs genau zur Überprüfung ausgeführt werden müssen, hängt von der Anwendungsumgebung und der Wichtigkeit des Systems ab.

Nach dem Wiederherstellen des Systems muss die Integrität der Wiederherstellung überprüft werden. Der Test kann ganz einfach sein, indem Sie beispielsweise eine duplizierte Datei in einer anderen Verzeichnisstruktur platzieren und auf Unterschiede innerhalb der Datei testen. Vergewissern Sie sich dann, dass die Datei mithilfe einer bekannten Anwendung geöffnet werden kann und dass Sie E-Mails an eine bekannte Adresse senden können. Der Test kann auch komplex sein, wie die Ausführung einer SQL-Abfrage für einen bekannten Satz von Datenbanken.

Bei jeder Art von Test müssen sowohl die Liste als auch der Test während des normalen Systembetriebs geplant und ausgeführt werden.

7.4 Probleme bei der Wiederherstellung

Falls ein Wiederherstellungsjob fehlschlägt, stellen Sie sich die folgenden Fragen:

- Wurde das System mit derselben Betriebssystemversion wiederhergestellt?
- Welche möglichen Unterschiede gab es bei den Hardware- oder Softwareeinstellungen, die die Wiederherstellung möglicherweise beeinträchtigt haben?
- Wurden in der Fehlerprotokolldatei Fehler berichtet?
- Waren alle erforderlichen Treiber installiert?
- Wurden die anwendbaren Betriebssystem-Patches hinzugefügt?
- War ausreichender Speicherplatz für alle wiederhergestellten Daten vorhanden?

8 Sichern und Wiederherstellen von Oracle-Datenbanken mit dem Oracle-Plug-in

Das Oracle Plug-in ist ein Add-On für den Linux-Agenten, mit dem Sie Datenbanksicherungen von Oracle-Datenbanken ausführen können.

Das Plug-in wird zusammen mit dem Agenten auf dem Datenbankhost installiert.

Ein Benutzer, in der Regel ein Datenbankadministrator, konfiguriert die Sicherung über das Portal oder die alte Windows CentralControl. Ein Benutzer kann einen Zeitplan für die Datenbanksicherung festlegen. Zu den jeweils festgelegten Zeitpunkten sendet der Agent dann (mithilfe des Oracle Plug-ins) Datenbankinformationen an den Vault.

Das Oracle Plug-in bietet ARCHIVELOG-basierte, Nicht-RMAN-Sicherungen vollständiger Online-Datenbankinstanzen. Sämtliche nichttemporäre Tablespaces und Instanzparameterdateien werden automatisch gesichert.

Vollständige und teilweise Datenbanken werden über gewöhnliche, vom Benutzer verwaltete Oracle-Wiederherstellungsmechanismen wiederhergestellt.

Agenten geben Datenbanken mithilfe von Oracle-Dienstnamen an. Sie erfordern keine ORACLE_HOME-Anpassung auf Skript- oder Sicherungsebene.

Datenbank-Kennwörter werden zur Erhöhung der Sicherheit über skriptbasierte Methoden verschlüsselt.

Einschränkungen

- Nur lokale, festplattenbasierte Datenbanken mit einer Instanz werden gesichert.
- Datenbank-Cluster werden nicht gesichert.
- Unformatierte Medien werden nicht gesichert.
- Remote-Datenbanken werden nicht gesichert.
- Die Datenbank muss sich im ARCHIVELOG-Modus befinden und der Benutzer, der die Sicherung konfiguriert, muss über SYSDBA-Privilegien verfügen.

8.1 Installieren des Oracle Plug-ins für Linux

Installieren Sie das Oracle Plug-in mit dem Linux-Agenten, um Oracle-Datenbanken zu schützen. Informationen zu unterstützten Plattformen und Datenbankversionen finden Sie im Oracle-Plug-in für Linux-Versionshinweisen.

Um herauszufinden, welche Oracle-Version installiert ist, können Sie `BANNER` in `V$VERSION` oder `VERSION` in `V$INSTANCE` abfragen:

```
SELECT banner
  FROM v$version

SELECT version
  FROM v$instance
```

Das Oracle Plug-in findet die TNS-Namensliste (`tnsnames.ora`) *ausschließlich* unter dem globalen Speicherort `/etc/oratab`. Dabei kann es sich um eine Kopie oder um eine symbolische Verknüpfung mit der `tnsnames.ora` handeln, mit der der Listener gestartet wurde.

Das Installationskit des Oracle Plug-ins wird als tar.gz-Datei zur Verfügung gestellt. Sie müssen das Oracle Plug-in auf dem System mit dem Oracle-Datenbankserver installieren. Der Linux-Agent muss vor dem Plug-in installiert werden.

Für die Installation des Oracle Plug-ins für Linux sind Root-Privilegien für das Zielsystem erforderlich.

So installieren Sie das Oracle Plug-in für Linux:

1. Laden Sie das Installationspaket zum Oracle Plug-in für Linux (tar.gz) auf dem Rechner herunter, auf dem Sie das Plug-in installieren möchten.
2. Führen Sie den folgenden Befehl aus, um die Dateien aus dem Installationspaket zu extrahieren:

   ```
   tar -zxf packageName.tar.gz
   ```

   packageName steht für den Namen des Installationskits des Oracle Plug-ins.
3. Führen Sie den folgenden Befehl aus, um das Verzeichnis für das Installationskit des Oracle Plug-ins zu ändern:
   ```
   cd packageName
   ```
4. Führen Sie den folgenden Befehl aus, um die Installation zu starten:

   ```
   ./install.sh
   ```
5. Befolgen Sie die Installationsanweisungen auf dem Bildschirm.

8.2 Hinzufügen von Oracle Datenbank-Sicherungsjobs

Das Oracle Plug-in führt eine von der Oracle Corporation als „inkonsistent“ bezeichnete vollständige Datenbanksicherung durch, für die die Datenbank im Modus „ARCHIVELOG“ ausgeführt werden muss. Während einer Live-Sicherung werden alle Änderungen an der Datenbank in archivierte Protokolle geschrieben. Der Datenbankadministrator muss sicherstellen, dass sich die Datenbank im Modus „ARCHIVELOG“ befindet.

Das Oracle Plug-in sichert Wiederholungs- und Archivierungsprotokolle, die während der Ausführung des Datenbanksicherungsjobs erstellt werden. Beispiel: Wenn ein Oracle-Datenbanksicherungsjob jeden Tag von 22:00 bis 01:00 Uhr ausgeführt wird, sichert das Plug-in Wiederholungs- und Archivierungsprotokolle, die zwischen 22:00 und 01:00 Uhr erstellt werden. Sichern Sie Protokolle, die nach Ausführung des Oracle-Datenbanksicherungsjobs erstellt wurden, jeden Tag zu einem anderen Zeitpunkt anhand eines lokalen System- . Bei Ausführung eines lokalen System- können Sie die Datenbank auf einen Zeitpunkt zurücksetzen, der nach dem Zeitpunkt liegt, zu dem der Oracle-Datenbanksicherungsjob ausgeführt wurde.

Um sicherzustellen, dass archivierte Protokolldateien nicht zu viel Speicherplatz auf Ihrem System beanspruchen, können Sie über das Oracle Plug-in archivierte Wiederholungsprotokolle nach einer erfolgreichen Sicherung löschen. Diese Funktionalität ist bei Verwendung des Oracle Plug-ins für den Linux-Agent ab Version 8.60 verfügbar. Wenn Sie angeben, dass archivierte Protokolle nach einer Sicherung gelöscht werden sollen, stellen Sie sicher, dass die Protokolle mit einem lokalen System- gesichert werden.

Um die Daten zu sichern, können Sie den Sicherungsjob manuell ausführen oder einen geplanten Sicherungsjob einrichten. 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 32.

So fügen Sie einen Oracle Datenbank-Sicherungsjob hinzu:

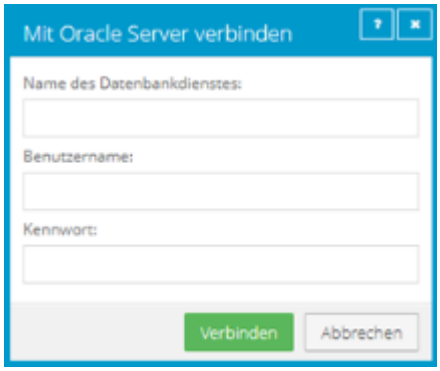
1. Klicken Sie in der Navigationsleiste auf **Computer**.

   Die Seite „Computer“ zeigt registrierte Computer an.

2. Suchen Sie den Computer mit dem Oracle Plug-in und erweitern Sie durch Klicken auf die jeweilige Computerzeile die Ansicht.
3. Klicken Sie auf die Registerkarte **Jobs**.

   Wenn keine gültige Vault-Verbindung für den Computer verfügbar ist, können Sie nicht auf die Registerkarte mit den Jobs zugreifen.

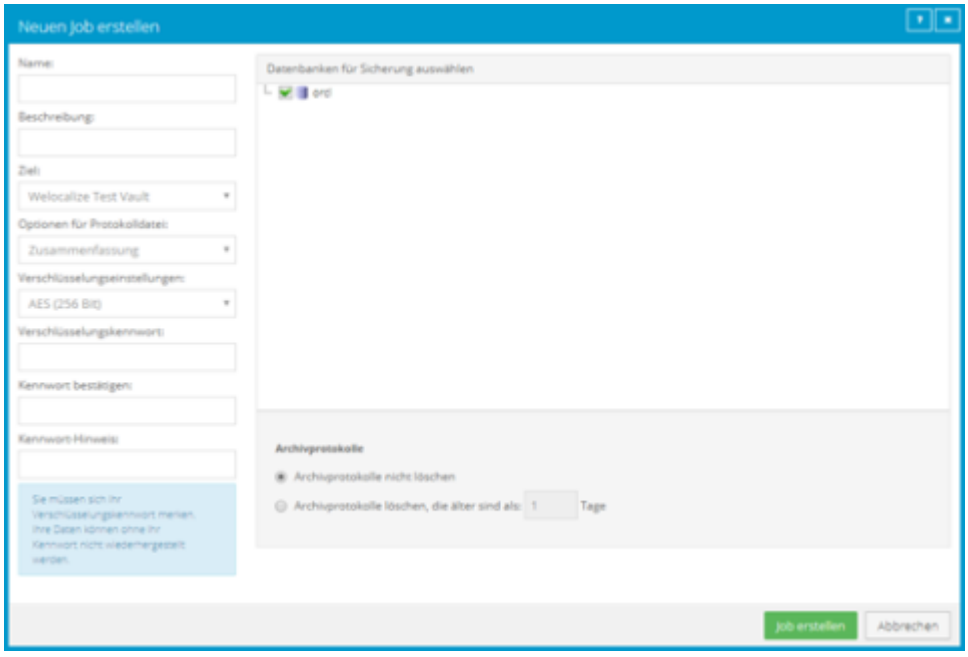
4. Klicken Sie im Menü **Jobaufgabe auswählen** auf **Neuen Job für Oracle erstellen**.
5. Geben Sie im Dialogfeld „Mit Oracle Server verbinden“ folgende Informationen an:
   - Geben Sie in das Feld **Datenbankdienstname** den Namen der zu sichernden Datenbank ein.
   - Geben Sie im Feld **Benutzername** den Namen eines Benutzers ein, der über SYSDBA-Privilegien verfügt.
   - Geben Sie im Feld **Kennwort** das Kennwort des angegebenen Benutzers ein.

6. Klicken Sie auf **Verbinden**.
7. 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 29.
   - Neue Sicherungsjobs verwenden die Verschlüsselungsmethode AES (256 Bit). Vorhandene Jobs können andere Verschlüsselungsmethoden nutzen. Siehe *Verschlüsselungseinstellungen* auf Seite 30.
   - Geben Sie in die Felder **Kennwort** und **Kennwort bestätigen** ein Verschlüsselungskennwort ein. Sie können auch einen Kennworthinweis in das Feld **Kennworthinweis** eingeben.



8. Wählen Sie im Feld **Datenbanken für die Sicherung auswählen** die zu sichernde Datenbank aus.
9. Führen Sie eine der folgenden Aktionen aus:
   - Um archivierte Oracle-Wiederholungsprotokolle auf dem System zu lassen, klicken Sie auf **Archivprotokolle nicht löschen**.
   - Um archivierte Oracle-Wiederholungsprotokolle nach einer erfolgreichen Sicherung zu löschen, klicken Sie auf **Archivprotokolle löschen, die älter sind als [...] Tage** klicken. Geben Sie die Anzahl der Tage ein, nach denen archivierte Protokolle gelöscht werden können.
10. Klicken Sie auf **Speichern**.

    Der Job wird erstellt und das Dialogfeld „Zeitplan anzeigen/hinzufügen“ wird angezeigt. Sie können nun einen Zeitplan zum Ausführen der Sicherung erstellen. Klicken Sie auf **Abbrechen**, wenn Sie aktuell keinen Zeitplan erstellen möchten.

    Weitere Informationen zum Ausführen und Planen von Sicherungsjobs finden Sie unter *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 32.

7.2.1 Info zu Oracle-Sicherungen

Das Oracle-Plug-in für den Linux-Agenten führt eine von der Oracle Corporation als „inkonsistent“ bezeichnete vollständige Datenbanksicherung durch, für die die Datenbank im Modus ARCHIVELOG ausgeführt werden muss. Während einer Live-Sicherung werden alle Änderungen an der Datenbank in Archivprotokolle geschrieben. Der DBA muss sicherstellen, dass sich die Datenbank im Modus ARCHIVELOG befindet.

```
SELECT log_mode
FROM v$database
```

Der Wert ARCHIVELOG muss zurückgegeben werden. Versetzen Sie andernfalls die Datenbank mithilfe des normalen Oracle-Verfahrens in den Modus ARCHIVELOG. Die normale Vorgehensweise sieht folgendermaßen aus:

```
> shutdown normal
> startup mount
> alter database archivelog;
> archive log start
> alter database open
```

In Oracle wird dies direkt über SQL*Plus ausgeführt. Sie können die Datenbank auch bei der anfänglichen Einrichtung in den Modus ARCHIVELOG versetzen. Alternativ können Sie die Benutzeroberfläche von Enterprise Manager oder andere DBA-Tools verwenden.

Vor dem Beginn eines Sicherungsjobs darf sich kein Tablespace im Sicherungsmodus befinden. Dies können Sie folgendermaßen prüfen:

```
SELECT d.file_name, b.status
 FROM dba_data_files d, v$backup b
 WHERE b.file# = d.file_id;
```

Wenn Dateien mit dem Status AKTIV angezeigt werden, kann der Sicherungsjob nicht gestartet werden.

Hinweis: Nach dem erfolgreichen Abschluss einer Sicherung belässt der Agent die Datenbank in einem geeigneten Zustand.

Damit Sie mit dem Oracle Plug-in Sicherungsjobs erstellen können, muss im Vault eine Lizenz verfügbar sein. Weitere Informationen finden Sie im Betriebshandbuch des Vault.

7.2.2 Funktionsweise von Sicherungen

Nach dem Start einer Sicherung durchläuft das Oracle Plug-in für den Linux-Agenten alle nicht-TEMPORÄREN Tablespaces (einschließlich ONLINE-, OFFLINE- und READONLY-Tablespaces). Alle ONLINE-Tablespaces werden in den Modus ARCHIVELOG versetzt, in dem ein Snapshot der Dateien des Tablespace erstellt wird. Die Komponentendateien des Tablespace werden gesichert. Wenn die Sicherung der Dateien eines ONLINE-Tablespace abgeschlossen ist, kehrt der Tablespace in den normalen Modus zurück.

Nach dem Sichern aller Tablespaces löscht das Plug-in alle ausstehenden Wiederholungsprotokolle und sichert die generierten Archivprotokolle. Bei diesen Protokollen handelt es sich stets um neue Dateien.

Die Instanzkontrolldateien werden sowohl als Binärdateien als auch als Verlaufsprotokolleinträge gesichert. Die Instanzparameterdateien (**init**<ORACLE_SID>**.ora** und/oder **spfile**<ORACLE_SID>**.ora**, je nach verwendeter Oracle-Version und -Konfiguration) und die Oracle-Kennwortdatei werden ebenfalls gesichert.

Hinweis: Nicht instanzspezifische Betriebssystem- oder Oracle-Konfigurationsdateien (wie **kernel parameters, tnsnames.ora, sqlnet.ora** und **listener.ora**) werden vom Plug-in nicht gesichert. Sie können diese Dateien mit einem gewöhnlichen dateibasierten Agenten sichern.

7.2.3 Tabelle mit Sicherungsinformationen

Bevor Sie die Sicherungs- oder Wiederherstellungsvorgänge für Oracle-Datenbanken auf einem Linux-Server durchführen, stellen Sie sicher, dass Sie über alle Informationen wie Namen, Speicherorte, Kennwörter usw. verfügen, die Sie im Assistenten angeben müssen. Sie können die folgende Tabelle zu Rate ziehen.

Systemanforderung	Vom Kunden/Benutzer angegebener Wert	Kommentare
Neuer Jobname	Jobname =	Name des Jobs zur Kommunikation mit einem Agenten, der über das Oracle Plug-in verfügt
Typ der Sicherungsquelle	Oracle	Wählen Sie **Oracle** aus dem Dropdown-Menü.
Oracle-Optionen (zu sichernde Datenbank und Kontoinformationen für die Datenbank)	Name des Datenbankdienstes * = Benutzername = Kennwort =	Überprüft die Felder und ermöglicht eine Verbindung zu der Datenbank. Legen Sie im Portal unter „Name des Datenbankdienstes“ (Database Service Name) die Datenbankinstanz aus Oracle fest (nicht den Instanznamen aus Oracle). Legen Sie in Windows CentralControl für den Oracle-Dienstnamen die Datenbankinstanz aus Oracle fest (und nicht den Instanznamen aus Oracle).
Verschlüsselungstyp	Verschlüsselungstyp = Kennwort = Kennworthinweis =	Wenn Sie einen Typ auswählen, müssen Sie ein Kennwort angeben.
Protokollierungsoptionen	Protokolldatei erstellen = J/N Detailebene des Protokolls = Protokolldateien beibehalten oder entfernen = Anzahl der zu speichernden Protokolle =	
Zeitplan		Sie können Sicherungsjobs sofort oder nach einem Zeitplan ausführen. Optional können Sie den Assistenten für die Zeitplanung verwenden.
Ziel-Vault	Vault-Name = Netzwerkadresse =	Verwenden Sie die Dropdownliste der Vaults für die Auswahl.

* Wenn Sie eine Verbindung mit einer Datenbank herstellen, die einen anderen Port als den Standardport überwacht, lautet das Format für den Namen des Datenbankdiensts **Dienstname:Portnummer** (Beispiel: **orcl:1523**).

8.3 Wiederherstellen von Oracle-Datenbanken

Sie müssen möglicherweise eine vollständige Datenbank oder ein System von Grund auf ohne Systemsicherung wiederherstellen („Bare Metal“) – Installation des Betriebssystems, der Anwendungen und anschließend der vollständigen Datenbank sowie sämtlicher Transaktionsprotokolle auf einem neuen System.

Stellen Sie das System bei einer Oracle-Sicherung und einer vollständigen Systemsicherung wieder her (stellen Sie die Inhalte von ORACLE_HOME, insbesondere die Datenbankinstallation, wieder her). Dabei können Sie die vom Plug-in gesicherten Datendateien und Archivprotokolle sicher ausschließen.

Stellen Sie schließlich die Oracle-Datenbank wieder her und kopieren Sie die erforderlichen Komponenten in die jeweiligen Verzeichnisse. Halten Sie sich dabei an das benutzerverwaltete Standardverfahren für Oracle-Wiederherstellungen, das in dem für das entsprechende Betriebssystem geltenden Sicherungs- und Wiederherstellungshandbuch von Oracle beschrieben ist (verfügbar auf der Oracle-Website).

Ein Oracle-Wiederherstellungsvorgang wird von einem Datenbankadministrator durchgeführt. Im Wesentlichen sind folgende Schritte durchzuführen:

1. Fahren Sie die Datenbank herunter.
2. Stellen Sie die Dateien mit der Option **An alternativem Speicherort wiederherstellen** (Restore to an Alternate Location) wieder her.
3. Wenn die Dateien umbenannt wurden, müssen Sie ihnen wieder die ursprünglichen Dateinamen geben (d. h. den Steuerungsdateien).
4. Setzen Sie bei Bedarf die Steuerungsinformationen für die Datenbank zurück.
5. Starten Sie die Datenbank und stellen Sie sie wieder her.
6. Öffnen Sie die Datenbank erneut, um sie zu verwenden.

Das Plug-in führt keine Wiederherstellungen auf Tabellenebene aus.

7.3.1 Leitlinien für die Wiederherstellung

Hinweis: Bei einer vollständigen Desaster-Wiederherstellung (bei der die gesamte Datenbankinstanz wiederhergestellt wird) müssen Sie bei der Wiederherstellung der Datenbank vorsichtig sein, da das Oracle Plug-in für Linux keine TEMPORÄREN Tablespaces sichert.

Starten Sie die Datenbankwiederherstellung mit einem expliziten PFILE- oder SPFILE-Verweis:

SQL> STARTUP PFILE='Pfad-zu-pfile\initSIDNAME.ora'

Möglicherweise müssen die temporären Tablespace-Dateien offline gestellt werden:

SQL> ALTER DATABASE DATAFILE 'Pfad-zu-Datendatei' OFFLINE

Stellen Sie die Datenbank wie gewöhnlich wieder her. Verwenden Sie jedoch folgenden Befehl, wenn Sie die Datenbank nach der Wiederherstellung öffnen:

SQL> ALTER DATABASE OPEN NORESETLOGS

TEMPORÄRE Tablespaces sollten gelöscht, die Datendateien für die temporären Tablespaces sollten entfernt und die TEMPORÄREN Tablespaces sollten neu erstellt werden (möglicherweise auch der TEMP-Standard-Tablespace).

An diesem Punkt kann die Datenbank normal geschlossen und neu gestartet werden (beispielsweise mit RESETLOGS).

Hinweis: Oracle-Parameterdateien werden standardmäßig in einem anderen Verzeichnis gesichert.

8.4 Deinstallieren des Oracle Plug-ins für Linux

Deinstallieren Sie das Oracle Plug-in als **root**-Benutzer.

Führen Sie zum Deinstallieren des Oracle Plug-ins das Deinstallationsskript aus:

```
# ./uninstall-oracle.sh
```

Dieses Skript befindet sich in dem Verzeichnis, in dem das Installationskit abgelegt ist (im Allgemeinen „/tmp/Oracle-Plugin-Linux<**Version>**“).

Verwenden Sie nach der Ausführung des Deinstallationsskripts das VVAgent-Skript, um den Agenten zu stoppen und zu starten.

9 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 68. Administratoren können Computer 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 72.

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 69.

  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 71.

- 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 73.

  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 75.

- Spezifische Sicherungen aus Vaults löschen. Diese Option ist ab Portal 8.90 verfügbar. Siehe *Löschen von spezifischen Sicherungen aus Vaults* auf Seite 76.

  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.

9.1 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 69.

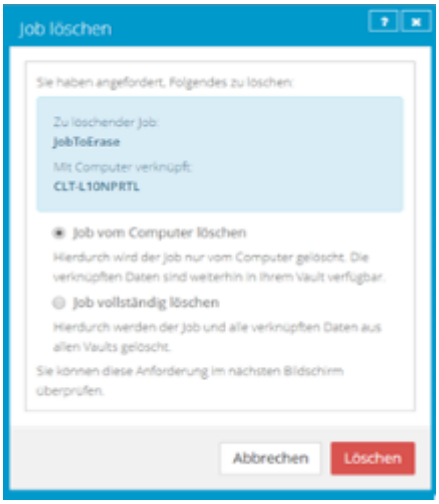
So löschen Sie einen Sicherungsjob, ohne die zugehörigen Daten aus den Vaults zu löschen.

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**.

9.2 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 71.

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:

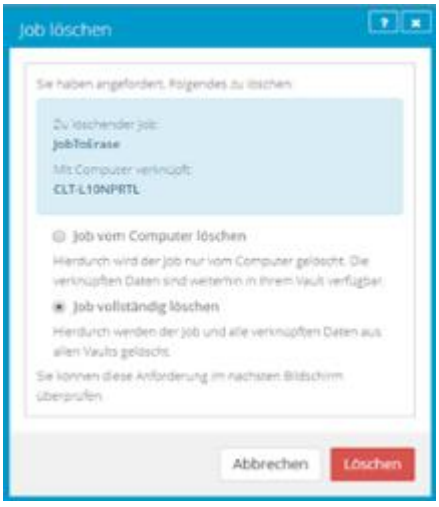
1. Melden Sie sich als Administrator an und klicken Sie in der Navigationsleiste auf **Computer**.

   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 68.

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.

9.3 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.

9.4 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**.

9.5 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 75.

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 72.

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.

9.6 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 73.

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.

9.7 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 69.

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**.

10 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 78.
- 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 79. Zudem können Sie auf dieser Seite auf Protokolle für nicht konfigurierte Computer zugreifen. Siehe *Anzeigen von Protokollen zu nicht konfigurierten Computern* auf Seite 84.
- 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 84.
- 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 86.
- 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 .

10.1 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 Lizenzeinschränkung 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 vorhandenen 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.
- Tresor**Computer mit Zertifikatfehlern** – Anzahl der Computer, die einen melden. Siehe *Beheben von Zertifikatfehlern* auf Seite 21.
- **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.

10.2 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.

Wenn Sie auf das Symbol „Prozessdetails“ klicken, wird das Dialogfeld „Prozessdetails“ mit Informationen über die Prozesse für den Job geöffnet. Siehe *Anzeigen von aktuellen Prozessinformationen eines Jobs* auf Seite 84.

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.
- 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. Siehe *Übersprungene Sicherungen* auf Seite 39.
- 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.
- 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 69.

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.

10.3 Anzeige der Übersprungen-Rate und der Sicherungsstatus-Historie

Ab Version 9.00, wenn ein AIX-Agent Daten in einem Vault ab Version 8.60 sichert, werden in einigen Fällen Sicherungen übersprungen, die mehrmals täglich ausgeführt werden sollen. Um festzustellen, ob Sicherungen übersprungen wurden, können Benutzer E-Mail-Benachrichtigungen, die Seiten „Computer“ und „Überwachung“ sowie den täglichen Statusbericht anzeigen. Siehe *Übersprungene Sicherungen* auf Seite 39. In einigen Portal-Instanzen können Benutzer auch die Übersprungen-Rate und die Historie des Sicherungsstatus anzeigen.

- Übersprungen-Rate für einen Job Wenn für einen Job in den 48 Stunden vor dem letzten Sicherungsversuch eine Sicherung übersprungen wurde, wird für den Job auf der Seite „Computer“ und auf der Seite „Überwachung“ eine Übersprungen-Rate angezeigt. Die Übersprungen-Rate ist der Prozentsatz der Sicherungen, die in den 48 Stunden vor dem letzten Sicherungsversuch übersprungen wurden, und wird anhand der folgenden Formel berechnet:

  JobÜbersprungenRate = AnzahlÜbersprungeneSicherungen / AnzahlSicherungsversuche

  Dabei gilt Folgendes:

  - Die *AnzahlÜbersprungeneSicherungen* ist die Anzahl der Sicherungen, die für den Job in den 48 Stunden vor dem letzten Sicherungsversuch übersprungen wurden.
  - Die *AnzahlSicherungsversuche* ist die Gesamtzahl der Sicherungsversuche für den Job während des 48-Stunden-Zeitraums, einschließlich übersprungener, laufender, verschobener, abgebrochener, fehlgeschlagener und abgeschlossener Sicherungen.

  Wenn für einen Job in den 48 Stunden vor dem letzten Sicherungsversuch keine Sicherungen übersprungen wurden oder wenn der letzte Sicherungsversuch mehr als sieben Tage zurückliegt, wird für den Job keine Übersprungen-Rate angezeigt.
- Übersprungen-Rate für einen Computer. Wenn für einen oder mehrere Jobs auf einem Computer eine Übersprungen-Rate gemeldet wird, wird die höchste Übersprungen-Rate auf dem Computer auf der Seite „Computer“ angezeigt.
- Historie des 48-Stunden-Sicherungsstatus für einen Job. Wenn für einen Job auf der Seite „Computer“ oder „Überwachung“ eine Übersprungen-Rate angezeigt wird, können Sie die Historie der Jobsicherung für die 48 Stunden vor dem letzten Sicherungsversuch anzeigen. Die Statushistorie zeigt die Daten und Uhrzeiten der Sicherungsversuche an und gibt den Status der einzelnen Sicherungsversuche an (z. B. übersprungen, in Arbeit, abgeschlossen oder fehlgeschlagen). Sie können die Statushistorie in kommagetrennten Werten (.csv), im Microsoft Excel-Format (.xls) oder Adobe Acrobat-Format (.pdf) exportieren.

Zur Anzeige der Übersprungen-Rate und der Sicherungsstatus-Historie finden Sie weitere Informationen unter *Anzeige der Übersprungen-Rate und der Sicherungsstatus-Historie auf der Seite „Computer“* auf Seite

82 und *Anzeige der Übersprungen-Rate und der Sicherungsstatus-Historie auf der Seite „Überwachung“* auf Seite 83.

9.3.1 Anzeige der Übersprungen-Rate und der Sicherungsstatus-Historie auf der Seite „Computer“

Um eine Zeitplanüberlastung zu vermeiden, werden Sicherungen, die mehrmals am Tag ausgeführt werden sollen, in einigen Fällen übersprungen. Benutzer können Informationen über übersprungene Sicherungen durch E-Mail-Benachrichtigungen, auf der Seite „Computer“ und im täglichen Statusbericht erhalten. Siehe *Übersprungene Sicherungen* auf Seite 39.

In einigen Portal-Instanzen können Benutzer auf der Seite „Computer“ die Anzahl der übersprungenen Sicherungen für Jobs und Computer anzeigen und die Historie des Sicherungsstatus eines Jobs für die 48 Stunden vor dem letzten Sicherungsversuch anzeigen und exportieren. Weitere Informationen finden Sie unter *Anzeige der Übersprungen-Rate und der Sicherungsstatus-Historie* auf Seite 81.

So zeigen Sie die Übersprungen-Rate und die Sicherungsstatus-Historie auf der Seite „Computer“ an:

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

   In der Spalte „Übersprungen“ wird ein Wert für jeden Computer angezeigt, auf dem mindestens ein Job eine Übersprungen-Rate aufweist. Wenn mehr als ein Job auf einem Computer eine Übersprungen-Rate aufweist, wird die höchste Übersprungen-Rate in der Spalte „Übersprungen“ angezeigt.

   Hinweis: Wenn die Spalte „Übersprungen“ nicht angezeigt wird, sind die Übersprungen-Raten und die 48-Stunden-Historie des Sicherungsstatus in Ihrer Portal-Instanz nicht verfügbar.

2. Suchen Sie einen Computer mit einem Wert in der Spalte „Übersprungen“ und klicken Sie auf die Computerzeile, um die Ansicht zu erweitern.

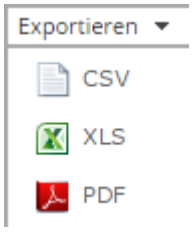
   In der Registerkarte „Jobs“ wird in der Spalte „Übersprungen-Rate“ ein Wert für jeden Job angezeigt, bei dem in den 48 Stunden vor dem letzten Sicherungsversuch eine Sicherung übersprungen wurde und der letzte Sicherungsversuch in den letzten sieben Tagen stattfand.

3. Um zu sehen, welche Sicherungen in den 48 Stunden vor dem letzten Sicherungsversuch für einen Job übersprungen wurden, klicken Sie auf den Wert für die Übersprungen-Rate des Jobs.

   Die 48-Stunden-Statushistorie für den Job zeigt das Datum, die Uhrzeit und den Status (z. B. übersprungen, in Bearbeitung, abgeschlossen oder fehlgeschlagen) jedes Sicherungsversuchs an.

   Wenn Sie die Statushistorie exportieren möchten, klicken Sie auf das Feld **Exportieren**. Klicken Sie in der angezeigten Liste auf eines der folgenden Formate für die exportierte Daten:

   - CSV (kommagetrennte Werte)
   - XLS (Microsoft Excel)
   - PDF (Adobe Acrobat)

Die Datei mit den Statushistoriendaten wird im angegebenen Format auf Ihren Computer heruntergeladen.

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

9.3.2 Anzeige der Übersprungen-Rate und der Sicherungsstatus-Historie auf der Seite „Überwachung“

Um eine Zeitplanüberlastung zu vermeiden, werden Sicherungen, die mehrmals am Tag ausgeführt werden sollen, in einigen Fällen übersprungen. Benutzer können Informationen über übersprungene Sicherungen durch E-Mail-Benachrichtigungen, auf der Seite „Computer“ und im täglichen Statusbericht erhalten. Siehe *Übersprungene Sicherungen* auf Seite 39.

In einigen Portal-Instanzen können Benutzer auf der Seite „Überwachung“ die Anzahl der übersprungenen Sicherungen für Jobs anzeigen und die Historie des Sicherungsstatus eines Jobs für die 48 Stunden vor dem letzten Sicherungsversuch anzeigen und exportieren. Weitere Informationen finden Sie unter *Anzeige der Übersprungen-Rate und der Sicherungsstatus-Historie* auf Seite 81.

So zeigen Sie die Übersprungen-Rate und die Sicherungsstatus-Historie auf der Seite „Überwachung“ an:

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

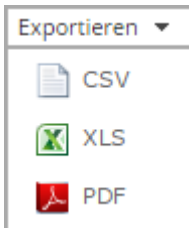
   In der Spalte „Übersprungen“ wird ein Wert für jeden Job angezeigt, bei dem in den 48 Stunden vor dem letzten Sicherungsversuch eine Sicherung übersprungen wurde und der letzte Sicherungsversuch in den letzten sieben Tagen stattfand.

2. Um zu sehen, welche Sicherungen in den 48 Stunden vor dem letzten Sicherungsversuch für einen Job übersprungen wurden, klicken Sie auf den Übersprungen-Wert des Jobs.

   Die 48-Stunden-Statushistorie für den Job zeigt das Datum, die Uhrzeit und den Status (z. B. übersprungen, in Bearbeitung, abgeschlossen oder fehlgeschlagen) jedes Sicherungsversuchs an.

   Wenn Sie die Statushistorie exportieren möchten, klicken Sie auf das Feld **Exportieren**. Klicken Sie in der angezeigten Liste auf eines der folgenden Formate für die exportierte Daten:

   - CSV (kommagetrennte Werte)
   - XLS (Microsoft Excel)
   - PDF (Adobe Acrobat)

   Die Datei mit den Statushistoriendaten wird im angegebenen Format auf Ihren Computer heruntergeladen.

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

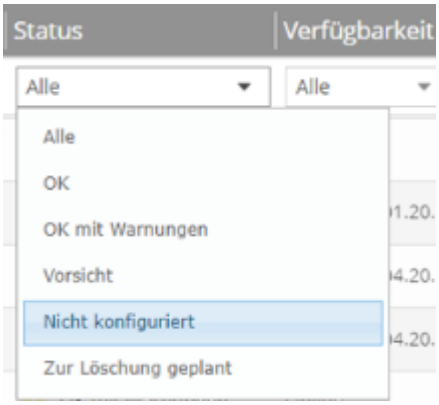
10.4 Anzeigen von Protokollen zu nicht konfigurierten Computern

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.

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.

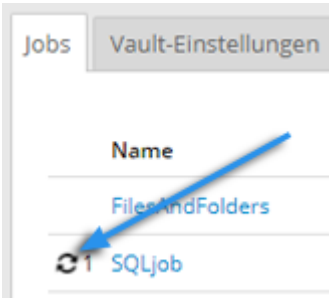
10.5 Anzeigen von aktuellen Prozessinformationen eines Jobs

In Dialogfeld „Prozessdetails“ können Sie Informationen über ausgeführte, in der Warteschlange befindliche und kürzlich abgeschlossene Prozesse eines Jobs anzeigen. Prozesse umfassen Sicherungen,

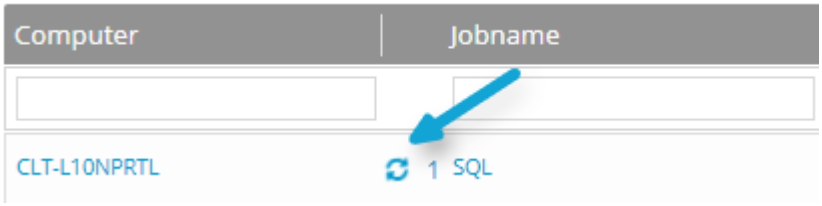
Wiederherstellungen und Synchronisierungen, und werden normalerweise innerhalb von einer Stunde nach Prozessende gelöscht.

So zeigen Sie aktuelle Prozessinformationen eines Jobs an:

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



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



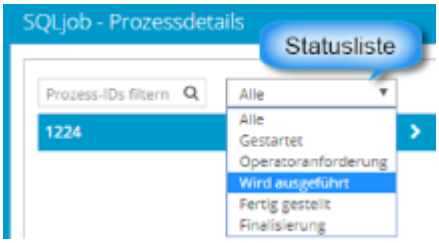
   Falls Sie auf eines der „Prozessdetails“-Symbole geklickt haben, wird das Dialogfeld „Prozessdetails“ mit einer Liste der Sicherungs-, Wiederherstellungs- und Synchronisierungsprozesse geöffnet, die für den Job ausgeführt werden, sich in der Warteschlange befinden oder kürzlich abgeschlossen wurden.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

2. Um Informationen zu einem anderen Prozess 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**.



10.6 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 86.

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 89.

9.6.1 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**.

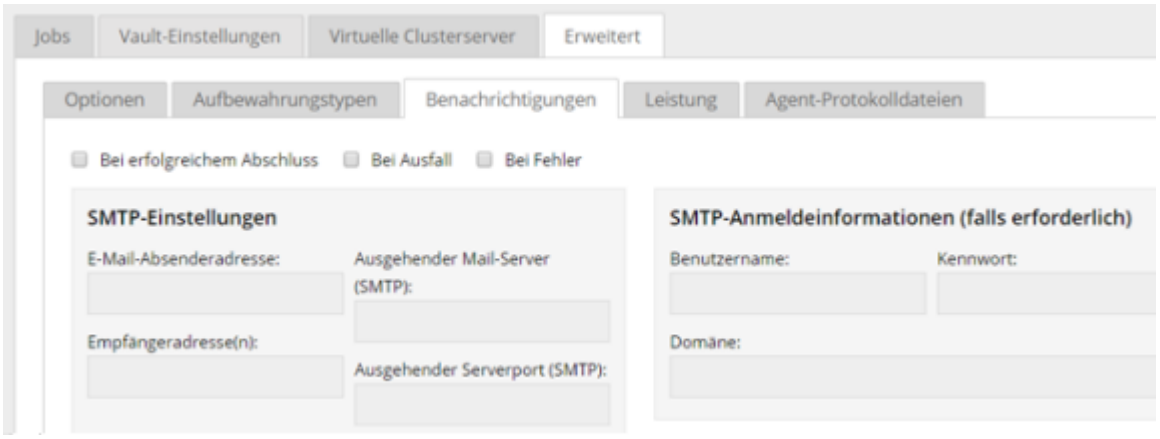
   Die Seite „Computer“ zeigt registrierte Computer an.

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 88.

   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**.

9.6.2 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.

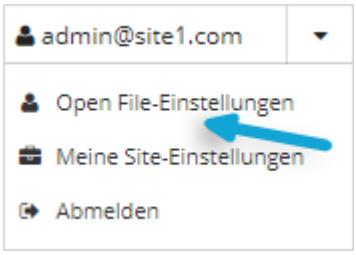
Hinweis: E-Mail-Benachrichtigungen, die in den Profileinstellungen des Administratorbenutzers ausgewählt werden, werden nur auf Englisch gesendet. E-Mail-Benachrichtigungen für E-Mail-Adressen auf untergeordneten Sites werden in mehreren Sprachen unterstützt.

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 86.

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 86.

   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.Siehe *Übersprungene Sicherungen* auf Seite 39.

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

9.6.3 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.

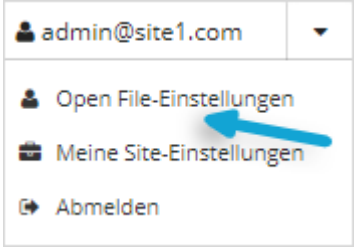
Wenn E-Mail-Benachrichtigungen zentral in einer Portal-Instanz konfiguriert werden, können zusätzliche E-Mail-Adressen für Benachrichtigungen für jede untergeordnete Site angegeben werden.

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**.

10.7 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:

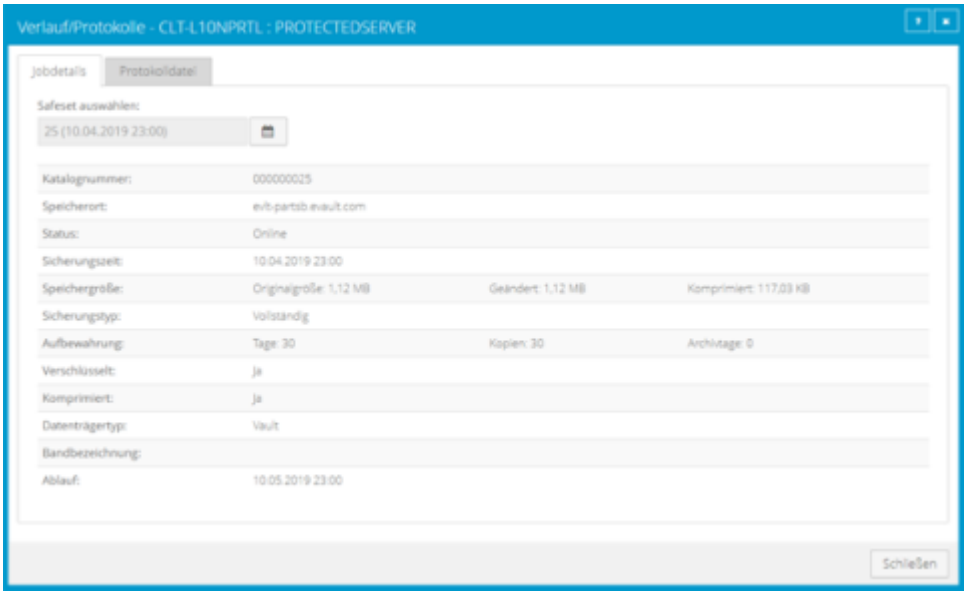
1. Klicken Sie in der Navigationsleiste auf **Computer**.

   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.



10.8 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.

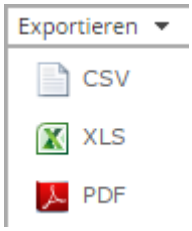
Sie können über die Seite „Überwachung“ zu verwandten Informationen auf der Seite „Computer“ oder im Fenster „Protokolle“ navigieren.

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.