Dell EMC Avamar

Version 7.5.1

Administrationshandbuch

302-004-297

REV 02

DELL EMC

Stand Februar 2018

EMC Deutschland GmbH
Am Kronberger Hang 2a 65824 Schwalbach/Taunus
Tel.: +49 6196 4728-0
www.DellEMC.com/de-de/index.htm

INHALT

ABBILDUNGEN

TABELLEN

VORWORT

Zur fortlaufenden Verbesserung der Produktlinien werden regelmäßig neue Software- und Hardwareversionen veröffentlicht. Aus diesem Grund werden einige in diesem Dokument beschriebene Funktionen eventuell nicht von allen Versionen der von Ihnen derzeit verwendeten Software oder Hardware unterstützt. In den Versionshinweisen zum Produkt finden Sie aktuelle Informationen zu Produktfunktionen.

Wenden Sie sich an den Experten für technischen Support, wenn ein Produkt nicht ordnungsgemäß oder nicht wie in diesem Dokument beschrieben funktioniert.

Hinweis

Dieses Dokument war zum Veröffentlichungszeitpunkt korrekt. Die neueste Version dieses Dokuments finden Sie auf der Online Support-Website (https://support.emc.com/).

Zweck

In diesem Handbuch werden die Konfiguration, Administration, Überwachung und Wartung des Avamar-Systems beschrieben.

Zielgruppe

Die Informationen in diesem Handbuch sind in erster Linie für Systemadministratoren bestimmt, die für die Wartung von Servern und Clients in einem Netzwerk verantwortlich sind, sowie für Bediener, die tägliche Backups und Speichergeräte überwachen.

Revisionsverlauf

In der nachstehenden Tabelle wird der Revisionsverlauf für dieses Dokument dargestellt.

Tabelle 1 Revisionsverlauf

Version	Datum	Beschreibung
01	01. Februar 2018	GA-Version von Avamar 7.5.1
02	23. Februar 2018	Zusätzliche Aktualisierungen für Avamar 7.5.1.

Zugehörige Dokumentation

In den folgenden Publikationen finden Sie zusätzliche Informationen:

- *Avamar Kompatibilitäts- und Interoperabilitätsmatrix*
- *Avamar – Versionshinweise*
- *Betriebliche Best Practices für Avamar – Handbuch*
- *Avamar und Data Domain-System – Integrationshandbuch*
- *Avamar-Berichte – Handbuch*
- Alle Avamar-Client- und -Plug-in-Benutzerhandbücher

In diesem Dokument verwendete Konventionen für spezielle Hinweise
Für spezielle Hinweise werden die folgenden Konventionen verwendet:

GEFAHR

Weist auf gefährliche Situationen hin, die zum Tod oder zu schweren Verletzungen führen.

WARNUNG

Weist auf gefährliche Situationen hin, die zum Tod oder zu schweren Verletzungen führen können.

ACHTUNG

Weist auf gefährliche Situationen hin, die zu leichten oder mittelschweren Verletzungen führen können.

HINWEIS

Bezieht sich auf Praktiken, die nicht zu Verletzungen führen.

Hinweis

Enthält Informationen, die wichtig, aber nicht sicherheitsrelevant sind.

Typografische Konventionen
In diesem Dokument werden die folgenden typografischen Konventionen verwendet:

Tabelle 2 Typografische Konventionen

Fett	Für Bezeichnungen von Benutzeroberflächenelementen wie Namen von Fenstern, Dialogfeldern, Schaltflächen, Feldern, Registerkarten, Schlüsselnamen und Menüpfaden (die vom Benutzer ausgewählt oder angeklickt werden)
Kursiv	Für vollständige Publikationstitel, auf die im Text Bezug genommen wird
`Monospace`	Verwendet für: • Systemcode • Systemausgaben (z. B. Fehlermeldungen oder Skripte) • Pfad- und Dateinamen, Aufforderungen und Syntax • Befehle und Optionen
Kursive Monospace-Schrift	Verwendet für Variablen
`Fette Monospace-Schrift`	Verwendet für Benutzereingaben
[ ]	Eckige Klammern schließen optionale Werte ein
|	Vertikale Balken kennzeichnen alternative Möglichkeiten (der Strich bedeutet „oder“)

Tabelle 2 Typografische Konventionen (Fortsetzung)

{ }	Geschweifte Klammern umgeben Inhalte, die der Benutzer angeben muss (x oder y oder z)
...	Auslassungspunkte verweisen auf unwichtige Informationen, die im Beispiel ausgelassen wurden

Hier erhalten Sie Hilfe

Auf der Supportseite von Avamar haben Sie Zugriff auf Lizenzierungsinformationen, Produktdokumentationen, Ratgeber und Downloads sowie Anleitungen und Troubleshooting-Informationen. Diese Informationen können Ihnen bei der Lösung eines Produktproblems helfen, bevor Sie den Kundensupport kontaktieren.

So greifen Sie auf die Supportseite von Avamar zu:

1. Gehen Sie zu https://support.EMC.com/products.
2. Geben Sie im Feld **Find a Product by Name** einen Produktnamen ein.
3. Wählen Sie das Produkt aus der angezeigten Liste aus.
4. Klicken Sie auf den Pfeil neben dem Feld **Find a Product by Name**.
5. (Optional) Fügen Sie das Produkt zu der Liste **My Products** hinzu, indem Sie in der oberen rechten Ecke der Seite **Support by Product** auf **Add to My Saved Products** klicken.

Dokumentation

Die Produktdokumentation von Avamar liefert eine umfassende Übersicht über Funktionen, Betriebsaufgaben und technische Referenzen. Lesen Sie zusätzlich zu den Handbüchern zur Produktadministration und den Benutzerhandbüchern auch folgende Dokumente:

- Versionshinweise bieten eine Übersicht über neue Funktionen und bekannte Einschränkungen einer Version.
- Technische Hinweise stellen technische Details zu bestimmten Produktfunktionen bereit, falls erforderlich auch in schrittweisen Anleitungen.
- White Papers bieten ausführliche technische Informationen zu einem Produkt oder mehreren Produkten, die für kritische Geschäftsprobleme oder -anforderungen erforderlich sind.

Wissensdatenbank

Die Wissensdatenbank enthält passende Lösungen, nach denen Sie anhand der Lösungsnummer (z. B. esgxxxxxx) oder anhand eines Schlüsselworts suchen können.

So durchsuchen Sie die Wissensdatenbank:

1. Klicken Sie oben auf der Seite auf den Link **Search**.
2. Geben Sie entweder die Lösungsnummer oder die Schlüsselwörter in das Suchfeld ein.
3. (Optional) Begrenzen Sie die Suche auf spezifische Produkte oder geben Sie einen Produktnamen im Feld **Scope by product** ein und wählen Sie dann das Produkt aus der angezeigten Liste aus.
4. Wählen Sie **Knowledgebase** aus der Liste **Scope by resource** aus.
5. (Optional) Legen Sie erweiterte Optionen fest, indem Sie auf **Advanced options** klicken und Werte in die verfügbaren Felder eingeben.
6. Klicken Sie auf **Search**.

Onlinecommunity
Besuchen Sie das Community Network unter http://community.EMC.com, um Kontakt zu anderen Benutzern zu knüpfen, Gespräche zu führen und Inhalte für Produktsupport und Lösungen zu finden. Hier können Sie sich interaktiv und online mit Kunden, Partnern und zertifizierten Mitarbeitern über alle Produkte austauschen.

Livechat
Klicken Sie auf der Supportseite von Avamar im Bereich **Service Center** auf **Join Live Chat**, um sich mithilfe des interaktiven Livechats an den Kundensupport zu wenden.

Service-Requests
Ausführliche Hilfe vom Kundensupport erhalten Sie, wenn Sie einen Service-Request senden, indem Sie auf der Supportseite von Avamar im Bereich **Service Center** auf **Create Service Request** klicken.

Hinweis

Um einen Service-Request stellen zu können, müssen Sie über einen gültigen Supportvertrag verfügen. Wenden Sie sich an einen Vertriebsmitarbeiter, wenn Sie eine gültige Supportvereinbarung benötigen oder Fragen zu einem Konto haben.

Klicken Sie im Bereich **Service Center** auf den Link **Service Center** und dann auf **View and Manage Service Requests**.

Enhanced Support
Es wird empfohlen, ConnectEMC und Email Home auf allen Systemen von Avamar zu aktivieren:

- ConnectEMC generiert automatisch Service-Requests für Ereignisse mit hoher Priorität.
- Über „Email Home“ werden die Konfiguration, die Kapazität und allgemeine Systeminformationen an den Kundensupport gesendet.

Kommentare und Anregungen
Ihre Anregungen helfen, die Genauigkeit, Gestaltung und Gesamtqualität der Benutzerdokumentation immer weiter zu verbessern. Senden Sie Ihre Kommentare und Anregungen zu diesem Dokument an DPAD.Doc.Feedback@emc.com.

Geben Sie dabei folgende Informationen an:

- Produktname und Version
- Name des Dokuments, Art.-Nr. und Version (z. B. A01)
- Seitenzahlen
- Sonstige Einzelheiten, die uns bei der Behebung des Problems in der Dokumentation helfen

KAPITEL 1

Einführung

In diesem Kapitel werden folgende Themen behandelt:

Avamar-Systemübersicht

Ein Avamar-System ist eine Client-/Servernetzwerk-Backup- und Wiederherstellungslösung.

Ein Avamar-System besteht aus einem oder mehreren Avamar-Servern sowie aus den Netzwerkservern oder Desktopclients, die Daten auf diesen Servern sichern. Das Avamar-System ermöglicht über die grafische Managementkonsolen-Softwareanwendung von Avamar Administrator ein zentrales Management.

Avamar-Server

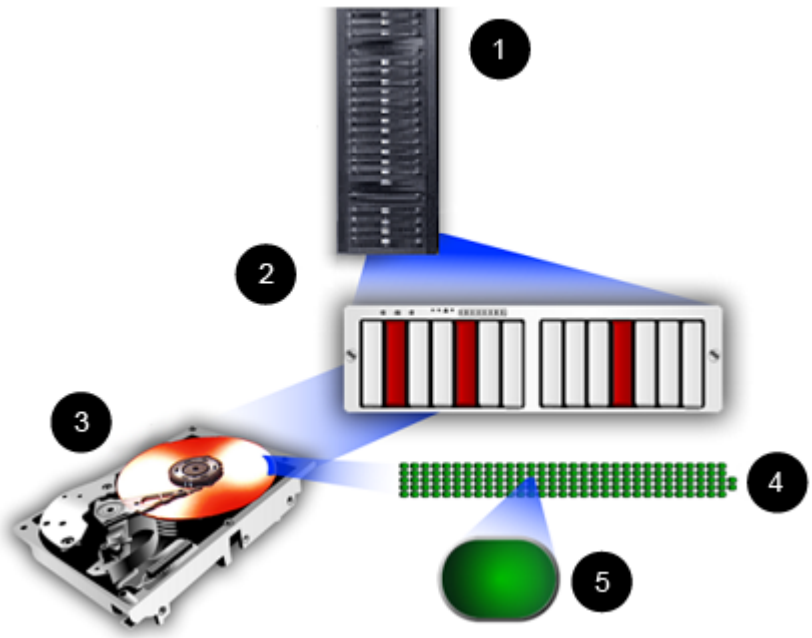
Avamar ist eine festplattenbasierte IP-Netzwerk-Backup- und Wiederherstellungslösung. Avamar-Server nutzen internen Festplattenspeicher. Ein Avamar-Server ist eine logische Gruppierung eines oder mehrerer Nodes für die Speicherung und das Management von Clientbackups.

Hardwarehersteller bezeichnen ihre Geräte in der Regel als Server (z. B. Dell PowerEdge 2950-Server). Im Kontext eines Avamar-Systems werden diese Geräte als *Nodes* bezeichnet. Ein Avamar-Node ist ein eigenständiger, rackmontierbarer, netzwerkadressierbarer Computer, der unter dem Linux-Betriebssystem Avamar-Serversoftware ausführt.

Avamar sorgt für Fehlertoleranz durch das Management von Festplattenspeicher in Speichereinheiten, die als *Stripes* bezeichnet werden.

Im Avamar-System ist ein *Objekt* eine einzelne Instanz deduplizierter Daten. Jedes Avamar-Objekt verfügt über eine eindeutige ID. Objekte werden auf dem Avamar-Server innerhalb von Stripes gespeichert und gemanagt.

Abbildung 1 Avamar-Server-Nodes, -Stripes und -Objekte



1. Avamar-Server
2. Avamar-Node
3. Festplattenspeicher auf dem Node

4. Stripe auf dem Festplattenlaufwerk
5. Objekt auf dem Stripe

Alle Avamar-Server speichern Clientbackups und stellen außerdem die für Clientzugriff und Remotesystemadministration erforderlichen Prozesse und Services zur Verfügung.

Avamar-Server sind entweder in Single-Node- oder skalierbaren Multi-Node-Konfigurationen verfügbar. Größtenteils verhalten sich alle Avamar-Server bei Verwendung der Avamar Administrator-Managementkonsolensoftware gleich und sehen gleich aus. Der Hauptunterschied zwischen den Avamar-Serverkonfigurationen liegt in der Anzahl der Nodes und Festplattenlaufwerke, die bei der Serverüberwachung gemeldet werden.

Die Dokumentierung spezifischer Unterschiede zwischen Avamar-Serverhardwarekonfigurationen ist im Rahmen dieses Handbuchs nicht möglich. Immer, wenn es spezifische Einschränkungen oder Best Practices zu bestimmten Konfigurationen gibt, wird darauf hingewiesen. Diese gelegentlichen Hinweise sollten allerdings nicht als endgültig oder vollständig betrachtet werden. Wenden Sie sich an einen Avamar-Vertriebsmitarbeiter oder einen Avamar-Reseller, um weitere Informationen zu bestimmter Hardware zu erhalten.

Nodes

Nodes stellen den wichtigsten Baustein eines jeden Avamar-Servers dar. Jeder Node ist ein eigenständiger, rackmontierbarer, netzwerkadressierbarer Computer, der unter einem Linux-Betriebssystem Avamar-Serversoftware ausführt.

Nodes können auch internen Speicher in Form von Festplattenlaufwerken enthalten. Wird der Node mit internem Speicher konfiguriert (d. h. einem Single-Node-Server), wird dieser intern gespiegelt, um für eine solide Fehlertoleranz zu sorgen.

Es gibt drei Arten von Nodes.

Utility-Node
Ein Utility-Node ist eigens für die Planung und das Management von im Hintergrund ausgeführten Avamar-Serverjobs vorgesehen. Bei skalierbaren Avamar-Multi-Node-Servern führt ein einziger Utility-Node wichtige interne Dienste für den Server aus:

- Management Console Server (MCS)
- Cronjob
- Externe Authentifizierung
- Network Time Protocol (NTP)
- Webzugriff

Da Utility-Nodes eigens auf die Ausführung dieser wichtigen Dienste auf Avamar-Multi-Node-Servern ausgerichtet sind, können sie nicht zum Speichern von Backups verwendet werden. Avamar-Single-Node-Server führen alle Merkmale und Funktionen von Utility-Nodes und Speicher-Nodes auf einem einzigen Node zusammen.

Speicher-Nodes
Speicher-Nodes sind Nodes für die Speicherung von Backupdaten. Mehrere Speicher-Nodes werden mit Avamar-Multi-Node-Servern konfiguriert, die auf Leistungs- und Kapazitätsanforderungen basieren. Sie können einem Avamar-Server im Laufe der Zeit Speicher-Nodes hinzufügen, um die Performance ohne Ausfallzeit zu steigern.

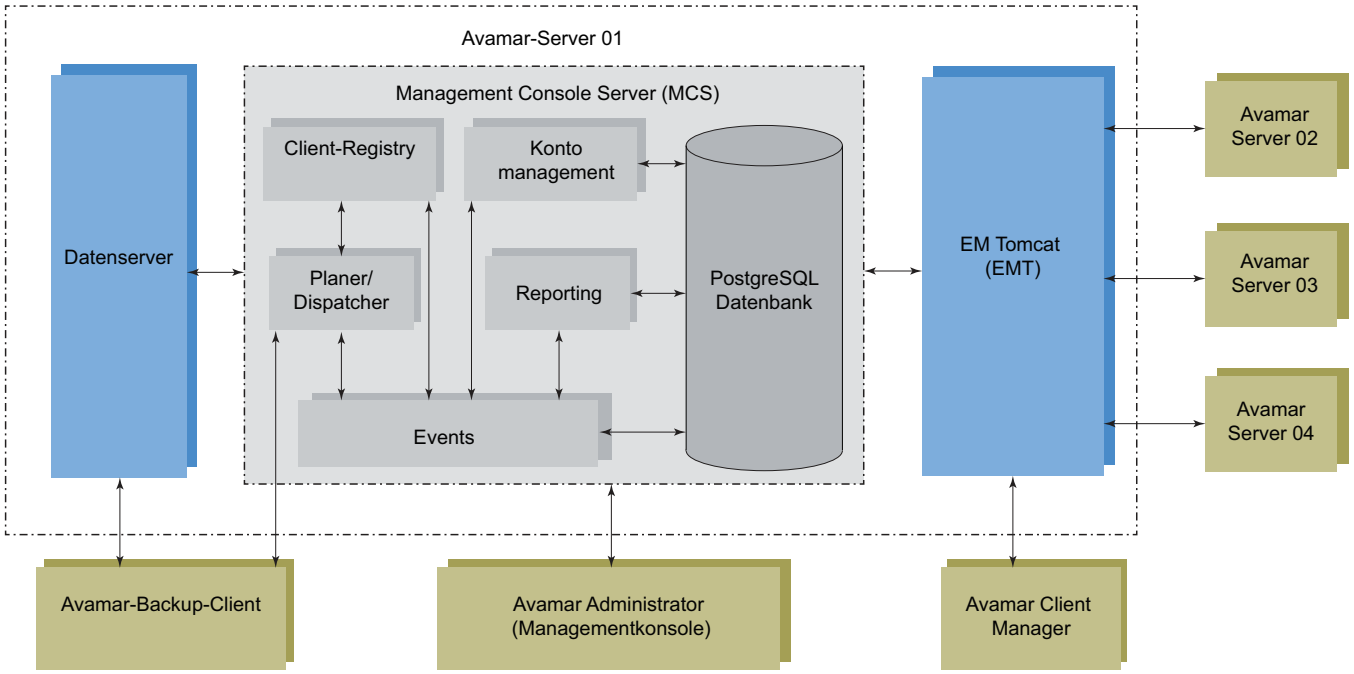
Avamar Clients stellen eine direkte Verbindung zu Avamar-Speicher-Nodes her. Clientverbindungen und -daten sind eine Last, die über Speicher-Nodes hinweg verteilt wird.

NDMP-Accelerator
Ein NDMP-Accelerator-Node ist ein spezieller Node, der über NDMP Datenschutz für bestimmte NAS-Geräte bereitstellt, u. a. für EMC Celerra®-IP-Speichersysteme und Network Appliance Filers.

Funktionelle Avamar-Serverblöcke

Die wichtigsten funktionellen Avamar-Serverblöcke umfassen den Datenserver, den Management Console Server (MCS) und den EM Tomcat-Server (EMT). In der folgenden Abbildung wird die Interaktion dieser Komponenten innerhalb des Servers und mit anderen Avamar-Komponenten veranschaulicht.

Abbildung 2 Diagramm zu den Funktionsblöcken von Avamar-Server



Datenserver

Bei der Durchführung eines Backups, einer Wiederherstellung oder einer Validierung kommunizieren Avamar-Backupclients direkt mit dem Datenserver. Alle geplanten Backups werden vom MCS-Planer initiiert.

Management Console Server (MCS)

Der MCS (Management Console Server) ermöglicht eine zentrale Administration (Planung, Überwachung und Management) des Avamar-Servers. Der MCS führt außerdem serverseitige Prozesse aus, die von der grafischen Avamar-Administrator-Managementkonsole verwendet werden.

In der folgenden Tabelle finden Sie Details zu den Funktionen des MCS.

Tabelle 3 MCS-Funktionen

Funktion	Beschreibung
Client registry	Steuert die Clientregistrierung und -aktivierung.

Tabelle 3 MCS-Funktionen (Fortsetzung)

Funktion	Beschreibung
Account management	Dient zur Erstellung und zum Management von Domains, Clients, Benutzern und Gruppen.
Reporting	Dient zur Erstellung und zum Export von Systemberichten. Im *Avamar-Berichte – Handbuch* finden Sie weitere Informationen.
Events	Zeigt Systemereignisse und Aktivitäten an.
Planer/Dispatcher	Steuert den Zeitpunkt der Backup- und Wiederherstellungsvorgänge oder ob Vorgänge zur Verarbeitung in die Warteschlange gestellt werden können.
PostgreSQL-Datenbank	Speichert Avamar-Serverdaten. PostgreSQL ist ein Datenbankmanagementsystem in einer offenen Architektur. Der Zugriff auf Informationen in der MCS-Datenbank ist über eine beliebige PostgreSQL-vorgabenkonforme ODBC-Schnittstelle möglich. Der Dateiname für die MCS-Datenbank lautet `mcdb`. Sie befindet sich auf dem Utility-Node im Verzeichnis `/usr/local/avamar/var/mc/server_data/postgres`. Die MCS-Datenbankinhalte werden auf dem Avamar-Server vollständig gesichert und können bei einem MCS-Ausfall wiederhergestellt werden. **HINWEIS** Die MCS-Datenbank ist für den schreibgeschützten Zugriff zwecks Reporting oder Abfrage vorgesehen. Ändern Sie Daten in `mcdb`-Tabellen nicht manuell, es sei denn, Sie werden vom Avamar-Support dazu aufgefordert. Das direkte Ändern von MCS-Betriebsdaten kann zum Verlust der referenziellen Integrität führen, was wiederum unwiederbringlichen Datenverlust zur Folge haben kann.

EM Tomcat-Server (EMT)

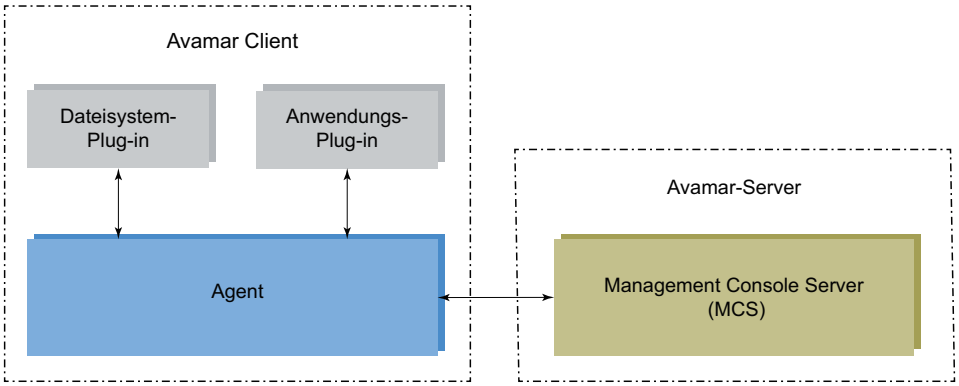
Der Avamar EM Tomcat-Server (EMT) stellt wichtige Services bereit, die zum Anzeigen von und Arbeiten mit Avamar-Serverinformationen erforderlich sind.

Der EMT kommuniziert außerdem direkt mit dem MCS. Diese Kommunikation ist ein erforderlicher Teil aller Avamar-Systeme.

Avamar-Clients

Avamar bietet Clientsoftware für verschiedene Computerplattformen. Jeder Client besteht aus einem Client-Agent und einem oder mehreren Plug-ins.

Abbildung 3 Avamar Client-Agent und Plug-ins



Agents

Avamar-Agents sind plattformspezifische Softwareprozesse, die auf dem Client ausgeführt werden und mit dem Management Console Server (MCS) sowie sämtlichen auf diesem Client installierten Plug-ins kommunizieren.

Plug-ins

Es gibt zwei Arten von Avamar-Plug-ins:

- Dateisystem-Plug-ins, die zum Durchsuchen, Sichern und Wiederherstellen von Dateien und Verzeichnissen auf einem bestimmten Clientdateisystem verwendet werden.
- Anwendungs-Plug-ins, die Backup und Wiederherstellung von Datenbanken oder anderen speziellen Anwendungen unterstützen.

In der folgenden Tabelle werden die von Avamar unterstützten Dateisystem- und Anwendungs-Plug-ins angegeben.

Tabelle 4 Unterstützte Plug-ins

Art des Plug-ins	Unterstützte Dateisysteme und Anwendungen
Dateisystem	• FreeBSD • HP-UX • IBM AIX • Linux • Mac OS X • Microsoft Windows • Microsoft Windows Volume Shadow Copy Service (VSS) • SCO Open Server • SCO UnixWare • Oracle Solaris • VMware
Anwendung	• IBM DB2

Tabelle 4 Unterstützte Plug-ins (Fortsetzung)

Art des Plug-ins	Unterstützte Dateisysteme und Anwendungen
	• Lotus Domino • Microsoft Exchange • Microsoft Hyper-V • Microsoft Office SharePoint Server (MOSS) • Microsoft SQL Server • NDMP für NAS-Geräte wie EMC Celerra-IP-Speichersysteme und Network Appliance Filers • Oracle • SAP mit Oracle • Sybase ASE

Im Kompatibilitätshandbuch im Onlinesupport (http://compatibilityguide.emc.com:8080/CompGuideApp) finden Sie die Anforderungen für die Clientkompatibilität und unterstützte Betriebssysteme und Anwendungsversionen.

Der Avamar-Dateisystemclient und das Plug-in, das Sie auf dem Host installieren, müssen dieselbe Versionsnummer aufweisen.

Benutzeroberflächen

Im Avamar-System stehen verschiedene Benutzeroberflächen zur Verfügung, um das Management und die Überwachung zu ermöglichen.

Avamar-Administrator
Avamar-Administrator ist eine grafische Managementkonsolen-Softwareanwendung, die die Administration eines Avamar-Systems über einen unterstützten Windows-Clientcomputer ermöglicht.

Avamar Backup and Recovery Manager
Backup and Recovery Manager managt alle Avamar-Systeme im Unternehmen. Backup and Recovery Manager verfügt außerdem über eine integrierte Benutzeroberfläche, um die NetWorker-Server und Data Domain-Backupziele des Unternehmens zu managen.

In der folgenden Tabelle sind einige der Managementfunktionen für Unternehmen von Backup and Recovery Manager aufgeführt. Die Tabelle enthält keine Zusatzfunktionen in Backup and Recovery Manager, die speziell für NetWorker-Server und Data Domain-Backupziele gelten.

Tabelle 5 Avamar-Systemmanagementfunktionen von Backup and Recovery Manager

Funktion	Backup and Recovery Manager
Softwarehost	VMware vSphere-Client
Dashboard auf einen Blick	Auswahl zwischen konsolidierten und individuellen Statusanzeigen der Avamar-

Tabelle 5 Avamar-Systemmanagementfunktionen von Backup and Recovery Manager (Fortsetzung)

Funktion	Backup and Recovery Manager
	Systeme, NetWorker-Server und Data Domain-Systeme
Detaillierte Backup- und Kapazitätsdaten für Avamar-Systeme	Ja
Überwachung von Backups	Ja, mithilfe des Bildschirms Activity Monitor. Mithilfe des Bildschirms Activity Monitor können Sie Details zu Backups und Replikationen anzeigen sowie Aufgaben starten, beenden und neu starten.
Replikationsmanagement	Ja
Starten sonstiger Managementanwendungen	• Avamar-Administrator • Avamar Client Manager • Avamar Installation Manager • AvInstaller-Dienst
Anzeige von Warnungen, Fehlern und Systemwarnmeldungen	Ja, über eine grafische Schnellanzeige mit detaillierten Informationen. Filterung der Anzeige nach Produkt, System und Kategorie.
Managementberichte: Auswählen, Anzeigen und Exportieren	• Backup • System • Konfiguration

Die Produktdokumentation zum Backup and Recovery Manager enthält alle Einzelheiten über die Benutzeroberfläche.

Avamar Client Manager

Avamar Client Manager ist eine webbasierte Managementanwendung, die zentrale Avamar-Clientadministrationsfunktionen für größere Unternehmen bereitstellt. Avamar Client Manager unterstützt das Management einer großen Anzahl von Avamar-Clients.

Avamar Client Manager funktioniert mit Avamar-Clients auf einem unterstützten nativen Betriebssystem und Avamar-Clients auf einem unterstützten Betriebssystem, das auf einer virtuellen VMware-Maschine ausgeführt wird. Avamar Client Manager funktioniert nicht mit Avamar-Clients über ein virtuelles Center, eine virtuelle Maschine oder virtuelle Proxykonfigurationen. Die Avamar Client Manager-Benutzeroberfläche zeigt unterstützte Avamar-Clients an und blendet alle nicht unterstützten Clients aus.

Avamar Desktop/Laptop

Avamar Desktop/Laptop ist eine Version der Avamar Client-Software, die erweiterte Funktionen für Enterprise-Desktop- und -Laptopcomputer bietet.

Die Avamar Desktop/Laptop-Funktionen sind zur Verbesserung der Funktionen des Avamar-Clients für Desktops und Laptops unter Windows und Macintosh konzipiert. Viele Funktionen werden auch auf qualifizierenden Linux-Computern unterstützt.

Die Avamar Desktop/Laptop-Funktionen sind über zwei Benutzeroberflächen verfügbar:

- Die lokale Clientbenutzeroberfläche wird bei der Installation von Avamar Client für Windows bzw. Avamar Client für Mac OS X auf dem Clientcomputer installiert. In der Clientbenutzeroberfläche von Windows-Computern wird ein Avamar-Symbol im Infobereich („Taskleiste“), bei Mac-Computern in der Menüleiste angezeigt. Klicken Sie unter Windows mit der rechten Maustaste auf das Symbol bzw. klicken Sie unter Mac auf das Symbol, um das Clientmenü zu öffnen, über das auf die Backup-, Wiederherstellungs- und Programmeinstellungen sowie die Protokolle zugegriffen werden kann.
- Über die Webbrowser-Benutzeroberfläche (Webbenutzeroberfläche) lassen sich ein On-Demand-Backup bzw. eine On-Demand-Wiederherstellung starten, die Backup- und Wiederherstellungsaktivität für einen Clientcomputer anzeigen oder andere Backupeinstellungen für einen Clientcomputer konfigurieren.

Avamar Installation Manager
Die Benutzeroberfläche von Avamar Installation Manager ist Teil der AvInstaller-Software, die der Kundensupport während der Installation oder des Upgrades der Avamar-Serversoftware auf dem Utility-Node installiert. Verwenden Sie Avamar Installation Manager zur Installation und zum Upgrade der Software auf dem Avamar-Server.

Avamar Downloader Service
Der Avamar Downloader Service managt den Prozess zum Prüfen und Herunterladen von Avamar-Serversoftwareupdates. Die Avamar Downloader Service-Software wird auf einem eigenständigen Microsoft Windows-Server ausgeführt, der Netzwerkzugriff auf Avamar-Standorte über das Internet und auf sämtliche Avamar-Server an einem Standort ermöglicht.

Avamar Web Restore
Avamar Web Restore bietet Zugriff auf folgende Funktionen:

- Suchen nach oder Durchsuchen von gesicherten Verzeichnissen und wiederherzustellenden Dateien
- Herunterladen der Avamar Client-Software
- Anzeigen der auf dem Avamar-Server gespeicherten Avamar-Produktdokumentation
- Öffnen der Avamar Administrator-Managementkonsolensoftware

Data Domain-Systemunterstützung

Sie können Backups entweder auf dem Avamar-Server oder auf einem Data Domain-System speichern. Die Backupmetadaten werden auf dem Avamar-Server gespeichert.

Bevor Sie Backups auf einem Data Domain-System speichern können, müssen Sie das Data Domain-System mithilfe von Avamar-Administrator der Avamar-Konfiguration hinzufügen. Bei der Durchführung eines On-Demand-Backups oder bei der Erstellung eines Dataset für ein geplantes Backup wählen Sie dann das Data Domain-System in den Plug-in-Optionen aus. Sie können Backups auf einem Data Domain-System auch mithilfe der Befehlszeilenoberfläche (CLI) durchführen.

Zur Wiederherstellung von Backups werden dieselben Schritte wie bei der Wiederherstellung vom Avamar-Server oder einem Data Domain-System durchgeführt. Beim Wiederherstellungsprozess wird der Speicherort des Backups festgelegt und das Backup wiederhergestellt.

Die Unterstützung für Data Domain Cloud Tier wurde in Avamar 7.4 initiiert. DD Cloud Tier verschiebt Daten von einer Data Domain in die Cloud. Sie können über Avamar-

Administrator Cloud-Tiering konfigurieren, um Avamar-Backups von Data Domain in die Cloud zu verschieben und eine nahtlose Recovery dieser Backups durchzuführen.

Die Unterstützung für Data Domain Cloud Tier Disaster Recovery wurde mit Avamar 7.5 initiiert. Sie können Backups aus der Cloud im Falle des Ausfalls eines Data Domain-Systems wiederherstellen und auch einen Avamar-Server aus der Cloud wiederherstellen.

Unter *Avamar und Data Domain-System – Integrationshandbuch* finden Sie weitere Informationen über Data Domain-Systeme in einer Avamar-Umgebung sowie detailliert erläuterte Schritte zum Hinzufügen eines Data Domain-Systems zu einer Avamar-Konfiguration.

Datendeduplizierung

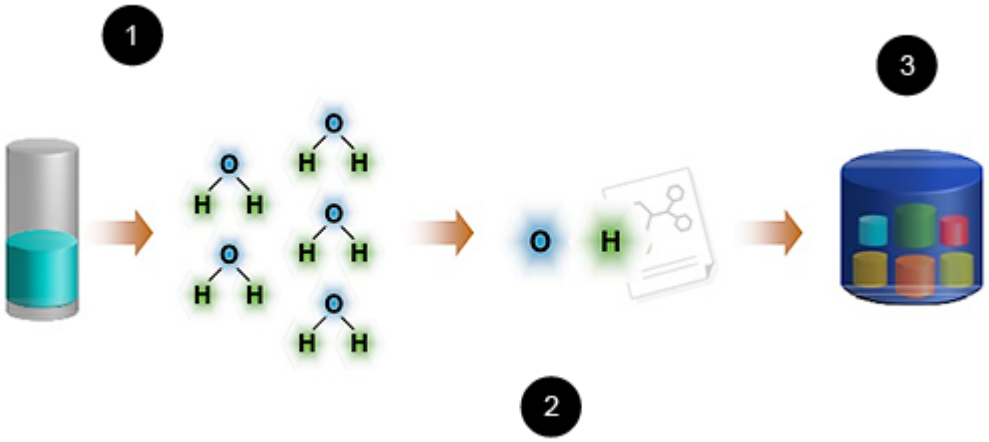
Die Datendeduplizierung ist eine wichtige Funktion des Avamar-Systems. Die Datendeduplizierung sorgt dafür, dass jedes eindeutige Sub-File-basierte Objekt variabler Länge standort- und serverübergreifend nur einmal gespeichert wird.

Während Backups überprüft die Avamar-Clientsoftware das Clientdateisystem und wendet einen Datendeduplizierungsalgorithmus an, der redundante Datensequenzen identifiziert und das Clientdateisystem in Sub-File-basierte Datensegmente variabler Länge aufspaltet. Jedem Datensegment wird eine eindeutige ID zugewiesen.

Die Clientsoftware ermittelt dann, ob diese eindeutige ID bereits auf dem Avamar-Server gespeichert wurde. Wenn sich dieses Objekt auf dem Avamar-Server befindet, wird im Backup ein Link zum gespeicherten Objekt referenziert.

Sobald ein Objekt auf dem Server gespeichert wurde, wird es nicht erneut über das Netzwerk gesendet, ganz gleich, wie oft es auf einer beliebigen Anzahl von Clients vorhanden ist. Diese Funktion reduziert den Netzwerkverkehr erheblich und sorgt für eine deutlich bessere Speichereffizienz auf dem Server.

Abbildung 4 Datendeduplizierung



1. Aufteilen der Daten in Atome (Dateidaten aus Segmenten mit variabler Länge)
2. Einmaliges Senden und Speichern jedes Atoms
3. Bis zu 500-fache Reduzierung der täglichen Backupdaten im Avamar-Backup-Repository.

Sicherheit und Netzwerke

In den folgenden Abschnitten wird eine Übersicht über wichtige Avamar-Sicherheits- und Netzwerkfunktionen bereitgestellt. Das *Avamar – Produktsicherheitshandbuch* enthält alle Einzelheiten zur Produktsicherheit und Netzwerkkonfiguration.

Verschlüsselung

Zur Verbesserung der Sicherheit ermöglicht Avamar eine In-Flight-Verschlüsselung aller zwischen Clients und Server gesendeten Daten.

Sie können die Verschlüsselungsstufe von Client zu Client in den Clienteigenschaften oder für eine vollständige Gruppe von Clients in den Gruppeneigenschaften festlegen. Sie können die In-Flight-Verschlüsselung auch vollständig deaktivieren.

Alle Avamar-Server können auch so konfiguriert werden, dass für auf dem Server gespeicherte Daten eine Data-at-Rest-Verschlüsselung durchgeführt wird. Die Entscheidung zur Verschlüsselung aller auf einem Avamar-Server gespeicherten Daten ist in der Regel eine einmalige Entscheidung, die bei der ersten Bereitstellung des Servers am Kundenstandort getroffen wird.

Unterstützung für IPv4 und IPv6

Internet Protocol (IP) ist ein Satz von Kommunikationsregeln für das Routing des Datenverkehrs in Netzwerken an adressierbare Geräte wie Avamar-Systemkomponenten. Das Avamar-System unterstützt die Adressnotationen IPv4 (Internet Protocol Version 4) und IPv6.

IPv4-Notation
Die IPv4-Notation wird in 4 Oktetten dargestellt, d. h. als 1- bis 3-stellige Dezimalzahlen im Bereich von 0 bis 255. Jedes Oktett wird durch Punkte getrennt und stellt 8 Bit an Daten für einen Gesamtadressraum von 32 Bit dar.

Eine Subnetzmaske identifiziert eine Reihe (ein Subnetz) von IP-Adressen im selben Netzwerk. Bei Avamar lautet die Subnetzmaske /24, stellvertretend für eine 255.255.255.0-Netzmaske.

Ein Beispiel für eine IPv4-Adresse und eine Subnetzmaske lautet `10.99.99.99/24`.

Die IPv4-Notation kann nicht abgekürzt werden. Wenn ein Oktett den Wert Null (0) enthält, wird in diesem Oktett eine 0 verwendet.

IPv6-Notation
Die IPv6-Notation wird in 16 Oktetten dargestellt, d. h. als 2-stellige Hexadezimalzahlen im Bereich von 00 bis FF. Bei der IPv6-Notation werden Oktette nach Paaren aus acht Gruppen kombiniert, die durch Doppelpunkte getrennt werden, wobei jede Gruppe 16 Bit Daten für einen Gesamtadressraum von 128 Bit darstellt.

Bei Avamar lautet die Subnetzmaske (bei IPv6 als Präfix bezeichnet) /64.

Ein Beispiel für eine IPv6-Adresse und ein Präfix lautet `2001:0db8:85a3:0042:1000:8a2e:0370:7334/64`.

Bei Gruppen, die einen Wert von Null (0) aufweisen, unterscheidet sich die IPv6-Notation von IPv4, die sich abkürzen lässt. Beispielsweise handelt es sich bei Folgendem um eine gültige IPv6-Adresse und ein Präfix: `2001:db8:abcd:0012::0/64`.

Avamar-IP-Konfigurationen

In der Avamar-Benutzeroberfläche kann eine IP-Adresse entweder in IPv4- oder als IPv6-Notation dargestellt werden. Der angezeigte Wert hängt von der jeweiligen Komponente ab, die bei der Hardware- und Softwareinstallation konfiguriert wurde.

IPv4 und IPv6 sind nicht interoperabel. Sie werden in unterschiedlichen Stapeln betrieben (d. h. parallele, unabhängige Netzwerke).

Avamar kann in einer Dual-Stapelkonfiguration eingerichtet werden. In diesem Fall kann jede Avamar-Komponente eine IPv4-Adresse, eine IPv6-Adresse oder beides (eine primäre und eine sekundäre Adresse) aufweisen. In der Avamar-Benutzeroberfläche können die primäre Adresse oder beide Dual-Stapeladressen einer Komponente angezeigt werden. Beispielsweise gibt die folgende IP-Adresse für ein bestimmtes Gerät an, dass es als dualer Stapel konfiguriert ist: `10.99.99.99/24,2001:db8:abcd:0012::0/64`.

TLS-1.2-Verschlüsselungsprotokoll erforderlich

Mithilfe der TLS-1.0- und -1.1- Protokolle verschlüsselter Datenverkehr wird nicht mehr unterstützt. Browser, Clients und andere Komponenten, die diese Protokolle erfordern, können nicht mit dem Server verbunden werden. Nur TLS-1.2-Verschlüsselung wird unterstützt.

SSH-MAC-Algorithmen

Die SSH-Konfiguration wurde geändert, um schwache MAC-Algorithmen zu entfernen, die für die SSH-Verbindungen verwendet werden.

Die folgenden MAC-Algorithmen werden für SSH-Verbindungen verwendet:

- hmac-sha2-512-etm@openssh.com
- hmac-sha2-512
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-256
- umac-128-etm@openssh.com
- umac-128@openssh.com
- hmac-ripemd160-etm@openssh.com
- hmac-ripemd160

Hinweis

Ältere Versionen der SSH-Clients, z. B. PuTTY oder Plink, verwenden schwache MAC-Algorithmen für eine SSH-Verbindung und müssen aktualisiert werden. Zum Anzeigen der neuesten Version von PuTTY siehe http://www.putty.org/

KAPITEL 2

Avamar Administrator

In diesem Kapitel werden folgende Themen behandelt:

Überblick über Avamar-Administrator

Avamar-Administrator ist eine grafische Managementkonsolen-Softwareanwendung, die verwendet wird, um ein Avamar-System über einen unterstützten Windows- oder Linux-Clientcomputer zu verwalten.

Installieren Sie Avamar-Administrator auf einem unterstützten Computer und starten Sie die Software über das Desktopsymbol oder eine Befehlszeile. Sie können auch die Java Web Start-Version der Konsolensoftware über einen Webbrowser oder Backup and Recovery Manager aufrufen.

Avamar-Administrator ist die primäre Benutzeroberfläche für die Überwachung und Konfiguration des Avamar-Systems. Sie können damit Backups, Wiederherstellungen und Systemwartungsaktivitäten überwachen sowie Backup-Policies konfigurieren, Clients und Benutzerkonten managen und sonstige Systemeinstellungen konfigurieren.

Sie können nur jeweils ein Avamar-System über Avamar-Administrator verwalten.

Das Dashboard Avamar-Administrator wird angezeigt, wenn Sie sich bei Avamar-Administrator anmelden. Das Dashboard bietet eine Anzeige auf einen Blick für den Avamar-Systemstatus sowie den Zugriff auf sämtliche Funktionen über Menüs und Links zum Startprogramm.

Installieren von Avamar Administrator

Sie können Avamar Administrator auf unterstützten Microsoft Windows- und 64-Bit-Linux-Plattformen installieren.

Details zur Unterstützung für bestimmte Betriebssystemversionen sind im *Avamar Kompatibilitäts- und Interoperabilitätsmatrix* beim Avamar-Support unter http://compatibilityguide.emc.com:8080/CompGuideApp verfügbar.

Hinweis

Stellen Sie vor der Installation von Avamar Administrator sicher, dass die Plattform bereits manuell auf Java 7 oder 8 aktualisiert wurde.

Hinweis

Stellen Sie sicher, dass Ihre DNS-Umgebung so konfiguriert ist, dass alle Clients, auf denen Administrator ausgeführt wird, die Hash-File-System-Adresse (hfsaddr) auflösen können.

Installieren von Avamar Administrator in Microsoft Windows

Vorgehensweise

1. Melden Sie sich beim Computer an, auf dem Sie Avamar Administrator installieren.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende URL ein:

   `https://Avamar_server/dtlt/home.html`

   Dabei steht Avamar_server für den DNS-Namen oder die IP-Adresse des Avamar-Servers.

   Die Seite **Avamar Web Restore** wird angezeigt.

3. Klicken Sie auf **Downloads**.
4. Führen Sie je nach Betriebssystem einen der folgenden Schritte aus:
   - Wenn Sie die Software unter 32-Bit-Windows installieren, klicken Sie neben dem Ordner **Windows (32 Bit)** auf **+**.
   - Wenn Sie die Software unter 64-Bit-Windows installieren, klicken Sie neben dem Ordner **Windows (64 Bit)** auf **+**.
5. Führen Sie je nach Betriebssystem einen der folgenden Schritte aus:
   - Wenn Sie die Software unter 32-Bit-Windows installieren, klicken Sie neben dem Ordner **Microsoft Windows Vista, 7, 8, 8.1, 10, Microsoft Windows Server 2008 (Console)** auf **+**.
   - Wenn Sie die Software unter 64-Bit-Windows installieren, klicken Sie neben dem Ordner **Microsoft Windows Vista, 7, 8, 8.1, 10, Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2 (Console)** auf **+**.
6. Suchen Sie das Java Runtime Environment(JRE)-Installationspaket. Dies ist normalerweise der letzte Eintrag im Ordner.
7. Wenn die JRE-Version auf dem Clientcomputer älter als die auf dem Avamar-Server vorhandene JRE-Version ist, laden Sie die neuere JRE-Version vom Avamar-Server herunter und installieren Sie sie:
   a. Klicken Sie auf das `jre-`*`version`*`.exe`-Installationspaket, wobei *version* für die JRE-Version steht.
   b. Öffnen Sie die Installationsdatei. Sie können die Datei auch herunterladen und dann vom Speicherort aus öffnen.
   c. Befolgen Sie die Anweisungen auf dem Bildschirm, um die JRE-Installation abzuschließen.
8. Klicken Sie auf das `AvamarConsoleMultiple-windows-`*`version`*`.exe`-Installationspaket, wobei *version* für die Version der Avamar Administrator-Software steht.
9. Öffnen Sie die Installationsdatei. Sie können die Datei auch herunterladen und dann vom Speicherort aus öffnen.
10. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation der Avamar Administrator-Software abzuschließen.

Installieren von Avamar Administrator unter Linux

Vorgehensweise

1. Melden Sie sich beim Computer an, auf dem Sie Avamar Administrator installieren.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende URL ein:

   `https://`*`Avamar_server/dtlt/home.html`*

   Dabei steht Avamar_server für den DNS-Namen oder die IP-Adresse des Avamar-Servers.

   Die Seite **Avamar Web Restore** wird angezeigt.
3. Klicken Sie auf **Downloads**.
4. Klicken Sie auf **+** neben dem Ordner **Linux for x86 (64 bit)**.
5. Klicken Sie auf **+** neben dem Ordner **Red Hat Enterprise Linux 5 (Console)**.

Hinweis

Verwenden Sie die Red Hat Enterprise Linux 5-Installationspakete für alle unterstützten Linux-Versionen.

6. Suchen Sie das JRE-RPM-Installationspaket. Dies ist normalerweise der letzte Eintrag im Ordner.
7. Wenn die JRE-Version auf dem Clientcomputer älter als die auf dem Avamar-Server vorhandene JRE-Version ist, laden Sie das Installationspaket in einen temporären Ordner wie `/tmp` herunter.

   Der Dateiname des Installationspaket lautet `jre-version-platform.rpm`, wobei *version* für die JRE-Version und *platform* für die Computerplattform steht.
8. Laden Sie das Installationspaket `AvamarConsole-linux-rhel5-x86_64-version.rpm` in einen temporären Installationsordner wie `/tmp` herunter.
9. Öffnen Sie eine Befehlsshell und melden Sie sich als „Root“ bei dem Computer an, auf dem die Software installiert werden soll.
10. Ändern Sie das Verzeichnis mithilfe eines Befehls wie **`cd /tmp`** zu dem temporären Ordner um, in den Sie die Installationspakete heruntergeladen haben.
11. Wenn Sie JRE heruntergeladen haben, installieren Sie JRE, indem Sie **`rpm -ivh JRE-version-platform.rpm`** eingeben.
12. Befolgen Sie die Anweisungen auf dem Bildschirm, um die JRE-Installation abzuschließen.
13. Installieren Sie Avamar Administrator, indem Sie **`rpm -ih AvamarConsole-linux-rhel5-x86_64-version.rpm`** eingeben.

    Beim Installationsprozess werden Sie aufgefordert, `avsetup_mcc` auszuführen, um Avamar Administrator zu konfigurieren.
14. Konfigurieren Sie Avamar Administrator, indem Sie **`/usr/local/avamar/version/bin/avsetup_mcc`** eingeben.

    Beim Konfigurationsprozess werden Sie aufgefordert, den Speicherort der JRE-Installation anzugeben.
15. Drücken Sie die **Enter**, um das standardmäßige Installationsverzeichnis zu übernehmen.

    Beim Konfigurationsprozess werden Sie aufgefordert, das Stammverzeichnis der Avamar-Software anzugeben.
16. Drücken Sie die **Enter**, um das standardmäßige Installationsverzeichnis zu übernehmen.

    Es wird eine Bestätigungsmeldung angezeigt.

Durchführen von Upgrades für Avamar Administrator

Sie können Avamar Administrator sowohl auf Microsoft Windows- als auch auf Linux-Computern per Upgrade aktualisieren.

Vorgehensweise

- Sie können mehrere Versionen von Avamar Administrator auf demselben Microsoft Windows-Computer installieren. Wenn Sie Avamar Administrator auf

einem Computer installieren, auf dem diese Software bereits vorhanden ist, gehen Sie während des Installationsverfahrens bei der Auswahl eines Zielordners sorgfältig vor:

- Wählen Sie einen anderen Installationsordner aus, um eine ältere Version beizubehalten.
- Wählen Sie für ein direktes Upgrade der Avamar Administrator-Installation denselben Installationsordner aus. Die beiden Versionen werden durch ihre vollständigen Versionsnummern identifiziert.

Hinweis

Stellen Sie vor der Installation/dem Upgrade von Avamar Administrator sicher, dass für die Plattform bereits ein manuelles Upgrade auf Java 7 oder 8 durchgeführt wurde.

- Um ein Upgrade für die Avamar Administrator-Software auf der Linux-Plattform durchzuführen, deinstallieren Sie die vorherige Version und installieren Sie die neue Software. Die Verwendung des Linux-Softwareupgradebefehls (`rpm -Uh`) wird nicht unterstützt.

Hinweis

Stellen Sie vor der Installation der neuen Version von Avamar Administrator sicher, dass für die Plattform bereits ein manuelles Upgrade auf Java 7 oder 8 durchgeführt wurde.

Deinstallieren von Avamar Administrator

Sie können Avamar Administrator auf Microsoft Windows- und Linux-Computern deinstallieren.

Bevor Sie beginnen

Schließen Sie alle geöffneten Avamar Administrator-Sitzungen. Anderenfalls kann der Deinstallationsprozess möglicherweise nicht erfolgreich abgeschlossen werden, was bei der zukünftigen Installation von Avamar Administrator Probleme verursachen kann.

Vorgehensweise

- Rufen Sie bei einem Microsoft Windows-Computer das Windows-Menü **Start** auf und wählen Sie **Programs > Avamar > Administrator > *version* > Uninstall** aus und klicken Sie in der Bestätigungsmeldung dann auf **OK**.
- Bei einem Linux-Computer:
  a. Öffnen Sie eine Befehlsshell und melden Sie sich als Root an.
  b. Legen Sie den Paketnamen fest, indem Sie **`rpm -qa | grep Av`** eingeben.
  c. Geben Sie **`rpm -e AvamarConsole-version`** ein, wobei *AvamarConsole-version* für das Avamar Administrator-Installationspaket steht.

Bearbeiten der Avamar Administrator-Clientvoreinstellungen

Einige Avamar Administrator-Clientvoreinstellungen können Sie direkt in Avamar Administrator bearbeiten. Allerdings stehen bestimmte Einstellungen ausschließlich für

die Bearbeitung in der Datei mit den Clienteinstellungen, `mcclient.xml`, zur Verfügung.

Vorgehensweise

1. Schließen Sie Avamar Administrator.
2. Öffnen Sie *install_dir*`/var/mc/gui_data/prefs/mcclient.xml` in einem Texteditor, wobei *install_dir* für das Avamar Administrator-Installationsverzeichnis steht.
3. Bearbeiten Sie die Einstellungselemente.
4. Speichern und schließen Sie die Datei.

   Die Änderungen werden beim nächsten Start von Avamar Administrator übernommen.

Einrichten eines Sitzungs-Timeout für Avamar Administrator

Eine Avamar Administrator-Sitzung bleibt solange aktiv, bis der Benutzer die Anwendung durch Auswahl von **Exit** im Menü schließt. Um die über Avamar Administrator verfügbaren Ressourcen zu schützen, legen Sie einen Timeout-Wert für die Sitzung fest. Der Wert gilt für alle Avamar Administrator-Sitzungen, für die eine Verbindung zum Avamar-Server hergestellt wurde.

Nachdem Sie einen Timeout-Wert für die Sitzung festgelegt haben, prüft Avamar Administrator die Benutzeroberfläche auf Aktivität. Wenn Avamar Administrator innerhalb der als Timeout-Wert festgelegten Anzahl von Minuten keine Maus- oder Tastaturaktivität auf der Benutzeroberfläche feststellt, werden alle Prozesse heruntergefahren, alle Fenster geschlossen und das Dialogfeld **Inactive** angezeigt.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

        `ssh-agent bashssh-add ~admin/.ssh/admin_key`
2. Beenden Sie den Service Management Console Server (`mcs`), indem Sie **`dpnctl stop mcs`** eingeben.
3. Ändern Sie das Arbeitsverzeichnis in `/usr/local/avamar/var/mc/server_data/prefs`, indem Sie **`cd /usr/local/avamar/var/mc/server_data/prefs`** eingeben.
4. Öffnen Sie `mcserver.xml` in einem Texteditor.
5. Suchen Sie den Eintrag `<node name="mon">`.
6. Bearbeiten Sie den Wert von Eintrag `<entry key="consoleInactiveMinutesToReport" value="`*n*`" />` im Eintrag `<node name="mon">`, wobei *n* der Sitzungs-Timeout-Wert in Minuten ist.

7. Speichern Sie die Änderung und schließen Sie den Texteditor.
8. Starten Sie den MCS und den Scheduler, indem Sie Folgendes eingeben:

```
dpnctl start mcs
dpnctl start sched
```

9. Schließen Sie die Befehlsshell.

   Avamar Administrator verwendet den neuen Timeout-Wert der Sitzung, wenn Sie Avamar Administrator das nächste Mal öffnen und eine Verbindung zum Avamar-Server herstellen.

Starten von Avamar-Administrator

Starten Sie Avamar-Administrator mithilfe der Konsolensoftware, die auf einem lokalen Computer installiert ist, oder starten Sie Avamar Administrator über die Java Web Start-Version der Konsolensoftware.

Bevor Sie beginnen

Achten Sie darauf, dass mindestens 512 MB Systemspeicher auf dem lokalen Computer zur Verfügung stehen. Anderenfalls können beim Start von Avamar Administrator Java-Heap-Fehler auftreten.

Vorgehensweise

1. Starten Sie Avamar-Administrator mit einem der folgenden Verfahren.

Version der Konsolensoftware	Methode
Microsoft Windows	Doppelklicken Sie auf das Symbol **Avamar Administrator** auf dem Windows-Desktop.
Linux	Öffnen Sie eine Befehlsshell und geben Sie Folgendes ein: `mcgui`.
Java Web Start	Geben Sie in das Adressfeld eines Webbrowsers `https://`*Avamar_server*`/mc-portal/mcgui` ein. Dabei ist *Avamar_server* die IP-Adresse oder der auflösbare Hostname eines Avamar-Servers.
Java Web Start-Version von Backup and Recovery Manager	Wählen Sie im Backup and Recovery Manager im Fenster **Systems** ein Avamar-System aus und klicken Sie auf **Launch Management Console**.

   Das Fenster **Login** wird angezeigt.

2. Geben Sie unter **Server** die IP-Adresse oder den DNS-Namen des Avamar-Servers ein, bei dem Sie sich anmelden möchten.

   Hinweis

   Übernehmen Sie den Namen eines Avamar-Servers und eine Avamar-Domain automatisch in die Felder **Server** und **Domain Name**, indem Sie auf **Options** klicken und den Servernamen in das Feld **Default Administrator Server** und den Domainnamen in das Feld **Default Domain** eingeben.

3. Geben Sie unter **User Name** einen Benutzernamen ein.

Damit auf alle Avamar-Administrator-Funktionen zugegriffen werden kann, muss dem diesem Benutzernamen zugewiesenen Konto die Administratorrolle zugewiesen werden. Bei anderen Rollen sind die Funktionen eingeschränkt.

Geben Sie lediglich einen Benutzernamen ein, um sich mithilfe des internen Authentifizierungssystems zu authentifizieren. Um sich mithilfe des Enterprise Authentication-Systems (veraltet) oder der Verzeichnisdienstauthentifizierung zu authentifizieren, geben Sie ***username@server*** ein, wobei *username* für den Benutzernamen und *server* für den vollständig qualifizierten Domainnamen des Authentifizierungsservers steht.

Wenn Sie das Format *username@server* für den Benutzernamen verwenden, versucht das System, den Benutzer mithilfe von Enterprise Authentication zu authentifizieren. Wenn die Authentifizierung mithilfe von Enterprise Authentication fehlschlägt, versucht das System, den Benutzer mithilfe der Verzeichnisdienstauthentifizierung zu authentifizieren.

4. Geben Sie unter **Password** das Passwort für das Benutzerkonto ein.
5. Geben Sie unter **Domain Name** die Avamar-Domain ein, bei der Sie sich anmelden möchten:
   - Die Root-Domain, für die standardmäßig ein Schrägstrich (`/`) als Eintrag verwendet wird
   - Eine bestimmte Domain oder Subdomain, für die der Domainpfad mithilfe der Syntax `/domain/subdomain1/subdomain2` eingegeben wird.
6. Klicken Sie auf **Log In**.

   Wenn dies das erste Mal ist, das Sie eine Verbindung mit diesem Avamar-Server hergestellt haben, wird die das Dialogfeld **Accept Server Certificate** geöffnet. Überprüfen Sie die Details des Serverzertifikats und klicken Sie auf **Yes**.

   Das Avamar-Administrator-Dashboard wird angezeigt.

Avamar Administrator-Dashboard

Das Avamar Administrator-Dashboard bietet eine Anzeige auf einen Blick für den Avamar-Systemstatus sowie den Zugriff auf sämtliche Funktionen über Menüs und Link zum Startprogramm.

Das Dashboard wird bei der Anmeldung bei Avamar Administrator angezeigt.

Abbildung 5 Avamar Administrator-Dashboard

Link zum Startprogramm

Der Dashboard Link zum Startprogramm führt permanente Fenster für Aufgaben in Avamar Administrator aus.

Tabelle 6 Dashboard Link zum Startprogramm

Schaltfläche	Fenster	Im Fenster verfügbare Aufgaben
Policy	Policy	Erstellung und Management von Gruppen, Datasets, Planungen und Aufbewahrungs-Policies
Backup & Restore	Backup, Restore, and Manage	Durchführung von On-Demand-Backups und Wiederherstellungen sowie Management von abgeschlossenen Backups
Datenverschiebungs-Policy	Datenverschiebungs-Policy	Konfiguration der Policy-basierten Replikation und von Cloud-Tier
Activity	Activity	Überwachung von Backups, Wiederherstellungen, Backupvalidierungen und Replikationsaktivitäten
Administration	Administration	Erstellung und Management von Domains, Clients, Benutzern, Systemereignissen und Diensten
Server	Server	Überwachung von Serveraktivität und Clientsitzungen

Bereich „System Information“

Der Bereich **System Information** im Avamar Administrator-Dashboard liefert eine Übersicht über wichtige Systemstatistiken.

Systemstatus
Das Symbol **System State** dient als Statusanzeige für den gesamten Systemstatus:

- Ein grünes Häkchensymbol weist darauf hin, dass das System vollständig betriebsbereit ist.
- Ein gelbes Vorsichtssymbol weist darauf hin, dass ein zu behebendes Problem mit dem System vorliegt, Backups jedoch weiterhin durchgeführt werden können.
- Ein rotes x-Symbol weist darauf hin, dass ein Problem vorliegt, das unverzüglich zu beheben ist. Backups können erst wieder durchgeführt werden, wenn das Problem behoben wurde.

Klicken Sie auf das Pfeilsymbol neben dem Feld **System State**, um ausführlichere Informationen zum Systemstatus anzuzeigen. In der folgenden Tabelle finden Sie ausführliche Informationen zum Systemstatus im Dashboard.

Tabelle 7 Systemstatusfelder im Avamar Administrator-Dashboard

Feld	Beschreibung
Avamar-Status	Fasst den aktuellen Betriebsstatus des Avamar-Servers zusammen: • Ein grünes Häkchensymbol weist darauf hin, dass der Avamar-Server vollständig betriebsbereit ist. • Ein gelbes Achtungsymbol weist darauf hin, dass mindestens ein zu behebendes Problem mit dem Avamar-Server vorliegt, Backups jedoch weiterhin durchgeführt werden können. • Ein rotes x-Symbol weist darauf hin, dass sich der Avamar-Server im Betriebsstatus „Inactive“, „Offline“, „Degraded“ oder „Unknown“ befindet.
Capacity State	Fasst die Kapazitätsauslastung und Integrität des Systems zusammen: • Ein grünes Häkchen weist darauf hin, dass das System mehr als 75 % der Gesamtspeicherkapazität belegt hat. • Ein gelbes Achtungsymbol weist darauf hin, dass das System mehr als 75 %, jedoch unter 90 % der Gesamtspeicherkapazität belegt hat. Erwägen Sie, Kapazität hinzuzufügen oder alte Backups zu löschen. • Ein rotes x-Symbol weist darauf hin, dass das System über 90 % der Gesamtspeicherkapazität belegt hat. Es

Tabelle 7 Systemstatusfelder im Avamar Administrator-Dashboard (Fortsetzung)

Feld	Beschreibung
	können erst neue Backups durchgeführt werden, wenn Sie Kapazität hinzugefügt oder alte Backups gelöscht haben.
Critical Events	Fasst nicht quittierte Systemereignisse zusammen: • Ein grünes Häkchen weist darauf hin, dass keine kritischen, zu quittierenden Systemereignisse vorliegen. • Ein gelbes Vorsichtssymbol weist darauf hin, dass mindestens ein zu quittierendes Warnereignis vorliegt. • Ein rotes x-Symbol weist darauf hin, dass mindestens ein zu quittierendes Systemfehlerereignis vorliegt.
Last Checkpoint	Gibt den Zeitraum seit dem letzten Kontrollpunkt an: • Ein grünes Häkchen weist darauf hin, dass innerhalb der letzten 24 Stunden ein Prüfpunkt auf diesem Avamar-Server erfolgreich abgeschlossen wurde. • Ein gelbes Achtungsymbol weist darauf hin, dass innerhalb der letzten 24 bis 48 Stunden ein Prüfpunkt auf diesem Avamar-Server erfolgreich abgeschlossen wurde. • Ein rotes x-Symbol weist darauf hin, dass über 48 Stunden verstrichen sind, seit ein Prüfpunkt auf diesem Avamar-Server erfolgreich abgeschlossen wurde.
Last Validated Checkpoint	Gibt den Zeitraum seit der letzten Kontrollpunktvalidierung an: • Ein grünes Häkchen weist darauf hin, dass innerhalb der letzten 48 Stunden eine Prüfpunktvalidierung auf diesem Avamar-Server erfolgreich abgeschlossen wurde. • Ein gelbes Achtungsymbol weist darauf hin, dass innerhalb der letzten 48 bis 72 Stunden eine Prüfpunktvalidierung auf diesem Avamar-Server erfolgreich abgeschlossen wurde. • Ein rotes x-Symbol weist darauf hin, dass über 72 Stunden verstrichen sind, seit auf diesem Avamar-Server eine Prüfpunktvalidierung erfolgreich abgeschlossen wurde.

Tabelle 7 Systemstatusfelder im Avamar Administrator-Dashboard (Fortsetzung)

Feld	Beschreibung
Last Garbage Collection	Gibt den Zeitraum seit der letzten automatischen Speicherbereinigung an: • Ein grünes Häkchen weist darauf hin, dass innerhalb der letzten 30 Stunden eine automatische Speicherbereinigung auf diesem Avamar-Server erfolgreich abgeschlossen wurde. • Ein gelbes Achtungsymbol weist darauf hin, dass innerhalb der letzten 30 Stunden eine automatische Speicherbereinigung auf diesem Avamar-Server nicht erfolgreich abgeschlossen wurde. • Ein rotes x-Symbol weist darauf hin, dass bei der letzten automatischen Speicherbereinigung ein Fehler aufgetreten ist.
Data Domain System(s) State	Fasst den Betriebsstatus aller Data Domain-Systeme zusammen, die diesem Avamar-Server hinzugefügt wurden: • Ein grünes Häkchen weist darauf hin, dass alle Data Domain-Systeme vollständig betriebsbereit sind. • Ein gelbes Achtungsymbol weist darauf hin, dass mindestens ein zu behebendes Problem mit Data Domain-Systemen vorliegt. Backups können jedoch weiterhin durchgeführt werden. • Ein rotes x-Symbol weist darauf hin, dass mindestens ein Problem mit Data Domain-Systemen vorliegt, das unverzüglich zu beheben ist. Backups können erst wieder durchgeführt werden, wenn alle Probleme behoben wurden.

Scheduler State

Das Feld **Scheduler State** weist darauf hin, ob geplante Aktivitäten ausgeführt werden oder angehalten wurden. Zu geplanten Aktivitäten zählen Backups, E-Mail-Benachrichtigungen und Replikationen. Geplante Aktivitäten werden zur geplanten Zeit ausgeführt. Wenn geplante Aktivitäten angehalten wurden, werden sie erst wieder ausgeführt, wenn Sie sie fortsetzen.

Klicken Sie auf **Suspend** oder **Resume**, um geplante Aktivitäten anzuhalten oder fortzusetzen.

Maintenance Activities State

Das Feld **Maintenance Activities State** weist darauf hin, ob Wartungsaktivitäten ausgeführt werden oder angehalten wurden. Zu Wartungsaktivitäten zählen Kontrollpunkte, Kontrollpunktvalidierungen und automatische Speicherbereinigungen. Wartungsaktivitäten werden zur geplanten Zeit ausgeführt. Wenn Wartungsaktivitäten

angehalten wurden, werden sie erst wieder durchgeführt, wenn Sie sie über das Fenster **Server** fortsetzen.

License Expiration
Das Feld **License Expiration** gibt das Kalenderdatum an, an dem die Lizenz für den Avamar-Server abläuft.

Data Protected
Das Feld **Data Protected** gibt die Gesamtmenge der geschützten Clientdaten (in Byte) an.

Data Protected in last 24 hours
Das Feld **Data Protected in last 24 hours** gibt die Gesamtmenge der geschützten Clientdaten (in Byte) während der letzten 24 Stunden an.

Bereich „Activities“

Der Bereich **Activities** im Avamar Administrator-Dashboard enthält den Status sowie detaillierte Informationen für Backup- und Replikationsjobs.

Backupjobs
Das Hauptstatussymbol für Backupjobs im Bereich **Activities** zeigt an, ob geplante Backups zur geplanten Zeit stattfinden oder ob ein Problem vorliegt, das die Durchführung geplanter Backups verhindert.

Klicken Sie auf die Schaltfläche mit dem Pfeil neben dem Feld **Backup Jobs**, um detaillierte Statusinformationen anzuzeigen. Die folgende Tabelle enthält Details zu verfügbaren Statusinformationen für Backupjobs.

Tabelle 8 Backupjobfelder im Avamar Administrator-Dashboard

Feld	Beschreibung
Scheduler State	Gibt an, ob der Planer für Aktivitäten wie Backups, E-Mail-Benachrichtigungen und Replikationen ausgeführt wird oder angehalten wurde.
Dispatcher State	Gibt an, ob der Dispatcher ausgeführt wird oder angehalten wurde. Wenn der Dispatcher angehalten wurde, hat der Avamar-Server den Grenzwert für die Integritätsprüfung erreicht und es können keine Backups durchgeführt werden. Kapazitätsbegrenzungen und Schwellenwerte auf Seite 326 enthält weitere Einzelheiten.
Backup Groups Enabled	Gibt die Anzahl der aktivierten Backupgruppen an. Klicken Sie auf das Fenstersymbol rechts neben dem Feld, um das Fenster **Policy** zu öffnen und Gruppen zu managen.

Sie können die Gesamtanzahl für Backupjobs mit folgenden Eigenschaften anzeigen:

- Ausstehend
- Aktuell ausgeführt
- Innerhalb des angegebenen Zeitraums fehlgeschlagen

- Innerhalb des angegebenen Zeitraums erfolgreich ausgeführt mit Ausnahmen
- Innerhalb des angegebenen Zeitraums erfolgreich ausgeführt

Wählen Sie in der Liste **Period** einen Wert aus, um den Zeitraum für die Ergebnisse von abgeschlossenen Backups zu steuern.

Klicken Sie auf eine Nummernschaltfläche, um detaillierte Informationen für einen Backupjob in der Funktion **Activity Monitor** anzuzeigen.

Replikationsjobs

Das Hauptstatussymbol für Replikationsjobs im Bereich **Activities** weist darauf hin, ob Replikationsjobs durchgeführt werden:

- Ein grünes Häkchensymbol weist darauf hin, dass geplante Replikationsjobs zur geplanten Zeit durchgeführt werden.
- Ein gelbes Vorsichtssymbol weist darauf hin, dass mindestens eine Replikationsgruppe deaktiviert ist.
- Ein rotes x-Symbol weist darauf hin, dass geplante Replikationsjobs gesperrt sind. Die Sperre kann darauf zurückgeführt werden, dass der Scheduler angehalten wurde, alle Replikationsgruppen deaktiviert sind oder ein anderes Problem mit dem System vorliegt.

Klicken Sie auf das Fenstersymbol rechts neben dem Symbol, um Replikationsgruppen im Fenster **Replication** zu konfigurieren.

Sie können die Gesamtanzahl für Replikationsjobs mit folgenden Eigenschaften anzeigen:

- Ausstehend
- Aktuell ausgeführt
- Innerhalb des angegebenen Zeitraums fehlgeschlagen
- Innerhalb des angegebenen Zeitraums erfolgreich ausgeführt mit Ausnahmen
- Innerhalb des angegebenen Zeitraums erfolgreich ausgeführt

Wählen Sie in der Liste **Period** einen Wert aus, um den Zeitraum für die Ergebnisse der abgeschlossenen Replikationsjobs zu steuern.

Klicken Sie auf eine Nummernschaltfläche, um detaillierte Informationen für einen Replikationsjob im „Replication Report“ anzuzeigen.

Bereich „Capacity“

Der Bereich **Capacity** im Avamar Administrator-Dashboard stellt Auslastungsinformationen zur Systemkapazität für den Avamar-Server und alle hinzugefügten Data Domain-Systeme bereit.

Kapazitätsinformationen des Avamar-Servers

Die Kapazitätsauslastung des Avamar-Servers wird als vertikaler Balken mit Farbindikatoren abhängig vom prozentualen Auslastungslevel der Gesamtkapazität dargestellt. In einem Textfeld ist der Prozentsatz der genutzten Kapazität angegeben.

Wenn die Avamar-Systemkonfiguration ein Data Domain-System beinhaltet, beinhalten die Kapazitätskalkulationen des Avamar-Servers Metadatenunterstützung für das Data Domain-System.

Klicken Sie auf den Link auf dem Avamar-Servernamen, um detaillierte Systeminformationen auf der Registerkarte **Server Monitor** anzuzeigen, einschließlich Data Domain-Metadatenauslastung, falls zutreffend.

Kapazitätsinformationen des Data Domain-Systems
Jedes konfiguriertes Data Domain-System wird separat im Bereich **Capacity** angezeigt.

Die Kapazitätsauslastung des Data Domain-Systems wird als vertikaler Balken mit Farbindikatoren abhängig vom prozentualen Auslastungslevel der Gesamtkapazität dargestellt.

In den Textfeldern werden die Gesamtkapazität des Data Domain-Systems in Gibibyte (GiB), die Menge der genutzten Kapazität als prozentualer Anteil und Wert in GiB und die Gesamtmenge der verfügbaren Kapazität in GiB angegeben.

Klicken Sie auf den Link auf dem Data Domain-Systemnamen, um die Webseite von Data Domain Enterprise Manager für dieses System anzuzeigen.

Bereich „Critical Events“

Der Bereich **Critical Events** im Avamar Administrator-Dashboard zeigt die Anzahl der aufgetretenen, nicht quittierten schwerwiegenden Systemfehler und Warnmeldungen sowie bestimmte definierte Systemwarnmeldungen an.

Um diese schwerwiegenden Systemfehler und Warnungen zu beheben (d. h. Rücksetzung des Zählers auf Null), müssen Sie diese ausdrücklich quittieren. Quittieren von Systemereignissen auf Seite 303 enthält weitere Einzelheiten.

In der folgenden Tabelle werden die Systemwarnmeldungen aufgeführt, die möglicherweise im Bereich **Critical Events** angezeigt werden.

Tabelle 9 Systemwarnmeldungen im Bereich „Critical Events“

Art der Warnmeldung	Beschreibung
HFS-Kontrollfehler	Wenn die letzte Kontrollpunktvalidierung fehlgeschlagen ist, wird eine Datenintegritätswarnmeldung erzeugt. Untersuchen und widmen Sie sich dem Problem so bald wie möglich. Weitere Informationen finden Sie unter Erstellen eines Kontrollpunkts auf Seite 252.
Kapazitätswarnungen	Diese Warnmeldungen warnen davor, dass das System kritische Schwellenwerte hinsichtlich Kapazitätsauslastung des Systemspeichers erreicht.
Warnungen zur Kapazitätsauslastung	Diese Warnmeldungen warnen davor, dass das System kritische Schwellenwerte hinsichtlich Kapazitätsprognose für den Systemspeicher erreicht.

Elemente der Avamar Administrator-Benutzeroberfläche

Sämtliche primären Fenster in der Avamar Administrator-Benutzeroberfläche weisen verschiedene gemeinsame Elemente und Funktionen auf, einschließlich der Statusleiste, der Funktionen der Navigationsbaumstruktur und der Maustastenkombinationen.

Statusleiste

Die unten in jedem dauerhaften Fenster von Avamar Administrator vorhandene Statusleiste liefert Statusinformationen und bietet eine Verknüpfung zu bestimmten Merkmalen und Funktionen mit einem Klick.

Abbildung 6 Avamar Administrator-Statusleiste

Startprogrammverknüpfungen

Die Verknüpfungssymbole auf der linken Seite der Statusleiste stellen Verknüpfungen zu den sechs Avamar Administrator-Hauptfenstern bereit.

Die folgende Tabelle enthält Verknüpfungssymbole, die auf der Statusleiste verfügbar sind.

Tabelle 10 Startschaltflächensymbole auf der Statusleiste

Schaltfläche	Fenster	Im Fenster verfügbare Aufgaben
Policy	Policy	Erstellung und Management von Gruppen, Datasets, Planungen und Aufbewahrungs-Policies
Backup & Restore	Backup, Restore, and Manage	Durchführung von On-Demand-Backups und Wiederherstellungen sowie Management von abgeschlossenen Backups
Datenverschiebungs-Policy	Datenverschiebungs-Policy	Konfiguration der Policy-basierten Replikation und von Cloud-Tier
Activity	Activity	Überwachung von Backups, Wiederherstellungen, Backupvalidierungen und Replikationsaktivitäten
Administration	Administration	Erstellung und Management von Domains, Clients, Benutzern, Systemereignissen und Diensten
Server	Server	Überwachung von Serveraktivität und Clientsitzungen

Statusmeldungen

Die rechte Seite der Statusleiste zeigt die Statusmeldungen für Planer und Backupdisponierung, nicht quittierte Ereignisse sowie die Avamar-Server und Data Domain-Systeme an.

Status von Planer und Backupdisponierung
Der Planer steuert, ob geplante Backups ausgeführt werden. Der Status zur Backupdisponierung gibt an, ob Backups durchgeführt werden können. Hierzu wird bestimmt, ob das Limit für die Integritätsprüfung erreicht wurde. In der folgenden Tabelle sind die verfügbaren Statusmeldungen aufgeführt.

Tabelle 11 Statusmeldungen für Planer und Backupdisponierung

Statusmeldung	Beschreibung
Sch/Disp: Running/Running	Backups werden zur geplanten Zeit durchgeführt. Geplante Backups sind aktiviert und das Limit für die Integritätsprüfung wurde nicht erreicht.
Sch/Disp: Running/Suspended	Obwohl geplante Backups aktiviert sind, werden Backups nicht zur geplanten Zeit durchgeführt, da das Limit für die Integritätsprüfung erreicht wurde. Lösen Sie die Systemkapazitätsprobleme und quittieren Sie das Systemereignis, um die Backups wiederaufzunehmen. Weitere Informationen erhalten Sie unter Kapazitätsmanagement auf Seite 325 und Quittieren von Systemereignissen auf Seite 303.
Sch/Disp: Suspended/Running	Obwohl das Limit für die Integritätsprüfung nicht erreicht wurde, werden keine Backups zur geplanten Zeit durchgeführt, da geplante Backups deaktiviert sind. Die Backups können wiederaufgenommen werden, wenn Sie die geplanten Vorgänge wieder aufnehmen.
Sch/Disp: Suspended/Suspended	Es finden keine Backups zur geplanten Zeit statt, da geplante Backups deaktiviert sind und das Limit für die Integritätsprüfung erreicht wurde. Unter Unterbrechen und Wiederaufnehmen geplanter Vorgänge auf Seite 243 Unterbrechen und Wiederaufnehmen geplanter Vorgänge auf Seite 243 erfahren Sie Details zur erneuten Aktivierung des Planers. Unter Kapazitätsmanagement auf Seite 325 und Quittieren von Systemereignissen auf Seite 303 erhalten Sie Details zum Lösen der Systemkapazitätsprobleme und zum Quittieren der Systemereignisse, damit geplante Backups wieder aufgenommen werden können.

Nicht quittierte Ereignisse

Bestimmte Systemereignisse, die bei jedem Auftreten einer Quittierung durch einen Avamar-Serveradministrator bedürfen. In der folgenden Tabelle sind die verfügbaren Statusmeldungen aufgeführt.

Tabelle 12 Statusmeldungen für nicht quittierte Ereignisse

Statusmeldung	Beschreibung
Have Unacknowledged Events	In der Liste mit den nicht quittierten Ereignissen sind Einträge vorhanden, die von einem Avamar-Serveradministrator explizit quittiert werden müssen. Klicken Sie auf das

Tabelle 12 Statusmeldungen für nicht quittierte Ereignisse (Fortsetzung)

Statusmeldung	Beschreibung
	Statussymbol bzw. die Beschriftung **Unacknowledged Events**, um im Fenster **Administration** den Bereich (die Registerkarte) **Unacknowledged Events** anzuzeigen. Quittieren von Systemereignissen auf Seite 303 enthält weitere Einzelheiten.
No Unacknowledged Events	In der Liste nicht quittierter Ereignisse sind keine Einträge vorhanden.

Status von Avamar-Server und Data Domain-System

Dieses Symbol führt den Betriebsstatus des Avamar-Servers bzw. der konfigurierten Data Domain-Systeme auf. In der folgenden Tabelle sind die verfügbaren Statusmeldungen aufgeführt.

Tabelle 13 Betriebsstatusmeldungen für Avamar-Server oder Data Domain-System

Statusmeldung	Beschreibung
Server: Full Access	Der normale Betriebsstatus eines Avamar-Servers. Alle Vorgänge sind zulässig.
Server: Admin	Der Avamar-Server befindet sich in einem administrativen Zustand, in dem Avamar-Server- und Root-Benutzer Daten lesen und schreiben können. Andere Benutzer dürfen die Daten nur lesen.
Server: Admin Only	Der Avamar-Server befindet sich in einem administrativen Zustand, in dem Avamar-Server- oder Root-Benutzer Daten lesen oder schreiben können. Andere Benutzer haben keinen Zugriff.
Server: Admin Read Only	Der Avamar-Server befindet sich in einem administrativen Schreibschutzzustand, in dem Avamar-Server- oder Root-Benutzer Daten lesen können. Andere Benutzer haben keinen Zugriff.
Server: Degraded	Auf einem oder mehreren Nodes des Avamar-Servers ist ein Festplattenausfall aufgetreten. Alle Vorgänge sind zulässig. Es sind jedoch sofortige Maßnahmen zur Problembehebung erforderlich.
Server: Inactive	Avamar Administrator konnte nicht mit dem Avamar-Server kommunizieren.
Server: Node Offline	Mindestens ein Avamar-Server-Node befindet sich im Offlinestatus.
Server: Read Only	Der Avamar-Server befindet sich in einem schreibgeschützten administrativen Zustand,

Tabelle 13 Betriebsstatusmeldungen für Avamar-Server oder Data Domain-System (Fortsetzung)

Statusmeldung	Beschreibung
	in dem alle Benutzer Daten lesen können. Das Schreiben von Daten ist ihnen jedoch nicht gestattet.
Server: Suspended	Avamar Administrator kann mit dem Avamar-Server kommunizieren, der normale Betrieb wurde jedoch vorübergehend ausgesetzt.
Server: Synchronizing	Der Avamar-Server befindet sich in einem Übergangszustand. Während des Starts und während kurzer Zeiträume bei Wartungsvorgängen ist es normal, dass der Server sich in diesem Status befindet.
Server: Unknown State	Avamar Administrator konnte den Avamar-Serverstatus nicht ermitteln.
Data Domain System Unresponsive	Avamar kann zwar eine Verbindung mit einem Data Domain-System herstellen, es gibt jedoch ein Problem mit der Verbindung.
DD System: Inactive	Avamar kann keine Verbindung zu einem Data Domain-System herstellen.

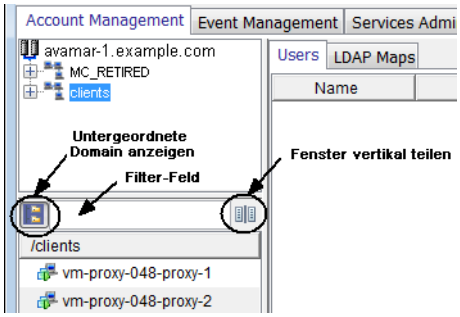
Zum Unterbrechen oder Wiederaufnehmen von Avamar-Serveraktivitäten klicken Sie auf das Symbol bzw. die Beschriftung **Server status**, um im Fenster **Avamar Server** die Registerkarte **Session Monitor** anzuzeigen. Wählen Sie von dort aus **Actions** > **Resume Backups/Restores** oder **Actions** > **Suspend Backups/Restores** aus, um Serveraktivitäten wieder aufzunehmen bzw. zu unterbrechen.

Öffnen Sie zum Anzeigen weiterer Details zum Data Domain-Systemstatus das Fenster **Server**, indem Sie auf **Navigation** > **Server** klicken. Wählen Sie die Registerkarte **Server Management** und anschließend das Data Domain-System aus der Baumstruktur aus. Der **Monitoring Status** des Data Domain-Systems wird im rechten Bereich angezeigt. Im *Avamar und Data Domain-System – Integrationshandbuch* finden Sie nähere Informationen zu den verfügbaren detaillierten Statusmeldungen.

Funktionen der Navigationsbaumstruktur

Die Navigationsbaumstrukturen in den Fenstern **Administration**, **Backup, Restore and Manage** und **Data Movement Policy** bieten mehrere Steuerelemente, um den Speicherort von mindestens einem Client zu vereinfachen.

Abbildung 7 Funktionen der Navigationsbaumstruktur



Der obere Bereich zeigt die Domainstruktur des Avamar-Servers an. Der untere Bereich zeigt Inhalte der im oberen Bereich ausgewählten Domains an. Sie können auf das Symbol zum Aufteilen des Bereichs links neben dem Filterfeld zwischen den zwei Bereichen klicken, um die zwei Bereiche vertikal statt horizontal zu trennen.

Klicken Sie auf das Doppelordnersymbol links neben dem Filterfeld, um alle Clients in Unterordnern anzuzeigen.

Geben Sie mindestens ein Zeichen in das Filterfeld ein, um die Liste nur auf Clients mit Namen zu filtern, die diese Zeichen enthalten.

Maustastenkombinationen

Die Avamar Administrator-Benutzeroberfläche unterstützt kontextsensitive Linksklick-, Rechtsklick- und Doppelklickbefehle.

Rechtsklick

Alle GUI-Elemente, die per Klick Merkmale oder Funktionen aktivieren können, unterstützen Rechtsklicks. Wenn ein GUI-Element jedoch lediglich als Navigationsmechanismus fungiert, wird das Klicken mit der rechten Maustaste nicht unterstützt. Die Clientstruktur des Fensters **Policy** verfügt beispielsweise über ein per Rechtsklick aufrufbares Kontextmenü, da bestimmte Merkmale und Funktionen abhängig vom in der Baumstruktur ausgewählten Node verfügbar werden.

Doppelklick

Doppelklicken Sie für alle Tabellen mit aufrufbaren Eigenschaften- oder Bearbeitungsdialogfeldern auf eine beliebige Zeile der Tabelle, um das Eigenschaften- oder Bearbeitungsdialogfeld anzuzeigen. Wenn Listen verwendet werden, doppelklicken Sie auf ein Element in der Liste, um das Bearbeitungsdialogfeld anzuzeigen.

Sortierung der Spaltenüberschrift

Klicken Sie auf die Spaltenüberschrift einer Tabelle, um nach dieser Spalte zu sortieren. Doppelklicken Sie beispielsweise auf die Spalte **Activity Monitor State**, um die Ansicht **Activity Monitor** nach dem Status jedes Backups zu sortieren.

Klicken Sie bei gedrückter **Umschalttaste** auf eine beliebige Spaltenüberschrift der Tabelle, um die Sortierung der Werte in einer Tabellenspalte umzukehren.

KAPITEL 3

Clientmanagement

In diesem Kapitel werden folgende Themen behandelt:

Übersicht über Avamar-Clients

Avamar-Clients sind vernetzte Computer oder Workstations, die über eine Netzwerkverbindung auf den Avamar-Server zugreifen.

Sie können Clients mithilfe von Avamar-Domains strukturieren und trennen. Domains sorgen für mehr Sicherheit, da auf Domainbasis Administrator-Benutzerkonten festgelegt werden können.

Bevor Avamar Daten auf einem Client sichern oder wiederherstellen kann, müssen Sie den Client dem Avamar-Server hinzufügen bzw. den Client bei diesem *registrieren* und dann aktivieren.

Für maximale Flexibilität bei der Bereitstellung von Avamar-Clients handelt es sich bei der Registrierung und Aktivierung um separate, asynchrone Ereignisse. Obwohl diese häufig nahezu zur selben Zeit erfolgen, kann die Zeit dazwischen allerdings auch mehrere Stunden, Tage oder Wochen betragen.

In Avamar Administrator muss der Clientname immer dem Clienthostnamen entsprechen. Wenn der Clientname in Avamar Administrator geändert werden soll, da sich der Hostname geändert hat, fahren Sie die Avamar-Software auf dem Clientcomputer herunter. Ändern Sie den Clientnamen, indem Sie die Clientinformationen bearbeiten, und starten Sie dann die Avamar-Clientsoftware neu. Nur mit dieser Methode können Sie dafür sorgen, dass die Registrierung des Clients bei der Management Console Server- (MCS-)Datenbank beibehalten wird, wodurch wiederum zurückliegende Backups weiterhin dem Client zugeordnet bleiben.

Clientdomains

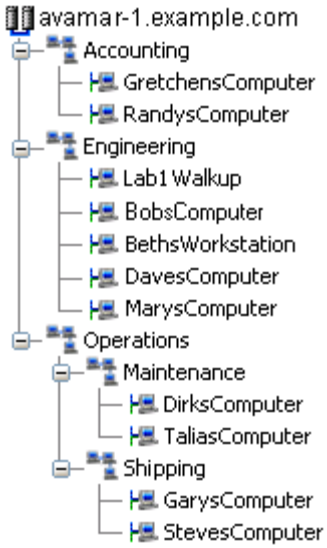
Avamar-Clientdomains sind unterschiedliche Zonen zur Organisation und Trennung der Clients im Avamar-Server. Der Server bietet mehr Sicherheit, da auf Domainbasis Administratorbenutzerkonten festgelegt werden können.

Avamar-Clientdomains sind ein vollständig integrierter Teil des Avamar-Servers und sind nicht mit Internetdomains zu verwechseln.

Verschachtelte Struktur

Sie können Domains verschachteln, um eine umfangreiche Baumstruktur zu erstellen. Stellen Sie sich die folgende Beispieldomain vor.

Abbildung 8 Beispiel für eine Avamar-Domain



Die Root-Domain `avamar-1.example.com` enthält drei Abteilungsdomains: Accounting, Engineering und Operations. Die Domain „Operations“ enthält die Subdomains „Maintenance“ und „Shipping“.

Es gibt keinen funktionalen Unterschied zwischen Domains und Subdomains. *Subdomain* ist lediglich ein Begriff, der sich auf Domains bezieht, die in einer anderen Domain auf höherer Ebene verschachtelt sind.

Hierarchisches Management

Die größte Stärke von Domains ist es, dass damit Administratoren einer bestimmten Ebene der Clientstruktur hinzugefügt werden können. Diese Administratoren auf Domainebene können dann die Clients und Policies in dieser Domain managen.

Wenn Sie zum Beispiel der Root-Domain einen Administrator hinzufügen, kann dieser Benutzer überall im System Clients und Policies verwalten. Wenn Sie jedoch einer Domain einen Administrator hinzufügen, kann der Benutzer nur Clients und Policies in dieser Domain sowie ihren Subdomains verwalten.

Bei den in diesem Handbuch beschriebenen Verfahren wird vorausgesetzt, dass Sie bei der Root-Domain angemeldet sind. Falls Sie sich bei einer Domain auf niedrigerer Ebene anmelden, haben Sie ggf. keinen Zugriff auf bestimmte Clients, Datasets, Gruppen und Ereignismanagementfunktionen außerhalb dieser Domain.

Spezielle Domains

Sie können die Domains `MC_RETIRED` und `REPLICATE` nicht löschen.

Die Domain `MC_RETIRED` enthält Clients, die stillgelegt wurden. Sie dient in erster Linie dazu, Wiederherstellungen von stillgelegten Clientbackups zu ermöglichen.

Die Domain `REPLICATE` enthält replizierte Daten von anderen Servern.

Erstellen einer Domain

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Account Management**.

3. Wählen Sie im linken Bereich den Speicherort aus der Baumstruktur aus, an dem die Domain erstellt werden soll.
4. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **New Domain** aus.

   Das Dialogfeld **New Domain** wird angezeigt.
5. Geben Sie im Feld **New Domain Name** den Namen der Domain ein.

   Domainnamen dürfen maximal 63 Zeichen lang sein und keines der folgenden Zeichen enthalten: `=~!@$^%(){}[]|,` ;#\/:*?<>'"&.
6. (Optional) Geben Sie in die restlichen Felder im Dialogfeld **New Domain** Name, Telefonnummer, E-Mail-Adresse und Standort für einen Kontakt für die Domain ein.
7. Klicken Sie auf **OK**.

   Es wird eine Bestätigungsmeldung angezeigt.
8. Klicken Sie auf **OK**.

Bearbeiten von Domaininformationen

Sie können die Kontakt- und Standortinformationen für eine Domain bearbeiten.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Account Management**.
3. Wählen Sie in der Baumstruktur die zu bearbeitende Domain aus.
4. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Edit Domain** aus.

   Das Dialogfeld **Edit Domain** wird angezeigt.
5. Bearbeiten Sie die Domainkontaktinformationen.
6. Klicken Sie auf **OK**.
7. Klicken Sie in der angezeigten Bestätigungsmeldung auf **OK**.

Löschen einer Domain

Beim Löschen einer Domain werden auch alle Clients in der Domain gelöscht. Wenn Sie die Clients im System behalten möchten, verschieben Sie die Clients in eine neue Domain, bevor Sie die Domain löschen.

Falls Sie darüber hinaus eine Verzeichnisdienstauthentifizierung verwenden, entfernt Avamar die LDAP-Zuordnungen, die diese Domain für den Zugriff nutzen. Die Löschung hat ansonsten keinerlei Einfluss auf die zugeordneten Verzeichnisdienstgruppen.

Vorgehensweise

1. (Optional) Verschieben Sie Clients in der Domain in eine neue Domain. Anweisungen finden Sie unter Verschieben eines Clients in eine neue Domain auf Seite 69.
2. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

Das Fenster **Administration** wird angezeigt.

3. Klicken Sie auf die Registerkarte **Account Management**.
4. Wählen Sie in der Baumstruktur die zu löschende Domain aus.
5. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Delete Domain** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
6. Klicken Sie auf **Yes**.
7. Klicken Sie in der zweiten angezeigten Bestätigungsmeldung auf **OK**.

Clientregistrierung

Die Clientregistrierung ist der Prozess, bei dem eine Identität für den Avamar-Server festgelegt wird. Sobald Avamar den Client „kennt“, wird eine eindeutige Client-ID (CID) zugewiesen, die während der Aktivierung an den Client zurückgegeben wird.

Es gibt drei Möglichkeiten zur Registrierung eines Clients:

- Clientseitige Registrierung
- Interaktive, serverseitige Registrierung mit Avamar Administrator
- Batchclientregistrierung

Hinweis

Wenn Sie einen Client auf einem anderen Server registrieren, befolgen Sie die Anweisungen zum Löschen eines Clients auf Seite 70, um die Registrierung für den Client auf dem ursprünglichen Server aufzuheben, bevor er auf dem anderen Server registriert wird.

Clientseitige Registrierung

Der clientseitige Registrierungsprozess hängt vom Betriebssystem ab.

Das *Avamar Backup Clients – Benutzerhandbuch* beschreibt die clientseitige Registrierung für jedes unterstützte Betriebssystem.

Bei der clientseitigen Registrierung wird außerdem gleichzeitig der Client aktiviert. Der Client wird allerdings automatisch der Standardgruppe hinzugefügt und muss das standardmäßige Dataset sowie die standardmäßige Planung und Aufbewahrungs-Policy nutzen. Folglich bietet diese Methode für bestimmte Standorte ggf. nicht genug Kontrolle.

Registrieren eines Clients in Avamar Administrator

Sie können Avamar Administrator verwenden, um dem System einen Client in einer Domain und Gruppe hinzuzufügen. Diese Aktion bietet ein hohes Maß an Kontrolle. Beispielsweise können Sie ein spezifisches Dataset sowie eine spezifische Planung und Aufbewahrungs-Policy zuweisen. Es kann allerdings zeitaufwändig sein, eine große Anzahl von Clients hinzuzufügen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Account Management**.

   In der Baumstruktur **Account Management** geben die Symbole für die Clients den Status an. Für deaktivierte Clients wird ein x angezeigt, für nicht registrierte ein Fragezeichen. Es gibt keine spezielle Symbolzuweisung für aktive Clients.

3. Wählen Sie aus der Baumstruktur die Domain für den neuen Client aus.
4. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **New Client** aus.

   Das Dialogfeld **New Client** wird angezeigt.

5. Wählen Sie aus der Liste **Client Type** die Option **Normal** aus.

   HINWEIS

   Im *Avamar for VMware – Benutzerhandbuch* erhalten Sie weitere Informationen über VMware vCenter™, Image-Proxy und Clienttypen virtueller Maschinen.

6. Geben Sie im Feld **New Client Name** den Clientnamen ein.
7. (Optional) Geben Sie in die restlichen Felder des Dialogfelds **New Client** Kontaktnamen, Telefonnummer, E-Mail-Adresse und Standort des Clients ein.
8. Klicken Sie auf **OK**.

   Es wird eine Bestätigungsmeldung angezeigt.

9. Klicken Sie auf **OK**.

Batchclientregistrierung

Bei großen Standorten mit vielen Clients ermöglicht Ihnen die Batch-Clientregistrierungsfunktion das Definieren mehrerer Clients in einer einzigen Clientdefinitionsdatei. Die Datei wird dann validiert und in den Avamar Server importiert.

Die Batch-Clientregistrierung an großen Standorten bietet nahezu genauso viel Kontrolle wie das interaktive Hinzufügen des Clients mithilfe von Avamar Administrator, ist dabei aber sehr viel schneller.

Clientdefinitionsdateien

Avamar unterstützt für die Clientdefinitionsdatei zur Batch-Clientregistrierung die Formate XML (Extensible Markup Language) und CSV (Comma-Separated Values).

XML-Format
XML-Clientdefinitionsdateien müssen die Erweiterung `.xml` aufweisen und der folgenden Struktur sowie folgendem Format entsprechen:

```
<?xml version="1.0" encoding="UTF-8" ?>
   <registration_stream>
      <registrants>
         <entry
            host_name="MyClient.Example.com"
            mcs_domain="clients"
            mcs_group="MyGroup"
            dataset="MyDataset"
            retention_policy="MyRetentionPolicy"
            contact_address="192.168.31.5"
            contact_port="28002"
```

```
            access_list="user1@avamar:password, user2@LDAP"
            encryption="high"
            encryption_override="false"
         />
      </registrants>
   </registration_stream>
```

HINWEIS

Die in diesem Thema gezeigte Clientdefinitionsdatei dient ausschließlich zu Referenzzwecken. Versuchen Sie nicht, dieses Beispiel zu kopieren und in eine Clientdefinitionsdatei einzufügen. Unsichtbare Formatierungszeichen verhindern den Erfolg eines solchen Vorgangs.

Legen Sie jeden Client über ein separates `<entry>`-Element fest. In der folgenden Tabelle werden die verfügbaren Attribute für jedes `<entry>`-Element beschrieben.

Tabelle 14 Attribute für jeden Eintrag in einer Clientdefinitionsdatei

Attribut	Beschreibung
`host_name`	Netzwerkhostname oder IP-Adresse für diesen Client.
`mcs_domain`	Optionale Avamar-Domain für diesen Client. Durch Angabe eines Werts für dieses Attribut wird die `clients`-Standarddomain überschrieben.
`mcs_group`	Optionale Standardgruppe für diesen Client. Durch Angabe eines Werts für dieses Attribut wird die Zuweisung zur Standardgruppe überschrieben.
`dataset`	Optionales Standard-Dataset für diesen Client zur Verwendung während Backups. Durch Angabe eines Werts für dieses Attribut wird das Standard-Dataset, das normalerweise von der Gruppe vererbt werden würde, überschrieben.
`retention_policy`	Optionale Standard-Policy zur Backupaufbewahrung für diesen Client. Durch Angabe eines Werts für dieses Attribut wird die Standardaufbewahrungs-Policy, die normalerweise von der Gruppe vererbt werden würde, überschrieben.
`contact_address`	Optionale IP-Adresse des Clients.
`contact_port`	Stellen Sie `contact_port` auf 28002 ein, den standardmäßigen Avamar-Datenport.
`access_list`	Optionale Liste von Benutzern, die von diesem Client aus auf den Avamar-Server zugreifen können. Das Format ist *`user@authentication`*`:password`. Wenn Sie das interne Authentifizierungssystem verwenden, muss nach dem Doppelpunkt das

Tabelle 14 Attribute für jeden Eintrag in einer Clientdefinitionsdatei (Fortsetzung)

Attribut	Beschreibung
	Wort `password` folgen. Dieser Schritt führt dazu, dass das System Benutzer beim Zugriff auf das System zur Authentifizierung auffordert. Wenn Sie das externe Authentifizierungssystem verwenden, lassen Sie die Zeichenfolge `:password` weg. Um mehrere Benutzer zu definieren, trennen Sie jeden Benutzereintrag mit einem Komma (,) und schließen Sie die gesamte Liste der Benutzer in Anführungszeichen (" ") ein.
`encryption`	Für die Client-Server-Datenübertragung verwendete Verschlüsselungsmethode: • Hoch • Keine **Hinweis** Die genaue Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-Server-Verbindung sind von mehreren Faktoren abhängig, u. a. von der Clientplattform und der Avamar-Serverversion. Im *Avamar – Produktsicherheitshandbuch* finden Sie nähere Informationen.
`encryption_override`	Optionale Außerkraftsetzung der Verschlüsselung. Falls `TRUE` eingestellt ist, verwendet dieser Client nicht die Gruppenverschlüsselungsmethode.

CSV-Format

Clientdefinitionsdateien im kommagetrennten CSV-Format verwenden die gleichen Element- und Attributnamen wie das XML-Format. Allerdings müssen Sie jeden Client in einer einzigen Zeile definieren und jeden Attributwert durch ein Komma trennen, wie im folgenden Beispiel gezeigt wird:

```
host_name,mcs_domain,mcs_group,dataset,retention_policy,
contact_address,contact_port,access_list,encryption,
encryption_override
```

Validieren und Importieren einer Clientdefinitionsdatei

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Account Management**.
3. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Import Clients from File** aus.

Das Dialogfeld **Validate** wird angezeigt.

4. Navigieren Sie zur gespeicherten Clientdefinitionsdatei und wählen Sie sie aus.
5. Klicken Sie auf **Validate**.

   Das Dialogfeld **Validation Results** wird angezeigt.
6. Falls die Clientdefinitionsdatei fehlerfrei ist, klicken Sie zum Importieren der Clientliste auf **Commit**. Falls die Clientdefinitionsdatei Fehler enthält, korrigieren Sie die Fehler, speichern Sie die Datei erneut und wiederholen Sie die Schritte dieses Verfahrens.

   Das Dialogfeld **Validation Results** wird geschlossen und die neuen Clients werden in der Baumstruktur **Account Management** angezeigt.

Aktivieren eines Clients

Die Clientaktivierung ist der Prozess, bei dem die CID (Client-ID) an den Client zurückgegeben wird, auf dem sie im Clientdateisystem in einer Datei gespeichert wird.

Bevor Sie beginnen

- Der Client muss im Netzwerk vorhanden sein.
- Die Avamar-Clientsoftware muss auf dem Client installiert sein und ausgeführt werden.
- Der Avamar-Server muss in der Lage sein, den bei der Registrierung des Clients verwendeten Hostnamen aufzulösen.

Zur Aktivierung eines Clients stehen zwei Möglichkeiten zur Verfügung:

- Starten Sie die Aktivierung beim Client. Im *Avamar Backup Clients – Benutzerhandbuch* wird diese Methode beschrieben.
- Bringen Sie den Client mithilfe von Avamar Administrator zur Aktivierung mit dem Server.

HINWEIS

HP-UX-, Linux- und Solaris-Clients können entweder während der Installation oder mithilfe von Avamar Administrator aktiviert werden. Es gibt keinen clientseitigen Befehl zum Starten der Clientaktivierung auf diesen Computerplattformen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Account Management**.

   In der Baumstruktur **Account Management** geben die Symbole für die Clients den Status an. Es wird ein x für deaktivierte Clients und ein Fragezeichen für nicht registrierte Clients angezeigt. Es gibt keine spezielle Symbolzuweisung für aktive Clients.
3. Wählen Sie den zu aktivierenden Client aus der Baumstruktur aus.
4. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Invite Client** aus.

   Eine Statusmeldung zeigt an, dass dem Client eine Einladung zur Aktivierung mit dem Server gesendet wurde.

5. Klicken Sie auf **OK**.

Erneutes Aktivieren eines Clients

Unter bestimmten Umständen, z. B. beim Ersetzen eines Clientcomputers, müssen Sie möglicherweise ein Clientkonto mit neu installierter Clientsoftware erneut aktivieren.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Clients**.
4. Wählen Sie den Client aus.
5. Wählen Sie aus dem Menü **Actions** den Befehl **Client** > **Edit Client** aus.

   Das Fenster **Edit Client** wird angezeigt.
6. Deaktivieren Sie die Auswahl von **Activated**.
7. Klicken Sie auf **OK**.

Weitere Erfordernisse

Befolgen Sie nach dem Deaktivieren des Clients die Anweisungen im Benutzerhandbuch für das spezifische Plug-in, um die Clientregistrierung abzuschließen. Bei diesem Verfahren wird der Client deaktiviert, sodass er wie unter Aktivieren eines Clients auf Seite 63 erläutert erneut aktiviert werden kann.

Clientauslagerung

Avamar-Clients sind entweder auslagerbar oder nicht. Wenn ein Client auslagerbar ist, können Sie Einstellungen angeben, um zu steuern, wie der MCS die Auslagerungseinstellungen für den Client festlegt. Es kann u. U. notwendig sein, dass Sie Workarounds für Einschränkungen, die in Umgebungen mit nicht auslagerbaren Clients bestehen, verwenden müssen.

Auslagerbare Clients

Durch auslagerbare Clients erhält der Avamar-Server eine Auslagerungsadresse und eine Portnummer, die die Leistung von On-Demand-Backups und Wiederherstellungen ermöglichen. Außerdem kann Avamar Administrator das Clientdateisystem bei Backups und Wiederherstellungen in Avamar Administrator durchsuchen.

Sie können eine der folgenden Clientauslagerungseinstellungen angeben, um zu steuern, wie der MCS die Auslagerungseinstellungen für einen Client festlegt:

- **Automatisch** – Bei der Standardeinstellung der automatischen Auslagerung versucht der MCS automatisch, die Auslagerungseinstellungen für den Client festzulegen. Wenn der MCS aktualisierte Auslagerungsinformationen vom Client erhält, aktualisiert er automatisch die Einstellungen.
- **Manuell** – Bei der manuellen Auslagerung geben Sie die IP-Adresse und die Datenportnummer für die Client-/MCS-Kommunikation an. Wenn Sie Network Address Translation (NAT) verwenden, sollten Sie die manuelle Auslagerung verwenden. Bei NAT ist der MCS wahrscheinlich nicht in der Lage, die richtigen Clientauslagerungseinstellungen automatisch festzulegen. Im manuellen Modus überschreibt der MCS nie die IP-Adress- und Portnummereinstellungen für den Client.

Sie können die automatische Auslagerung auch ohne Angabe einer IP-Adresse oder Datenportnummer für die Client-MCS-Kommunikation deaktivieren. Das Deaktivieren der automatischen Auslagerung kann hilfreich sein, um Clients, die für einen längeren Zeitraum nicht mit dem Netzwerk verbunden sind, zu unterstützen, wie es der Fall bei Laptops sein kann. Diese Clients müssen ihre eigenen On-Demand-Backups starten. Aus diesem Grund sollten Sie die Clientauslagerung wann immer möglich aktivieren.

Nicht auslagerbare Clients

Ein Client ist nicht auslagerbar, wenn der nicht auf dem Avamar-Server-Utility-Node oder auf einem Single-Node-Server ausgeführte Avamar Administrator-Server keine TCP/IP-Verbindung zum Port 28002 auf dem Avamar-Client herstellen kann.

Im Falle eines nicht auslagerbaren Clients
Ein Client kann in den folgenden Situationen nicht auslagerbar sein:

- Die Umgebung (einschließlich der Client) verfügt über Firewallregeln, die eingehende Verbindungen auf Port 28002 zum Client verhindern.
- Der Client befindet sich hinter einem Router, der keine Portweiterleitung für Verbindungen unterstützt, die vom Avamar-Server initiiert wurden. (Dieser Schritt ist die häufig anzutreffende Situation, denen zu aktivierende Managed Service Providers begegnen können, wenn sie Avamar ohne VPN bereitstellen.)
- Der Avamar Administrator-Server kann keine Verbindung zum Avamar-Client auf der Auslagerungsadresse herstellen, die vom Avamar Administrator-Server verwendet wird. Dies ist beispielsweise der Fall, wenn der Client mehrfach vernetzt ist und die Auslagerungsadresse, die vom Avamar Administrator-Server zum Herstellen einer Verbindung zum Client verwendet wird, keine Route zur Auslagerungsadresse besitzt.
- Die Umgebung erfordert Authentifizierung, um eine Host-zu-Host-Verbindung zum Port 28002 auf dem Client herzustellen, und der Avamar Administrator-Serverprozess kann das erforderliche Authentifizierungsprotokoll nicht unterstützen.
- Eine IPSec-Umgebung. In einer Windows-Umgebung empfehlen die Best Practices von Microsoft die Aktivierung von IPSec. Clients sind nicht in eine IPSec-Umgebung auslagerbar.

Der MCS sollte automatisch nicht auslagerbare Clients erkennen und die Einstellungen anpassen. In der Regel sind keine manuellen Änderungen im MCS notwendig. Sie können festlegen, ob ein Client auslagerbar oder nicht auslagerbar sein soll, indem Sie die Eigenschaften für den Client in der Registerkarte **Client** im Fenster **Policy** von Avamar Administrator anzeigen. Wenn **No** in der Spalte **Paging** für den Client angezeigt wird, dann kann der MCS keine Verbindung zum `avagent`-Prozess auf dem Client herstellen, wodurch der Client nicht auslagerbar wird.

Einschränkungen in Umgebungen mit nicht auslagerbaren Clients
Sie können Avamar Administrator zur Durchführung von Backups oder Wiederherstellungen verwenden oder Policies in Umgebungen mit nicht auslagerbaren Clients definieren. In einigen Fällen müssen Sie explizite Pfadnamen eingeben.

Die folgenden Einschränkungen gelten für nicht auslagerbare Clients:

- Wenn der MCS den Client nicht auf Port 28002 auslagern kann, kann Avamar mithilfe von Avamar Administrator keine Aktivierung des Clients ermöglichen.
- Sie können das Clientdateisystem durchsuchen, wenn Sie Datasets definieren oder zwecks Auswahl eines Ziels für die Wiederherstellung durchsuchen. Um diese Einschränkung zu umgehen, definieren Sie explizit das Backup-Dataset, ohne

einen Client zu durchsuchen. Geben Sie während einer Wiederherstellung explizit den Wiederherstellungszielpfad ein.

- Sie können durch Doppelklicken auf die Ansicht **Activities** keine Clientprotokolle anzeigen. Um diese Einschränkung zu umgehen, beziehen Sie die Protokolle vom Clientcomputer.
- Sie können den Client nicht auslagern, wenn ein Arbeitsauftrag vorliegt, für den der Client benötigt wird. In diesem Fall stellt der Client eine Verbindung zum MCS her und ruft ungefähr jede Minute das Vorhandensein eines Arbeitsauftrags ab. Wenn Sie mehrere Hundert nicht auslagerbare Clients oder mehr sichern, müssen Sie das Abrufintervall möglicherweise vergrößern. Das Standardabrufintervall beträgt 60 Sekunden. Wenn sich die Performance des MCS verschlechtert, erhöhen Sie das Abrufintervall, bis eine akzeptable Performance erreicht wird.

Bearbeiten von Clientauslagerungseinstellungen

Der MCS kann Clientauslagerungseinstellungen automatisch festlegen oder Sie können die Auslagerungseinstellungen für einen Client manuell angeben. Wenn Sie NAT verwenden, müssen Sie die Auslagerungseinstellungen möglicherweise manuell angeben.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Clients**.
4. Wählen Sie den Client aus.
5. Wählen Sie aus dem Menü **Actions** den Befehl **Client** > **Edit Client** aus.

   Das Fenster **Edit Client** wird angezeigt.
6. Klicken Sie auf die Registerkarte **Properties**.
7. Wählen Sie entweder den Auslagerungsmodus **Automatic** oder **Manual** aus.
8. Wenn Sie **Manual** ausgewählt haben, geben Sie die Clientinformationen für die Client-/MCS-Kommunikation an:
   - Wenn der MCS im automatischen Modus keinen Hostnamen für diesen Client automatisch festlegen kann, geben Sie im Feld **Address** eine gültig IP-Adresse (ohne NAT) für den Client ein.
   - Geben Sie im Feld **Port Number** die Datenportnummer an. Der Standarddatenport ist 28002.
9. Klicken Sie auf **OK**.

Bearbeiten von Clientinformationen

Sie können den Namen, die Kontaktdaten oder Standortinformationen für einen Client in Avamar Administrator bearbeiten.

In Avamar Administrator muss der Clientname immer dem Clienthostnamen entsprechen. Wann immer Sie den Clientnamen in Avamar Administrator ändern sollten, da sich der Clienthostname geändert hat, fahren Sie die Avamar-Software auf dem Client-Computer herunter. Ändern Sie den Clientnamen mithilfe dieses Verfahrens und starten Sie dann die Avamar-Clientsoftware. Nur mit dieser Aktion können Sie dafür sorgen, dass die Registrierung des Clients bei der Management

Console Server- (MCS-)Datenbank beibehalten wird, wodurch wiederum zurückliegende Backups weiterhin dem Client zugeordnet bleiben.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Account Management**.

   In der Baumstruktur **Account Management** geben die Symbole für die Clients den Status an. Es wird ein x für deaktivierte Clients und ein Fragezeichen für nicht registrierte Clients angezeigt. Es gibt keine spezielle Symbolzuweisung für aktive Clients.
3. Wählen Sie den zu bearbeitenden Client aus der Baumstruktur aus.
4. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Edit Client** aus.

   Das Dialogfeld **Edit Client** wird angezeigt.
5. Bearbeiten Sie den Namen, die Kontaktinformationen oder die Standortinformationen zum Client.
6. Klicken Sie auf **OK**.

   Es wird eine Bestätigungsmeldung angezeigt.
7. Klicken Sie auf **OK**.

Anzeigen von Clienteigenschaften

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Clients**.
4. Wählen Sie den Client aus.

   Die in der folgenden Tabelle beschriebenen Clienteigenschaften werden im Hauptbereich des Fensters angezeigt.

   Tabelle 15 Von Avamar Administrator angezeigte Clienteigenschaften

Spalte	Beschreibung
Client	Beschreibender Clientname.
Backups Disabled	Gibt an, ob Avamar Backups für den Client durchführen kann. Ungeachtet dieser Einstellung kann der Client Dateien wiederherstellen, solange im System ein vorheriges Backup vorhanden ist.
Aktiviert	Gibt an, ob der Client beim Avamar-Server aktiviert ist.
Domain	Die Avamar-Domain für den Client.

Tabelle 15 Von Avamar Administrator angezeigte Clienteigenschaften (Fortsetzung)

Spalte	Beschreibung
OS	Das Betriebssystem auf dem Client.
Paging	Gibt an, ob der Client dem Avamar-Server eine Seitenadresse und Portnummer bereitgestellt hat, sodass dieser On-Demand-Backups und -Wiederherstellungen durchführen kann. Außerdem können Sie mit Avamar Administrator dessen Dateisystem während von Avamar Administrator initiierter Backups und Wiederherstellungen durchsuchen.
Version	Die Version der Avamar-Clientsoftware auf dem Client.
Last Check-in	Datum und Uhrzeit, zu dem bzw. zu der der Avamar-Client-Agent zuletzt beim Avamar-Server eingecheckt war.
Encryption	Die für die Client-Server-Datenübertragung verwendete Verschlüsselungsmethode.
CID	Die Client-ID, eine eindeutige Kennung für diesen Client im Avamar-Server. CIDs werden während der Clientaktivierung zugewiesen.

Aktivieren und Deaktivieren eines Clients

Sie können einen Client deaktivieren, sodass er den Avamar-Server nicht zum Sichern von Dateien verwenden kann. Diese Aktion wird in der Regel durchgeführt, um das System in einen Zustand zu versetzen, der Wartungsaktivitäten unterstützt. Falls ein Client deaktiviert wurde, müssen Sie den Client erneut aktivieren, bevor Backups für den Client wieder aufgenommen werden können.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Clients**.
4. Wählen Sie den zu deaktivierenden bzw. zu aktivierenden Client aus.
5. Wählen Sie aus dem Menü **Actions** den Befehl **Client** > **Disable all backups of selected client** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
6. Klicken Sie auf **Yes**.

   Wenn der Client deaktiviert ist, wird im Menü **Actions** > **Client** neben der Option **Disable all backups of selected client** ein Häkchen angezeigt. Wenn der Client aktiviert ist, wird das Häkchen nicht angezeigt.

Verschieben eines Clients in eine neue Domain

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Account Management**.

   In der Baumstruktur **Account Management** geben die Symbole für die Clients den Status an. Es wird ein x für deaktivierte Clients und ein Fragezeichen für nicht registrierte Clients angezeigt. Es gibt keine spezielle Symbolzuweisung für aktive Clients.

3. Wählen Sie den zu verschiebenden Client aus der Baumstruktur aus.

4. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Move Client** aus.

   Das Dialogfeld **Move Client** wird angezeigt.

5. Wählen Sie die neue Domain für den Client aus.

6. Klicken Sie auf **OK**.

Stilllegen eines Clients

Wenn Sie einen Client stilllegen, führt Avamar keine weiteren Backups des Clients durch. Avamar verwendet die angegebene Aufbewahrungseinstellung für die vorhandenen Backups eines stillgelegten Clients, um zu bestimmen, wie lange die vorhandenen Backups aufbewahrt werden sollen. Avamar verwendet die angegebene Aufbewahrungseinstellung auch für vorhandene Replikate der Backups eines stillgelegten Clients, um zu bestimmen, wie lange die vorhandenen Replikate aufbewahrt werden sollen.

Verwenden Sie Avamar-Administrator, um Daten von vorhandenen Backups oder Replikaten eines stillgelegten Clients wiederherzustellen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Account Management**.

   In der Baumstruktur **Account Management** geben die Symbole für die Clients den Status an. Ein X wird für deaktivierte Clients und ein Fragezeichen für nicht registrierte Clients angezeigt. Es gibt keine spezielle Symbolzuweisung für aktive Clients.

3. Wählen Sie den stillzulegenden Client aus der Baumstruktur aus.

4. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Retire Client** aus.

   Das Dialogfeld **Retire Client** wird angezeigt.

5. Wählen Sie im Abschnitt **Lokale Backups** aus, wie lange Backups für den Client aufbewahrt werden sollen:

- Um Backups bis zu ihrem vorhandenen Ablaufdatum aufzubewahren, wählen Sie **Retain local backups with existing expiration date** aus.
- Um Backups ungeachtet des vorhandenen Ablaufdatums unbegrenzt aufzubewahren, wählen Sie **Retain all local backups indefinitely** aus.
- Um Backups bis zu einem neuen Ablaufdatum aufzubewahren, wählen Sie **Reset local backup expiration date** aus und wählen Sie unter **New Expiration Date** ein neues Ablaufdatum aus.

6. (Client mit Replikaten) Wählen Sie im Abschnitt **Remote Backups** aus, wie lange Replikate für den Client aufbewahrt werden sollen:
   - Um Replikate bis zu ihrem vorhandenen Ablaufdatum aufzubewahren, wählen Sie **Retain remote backups with existing expiration date** aus.
   - Um Replikate ungeachtet des vorhandenen Ablaufdatums unbegrenzt aufzubewahren, wählen Sie **Retain all remote backups indefinitely** aus.
   - Um Replikate bis zu einem neuen Ablaufdatum aufzubewahren, wählen Sie **Reset remote backup expiration date** aus und wählen Sie unter **New Expiration Date** ein neues Ablaufdatum aus.
7. Klicken Sie auf **OK**.

   Es wird eine Bestätigungsmeldung angezeigt.
8. Klicken Sie auf **Yes**.

Löschen eines Clients

Sie können einen Client und alle Backups des Clients löschen. Optional können Sie alle Replikate löschen, die auf Replikationszielsystemen vorhanden sind.

Wenn Sie einen Client löschen, löscht Avamar dauerhaft alle für diesen Client gespeicherten Backups. Sie sollten einen Client nur dann löschen, wenn Sie sicher sind, dass es keinen Anlass für die Aufbewahrung der Backups gibt. Legen Sie den Client im Zweifel stattdessen still.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Account Management**.

   In der Baumstruktur **Account Management** geben die Symbole für die Clients den Status an. Es wird ein X für deaktivierte Clients und ein Fragezeichen für nicht registrierte Clients angezeigt. Es gibt keine spezielle Symbolzuweisung für aktive Clients.
3. Wählen Sie den zu löschenden Client aus der Baumstruktur aus.
4. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Delete Client** aus.

   Das Dialogfeld **Client löschen** wird angezeigt. Es enthält die Anzahl der vorhandenen Backups für den Client.
5. (Clients mit Replikaten) Wählen Sie aus, wie mit den Replikaten des Clients verfahren werden soll:
   - Um alle Replikate für den Client zu löschen, wählen Sie **Also delete remote backups on external servers** aus.

- Um alle Replikate für den Client beizubehalten, deaktivieren Sie die Option **Also delete remote backups on external servers**.

6. Wählen Sie die Option **I understand this action is permanent and irreversible** aus.

   Bei diesem Feld handelt es sich um eine Sicherheitsmaßnahme um zu verhindern, dass ein Client und die Backups eines Clients unbeabsichtigt gelöscht werden.

7. Klicken Sie auf **Delete**.

KAPITEL 4

Benutzermanagement und -authentifizierung

In diesem Kapitel werden folgende Themen behandelt:

Übersicht über Avamar-Benutzerkonten

Ein Benutzerkonto in Avamar kann zur Verwaltung einer Domain oder eines Clients dienen. Das Benutzerkonto definiert das Authentifizierungssystem, mit dem Benutzern Zugriff auf den Avamar-Server gewährt wird. Es legt außerdem die Rolle und damit die zulässigen Vorgänge für den Benutzer fest.

Sie können Benutzerkonten zu Domains oder einzelnen Clients hinzufügen. Wenn Sie einer Domain ein Benutzerkonto hinzufügen, kann das Konto zur Administration dieser Domain sowie der dazugehörigen Subdomains dienen. Wenn Sie einem einzelnen Client ein Benutzerkonto hinzufügen, kann das Konto Backups und Wiederherstellungen dieses Clients durchführen und im System auf Backups zu diesem Client zugreifen.

In Avamar entsprechen Benutzer Einträgen in einer Domain- oder Clientzugriffsliste. Wenn Sie dem Avamar-System ein Benutzerkonto hinzufügen, fügen Sie einer Domain- oder Clientzugriffsliste einen Eintrag hinzu.

Im folgenden Beispiel wurde der Benutzer „Gretchen“ sowohl der Accounting-Domain als auch einem Computer hinzugefügt. Das Authentifizierungssystem und die Rolle sind jedoch vollkommen getrennte Benutzerkonten, die zufällig über den gleichen Benutzernamen verfügen.

Abbildung 9 Benutzer in Avamar-Domains

Die folgende Tabelle beschreibt die in einem Avamar-Benutzerkonto enthaltenen Informationen.

Tabelle 16 Informationen zu Avamar-Benutzerkonten

Information	Beschreibung
Benutzername	Der Benutzername hängt vom Authentifizierungssystem ab und muss ein vom Authentifizierungssystem akzeptiertes Format aufweisen. Beim internen Authentifizierungssystem muss z. B. bei den Benutzernamen die Groß- und Kleinschreibung beachtet werden, bei den Windows Active Directory-Benutzernamen jedoch nicht. Benutzernamen dürfen nicht mehr als 31 Zeichen umfassen.
Authentication system	Ein Authentifizierungssystem ist ein Benutzername-/Passwortsystem, das verwendet wird, um Benutzern Zugriff auf den Avamar-Server zu gewähren.

Tabelle 16 Informationen zu Avamar-Benutzerkonten (Fortsetzung)

Information	Beschreibung
Rolle	Rollen definieren die zulässigen Vorgänge für jedes Benutzerkonto.

Benutzerauthentifizierung

Ein Authentifizierungssystem ist ein Benutzername-/Passwortsystem, das verwendet wird, um Benutzern Zugriff auf den Avamar-Server zu gewähren.

Avamar unterstützt die folgenden Authentifizierungssysteme:

- Interne Avamar-Authentifizierung, wie in Interne Avamar-Authentifizierung auf Seite 76 beschrieben.
- Verzeichnisdienstauthentifizierung, beschrieben in Verzeichnisdienstauthentifizierung auf Seite 76.

Avamar unterstützt außerdem die veraltete Authentifizierungsmethode Enterprise Authentication. Ermöglichen der Abwärtskompatibilität mit Enterprise Authentication auf Seite 96 beschreibt, wie die Fortsetzung der Unterstützung für Enterprise Authentication aktiviert wird.

Authentifizierung von Benutzern und Zuweisung von Rollen durch Avamar

Um für Abwärtskompatibilität mit Enterprise Authentication zu sorgen und Benutzer in mehr als einer LDAP-zugewiesenen Gruppe zu ermöglichen, verwendet Avamar bei jedem Anmeldeversuch die folgende Authentifizierungs- und Rollenzuweisungsabfolge:

1. Wenn der Benutzername das Format *user* aufweist, wobei *user* ein Benutzername ohne den Anhang *@server* ist, prüft Avamar die interne Avamar-Authentifizierungsdatenbank.
   Falls Benutzername, Passwort und Domain übereinstimmen, ist die Anmeldung erfolgreich und Avamar weist dem Benutzer eine Rolle in der Avamar-Datenbank zu. Falls keine Übereinstimmung besteht, schlägt die Anmeldung fehl.
2. Wenn der Benutzername das Format *user@server* aufweist, wobei *user* für einen Benutzernamen und *server* für den vollständig qualifizierten Domainnamen des Authentifizierungsservers steht, prüft Avamar die Anmeldeinformationen mithilfe von Enterprise Authentication.
   Falls Benutzername, Passwort und Domain übereinstimmen, ist die Anmeldung erfolgreich und Avamar weist dem Benutzer eine Rolle in der Avamar-Datenbank zu. Falls keine Übereinstimmung besteht, wird die Evaluierung fortgeführt.
3. Wenn der Benutzername das Format *user@server* aufweist und die Authentifizierung über Enterprise Authentication fehlschlägt, prüft Avamar das LDAP-Zuordnungssystem.
   Der Anmeldeversuch wird in allen zugewiesenen Gruppen auf eine Übereinstimmung mit den folgenden Kennungen hin untersucht:
   - Benutzername, der Teil des Eintrags im Feld **User Name** vor dem @-Symbol
   - Passwort, das im Feld **Passwort** eingegeben wurde
   - Avamar-Domain, die in das Feld **Domain Name** eingegeben wurde.
   - Verzeichnisdienstdomain, der Teil des Eintrags im Feld **User Name** nach dem @-Symbol

Wenn alle Kennungen übereinstimmen, ist die Anmeldung erfolgreich und Avamar weist dem Benutzer eine Rolle aus der zugewiesenen Gruppe zu.

Ein Benutzer kann Mitglied zugewiesener Gruppen in verschiedenen Verzeichnisdienstdomains sein. Die Rolle der zugewiesenen Gruppe, die mit der während der Anmeldung angegebenen Verzeichnisdienstdomain übereinstimmt, wird dem Benutzer für diese Sitzung zugewiesen.

Wenn der Benutzer Mitglied von mehr als einer zugewiesenen Gruppe in der gleichen Verzeichnisdienstdomain ist, wird die Rolle mit der größten Autorität zugewiesen.

4. Wenn die Anmeldeinformationen nicht den Anforderungen eines der vorherigen Schritte entsprechen, schlägt die Anmeldung fehl und eine Fehlermeldung wird angezeigt.

Interne Avamar-Authentifizierung

Mit der internen Avamar-Authentifizierung können Sie den Benutzernamen und das Passwort für Avamar-Benutzerkonten definieren und Avamar speichert die Informationen. Bei den Benutzernamen, die nicht länger als 31 Zeichen sein dürfen, muss die Groß- und Kleinschreibung beachtet werden.

Für die Verwendung der internen Avamar-Authentifizierung zur Authentifizierung von Benutzerkonten sind keine zusätzlichen Schritte erforderlich. Legen Sie den Benutzernamen und das Passwort für jedes Konto fest, wenn Sie den Benutzer in Avamar Administrator hinzufügen.

Verzeichnisdienstauthentifizierung

Verwenden Sie die Verzeichnisdienstauthentifizierung, um sich mithilfe von Informationen von einem vorhandenen Verzeichnisdienst zu authentifizieren und Avamar-Benutzern Rollen zuzuweisen. Die Verzeichnisdienstauthentifizierung arbeitet mit LDAP-konformen Verzeichnisdiensten und bietet weitere Funktionen, wenn sie mit einem OpenLDAP-Verzeichnisdienst verwendet wird. Die Verzeichnisdienstauthentifizierung arbeitet auch mit einem Netzwerkinformationsdienst (Network Information Service, NIS) zusammen, eigenständig oder mit einem unterstützten LDAP-Verzeichnisdienst.

Avamar-Produkte mit Verzeichnisdienstauthentifizierung
Die folgenden Avamar-Produkte können die Verzeichnisdienstauthentifizierung zur Authentifizierung und Autorisierung von Benutzern verwenden:

- Avamar Administrator
- Avamar Web Restore
- Webbenutzeroberfläche des Avamar-Clients (Avamar Desktop/Laptop)

Avamar-Produkt, das Verzeichnisdienst-Clientdatensätze verwendet
Avamar Client Manager verwendet keine Verzeichnisdienstauthentifizierung zur Authentifizierung und Autorisierung von Benutzeranmeldungen. Avamar Client Manager kann jedoch den Verzeichnisdienstmechanismus verwenden, um Informationen über Computer abzurufen, die potenzielle Avamar-Clients sind. Avamar Client Manager richtet eine Abfrage an den Verzeichnisdienst, um Informationen über Clients und, falls verfügbar, Organisationseinheiten des Verzeichnisdiensts wie Verzeichnisdomains und Verzeichnisgruppen abzurufen.

Verzeichnisdiensttypen

Die Verzeichnisdienstauthentifizierung unterstützt die folgenden Typen von Verzeichnisdiensten:

Tabelle 17 Unterstützte Verzeichnisdiensttypen

Typ	Unterstützte Implementierungen
LDAP	• Active Directory für Windows Server 2003 • Active Directory Domain Services für Windows Server 2008 • Active Directory Domain Services für Windows Server 2012 • Active Directory Domain Services für Windows Server 2016 • 389 Directory Server, Version 1.1.35
OpenLDAP	SUSE OpenLDAP, Version 2.4
NIS	Network Information Service (Netzwerkinformationsdienst)

Avamar unterstützt die verschlüsselte LDAP- und OpenLDAP-Verzeichnisdienstauthentifizierung über SSL/TLS. Standardmäßig verwendet Avamar TLS 1.2, wenn vom LDAP- oder OpenLDAP-Server unterstützt. Andernfalls greift Avamar auf eine unterstützte Version von SSL/TLS zurück. Der Avamar-Server bietet jedoch kein SSL-/TLS Zertifikat für LDAP- oder OpenLDAP-Server für die Clientauthentifizierung.

LDAP-Zuordnungen

Die Verzeichnisdienstauthentifizierung nutzt LDAP-Zuordnungen, um mithilfe von Informationen von einem Verzeichnisdienst eine Gruppe von Avamar-Domainbenutzern zu bilden. Verknüpfen Sie Avamar-Autorisierungsstufen mit zugeordneten Verzeichnisdienst-Benutzerkonten, um LDAP-Zuordnungen zu erstellen. Weitere Informationen finden Sie im Abschnitt „Hinzufügen einer LDAP-Zuordnung“.

HINWEIS

Durch das Löschen einer Avamar-Domain werden die LDAP-Zuordnungen entfernt, die diese Avamar-Domain für den Zugriff nutzen. Das Entfernen von LDAP-Zuordnungen wirkt sich jedoch nicht auf die Verzeichnisdienstgruppen oder die Verzeichnisdienst-Benutzerdatensätze aus, die mit den entfernten Zuordnungen verknüpft sind.

LDAP-Verzeichnisdienstauthentifizierung

Avamar ermöglicht die Authentifizierung und Autorisierung von Avamar-Benutzern über unterstützte OpenLDAP-Verzeichnisdienste.

Vorbereitung auf die Verwendung der LDAP-Verzeichnisdienstauthentifizierung auf Seite 78 beschreibt, wie die Implementierung der LDAP-Verzeichnisdienstauthentifizierung vorbereitet wird.

Hinzufügen von Informationen für einen unterstützten LDAP-Verzeichnisdienst auf Seite 79 beschreibt, wie die erforderlichen Informationen über den LDAP-Verzeichnisdienst für das Avamar-System zur Verfügung gestellt werden.

Bearbeiten der Verzeichnisdienst-Konfigurationsdateien auf Seite 82 beschreibt, wie eine optionale manuelle Bearbeitung der Dateien `ldap.properties` und `krb5.conf` durchgeführt wird.

Anforderungen

Die Avamar-Verzeichnisdienstauthentifizierung unterstützt die Verwendung von LDAP-Verzeichnisdiensten, die folgende Bedingungen erfüllen:

- Der LDAP-Server lässt die Benutzernamenbindung über die folgenden beiden Formate zu:
  - *username*
  - *username@domain.com*
- Der LDAP-Server gestattet die Suche nach der Gruppenmitgliedschaft mithilfe eines Benutzernamens.
- Der LDAP-Server gestattet die Suche nach Gruppen mithilfe einer Suchzeichenfolge.
- Das LDAP-Serverkonto, das beim Hinzufügen einer LDAP-Zuordnung angegeben wird, verfügt über die Berechtigung zum Ausführen eines verschachtelten `ldapsearch`-Befehls.

Kerberos-Protokoll

Bei der LDAP-Verzeichnisdienstauthentifizierung von Avamar wird normalerweise das Kerberos-Protokoll für sämtliche Kommunikation mit dem Key Distribution Center eingesetzt. Avamar verschlüsselt Benutzernamen und Passwörter automatisch, bevor sie an Port 88 des Key Distribution Center gesendet werden.

Um die LDAP-Verzeichnisdienstauthentifizierung von Avamar ohne Kerberos-Protokoll in einer einfachen Bindung zu verwenden, bearbeiten Sie die Datei `ldap.properties` manuell.

Vorbereitung auf die Verwendung der LDAP-Verzeichnisdienstauthentifizierung

Um die Verwendung der LDAP-Verzeichnisdienstauthentifizierung vorzubereiten, geben Sie Avamar Zugriff auf bestimmte Ports auf dem Key Distribution Center. Erstellen Sie außerdem Verzeichnisdienstgruppen, die mit Avamar-LDAP-Zuordnungen verbunden sind.

Vorgehensweise

1. Achten Sie darauf, dass Avamar Zugriff auf die folgenden erkannten Ports auf dem Key Distribution Center (KDC) hat.

Tabelle 18 Erforderliche Schlüsselverteilungscenter-Ports

Portnummer	Beschreibung
88	Kerberos-Authentifizierungssystem
389	Lightweight Directory Access Protocol (LDAP)
464	Kerberos-Passwort ändern/festlegen
636	LDAP über SSL/TLS

Die Ports sind in den Dateien `krb5.conf` und `ldap.properties` definiert. Unter Bearbeiten der Verzeichnisdienst-Konfigurationsdateien auf Seite 82 finden Sie Anweisungen zum Bearbeiten dieser Dateien.

2. Erstellen Sie Verzeichnisdienstgruppen im Verzeichnisdienst (nicht in Avamar).

   Die Größe von Gruppen kann zwischen einem Mitglied und der je nach Verzeichnisdienst zulässigen maximalen Mitgliederanzahl variieren.

   Idealerweise sollten Sie Verzeichnisdienstgruppen speziell zur Verwendung mit einer Avamar-LDAP-Zuordnung erstellen. Mit dedizierten Verzeichnisdienstgruppen wird die Gruppenzusammensetzung im Kontext des gewährten Grads an Avamar-Zugriff gesehen. Außerdem kann der Gruppenname ein gängiges Zeichenmuster enthalten, um die Erkennung während der Zuordnung zu erleichtern. Beispielsweise kann jeder Gruppenname mit den Zeichen `av` beginnen, wie in `avAdministrators`. Sie können dann mithilfe der Platzhaltersuchzeichenfolge `av*` nach allen mit Avamar verbundenen Gruppen suchen.

3. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Wenn Sie sich bei einem Multi-Node-Server anmelden, melden Sie sich als Administrator beim Utility-Node an.
4. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie **`su -`** eingeben.
5. Sichern Sie den Keystore, indem Sie den folgenden Befehl in eine Zeile eingeben:

   ```
   cp -p /usr/local/avamar/lib/rmi_ssl_keystore /usr/local/
   avamar/lib/rmi_ssl_keystore.bak
   ```

6. Importieren Sie das LDAP-Serverzertifikat in den Keystore, indem Sie den folgenden Befehl in eine Zeile eingeben:

   ```
   keytool -importcert -file <certfile>.crt -keystore /usr/local/
   avamar/lib/rmi_ssl_keystore -storepass changeme
   ```

   wobei *< certfile>* der Name des LDAP-Serverzertifikats einschließlich Pfad ist.

7. Starten Sie den MCS neu, indem Sie den folgenden Befehle eingeben:

   ```
   mcserver.sh --restart
   ```

Weitere Erfordernisse

Konfigurieren Sie Avamar für die Verwendung des LDAP-Verzeichnisdiensts. Anweisungen finden Sie unter Hinzufügen von Informationen für einen unterstützten LDAP-Verzeichnisdienst auf Seite 79.

Hinzufügen von Informationen für einen unterstützten LDAP-Verzeichnisdienst

Mithilfe eines Assistenten fügen Sie Informationen für einen unterstützten LDAP-Verzeichnisdienst für die Authentifizierung und Autorisierung von Avamar-Benutzern hinzu.

Bevor Sie beginnen

Überprüfen Sie, ob der Verzeichnisdienst die folgenden Anforderungen erfüllt:

- Die Authentifizierung erfolgt über eine SASL-Bindung (Simple Authentication and Security Layer), die Kerberos nutzt.
- Es werden nur die LDAP v.3-Basisfunktionen verwendet.

- Die Benutzernamenbindung ist über die folgenden beiden Formate zulässig:
  - *username*
  - *username@domain.com*
- Die Suche nach der Gruppenmitgliedschaft kann anhand eines Benutzernamens durchgeführt werden.
- Die Suche nach Gruppen kann anhand einer Suchzeichenfolge durchgeführt werden.
- Er hat ein verfügbares LDAP-Serverkonto, das zur Ausführung eines verschachtelten `ldapsearch`-Befehls berechtigt ist.

HINWEIS

Verwenden Sie den Assistenten nicht, um einen Verzeichnisdienst hinzuzufügen, der die Authentifizierung über eine einfache Bindung (nur Text) durchführt. Bearbeiten Sie stattdessen die Datei `ldap.properties` manuell, wie in Bearbeiten der Verzeichnisdienst-Konfigurationsdateien auf Seite 82 beschrieben.

Vorgehensweise

1. Melden Sie sich in Avamar Administrator als Administrator bei der Root-Domain an.
   a. Starten Sie Avamar Administrator.
   b. Geben Sie unter **Server** die IP-Adresse oder den DNS-Namen des Avamar-Servers ein, bei dem Sie sich anmelden möchten.
   c. Geben Sie unter **User Name** einen Benutzernamen ein.

      Der Benutzername muss für ein Konto gelten, dem auf Root-Domain-Ebene die Administratorrolle zugewiesen ist.

      Wenn Avamar bereits für die Verwendung eines Verzeichnisdiensts konfiguriert ist, können Sie sich alternativ mit einem LDAP-Konto mit Administratorberechtigungen auf Root-Domainebene anmelden. Verwenden Sie das folgende Format: ***username@ldap-domain***.

   d. Geben Sie unter **Password** das Passwort für das Benutzerkonto ein.
   e. Verwenden Sie unter **Domain Name** die Standardeingabe, einen Schrägstrich (`/`), um die Root-Domain festzulegen.
   f. Klicken Sie auf **Log In**.

      Wenn dies das erste Mal ist, das Sie eine Verbindung mit diesem Avamar-Server hergestellt haben, wird die das Dialogfeld **Accept Server Certificate** geöffnet. Überprüfen Sie die Details des Serverzertifikats und klicken Sie auf **Yes**.

      Das Avamar-Administrator-Dashboard wird angezeigt.
2. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
3. Klicken Sie auf die Registerkarte **LDAP Management**.
4. Klicken Sie auf **Directory Service Management**.

   Das Dialogfeld **Directory Service Management** wird angezeigt.

5. Fügen Sie den Verzeichnisdienst hinzu:
   a. Klicken Sie auf **Add**.

      Daraufhin wird der Abschnitt **Adding a new Directory Service** angezeigt.

   b. Wählen Sie **LDAP** aus.

   c. Geben Sie unter **Enter a fully qualified domain name** den vollständig qualifizierten Domainnamen (Fully Qualified Domain Name, FQDN) eines Verzeichnisservers ein.

   d. (Optional) Wenn der Verzeichnisserver die standardmäßige Verzeichnisdienstdomain der Organisation darstellt, dann wählen Sie **Diese Domain als LDAP-Standarddomain festlegen** aus.

      Damit über die Webbenutzeroberfläche des Avamar-Clients Benutzer von Macintosh-Computern authentifiziert werden können, muss der den Macintosh-Benutzern zugewiesene LDAP-Server als Standardserver konfiguriert werden.

   e. Klicken Sie auf **Add**.

      Es wird eine Bestätigungsmeldung angezeigt.

   f. Klicken Sie auf **Yes**.

      Daraufhin wird eine Erfolgsmeldung angezeigt. Wenn stattdessen eine Fehlermeldung angezeigt wird, beheben Sie das Problem und fügen Sie den Verzeichnisdienst erneut hinzu. Fehlermeldungen während der Verzeichnisdienstkonfiguration auf Seite 92 enthält weitere Einzelheiten.

   g. Klicken Sie auf **OK**.

      Die Änderungen werden auf den MMC-Dienst (Management Console Server) (`mcs`) und den EM Tomcat-Dienst (`emt`) angewendet.

6. (Optional) Wiederholen Sie den vorherigen Schritt, um weitere Authentifizierungsdomains hinzuzufügen.
7. Prüfen Sie die Verzeichnisdiensteinträge:
   a. Wählen Sie im Dialogfeld **Directory Service Management** einen der Einträge aus der Liste **Configured Directory Services** aus.

      Der Abschnitt **Testing** wird angezeigt.

   b. Geben Sie im Feld **Username** den Benutzernamen für ein Konto ein, das über eine Leseberechtigung für die Datenbank des Verzeichnisdiensts verfügt.

   c. Geben Sie unter **Passwort** das Passwort für den Benutzernamen ein.

   d. Klicken Sie auf **Run Test**.

      Sollte eine Fehlermeldung angezeigt werden, beheben Sie das Problem. Fehlermeldungen während der Verzeichnisdienstkonfiguration auf Seite 92 enthält weitere Einzelheiten.

   e. Klicken Sie auf **Close**, um den Abschnitt **Testing** zu schließen.
8. Klicken Sie im Dialogfeld **Directory Service Management** auf **Close**.

Weitere Erfordernisse

Erstellen Sie eine LDAP-Zuordnung, um der Verzeichnisdienstgruppe Avamar-Benutzerinformationen zuzuweisen. Anweisungen finden Sie unter Hinzufügen einer LDAP-Zuordnung auf Seite 93.

Bearbeiten der Verzeichnisdienst-Konfigurationsdateien

Das LDAP-Managementtool ermöglicht es, die Verzeichnisdienst-Konfigurationsdateien `ldap.properties` und `krb5.conf` manuell zu bearbeiten. Bearbeiten Sie diese Dateien manuell, um nicht standardmäßige Einstellungen zu konfigurieren und Probleme zu beheben, die auftreten, wenn Avamar zur Verwendung eines Verzeichnisdiensts konfiguriert wird.

Bevor Sie beginnen

Ermitteln Sie das korrekte Format für Schlüssel und Werte in den Konfigurationsdateien.

Vorgehensweise

1. Melden Sie sich in Avamar Administrator als Administrator bei der Root-Domain an.
   a. Starten Sie Avamar Administrator.
   b. Geben Sie unter **Server** die IP-Adresse oder den DNS-Namen des Avamar-Servers ein, bei dem Sie sich anmelden möchten.
   c. Geben Sie unter **User Name** einen Benutzernamen ein.

      Der Benutzername muss für ein Konto gelten, dem auf Root-Domain-Ebene die Administratorrolle zugewiesen ist.

      Wenn Avamar bereits für die Verwendung eines Verzeichnisdiensts konfiguriert ist, können Sie sich alternativ mit einem LDAP-Konto mit Administratorberechtigungen auf Root-Domainebene anmelden. Verwenden Sie das folgende Format: ***username*@*ldap-domain***.
   d. Geben Sie unter **Password** das Passwort für das Benutzerkonto ein.
   e. Verwenden Sie unter **Domain Name** die Standardeingabe, einen Schrägstrich (`/`), um die Root-Domain festzulegen.
   f. Klicken Sie auf **Log In**.

      Wenn dies das erste Mal ist, das Sie eine Verbindung mit diesem Avamar-Server hergestellt haben, wird die das Dialogfeld **Accept Server Certificate** geöffnet. Überprüfen Sie die Details des Serverzertifikats und klicken Sie auf **Yes**.

      Das Avamar-Administrator-Dashboard wird angezeigt.
2. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
3. Klicken Sie auf die Registerkarte **LDAP Management**.
4. Klicken Sie auf **Edit LDAP file**, um `ldap.properties` zu bearbeiten, bzw. auf **Edit KRB5 file**, um `krb5.conf` zu bearbeiten.
5. Geben Sie zusätzliche Informationen und Änderungen direkt im Fenster **Edit file** ein.
6. Klicken Sie auf **Save** und klicken Sie dann auf **Close**.

Formatanforderungen und Einstellungen für LDAP-Basisfunktionen

Das LDAP-Managementtool in Avamar Administrator erstellt eine ordnungsgemäß formatierte `ldap.properties`-Datei für LDAP-Verzeichnisdienste. Wenn Sie die

Datei manuell mit dem LDAP-Managementtool bearbeiten, muss das Format bestimmte Parameteranforderungen erfüllen. Sie können `ldap.properties` manuell andere Einstellungen hinzufügen, um die Authentifizierungsanforderungen eines Unternehmens zu erfüllen.

Anforderungen an Parameter für die LDAP-Basisfunktionen
Die folgende Tabelle enthält die Parameteranforderungen für die LDAP-Basisfunktionen.

Tabelle 19 Parameteranforderungen für LDAP-Basisfunktionen

Regel	Beschreibung	Format

Ein LDAP-URL-Parameter für jeden LDAP-Server	Der LDAP-URL-Parameter ordnet einen LDAP-Server einem bestimmten Domaincontroller zu.	`ldap.url.`*`ds.example.abc.com`*`=ldap:`
		`//dchost.r1.example.abc.com:389`
		oder
		`ldap.url.`*`ds.example.abc.com`*`=ldaps:`
		`//dchost.r1.example.abc.com:636`
		• *ds.example.abc.com* steht für den vollständig qualifizierten Domainnamen des LDAP-Servers.
		• *dchost.example.abc.com* steht für den vollständig qualifizierten Domainnamen des Domaincontroller für den LDAP-Server.
		• *389* ist der vom LDAP-Dienst verwendete Port.
		• *636* ist der vom LDAP-Dienst verwendete Port bei Verschlüsselung mit SSL/TLS.

Genau ein Standardserverparameter	Der Standardserverparameter wird während der Authentifizierung von Benutzern an Clients verwendet, die keiner spezifischen Domain zugeordnet sind. Beispiel: Lokale Benutzer und Benutzer, die sich über einen AIX-, FreeBSD-, HP-UX-, Linux-, SCO- oder Solaris-Computer anmelden.	`ldap.qualified-name-default=`*`dshost.example.abc.com`*. Dabei steht *dshost.example.abc.com* für den vollständig qualifizierten Domainnamen des standardmäßigen LDAP-Servers.

Zusätzliche Parameter
Mit dem LDAP-Managementtool in Avamar Administrator können Sie weitere Parameter zu `ldap.properties` hinzufügen. In der folgenden Tabelle sind die verfügbaren Einstellungen aufgeführt.

Tabelle 20 Weitere Parameter für LDAP-Basisfunktionen

Parameter	Beschreibung und Werte
`ldap.auth.domain.`*`login-domain-suffix`*	Legt ein Namenssuffix für die Anmeldedomain fest, das als Teil des Benutzernamenwerts bei einer LDAP-Authentifizierung enthalten ist. Dabei steht *login-domain-suffix* für das Anmeldedomain-Namenssuffix; der Wert ist eine Authentifizierungsdomain. Beispielsweise können sich

Tabelle 20 Weitere Parameter für LDAP-Basisfunktionen (Fortsetzung)

Parameter	Beschreibung und Werte
	Benutzer mit einem der beiden folgenden Formate anmelden: „username@boston“ oder „username@boston.edu“, wobei dieser Parameter wie folgt festgelegt wird: `ldap.auth.domain.boston=boston.edu` Verwenden Sie diesen Parameter zusammen mit dem nächsten Parameter, `ldap.query.domain`, um mehrere Authentifizierungsdomains einem einzigen Anmeldedomain-Namenssuffix zuzuordnen.

`ldap.query.domain.`*`log-in-domain-suffix`*	Ordnet zusätzliche Authentifizierungsdomains einem einzigen Anmeldedomainsuffix zu. Dabei definiert der Parameter „ldap.auth.domain“ *`login-domain-suffix`* und die Werte „ldap.query.domain“ sind zusätzliche Authentifizierungsdomains innerhalb des Intranets des Unternehmens. Beispielsweise können sich Benutzer aus jeder Authentifizierungsdomain mit dem Format „username@boston“ anmelden, wobei die beiden Parameter wie folgt festgelegt werden:
	`ldap.auth.domain.boston=boston.edu`
	`ldap.query.domain.boston=science.boston.edu,art.boston.edu`

`ldap.entry.lookup.type.`*`ldap-domain`*	Definiert die Methode, die der LDAP-Server bei der Suche nach einem Benutzernamen verwendet, wobei *`ldap-domain`* die Authentifizierungsdomain ist. Die möglichen Werte sind: • `UN` für Benutzername – die Methode, die häufig von LDAP-Verzeichnisdiensten verwendet wird. (Standard) • `DN` für Distinguished Name – die Methode, die häufig von OpenLDAP-Verzeichnisdiensten verwendet wird.
`user-login-module`	Steuert den Authentifizierungsmechanismus. Die folgenden Werte sind verfügbar: • `kerberos` – LDAP-Authentifizierung mit Kerberos-Verschlüsselung. Dieser Wert ist der Standardwert. • `ldap` – LDAP-Authentifizierung im Klartext. Dieser Parameter benötigt auch den Parameter `ldap.auth.force.username.input=true`, um die Benutzeranmeldung auch auf einem Windows-Domaincomputer zu erzwingen. • `avamar` – Avamar-Authentifizierung. • `mix` – Sowohl `kerberos` als auch `avamar`.
`ldap.auth.force.username.input`	Steuert, ob Avamar eine Benutzeranmeldung über einen Anmeldebildschirm in Webanwendungen benötigt, die die

Tabelle 20 Weitere Parameter für LDAP-Basisfunktionen (Fortsetzung)

Parameter	Beschreibung und Werte
	Kerberos-Pass-Through-Authentifizierung zulassen. Die möglichen Werte sind: • `False` – Anmeldung ist nicht erforderlich. Dieser Wert ist der Standardwert. • `True` – Anmeldung ist erforderlich. Benötigt für den folgenden Parameter: `user-login-module=ldap`.
`avamar-authentication-domains`	Benötigt vom folgenden Parameter: `user-login-module=mix`. Bei dem Wert handelt es sich um eine kommagetrennte Liste von Domains. Avamar-Authentifizierung wird für Benutzer aus allen aufgelisteten Domains angewendet. LDAP-Authentifizierung wird für alle anderen Benutzer angewendet.
`support-nis-authentication`	Aktiviert (`true`) oder deaktiviert (`false`) die Unterstützung für die NIS-Authentifizierung. Der Standardwert ist `false`.
`nis.qualified-name-default`	Legt den vollständig qualifizierten Domainnamen des NIS-Domainservers fest.
`nis.url.`*`nisdomainname`*	Legt die IP-Adresse des NIS-Domainservers fest. Dabei steht *`nisdomainname`* für den Wert `nis.qualified-name-default`.

OpenLDAP-Verzeichnisdienstauthentifizierung

Avamar unterstützt die Authentifizierung und Autorisierung von Avamar-Benutzern über einen OpenLDAP-Verzeichnisdienst.

Das Hinzufügen von Informationen über einen OpenLDAP-Verzeichnisdienst zu Avamar wird unter Hinzufügen eines OpenLDAP-Verzeichnisdiensts auf Seite 85 beschrieben.

Die Konfiguration von Avamar zur Verwendung eines OpenLDAP-Verzeichnisdiensts für die Authentifizierung schließt die Möglichkeit ein, optionale Parameter zu verwenden, die es für OpenLDAP gibt. OpenLDAP-Verzeichnisdienstparameter auf Seite 89 beschreibt die erforderlichen und optionalen Parameter für OpenLDAP.

Hinzufügen eines OpenLDAP-Verzeichnisdiensts

Bearbeiten Sie die Datei `ldap.properties`, um ein Avamar-System so zu konfigurieren, dass ein OpenLDAP-Verzeichnisdienst für die Authentifizierung verwendet wird.

Fügen Sie einen OpenLDAP-Verzeichnisdienst hinzu, indem Sie die Datei `ldap.properties` des Avamar-Servers manuell bearbeiten und die erforderlichen Parameter hinzufügen. Optionale Parameter können ebenfalls hinzugefügt werden, um zu steuern, wie das Avamar-System mit dem OpenLDAP-Verzeichnisdienst interagiert. OpenLDAP-Verzeichnisdienstparameter auf Seite 89 bietet weitere Informationen über die erforderlichen und optionalen Parameter.

Vorgehensweise

1. Melden Sie sich in Avamar Administrator als Administrator bei der Root-Domain an.

a. Starten Sie Avamar Administrator.

b. Geben Sie unter **Server** die IP-Adresse oder den DNS-Namen des Avamar-Servers ein, bei dem Sie sich anmelden möchten.

c. Geben Sie unter **User Name** einen Benutzernamen ein.

Der Benutzername muss für ein Konto gelten, dem auf Root-Domain-Ebene die Administratorrolle zugewiesen ist.

Wenn Avamar bereits für die Verwendung eines Verzeichnisdiensts konfiguriert ist, können Sie sich alternativ mit einem LDAP-Konto mit Administratorberechtigungen auf Root-Domainebene anmelden. Verwenden Sie das folgende Format: ***username*@*ldap-domain***.

d. Geben Sie unter **Password** das Passwort für das Benutzerkonto ein.

e. Verwenden Sie unter **Domain Name** die Standardeingabe, einen Schrägstrich (`/`), um die Root-Domain festzulegen.

f. Klicken Sie auf **Log In**.

Wenn dies das erste Mal ist, das Sie eine Verbindung mit diesem Avamar-Server hergestellt haben, wird die das Dialogfeld **Accept Server Certificate** geöffnet. Überprüfen Sie die Details des Serverzertifikats und klicken Sie auf **Yes**.

Das Avamar-Administrator-Dashboard wird angezeigt.

2. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

Das Fenster **Administration** wird angezeigt.

3. Klicken Sie auf die Registerkarte **LDAP Management**.

4. Klicken Sie auf **Edit LDAP file**, um die Datei `ldap.properties` zu bearbeiten.

Das Dialogfeld **ldap.properties-Datei bearbeiten** wird angezeigt.

5. Geben Sie im Texteingabebereich Folgendes in eine neue Zeile ein:

`ldap.entry.lookup.type.`*`ldap-domain`*`=DN`
Dabei ist *ldap-domain* der Domainname des OpenLDAP-Servers.

Dieser Parameter ist erforderlich.

6. Geben Sie im Texteingabebereich Folgendes in eine neue Zeile ein:

`ldap.userdn.`*`ldap-domain=rdn-values`*

Hierbei gilt:

- *ldap-domain* ist der Domainname des OpenLDAP-Servers.
- *rdn-values* ist eine durch Semikola getrennte Liste der relativen Basis-DN (Distinguished Names) für Benutzer, vom Root-DN (Distinguished Name) der LDAP-Struktur.

  Bei jedem Eintrag in der Liste handelt es sich um eine kommagetrennte, umgekehrt hierarchische Darstellung der relativen Basis-DNs (Distinguished Names) einer Benutzergruppe.

Dieser Parameter ist erforderlich, es sei denn, die Benutzer befinden sich direkt unter dem Root-DN (Distinguished Name) oder der LDAP-Server lässt anonyme Suchvorgänge zu.

Beispiel: Wenn die Benutzer für die Domain `example.com` in `Users`, in `Employees`, in `People` und in `Admins` am Stamm der Struktur zu finden sind, geben Sie Folgendes ein:

`ldap.userdn.example.com=ou=Users,ou=Employees,ou=People;ou=Admins`

7. Geben Sie im Texteingabebereich Folgendes in eine neue Zeile ein:

   `ldap.rootdn.`*`ldap-domain=rootdn-format`*
   Hierbei gilt:

   - *ldap-domain* ist der Domainname des OpenLDAP-Servers.
   - *rootdn-format* ist das vom LDAP-Server verwendete Format des Root-DNs (Distinguished Name).

   Dieser Parameter ist erforderlich, es sei denn, der LDAP-Server verwendet das folgende Format für den Root-DN (Distinguished Name): **`dc=`*`domain-segment`*`,dc=`*`domain-segment`***

   Beispielsweise ist auf einem LDAP-Server, der den Root-DN (Distinguished Name) als `dc=example, dc=com` speichert, dieser Parameter in der Datei `ldap.properties` nicht erforderlich.

   Ein LDAP-Server, der den Root-DN (Distinguished Name) als `u=example, o=com` speichert, benötigt jedoch den folgenden Parameter in der Datei `ldap.properties`: **`ldap.rootdn.exaple.com=u=example,o=com`**

8. Fügen Sie im Texteingabebereich optionale OpenLDAP-Parameter hinzu.

   Geben Sie jeden Parameter in einer neuen Zeile ein.

9. Klicken Sie auf **Save**.
10. Prüfen Sie die Verzeichnisdiensteinträge:

    a. Wählen Sie im Dialogfeld **Directory Service Management** einen der Einträge aus der Liste **Configured Directory Services** aus.

    Der Abschnitt **Testing** wird angezeigt.

    b. Geben Sie im Feld **Username** den Benutzernamen für ein Konto ein, das über eine Leseberechtigung für die Datenbank des Verzeichnisdiensts verfügt.

    c. Geben Sie unter **Passwort** das Passwort für den Benutzernamen ein.

    d. Klicken Sie auf **Run Test**.

    Sollte eine Fehlermeldung angezeigt werden, beheben Sie das Problem. Fehlermeldungen während der Verzeichnisdienstkonfiguration auf Seite 92 enthält weitere Einzelheiten.

    e. Klicken Sie auf **Close**, um den Abschnitt **Testing** zu schließen.

11. Klicken Sie im Dialogfeld **Directory Service Management** auf **Close**.

Ergebnisse

Das Avamar-System unterstützt die Authentifizierung über den OpenLDAP-Verzeichnisdienst.

Weitere Erfordernisse

Erstellen Sie eine LDAP-Zuordnung, um der Verzeichnisdienstgruppe Avamar-Benutzerinformationen zuzuweisen. Anweisungen finden Sie unter Hinzufügen einer LDAP-Zuordnung auf Seite 93.

Aktivieren der OpenLDAP- und der Avamar-Authentifizierung

Bearbeiten Sie die Datei `ldap.properties`, um ein Avamar-System für die Verwendung der Avamar-Authentifizierung und der OpenLDAP-Authentifizierung zu konfigurieren.

Bevor Sie beginnen

Fügen Sie dem Avamar-System einen OpenLDAP-Verzeichnisdienst hinzu.

Nachdem Sie den OpenLDAP-Verzeichnisdienst für die Authentifizierung hinzugefügt haben, konfigurieren Sie das Avamar-System so, dass die Avamar-Authentifizierung für einige der Avamar-Domains verwendet wird.

Vorgehensweise

1. Melden Sie sich in Avamar Administrator als Administrator bei der Root-Domain an.
   a. Starten Sie Avamar Administrator.
   b. Geben Sie unter **Server** die IP-Adresse oder den DNS-Namen des Avamar-Servers ein, bei dem Sie sich anmelden möchten.
   c. Geben Sie unter **User Name** einen Benutzernamen ein.

      Der Benutzername muss für ein Konto gelten, dem auf Root-Domain-Ebene die Administratorrolle zugewiesen ist.

      Wenn Avamar bereits für die Verwendung eines Verzeichnisdiensts konfiguriert ist, können Sie sich alternativ mit einem LDAP-Konto mit Administratorberechtigungen auf Root-Domainebene anmelden. Verwenden Sie das folgende Format: ***username*@*ldap-domain***.
   d. Geben Sie unter **Password** das Passwort für das Benutzerkonto ein.
   e. Verwenden Sie unter **Domain Name** die Standardeingabe, einen Schrägstrich (`/`), um die Root-Domain festzulegen.
   f. Klicken Sie auf **Log In**.

      Wenn dies das erste Mal ist, das Sie eine Verbindung mit diesem Avamar-Server hergestellt haben, wird die das Dialogfeld **Accept Server Certificate** geöffnet. Überprüfen Sie die Details des Serverzertifikats und klicken Sie auf **Yes**.

      Das Avamar-Administrator-Dashboard wird angezeigt.
2. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
3. Klicken Sie auf die Registerkarte **LDAP Management**.
4. Klicken Sie auf **Edit LDAP file**, um die Datei `ldap.properties` zu bearbeiten.

   Das Dialogfeld **ldap.properties-Datei bearbeiten** wird angezeigt.
5. Geben Sie im Texteingabebereich Folgendes in eine neue Zeile ein:

   `user-login-module=mix`
   Dieser Parameter ist erforderlich, wenn die Avamar-Authentifizierung mit OpenLDAP-Authentifizierung aktiviert wird.

6. Geben Sie im Texteingabebereich Folgendes in eine neue Zeile ein:

   `user-login-module-mix-ldap=ldap`
   Dieser Parameter ist erforderlich, wenn die Avamar-Authentifizierung mit OpenLDAP-Authentifizierung aktiviert wird.

7. Geben Sie im Texteingabebereich Folgendes in eine neue Zeile ein:

   `avamar-authentication-domains=`*`av-domain-list`*
   Dabei steht *av-domain-list* für eine kommagetrennte Liste von Avamar-Domains.

   Das Avamar-System verwendet die Avamar-Authentifizierung zur Authentifizierung der Anmeldung von Benutzern aus jeder aufgelisteten Domain. Das Avamar-System verwendet die OpenLDAP-Authentifizierung für alle übrigen Benutzer.

8. Klicken Sie auf **Save**.
9. Klicken Sie im Dialogfeld **Directory Service Management** auf **Close**.

Ergebnisse

Das Avamar-System ermöglicht die angegebene Kombination aus Avamar-Authentifizierung und OpenLDAP-Authentifizierung.

OpenLDAP-Verzeichnisdienstparameter

In der folgenden Tabelle werden die Parameter der `ldap.properties` für die Verwendung mit einem OpenLDAP-Verzeichnisdienst beschrieben, zusätzlich zu den in Tabelle 19 auf Seite 83 beschriebenen Basisparametern.

Tabelle 21 OpenLDAP-Verzeichnisdienstparameter

Parameter und Beispiel	Beschreibung

`ldap.entry.lookup.type.`*`ldap-domain`*`=DN`
Für eine LDAP-Domain „xyz.com“, die OpenLDAP verwendet:
`ldap.entry.lookup.type.xyz.com=DN`
	Gibt den OpenLDAP an. Ersetzen Sie *ldap-domain* durch den Domainnamen des LDAP-Servers. Verwenden Sie diesen Parameter für OpenLDAP-Server, die Benutzeranmeldungen nur im DN-Format (Distinguished Name) akzeptieren. Beispiel: **`uid=jsmith,dc=example,dc=com`**. Dieser Parameter aktiviert die anderen OpenLDAP-Parameter in dieser Tabelle.

`ldap.userdn.`*`ldap-domain=rdn-values`* Für die LDAP-Domain „xyz.com“, in der Benutzer in den folgenden Organisationseinheiten organisiert sind: • `Managers` unter dem Strukturstamm • `Accountants`, unter `people`, unter dem Strukturstamm • `HRs`, unter `Employees`, unter `Users`, unter dem Strukturstamm • `Users`, unter dem Strukturstamm `ldap.userdn.xyz.com=ou=Managers;ou=Accountants,ou=people;ou=HRs,ou=Employees,ou=Users;ou=Users`	Gibt die relativen Basis-DNs (Distinguished Names) an, die den Organisationseinheiten zugewiesen sind, die Benutzer enthalten. Ersetzen Sie *ldap-domain* durch den Domainnamen des LDAP-Servers und ersetzen Sie *rdn-values* durch eine durch Semikola getrennte Liste relativer Basis-DNs (Distinguished Names) für Benutzer, vom Stamm-DN (Distinguished Name) der LDAP-Struktur. Bei jedem Eintrag in der Liste handelt es sich um eine kommagetrennte, umgekehrt hierarchische Darstellung der relativen Basis-DNs (Distinguished Names) einer Benutzergruppe.
`ldap.rootdn.`*`ldap-domain=rootdn-format`* Für eine LDAP-Domain „xyz.com“, in der der Root-DN (Distinguished Name) als „u=xyz, o=com“ gespeichert wird:	Gibt das Format des Root-DNs (Distinguished Name) für den LDAP-Server an. Dieser Parameter ist erforderlich, es sei denn, der Root-DN (Distinguished Name) weist folgendes Format auf: **`dc=`*`domain-segment`*`,dc=`*`domain-segment`***.

Tabelle 21 OpenLDAP-Verzeichnisdienstparameter (Fortsetzung)

Parameter und Beispiel	Beschreibung
`ldap.rootdn.xyz.com=u=xyz,o=com`	Ersetzen Sie *ldap-domain* durch den Domainnamen des LDAP-Servers und ersetzen Sie *rootdn-format* durch das vom LDAP-Server verwendete Format des Root-DNs (Distinguished Name).
`ldap.user.search.classes.`*`ldap-domain=search-object`* Für die LDAP-Domain „xyz.com“, die den Objektklassentyp „person“ in Benutzersuchvorgängen verwendet: `ldap.user.search.classes.xyz.com=person`	Gibt den vom Benutzersuchfilter verwendeten Objektklassentyp an. Dieser Parameter ist optional. Ersetzen Sie *ldap-domain* durch den Domainnamen des LDAP-Servers und ersetzen Sie *search-object* durch den Wert, mit dem der vom Benutzersuchfilter verwendete Objektklassentyp angegeben wird. Es können kommagetrennte Werte verwendet werden. Der Standardwert ist `*`.
`ldap.user.search.attrs.`*`ldap-domain=search-attribute`* Für die LDAP-Domain „xyz.com“, die das Objektklassenattribut „cn“ in Benutzersuchvorgängen verwendet: `ldap.user.search.attrs.xyz.com=cn`	Gibt das vom Benutzersuchfilter verwendete Objektklassenattribut an. Dieser Parameter ist optional. Ersetzen Sie *ldap-domain* durch den Domainnamen des LDAP-Servers und ersetzen Sie *search-attribute* durch ein einzelnes, vom Benutzersuchfilter verwendetes Attribut. Der Standardwert ist `uid`.
`ldap.group.search.byUpn.classes.`*`ldap-domain=search-upn`* Für eine LDAP-Domain „xyz.com“, die die folgenden Objektklassentypen „User Principal Name“ verwendet: sambaGroupMapping und posixGroup in Gruppensuchen: `ldap.group.search.byUpn.classes.xyz.com=sambaGroupMapping,posixGroup`	Gibt den vom Gruppensuchfilter „Benutzerprinzipalname“ verwendeten Objektklassentyp an. Dieser Parameter ist optional. Ersetzen Sie *ldap-domain* durch den Domainnamen des LDAP-Servers und ersetzen Sie *search-upn* durch den Wert, mit dem der vom Gruppensuchfilter „User Principal Name“ verwendete Objektklassentyp angegeben wird. Es können kommagetrennte Werte verwendet werden. Der Standardwert ist `*`.
`ldap.group.search.byUpn.attrs.`*`ldap-domain=upn-attributes`* Für eine LDAP-Domain „xyz.com“, die die Objektklassenattribute „User Principal Name“ memberUid und uniqueMember in Gruppensuchvorgängen verwendet: `ldap.group.search.byUpn.attrs.xyz.com=memberUid,uniqueMember`	Gibt die vom Gruppensuchfilter „Benutzerprinzipalname“ verwendeten Objektklassenattribute an. Dieser Parameter ist optional. Ersetzen Sie *ldap-domain* durch den Domainnamen des LDAP-Servers und ersetzen Sie *upn-attributes* durch den Wert, mit dem die vom Gruppensuchfilter „User Principal Name“ verwendeten Objektklassenattribute angegeben werden. Es können kommagetrennte Werte verwendet werden. Der Standardwert ist `memberUid, uniqueMember`.
`ldap.unique.group.search.classes.`*`ldap-domain=unique-type`* Für die LDAP-Domain „xyz.com“, die den Objektklassentyp „posixGroup“ in Gruppensuchvorgängen für eindeutige Gruppen verwendet: `ldap.unique.group.search.classes.xyz.com=posixGroup`	Gibt den Objektklassentyp an, der vom Gruppensuchfilter „Eindeutige Gruppen“ verwendet wird. Dieser Parameter ist optional. Ersetzen Sie *ldap-domain* durch den Domainnamen des LDAP-Servers und ersetzen Sie *unique-type* durch den Wert, mit dem der vom Gruppensuchfilter „Unique Groups“ verwendete Objektklassentyp angegeben wird. Es können kommagetrennte Werte verwendet werden. Der Standardwert ist `sambaGroupMapping,posixGroup,groupOfUniqueNames`.
`ldap.unique.group.search.attrs.`*`ldap-domain=unique-attributes`* Für die LDAP-Domain „xyz.com“, die die Objektklassenattribute „cn“ und „uid“ in Gruppensuchvorgängen für eindeutige Gruppen verwendet:	Gibt die Objektklassenattribute an, die vom Gruppensuchfilter „Eindeutige Gruppen“ verwendet werden. Dieser Parameter ist optional. Ersetzen Sie *ldap-domain* durch den Domainnamen des LDAP-Servers und ersetzen Sie *unique-attributes* durch den Wert, mit dem die vom

Tabelle 21 OpenLDAP-Verzeichnisdienstparameter (Fortsetzung)

Parameter und Beispiel	Beschreibung
`ldap.unique.group.search.attrs.xyz.com=cn,uid`	Gruppensuchfilter „Unique Groups“ verwendeten Objektklassenattribute angegeben werden. Es können kommagetrennte Werte verwendet werden. Der Standardwert ist `cn`.
`user-login-module=mix`	Ermöglicht die Authentifizierung im kombinierten Modus der Avamar-Authentifizierung mit OpenLDAP-Authentifizierung. Die Konfiguration muss außerdem Folgendes enthalten: `user-login-module-mix-ldap=ldap` und `avamar-authentication-domains=`*av-domain-list*.
`user-login-module-mix-ldap=ldap`	Gibt an, dass das Avamar-System die Avamar-Authentifizierung mit OpenLDAP-Authentifizierung verwendet. Die Konfiguration muss außerdem Folgendes enthalten: `user-login-module=mix` und `avamar-authentication-domains=`*av-domain-list*.
`avamar-authentication-domains=`*av-domain-list* Für ein Avamar-System, das OpenLDAP und die Avamar-Authentifizierung für die folgenden Domains verwendet: `/`, `/swclients`, and `/adminclients`: `avamar-authentication-domains=/,/swclients,/adminclients`	Gibt die internen Avamar-Domains an, die das Avamar-System bei der Avamar-Authentifizierung prüft. Ersetzen Sie *av-domain-list* durch eine kommagetrennte Liste von Avamar-Domains. Die Konfiguration muss außerdem Folgendes enthalten: `user-login-module=mix` und `user-login-module-mix-ldap=ldap`.

Hinzufügen eines NIS-Verzeichnisdiensts

Sie können die Authentifizierung und Autorisierung von Avamar-Benutzern über einen NIS-Verzeichnisdienst durchführen.

Vorgehensweise

1. Melden Sie sich in Avamar Administrator als Administrator bei der Root-Domain an.
   a. Starten Sie Avamar Administrator.
   b. Geben Sie unter **Server** die IP-Adresse oder den DNS-Namen des Avamar-Servers ein, bei dem Sie sich anmelden möchten.
   c. Geben Sie unter **User Name** einen Benutzernamen ein.

      Der Benutzername muss für ein Konto gelten, dem auf Root-Domain-Ebene die Administratorrolle zugewiesen ist.

      Wenn Sie bereits einen Verzeichnisdienst konfiguriert haben, können Sie sich mit dem Konto eines LDAP-Benutzers mit der Administratorrolle auf Root-Domainebene anmelden.
   d. Geben Sie unter **Password** das Passwort für das Benutzerkonto ein.
   e. Verwenden Sie unter **Domain Name** die Standardeingabe, einen Schrägstrich (`/`), um die Root-Domain festzulegen.
   f. Klicken Sie auf **Log In**.

      Wenn dies das erste Mal ist, das Sie eine Verbindung mit diesem Avamar-Server hergestellt haben, wird die das Dialogfeld **Accept Server Certificate**

geöffnet. Überprüfen Sie die Details des Serverzertifikats und klicken Sie auf **Yes**.

Das Avamar-Administrator-Dashboard wird angezeigt.

2. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
3. Klicken Sie auf die Registerkarte **LDAP Management**.
4. Klicken Sie auf **Directory Service Management**.

   Das Dialogfeld **Directory Service Management** wird angezeigt.
5. Klicken Sie im Dialogfeld **Directory Service Management** auf **Add**.

   Daraufhin wird der Abschnitt **Adding a new Directory Service** angezeigt.
6. Wählen Sie **NIS** aus.
7. Geben Sie unter **Enter a fully qualified domain name** den NIS-Domainnamen ein.
8. Geben Sie im Feld **NIS Domain IP address** die IP-Adresse des NIS-Servers ein.
9. Klicken Sie auf **Add**.

   Es wird eine Bestätigungsmeldung angezeigt.
10. Klicken Sie auf **Yes**.

    Wenn eine Fehlermeldung angezeigt wird, beheben Sie das Problem und bearbeiten Sie die Aufgabe erneut. Fehlermeldungen während der Verzeichnisdienstkonfiguration auf Seite 92 enthält weitere Einzelheiten.

    Daraufhin wird eine Erfolgsmeldung angezeigt.
11. Klicken Sie auf **OK**.

Ergebnisse

Die Änderungen werden auf den MMC-Dienst (Management Console Server) (`mcs`) und den EM Tomcat-Dienst (`emt`) angewendet.

Weitere Erfordernisse

Erstellen Sie eine LDAP-Zuordnung, um der Verzeichnisdienstgruppe Avamar-Benutzerinformationen zuzuweisen. Anweisungen finden Sie unter Hinzufügen einer LDAP-Zuordnung auf Seite 93.

Fehlermeldungen während der Verzeichnisdienstkonfiguration

Fehlermeldungen werden angezeigt, wenn Probleme während der Aufnahme oder Prüfung einer Verzeichnisdienstkonfiguration auftreten.

In der folgenden Tabelle finden Sie eine Liste einiger möglicher Meldungen und eine Beschreibung der jeweiligen Ursache.

Tabelle 22 Fehlermeldungen während der Verzeichnisdienstkonfiguration

Fehlermeldung	Beschreibung
`Cannot discover KDC`	Anhand der angegebenen Domaininformationen wurde kein Schlüsselverteilungscenter (Key Distribution Center, KDC) gefunden.

Tabelle 22 Fehlermeldungen während der Verzeichnisdienstkonfiguration (Fortsetzung)

Fehlermeldung	Beschreibung
`No URL is present`	Die angegebene Domain ist nicht in der Datei `ldap.properties` vorhanden.
`Parameters are not correct`	Die Verzeichnisdienst-Domaininformationen in der Datei `ldap.properties` sind ungültig.
`Client not found in Kerberos database`	Der angegebene Benutzername ist ungültig.
`Pre-authentication information was invalid`	Das angegebene Passwort ist falsch.
`Query fails`	Das angegebene Benutzerkonto verfügt nicht über ausreichende Leserechte für die Verzeichnisdienstdatenbank.
`Clock skew too great`	Der Unterschied zwischen der Uhr auf dem Avamar-Serverhost und der Uhr auf dem Verzeichnisdiensthost ist zu groß.
`Cannot open LDAP configuration file`	Die `ldap.properties`-Datei ist nicht vorhanden oder die Berechtigungen der Datei verhindern einen Zugriff.
`Cannot open Kerberos configuration file`	Die `krb5.conf`-Datei ist nicht vorhanden oder die Berechtigungen der Datei verhindern einen Zugriff.
`GSS initiate failed`	Die Authentifizierung der Anmeldedaten ist fehlgeschlagen. Üblicherweise tritt ein Authentifizierungsfehler auf, wenn der umgekehrte DNS nicht ordnungsgemäß konfiguriert ist. Fügen Sie den KDC-Host zu `/etc/hosts` auf dem Avamar-Server hinzu.
`Cannot get kdc for realm`	Das Schlüsselverteilungscenter ist in der Datei `krb5.conf` nicht ordnungsgemäß konfiguriert.
`Domain <domain> exists in ldap.properties file`	Die angegebene Domain ist bereits in der Datei `ldap.properties` enthalten.

Hinzufügen einer LDAP-Zuordnung

Erstellen Sie eine LDAP-Zuordnung, um der Verzeichnisdienstgruppe Avamar-Benutzerinformationen zuzuweisen. Eine LDAP-Zuordnung ist ein Datenbankkonstrukt, das eine Gruppe von Benutzern an ein Authentifizierungssystem, eine Domain- bzw. Subdomainzugriffsliste sowie eine Rolle bindet.

Bevor Sie beginnen

Fügen Sie der Avamar-Konfiguration Verzeichnisdienstdomains hinzu.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Account Management**.
3. Klicken Sie auf die Registerkarte **LDAP Maps**.

4. Wählen Sie im linken Bereich der hierarchischen Baumstruktur eine Domain oder eine Subdomain aus, um die Zugriffsebene der Verzeichnisdienstgruppe festzulegen.
5. Wählen Sie **Actions** > **Account Management** > **New LDAP Map** aus.

   Das Dialogfeld **New LDAP Group Map** wird angezeigt.
6. Wählen Sie aus der Liste **LDAP Domains** eine zuzuordnende Verzeichnisdienstdomain aus.
7. Geben Sie im Feld **Group Search** eine Suchzeichenfolge zu der Gruppe ein, die zugeordnet werden soll.

   Sie können ein Sternchen (*) als Platzhalter für ein oder mehrere alphanumerische Zeichen verwenden.
8. Klicken Sie auf **Search**.

   Das Dialogfeld **Directory Service Authentication** wird angezeigt.
9. Geben Sie die für die Abfrage des Verzeichnisdiensts erforderlichen Authentifizierungsinformationen an.

   Die Authentifizierung kann über eine andere Domain erfolgen als diejenige, die zugeordnet wird, solange zwischen den beiden Domains eine Vertrauensbeziehung besteht.

   a. Wählen Sie aus der Liste **Auth Domain** eine für die Authentifizierung zu verwendende Domain aus.

   b. Geben Sie im Feld **User Name** einen Benutzernamen für ein Konto ein, das Leseberechtigungen für diese Domain besitzt.

   c. Geben Sie im Feld **Password** das Passwort für den Benutzernamen ein.

   d. Klicken Sie auf **OK**.

   Das Dialogfeld **Directory Service Authentication** wird geschlossen und die Suche wird gestartet. Die Schaltfläche **Search** auf dem Dialogfeld **New LDAP Group Map** wechselt zu **Stop**.

   Klicken Sie zum Beenden eines Suchvorgangs auf **Stop**. Das Durchsuchen eines Verzeichnisdiensts kann viel Zeit in Anspruch nehmen.

   Die Suche ist abgeschlossen, wenn die Gruppen in der Liste **LDAP Groups** angezeigt werden.
10. Wählen Sie aus der Liste **LDAP Groups** die zuzuordnende Gruppe aus.
11. Wählen Sie aus der Liste **Role** eine Rolle für die Gruppe aus.
12. Klicken Sie auf **OK**.

    Die Gruppe wird zugeordnet und das Dialogfeld **New LDAP Group Map** wird geschlossen. Wählen Sie den administrativen Node aus, damit die Zuordnung auf der Registerkarte **LDAP Maps** angezeigt wird.

Bearbeiten der Rolle einer LDAP-Zuordnung

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Account Management**.

3. Klicken Sie auf die Registerkarte **LDAP Maps**.
4. Wählen Sie im linken Bereich der hierarchischen Baumstruktur eine Domain oder eine Subdomain aus.

   Die Zuordnungen für die Domain oder die Subdomain werden im Bereich **LDAP Maps** angezeigt.
5. Wählen Sie die zu bearbeitende Zuordnung aus.
6. Wählen Sie **Actions** > **Account Management** > **Edit LDAP Map** aus.

   Das Dialogfeld **Edit LDAP Maps** wird angezeigt.
7. Wählen Sie unter **Role** eine neue Rolle aus, die der Zuordnung zugewiesen werden soll.
8. Klicken Sie auf **OK**.

   Der Zuordnung wird eine neue Rolle zugewiesen. Den Gruppenmitgliedern wird die neue Rolle in allen folgenden Sitzungen zugewiesen.

Löschen einer LDAP-Zuordnung

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Account Management**.
3. Klicken Sie auf die Registerkarte **LDAP Maps**.
4. Wählen Sie im linken Bereich der hierarchischen Baumstruktur eine Domain oder eine Subdomain aus.

   Die Zuordnungen für die Domain oder die Subdomain werden im Bereich **LDAP Maps** angezeigt.
5. Wählen Sie die zu löschende Zuordnung aus.
6. Wählen Sie **Actions** > **Account Management** > **Delete LDAP Map** aus.

   Das Dialogfeld **Delete LDAP Map** wird angezeigt.
7. Klicken Sie auf **Yes**.

Bearbeiten des Timeout-Werts für Verzeichnisdienstprozesse

Bei Verzeichnisdienstprozessen wird bis zu 5 Minuten auf eine Antwort vom Verzeichnisdienst gewartet. Nach dieser Zeitspanne wird der Versuch verworfen und es wird eine Zeitüberschreitungsmeldung angezeigt. Sie können den Timeout-Wert bearbeiten.

Der Timeout-Wert wird von den folgenden Verzeichnisdienstauthentifizierungsprozessen verwendet:

- Authentifizierungsanforderungen durch den Verzeichnisdienst
- Hinzufügen eines Verzeichnisdiensts zur Avamar-Konfiguration
- Testen eines Verzeichnisdiensts in der Avamar-Konfiguration

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:

- Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
- Bei einem Multi-Node-Server:
  a. Melden Sie sich als Administrator beim Utility Node an.
  b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

  ```
  ssh-agent bashssh-add ~admin/.ssh/admin_key
  ```

2. Beenden Sie den Service Management Console Server (`mcs`), indem Sie **`dpnctl stop mcs`** eingeben.
3. Wechseln Sie mit folgendem Befehl das Arbeitsverzeichnis:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

4. Öffnen Sie `mcserver.xml` in einem Texteditor.
5. Navigieren Sie zum `<node name="ldap">`-Node.
6. Ändern Sie den Wert von `<entry key="ldap_services_timeout_seconds" value="`*n*`" />` in einen neuen Zeitüberschreitungswert in Sekunden an, wobei *n* der neue Wert ist.

   Der Standardwert ist 300 Sekunden (5 Minuten).
7. Speichern Sie die Änderung und schließen Sie die Datei.
8. Starten Sie den MCS und den Scheduler, indem Sie Folgendes eingeben:

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

9. Schließen Sie die Befehlsshell.

Ermöglichen der Abwärtskompatibilität mit Enterprise Authentication

Aktivieren Sie diese Funktion, um Benutzer weiterhin über den veralteten Mechanismus Enterprise Authentication zu authentifizieren.

Bei Enterprise Authentication verwendet Avamar die Pluggable Authentication Module- (PAM-)Bibliothek des Linux-Hostbetriebssystems, um Zugriff auf externe Authentifizierungsdatenbanken zu gewähren. Die im *Avamar – Produktsicherheitshandbuch* beschriebene Methode Enterprise Authentication ist veraltet und wird in zukünftigen Versionen nicht mehr enthalten sein. Sie können standardmäßig keine Enterprise Authentication-Domain auswählen, wenn Sie einer Domain oder einem Client einen Benutzer hinzufügen. Damit Enterprise Authentication weiterhin als Authentifizierungsmechanismus verwendet werden kann, konfigurieren Sie das System zum Aktivieren der Auswahl von Enterprise Authentication beim Hinzufügen eines Benutzers, indem Sie die Enterprise Authentication-Auswahleinstellung in der Datei `mcserver.xml` entsprechend ändern.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.

- Bei einem Multi-Node-Server:
  a. Melden Sie sich als Administrator beim Utility Node an.
  b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ssh-agent bashssh-add ~admin/.ssh/admin_key

2. Beenden Sie den Dienst msc (Management Console Server), indem Sie **dpnctl stop mcs** eingeben.
3. Wechseln Sie mit folgendem Befehl das Arbeitsverzeichnis:

   cd /usr/local/avamar/var/mc/server_data/prefs
4. Öffnen Sie `mcserver.xml` in einem Texteditor.
5. Navigieren Sie zum `<node name="ldap">`-Node.
6. Ändern Sie den Wert von `<entry key="enable_new_user_authentication_selection" value="false" />` von `false` in `true`.
7. Speichern Sie die Änderung und schließen Sie die Datei.
8. Starten Sie den MCS und den Scheduler, indem Sie Folgendes eingeben:

   dpnctl start mcs
   dpnctl start sched
9. Schließen Sie die Befehlsshell.

Rollen

Rollen definieren die zulässigen Vorgänge für jedes Benutzerkonto.

Es gibt drei Arten von Rollen:

- Administratorrollen
- Operatorrollen
- Benutzerrollen

Administratorrollen

Administratoren sind für die Wartung des Systems zuständig.

Die Administratorrolle können Sie nur Benutzerkonten auf Domainebene zuweisen. Die Domainebene umfasst die Domain der obersten Ebene (Stammdomain) sowie jede andere Domain oder Subdomain. Sie können die Administratorrolle Benutzerkonten nicht auf Clientebene zuweisen.

Sie können Benutzern der (Root-)Domain der obersten Ebene oder einer bestimmten Domain bzw. Subdomain die Administratorrolle zuweisen.

Tabelle 23 Administratorrollen

Administratortyp	Beschreibung
Root-Administratoren	Administratoren in der (Root-)Domain der obersten Ebene besitzen die vollkommene Kontrolle über das System. Sie werden auch als „Root-Administratoren“ bezeichnet.

Tabelle 23 Administratorrollen (Fortsetzung)

Administratortyp	Beschreibung
Domainadministratoren	Administratoren in anderen Domains als der Stammdomain haben generell Zugriff auf die meisten der in diesem Handbuch beschriebenen Funktionen. Administratoren können in der Regel nur Objekte in der Domain anzeigen oder bearbeiten. Jede Aktivität, die einem Domainadministrator das Anzeigen von Daten von außerhalb der Domain ermöglicht, ist nicht zulässig. Der Zugriff auf globale Serverfunktionen (z. B. das Unterbrechen oder Wiederaufnehmen geplanter Vorgänge oder das Ändern von Laufzeiten für Wartungsaktivitäten) ist nicht zulässig. Domainadministratoren: • Hinzufügen oder Bearbeiten anderer Subdomainadministratoren • Ändern ihrer zugewiesenen Rolle • Ändern ihres Passworts

Operatorrollen

Operatorrollen werden generell implementiert, um bestimmten Benutzern begrenzten Zugriff auf bestimmte Bereiche des Systems zu gewähren, damit diese Backups und Wiederherstellungen durchführen, den Status abrufen und Berichte ausführen können. Diese Rollen ermöglichen mehr Flexibilität bei der Zuweisung von Backup-, Wiederherstellungs- und Berichtsaufgaben an andere Personen als Administratoren.

Sie können Operatorrollen nur Benutzerkonten auf Domainebene zuweisen. Sie können diese Operatorrollen nicht Benutzerkonten auf Clientebene zuweisen. Um das Benutzerkonto zu Subdomains hinzuzufügen, müssen Sie über Administratorrechte in der übergeordneten Domain oder einer noch höheren Domain verfügen.

Benutzer mit einer Operatorrolle haben nicht auf alle Funktionen in Avamar Administrator Zugriff. Stattdessen wird ihnen nach der Anmeldung ein Fenster angezeigt, das Zugriff auf die Funktionen bietet, die diese verwenden dürfen.

Die folgende Tabelle beschreibt die vier Operatorrollen.

Tabelle 24 Operatorrollen

Operatortyp	Beschreibung
Restore only operator	Die Rolle Restore only operator darf in der Regel nur Wiederherstellungen durchführen und diese Aktivitäten überwachen, um zu bestimmen, wann diese abgeschlossen werden und ob sie ohne Fehler abgeschlossen wurden. Die Rolle Restore only operator in der (Root-)Domain der obersten Ebene kann Wiederherstellungen für jeden Client im System durchführen. In einer anderen Domain als der Root-Domain kann diese Rolle nur Wiederherstellungen für Clients in dieser Domain durchführen. Die Rolle Restore only operator kann Backupdaten wiederherstellen und Aktivitäten in der zugewiesenen Domain überwachen. • Standardmäßig kann die Rolle Restore only operator keine Wiederherstellungen an einem anderen Speicherort oder an mehreren Speicherorten durchführen. Um diese Option zu aktivieren, müssen Sie das Attribut restore_admin_can_direct_restores in der Datei mcserver.xml auf „true“ festlegen. • Standardmäßig können Operatoren mit der Rolle „Restore only operator“ keine Backups über die Befehlszeile oder die Avamar Web Restore-Schnittstelle durchsuchen. Um diese Aktivitäten für die Rolle „Restore only operator“ zu aktivieren, fügen Sie die Berechtigung `noticketrequired` mithilfe des folgenden `avmgr chgv`-Befehls hinzu: **`avmgr chgv --acnt=`*`location`*` --u=`*`name`*` --ud=`*`auth`*` \ --`**

Tabelle 24 Operatorrollen (Fortsetzung)

Operatortyp	Beschreibung
	pv="enabled,read,mclogin,noticketrequired". Dabei steht *location* für die Subdomain des Operators, *name* für den Avamar-Benutzernamen des Benutzers und *auth* für das zur Authentifizierung des Benutzers verwendete externe Authentifizierungssystem.
Backup only operator	Die Rolle Backup only operator darf in der Regel nur Backups durchführen und diese Aktivitäten überwachen, um zu bestimmen, wann diese abgeschlossen werden und ob sie ohne Fehler abgeschlossen wurden. Die Rolle Backup only operator in der (Root-)Domain der obersten Ebene kann Backups für jeden Client und jede Gruppe im System durchführen. In anderen Domains als der Root-Domain kann diese Rolle nur Backups für Clients oder Gruppen in dieser Domain durchführen. Die Rolle Backup only operator kann On-Demand-Backups eines Clients oder einer Gruppe durchführen sowie Aktivitäten in der zugewiesenen Domain überwachen. • Standardmäßig kann die Rolle Backup only operator keine Wiederherstellungen an einem anderen Speicherort oder an mehreren Speicherorten durchführen. Um diese Option zu aktivieren, müssen Sie das Attribut restore_admin_can_direct_restores in der Datei mcserver.xml auf „true“ festlegen. • Standardmäßig können Operatoren mit der Rolle „Backup only operator“ keine Backups über die Befehlszeile durchführen. Um Befehlszeilenbackups für die Rolle „Backup only operator“ zu aktivieren, fügen Sie die Berechtigung `noticketrequired` mithilfe des folgenden `avmgr chgv`-Befehls hinzu: **avmgr chgv --acnt=*location* --u=*name* --ud=*auth* \ --pv="enabled,read,mclogin,backup,noticketrequired"**. Dabei steht *location* für die Subdomain des Operators, *name* für den Avamar-Benutzernamen des Benutzers und *auth* für das zur Authentifizierung des Benutzers verwendete externe Authentifizierungssystem.
Backup/restore operator	Operatoren mit der Rolle „Backup/restore operator“ dürfen in der Regel nur Backups oder Wiederherstellungen durchführen und diese Aktivitäten überwachen, um zu ermitteln, wann diese abgeschlossen werden und ob sie ohne Fehler abgeschlossen wurden. Genau wie bei Rollen, die anderen Domainbenutzerkonten zugewiesen sind, können Operatoren mit der Rolle „Backup/restore operator“ in der (Root-)Domain der obersten Ebene Backups und Wiederherstellungen für jeden Client und jede Gruppe im System durchführen. In anderen Domains als der Root-Domain kann diese Rolle nur Backups und Wiederherstellungen für Clients oder Gruppen in dieser Domain durchführen. Die Rolle Backup/restore operator kann in der zugewiesenen Domain die folgenden Aufgaben durchführen: • Durchführen von On-Demand-Backups für einen Client oder eine Gruppe • Durchführen von Wiederherstellungen • Überwachen von Aktivitäten Standardmäßig können Operatoren mit der Rolle „Backup/restore operator“ Backups nicht über die Befehlszeile oder die Avamar Web Restore-Schnittstelle durchsuchen und auch keine Backups über die Befehlszeile durchführen. Um diese Aktivitäten zu aktivieren, fügen Sie die Berechtigung `noticketrequired` mithilfe des folgenden `avmgr chgv`-Befehls hinzu: **avmgr chgv --acnt=*location* --u=*name* --ud=*auth* \ --pv="enabled,read,mclogin,backup,noticketrequired"**. Dabei steht *location* für die Subdomain des Operators, *name* für den Avamar-Benutzernamen des Benutzers und *auth* für das zur Authentifizierung des Benutzers verwendete externe Authentifizierungssystem.
Activity operator	Die Rolle Activity operator darf in der Regel lediglich Backup- und Wiederherstellungsaktivitäten überwachen und bestimmte Berichte erstellen. Die Rolle Activity operator in der (Root-)Domain der obersten Ebene kann Berichte zu Backup- und Wiederherstellungsaktivitäten in allen Domains und Subdomains anzeigen oder erstellen. In anderen Domains als der Root-Domain kann diese Rolle nur

Tabelle 24 Operatorrollen (Fortsetzung)

Operatortyp	Beschreibung
	Berichte zu Backup- und Wiederherstellungsaktivitäten in dieser Domain anzeigen oder erstellen. Die Rolle Activity operator kann in der zugewiesenen Domain die folgenden Aufgaben durchführen: • Überwachen von Aktivitäten • Anzeigen der Group Status Summary • Anzeigen des Activity Report • Anzeigen des Replication Report

Benutzerrollen

Benutzerrollen schränken die für ein Benutzerkonto auf einem bestimmten Client zulässigen Vorgänge ein.

Benutzer, denen eine der Benutzerrollen zugewiesen ist, können sich nicht bei Avamar Administrator, Avamar Client Manager bzw. bei der Webbenutzeroberfläche des Avamar-Clients anmelden.

Die folgende Tabelle beschreibt die vier Benutzerrollen.

Tabelle 25 Benutzerrollen

Benutzertyp	Beschreibung
Back Up Only User	Benutzer, denen diese Rolle zugewiesen ist, können mithilfe der Befehlszeile `avtar` Backups direkt vom Client aus starten.
Restore (Read) Only User	Benutzer, denen diese Rolle zugewiesen ist, können mit der Befehlszeile `avtar` oder mit den Management Console Server- (MCS-)Webdiensten Wiederherstellungen direkt vom Client aus starten.
Back Up/Restore User	Benutzer, denen diese Rolle zugewiesen ist, können mithilfe der Befehlszeile `avtar` oder mit den MCS-Webdiensten Backups und Wiederherstellungen direkt vom Client aus starten.
Restore (Read) Only/ Ignore File Permissions	Ähnelt der Rolle „Restore (Read) Only User“, abgesehen davon, dass Betriebssystem-Dateiberechtigungen bei der Durchführung von Wiederherstellungen ignoriert werden. Diesem Benutzer ist es erlaubt, alle für einen Avamar-Client gespeicherten Dateien wiederherzustellen. Diese Rolle ist nur verfügbar, wenn Benutzer mithilfe der internen Avamar-Authentifizierung authentifiziert werden. Windows-Clientbenutzerkonten sollten dieser Rolle zugewiesen werden, damit fehlerfreie Wiederherstellungen möglich sind. Dies ist nur unter den beiden folgenden Bedingungen möglich: • Benutzer werden mithilfe der internen Avamar-Authentifizierung authentifiziert. • Benutzer benötigen keinen Zugriff auf die Webbenutzeroberfläche des Avamar-Clients.

Hinzufügen eines Benutzers zu einem Client oder einer Domain

Sie können einem Client oder einer Domain ein Benutzerkonto hinzufügen, wenn das Benutzerkonto mithilfe der internen Avamar-Authentifizierung oder des veralteten Enterprise Authentication-Systems authentifiziert wird.

Unter Vorbereitung auf die Verwendung der LDAP-Verzeichnisdienstauthentifizierung auf Seite 78 erfahren Sie weitere Details zum Hinzufügen eines Benutzers, der für die Authentifizierung einen vorhandenen Verzeichnisdienst verwendet.

Vorgehensweise

1. Lesen Sie Rollen auf Seite 97 nochmals durch, um sich zu vergewissern, dass Sie diesem Benutzer die richtige Rolle zuweisen.
2. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Account Management**.
4. Klicken Sie auf die Registerkarte **Users**.
5. Wählen Sie im linken Bereich der hierarchischen Baumstruktur die Domain oder den Client für den neuen Benutzer aus.

   Hinweis

   Sie können der Domain `MC_RETIRED` oder den Clients in der Domain `MC_RETIRED` keine Benutzerkonten hinzufügen.
6. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **New User(s)** aus.

   Das Dialogfeld **New User(s)** wird angezeigt.
7. (Optional) Wählen Sie aus der Liste **Authentication System** ein Authentifizierungssystem aus.

   Die Liste **Authentication System** wird normalerweise in einem abgeblendeten Zustand angezeigt, wobei **Axion Authentication System** (das interne System) ausgewählt ist. Dieser Schritt zeigt an, dass die Möglichkeit zur Auswahl eines Enterprise Authentication-Systems derzeit nicht aktiviert ist.

   Das im *Avamar – Produktsicherheitshandbuch* beschriebene Enterprise Authentication-System ist veraltet und wird in zukünftigen Versionen nicht mehr enthalten sein. Es kann allerdings mit dieser Version verwendet werden. Um die Möglichkeit zur Auswahl eines Enterprise Authentication-Systems zu aktivieren, führen Sie das unter Ermöglichen der Abwärtskompatibilität mit Enterprise Authentication auf Seite 96 beschriebene Verfahren aus.

   Eine solidere Alternative zu Enterprise Authentication erhalten Sie mithilfe der unter Vorbereitung auf die Verwendung der LDAP-Verzeichnisdienstauthentifizierung auf Seite 78 beschriebenen Methode.
8. (Optional) Falls Sie sich für das Enterprise Authentication-System entscheiden, wählen Sie die Option **Everyone** aus, um allen Benutzern auf diesem Client oder in dieser Domain Rollen zuzuweisen.

9. Wählen Sie die Option **User Name** aus und geben Sie den neuen Benutzernamen ein.

   Der Benutzername muss folgende Anforderungen erfüllen:

   - Falls Sie Enterprise Authentication verwenden, muss diese Option der vom System zugewiesene Benutzername sein.
   - Der Benutzername darf maximal 31 Zeichen enthalten.
   - Der Benutzername darf keines der folgenden Zeichen enthalten: `~!@$^%()\{}[]|,`;#\/:*?<>'"&.`

10. Wählen Sie aus der Liste **Role** eine Rolle für den Benutzer aus.
11. Geben Sie im Feld **Password** ein Passwort für den Benutzer ein.

    Bei den Passwörtern muss die Groß- und Kleinschreibung beachtet werden und die folgenden Anforderungen müssen erfüllt sein:

    - Das Passwort muss zwischen 6 und 31 Zeichen lang sein.
    - Das Passwort darf ausschließlich alphanumerische Zeichen, Bindestriche, Punkte und Unterstriche enthalten.
    - Das Passwort muss mindestens ein alphabetisches Zeichen enthalten.

    Dieses Feld wird nicht für Enterprise Authentication verwendet.

12. Geben Sie im Feld **Confirm** das Passwort erneut ein.

    Dieses Feld wird nicht für Enterprise Authentication verwendet.

13. Klicken Sie auf **OK**.

    Es wird eine Bestätigungsmeldung angezeigt.

14. Klicken Sie auf **OK**.

Bearbeiten von Benutzerinformationen

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Account Management**.

   In der Baumstruktur **Account Management** geben die Symbole für die Clients den Status an. Für deaktivierte Clients wird ein x angezeigt, für nicht registrierte ein Fragezeichen. Für aktive Clients gibt es keine spezielle Symbolzuweisung.

3. Wählen Sie im linken Bereich der hierarchischen Baumstruktur die Domain oder den Client für den Benutzer aus.
4. Wählen Sie den Benutzer aus.
5. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Edit User** aus.

   Das Dialogfeld **Edit User** wird angezeigt.

6. Wählen Sie die Rolle für den Benutzer aus.
7. (Optional) Ändern Sie das Passwort für den Benutzer:

a. Klicken Sie auf **Set Password**.

   Das Dialogfeld **Set Password** wird angezeigt.

b. Geben Sie das neue Passwort sowohl im Feld **New Password** als auch im Feld **Confirm Password** ein.

c. Klicken Sie im Dialogfeld **Set Password** auf **OK**.

8. Klicken Sie auf **OK**.

   Es wird eine Bestätigungsmeldung angezeigt.

9. Klicken Sie auf **OK**.

Löschen eines Benutzers

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Account Management**.
3. Wählen Sie im linken Bereich der hierarchischen Baumstruktur die Domain oder den Client für den Benutzer aus.
4. Wählen Sie den Benutzer aus.
5. Wählen Sie aus dem Menü **Actions** den Befehl **Account Management** > **Delete User** aus.

   Es wird eine Bestätigungsmeldung angezeigt.

6. Klicken Sie auf **Yes**.

   Es wird eine zweite Bestätigungsmeldung angezeigt.

7. Klicken Sie auf **OK**.

KAPITEL 5

Backup

In diesem Kapitel werden folgende Themen behandelt:

Durchführen von Backups nach Bedarf

Sie können On-Demand-Backup eines einzelnen Clients durchführen. Wenn Sie geplante Backups für eine Gruppe von Clients konfigurieren, können Sie mithilfe der Gruppen-Policy-Einstellungen auch ein On-Demand-Backup einer Gruppe oder eines Clients durchführen.

Ein On-Demand-Backup ist ein einmaliges Backup von Daten auf einem Avamar-Clientcomputer. Sie sollten nach der Installation der Avamar-Clientsoftware umgehend ein On-Demand-Backup für das erste Backup des Clients durchführen. Führen Sie vor einer Systemwartung, vor Softwareinstallationen oder Softwareupgrades ein On-Demand-Backup durch.
Wenn der Avamar-Server Data Domain als Back-end-Speicher verwendet, werden On-Demand-Backups standardmäßig in das Data Domain-System geschrieben.

Durchführen von On-Demand-Backups von einem Client

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Wählen Sie in der Domainstruktur die Domain für den Client aus.
3. Wählen Sie aus der Liste der Clients den zu sichernden Clientcomputer aus.

   Clients können lediglich in der Domain des Anmeldekontos angezeigt werden. Melden Sie sich zum Anzeigen aller Clients bei der Root Domain an.
4. Klicken Sie auf die Registerkarte **Backup**.

   Eine Liste der Plug-ins auf dem Client wird im linken Bereich der Registerkarte **Backup** angezeigt.
5. Navigieren Sie zu den zu sichernden Daten und aktivieren Sie das daneben stehende Kontrollkästchen.
6. Geben Sie beim Durchsuchen des Clientdateisystems eine gültige Kombination von Clientbenutzername und Clientpasswort ein und klicken Sie dann auf **OK**.

   Der Benutzername und das Passwort müssen über Leseberechtigungen für die von Ihnen zum Backup ausgewählten Dateien und Verzeichnisse verfügen.
7. (Optional) Um eine Übersicht aller von Ihnen zum Backup ausgewählten Verzeichnisse und Dateien anzuzeigen, wählen Sie **Actions** > **Preview List** aus.
8. Wählen Sie **Actions** > **Back Up Now** aus.

   Das Dialogfeld **On Demand Backup Options** wird angezeigt.
9. Wählen Sie die Backup-Aufbewahrungseinstellung aus:
   - Um dieses Backup nach einer bestimmten Zeit automatisch vom Avamar-Server zu löschen, wählen Sie **Retention period** aus. Geben Sie die Anzahl der Tage, Wochen, Monate oder Jahre für die Aufbewahrungsfrist ein.
   - Um dieses Backup an einem bestimmten Kalendertag automatisch vom Avamar-Server zu löschen, wählen Sie **End date** aus und navigieren zum gewünschten Datum im Kalender.
   - Um dieses Backup während der ganzen Aktivierungszeit des Clients auf dem Avamar-Server aufzubewahren, wählen Sie **No end date** aus.

10. Wählen Sie aus der Liste **Avamar encryption method** die Verschlüsselungsmethode für den Datentransfer zwischen dem Client und dem Avamar-Server beim Backup aus.

    Die genaue Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-Server-Verbindung sind von mehreren Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.

11. Klicken Sie auf **More Options**.

    Das Dialogfeld **Backup Command Line Options** wird angezeigt.

12. (Optional) Aktivieren Sie das Kontrollkästchen **Show Advanced Options**, um die in rot gekennzeichneten erweiterten Optionen anzuzeigen.
13. Legen Sie die Plug-in-Optionen fest. Im Benutzerhandbuch für das jeweilige Plug-in finden Sie Details zu den einzelnen Optionen.
14. Klicken Sie im Dialogfeld **Backup Command Line Options** auf **OK**.
15. Klicken Sie im Dialogfeld **On Demand Backup Options** auf **OK**.

    Im Dialogfeld **On Demand Backup Request** wird angegeben, dass das Backup gestartet wurde.

16. Klicken Sie auf **Close**.

Durchführen von On-Demand-Gruppenbackups

Mithilfe von On-Demand-Gruppenbackups können Sie eine gesamte Gruppe von Clients oder einen einzelnen Client mit Gruppen-Policy-Einstellungenzu einem anderen Zeitpunkt als dem regulär geplanten Zeitpunkt sichern.

Sie können einzelne On-Demand-Backups für die einzelnen Clients vornehmen, sind viele Clients vorhanden, kann dieser Schritt jedoch sehr zeitaufwändig sein. Sie können On-Demand-Backups jedoch nicht mit erweiterten Aufbewahrungseinstellungen managen. Ihnen kann nur ein statisches Ablaufdatum zugewiesen werden. Stattdessen können Sie ein On-Demand-Gruppenbackup durchführen. Dies ist weniger zeitaufwendig und Sie können die Backups mit erweiterten Aufbewahrungseinstellungen managen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Um eine Gruppe zu sichern, wählen Sie die Gruppe oder den Client aus:
   - Um eine Gruppe zu sichern, klicken Sie auf die Registerkarte **Groups** und wählen Sie dann die Gruppe aus der Liste aus.
   - Um einen Client zu sichern, klicken Sie auf die Registerkarte **Client** und wählen Sie dann den Client aus der Liste aus.
4. Klicken Sie auf **Back up**.
5. Klicken Sie in der Bestätigungsmeldung auf **OK**.

Planen von Backups

Geplante Backups werden automatisch ausgeführt, um sicherzugehen, dass Backups kontinuierlich vorgenommen werden. Sie können Backups so planen, dass sie täglich,

wöchentlich oder monatlich ausgeführt werden. Das geplante Backup kann mehrere Clients oder einen einzigen Server umfassen.

Vorgehensweise

1. Erstellen Sie ein Dataset, um die in die Backups einzuschließenden Daten festzulegen.
2. Erstellen Sie eine Planung für den Zeitpunkt der Backups.
3. Erstellen Sie eine Aufbewahrungs-Policy, um die Aufbewahrungsdauer der Backups im System festzulegen.
4. Erstellen Sie für die Backups eine Gruppe.
    a. Zuweisen eines neuen Dataset zur neuen Gruppe
    b. Zuweisen einer Planung zur neuen Gruppe
    c. Zuweisen einer Aufbewahrungs-Policy zur neuen Gruppe
    d. Zuweisen von einem oder mehreren Clients zur neuen Gruppe
5. Aktivieren Sie die Planung für die Gruppe.

Datasets

Wenn Sie ein On-Demand-Backup durchführen, sind die in einem Clientdateisystem für das Backup ausgewählten Verzeichnisse und Dateien nur für dieses Backup gültig. Sie werden also nicht für zukünftige Backups gespeichert. Ein Avamar-Dataset ist eine Liste aus Verzeichnissen und Dateien, die von einem Client gesichert werden soll. Wenn Sie ein Dataset einem Client oder einer Gruppe zuweisen, können Sie die Auswahl für das Backup speichern.

Jedes Dataset definiert:

- Liste der Quelldaten
- Ausschlussliste
- Einschlussliste
- Plug-in-Optionen

Liste der Quelldaten
Definitionen von Datasets beginnen mit einer Liste der Quelldaten, die aus folgenden Elementen besteht:

- Daten aus einem oder mehreren Plug-ins
- Eine definierte Dateisystemhierarchie – entweder das gesamte Dateisystem oder ausgewählte Verzeichnisse – innerhalb der einzelnen Plug-ins

Ausschluss- und Einschlusslisten
Datasets können den Umfang der Quelldatenliste beschränken, indem explizit bestimmte Verzeichnisse und Dateitypen festgelegt werden, die für das Backup aus- bzw. eingeschlossen werden sollen.

Da standardmäßig alle Elemente in der Quelldatenliste des Dataset eingeschlossen sind, enthalten die expliziten Ausschluss- und Einschlusslisten in der Regel nur wenige Einträge.

Bei der Festlegung von Ausschluss- und Einschlusslisten variiert die Groß- und Kleinschreibung je nach Ziel-Computing-Plattform für das Backup. Bei Ausschluss- und Einschlusslisten für Windows-Plattformen muss die Groß- und Kleinschreibung nicht beachtet werden, bei Listen für die meisten anderen Plattformen dagegen schon.

HINWEIS

Sie können keine Einschluss- und Ausschlusslisten für mehrere Plug-ins definieren, einschließlich des Exchange VSS-Plug-ins, des SharePoint VSS-Plug-ins und des VMware-Image-Backup-Plug-ins.

Verarbeitungsbeziehung

Avamar verarbeitet diese Dataset-Elemente in der folgenden Reihenfolge:

1. **Source data** – Quelldaten aus einem oder mehreren Plug-ins sind definiert. Standardmäßig werden alle Daten aus allen definierten Plug-ins eingeschlossen.
2. **Exclusion list** – Anschließend wird die Ausschlussliste verwendet, um bestimmte Verzeichnisse und Dateitypen aus dem Dataset auszuschließen.
3. **Inclusion list** – Die Einschlussliste wird letztlich verwendet, um alle Dateien, die in der Ausschlussliste aus dem Dataset ausgeschlossen wurden, wieder hinzuzufügen.

Plug-in-Optionen

Mit Plug-in-Optionen haben Sie die Möglichkeit, das Verhalten eines Dataset weiter anzupassen. Im Benutzerhandbuch der einzelnen Plug-ins finden Sie Details zu den verfügbaren Optionen für das Plug-in.

Dataset-Katalog

Das Avamar-System beinhaltet standardmäßig einen Satz von vorkonfigurierten Datasets. Sie können diese Datasets für geplante Backups von Clients verwenden oder ein benutzerspezifisches Dataset erstellen.

Basis-Dataset

Das Basis-Dataset definiert die Mindest- oder Baselineanforderungen für Backups. Die Anfangseinstellungen des Basis-Dataset sind:

- Keine Quelldaten-Plug-ins
- Keine expliziten Ausschluss- oder Einschlusslisteneinträge

Im Grunde handelt es sich um ein leeres Dataset.

Standard-Dataset

Das Standard-Dataset definiert die dauerhafte Backupauswahl für die Standardgruppe. Die Anfangseinstellungen des Standard-Dataset sind:

- Alle verfügbaren Quelldaten-Plug-ins
- Keine expliziten Ausschluss- oder Einschlusslisteneinträge

Dies ermöglicht, dass alle Mitglieder der Standardgruppe ihre Clientcomputer ungeachtet des Plattformtyps sichern können.

Wenn Sie diese Einstellungen bearbeiten, werden die Änderungen für alle Mitglieder der Standardgruppe durchgesetzt, es sei denn, Sie setzen die Gruppeneinstellungen außer Kraft und weisen ein anderes Dataset auf Clientebene zu.

Die Verzeichnisse in der folgenden Tabelle sind auch prinzipiell von allen Backups ausgeschlossen, auch wenn sie nicht explizit in der Ausschlussliste angezeigt werden.

Tabelle 26 Von Standard-Dataset-Backups ausgeschlossene Verzeichnisse

Ausschluss	Beschreibung
`.snapshot/`	NetApp-Mounts

Tabelle 26 Von Standard-Dataset-Backups ausgeschlossene Verzeichnisse (Fortsetzung)

Ausschluss	Beschreibung
VARDIR/f_cache.dat	Lokaler avtar-Dateicache
VARDIR/p_cache.dat	Lokaler vorhandener avtar-Cache

UNIX-Dataset

Das UNIX-Dataset ist für die Verwendung mit AIX-, FreeBSD-, HP-UX-, Linux- und Solaris-Clients optimiert. Die Anfangseinstellungen des UNIX-Dataset sind:

- Nur die Quelldaten-Plug-ins aus AIX-, FreeBSD-, HP-UX-, Linux-, Macintosh OS X- und Solaris-Dateisystemen
- Expliziter Ausschluss von verschiedenen temporären Verzeichnissen (/tmp, /var/tmp, /usr/tmp), wichtigen Speicherauszugsdateien (core) und lokalen Cachedateien (*cache.dat, *scan.dat)
- Keine expliziten Einschlusslisteneinträge

Die Verzeichnisse in der folgenden Tabelle sind auch prinzipiell von allen UNIX-Dataset-Backups ausgeschlossen, auch wenn sie nicht explizit in der Ausschlussliste angezeigt werden.

Tabelle 27 Von UNIX-Dataset-Backups ausgeschlossene Verzeichnisse

Ausschluss	Beschreibung
.snapshot/	NetApp-Mounts
VARDIR/f_cache.dat	Lokale avtar-Cachedateien
VARDIR/p_cache.dat	Lokale avtar-Cachedateien
/proc	Nicht wiederherstellbares Pseudo-Dateisystem
/dev	Wird nur ausgeschlossen, wenn nicht als Root ausgeführt
/devices	Nur für Solaris ausgeschlossen

Windows-Dataset

Das Windows-Dataset ist für die Verwendung mit Microsoft Windows-Clients optimiert. Die Anfangseinstellungen des Windows-Dataset sind:

- Nur Quelldaten-Plug-in des Windows-Dateisystems
- Keine expliziten Ausschluss- oder Einschlusslisteneinträge

Die Verzeichnisse in der folgenden Tabelle sind auch prinzipiell von allen Windows-Dataset-Backups ausgeschlossen, auch wenn sie nicht explizit in der Ausschlussliste angezeigt werden.

Tabelle 28 Von Windows-Dataset-Backups ausgeschlossene Verzeichnisse

Ausschluss	Beschreibung
.snapshot/	NetApp-Mounts
VARDIR/f_cache.dat	Lokale avtar-Cachedateien

Tabelle 28 Von Windows-Dataset-Backups ausgeschlossene Verzeichnisse (Fortsetzung)

Ausschluss	Beschreibung
`VARDIR/p_cache.dat`	Lokale `avtar`-Cachedateien
Alle Dateien, auf die die folgenden Registrierungsschlüssel verweisen: • `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup` • `HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`	Dateien, die von Microsoft explizit von Backups ausgeschlossen wurden
Temporäre Internetdateien	Temporäre Dateien des Internet Explorer
`outlook.ost`	Lokale Outlook-Cachedateien
`outlook\*.ost`	Lokale Outlook-Cachedateien

VMware Image Dataset

Das VMware Image Dataset ist das Standard-Dataset zum Schutz von VMware-Entitäten mit Image-Backup. Das VMware Image Dataset ist in vielerlei Hinsicht einfacher als der Großteil der anderen Datasets:

- Die einzigen verfügbaren Quelldaten-Plug-ins sind virtuelle Linux- und Windows-Laufwerke. Beide werden standardmäßig ausgewählt.
- Die Option **Select Files and/or Folders** sowie die Registerkarten **Exclusions** und **Inclusions** sind deaktiviert.
- Change Block Tracking ist standardmäßig aktiviert. Dazu wird eine integrierte Plug-in-Optionsanweisung (`utilize_changed_block_list=true`) verwendet.

Im *Avamar for VMware – Benutzerhandbuch* erfahren Sie weitere Details zur Verwendung von VMware Image Dataset zur Sicherung von VMware-Entitäten.

Erstellen eines Dataset

Hinweis

Wenn der Avamar-Server Data Domain als Back-end-Speicher verwendet, ist das Data Domain-System der Standardspeicherort für Backups. Dieses System kann auf der Registerkarte **Options** geändert werden.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Datasets** aus.
   Das Fenster **Manage All Datasets** wird angezeigt.
2. Klicken Sie auf **New**.
   Das Dialogfeld **New Dataset** wird angezeigt.
3. Geben Sie im Feld **Name** einen Namen für das Dataset ein.
   Der Name kann alphanumerischen Zeichen (A-Z, a-z, 0-9) sowie folgende Sonderzeichen beinhalten: Punkte (.), Gedankenstriche (-) und Unterstriche

(_). Verwenden Sie keine Unicode-Zeichen oder folgende Sonderzeichen: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?

4. Klicken Sie auf die Registerkarte **Source Data** und definieren Sie die Quelldaten-Plug-ins, aus denen die Daten für dieses Dataset bezogen werden.

Option	Beschreibung
Einbeziehen von Daten aller Plug-ins auf dem Client	Wählen Sie **Select All Data for All Local File Systems** aus.
Nur Einbeziehen von Daten eines bestimmten Plug-ins und Beschränken des Dataset auf bestimmte Daten	a. Wählen Sie **Enter Explicitly** aus. b. Wählen Sie aus der Liste **Select Plug-In Type** das für die Backups zu verwendende Plug-in aus. Weitere Optionen werden gegebenenfalls unter der Liste **Select Plug-In Type** angezeigt. c. Um alle verfügbaren Daten mit dem Plug-in zu sichern, wählen Sie die Option aus oder wählen Sie **Select Files and/or Folders** aus und navigieren Sie dann zu den in die Backups einzuschließenden Daten. **Hinweis** Sie können auch den Pfad zu den zu sichernden Daten eingeben. Eingeben des Datenpfads für ein Dataset auf Seite 113 enthält Anweisungen für die Eingabe des Pfads.

5. Klicken Sie auf die Registerkarte **Exclusions** und legen Sie anschließend die vom Dataset auszuschließenden Daten fest:
   a. Wählen Sie aus der Liste **Select Plug-in Type** das Plug-in aus, das Sie für die Backups verwenden.
   b. Geben Sie den Pfad zu den auszuschließenden Daten ein oder klicken Sie auf **...**, um zu den Daten zu navigieren.
   c. Klicken Sie auf **+**.
   d. Wiederholen Sie diese Schritte für jeden aus den Backups auszuschließenden Datenpfad.

   Ausschlusslisten enthalten in der Regel /temp-Dateien und Verzeichnisse und UNIX-Core-Speicherauszugsdateien.

6. Klicken Sie auf die Registerkarte **Inclusions** und legen Sie dann die in das Dataset einzuschließenden Daten fest, die andernfalls je nach Auswahl in der Registerkarte **Exclusions** ausgeschlossen werden würden:
   a. Wählen Sie aus der Liste **Select Plug-in Type** das Plug-in aus, das Sie für die Backups verwenden.
   b. Geben Sie den Pfad zu den einzuschließenden Daten ein oder klicken Sie auf **...**, um zu den Daten zu navigieren.
   c. Klicken Sie auf **+**.
   d. Wiederholen Sie diese Schritte für jeden in die Backups einzuschließenden Datenpfad.

7. Klicken Sie auf die Registerkarte **Options** und stellen Sie verschiedene Plug-in-Optionen ein, indem Sie entweder grafische Steuerungen nutzen oder Optionsnamen und Werte als Texteinträge eingeben.

   Im Benutzerhandbuch der einzelnen Plug-ins finden Sie Details zu den verfügbaren Optionen.

8. Klicken Sie auf **OK**.

Eingeben des Datenpfads für ein Dataset

Sie können geplante Backups auf einen Satz von Daten beschränken, indem Sie den Pfad zu den Daten im Dataset angeben. Hierzu können Sie zu den Daten navigieren oder den Pfad zu den Daten eingeben. Für die Eingabe des Pfads gelten verschiedene Regeln.

Platzhalter
Wenn Sie ein Dateisystem-Plug-in verwenden, wird das erste Vorkommen eines Sternchens (*) in einem Pfad als Ordnerplatzhalter behandelt. Zur Angabe des Ordners `My Documents` für alle Benutzer auf einem Windows-Computer beispielsweise geben Sie **`C:\Dokumente und Einstellungen\*\Eigene Dokumente`** ein. Zur Angabe des Ordners `Documents` für alle Benutzer auf einem Macintosh geben Sie **`/Benutzer/*/Dokumente`** ein.

HINWEIS

Bei der Angabe eines Datenpfads wird nur das erste Vorkommen eines Sternchens als Platzhalter für einen Ordner behandelt. Nachfolgende Vorkommen werden buchstäblich interpretiert.

Unterstützte Zeichen im Datenpfad
Der Pfad kann alphanumerische Zeichen (A-Z, a-z, 0-9) und ein Sternchen (*) als Platzhalter beinhalten. Der Datenpfad darf keines der folgenden Zeichen enthalten: `~ ! @ $ ^ % ( ) { } [ ] | , ` ; # : * ? < > ' " & .`

Bearbeiten eines Dataset

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Datasets** aus.

   Das Fenster **Manage All Datasets** wird angezeigt.

2. Wählen Sie ein Dataset aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Dataset** wird angezeigt.

3. Bearbeiten Sie die Dataset-Einstellungen.
4. Klicken Sie auf **OK**.

   Dataset-Änderungen wirken sich auf das nächste geplante Backup aus. Backups, die bereits begonnen haben oder abgeschlossen sind, werden nicht beeinflusst.

Kopieren eines Dataset

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Datasets** aus.

   Das Fenster **Manage All Datasets** wird angezeigt.

2. Wählen Sie das Dataset aus und klicken Sie auf **Copy**.

Das Dialogfeld **Save As** wird angezeigt.

3. Geben Sie einen Namen für das neue Dataset ein und klicken Sie auf **OK**.

Löschen eines Dataset

Bevor Sie beginnen

Vergewissern Sie sich, dass das Dataset aktuell keinem Client und keiner Gruppe zugewiesen ist. Andernfalls kann das Dataset nicht gelöscht werden.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Datasets** aus.

   Das Fenster **Manage All Datasets** wird angezeigt.
2. Wählen Sie das Dataset aus und klicken Sie auf **Delete**.
3. Klicken Sie in der Bestätigungsmeldung auf **Yes**.

Planungen

Planungen sind wiederverwendbare Objekte, die steuern, wann Gruppenbackups, E-Mail-Benachrichtigungen zu benutzerspezifischen Ereignisprofilen und Policy-basierte Replikationen stattfinden.

Planungstypen

Sie können eine Avamar-Planung konfigurieren, um eine Systemaktivität in einem der Intervalle in der folgenden Tabelle zu wiederholen.

Tabelle 29 Planungstypen

Planungstyp	Beschreibung
Daily	Wiederholt eine Systemaktivität täglich einmal oder mehrmals. Bei täglichen Planungen müssen Sie außerdem die Dauer der Aktivität begrenzen, um Jobüberschneidungen zu vermeiden.
Wöchentlich	Wiederholt eine Systemaktivität wöchentlich an einem oder mehreren Tagen der Woche. Bei wöchentlichen Planungen müssen Sie außerdem die früheste Startzeit der Aktivität und den Zeitpunkt definieren, an dem die Aktivität gestoppt wird, auch wenn sie noch ausgeführt wird.
Monthly	Wiederholt eine Systemaktivität zu einem bestimmten Kalenderdatum oder an einem ausgewiesenen Wochentag jeden Monat, z. B. an jedem ersten Sonntag des Monats. Bei monatlichen Planungen müssen Sie außerdem die früheste Startzeit der Aktivität und den Zeitpunkt definieren, an dem die Aktivität gestoppt wird, auch wenn sie noch ausgeführt wird.
On-demand	Definiert eine Planung, die nicht automatisch ausgeführt wird. Diese Option ist nützlich zum Einrichten von Planungen, die Sie bereits

Tabelle 29 Planungstypen (Fortsetzung)

Planungstyp	Beschreibung
	heute zuweisen, aber in der Zukunft aktivieren können. Außerdem eignet sich diese Option zum Erstellen von Planungen, die Gruppen zugewiesen werden, die nur On-Demand-Backups durchführen (beispielsweise Gruppen, die nur Laptop-Clients enthalten).

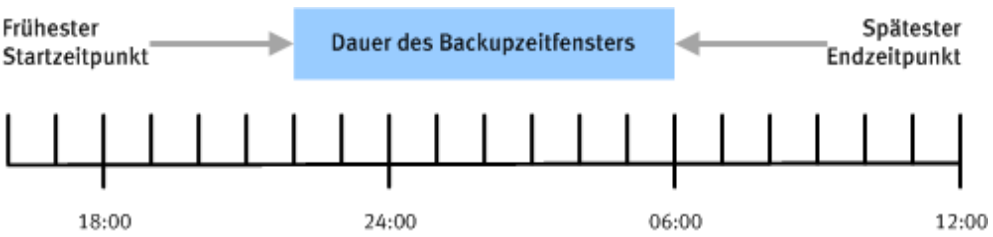
Planen von Startzeit, Endzeit und Dauer

Wenn Sie eine Planung erstellen, geben Sie außerdem an, wann die Planung in Kraft tritt und wann sie unterbrochen wird. Angenommen, Sie wissen, dass die für ein bestimmtes Entwicklungsprojekt verwendeten Clientcomputer an einem bestimmten Termin in der Zukunft überflüssig werden. Sie können eine Planung für diese Gruppenbackups erstellen, durch den die Backuperstellung automatisch an einem bestimmten Datum eingestellt wird. Und wenn Sie einen großen Standort verwalten, können Sie im Vorfeld Planungen erstellen, diese anschließend Gruppen zuweisen und zu einem bestimmten Zeitpunkt aktivieren. Diese Gruppenbackups werden erst ausgeführt, wenn die Planung in Kraft tritt.

Da sich geplante Aktivitäten oftmals über zwei Kalendertage erstrecken, ist es wichtig zu wissen, dass Avamar das vollständige Zeitfenster allen Aktivitäten zuweist, die durch eine Planung gestartet werden. Stellen Sie sich z. B. eine Planung vor, die frühestens um 22 Uhr beginnt, spätestens um 6 Uhr (am Folgemorgen) endet und nach dem 31. Dezember des aktuellen Kalenderjahrs beendet wird. Am Abend des 31. Dezembers wird die Aktivität wie geplant gestartet und bis zum Abschluss – in der Regel am Morgen des 1. Januars des folgenden Jahrs – durchgeführt. Ab 1. Januar werden jedoch keine neuen geplanten Aktivitäten gestartet.

Die folgende Abbildung illustriert, wie die Startzeit, Endzeit und Dauer einer Planung bei der Verwendung der Anfangseinstellungen der Standardplanung miteinander interagieren.

Abbildung 10 Planen von Startzeit, Endzeit und Dauer



Diese Systemaktivität beginnt um 22:00 Uhr und kann bis 6:00 Uhr des nächsten Tages ausgeführt werden, sodass sie effektiv 8 Stunden dauert.

In der Praxis starten und enden geplante Aktivitäten selten pünktlich. Die Serverlast wirkt sich auf die tatsächlichen Startzeiten aus und die Komplexität wirkt sich auf die tatsächlichen Endzeiten aus. Die Komplexität der Aktivität umfasst die Menge der neuen Clientdaten, die gesichert werden müssen, die Anzahl der gestarteten Gruppenbackups und die Anzahl der zu sendenden E-Mail-Nachrichten.

Eine für eine Planung festgelegte Startzeit wird als der früheste Zeitpunkt festgelegt, an dem die Systemaktivität beginnen kann. Die festgelegte Dauer oder Endzeit in der Planung bezeichnet zudem den spätestmöglichen Zeitpunkt für die Systemaktivität.

Zeitzonen der Planung
Wenn Sie Planungen erstellen oder bearbeiten, werden alle Zeitangaben im Verhältnis zur lokalen Zeitzone für den Avamar Administrator-Client angezeigt. Angenommen, Sie erstellen eine Planung in der PST-Zeitzone (Pacific Standard Time) mit einer nächsten Laufzeit um 22:00 Uhr. Die nächste Laufzeit für die Planung für einen Administratorbenutzer in der EST-Zeitzone (Eastern Standard Time) wird als 01:00 Uhr am nächsten Tag (3 Stunden später) angezeigt.

Planungskatalog

Das Avamar-System beinhaltet standardmäßig einen Satz vorkonfigurierter Planungen. Sie können diese Planungen verwenden oder eine benutzerspezifische Planung erstellen.

Die folgenden Planungen sind standardmäßig verfügbar.

Tabelle 30 Planungskatalog

Planungsname	Beschreibung
Default Schedule	Steuert die Backupplanung für die Standardgruppe. Sie ist anfänglich so konfiguriert, dass sie täglich um 22:00 Uhr ausgeführt wird. Wenn Sie diese Einstellungen bearbeiten, werden die Änderungen für alle Mitglieder der Standardgruppe vorgenommen.
Default Replication	Steuert Replikation für Replikationsgruppen.
Daily Schedule	Avamar beinhaltet eine vordefinierte tägliche Planung.
Evaluation Schedule	Steuert, wann eine E-Mail-Benachrichtigung zum Evaluierungsprofil gesendet wird. Sie ist anfänglich so konfiguriert, dass sie jeden Montag um 6 Uhr ausgeführt wird.
Notification Schedule	Steuert, wann E-Mail-Benachrichtigungen zu einem benutzerspezifischen Ereignisprofil gesendet werden.
Override Daily Schedule	Definiert die verfügbaren Startzeiten für Clients, bei denen die Einstellung **Override group schedules** aktiviert ist. Diese Planung kann bearbeitet werden. Kopien dieser Planung werden nicht mit der Einstellung **Override group schedules** verwendet.
Statistics Schedule	Steuert, wie oft verschiedene Avamar-Serverstatistiken (z. B. der Avamar-Serverdetailwert **Bytes protected**) abgerufen oder berechnet werden. Die Standardeinstellung für diese Planung ist hourly.
Usage Intelligence Schedule	Steuert, wie oft der Avamar-Server Berichtsinformationen erfasst und über das

Tabelle 30 Planungskatalog (Fortsetzung)

Planungsname	Beschreibung
	ESRS-Gateway an den Avamar-Support überträgt.

Erstellen einer Planung

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.

   Das Fenster **Manage All Schedules** wird angezeigt.
2. Klicken Sie auf **New**.

   Das Dialogfeld **New Schedule** wird angezeigt.
3. Geben Sie im Feld **Name** einen Namen für die Planung ein.

   Der Name darf keines der folgenden Zeichen enthalten: `~!@$^%(){}[]|,`;# \/:*?<>'"&`.
4. Wählen Sie im Abschnitt **Repeat this schedule** den Planungstyp aus:
   - **Daily**
   - **Wöchentlich**
   - **Monthly**
   - **On-Demand**
5. Geben Sie die Planungseinstellungen an.
6. Achten Sie darauf, dass das Datum und die Uhrzeit neben der Option **Next Run Time** im oberen Bereich des Dialogfelds **New Schedule** korrekt sind.
7. Klicken Sie auf **OK**.

Planungseinstellungen

In der folgenden Tabelle sind die Planungseinstellungen beschrieben.

Tabelle 31 Einstellungen für jeden Planungstyp

Planungstyp	Einstellungen
Daily	1. Verwenden Sie die Listen **Select Daily Times**, um die Tageszeit anzugeben, zu der die Planung ausgeführt werden soll, und klicken Sie anschließend auf **Add**, um die Zeit zur Liste „Scheduled Times“ hinzuzufügen. 2. Wiederholen Sie diese Schritte für jeden Zeitpunkt, an dem die Planung an den einzelnen Tagen ausgeführt werden soll. 3. (Optional) Um einen Zeitpunkt aus der Liste **Scheduled Times** zu entfernen,

Tabelle 31 Einstellungen für jeden Planungstyp (Fortsetzung)

Planungstyp	Einstellungen
	wählen Sie den Zeitpunkt aus und klicken Sie auf **Remove**. 4. Um Jobüberschneidungen zu vermeiden, begrenzen Sie die Dauer von geplanten Systemaktivitäten, indem Sie eine Zeitbegrenzung aus der Liste **Limit each run to (hours)** auswählen. 5. Wählen Sie in der Liste **Delay until** das Datum aus, an dem die Planung in Kraft treten soll. Wählen Sie das aktuelle Datum in der Liste aus, wenn die Planung sofort in Kraft treten soll. 6. Wählen Sie aus, wann die Planung unterbrochen werden soll: • Wenn eine Planung unbegrenzt fortgesetzt werden soll, wählen Sie **No End Date** aus. • Um eine Planung an einem bestimmten Datum zu unterbrechen, wählen Sie **End after** und anschließend ein Datum aus der Liste aus.
Wöchentlich	1. Aktivieren Sie das Kontrollkästchen neben den Wochentagen, an denen die Planung ausgeführt werden soll. 2. Legen Sie die Dauer der Aktivität über die Felder **Earliest start time** und **End no later than** fest. Sie können die Zeiten eingeben oder die Zeit auswählen und mithilfe der Pfeiltasten ändern. Die Arbeitslast des Servers beeinflusst die Startzeit einer Aktivität. Wird ein Backup zum ersten Mal für einen Client durchgeführt, ist es außerdem zulässig, das Backup über die angegebene Endzeit hinaus auszuführen. Dieses Verhalten ist zulässig, da erste Backups erheblich länger dauern können als nachfolgende Backups für denselben Client. 3. Wählen Sie in der Liste **Delay until** das Datum aus, an dem die Planung in Kraft treten soll. Wählen Sie das aktuelle Datum in der Liste aus, wenn die Planung sofort in Kraft treten soll. 4. Wählen Sie aus, wann die Planung unterbrochen werden soll:

Tabelle 31 Einstellungen für jeden Planungstyp (Fortsetzung)

Planungstyp	Einstellungen
	• Wenn eine Planung unbegrenzt fortgesetzt werden soll, wählen Sie **No End Date** aus. • Um eine Planung an einem bestimmten Datum zu unterbrechen, wählen Sie **End after** und anschließend ein Datum aus der Liste aus.
Monthly	1. Wählen Sie, ob die Aktivität an einem bestimmten Kalenderdatum oder an einem ausgewiesenen Wochentag jeden Monat wiederholt wird: • Um die Aktivität an einem bestimmten Kalenderdatum zu wiederholen, wählen Sie die Option **Day of every month** und anschließend in der Liste den entsprechenden Tag aus. • Um die Aktivität an einem ausgewiesenen Wochentag jeden Monat zu wiederholen, wählen Sie die Option **The ... of every month** und anschließend in der Liste den entsprechenden Tag aus. 2. Legen Sie die Dauer der Aktivität über die Felder **Earliest start time** und **End no later than** fest. Sie können die Zeiten eingeben oder die Zeit auswählen und mithilfe der Pfeiltasten ändern. Die Arbeitslast des Servers beeinflusst die Startzeit einer Aktivität. Wird ein Backup zum ersten Mal für einen Client durchgeführt, ist es außerdem zulässig, das Backup über die angegebene Endzeit hinaus auszuführen. Dieses Verhalten ist zulässig, da erste Backups erheblich länger dauern können als nachfolgende Backups für denselben Client. 3. Wählen Sie in der Liste **Delay until** das Datum aus, an dem die Planung in Kraft treten soll. Wählen Sie das aktuelle Datum in der Liste aus, wenn die Planung sofort in Kraft treten soll. 4. Wählen Sie aus, wann die Planung unterbrochen werden soll:

Tabelle 31 Einstellungen für jeden Planungstyp (Fortsetzung)

Planungstyp	Einstellungen
	• Wenn eine Planung unbegrenzt fortgesetzt werden soll, wählen Sie **No End Date** aus. • Um eine Planung an einem bestimmten Datum zu unterbrechen, wählen Sie **End after** und anschließend ein Datum aus der Liste aus.
On-demand	Es sind keine weiteren Einstellungen für On-Demand-Planungen vorhanden.

Bearbeiten einer Planung

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.

   Das Fenster **Manage All Schedules** wird angezeigt.
2. Wählen Sie eine Planung aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Schedule** wird angezeigt.
3. Bearbeiten Sie die Planungseinstellungen.
4. Klicken Sie auf **OK**.

Bearbeiten der Startzeiten für Clientaußerkraftsetzungen von Gruppenplanungen

Wenn Sie Benutzern das Außerkraftsetzen von Gruppenbackupplänen über die Webbenutzeroberfläche erlauben, müssen Sie die verfügbaren, für Clients zu verwendenden Startzeiten konfigurieren. Zur Konfiguration der Startzeiten fügen Sie der Option „Override Daily Schedule“ Zeiteinträge hinzu.

Der Zugriff auf die Webbenutzeroberfläche ist Teil der erweiterten Funktionen für Enterprise-Desktop- und -Laptopcomputer.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.

   Das Fenster **Manage All Schedules** wird angezeigt.
2. Wählen Sie aus der Liste der Planungen die Option **Override Daily Schedule** aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Schedule** wird angezeigt.
3. Verwenden Sie die Listen **Select Daily Times**, um eine Tageszeit anzugeben, die der für Benutzer auf der Webbenutzeroberfläche verfügbaren Auswahlliste hinzugefügt wird, und klicken Sie anschließend auf **Add**, um die Zeit zur Liste **Scheduled Times** hinzuzufügen.

   Um einen Zeitpunkt aus der Liste **Scheduled Times** zu entfernen, wählen Sie den Zeitpunkt aus und klicken Sie auf **Remove**.

4. Wiederholen Sie diese Schritte, um Zeiteinträge der für Benutzer verfügbaren Auswahlliste hinzuzufügen.
5. Begrenzen Sie die Dauer der geplanten Systemaktivitäten, um Jobüberschneidungen zu vermeiden, indem Sie eine Zeitbegrenzung aus der Liste **Limit each run to (hours)** auswählen.
6. Klicken Sie auf **OK**.

Kopieren einer Planung

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.

   Das Fenster **Manage All Schedules** wird angezeigt.
2. Wählen Sie die Planung aus und klicken Sie auf **Copy**.

   Das Dialogfeld **Save As** wird angezeigt.
3. Geben Sie einen Namen für die neue Planung ein und klicken Sie auf **OK**.

Ausführen einer On-Demand-Planung

Sie können geplante Vorgänge auf einer On-Demand-Basis sofort initiieren. Der Planer muss nicht ausgeführt werden, wenn Sie eine On-Demand-Planung ausführen.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.

   Das Fenster **Manage All Schedules** wird angezeigt.
2. Wählen Sie eine Planung aus und klicken Sie auf **Run Now**.

Löschen einer Planung

Bevor Sie beginnen

Vergewissern Sie sich, dass die Planung aktuell keiner Gruppe zugewiesen ist. Andernfalls kann die Planung nicht gelöscht werden.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.

   Das Fenster **Manage All Schedules** wird angezeigt.
2. Wählen Sie die Planung aus und klicken Sie auf **Delete**.
3. Klicken Sie in der Bestätigungsmeldung auf **Yes**.

Regeln

Regeln werden vom Avamar-Server für Domain-Zuordnung und automatische Backup-Policy-Zuweisung für automatisch erkannt VMs verwendet.

Weitere Informationen zu Regeln finden Sie im *Avamar for VMware – Benutzerhandbuch*

Erstellen einer Regel

Regeln werden verwendet, um automatisch VMs, die automatisch erkannt wurden, Domains zuzuordnen und den automatisch erkannten VMs automatisch Backup-

Policies zuzuweisen. Die Regeln verwenden eine oder mehrere Filtermethoden, um festzustellen, ob die VMs sich unter der Regel qualifizieren.

Es gibt drei Möglichkeiten, das Dialogfeld **New Rules** zu öffnen:

- Indem Sie während der vCenter-Clientkonfiguration erst **Enable dynamic VM import by rule** und dann **New Rule...** aus der Drop-down-Liste **Rule** in der Liste **Domain Mapping** auswählen.

  Hinweis

  Um stillgelegte virtuelle Maschinen zurück auf den Avamar-Server mit dynamischen Regel zu importieren, führen Sie die folgenden Schritte aus:

  1. Bearbeiten Sie das folgende Skript:
     `f/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml`
     `<entry key="auto_discover_retired_vms" value="true" />`
  2. Starten Sie den Management Console Server (MCS) neu.

- Wählen Sie während der Gruppenkonfiguration auf der Seite **Include clients** des Assistenten **Enable automatic group selection by rule** aus und dann **New Rule...** im Drop-down-Menü.
- Durch die Auswahl von **Tools** > **Manage Rules** unter Avamar-Administrator und dann Klicken auf **New**.

Vorgehensweise

1. Öffnen Sie das Dialogfeld **New Rules**, indem Sie eine der aufgeführten Methoden verwenden.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie im Bereich **Rule Definition**, ob eine Regel **Any** der gelisteten Filtermechanismen entsprechen soll oder **All**.

   Mit dieser Auswahl können Sie mehrere verschiedene Filter konfigurieren, um virtuelle Maschinen auszuwählen und zu bestimmen, wie diese Filter miteinander interagieren, um die korrekten VMs auszuwählen. Beispielsweise können Sie einen Filter erstellen, der einen VM-Ordnerpfad verwendet, um virtuelle Maschinen auszuwählen und einen anderen Filter, der eine VM-Benennungskonvention verwendet. Diese Option kann dann wie folgt verwendet werden, um zu bestimmen, welche VMs nach dieser Regel enthalten sind:

   - Um nur VMs einzuschließen, die sich unter dem definierten Ordnerpfad befinden und ebenfalls der Benennungskonvention folgen, wählen Sie **All**. Dieser Schritt schließt VMs aus, die sich unter dem Ordnerpfad befinden, jedoch nicht der Benennungskonvention folgen. Außerdem ausgeschlossen sind VMs, die der Benennungskonvention folgen, sich jedoch nicht unter dem Ordnerpfad befinden.
   - Um sämtliche VMs einzuschließen, die sich entweder unter dem VM-Ordnerpfad befinden oder der Benennungskonvention folgen, können Sie alternativ **Any** auswählen.

4. Gehen Sie für den ersten Filter wie folgt vor:

   a. Wählen Sie den Dateityp aus.

      Wählen Sie beispielsweise zum Erstellen eines Filters, der eine VM-Benennungskonvention verwendet, **VM Name** aus, oder **VM Tag**, um einen Filter zu erstellen, der ein vCenter-VM-Tag verwendet.

Hinweis

Die Auswahl **VM Tag** ist nur in vCenter 6.0 und höher verfügbar.

b. Wählen Sie den Operanden.

Wenn beispielsweise **VM Name** für den Filtertyp und **begins with** für den Operanden ausgewählt ist, werden alle VMs ausgewählt, deren Name mit dem ausgewählten Filtertext beginnt.

c. Geben Sie den Filtertext ein.

Um beispielsweise einen Filter zu erstellen, der alle VMs wählt, deren Name mit der Textzeichenfolge `HR_` beginnt, wählen Sie **VM Name** als Filtertyp, **begins with** für den Operanden und geben Sie `HR_` als Filtertext ein.

5. Um zusätzliche Filter zu erstellen, klicken Sie auf das Pluszeichen (**+**).

Dieser Schritt fügt eine Zeile zur Filterliste hinzu. Um eine vorhandene Zeile zu löschen, klicken Sie auf das Minuszeichen (**-**).

6. Klicken Sie auf **OK**.

Änderungen an Tags werden erst nach einer Verzögerung wirksam. Nach 12 Stunden werden sie erzwungen. Aus diesem Grund sollten Sie Tags mit Vorsicht bearbeiten oder einen synchronisierten vCenter-Vorgang ausführen, der automatisch vCenter mit dem Avamar-Server synchronisiert.
Best Practice für die Regelerstellung ist es, sicherzustellen, dass die Regeln sich gegenseitig ausschließen, um zu vermeiden, dass sich eine VM unter mehrere Regeln qualifiziert.

Bearbeiten einer Regel

Vorgehensweise

1. Wählen Sie in Avamar-Administrator **Tools** > **Manage Rules** aus.

   Das Fenster **Manage All Rules** wird angezeigt.
2. Wählen Sie eine Regel aus und klicken Sie auf **Bearbeiten**.
3. Nehmen Sie alle notwendigen Änderungen vor und klicken Sie auf **Close**.

Löschen einer Regel

Vorgehensweise

1. Wählen Sie in Avamar-Administrator **Tools** > **Manage Rules** aus.

   Das Fenster **Manage All Rules** wird angezeigt.
2. Wählen Sie eine Regel aus und klicken Sie auf **Delete**.
3. Klicken Sie in der Bestätigungsmeldung auf **Yes**.

Aufbewahrungs-Policies

Mithilfe von Backupaufbewahrungs-Policies kann festgelegt werden, wie lange ein Backup im System aufbewahrt wird.

Eine Aufbewahrungs-Policy wird jedem Backup während des Backupvorgangs zugewiesen. Geben Sie eine benutzerdefinierte Aufbewahrungs-Policy an, wenn Sie ein Backup nach Bedarf durchführen, oder erstellen Sie eine Aufbewahrungs-Policy,

die während eines geplanten Backups automatisch einer Gruppe von Clients zugewiesen wird.

Wenn die Aufbewahrungsfrist für ein Backup abläuft, wird das Backup automatisch zum Löschen markiert. Das Löschen erfolgt anschließend in Batches zu Zeiten mit geringen Systemaktivitäten.

Bei Bedarf können Sie die Aufbewahrungseinstellung für ein einzelnes Backup, das bereits stattgefunden hat, manuell ändern. Anweisungen finden Sie unter Ändern des Aufbewahrungstyps für ein Backup auf Seite 144. Wenn Sie eine konfigurierte Aufbewahrungs-Policy ändern, werden die Änderungen jedoch nur für Backups angewendet, die nach der Änderung stattfinden. Die Aufbewahrungseinstellung wird für bereits ausgeführte Backups beibehalten. Daher ist es wichtig, die beste Aufbewahrungs-Policy für einen Standort zu planen und zu implementieren, bevor zu viele Backups stattfinden.

Es gibt zwei Arten von Aufbewahrungseinstellungen:

- Grundlegende Aufbewahrungseinstellungen legen ein festes Ablaufdatum fest.
- Erweiterte Aufbewahrungseinstellungen legen die Anzahl der täglich, wöchentlich, monatlich und jährlich aufzubewahrenden Backups fest.

Grundlegende Aufbewahrungseinstellungen

Grundlegende Aufbewahrungseinstellungen werden verwendet, um einem Backup mit einer der Einstellungen in der folgenden Tabelle ein festes Ablaufdatum zuzuweisen.

Tabelle 32 Grundlegende Aufbewahrungseinstellungen

Aufbewahrungseinstellung	Beschreibung
Retention period	Definiert eine fixe Aufbewahrungsfrist in Tagen, Wochen, Monaten oder Jahren für die Zeit nach dem Backup. Beispielsweise können Sie festlegen, dass Backups nach 6 Monaten ablaufen.
End date	Weist ein Kalenderdatum als Ablaufdatum zu. Beispielsweise können Sie als Ablaufdatum für Backups den 31. Dezember 2014 angeben.
No end date	Bewahrt Backups auf unbestimmte Zeit auf. Diese Einstellung ist nützlich, wenn dafür gesorgt werden soll, dass alle dieser Aufbewahrungs-Policy zugewiesenen Backups während des gesamten Lebenszyklus des Systems aufbewahrt werden.

HINWEIS

Weisen Sie für Backups von 32-Bit-Windows- oder 32-Bit-Linux-Clientcomputern nicht eine Aufbewahrungsfrist für ein Datum nach dem 7. Februar 2106 zu. Wenn Sie einem 32-Bit-Windows-Client eine erweiterte Aufbewahrungsfrist zuweisen, wird das Backup mit Ausnahmen abgeschlossen. Die Backups für 32-Bit-Linux-Clients werden zwar abgeschlossen, jedoch nicht in Avamar-Administrator angezeigt.

Erweiterte Aufbewahrungseinstellungen

Mit erweiterten Aufbewahrungseinstellungen können Sie den Ablauf von Backups dynamisch zuweisen, indem Sie die Anzahl der täglichen Backups, wöchentlichen

Backups, monatlichen Backups und jährlichen Backups festlegen, die im System aufbewahrt werden sollen.

Einige geplante tägliche Backups werden automatisch einem erweiterten Aufbewahrungstyp zugewiesen:

- Das erste erfolgreich durchgeführte geplante Backup jedes Tages wird als das tägliche Backup ausgewiesen.
- Das erste erfolgreich durchgeführte geplante Backup jeder Woche wird als das wöchentliche Backup ausgewiesen.
- Das erste erfolgreich durchgeführte geplante Backup jedes Monats wird als das monatliche Backup ausgewiesen.
- Das erste erfolgreich durchgeführte geplante Backup jedes Jahres wird als das jährliche Backup ausgewiesen.

Um erweiterte Aufbewahrungstypen zuweisen zu können, beginnt jeder Tag um 00:00:01 GMT, jede Woche am Sonntag, jeder Monat am ersten Kalendertag des Monats und jedes Jahr am 1. Januar.

HINWEIS

Erweiterte Aufbewahrungseinstellungen können nicht auf On-Demand-Backups angewendet werden. On-Demand-Backups können jederzeit stattfinden und sind daher prinzipiell asynchron – das System kann sie nicht als tägliche, wöchentliche, monatliche oder jährliche Backups kennzeichnen.

Verwenden Sie geplante tägliche Backups mit Aufbewahrungs-Policies immer mit erweiterten Aufbewahrungseinstellungen. Die Einstellung **Always keep: n weeks of daily backups** wird erst aktiv, wenn im System tägliche Backups konfiguriert sind. Je nach verwendeter Planung sind tägliche Backups möglicherweise nicht im System. Wenn Sie z. B. eine Planung einer Gruppe zuweisen, für die nur wöchentliche Backups durchgeführt werden, sind für diese Gruppe keine täglichen Backups im System konfiguriert.

Katalog der Aufbewahrungs-Policies

Das Avamar-System beinhaltet standardmäßig einen Satz vorkonfigurierter Aufbewahrungs-Policies. Sie können diese Aufbewahrungs-Policies für geplante Backups von Clients verwenden oder eine benutzerspezifische Aufbewahrungs-Policy erstellen.

Die Aufbewahrungs-Policies in der folgenden Tabelle sind standardmäßig verfügbar.

Tabelle 33 Katalog der Aufbewahrungs-Policies

Name der Aufbewahrungs-Policy	Beschreibung
Minimal Retention	Ermöglicht Ihnen, die minimale grundlegende Aufbewahrungseinstellung für einen gesamten Standort durchzusetzen. Sie können z. B. alle Backups ungeachtet der sonstigen festgelegten Aufbewahrungs-Policies für mindestens 90 Tage aufbewahren. Diese Funktion richtet sich an große Unternehmen, die für den gesamten Standort minimale Aufbewahrungsstandards durchsetzen möchten, egal, welche Ziele einzelne Organisationen mit der Implementierung

Tabelle 33 Katalog der Aufbewahrungs-Policies (Fortsetzung)

Name der Aufbewahrungs-Policy	Beschreibung
	anderer Aufbewahrungs-Policies verfolgen. Die Policy „Minimal Retention“ ist ein globales Systemobjekt, das nur die minimale Aufbewahrungseinstellung steuert. Daher können Sie die Policy „Minimal Retention“ keiner Gruppe zuweisen.
Default Retention	Definiert Backupaufbewahrungseinstellungen für die Standardgruppe. Standardmäßig weist die Policy „Default Retention“ eine Aufbewahrungsfrist von 60 Tagen zu und bewahrt die täglichen Backups 60 Tage lang auf.
End User On Demand Retention	Steuert die Aufbewahrungseinstellungen für On-Demand-Backups, mit denen der Client beginnt, z. B. die Verwendung des Befehls **Back Up Now** auf dem Avamar-Windows-Client. Die erweiterten Aufbewahrungseinstellungen sind für diese Aufbewahrungs-Policy deaktiviert, da diese nicht auf On-Demand-Backups angewendet werden können. Die Policy „End User On Demand Retention“ ist ein globales Systemobjekt, das nur die Aufbewahrung für On-Demand-Backups steuert, mit denen der Client beginnt. Daher können Sie die Policy keiner Gruppe zuweisen.
Monthly Retention policy	Stellt das Ablaufdatum auf 1 Monat nach Durchführung des Backup ein
Weekly Retention policy	Stellt das Ablaufdatum auf 1 Woche nach Durchführung des Backups ein.

Erstellen einer Aufbewahrungs-Policy

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Retention Policies** aus.

   Das Fenster **Manage All Retention Policies** wird angezeigt.

2. Klicken Sie auf **New**.

   Das Dialogfeld **New Retention Policy** wird angezeigt.

3. Geben Sie im Feld **Name** einen Namen für die Aufbewahrungs-Policy ein.

   Der Name darf keines der folgenden Zeichen enthalten: `~!@$^%(){}[]|,`;#\/:*?<>'"&`.

4. Führen Sie die folgenden Schritte entweder für grundlegende Aufbewahrungseinstellungen oder für erweiterte Aufbewahrungseinstellungen aus.

Aufbewahrungseinstellung	Schritte
Basic	Wählen Sie eine der folgenden Einstellungen aus: • Um Sicherungen automatisch nach einer bestimmten Anzahl von Tagen, Wochen, Monaten oder Jahren zu löschen, wählen Sie die Option **Aufbewahrungszeitraum** aus und geben Sie die Anzahl der Tage, Wochen, Monate oder Jahre an. • Um Backups an einem bestimmten Kalendertag automatisch zu löschen, wählen Sie die Option **Enddatum** aus und navigieren Sie zum gewünschten Datum im Kalender. • Um Backups für den Zeitraum aufzubewahren, in dem ein Client aktiv ist, wählen Sie die Option **Kein Enddatum** aus. Die Best Practice ist es, eine Aufbewahrung von mindestens 14 Tagen festzulegen. Wenn Sie eine Aufbewahrungs-Policy für weniger als 14 Tage erstellen, wird eine Warnmeldung angezeigt.
Advanced	a. Wählen Sie **Override basic retention policy for scheduled backups** aus. b. Klicken Sie auf **Advanced**. Das Dialogfeld **Edit Advanced Retention Policy** wird angezeigt. c. Legen Sie die maximale Anzahl der aufzubewahrenden täglichen, wöchentlichen, monatlichen und jährlichen Backups fest. d. Klicken Sie im Dialogfeld **Edit Advanced Retention Policy** auf **OK**.

5. Klicken Sie im Dialogfeld **New Retention Policy** auf **OK**.

Bearbeiten einer Aufbewahrungs-Policy

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Retention Policies** aus.

   Das Fenster **Manage All Retention Policies** wird angezeigt.
2. Wählen Sie eine Aufbewahrungs-Policy aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Retention Policy** wird angezeigt.
3. Bearbeiten Sie die Einstellungen der Aufbewahrungs-Policy.

   Klicken Sie auf **OK**.

Kopieren einer Aufbewahrungs-Policy

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Retention Policies** aus.

Das Fenster **Manage All Retention Policies** wird angezeigt.

2. Wählen Sie eine Aufbewahrungs-Policy aus und klicken Sie auf **Copy**.

   Das Dialogfeld **Save As** wird angezeigt.

3. Geben Sie einen Namen für die neue Aufbewahrungs-Policy ein und klicken Sie auf **OK**.

Löschen einer Aufbewahrungs-Policy

Bevor Sie beginnen

Vergewissern Sie sich, dass die Aufbewahrungs-Policy aktuell keinem Client und keiner Gruppe zugewiesen ist. Andernfalls kann die Aufbewahrungs-Policy nicht gelöscht werden.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Retention Policies** aus.

   Das Fenster **Manage All Retention Policies** wird angezeigt.

2. Wählen Sie die Aufbewahrungs-Policy aus und klicken Sie auf **Delete**.
3. Klicken Sie in der Bestätigungsmeldung auf **Yes**.

Durchsetzen einer minimalen Aufbewahrungseinstellung

Mit der minimalen Aufbewahrung können Sie eine minimale grundlegende Aufbewahrungeinstellung für einen gesamten Standort durchsetzen. Sie können z. B. alle Backups ungeachtet der sonstigen festgelegten Aufbewahrungs-Policies für mindestens 90 Tage aufbewahren.

Diese Funktion richtet sich an große Unternehmen, die für den gesamten Standort minimale Aufbewahrungsstandards durchsetzen möchten, egal, welche Ziele einzelne Organisationen mit der Implementierung anderer Aufbewahrungs-Policies verfolgen.

Um die minimale Aufbewahrung durchzusetzen, aktivieren und konfigurieren Sie die Policy Minimal Retention. Dies ist die standardmäßige Aufbewahrungs-Policy des Systems. Die Policy Minimal Retention ist ein globales Systemobjekt, das nur die minimale Aufbewahrungseinstellung steuert. Daher können Sie die Policy Minimal Retention keiner Gruppe zuweisen.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Retention Policies** aus.

   Das Fenster **Manage All Retention Policies** wird angezeigt.

2. Wählen Sie die Policy **Minimal Retention** aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Retention Policy** wird angezeigt.

3. Wählen Sie **Retention period** aus.
4. Legen Sie die Anzahl der Tage, Wochen, Monate oder Jahre fest, um dafür zu sorgen, dass Backups aufbewahrt werden.
5. Klicken Sie auf **OK**.

Automatisches Aufbewahren des letzten Backups

Aktivieren Sie die Option zur Aufbewahrung des letzten Backups, wenn Sie das letzte Backup aller Clients auch nach Ablauf der Aufbewahrungsfrist aufbewahren möchten. Die Option zur Aufbewahrung des letzten Backups ändert das standardmäßige

Aufbewahrungsverhalten für Clientbackups, die nach der Aktivierung dieser Option stattfinden. Bei der Aufbewahrung des letzten Backups wird das letzte Backup eines Clients nach Ablauf der Aufbewahrungsfrist nicht zur Löschung markiert. Stattdessen ist das aktuelle Backup das „letzte Backup“ und das vorhergehende „letzte Backup“ läuft ab oder wird gemäß der Aufbewahrungs-Policy aufbewahrt.

Die Option ist für Clients vorgesehen, für die nicht regelmäßig ein Backup erstellt wird. Bei diesen Clients kann das Standardverhalten dazu führen, dass das letzte Backup abläuft, bevor ein neues stattfindet, und dass für die Clients kein Backup zur Verfügung steht.

Bei Clients, die nicht permanent mit einer Domain verbunden sind, z. B. Remotedesktops und -laptops, kommt diese Situation häufiger vor als bei Clients, die kontinuierlich auf den Server zugreifen.

HINWEIS

Wenn Sie die Aufbewahrung des letzten Backups aktivieren, bewahrt Avamar ein einziges Backup für jeden Client auf, selbst, wenn Sie mehrere Arten von Backups eines Clients durchführen. Wenn Sie beispielsweise Backups sowohl von Dateisystemen als auch von Anwendungen eines Clients durchführen und das Backup des Dateisystems das letzte Backup ist, können alle Backups von Anwendungen ablaufen.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
2. Ändern Sie die Verzeichnisse durch folgende Eingabe:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```
3. Öffnen Sie `mcserver.xml` in einem Texteditor.
4. Navigieren Sie zum `dpn`-Node.
5. Ändern Sie im Node `dpn` den Wert des Eintragsschlüssels `keep_last_backup` von `false` zu `true`.
6. Speichern Sie die Änderung und schließen Sie den Texteditor.
7. Beenden Sie den MCS und starten Sie ihn wieder. Starten Sie anschließend den Planer, indem Sie die folgenden Befehle eingeben:

   ```
   dpnctl stop mcsdpnctl start mcsdpnctl start sched
   ```
8. Schließen Sie die Befehlsshell.

Gruppen

Avamar verwendet Gruppen für die Implementierung verschiedener Policies zur Automatisierung von Backups und zur Durchsetzung von konsistenten Regeln und

konsistentem Systemverhalten in einem gesamten Segment oder einer ganzen Gruppe der Benutzercommunity.

Gruppenmitglieder
Gruppenmitglieder sind Clientmaschinen, die für die Durchführung geplanter Backups einer bestimmten Gruppe hinzugefügt wurden. Da die normalen Regeln für Domainadministratoren gelten, müssen diese Clients sich in der gleichen Domain wie die Gruppe oder innerhalb einer Subdomain befinden.

Gruppen-Policy
Wenn Sie eine Gruppe erstellen, geben Sie das Dataset, die Planung und die Aufbewahrungs-Policy für die Gruppe an. Diese drei Objekte bilden die *Gruppen-Policy*. Die Gruppen-Policy steuert das Backupverhalten für alle Mitglieder der Gruppe.

Sie können Dataset- und Aufbewahrungs-Policy-Einstellungen der Gruppe für einen Client außer Kraft setzen, indem Sie explizite Dataset- oder Aufbewahrungs-Policy-Zuweisungen für den Client vornehmen. Planungen gelten jedoch nur für Gruppen, nicht für einzelne Clients.

Standardgruppe
Das Avamar-System beinhaltet eine Standardgruppe (Default Group). In der standardmäßigen Avamar-Serverkonfiguration verwendet die Standardgruppe immer das standardmäßige Dataset sowie die standardmäßige Planung und Aufbewahrungs-Policy des Systems. Sie können diese standardmäßigen Zuweisungen des Systems nicht ändern. Sie können allerdings die Einstellungen innerhalb des standardmäßigen Dataset sowie der standardmäßigen Planung und Aufbewahrungs-Policy des Systems bearbeiten.

Falls Sie keine anderen Gruppen erstellen, werden neue Clients automatisch der Standardgruppe hinzugefügt.

VMware-Gruppen
Die folgende Tabelle beschreibt die speziellen Gruppen, die auf VMware-Umgebungen zutreffen.

Tabelle 34 VMware-Gruppen

Gruppe	Beschreibung
Default Proxy Group	Die Default Proxy Group ist die Standardgruppe für VMware-Image-Proxyclients. Die Default Proxy Group kann nicht gelöscht werden. Die Aktivierung der Default Proxy Group hat keine Auswirkungen auf geplante Backups, die von anderen, auf dem Proxyclient konfigurierten Plug-ins ausgeführt werden.
Default Virtual Machine Group	Neue VM-Clients werden automatisch der Default Virtual Machine Group hinzugefügt, wenn sie registriert werden. Sie können die Default Virtual Machine Group nicht manuell löschen, sie wird jedoch automatisch gelöscht, wenn Sie die vCenter-Domain löschen.
VM Backup Validation Groups	VM Backup Validation Groups werden zur Implementierung der

Tabelle 34 VMware-Gruppen (Fortsetzung)

Gruppe	Beschreibung
	Wiederherstellungstestfunktion für virtuelle VMware-Maschinen verwendet.

Das *Avamar for VMware – Benutzerhandbuch* liefert weitere Einzelheiten zu diesen Gruppen.

Erstellen einer Gruppe

Bei der Erstellung einer Gruppe legen Sie das Dataset, die Planung und die Aufbewahrungs-Policy fest, die zusammen die Gruppen-Policy für geplante Backups sämtlicher Gruppenmitglieder bilden. Eine Gruppe muss mindestens einen Avamar-Client enthalten. Wenn die Gruppe mindestens zwei Clients enthält, müssen die Clients zur selben Avamar-Domain gehören. Sie können die Gruppen-Policy-Einstellungen auf Clientebene außer Kraft setzen.

Bevor Sie beginnen

Wenn Sie den Assistenten **New Group** zur Erstellung einer Gruppe verwenden, können Sie keine Planungen oder Aufbewahrungs-Policies bearbeiten. Prüfen Sie die bestehenden Planungen und Aufbewahrungs-Policies. Falls erforderlich, erstellen Sie Planungen und Aufbewahrungs-Policies, bevor Sie die Gruppe erstellen.

Hinweis

Wenn der Avamar-Server Data Domain als Back-end-Speicher verwendet, ist das Data Domain-System der Standardspeicherort für Backups. Diese Option kann auf der Registerkarte **Options** geändert werden.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Groups**.
4. Wählen Sie die Domain für die Gruppe aus.

   Im Fenster **Policy** wird eine Tabelle mit Gruppen für die Domain angezeigt.
5. Wählen Sie **Actions** > **Group** > **New** > **Backup Group** aus.

   Der Assistent **New Group** wird angezeigt.
6. Geben Sie einen Namen für die neue Gruppe im Feld **Name** ein.

   Der Name kann alphanumerische Zeichen (A–Z, a–z, 0–9) und die folgenden Sonderzeichen enthalten: Punkt (.), Bindestrich (-) und Unterstrich (_). Verwenden Sie weder Unicode-Zeichen noch die folgenden Sonderzeichen: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?
7. Deaktivieren Sie das Kontrollkästchen **Disabled**, um diese Gruppe zur Durchführung geplanter Clientbackups zu verwenden.

   Durch Auswahl des Kontrollkästchens werden Backups für die Gruppe deaktiviert.

8. Wählen Sie aus der Liste **Avamar encryption method** eine Verschlüsselungsmethode aus, die bei der Datenübertragung zwischen dem Avamar-Server und dem Client während des Backups verwendet werden soll.

   Die genaue Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-Server-Verbindung sind von mehreren Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.

9. (Optional) Wählen Sie **Override Schedule aus**, um den zugewiesenen Plan für diese Gruppe außer Kraft zu setzen:

   - Um das nächste geplante Backup zu überspringen, wählen Sie **Skip Next Backup** aus.
   - Um das nächste geplante Backup nur einmalig auszuführen, wählen Sie **Run Next Backup Once** aus.

10. Klicken Sie auf **Next**.

    Die nächste Seite des Assistenten **New Group** wird mit Dataset-Informationen angezeigt.

11. Wählen Sie aus der Liste **Select An Existing Dataset** das von Ihnen erstellte Dataset aus und klicken Sie dann auf **Next**.

    Die nächste Seite des Assistenten **New Group** wird mit Planungsinformationen angezeigt.

12. Wählen Sie eine Planung aus der Liste **Select An Existing Schedule** aus und klicken Sie auf **Next**.

    Die nächste Seite des Assistenten **New Group** wird mit Informationen zur Aufbewahrungs-Policy angezeigt.

13. Wählen Sie eine Aufbewahrungs-Policy aus der Liste **Select An Existing Retention Policy** aus und klicken Sie auf **Next**.

    Die nächste Seite des Assistenten **New Group** wird angezeigt. Eine Liste mit Domains wird im linken Bereich angezeigt.

14. Wählen Sie die Domain für den Client aus.

    Eine Liste mit Avamar-Clients wird im rechten Bereich angezeigt.

15. Markieren Sie die Clients, die in die Gruppe eingefügt werden sollen, und klicken Sie auf **Include**.

16. (Optional) Um einen Client aus der Gruppe zu entfernen, wählen Sie den Client aus der Liste „Members“ aus und klicken Sie auf die Schatlfläche **Exclude**.

17. Klicken Sie auf **Finish**.

Mangen von Gruppenmitgliedschaften

Sie können Gruppenmitgliedschaften in Avamar Administrator managen, indem Sie Mitglieder für eine Gruppe hinzufügen bzw. entfernen oder indem Sie Gruppen, zu denen ein Client gehört, hinzufügen bzw. entfernen.

Die Methode, die Sie zum Managen von Gruppenmitgliedschaften verwenden, hängt von der Situation ab. Wenn Sie zum Beispiel mehrere Clients einer einzelnen Gruppe hinzufügen bzw. aus dieser entfernen möchten, ist die gruppenorientierte Methode effizient. Möchten Sie jedoch einen einzelnen Client mehreren Gruppen hinzufügen bzw. aus mehreren Gruppen entfernen, ist die clientorientierte Methode die effizienteste Vorgehensweise.

Bearbeiten der Mitgliedschaft für eine Gruppe

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Groups**.
4. Wählen Sie die Gruppe aus.
5. Wählen Sie **Actions** > **Group** > **Edit Group** aus.

   Das Dialogfeld **Edit Group** wird angezeigt.
6. Klicken Sie auf die Registerkarte **Members**.
7. Wählen Sie eine Domain oder Subdomain aus der Domainstruktur aus.

   Um einen Subdomainclient auszuwählen, wählen Sie **Show Sub-Domain Clients** aus.
8. Um ein Mitglied einer Gruppe automatisch hinzuzufügen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie für Gruppen, die sich unter der vCenter-Domain befinden und Image-Schutz der virtuellen VMware-Machine erfordern, **Enable automatic member selection by rule** aus.
   b. Wählen Sie im Drop-down-Menü eine Regel aus.

      Wenn eine Regel auf einen Client zutrifft, wird **Included (by rule)** neben dem Client in der Liste angezeigt.
   c. Zum Filtern der Liste der Clients wählen Sie im Drop-down-Menü **Filter** eine Option aus.
   d. Um einen Client in die Gruppe einzuschließen, wählen Sie einen Client aus der Liste aus und klicken Sie dann auf **Include**.

      Included (by user) wird neben dem ausgewählten Client angezeigt.

      Hinweis

      Alle Clients auf virtuellen Maschinen, die entweder als **Included (by user)** oder als **Included (by rule)** markiert sind, können die Gruppe ausführen.
   e. Um einen Client aus der Gruppe auszuschließen, wählen Sie einen Client aus der Liste aus und klicken Sie dann auf **Exclude**.

      Neben dem ausgewählten Client wird **Excluded** angezeigt.
   f. Um den Status eines Clients zurückzusetzen, wählen Sie einen Client aus der Liste aus und klicken Sie dann auf **Reset**.

      Wenn keine Regel auf den Client zutrifft, ändert sich der Status des Clients in **Not Selected**.

      Wenn eine Regel auf den Client zutrifft, ändert sich der Status des Clients in **Included (by rule)**.
   g. Um das Gruppen-Dataset zu überschreiben, wählen Sie in der Spalte **Override Dataset** ein Dataset aus dem Drop-down-Menü aus.

Hinweis

Nur Clients, die entweder als **Included (by user)** oder **Included (by rule)** markiert sind, können das Dataset überschreiben.

9. Um ein Mitglied einer Gruppe manuell hinzuzufügen, führen Sie die folgenden Schritte aus:
   a. Löschen Sie **Enable automatic member selection by rule**.
   b. Zum Filtern der Liste der Clients wählen Sie im Drop-down-Menü **Filter** eine Option aus.
   c. Um einem Client die Ausführung der Gruppe zu erlauben, wählen Sie einen Client aus der Liste aus und klicken Sie dann auf **Include**.

      Included (by user) wird neben dem ausgewählten Client angezeigt.

      Hinweis

      Nur Clients auf virtuellen Maschinen, die als **Included (by user)** markiert sind, können die Gruppe ausführen.

   d. Um den Status eines Clients zurückzusetzen, wählen Sie einen Client aus der Liste aus und klicken Sie dann auf **Reset**.

      Not Selected wird neben dem Client in der Liste angezeigt.

   e. Um das Gruppen-Dataset zu überschreiben, wählen Sie in der Spalte **Override Dataset** ein Dataset aus dem Drop-down-Menü aus.

      Hinweis

      Nur Clients, die als **Included (by user)** markiert sind, können das Dataset überschreiben.

10. Klicken Sie auf **Finish**.

Bearbeiten der Gruppen für einen Client

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Clients**.
4. Wählen Sie den zu bearbeitenden Client aus.
5. Wählen Sie **Actions** > **Group** > **Edit Client** aus.

   Das Dialogfeld **Edit Client** wird angezeigt.
6. Klicken Sie auf die Registerkarte **Groups**.
7. Fügen Sie dem Client Gruppen hinzu und entfernen Sie Gruppen aus dem Client:
   - Klicken Sie zum Hinzufügen von Gruppen auf **Add**, wählen Sie die Gruppen aus und klicken Sie dann auf **OK**.
   - Wählen Sie zum Entfernen von Gruppen die Gruppen aus, aus denen der Client entfernt werden soll, und klicken Sie auf **Remove**.

8. Klicken Sie auf **OK**.

Überwachen von Gruppen

Sie können Gruppen mithilfe der Group Summary Reports und Group Status Summary überwachen.

Vorgehensweise

- Um die „Group Summary Reports“ anzuzeigen, klicken Sie in Avamar Administrator auf den **Policy**Link zum Startprogramm und dann auf die Registerkarte **Group Summary Reports** im Fenster **Policy**.

  Bei den Group Summary Reports handelt es sich um einen kombinierten Systemstatus auf einen Blick aller aktuellen Gruppeneigenschaften und -einstellungen, darunter auch Außerkraftsetzungen von Gruppen-Policies. In diesen Berichten werden außerdem die den verschiedenen Gruppen zugewiesenen Datasets, Planungen und Aufbewahrungs-Policies angezeigt.

- Um die „Group Status Summary“ anzuzeigen, klicken Sie in Avamar Administrator auf den **Activity**Link zum Startprogramm und dann auf die Registerkarte **Group Status Summary** im Fenster **Activity**.

  Bei der „Group Status Summary“ handelt es sich um eine vereinfachte Darstellung aller infolge von Gruppen-Policies initiierten Backupaktivitäten. Die Richtlinien umfassen die Gesamtzahl der Backups, mit denen die Gruppen-Policy mit einer Methode beginnt, sowie die Anzahl der aktiven, erfolgreich abgeschlossenen, abgebrochenen und fehlgeschlagenen Backups.

Bearbeiten von Gruppeneigenschaften

Sie können die Eigenschaften für eine Gruppe oder mehrere Gruppen bearbeiten. Wenn Sie mehrere Gruppen auswählen, können Sie nicht alle Gruppeneigenschaften bearbeiten.

Die Default Proxy Group und die Default Virtual Machine Group enthalten spezielle Einstellungen, die nur für Personen von Interesse sind, die für das Management der VMware-Image-Backup- und -Wiederherstellungsfunktion zuständig sind. Im *Avamar for VMware – Benutzerhandbuch* erfahren Sie weitere Details zu diesen Einstellungen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Groups**.
4. Wählen Sie eine oder mehrere zu bearbeitende Gruppen aus.
5. Wählen Sie **Actions** > **Group** > **Edit Group** aus.

   Wenn Sie eine einzige Gruppe ausgewählt haben, wird das Dialogfeld **Edit Group** angezeigt. Wenn Sie mehrere Gruppen ausgewählt haben, wird das Dialogfeld **Edit Multiple Groups** angezeigt.
6. Bearbeiten Sie die Gruppeninformationen:
   - Beim Bearbeiten einer einzigen Gruppe können Sie nur grundlegende Gruppeneigenschaften bearbeiten, wie zum Beispiel den Namen, die Clientliste sowie Dataset, Planung und Aufbewahrungs-Policy, die der Gruppe zugewiesen sind. Die Einstellungen für das zugewiesene Dataset, die Planung und die Aufbewahrungs-Policy können nicht bearbeitet werden.

- Beim Bearbeiten der Default Group können Sie die Policy-Objektzuweisungen der Default Group nicht bearbeiten. Die Default Group verwendet immer das Standard-Dataset sowie die Standardaufbewahrungs-Policy und -planung. Daher werden die Registerkarten **Dataset**, **Schedule** und **Retention Policy** nicht angezeigt, wenn Sie die Default Group bearbeiten.
- Beim Bearbeiten mehrer Gruppen wählen Sie die neuen Einstellungen aus den Listen aus oder wählen Sie **Don't Change** aus, um die Einstellung für die ausgewählten Gruppen unverändert zu lassen. Sie können nur grundlegende Gruppeneigenschaften ändern, z. B. ob die Gruppe aktiviert oder deaktiviert ist, die Verschlüsselungseinstellung, die den Gruppen zugewiesenen Datasets, Planungen und Aufbewahrungs-Policies. Die Einstellungen für das zugewiesene Dataset, die Planung und die Aufbewahrungs-Policy können nicht bearbeitet werden.

7. Klicken Sie auf **OK**.

Kopieren einer Gruppe

Gruppen müssen innerhalb derselben Domain kopiert werden. Es ist nicht möglich, eine Gruppe in eine andere Domain zu kopieren.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Groups**.
4. Wählen Sie die zu kopierende Gruppe aus.
5. Wählen Sie **Actions** > **Group** > **Copy Group** aus.

   Das Dialogfeld **Save As** wird angezeigt.
6. Geben Sie einen Namen für die neue Gruppe ein.
7. Aktivieren Sie die Option **Include Client Members**, um die vollständige Clientliste in diese neue Gruppe zu kopieren.
8. Klicken Sie auf **OK**.

Aktivieren und Deaktivieren einer Gruppe

Eine Gruppe kann deaktiviert werden, um geplante Backups für die Gruppe zu verhindern. Dieser Schritt erfolgt in der Regel, um das System in einen Zustand zu versetzen, der verschiedene Wartungsaktivitäten unterstützt.

Im Falle einer Deaktivierung einer Gruppe muss die Gruppe erneut aktiviert werden, um geplante Gruppenbackups wieder aufnehmen zu können.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Groups**.
4. Wählen Sie die zu aktivierende oder deaktivierende Gruppe aus.
5. Klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie **Disable Group** aus.

Wenn die Gruppe deaktiviert ist, wird durch diese Aktion das Häkchen entfernt und die Gruppe aktiviert. Wenn die Gruppe aktiviert ist, wird durch diese Aktion das Häkchen gesetzt und die Gruppe deaktiviert.

6. Klicken Sie auf **Yes**.

Löschen einer Gruppe

Bevor Sie beginnen

Weisen Sie die Clients in der Gruppe einer anderen Gruppe zu, sodass geplante Backups für die Clients ohne Unterbrechungen fortgesetzt werden können.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Groups**.
4. Wählen Sie die zu löschende Gruppe aus.
5. Wählen Sie **Actions** > **Group** > **Delete Group** aus.
6. Klicken Sie in der Bestätigungsmeldung auf **Yes**.

   Es wird eine zweite Bestätigungsmeldung angezeigt.
7. Klicken Sie auf **OK**.

Außerkraftsetzen von Gruppen-Policy-Einstellungen für einen Client

Sie können die Gruppen-Policy-Einstellungen für einen einzigen Client außer Kraft setzen, einschließlich Dataset, Planung und Verschlüsselungsmethode für die Client-Server-Datenübertragung. Mithilfe der Webbenutzeroberfläche des Avamar-Clients können Sie Benutzern den Start von On-Demand-Backups vom Client ermöglichen oder eine maximale Größe in MB für Backups vom Client angeben.

HINWEIS

Durch zu viele Außerkraftsetzungen können Gruppen-Policies ggf. weniger effektiv sein. Implementieren Sie stattdessen eine neue Gruppen-Policy auf Clientebene.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Clients**.
4. Wählen Sie im linken Bereich die Domain für den Client aus.
5. Wählen Sie im rechten Bereich den Client aus.
6. Klicken Sie auf **Edit**.

   Das Fenster **Edit Client** wird angezeigt.
7. Klicken Sie auf die Registerkarte **Properties**.
8. Um Benutzern auf dem Client den Start von On-Demand-Backups zu gestatten, wählen Sie **Allow client initiated backups** aus.

   Wenn keine weiteren Konfigurationsschritte durchgeführt werden, enthalten vom Client aus gestartete Backups nur die vom Benutzer ausgewählten Dateien.

Außerdem wird die On-Demand-Aufbewahrung für Anwender verwendet. Sie können jedoch die Verwendung eines bestimmten Dataset oder einer bestimmten Aufbewahrungs-Policy für alle vom Client initiierte Backups durchsetzen.

9. Um Benutzern die Erstellung von Ordner- und Dateisätzen zum Backup über ein On-Demand-Backup mithilfe der Webbenutzeroberfläche des Avamar-Clients zu ermöglichen, wählen Sie **Allow file selection on client initiated backups** aus.

   Ist diese Funktion aktiviert, haben Benutzer folgende Möglichkeiten:

   - Sie können die Ordner und Dateien spezifizieren, die in einen Backupsatz integriert werden.
   - Sie können mehrere Backupsätze erstellen.
   - Sie können Backupsätze zur erneuten Verwendung speichern.
   - Sie können ein On-Demand-Backup der Ordner und Dateien in den Backupsätzen durchführen, die von ihnen erstellt wurden.

   HINWEIS

   Über diese Funktion ausgewählte Ordner und Dateien unterliegen keinen Quellbegrenzungen, -ausschlüssen oder -einschlüssen des Gruppen-Datasets. Diese Funktion wirkt sich zudem nicht auf automatische Backups von Clients gemäß deren Gruppen-Policies aus.

   Hinweis

   Für Windows-, Mac- und Linux-Clients, die die Desktop- und Laptopclientverbesserungen verwenden, ist zur Aktivierung dieser Einstellung ein zusätzlicher Konfigurationsschritt erforderlich. Zulassen der benutzerseitigen Erstellung von On-Demand-Backupsätzen auf Seite 464 bietet weitere Informationen.

10. Wählen Sie aus, ob die Einstellung für die Dauer der Gruppenplanung für einen Client außer Kraft gesetzt werden soll, indem Sie einen Wert aus der Liste **Overtime** auswählen:

Option	Beschreibung
No overtime allowed	Geplante Gruppenbackups dürfen nie über die eingestellte geplante Dauer hinaus ausgeführt werden.
Overtime on next backup only	Nur das nächste geplante Gruppenbackup darf über die eingestellte geplante Dauer hinaus ausgeführt werden.
Overtime until successful backup	Geplante Gruppenbackups dürfen über die eingestellte geplante Dauer hinaus ausgeführt werden, bis ein erfolgreiches Backup abgeschlossen ist.
Always allow overtime	Geplante Gruppenbackups dürfen immer über die eingestellte geplante Dauer hinaus ausgeführt werden.

11. Wählen Sie **Override group encryption to** und dann die Verschlüsselungseinstellung für die Verwendung für die Client-Server-Datenübertragung für den Client aus.

    Die genaue Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-Server-Verbindung sind von mehreren Faktoren abhängig, u. a. vom Clientbetriebssystem und von der Avamar-Serverversion. Im *Avamar – Produktsicherheitshandbuch* finden Sie nähere Informationen.

12. Um Benutzern in der Webbenutzeroberfläche des Avamar-Clients die Auswahl einer anderen Backupstartzeit für tägliche Backups aus einer Liste mit verfügbaren, von Ihnen angegebenen Zeiten zu ermöglichen, wählen Sie **Allow override of group's daily schedule** aus.

    Unter Bearbeiten der Startzeiten für Clientaußerkraftsetzungen von Gruppenplanungen auf Seite 120 erhalten Sie weitere Informationen zur Angabe der Liste mit verfügbaren Zeiten.

13. Wenn Sie Benutzern auf dem Client den Start von On-Demand-Backups gestatten möchten, wählen Sie die Aufbewahrungs-Policy für alle vom Client initiierten Backups aus:

    a. Klicken Sie auf die Registerkarte **Retention Policy**.

    b. Wählen Sie aus, ob die Gruppen-Aufbewahrungs-Policy oder eine andere Aufbewahrungs-Policy für alle vom Client initiierten Backups verwendet wird, indem Sie das Kontrollkästchen **Override group retention policy** deaktivieren. Deaktivieren Sie das Kontrollkästchen, um die der Gruppe zugewiesene Aufbewahrungs-Policy zu verwenden, oder aktivieren Sie das Kontrollkästchen, um eine andere Aufbewahrungs-Policy zu verwenden.

    c. Wenn Sie das Kontrollkästchen für die Verwendung einer anderen Aufbewahrungs-Policy aktivieren, aktivieren Sie das Kontrollkästchen **Override retention policy on client initiated backups** und wählen Sie dann die Aufbewahrungs-Policy aus der Liste **Select an Existing Retention Policy** aus.

14. So weisen Sie jeder Gruppe, deren Mitglied der Client ist, separate, außer Kraft zu setzende Datasets zu:

    a. Klicken Sie auf die Registerkarte **Groups**.

    b. Wählen Sie aus der Liste in der Spalte **Override Dataset** für jede Gruppe, deren Mitglied der Client ist, ein Dataset aus.

15. Um Benutzern das Hinzufügen von Ordnern zu den Quelldaten für die Gruppen-Datasets, die den Clients des Benutzers zugewiesen sind, über die Webbenutzeroberfläche des Avamar-Clients zu ermöglichen, klicken Sie auf die Registerkarte **Dataset Additions** und wählen Sie dann **Allow additions to source data** aus.

    Das Avamar-System integriert die ausgewählten Ordner in jedem automatischen und On-Demand-Backup für jede dem Client zugewiesene Gruppe und Gruppenausschluss- und -einschlusslisten werden auf die hinzugefügten Daten angewandt.

16. Klicken Sie auf **OK**.

Außerkraftsetzen von Gruppen-Policy-Einstellungen für mehrere Clients

Sie können Gruppen-Policy-Einstellungen für mehrere Clients gleichzeitig außer Kraft setzen, einschließlich der Verschlüsselungsmethode, ob Backups über die Endzeit der

Planung hinaus ausgeführt werden können und ob Benutzer auf dem Client On-Demand-Backups beginnen und eine andere Backupstartzeit auswählen können.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Clients**.
4. Wählen Sie die Clients aus.
5. Klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Multiple Clients** wird angezeigt.
6. Wählen Sie einen außer Kraft zu setzenden Wert aus der Liste und die Option **Apply the change** aus.

   Unter Außerkraftsetzen von Gruppen-Policy-Einstellungen für einen Client auf Seite 137 erhalten Sie weitere Informationen zu den einzelnen Einstellungen.
7. Klicken Sie auf **OK**.

Aktivieren geplanter Backups

Geplante Backups treten nur für aktivierte Gruppen auf. Gruppen werden standardmäßig deaktiviert, es sei denn, Sie aktivieren das Kontrollkästchen **Enabled** auf der ersten Seite des Assistenten **New Group**. Wenn Sie die Gruppe bei ihrer Erstellung nicht aktiviert haben, verwenden Sie zum Aktivieren von Backups die Menüoptionen im Fenster **Policy**.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Groups**.
4. Wählen Sie die erstellte Gruppe aus.
5. Aktivieren Sie die Gruppe, indem Sie **Actions** > **Group** > **Disable Group** auswählen.

   Führen Sie diesen Schritt nur durch, wenn ein Häkchen neben der Menüoption **Disable Group** angezeigt wird.
6. Klicken Sie auf **Yes**, um diese Gruppe zu aktivieren.

Überwachen von Backups

Sie können Backups überwachen, um sich des erfolgreichen Abschlusses zu vergewissern und ein Troubleshooting im Falle von Problemen durchzuführen. Mit dem Activity Monitor in Avamar Administrator können Sie Statusinformationen für On-Demand- und geplante Backups anzeigen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Eine Liste sämtlicher Aktivitäten wird angezeigt.

3. Um die Ergebnisse so zu filtern, dass ausschließlich Backupaktivitäten angezeigt werden, wählen Sie **Actions** > **Filter** aus.

   Das Dialogfeld **Filter Activity** wird angezeigt.

4. Wählen Sie aus der Liste **Type** die Option **All Backups** aus.
5. Klicken Sie auf **OK**.

Abbrechen von Backups

Sie können ein Backup jederzeit vor dessen Abschluss abbrechen. Der Abbruchvorgang kann 5 Minuten oder länger dauern. Das Backup wird u. U. vor Abschluss des Abbruchvorgangs abgeschlossen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Eine Liste sämtlicher Aktivitäten wird angezeigt.

3. Wählen Sie das Backup aus der Liste aus.
4. Wählen Sie **Actions** > **Cancel Activity** aus.

   Es wird eine Bestätigungsmeldung angezeigt.

5. Klicken Sie auf **Yes**.

Managen abgeschlossener Backups

Nachdem Sie ein On-Demand- oder ein geplantes Backup durchgeführt haben, können Sie das Backup validieren, die Einstellungen für das Backup ändern oder das Backup löschen.

Suchen nach einem abgeschlossenen Backup zum Managen

Sie können ein abgeschlossenes Backup suchen, indem Sie nach einem Backup, das an einem bestimmten Kalenderdatum oder in einem bestimmten Datumsbereich stattfand, oder nach einem Backup mit einem bestimmten Aufbewahrungstyp suchen.

HINWEIS

Avamar unterstützt im Allgemeinen die Verwendung bestimmter unterstützter internationaler Zeichen in Verzeichnis-, Ordner- und Dateinamen. Die ordnungsgemäße Anzeige internationaler Sprachzeichen hängt jedoch vom Java-Gebietsschema des Clientcomputers und der auf dem System installierten, mit der Ausgangssprache kompatiblen Schriftarten ab. Wenn Sie mit internationalen Zeichen erstellte Backups durchsuchen, auf Ihrem System jedoch keine kompatible Schriftart installiert ist, werden alle Zeichen, die das System nicht auflösen kann, als Rechtecke angezeigt. Hierbei handelt es sich um eine normale Beschränkung für diese bestimmte Situation, was keinerlei Einfluss auf die Wiederherstellungsfähigkeit dieser Verzeichnisse, Ordner oder Dateien hat. Unter *Avamar – Versionshinweise* sind zusätzliche Informationen zur internationalen Sprachunterstützung enthalten.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Navigieren Sie in der Clientstruktur zum Client mit den zu managenden Backups und wählen Sie ihn aus.
3. Klicken Sie auf die Registerkarte **Manage**.
4. Führen Sie die folgenden Schritte aus, um das Backup nach Datum, Datumsbereich oder Aufbewahrungstyp zu suchen.

Suchmethode	Schritte
Nach Datum	a. Wählen Sie **By day** aus. b. Wählen Sie das Backupdatum aus dem Kalender aus. Gültige Backups wurden an den gelb markierten Daten durchgeführt.
Nach Datumsbereich	a. Wählen Sie **By date range** aus. b. Klicken Sie auf die Liste **From Date** und suchen Sie im Kalender nach dem Startdatum des Bereichs. c. Klicken Sie auf die Liste **To Date** und suchen Sie im Kalender nach dem Enddatum des Bereichs. d. Klicken Sie auf **Retrieve**.
Nach Aufbewahrungstyp	a. Wählen Sie **By retention** aus. b. Aktivieren Sie das Kontrollkästchen neben dem Aufbewahrungstyp für das Backup. c. Klicken Sie auf **Retrieve**.

Eine Liste mit Backups an diesem Datum, innerhalb dieses Datumsbereichs oder mit dem Aufbewahrungstyp wird in der Liste **Backup History** angezeigt.

Validierung eines Backups

Sie können überprüfen, ob sich Dateien aus einem Backup wiederherstellen lassen. Bei einer solchen Validierung beginnt eine „virtuelle“ Wiederherstellung aller Dateien im

Backup, ohne dass tatsächlich Dateien im Clientdateisystem wiederhergestellt werden.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Suchen Sie das Backup. Anweisungen finden Sie unter Suchen nach einem abgeschlossenen Backup zum Managen auf Seite 141.
3. Wählen Sie in der Liste **Backup History** das zu validierende Backup aus.
4. Wählen Sie **Actions** > **Validate Backup** aus.

   Das Dialogfeld **Select Client to Perform Validation** wird angezeigt.
5. Wählen Sie den Client aus, auf dem das Backup validiert werden soll:
   - Um das Backup auf demselben Client zu validieren, über den das Backup ursprünglich durchgeführt wurde, wählen Sie **Validate using the backup client** aus.
   - Um das Backup auf einem anderen Client zu validieren, wählen Sie **Validate using a different client** aus. Klicken Sie dann auf **Browse**, um zum Client zu navigieren.
6. Wählen Sie aus der Liste **Validation Plug-in Type** das Plug-in aus, in dem das Backup validiert werden soll. Nur die auf dem ausgewählten Client installierten Plug-ins werden in der Liste angezeigt.
7. Wählen Sie aus der Liste **Avamar encryption method** die Verschlüsselungsmethode für die Client-Server-Datenübertragung während der Validierung aus.

   Hinweis

   Die standardmäßige Verschlüsselungseinstellung für Backupvalidierungen ist auf hoch eingestellt, unabhängig von der im ursprünglichen Backup verwendeten Verschlüsselungseinstellung.
8. Klicken Sie auf **OK**.

   Es wird eine Bestätigungsmeldung angezeigt.
9. Klicken Sie auf **OK**.

Weitere Erfordernisse

Backupvalidierungen werden als Aktivitäten im Fenster **Activity** angezeigt. Sie können die Backupvalidierungsaktivität auf dieselbe Weise überwachen oder abbrechen, auf die Sie ein Backup überwachen oder abbrechen. Überwachen von Backups auf Seite 140 und Abbrechen von Backups auf Seite 141 enthalten Anweisungen.

Ändern des Ablaufdatums für ein Backup

Sie können das Datum, an dem ein Backup abläuft, ändern. Wenn das Backup abläuft, können Avamar-Benutzer keine Daten aus dem abgelaufenen Backup wiederherstellen. Ein Prozess zur automatischen Speicherbereinigung wird jede Nacht durchgeführt, um den Speicher von verwaisten Daten (abgelaufenen Backups vorbehaltenen Daten) zu bereinigen und wiederzugewinnen.

Das Ablaufdatum kann ein bestimmtes Datum sein, das Sie auswählen, oder eine Aufbewahrungsfrist von einer bestimmten Anzahl von Tagen, Wochen, Monaten oder

Jahren. Sie können ein Backup außerdem so konfigurieren, dass es im Backupspeicher verbleibt, solange der Client auf dem Avamar-Server aktiv ist.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Suchen Sie das Backup. Anweisungen finden Sie unter Suchen nach einem abgeschlossenen Backup zum Managen auf Seite 141.
3. Wählen Sie in der Liste **Backup History** das zu managende Backup aus. Halten Sie zur Auswahl mehrerer Backups die **Strg**-Taste während dieses Vorgangs gedrückt.
4. Wählen Sie **Actions** > **Change Expiration Date** aus.

   Das Dialogfeld **Change Expiration Date** wird angezeigt.
5. Wählen Sie das neue Ablaufdatum aus:
   - Um dieses Backup nach einer bestimmten Zeit automatisch vom Avamar-Server zu löschen, wählen Sie **Retention period** aus und geben als Aufbewahrungsfrist die entsprechende Anzahl an Tagen, Wochen, Monaten oder Jahren an.
   - Um dieses Backup an einem bestimmten Kalendertag automatisch vom Avamar-Server zu löschen, wählen Sie **End date** aus und navigieren zum gewünschten Datum im Kalender.
   - Um dieses Backup während der ganzen Aktivierungszeit des Clients auf dem Avamar-Server aufzubewahren, wählen Sie **No end date** aus.
6. Klicken Sie auf **OK**.

   Es wird eine Bestätigungsmeldung angezeigt.
7. Klicken Sie auf **Yes**.

   Ein Dialogfeld mit dem Ereigniscode wird angezeigt.
8. Klicken Sie auf **OK**.
9. Klicken Sie in der Bestätigungsmeldung auf **OK**.

Ändern des Aufbewahrungstyps für ein Backup

Um bestimmte erweiterte Funktionen zu unterstützen, weist Avamar Administrator jedem Backup automatisch einen oder mehrere Aufbewahrungstypen zu. Beispielsweise ist das erste auf dem Avamar-System erstellte Backup als täglich, wöchentlich, monatlich oder jährlich gekennzeichnet. Die einem Backup zugewiesenen Aufbewahrungstypen können manuell geändert werden.

Stellen Sie bei der manuellen Änderung der einem Backup zugewiesenen Aufbewahrungstypen, insbesondere bei einem Backup mit mehreren Aufbewahrungstypen, sicher, dass ein zu erhaltendes wöchentliches, monatliches oder jährliches Backup nicht versehentlich entfernt wird. Nehmen wir einmal ein Backup als Beispiel, dem ein täglicher, wöchentlicher, monatlicher und jährlicher Aufbewahrungstyp zugewiesen ist. Wenn die Zuweisung für den jährlichen Aufbewahrungstyp entfernt wird, steht Ihnen womöglich für eine relativ lange Zeit kein anderes jährliches Backup im System zur Verfügung.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

Das Fenster **Backup, Restore and Manage** wird angezeigt.

2. Suchen Sie das Backup. Anweisungen finden Sie unter Suchen nach einem abgeschlossenen Backup zum Managen auf Seite 141.
3. Wählen Sie in der Liste **Backup History** das zu managende Backup aus. Halten Sie zur Auswahl mehrerer Backups die **Strg**-Taste während dieses Vorgangs gedrückt.
4. Wählen Sie **Actions** > **Change Retention Type** aus.

   Das Dialogfeld **Change Retention Type** wird angezeigt.
5. Wählen Sie für die Backups einen der folgenden Aufbewahrungstypen aus:
   - Um diesem Backup ausdrücklich einen täglichen, wöchentlichen, monatlichen oder jährlichen Aufbewahrungstyp zuzuweisen, wählen Sie **Tags** aus und aktivieren Sie dann das Kontrollkästchen neben den Aufbewahrungstypen.
   - Wenn dem Backup ausdrücklich kein täglicher, wöchentlicher, monatlicher oder jährlicher Aufbewahrungstyp zugewiesen werden soll, wählen Sie **Not tagged** aus. Das Backup wird als Backup ohne Tag gekennzeichnet.
6. Klicken Sie auf **OK**.

   Es wird eine Bestätigungsmeldung angezeigt.
7. Klicken Sie auf **Yes**.

   Es wird eine zweite Bestätigungsmeldung angezeigt.
8. Klicken Sie auf **OK**.

Anzeigen der Backupstatistik

Sie können im Fenster **Activity** und über die Registerkarte **Manage** des Fensters **Backup, Restore and Manage** detaillierte Statistiken für abgeschlossene Backups anzeigen.

Die Registerkarte **Manage** des Fensters **Backup, Restore and Manage** enthält Statistiken zu allen gespeicherten Backups. Im Fenster **Activity** hingegen wird nur die aktuelle Backupaktivität angezeigt. In der Regel werden im Fenster **Activity** nur die Backups der letzten 72 Stunden angezeigt.

Für alle Backups werden dieselben Statistiken angezeigt, unabhängig davon, ob die statistischen Daten über das Fenster **Backup, Restore and Manage** oder **Activity** angezeigt werden.

Vorgehensweise

1. Suchen Sie das Backup entweder im Fenster **Backup, Restore and Manage** oder im Fenster **Activity**. Schließen Sie die Schritte ab.

Fenster	Schritte
Fenster Backup, Restore and Manage	a. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm. Das Fenster **Backup, Restore and Manage** wird angezeigt. b. Suchen Sie das Backup. Anweisungen finden Sie unter Suchen nach einem abgeschlossenen Backup zum Managen auf Seite 141. c. Wählen Sie in der Liste **Backup History** das Backup aus.

Fenster	Schritte
Fenster Aktivität	a. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm. Das Fenster **Activity** wird angezeigt. b. Klicken Sie auf die Registerkarte **Activity Monitor**. c. Wählen Sie eine Backupaktivität aus der Liste aus.

2. Wählen Sie **Actions** > **View Statistics** aus.

   Das Dialogfeld **Backup Statistics** wird angezeigt.
3. (Optional) Um die Daten auf einer Registerkarte des Dialogfelds **Backupstatistiken** in eine kommagetrennte Datei (`.csv`) zu exportieren, klicken Sie auf **Export** und geben Sie dann den Speicherorten und den Namen für die Datei an.
4. Klicken Sie auf **Close**.

Informationen im Dialogfeld „Backupstatistik“

Die folgenden Informationen werden auf den Registerkarten des Dialogfelds **Backup Statistics** angezeigt.

Tabelle 35 Informationen im Dialogfeld „Backupstatistik“

Registerkarte	Informationen
Details	Detaillierte Informationen in der Datenbankansicht `v_activities_2`. Im *Avamar-Berichte – Handbuch* finden Sie weitere Informationen über die Ansicht `v_activities_2 database`.
Files	Eine Liste der im Backup enthaltenen Dateien
File Aggregation	Ein repräsentativer Auszug der im Backup enthaltenen ressourcenintensiven Dateitypen sowie eine kumulierte Deduplizierungsstatistik nach Dateityp
Optionen	Besondere Optionen für das Backup
Errors	Während des Backups aufgetretene Fehler

Löschen eines Backups

Beim Löschen eines Backups löscht Avamar alle Daten in diesem Backup sofort und dauerhaft vom Server.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Suchen Sie nach dem zu löschenden Backup. Anweisungen finden Sie unter Suchen nach einem abgeschlossenen Backup zum Managen auf Seite 141.

3. Wählen Sie in der Liste **Backup History** das zu löschende Backup aus.
4. Wählen Sie **Actions** > **Delete Backup** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
5. Klicken Sie auf **OK**.

KAPITEL 6

Anwendungskonsistentes SQL VM-Image-Backup

Dieses Kapitel beinhaltet die folgenden Themen:

Informationen zu erweiterten Policies

Konfigurieren Sie eine erweiterte Policy, um das Backup von anwendungskonsistenten virtuellen SQL-Maschinen zu verwalten, einschließlich automatische SQL-Erkennung, automatisches Backupgruppenmanagement und automatische Client-SQL-Plug-in-Installation und -Registrierung.

Voraussetzungen

Prüfen Sie die folgenden Voraussetzungen, bevor Sie eine erweiterte Policy für den anwendungskonsistenten Schutz von SQL-VMs einrichten.

- Administratorbenutzer und lokale Benutzer mit Administratorrolle können erweiterte anwendungskonsistente Backups von virtuellen SQL-Maschinen durchführen. Aufgrund der Einführung von User Account Control (UAC) in Microsoft Windows 7 und späteren Versionen muss ein lokaler Benutzer mit Administratorrolle jedoch zusätzlich die Option **Admin Approval Mode** in den UAC-Einstellungen für die Administratorgruppe auf dem Gastbetriebssystem deaktivieren. Andernfalls schlägt die Installation/das Upgrade/die Registrierung von Client-Agents auf virtuellen SQL-Maschinen durch **Advanced Policy Builder** fehl.
- Wenn der vCenter-Bestandsname der virtuellen Maschine (VM) identisch mit dem Gastcomputernamen ist, ändern Sie die mcserver.xml-Einstellung zu `<entry key="allow_duplicate_client_names" value="true" />`. Wenn Sie die Einstellung nicht ändern, kann die Registrierung während der Registrierung des Avamar-Clients mit MCS fehlschlagen.

Bearbeiten einer erweiterten Policy

Vorgehensweise

1. Zum Starten der Avamar-Webbenutzeroberfläche öffnen Sie einen Webbrowser und geben Sie die folgende URL ein:

   `https://`*`Avamar_server`*`/aui`

   Dabei steht *Avamar_server* für den DNS-Namen oder die IP-Adresse des Avamar-Servers.

   Hinweis

   Wenn eine Benutzerumgebung die HTTPS-Zertifikatvalidierungsanforderungen nicht erfüllt, schlägt die Validierung des Zertifikats fehl und eine Fehlermeldung wird angezeigt, die die Benutzer fragt, ob sie weiterhin Pakete herunterladen möchten. Das Ignorieren einer Zertifikatsvalidierung kann zu Sicherheitsproblemen führen.

   a. Geben Sie im Feld **Avamar Username** einen Benutzernamen mit Administratorrechten ein.

   b. Geben Sie im Feld **Avamar Password** das Passwort für den Administratorbenutzer ein.

   c. Wählen Sie **Avamar** als **Auth Type**.

d. Klicken Sie auf **Log In**.

2. Klicken Sie im Navigationsbereich auf der linken Seite auf » und klicken Sie dann auf **Policy** > **Advanced Policy** .

   Das Fenster **Advanced Policy** wird angezeigt.

3. Wählen Sie in der Domainstruktur die Domain oder Sudbomain für den Client aus.

4. Um eine erweiterte Policy hinzuzufügen, klicken Sie auf +.

   Die Seite **Advanced Policy Builder** wird angezeigt.

5. Benennen Sie die Lösung.

6. Um die Lösung zu aktivieren, deaktivieren Sie **Disable this solution**.

Konfigurieren einer Quelle

Vorgehensweise

1. Klicken Sie auf **Quelle**.

   Die Seite **Source** wird angezeigt.

2. Wählen Sie ein Ziel-vCenter aus oder fügen Sie ein Ziel-vCenter hinzu.

   Hinweis

   Wenn vCenter in der Drop-down-Liste nicht aufgeführt ist, stellen Sie sicher, dass die Domain, unter der die Policy erstellt wird, auf die den vCenter zugreifen kann, in dem die Regel ursprünglich erstellt wurde.

3. Um ein vCenter zu erstellen, klicken Sie auf **Add vCenter**:

   Der Assistent **New vCenter** wird angezeigt.

   a. Geben Sie im Assistenten die folgenden Informationen an:

   - Clientinformationen, einschließlich Clienttyp und Clientname oder IP-Adresse
   - vCenter-Informationen, einschließlich Benutzername, Passwort und Portnummer
   - Kontaktinformationen

   b. Überprüfen Sie die Zusammenfassung.

   c. Klicken Sie auf **Create**.

Konfigurieren der Gruppen-Policy

Eine Gruppen-Policy enthält alle erforderlichen Informationen zur Durchführung von Backups von Gruppen von Instanzen.

Gruppenrichtlinienobjekte enthalten drei untergeordneten Objekte:

- Planung: Eine Policy, die die Häufigkeit sowie die tägliche Start- und Endzeit für Backups von Clients in einer Gruppe steuert. Ein Plan ist eine dauerhafte und wiederverwendbare Avamar-Policy, die benannt und mit mehreren Gruppen verbunden werden kann.

- Aufbewahrung: Eine Policy, die definiert, wie lange das Backup in der Backup-Appliance gespeichert bleibt.
- Dataset: Eine Policy, die einen Satz aus Dateien, Verzeichnissen und Dateisystemen für jede unterstützte Plattform definiert, die in einer Clientgruppe in Backups eingeschlossen bzw. aus diesen ausgeschlossen sind. Ein Dataset ist eine dauerhafte und wiederverwendbare Avamar-Policy, die benannt und mit mehreren Gruppen verbunden werden kann.

Vorgehensweise

1. Klicken Sie auf der Seite **Advanced Solution Builder** auf **Type**.
2. Wählen Sie im Feld **Advanced Policy Type** die Option **SQL Server**.
3. Um eine Backupgruppe hinzuzufügen, klicken Sie auf + und wählen Sie dann eine Backupgruppe aus der Liste aus.
4. Wählen Sie in der Spalte **Schedule** eine Planung für jede Backupgruppe aus.

   Geplante Backups werden automatisch ausgeführt, um sicherzugehen, dass Backups kontinuierlich vorgenommen werden. Sie können Backups so planen, dass sie täglich, wöchentlich oder monatlich ausgeführt werden.

   So erstellen Sie eine Backupplanung:

   a. Wählen Sie aus der Drop-down-Planungsliste **Create**.
   b. Geben Sie im Feld **Planungsname** einen Namen für die Planung ein.
   c. Geben Sie im Feld **Backup Window** Feld die Zeit in Stunden an, in der die Daten wiederhergestellt sein müssen.
   d. Wählen Sie im Feld **Recurrence Type**, wie oft die Planung ausgeführt werden soll, und klicken Sie dann auf **Next**.
   e. Wählen Sie den Tag der Woche, an dem die Planung ausgeführt werden soll, und klicken Sie auf **Next**.
   f. Geben Sie das Datum ein, an dem die Planung beginnt, und das Datum, an dem die Planung abläuft.
   g. Klicken Sie auf **Finish**.
5. Wählen Sie in der Spalte **Dataset** ein Dataset für jede Backupgruppe aus.

   Wie Sie ein Dataset mithilfe von Avamar Administrator erstellen, erfahren Sie unter Datasets auf Seite 108.

   Ein Dataset gibt die Daten an, die bei einem geplanten Backup einbezogen werden sollten, sowie die beim Backup zu verwendenden Optionen. Erstellen Sie mindestens ein Dataset für geplante Backups auf einem Client oder für eine Gruppe an Clients. Erstellen Sie mehrere Datasets, um Clientdaten zu trennen.
6. Wählen Sie in der Spalte **Retention** eine Aufbewahrungs-Policy für jede Backupgruppe aus.

   Die Aufbewahrungszeit ist die Zeiteinstellung zum automatischen Löschen von Backups auf einem Avamar-Server. Für Backups, die nicht von einem Avamar-Server gelöscht werden sollten, kann eine dauerhafte Aufbewahrung eingestellt werden.

   Informationen zum Erstellen einer Aufbewahrungs-Policy mithilfe von Avamar Administrator finden Sie im *Avamar-Administrationshandbuch*.

Konfigurieren von Mitgliedern

Das gleichzeitige Pushen von Clients in eine Gruppe von Ziel-VMs hat möglicherweise Auswirkungen auf die Performance. Passen Sie zur Verbesserung der Performance die Avamar-Drosselungseinstellungen für vCenter und Esxi an.

Zugriff auf die folgenden Avamar-Drosselungseinstellungen für `/usr/local/avamar/bin/vabm/vabm.cfg`:

- `vabm_esxi_throttling` erlaubt die gleichzeitige Ausführung der maximalen Anzahl der Installationsjobs für jeden Esxi.
- `vabm_vcenter_throttling` erlaubt die gleichzeitige Ausführung der maximalen Anzahl der vCenter-Anforderungen jedes vCenter.
- `vabm_cache_timeout` erlabut die maximalen Minuten zur Cacheerkennung. Das Ergebnis der Erkennung von Betriebssystem- und Plug-in-Version wird in Avamar für eine bestimmte Zeit zwischengespeichert.

Vorgehensweise

1. Klicken Sie auf der Seite **Advanced Solution Builder** auf **Members**.
2. So installieren, aktualisieren oder registrieren Sie Client-Agents automatisch auf diesen virtuellen Maschinen:
   a. Stellen Sie sicher, dass das UpgradeClientDownloads-Paket auf dem Avamar-Server installiert wurde.
   b. Aktivieren Sie das Kontrollkästchen **Install/Upgrade/Register client agents on these VMs automatically**.
3. Um eine Registrierung des Client-Agent vom vorherigen Avamar-Server auf den Avamar-Zielserver zu erzwingen, wählen Sie **Force register client agents to this Avamar**.

   So wird eine Registrierung des Zielclients auf dem aktuellen Avamar-Server erzwungen.
4. Wählen Sie im Feld **Rule to apply** eine Option.

   Wenn keine Regel in der Drop-down-Liste aufgeführt ist, stellen Sie sicher, dass die Domain, unter der die Policy erstellt wird, auf die Domain zugreifen kann, in der die Regel ursprünglich erstellt wurde. Eine Regel wird einer Policy zugeordnet. Stellen Sie sicher, dass die Regel nicht bereits für eine andere erweiterte Policy verwendet wird.
5. Geben Sie den Benutzernamen für das Gastbetriebssystem der virtuellen Maschine ein.

   Wenn Sie einen Benutzernamen für die virtuelle Maschine auswählen, beachten Sie die folgenden Informationen:

   - Wenn auf der virtuellen Zielmaschine UAC aktiviert ist, verwenden Sie das Administratorkonto oder das Verwaltungskonto mit deaktiviertem Admin Approval-Modus.
   - Wenn auf der virtuellen Zielmaschine UAC deaktiviert ist, verwenden Sie das Administratorkonto oder das Verwaltungskonto.

Hinweis

Wenn Sie nicht das Objekt BUILTIN\users für die SQL-Anmeldung hinzugefügt haben, kann die erweiterte Policy die Sysadmin-Rolle nicht automatisch zum NT AUTHORITY\SYSTEM-Objekt hinzufügen. Zur Verwendung der NT-Authentifizierung für SQL-Backup fügen Sie die Sysadmin-Rolle manuell hinzu, bevor Sie fortfahren. Weitere Informationen finden Sie in Ihrer SQL Server-Dokumentation.

6. Geben Sie das Passwort für die virtuelle Maschine ein.
7. Um die Client-Agents auf diesen virtuellen Maschinen manuell zu verschieben, klicken Sie auf **Retry Installation**.
8. Klicken Sie zum Anzeigen der Mitgliederliste und der Informationen für eine virtuelle Maschine auf **Refresh**.

   Diese Aktion scannt alle virtuellen Maschinen unter dem konfigurierten vCenter, bewertet die übereinstimmenden Regelmitglieder und erkennt dann die Mitgliedsinformationen. Der Vorgang dauert möglicherweise einen Moment.

Konfigurieren eines Proxys für das Image-Backup

Vorgehensweise

1. Klicken Sie auf der Seite **Advanced Solution Builder** auf **Proxies**.

   Die Seite **Proxy** wird angezeigt.
2. Um die **Auto-Proxy-Zuordnung** zu aktivieren, aktivieren Sie das Kontrollkästchen.
3. Wählen Sie einen Proxy aus der Liste aus.
4. Um die Plug-in-Installation und -Registrierung zu starten, klicken Sie auf **Submit**.

Entfernen einer erweiterten Policy

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Policy** > **Advanced Policy**.

   Das Fenster **Advanced Policy** wird angezeigt.
2. Wählen Sie in der Domainstruktur die Domain oder Sudbomain für den Client aus.
3. Wählen Sie die Lösung, die Sie entfernen möchten, und klicken Sie dann auf ⊗.

Bearbeiten einer erweiterten Policy

Konfigurieren Sie die einzelnen Policies, die als Teil einer erweiterten Policy erstellt wurden, nicht erneut.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Policy** > **Advanced Policy**.

   Das Fenster **Advanced Policy** wird angezeigt.

2. Wählen Sie in der Domainstruktur die Domain oder Sudbomain für den Client aus.
3. Klicken Sie auf die Policy, die Sie bearbeiten möchten, und klicken Sie auf .

   Die Seite **Advanced Policy Builder** wird angezeigt.

Hinweis

Wenn Sie eine erweiterte Policy bearbeiten, können Sie den Policy-Namen nicht ändern oder einen anderen vCenter wählen.

Anzeigen von Details zur erweiterten Policy

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Policy** > **Advanced Policy**.

   Das Fenster **Advanced Policy** mit den konfigurierten Policies wird angezeigt.
2. Überprüfen Sie die Details der Policy.
3. Um detaillierte Informationen für Mitglieder der erweiterten Policy anzuzeigen, klicken Sie auf .

Anzeigen von -Protokollen

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Policy** > **Advanced Policy**.

   Das Fenster **Advanced Policy** mit den Policies wird angezeigt.
2. Um die Protokolle für eine Policy anzuzeigen, wählen Sie eine Policy aus der Liste aus und klicken Sie dann auf .

   Das Fenster **VM List** wird angezeigt.
3. Wählen Sie eine virtuelle Maschine aus der Liste aus und klicken Sie dann auf **View Logs**.
4. Um Systemprotokolle anzuzeigen, navigieren Sie zu `/usr/local/avamar/var/vabm/log/daemon/`.
5. Um ein detailliertes Protokoll für jede virtuelle Maschine anzuzeigen, navigieren Sie zu `/usr/local/avamar/var/vabm/log/<vm-uuid>/<vm-uuid.log>`.

Wiederherstellungsanforderungen

Um eine erfolgreiche Wiederherstellung zu ermöglichen, stellen Sie sicher, dass die Umgebung die notwendigen Anforderungen erfüllt.

Das Avamar-Plug-in für SQL Server führt nur Offlinewiederherstellungen von SQL Server-Daten durch. Onlinewiederherstellungen werden nicht unterstützt. Das Avamar-Plug-in für SQL Server bietet keine Unterstützung für die Wiederherstellung einzelner Dateien, mit Ausnahme von Teildateien aus einem SQL-Backup in derselben Instanz und Datenbank, wenn die Datenbank während der Wiederherstellung online ist.

Um eine Recovery auf Tabelleneben (Table Level Recovery, TLR) durchzuführen, ist das Avamar-Plug-in für SQL TLR erforderlich. Wenn das Avamar-Plug-in für SQL TLR installiert ist, wird der ItemPoint für Microsoft SQL Server ebenfalls installiert.

Anforderungen an die Software für die Wiederherstellung

Um eine Instanz, Datenbank, Dateigruppe oder Datei auf SQL Server mit dem Avamar Plug-in for SQL Server wiederherzustellen, stellen Sie sicher, dass die Software in der Umgebung die notwendigen Anforderungen erfüllt.

- Die folgende Software muss auf den Quell- und Zielsystemen ausgeführt werden:
  - Microsoft SQL Server
  - Avamar Client für Windows
  - Avamar-Plug-in für SQL Server

  Wenn Avamar-Plug-in für SQL Server nicht auf dem Zielserver installiert ist oder Sie die Standardwiederherstellungstools von SQL Server für Funktionen verwenden möchten, die Avamar-Plug-in für SQL Server nicht bietet, können Sie eine SQL Server-Datenbank von einem Avamar-Backup aus in die Betriebssystemdateien wiederherstellen. Dann können Sie die Datenbank mit SQL Server-Tools wiederherstellen.
- Um die ein Recovery auf Tabelleneben durchzuführen, muss das Avamar Plug-in for SQL TLR installiert sein.
- Um eine Systemdatenbank wiederherzustellen, benötigt die SQL Server-Zielinstallation für die Wiederherstellung dieselbe SQL Server-Version und dasselbe Service Pack wie die SQL Server-Installation, auf der das Backup stattgefunden hat. Andernfalls schlägt die Wiederherstellung fehl. Weitere Details finden Sie im Artikel „You cannot restore system database backups to a different build of SQL Server“ auf der Microsoft Support-Website.
- Um eine Benutzerdatenbank wiederherzustellen, benötigt die SQL Server-Zielinstallation für die Wiederherstellung dieselbe SQL Server-Version oder höher und dasselbe Service Pack oder höher wie die SQL Server-Installation, auf der das Backup stattgefunden hat. Die Wiederherstellung schlägt fehl, wenn Sie versuchen, von einer neueren Version von SQL Server auf eine ältere Version von SQL Server wiederherzustellen. Beispielsweise können Sie ein Backup einer SQL Server 2008-Benutzerdatenbank auf eine SQL Server 2012-Instanz wiederherstellen. Allerdings wird die Wiederherstellung einer SQL Server 2012-Benutzerdatenbank auf eine SQL Server 2008-Instanz nicht unterstützt. Diese Kompatibilitätsanforderung wird von Microsoft SQL Server erzwungen und ist keine Avamar-Einschränkung.

  HINWEIS

  Das Wiederherstellen einer Benutzerdatenbank auf eine neuere Version von SQL Server (z. B. von SQL Server 2008 auf SQL Serve 2012) funktioniert in den meisten Fällen, in denen die SQL Server-Versionskompatibilitätrichtlinien eingehalten werden. Jedoch wurden nicht alle Wiederherstellungsszenarien mit dem SQL Server-Plug-in geprüft.
- Der Zielserver muss mit demselben Avamar-Server wie die Quelle registriert werden.
- Wenn sich die SQL Server-Installation in einem Failover-Cluster befindet, haben Sie den Avamar-Clusterclient für alle SQL Server-Cluster-Nodes konfiguriert.

- Wenn Sie AlwaysOn-Verfügbarkeitsgruppen aktiviert haben, haben Sie den Avamar-Clusterclient für den Verfügbarkeitsgruppen-Listener konfiguriert.

Anforderungen für Protokollfragmentbackup- und Point-in-Time-Wiederherstellungen

Überprüfen Sie die Anforderungen zur Ausführung eines Protokollfragmentbackups oder einer Point-in-Time-Wiederherstellung, um den erfolgreichen Abschluss der Wiederherstellung zu gewährleisten.

- Für ein Protokollfragmentbackup während des Wiederherstellungsprozesses muss die Datenbank online geschaltet sein und entweder das vollständige oder massenprotokollierte Recovery-Modell verwenden. Um eine Point-in-Time-Wiederherstellung durchzuführen, muss die Datenbank das komplette Recovery-Modell verwenden. Daher können Sie kein Protokollfragmentbackup und keine Point-in-Time-Wiederherstellung für Systemdatenbanken wie Master- und msdb-Datenbanken durchführen, da diese Datenbanken das einfache Recovery-Modell nutzen.
- Um auf einen bestimmten Point-in-Time wiederherzustellen, müssen das Transaktionsdatum und die Uhrzeit oder die benannte Markierung angegeben werden, auf der über das SQL Server-Transaktionsprotokoll wiederhergestellt werden soll. Die SQL Server-Dokumentation auf der Microsoft-Website enthält Details zum Zugriff auf Transaktionsprotokollinformationen.
- Der Point-in-Time, auf den Sie wiederherstellen, muss nach dem Ablauf der Zeit für das letzte komplette Backup liegen. Liegt der Point-in-Time vor der Startzeit des letzten Backuptransaktionsprotokolls (inkrementell), ist ein Protokollfragmentbackup nicht erforderlich. Jedoch ist ein Protokollfragmentbackup erforderlich, wenn der Point-in-Time nach dem letzten Transaktionsprotokollbackup liegt.
- Wenn Sie den Point in-Time für die Wiederherstellung angeben, legen Sie nicht die Startzeit des ausgewählten Transaktionsprotokollbackups fest, wenn es sich nicht um das letzte Backup in dieser Backupsequenz handelt. Andernfalls schlägt die Wiederherstellung fehl und ein Protokollfragmentbackup wird nicht durchgeführt, selbst wenn Sie die Option **Tail-log backup** auswählen.

Anforderungen für Point-in-Time-Wiederherstellungen nach dem Ändern des Backupspeichers

Sie können eine Point-in-Time-Wiederstellung zwischen zwei kompletten Backups durchführen, wenn Sie den Backupspeicher von einem Data Domain-System auf ein anderes Data Domain-System ändern.

Um eine Point-in-Time-Wiederherstellung zwischen einem kompletten Backup auf dem ersten Data Domain-System und dem ersten kompletten Backup auf dem neuen Data Domain-System durchzuführen, aktivieren Sie das Kontrollkästchen **Force incremental backup**, wenn Sie das erste komplette Backup im neuen Data Domain-System durchführen. Deaktivieren Sie anderenfalls das Kontrollkästchen **Force incremental backup**.

Bei Aktivierung des Kontrollkästchens **Force incremental backup** wird ein Wiederherstellungsfehler angezeigt, weil komplette Backups auf einem Data Domain-System und inkrementelle (Transaktionsprotokoll) Backups auf einem anderen Data Domain-System nicht unterstützt werden. Daher erstellt der Backupprozess einen einzigen Backupsatz, der sowohl das neue komplette Backup als auch das erzwungene inkrementelle Backup enthält.

So führen Sie eine Point-in-Time-Wiederherstellung der Datenbank zwischen dem kompletten Backup auf dem ersten Data Domain-System und dem kompletten Backup auf dem zweiten Data Domain-System durch:

1. Stellen Sie das komplette Backup vom Data Domain-System in einer Datei wieder her.
2. Stellen Sie das erzwungene inkrementelle (Transaktionsprotokoll) Backup vom zweiten Data Domain-System in einer Datei wieder her.
3. Verwenden Sie diese Dateien zur Wiederherstellung der Datenbank auf den erforderlichen Point-in-Time mithilfe von SQL Server-Tools, z. B. SQL Server Management Studio oder das Microsoft SQL Server `sqlcmd`-Utility. Die Microsoft-Website bietet Einzelheiten zur Verwendung von SQL Server Management Studio, um ein Datenbankbackup für einen bestimmten Point-in-Time wiederherzustellen.

Anforderungen für die Wiederherstellung der sekundären Datenbankdateien

Wenn Sie sekundäre Datendateien einer Datenbank am ursprünglichen Speicherort wiederherstellen, muss die Wiederherstellung die folgenden Anforderungen erfüllen.

- Sie müssen das letzte Backup der Datenbank für die Wiederherstellung auswählen.
- Sie müssen ein Protokollfragmentbackup durchführen.
- Sie müssen die Wiederherstellung mit einem einzigen Wiederherstellungsvorgang durchführen.

Sie können keine zusätzlichen sekundären Datendateien wiederherstellen, nachdem Sie eine Wiederherstellung mit einem Protokollfragmentbackup durchgeführt haben.

Zur Wiederherstellung der sekundären Datendateien einer Datenbank mit zwei unterschiedlichen Wiederherstellungsvorgängen stellen Sie das Backup in einer Datei wieder her und nutzen Sie dann die SQL Server Management Tools für die Durchführung der Wiederherstellungen.

Anforderungen für die Wiederherstellung der Berichtsserver-Datenbank

Beenden Sie die SQL Server Reporting Services, bevor Sie die Berichtsserver-Datenbank wiederherstellen. Andernfalls wird die Berichtsserver-Datenbank nicht ordnungsgemäß wiederhergestellt.

Anforderungen für die SQL Server-Schreibberechtigungen

SQL Server muss Schreibberechtigungen für den Speicherort haben, in dem Sie Daten wiederherstellen. Andernfalls schlägt die Wiederherstellung mit einem Fehler `Access is denied` fehl.

Suchen nach einem Backup

Der erste Schritt zum Wiederherstellen von Daten ist das Suchen nach dem Backup mit den wiederherzustellenden Daten. Sie können Avamar-Clientbackups entweder nach einem bestimmten Datum oder nach bestimmten Inhalten suchen.

Führen Sie eine Backupsuche anhand des Datums durch, wenn eine oder mehrere der folgenden Möglichkeiten zutreffen:

- Sie haben alle Daten für den Client in einem einzigen Backupsatz gespeichert.
- Der genaue Pfadname oder der Name der wiederherzustellenden Daten ist unbekannt.
- Das wiederherzustellende Backup liegt vor einem bestimmten Datum bzw. Ereignis. Beispielsweise kennen Sie das ungefähre Datum, wann Daten verloren gingen oder beschädigt wurden. Suchen Sie dann ein Backup vor diesem Datum.

- Die spezifischen Backuptypen sind bekannt. Sie führen beispielsweise immer mittwoch- und samstagnachts geplante Disaster-Recovery-Backups und täglich komplette Volume-Backups aus. Wenn Sie einen Server erneut aufbauen, können Sie das Disaster-Recovery-Backup mit dem Datum auswählen, das dem Ereignis am nächsten liegt, durch das der Datenverlust verursacht wurde.

Führen Sie eine Backupsuche anhand des Backupinhalts durch, wenn eine oder mehrere der folgenden Möglichkeiten zutreffen:

- Sie haben Daten auf dem Client in separate Backupsätze gespeichert.
- Sie möchten mehrere Versionen derselben Datei anzeigen, um die wiederherzustellende Version auswählen zu können.
- Das Datum oder der Inhalt des Backups ist zwar unbekannt, Sie kennen allerdings den Namen der wiederherzustellenden Daten.

HINWEIS

Avamar unterstützt im Allgemeinen die Verwendung bestimmter unterstützter internationaler Zeichen in Verzeichnis-, Ordner- und Dateinamen. Die ordnungsgemäße Anzeige internationaler Sprachzeichen hängt jedoch vom Java-Gebietsschema des Clientcomputers und der auf dem System installierten, mit der Ausgangssprache kompatiblen Schriftarten ab. Wenn Sie mit internationalen Zeichen erstellte Backups durchsuchen, auf Ihrem System jedoch keine kompatible Schriftart installiert ist, werden alle Zeichen, die das System nicht auflösen kann, als Rechtecke angezeigt. Hierbei handelt es sich um eine normale Beschränkung für diese bestimmte Situation, was keinerlei Einfluss auf die Wiederherstellungsfähigkeit dieser Verzeichnisse, Ordner oder Dateien hat. Unter *Avamar – Versionshinweise* sind zusätzliche Informationen zur internationalen Sprachunterstützung enthalten.

Suchen nach einem Backup nach Datum

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Restore**.

   Der Bereich links oben enthält eine Liste mit Domains.

3. Wählen Sie die Domain mit dem Client aus.

   Clients außerhalb der Domain des Anmeldekontos können nicht angezeigt werden. Melden Sie sich zum Anzeigen aller Clients bei der Root Domain an.

   Eine Liste mit Avamar Clients wird im Bereich unter der Liste mit Domains angezeigt.

4. Wählen Sie aus der Liste der Clients den Computer aus, auf dem SQL Server ausgeführt wird. Beachten Sie die folgenden Punkte, wenn Sie einen Client auswählen:

   - Wenn Sie Datenbanken in einer AlwaysOn-Verfügbarkeitsgruppe wiederherstellen, wählen Sie den Clusterclient für den Verfügbarkeitsgruppen-Listener.
   - Wenn Sie Datenbanken auf einem gemeinsamen Speicher in einem Failover-Cluster wiederherstellen, wählen Sie den Clusterclient für den virtuellen Server.

- Clients außerhalb der Domain des Anmeldekontos können nicht angezeigt werden. Melden Sie sich zum Anzeigen aller Clients bei der Root Domain an.

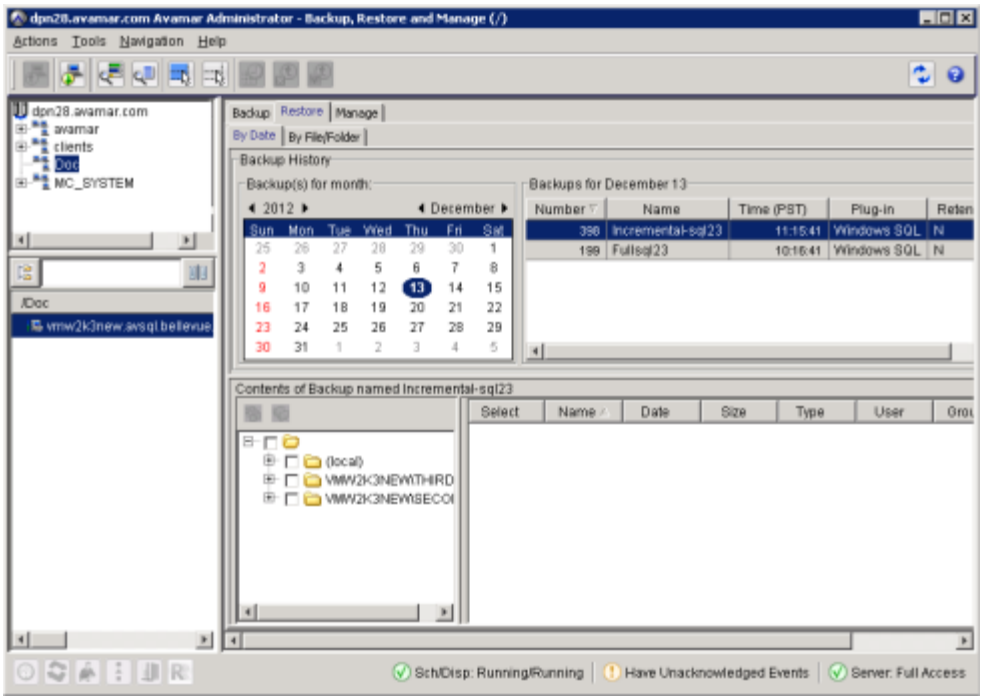
5. Klicken Sie auf die Registerkarte **Restore**.
6. Klicken Sie auf die Registerkarte **By Date**.
7. Wählen Sie das Backupdatum aus dem Kalender aus. Gültige Backups wurden an den gelb markierten Daten durchgeführt.

   Eine Liste der an diesem Datum durchgeführten Backups wird neben dem Kalender in der Tabelle **Backups** angezeigt.
   Wenn ein Backup das zweite oder spätere komplette Backup ist und Sie das Kontrollkästchen **Force incremental backup after full backup** für das Backup aktiviert haben, werden drei Backups in der Tabelle **Backups** angezeigt:

   - Das erste Backup in der Liste ist das erzwungene inkrementelles Backup Backup. Sie können dieses Backup verwenden, um über ein erzwungenes inkrementelles Backup von einem kompletten Backup wiederherzustellen.
   - Das Backup mit `forced_incremental` an der Backupbezeichnung ist das erzwungene inkrementelle Backup. Sie können dieses Backup verwenden, um über ein erzwungenes inkrementelles Backup von einem vorherigen kompletten Backup wiederherzustellen.
   - Das Backup mit `full_backup_only` an der Backupbezeichnung ist das komplette Backup.

8. Wählen Sie das wiederherzustellende Backup aus der Tabelle **Backups** aus.

Abbildung 11 Fenster Backup, Restore and Manage



Beachten Sie die folgenden Punkte, wenn Sie das Backup auswählen:

- In der Spalte **Type** im unteren rechten Bereich stehen f–0 für ein komplettes Backup, d–*n* für ein differenzielles Backup und i–*n* für ein Transaktionsprotokollbackup (inkrementell).
- Wenn Sie von einem Transaktionsprotokoll oder einem differenziellen Backup wiederherstellen, wählen Sie das Backup, das dem Datum und der Uhrzeit entspricht, zu denen Sie wiederherstellen möchten.

Während des Wiederherstellungsprozesses stellt Avamar automatisch alle erforderlichen Daten aus einem kompletten Backup wieder her. Dann stellt er gegebenenfalls die dazwischenliegenden Backupdateien wieder her und wendet sie an. Mit anderen Worten: Sie müssen nicht das komplette Backup zusätzlich zum Transaktionsprotokoll- oder differenziellen Backup auswählen.

- Wählen Sie das letzte Backup, wenn Sie vorhaben, ein Protokollfragmentbackup durchzuführen und auf einen Point-in-Time seit diesem letzten Backup wiederherzustellen. Ein Protokollfragmentbackup umfasst nur Transaktionen, die noch nicht in das Backup einbezogen wurden.

9. Wählen Sie in den zwei unteren Bereichen des Fensters **Backup, Restore and Manage** die wiederherzustellenden Daten aus:
   - Um alles, was für die Instanz aufgeführt wurde, wiederherzustellen, aktivieren Sie das Kontrollkästchen neben der Instanz in der Ordnerstruktur im unteren linken Bereich.
   - Um eine Datenbank und ihre Protokolle wiederherzustellen, erweitern Sie den Node für die Instanz in der Ordnerstruktur im unteren linken Bereich und aktivieren Sie dann das Kontrollkästchen neben der Datenbank.
   - Um eine Dateigruppe wiederherzustellen, erweitern Sie den Node für die Instanz in der Ordnerstruktur im unteren linken Bereich, wählen Sie die Datenbank im unteren linken Bereich und aktivieren Sie dann das Kontrollkästchen neben den Dateien in der Dateigruppe im unteren rechten Bereich.
     Wenn mehrere Dateien in der Dateigruppe vorhanden sind, stellen Sie sicher, dass Sie das Kontrollkästchen neben jeder Datei aktivieren, um sicherzustellen, dass Sie die gesamte Dateigruppe wiederherstellen.

     Der Name der Dateigruppe, zu der eine Datei gehört, wird in der Spalte **Filegroup** im unteren rechten Bereich angezeigt.

     Wenn Sie ein Transaktionsprotokoll- oder differenzielles Backup wiederherstellen und planen, die Dateien auf einer anderen Instanz wiederherzustellen, stellen Sie sicher, dass Sie das Kontrollkästchen neben allen Dateien in allen Dateigruppen aktivieren. Sie können keine einzelnen Dateien von einem Transaktionsprotokoll- oder differenziellen Backup auf einer anderen Instanz wiederherstellen.

Hinweis

Sie können die exakte Größe einer wiederhergestellten Datenbank erst nach Abschluss des Wiederherstellungsvorgangs genau bestimmen. Datenbankgrößen, die in Avamar Administrator angezeigt werden, wenn Sie eine Wiederherstellung durchführen, sind daher möglicherweise kleiner als wenn Sie ein Backup durchführen.

---

10. Setzen Sie die Wiederherstellung wie in den folgenden Themen beschrieben fort:
    - Wiederherstellen am ursprünglichen Speicherort auf Seite 167
    - Wiederherstellen auf einer neuen Datenbank in der ursprünglichen Instanz auf Seite 169
    - Wiederherstellen auf einer anderen Instanz auf Seite 171

- Wiederherstellen in einer Datei auf Seite 173
- Wiederherstellen von Systemdatenbanken auf Seite 182

Suchen nach einem Backup nach Inhalt

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Restore**.

   Der Bereich links oben enthält eine Liste mit Domains.
3. Wählen Sie die Domain mit dem Client aus.

   Clients außerhalb der Domain des Anmeldekontos können nicht angezeigt werden. Melden Sie sich zum Anzeigen aller Clients bei der Root Domain an.

   Eine Liste mit Avamar Clients wird im Bereich unter der Liste mit Domains angezeigt.
4. Wählen Sie aus der Liste der Clients den Computer aus, auf dem SQL Server ausgeführt wird. Beachten Sie die folgenden Punkte, wenn Sie einen Client auswählen:
   - Wenn Sie Datenbanken in einer AlwaysOn-Verfügbarkeitsgruppe wiederherstellen, wählen Sie den Clusterclient für den Verfügbarkeitsgruppen-Listener.
   - Wenn Sie Datenbanken auf einem gemeinsamen Speicher in einem Failover-Cluster wiederherstellen, wählen Sie den Clusterclient für den virtuellen Server.
   - Clients außerhalb der Domain des Anmeldekontos können nicht angezeigt werden. Melden Sie sich zum Anzeigen aller Clients bei der Root Domain an.
5. Klicken Sie auf die Registerkarte **Restore**.
6. Klicken Sie auf die Registerkarte **By File/Folder**.
7. Geben Sie im Textfeld **Enter path to retrieve history for** mit einer der in der folgenden Tabelle genannten Methoden den Pfadnamen zur Instanz oder zur Datenbank an.

Tabelle 36 Eingabe des Pfads, um den Verlauf für das Textfeld zu ermitteln

Methode	Schritte zur Angabe des Pfads
Navigieren zur Instanz oder Datenbank	a. Klicken Sie auf **Browse**. Das Dialogfeld **Select Files or Folders** wird angezeigt. b. Wählen Sie im linken Bereich in der Struktur **Clients** den Client aus. c. Erweitern Sie im mittleren Bereich den Plug-in-Node **Windows SQL**. d. Wählen Sie unter dem Plug-in-Node **Windows SQL** die SQL Server-Instanz,

Tabelle 36 Eingabe des Pfads, um den Verlauf für das Textfeld zu ermitteln (Fortsetzung)

Methode	Schritte zur Angabe des Pfads
	die die Datenbanken zur Wiederherstellung enthält. Eine Liste der Datenbanken für diese Instanz wird im rechten Bereich des Dialogfelds **Select File or Folder** angezeigt. e. Um alle Datenbanken in einer Instanz auszuwählen, aktivieren Sie das Kontrollkästchen neben der Instanz im mittleren Bereich. Um eine einzelne Datenbank auszuwählen, aktivieren Sie das Kontrollkästchen neben der Datenbank im rechten Bereich. f. Klicken Sie auf **OK**.
Angeben des Pfads für die Instanz oder Datenbank	Geben Sie im Textfeld **Enter path to retrieve history for** den vollständigen Pfad zum Clientordner bzw. zur Clientdatei in einem der folgenden Formate ein: • Um die lokale Instanz wiederherzustellen, geben Sie `(local)` ein. • Geben Sie zum Wiederherstellen einer Datenbank in der lokalen Instanz `(local) /database/` ein. • Um eine benannte Instanz wiederherzustellen, geben Sie `client\instance/` ein. • Geben Sie zum Wiederherstellen einer Datenbank in einer benannten Instanz `client\instance/database/` ein. • Geben Sie zum Wiederherstellen einer Datenbank `client/database/` ein,wenn nur eine Instanz auf dem Client vorhanden ist und es nicht die lokale Instanz ist. Dabei ist *c* der Name des Computers, auf dem SQL Server ausgeführt wird, *instance* der Name der benannten Instanz und *database* der Name der Datenbank.

8. Klicken Sie auf **Retrieve**.

   In der Tabelle **Version History** werden alle Versionen und Größen des Inhalts in Backups für den Client angegeben.

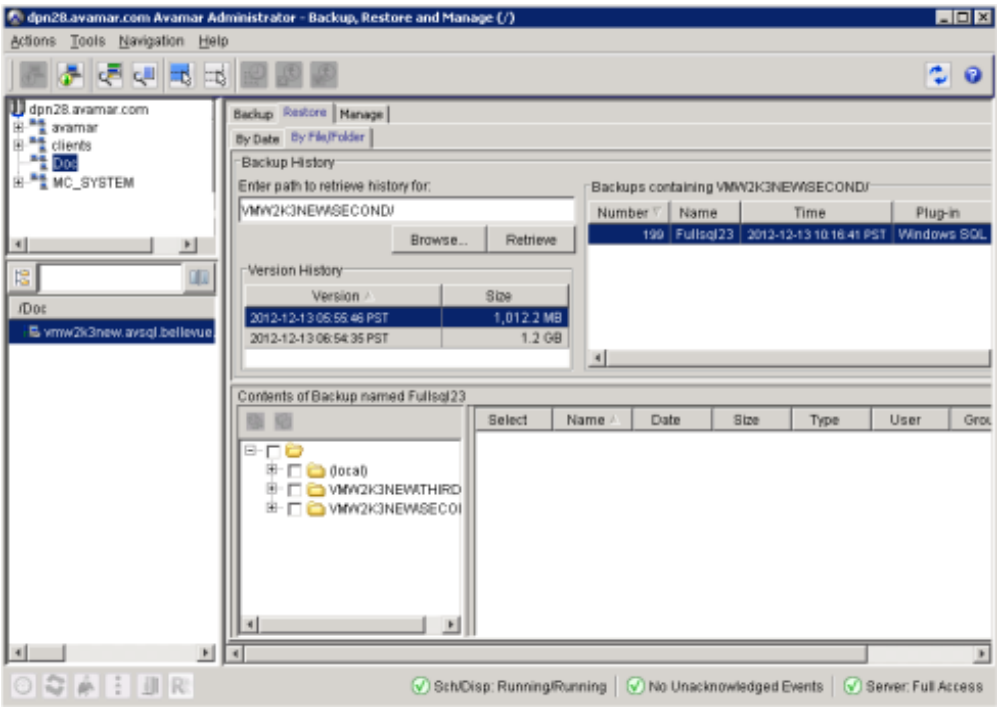
9. Wählen Sie die Version in der Tabelle **Version History** aus.

   Alle Backups für den Client, die die ausgewählte Version enthalten, werden in der Tabelle **Backups** neben der Tabelle **Version History** angezeigt.

10. Wählen Sie das wiederherzustellende Backup aus der Tabelle **Backups** aus.

    Beachten Sie die folgenden Punkte, wenn Sie das Backup auswählen:

    Abbildung 12 Fenster Backup, Restore and Manage



    - In der Spalte **Type** im unteren rechten Bereich stehen f–0 für ein komplettes Backup, d–*n* für ein differenzielles Backup und i–*n* für ein Transaktionsprotokollbackup (inkrementell).
    - Wenn Sie von einem Transaktionsprotokoll oder einem differenziellen Backup wiederherstellen, wählen Sie das Backup, das dem Datum und der Uhrzeit entspricht, zu denen Sie wiederherstellen möchten. Während des Wiederherstellungsprozesses stellt Avamar automatisch alle erforderlichen Daten aus einem kompletten Backup wieder her. Dann stellt er gegebenenfalls die dazwischenliegenden Backupdateien wieder her und wendet sie an. Mit anderen Worten: Sie müssen nicht das komplette Backup zusätzlich zum Transaktionsprotokoll- oder differenziellen Backup auswählen.
    - Wählen Sie das letzte Backup, wenn Sie vorhaben, ein Protokollfragmentbackup durchzuführen und auf einen Point-in-Time seit diesem letzten Backup wiederherzustellen. Ein Protokollfragmentbackup umfasst nur Transaktionen, die noch nicht in das Backup einbezogen wurden.

11. Wählen Sie in den zwei unteren Bereichen des Fensters **Backup, Restore and Manage** die wiederherzustellenden Daten aus:
    - Um alles, was für die Instanz aufgeführt wurde, wiederherzustellen, aktivieren Sie das Kontrollkästchen neben der Instanz in der Ordnerstruktur im unteren linken Bereich.
    - Um eine Datenbank und ihre Protokolle wiederherzustellen, erweitern Sie den Node für die Instanz in der Ordnerstruktur im unteren linken Bereich und aktivieren Sie dann das Kontrollkästchen neben der Datenbank.

- Um eine Dateigruppe wiederherzustellen, erweitern Sie den Node für die Instanz in der Ordnerstruktur im unteren linken Bereich, wählen Sie die Datenbank im unteren linken Bereich und aktivieren Sie dann das Kontrollkästchen neben den Dateien in der Dateigruppe im unteren rechten Bereich.
  Wenn mehrere Dateien in der Dateigruppe vorhanden sind, stellen Sie sicher, dass Sie das Kontrollkästchen neben jeder Datei aktivieren, um sicherzustellen, dass Sie die gesamte Dateigruppe wiederherstellen.

  Der Name der Dateigruppe, zu der eine Datei gehört, wird in der Spalte **Filegroup** im unteren rechten Bereich angezeigt.

  Wenn Sie ein Transaktionsprotokoll- oder differenzielles Backup wiederherstellen und planen, die Dateien auf einer anderen Instanz wiederherzustellen, stellen Sie sicher, dass Sie das Kontrollkästchen neben allen Dateien in allen Dateigruppen aktivieren. Sie können keine einzelnen Dateien von einem Transaktionsprotokoll- oder differenziellen Backup auf einer anderen Instanz wiederherstellen.

Hinweis

Sie können die exakte Größe einer wiederhergestellten Datenbank erst nach Abschluss des Wiederherstellungsvorgangs genau bestimmen. Datenbankgrößen, die in Avamar Administrator angezeigt werden, wenn Sie eine Wiederherstellung durchführen, sind daher möglicherweise kleiner als wenn Sie ein Backup durchführen.

12. Setzen Sie die Wiederherstellung wie in den folgenden Themen beschrieben fort:
    - Wiederherstellen am ursprünglichen Speicherort auf Seite 167
    - Wiederherstellen auf einer neuen Datenbank in der ursprünglichen Instanz auf Seite 169
    - Wiederherstellen auf einer anderen Instanz auf Seite 171
    - Wiederherstellen in einer Datei auf Seite 173
    - Wiederherstellen von Systemdatenbanken auf Seite 182

Bestimmen der Wiederherstellungsgröße für eine SQL Server-Datenbank

Verwenden Sie die folgenden Verfahren, um die Speicherplatzanforderungen der einzelnen Datenbanken im Backupsatz sowie die Gesamtplatzanforderungen zu ermitteln. Diese Verfahren bestimmen die Größe der Wiederherstellung einer Datenbank ohne Herunterladen des vollständigen Backupinhalts. Der Backup-Header wird heruntergeladen, um die Größeninformationen abzurufen.

Hinweis

Dieser Vorgangs führt möglicherweise zu einem Protokolleintrag, der besagt, dass der Vorgang extern abgebrochen wurde, und die Warnmeldung `Restore interrupted` wird angezeigt. Diese Warnung kann ignoriert werden.

Bestimmen des erforderlichen Speicherplatzes für die Wiederherstellung der Systemdatenbank

Verwenden Sie zum Ermitteln des erforderlichen Speicherplatzes zur Wiederherstellung der Datenbank das Flag --print-restore-size.

Hinweis

Verwenden Sie zum Ermitteln der Wiederherstellungsgröße der Systemdatenbank das Flag --restoresystem.

Bestimmen des erforderlichen Speicherplatzes für die Wiederherstellung einer einzigen SQL Server-Datenbank

Bestimmen Sie vor der Wiederherstellung einer einzigen SQL Server-Datenbank „DB1“ die Speicherplatzanforderungen mithilfe der CLI.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
avsql --operation=restore --server=12.34.56.78 --id=AvamarAdmin --
ap=password --path=/SQL/SQLServer1 --print-restore-size --hostname-
sql=SQLServer1 --labelnum=28 "(local)/DB1"
```

Daraufhin wird die folgende Ausgabe angezeigt:

```
================================================
Size of the Database (local)\DB1: 3.000 MB
Size of the Database (local)\DB1_log: 1.000 MB
------------------------------------------------------------------------
-----------------
Total require restore size: 4.000 MB
================================================
```

In diesem Beispiel ist DB1 der Name der Datenbank, die wiederhergestellt wird.

Bestimmen des erforderlichen Speicherplatzes für die Wiederherstellung mehrerer SQL Server-Datenbanken

Bestimmen Sie vor der Wiederherstellung mehrerer SQL Server-Datenbanken die Speicherplatzanforderungen mithilfe der CLI.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
avsql --operation=restore --server=12.34.56.78 --id=AvamarAdmin --
ap=password --path=/SQL/SQLServer1 --print-restore-size --hostname-
sql=SQLServer1 --labelnum=28 "(local)/DB2" "(local)/DB3"
```

Daraufhin wird die folgende Ausgabe angezeigt:

```
================================================
 Size of the Database (local)\DB2: 2.489 GB
 Size of the Database (local)\DB2_log: 984.4 MB
 Size of the Database (local)\DB3: 3.000 MB
 Size of the Database (local)\DB3_log: 1.000 MB
------------------------------------------------------------------------
-----------------
 Total require restore size: 3.454 GB
 ================================================
```

Wiederherstellen am ursprünglichen Speicherort

Sie können eine SQL Server-Instanz, Datenbank, Dateigruppe oder Datei am ursprünglichen Speicherort wiederherstellen.

HINWEIS

Wenn Sie in einer AlwaysOn-Verfügbarkeitsgruppe am ursprünglichen Speicherort wiederherstellen, verwenden Sie die Anweisungen unter Wiederherstellen in einer AlwaysOn-Verfügbarkeitsgruppe auf Seite 190.

Es gibt zwei Wiederherstellungsoptionen für die Wiederherstellung einer SQL Server-Instanz, Datenbank, Dateigruppe oder Datei am ursprünglichen Speicherort.

- Die Standardwiederherstellung mit Protokollfragmentbackup ist das häufigste Wiederherstellungsverfahren. Während dieses Verfahrens wird ein Protokollfragmentbackup erstellt, um die nicht im Backup enthaltenen Transaktionen zu erfassen. Die Datenbank wird dann aus dem letzten kompletten Backup sowie etwaigen differenziellen Backups bzw. Transaktionsprotokollbackups wiederhergestellt.
- Eine Wiederherstellung mit der SQL Server-Option `REPLACE`, die die Datenbank vollständig überschreibt, kann erforderlich sein, z. B. wenn eine vorherige Datenbankwiederherstellung mit dem folgenden SQL Server-Fehler im Avamar SQL-Wiederherstellungsprotokoll beendet wurde:

  ```
  One or more devices or files already exist.
  Reissue the statement using the WITH REPLACE
  option to overwrite these files and devices.
  ```

  HINWEIS

  Wenn Sie die Avamar-Option auswählen, um die SQL Server-Option `REPLACE` zu verwenden, wird ein SQL `WITH REPLACE`-Aussagesatz hinzugefügt, um den Transact-SQL-Befehl wiederherzustellen. Hierdurch wird die SQL Server-Sicherheitsprüfung überschrieben, die ein versehentliches Überschreiben einer anderen Datenbank oder Datei verhindern soll. Die Microsoft Transact-SQL-Dokumentation enthält weitere Informationen im Befehlsabschnitt `RESTORE`.

Vorgehensweise

1. Stellen Sie sicher, dass die Umgebung die Richtlinien unter Wiederherstellungsanforderungen auf Seite 155 erfüllt.
2. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
3. Suchen Sie nach dem wiederherzustellenden Backup:
   - Suchen nach einem Backup nach Datum auf Seite 159
   - Suchen nach einem Backup nach Inhalt auf Seite 162

   Das wiederherzustellende Backup ist in der Tabelle **Backups** ausgewählt.
4. Wählen Sie **Actions** > **Restore Now** aus.

   Das Dialogfeld **Restore Options** wird angezeigt.

5. Stellen Sie sicher, dass **Windows SQL** in der Liste **Restore Plug-in** angezeigt wird.
6. Wählen Sie über die Liste **Avamar encryption method** die Verschlüsselungsmethode aus, die für die Datenübertragung zwischen dem Avamar-Server und dem Client während der Wiederherstellung verwendet werden soll.

   Die Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-/Serververbindung sind von einer Reihe von Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.
7. Behalten Sie die Standardeinstellung für **Restore to the original location** bei.
8. Klicken Sie auf **More Options**.

   Das Dialogfeld **Restore Command Line Options** wird angezeigt.
9. Wählen Sie die Recovery- oder Wiederherstellungsoptionen aus:
   - Zum Erstellen eines Protokollfragmentbackups und Durchführen einer direkten Wiederherstellung mit Recovery lassen Sie die Kontrollkästchen **Use SQL REPLACE option** und **Tail-log backup** aktiviert.
   - Zum Durchführen einer direkten Wiederherstellung mit `REPLACE` aktivieren Sie die Kontrollkästchen **Use SQL REPLACE option** und deaktivieren Sie **Tail-log backup**.
10. Wenn Sie in einer AlwaysOn-Verfügbarkeitsgruppe wiederherstellen und Sie nur auf das primäre Replikat wiederherstellen wollen, aktivieren Sie das Kontrollkästchen **Restore only on primary replica**.

    Lassen Sie das Kontrollkästchen deaktiviert, um automatisch sowohl auf das primäre als auch das sekundäre Replikat wiederherzustellen.
11. Wählen Sie aus der Liste **Encryption method to Data Domain system** die Verschlüsselungsmethode für den Datentransfer während der Wiederherstellung aus, wenn das Backup in einem Data Domain-System gespeichert war.
12. Legen Sie die Plug-in-Optionen zum Wiederherstellen von Systemdatenbanken wie unter Optionen zur Wiederherstellung der Systemdatenbank auf Seite 201 beschrieben fest.
13. (Optional) Wählen Sie **Show Advanced Options** und legen Sie die erweiterten Optionen fest, wie in den folgenden Themen beschrieben:
    - Optionen für den Recovery-Vorgang auf Seite 199
    - Authentifizierungsoptionen auf Seite 202
    - Point-in-Time-Recovery-Optionen auf Seite 203
14. Ignorieren Sie die Optionen für eine umgeleitete Wiederherstellung, die nur erforderlich sind, wenn Sie an einem anderen Speicherort wiederherstellen möchten.
15. Klicken Sie im Dialogfeld **Restore Command Line Options** auf **OK**.
16. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

    Die folgende Statusmeldung wird angezeigt: `Restore initiated`.
17. Klicken Sie auf **OK**.

Weitere Erfordernisse

- Wenn Sie ein Protokollfragmentbackup durchführen und das Protokollfragmentbackup nicht abgeschlossen werden kann, kann die Wiederherstellung nicht durchgeführt werden. Prüfen Sie die Protokolldatei, um die Ursache des Problems zu bestimmen. Beheben Sie das Problem und starten Sie die Wiederherstellung erneut.

  Denken Sie daran, dass die Wiederherstellung nur die Transaktionen bis zum ausgewählten Backup umfasst, wenn Sie das Kontrollkästchen **Tail-log backup** deaktivieren, um die Erstellung des Protokollfragmentbackups zu verhindern. Möglicherweise verlieren Sie dadurch alle Transaktionen am Ende des Protokolls.
- Nachdem die Wiederherstellung erfolgreich abgeschlossen wurde, führen Sie ein komplettes Backup der Datenbank aus und deaktivieren Sie das Kontrollkästchen **Force incremental backup after full backup** in den Plug-in-Optionen für das Backup. Wenn das Kontrollkästchen aktiviert ist, wenn ein komplettes Backup nach einer Wiederherstellung durchgeführt wird, schlägt das automatisch nach kompletten Backups erstellte Transaktionsprotokollbackup fehl.

Wiederherstellen auf einer neuen Datenbank in der ursprünglichen Instanz

Sie können eine Datenbank in der ursprünglichen SQL Server-Instanz auf demselben SQL Server-Client aber mit einem neuen Datenbanknamen wiederherstellen.

Vorgehensweise

1. Stellen Sie sicher, dass die Umgebung die Richtlinien unter Wiederherstellungsanforderungen auf Seite 155 erfüllt.
2. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
3. Suchen Sie nach dem wiederherzustellenden Backup:

   - Suchen nach einem Backup nach Datum auf Seite 159
   - Suchen nach einem Backup nach Inhalt auf Seite 162

   Das wiederherzustellende Backup ist in der Tabelle **Backups** ausgewählt.
4. Wählen Sie **Actions** > **Restore Now** aus.

   Das Dialogfeld **Restore Options** wird angezeigt.
5. Stellen Sie sicher, dass **Windows SQL** in der Liste **Restore Plug-in** angezeigt wird.
6. Wählen Sie über die Liste **Avamar encryption method** die Verschlüsselungsmethode aus, die für die Datenübertragung zwischen dem Avamar-Server und dem Client während der Wiederherstellung verwendet werden soll.

   Die Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-/Serververbindung sind von einer Reihe von Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.
7. Behalten Sie die Standardeinstellung für **Restore to the original location** bei.
8. Klicken Sie auf **More Options**.

Das Dialogfeld **Restore Command Line Options** wird angezeigt.

9. Aktivieren Sie das Kontrollkästchen **Show Advanced Options**.

   Mehrere erweiterte Optionen werden in Rot angezeigt.
10. Lassen Sie das Kontrollkästchen **Use SQL REPLACE option** deaktiviert.
11. Geben Sie an, ob während der Wiederherstellung ein Protokollfragmentbackup durchgeführt werden soll, indem Sie das Kontrollkästchen **Tail-log backup** aktivieren oder deaktivieren.
12. Wenn Sie in einer AlwaysOn-Verfügbarkeitsgruppe wiederherstellen und Sie die Datenbank mit dem neuen Namen nur auf das primäre Replikat wiederherstellen wollen, aktivieren Sie das Kontrollkästchen **Restore only on primary replica**.
13. Wählen Sie aus der Liste **Encryption method to Data Domain system** die Verschlüsselungsmethode für den Datentransfer während der Wiederherstellung aus, wenn das Backup in einem Data Domain-System gespeichert war.
14. Geben Sie im Feld **New database name** den neuen Datenbanknamen an.
15. Geben Sie im Feld **Alternate database location** den Pfad an, an den die Datenbankdateien wiederhergestellt werden sollen, oder lassen Sie das Feld leer, um die Dateien am ursprünglichen Speicherort wiederherzustellen.
16. Wählen Sie den Speicherort aus, an den die Protokolldateien für die Datenbank wiederhergestellt werden sollen:
    - Um die Protokolldateien am selben Speicherort wie die Datenbank wiederherzustellen, wählen Sie **Same as alternate database location** aus der Liste **Alternate log location** aus.
    - Um die Protokolldateien an einem anderen Speicherort als der Datenbank wiederherzustellen, wählen Sie **Different location than database** aus der Liste **Alternate log location** aus und geben Sie den Pfad für die Protokolldateien im Feld **Path to alternate log location** an.
17. (Optional) Legen Sie die anderen Plug-in-Optionen, wie in den folgenden Themen beschrieben, fest:
    - Optionen für den Recovery-Vorgang auf Seite 199
    - Authentifizierungsoptionen auf Seite 202
    - Point-in-Time-Recovery-Optionen auf Seite 203
18. Ignorieren Sie die Systemdatenbankoptionen, die nur erforderlich sind, wenn Sie eine Systemdatenbank wiederherstellen.
19. Klicken Sie im Dialogfeld **Restore Command Line Options** auf **OK**.
20. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

    Die folgende Statusmeldung wird angezeigt: `Restore initiated`.
21. Klicken Sie auf **OK**.

Weitere Erfordernisse

- Wenn Sie ein Protokollfragmentbackup durchführen und das Protokollfragmentbackup nicht abgeschlossen werden kann, kann die Wiederherstellung nicht durchgeführt werden. Prüfen Sie die Protokolldatei, um die Ursache des Problems zu bestimmen. Beheben Sie das Problem und starten Sie die Wiederherstellung erneut.

  Denken Sie daran, dass die Wiederherstellung nur die Transaktionen bis zum ausgewählten Backup umfasst, wenn Sie das Kontrollkästchen **Tail-log backup**

deaktivieren, um die Erstellung des Protokollfragmentbackups zu verhindern. Möglicherweise verlieren Sie dadurch alle Transaktionen am Ende des Protokolls.

- Nachdem die Wiederherstellung erfolgreich abgeschlossen wurde, führen Sie ein komplettes Backup der Datenbank aus und deaktivieren Sie das Kontrollkästchen **Force incremental backup after full backup** in den Plug-in-Optionen für das Backup. Wenn das Kontrollkästchen aktiviert ist, wenn ein komplettes Backup nach einer Wiederherstellung durchgeführt wird, schlägt das automatisch nach kompletten Backups erstellte Transaktionsprotokollbackup fehl.

Wiederherstellen auf einer anderen Instanz

Sie können eine oder mehrere Instanzen, Datenbanken, Dateigruppen oder Dateien auf einer anderen SQL Server-Instanz auf demselben SQL Server-Client oder einem anderen SQL Server-Client wiederherstellen.

Vorgehensweise

1. Stellen Sie sicher, dass die Umgebung die Richtlinien unter Wiederherstellungsanforderungen auf Seite 155 erfüllt.
2. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
3. Suchen Sie nach dem wiederherzustellenden Backup:
   - Suchen nach einem Backup nach Datum auf Seite 159
   - Suchen nach einem Backup nach Inhalt auf Seite 162

   Das wiederherzustellende Backup ist in der Tabelle **Backups** ausgewählt.
4. Wählen Sie **Actions** > **Restore Now** aus.

   Das Dialogfeld **Restore Options** wird angezeigt.
5. Stellen Sie sicher, dass **Windows SQL** in der Liste **Restore Plug-in** angezeigt wird.
6. Wählen Sie über die Liste **Avamar encryption method** die Verschlüsselungsmethode aus, die für die Datenübertragung zwischen dem Avamar-Server und dem Client während der Wiederherstellung verwendet werden soll.

   Die Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-/Serververbindung sind von einer Reihe von Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.
7. Geben Sie den Zielclient im Feld **Feld Restore Destination Client** ein:
   - Um den ursprünglichen Client wiederherzustellen, lassen Sie die Standardeinstellung der ursprünglichen Clientdomain und des Namens unverändert.
   - Um die Wiederherstellung auf einem anderen Client durchzuführen, klicken Sie auf **Browse** und navigieren Sie anschließend zum Client.
8. Wählen Sie **Restore to a different SQL Server instance or location**.
9. Wählen Sie die Instanz auf dem Zielclient für die Wiederherstellung aus:
   a. Klicken Sie neben dem **Select the SQL instance on the destination client where the items should be restored**-Feld auf **Browse**.

Das Dialogfeld **Browse for Restore Destination** wird angezeigt.

b. Wählen Sie **Windows SQL**.

c. Aktivieren Sie im rechten Bereich das Kontrollkästchen neben der Instanz.

d. Klicken Sie auf **OK**.

10. Legen Sie den Zieldateipfad für die Datenbank und Protokolldateien zur Wiederherstellung fest:

    a. Klicken Sie auf **Set Destination**.

    Das Dialogfeld **Set Destination** wird angezeigt.

    b. Um einen Pfad für eine einzige Datei anzugeben, wählen Sie die Zeile in der Tabelle aus. Drücken Sie alternativ die **Umschalttaste**, um denselben Pfad für mehrere Dateien in der Liste anzugeben, und wählen Sie die Zeilen aus.

    c. Klicken Sie auf **Browse**.

    Das Dialogfeld **Browse for File, Folder, or Directory** wird angezeigt.

    d. Wählen Sie **Windows File System** aus.

    e. Navigieren Sie im rechten Bereich zum Kontrollkästchen für den Ordner, in dem die ausgewählten Dateien wiederhergestellt werden sollen, und aktivieren Sie es.

    f. Klicken Sie auf **OK**, um zum **Set Destination**-Dialogfeld zurückzukehren.

    g. Wiederholen Sie Schritt b bis f für die verbleibenden Zeilen im **Set Destination**-Dialogfeld.

    h. Klicken Sie auf **OK**, um zum Dialogfeld **Restore Options** zurückzukehren.

11. Klicken Sie auf **More Options**.

    Das Dialogfeld **Restore Command Line Options** wird angezeigt.

12. Aktivieren Sie das Kontrollkästchen **Show Advanced Options**.

    Mehrere erweiterte Optionen werden in Rot angezeigt.

13. Lassen Sie das Kontrollkästchen **Use SQL REPLACE option** deaktiviert.

14. Deaktivieren Sie das **Tail-log backup**-Kontrollkästchen, um das Protokollfragmentbackup zu deaktivieren. Das Protokollfragmentbackup wird nicht unterstützt, wenn Sie auf einer anderen SQL Server-Instanz wiederherstellen.

15. Wenn Sie in einer AlwaysOn-Verfügbarkeitsgruppe auf einer anderen SQL Server-Instanz wiederherstellen, aktivieren Sie das Kontrollkästchen **Restore only on primary replica**, um die Datenbank nur auf dem primären Replikat wiederherzustellen.

16. Wählen Sie aus der Liste **Encryption method to Data Domain system** die Verschlüsselungsmethode für den Datentransfer während der Wiederherstellung aus, wenn das Backup in einem Data Domain-System gespeichert war.

17. Ignorieren Sie die **System Database**-Optionen. Stellen Sie Systemdatenbanken nicht auf einer anderen Instanz wieder her.

18. (Optional) Um die Datenbank mit einem neuen Namen wiederherzustellen, geben Sie den neuen Namen im Feld **New database name** an.

19. Ignorieren Sie die verbleibenden **Redirected Restore**-Einstellungen (**Alternate database location**, **Alternate log location** und **Path to alternate log location**). Diese Einstellungen haben Sie bereits im Dialogfeld **Set Destination** angegeben.

20. (Optional) Legen Sie die anderen Plug-in-Optionen, wie in den folgenden Themen beschrieben, fest:
    - Optionen für den Recovery-Vorgang auf Seite 199
    - Authentifizierungsoptionen auf Seite 202
    - Point-in-Time-Recovery-Optionen auf Seite 203
21. Weist der Zielserver für die Wiederherstellung Version 6.1 oder früher des SQL Server-Plug-ins auf, müssen Sie die Größe des Puffers möglicherweise verringern, die SQL Server zum Lesen und Schreiben von Backup-Images verwendet. Die Größe des Puffers wurde in Version 7.0 des SQL Server-Plug-ins zur Optimierung der Backup- und Wiederherstellungsleistung erhöht.

    Um die Größe des Puffers auf die Größe vor Version 7.0 zu verringern, legen Sie das `--max-transfer-size`-Attribut auf `65536` fest (64 KB):

    a. Klicken Sie im Dialogfeld **Restore Command Line Options** auf **More**.

    b. Geben Sie **`--max-transfer-size`** im Feld **Enter Attribute** ein.

    c. Geben Sie im Feld **`Enter Attribute Value`** den Wert **65536** ein.

    d. Klicken Sie auf **+**.
22. Klicken Sie im Dialogfeld **Restore Command Line Options** auf **OK**.
23. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

    Die folgende Statusmeldung wird angezeigt: `Restore initiated`.
24. Klicken Sie auf **OK**.

Weitere Erfordernisse

Nachdem die Wiederherstellung erfolgreich abgeschlossen wurde, führen Sie ein komplettes Backup der Datenbank aus und deaktivieren Sie das Kontrollkästchen **Force incremental backup after full backup** in den Plug-in-Optionen für das Backup. Wenn das Kontrollkästchen aktiviert ist, wenn ein komplettes Backup nach einer Wiederherstellung durchgeführt wird, schlägt das automatisch nach kompletten Backups erstellte Transaktionsprotokollbackup fehl.

Wiederherstellen in einer Datei

Sie können SQL Server-Benutzer und -Systemdatenbanken aus Avamar-Backups in Betriebssystemdateien wiederherstellen.

In den folgenden Situationen empfiehlt sich diese Art von Wiederherstellung:

- Das Avamar-Plug-in für SQL Server ist nicht auf dem Zielserver installiert.
- Sie möchten die standardmäßigen SQL Server-Wiederherstellungstools für Funktionen zu verwenden, die das SQL Server-Plug-in nicht bietet.

Sie können entweder das Avamar-Plug-in für SQL Server oder das Avamar-Plug-in für das Windows-Dateisystem für das Wiederherstellen einer Datenbank in einer Datei nutzen. SQL Server-Tools können dann die Daten auf einem SQL Server wiederherstellen.

Wiederherstellen einer Datei mit dem SQL Server-Plug-in

Sie können eine Instanz oder Datenbank mithilfe des Avamar-Plug-in für SQL Server in Betriebssystemdateien wiederherstellen.

Vorgehensweise

1. Stellen Sie sicher, dass die Umgebung die Richtlinien unter Wiederherstellungsanforderungen auf Seite 155 erfüllt.
2. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
3. Suchen Sie nach dem wiederherzustellenden Backup:
   - Suchen nach einem Backup nach Datum auf Seite 159
   - Suchen nach einem Backup nach Inhalt auf Seite 162

   Das wiederherzustellende Backup ist in der Tabelle **Backups** ausgewählt.
4. Wählen Sie **Actions** > **Restore Now** aus.

   Das Dialogfeld **Restore Options** wird angezeigt.
5. Stellen Sie sicher, dass **Windows SQL** in der Liste **Restore Plug-in** angezeigt wird.
6. Wählen Sie über die Liste **Avamar encryption method** die Verschlüsselungsmethode aus, die für die Datenübertragung zwischen dem Avamar-Server und dem Client während der Wiederherstellung verwendet werden soll.

   Die Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-/Serververbindung sind von einer Reihe von Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.
7. Geben Sie den Zielclient im Feld **Feld Restore Destination Client** ein:
   - Um den ursprünglichen Client wiederherzustellen, lassen Sie die Standardeinstellung der ursprünglichen Clientdomain und des Namens unverändert.
   - Um die Wiederherstellung auf einem anderen Client durchzuführen, klicken Sie auf **Browse** und navigieren Sie anschließend zum Client.
8. Wählen Sie **Restore SQL Server backup as files to the file system**.
9. Legen Sie den Zieldateipfad für die Datenbank und Protokolldateien zur Wiederherstellung fest:
   a. Klicken Sie auf **Set Destination**.

      Das Dialogfeld **Set Destination** wird angezeigt.
   b. Klicken Sie auf **Browse**.

      Das Dialogfeld **Browse for File, Folder, or Directory** wird angezeigt.
   c. Wählen Sie **Windows File System** aus.
   d. Navigieren Sie im rechten Bereich zum Kontrollkästchen für den Ordner, in dem die ausgewählten Dateien wiederhergestellt werden sollen, und aktivieren Sie es.
   e. Klicken Sie auf **OK**, um zum **Set Destination**-Dialogfeld zurückzukehren.
   f. Klicken Sie auf **OK**, um zum Dialogfeld **Restore Options** zurückzukehren.
10. Klicken Sie auf **More Options**.

    Das Dialogfeld **Restore Command Line Options** wird angezeigt.

11. Wählen Sie aus der Liste **Encryption method to Data Domain system** die Verschlüsselungsmethode für den Datentransfer während der Wiederherstellung aus, wenn das Backup in einem Data Domain-System gespeichert war.
12. Wenn die Wiederherstellung Systemdatenbanken enthält, aktivieren Sie das **Restore system databases**-Kontrollkästchen.
13. Ignorieren Sie die verbleibenden Optionen, die beim Wiederherstellen in einer Datei nicht angewendet werden.
14. Klicken Sie im Dialogfeld **Restore Command Line Options** auf **OK**.
15. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

    Die folgende Statusmeldung wird angezeigt: `Restore initiated`.
16. Klicken Sie auf **OK**.

Ergebnisse

Das Backup wird als eine oder mehrere Dateien am angegebenen Zielspeicherort unter dem Pfad *destination*`\`*client*`\`*instance*`\`*database*`\`*file*wiederhergestellt, wobei:

- *destination* das Ziel für die Dateien ist, die Sie im Dialogfeld **Set Destination** angegeben haben.
- *client* der Name des Computers ist, auf dem der SQL Server installiert ist.
- *instance* der Name der SQL Server-Instanz des Backups ist.
- *database* der Name der Datenbank des Backups ist.
- *filename*der Name der Datei ist.

Ein einziges Backup kann abhängig von der Anzahl der Streams im Backup mehrere Dateien beinhalten. Der Dateiname jeder Datei besteht aus dem Backuptyp und der Streamanzahl:

- `f-0` für komplette Backups
- `d-`*n* für differenzielle Backups
- `i-`*n* für (inkrementelle) Backups von Transaktionsprotokollen

wobei *n* die Sequenznummer des differenziellen oder inkrementellen Backups seit dem vorhergegangenen kompletten Backup ist. Beispielsweise führt ein komplettes Backup mit zwei Ergebnissen zu zwei Dateien: `f-0.stream0` und `f-0.stream1`.

Weitere Erfordernisse

- Stellen Sie sicher, dass die SQL-Backupformatdateien, die Sie wiederhergestellt haben, für den SQL Server zugänglich sind. Möglicherweise müssen Sie die Daten für den SQL Server sichtbar machen oder die Daten kopieren.
- Stellen Sie die Datenbank mithilfe von SQL Server-Tools manuell wieder her.

Wiederherstellen in einer Datei mit dem Windows-Dateisystem-Plug-in

Sie können eine Instanz oder Datenbank mithilfe des Avamar-Plug-ins für das Windows-Dateisystem in Betriebssystemdateien wiederherstellen.

Vorgehensweise

1. Stellen Sie sicher, dass die Umgebung die Richtlinien unter Wiederherstellungsanforderungen auf Seite 155 erfüllt.
2. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

Das Fenster **Backup, Restore and Manage** wird angezeigt.

3. Suchen Sie nach dem wiederherzustellenden Backup:
   - Suchen nach einem Backup nach Datum auf Seite 159
   - Suchen nach einem Backup nach Inhalt auf Seite 162

   Das wiederherzustellende Backup ist in der Tabelle **Backups** ausgewählt.
4. Wählen Sie **Actions** > **Restore Now** aus

   Das Dialogfeld **Restore Options** wird angezeigt.
5. Wählen Sie in der Liste **Restore Plug-in Windows File System** aus.
6. Wählen Sie über die Liste **Avamar encryption method** die Verschlüsselungsmethode aus, die für die Datenübertragung zwischen dem Avamar-Server und dem Client während der Wiederherstellung verwendet werden soll.

   Die Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-/Serververbindung sind von einer Reihe von Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.
7. Geben Sie den Zielclient im Feld **Feld Restore Destination Client** ein:
   - Um den ursprünglichen Client wiederherzustellen, lassen Sie die Standardeinstellung der ursprünglichen Clientdomain und des Namens unverändert.
   - Um die Wiederherstellung auf einem anderen Client durchzuführen, klicken Sie auf **Browse** und navigieren Sie anschließend zum Client.
8. Wählen Sie **Restore everything to a different location** aus.
9. Legen Sie den Zieldateipfad für die Datenbank und Protokolldateien zur Wiederherstellung fest:
   a. Klicken Sie auf **Set Destination**.

      Das Dialogfeld **Set Destination** wird angezeigt.
   b. Klicken Sie auf **Browse**.

      Das Dialogfeld **Browse for File, Folder, or Directory** wird angezeigt.
   c. Wählen Sie **Windows File System** aus.
   d. Navigieren Sie im rechten Bereich zum Kontrollkästchen für den Ordner, in dem die ausgewählten Dateien wiederhergestellt werden sollen, und aktivieren Sie es.
   e. Klicken Sie auf **OK**, um zum **Set Destination**-Dialogfeld zurückzukehren.
   f. Klicken Sie auf **OK**, um zum Dialogfeld **Restore Options** zurückzukehren.
10. (Optional) Klicken Sie auf **More Options** und legen Sie die Plug-in-Optionen für die Wiederherstellung fest. Im *Avamar for Windows-Server – Benutzerhandbuch* finden Sie Details zu den verfügbaren Plug-in-Optionen.
11. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

    Die folgende Statusmeldung wird angezeigt: `Restore initiated`.
12. Klicken Sie auf **OK**.

Ergebnisse

Das Backup wird als eine oder mehrere Dateien am angegebenen Zielspeicherort unter dem Pfad *destination**client**instance**database**file*wiederhergestellt, wobei:

- *destination* das Ziel für die Dateien ist, die Sie im Dialogfeld **Set Destination** angegeben haben.
- *client* der Name des Computers ist, auf dem der SQL Server installiert ist.
- *instance* der Name der SQL Server-Instanz des Backups ist.
- *database* der Name der Datenbank des Backups ist.
- *filename*der Name der Datei ist.

Ein einziges Backup kann abhängig von der Anzahl der Streams im Backup mehrere Dateien beinhalten. Der Dateiname jeder Datei besteht aus dem Backuptyp und der Streamanzahl:

- `f-0` für komplette Backups
- `d-`*n* für differenzielle Backups
- `i-`*n* für (inkrementelle) Backups von Transaktionsprotokollen

wobei *n* die Sequenznummer des differenziellen oder inkrementellen Backups seit dem vorhergegangenen kompletten Backup ist. Beispielsweise führt ein komplettes Backup mit zwei Ergebnissen zu zwei Dateien: `f-0.stream0` und `f-0.stream1`.

Weitere Erfordernisse

- Stellen Sie sicher, dass die SQL-Backupformatdateien, die Sie wiederhergestellt haben, für den SQL Server zugänglich sind. Möglicherweise müssen Sie die Daten für den SQL Server sichtbar machen oder die Daten kopieren.
- Stellen Sie die Datenbank mithilfe von SQL Server-Tools manuell wieder her.

Wiederherstellen einer Datenbank mit SQL Server-Tools

Wenn Sie das SQL Server-Plug-in oder das Windows File System-Plug-in verwenden, um ein SQL Server-Backup in einer Datei wiederherzustellen, können Sie die SQL Server-Tools zur Wiederherstellung einer Datenbank auf einem SQL Server verwenden. SQL Server Management Studio, ein Transact-SQL `RESTORE`-Befehl und das `sqlcmd`-Utility werden unterstützt.

Wiederherstellen einer Datenbank mit SQL Server Management Studio

Über die Benutzeroberfläche in SQL Server Management Studio können Sie eine Datenbank aus einer SQL-formatierten Backupdatei auf einem SQL Server wiederherstellen. Die Microsoft-Website enthält nähere Informationen zur Verwendung von SQL Server Management Studio zur Wiederherstellung von Datenbankbackups.

Dieses Verfahren bietet Details zur Verwendung von SQL Server Management Studio für SQL Server 2008 zur Wiederherstellung einer Datenbank aus SQL-formatierten Backupdateien. Die Schritte für andere SQL Server-Versionen können abweichen.

Vorgehensweise

1. Wiederherstellen des Datenbankbackups in einer Datei mithilfe der Anweisungen in einem der folgenden Themen:
   - Wiederherstellen einer Datei mit dem SQL Server-Plug-in auf Seite 173

- Wiederherstellen in einer Datei mit dem Windows-Dateisystem-Plug-in auf Seite 175

2. Stellen Sie sicher, dass die SQL-Backupformatdateien, die Sie wiederhergestellt haben, für den SQL Server zugänglich sind. Möglicherweise müssen Sie die Daten für den SQL Server sichtbar machen oder die Daten kopieren.
3. Stellen Sie das komplette Backup (`f-0`-Datei) auf SQL Server wieder her:
   a. Öffnen Sie das **Restore Database**-Fenster.
      - Wenn die Datenbank bereits vorhanden ist, klicken Sie mit der rechten Maustaste auf die Datenbank im **Object Explorer** und wählen Sie **Tasks** > **Restore** > **Database**.
      - Wenn die Datenbank verloren gegangen ist, klicken Sie mit der rechten Maustaste auf den **Databases**-Node im **Object Explorer** und wählen Sie **Restore Database**.

   b. Wählen Sie auf der Seite **General** im Fenster **Restore Database From device**.
   c. Klicken Sie auf die Schaltfläche **...**.

      Das Dialogfeld **Specify Backup** wird angezeigt.
   d. Klicken Sie auf **Add**.

      Das Dialogfeld **Locate Backup File** wird angezeigt.
   e. Wählen Sie den Ordner, in dem sich die kompletten Backupdateien befinden.
   f. Wählen Sie in der Liste **Files of type All files(*)**.
   g. Wählen Sie die komplette Backupdatei (`f-0`).
   h. Klicken Sie auf **OK**.
   i. Wenn mehrere komplette Backupdateien durch Multistreaming vorhanden sind (z. B. `f-0.stream0`, `f-0.stream1`, `f-0.stream2` usw.), wiederholen Sie Schritt d bis h, um jede Datei hinzufügen.
   j. Klicken Sie auf **OK** im **Specify Backup**-Dialogfeld.
   k. Aktivieren Sie auf der **General**-Seite im Fenster **Restore Database** die Kontrollkästchen neben den wiederherzustellenden Backupdateien.
   l. Klicken Sie im linken Bereich auf **Options**, um die **Options**-Seite zu öffnen.
   m. Wählen Sie in der **Restore the database files as**-Liste jede Datei aus und klicken Sie auf die Schaltfläche **...**, um den Wiederherstellungsort für die Dateien anzugeben.
   n. Wählen Sie unter **Recovery state RESTORE WITH NORECOVERY**.
   o. Klicken Sie auf **OK**, um mit der Wiederherstellung zu beginnen.
4. Stellen Sie die differenziellen (`d-n`) oder Transaktionsprotokolldateien (`i-n`) wieder her, beginnend bei der ältesten:
   a. Klicken Sie mit der rechten Maustaste auf die Datenbank im **Object Explorer** und wählen Sie **Tasks** > **Restore** > **Database**.
   b. Wählen Sie auf der Seite **General** im Fenster **Restore Database From device**.
   c. Klicken Sie auf die Schaltfläche **...**.

      Das Dialogfeld **Specify Backup** wird angezeigt.

d. Klicken Sie auf **Add**.

Das Dialogfeld **Locate Backup File** wird angezeigt.

e. Wählen Sie den Ordner, in dem sich die differenziellen oder Transaktionsprotokoll-Backupdateien befinden.

f. Wählen Sie in der Liste **Files of type All files(*)**.

g. Wählen Sie die differenzielle (`d-n`) oder Transaktionsprotokoll-Backupdatei (`i-n`), wobei *n* die Sequenznummer des differenziellen oder inkrementellen Backups seit dem vorhergegangenen kompletten Backup ist.

h. Klicken Sie auf **OK**.

i. Wenn mehrere differenzielle oder Transaktionsprotokoll-Backupdateien durch Multi-Streaming vorhanden sind (z. B. `d-3.stream0`, `d-3.stream1`, `d-3.stream2` oder `i-6.stream0`, `i-6.stream1`, `i-6.stream2` und `i-6.stream3`), wiederholen Sie Schritt d bis h, um jede Datei hinzufügen.

j. Klicken Sie auf **OK** im **Specify Backup**-Dialogfeld.

k. Aktivieren Sie auf der **General**-Seite im Fenster **Restore Database** die Kontrollkästchen neben den wiederherzustellenden Backupdateien.

l. Klicken Sie im linken Bereich auf **Options**, um die **Options**-Seite zu öffnen.

m. Wählen Sie in der **Restore the database files as**-Liste jede Datei aus und klicken Sie auf die Schaltfläche **...**, um den Wiederherstellungsort für die Dateien anzugeben.

n. Wählen Sie als **Recovery state RESTORE WITH NORECOVERY** für alle Backupdateien bis auf die aktuelle. Wenn Sie die aktuelle Backupdatei wiederherstellen, wählen Sie **RESTORE WITH RECOVERY**.

o. Klicken Sie auf **OK**, um mit der Wiederherstellung zu beginnen.

5. Wenn die Datenbank in SQL Server Management Studio nicht bereits aufgeführt ist, aktualisieren Sie die Liste oder stellen Sie eine Verbindung zur Datenbank her.

Weitere Erfordernisse

Nachdem die Wiederherstellung erfolgreich abgeschlossen wurde, führen Sie ein komplettes Backup der Datenbank aus und deaktivieren Sie das Kontrollkästchen **Force incremental backup after full backup** in den Plug-in-Optionen für das Backup. Wenn das Kontrollkästchen aktiviert ist, wenn ein komplettes Backup nach einer Wiederherstellung durchgeführt wird, schlägt das automatisch nach kompletten Backups erstellte Transaktionsprotokollbackup fehl.

Wiederherstellen einer Datenbank mit einem Transact-SQL RESTORE-Befehl

Sie können einen Transact-SQL `RESTORE`-Befehl zur Wiederherstellung einer Datenbank von einer SQL-formatierten Backupdatei auf einen SQL Server ausführen. Die Microsoft-Website enthält nähere Informationen zum Ausführen eines Transact-SQL-Befehls, einschließlich Details zu den verfügbaren Optionen für den `RESTORE`-Befehl.

Vorgehensweise

1. Wiederherstellen des Datenbankbackups in einer Datei mithilfe der Anweisungen in einem der folgenden Themen:

- Wiederherstellen einer Datei mit dem SQL Server-Plug-in auf Seite 173
- Wiederherstellen in einer Datei mit dem Windows-Dateisystem-Plug-in auf Seite 175

2. Stellen Sie sicher, dass die SQL-Backupformatdateien, die Sie wiederhergestellt haben, für den SQL Server zugänglich sind. Möglicherweise müssen Sie die Daten für den SQL Server sichtbar machen oder die Daten kopieren.
3. Wiederherstellen des kompletten Backups (`f-0`-Datei) auf einen SQL Server mit einem Transact-SQL-Befehl ähnlich dem folgenden:

   ```
   RESTORE DATABASE dbname FROM DISK = 'drive:\folder\f-0.stream0'
   WITH MOVE 'dbname_data' TO 'drive:\folder\dbname.mdf', MOVE
   'dbname_logfile' TO 'drive:\folder\dbname.ldf', NORECOVERY
   ```

   Hierbei gilt:

   - *dbname* ist der Name der Datenbank, die wiederhergestellt werden soll.
   - Die `FROM DISK`-Klausel gibt die Backupdatei an, aus der wiederhergestellt werden soll, und *drive:\folder\f-0.stream0* ist der Pfad und der Dateiname der kompletten Backupdatei.
   - Die `MOVE`-Klausel gibt den Pfad und Namen für die wiederhergestellten Dateien an:
     - *dbname_data* ist der Name der Datenbankdatendatei im Backup.
     - *drive:\folder\dbname.mdf* ist der Pfad und der Name für die wiederhergestellte Datenbankdatei.
     - *dbname_logfile* ist der Name der Datenbankprotokolldatei im Backup.
     - *drive:\folder\dbname.mdf* ist der Pfad und der Name für die wiederhergestellte Datenbankprotokolldatei.
   - Durch die `NORECOVERY`-Option wird festgelegt, dass die Datenbank im Wiederherstellungsstatus bleibt, wodurch Sie zusätzliche Backups wiederherstellen können, bevor Sie die Datenbank online festlegen.

4. Stellen Sie alle bis auf die aktuellen differenziellen (`d-n`) oder Transaktionsprotkoll-Backupdateien (`i-n`) mit dem Transact-SQL-Befehl wieder her, beginnend bei der ältesten Datei, ähnlich dem Befehl aus dem vorherigen Schritt. Ersetzen Sie dabei jedoch den *f-0.stream0*-Dateinamen in der `FROM DISK`-Klausel durch den Dateinamen für die differenzielle oder Transaktionsprotokoll-Backupdatei.
5. Stellen Sie die aktuellen differenziellen oder Transaktionsprotkoll-Backupdateien mit dem Transact-SQL-Befehl wieder her, ähnlich dem Befehl aus dem vorherigen Schritt:

   ```
   RESTORE DATABASE dbname FROM DISK = 'drive:\folder\i-7.stream0'
   WITH MOVE 'dbname_data' TO 'drive:\folder\dbname.mdf', MOVE
   'dbname_logfile' TO 'drive:\folder\dbname.ldf', RECOVERY
   ```

   Hierbei gilt:

   - *dbname* ist der Name der Datenbank, die wiederhergestellt werden soll.
   - Die `FROM DISK`-Klausel gibt die Backupdatei an, aus der wiederhergestellt werden soll, und *drive:\folder\i-7.stream0* ist der Pfad und der Dateiname der aktuellen Transaktionsprotokoll-Backupdatei.

- Die `MOVE`-Klausel gibt den Pfad und Namen für die wiederhergestellten Dateien an:
  - *dbname_data* ist der Name der Datenbankdatendatei im Backup.
  - *drive:\folder\dbname.mdf* ist der Pfad und der Name für die wiederhergestellte Datenbankdatei.
  - *dbname_logfile* ist der Name der Datenbankprotokolldatei im Backup.
  - *drive:\folder\dbname.mdf* ist der Pfad und der Name für die wiederhergestellte Datenbankprotokolldatei.
- Die `RECOVERY`-Option stellt die Datenbank nach der Wiederherstellung online.

6. Wenn die Datenbank in SQL Server Management Studio nicht bereits aufgeführt ist, aktualisieren Sie die Liste oder stellen Sie eine Verbindung zur Datenbank her.

Weitere Erfordernisse

Nachdem die Wiederherstellung erfolgreich abgeschlossen wurde, führen Sie ein komplettes Backup der Datenbank aus und deaktivieren Sie das Kontrollkästchen **Force incremental backup after full backup** in den Plug-in-Optionen für das Backup. Wenn das Kontrollkästchen aktiviert ist, wenn ein komplettes Backup nach einer Wiederherstellung durchgeführt wird, schlägt das automatisch nach kompletten Backups erstellte Transaktionsprotokollbackup fehl.

Wiederherstellen einer Datenbank mit dem Utility sqlcmd

Das `sqlcmd`-Utility ist ein Befehlszeilen-Utility für die Eingabe von Transact-SQL-Anweisungen und Skripten. Sie können eine Datenbank von einer Backupdatei durch Angabe der Transact-SQL `RESTORE`-Anweisungen mit dem Utility `sqlcmd` wiederherstellen. Die Microsoft-Website enthält alle Einzelheiten zur Verwendung des Utility `sqlcmd`.

Hinweis

Sie können das Microsoft SQL Server-Utility `osql` verwenden, aber Microsoft empfiehlt das Utility `sqlcmd`.

Wiederherstellen einer einzigen Datenbank von einer einzigen kompletten Backupdatei

```
sqlcmd -S server -E1> restore database dbname2> from disk = 'drive:
\folder\f-0.stream0'3> with recovery;4> go
```

Hierbei gilt:

- *server* ist der Server, der SQL Server und optional die Instanz ausführt, auf der das Backup wiederhergestellt wird.
- *dbname* ist die Datenbank, die wiederhergestellt werden soll.
- *drive:\folder\f-0.stream0* ist der Pfad und der Dateiname der Backupdatei, über die die Datenbank wiederhergestellt wird.

Ermittlung der Anzahl und Namen der Dateien in der wiederherzustellenden Datenbank

```
sqlcmd -S server -E1> restore filelistonly2> from disk = 'drive:
\folder\f-0.stream0'3> go1> restore database dbname2> from disk =
```

```
'drive:\folder\f-0.stream0'3> with norecovery,4> move 'dbname_data' to
'drive:\dbname.mdf',5> move 'dbname_log' to 'drive:\dbname.ldf'6> go
```

Wiederherstellen einer Datenbank auf einen Point-in-Time mithilfe der STOPAT-Syntax

```
RESTORE DATABASE dbnameFROM disk= 'drive:\folder\f-0.stream0'WITH
NORECOVERY, STOPAT = 'Apr 25, 2014 12:00 AM'goRESTORE LOG dbnameFROM
disk= 'drive:\folder\i-1.stream0'WITH RECOVERY, STOPAT = 'Apr 25, 2013
12:00 AM'go
```

Hierbei gilt:

- *dbname* ist die Datenbank, die wiederhergestellt werden soll.
- *drive:\folder\f-0.stream0* ist der Pfad und der Dateiname der kompletten Backupdatei, über die die Datenbank wiederhergestellt wird.
- *drive:\folder\i-1.stream0* ist der Pfad und der Dateiname der Transaktionsprotokoll-Backupdatei, über die wiederhergestellt wird.

Durchführen eines kompletten Backups nach der Wiederherstellung
Nachdem die Wiederherstellung erfolgreich abgeschlossen wurde, führen Sie ein komplettes Backup der Datenbank aus und deaktivieren Sie das Kontrollkästchen **Force incremental backup after full backup** in den Plug-in-Optionen für das Backup. Wenn das Kontrollkästchen aktiviert ist, wenn ein komplettes Backup nach einer Wiederherstellung durchgeführt wird, schlägt das automatisch nach kompletten Backups erstellte Transaktionsprotokollbackup fehl.

Wiederherstellen von Systemdatenbanken

Nur selten ist es erforderlich, ausschließlich Systemdatenbanken wiederherzustellen. Dies kann der Fall sein, wenn in einer oder mehreren Systemdatenbanken Fehler aufgetreten sind. Beim Wiederherstellen von Systemdatenbanken, kann das Avamar-Plug-in für SQL Server automatisch die Datenbanken in der richtigen Reihenfolge wiederherstellen und SQL Server-Services managen. Falls erforderlich, können Sie jedoch einzelne Systemdatenbanken wiederherstellen und die Services manuell managen.

HINWEIS

Systemdatenbanken in einer Replikationsumgebung umfassen das Veröffentlichen, Verteilen und Abonnieren von Abonnementdatenbanken. Die Schritte zum Wiederherstellen dieser Datenbanken und anderer Systemdatenbanken in einer SQL Server-Replikationsumgebung hängen von der Replikationskonfiguration ab und werden nicht in diesem Leitfaden behandelt. Das SQL Server-Plug-in kann automatisch die Datenbanken in der richtigen Reihenfolge wiederherstellen und SQL Server-Services managen. Die Schritte zum manuellen Wiederherstellen von Datenbanken in einer Replikationsumgebung werden nicht in diesem Leitfaden behandelt. Lesen Sie das Thema „Back Up and Restore Replicated Databases“ in der SQL Server-Dokumentation auf der MSDN-Website, um ausführliche Schritte zum manuellen Wiederherstellen von Systemdatenbanken in einer Replikationsumgebung zu erhalten.

Automatisches Wiederherstellen von Systemdatenbanken am ursprünglichen Speicherort

Wenn Sie mehrere Systemdatenbanken am ursprünglichen Speicherort wiederherstellen, stellt das Avamar-Plug-in für SQL Server automatisch die Datenbanken in der richtigen Reihenfolge wieder her. Das SQL Server-Plug-In kann auch automatisch das Anhalten und Neustarten der erforderlichen SQL Server-Services während der Wiederherstellung managen.

Bevor Sie beginnen

- Stellen Sie sicher, dass die Umgebung die Richtlinien unter Wiederherstellungsanforderungen auf Seite 155 erfüllt.
- Schließen Sie alle Instanzen von SQL Server Management Studio und deaktivieren Sie alle anderen möglichen Verbindungen mit den Systemdatenbanken. Wenn andere Verbindungen mit den Systemdatenbanken vorhanden sind, kann Avamar möglicherweise die Masterdatenbank nicht wiederherstellen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Suchen Sie nach dem Backup und wählen Sie die für die Wiederherstellung zu verwendende Systemdatenbank aus:
   - Suchen nach einem Backup nach Datum auf Seite 159
   - Suchen nach einem Backup nach Inhalt auf Seite 162
3. Wählen Sie **Actions** > **Restore Now** aus.

   Das Dialogfeld **Restore Options** wird angezeigt.
4. Stellen Sie sicher, dass **Windows SQL** in der Liste **Restore Plug-in** angezeigt wird.
5. Wählen Sie über die Liste **Avamar encryption method** die Verschlüsselungsmethode aus, die für die Datenübertragung zwischen dem Avamar-Server und dem Client während der Wiederherstellung verwendet werden soll.

   Die Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-/Serververbindung sind von einer Reihe von Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.
6. Behalten Sie die Standardeinstellung für **Restore to the original location** bei.

   Wenn Sie die Systemdatenbanken in einer Datei wiederherstellen möchten, befolgen Sie die Schritte in Wiederherstellen in einer Datei auf Seite 173 anstelle der Schritte in diesem Verfahren.
7. Klicken Sie auf **More Options**.

   Das Dialogfeld **Restore Command Line Options** wird angezeigt.
8. Aktivieren Sie das **Use SQL REPLACE option**-Kontrollkästchen.
9. Deaktivieren Sie das Kontrollkästchen **Tail-log backup**.
10. Wählen Sie aus der Liste **Encryption method to Data Domain system** die Verschlüsselungsmethode für den Datentransfer während der

Wiederherstellung aus, wenn das Backup in einem Data Domain-System gespeichert war.

11. Aktivieren Sie das Kontrollkästchen **Restore system databases**.
12. Aktivieren Sie das Kontrollkästchen **Manage SQL services automatically during restore**.
13. (Optional) Aktivieren Sie das Kontrollkästchen **Show Advanced Options** und legen Sie die anderen Plug-in-Optionen fest, wie in den folgenden Themen beschrieben:
    - Optionen für den Recovery-Vorgang auf Seite 199
    - Authentifizierungsoptionen auf Seite 202
14. Ignorieren Sie die Optionen für umgeleitete Wiederherstellungen, die nur erforderlich sind, wenn Sie an einem anderen Speicherort wiederherstellen möchten.
15. Ignorieren Sie die Optionen für eine Recovery auf einen Point-inTime, die nur für Datenbanken unterstützt werden, die das vollständige Recovery-Modell verwenden.
16. Klicken Sie im Dialogfeld **Restore Command Line Options** auf **OK**.
17. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

    Die folgende Statusmeldung wird angezeigt: `Restore initiated`.
18. Klicken Sie auf **OK**.

Manuelles Wiederherstellen von Systemdatenbanken am ursprünglichen Speicherort

Wenn Sie manuell Systemdatenbanken am ursprünglichen Speicherort wiederherstellen, müssen Sie in der richtigen Reihenfolge die Services managen und Datenbanken wiederherstellen.

HINWEIS

Die Schritte zum Wiederherstellen von Systemdatenbanken in einer SQL Server-Replikationsumgebung hängen von der Replikationskonfiguration ab und werden nicht in diesem Leitfaden behandelt. Lesen Sie das Thema „Back Up and Restore Replicated Databases“ in der SQL Server-Dokumentation auf der MSDN-Website, um ausführliche Schritte zum manuellen Wiederherstellen von Systemdatenbanken in einer Replikationsumgebung zu erhalten.

Vorgehensweise

1. Fahren Sie die SQL Server-Instanz herunter und stellen Sie sicher, dass abhängige Services, z. B. der SQL Server Agent-Service und der Analysis Service beendet sind.
2. Schließen Sie alle Instanzen von SQL Server Management Studio und deaktivieren Sie alle anderen möglichen Verbindungen mit den Systemdatenbanken.

   Wenn andere Verbindungen mit den Systemdatenbanken vorhanden sind, kann Avamar möglicherweise die Masterdatenbank nicht wiederherstellen.
3. Starten Sie die SQL Server-Instanz im Einzelbenutzermodus durch Ausführen der `sqlservr.exe`-Anwendung mit den Optionen `-m` und `-c`:

- Um die Standardinstanz im Einzelbenutzermodus zu starten, öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus:

  ```
  cd \MSSQLPATH\Binnsqlservr.exe -m -c
  ```

- Um die benannte Instanz im Einzelbenutzermodus zu starten, öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus:

  ```
  cd \MSSQLPATH\Binnsqlservr.exe instance -m -c
  ```

wobei *\MSSQLPATH\Binn* der Pfad zum `Binn`-Ordner für die Instanz ist und *instance* der Name der zu startenden Instanz.

4. Warten Sie, bis die `Recovery Complete`-Meldung in der Konsole angezeigt wird.

   Wenn Sie sich am SQL Server-Computer als lokaler oder Domainadministrator anmelden, während die SQL-Services unter dem lokalen Systemkonto ausgeführt werden, schlägt möglicherweise der `sqlservr.exe`-Befehl fehl, der die SQL-Services korrekt im Einzelbenutzermodus startet. In diesem Fall führen Sie Schritte 4.a auf Seite 185 bis 4.e auf Seite 185 aus, anstatt `sqlservr.exe` über die Befehlszeile auszuführen. Andernfalls fahren Sie mit Schritt 5 auf Seite 185 fort.

   Führen Sie die folgenden Schritte aus, wenn die SQL-Services nicht korrekt im Einzelbenutzermodus gestartet werden:

   a. Stoppen Sie den SQL-Service: Wenn der SQL Server auf einem eigenständigen Server installiert ist, verwenden Sie die Windows Services-Konsole. Wenn der SQL Server in einem Cluster installiert ist, verwenden Sie Cluster Manager.

   b. Klicken Sie mit der rechten Maustaste auf den SQL-Service in der Windows **Services**-Konsole und klicken Sie dann auf **Properties**.

   c. Geben Sie im Feld **Start parameters** `-m -c` ein.

   d. Klicken Sie auf **Start**, um den Service zu starten.

   e. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

5. Stellen Sie die Masterdatenbank am ursprünglichen Speicherort wieder her:

   a. Stellen Sie sicher, dass die Umgebung die Richtlinien unter Wiederherstellungsanforderungen auf Seite 155 erfüllt.

   b. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

      Das Fenster **Backup, Restore and Manage** wird angezeigt.

   c. Suchen Sie nach dem Backup und wählen Sie die für die Wiederherstellung zu verwendende Masterdatenbank aus:

      - Suchen nach einem Backup nach Datum auf Seite 159
      - Suchen nach einem Backup nach Inhalt auf Seite 162

   d. Wählen Sie **Actions** > **Restore Now** aus

      Das Dialogfeld **Restore Options** wird angezeigt.

   e. Stellen Sie sicher, dass **Windows SQL** in der Liste **Restore Plug-in** angezeigt wird.

f. Wählen Sie über die Liste **Avamar encryption method** die Verschlüsselungsmethode aus, die für die Datenübertragung zwischen Avamar-Server und Client während der Wiederherstellung verwendet werden soll.

   Die Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-/Serververbindung sind von einer Reihe von Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.

g. Behalten Sie die Standardeinstellung für **Restore to the original location** bei.

h. Klicken Sie auf **More Options**.

   Das Dialogfeld **Restore Command Line Options** wird angezeigt.

i. Aktivieren Sie das Kontrollkästchen neben der Option **Use SQL REPLACE** und **Restore system databases**.

j. Deaktivieren Sie das Kontrollkästchen **Tail-log backup**.

k. (Optional) Wählen Sie **Show Advanced Options** und legen Sie die Authentifizierungsoptionen wie unter Authentifizierungsoptionen auf Seite 202 beschrieben fest.

l. Ignorieren Sie die verbleibenden Wiederherstellungsoptionen, die beim Wiederherstellen der Masterdatenbank nicht angewendet werden.

m. Klicken Sie im Dialogfeld **Restore Command Line Options** auf **OK**.

n. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

   Die folgende Statusmeldung wird angezeigt: `Restore initiated.`

o. Klicken Sie auf **OK**.

Nachdem Sie die Masterdatenbank wiederhergestellt haben, wird der SQL Server-Service automatisch beendet.

6. Starten Sie die SQL Server-Services neu:
   - Um die standardmäßige Instanz von SQL Server zu starten, öffnen Sie eine Eingabeaufforderung und geben Sie **`net start MSSQLServer`** ein.
   - Um eine benannte Instanz von SQL Server zu starten, öffnen Sie eine Eingabeaufforderung und geben Sie **`net start MSSQL$`*`instance`*** ein, wobei *instance* der Name der Instanz ist.
7. Stellen Sie die msdb- und Modelldatenbanken wieder her:
   a. Stellen Sie sicher, dass die Umgebung die Richtlinien unter Wiederherstellungsanforderungen auf Seite 155 erfüllt.
   b. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

      Das Fenster **Backup, Restore and Manage** wird angezeigt.

   c. Suchen Sie nach dem Backup und wählen Sie die für die Wiederherstellung zu verwendenden msdb- und Modelldatenbank aus:
      - Suchen nach einem Backup nach Datum auf Seite 159
      - Suchen nach einem Backup nach Inhalt auf Seite 162

d. Wählen Sie **Actions** > **Restore Now** aus

   Das Dialogfeld **Restore Options** wird angezeigt.

e. Stellen Sie sicher, dass **Windows SQL** in der Liste **Restore Plug-in** angezeigt wird.

f. Wählen Sie über die Liste **Avamar encryption method** die Verschlüsselungsmethode aus, die für die Datenübertragung zwischen Avamar-Server und Client während der Wiederherstellung verwendet werden soll.

   Die Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-/Serververbindung sind von einer Reihe von Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Zusätzliche Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.

g. Behalten Sie die Standardeinstellung für **Restore to the original location** bei.

h. Klicken Sie auf **More Options**.

   Das Dialogfeld **Restore Command Line Options** wird angezeigt.

i. Aktivieren Sie das Kontrollkästchen neben der Option **Use SQL REPLACE** und **Restore system databases**.

j. Deaktivieren Sie das Kontrollkästchen **Tail-log backup**.

k. (Optional) Wählen Sie **Show Advanced Options** und legen Sie die Authentifizierungsoptionen wie unter Authentifizierungsoptionen auf Seite 202 beschrieben fest.

l. Ignorieren Sie die verbleibenden Wiederherstellungsoptionen, die beim Wiederherstellen der msdb- und Modelldatenbanken nicht angewendet werden.

m. Klicken Sie im Dialogfeld **Restore Command Line Options** auf **OK**.

n. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

   Die folgende Statusmeldung wird angezeigt: `Restore initiated.`

o. Klicken Sie auf **OK**.

8. Falls erforderlich, starten Sie den SQL Server Agent-Service neu:
   - Um die standardmäßige Instanz von SQL Server Agent zu starten, öffnen Sie eine Eingabeaufforderung und geben Sie **`net start SQLSERVERAGENT`** ein.
   - Um eine benannte Instanz von SQL Server zu starten, öffnen Sie eine Eingabeaufforderung und geben Sie **`net start SQLAGENT$`*`instance`*** ein, wobei *instance* der Name der Instanz ist.

Wiederherstellen von Systemdatenbanken auf einer anderen Instanz

Beim Wiederherstellen von Systemdatenbanken auf einer anderen Instanz überschreibt der Wiederherstellungsprozess die Systemdatenbanken in der Zielinstanz. Sie müssen die Masterdatenbank wiederherstellen, bevor Sie andere Systemdatenbanken wiederherstellen können. Sie können die Modell- und msdb-Datenbanken separat oder gleichzeitig wiederherstellen.

Bevor Sie beginnen

- Die SQL Server-Zielinstallation für die Wiederherstellung muss dieselbe SQL Server-Version und dasselbe Service Pack aufweisen wie die SQL Server-Installation, auf der das Backup stattgefunden hat.
- Der Name der Zielinstanz für die Wiederherstellung ist identisch mit der ursprünglichen SQL Server-Instanz für das Backup.
- Das Benutzerkonto und die Domain für die Authentifizierung auf der SQL Server-Zielinstanz sind identisch mit der ursprünglichen Instanz von SQL Server für das Backup.
- Schließen Sie alle Instanzen von SQL Server Management Studio auf der SQL Server-Zielinstallation und deaktivieren Sie alle anderen möglichen Verbindungen mit den Systemdatenbanken. Wenn andere Verbindungen mit den Systemdatenbanken vorhanden sind, kann Avamar möglicherweise die Masterdatenbank nicht wiederherstellen.
- Stellen Sie sicher, dass keine `avsql`- oder `avtar`-Prozesse auf der SQL Server-Zielinstallation ausgeführt werden.

Sie müssen die Master- und Modelldatenbankdateien im selben Dateisystempfad auf dem Zielserver wiederherstellen, wie den Dateisystempfad auf dem Originalserver für das Backup. Sie können die msdb-Datenbankdateien an einem anderen Speicherort im Dateisystem wiederherstellen. Zum Wiederherstellen der msdb-Datenbankdateien an einem anderen Speicherort im Dateisystem stellen Sie die msdb-Datenbank in einem separaten Wiederherstellungsvorgang als die Modelldatenbank wieder her und wählen Sie den Zieldateisystem-Speicherort für die wiederhergestellten Dateien aus.

Zum Ändern des Dateisystemspeicherorts der Master- und Modelldatenbankdateien stellen Sie die Datenbankdateien am selben Dateisystemspeicherort auf der Zielinstanz wieder her und verschieben Sie die Dateien dann manuell, wie im Artikel „Move System Databases“ auf der MSDN-Website unter http://msdn.microsoft.com/de-de/library/ms345408%28v=sql.110%29.aspx beschrieben.

Vorgehensweise

1. Stellen Sie die Masterdatenbanken auf der Zielinstanz wieder her:
   a. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

      Das Fenster **Backup, Restore and Manage** wird angezeigt.

   b. Suchen Sie nach dem Backup und wählen Sie die für die Wiederherstellung zu verwendende Masterdatenbank aus:

      - Suchen nach einem Backup nach Datum auf Seite 159
      - Suchen nach einem Backup nach Inhalt auf Seite 162

   c. Wählen Sie **Actions** > **Restore Now** aus.

      Das Dialogfeld **Restore Options** wird angezeigt.

   d. Stellen Sie sicher, dass **Windows SQL** in der Liste **Restore Plug-in** angezeigt wird.

   e. Wählen Sie über die Liste **Avamar encryption method** die Verschlüsselungsmethode aus, die für die Datenübertragung zwischen dem Avamar-Server und dem Client während der Wiederherstellung verwendet werden soll.

   f. Geben Sie den Zielclient im Feld **Restore Destination Client** ein oder klicken Sie auf **Browse**, um zum Client zu navigieren.

g. Wählen Sie **Restore to a different SQL Server instance or location**.

h. Klicken Sie neben dem Feld **Select the SQL instance on the destination client where the items should be restored** auf **Browse**, wählen Sie **Windows SQL** aus und aktivieren Sie dann das Kontrollkästchen neben der Zielinstanz.

i. Klicken Sie auf **OK**.

j. Klicken Sie im Dialogfeld **Restore Options** auf **More Options**.

Das Dialogfeld **Restore Command Line Options** wird angezeigt.

k. Aktivieren Sie das Kontrollkästchen **Show Advanced Options**.

Mehrere erweiterte Optionen werden in Rot angezeigt.

l. Legen Sie die Optionen fest, wie in der folgenden Tabelle beschrieben.

Tabelle 37 Erweiterte Optionen

Option	Auswahl
Verwenden der SQL REPLACE-Option	Aktivieren Sie das Kontrollkästchen.
Protokollfragmentbackup	Deaktivieren Sie das Kontrollkästchen, um das Protokollfragmentbackup zu deaktivieren. Das Protokollfragmentbackup wird nicht unterstützt, wenn Sie auf einer anderen Instanz wiederherstellen.
Verschlüsselungsmethode für das Data Domain-System	Wählen Sie die Verschlüsselungsmethode für den Datentransfer während der Wiederherstellung aus, wenn das Backup in einem Data Domain-System gespeichert war.
Systemdatenbanken wiederherstellen	Aktivieren Sie das Kontrollkästchen.
Automatisches Managen von SQL-Services während der Wiederherstellung	Aktivieren Sie das Kontrollkästchen.

m. Ignorieren Sie die verbleibenden Optionen.

n. Klicken Sie im Dialogfeld **Restore Command Line Options** auf **OK**.

o. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

Die folgende Statusmeldung wird angezeigt: `Restore initiated.`

p. Klicken Sie auf **OK**.

2. Stellen Sie die msdb-Datenbank auf der Zielinstanz mit den gleichen Schritten und Optionen wieder her, die Sie für die Wiederherstellung der Masterdatenbank verwendet haben.

Hinweis

Sie können die Modell- und die msdb-Datenbanken gleichzeitig wiederherstellen, wenn Sie sie im selben Dateisystempfad auf dem Zielserver wiederherstellen wie auf dem ursprünglichen Server . Wenn Sie die msdb-Datenbankdateien in einem anderen Dateisystempfad auf dem Zielserver wiederherstellen möchten, stellen Sie die msdb- und Modelldatenbanken mit separaten Wiederherstellungsvorgängen wieder her und geben Sie den Dateisystemspeicherort für die msdb-Datenbankdateien an, indem Sie auf **Set Destination** im Dialogfeld **Restore Options** klicken und den Speicherort auswählen.

3. Wenn Sie die Modelldatenbank im vorherigen Schritt nicht wiederhergestellt haben, stellen Sie die Modelldatenbank mithilfe derselben Schritte und Optionen wieder her, mit denen Sie die Master- und msdb-Datenbanken wiederhergestellt haben.

Wiederherstellen in einer AlwaysOn-Verfügbarkeitsgruppe

Wenn Sie Datenbanken in einer AlwaysOn-Verfügbarkeitsgruppe sichern, können Sie die Datenbanken auf den folgenden Speicherorten wiederherstellen:

- Am ursprünglichen Speicherort in der ursprünglichen Verfügbarkeitsgruppe
- In einer neuen Datenbank in der ursprünglichen Verfügbarkeitsgruppe
- In einer anderen Verfügbarkeitsgruppe
- In einer SQL Server-Instanz, die keine Verfügbarkeitsgruppen verwendet
- Betriebssystemdateien

In einer Hybrid-IT-Umgebung mit AlwaysOn-Verfügbarkeitsgruppen und Microsoft Azure hängen die Schritte zur Wiederherstellung einer Datenbank vom Speicherort des primären Replikats ab:

- Wenn das primäre Replikat vor Ort ist, stellen Sie Daten nur auf dem primären Replikat wieder her. Versuchen Sie nicht, auf die primären und sekundären Replikate wiederherzustellen. Wenn es eine entsprechende Datenbank auf den sekundären Replikaten gibt, wenn Sie eine Datenbank auf dem primären Replikat wiederherstellen, liegt die entsprechende Datenbank auf dem sekundären Replikat in einem Wiederherstellungsstatus vor. Um die Datenbanken auf den sekundären Replikaten als Teil der Verfügbarkeitsgruppe wiederherzustellen, bereiten Sie die Datenbanken manuell vor und stellen Sie diese dann wieder her. Fügen Sie sie dann zur Verfügbarkeitsgruppe des sekundären Replikats hinzu.
- Wenn das primäre Replikat auf einer virtuellen Maschine von Microsoft Azure ist, stellen Sie die Datenbank auf Betriebssystemdateien wieder her und verwenden Sie SQL Server-Tools zur Wiederherstellung der Datenbank in der Verfügbarkeitsgruppe.

Wiederherstellen in der ursprünglichen Verfügbarkeitsgruppe

Beim Wiederherstellen am ursprünglichen Speicherort in einer AlwaysOn-Verfügbarkeitsgruppe kann der Wiederherstellungsprozess die Datenbanken automatisch sowohl auf dem primären Replikat als auch auf dem sekundären Replikat wiederherstellen. Sie können auch Datenbanken nur auf dem primären Replikat wiederherstellen.

Automatisches Wiederherstellen auf primäre und sekundäre Replikate

Um die Datenbanken automatisch sowohl auf dem primären Replikat als auch auf dem sekundären Replikat wiederherzustellen, führen Sie die Schritte unter Wiederherstellen am ursprünglichen Speicherort auf Seite 167 aus. Legen Sie während der Wiederherstellung die folgenden Werte fest:

- Wählen Sie den Client für den Verfügbarkeitsgruppen-Listener bei der Suche nach einem Backup zur Wiederherstellung.
- Legen Sie die Plug-in-Optionen mit den folgenden Werten fest:
  - Deaktivieren Sie das Kontrollkästchen **Restore only on primary replica**.
  - Lassen Sie die Optionen **System Databases** deaktiviert. SQL Server unterstützt keine Systemdatenbanken in einer Verfügbarkeitsgruppe.
  - (Optional) Führen Sie ein Protokollfragmentbackup aus oder verwenden Sie SQL `REPLACE`, um eine Wiederherstellung zu erzwingen, selbst wenn die Datenbank bereits vorhanden ist.
  - Ignorieren Sie die **Redirect Restore**-Optionen.
  - (Optional) Geben Sie Authentifizierungsinformationen an.
  - (Optional) Führen Sie eine Point-in-Time-Recovery aus.

Wiederherstellen ausschließlich auf das primäre Replikat

Vorgehensweise

1. Führen Sie die Schritte in Wiederherstellen am ursprünglichen Speicherort auf Seite 167 aus. Legen Sie während der Wiederherstellung die folgenden Werte fest:
   - Wählen Sie den Client für den Verfügbarkeitsgruppen-Listener bei der Suche nach einem Backup zur Wiederherstellung.
   - Lassen Sie das Kontrollkästchen **Restore only on primary replica** in den Plug-in-Optionen aktiviert.
   - Lassen Sie die Optionen **System Databases** deaktiviert. SQL Server unterstützt keine Systemdatenbanken in einer Verfügbarkeitsgruppe.
   - (Optional) Führen Sie ein Protokollfragmentbackup aus oder verwenden Sie SQL `REPLACE`, um eine Wiederherstellung zu erzwingen, selbst wenn die Datenbank bereits vorhanden ist.
   - Ignorieren Sie die **Redirect Restore**-Optionen.
   - (Optional) Geben Sie Authentifizierungsinformationen an.
   - (Optional) Führen Sie eine Point-in-Time-Recovery aus.

   Nachdem eine Datenbank ausschließlich auf dem primären Replikat wiederhergestellt wurde, liegt die entsprechende Datenbank auf dem sekundären Replikat in einem Status „Restoring“ vor.
2. (Optional) Stellen Sie die Datenbanken auf den sekundären Replikaten wieder her, indem Sie die Datenbanken manuell vorbereiten und wiederherstellen und diese dann zu den Verfügbarkeitsgruppen auf den sekundären Replikaten hinzufügen.

Wiederherstellen auf einer neuen Datenbank in der ursprünglichen Verfügbarkeitsgruppe

Sie können eine Datenbank in einer AlwaysOn-Verfügbarkeitsgruppe auf der ursprünglichen Instanz aber mit einem neuen Namen wiederherstellen und so eine neue Datenbank in der Instanz erstellen.

Um die Datenbanken automatisch sowohl auf dem primären Replikat als auch auf dem sekundären Replikat wiederherzustellen, führen Sie die Schritte unter Wiederherstellen auf einer neuen Datenbank in der ursprünglichen Instanz auf Seite 169 aus. Legen Sie während der Wiederherstellung die folgenden Werte fest:

- Wählen Sie den Client für den Verfügbarkeitsgruppen-Listener bei der Suche nach einem Backup zur Wiederherstellung.
- Legen Sie die Plug-in-Optionen mit den folgenden Werten fest:
  - Lassen Sie das Kontrollkästchen **Use SQL REPLACE option** deaktiviert.
  - (Optional) Führen Sie ein Protokollfragmentbackup aus.
  - Deaktivieren Sie das Kontrollkästchen **Restore only on primary replica**.
  - (Optional) Geben Sie die Optionen für den Recovery-Vorgang an.
  - Lassen Sie die Optionen **System Databases** deaktiviert. SQL Server unterstützt keine Systemdatenbanken in einer Verfügbarkeitsgruppe.
  - Geben Sie im Feld **New database name** einen Namen für die neue Datenbank an.
  - (Optional) Geben Sie einen neuen Pfad für die Datenbankdateien im Feld **Alternate database location** an.
  - (Optional) Wählen Sie den Speicherort für die Protokolldateien für die Datenbank aus.
  - (Optional) Geben Sie Authentifizierungsinformationen an.
  - (Optional) Führen Sie eine Point-in-Time-Recovery aus.

Wiederherstellen in einer anderen Verfügbarkeitsgruppe

Sie können Datenbanken aus einer Verfügbarkeitsgruppe in einer Verfügbarkeitsgruppe in einem anderen Cluster wiederherstellen.

Vorgehensweise

1. Führen Sie die Schritte in Wiederherstellen auf einer anderen Instanz auf Seite 171 aus. Legen Sie während der Wiederherstellung die folgenden Werte fest:
   - Wählen Sie den Client für den ursprünglichen Verfügbarkeitsgruppen-Listener bei der Suche nach einem Backup zur Wiederherstellung.
   - Lassen Sie das **Use SQL REPLACE option**-Kontrollkästchen in den Plug-in-Optionen deaktiviert.
   - Deaktivieren Sie das Kontrollkästchen **Tail-log backup**. Dieses Wiederherstellungsszenario unterstützt kein Protokollfragmentbackup.
   - Lassen Sie das Kontrollkästchen **Restore only on primary replica** aktiviert.
   - (Optional) Geben Sie die Optionen für den Recovery-Vorgang an.
   - Lassen Sie die Optionen **System Databases** deaktiviert. SQL Server unterstützt keine Systemdatenbanken in einer Verfügbarkeitsgruppe.

- Ignorieren Sie die **Redirect Restore**-Optionen. Diese Einstellungen haben Sie bereits im Dialogfeld **Set Destination** angegeben.
- (Optional) Geben Sie Authentifizierungsinformationen an.
- (Optional) Führen Sie eine Point-in-Time-Recovery aus.

2. Fügen Sie nach dem Abschluss der Wiederherstellung die neue Datenbank der Verfügbarkeitsgruppe hinzu.

   Wenn Sie die Datenbank der Verfügbarkeitsgruppe hinzufügen, erstellt der Prozess automatisch die Datenbanken auf den sekundären Replikaten und synchronisiert diese.

Wiederherstellen in einer SQL Server-Instanz ohne Verfügbarkeitsgruppen

Wenn Sie Datenbanken in einer Verfügbarkeitsgruppe sichern, können Sie die Datenbanken auf einer anderen SQL Server-Instanz wiederherstellen, die keine Verfügbarkeitsgruppen verwendet, entweder auf demselben Server oder auf einem anderen Server.

Die Schritte sind identisch, unabhängig davon, ob Sie aus dem Backup von Datenbanken auf einem eigenständigen Server, auf einem gemeinsamen Speicher in einem Failover-Cluster oder in einer Verfügbarkeitsgruppe wiederherstellen. Details dazu finden Sie unter Wiederherstellen auf einer anderen Instanz auf Seite 171.

Wiederherstellen in Betriebssystemdateien

Wenn Sie Datenbanken in einer Verfügbarkeitsgruppe sichern, können Sie die Datenbanken in Betriebssystemdateien wiederherstellen.

Die Schritte sind identisch, unabhängig davon, ob Sie aus dem Backup von Datenbanken auf einem eigenständigen Server, auf einem gemeinsamen Speicher in einem Failover-Cluster oder in einer Verfügbarkeitsgruppe wiederherstellen. Details dazu finden Sie unter Wiederherstellen in einer Datei auf Seite 173.

Wiederherstellen einer Datenbank mit einer intakten Protokolldatei

Wenn eine Datenbank beschädigt wird oder auf andere Weise verloren gegangen ist, aber eine intakte Datenbankprotokolldatei verfügbar ist, können Sie die Datenbank wiederherstellen und die Protokolldatei zum Wiederherstellen von Transaktionen nach dem letzten Backup verwenden.

Vorgehensweise

1. Durchführen eines Transaktionsprotokollbackups des intakten Datenbankprotokolls durch Ausführung folgenden Transact-SQL-Befehls:

   ```
   BACKUP LOG dbname TO DISK = 'drive:\folder\filename' WITH
   NO_TRUNCATE
   ```

   wobei *dbname* der Name der Datenbank ist und *drive:\folder\file* der Pfad zum Ordner und der Dateiname, unter dem das Backup gespeichert werden soll.

2. In Avamar Administrator finden Sie das letzte Backup der Datenbank mithilfe der Anweisungen unter Suchen nach einem Backup nach Inhalt auf Seite 162.
3. Stellen Sie in Avamar Administrator das Backup an seinem ursprünglichen Speicherort anhand der Anweisungen unter Wiederherstellen am ursprünglichen Speicherort auf Seite 167 wieder her.

Aktivieren Sie im **Restore Command Line Options**-Dialogfeld während der Wiederherstellung das **Show Advanced Options**-Kontrollkästchen und konfigurieren Sie dann die Einstellungen wie folgt:

- Aktivieren Sie das **Use SQL REPLACE option**-Kontrollkästchen.
- Deaktivieren Sie das Kontrollkästchen **Tail-log backup**.
- (Optional) Wenn das Backup in einem Data Domain-System gespeichert ist, wählen Sie aus der Liste **Encryption method to Data Domain system** die Verschlüsselungsmethode für den Datentransfer während der Wiederherstellung aus.
- Wählen Sie **NORECOVERY** aus der **Recovery operation**-Liste.
- Ignorieren Sie die verbleibenden Optionen, die bei diesem Wiederherstellungsprozess nicht angewendet werden.

4. Wiederherstellen eines Transaktionsprotokollbackups des intakten Datenbankprotokolls durch Ausführung des folgenden Transact-SQL-Befehls:

   RESTORE LOG *dbname* FROM DISK = '*drive:folder**filename*' WITH RECOVERY**

   wobei *dbname* der Name der Datenbank ist und *drive:**folder**file* der Ordner und Dateiname für die Transaktionsprotkoll-Backupdatei.

5. Wenn die Datenbank in SQL Server Management Studio nicht aufgeführt wird, aktualisieren Sie die Liste oder stellen Sie eine Verbindung zur Datenbank her.

Weitere Erfordernisse

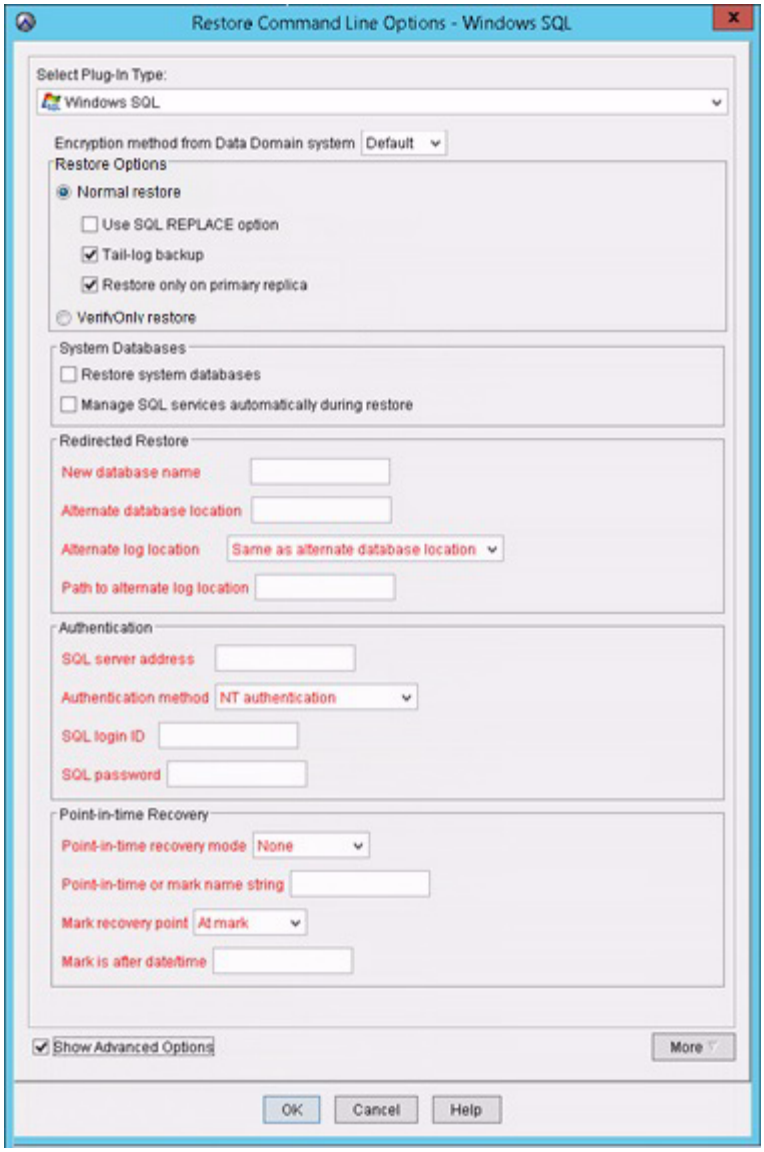
Nachdem die Wiederherstellung erfolgreich abgeschlossen wurde, führen Sie ein komplettes Backup der Datenbank aus und deaktivieren Sie das Kontrollkästchen **Force incremental backup after full backup** in den Plug-in-Optionen für das Backup. Wenn das Kontrollkästchen aktiviert ist, wenn ein komplettes Backup nach einer Wiederherstellung durchgeführt wird, schlägt das automatisch nach kompletten Backups erstellte Transaktionsprotokollbackup fehl.

Festlegen von Wiederherstellungsoptionen

Sie richten Plug-in-Optionen während der Wiederherstellung über das Dialogfeld **Restore Command Line Options** ein.

Um alle Plug-in-Optionen anzuzeigen, auch die erweiterten Optionen, aktivieren Sie das Kontrollkästchen **Show Advanced Options**. Die erweiterten Optionen werden in Rot angezeigt.

Abbildung 13 Restore Command Line Options, Dialogfeld



Allgemeine Wiederherstellungsoptionen

Allgemeine Optionen im Dialogfeld **Restore Command Line Options** umfassen die Option **Encyrption method from Data Domain system**, die Auswahl **Normal restore** mit den Kontrollkästchen **Use SQL REPLACE**, **Tail-log backup** und **Restore only on primary replica**, das Auswahlfeld **VerifyOnly** und das Kontrollkästchen **Enable debugging messages**.

Verschlüsselungsmethode für das Data Domain-System

Wenn das Backup in einem Data Domain-System gespeichert ist, wählen Sie aus der Liste **Encryption method to Data Domain system** die Verschlüsselungsmethode für den Datentransfer zwischen dem Data Domain-System und dem Client während der Wiederherstellung aus.

Normale Wiederherstellung

Führt eine normale Wiederherstellung der Datenbanken durch. Bei Auswahl dieser Option können Sie auch die Kontrollkästchen **Use SQL REPLACE**, **Tail-log backup** und **Restore only on primary replica** aktivieren.

Verwenden der SQL REPLACE-Option

Bei Aktivierung des Kontrollkästchens **Use SQL REPLACE option** im Dialogfeld **Restore Command Line Options** wird eine SQL-Klauselanweisung `WITH REPLACE` zum Befehl Restore Transact-SQL hinzugefügt. Durch diese Anweisung wird festgelegt, dass SQL Server alle erforderlichen Datenbanken und zugehörigen Dateien erstellt, selbst wenn bereits eine andere Datenbank oder Datei desselben Namens vorhanden ist.

HINWEIS

Hierdurch wird die SQL Server-Sicherheitsprüfung außer Kraft gesetzt, die ein versehentliches Überschreiben einer anderen Datenbank oder Datei verhindern soll. Die Microsoft Transact-SQL-Dokumentation enthält weitere Informationen im Befehlsabschnitt `RESTORE`.

Aktivieren Sie das Kontrollkästchen nur, wenn Sie eine Instanz, Datenbank, Dateigruppe oder Datei am ursprünglichen Speicherort wiederherstellen und das Überschreiben der Originaldaten erzwingen müssen. Möglicherweise müssen Sie das Überschreiben erzwingen, wenn eine vorherige Datenbankwiederherstellung mit dem folgenden SQL Server-Fehler im Avamar SQL-Wiederherstellungsprotokoll beendet wurde:

```
One or more devices or files already exist. Reissue the
statement using the WITH REPLACE option to overwrite these
files and devices.
```

Verwenden Sie diese Option auch, wenn Sie die Systemdatenbanken wiederherstellen.

Protokollfragmentbackup

Bei Aktivierung des Kontrollkästchens **Tail-log backup** im Dialogfeld **Restore Command Line Options** sichert Avamar das Ende des Transaktionsprotokolls während der Wiederherstellung, um die Protokolldatensätze zu erfassen, die nicht in einem Backup enthalten sind. Der Wiederherstellungsvorgang verwendet dann das Protokollfragmentbackup nach der Wiederherstellung der Datenbank, um die Transaktionen wiederherzustellen, die nicht im Backup enthalten waren.

Für ein Protokollfragmentbackup muss die Datenbank online geschaltet sein und entweder das komplette oder massenprotokollierte Recovery-Modell verwenden. Daher können Sie kein Protokollfragmentbackup für Systemdatenbanken wie Master- und msdb-Datenbanken durchführen, da diese Datenbanken das einfache Recovery-Modell nutzen.

Wenn Sie eine benutzerdefinierte Dateigruppe oder sekundäre Datendatei wiederherstellen möchten und ein Protokollfragmentbackup durchführen, müssen Sie das letzte Backup als das Backup für die Wiederherstellung auswählen. Andernfalls schlägt die Wiederherstellung fehl und eine Fehlermeldung wird in die Protokolldatei geschrieben.

Sie können ein Protokollfragmentbackup durchführen, wenn Sie eine Instanz, Datenbank, Dateigruppe oder Datei ohne die SQL-Option `WITH REPLACE` am ursprünglichen Speicherort wiederherstellen. Mit anderen Worten, wenn Sie bei der

Wiederherstellung am ursprünglichen Speicherort das Kontrollkästchen **Use SQL REPLACE option** aktivieren, lassen Sie das Kontrollkästchen **Tail-log backup** deaktiviert.

Sie können ein Protokollfragmentbackup auch dann ausführen, wenn Sie eine Datenbank in der ursprünglichen Instanz mit einem neuen Datenbanknamen wiederherstellen.

Wenn Sie eine Point-in-Time-Wiederherstellung durchführen und der Point-in-Time, auf den Sie wiederherstellen möchten, nach dem letzten Transaktionsprotokollbackup liegt, müssen Sie ein Protokollfragmentbackup durchführen.

Ein Protokollfragmentbackup ist auch erforderlich, wenn Sie eine Datei aus einer benutzerdefinierten Dateigruppe an ihrem ursprünglichen Speicherort wiederherstellen.

Führen Sie kein Protokollfragmentbackup aus, wenn Sie eine umgeleitete Wiederherstellung auf einer anderen SQL Server-Instanz durchführen.

HINWEIS

Wenn das Protokollfragmentbackup fehlschlägt, kann die Wiederherstellung nicht durchgeführt werden. Prüfen Sie die Protokolldatei, um die Ursache des Problems zu bestimmen. Beheben Sie das Problem und starten Sie die Wiederherstellung erneut. Wenn Sie das Kontrollkästchen **Tail-log backup** deaktivieren, um die Erstellung des Protokollfragmentbackups zu verhindern, umfasst die Wiederherstellung nur Transaktionen bis zum ausgewählten Backup. Möglicherweise verlieren Sie dadurch alle Transaktionen am Ende des Protokolls.

Nur auf primärem Replikat wiederherstellen

Das Kontrollkästchen **Restore only on primary replica** steuert, ob Datenbanken nur auf das primäre Replikat oder auf das primäre Replikat und alle sekundären Replikate in einer AlwaysOn-Verfügbarkeitsgruppe wiederhergestellt werden.

Wenn Sie das Kontrollkästchen deaktivieren, werden die Datenbanken automatisch am ursprünglichen Speicherort auf dem primären Replikat und den sekundären Replikaten wiederhergestellt. Deaktivieren Sie das Kontrollkästchen nur, wenn Sie in der ursprünglichen Verfügbarkeitsgruppe am ursprünglichen Speicherort wiederherstellen und auf alle Replikate wiederherstellen möchten.

Wenn Sie das Kontrollkästchen aktivieren und die Datenbank ausschließlich auf dem primären Replikat wiederherstellen, liegt die entsprechende Datenbank auf dem sekundären Replikat in einem Wiederherstellungsstatus vor. Um die Datenbanken auf den sekundären Replikaten als Teil der Verfügbarkeitsgruppe wiederherzustellen, bereiten Sie die Datenbanken manuell vor und stellen Sie diese dann wieder her. Fügen Sie sie dann zur Verfügbarkeitsgruppe des sekundären Replikats hinzu.

Sie können auch die Datenbank auf einem sekundären Replikat online festlegen, ohne sie wieder mit der Verfügbarkeitsgruppe zu vereinen, indem sie die Datenbank mit dem Recovery-Vorgang `RECOVERY` wiederherstellen. Details dazu finden Sie in der Dokumentation zu Microsoft SQL Server auf der Microsoft-Website.

Aktivieren Sie das Kontrollkästchen in den folgenden Wiederherstellungsszenarien:

- Wiederherstellung an einem anderen Speicherort in der ursprünglichen Verfügbarkeitsgruppe
- Wiederherstellung in einer anderen Verfügbarkeitsgruppe
- Wiederherstellung auf einem lokalen primären Replikat in einer Hybrid-IT-Umgebung mit Microsoft Azure

Sie können auch das Kontrollkästchen aktivieren, wenn Sie nur das primäre Replikat in der ursprünglichen Verfügbarkeitsgruppe wiederherstellen möchten.

Wiederherstellen in einer AlwaysOn-Verfügbarkeitsgruppe auf Seite 190 enthält zusätzliche Details zur Wiederherstellung in einer Verfügbarkeitsgruppe.

Einzelne Wiederherstellung eines inkrementellen oder differenziellen Backups

Diese Funktion wird für eigentändige, Cluster- und AG-Umgebungen, die mit einer oder mehreren SQL-Datenbanken konfiguriert sind, unterstützt.

Overwrite default recoveryplan-Kontrollkästchen in Avamar Administrator

Verwenden von Avamar Administrator

So stellen Sie einzelne inkrementelle oder differenzielle Backups wieder her:

1. Stellen Sie sicher, dass die Umgebung die Richtlinien unter Wiederherstellungsanforderungen auf Seite 155 erfüllt.
2. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.
   Das Fenster **Backup, Restore and Manage** wird angezeigt.
3. Suchen Sie nach dem wiederherzustellenden Backup:
   - Suchen nach einem Backup nach Datum auf Seite 159
   - Suchen nach einem Backup nach Inhalt auf Seite 162

   Das wiederherzustellende Backup ist in der Tabelle **Backups** ausgewählt.
4. Wählen Sie **Actions** > **Restore Now** aus.
   Das Dialogfeld **Restore Options** wird angezeigt.
5. Stellen Sie sicher, dass **Windows SQL** in der Liste **Restore Plug-in** angezeigt wird.
6. Aktivieren Sie im Feld **Recovery operation** eine der folgenden Optionen:
   - Um den korrekten Prüfpunkt bis zur Wiederherstellung während eines Wiederherstellungsvorgangs festzulegen, wählen Sie **WITH NO Recovery**.
   - Um den korrekten Prüfpunkt bis zur Wiederherstellung während eines Wiederherstellungsvorgangs festzulegen und die Daten während der Wiederherstellung anzuzeigen und zu lesen, wählen Sie **WITH STANDBY**.
   - Um die Datenbank in den normalen Modus zu versetzen und den einzelnen Backupstream wiederherzustellen, wählen Sie **WITH Recovery**.
   - Um den letzten Prüfpunkt und den einzelnen Backupstream wiederherzustellen, wählen Sie **WITH Recovery**.
7. Wenn die **WITH STANDBY**-Option im Feld **Standby file location** ausgewählt wurde, geben Sie den Dateispeicherort ein.
8. Aktivieren Sie das Kontrollkästchen **Overwrite default recovery plan**.
9. Klicken Sie auf **OK**.

Verwenden der CLI

Stellen Sie einzelne inkrementelle oder differenzielle Backups wieder her, indem Sie das `--overwrite-default-recoveryplan`-Flag verwenden.

Wenn Sie einzelne Streams von inkrementellen oder differenziellen Backups wiederherstellen, beachten Sie die folgenden Optionen:

- Um den korrekten Prüfpunkt bis zur Wiederherstellung während eines Wiederherstellungsvorgangs festzulegen, verwenden Sie das `WITH NORECOVERY`-Flag.

- Um den korrekten Prüfpunkt bis zur Wiederherstellung während eines Wiederherstellungsvorgangs festzulegen und die Daten während der Wiederherstellung anzuzeigen und zu lesen, verwenden Sie das `WITH STANDBY`-Flag.
- Um die Datenbank in den Normalmodus zu versetzen, stellen Sie den einzelnen Backupstream mithilfe des `WITH RECOVERY`-Flag wieder her.
- Zum Wiederherstellen des letzte Prüfpunkts stellen Sie den einzelnen Backupstream mithilfe des `WITH RECOVERY`-Flag wieder her.

Überlegungen zu Verfügbarkeitsgruppen
In VG-Umgebungen können einzelne Wiederherstellungsvorgänge nur auf dem primären Node durchgeführt werden.

Wenn die VG-Datenbank während der Durchführung einer einzelnen Wiederherstellung aus der VG entfernt wird, gehen Sie wie folgt vor:

1. Suchen Sie auf dem primären Node den erforderlichen Prüfpunkt durch eine inkrementelle oder differenzielle Wiederherstellung.
2. Fügen Sie die Datenbank manuell der VG hinzu.
   Sie können mit einer der folgenden Methoden fortfahren:
   - Verwenden Sie SQL Server.
   - Führen Sie einen Wiederherstellungsvorgang in Avamar Administrator durch:
     a. Wählen Sie im Feld **Recovery operation** die Option **RECOVERY**.
     b. Aktivieren Sie das Kontrollkästchen **Overwrite default recovery plan**.
     c. Deaktivieren Sie das Kontrollkästchen **Restore primary only**.
     d. Klicken Sie auf **OK**.

VerifyOnly-Wiederherstellung

Diese Optionen führen eine Verify-Only-Wiederherstellung durch, bei der das Backup nur geprüft, aber wird nicht wiederhergestellt wird.

Debugging-Meldungen aktivieren

Bei Auswahl der Option **Enable debugging messages** werden während des Vorgangs maximal viele Informationen in Protokolldateien geschrieben. Wenn Sie das Kontrollkästchen aktivieren, werden dabei sehr große Protokolldateien erzeugt. Verwenden Sie diese Option lediglich zu Debugging-Zwecken.

Optionen für den Recovery-Vorgang

Die Liste **Recovery operation** und das Feld **Standby file location** im Dialogfeld **Restore Command Line Options** ermöglichen die Steuerung des Recovery-Vorgangs nach der Wiederherstellung.

Tabelle 38 Optionen für den Recovery-Vorgang

Recovery-Vorgang	Beschreibung
`RECOVERY`	Die Datenbank ist vollständig wiederhergestellt und online nach der Wiederherstellung. Diese Funktion ist die Standardeinstellung.

Tabelle 38 Optionen für den Recovery-Vorgang (Fortsetzung)

Recovery-Vorgang	Beschreibung
NORECOVERY	Die Datenbank verbleibt nach der Wiederherstellung in einem Wiederherstellungszustand. Mit dieser Funktion können Sie zusätzliche manuelle Wiederherstellungsaufgaben wie die Anwendung zusätzlicher SQL-Transaktionsprotokolldateien durchführen.
STANDBY	Die Datenbank ist nach der Wiederherstellung im Stand-by-Modus (schreibgeschützt). Mit dieser Funktion können Sie eine Datenbank in den schreibgeschützten Zustand zwischen Transaktionsprotokollwiederherstellungen bringen. Die Funktion kann in aktiven Stand-by-Serversituationen oder speziellen Recovery-Situationen verwendet werden, in denen sie nützlich ist, um die Datenbank zwischen Protokollwiederherstellungen zu untersuchen. Diese Option erstellt auch eine Datei mit Recovery-Änderungen. Falls erforderlich, können Sie die Datei nutzen, um die Recovery-Änderungen rückgängig zu machen. Die Größe der Datei hängt von der Anzahl der Aktionen zur Rückgängigmachung von nicht bestätigten Transaktionen ab. Geben Sie im Feld „Standby File Location“ den Pfad zu dieser Datei an. Das Format lautet wie folgt: *drive:\folder\subfolder* wobei *drive* der Laufwerksbuchstabe auf dem Zielclient und *folder\subfolder* der Pfad zum Laufwerksbuchstaben ist, in dem Sie die Datei erstellen. Wenn eine Datei mit den Recovery-Änderungen im angegebenen Speicherort vorhanden ist, überschreibt SQL Server diese. Wenn Sie keinen Pfad angeben, erstellt Avamar die Datei im Ordner *C:\Program Files\avs\var*, wobei *C:\Program Files\avs* der Avamar-Installationsordner ist. Verwenden Sie STANDBY nicht, wenn ein Datenbankupgrade erforderlich ist. Sie müssen möglicherweise ein Datenbankupgrade durchführen, wenn Sie Backupsätze aus einer früheren Version von SQL Server wiederherstellen.

Sie können den Recovery-Vorgang in den folgenden Wiederherstellungsszenarien angeben:

- Sie stellen eine Instanz, Datenbank, Dateigruppe oder Datei am ursprünglichen Speicherort wieder her.
- Sie stellen eine Datenbank in der ursprünglichen Instanz, jedoch mit einem neuen Datenbanknamen wieder her.
- Sie stellen eine Instanz, Datenbank, Dateigruppe oder Datei auf einer anderen Instanz auf dem ursprünglichen Server oder einem anderen Server wieder her.
- Sie stellen ein oder mehrere Systemdatenbanken wieder her. Beachten Sie jedoch die folgenden Punkte:
  - Wenn Sie die Master- oder Modelldatenbank wiederherstellen möchten, müssen Sie die `RECOVERY`-Option auswählen. Verwenden Sie weder `NORECOVERY` noch `STANDBY`.
  - Wenn Sie die msdb-Datenbank wiederherstellen, können Sie einige beliebige Recovery-Option auswählen. Wenn Sie jedoch `NORECOVERY` oder `STANDBY` auswählen, kann auf keine Datenbank zugegriffen werden, bis die Wiederherstellung der msdb-Datenbank abgeschlossen ist.
  - Wenn Sie die Systemdatenbank wiederherstellen möchten, müssen Sie die `RECOVERY`-Option auswählen. Verwenden Sie weder `NORECOVERY` noch `STANDBY`.

Sie müssen keinen Recovery-Vorgang angeben, wenn Sie auf eine Betriebssystemdatei wiederherstellen.

Wenn Sie den Recovery-Vorgang `NORECOVERY` oder `STANDBY` festlegen, können Sie die Datenbank nach jedem manuellen Vorgang mithilfe einer der folgenden Methoden wieder online bringen:

- Stellen Sie die Datenbank mit Avamar-Plug-in für SQL Server erneut wieder her, aber wählen Sie `RECOVERY` aus der Liste **Recovery operation**.
- Führen Sie den Befehl **`RESTORE DATABASE`** ***`dbname`*** **`WITH RECOVERY`** mit SQL Server Management Studio aus, wobei *dbname* der Name der wiederherzustellenden Datenbank ist.

Optionen zur Wiederherstellung der Systemdatenbank

Die Kontrollkästchen **Restore system databases** und **Manage SQL services automatically during restore** im Dialogfeld **Restore Command Line Options** ermöglichen die korrekte Wiederherstellung von Systemdatenbanken, z. B. Master-, msdb- und Modelldatenbanken.

Bei der Wiederherstellung einer gesamten Instanz oder wenn Sie bestimmte Systemdatenbanken für die Wiederherstellung auswählen, aktivieren Sie das Kontrollkästchen **Restore system databases**, um sicherzustellen, dass die Systemdatenbanken wiederhergestellt werden. Wenn Sie das Kontrollkästchen deaktiviert lassen, werden die Systemdatenbanken nicht wiederhergestellt.

Die Option **Manage SQL services automatically during restore** hält SQL-Services während der Wiederherstellung automatisch an und startet sie neu:

- Wenn Sie die Masterdatenbank wiederherstellen, hält diese Option die SQL Server-Instanz automatisch an, einschließlich der abhängigen Services wie SQL Server-Agent-Service und Analysis-Service. Die Option startet die Instanz vor der Wiederherstellung im Einzelbenutzermodus neu. Nach der Wiederherstellung wird die Instanz automatisch neu gestartet.
- Wenn Sie die msdb-Datenbank wiederherstellen, hält diese Option den SQL Server-Agent-Service automatisch an und startet ihn neu, wenn die Wiederherstellung abgeschlossen ist.

Wenn Sie sowohl die System- als auch die Benutzerdatenbanken zur Wiederherstellung auswählen, werden zuerst die Systemdatenbanken wiederhergestellt. Sie müssen das Kontrollkästchen **Manage SQL services automatically during restore** aktivieren, um sicherzustellen, dass alle Systemdatenbanken in der richtigen Reihenfolge und mit den erforderlichen Service-Stopps und -Neustarts wiederhergestellt werden.

Optionen für die umgeleitete Wiederherstellung

Mit den Optionen für die umgeleitete Wiederherstellung im Dialogfeld **Restore Command Line Options** können Sie den Datenbanknamen und die Dateispeicherorte beim Wiederherstellen einer Datenbank auf der ursprünglichen Instanz aber mit einem neuen Namen steuern.

Sie können die Dateispeicherorte auch angeben, indem Sie auf **Set Destination** im **Restore Options**-Dialogfeld klicken. Wenn Sie die Dateispeicherorte im Dialogfeld **Restore Options** angeben, müssen Sie diese im **Restore Command Line Options**-Dialogfeld nicht angeben.
Sie können auch einen neuen Datenbanknamen angeben, wenn Sie eine Datenbank auf einer anderen Instanz aber mit einem neuen Namen wiederherstellen.

Vorgehensweise

1. Aktivieren Sie im Dialogfeld **Restore Command Line Options** das Kontrollkästchen **Show Advanced Options**.

   Mehrere erweiterte Optionen, darunter die Point-in-Time-Recovery-Optionen, werden in Rot angezeigt.
2. (Optional) Wenn Sie eine einzige Datenbank mit einem neuen Namen wiederherstellen, geben Sie den neuen Namen im Namensfeld **New Database** ein.
3. Um die Datenbankdateien auf einem anderen Pfad als dem ursprüngliche Pfad wiederherzustellen, geben Sie den vollständigen Pfad des neuen Datenbankdateispeicherorts (`*.mdf`) auf dem Client im Feld **Alternate database location** an. Ein Beispiel hierfür ist `C:\temp`.
4. Wählen Sie den Pfad aus, an den die Datenbankprotokolldatei wiederhergestellt werden soll (`*.ldf`):
   - Um die Datenbankprotokolldateien am selben Speicherort wie die Datenbank wiederherzustellen (wie im Feld **Alternate database location** angegeben), wählen Sie **Same as alternate database location** aus der Liste **Alternate log location** aus.
   - Um die Datenbankprotokolldateien an einem anderen Speicherort als den Datenbankdateien wiederherzustellen, wählen Sie **Different location than database** aus der Liste **Alternate log location** aus und geben Sie den Pfad zum Speicherort auf dem Client im Feld **Path to alternate log location** ein. Ein Beispiel hierfür ist `C:\temp\logs`.

Authentifizierungsoptionen

Mit Authentifizierungsoptionen können Sie angeben, ob Avamar die Windows (NT)-Authentifizierung oder die SQL Server-Authentifizierung für die SQL Server-Verbindung verwenden soll, wenn Sie eine Instanz, Datenbank, Dateigruppe oder Datei entweder am ursprünglichen Speicherort oder an einem anderen Speicherort wiederherstellen.

Wenn Sie keine Authentifizierungsmethode angeben, verwendet das SQL Server-Plug-in die NT-Authentifizierung und meldet sich mit dem Konto NT AUTHORITY \SYSTEM an.

Sie müssen keine Authentifizierungsoptionen angeben, wenn Sie in eine Betriebssystemdatei wiederherstellen, da es nicht erforderlich sind, sich bei dieser Wiederherstellung mit SQL Server zu verbinden.

Vorgehensweise

1. Aktivieren Sie im Dialogfeld **Restore Command Line Options** das Kontrollkästchen **Show Advanced Options**.

   Mehrere erweiterte Optionen, einschließlich der Authentifizierungsoptionen, werden wird in Rot angezeigt.

2. Geben Sie im Feld **SQL server address** den Hostnamen oder die IP-Adresse des zu verbindenden Servers ein.
3. Wählen Sie aus der Liste **Authentication method** aus, ob die NT-Authentifizierung oder die SQL Server-Authentifizierung verwendet werden soll.
4. Wenn Sie die SQL Server-Authentifizierung auswählen, geben Sie die Anmelde-ID und das Passwort für das SQL Server-Konto in den Feldern **SQL Login ID** und **SQL password** ein.

Point-in-Time-Recovery-Optionen

Wenn Sie eine Datenbank wiederherstellen, die das vollständige Recovery-Modell entweder am ursprünglichen Speicherort oder an einem anderen Speicherort verwendet, können Sie auf ein bestimmtes Datum und eine Uhrzeit oder eine benannte Markierung im Transaktionsprotokoll wiederherstellen.

Die Durchführung einer Point-in-Time-Wiederherstellung von Systemdatenbanken wie Master- und msdb-Datenbanken ist nicht möglich, da diese Datenbanken das einfache Recovery-Modell nutzen.

Um auf einen bestimmten Point-in-Time wiederherzustellen, müssen das Transaktionsdatum und die Uhrzeit oder die benannte Markierung angegeben werden, auf der über das SQL Server-Transaktionsprotokoll wiederhergestellt werden soll. Die SQL Server-Dokumentation auf der Microsoft-Website enthält Details zum Zugriff auf Transaktionsprotokollinformationen.

Der Point-in-Time, auf den Sie wiederherstellen, muss nach dem Ablauf der Zeit für das letzte komplette Backup liegen. Liegt der Point-in-Time vor der Startzeit des letzten Backuptransaktionsprotokolls (inkrementell), ist ein Protokollfragmentbackup nicht erforderlich. Jedoch ist ein Protokollfragmentbackup erforderlich, wenn der Point-in-Time nach dem letzten Transaktionsprotokollbackup liegt.

Wenn Sie den Point in-Time für die Wiederherstellung angeben, legen Sie nicht die Startzeit des ausgewählten Transaktionsprotokollbackups fest, wenn es sich nicht um das letzte Backup in dieser Backupsequenz handelt. Andernfalls schlägt die Wiederherstellung fehl und ein Protokollfragmentbackup wird nicht durchgeführt, selbst wenn Sie die Protokollfragmentbackup-Option auswählen.

Vorgehensweise

1. Aktivieren Sie im Dialogfeld **Restore Command Line Options** das Kontrollkästchen **Show Advanced Options**.

   Mehrere erweiterte Optionen, darunter die Point-in-Time-Recovery-Optionen, werden in Rot angezeigt.

2. Wählen Sie in der Liste **Point-in-time recovery mode** aus, ob auf einen Point-in-Time oder einer benannten Markierung wiederhergestellt werden soll:
3. Geben Sie im Feld **Point-in-time or mark name string** entweder den Point-in-Time oder die benannte Markierung an, auf die wiederhergestellt werden soll:
   - Um auf einen bestimmten Point-in-Time wiederherzustellen, geben Sie Datum und Uhrzeit im Format yyyy-mm-ddThh:mm:ss ein. Beispielsweise steht 2013-10-15T14:15:45 für den 15. Oktober 2013 um 14:15:45 Uhr.
   - Um auf eine benannte Markierung wiederherzustellen, geben Sie die Markierung ein.
4. Wenn Sie eine Markierung angegeben haben, wählen Sie aus, ob die Markierung in der Recovery eingeschlossen werden soll:
   - Um anzugeben, dass der Protokolldatensatz unmittelbar vor der Markierung der Recovery-Punkt ist, wählen Sie **Before mark** aus der **Mark recovery point**-Liste. Mit anderen Worten führt die Recovery einen Rollforward zur Markierung aus und schließt die markierte Transaktion aus.
   - Um anzugeben, dass die markierte Transaktion der Recovery-Punkt ist, wählen Sie **At mark** aus der **Mark recovery point**-Liste aus. Mit anderen Worten führt die Recovery einen Rollforward zur Markierung aus und schließt die markierte Transaktion ein.
5. Wenn Sie eine Markierung angegeben haben und die benannte Markierung im Transaktionsprotokoll nicht eindeutig ist, verwenden Sie das Feld **Mark is after date/time**, um die Markierung zu suchen, auf die wiederhergestellt werden soll. Der Recovery-Prozess wird bei der ersten Markierung mit dem angegebenen Namen, genau am oder nach dem angegebenen Datum und der angegebenen Uhrzeit beendet. Geben Sie Datum und Uhrzeit im Format yyyy-mm-ddThh:mm:ss an.

Recovery auf Tabellenebene

Sie können einzelne Tabellen aus dem Backup von einer SQL-Datenbank durch die Durchführung einer Tabellen-Recovery in Verbindung mit ItemPoint für Microsoft SQL Server wiederherstellen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf die Schaltfläche **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Suchen Sie ein komplettes Backup, das die wiederherzustellenden Elemente enthält:
   - Suchen nach einem Backup nach Datum auf Seite 159
   - Suchen nach einem Backup nach Inhalt auf Seite 162

   Wählen Sie beim Auswählen der differenziellen Backups für eine Recovery auf Tabellenebene nur komplette Backups und die erforderlichen differenziellen Backups aus. Das Auswählen mehrerer differenzieller Backups wird nicht unterstützt.
3. Wählen Sie das **Browse for Granular Restore**-Symbol im linken oberen Bereich der **Restore**-Registerkarte aus.

   Das Dialogfeld **Select Destination Client** wird angezeigt.

4. Wählen Sie die Zielmaschine, auf der die Datenbank für TLR. gemountet wird.
   - Um die Datenbank auf der ursprünglichen Maschine zu mounten, wählen Sie **Restore everything to its original location**.
   - Um die Datenbank auf einer anderen Maschine zu mounten, wählen Sie **Restore everything to a different location**.

   Hinweis

   TLR kann nur auf physischen Nodes durchgeführt werden. Bei einem Failover eines Clusters oder einer AlwaysOn-Verfügbarkeitsgruppe muss die Wiederherstellung auf physische Nodes umgeleitet werden, auf denen TLR installiert ist.

5. Klicken Sie auf **OK**.

   Eine Meldung zeigt an, dass der Mountvorgang lange dauern kann.
6. Klicken Sie auf **OK**, um mit dem Mountvorgang fortzufahren.

   Das **Restore Browse Options**-Dialogfeld wird geöffnet.
7. Geben Sie im **Restore Browse Options**-Dialogfeld Folgendes an:
   a. Geben Sie im Feld **Drive letter or mount path** den Buchstaben des Laufwerks ein, das für das Mounten der SQL-Backupdaten verwendet wird, oder einen Schrägstrich (`/`) oder umgekehrten Schrägstrich (`\`), um das Laufwerk mit dem ersten verfügbaren Laufwerksbuchstaben zu mounten, beginnend bei `z:`.

      Bei dieser Option muss die Groß- und Kleinschreibung nicht beachtet werden. Wenn auf dem hier angegebenen Laufwerk bereits ein Laufwerk gemountet ist und dieses Laufwerk nicht durch das Avamar- Plug-in for SQL TLR gesteuert wird, schlägt der Mountvorgang fehl. Wenn das Avamar-Plug-in for SQL TLR auf diesem Laufwerk bereits ein Laufwerk gemountet hat, wird das vorhandene Laufwerk nicht gemountet und das neue Laufwerk wird gemountet.

   b. Wählen Sie unter **Amount of time to leave AvFS mounted** den Zeitpunkt für das automatische Unmounten des Laufwerks aus. Wenn die Zeit während der Recovery verlängert werden muss, verwenden Sie den `avsqltlr`-Befehl.
8. Öffnen Sie auf der Zielmaschine ItemPoint for Microsoft SQL Server im Microsoft Windows-**Startmenü**:
   a. Wählen Sie **Programs** aus.
   b. Wählen Sie den `EMC ItemPoint for Microsoft SQL Server`-Ordner aus.
   c. Wählen Sie das `EMC ItemPoint for Microsoft SQL Server`-Programm aus.

   Befolgen Sie die Anweisungen in der ItemPoint for Microsoft SQL Server-Dokumentation, um eine Recovery auf Tabellenebene durchzuführen.

Überwachen von Wiederherstellungen

Sie können Wiederherstellungen überwachen, um sich des erfolgreichen Abschlusses der Wiederherstellung zu vergewissern und ein Troubleshooting im Falle von

Problemen durchzuführen. Mit dem Activity Monitor in Avamar Administrator können Sie Statusinformationen für Wiederherstellungen anzeigen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Eine Liste sämtlicher Aktivitäten wird angezeigt.
3. Um die Ergebnisse so zu filtern, dass ausschließlich Wiederherstellungsaktivitäten angezeigt werden, wählen Sie **Actions** > **Filter** aus.

   Das Dialogfeld **Filter Activity** wird angezeigt.
4. Wählen Sie aus der Liste **Type** die Option **Restore** aus.
5. Klicken Sie auf **OK**.

Abbrechen von Wiederherstellungen

Sie können eine Wiederherstellung jederzeit vor deren Abschluss abbrechen. Der Abbruchvorgang kann 5 Minuten oder länger dauern. Die Wiederherstellung wird u. U. vor Abschluss des Abbruchvorgangs abgeschlossen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Eine Liste sämtlicher Aktivitäten wird angezeigt.
3. Wählen Sie die Wiederherstellung aus der Liste aus.
4. Wählen Sie **Actions** > **Cancel Activity** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
5. Klicken Sie auf **Yes**.

KAPITEL 7

Wiederherstellung und Recovery

In diesem Kapitel werden folgende Themen behandelt:

Wiederherstellen von Daten aus einem Backup

Sie können ein Backup zur Wiederherstellung nach Datum oder nach Inhalten des Backups suchen. Bei der Durchführung der Wiederherstellung können Sie die Wiederherstellung entweder am ursprünglichen Speicherort, einem anderen Speicherort oder an mehreren Speicherorten vornehmen.

HINWEIS

Die Optionen für das Wiederherstellungsziel sind vom Plug-in-Typ abhängig. Mithilfe des SQL Server-Plug-ins können Sie beispielsweise statt auf einen SQL Server in eine Datei wiederherstellen, während etwa mit dem Oracle-Plug-in eine Wiederherstellung an mehreren Speicherorten nicht möglich ist. Im Benutzerhandbuch für das jeweilige Plug-in sind Details zu den verfügbaren Optionen und zu den einzelnen Wiederherstellungstypen enthalten.

Suchen nach einem Backup

Der erste Schritt zum Wiederherstellen von Daten ist das Suchen nach dem Backup mit den wiederherzustellenden Daten. Sie können Avamar-Clientbackups entweder nach einem bestimmten Datum oder nach bestimmten Inhalten suchen.

Führen Sie eine Backupsuche anhand des Datums durch, wenn eine oder mehrere der folgenden Möglichkeiten zutreffen:

- Sie haben alle Daten für den Client in einem einzigen Backupsatz gespeichert.
- Der genaue Pfadname oder der Name der wiederherzustellenden Daten ist unbekannt.
- Das wiederherzustellende Backup liegt vor einem bestimmten Datum bzw. Ereignis. Beispielsweise kennen Sie das ungefähre Datum, wann Daten verloren gingen oder beschädigt wurden. Suchen Sie dann ein Backup vor diesem Datum.
- Die spezifischen Backuptypen sind bekannt. Sie führen beispielsweise immer mittwoch- und samstagnachts geplante Disaster-Recovery-Backups und täglich komplette Volume-Backups aus. Wenn Sie einen Server erneut aufbauen, können Sie das Disaster-Recovery-Backup mit dem Datum auswählen, das dem Ereignis am nächsten liegt, durch das der Datenverlust verursacht wurde.

Führen Sie eine Backupsuche anhand des Backupinhalts durch, wenn eine oder mehrere der folgenden Möglichkeiten zutreffen:

- Sie haben Daten auf dem Client in separate Backupsätze gespeichert.
- Sie möchten mehrere Versionen derselben Datei anzeigen, um die wiederherzustellende Version auswählen zu können.
- Das Datum oder der Inhalt des Backups ist zwar unbekannt, Sie kennen allerdings den Namen der wiederherzustellenden Daten.

HINWEIS

Avamar unterstützt im Allgemeinen die Verwendung bestimmter unterstützter internationaler Zeichen in Verzeichnis-, Ordner- und Dateinamen. Die ordnungsgemäße Anzeige internationaler Sprachzeichen hängt jedoch vom Java-Gebietsschema des Clientcomputers und der auf dem System installierten, mit der Ausgangssprache kompatiblen Schriftarten ab. Wenn Sie mit internationalen Zeichen erstellte Backups durchsuchen, auf Ihrem System jedoch keine kompatible Schriftart installiert ist, werden alle Zeichen, die das System nicht auflösen kann, als Rechtecke angezeigt. Hierbei handelt es sich um eine normale Beschränkung für diese bestimmte Situation, was keinerlei Einfluss auf die Wiederherstellungsfähigkeit dieser Verzeichnisse, Ordner oder Dateien hat. Unter *Avamar – Versionshinweise* sind zusätzliche Informationen zur internationalen Sprachunterstützung enthalten.

Replikate

Wenn die Funktion „Replicas at Source“ auf dem Avamar-Server aktiviert ist, listet Avamar-Administrator Replikate auf der Registerkarte „Restore“ in derselben Tabelle auf, in der auch Backups aufgeführt sind.

Verwenden Sie die Registerkarte „Restore“ von Avamar-Administrator, um Daten aus Replikaten anzuzeigen und wiederherzustellen. Replikate werden mit den folgenden Informationen angezeigt:

- `Remote` in der Spalte **Type**
- Name/IP-Adresse des Systemtyps des Remotezielsystems in der Spalte **Server**

Hinweis

Wenn Avamar-Administrator Daten aus einem Backup sowohl als `Local` als auch als `Remote` auflistet, verwendet das Avamar-System immer das lokale Backup zur Wiederherstellung der Daten. Werden jedoch als `Remote` aufgelistete Backupdaten zur Überprüfung ausgewählt, stellt das Avamar-System die referenzierten Replikate bereit und überprüft diese.

Replikate auf Quelle (Replicas at Source) auf Seite 334 bietet weitere Informationen zur Funktion „Replicas at Source“.

Suchen nach einem Backup nach Datum

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Restore**.

   Der Bereich links oben enthält eine Liste mit Domains.
3. Wählen Sie die Domain mit dem Client aus.

   Clients außerhalb der Domain des Anmeldekontos können nicht angezeigt werden. Melden Sie sich zum Anzeigen aller Clients bei der Root Domain an.

   Eine Liste mit Avamar Clients wird im Bereich unter der Liste mit Domains angezeigt.
4. Wählen Sie den Client aus der Liste aus.

5. Klicken Sie auf die Registerkarte **By Date**.
6. Wählen Sie das Backupdatum aus dem Kalender aus. Gültige Backups wurden an den gelb markierten Daten durchgeführt.

   Eine Liste der an diesem Datum durchgeführten Backups wird neben dem Kalender in der Tabelle **Backups** angezeigt.
7. Wählen Sie das wiederherzustellende Backup aus der Tabelle **Backups** aus.
8. Wählen Sie die wiederherzustellenden Daten unten in der Registerkarte **Select for Restore** im Bereich **Contents of Backup** aus.
9. Geben Sie beim Durchsuchen des Clientdateisystems eine gültige Kombination von Clientbenutzername und Clientpasswort ein und klicken Sie dann auf **OK**.

   Der Benutzername und das Passwort müssen über Leseberechtigungen für die von Ihnen zur Wiederherstellung ausgewählten Dateien und Verzeichnisse verfügen.
10. Wählen Sie **Actions** > **Restore Now** aus.

Suchen nach einem Backup nach Inhalt

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Restore**.

   Der Bereich links oben enthält eine Liste mit Domains.
3. Wählen Sie die Domain mit dem Client aus.

   Clients außerhalb der Domain des Anmeldekontos können nicht angezeigt werden. Melden Sie sich zum Anzeigen aller Clients bei der Root Domain an.

   Eine Liste mit Avamar Clients wird im Bereich unter der Liste mit Domains angezeigt.
4. Wählen Sie den Client aus der Liste aus.
5. Klicken Sie auf die Registerkarte **By File/Folder**.
6. Geben Sie im Textfeld **Enter path to retrieve history for** mit einer der in der folgenden Tabelle genannten Methoden den Pfadnamen zum Inhalt an.

Option	Beschreibung
Type the path	Geben Sie den vollständigen Pfadnamen zum Inhalt im Feld **Enter path to retrieve history for** ein.
Durchsuchen	a. Klicken Sie auf **Browse**. Das Fenster **Select File or Folder** wird angezeigt. b. Wählen Sie den Client aus. c. Wählen Sie das Plug-in aus. Eine Ordnerliste wird in einer Tabelle rechts vom Plug-in-Bereich angezeigt. d. Wählen Sie den wiederherzustellenden Inhalt aus. e. Klicken Sie auf **OK**.

Option	Beschreibung
	Der ausgewählte Inhalt wird im Feld **Enter path to retrieve history for** angezeigt.

7. Klicken Sie auf **Retrieve**.

   In der Tabelle **Version History** werden alle Versionen und Größen des Inhalts in Backups für den Client angegeben.

8. Wählen Sie die Version in der Tabelle **Version History** aus.

   Alle Backups für den Client, die die ausgewählte Version enthalten, werden in der Tabelle **Backups** neben der Tabelle **Version History** angezeigt.

9. Wählen Sie die wiederherzustellenden Daten unten in der Registerkarte **Select for Restore** im Bereich **Contents of Backup** aus.

10. Geben Sie beim Durchsuchen des Clientdateisystems eine gültige Kombination von Clientbenutzername und Clientpasswort ein und klicken Sie dann auf **OK**.

    Der Benutzername und das Passwort müssen über Leseberechtigungen für die von Ihnen zur Wiederherstellung ausgewählten Dateien und Verzeichnisse verfügen.

11. Wählen Sie **Actions** > **Restore Now** aus.

Wiederherstellen am ursprünglichen Speicherort

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.

2. Suchen Sie nach dem wiederherzustellenden Backup:

   - Suchen nach einem Backup nach Datum auf Seite 209
   - Suchen nach einem Backup nach Inhalt auf Seite 210

   Das wiederherzustellende Backup ist in der Tabelle **Backups** ausgewählt.

3. Wählen Sie **Actions** > **Restore Now** aus.

   Das Dialogfeld **Restore Options** wird angezeigt.

4. Übernehmen Sie im Feld **Restore Destination Client** die Standardauswahl des ursprünglichen Clients.

5. Übernehmen Sie in der Liste **Restore Plug-in** die Standardauswahl des ursprünglichen Backup-Plug-ins.

6. Wählen Sie aus der Liste **Avamar encryption method** eine Verschlüsselungsmethode für Client-Server-Datenübertragungen während der Wiederherstellung aus.

   Hinweis

   Die genaue Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-Server-Verbindung sind von mehreren Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.

7. Wählen Sie **Restore everything to its original location** aus.
8. Um bei dieser Wiederherstellung Plug-in-Optionen einzubeziehen, klicken Sie auf **More Options** und konfigurieren Sie dann die Einstellungen. Im Benutzerhandbuch für das jeweilige Plug-in finden Sie Details zu den einzelnen Plug-in-Optionen.
9. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.
10. Klicken Sie auf **Close**.

Wiederherstellen an einem anderen Speicherort

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Suchen Sie nach dem wiederherzustellenden Backup:
   - Suchen nach einem Backup nach Datum auf Seite 209
   - Suchen nach einem Backup nach Inhalt auf Seite 210

   Das wiederherzustellende Backup ist in der Tabelle **Backups** ausgewählt.
3. Wählen Sie **Actions** > **Restore Now** aus.

   Das Dialogfeld **Restore Options** wird angezeigt.
4. Wählen Sie den Zielclient für die wiederherzustellenden Daten aus:
   - Zum Wiederherstellen an einem anderen Speicherort auf demselben Client übernehmen Sie im Feld **Restore Destination Client** die Standardauswahl des ursprünglichen Clients.
   - Um einen anderen Client wiederherzustellen, klicken Sie neben dem Feld **Restore Destination Client** auf die Schaltfläche **Browse**, navigieren Sie zum Zielclient und wählen Sie ihn aus.
5. Wählen Sie aus der Liste **Restore Plug-in** das für die Wiederherstellung zu verwendende Plug-in aus.
6. Wählen Sie aus der Liste **Avamar encryption method** eine Verschlüsselungsmethode für Client-Server-Datenübertragungen während der Wiederherstellung aus.

   Hinweis

   Die genaue Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-Server-Verbindung sind von mehreren Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.
7. Wählen Sie **Restore everything to a different location** aus.

   HINWEIS

   Beim Wiederherstellen eines einzigen Verzeichnisses an einem anderen Speicherort stellt Avamar lediglich den Inhalt des Verzeichnisses wieder her. Das ursprüngliche übergeordnete Verzeichnis wird von Avamar nicht wiederhergestellt.

8. Wählen Sie auf dem Client das Zielverzeichnis für die wiederherzustellenden Daten aus:
   a. Klicken Sie unterhalb der Liste **Items Marked for Restore** auf **Set Destination**.

      Das Dialogfeld **Set Destination** wird angezeigt.

   b. Geben Sie im Feld **Save Target(s) in Directory** den Pfad zum Zielverzeichnis ein oder klicken Sie auf **Browse**, um zu einem Verzeichnis zu navigieren.

      Wenn Sie einen Pfad eingeben und das Verzeichnis nicht vorhanden ist, wird das Verzeichnis im Rahmen des Wiederherstellungsprozesses erstellt.

   c. Klicken Sie im Dialogfeld **Set Destination** auf **OK**.

      Wenn im Pfad, in dem Sie eine Datei wiederherstellen möchten, eine Datei mit demselben Namen vorhanden ist, dann steuern Sie mit der Option **Overwrite Existing Files** des Dialogfelds **Restore Command Line Options**, ob die Datei während des Wiederherstellungsprozesses überschrieben wird.
9. Um bei dieser Wiederherstellung Plug-in-Optionen einzubeziehen, klicken Sie auf **More Options** und konfigurieren Sie dann die Einstellungen. Im Benutzerhandbuch für das jeweilige Plug-in finden Sie Details zu den einzelnen Plug-in-Optionen.
10. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.
11. Klicken Sie auf **Close**.

Wiederherstellen an mehreren Speicherorten

Sie können Backupdaten an mehreren Speicherorten auf einem Zielclient wiederherstellen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.
2. Suchen Sie nach dem wiederherzustellenden Backup:
   - Suchen nach einem Backup nach Datum auf Seite 209
   - Suchen nach einem Backup nach Inhalt auf Seite 210

   Das wiederherzustellende Backup ist in der Tabelle **Backups** ausgewählt.
3. Wählen Sie **Actions** > **Restore Now** aus.

   Das Dialogfeld **Restore Options** wird angezeigt.
4. Wählen Sie den Zielclient für die wiederherzustellenden Daten aus:
   - Zum Wiederherstellen an mehreren Speicherorten auf demselben Client übernehmen Sie im Feld **Restore Destination Client** die Standardauswahl des ursprünglichen Clients.
   - Um an mehreren Speicherorten auf einem anderen Client wiederherzustellen, klicken Sie neben dem Feld **Restore Destination Client** auf die Schaltfläche **Browse**, navigieren Sie zum Zielclient und wählen Sie ihn aus.
5. Wählen Sie aus der Liste **Restore Plug-in** das für die Wiederherstellung zu verwendende Plug-in aus.

6. Wählen Sie aus der Liste **Avamar encryption method** eine Verschlüsselungsmethode für Client-Server-Datenübertragungen während der Wiederherstellung aus.

   Hinweis

   Die genaue Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-Server-Verbindung sind von mehreren Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.

7. Wählen Sie **Restore everything to multiple locations** aus.

   HINWEIS

   Bei der Wiederherstellung mehrerer Verzeichnisse an mehreren Speicherorten stellt Avamar lediglich die Inhalte des Verzeichnisses wieder her. Das ursprüngliche übergeordnete Verzeichnis wird von Avamar nicht wiederhergestellt.

8. Wählen Sie auf dem Client die Zielverzeichnisse für die wiederherzustellenden Daten aus:

   a. Klicken Sie unterhalb der Liste **Items Marked for Restore** auf **Set Destination**.

      Das Dialogfeld **Set Destination** wird angezeigt.

   b. Wählen Sie eine Zeile in der Liste aus.

   c. Geben Sie in die Listenspalte **Destination (Save As)** den Pfad zum Zielverzeichnis ein oder klicken Sie auf **Browse**, um zu einem Verzeichnis zu navigieren.

      Wenn Sie einen Pfad eingeben und das Verzeichnis nicht vorhanden ist, wird das Verzeichnis im Rahmen des Wiederherstellungsprozesses erstellt.

   d. Wiederholen Sie die vorherigen zwei Schritte für jede Zeile in der Liste im Dialogfeld **Set Destination**.

   e. Klicken Sie im Dialogfeld **Set Destination** auf **OK**.

      Wenn im Pfad, in dem Sie eine Datei wiederherstellen möchten, eine Datei mit demselben Namen vorhanden ist, dann steuern Sie mit der Option **Overwrite Existing Files** des Dialogfelds **Restore Command Line Options**, ob die Datei während des Wiederherstellungsprozesses überschrieben wird.

9. Um bei dieser Wiederherstellung Plug-in-Optionen einzubeziehen, klicken Sie auf **More Options** und konfigurieren Sie dann die Einstellungen. Im Benutzerhandbuch für das jeweilige Plug-in finden Sie Details zu den einzelnen Plug-in-Optionen.
10. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.
11. Klicken Sie auf **Close**.

Überwachen von Wiederherstellungen

Sie können Wiederherstellungen überwachen, um sich des erfolgreichen Abschlusses der Wiederherstellung zu vergewissern und ein Troubleshooting im Falle von

Problemen durchzuführen. Mit dem Activity Monitor in Avamar Administrator können Sie Statusinformationen für Wiederherstellungen anzeigen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Eine Liste sämtlicher Aktivitäten wird angezeigt.
3. Um die Ergebnisse so zu filtern, dass ausschließlich Wiederherstellungsaktivitäten angezeigt werden, wählen Sie **Actions** > **Filter** aus.

   Das Dialogfeld **Filter Activity** wird angezeigt.
4. Wählen Sie aus der Liste **Type** die Option **Restore** aus.
5. Klicken Sie auf **OK**.

Abbrechen von Wiederherstellungen

Sie können eine Wiederherstellung jederzeit vor deren Abschluss abbrechen. Der Abbruchvorgang kann 5 Minuten oder länger dauern. Die Wiederherstellung wird u. U. vor Abschluss des Abbruchvorgangs abgeschlossen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Eine Liste sämtlicher Aktivitäten wird angezeigt.
3. Wählen Sie die Wiederherstellung aus der Liste aus.
4. Wählen Sie **Actions** > **Cancel Activity** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
5. Klicken Sie auf **Yes**.

Recovery von Windows-Clientsystemen

Umfassende Details über die erforderlichen Backups zur Recovery von Windows-Clientsystemen und die Verfahren zur Durchführung der Recovery werden im *Avamar for Windows-Server – Benutzerhandbuch* angegeben.

Recovery von Red Hat- und CentOS Linux-Systemen

In den folgenden Themen wird die Wiederherstellung eines Red Hat- bzw. CentOS Linux-Clientsystems in seinen ursprünglichen Systemstatus beschrieben.

Erneutes Aufbauen der Partitionstabelle

Bevor Sie die System-Recovery eines Linux-Clients durchführen, müssen Sie die Partitionstabelle rekonstruieren, die im ursprünglichen Avamar-Backup verwendet wird. Diese Aktion wird durchgeführt, indem der Befehl `avtar --showlog mounts` auf einem temporären Clientcomputer ausgeführt wird. Diese Aktion untersucht dann

die Ausgabe, um die Anzahl und Größe der Partitionen zu ermitteln, die zu erstellen sind, wenn Sie das Betriebssystem auf dem Recovery-Zielclient installieren.

Vorgehensweise

1. Suchen Sie nach dem für die Systemstatus-Recovery zu verwendenden Backup:
   a. Klicken Sie in Avamar Administrator auf den **Backup & Restore** Link zum Startprogramm.

      Das Fenster **Backup, Restore and Manage** wird angezeigt.

   b. Klicken Sie auf die Registerkarte **Restore**.
   c. Wählen Sie in der Clientstruktur den ursprünglichen Linux-Client aus.
   d. Suchen Sie nach dem kompletten für die Wiederherstellung des Systemstatus zu verwendenden Systembackup.
   e. Notieren Sie sich die Backupbezeichnungsnummer.
   f. Lassen Sie Avamar Administrator während des restlichen Verfahrens zur Systemstatus-Recovery geöffnet.
2. Öffnen Sie auf einem temporären Clientcomputer mit Netzwerkverbindung zum Avamar-Server eine Befehlsshell und melden Sie sich als „Root“ an.
3. Geben Sie den folgenden Befehl ein:

   /usr/local/avamar/bin/avtar --avamaronly --showlog mounts --server=*Avamar_server* --id=*username* --ap=*password* --path=*/domain/client* --labelnumber=*n*

   Hierbei gilt:

   - *Avamar_server* ist die IP-Adresse oder der vollständig qualifizierte Hostname, wie im DNS für den Avamar-Server definiert.
   - *username* und „password“ sind die Anmeldedaten für ein Benutzerkonto, das über eine für Wiederherstellungen geeignete Rolle und entsprechende Berechtigungen verfügt.
   - */domain/client* ist der vollständige Speicherort des ursprünglichen Linux-Clients auf dem Avamar-Server.
   - *n* ist die Bezeichnungsnummer des für die Systemstatus-Recovery zu verwendenden Backups.

4. Untersuchen Sie die Befehlsausgabe, um nach mit `mount_decision` beginnenden Einträgen zu suchen.

   Beispiel:

   ```
   mount_decision: reason="starting_point" fstype="ext3"
   path="/"
   mount_decision: reason="default_backup" fstype="ext3"
   path="/boot"
   mount_decision: reason="default_backup" fstype="ext3"
   path="/home"
   ```

   Hierbei handelt es sich um Einträge für die Mount-Punkte auf dem ursprünglichen System. An früherer Stelle in der Ausgabe befinden sich Einträge für jeden dieser Mount-Punkte. Beispiel:

   ```
   mount: status="user_directed_backup" path="/" hdev="/dev/
   root" kind="ext3" blksize=4096 freeblks=1189334
   ```

```
maxblks=2405872 freefiles=2259654 maxfiles=2432000
dev=2050

mount: status="default_backup" path="/boot" hdev="/dev/
sda1" kind="ext3" blksize=1024 freeblks=183371
maxblks=194442 freefiles=50167 maxfiles=50200 dev=2049

mount: status="default_backup" path="/home" hdev="/dev/
sdb1" kind="ext3" blksize=4096 freeblks=1027161
maxblks=5158925 freefiles=2530548 maxfiles=2621440
dev=2065
```

Diese Einträge enthalten neben der Mount-Punktgröße auch Pfadinformationen.

5. Berechnen Sie die ursprüngliche Dateisystemgröße bzw. jeden Mount-Punkt in Byte, indem Sie den Wert `blksize` mit dem Wert `maxblks` multiplizieren.

   HINWEIS

   Durch die Multiplikation des Werts `blksize` mit dem Wert `maxblks` wird der auf dem ursprünglichen Gerät verwendete freie Speicherplatz berechnet. Sie sollten jedoch die Partition des Stammverzeichnisses mit zusätzlichen 2 bis 3 GB an freiem Speicherplatz erstellen, damit ausreichend Speicherplatz für die im Wiederherstellungsprozess genutzte minimale Installation vorhanden ist.

6. Notieren Sie, welche Pfade von den verschiedenen Dateisystemen gemountet werden. Diese Informationen werden zu einem späteren Zeitpunkt im Wiederherstellungsprozess benötigt.

Vorbereiten des Recovery-Zielclients

Vorgehensweise

1. Achten Sie darauf, dass die Recovery-Zielfestplatte mit dem Recovery-Zielclient verbunden ist.
2. Führen Sie eine minimale Installation eines kompatiblen Betriebssystems durch. Für dieses Verfahren:
   - Eine minimale Installation bedeutet, dass Einträge zur Desktopumgebung wie **Desktop – Gnome** nicht zur Installation ausgewählt werden sollten.
   - Wählen Sie in der Kategorie **Base System** im Dialogfeld **Customize Now** die Option **Base** aus. Lassen Sie alle sonstigen Optionen deaktiviert.
   - Kompatibles Betriebssystem ist gleichbedeutend mit der gleichen Version. Wenn beispielsweise das ursprüngliche Clientbackup auf dem Avamar-Server von einem RHEL3-Client stammt, installieren Sie RHEL3 auf dem Recovery-Zielclient.
   - Verwenden Sie die während des Verfahrens Erneutes Aufbauen der Partitionstabelle auf Seite 215 gesammelten Informationen, um genügend Partitionen für die Replikation der ursprünglichen Konfiguration zu erstellen.
3. (Optional) Speichern Sie eine Kopie der Datei `/etc/fstab`, damit Sie diese mit der wiederhergestellten Datei `/etc/fstab` vergleichen können.
4. Installieren Sie Avamar Client für Linux. Anweisungen finden Sie im *Avamar Backup Clients – Benutzerhandbuch*.

Durchführen einer System-Recovery auf einem Red Hat- oder CentOS Linux-Client

Bevor Sie beginnen

Führen Sie die Schritte in Erneutes Aufbauen der Partitionstabelle auf Seite 215 und Vorbereiten des Recovery-Zielclients auf Seite 217 aus.

Vorgehensweise

1. Starten Sie den Recovery-Zielclient über die Installationsmedien (erste CD/DVD):
   - Geben Sie bei der Eingabeaufforderung in Red Hat oder CentOS 4 bzw. 5 **`linux rescue`** ein.
   - Wählen Sie unter Red Hat oder CentOS 6.0 **Rescue installed system** aus.
   - Unter Red Hat oder CentOS 7.0 oder höher:
     a. Wählen Sie **Troubleshooting** aus.
        a. Wählen Sie **Rescue a Red Hat Enterprise Linux system** aus.
2. Befolgen Sie die Anweisungen auf dem Bildschirm.

   Aktivieren Sie die Netzwerkfunktion, indem Sie bei Aufforderung die IP-Adresse, die Netzwerkmaske, das Standardgateway sowie die DNS-Serverwerte angeben. Sie können einen temporären Hostnamen und eine temporäre IP-Adresse oder die ursprünglichen Informationen von dem Computer verwenden, den Sie wiederherstellen.
3. Richten Sie auf Red Hat oder CentOS 7.0 oder höher die Netzwerkverbindungen ein, indem Sie die folgenden Schritte ausführen:

   a. Melden Sie sich als root an.

   b. **`chroot /mnt/sysimage`**

   c. Ändern Sie `/etc/hosts`, `/etc/resolv.conf` und `/etc/sysconfig/network`, soweit für die Netzwerkkonfiguration erforderlich.

   d. Starten Sie die Netzwerkservice neu, damit die Änderungen wirksam werden:

   `service network restart`

   e. Geben Sie **`exit`** ein, um in den Einzelbenutzermodus zurückzukehren.
4. Lassen Sie zu, dass das Installationsprogramm nach Installationen sucht und mounten Sie das Dateisystem `/mnt/sysimage` mit Lese-/Schreibrechten.

   Das Dateisystem `/mnt/sysimage` ist das Ziel der Wiederherstellung und wird auch als *Recovery-Zielfestplatte* bezeichnet.

Hinweis

Sie können das Stammdateisystem nicht direkt in `/mnt/sysimage` wiederherstellen, da es keine Methode gibt, den Wiederherstellungsvorgang nur auf die lokale Partition ohne Durchlauf der Netzwerk-Mount-Punkte zu beschränken. Daher könnten durch eine direkte Wiederherstellung in `/mnt/sysimage` Dateien von allen Partitionen kopiert werden und `/mnt/sysimage` könnte aufgefüllt werden, bevor alle erforderlichen Dateien wiederhergestellt sind.

5. Sorgen Sie dafür, dass die folgenden Verzeichnisse in der Systemvariable `LD_LIBRARY_PATH` vorhanden sind:
   - `/lib`
   - `/lib64`
   - `/usr/lib`
   - `/usr/lib64`
   - `/mnt/sysimage/lib`
   - `/mnt/sysimage/lib64`
   - `/mnt/sysimage/usr/local/avamar/lib`

   Falls Verzeichnisse aus `LD_LIBRARY_PATH` fehlen, fügen Sie diese hinzu.
6. Erstellen Sie mithilfe eines UNIX-Texteditors eine temporäre `/tmp/avtar.cmd`-Flag-Datei. Beispiel:

   cd /tmpvi avtar.cmd--bindir=/mnt/sysimage/usr/local/avamar/bin--vardir=/mnt/sysimage/usr/local/avamar/var--sysdir=/mnt/sysimage/usr/local/avamar/etc--server=*Avamar_server*--account=/*domain/client*--id=*username*--ap=*password*--target=.

   Hierbei gilt:
   - *Avamar_server* steht für die IP-Adresse bzw. den vollständig qualifizierten Hostnamen des Avamar-Servers, wie im DNS definiert.
   - */domain/client* ist der vollständige Speicherort des ursprünglichen Linux-Clients auf dem Avamar-Server.
   - *username* und *password* sind die Anmeldedaten für ein Benutzerkonto, das über eine für die Wiederherstellung geeignete Rolle und entsprechende Berechtigungen verfügt.
7. Stellen Sie die meisten der ursprünglich unter dem Stammverzeichnis (**/**) vorhandenen Verzeichnisse wieder her:

   HINWEIS

   Stellen Sie zu diesem Zeitpunkt keine Dateien auf Dateisystemen wieder her, bei denen es sich nicht um das Stammdateisystem handelt. Diese Verzeichnisse und Dateien werden später in diesem Verfahren wiederhergestellt.

   a. Erstellen Sie ein temporäres Wiederherstellungsverzeichnis unter dem Clientverzeichnis `/mnt/sysimage` und ändern Sie das Verzeichnis darauf, indem Sie den folgenden Beispielen ähnelnde Befehle eingeben:

```
mkdir /mnt/sysimage/restorecd /mnt/sysimage/restore
```

b. Stellen Sie den Inhalt des Stammdateisystems aus dem Backup wieder her, indem Sie den folgenden Befehl in eine einzige Befehlszeile eingeben:

```
/mnt/sysimage/usr/local/avamar/bin/avtar.bin -x --
flagfile=/tmp/avtar.cmd --labelnumber=n [--exclude=./boot --
exclude=./home] /
```

n ist dabei die Bezeichnungsnummer des für die Systemstatus-Recovery zu verwendenden Backups.

Verwenden Sie `--exclude=`*path*-Optionen, um als separate Mount-Punkte identifizierte Pfade auszuschließen. Diese Verzeichnisse und Dateien werden später in diesem Verfahren separat wiederhergestellt.

Die ersten beiden `--exclude`-Optionen im vorherigen Befehl werden als Beispiel angegeben. Ersetzen Sie die Werte durch Optionen, die dem wiederherzustellenden System entsprechen. Geben Sie Ausschlussoptionen in Bezug auf das Stammverzeichnis des ursprünglichen Backups an. z. B. **`--exclude=./boot`** statt **`--exclude=/boot`**.

c. Löschen Sie für jedes wiederhergestellte Verzeichnis das ursprüngliche Verzeichnis aus `/mnt/sysimage` und verschieben Sie das wiederhergestellte Verzeichnis von dem Verzeichnis `/mnt/sysimage/restore` zu `/mnt/sysimage`. Geben Sie hierzu den folgenden Beispielen ähnelnde Befehle ein:

```
rm -rf /mnt/sysimage/etcmv /mnt/sysimage/restore/etc /mnt/
sysimage/etc
```

d. Wiederholen Sie den vorherigen Schritt für jedes Verzeichnis, das erfolgreich in `/mnt/sysimage/restore` wiederhergestellt wurde.

8. Stellen Sie die einzelnen Dateien im Stammverzeichnis (`/`) wieder her:

a. Wechseln Sie in das Verzeichnis `/mnt/sysimage/restore`, indem Sie den folgenden Befehl eingeben:

```
cd /mnt/sysimage/restore
```

b. Stellen Sie die einzelnen Dateien im Stammverzeichnis (`/`) wieder her, indem Sie die folgenden Befehle eingeben:

```
mv ./* /mnt/sysimagemv ./.* /mnt/sysimage
```

9. Stellen Sie andere Mount-Punkte wieder her:

a. Prüfen Sie, ob die Dateisysteme erwartungsgemäß gemountet wurden, indem Sie **`df -h`** an der Eingabeaufforderung eingeben.

b. Vergleichen Sie die Ausgabe mit dem erwarteten Satz an gemounteten Dateisystemen. Mounten Sie die Geräte bei Diskrepanzen auf die richtigen Mount-Punkte.

c. Ändern Sie das Verzeichnis zu jedem Mount-Punkt, indem Sie einen dem folgenden Beispiel ähnelnden Befehl eingeben:

```
cd /mnt/sysimage/home
```

d. Erstellen Sie eine temporäres Wiederherstellungsverzeichnis und ändern Sie das Verzeichnis darauf, indem Sie den folgenden Beispielen ähnelnde Befehle eingeben:

```
mkdir ./restorecd ./restore
```

e. Stellen Sie den Inhalt des Mount-Punkts wieder her, indem Sie den folgenden Befehl eingeben:

```
/mnt/sysimage/usr/local/avamar/bin/avtar.bin -x --
flagfile=/tmp/avtar.cmd --labelnumber=n /home
```

Dabei steht *n* für die Bezeichnungsnummer des zum Wiederherstellen zu verwendenden Backups und */home* für ein Beispiel für einen Mount-Punkt.

f. Kehren Sie zum Mount-Punktverzeichnis zurück und löschen Sie alle Dateien außer das Wiederherstellungsverzeichnis, indem Sie den folgenden Beispielen ähnelnde Befehle eingeben:

```
alias ls=/usr/bin/lscd /mnt/sysimage/home; rm -rf `ls --hide
restore`rm -rf ./.*
```

g. Wechseln Sie in das `restore`-Verzeichnis und verschieben Sie dann den Inhalt an die richtige Stelle im Mount-Punkt, indem Sie den folgenden Befehl eingeben:

```
cd ./restore;mv `ls -A ./` ..
```

h. Entfernen Sie das `restore`-Verzeichnis, indem Sie die folgenden Befehle eingeben:

```
cd ..rmdir restore
```

i. Wiederholen Sie die Schritte d bis i für alle übrigen Mount-Punkte.

10. So führen Sie endgültige Systemprüfungen durch:

a. Überprüfen Sie `/mnt/sysimage/etc/fstab` und vergewissern Sie sich, dass für jedes auf dem neuen System zu mountende Dateisystem gültige Anweisungen vorhanden sind.

Es gibt drei Möglichkeiten, wie Geräte in der Datei `fstab` aufgelistet sein können: Gerätepfad, Volume-Bezeichnung und Universally Unique Identifier (UUID).

Sie können diese Informationen über die Dateisysteme ermitteln, indem Sie **/mnt/sysimage/lib/udev/vol_id *device_path*** eingeben. Dabei steht *device_path* für den `/dev`-Pfad zum Gerät.

Wenn dieses Programm nicht im System vorhanden ist, geben Sie **/mnt/sysimage/sbin/blkid *device_path*** ein.

Wenn Sie während der minimalen Systeminstallation Partitionen manuell erstellt haben, haben sich die Geräte-UUIDs ggf. geändert. Aktualisieren Sie die Geräte-UUIDs in `/mnt/sysimage/etc/fstab`. Wenn einigen Volumes die erwarteten Bezeichnungen fehlen, legen Sie die entsprechende Bezeichnung fest, indem Sie **/mnt/sysimage/sbin/e2label *device_path label*** eingeben.

b. Prüfen Sie `fstab` nochmals sorgfältig.

Das wiederhergestellte System kann nicht korrekt gestartet werden, wenn die `fstab` -Einträge nicht exakt mit der Speichergerätekonfiguration übereinstimmen. Das Wiederherstellungssystem auf den Installationsmedien hat Probleme bei der Erkennung der auf `/mnt/sysimage` zu mountenden Dateisysteme.

Hinweis

Wenn Sie eine Referenzkopie der Datei `fstab` bei der Vorbereitung des Zielclients auf die Recovery gespeichert haben, können Sie die Festplatteninformationen in dieser Datei finden. Bei Systemen mit geringfügigen manuellen Änderungen der wiederhergestellten `fstab`-Datei ist es ggf. möglich, die `fstab`-Referenzdatei statt der wiederhergestellten Dateikopie zu verwenden.

c. Überprüfen Sie, dass keine weiteren Dateien in `/mnt/sysimage/restore` vorhanden sind, indem Sie den folgenden Befehl eingeben:

```
ls -al /mnt/sysimage/restore
```

d. Wenn das Verzeichnis leer ist, entfernen Sie es, indem Sie den folgenden Befehl eingeben:

```
rmdir /mnt/sysimage/restore
```

e. Wenn der Befehl fehlschlägt, weil das Verzeichnis nicht leer ist, sind womöglich Verzeichnisse vorhanden, die Sie bei der Wiederherstellung der meisten Verzeichnisse im Stammverzeichnis (`/`) nicht verschieben konnten. Verschieben Sie die Verzeichnisse an die entsprechenden Speicherorte für die Wiederherstellung.

11. Beenden Sie die Befehlsshell und starten Sie das System neu, indem Sie **`exit`** eingeben.

    Bei einem Neustart eines Red Hat- oder CentOS 6-Systems wird ein Menü angezeigt.

12. Wählen Sie **reboot** und dann **OK** aus. Drücken Sie anschließend die **Enter**.

    Das System wird neu gestartet.

13. Werfen Sie die Installationsmedien aus und starten Sie wie gewohnt.
14. Vergewissern Sie sich eines ordnungsgemäßen Clientbetriebs.

Troubleshooting einer System-Recovery auf einem Red Hat- oder CentOS Linux-Client

In den folgenden Abschnitten werden Details zum Troubleshooting von Problemen beschrieben, die nach der Durchführung einer System-Recovery auf einem Red Hat- oder CentOS Linux-Client auftreten können.

Troubleshooting eines Startfehlers nach einer System-Recovery

Wenn das wiederhergestellte System am Ende des Wiederherstellungsverfahrens nicht startet, weist die während der minimalen Betriebssysteminstallation eingerichtete GRUB-Version u. U. zu große Unterschiede zu der zuvor auf dem Server genutzten Version auf. Starten Sie in der Wiederherstellungsumgebung und installieren Sie GRUB neu.

Vorgehensweise

1. Starten Sie in der Wiederherstellungsumgebung, indem Sie den Client von den Installationsmedien mit der Rescue-Option starten.
2. Wenn das wiederhergestellte Betriebssystem nicht im Rahmen des Startprozesses gefunden werden kann, dann ist `fstab` wahrscheinlich nicht korrekt konfiguriert. Mounten Sie die Partitionen manuell und korrigieren sie den Inhalt der Datei.
3. Installieren Sie GRUB neu, indem Sie die folgenden Befehle eingeben:

   `chroot /mnt/sysimagegrub-install` ***`device`***

   device steht dabei für das Startgerät (z. B. `/dev/sda`).

4. Beenden Sie die chroot-Umgebung, indem Sie **`exit`** eingeben.
5. Beenden Sie die Befehlsshell und starten Sie das System neu, indem Sie **`exit`** eingeben.

   Bei einem Neustart eines Red Hat- oder CentOS 6-Systems wird ein Menü angezeigt.
6. Wählen Sie **reboot** und dann **OK** aus. Drücken Sie anschließend die **Enter**.

   Das System wird neu gestartet.
7. Werfen Sie die Installationsmedien aus und starten Sie wie gewohnt.

Wiederherstellen der Netzwerkeinstellungen nach einer System-Recovery eines Linux-Clients

Wenn das Betriebssystem erkennt, dass das System auf neue Hardware wiederhergestellt wurde, werden die Netzwerkeinstellungen möglicherweise auf die Standardwerte zurückgesetzt (z. B. DHCP-Namensauflösung statt statischer IP). Die vorherigen Netzwerkeinstellungen lassen sich durch eine manuelle Neukonfiguration der Einstellungen wiederherstellen.

Zur Prüfung der vorherigen Einstellungen öffnen Sie die `.bak`-Dateien in `/etc/sysconfig/network-scripts` in einem Texteditor. Diese Dateien beinhalten zwar nützliche Informationen, sie sollten in der aktuellen Konfiguration jedoch nicht in unveränderter Form verwendet werden, da sie MAC-Adressinformationen aus vorheriger Hardware aufweisen.

Recovery von SUSE Linux-Systemen

In den folgenden Themen wird die Wiederherstellung eines SUSE Linux-Clientsystems in seinen ursprünglichen Systemstatus beschrieben.

Erneutes Aufbauen der Partitionstabelle

Bevor Sie die System-Recovery eines Linux-Clients durchführen, müssen Sie die Partitionstabelle rekonstruieren, die im ursprünglichen Avamar-Backup verwendet wird. Diese Aktion wird durchgeführt, indem der Befehl `avtar --showlog mounts` auf einem temporären Clientcomputer ausgeführt wird. Diese Aktion untersucht dann die Ausgabe, um die Anzahl und Größe der Partitionen zu ermitteln, die zu erstellen sind, wenn Sie das Betriebssystem auf dem Recovery-Zielclient installieren.

Vorgehensweise

1. Suchen Sie nach dem für die Systemstatus-Recovery zu verwendenden Backup:

a. Klicken Sie in Avamar Administrator auf den **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.

b. Klicken Sie auf die Registerkarte **Restore**.

c. Wählen Sie in der Clientstruktur den ursprünglichen Linux-Client aus.

d. Suchen Sie nach dem kompletten für die Wiederherstellung des Systemstatus zu verwendenden Systembackup.

e. Notieren Sie sich die Backupbezeichnungsnummer.

f. Lassen Sie Avamar Administrator während des restlichen Verfahrens zur Systemstatus-Recovery geöffnet.

2. Öffnen Sie auf einem temporären Clientcomputer mit Netzwerkverbindung zum Avamar-Server eine Befehlsshell und melden Sie sich als „Root“ an.
3. Geben Sie den folgenden Befehl ein:

   /usr/local/avamar/bin/avtar --avamaronly --showlog mounts --server=*Avamar_server* --id=*username* --ap=*password* --path=*/domain/client* --labelnumber=*n*

   Hierbei gilt:

   - *Avamar_server* ist die IP-Adresse oder der vollständig qualifizierte Hostname, wie im DNS für den Avamar-Server definiert.
   - *username* und „password“ sind die Anmeldedaten für ein Benutzerkonto, das über eine für Wiederherstellungen geeignete Rolle und entsprechende Berechtigungen verfügt.
   - */domain/client* ist der vollständige Speicherort des ursprünglichen Linux-Clients auf dem Avamar-Server.
   - *n* ist die Bezeichnungsnummer des für die Systemstatus-Recovery zu verwendenden Backups.

4. Untersuchen Sie die Befehlsausgabe, um nach mit `mount_decision` beginnenden Einträgen zu suchen.

   Beispiel:

   ```
   mount_decision: reason="starting_point" fstype="ext3"
   path="/"
   mount_decision: reason="default_backup" fstype="ext3"
   path="/boot"
   mount_decision: reason="default_backup" fstype="ext3"
   path="/home"
   ```

   Hierbei handelt es sich um Einträge für die Mount-Punkte auf dem ursprünglichen System. An früherer Stelle in der Ausgabe befinden sich Einträge für jeden dieser Mount-Punkte. Beispiel:

   ```
   mount: status="user_directed_backup" path="/" hdev="/dev/
   root" kind="ext3" blksize=4096 freeblks=1189334
   maxblks=2405872 freefiles=2259654 maxfiles=2432000
   dev=2050

   mount: status="default_backup" path="/boot" hdev="/dev/
   sda1" kind="ext3" blksize=1024 freeblks=183371
   maxblks=194442 freefiles=50167 maxfiles=50200 dev=2049

   mount: status="default_backup" path="/home" hdev="/dev/
   sdb1" kind="ext3" blksize=4096 freeblks=1027161
   ```

```
maxblks=5158925 freefiles=2530548 maxfiles=2621440
dev=2065
```

Diese Einträge enthalten neben der Mount-Punktgröße auch Pfadinformationen.

5. Berechnen Sie die ursprüngliche Dateisystemgröße bzw. jeden Mount-Punkt in Byte, indem Sie den Wert `blksize` mit dem Wert `maxblks` multiplizieren.

   HINWEIS

   Durch die Multiplikation des Werts `blksize` mit dem Wert `maxblks` wird der auf dem ursprünglichen Gerät verwendete freie Speicherplatz berechnet. Sie sollten jedoch die Partition des Stammverzeichnisses mit zusätzlichen 2 bis 3 GB an freiem Speicherplatz erstellen, damit ausreichend Speicherplatz für die im Wiederherstellungsprozess genutzte minimale Installation vorhanden ist.

6. Notieren Sie, welche Pfade von den verschiedenen Dateisystemen gemountet werden. Diese Informationen werden zu einem späteren Zeitpunkt im Wiederherstellungsprozess benötigt.

Vorbereiten des Recovery-Zielclients

Vorgehensweise

1. Achten Sie darauf, dass die Recovery-Zielfestplatte mit dem Recovery-Zielclient verbunden ist.
2. Führen Sie eine minimale Installation eines kompatiblen Betriebssystems durch. Für dieses Verfahren:
   - Eine minimale Installation bedeutet, dass über die Seite **Software selection** nur die Pakete **Base System** und **Minimal System (Appliances)** installiert werden. Löschen Sie die Auswahl aller anderen Pakete, damit diese nicht installiert werden.
   - Kompatibles Betriebssystem ist gleichbedeutend mit der gleichen Version. Wenn beispielsweise das ursprüngliche Clientbackup auf dem Avamar-Server von einem SLES10-Client stammt, installieren Sie SLES10 auf dem Recovery-Zielclient.
   - Verwenden Sie die während des Verfahrens Erneutes Aufbauen der Partitionstabelle auf Seite 215 gesammelten Informationen, um genügend Partitionen für die Replikation der ursprünglichen Konfiguration zu erstellen.
3. (Optional) Speichern Sie eine Kopie der Datei `/etc/fstab`, damit Sie diese mit der wiederhergestellten Datei `/etc/fstab` vergleichen können.
4. Installieren Sie Avamar Client für Linux. Anweisungen finden Sie im *Avamar Backup Clients – Benutzerhandbuch*.

Durchführen einer System-Recovery auf einem SUSE Linux-Client

Bevor Sie beginnen

Führen Sie die Schritte in Erneutes Aufbauen der Partitionstabelle auf Seite 215 und Vorbereiten des Recovery-Zielclients auf Seite 225 aus.

Vorgehensweise

1. Starten Sie den Recovery-Zielclient über die Installationsmedien (erste CD/DVD) und wählen Sie **Rescue System** aus.

2. Öffnen Sie eine Befehlsshell auf dem Recovery-Zielclient und melden Sie sich als Root an.
3. Mounten Sie die während der minimalen Installation erstellte Partition des Stammverzeichnisses auf `/mnt`, indem Sie den folgenden Befehl eingeben:

   mount */dev/sda#* /mnt

   Dabei steht */dev/sda#* für das Gerät mit dem Stammdateisystem. Wenn das Laufwerk zur Verwendung von Linux Logical Volume Management konfiguriert wurde, liegt das Stammgerät ggf. in der Form `/dev/VolGroup##/LogVol##` vor.

4. Binden Sie die Pseudo-Dateisysteme erneut an die `/mnt`-Baumstruktur, indem Sie die folgenden Befehle eingeben:

   mount --rbind /proc /mnt/procmount --rbind /sys /mnt/sysmount --rbind /dev /mnt/dev

5. Ändern Sie den aktuellen Dateisystemstamm, indem Sie den folgenden Befehl eingeben:

   chroot /mnt

6. Starten Sie das Netzwerk, wie in den Voraussetzungen konfiguriert, indem Sie den folgenden Befehl eingeben:

   rcnetwork start

7. Mounten Sie die automatisch gemounteten Dateisysteme und überprüfen Sie, ob die richtigen Dateisysteme gemountet wurden, indem Sie den folgenden Befehl eingeben:

   mount -a;df -h

8. Wenn Dateisysteme fehlen (wenn z. B. `/boot` nicht auf Auto-Mount eingestellt ist), mounten Sie sie manuell auf die richtigen Speicherorte mithilfe zusätzlicher `mount`-Befehle.
9. Beenden Sie die chroot-Umgebung, indem Sie **exit** eingeben.
10. Kopieren Sie die Namensauflösungsdatei des Netzwerks aus der chroot-Umgebung in die Arbeitsumgebung für die Wiederherstellung, indem Sie den folgenden Befehl eingeben:

    cp /mnt/etc/resolv.conf /etc/resolv.conf

11. Sorgen Sie dafür, dass die folgenden Verzeichnisse in der Systemvariable `LD_LIBRARY_PATH` vorhanden sind:

    - `/lib`
    - `/lib64`
    - `/usr/lib`
    - `/usr/lib64`
    - `/mnt/lib`
    - `/mnt/lib64`
    - `/mnt/usr/local/avamar/lib`

    Falls Verzeichnisse aus `LD_LIBRARY_PATH` fehlen, fügen Sie diese hinzu.

12. Erstellen Sie mithilfe eines UNIX-Texteditors eine temporäre `/tmp/avtar.cmd`-Flag-Datei. Beispiel:

cd /tmpvi avtar.cmd--bindir=/mnt/usr/local/avamar/bin--vardir=/mnt/usr/local/avamar/var--sysdir=/mnt/usr/local/avamar/etc--server=*Avamar_server*--account=*/domain/client*--id=*username*--ap=*password*--target=.

Hierbei gilt:

- *Avamar_server* ist die IP-Adresse des Avamar-Servers oder der vollständig qualifizierte Hostname, wie im DNS definiert.
- */domain/client* ist der vollständige Speicherort des ursprünglichen Linux-Clients auf dem Avamar-Server.
- *username* und *password* sind die Anmeldedaten für ein Benutzerkonto, das über eine für die Wiederherstellung geeignete Rolle und entsprechende Berechtigungen verfügt.

13. Stellen Sie die meisten der ursprünglich unter dem Stammverzeichnis (`/`) vorhandenen Verzeichnisse wieder her:

HINWEIS

Stellen Sie zu diesem Zeitpunkt keine Dateien auf Dateisystemen wieder her, bei denen es sich nicht um das Stammdateisystem handelt. Diese Verzeichnisse und Dateien werden später in diesem Verfahren wiederhergestellt.

a. Erstellen Sie ein temporäres Wiederherstellungsverzeichnis unter dem Clientverzeichnis `/mnt` und ändern Sie das Verzeichnis darauf, indem Sie den folgenden Beispielen ähnelnde Befehle eingeben:

mkdir /mnt/restorecd /mnt/restore

b. Stellen Sie den Inhalt des Stammdateisystems aus dem Backup wieder her, indem Sie den folgenden Befehl in eine einzige Befehlszeile eingeben:

/mnt/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/avtar.cmd --labelnumber=*n* [--exclude=./boot --exclude=./home] /

n ist dabei die Bezeichnungsnummer des für die Systemstatus-Recovery zu verwendenden Backups.

Verwenden Sie `--exclude=`*path*-Optionen, um als separate Mount-Punkte identifizierte Pfade auszuschließen. Diese Verzeichnisse und Dateien werden später in diesem Verfahren separat wiederhergestellt.

Die ersten beiden `--exclude`-Optionen im vorherigen Befehl werden als Beispiel angegeben. Ersetzen Sie die Werte durch Optionen, die dem wiederherzustellenden System entsprechen. Geben Sie Ausschlussoptionen in Bezug auf das Stammverzeichnis des ursprünglichen Backups an. z. B. **--exclude=./boot** statt **--exclude=/boot**.

c. Löschen Sie für jedes wiederhergestellte Verzeichnis das ursprüngliche Verzeichnis aus `/mnt` und verschieben Sie das wiederhergestellte Verzeichnis von dem Verzeichnis `/mnt/restore` zu `/mnt`. Geben Sie hierzu den folgenden Beispielen ähnelnde Befehle ein:

rm -rf /mnt/etcmv /mnt/restore/etc /mnt/etc

d. Wiederholen Sie den vorherigen Schritt für jedes Verzeichnis, das erfolgreich in `/mnt/restore` wiederhergestellt wurde.

14. Stellen Sie die einzelnen Dateien im Stammverzeichnis (`/`) wieder her:

    a. Wechseln Sie in das Verzeichnis `/mnt/restore`, indem Sie **`cd /mnt/restore`** eingeben.

    b. Stellen Sie die einzelnen Dateien im Stammverzeichnis (`/`) wieder her, indem Sie die folgenden Befehle eingeben:

    ```
    mv ./* /mntmv ./.* /mnt
    ```

15. Stellen Sie andere Mount-Punkte wieder her:

    a. Prüfen Sie, ob die Dateisysteme erwartungsgemäß gemountet wurden, indem Sie **`df -h`** an der Eingabeaufforderung eingeben.

    b. Vergleichen Sie die Ausgabe mit dem erwarteten Satz an gemounteten Dateisystemen. Mounten Sie die Geräte bei Diskrepanzen auf die richtigen Mount-Punkte.

    c. Ändern Sie das Verzeichnis zu jedem Mount-Punkt, indem Sie einen dem folgenden Beispiel ähnelnden Befehl eingeben:

    ```
    cd /mnt/home
    ```

    d. Erstellen Sie eine temporäres Wiederherstellungsverzeichnis und ändern Sie das Verzeichnis darauf, indem Sie den folgenden Beispielen ähnelnde Befehle eingeben:

    ```
    mkdir ./restorecd ./restore
    ```

    e. Stellen Sie den Inhalt des Mount-Punkts wieder her, indem Sie den folgenden Befehl eingeben:

    ```
    /mnt/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/
    avtar.cmd --labelnumber=n /home
    ```

    Dabei steht *n* für die Bezeichnungsnummer des zum Wiederherstellen zu verwendenden Backups und */home* für ein Beispiel für einen Mount-Punkt.

    f. Kehren Sie zum Mount-Punktverzeichnis zurück und löschen Sie alle Dateien außer das Wiederherstellungsverzeichnis, indem Sie den folgenden Beispielen ähnelnde Befehle eingeben:

    ```
    alias ls=/usr/bin/lscd /mnt/home; rm -rf `ls --hide restore`rm
    -rf ./.*
    ```

    g. Wechseln Sie in das `restore`-Verzeichnis und verschieben Sie dann den Inhalt an die richtige Stelle im Mount-Punkt, indem Sie den folgenden Befehl eingeben:

    ```
    cd ./restore;mv `ls -A ./` ..
    ```

    h. Entfernen Sie das `restore`-Verzeichnis, indem Sie die folgenden Befehle eingeben:

    ```
    cd ..rmdir restore
    ```

    i. Wiederholen Sie die Schritte d bis i für alle übrigen Mount-Punkte.

16. So führen Sie endgültige Systemprüfungen durch:

    a. Überprüfen Sie `/mnt/etc/fstab` und vergewissern Sie sich, dass für jedes auf dem neuen System zu mountende Dateisystem gültige Anweisungen vorhanden sind.

    Es gibt drei Möglichkeiten, wie Geräte in der Datei `fstab` aufgelistet sein können: Gerätepfad, Volume-Bezeichnung und Universally Unique Identifier (UUID).

    Sie können diese Informationen über die Dateisysteme ermitteln, indem Sie **`/mnt/lib/udev/vol_id`** ***`device_path`*** eingeben. Dabei steht ***`device_path`*** für den `/dev`-Pfad zum Gerät.

    Wenn Sie während der minimalen Systeminstallation Partitionen manuell erstellt haben, haben sich die Geräte-UUIDs ggf. geändert. Aktualisieren Sie die Geräte-UUIDs in `/mnt/etc/fstab`. Wenn bestimmten Werten die erwarteten Bezeichnungen fehlen, legen Sie die entsprechende Bezeichnung fest, indem Sie **`/mnt/sbin/e2label`** ***`device_path label`*** eingeben.

    b. Prüfen Sie `fstab` nochmals sorgfältig.

    Das wiederhergestellte System kann nicht korrekt gestartet werden, wenn die `fstab` -Einträge nicht exakt mit der Speichergerätekonfiguration übereinstimmen. Das Wiederherstellungssystem auf den Installationsmedien hat Probleme bei der Erkennung der auf `/mnt` zu mountenden Dateisysteme.

    Hinweis

    Wenn Sie eine Referenzkopie der Datei `fstab` bei der Vorbereitung des Zielclients auf die Recovery gespeichert haben, können Sie die Festplatteninformationen in dieser Datei finden. Bei Systemen mit geringfügigen manuellen Änderungen der wiederhergestellten `fstab`-Datei ist es ggf. möglich, die `fstab`-Referenzdatei statt der wiederhergestellten Dateikopie zu verwenden.

    c. Überprüfen Sie, dass keine weiteren Dateien in `/mnt/sysimage/restore` vorhanden sind, indem Sie den folgenden Befehl eingeben:

    `ls -al /mnt/restore`

    d. Wenn das Verzeichnis leer ist, entfernen Sie es, indem Sie den folgenden Befehl eingeben:

    `rmdir /mnt/restore`

    e. Wenn der Befehl fehlschlägt, weil das Verzeichnis nicht leer ist, sind womöglich Verzeichnisse vorhanden, die Sie bei der Wiederherstellung der meisten Verzeichnisse im Stammverzeichnis (**`/`**) nicht verschieben konnten. Verschieben Sie die Verzeichnisse an die entsprechenden Speicherorte für die Wiederherstellung.

17. Starten Sie das System neu, indem Sie **`reboot`** eingeben.
18. Werfen Sie die Installationsmedien aus und starten Sie wie gewohnt.
19. Vergewissern Sie sich eines ordnungsgemäßen Clientbetriebs.

Troubleshooting einer System-Recovery auf einem SUSE Linux-Client

In den folgenden Themen werden Details zum Troubleshooting von Problemen beschrieben, die nach der Durchführung einer System-Recovery auf einem SUSE Linux-Client auftreten können.

Troubleshooting eines Startausfalls nach einer System-Recovery

Wenn das wiederhergestellte System am Ende des Wiederherstellungsverfahrens nicht startet, weist die während der minimalen Betriebssysteminstallation eingerichtete GRUB-Version u. U. zu große Unterschiede zu der zuvor auf dem Server genutzten Version auf. Starten Sie in der Wiederherstellungsumgebung und installieren Sie GRUB neu.

Vorgehensweise

1. Starten Sie in der Wiederherstellungsumgebung:
   a. Starten Sie den Recovery-Zielclient über die Installationsmedien (erste CD/DVD) und wählen Sie **Rescue System** aus.
   b. Öffnen Sie eine Befehlsshell auf dem Recovery-Zielclient und melden Sie sich als Root an.
   c. Mounten Sie die während der minimalen Installation erstellte Partition des Stammverzeichnisses auf `/mnt`, indem Sie den folgenden Befehl eingeben:

      mount */dev/sda#* /mnt

      Dabei steht */dev/sda#* für das Gerät mit dem Stammdateisystem. Wenn das Laufwerk zur Verwendung von Linux Logical Volume Management konfiguriert wurde, liegt das Stammgerät ggf. in der Form `/dev/VolGroup##/LogVol##` vor.

   d. Binden Sie die Pseudo-Dateisysteme erneut an die `/mnt`-Baumstruktur, indem Sie die folgenden Befehle eingeben:

      mount --rbind /proc /mnt/procmount --rbind /sys /mnt/sysmount --rbind /dev /mnt/dev

   e. Ändern Sie den aktuellen Dateisystemstamm, indem Sie den folgenden Befehl eingeben:

      chroot /mnt

   f. Starten Sie das Netzwerk, wie in den Voraussetzungen konfiguriert, indem Sie den folgenden Befehl eingeben:

      rcnetwork start

   g. Mounten Sie die automatisch gemounteten Dateisysteme und überprüfen Sie, ob die richtigen Dateisysteme gemountet wurden, indem Sie den folgenden Befehl eingeben:

      mount -a;df -h

   h. Wenn Dateisysteme fehlen (wenn z. B. `/boot` nicht auf Auto-Mount eingestellt ist), mounten Sie sie manuell auf die richtigen Speicherorte mithilfe zusätzlicher `mount`-Befehle.
2. Installieren Sie GRUB neu, indem Sie die folgenden Befehle eingeben:

chroot /mntgrub-install *device*

device steht dabei für das Startgerät (z. B. `/dev/sda`).

3. Beenden Sie die chroot-Umgebung, indem Sie **exit** eingeben.
4. Starten Sie das System neu, indem Sie **reboot** eingeben.
5. Werfen Sie die Installationsmedien aus und starten Sie wie gewohnt.

Wiederherstellen der Netzwerkeinstellungen nach einer System-Recovery eines Linux-Clients

Wenn das Betriebssystem erkennt, dass das System auf neue Hardware wiederhergestellt wurde, werden die Netzwerkeinstellungen möglicherweise auf die Standardwerte zurückgesetzt (z. B. DHCP-Namensauflösung statt statischer IP). Die vorherigen Netzwerkeinstellungen lassen sich durch eine manuelle Neukonfiguration der Einstellungen wiederherstellen.

Zur Prüfung der vorherigen Einstellungen öffnen Sie die `.bak`-Dateien in `/etc/sysconfig/network-scripts` in einem Texteditor. Diese Dateien beinhalten zwar nützliche Informationen, sie sollten in der aktuellen Konfiguration jedoch nicht in unveränderter Form verwendet werden, da sie MAC-Adressinformationen aus vorheriger Hardware aufweisen.

Oracle Solaris-System-Recovery

In den folgenden Themen wird die Wiederherstellung eines Oracle Solaris-Clientsystems in seinen ursprünglichen Systemstatus beschrieben.

Vorbereiten für eine Oracle Solaris-System-Recovery

Vergewissern Sie sich, dass die Umgebung die folgenden Voraussetzungen erfüllt, bevor Sie eine System-Recovery für ein Oracle Solaris-System durchführen.

Verfügbares Backup mit wichtigen Systemdateien
Um ein Oracle Solaris-Clientsystem erfolgreich in seinen ursprünglichen Systemstatus wiederherzustellen, müssen Sie über ein Avamar-Backup des gesamten lokalen Dateisystems und der folgenden wichtigen Systemdateien und virtuellen Dateisysteme verfügen. Erreicht wird dies, indem während des Backups ein Durchlauf der in der folgenden Tabelle aufgeführten Ziele erzwungen wird.

Tabelle 39 Zielspeicherorte für System-Recovery-Backups eines Oracle Solaris-Clients

Ziel	Beschreibung
`mntfs`	`/etc/svc/volatile`
`tmpfs`	`/etc/mnttab`
`cachefs`	Solaris Cache File System
`fdfs`	Solaris File Descriptor File System
`fifofs`	Solaris FIFO File System
`namefs`	Solaris Name File System
`specfs`	Solaris Device Special File System
`swapfs`	Solaris Swap File System

Tabelle 39 Zielspeicherorte für System-Recovery-Backups eines Oracle Solaris-Clients (Fortsetzung)

Ziel	Beschreibung
`tfs`	Solaris Translucent File System

Verwenden Sie eine der folgenden Backupmethoden, um dafür zu sorgen, dass diese Ziele in ein Backup eingeschlossen werden:

- Fügen Sie in Avamar Administrator diese Ziele explizit zu einem On-Demand-Backup oder Dataset hinzu, indem Sie **`mntfs,tmpfs,cachefs,fdfs,fifofs,namefs,specfs,swapfs,tfs`** im Feld **Force traversal of the specified file system type(s)** der Plug-in-Optionen angeben.
- Geben Sie **`--forcefs="mntfs,tmpfs,cachefs,fdfs,fifofs,namefs,specfs,swapfs,tfs"`** in der `avtar`-Befehlszeile an.

Verfügbare /var- und /opt-Dateisysteme
Die ursprünglichen Dateisystemtabellen müssen Partitionen für `/opt` und `/var` haben. Die Partitionen für `/opt` und `/var` werden gemountet, wenn Sie Solaris im schreibgeschützten Modus starten.

Wenn die Partitionen nicht gemountet werden, müssen Sie beim Installieren einer Solaris-Minimalversion auf dem Client neue, temporäre Dateisysteme für `/opt` und `/var` erstellen.

Andere Dateisysteme
Vergewissern Sie sich bei Verwendung von `zfs` oder einem anderen Add-on-Dateisystem, dass diese Dateisysteme vor Beginn der System-Recovery korrekt neu erstellt und gemountet wurden.

Installation einer Minimalversion von Solaris
Erstellen Sie ein Dateisystemlayout, das dem ursprünglichen System möglichst nahekommt. Achten Sie darauf, dass separate Dateisysteme für `/opt` und `/var` vorhanden sind.

Durchführen einer System-Recovery eines Oracle Solaris-Clients

Bevor Sie beginnen

Führen Sie die Schritte in Vorbereiten für eine Oracle Solaris-System-Recovery auf Seite 231 aus.

Vorgehensweise

1. Führen Sie einen Start von CD aus, wobei Sie **`reboot -- cdrom`** eingeben oder die Startreihenfolge je nach Plattform im BIOS-Menü ändern.
2. (Nur Solaris 11 und 10) Wählen Sie im Menü der Startoptionen eine der folgenden Optionen aus:
   - **3. Solaris Interactive Text (Desktop session)**
   - **4. Solaris Interactive Text (Console session)**
3. Folgen Sie den Eingabeaufforderungen und geben Sie bei Aufforderung den Clienthostnamen, die IP-Adresse, das Standardgateway und den Namen des DNS-Servers des Unternehmens an.

4. Beenden Sie die Eingabeaufforderung und kehren Sie zu einer Shelleingabeaufforderung zurück:
   - Drücken Sie unter Solaris 8 **!**, wenn Sie zur Installation der Software für Solaris mit Solaris Web Start aufgefordert werden.
   - Drücken Sie unter Solaris 10 oder 11 **F5**, um die Eingabeaufforderung bei der Auswahl des Installationstyps zu beenden, und drücken Sie dann **F2**, um das Beenden zu bestätigen.
5. Mounten Sie die Partition `/` unter `/a` als Ziel der Wiederherstellung. Geben Sie dazu folgenden Befehl ein:

   ```
   mount /dev/dsk/c1t0d0s0 /a
   ```

   Verwenden Sie die korrekten speicherortspezifischen Laufwerkspartitions- und Mount-Parameter für das Stamm-Volume.
6. Geben Sie den folgenden Befehl ein, um die Partition `/opt` unter `/opt` zu mounten:

   ```
   mount /dev/dsk/c1t0d0s5 /opt
   ```

   Verwenden Sie die korrekten speicherortspezifischen Laufwerkspartitions- und Mount-Parameter für das `/opt`-Volume.
7. Geben Sie den folgenden Befehl ein, um die Partition `/var` unter `/var` zu mounten:

   ```
   mount /dev/dsk/c1t0d0s4 /var
   ```

   Verwenden Sie die korrekten speicherortspezifischen Laufwerkspartitions- und Mount-Parameter für das `/var`-Volume.
8. Mounten Sie zusätzliche Dateisysteme in den jeweiligen Mount-Punkten unter `/a`.

   Wenn der Mount-Punkt nicht existiert, erstellen Sie ihn. Geben Sie beispielsweise den folgenden Befehl ein, um das Dateisystem `/data01` auf `c1t0d0s7` zu mounten:

   ```
   mount /dev/dsk/c1t0d0s7 on /a/data01
   ```
9. Installieren Sie mithilfe der Anweisungen im Avamar Client für Solaris die richtige Version der *Avamar Backup Clients – Benutzerhandbuch*-Software.

   HINWEIS

   Beim Versuch, `/etc/init.d/avagent` und verschiedene Links in `/usr/bin` und `/etc/rc.d/rcX.d` zu erstellen, zeigt das Installationsprogramm eine Warnung an, laut der im Stammverzeichnis (`/`) 0 freie Byte vorhanden sind. Außerdem werden Fehler in Bezug auf schreibgeschützte Dateisysteme ausgegeben. Trotz dieser Warnungen sind jedoch alle Binärdateien ordnungsgemäß unter `/opt/AVMRclnt/bin` installiert.
10. Stellen Sie `/etc` auf `/a/etc` wieder her, indem Sie die folgenden Befehle eingeben:

    ```
    cd /a/etc/opt/AVMRclnt/bin/avtar -x --server=Avamar_server --
    id=username --password=password --account=/domain/client --
    target=. /etc --labelnumber=n --overwrite=always
    ```

Hierbei gilt:

- *Avamar_server* ist der Hostname oder die IP-Adresse des Avamar-Servers.
- *username* und *password* sind die Avamar-Anmeldedaten für einen Benutzer mit einer Rolle, die Zugriff auf die Backups für diesen Client ermöglicht.
- */domain/client* ist die wiederherzustellende Avamar-Domain und der wiederherzustellende Solaris-Client.
- *n* ist die Bezeichnungsnummer des wiederherzustellenden Backups. Wenn Sie keine Bezeichnungsnummer angeben, wird das letzte Backup zur Wiederherstellung verwendet.

HINWEIS

Sie können das Stammdateisystem nicht direkt in `/a` wiederherstellen, da es derzeit keinen Weg gibt, den Wiederherstellungsvorgang nur auf die lokale Partition ohne Durchlauf der Netzwerk-Mount-Punkte zu beschränken. Durch eine direkte Wiederherstellung in `/a` könnten Dateien von allen Partitionen kopiert werden und `/a` könnte aufgefüllt werden, bevor alle erforderlichen Dateien wiederhergestellt sind.

11. Prüfen Sie `/a/etc/vfstab`, um die ursprünglichen Mount-Punkte für das lokale Dateisystem zu überprüfen.
12. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

    Das Fenster **Backup, Restore and Manage** wird angezeigt.
13. Klicken Sie auf die Registerkarte **Restore**.
14. Wählen Sie in der Clientstruktur den ursprünglichen Solaris-Client aus.
15. Suchen Sie nach dem für die Wiederherstellung zu verwendenden Backup und wählen Sie es aus.
16. Untersuchen Sie die Verzeichnisse und Dateien, die sich ursprünglich im Stammverzeichnis (**/**) befanden.
17. Gehen Sie für jedes Verzeichnis, das sich ursprünglich im Stammverzeichnis (**/**) befand, wie folgt vor:
    a. Wenn das Verzeichnis nicht vorhanden ist, erstellen Sie unter `/a` manuell ein leeres Verzeichnis mit demselben Namen.
    b. Wechseln Sie in dieses Verzeichnis.
    c. Stellen Sie über die Befehlszeile den Inhalt des Verzeichnisses aus dem Backup wieder her.

    Setzen Sie etwa die folgenden Befehle zum Wiederherstellen von `/usr` ein:

    ```
    mkdir /a/usr; cd /a/usr/opt/AVMRclnt/bin/avtar -x --
    server=Avamar_server --id=username --password=password --
    account=/domain/client --labelnumber=n --overwrite=always --
    target=. /usr
    ```

    Wenn sich `/opt` und `/var` ursprünglich auf der Stammpartition befanden, können Sie die Wiederherstellung zu `/a/opt` und `/a/var` durchführen. Handelte es sich bei `/opt` und `/var` um separate Dateisysteme, führen Sie die Wiederherstellung auf neue, temporäre Speicherorte durch, wie beispielsweise `/a/newopt` und `/a/newvar`. Nach Durchführung sämtlicher

Wiederherstellungen verschieben Sie die Inhalte von `/a/newopt` zu `/opt` und von `/a/newvar` zu `/var`.

18. Um die einzelnen, ursprünglich unter dem Stammverzeichnis vorhandenen Dateien wiederherzustellen, führen Sie den Wiederherstellungsbefehl mit der Option `--norecursion` zum Wiederherstellen von Dateien ohne Wechsel in Unterverzeichnisse aus:

    /opt/AVMRclnt/bin/avtar -x --server=*Avamar_server* --id=*username* --password=*password* --account=*/domain/client* --labelnumber=*n* --norecursion --overwrite=always --target=. /

19. Starten Sie den Client wie gewohnt neu und vergewissern Sie sich eines ordnungsgemäßen Betriebs.

KAPITEL 8

Serveradministration

In diesem Kapitel werden folgende Themen behandelt:

Herunterfahren und Neustarten des Servers

Die Komponenten, aus denen ein Avamar-Server besteht, werden in Stufen heruntergefahren:

- Herunterfahren der Avamar-Software oder einzelner Subsysteme als Teil der Wartung und andere angegebener Aktivitäten
- Herunterfahren der Avamar-Software, des Betriebssystems und der Hardware als Teil einer vollständigen Ausschaltung

Die folgenden Themen beschreiben beide Prozesse ausführlicher.

Verwalten der Avamar-Subsysteme

Das `dpnctl`-Programm ermöglicht Ihnen das ordnungsgemäße Herunterfahren und Neustarten der Avamar-Software oder ausgewählter Subsysteme über die Befehlszeilenoberfläche. Dieser Prozess ist unabhängig von einem Neustart des Betriebssystems.

Das Herunterfahren oder Neustarten der Avamar-Software stoppt alle Avamar-Subsysteme als Gruppe bzw. startet sie als Gruppe neu.

Herunterfahren der Avamar-Software

Bevor Sie beginnen

Achten Sie darauf, dass ein aktueller und validierter Prüfpunkt vorhanden ist, bevor Sie das System komplett herunterfahren.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
2. Geben Sie **`dpnctl stop`** ein.

   Daraufhin werden Sie aufgefordert zu bestätigen, dass Sie die lokale Instanz von EM Tomcat herunterfahren möchten.
3. Geben Sie **`y`** ein, um die lokale EM Tomcat-Instanz herunterzufahren, und drücken Sie die **Enter**.

   Die Ausgabe zeigt den Status des Herunterfahrens an, bis der Vorgang abgeschlossen ist.

Neustart der Avamar-Software

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:

- Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
- Bei einem Multi-Node-Server:
  a. Melden Sie sich als Administrator beim Utility Node an.
  b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

  ```
  ssh-agent bashssh-add ~admin/.ssh/admin_key
  ```

2. Geben Sie `dpnctl start` ein.

   Die Ausgabe zeigt eine Bestätigungsmeldung an.
3. Geben Sie `y` ein, um das Neustarten der Software zu beginnen, und drücken Sie die **Enter**.

   Die Ausgabe zeigt den Status des Neustartens an, bis der Vorgang abgeschlossen ist.

Stoppen des MCS

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```

2. Geben Sie `dpnctl stop mcs` ein.

Starten des MCS

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```

2. Geben Sie `dpnctl start mcs` ein.
3. Setzen Sie die geplanten Vorgänge fort, indem Sie `dpnctl start sched` eingeben.

Abrufen des MCS-Status

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
2. Geben Sie `dpnctl status mcs` ein.

Beenden des EM Tomcat-Servers

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Wenn Sie sich bei einem Multi-Node-Server anmelden, melden Sie sich als Administrator beim Utility-Node an.
2. Geben Sie `dpnctl stop emt` ein.

Starten des EM Tomcat-Servers

Bevor Sie beginnen

Vergewissern Sie sich, dass der EM Tomcat-Server korrekt heruntergefahren wurde.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Wenn Sie sich bei einem Multi-Node-Server anmelden, melden Sie sich als Administrator beim Utility-Node an.
2. Geben Sie `dpnctl start emt` ein.

Anfordern des EM Tomcat-Serverstatus

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:

a. Melden Sie sich als Administrator beim Utility Node an.

b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. Geben Sie `dpnctl status emt` ein.

Ausschalten oder Neustarten des Servers

Mit Avamar Administrator können Sie den gesamten Avamar-Server einschließlich der Avamar-Software, des Betriebssystems und der Hardware (sofern zutreffend) ordnungsgemäß ausschalten oder neu starten.

Hinweis

Für Avamar Data Store schaltet dieser Prozess alle Nodes aus oder startet sie neu.

Voraussetzungen

Vor dem Ausschalten oder Neustarten des Avamar-Servers sind die folgenden Voraussetzungen zu erfüllen:

- Beenden Sie alle Backup-, Wiederherstellungs- und Datenverschiebungsvorgänge. Der Prozess zum Herunterfahren beendet alle aktiven Vorgänge, bevor er fortfährt.
- Beenden Sie alle aktiven Avamar Installation Manager-Paketvorgänge.
- Stellen Sie sicher, dass während der letzten 36 Stunden ein validierter Prüfpunkt erstellt wurde.
- Stellen Sie sicher, dass der MCS während der letzten 12 Stunden geleert wurde.
- Beenden oder stoppen Sie alle automatischen Speicherbereinigungen und HFS-Prüfvorgänge.
  Der Prozess zum Herunterfahren beendet alle aktiven Vorgänge, bevor er fortfährt.
- Stellen Sie sicher, dass genügend freier Speicherplatz vorhanden ist.
  Die Serverauslastung muss weniger als 85 % der Gesamtkapazität und 62 % der verfügbaren Avamar-Subsystemspeicherkapazität betragen.

Ausschalten des Servers

Schalten Sie den Server aus, um Wartungsarbeiten wie die Behebung von Standortstromausfällen oder Verlagerung von physischer Ausrüstung zu ermöglichen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Server Management**.
3. Wählen Sie den Server aus, den Sie ausschalten möchten.
4. Wählen Sie **Actions** > **Shut Down Avamar System** aus.

   Ein Bestätigungsdialogfeld wird angezeigt.
5. Klicken Sie auf **Yes**.

   Der Server gibt eine Benachrichtigung über das bevorstehende Herunterfahren aus.

6. Klicken Sie auf **OK**.

   Der Server startet den Ausschaltprozess.

Ergebnisse

Die folgenden Protokolle bieten weitere Informationen und Aktualisierungen zum Fortschritt:

- `/usr/local/avamar/var/log/avosshutdown.log`
- `/usr/local/avamar/var/log/dpnctl.log`

Weitere Erfordernisse

Nach Abschluss der Wartung schalten Sie den Server mithilfe einer der folgenden Methoden ein:

- Netzschalter auf der Frontplatte des Controllers (Gen4S)
- Netzschalter/Reset-Taste auf der hinteren I/O-Platte (Gen4T)
- Fenster der RMM4- oder RMC-Stromregelung
- Steuerungskonsole oder Steuerungsschnittstelle für die virtuelle Umgebung

Bei Multi-Node-Servern schalten Sie alle Speicher-Nodes der Reihe nach und dann den Utility-Node ein.

Hinweis

Das Einschalten des Utility-Node vor den Speicher-Nodes kann zu Verzögerungen beim Startvorgang führen.

Neustarten des Servers

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Server Management**.
3. Wählen Sie den neu zu startenden Server aus.
4. Wählen Sie **Actions** > **Reboot Avamar System** aus.

   Ein Bestätigungsdialogfeld wird angezeigt.
5. Klicken Sie auf **Yes**.

   Der Server gibt eine Benachrichtigung über das bevorstehende Neustarten aus.
6. Klicken Sie auf **OK**.

   Der Server startet den Neustartvorgang.

Ergebnisse

Die folgenden Protokolle bieten weitere Informationen und Aktualisierungen zum Fortschritt:

- `/usr/local/avamar/var/log/avosshutdown.log`
- `/usr/local/avamar/var/log/dpnctl.log`

Unterbrechen und Wiederaufnehmen von Serveraktivitäten

Backups und Wiederherstellungen, geplante Vorgänge und Wartungsaktivitäten können unterbrochen und wieder aufgenommen werden.

Unterbrechen und Wiederaufnehmen von Backups und Wiederherstellungen

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Server Management**.
3. Wählen Sie im linken Bereich den Avamar-Server-Node aus.
4. Öffnen Sie das Menü **Actions** und wählen Sie **Suspend Backups/Restores** oder **Resume Backups/Restores** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
5. Klicken Sie auf **Yes**.

Unterbrechen und Wiederaufnehmen geplanter Vorgänge

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.

   Das Fenster **Manage All Schedules** wird angezeigt.
2. Klicken Sie auf **Suspend All** oder **Resume All**.

Unterbrechen und Wiederaufnehmen von Wartungsaktivitäten

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.
2. Öffnen Sie das Menü **Actions** und wählen Sie **Suspend Maintenance Activities** oder **Resume Maintenance Activities** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
3. Klicken Sie auf **OK**.

Managen der Clientsitzungen

Sie können zum Troubleshooting oder zur Analyse eines Backups oder einer Wiederherstellung ein ausführliches Protokoll einer Clientsitzung anzeigen. Falls erforderlich, können Sie bei unerwartetem Systemverhalten eine Clientsitzung abbrechen oder einen Client zurücksetzen.

Überwachen von Clientsitzungen

Auf der Registerkarte „Session Monitor“ ist eine Liste der aktiven Clientbackup- und -wiederherstellungssitzungen aufgeführt.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Session Monitor**.

   Die Informationen in der folgenden Tabelle werden für jede Sitzung in „Session Monitor“ angezeigt.

   Tabelle 40 Registerkarte „Session Monitor“ – Eigenschaften

Eigenschaft	Beschreibung
User	
User	Avamar-Benutzer-ID (Kontoname).
Path	Legt einen hierarchischen Speicherort auf dem Avamar-Server fest. Diese Option hängt mit dem Startspeicherort des Benutzers zusammen, es sei denn, vor der Pfadzuweisung steht ein Schrägstrich (/) als Präfix. In diesem Fall wird von einem absoluten Pfad ausgegangen.
Domain	Avamar-Domain, in der sich der Benutzer befindet.
Client ID	Eindeutige Kennung für diesen Avamar-Client.
Sitzung	
Type	Diese Aktivität ist entweder `avtarbackup` oder `avtarrestore`.
Root	Oberste gesicherte, wiederhergestellte oder validierte Ebene des Dateisystems.
Start time	Datum und Uhrzeit, zu der diese Clientsitzung gestartet wurde.
Plug-in	Für diese Aktivität verwendetes Plug-in.
Session ID	Eindeutige Kennung für diese Clientsitzung.
Work order ID	Eindeutige Kennung für diese Aktivität.
Elapsed	Bisherige Ausführungsdauer der Clientsitzung.
Progress bytes	Gesamtmenge der während dieser Aktivität untersuchten Byte.
New bytes	Prozentsatz der neuen auf dem Avamar-Server oder einem Data Domain-System gesicherten Byte. Eine niedrige Zahl steht für ein hohes Maß an Datendeduplizierung.
System	
Name	Clienthostname.
OS name	Von diesem Client verwendetes Betriebssystem.

Tabelle 40 Registerkarte „Session Monitor“ – Eigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
App version	Version der Avamar-Clientsoftware.

Anzeigen eines detaillierten Clientsitzungsprotokolls

Sie können für Troubleshooting- oder Analysezwecke ein ausführliches Protokoll einer Clientsitzung anzeigen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Standardmäßig zeigt „Activity Monitor“ ein detailliertes Protokoll aller Clientbackupaktivitäten aus den letzten 72 Stunden an.

3. Legen Sie die Optionen für das Sitzungsprotokoll fest:

   a. Wählen Sie **Action** > **Session Log Options** aus.

      Das Dialogfeld **Session Log Options** wird angezeigt.

   b. Wählen Sie **Show HTML logs** aus, um die Zusammenfassung des Sitzungsprotokolls im HTML-Format anzuzeigen, oder klicken Sie auf **Show raw logs**, um die Sitzungsprotokollübersicht unformatiert anzuzeigen.

   c. (Optional) Wenn Sie das HTML-Protokollformat auswählen, aktivieren Sie das Kontrollkästchen **Show debug information**, um Troubleshooting-Informationen in die Sitzungsprotokollübersicht aufzunehmen.

   d. Klicken Sie auf **OK**.

4. Wählen Sie eine Aktivität aus der Liste aus.

5. Wählen Sie **Actions** > **View Session Log** aus.

   Das Dialogfeld **Activity Session Drill-down** wird angezeigt.

6. Führen Sie beliebige der folgenden Aufgaben in der Sitzungsprotokollübersicht durch:

   - (Nur HTML-Format) Klicken Sie im Abschnitt **Log Files** auf einen Hyperlink, um zur Protokolldatei zu wechseln.
   - Suchen Sie nach einer bestimmten Textzeichenfolge in der Sitzungsprotokollübersicht, indem Sie eine Textzeichenfolge im Feld **Find** eingeben und dann auf **Next** oder **Previous** klicken.
   - Klicken Sie auf **Back to Top**, um zum oberen Bereich der Sitzungsprotokollübersicht zurückzukehren.
   - Exportieren Sie die Sitzungsprotokollübersicht in eine Datei, indem Sie auf **Export** klicken, einen Speicherort für die Datei angeben und auf **Save** klicken.
   - Aktualisieren Sie den Inhalt in der Sitzungsprotokollübersicht, indem Sie auf **Refresh** klicken.

7. Klicken Sie auf **Close**.

Erstellen einer Zip-Datei für Avamar-Support

Mithilfe des Fensters **Activity** können Sie eine ZIP-Datei mit Informationen des Sitzungsprotokolls für den Avamar-Support erstellen und die ZIP-Datei auf den Avamar-Server hochladen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.
2. Wählen Sie eine Aktivität aus der Liste aus.
3. Wählen Sie **Actions** > **Download Support Bundle** aus.

   Das Dialogfeld **Download Support Bundle** wird angezeigt.
4. Navigieren Sie zu einem Verzeichnis für die ZIP-Datei.
5. Klicken Sie auf **Save**.

   In einem Fortschrittsdialogfeld wird der Status des Vorgangs angezeigt.
6. Wenn der Vorgang abgeschlossen ist, klicken Sie im Fortschrittsdialogfeld auf **Close**.
7. Wählen Sie **Actions** > **Upload Support Bundle to Server** aus, um eine ZIP-Datei zu erstellen und sie auf den Avamar-Server zu kopieren.

   Während des Prozesses zum Hochladen wird eine ZIP-Datei für Sitzungsprotokollübersichtsinformationen erstellt und diese ZIP-Datei wird in den Ordner `/tmp` auf dem Avamar-Server kopiert. In einem Fortschrittsdialogfeld wird der Status des Vorgangs angezeigt.

Abbrechen einer Clientsitzung

Gelegentlich kann bei einem Client während eines Backups oder einer Wiederherstellung ein unerwartetes Systemverhalten auftreten. In diesen Fällen kann es notwendig sein, das Ende dieser Clientsitzungen über Avamar-Administrator zu erzwingen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Session Monitor**.

   Eine Liste aktiver Clientsitzungen wird angezeigt.
3. Wählen Sie die abzubrechende Clientsitzung aus.
4. Wählen Sie **Actions** > **Cancel Session** aus.

   In einem Dialogfeld wird der Fortschritt für den Abbruchvorgang angezeigt.
5. Wenn der Abbruchvorgang abgeschlossen ist, klicken Sie auf **Close**.

Weitere Erfordernisse

Wenn Sie die Clientsitzung nicht abbrechen können, setzen Sie den Client zurück. Durch diesen Schritt werden aktive `avtar`-Sitzungen auf dem Client sofort und erzwungenermaßen beendet.

Zurücksetzen eines Clients

Durch das unmittelbare und erzwungene Zurücksetzen eines Clients wird die aktive Client-`avtar`-Sitzung auf diesem Client beendet. In den meisten Fällen sollten Sie versuchen, die Clientsitzung vor dem Zurücksetzen abzubrechen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Clients**.
4. Wählen Sie den zurückzusetzenden Client aus.
5. Wählen Sie aus dem Menü **Actions** den Befehl **Client** > **Reset Client** aus.

Managen von Client-Agents und Plug-ins

Wenn ein Client mit einem Avamar-Server kommuniziert, identifiziert er sich selbst, indem er Folgendes sendet:

- Die Client-ID
- Die spezifische Agent-Version
- Den auf diesem Client ausgeführten Build
- Eine Liste der derzeit auf diesem Client installierten Plug-ins (Version und Build)

Mitunter sollten Sie dem Avamar-Server aufgrund bekannter Inkompatibilitätsprobleme möglicherweise den Zugriff auf alle Clients mit einer bestimmten Version (allen Builds) oder einem bestimmten Build eines Client-Agent oder Plug-ins verweigern.

Außerdem können Sie die folgenden Plug-in-Vorgänge für alle Clients mit einer bestimmten Plug-in-Version (alle Builds) oder einem bestimmten Build wahlweise zulassen oder nicht zulassen:

- Vom Client initiierte Clientaktivierungen
- Vom Client initiierte On-Demand-Backups
- Geplante Backups
- Wiederherstellungen
- Backupvalidierung
- Möglichkeit zum Durchsuchen gespeicherter Backups auf dem Server

Jeder spezifischen Version (allen Builds) bzw. jedem Build, die bzw. der als veraltet gekennzeichnet wurde, wird der Zugriff auf den Avamar-Server verweigert. Ein Build wird nur in Fällen bekannter Inkompatibilität zwischen Client-Agent oder Plug-in und der spezifischen Version der installierten Serversoftware als veraltet gekennzeichnet. Diese zur Bestimmung veralteter Versionen und Builds verwendete Kennzeichnung kann nicht mithilfe der Funktion zur Bearbeitung von Eigenschaften dieser Version bzw. dieses Build überschrieben werden, um potenzielle Probleme zu verhindern.

Hinzufügen eines Build-Datensatzes

Sie können einen MCS-Datenbankdatensatz für einen bestimmten Build eines Client-Agent oder Plug-ins hinzufügen. Sie können Datensätze ausschließlich auf Build-

Ebene hinzufügen. Datensätze für eine neue Version werden nach dem Durchführen von Upgrades der Avamar-Serversoftware automatisch hinzugefügt.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Agents & Plug-ins** aus.

   Das Fenster **Manage All Agents & Plug-ins** wird angezeigt.
2. Wählen Sie im linken Bereich die Agent- oder Plug-in-Version für den Build aus.
3. Klicken Sie auf **New**.

   Das Dialogfeld **New Build** wird angezeigt.
4. Geben Sie im Feld **Build** eine gültige Agent- oder Plug-in-Nummer ein.
5. Aktivieren Sie das Kontrollkästchen **Disable**, um dem Avamar-Server den Zugriff auf Clients mit diesem Agent- oder Plug-in-Build zu verweigern.
6. (Optional) Geben Sie im Feld **Kommentar** einen beschreibenden Kommentar ein.
7. Klicken Sie auf **OK**.

Bearbeiten von Versions- bzw. Build-Datensätzen

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Agents & Plug-ins** aus.

   Das Fenster **Manage All Agents & Plug-ins** wird angezeigt.
2. Wählen Sie im linken Bereich den Agent oder das Plug-in aus.
3. Wählen Sie im rechten Bereich die zu bearbeitende Version bzw. den zu bearbeitenden Build aus.
4. Klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Build** wird angezeigt.
5. Aktivieren Sie das Kontrollkästchen **Disable**, um dem Avamar-Server den Zugriff auf Clients mit diesem Agent- oder Plug-in-Build zu verweigern.
6. (Optional) Geben Sie im Feld **Kommentar** einen beschreibenden Kommentar ein.
7. Klicken Sie auf **OK**.

Löschen eines Build-Datensatzes

Sie können einen MCS-Datenbankdatensatz für einen bestimmten Build eines Client-Agent oder Plug-ins löschen. Sie können einen Datensatz für eine gesamte Version nicht löschen.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Agents & Plug-ins** aus.

   Das Fenster **Manage All Agents & Plug-ins** wird angezeigt.
2. Wählen Sie im linken Bereich den Agent oder das Plug-in aus.
3. Wählen Sie im rechten Bereich den zu löschenden Build aus.

Klicken Sie auf **Delete**.

Deaktivieren aller clientinitiierten Aktivierungen

Sie sollten Clients vorübergehend an der Aktivierung mit dem Avamar-Server hindern, um das System in einen Zustand zu versetzen, der Wartungsaktivitäten unterstützt. Die Clienteinladung funktioniert nicht, wenn Clients nicht aktiviert werden können.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Agents & Plug-ins** aus.

   Das Fenster **Manage All Agents & Plug-ins** wird angezeigt.
2. Klicken Sie auf **Disable All Client Initiated Activations**.
3. Um clientinitiierte Aktivierungen wieder zu aktivieren, klicken Sie auf **Enable All Client Initiated Activations**.

Deaktivieren aller clientinitiierten Backups

Sie können Avamar-Clients vorübergehend an der Initiierung von On-Demand-Backups hindern, um das System in einen Zustand zu versetzen, der verschiedene Wartungsaktivitäten unterstützt.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Agents & Plug-ins** aus.

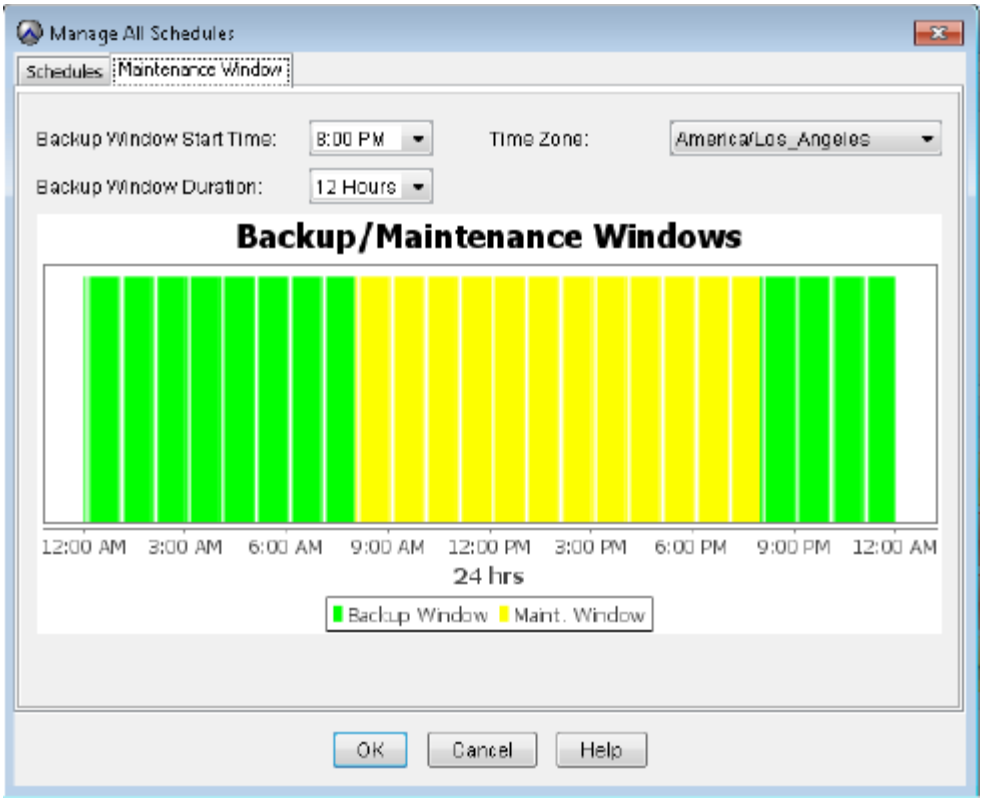
   Das Fenster **Manage All Agents & Plug-ins** wird angezeigt.
2. Klicken Sie auf **Disable All Client Initiated Backups**.
3. Um clientinitiierte On-Demand-Backups wieder zu aktivieren, klicken Sie auf **Enable All Client Initiated Backups**.

Backup- und Wartungszeitfenster

Jeder 24 Stunden umfassende Tag ist in zwei Betriebszeitfenster unterteilt: das Backupzeitfenster und das Wartungszeitfenster.

Die folgende Abbildung zeigt die standardmäßigen Backup- und Wartungszeitfenster an.

Abbildung 14 Standardbackup- und Wartungszeitfenster



Backupzeitfenster

Das Backupzeitfenster ist der Teil jedes Tages, der zur Durchführung von normal geplanten Backups reserviert ist. Während des Backupzeitfensters werden keine Wartungsaktivitäten durchgeführt.

Das standardmäßige Backupzeitfenster beginnt um 20 Uhr lokaler Serverzeit und läuft 12 Stunden ununterbrochen bis um 8 Uhr am folgenden Morgen. Startzeit und Dauer des Backupzeitfensters lassen sich anpassen.

Wartungszeitfenster

Das Wartungszeitfenster ist der Teil jedes Tages, der für die Durchführung von Routineaktivitäten für die Serverwartung in der folgenden Tabelle reserviert ist.

Tabelle 41 Avamar-Serverwartungsaktivitäten

Aktivität	Beschreibung
Kontrollpunkt	Ein Snapshot des Avamar-Servers, der ausdrücklich für Server-Rollbacks erstellt wird.
Kontrollpunktvalidierung	Ein interner Vorgang, der die Integrität eines bestimmten Kontrollpunkts validiert. Die Kontrollpunktvalidierung wird auch als HFS-Kontrolle (Hash File System) bezeichnet. Nachdem ein Kontrollpunkt eine HFS-Kontrolle bestanden hat, kann er als zuverlässig genug betrachtet werden, um ein Serverrollback durchzuführen.

Tabelle 41 Avamar-Serverwartungsaktivitäten (Fortsetzung)

Aktivität	Beschreibung
Automatische Speicherbereinigung	Ein interner Vorgang, der Speicherplatz von gelöschten oder abgelaufenen Backups wiederherstellt.

Obwohl Backups und Wiederherstellungen während des Wartungszeitfensters möglich sind, haben diese Auswirkungen auf Backup-, Wiederherstellungs- und Wartungsaktivitäten. Beschränken Sie daher während des Wartungsfensters Backup-, Wiederherstellungs- oder Administrationsaktivitäten auf ein Minimum. Kurzzeitig sind ggf. weder Backup- noch Administrationsaktivitäten zulässig.

Das standardmäßige Wartungszeitfenster beginnt um 8:00 Uhr lokaler Serverzeit und läuft 12 Stunden ununterbrochen bis um 20:00 Uhr. Obwohl Sie das Wartungszeitfenster nicht direkt ändern können, werden seine Startzeit und Dauer von Einstellungen des Backupzeitfensters abgeleitet.

Bearbeiten der Backup- und Wartungszeitfenster

Sie können die Backup- und Wartungszeitfenster durch Festlegen der Startzeit und Dauer für das Backupzeitfenster sowie der Zeitzone für die Backup- und Wartungszeitfenster bearbeiten.

Alle Änderungen in Bezug auf die Dauer des Backupzeitfensters wirken sich auch auf die Dauer des Wartungszeitfensters aus. Wenn Sie beispielsweise die Dauer des Backupzeitfensters von 12 Stunden zu 14 Stunden ändern, verkürzt sich hierdurch die Dauer des Wartungszeitfenster um 2 Stunden.

Die folgenden Best Practices gelten für die Planung von Systemaktivitäten:

- Zahl der On-Demand-Backups während des Wartungszeitfensters begrenzen

  Möglicherweise sollten Sie Benutzern dazu raten, während der ersten eineinhalb Stunden des Wartungszeitfensters (bei den meisten Systemen zwischen 8:00 und 20:00 Uhr lokaler Zeit) die Initiierung von On-Demand-Backups über Clientcomputer zu vermeiden.
- Initiierung von On-Demand-Wartungsaktivitäten vermeiden

  Durch die manuelle Initiierung von Wartungsaktivitäten, wie zum Beispiel Kontrollpunkte, Kontrollpunktvalidierungen oder automatische Speicherbereinigung, werden bis zum Abschluss der manuell initiierten Prozesse vorübergehend alle geplanten Wartungsaktivitäten deaktiviert. Sofern die Initiierung einer On-Demand-Wartungsaktivität nicht verpflichtend ist, ist als Best Practice auf geplante Wartungsaktivitäten zu setzen, damit allen Aktivitäten täglich ausreichend Zeit zugewiesen ist.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.

   Das Fenster **Manage All Schedules** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Maintenance Window**.
3. Ändern Sie die Startzeit und Dauer des Backupzeitfensters oder die Zeitzone, indem Sie aus der entsprechenden Liste einen neuen Wert auswählen.
4. Klicken Sie auf **OK**.

Kontrollpunkte

Bei Prüfpunkten handelt es sich um systemweite, zur Unterstützung bei der Disaster Recovery erstellte Backups.

Ein Kontrollpunkt wird automatisch während des Wartungszeitfensters ausgeführt. Sie können Kontrollpunkte auch jederzeit manuell starten.

Sie können Kontrollpunkte löschen, um Serverspeicherkapazität wiederzugewinnen.

Auf der Registerkarte **Checkpoint Management** im Fenster **Server** von Avamar Administrator wird der Status der einzelnen Prüfpunkte angezeigt. In der folgenden Tabelle sind die möglichen Status für einen Kontrollpunkt angegeben.

Tabelle 42 Kontrollpunktstatus

Status	Beschreibung
	Die Kontrollpunktvalidierung ist fehlgeschlagen oder wurde vor Abschluss abgebrochen.
	Der Kontrollpunkt wurde noch nicht validiert.
	Validierung wird für diesen Kontrollpunkt durchgeführt.
	Die Validierung des Kontrollpunkts ist erfolgt.

Erstellen eines Kontrollpunkts

Ein Kontrollpunkt wird automatisch während des Wartungszeitfensters ausgeführt. Sie können Prüfpunkte auch jederzeit manuell starten.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Checkpoint Management**.
3. Wählen Sie **Actions** > **Create Checkpoint** aus.

   In einem Fortschrittsdialogfeld wird der Status des Vorgangs angezeigt.
4. Klicken Sie nach Fertigstellung des Kontrollpunkts auf **Close**.

Löschen eines Kontrollpunkts

Sie können Kontrollpunkte löschen, um zusätzliche Serverspeicherkapazität wiederzugewinnen. Es ist allgemein besser, nicht validierte Kontrollpunkte zu löschen, bevor Sie validierte Kontrollpunkte löschen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Checkpoint Management**.

3. Wählen Sie den Kontrollpunkt und dann die Option **Actions** > **Delete Checkpoint** aus.

   Es wird eine Bestätigungsmeldung angezeigt.

4. Klicken Sie auf **OK**.

Ausführen eines Rollbacks auf einen Kontrollpunkt

Bei einem Rollback wird mithilfe der in einem validierten Prüfpunkt gespeicherten Daten ein bekannter fehlerfreier Zustand des Avamar-Servers wiederhergestellt. Für einen Avamar-Server Version 7.x kann kein Rollback auf Version 4.x oder einen früheren Prüfpunkt durchgeführt werden.

Bevor Sie beginnen

Wenn Sie nach der Prüfpunkterstellung Nodes zum Avamar-Server hinzugefügt haben, entfernen Sie die Einträge für die Nodes aus der Datei `probe.out`.

Verwenden Sie für Rollbacks nur validierte Prüfpunkte. Eine Kontrollpunktvalidierung erfolgt in jedem Wartungszeitfenster.

Hinweis

Wenn Sie vor Abschluss des nächsten Wartungszeitfensters einen validierten Prüfpunkt benötigen, setzen Sie sich zwecks Hilfestellung mit dem Avamar-Support in Verbindung.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```

2. Fahren Sie den Server herunter, indem Sie **`dpnctl stop`** eingeben.
3. Zeigen Sie eine Liste der Kontrollpunkte an, indem Sie **`cplist`** eingeben.

   Die daraufhin angezeigte Kontrollpunktliste ähnelt dem folgenden Beispiel:

   ```
   cp.20140106170113 Fri Jan 6 17:01:13 2014 valid hfs del
   nodes 4 stripes 396
   cp.20140107170042 Sat Jan 7 17:00:42 2014 valid hfs del
   nodes 4 stripes 396
   cp.20140108170040 Sun Jan 8 17:00:40 2014 valid hfs ...
   nodes 4 stripes 396
   cp.20140109170043 Mon Jan 9 17:00:43 2014 valid hfs ...
   nodes 4 stripes 396
   ```

   Hierbei gilt:

   - *cp.yyyymmddhhmmss* ist die Kontrollpunkt-ID.
   - `valid hfs` gibt einen validierten Prüfpunkt an.

- `valid par` gibt einen teilweise validierten Prüfpunkt an.

4. Achten Sie auf die Kontrollpunkt-ID des Kontrollpunkts, die für das Rollback verwendet werden soll.

   Führen Sie grundsätzlich ein Rollback auf den zuletzt vollständig validierten Kontrollpunkt durch, es sei denn, ein Rollback auf einen früheren Kontrollpunkt ist aus guten Gründen erforderlich.

5. Starten Sie das Rollback, indem Sie den folgenden Befehl eingeben:

   `rollback.dpn --cptag=`*`checkpoint_id`*` >& `*`file`

   Dabei steht *checkpoint_id* für die Kontrollpunkt-ID und *file* für eine temporäre Datei.

6. Warten Sie, bis das Rollback abgeschlossen ist. Je nach Datenmenge auf dem Avamar-Server kann das Rollback bis zu einer Stunde in Anspruch nehmen.

   Nach Abschluss des Rollbacks wird erneut die Eingabeaufforderung angezeigt.

7. Öffnen Sie die während des Rollbacks erstellte benutzerdefinierte temporäre Datei und vergewissern Sie sich, dass das Rollback erfolgreich und ohne Fehler abgeschlossen wurde.

   Der Server wird nach einem erfolgreichen Rollback automatisch neu gestartet.

Löschen einer Datenintegritätswarnmeldung

Um Datenintegrität zu ermöglichen, gibt der Avamar-Server eine Warnmeldung aus, wenn eine Prüfpunktvalidierung fehlschlägt. Die einzige Möglichkeit zum Löschen dieser Warnmeldung besteht darin, den Avamar-Support zu kontaktieren, um einen Code zum Zurücksetzen zu beziehen, und diesen Code in das Dialogfeld **Clear Data Integrity Alert** einzugeben.

Bevor Sie beginnen

Beziehen Sie einen Code zum Zurücksetzen vom Avamar-Support.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Event Management**.
3. Klicken Sie auf die Registerkarte **Unacknowledged Events** im unteren Bereich des Fensters.
4. Wählen Sie **Actions** > **Event Management** > **Clear Data Integrity Alert** aus.

   Das Dialogfeld **Clear Data Integrity Alert** wird angezeigt.

5. Geben Sie den Code zum Zurücksetzen im Feld **Enter reset code** ein und klicken Sie auf **OK**.

Aktivieren der Avamar-Software und Installieren einer Serverlizenz

Der Avamar-Server benötigt für den dauerhaften Betrieb einen Lizenzschlüssel. Andernfalls können verschiedene Funktionen des Avamar-Servers nach Ablauf einer Toleranzperiode von 30 Tagen nicht mehr verwendet werden. Ab Avamar-Version 7.3 wird die Avamar-Software über ihre Common Licensing Platform lizenziert. Die

Legacy-Lizenzierung für Avamar wird ebenfalls unterstützt. Bei früheren Versionen der Avamar-Software ist nur der Legacy-Mechanismus verfügbar.

Aktivieren der Avamar-Software bei Verwendung der Common Licensing Platform

Aktivieren Sie die Avamar-Software bei Verwendung der Common Licensing Platform anhand des folgenden Verfahrens:

Bevor Sie beginnen

Dieses Verfahren erfordert einen Lizenzauthorisierungscode (License Authorization Code, LAC), den Sie in der LAC-E-Mail erhalten haben. Wenn Sie die E-Mail nicht finden können, senden Sie eine E-Mail an licensing@emc.com, um einen erneuten Versand der Lizenzautorisierung anzufordern. Geben Sie die SO-Nummer des Avamar-Produkts in der E-Mail an. Die SO-Nummer des Avamar-Produkts ist erforderlich.

Vorgehensweise

1. Melden Sie sich mit den Anmeldedaten in der Lizenzauthorisierungs-E-Mail, die Sie erhalten haben, beim Avamar-Support (https://support.emc.com) an.
2. Klicken Sie in der Drop-down-Liste **Service Center** auf **Manage Licenses**.
3. Klicken Sie in der Produktliste auf **Avamar**.
4. Klicken Sie auf **Activate my software**.

   Der **Activation wizard** wird geöffnet.
5. Suchen Sie nach verfügbaren Produkten für die Lizenzierung, indem Sie den LAC (License Authorization Code) eingeben und auf **Search** klicken.
6. Befolgen Sie die Anweisungen im Assistenten, um die Lizenzierungsinformationen einzugeben.
7. Nachdem der Lizenzschlüssel erzeugt wurde, laden Sie ihn zur Lizenzierung der Software herunter.

Erzeugen eines Serverlizenzschlüssels mithilfe der Legacy-Lizenzierung

Die folgenden Verfahren beschreiben, wie ein Avamar-Lizenzschlüssel mithilfe des Legacy-Lizenzierungsmechanismus erzeugt wird.

Beziehen zugewiesener Lizenzschlüssel

Der zugewiesene Lizenzschlüssel für die Avamar-Serversoftware beinhaltet die Identifikationsnummern für das Kundenkonto sowie die Avamar-Systemressource. Diese Werte sind erforderlich, um eine permanente Lizenz zu erzeugen.

Bei folgendem Beispiel handelt es sich um einen zugewiesenen Lizenzschlüssel:

```
Avamar Software License Key Information
Avamar System Customer Account ID: CN-10062734404
Avamar System Asset ID: A-2010014578
```

Vorgehensweise

1. Suchen Sie die zugewiesenen Lizenzschlüssel beim Avamar-Support auf der Lizenzmanagementseite.

   Um auf den Avamar-Support zuzugreifen, geben Sie die Anmeldedaten aus der Lizenzauthorisierungs-E-Mail, die Sie von `licensingnorthamerica@emc.com`, `licensingemea@emc.com` oder `licensingapj@emc.com` erhalten haben. Wenn Sie die E-Mail nicht finden

können, wenden Sie sich per E-Mail an licensing@emc.com, um die Lizenzauthorisierungs-E-Mail erneut anzufordern. Geben Sie die SO-Nummer des Avamar-Produkts in der E-Mail an. Die SO-Nummer des Avamar-Produkts ist erforderlich.

2. Um auf die Lizenzmanagementseite auf der Avamar-Support-Website zuzugreifen, klicken Sie auf den Link **Manage License** unter dem Abschnitt **Service Center** auf der Startseite.

Generieren einer Lizenzschlüssel-Informationsdatei

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
2. Geben Sie `gathergsankeydata` ein.

   Über die Ausgabe werden Sie zur Angabe der Nummer des Kundenkontos aufgefordert.
3. Geben Sie die Nummer Ihres Avamar-Systemkundenkontos an und drücken Sie die **Enter**.

   Eine gültige Nummer für das Avamar-Systemkundenkonto (Konto-ID) entspricht dem Format CN-*jjmmttnnnnn*. Dabei steht *jjmmtt* für die Angabe von Jahr, Monat und Tag und *nnnnn* ist eine fünfstellige numerische Abfolge.

   Über die Ausgabe werden Sie zur Angabe der Ressourcen-ID-Nummer für das Avamar-System aufgefordert.
4. Geben Sie die Ressourcen-ID-Nummer des Avamar-Systems ein und drücken Sie die **Enter**.

   Eine gültige Ressourcen-ID-Nummer für das Avamar-System (Ressourcenreferenz-ID) entspricht dem Format A-*jjjjnnnnnn*. Dabei steht *jjjj* für eine Jahresangabe und *nnnnnn* ist eine sechsstellige numerische Abfolge.

   Über die Ausgabe werden Sie zur Angabe der Internetdomain für das Konto aufgefordert.
5. Geben Sie die Internetdomain ein und drücken Sie die **Enter**.

   Über die Ausgabe werden Sie zur Bestätigung der von Ihnen angegebenen Daten aufgefordert.
6. Geben Sie `y` ein und drücken Sie die **Enter**.

   Das lokale Verzeichnis enthält jetzt die Lizenzschlüssel-Informationsdatei `gsankeydata.xml`. Diese Datei wird zur Generierung des ständigen Lizenzschlüssels verwendet.

Generieren einer ständigen Lizenzschlüsseldatei

Vorgehensweise

1. Geben Sie für den Zugriff auf den Avamar-Support (https://support.EMC.com) die Anmeldedaten ein, die Sie in der Lizenzauthorisierungs-E-Mail von `licensingnorthamerica@emc.com`, `licensingemea@emc.com` oder `licensingapj@emc.com` erhalten haben.

   Die Seite **Welcome to the Avamar Support Site** wird angezeigt.

   Hinweis

   Wenn Sie die E-Mail von LAC nicht finden können, senden Sie eine E-Mail an licensing@emc.com, um die LAC-E-Mail erneut anzufordern. Geben Sie die SO-Nummer des Avamar-Produkts in der E-Mail an. Die SO-Nummer des Avamar-Produkts ist erforderlich.

2. Um auf die Lizenzmanagementseite beim Avamar-Support zuzugreifen, klicken Sie auf den Link **Get Manage License** unter dem Abschnitt **Service Center**.

   Die Seite **Lizenzen managen** wird angezeigt.

3. Klicken Sie in der Produktliste auf **Avamar**.
4. Klicken Sie auf **Activate Licenses** und laden Sie die Datei `gsankeydata.xml` hoch.
5. Geben Sie in das Feld **Qty** die autorisierte Anzahl der Terabytelizenzen an, die Sie dem System zuweisen möchten.
6. Klicken Sie auf **Next**.

   Mit diesem Verfahren wird die XML-Datei erstellt, die einen aktivierten Lizenzschlüssel enthält.

7. Speichern Sie die XML-Datei auf Ihrem lokalen Laufwerk.

   Sie können die XML-Datei auch an eine oder mehrere E-Mail-Adressen senden.

Installieren und Aktivieren einer Lizenz

Nachdem Sie die Lizenzschlüsseldatei von Avamar erhalten haben, installieren und aktivieren Sie die Lizenz auf dem Avamar-Server.

Vorgehensweise

1. Erwerben Sie den Avamar-Lizenzschlüssel.
   - Befolgen Sie für den Common License-Mechanismus das Verfahren unter Aktivieren der Avamar-Software bei Verwendung der Common Licensing Platform auf Seite 255, um den Lizenzschlüssel zu beziehen.
   - Führen Sie für den Legacy-Lizenzierungsmechanismus folgende Schritte aus:
     a. Melden Sie sich bei dem E-Mail-Konto an, an das die Lizenzschlüsseldatei gesendet wurde.
     b. Öffnen Sie die E-Mail von `info@Avamar.com` mit der Betreffzeile `Avamar Key Information`.
     Die E-Mail enthält die Lizenzschlüsseldatei als angefügte XML-Datei namens *`asset`*`_Key.xml`. Dabei steht *asset* für den DNS-Namen des Avamar-Servers.
     c. Speichern Sie den Anhang in einem temporären Verzeichnis.

2. Kopieren Sie mit `WinSCP` oder einem vergleichbaren Programm die Lizenzschlüsseldatei in das Verzeichnis `/tmp` auf einem Single-Node-Server bzw. in das Verzeichnis `/tmp` auf dem Utility-Node eines Multi-Node-Servers.
3. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
4. Vergewissern Sie sich, dass das Avamar-Serversubsystem (auch als Avamar-Server bezeichnet) in Betrieb ist, indem Sie **`dpnctl status gsan`** eingeben.

   Wird GSAN ausgeführt, wird in der Ausgabe der Status `ready` angezeigt.
5. Verwenden Sie die richtige Befehlsfolge, um die Dateiberechtigungen für die Avamar-Lizenzschlüsseldatei zu ändern und die Lizenz zu aktivieren.

Serverstatus	Befehlsfolge
Running	a. **`chmod 644 /tmp/`*`license_key_file`*** b. **`avmaint license /tmp/`*`license_key_file`*` --avamaronly`** Dabei steht *license_key_file* für die Lizenzschlüsseldatei.
Not running	• Bei Verwendung des Common License-Mechanismus: a. **`cd /usr/local/avamar/etc mv license.lic license.lic.old`** b. **`cp /tmp/`*`license_key_file`*` license.lic chmod 644 license.lic`** c. **`chmod 644 license.lic`** Dabei steht *license_key_file* für die Lizenzschlüsseldatei. • Bei Verwendung des Legacy-Lizenzierungsmechanismus: a. **`cd /usr/local/avamar/etc mv license.xml license.xml.old`** b. **`cp /tmp/`*`asset`*`Key.xml license.xml`** c. **`chmod 644 license.xml`** Dabei steht *asset*`_Key.xml` für die Lizenzschlüsseldatei.

6. Wenn der Avamar-Server nicht ausgeführt wird, starten Sie ihn durch Eingabe von **`dpnctl start`**.
7. Überprüfen Sie nach dem Neustarten des Avamar-Servers, ob die Serverlizenz korrekt installiert ist, indem Sie den folgenden Befehl eingeben:

   ```
   avmaint license --avamaronly
   ```

In der Befehlsshell werden die Lizenzinformationen angezeigt.

Managen von Diensten

Über die Registerkarte **Services Administration** im Fenster **Administration** von Avamar Administrator können Sie einzelne Dienste auf dem Avamar-Server starten, beenden, unterbrechen oder wieder aufnehmen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Services Administration**.
3. Managen Sie die Dienste:
   - Klicken Sie zum Starten eines Diensts mit der rechten Maustaste auf den Dienst und wählen Sie **Start** aus.
   - Klicken Sie zum Stoppen eines Diensts mit der rechten Maustaste auf den Dienst und wählen Sie **Stop** aus.
   - Klicken Sie zum vorübergehenden Anhalten eines Diensts bis zu seiner expliziten Fortsetzung mit der rechten Maustaste auf den Dienst und wählen Sie **Suspend** aus.
   - Klicken Sie zum Fortsetzen eines zuvor angehaltenen Diensts mit der rechten Maustaste auf den Dienst und wählen Sie **Resume** aus.

Informationen auf der Registerkarte „Serviceadministration“

Die folgenden Informationen werden auf der Registerkarte **Services Administration** angezeigt.

Tabelle 43 Informationen auf der Registerkarte „Serviceadministration“

Name	Beschreibung
Hostname	DNS-Name des Avamar-Servers.
IP Address	IP-Adresse des Avamar-Servers.
Load Average	Durchschnittliche Anzahl von CPU-Threads in der letzten Minute.
Last Administrator Datastore Flush	Datum und Uhrzeit der letzten MCS-Leerung.
PostgreSQL-Datenbank	Status der MCS-Datenbank.
Web Services	Status der MCS-Webdienste.
Web Restore Disk Space Available	Anzahl der Festplattenbyte, die die MCS-Webdienste verwenden können, um die Wiederherstellungs-ZIP-Datei zu erstellen.
Login Manager	Status des Avamar Login Manager-Diensts.
snmp sub-agent	Status des Avamar-SNMP-Sub-Agent-Diensts.
ConnectEMC	Status des Diensts ConnectEMC.

Tabelle 43 Informationen auf der Registerkarte „Serviceadministration“ (Fortsetzung)

Name	Beschreibung
VMware vCenter Connection Monitor	Status der VMware vCenter-Verbindungen. Dieser Service ist nur aufgeführt, wenn dem System mindestens ein vCenter-Client hinzugefügt wurde.
snmp daemon	Status des Avamar-SNMP-Master-Agent-Diensts.
ssh daemon	Status des Avamar Secure Shell (SSH)-Diensts.
syslog daemon	Status des Avamar-syslog-Diensts.
Data Domain SNMP Manager	Status des SNMP-Diensts für die Überwachung konfigurierter Data Domain-Systeme.
Remote Backup Manager Service	Status des externen Backupmanagerservices, der von der Funktion „Replikate auf Quelle“ (Replicas at Source) verwendet wird.
RabbitMQ	Status des RabbitMQ Message Broker-Services.
Replication cron job	Status des Replikations-Cron-Jobs auf dem Avamar-Server.

Hinweis

Die Liste der Services auf der Registerkarte **Services Administration** variiert je nach Konfiguration des Avamar-Systems.

Ändern von Serverpasswörtern und OpenSSH-Schlüsseln

Verwenden Sie das Dienstprogramm `change-passwords`, um die Passwörter für die Benutzerkonten des Betriebssystems und die Benutzerkonten des Avamar-Servers zu ändern. Verwenden Sie außerdem die Option `change-passwords`, um SSH-Schlüssel für diese Konten zu erstellen und zu ändern.

Das `change-passwords`-Utility unterstützt Sie bei den folgenden Vorgängen:

- Ändern der Passwörter für die Betriebssystemkonten admin und root
- Ändern der Passwörter für die internen Avamar-Serverkonten root, MCUser, repluser und viewuser
- Erstellen und Ändern von SSH-Schlüsseln

Vorgehensweise

1. Unterbrechen Sie alle geplanten Vorgänge:
   a. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.
   b. Klicken Sie im Fenster **Manage All Schedules** auf **Suspend All**.
2. Öffnen Sie eine Befehlsshell:

a. Melden Sie sich beim Server als Administrator an.

b. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie `su -` eingeben.

c. Laden Sie für einen Multi-Node-Server den OpenSSH-Schlüssel rootid, indem Sie Folgendes eingeben:

```
ssh-agent bashssh-add /root/.ssh/rootid
```

3. Starten Sie das Utility, indem Sie `change-passwords` eingeben.

   Auf einem Multi-Node-Server werden Sie über die Ausgabe aufgefordert, anzugeben, ob die Passwörter auf allen Nodes oder ausgewählten Nodes geändert werden sollen.

4. Geben Sie `y` ein, um die Passwörter auf allen Nodes zu ändern, oder geben Sie `n` ein, um die Passwörter auf ausgewählten Nodes zu ändern. Drücken Sie dann die **Enter**.

   Über die Ausgabe werden Sie aufgefordert, anzugeben, ob Sie private, für Root-Vorgänge autorisierte SSH-Schlüssel angeben möchten.

5. Geben Sie `n` ein und drücken Sie die **Enter**.

   Über die Ausgabe werden Sie aufgefordert, anzugeben, ob die Passwörter für die admin- oder root-Betriebssystembenutzerkonten geändert werden sollen.

6. Geben Sie `y` ein, um die Passwörter zu ändern, oder geben Sie `n` ein, um den Vorgang zur Änderung von Passwörtern zu überspringen, und drücken Sie dann die **Enter**.

7. Wenn Sie im vorherigen Schritt `y` eingegeben haben, befolgen Sie die Eingabeaufforderungen des Systems, um die Passwörter für ein oder mehrere admin- oder root-Betriebssystembenutzerkonten zu ändern.

   Über die Ausgabe werden Sie aufgefordert, anzugeben, ob SSH-Schlüssel geändert werden sollen.

8. Geben Sie `y` ein, um einen SSH-Schlüssel zu ändern oder zu erstellen, oder geben Sie `n` ein und drücken Sie **Enter**.

9. Wenn Sie im vorherigen Schritt `y` eingegeben haben, befolgen Sie die Eingabeaufforderungen des Systems, um die Schlüssel zu ändern oder zu erstellen.

   Über die Ausgabe werden Sie aufgefordert, anzugeben, ob Avamar-Serverpasswörter geändert werden sollen.

10. Wenn Sie dazu aufgefordert werden, geben Sie `y` ein, um das MCUser-Passwort und die Avamar-Passwörter (root, repluser und viewuser) zu ändern. Wenn Sie die Passwörter nicht ändern möchten, geben Sie `n` ein und drücken Sie anschließend **Enter**.

11. Wenn Sie im vorherigen Schritt `y` eingegeben haben, befolgen Sie die Eingabeaufforderungen des Systems, um die Passwörter zu ändern.

    In der Ausgabe werden Sie aufgefordert, die an den Passwörtern oder den SSH-Schlüsseln während der Dienstprogrammsitzung vorgenommenen Änderungen zu akzeptieren oder zu verwerfen.

12. Geben Sie `y` ein, um die Änderungen zu übernehmen, oder geben Sie `n` ein, um die Dienstprogrammsitzung ohne Änderungen zu beenden. Drücken Sie dann **Enter**.

    Über die Ausgabe wird der Status des Vorgangs angegeben.

13. Nehmen Sie nach abgeschlossenem Vorgang die geplanten Prozesse wieder auf:
    a. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Schedules** aus.
    b. Klicken Sie im Fenster **Manage All Schedules** auf **Resume All**.

MCS-Konfigurationseinstellungen

Avamar Administrator besteht sowohl aus Client- als auch aus Serversoftwareanwendungen. Es ist möglich, die einzelnen Anwendungen durch Bearbeiten der Voreinstellungsdatei für den Server oder Client unabhängig voneinander zu konfigurieren.

Änderungen an der Voreinstellungsdatei des Servers, `mcserver.xml`, wirken sich auf alle Avamar Administrator-Sitzungen aus. Änderungen an der Voreinstellungsdatei eines Clients, `mcclient.xml`, betreffen nur die Avamar Administrator-Sitzungen auf diesem Client. Beide Dateien entsprechen der XML-DTD-Datei (DTD, Document Type Definition) `preferences.dtd`, auf die die JSDK 1.4-API verweist.

Standard- und Livekopien
Im System gibt es zwei Kopien dieser Dateien:

- Eine erste Standardkopie wird zur Initiierung jeder Anwendung nach der Installation verwendet.
- Eine Livekopie enthält die aktuellen Einstellungen, die von der Anwendung verwendet werden.

Die Standardkopien befinden sich im Verzeichnis `/lib` der einzelnen Anwendungen. Die Livekopien befinden sich in einem Verzeichnis mit der Bezeichnung „live file“. In der folgenden Tabelle ist das Standardverzeichnis für Livedateien der jeweiligen Anwendung aufgeführt.

Tabelle 44 Standardverzeichnis für Livekopien von MCS-Konfigurationsdateien

Anwendung	Standardverzeichnis für Livedateien
Server	`/usr/local/avamar/var/mc/server_data/prefs`
Client	*`install_directory`*`/var/mc/gui_data/prefs`; dabei ist *`install_directory`* typischerweise `C:\Program Files\avs\administrator` auf Microsoft Windows-Computern und `/usr/local/avamar` auf Linux-Computern.

Initiierungsverhalten
Werden entweder die Server- oder die Clientanwendung initiiert, wird die entsprechende standardmäßige Voreinstellungsdatei im `\lib`-Verzeichnis in den Speicher geladen und in das Verzeichnis der Livedatei repliziert.

Hinweis

Die erneute Initialisierung eines laufenden MCS kann zu schwerwiegenden Schäden führen. Benutzerdefinierte Voreinstellungen, die in der Livedatei gespeichert sind, werden vollständig überschrieben und die Systemkonfiguration wird auf die Standardeinstellungen zurückgesetzt. Tritt dieser Schritt ein, müssen Sie die benutzerdefinierten Voreinstellungen aus einer vorhergehenden Leerung (Backup) wiederherstellen, wenn sie überschrieben wurden.

Upgradeverhalten

Alle `mcserver.xml`-Einträge, die mit dem Attribut `merge="delete"` in der neuen `mcserver.xml`-Standarddatei gekennzeichnet sind, werden während des Serverupgrades nicht in der neuen Livekopie zusammengeführt. Diese Einträge sind veraltet. Sie werden in der standardmäßigen `mcserver.xml`-Datei aufbewahrt, sodass der MCS die Voreinstellungen auf einem aktualisierten Kundensystem löschen kann.

Sie können ein Attribut `merge="keep"` jedem Eintrag in der Livedatei `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` manuell hinzufügen. Einstellungen mit `merge="keep"`-Attributen werden nach dem Upgrade in der neuen Livekopie aufbewahrt.

Sichern von MCS-Daten

Um sich selbst vor Hardwareausfällen zu schützen, sichert oder *leert* der MCS seine dauerhaften Daten automatisch stündlich und im Rahmen von Systemprüfpunkten auf den Avamar-Server. Die Leerung erfolgt über eine `avtar`-Clientsitzung. Sie können eine On-Demand-Leerung auch erzwingen.

Beim Leerungsprozess werden die Zeitstempeldateien in der folgenden Tabelle erzeugt.

Tabelle 45 Zeitstempeldateien des MCS-Backups

Datei	Beschreibung
`flush.timestamp`	Vor jeder Leerung wird `flush.timestamp` im Verzeichnis `server_data` erstellt. Diese Datei enthält die Uhrzeit und das Datum der Leerung. Bei einem Serverrollback wird diese Datei wiederhergestellt und kann dazu verwendet werden, zu überprüfen, ob das Rollback für die ausgewählte Uhrzeit und das Datum erfolgreich ausgeführt wurde. Auf den Inhalt von `flush.timestamp` kann ebenfalls über den Befehl `mcserver.sh --status` zugegriffen werden.
`init.timestamp`	Während der Systeminitiierung wird die Datei `init.timestamp` im Verzeichnis `server_data` erstellt oder überschrieben. Diese Datei enthält die Uhrzeit und das Datum der Systeminitiierung und kann dazu verwendet werden, zu überprüfen, ob die Initiierung für die ausgewählte Uhrzeit und das Datum erfolgreich ausgeführt wurde.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
2. Geben Sie den folgenden Befehl ein, um eine On-Demand-MCS-Leerung zu initiieren:

   ```
   mcserver.sh --flush
   ```

Wiederherstellen von MCS-Daten

Bevor Sie beginnen

Wenn MCS-Daten in einem bestimmten Backup wiederhergestellt werden sollen, ermitteln Sie die Bezeichnungsnummer für das Backup, indem Sie nach dem Backup in Avamar Administrator suchen oder den Befehl `avtar` verwenden:

- Öffnen Sie in Avamar Administrator das Fenster **Backup, Restore and Manage** und suchen Sie im Konto `/MC_BACKUPS` nach Backups.
- Geben Sie den folgenden Befehl in einer einzigen Befehlszeile ein:

  avtar --backups --id=root --ap=*password* --path=/MC_BACKUPS --hfsaddr=*Avamar_server* --count=*n*

  Dabei steht *password* für das Passwort des Avamar-Root-Benutzerkontos (nicht das Root-Passwort des Betriebssystems), *Avamar_server* für die IP-Adresse oder den DNS-Namen des Avamar-Servers und *n* für die Anzahl der aufzuführenden Backups. Insgesamt werden für einen Avamar-Server jeden Tag 26 MCS-Leerungen durchgeführt – einmal stündlich und je eine Leerung morgens und abends während der Systemprüfpunkte. Um alle MCS-Backups für eine bestimmte Anzahl vergangener Tage aufzuführen, geben Sie daher `--count=`*n* in 26er Schritten an.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
2. Stoppen Sie den MCS, indem Sie **`dpnctl stop mcs`** eingeben.
3. Stellen Sie den MCS durch Eingabe von einem der folgenden Befehle wieder her:

- Um das letzte Backup wiederherzustellen, geben Sie **mcserver.sh --restore** ein.
- Um ein bestimmtes Backup wiederherzustellen, geben Sie **mcserver.sh --restore --labelnum=*n*** ein. Dabei steht *n* für die Bezeichnungsnummer des Backups.

4. Öffnen Sie `/usr/local/avamar/var/mc/server_log/restore.log`, um den Erfolg der Wiederherstellung zu überprüfen.
5. Starten Sie den MCS und den Scheduler, indem Sie Folgendes eingeben:

```
dpnctl start mcs
dpnctl start sched
```

Wiederherstellen der standardmäßigen MCS-Konfigurationseinstellungen

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

        ```
        ssh-agent bashssh-add ~admin/.ssh/admin_key
        ```
2. Stoppen Sie den MCS, indem Sie **dpnctl stop mcs** eingeben.
3. Wechseln Sie das Arbeitsverzeichnis, indem Sie den folgenden Befehl eingeben:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```
4. Benennen Sie `mcserver.xml` in `old.mcserver.xml` um, indem Sie den folgenden Befehl eingeben:

   ```
   mv mcserver.xml old.mcserver.xml
   ```
5. Kopieren Sie die standardmäßige Servervoreinstellungsdatei in das aktuelle Verzeichnis, indem Sie den folgenden Befehl in eine einzige Befehlszeile eingeben:

   ```
   cp /usr/local/avamar/lib/mcserver.xml /usr/local/avamar/var/mc/
   server_data/prefs/mcserver.xml
   ```
6. Starten Sie den MCS und den Scheduler, indem Sie Folgendes eingeben:

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

Verwenden von Network Address Translation (NAT)

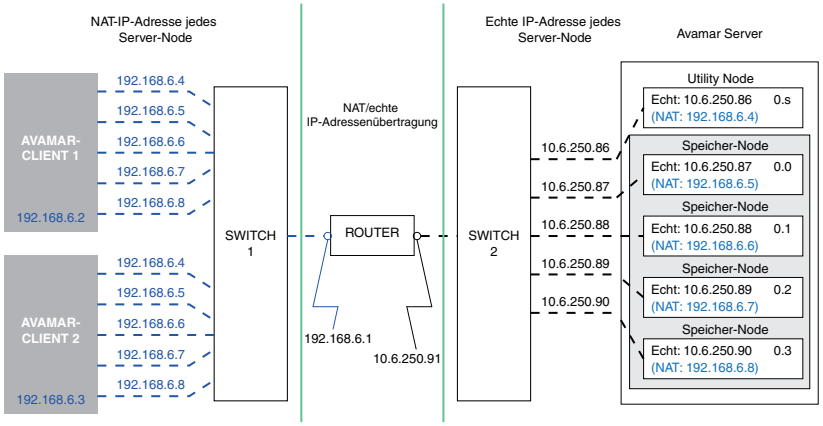
Avamar-Clients können mithilfe von einem unter NAT laufenden Adresssatz auf Avamar-Speicher-Nodes zugreifen.

Damit der Avamar-Server verfügbare NAT-Informationen erkennt, muss die `probe.xml`-Datei `nat-address`-Elemente für die Speicher-Nodes enthalten. Nach

dem ersten Kontakt zwischen einem Client und dem Utility-Node auf dem Avamar-Server stellt der Avamar-Server für die Speicher-Nodes der Clients verschiedene routbare Adressen zur Verfügung. Ist kein `nat-address`-Element vorhanden, verwendet ein Client eine vorkonfigurierte „reale“ (nicht übersetzte) Netzwerkschnittstellenadresse.

Die folgende Abbildung illustriert ein Beispiel einer 1x4-Multi-Node-Serverkonfiguration, bei der Avamar NAT verwendet.

Abbildung 15 Multi-Node-Serverkonfiguration mit NAT



In den folgenden Anweisungen wird vorausgesetzt, dass jeder Avamar-Node über eine eindeutige Adresse (aus Sicht des Avamar-Clients) verfügt, und dass Sie einen Router im Netzwerk konfigurieren, um transparentes One-to-One-NAT zu verwenden. Mithilfe dieser Anweisungen können Sie NAT jedoch auch für eine Single-Node-Serverkonfiguration aktivieren.

Vorgehensweise

1. Verwenden Sie entweder die Programme `dpnnetutil` oder `nodedb`, um `probe.xml` NAT-Adressen hinzuzufügen.

Befehl	Befehlseingabe – Beispiel
`dpnnetutil`	**`su - rootdpnnetutil`** Reaktion auf die interaktiven Eingabeaufforderungen von `dpnnetutil`.
`nodedb`	**`nodedb update if --addr=10.6.250.87 --new-nat=192.168.6.4=192.168.6.5`**

2. Wurde das Avamar-Speichersubsystem angehalten, starten Sie es neu, indem Sie **`dpnctl start gsan`** eingeben.
3. Wird das Avamar-Speichersubsystem ausgeführt, lesen Sie die Datei `probe.xml` neu ein, indem Sie den folgenden Befehl eingeben:

   `avmaint networkconfig /usr/local/avamar/var/probe.xml --avamaronly`

4. Registrieren Sie Clients, indem Sie den Befehl `avregister` (UNIX) bzw. `avregister.bat` (Windows) oder Avamar Administrator verwenden.

Lösungen für häufig vorkommende NAT-Probleme

Um zu ermitteln, ob NAT verwendet wird, müssen der Client und der Avamar-Server mit einem Netzwerk verbunden sein. In der folgenden Tabelle finden Sie Lösungen für allgemeine Probleme bei der Verbindung und Konfiguration von NAT.

Tabelle 46 Lösungen für häufig vorkommende NAT-Probleme

Problem	Lösung
Der Avamar-Server wird beendet und es wird die Meldung `FATAL ERROR` ausgegeben.	Vergewissern Sie sich, dass die Datei `probe.xml` folgende Bedingungen aufweist: • Die Datei liegt im Verzeichnis `/usr/local/avamar/var/` vor. • Die Datei ist eine gültige XML-Datei und stimmt mit dem Format für Node-Ressourcendatenbanken überein. • Die Datei listet NAT-IP-Adressen korrekt auf. Verwenden Sie den Befehl `nodedb print --say`, um den Inhalt der Datei `probe.xml` anzuzeigen. Die Option `--say` zeigt den Pfad und den Namen der aktuellen Node-Ressourcendatenbank an.
Die Server-Client-Verbindung schlägt fehl.	Verwenden Sie Netzwerkdiagnosetools, wie `ping`, `traceroute`, `tracert` oder `iperf`, um die Netzwerkverbindung zu überprüfen.

Bearbeiten von Netzwerkeinstellungen für einen Single-Node-Server

Die technischen Hinweise *Changing the Name and IP Addressing of Avamar Systems Technical Note*, die beim Avamar-Support unter https://support.EMC.com verfügbar sind, enthalten Anweisungen zum Bearbeiten der Netzwerkeinstellungen für einen Single-Node-Server.

Hinzufügen einer benutzerspezifischen Sicherheitsbenachrichtigung für Webbrowseranmeldungen

Auf der Anmeldeseite von Avamar Web Restore können Sie eine benutzerspezifische Sicherheitsbenachrichtigung einschließen. In dieser Benachrichtigung wird in der Regel angegeben, dass nur autorisierte Benutzer eine Zugriffsberechtigung haben. Außerdem enthält sie die Strafmaßnahmen für unbefugten Zugriff.

Vorgehensweise

1. Erstellen Sie in einem Texteditor eine Datei mit dem Namen `disclaimer_Web_Restore.txt`.
2. Fügen Sie den Inhalt der Benachrichtigung der Datei hinzu.

Im Inhalt der Benachrichtigung können Sie einige grundlegende HTML-Tags und CSS-Inline-Formatvorlagen verwenden.

3. Kopieren Sie die Datei in den folgenden Speicherort auf einem Single-Node-Server oder auf den Utility-Node eines Multi-Node-Servers:

   `/usr/local/avamar/var/em/server_data/`

Anzeigen und Bearbeiten von serverbezogenen Kontaktinformationen

Der Avamar-Server sendet mit jedem gemeldeten Ereignis Kontaktinformationen für den Avamar-Server an Avmar. Dies gilt auch für Kapazitätsberichte, die verhindern, dass das System kritische Schwellenwerte überschreitet. Halten Sie diese Informationen immer auf dem neuesten Stand.

Durch ein Serverrollback werden die Kontaktinformationen, die zum Zeitpunkt des Kontrollpunkts vorhanden sind, angewendet. Nach Abschluss des Rollbacks können Sie die Kontaktinformationen anzeigen oder bearbeiten, damit die Informationen auch dem aktuellen Stand entsprechen.

Vorgehensweise

1. Wählen Sie in Avamar-Administrator den Befehl **Help** > **View/Edit Contact Information** aus.

   Das Dialogfeld **View/Edit Contact Information** wird angezeigt. Die Felder in der folgenden Tabelle sind im Dialogfeld schreibgeschützt.

   Tabelle 47 Schreibgeschützte Felder im Dialogfeld **Kontaktinformationen anzeigen/bearbeiten**

Feld	Beschreibung
Avamar-Standort-ID	Eindeutige, während der Erstinstallation des Servers angegebene ID für den Kundenstandort. Dieses Feld ist schreibgeschützt.
System-ID	Eindeutige, während der Erstinstallation des Servers erstellte Avamar-Server-ID. Dieses Feld ist schreibgeschützt.
AVE	Ja (**Y** für Yes), wenn es sich bei diesem Server um einen Avamar Virtual Edition(AVE)-Server handelt; andernfalls Nein (**N** für No). Dieses Feld ist schreibgeschützt.

2. Bearbeiten Sie die Kontaktinformationen.

   Tabelle 48 Bearbeitbare Felder im Dialogfeld **Kontaktinformationen anzeigen/bearbeiten**

Feld	Beschreibung
Data Domain S/N	Seriennummer der Data Domain-Systeme, die diesem Server hinzugefügt wurden. Wenn

Tabelle 48 Bearbeitbare Felder im Dialogfeld **Kontaktinformationen anzeigen/bearbeiten** (Fortsetzung)

Feld	Beschreibung
	keine Data Domain-Systeme hinzugefügt wurden, geben Sie (**N/V**) ein.
Server location	Physischer Standort des Avamar-Servers am Kundenstandort.
Company Information	Name und Adresse des Unternehmens, dem dieser Avamar-Server gehört.
Contact Information	Name, Telefonnummer und E-Mail-Adresse des primären Ansprechpartners für diesen Avamar-Server.

3. Klicken Sie auf **OK**.

KAPITEL 9

Serverüberwachung

In diesem Kapitel werden folgende Themen behandelt:

Empfohlene tägliche Serverüberwachung

Um dafür zu sorgen, dass der Avamar-Server korrekt funktioniert, empfehlen wir die tägliche Durchführung der in der folgenden Tabelle aufgeführten Aufgaben zur Systemüberwachung.

Tabelle 49 Tools und Aufgaben zur Systemüberwachung

Überwachungstool	Überwachungsaufgabe
Activity Monitor	Überprüfen Sie alle ungewöhnlichen Clientaktivitäten, wie mit Ausnahmen abgeschlossene Backups.
Server Monitor	Bestätigen Sie, dass der letzte Kontrollpunkt und der validierte Kontrollpunkt kürzlich erfolgt sind. Idealerweise sollten diese innerhalb der letzten 24 Stunden erfolgt sein.
Event Monitor	Überprüfen Sie alle Systemfehler oder Warnungen.
Liste „Unacknowledged Events“	Ermitteln Sie nicht quittierte Ereignisse und löschen (quittieren) Sie diese.

HINWEIS

Aktivieren Sie die Funktionen „Email Home“ und „ConnectEMC“, mit denen der Status der Datenintegritätsprüfung sowie andere wichtige Servermeldungen automatisch per E-Mail an den Avamar-Support gesendet werden.

Überwachen von Aktivitäten

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Details zur Aktivitätsüberwachung auf Seite 272 enthält Details zu den auf der Registerkarte „Activity Monitor“ verfügbaren Informationen.
3. (Optional) Filtern Sie die Informationen auf der Registerkarte „Activity Monitor“, um nur Aktivitäten mit einem bestimmten Status, Typ, Client oder Plug-in bzw. einer bestimmten Gruppe anzuzeigen:
   a. Wählen Sie **Actions** > **Filter** aus.

      Das Dialogfeld **Filter Activity** wird angezeigt.
   b. Legen Sie die Filterkriterien fest und klicken Sie auf **OK**.

Details zur Aktivitätsüberwachung

Standardmäßig werden auf der Registerkarte „Activity Monitor“ die letzten 5.000 Clientaktivitäten während der zurückliegenden 72 Stunden angezeigt. Sie können die Menge der in der Funktion „Activity Monitor“ angezeigten Informationen

erhöhen oder reduzieren, indem Sie die Voreinstellung `com.avamar.mc.wo completed_job_retention_hours` in der Datei `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` bearbeiten und den MCS neu starten.

In der folgenden Tabelle sind Details zu den auf der Registerkarte „Activity Monitor“ verfügbaren Informationen angegeben.

Tabelle 50 Im Activity Monitor verfügbare Sitzungsdetails

Spalte	Beschreibung
Status	Status der Backup-, Wiederherstellungs- oder Validierungsaktivität. Die Avamar Administrator-Onlinehilfe liefert weitere Einzelheiten zu jedem Status.
Error Code	Wenn die Aktivität nicht erfolgreich abgeschlossen wurde, wird ein numerischer Fehlercode angezeigt. Doppelklicken Sie auf den Fehlercode, um eine ausführliche Erklärung anzuzeigen.
Start Time	Datum und Uhrzeit, zu dem bzw. zu der die Aktivität begonnen wurde, angepasst an die aktuelle, in Klammern angezeigte Zeitzone. Sommerzeitbezogene Umstellungen werden automatisch berücksichtigt.
Elapsed Time	Die für diese Aktivität verstrichene Zeit.
End Time	Datum und Uhrzeit, zu dem bzw. zu der die Aktivität abgeschlossen wurde, angepasst an die aktuelle, in Klammern angezeigte Zeitzone. Sommerzeitbezogene Umstellungen werden automatisch berücksichtigt.
Type	Typ der Aktivität. Die Avamar Administrator-Onlinehilfe liefert weitere Einzelheiten zu jedem Typ.
Server	Server, auf dem die Aktivität auftrat: entweder der Avamar-Server oder ein Data Domain-System.
Progress Bytes	Gesamtmenge der während dieser Aktivität untersuchten Byte.
New Bytes	Prozentsatz der neuen auf dem Avamar-Server oder einem Data Domain-System gesicherten Byte. Eine niedrige Zahl steht für ein hohes Maß an Datendeduplizierung.

Tabelle 51 Im Activity Monitor verfügbare Clientdetails

Spalte	Beschreibung
Client	Name des Avamar-Clients.

Tabelle 51 Im Activity Monitor verfügbare Clientdetails (Fortsetzung)

Spalte	Beschreibung
Domain	Vollständige Speicherortangabe des Clients auf dem Avamar-Server.
OS	Clientbetriebssystem.
Client Release	Version der Avamar-Clientsoftware. Falls es sich bei dieser Aktivität um ein VMware-Image-Backup oder eine VMware-Wiederherstellung handelt, ist dieser Wert die Version der auf dem Image-Proxyclient ausgeführten Avamar-Clientsoftware.
Proxy	Falls es sich bei dieser Aktivität um ein VMware-Image-Backup oder eine VMware-Wiederherstellung handelt, ist dieser Wert der Name des Proxyclients, der das Backup oder die Wiederherstellung im Auftrag der virtuellen Maschine durchführt. Bei allen anderen Aktivitäten ist hier nichts angegeben.

Tabelle 52 Im Activity Monitor verfügbare Policy-Details

Spalte	Beschreibung
Sched. Start Time	Datum und Uhrzeit des geplanten Starts dieser Aktivität.
Sched. End Time	Datum und Uhrzeit des geplanten Endes dieser Aktivität.
Elapsed Wait	Gesamtzeit, für die diese Aktivität sich in der Aktivitätswarteschlange befand. D. h. die geplante Startzeit abzüglich der tatsächlichen Startzeit.
Group	Gruppe, die diese Aktivität gestartet hat. Einer der folgenden Werte: • Wenn es sich bei der Aktivität um ein geplantes Backup gehandelt hat, die Gruppe, in der dieser Client ein Mitglied war, als diese geplante Aktivität gestartet wurde. • **On-Demand** wird für andere Backup-, Wiederherstellungs- und Validierungsaktivitäten angezeigt. • Wenn es sich bei der Aktivität um eine geplante Replikation handelt, ist dieser Wert die Replikationsgruppe. • **Admin On-Demand Group** wird für durchgeführte On-Demand-Replikationsaktivitäten angezeigt.

Tabelle 52 Im Activity Monitor verfügbare Policy-Details (Fortsetzung)

Spalte	Beschreibung
Plug-in	Für diese Aktivität verwendetes Plug-in.
Retention	Diesem Backup zugewiesene Aufbewahrungstypen. Einer oder mehrere der folgenden Werte: • **D** – Täglich (Daily) • **W** – Wöchentlich (Weekly) • **M** – Monatlich (Monthly) • **Y** – Jährlich (Yearly) • **N** – Kein bestimmter Aufbewahrungstyp (No specific retention type)
Schedule	Falls es sich bei der Aktivität um ein geplantes Backup handelte, ist dies die Planung, die diese Aktivität begonnen hat. Für alle anderen Aktivitäten, die von Avamar Administrator bzw. vom Client gestartet wurden, wird „On-Demand“ oder „End User Request“ angezeigt.
Dataset	Name des Datasets, das zum Erstellen des Backups verwendet wird. Falls es sich bei dieser Aktivität um einen Replikationsjob handelt, werden in dieser Spalte der Name des Quellsystems im Zielsystem sowie der Zielname im Quellsystem aufgeführt.
WID	Arbeitsauftrags-ID. Eindeutige Kennung für diese Aktivität.

Überwachen von Serverstatus und Serverstatistiken

Über das Fenster **Server** in Avamar Administrator können Sie Status und Statistiken für den Avamar-Server als Ganzes, für einzelne Nodes auf dem Avamar-Server und für konfigurierte Data Domain-Systeme überwachen.

Die folgenden Registerkarten werden im Fenster **Server** angezeigt:

- Auf der Registerkarte **Server Monitor** werden Zusammenfassungen der Statistiken zur CPU-, Netzwerk- und Laufwerkleistung für den Avamar-Server angezeigt. Eine separate Unterregisterkarte enthält dieselben Informationen für konfigurierte Data Domain-Systeme.
- Die Registerkarte **Server Management** enthält eine detaillierte Ansicht der Hardwareressourcen des Servers, einschließlich des Avamar-Servers und der konfigurierten Data Domain-Systeme.
- Auf der Registerkarte **Session Monitor** ist eine Liste der aktiven Clientbackup- und -wiederherstellungssitzungen aufgeführt.
- Die Registerkarte **Checkpoint Management** zeigt detaillierte Informationen zu allen Systemprüfpunkten an, die für diesen Avamar-Server durchgeführt werden.

- Die Registerkarte **Data Domain NFS Datastores** enthält die temporäre NFS-Share für den sofortigen VMware-Zugriff auf konfigurierte Data Domain-Systeme. Weitere Informationen über den sofortigen Zugriff finden Sie im *Avamar for VMware – Benutzerhandbuch*.

Registerkarte „Server Monitor“

Die Registerkarte **Server Monitor** im Fenster **Server** in Avamar Administrator umfasst verschiedene Registerkarten für den Avamar-Server und konfigurierte Data Domain-Systeme.

Registerkarte Avamar

Auf der Registerkarte **Avamar** der Funktion „Server Monitor“ werden Zusammenfassungen der Statistiken zur CPU-, Netzwerk- und Laufwerkleistung für den Avamar-Server angezeigt.

In den folgenden Tabellen sind die auf der Registerkarte **Avamar** verfügbaren Informationen beschrieben.

Tabelle 53 Node-Details auf der Registerkarte Avamar der Funktion „Server Monitor“

Eigenschaft	Beschreibung
Statusanzeigen	Status des Node. Einer der folgenden Werte: • Online (grün) – Der Node funktioniert ordnungsgemäß. • Read-Only (blau) – Dieser Status tritt in der Regel ein, wenn Vorgänge im Hintergrund durchgeführt werden und Backups unterbrochen wurden. • Time-Out (grau) – MCS konnte nicht mit diesem Node kommunizieren. • Unknown (gelb) – Node-Status kann nicht bestimmt werden. • Offline (rot) – Auf dem Node ist ein Problem aufgetreten. Falls ConnectEMC aktiviert wurde, wird ein Service-Request (SR) protokolliert. Besuchen Sie den Avamar-Support, um bestehende SRs anzuzeigen. Durchsuchen Sie die Wissensdatenbank nach „Avamar Data Node offline solution esg112792“.
ID	Jeder Node auf dem Avamar-Server hat eine eindeutige logische Kennung. Diese Node-ID wird im Format *modul.node* ausgedrückt. **Hinweis** Die Nummerierung von Modul und Node beginnt mit Null. Daher lautet die ID für den dritten Node im ersten Modul 0.2.

Tabelle 54 CPU-Details auf der Registerkarte Avamar der Funktion „Server Monitor“

Eigenschaft	Beschreibung
Load	Durchschnittliche Anzahl von CPU-Threads in der letzten Minute.
User	Prozentsatz der durch die Ausführung von Serveranweisungen verbrauchten CPU-Kapazität (ausgenommen Betriebssystem-Overhead).
Sys	Prozentsatz der vom Betriebssystem-Overhead verbrauchten CPU-Kapazität.

Tabelle 55 Netzwerkdetails auf der Registerkarte Avamar der Funktion „Server Monitor“

Eigenschaft	Beschreibung
Ping	Zeit in Sekunden, die dieser Node für die Reaktion auf eine Ping-Anforderung benötigt hat.
In	Empfangener Paketdurchsatz in KB pro Sekunde.
Out	Gesendeter Paketdurchsatz in KB pro Sekunde.

Tabelle 56 Datenträgerdetails auf der Registerkarte Avamar der Funktion „Server Monitor“

Eigenschaft	Beschreibung
Reads	Durchschnittliche Anzahl der vom Betriebssystem gemeldeten Festplattenlesevorgänge pro Sekunde.
Writes	Durchschnittliche Anzahl der vom Betriebssystem gemeldeten Festplattenschreibvorgänge pro Sekunde.
Utilization	Prozentsatz der gesamten verfügbaren Serverspeicherkapazität, der derzeit genutzt wird.

Registerkarte „Data Domain“

Auf der Registerkarte **Data Domain** der Funktion „Server Monitor“ werden die CPU-, Festplatten- und Netzwerkaktivität für jeden Node im Data Domain-System angezeigt.

In den folgenden Tabellen sind die auf der Registerkarte „Data Domain“ verfügbaren Informationen beschrieben.

Tabelle 57 Node-Details auf der Registerkarte „Data Domain“ von Server Monitor

Eigenschaft	Beschreibung
Statusanzeigen	Status des Node. Einer der folgenden Werte:

Tabelle 57 Node-Details auf der Registerkarte „Data Domain“ von Server Monitor (Fortsetzung)

Eigenschaft	Beschreibung
	• OK (grün) – Das Data Domain-System funktioniert korrekt. • Warning (gelb) – Es liegt ein Problem mit dem Data Domain-System vor, aber Backups und Wiederherstellungen können fortgesetzt werden. • Fehler (rot) – Es liegt ein Problem mit dem Data Domain-System vor und Backups und Wiederherstellungen wurden angehalten, bis das Problem behoben ist. Falls der Status gelb oder rot ist, können Sie zusätzliche Statusinformationen zur Bestimmung und Lösung des Problems anzeigen. Im *Avamar und Data Domain-System – Integrationshandbuch* finden Sie nähere Informationen.
Name	Der Hostname des Data Domain-Systems, wie im Unternehmens-DNS definiert.

Tabelle 58 CPU-Details auf der Registerkarte „Data Domain“ von Server Monitor

Eigenschaft	Beschreibung
Busy Avg.	Durchschnittliche CPU-Nutzung in Prozent der möglichen CPU-Gesamtnutzung.
Max	Maximal aufgetretene CPU-Nutzung in Prozent der möglichen CPU-Gesamtnutzung.

Tabelle 59 Datenträgerdetails (KB/s) auf der Registerkarte „Data Domain“ von Server Monitor

Eigenschaft	Beschreibung
Read	Festplattenlesedurchsatz in Kilobyte pro Sekunde.
Write	Festplattenschreibdurchsatz in Kilobyte pro Sekunde.
Busy	Festplatten-I/O-Nutzung in Prozent der möglichen Festplatten-I/O-Gesamtnutzung.

Tabelle 60 Netzwerkdetails (KB/s) auf der Registerkarte „Data Domain“ von Server Monitor

Eigenschaft [a]	Beschreibung
Eth#1	Desc – Beschreibung der Netzwerkschnittstelle.

Tabelle 60 Netzwerkdetails (KB/s) auf der Registerkarte „Data Domain“ von Server Monitor (Fortsetzung)

Eigenschaft [a]	Beschreibung
	In/Out – Netzwerkbandbreitennutzung in Kilobyte pro Sekunde auf Netzwerkschnittstelle 1.
Eth#2	Desc – Beschreibung der Netzwerkschnittstelle. In/Out – Netzwerkbandbreitennutzung in Kilobyte pro Sekunde auf Netzwerkschnittstelle 2.
Eth#3	Desc – Beschreibung der Netzwerkschnittstelle. In/Out – Netzwerkbandbreitennutzung in Kilobyte pro Sekunde auf Netzwerkschnittstelle 3.
Eth#4	Desc – Beschreibung der Netzwerkschnittstelle. In/Out – Netzwerkbandbreitennutzung in Kilobyte pro Sekunde auf Netzwerkschnittstelle 4.

a. Die Anzahl der Spalten „Eth#“ von der Maximalanzahl der Netzwerkschnittstellen ab, die die konfigurierten Data Domain-Systeme unterstützen.

Registerkarte „Server Management“

Die Registerkarte **Server Management** im Fenster **Server** in Avamar Administrator enthält eine detaillierte Ansicht der Hardwareressourcen des Servers, einschließlich des Avamar-Servers und der konfigurierten Data Domain-Systeme.

Avamar-Serverinformationen sind in der Baumstruktur unter dem **Avamar**-Ordner aufgeführt und konfigurierte Data Domain-Systeme in der Baumstruktur unter dem **Data Domain**-Ordner.

Die Informationen im rechten Bereich des Fensters ändern sich, wenn Sie verschiedene Elemente in der Baumstruktur auswählen.

Tabelle 61 Datenanzeige basierend auf der Auswahl in der Registerkarte „Server Management“

Ausgewähltes Element	Informationen im rechten Bereich der Registerkarte „Server Management“
Server-Node	Zusammenfassung der geschützten Byte
Avamar- oder Data Domain-Nodes	Leer
Avamar-Servername	Detaillierte Informationen für den Avamar-Server
Module	Detaillierte Informationen für dieses Modul
Node	Detaillierte Informationen für diesen Node

Tabelle 61 Datenanzeige basierend auf der Auswahl in der Registerkarte „Server Management“ (Fortsetzung)

Ausgewähltes Element	Informationen im rechten Bereich der Registerkarte „Server Management“
Partition	Detaillierte Informationen für diese logische Festplattenpartition
Data Domain system	Detaillierte Informationen für dieses Data Domain-System

HINWEIS

Avamar wird in Dezimaleinheiten lizenziert. Daher werden **Total capacity** und **Capacity used** in Dezimaleinheiten auf der Registerkarte **Server Management** angezeigt. Alle anderen Teile des Produkts, die die Kapazität ausgeben, werden in Binäreinheiten dargestellt.

Bytes Protected Summary

Die folgende Tabelle enthält Details zu den **Bytes Protected Summary**-Eigenschaften auf der Registerkarte **Server Management**.

Tabelle 62 „Bytes Protected Summary“-Eigenschaften auf der Registerkarte „Server Management“

Eigenschaft	Beschreibung
Properties	Name des Avamar-Servers und aller konfigurierten Data Domain-Systeme
Werte	Anzahl an Byte geschützter Daten auf dem Server oder dem Data Domain-System

Serverinformationen

In den folgenden Tabellen werden die **Serverinformationen** beschrieben, die zur Verfügung gestellt werden, wenn ein Avamar-Server auf der Registerkarte **Servermanagement** ausgewählt wird.

Tabelle 63 Serverdetails auf der Registerkarte „Servermanagement“

Eigenschaft	Beschreibung
Active sessions	Derzeitige Anzahl der aktiven Clientsitzungen. Klicken Sie auf die Registerkarte **Sitzungsmonitor**, um zusätzliche Informationen zu erhalten.
Total capacity	Gesamtmenge der Serverspeicherkapazität.
Server utilization	Prozentsatz der gesamten verfügbaren Serverspeicherkapazität, der derzeit genutzt wird. Dieser Wert wird vom größten Wert **Disk Utilization** abgeleitet, der auf der Registerkarte **Avamar** in der Funktion

Tabelle 63 Serverdetails auf der Registerkarte „Servermanagement“ (Fortsetzung)

Eigenschaft	Beschreibung
	„Server Monitor“ angezeigt wird. Daher stellt er die absolute Maximalspeicherauslastung des Avamar-Servers dar. Die tatsächliche Auslastung über alle Module, Nodes und Festplatten hinweg kann ggf. geringfügig geringer sein.
Bytes protected	Gesamtmenge der auf diesem Server gesicherten (geschützten) Clientdaten in Byte.
Bytes protected quota	Maximale Menge an Clientdaten in Byte, die für den Schutz auf diesem Server lizenziert ist.
License expiration	Kalenderdatum, an dem die Lizenz dieses Servers abläuft. Wenn die Lizenz unbefristet ist, ist der Wert `never`.
Time since Server initialization	Anzahl der verstrichenen Stunden, Tage und Minuten seit der Initialisierung dieses Avamar-Servers.
Last checkpoint	Datum und Uhrzeit der letzten Durchführung eines Serverkontrollpunkts. Kontrollpunkte werden in der Regel zweimal täglich durchgeführt.
Last validated checkpoint	Datum und Uhrzeit der letzten Validierung eines Serverkontrollpunkts. Die Kontrollpunktvalidierung erfolgt in der Regel einmal täglich. Daher kann unter **Last validated checkpoint** eine andere Zeit angegeben sein, als unter **Last checkpoint**, je nachdem, zu welcher Uhrzeit Sie diese Informationen aufrufen. **Hinweis** Wenn die Werte unter **Letzter überprüfter Kontrollpunkt** und **Letzte Kontrollpunktzeiten** mehr als 36 Stunden voneinander abweichen, findet keine Kontrollpunktüberprüfung statt. Dies stellt ein Problem dar.
System Name	Vom Benutzer zugewiesener Name dieses Avamar-Servers.
System ID	Eindeutige Kennung für diesen Avamar-Server.
HFSAddr	Hash-Dateisystem(HFS)-Adresse (Addr). Der Hostname oder die IP-Adresse, die

Tabelle 63 Serverdetails auf der Registerkarte „Servermanagement“ (Fortsetzung)

Eigenschaft	Beschreibung
	Backupclients für die Verbindung mit diesem Avamar-Server verwenden.
HFSPort	HFS-Datenport. Der Datenport, den Backupclients für die Verbindung mit diesem Avamar-Server verwenden. Die Standardeinstellung ist Port 27000.
IP Address	IP-Adresse dieses Avamar-Servers. Falls es sich bei der HFSAddr um eine IP-Adresse handelt, entspricht dieser Wert der HFSAddr.

Tabelle 64 Details zu Wartungsaktivitäten auf der Registerkarte „Servermanagement“

Eigenschaft	Beschreibung
Suspended	Einer der folgenden Werte: • No – Die Serverwartungsaktivitäten sind derzeit nicht unterbrochen (d. h., die Serverwartungsaktivitäten werden während des nächsten Wartungszeitfensters normal ausgeführt). • Yes – Die Serverwartungsaktivitäten sind derzeit unterbrochen.

Tabelle 65 Details zur automatischen Speicherbereinigung auf der Registerkarte „Servermanagement“

Eigenschaft	Beschreibung
Status	Einer der folgenden Werte: • Idle – Es findet derzeit keine automatische Speicherbereinigung statt. • „Wird verarbeitet“ – Die Sammlung veralteter Daten wird durchgeführt.
Result	Einer der folgenden Werte: • OK – Die letzte Aktivität zur automatischen Speicherbereinigung wurde erfolgreich abgeschlossen. • Error Code – Die letzte Aktivität zur automatischen Speicherbereinigung wurde nicht erfolgreich abgeschlossen.
Start time	Datum und Uhrzeit des Starts der letzten Aktivität zur automatischen Speicherbereinigung.

Tabelle 65 Details zur automatischen Speicherbereinigung auf der Registerkarte „Servermanagement“ (Fortsetzung)

Eigenschaft	Beschreibung
End time	Datum und Uhrzeit des Endes der letzten Aktivität zur automatischen Speicherbereinigung.
Passes	Gesamtanzahl der Durchläufe während der letzten Aktivität zur automatischen Speicherbereinigung.
Bytes recovered	Gesamtmenge des Speicherplatzes in Byte, der während der letzten Aktivität zur automatischen Speicherbereinigung wiederhergestellt wurde.
Chunks deleted	Gesamtanzahl der Datenblöcke, die während der letzten Aktivität zur automatischen Speicherbereinigung gelöscht wurden.
Index stripes	Gesamtanzahl der Index-Stripes.
Index stripes processed	Gesamtanzahl der Index-Stripes, die während der letzten Aktivität zur automatischen Speicherbereinigung verarbeitet wurden.

Modulinformationen

Die folgende Tabelle enthält Details zu den **Module**-Eigenschaften auf der Registerkarte **Server Management**.

Tabelle 66 Moduleigenschaften auf der Registerkarte „Server Management“

Eigenschaft	Beschreibung
Total capacity	Gesamtmenge der Serverspeicherkapazität.
Server utilization	Prozentsatz der gesamten verfügbaren Serverspeicherkapazität, der derzeit genutzt wird. Dieser Wert wird vom größten Werte **Disk Utilization** abgeleitet, der auf der Registerkarte Avamar in der Funktion „Server Monitor“ angezeigt wird. Daher stellt er die absolute Maximalspeicherauslastung des Avamar-Servers dar. Die tatsächliche Auslastung über alle Module, Nodes und Festplatten hinweg kann ggf. geringfügig geringer sein.
Number of nodes	Gesamtanzahl der Nodes in diesem Modul.
IP address	Basis-IP-Adresse dieses Moduls.

Node-Informationen

Die folgenden Tabellen enthalten Details zu den **Node**-Eigenschaften auf der Registerkarte **Servermanagement**.

Tabelle 67 Statusindikatoren im Bereich mit Node-Informationen der Registerkarte „Servermanagement“

Eigenschaft	Beschreibung
Statusanzeigen	Einer der folgenden Werte: • Online (grün) – Node funktioniert korrekt. • Read-Only (blau) – Diese Option tritt in der Regel ein, wenn Vorgänge im Hintergrund durchgeführt werden und Backups unterbrochen wurden. • Time-Out (grau) – MCS konnte nicht mit diesem Node kommunizieren. • Unknown (gelb) – Node-Status kann nicht bestimmt werden. • Offline (rot) – Auf dem Node ist ein Problem aufgetreten. Falls ConnectEMC aktiviert wurde, hätte ein Service-Request (SR) protokolliert werden sollen. Besuchen Sie den Avamar-Support, um bestehende SRs anzuzeigen. Durchsuchen Sie die Wissensdatenbank nach „Avamar Data Node offline solution esg112792“.

Tabelle 68 Serverdetails im Bereich mit Node-Informationen der Registerkarte „Servermanagement“

Eigenschaft	Beschreibung
Status	Aktueller Betriebsstatus des Servers. Einer der folgenden Werte: • ONLINE – Node funktioniert korrekt. • DEGRADED – Mindestens ein Festplattenfehler wurde erkannt. • OFFLINE – Auf dem Node ist ein Problem aufgetreten. Falls ConnectEMC aktiviert wurde, hätte ein Service-Request (SR) protokolliert werden sollen. Besuchen Sie den Avamar-Support, um bestehende SRs anzuzeigen. Durchsuchen Sie die Wissensdatenbank nach „Avamar Data Node offline solution esg112792“. • READONLY – Dies tritt in der Regel ein, wenn Vorgänge im Hintergrund durchgeführt werden und Backups unterbrochen wurden.
Runlevel	Aktueller Betriebsstatus des Servers. Einer der folgenden Werte:

Tabelle 68 Serverdetails im Bereich mit Node-Informationen der Registerkarte „Servermanagement“ (Fortsetzung)

Eigenschaft	Beschreibung
	• fullaccess – Dieser Avamar-Server ist voll funktionsfähig. • admin – Der Avamar-Server ist voll funktionsfähig, allerdings kann nur das Administrator-Root-Konto auf den Server zugreifen. • adminonly – Der Avamar-Server ist voll funktionsfähig, allerdings kann nur das Administrator-Root-Konto auf den Server zugreifen. • adminreadonly – Der Avamar-Server befindet sich in einem schreibgeschützten Zustand und nur das Administrator-Root-Konto kann auf den Server zugreifen. • readonly – Der Avamar-Server befindet sich in einem schreibgeschützten Zustand. Wiederherstellungen sind zulässig, es können allerdings keine Backups vorgenommen werden. • suspended – Geplante Backups sind deaktiviert bis Sie den Planer erneut aktivieren. • synchronizing – Der Avamar-Server macht Stripes betriebsfertig oder synchronisiert sie. Eine temporäre Bedingung. Manche Vorgänge können verzögert werden.
Accessmode	Derzeitige Zugriffsebene des Servers. Der volle Serverzugriffsmodus wird in der Regel als 3 4-Bit-Felder dargestellt. Beispiel: `mhpu +mhpu+0000` Die wichtigsten Bit zeigen Serverberechtigungen an, die mittleren Bit Root-Benutzerberechtigungen und die am wenigsten wichtigen Bit Berechtigungen für alle anderen Benutzer. Die einzelnen Bit in diesen Feldern transportieren die folgenden Informationen: • m – Migration zulässig. • h – Hash-Dateisystem ist beschreibbar. • p – Dauerhafter Speicher ist beschreibbar. • u – Benutzerkonten sind beschreibbar.
Port	Für die Kommunikation innerhalb des Nodes verwendeter Datenport.

Tabelle 68 Serverdetails im Bereich mit Node-Informationen der Registerkarte „Servermanagement“ (Fortsetzung)

Eigenschaft	Beschreibung
Dispatcher	Von verschiedenen Dienstprogrammen verwendeter Datenport für die Kommunikation mit diesem Node.
Server uptime	Anzahl der verstrichenen Stunden, Tage und Minuten seit der Initialisierung dieses Avamar-Servers.
Total capacity	Gesamtmenge der Serverspeicherkapazität.
Capacity used	Gesamtmenge der Serverspeicherkapazität, die aus beliebigen Gründen belegt wurde.
Server utilization	Prozentsatz der gesamten verfügbaren Node-Speicherkapazität, der derzeit genutzt wird.
Number of stripes	Gesamtanzahl der Stripes auf diesem Node.
Server version	Auf diesem Node ausgeführte Version der Avamar-Software.

Tabelle 69 BS-Details im Bereich mit Node-Informationen der Registerkarte „Servermanagement“

Eigenschaft	Beschreibung
Version	Derzeit auf diesem Node ausgeführte Betriebssystemversion.
Node uptime	Anzahl der verstrichenen Stunden, Tage und Minuten seit dem letzten Start dieses Nodes.
Load average	Die durchschnittliche Anzahl von CPU-Threads in der letzten Minute.
CPU %	Prozentsatz, zu dem die CPU dieses Node derzeit belegt ist.
Ping time (sec)	Zeit in Sekunden, die dieser Node für die Reaktion auf eine Ping-Anforderung benötigt hat.
Disk reads	Anzahl der Festplattenlesevorgänge pro Sekunde.
Disk writes	Anzahl der Schreibvorgänge pro Sekunde für das Festplattenlaufwerk.
Network reads	Anzahl der Kilobyte pro Sekunde, die über die Netzwerkverbindung dieses Node gelesen werden.
Network writes	Anzahl der Kilobyte pro Sekunde, die über die Netzwerkverbindung dieses Node geschrieben werden.

Tabelle 70 Hardwaredetails im Bereich mit Node-Informationen der Registerkarte „Servermanagement“

Eigenschaft	Beschreibung
IP address	IP-Adresse dieses Node.
MAC address	Media Access Control (MAC)-Adresse. Eine Low-Level-Hardwareadresse, die diesem Node auf dem Avamar-Server eine eindeutige Kennung zuweist.
Number of partitions	Gesamtanzahl der logischen Festplattenpartitionen in diesem Node.

Partitionsinformationen

Die folgenden Tabellen enthalten Details zu den **Partitionsinformationen**, die verfügbar sind, wenn eine Partition auf der Registerkarte **Server Management** ausgewählt wird.

Tabelle 71 Statusindikatoren im Bereich mit Partitionsinformationen der Registerkarte „Servermanagement“

Eigenschaft	Beschreibung
Statusanzeigen	Einer der folgenden Werte: • Online (grün) – Die Partition funktioniert korrekt. • Offline (gelb) – Mindestens ein Stripe auf der Partition ist offline. Falls ConnectEMC aktiviert wurde, hätte ein Service-Request (SR) protokolliert werden sollen. Besuchen Sie die Avamar-Support-Website, um bestehende SRs anzuzeigen. • Read-Only (blau) – Die Partition ist schreibgeschützt. • Nonfunctional (red) – Die Partition funktioniert nicht. Durchsuchen Sie die Wissensdatenbank auf der Avamar-Support-Website nach „solution esg108474“.

Tabelle 72 Serverdetails im Bereich mit Node-Informationen der Registerkarte „Servermanagement“

Eigenschaft	Beschreibung
Total capacity	Gesamtmenge der Serverspeicherkapazität.
Server utilization	Prozentsatz der gesamten verfügbaren Partitionsspeicherkapazität, der genutzt wird.

Tabelle 72 Serverdetails im Bereich mit Node-Informationen der Registerkarte „Servermanagement“ (Fortsetzung)

Eigenschaft	Beschreibung
Status	Aktueller Betriebsstatus dieser Partition. Einer der folgenden Werte: • ONLINE – Die Partition funktioniert korrekt. • MIGRATING – Übergangsstatus, der Teil des normalen Betriebs sein kann oder nicht. • OFFLINE – Übergangsstatus, der Teil des normalen Betriebs sein kann oder nicht. • READY – Übergangsstatus, der Teil des normalen Betriebs sein kann oder nicht. • RESTARTING – Übergangsstatus, der Teil des normalen Betriebs sein kann oder nicht.
Number of offline stripes	Gesamtanzahl der Stripes auf dieser Partition, die aufgrund von Medienfehlern offline sind.
Number of transitioning stripes	Gesamtanzahl der Stripes auf dieser Partition, die sich in einem Übergangsstatus befinden, der Teil des normalen Betriebs sein kann oder nicht.
Properties	Verschiedene Betriebssystemeigenschaften (falls bekannt).
Werte	Einstellungen zu Betriebssystemeigenschaften (falls bekannt).

Data Domain-Systeminformationen

Die folgende Tabelle enthält Details zu den Data Domain-Systemeigenschaften auf der Registerkarte „Server Management“.

Tabelle 73 Data Domain-Systemeigenschaften auf der Registerkarte „Server Management“

Eigenschaft	Beschreibung
Statusanzeigen	Einer der folgenden Werte: • Online (grün) – Das Data Domain-System funktioniert korrekt. • Offline (gelb) – Das Data Domain-System ist offline. Im *Data Domain Offline Diagnostics Suite User Guide*, erhältlich beim Avamar-Support, finden Sie weitere Informationen. • Read-Only (blau) – Das Data Domain-System ist schreibgeschützt.

Tabelle 73 Data Domain-Systemeigenschaften auf der Registerkarte „Server Management“ (Fortsetzung)

Eigenschaft	Beschreibung
	• Nonfunctional (rot) – Das Data Domain-System funktioniert nicht. Im *Data Domain Offline Diagnostics Suite User Guide* finden Sie weitere Informationen.
Hostname	Der Netzwerkhostname des Data Domain-Systems, wie im DNS definiert.
Total Capacity (post-comp size)	Die Gesamtkapazität für komprimierte Daten auf dem Data Domain-System.
Server Utilization (post-comp use%)	Der Prozentsatz der aus beliebigem Grund verwendeten Kapazität auf dem Data Domain-System nach der Komprimierung der Daten.
Bytes Protected	Die Gesamtanzahl der Byte an Daten, die auf dem Data Domain-System geschützt oder gesichert sind. Dieser Wert entspricht der Zahl an Byte vor der Komprimierung der Daten.
File System Available (post-comp avail)	Die Gesamtmenge des verfügbaren Festplattenspeichers für komprimierte Daten, der im DDFS verfügbar ist.
File System Used (post-comp used)	Die Gesamtmenge des im DDFS für komprimierte Daten verwendeten Festplattenspeichers.
Username	Der Benutzername des Data Domain OpenStorage- (OST-)Kontos, den Avamar für den Zugriff auf das Data Domain-System für Backups, Wiederherstellungen und Replikationen verwenden sollte. Dieser Benutzername wird festgelegt, wenn Sie das Data Domain-System der Avamar-Konfiguration hinzufügen.
Default Replication Storage System	Gibt an, ob das Data Domain-System als standardmäßiger Replikationsspeicher konfiguriert ist. Diese Option wird aktiviert oder deaktiviert, wenn Sie das Data Domain-System der Avamar-Konfiguration hinzufügen.
Maximum Streams	Die maximale Anzahl an Data Domain-Systemstreams, die Avamar zur Durchführung von Backups und Wiederherstellungen verwenden kann. Diese Zahl wird für das Data Domain-System konfiguriert, wenn Sie das System der Avamar-Konfiguration hinzufügen.
DDOS Version	Versionsnummer des Data Domain-Betriebssystems (DD OS) auf dem Data Domain-System.

Tabelle 73 Data Domain-Systemeigenschaften auf der Registerkarte „Server Management“ (Fortsetzung)

Eigenschaft	Beschreibung
Serial Number	Die Seriennummer des Herstellers zur Festplatte im Data Domain-System.
Model number	Modellnummer des Data Domain-Systems.
Monitoring Status	Überwachungsstatus des Data Domain-Systems. Im *Avamar und Data Domain-System – Integrationshandbuch* finden Sie nähere Informationen zu den verfügbaren Werten.
Monitoring status details	Wenn der „Monitoring Status“ ein anderer Wert als „OK“ ist, werden zusätzliche Informationen in einer Liste unter der Zeile **Monitoring Status** angezeigt. In den folgenden Einträgen sind die verfügbaren Werte beschrieben. **Hinweis** Im *Avamar und Data Domain-System – Integrationshandbuch* erfahren Sie weitere Details zum Troubleshooting von Fehlerzuständen, die jeweils aus diesen Werten resultieren. DD Boost-Lizenzierungsstatus: • DDBoost Licensed • DDBoost not Licensed DD Boost-Status: • DDBoost Enabled • DDBoost Disabled Ob der DD Boost-Benutzer aktiviert oder deaktiviert ist: • DDBoost User Enabled • DDBoost User Disabled DD Boost-Benutzerstatus: • DDBoost User Valid • DDBoost User Changed DD Boost-Optionsstatus: • DDBoost Option Enabled • DDBoost Option Disabled • DDBoost Option not Available Status des Nicht-OST-Benutzers, sofern konfiguriert:

Tabelle 73 Data Domain-Systemeigenschaften auf der Registerkarte „Server Management“ (Fortsetzung)

Eigenschaft	Beschreibung
	• Non-ost user state is Unknown • Non-ost user Invalid • Non-ost user disabled • Non-ost user is not an admin user **Hinweis** Die Zeile „non-OST user“ wird nicht angezeigt, wenn der Nicht-OST-Benutzer nicht konfiguriert wurde. SNMP-Status: • SNMP Enabled • SNMP Disabled Status des Data Domain-Dateisystems: • File System Running • File System Enabled • File System Disabled • File System Unknown • File system status unknown since SNMP is disabled Ob die Synchronisation der Wartungsvorgänge, z. B. Prüfpunkte, HFS-Kontrollen und die automatische Speicherbereinigung, zwischen dem Avamar-Server und dem Data Domain-System erfolgen kann: • Synchronization of maintenance operations is off. • Synchronization of maintenance operations is on.

Ereignisüberwachung

Alle Avamar-Systemaktivitäten und der Betriebsstatus werden als Ereignisse an den MCS gesendet. Beispiele für Avamar-Ereignisse sind die Clientregistrierung und -aktivierung, erfolgreiche und fehlgeschlagene Backups und der Festplattenstatus.

Jedes Ereignis umfasst die Informationen in der folgenden Tabelle.

Tabelle 74 Ereignisinformationen

Information	Beschreibung
Event code	Eindeutige Kennung
Date and time	Datum und Uhrzeit der Ereignismeldung
Kategorie	Kategorie des Ereignisses: • SYSTEM • APPLICATION • USER • SECURITY
Typ	Typ des Ereignisses: • INTERNAL • ERROR • WARNUNG • INFORMATION • DEBUG
Zusammenfassung	Eine einzeilige Beschreibung des Ereignisses
Hardware source	System-Node, von dem das Ereignis gemeldet wurde
Software source	System- oder Anwendungsmodul, von dem das Ereignis gemeldet wurde

Ereignisbenachrichtigungen

Mit den folgenden Funktionen werden beim Eintreten bestimmter Ereignisse Benachrichtigungen generiert.

Pop-up-Warnmeldungen
Sie können einzelne Ereignisse so konfigurieren, dass eine grafische Pop-up-Warnmeldung bei jedem Eintreten des Ereignisses erzeugt wird. Avamar-Administrator muss ausgeführt werden, damit die Pop-up-Warnmeldungen angezeigt werden.

Liste zu quittierender Ereignisse
Sie können festlegen, dass der Avamar-Systemadministrator einen bestimmten Ereignistyp quittieren muss, wenn ein entsprechendes Ereignis auftritt.

E-Mail-Benachrichtigungen
Sie können festlegen, dass eine E-Mail-Nachricht an ausgewählte Empfänger gesendet wird, wenn ein bestimmter Ereignistyp auftritt. Diese Nachrichten können sofort oder in Batches zu geplanten Zeiten versendet werden.

Eine typische Batch-E-Mail-Benachrichtigung sieht wie folgt aus:

Tabelle 75 Beispiel einer Batch-E-Mail-Benachrichtigung

```
MCS: avamar-1.example.com
```

Tabelle 75 Beispiel einer Batch-E-Mail-Benachrichtigung (Fortsetzung)

```
MCS Version: 7.1.0-nnn
Avamar Server: avamar-1.example.com
Avamar Server Version: 7.1.0-nnn

Event profile: My Custom Profile
Count of events: 3

Summary of events:
Type
-----------
INFORMATION
INFORMATION
INFORMATION

Type           Code           Count          Summary
-----------    ------         ------         -------
INFORMATION    22207          1              New group
INFORMATION    22208          1              created
INFORMATION    22209          1              Group modified
                                             Group deleted
```

```
Event Code = 22207
Event Date/Time = 5/10/14 09:58:20 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = New group created
Software Source = MCS:CR

Event Code = 22209
Event Date/Time = 5/10/14 09:58:25 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = Group deleted
Software Source = MCS:CR

Event Code = 22208
Event Date/Time = 5/10/14 10:55:28 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = Group modified
Software Source = MCS:CR
```

Unterstützung für Syslog

Sie können festlegen, dass Avamar beim Auftreten eines Ereignistyps basierend auf Filterregeln, die für den Syslog-Daemon konfiguriert wurden, bei dem die Ereignisse eingehen, Informationen in lokalen oder externen Syslog-Dateien protokolliert. Überwachungstools und Utilitys von Drittanbietern zur Überprüfung von Protokolleinträgen ermöglichen den Zugriff auf und die Verarbeitung von syslog-

Dateien und dadurch die Integration von Avamar-Ereignisinformationen in Aktivitäts- und Statusberichte großer Standorte.

Unterstützung für SNMP
Die Avamar-SNMP-Implementierung bietet zwei Möglichkeiten für den Zugriff auf Avamar-Serverereignisse und den Abschlussstatus für Aktivitäten:

- SNMP-Anforderungen umfassen einen Mechanismus für SNMP-Managementanwendungen, um Informationen von einem SNMP-fähigen Remoteclient (in diesem Fall dem Avamar-Server) zu beziehen („Pull“).
- SNMP-Traps umfassen einen Mechanismus für den Avamar-Server, um Informationen in die SNMP-Managementanwendungen zu verschieben („Push“), wenn ausgewiesene Avamar-Ereignisse auftreten. Sie können einen Ereignistyp so konfigurieren, dass SNMP-Traps ausgegeben werden.

Usage Intelligence
Ermöglicht dem Avamar-Server, Berichtsinformationen automatisch zu erfassen und über das ESRS-Gateway an den Avamar-Support zu übertragen.

Ereignisprofile

Profile sind eine Funktion zum Managen von Benachrichtigungen, die verwendet wird, um bestimmte Ereigniscodes logisch zu gruppieren und festzulegen, welche Benachrichtigungen bei welchen Ereignissen generiert werden.

Es gibt zwei grundlegende Typen von Ereignisprofilen:

- **Systemprofil** – Es gibt nur ein Systemereignisprofil. Es enthält alle möglichen Systemereigniscodes.
- **Benutzerspezifische Profile** – Benutzerspezifische Profile werden dazu verwendet, verschiedene Benachrichtigungen zu senden, wenn bestimmte Systemereignisse auftreten. Sie können so viele benutzerspezifische Profile erstellen, wie Sie sollten. Dieser Schritt erfolgt, um Systemereignisse zu organisieren und Benachrichtigungen zu erzeugen, wenn eines dieser Ereignisse eintritt.

Profilkatalog

Das Avamar-System beinhaltet standardmäßig einen Satz von vorkonfigurierten Ereignisprofilen.

System
Es gibt nur ein Systemereignisprofil. Es enthält alle möglichen Systemereigniscodes.

Evaluation
Dieses Profil ist hauptsächlich zur Unterstützung von Systemevaluierungen vorgesehen. Ist es aktiviert, generiert dieses Profil eine E-Mail-Benachrichtigung und hängt die Berichtsinformation „Activities – DPN Summary“ der letzten 2 Wochen an. Im *Avamar-Berichte – Handbuch* finden Sie weitere Informationen zum Bericht „Activities – DPN Summary“.

High Priority Events
Dieses Profil ist standardmäßig aktiviert. Dieses spezielle Ereignisprofil sendet zweimal täglich automatisch die folgenden Informationen per E-Mail an den Avamar-Support (`emailhome@avamar.com`):

- Status der täglichen Datenintegritätsprüfung
- Ausgewählte Avamar-Serverwarnungen und Informationsmeldungen

- Alle Avamar-Serverfehler

Ihre einzige Änderungsmöglichkeit beim Profil „High Priority Events“ besteht darin, E-Mail-Adressen zur Liste „Recipient Email List“ hinzuzufügen. Wenn Sie benutzerspezifische Anpassungen an diesem Profil vornehmen möchten, kopieren Sie es und bearbeiten Sie die Kopie.

Local SNMP Trap
Dieses Profil ist schreibgeschützt und ist nur für Testzwecke vorgesehen. Mit diesem Profil können Sie überprüfen, ob Traps erfolgreich generiert und beim lokalen `snmptrapd`-Prozess eingegangen sind, der dann die Trap-Informationen in eine syslog-Datei schreibt.

Local Syslog
Ist dieses Profil aktiviert, meldet es über den lokalen `syslogd`-Prozess den Status an den Avamar-Server.

Profil „Usage Intelligence“
Ermöglicht dem Avamar-Server, Berichtsinformationen automatisch zu erfassen und über das ESRS-Gateway an den Avamar-Support zu übertragen.

Bearbeiten des Systemereignisprofils

Das Systemereignisprofil enthält alle möglichen Systemereigniscodes. Sie können das Systemereignisprofil so bearbeiten, dass eine Pop-up-Warnmeldung in Avamar Administrator, ein Eintrag in der allgemeinen Liste der nicht quittierten Ereignisse oder keines von beiden erzeugt wird.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Profiles** aus.

   Das Fenster **Manage All Profiles** wird angezeigt.
2. Wählen Sie im linken Bereich **System Profile** aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Profile** wird mit einer Liste an Ereigniscodes angezeigt.
3. Damit bei jedem Ereignis in Avamar Administrator eine grafische Pop-up-Warnmeldung angezeigt wird, aktivieren Sie das Kontrollkästchen **GUI Alert** neben dem Ereignis.
4. Damit bei jedem Ereignis ein Eintrag zur allgemeinen Liste der nicht quittierten Ereignisse hinzugefügt wird, aktivieren Sie das Kontrollkästchen **Acknowledgement Required**.
5. Klicken Sie auf **OK**.

Erstellen eines benutzerspezifischen Ereignisprofils

Über benutzerspezifische Ereignisprofile können Sie im Falle bestimmter Systemereignisse Benachrichtigungen senden.

Sie können Systemereignisse und Profile nur innerhalb der Domain anzeigen, bei der Sie angemeldet sind. Dieser Schritt hat Einfluss auf die von Ihnen bearbeitbaren Profile sowie auf die Ereignisse, die Sie einem Profil hinzufügen können.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Profiles** aus.

   Das Fenster **Manage All Profiles** wird angezeigt.
2. Wählen Sie im linken Bereich die Domain für das benutzerspezifische Ereignisprofil aus und klicken Sie auf **New**.

   Der Assistent **New Profile** wird angezeigt.

3. Geben Sie im Feld **Profile Name** einen Namen für das Ereignisprofil ein.
4. Behalten Sie für **Profile type** die Standardeinstellung **Email, Syslog, and SNMP Trap Notification** bei.

   Hinweis

   Da die Funktion „Usage Intelligence“ das vorkonfigurierte Profil „Usage Intelligence“ verwendet, erstellen Sie kein Profil, das auf dem Profiltyp „Usage Intelligence“ basiert. Dieser Schritt führt dazu, dass redundante Daten an den Avamar-Support gesendet werden.

5. Legen Sie durch Aktivieren oder Deaktivieren des Kontrollkästchens **Profile Enabled** fest, ob das Profil aktiviert oder deaktiviert werden soll.
6. Legen Sie durch Aktivieren oder Deaktivieren des Kontrollkästchens **Email Enabled** fest, ob E-Mail-Benachrichtigungen aktiviert oder deaktiviert werden sollen.
7. Legen Sie bei aktivierten E-Mail-Benachrichtigungen fest, ob E-Mail-Benachrichtigungen bei Eintritt eines Ereignisses oder planungsgemäß gesendet werden sollen:
   - Um E-Mail-Benachrichtigungen bei Eintreten von Ereignissen zu senden, wählen Sie **Send data as events occur** aus.
   - Um E-Mail-Benachrichtigungen planungsgemäß zu senden, klicken Sie auf **Send data on a schedule** und wählen Sie dann die gewünschte Planung aus der Liste aus.
8. Legen Sie durch Aktivieren oder Deaktivieren des Kontrollkästchens **Syslog Notification – Enabled** fest, ob syslog-Benachrichtigungen für das Profil aktiviert oder deaktiviert werden sollen.
9. Legen Sie durch Aktivieren oder Deaktivieren des Kontrollkästchens **SNMP Trap Notification – Enabled** fest, ob SNMP-Benachrichtigungen für das Profil aktiviert oder deaktiviert werden sollen.
10. Klicken Sie auf **Next**.

    Die Seite **Event Codes** wird angezeigt.
11. Klicken Sie auf die Registerkarte **All Codes** und aktivieren Sie dann das Kontrollkästchen **Notify** neben den Fehlern, durch die Benachrichtigungen ausgelöst werden sollen.

    HINWEIS

    Ein Sternchen (*) neben einem Ereignis gibt ein Ereignis mit einem so hohen Schweregrad an, dass für dieses Ereignis eine Benachrichtigung gesendet wird, auch wenn andere Ereignisbenachrichtigungen anhand einer Planung gesendet werden.

12. Klicken Sie auf die Registerkarte **Audit Codes** und aktivieren Sie dann das Kontrollkästchen **Notify** neben den Auditereignissen, durch die Benachrichtigungen ausgelöst werden sollen.

HINWEIS

Ein Sternchen (*) neben einem Ereignis gibt ein Ereignis mit einem so hohen Schweregrad an, dass für dieses Ereignis eine Benachrichtigung gesendet wird, auch wenn andere Ereignisbenachrichtigungen anhand einer Planung gesendet werden.

13. Wenn Sie dieses benutzerspezifische Ereignisprofil auf der obersten Ebene (also nicht zu einer Domain oder Subdomain) hinzufügen, legen Sie die Parameter zur Steuerung von Warnmeldungen zur Kapazitätsprognose fest:
    a. Klicken Sie auf die Registerkarte **Parameters**.
    b. Aktivieren Sie das Kontrollkästchen neben dem Parameter und geben Sie einen neuen Wert für den Parameter ein.
    c. Wiederholen Sie die oben angegebenen Schritte bei Bedarf für jeden Parameter.
14. Klicken Sie auf **Next**.

    Die Seite **Attachments** wird angezeigt.
15. (Optional) Wenn das Profil E-Mail-Benachrichtigungen enthält, aktivieren Sie das Kontrollkästchen **Attach Server status in email (XML)**, um einen des allgemeinen Avamar-Serverstatus im XML-Format in die Meldungen aufzunehmen.
16. (Optional) Um Avamar-Serverprotokolle in die E-Mail-Benachrichtigungen zu integrieren, aktivieren Sie das Kontrollkästchen **Attach Server logs in email** und geben Sie dann den vollständigen Pfad zum Speicherort der Avamar-Serverprotokolle in das Textfeld **Directory** ein. Der Standardspeicherort lautet `/usr/local/avamar/var/cron/`.
17. Legen Sie die Berichte fest, die in die E-Mail-Benachrichtigung integriert werden sollen:
    a. Aktivieren Sie das Kontrollkästchen **Attach** neben dem einzuschließenden Bericht.
    b. Aktivieren Sie das Kontrollkästchen neben dem Bericht für die Dateiformate, in denen der Bericht gesendet werden soll. Sie können zwischen **XML**, **CSV** oder **TXT** wählen.
    c. Legen Sie mithilfe der Felder **Since Count** und **Since Unit** die Anzahl der historischen Berichte dieses Typs fest, die zusammen mit jeder Benachrichtigung gesendet werden. Senden Sie beispielsweise diese Berichte der letzten 2 Monate.

       Die folgenden Werte sind in der Liste **Since Count** verfügbar:

       - **day(s) ago**
       - **week(s) ago**
       - **month(s) ago**
       - **since last modified**
18. Klicken Sie auf **Next**.

    Die Seite **Email Notification** wird angezeigt.
19. Wenn das Profil E-Mail-Benachrichtigungen enthält, legen Sie die Empfänger und Optionen für diese E-Mail-Benachrichtigungen fest:

a. Geben Sie im Feld **Email Subject Header** eine E-Mail-Betreffzeile für die Benachrichtigung ein.

b. Fügen Sie der Liste einen E-Mail-Empfänger hinzu, indem Sie eine gültige E-Mail-Adresse im Feld **Enter Recipient** eingeben und dann auf **+** klicken.

c. (Optional) Um einen Empfänger aus der Liste **Recipient Email** zu entfernen, wählen Sie den Empfänger aus und klicken Sie auf **-**.

d. Um alle Anhänge in den Textkörper der E-Mail-Benachrichtigung einzufügen, aktivieren Sie das Kontrollkästchen **Inline attachments**.

HINWEIS

Wenn Sie die Anhänge einfügen, kann die E-Mail sehr lang werden.

e. Um sofort eine Test-E-Mail zu senden, klicken Sie auf **Send Email**.

Wenn die Testnachricht erfolgreich gesendet wurde, wird eine Bestätigungsmeldung `Email accepted by transport layer` angezeigt.

20. Klicken Sie auf **Next**.

Die Seite **Syslog Notification** wird angezeigt.

21. Wenn das Profil syslog-Benachrichtigungen enthält, geben Sie die zugehörigen Parameter an:

a. Geben Sie in das Feld **Address (IP or hostname)** die IP-Adresse oder den Hostnamen des Avamar-Server-Node ein, auf dem der `syslogd`-Prozess ausgeführt wird.

b. Geben Sie in das Feld **Port Number** die für die syslog-Kommunikation verwendete Portnummer ein.

c. Legen Sie durch Aktivieren oder Deaktivieren des Kontrollkästchens **Include extended event data** fest, ob erweiterte Informationen zum Ereigniscode in die syslog-Meldung aufgenommen werden sollen.

Die erweiterten Informationen werden durch die folgenden Tags getrennt:

```
<Code>
<Type>
<Severity>
<Category>
<HwSource>
<Summary>
<active>
<lastEmailSendDate>
<domain>
<scheduleID>
<num_prefs>
<name>
<isSystem>
```

d. Wählen Sie aus der Liste **Facility** eine der folgenden Optionen aus: **user**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6** oder **local7**.

e. Um die Parameter für die syslog-Benachrichtigung zu testen, klicken Sie auf **Send Test Syslog Entry**.

22. Klicken Sie auf **Next**.

    Die Seite **SNMP Trap Notification** wird angezeigt.

23. Wenn das Profil SNMP-Benachrichtigungen enthält, geben Sie die zugehörigen Parameter an:

    a. Geben Sie in das Feld **SNMP Trap Address (IP or hostname)** die IP-Adresse oder den Hostnamen des Computers ein, auf dem eine für den Empfang und die Verarbeitung von SNMP-Traps geeignete Anwendung ausgeführt wird.

    b. Geben Sie in das Feld **Port Number** die Nummer des Ports auf dem Hostrechner ein, an dem SNMP-Traps eingehen. Der Standarddatenport ist 162.

    c. Geben Sie im Feld **SNMP Community** den Namen der SNMP-Community ein, die der SNMP-Trap-Listener laut Konfiguration verwenden soll.

    Die SNMP-Community ist eine Textzeichenfolge, die der lokale Net-SNMP-Agent zur eigenen Authentifizierung bei der SNMP-Managementanwendung verwendet.

    d. Um die Parameter für die SNMP-Benachrichtigung zu testen, klicken Sie auf **Send Test SNMP Trap**.

24. Klicken Sie auf **Finish**.

Bearbeiten eines benutzerspezifischen Ereignisprofils

Nach der Erstellung eines benutzerspezifischen Ereignisprofils für Benachrichtigungen über bestimmte Systemereignisse können Sie beliebige Eigenschaften des Profils bearbeiten.

Sie können Systemereignisse und Profile nur innerhalb der Domain anzeigen, bei der Sie angemeldet sind. Dieser Schritt hat Einfluss auf die von Ihnen bearbeitbaren Profile sowie auf die Ereignisse, die Sie einem Profil hinzufügen können.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Profiles** aus.

   Das Fenster **Manage All Profiles** wird angezeigt.

2. Wählen Sie im linken Bereich das benutzerspezifische Ereignisprofil aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Profile** wird angezeigt.

3. Bearbeiten Sie das benutzerspezifische Ereignisprofil. Die Eigenschaften unterscheiden sich nicht von denen bei einer Erstellung des Profils.

4. Klicken Sie auf **OK**.

Kopieren eines benutzerspezifischen Ereignisprofils

Sie können ein benutzerspezifisches Ereignisprofil erstellen, dessen Eigenschaften mit denen des bereits erstellten Profils übereinstimmen, indem Sie das Profil kopieren. Sie können das Profil in dieselbe Domain oder in eine andere Domain kopieren.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Profiles** aus.

   Das Fenster **Manage All Profiles** wird angezeigt.

2. Wählen Sie im linken Bereich ein Profil aus und klicken Sie auf **Copy**.

Das Dialogfeld **Save As** wird angezeigt.

3. Geben Sie im Feld **Save As** einen Namen für das neue benutzerspezifische Ereignisprofil ein.
4. (Optional) Um das neue benutzerspezifische Ereignisprofil in eine andere Domain zu kopieren, klicken Sie auf die Schaltfläche **...**, navigieren Sie zu der neuen Domain und klicken Sie auf **OK**.
5. Klicken Sie auf **OK**.

Testen von benutzerspezifischen Ereignisprofilbenachrichtigungen

Sie können Mechanismen für benutzerspezifische Ereignisprofilbenachrichtigungen testen, indem Sie eine kurze E-Mail-Nachricht senden oder eine kurze Meldung in die syslog-Datei schreiben.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Profiles** aus.

   Das Fenster **Manage All Profiles** wird angezeigt.
2. Wählen Sie im linken Bereich das benutzerspezifische Ereignisprofil aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Profile** wird angezeigt.
3. Testen Sie das benutzerspezifische Ereignisprofil:
   - Um eine E-Mail-Testnachricht zu senden, wählen Sie die Registerkarte **Email Notification** aus und klicken Sie auf **Send Email**.
   - Um eine Testnachricht in die syslog-Datei zu schreiben, wählen Sie die Registerkarte **Syslog Notification** aus und klicken Sie auf **Send Test Syslog Entry**.
   - Um eine SNMP-Trap-Testnachricht zu senden, wählen Sie die Registerkarte **SNMP Trap Notification** aus und klicken Sie auf **Test Send SNMP Trap**.

   Wenn die Testnachricht erfolgreich gesendet wurde, wird eine Bestätigungsmeldung angezeigt.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **OK**, um das Dialogfeld **Edit Profile** zu schließen.

Aktivieren und Deaktivieren eines benutzerspezifischen Ereignisprofils

Wenn Sie ein Ereignisprofil deaktivieren, werden E-Mail-Benachrichtigungen erst wieder nach der erneuten Aktivierung des Profils gesendet. Sie können alle Profile mit Ausnahme des Systemereignisprofils deaktivieren.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Profiles** aus.

   Das Fenster **Manage All Profiles** wird angezeigt.
2. Wählen Sie im linken Bereich ein Ereignisprofil aus.
3. Klicken Sie auf **Disable**, um das Ereignisprofil zu deaktivieren, oder auf **Enable**, um das Ereignisprofil zu aktivieren.

Löschen eines benutzerspezifischen Ereignisprofils

Sie können alle benutzerspezifischen Ereignisprofile mit Ausnahme des Systemereignisprofils dauerhaft löschen.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Profiles** aus.

   Das Fenster **Manage All Profiles** wird angezeigt.
2. Wählen Sie ein Ereignisprofil aus und klicken Sie auf **Delete**.

   Es wird eine Bestätigungsmeldung angezeigt.
3. Klicken Sie auf **Yes**.

Anzeigen der Ereignisse im Event Monitor

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Event Management**.
3. Klicken Sie auf die Registerkarte **Event Monitor** im unteren Bereich des Fensters.

   Die Avamar Administrator-Onlinehilfe liefert weitere Einzelheiten zu den Spalten im Event Monitor.
4. Wählen Sie den Anzeigemodus für den Event Monitor aus:
   - Wählen Sie **Query** aus, um die neuesten 5.000 Systemereignisse für einen festgelegten Datumsbereich anzuzeigen.
   - Wählen Sie **Monitor** aus, um die neuesten 5.000 Systemereignisse während der letzten 24 Stunden anzuzeigen.
5. (Optional) Filtern Sie die Ereignisse, die im Event Monitor angezeigt werden:
   a. Öffnen Sie das Menü **Actions** und wählen Sie **Event Management** > **Filter** aus.

      Das Dialogfeld **Filter** wird angezeigt.
   b. Wenn Sie den Anzeigemodus **Query** für den Event Monitor ausgewählt haben, wählen Sie über die Felder **From Date** und **To Date** den für die Ereignisse anzuzeigenden Datumsbereich aus.
   c. Wählen Sie aus der Liste **Category** die anzuzeigende Ereigniskategorie aus.
   d. Wählen Sie aus der Liste **Type** den anzuzeigenden Ereignistyp aus.
   e. Wählen Sie aus der Liste **Severity** den Schweregrad der anzuzeigenden Ereignisse aus.
   f. Um Ereignisse für alle Domains anzuzeigen, wählen Sie **All Domains** aus. Um alternativ Ereignisse für eine bestimmte Domain anzuzeigen, wählen Sie **Domain** aus und navigieren Sie zum Domainnamen oder geben Sie diesen ein.
   g. Um nur Ereignisse anzuzeigen, die bestimmte Schlüsselwörter unter Beachtung der Groß- und Kleinschreibung im XML-Datenelement des Ereigniscodes enthalten, geben Sie das Schlüsselwort in das Feld **Data** ein.

      Dieses Kriterium vereinfacht das ereignisattributübergreifende Filtern nach wichtigen Schlüsselwörtern. Beim Filtern der Anzeige Event Monitor auf `error` werden beispielsweise alle Ereignisse angezeigt, die das Wort `error`

in einem beliebigen XML-Attribut enthalten (z. B. Kategorie, Typ oder Schweregrad).

h. Wählen Sie aus, ob Ereignisse von allen Quellen, nur vom Avamar-Server, von allen Data Domain-Systemen oder von einem einzigen Data Domain-System angezeigt werden sollen:

- Behalten Sie die Standardauswahl **All Sources** in der Liste **Source** bei, um Ereignisse von allen Quellen anzuzeigen.
- Wählen Sie Avamar aus der Liste **Source** aus, um nur Ereignisse vom **Avamar**-Server anzuzeigen.
- Wählen Sie **Data Domain Systems** aus der Liste **Source** aus und behalten Sie die Standardauswahl **All Systems** bei, um Ereignisse von allen Data Domain-Systemen anzuzeigen.
- Um Ereignisse von einem einzigen Data Domain-System anzuzeigen, wählen Sie **Data Domain Systems** aus der Liste **Source** aus, wählen Sie die Option **System** aus und geben Sie das Data Domain-System ein bzw. navigieren Sie zum entsprechenden Data Domain-System.

i. Klicken Sie auf **More**, um weitere Filterkriterien anzuzeigen.

j. Um den Event Monitor auf Ereignisse mit einem bestimmten Ereigniscode zu beschränken, wählen Sie **Only include codes** aus und fügen Sie der Liste Codes hinzu oder entfernen Sie Codes aus der Liste. Um alternativ Ereignisse mit einem bestimmten Ereigniscode vom Event Monitor auszuschließen, wählen Sie **Exclude codes** aus und fügen Sie der Liste Codes hinzu oder entfernen Sie Codes aus der Liste.

k. Klicken Sie auf **OK**.

Anzeigen des Ereigniskatalogs

Eine sequenzielle Auflistung aller Ereigniscodes und zusammenfassender Informationen ist in `/usr/local/avamar/doc/event_catalog.txt` auf dem Avamar-Server verfügbar. Sie können `event_catalog.txt` auch über einen Webbrowser anzeigen.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und geben Sie die folgende URL ein:

   `https://`*`Avamar_server`*

   Dabei steht *Avamar_server* für den DNS-Namen oder die IP-Adresse des Avamar-Servers.

   Die Seite **Avamar Web Restore** wird angezeigt.
2. Klicken Sie auf **Documentation**.

   Die Seite **Avamar Documentation** wird angezeigt.
3. Klicken Sie auf das Plussymbol neben **Avamar Event Codes**.
4. Klicken Sie auf **event_catalog.txt**.

   Die Datei wird in einem Webbrowser geöffnet.

Quittieren von Systemereignissen

Systemereignisse, die so konfiguriert sind, dass bei jedem Auftreten eine Quittierung erforderlich ist, bleiben so lange in der Liste mit den nicht quittierten Ereignissen, bis sie von einem Avamar-Serveradministrator explizit gelöscht oder quittiert werden.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Event Management**.
3. Klicken Sie auf die Registerkarte **Unacknowledged Events** im unteren Bereich des Fensters.
4. Quittieren Sie die Ereignisse:
   - Um ein oder mehrere Ereignisse zu quittieren, markieren Sie die Ereigniseinträge und wählen Sie **Actions** > **Event Management** > **Acknowledge Unacknowledged Events** aus.
   - Um alle Ereignisse in der Liste zu quittieren, wählen Sie **Actions** > **Event Management** > **Clear All Alerts** aus.

Anpassen von Fehlerereignissen

Standardmäßig überwacht die Avamar-Software kontinuierlich den Ordner `/var/log/messages` hinsichtlich der schreibweisenunabhängigen Suchzeichenfolge `error`. Wird die Suchzeichenfolge `error` erkannt, wird ein Ereigniscode des Typs „ERROR“ erstellt. Sie können dieses Standardverhalten anpassen.

Vorgehensweise

1. Legen Sie zusätzliche schreibweisenunabhängige Suchzeichenfolgen fest, mit denen Avamar-ERROR-Ereignisse erstellt werden.
2. Fügen Sie die Suchzeichenfolgen zu `/usr/local/avamar/var/mc/server_data/adminlogpattern.xml` hinzu.

Serverüberwachung mit syslog

Mit der syslog-Systemprotokollierungsfunktion auf Unix- und Linux-Systemen werden Systemprotokollmeldungen gesammelt und in eine bestimmte Protokolldatei geschrieben. Sie können den Avamar-Server so konfigurieren, dass Ereignisinformationen im syslog-Format gesendet werden.

Der Avamar-Server unterstützt sowohl syslog- als auch syslog-ng-Implementierungen.

Hinweis

Benutzer, die die syslog-Überwachung eines Avamar-Servers konfigurieren, sollten mit den grundlegenden syslog-Konzepten vertraut sein. Eine vollständige Erläuterung grundlegender syslog-Konzepte und deren Implementierung ist in diesem Handbuch leider nicht möglich. Zusätzliche Informationen erhalten Sie auf der Website www.syslog.org.

Auf Betriebssystemsebene wird bei der Systemüberwachung und -protokollierung auf den `syslogd`-Prozess zurückgegriffen, um Systemprotokollmeldungen zu sammeln

und sie in eine hierfür vorgesehene Protokolldatei zu schreiben. Der `syslogd`-Prozess wird lokal auf jedem Avamar-Server-Node ausgeführt.

Ohne zusätzliche Konfiguration sammelt der `syslogd`-Prozess jedes Node allerdings nur die Systeminformationen für diesen Node und schreibt diese in eine lokale Protokolldatei auf dem entsprechenden Node. Aus syslog-Sicht „wissen“ die einzelnen Avamar-Server-Nodes nicht von der Existenz anderer Server-Nodes. Außerdem ist dem syslog-Prozess auf dem Utility-Node nicht bekannt, dass der Avamar Management Console Server (MCS) Avamar-Ereignisinformationen sammelt und protokolliert.

Sie können ein Avamar-Ereignisprofil so konfigurieren, dass Ereignismeldungen des Avamar-Servers im syslog-Format formatiert und diese Daten an den auf dem Avamar-Server-Utility-Node ausgeführten `syslogd`-Prozess gesendet werden.

In der folgenden Tabelle wird beschrieben, wie mithilfe eines Ereignisprofils Ereignisdaten eines Avamar-Servers syslog-Feldern zugeordnet werden.

Tabelle 76 Zuordnungen von syslog-Feldern zu Avamar-Ereignisdaten

Feld in syslog	Avamar-Ereignisdaten
Facility	Entweder `User` oder `Local#`; dabei ist # eine Zahl von 0 bis 7.
Priority	Einer der folgenden Werte, die auf dem Avamar-Ereignistyp basieren: • `debug`, wenn der Avamar-Ereignistyp DEBUG ist • `err`, wenn der Avamar-Ereignistyp ERROR ist • `info`, wenn der Avamar-Ereignistyp INFO ist • `none`, wenn der Avamar-Ereignistyp INTERNAL ist • `warning`, wenn der Avamar-Ereignistyp WARNING ist
Date	Datum des Avamar-Ereignisses
Time	Uhrzeit des Avamar-Ereignisses
Hardware source	Hardwarequelle des Avamar-Ereignisses
Software source	Softwarequelle des Avamar-Ereignisses
Message	Die folgenden Felder aus dem Avamar-Ereigniscode: • event code • category • summary • event data

Konfigurieren von lokalem syslog

Die grundlegende Methode zur Implementierung der Avamar-Server-syslog-Überwachung besteht darin, den MCS so zu konfigurieren, dass Avamar-Ereignisinformationen im lokalen, auf dem Utility-Node ausgeführten `syslogd`-Prozess ausgegeben werden. Der lokale `syslogd`-Dienst führt die Avamar-Ereignisinformationen und die Betriebssystemmeldungen in einer einzigen lokalen Protokolldatei zusammen.

Vorgehensweise

1. Aktivieren Sie das Ereignisprofil „Local Syslog“ auf dem Avamar-Server:
   a. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Profiles** aus.
   b. Wählen Sie im linken Bereich das Ereignisprofil **Local Syslog** aus und klicken Sie auf **Enable**.
2. Konfigurieren Sie auf Single-Node-Servern und Utility-Nodes mit SLES 11 oder höher den lokalen Utility-Node-syslogd-Prozess so, dass der UDP-Datenport 514 auf MCS-Ereignismeldungen überwacht wird:
   a. Öffnen Sie eine Befehlsshell und melden Sie sich als Administrator bei dem Single-Node-Server oder bei dem Utility-Node eines Multi-Node-Servers an.
   b. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie **`su -`** eingeben.
   c. Öffnen Sie `/etc/syslog-ng/syslog-ng.conf` in einem Texteditor.
   d. Suchen Sie nach dem folgenden Eintrag:

```
#
# uncomment to process log messages from network:
#
# udp(ip("0.0.0.0") port(514));
```

   e. Fügen Sie den folgenden Eintrag hinzu, einschließlich des Kommentars:

```
#
# uncomment to process log messages from MCS:
#
udp(ip("0.0.0.0") port(514));
```

   f. Speichern und schließen Sie die Datei.
   g. Starten Sie den syslog-Prozess neu, indem Sie den folgenden Befehl eingeben:

```
service syslog restart
```

   h. Überprüfen Sie, ob syslog den Port 514 abhört, indem Sie den folgenden Befehl eingeben:

```
netstat -nap | grep 514
```

   In der Befehlsshell wird die folgende Ausgabe angezeigt:

```
udp 0 0 127.0.0.1:514 127.0.0.1:* 8043/syslog-ng
```

Konfigurieren von Remote-syslog

Die Remote-syslog-Überwachung umfasst Folgendes:

- Konfigurierung aller Server-Nodes zum Senden von syslog-Daten an einen Remoteprotokollierungshost.
- Erstellen eines benutzerspezifischen syslog-Ereignisprofils, das Ereignismeldungen des Avamar-Servers im syslog-Format an den Remoteprotokollierungshost sendet.

Standorte, die die Remote-syslog-Überwachung eines Avamar-Servers implementieren, haben in den meisten Fällen bereits einen Remoteprotokollierungshost konfiguriert und bereitgestellt.

Es sind zahlreiche syslog-Überwachungstools verfügbar. Grundsätzlich können alle syslog-Überwachungstools mit Avamar verwendet werden, solange das jeweilige Tool so konfiguriert ist, dass es den UDP-Datenport 514 über eine LAN-Verbindung auf Remote-syslog-Meldungen überwacht.

HINWEIS

Um eine maximale Sicherheit zu erreichen, implementieren Sie die Remote-syslog-Überwachung.

Vorgehensweise

1. Erstellen Sie ein benutzerspezifisches syslog-Ereignisprofil, das Ereignismeldungen des Avamar-Servers im syslog-Format an den Remoteprotokollierungshost sendet.
2. Konfigurieren Sie alle Server-Nodes so, dass syslog-Meldungen an den Remoteprotokollierungshost gesendet werden.
3. Konfigurieren Sie den Remoteprotokollierungshost so, dass er den UDP-Datenport 514 über eine LAN-Verbindung auf syslog-Meldungen überwacht.
4. Konfigurieren Sie bei aktivierter Firewall auf dem Remoteprotokollierungshost die Firewall so, dass für einen definierten IP-Bereich UDP-Datenverkehr auf Port 514 zugelassen wird.

Erstellen eines benutzerspezifischen syslog-Ereignisprofils

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Profiles** aus.

   Das Fenster **Manage All Profiles** wird angezeigt.
2. Wählen Sie im linken Bereich das Ereignisprofil **Local Syslog** aus und klicken Sie auf **Copy**.

   Das Dialogfeld **Save As** wird angezeigt.
3. Geben Sie im Feld **Save As** einen Namen für das neue benutzerspezifische Ereignisprofil ein.
4. Lassen Sie die Domain auf Root (/) eingestellt. Benutzerspezifische syslog-Profile müssen sich in der Root-Domain befinden.
5. Klicken Sie auf **OK**.
6. Wählen Sie im Dialogfeld **Manage All Profiles** das benutzerspezifische, von Ihnen erstellte syslog-Ereignisprofil aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Profile** wird angezeigt.

7. Wählen Sie die Registerkarte **Syslog Notification** aus und geben Sie die entsprechenden Parameter an:
   a. Geben Sie im Feld **Address (IP or hostname)** die IP-Adresse oder den Hostnamen des Remoteprotokollierungshosts ein.
   b. Lassen Sie im Feld **Port Number** die Portnummer auf **514** eingestellt.
   c. Wählen Sie die Option **Include extended event data** aus, wenn Sie erweiterte Ereigniscodeinformationen in die syslog-Meldung integrieren möchten.

      Die erweiterten Informationen werden durch die folgenden Tags getrennt:

      ```
      <Code>
      <Type>
      <Severity>
      <Category>
      <HwSource>
      <Summary>
      <active>
      <lastEmailSendDate>
      <domain>
      <scheduleID>
      <num_prefs>
      <name>
      <isSystem>
      ```

   d. Wählen Sie aus der Liste **Facility** einen der folgenden Werte aus: **user**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6** or **local7**.
8. (Optional) Um die Parameter für die syslog-Benachrichtigung zu testen, klicken Sie auf **Send Test Syslog Entry**.
9. Klicken Sie auf **OK**.

Konfigurieren von Server-Nodes zum Senden von syslog-Meldungen an den Remoteprotokollierungsserver

Als Teil des Remote-syslog-Konfigurationsprozesses müssen Sie alle Avamar-Server-Nodes so konfigurieren, dass syslog-Meldungen über UDP-Datenport 514 per LAN-Verbindung an einen Remoteprotokollierungsserver gesendet werden.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell:
   a. Melden Sie sich beim Server als Administrator an.
   b. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie `su -` eingeben.
   c. Laden Sie für einen Multi-Node-Server den OpenSSH-Schlüssel rootid, indem Sie Folgendes eingeben:

      ```
      ssh-agent bashssh-add /root/.ssh/rootid
      ```

2. Öffnen Sie `/etc/syslog-ng/syslog-ng.conf` in einem Texteditor.
3. Fügen Sie den folgenden Eintrag hinzu:

   ```
   destination logserver {udp("ip_address" port(514)); };
   log { source(src); destination(logserver); };
   ```

   Dabei steht *ip_address* für die IP-Adresse des Remoteprotokollierungshosts.

4. Speichern und schließen Sie die Datei .
5. Starten Sie den syslog-Prozess neu, indem Sie den folgenden Befehl eingeben:

   service syslog restart

6. Wiederholen Sie auf Multi-Node-Servern die vorherigen Schritte für jeden Node.

Konfigurieren von RHEL-Remoteprotokollierungshosts mit syslog

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich beim Remoteprotokollierungshost als Root an.
2. Öffnen Sie `/etc/sysconfig/syslog` in einem Texteditor.
3. Suchen Sie nach dem folgenden Eintrag:

   ```
   SYSLOGD_OPTIONS="-m 0"
   ```

4. Fügen Sie dem folgenden Eintrag den Parameter `-r` hinzu:

   ```
   SYSLOGD_OPTIONS="-r -m 0"
   ```

5. Speichern und schließen Sie die Datei.
6. Starten Sie den `syslogd`-Prozess neu, indem Sie den folgenden Befehl eingeben:

   service syslog restart

Konfigurieren von SLES-Remoteprotokollierungshosts mit syslog-ng

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich beim Remoteprotokollierungshost als Root an.
2. Öffnen Sie `/etc/syslog-ng/syslog-ng.conf` in einem Texteditor.
3. Suchen Sie nach dem folgenden Eintrag:

   ```
   #
   # uncomment to process log messages from network:
   #
   # udp(ip("0.0.0.0") port(514));
   ```

4. Heben Sie die Auskommentierung des folgenden Eintrags auf:

   ```
   #
   # uncomment to process log messages from network:
   #
   udp(ip("0.0.0.0") port(514));
   ```

5. Speichern und schließen Sie die Datei.
6. Starten Sie den syslog-Prozess neu, indem Sie den folgenden Befehl eingeben:

   service syslog restart

7. Überprüfen Sie, ob syslog den Port 514 abhört, indem Sie den folgenden Befehl eingeben:

   netstat -nap | grep 514

In der Befehlsshell wird die folgende Ausgabe angezeigt:

```
udp 0 0 0.0.0.0:514 0.0.0.0:* 8043/syslog-ng
```

Konfigurieren der Firewall auf dem Remoteprotokollierungshost

Konfigurieren Sie bei aktivierter Firewall auf dem Remoteprotokollierungshost die Firewall so, dass für einen definierten IP-Bereich UDP-Datenverkehr auf Port 514 zugelassen wird.

Vorgehensweise

1. Beschränken Sie die Quell-IP-Adressen der Remoteprotokollmeldungen in iptables oder einer anderen Firewall, um DoS-Angriffe (Denial of Service) auf dem Remoteprotokollierungshost zu vermeiden.

   Die folgende Beispielregel für iptables lässt Clientsystemprotokolle für einen IP-Adressbereich von Avamar-Server-Nodes zu:

   ```
   # Rules to allow remote logging for syslog(-ng) on the log
   HOST system
   iptables -A INPUT -p udp -s 192.168.1.0/24 --dport 514 -j
   ACCEPT
   ```

   Dabei ist *192.168.1.0/24* der IP-Adressbereich der Avamar-Server-Nodes.

   Die folgende Beispielregel für iptables legt die IP-Adresse für jeden Avamar-Server-Node in einer Zeile fest und umfasst die Mac-Adresse der Netzwerkschnittstellenkarte (NIC) für den Node:

   ```
   iptables -A INPUT -p udp -s 192.168.1.12 -m mac --mac-
   source 00:50:8D:FD:E6:32 --dport 514 -j ACCEPT

   iptables -A INPUT -p udp -s 192.168.1.13 -m mac --mac-
   source 00:50:8D:FD:E6:33 --dport 514 -j ACCEPT

   iptables -A INPUT -p udp -s 192.168.1.14 -m mac --mac-
   source 00:50:8D:FD:E6:34 --dport 514 -j ACCEPT

   iptables -A INPUT -p udp -s 192.168.1.15 -m mac --mac-
   source 00:50:8D:FD:E6:35 --dport 514 -j ACCEPT

   ...
   ```

   Es sind keine Regeln für den ausgehenden, clientseitigen syslog-Datenverkehr erforderlich.

2. Starten Sie den Firewalldienst auf dem Remoteprotokollierungshost neu, damit die Änderungen wirksam werden.
3. Starten Sie den `syslog-ng`-Dienst auf allen Server-Nodes und dem Remoteprotokollierungshost neu, damit die Änderungen wirksam werden:

   ```
   service syslog restart
   ```

Serverüberwachung mit SNMP

SNMP (Simple Network Management Protocol) ist ein Protokoll zur Kommunikation und Überwachung von Ereignisbenachrichtigungsinformationen zwischen einer Anwendung, einem Hardwaregerät oder einer Softwareanwendung und einer beliebigen Anzahl von Überwachungsanwendungen oder -geräten.

Hinweis

Personen, die einen Avamar-Server zum Senden von Ereignisinformationen über SNMP konfigurieren, müssen mit grundlegenden SNMP-Konzepten vertraut sein. Eine vollständige Erläuterung grundlegender SNMP-Konzepte und deren Implementierung ist in diesem Handbuch nicht möglich. Zusätzliche Informationen erhalten Sie auf der Website www.net-SNMP.org.

Die Avamar-SNMP-Implementierung bietet SNMP-Anforderungen und SNMP-Traps für den Zugriff auf Avamar-Serverereignisse und den Aktivitätsstatus. Der Avamar-Server unterstützt die SNMP-Versionen 1 und 2c.

SNMP-Anforderungen
SNMP-Anforderungen umfassen einen Mechanismus für SNMP-Managementanwendungen, um Informationen von einer SNMP-fähigen Remoteanwendung oder einem SNMP-fähigen Remotegerät (in diesem Fall dem Avamar-Server) zu beziehen („Pull“). Die SNMP-Managementanwendung sendet eine Anforderung an den SNMP-Master-Agent, der auf dem Avamar-Server ausgeführt wird. Der SNMP-Master-Agent kommuniziert anschließend mit dem Avamar-SNMP-Subagent, der die Anforderung an den MCS weiterleitet. Der MCS ruft die Daten ab und sendet sie an den Avamar-SNMP-Subagent zurück, der sie über den SNMP-Master-Agent wieder an die Managementanwendung zurückleitet. Datenport 161 ist der Standarddatenport für SNMP-Anforderungen.

Avamar-Server, die direkt bei Avamar gekauft werden, verwenden den Net-SNMP-Master-Agent. Avamar-Server, die mit anderer dem Branchenstandard entsprechender Hardware zusammengestellt wurden, verwenden meistens einen vom Hardwarehersteller bereitgestellten SNMP-Master-Agent.

SNMP-Traps
SNMP-Traps umfassen einen Mechanismus für den Avamar-Server, um Informationen in die SNMP-Managementanwendungen zu verschieben („Push“), wenn ausgewiesene Avamar-Ereignisse auftreten. Datenport 162 ist der Standarddatenport für SNMP-Traps. In der Regel wird die SNMP-Managementanwendung von allen SNMP-Traps aufgerufen, die von ausgewiesenen Remote-Hosts generiert wurden.

Konfigurieren der Serverüberwachung mit SNMP

Vorgehensweise

1. Um die SNMP-Managementanwendung zur Überwachung eines Avamar-Servers zu aktivieren, laden Sie die Avamar MIB-Definitionsdatei (`AVAMAR-MCS-MIB.txt`) in die von der SNMP-Managementanwendung verwendeten Master-MIB (Management Information Base).

   Die MIB enthält Definitionen der Informationen, die überwacht werden können, oder die Traps, die für jede SNMP-Anwendung oder jedes SNMP-Gerät gesendet werden.

   In der folgenden Tabelle sind die Speicherorte für die Avamar-MIB-Definitionsdatei aufgeführt.

   Tabelle 77 Speicherorte für die Avamar-MIB-Definitionsdatei

Computertyp	MIB-Speicherort
Single-Node-Server	`/usr/local/avamar/doc`

Tabelle 77 Speicherorte für die Avamar-MIB-Definitionsdatei (Fortsetzung)

Computertyp	MIB-Speicherort
Multi-Node-Server	`/usr/local/avamar/doc on the utility node`
Computer mit Avamar Administrator	*`install_dir`*`/doc`. Dabei steht *install_dir* in der Regel für: • `C:\Program Files\avs \administrator` auf Microsoft Windows-Computern • `/usr/local/avamar` auf Linux-Computern • `/opt/AVMRconsl` auf Solaris-Computern

Eine Kopie der Avamar-MIB-Definitionsdatei befindet sich auch im Verzeichnis `/usr/share/snmp/mibs` auf Single-Node-Servern und Utility-Nodes. Diese Kopie wird vom Avamar-SNMP-Subagent verwendet und darf weder verschoben noch verteilt werden.

2. Konfigurieren Sie den Net-SNMP-Agent. Anweisungen finden Sie unter Konfigurieren des Net-SNMP-Agent auf Seite 311.
3. Konfigurieren Sie ein benutzerspezifisches Ereignisprofil, sodass es Avamar-Serverereignisse an einen SNMP-Trap ausgibt. Anweisungen finden Sie unter Erstellen eines benutzerspezifischen Ereignisprofils für einen SNMP-Trap auf Seite 313.

Konfigurieren des Net-SNMP-Agent

Das Befehlszeilendienstprogramm `avsetup_snmp` konfiguriert den Net-SNMP-Agent, um mit dem Avamar-Server mithilfe des Avamar-SNMP-Subagent zu kommunizieren.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell:
   a. Melden Sie sich beim Server als Administrator an.
   b. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie **`su -`** eingeben.
   c. Laden Sie für einen Multi-Node-Server den OpenSSH-Schlüssel rootid, indem Sie Folgendes eingeben:

      ```
      ssh-agent bashssh-add /root/.ssh/rootid
      ```

2. Geben Sie folgende Befehle ein, um das Dienstprogramm zu starten:

   ```
   cd /rootavsetup_snmp
   ```

   Über die Ausgabe werden Sie aufgefordert, den Port anzugeben, der auf SNMP-Anforderungen überwacht werden soll.
3. Geben Sie den Datenport für SNMP-Anforderungen an:
   - Um den Standarddatenport für SNMP-Anforderungen, Port 161, zu nutzen, drücken Sie die **Enter**.

- Um einen anderen Port für SNMP-Anforderungen zu nutzen, geben Sie die Datenportnummer ein und drücken Sie die **Enter**.

Wenn `avsetup_snmp` keine SNMP-Communitys erkennen konnte, werden Sie über die Ausgabe aufgefordert, anzugeben, ob ein benutzerabhängiger SNMPv3-Lese-/Schreibzugriff zugelassen werden soll.

4. Geben Sie **n** ein und drücken Sie die **Enter**.

   Über die Ausgabe werden Sie aufgefordert, anzugeben, ob ein benutzerabhängiger, schreibgeschützter SNMPv3-Zugriff zugelassen werden soll.

5. Geben Sie **n** ein und drücken Sie die **Enter**.

   Über die Ausgabe werden Sie aufgefordert, anzugeben, ob ein SNMPv1/v2c-Community-Lese-/Schreibzugriff zugelassen werden soll.

6. Geben Sie **n** ein und drücken Sie die **Enter**.

   Über die Ausgabe werden Sie aufgefordert, anzugeben, ob ein schreibgeschützter SNMPv1/v2c-Communityzugriff zugelassen werden soll.

7. Drücken Sie die **Enter**, um den Standardwert **y** zu übernehmen.

   Über die Ausgabe werden Sie aufgefordert, den Communitynamen anzugeben, für den der schreibgeschützte Zugriff ermöglicht werden soll. Die SNMP-Community ist eine Textzeichenfolge, die der lokale Net-SNMP-Agent zur eigenen Authentifizierung bei der SNMP-Managementanwendung verwendet.

8. Geben Sie den Namen der SNMP-Community ein und drücken Sie die **Enter**.

   Über die Ausgabe werden Sie aufgefordert, den Hostnamen oder die Netzwerkadresse anzugeben, von der Sie den Namen der Community übernehmen möchten.

9. Drücken Sie die **Enter**, um den Namen der Community von sämtlichen Hostnamen oder Netzwerkadressen zu übernehmen.

   Über die Ausgabe werden Sie aufgefordert, die OID anzugeben, für die diese Community beschränkt werden soll.

10. Drücken Sie die **Enter**, um keine Beschränkung anzugeben.

    Über die Ausgabe werden Sie aufgefordert, anzugeben, ob eine andere Community konfiguriert werden soll.

11. Geben Sie **n** ein und drücken Sie die **Enter**.

    Die Ausgabe zeigt an, dass `/etc/snmp/snmpd.conf` erstellt und zur Konfiguration der system_setup-Gruppe ausgeführt wurde. Anschließend werden Sie über die Ausgabe aufgefordert, den Standort des Systems anzugeben.

12. Geben Sie den physischen Standort des Avamar-Servers ein und drücken Sie die **Enter**.

    Über die Ausgabe werden Sie aufgefordert, die Kontaktinformationen anzugeben.

13. Geben Sie die Kontaktdaten (z. B. E-Mail-Adresse, Telefondurchwahl) ein und drücken Sie die **Enter**.

    Über die Ausgabe werden Sie aufgefordert, anzugeben, ob der Wert der sysServices.0-OID korrekt festgelegt werden soll.

14. Geben Sie **n** ein und drücken Sie die **Enter**.

Die Ausgabe zeigt an, dass `/etc/snmp/snmpd.conf` installiert und dass `snmpd` aktiviert wurde.

Erstellen eines benutzerspezifischen Ereignisprofils für einen SNMP-Trap

Erstellen Sie als Teil des Prozesses zur Konfiguration der Serverüberwachung mit SNMP ein benutzerspezifisches Ereignisprofil, um die vorgesehenen Avamar-Serverereignisse auf einem SNMP-Trap auszugeben.

Die Avamar-Standardkonfiguration beinhaltet ein **Local SNMP Trap**-Profil, das Avamar-Serverereignismeldungen auf den lokalen Net-SNMP-Trap-Listener ausgibt (`snmptrapd`-Prozess). Sie können das lokale SNMP-Trap-Profil jedoch nicht bearbeiten. Das Profil dient nur zu Testzwecken, um zu überprüfen, ob der lokale `snmptrapd`-Prozess die Traps erfolgreich generieren und erhalten kann. Der Prozess schreibt die Trap-Informationen anschließend in eine Syslog-Datei. Normalerweise besteht der nächste Schritt darin, ein anderes benutzerspezifisches Profil zu konfigurieren, um Avamar-SNMP-Traps an einen externen Net-SNMP-Trap-Listener zu senden.

Vorgehensweise

1. Erstellen Sie mithilfe der Schritte unter Erstellen eines benutzerspezifischen Ereignisprofils auf Seite 295 ein benutzerspezifisches Ereignisprofil.

   Wählen Sie auf der ersten Seite des Assistenten **New Profile** die Option zum Aktivieren von SNMP-Trap-Benachrichtigungen aus.
2. Durchlaufen Sie den Assistenten, bis die Seite **SNMP Trap Notification** angezeigt wird.
3. Geben Sie im Feld **SNMP Trap address (IP or hostname)** die IP-Adresse oder den Hostnamen eines Computers ein, auf dem eine für den Empfang und die Verarbeitung von SNMP-Traps fähige Anwendung ausgeführt wird.
4. Geben Sie im Feld **Portnummer** die Nummer des Ports auf dem Hostcomputer ein, an dem SNMP-Traps eingehen.
5. Geben Sie im Feld **SNMP Community** den Namen der SNMP-Community ein, die der SNMP-Trap-Listener laut Konfiguration verwenden soll.
6. (Optional) Um die Parameter für die SNMP-Benachrichtigung zu testen, klicken Sie auf **Send Test SNMP Trap**.
7. Klicken Sie auf **Finish.**

Anzeigen der Protokolldateien des Avamar-Servers

Standardmäßig ist die Avamar-Speicherprozess-Protokolldatei (`gsan.log`) auf 25 MB beschränkt und enthält die neuesten Informationen. Zusätzliche verlaufsbezogene Protokolldateien (beispielsweise `gsan.log.1`, `gsan.log.2` usw.) können ebenfalls vorhanden sein. Sie können diese Protokolldateien durch Verwendung von Befehlszeilenvorgängen sammeln und anzeigen.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:

a. Melden Sie sich als Administrator beim Utility Node an.

b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. Erstellen Sie ein neues benutzerdefiniertes temporäres Verzeichnis und ändern Sie das Verzeichnis zu diesem, indem Sie die folgenden Befehle eingeben:

   mkdir *directory*cd *directory*

   Dabei steht *directory* für den Verzeichnisnamen.

3. Rufen Sie Kopien der Speicher-Node-Protokolldateien ab, indem Sie den folgenden Befehl eingeben:

   getlogs

   Der Befehl `getlogs` sammelt die wichtigen Protokolldateien eines bestimmten Node, komprimiert diese in eine tar-Datei (`nodelogs.tgz`) und kopiert diese Dateien in nummerierte Unterverzeichnisse im derzeitigen Arbeitsverzeichnis.

4. Suchen Sie in den Dateien `nodelogs.tgz` alle Einträge mit der Zeichenfolge `ERROR`. Führen Sie hierzu die folgenden Shell-Befehle aus, durch die alle `nodelogs.tgz`-Einträge mit der Zeichenfolge `ERROR` in eine benutzerdefinierte temporäre Datei geschrieben werden:

   ```
   for p in [01].[!sm]*/nodelogs.tgz; dotar xzf $pgrep ERROR: cur/
   gsan.log*rm -rf cur/*done
   ```

5. Entfernen Sie das benutzerdefinierte temporäre Verzeichnis, indem Sie die folgenden Befehle eingeben:

   cd ../rm -rf *directory*

Auditprotokollierung

Diese Auditprotokollierung protokolliert fortlaufend Systemaktionen, mit denen Benutzer beginnen. Mithilfe der Daten in diesem Protokoll können Unternehmen, die Avamar bereitstellen, Sicherheits-Policies durchsetzen, Sicherheitsverletzungen oder Abweichungen von Policies erkennen und Benutzer für diese Aktionen zur Verantwortung ziehen.

Es werden nur die Aktionen protokolliert, mit denen Benutzer beginnen. Aktionen, mit denen das System ohne ein Benutzerkonto beginnt, z. B. geplante Backups, Wartungsaktivitäten usw., werden nicht protokolliert.

Die Systemereignisse mit der Kategorie „SECURITY“ und dem Typ „AUDIT“ werden zur Implementierung der Avamar-Auditprotokollierungsfunktion verwendet. Da die zugrunde liegenden Daten für Auditprotokolleinträge Systemereignisse sind, sind diese Informationen an zwei Stellen verfügbar:

- Event Monitor – Enthält auch alle anderen Systemereignisse
- Auditprotokoll – Enthält nur Ereignisse, die gleichzeitig Auditprotokolleinträge sind

Standardmäßig werden Auditprotokollinformationen 1 Jahr lang aufbewahrt.

Sie können die Aufbewahrungsfrist für Auditprotokolle verlängern oder verkürzen, indem Sie den Wert von `clean_db_audits_days` in `/usr/local/`

`avamar/var/mc/server_data/prefs/mcserver.xml` bearbeiten und den MCS neu starten.

Anzeigen des Auditprotokolls

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Event Management**.
3. Klicken Sie auf die Registerkarte **Audit Log** im unteren Bereich des Fensters.

   Die Avamar Administrator-Onlinehilfe liefert weitere Einzelheiten zu den Spalten im Auditprotokoll.
4. Wählen Sie den Anzeigemodus für die Registerkarte „Audit Log“ aus:
   - Wählen Sie **Query** aus, um die neuesten 5.000 Auditprotokolleinträge für einen festgelegten Datumsbereich anzuzeigen.
   - Wählen Sie **Monitor** aus, um die neuesten 5.000 Auditprotokolleinträge während der letzten 24 Stunden anzuzeigen.
5. (Optional) Filtern Sie die Einträge, die in der Registerkarte „Audit Log“ angezeigt werden:
   a. Öffnen Sie das Menü **Actions** und wählen Sie **Event Management** > **Filter** aus.

      Das Dialogfeld **Filter** wird angezeigt.
   b. Wenn Sie den Anzeigemodus **Query** für das Auditprotokoll ausgewählt haben, wählen Sie über die Felder **From Date** und **To Date** den für die Einträge anzuzeigenden Datumsbereich aus.
   c. Wählen Sie aus der Liste **Severity** den Schweregrad der anzuzeigenden Protokolleinträge aus.
   d. Um Protokolleinträge für alle Domains anzuzeigen, wählen Sie **All Domains** aus. Um alternativ Einträge für eine bestimmte Domain anzuzeigen, wählen Sie **Domain** aus und navigieren Sie zum Domainnamen oder geben Sie diesen ein.
   e. Um nur Protokolleinträge anzuzeigen, die bestimmte Schlüsselwörter unter Beachtung der Groß- und Kleinschreibung im XML-Datenelement des Auditprotokolleintrags enthalten, geben Sie das Schlüsselwort in das Feld **Data** ein.

      Dieses Kriterium vereinfacht das protokolleintragsattributübergreifende Filtern nach wichtigen Schlüsselwörtern. Beim Filtern des Protokolls in `error` werden beispielsweise alle Protokolleinträge angezeigt, die das Wort `error` in einem beliebigen XML-Attribut enthalten (z. B. Kategorie, Typ oder Schweregrad).
   f. Klicken Sie auf **More**, um weitere Filterkriterien anzuzeigen.
   g. Um das Auditprotokoll auf Ereignisse mit einem bestimmten Ereigniscode zu beschränken, wählen Sie **Only include codes** aus und fügen Sie der Liste Codes hinzu oder entfernen Sie Codes aus der Liste. Um alternativ Ereignisse mit einem bestimmten Ereigniscode vom Auditprotokoll

auszuschließen, wählen Sie **Exclude codes** aus und fügen Sie der Liste Codes hinzu oder entfernen Sie Codes aus der Liste.

h. Klicken Sie auf **OK**.

Automatische Benachrichtigungen an den Avamar-Support

Über die Funktionen „Email Home“ und „ConnectEMC“ werden automatisch Benachrichtigungen an den Avamar-Support gesendet. Diese Benachrichtigungen umfassen Warnmeldungen für Ereignisse hoher Priorität sowie tägliche Berichte, um die Überwachung des Avamar-Servers zu unterstützen.

Usage Intelligence

„Usage Intelligence“ ist eine Funktion, mit der der Avamar-Server automatisch Berichtsinformationen erfasst und an den Avamar-Support übermittelt. Die Typen von Berichten, die an den Avamar-Support gesendet werden, variieren je nachdem, wie der Avamar-Server lizenziert ist.

Die Verwendung dieser Funktion erfordert Folgendes:

- Das ESRS-Gateway ist installiert und in der lokalen Umgebung bereitgestellt.
- Sie haben die Anmeldedaten für die Autorisierung der Registrierung bei ESRS.

Installieren und Aktivieren der ESRS-Lizenz

Um Avamar mit ESRS zu verwenden, benötigen Sie eine Avamar-Lizenzschlüsseldatei, die eine ESRS-Lizenzierung enthält.

Installieren und Aktivieren einer Lizenz auf Seite 257 enthält Informationen zur Installation und Aktivierung einer Avamar-Lizenzschlüsseldatei.

Importieren des ESRS Gateway-Zertifikats in den Keystore des Avamar-Servers

Bevor Sie den Avamar-Server beim ESRS Gateway registrieren, müssen Sie das ESRS Gateway-Zertifikat in den Keystore des Avamar-Servers importieren.

Vorgehensweise

1. Exportieren Sie das ESRS Gateway-Zertifikat:
   a. Rufen Sie mit einem Browser die folgende Adresse auf: https://*Esrs_gateway*: 9443

      wobei *Esrs_gateway* der Hostname oder die IP-Adresse des lokalen ESRS-Gateways ist.

   b. Verwenden Sie die Browserfunktionen, um das Zertifikat zu exportieren.

      Z. B. in Internet Explorer 11:

      a. Klicken Sie auf das Sperrsymbol im Feld „URL“ und wählen Sie **View Certificates** aus.

      b. Klicken Sie auf die Registerkarte **Details**.

      c. Klicken Sie auf **Copy to File** und führen Sie die Schritte im **Certificate Export Wizard** aus.

2. Kopieren Sie das exportierte Zertifikat an einen temporären Speicherort auf dem Avamar-Server.
3. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:

- Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
- Wenn Sie sich bei einem Multi-Node-Server anmelden, melden Sie sich als Administrator beim Utility-Node an.

4. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie `su -` eingeben.
5. Sichern Sie den Keystore, indem Sie den folgenden Befehl in eine Zeile eingeben:

   ```
   cp -p /usr/local/avamar/lib/rmi_ssl_keystore /usr/local/
   avamar/lib/rmi_ssl_keystore.bak
   ```

6. Importieren Sie das ESRS-Serverzertifikat in den Keystore, indem Sie den folgenden Befehl in eine Zeile eingeben:

   ```
   keytool -importcert -keystore /usr/local/avamar/lib/
   rmi_ssl_keystore -storepass changeme -file <certfile>.crt
   ```

   wobei *< certfile>* der Name des ESRS-Serverzertifikats einschließlich Pfad ist.

7. Starten Sie den MCS neu, indem Sie den folgenden Befehle eingeben:

   ```
   mcserver.sh --restart
   ```

Registrieren von Avamar mit ESRS

Um die Usage Intelligence-Funktion zu aktivieren, müssen Sie den Avamar-Server bei ESRS registrieren.

Vorgehensweise

1. Wählen Sie in Avamar-Administrator die Optionen **Tools** > **Manage Rules**.

   Das Fenster **Edit ESRS Gateaway Information** wird geöffnet.
2. Geben Sie die IP-Adresse von ESRS Gateway in das Feld **ESRS Gateway** ein.
3. Geben Sie die Portnummer von ESRS Gateway in das Feld **Port** ein.
4. Geben Sie den Benutzernamen und das Passwort des ESRS Gateway-Benutzers ein, der berechtigt ist, das Gateway zu registrieren.
5. Klicken Sie auf **Register**.
6. Ein Meldungsfenster zeigt an, dass die Registrierung erfolgreich war. Klicken Sie zum Deaktivieren auf **OK**.

Ergebnisse

Sobald der Avamar-Server mit ESRS Gateway registriert wurde, ist keine weitere Konfiguration der Usage Intelligence-Funktion erforderlich.

Email Home

Mithilfe der Avamar-Funktion „Email Home“ werden Konfigurations-, Kapazitäts- und allgemeine Systeminformationen einmal täglich automatisch an den Avamar-Support gesendet und bei Bedarf wichtige Warnmeldungen nahezu in Echtzeit bereitgestellt.

Standardmäßig werden geplante E-Mail-Benachrichtigungen täglich um 6 Uhr und um 15 Uhr gesendet. Die „Notification Schedule“ steuert das Timing dieser Nachrichten. Planungen auf Seite 114 bietet weitere Informationen zur Bearbeitung von Planungen.

Bearbeiten der E-Mail-Einstellungen für die E-Mail-Home-Funktion

Die Funktion „Email Home“ wird während der Installation des Avamar-Servers konfiguriert und aktiviert. Sie können die E-Mail-Einstellungen für die E-Mail-Home-Funktion nach der Installation bearbeiten.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
2. Wechseln Sie mit dem folgenden Befehl die Verzeichnisse:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```
3. Öffnen Sie `mcserver.xml` in einem UNIX-Texteditor.
4. Navigieren Sie zum `com.avamar.asn.module.mail`-Node.

   Der Node `com.avamar.asn.module.mail` enthält die Einträge `smtpHost` und `admin_mail_sender_address`.
5. Vergewissern Sie sich, dass der Wert für den Eintrag `smtpHost` der DNS-Name des SMTP-Mail-Ausgangsservers ist, der zum Senden von Meldungen der E-Mail-Home-Funktion wie `smtp.example.com` verwendet wird.

   Wenn der Wert für den Eintrag falsch ist, bearbeiten Sie den Wert.

   HINWEIS

   Bei Serverinstallationen oder -upgrades von Avamar 6.0 und höher wird der Wert für den Eintrag `smtpHost` automatisch gefüllt. In den meisten Fällen müssen verschiedene Einstellungen vorgenommen werden, um E-Mails vom Avamar-Server über den SMTP-Mail-Ausgangsserver via Internet an den Avamar-Support weiterzuleiten.
6. Geben Sie eine gültige E-Mail-Adresse mit Zugriff auf einen SMTP-Mail-Ausgangsserver des Unternehmens als Wert für den Eintrag `admin_mail_sender_address` an.

HINWEIS

Wenn die Funktion „Email Home“ nicht so konfiguriert wurde, dass Nachrichten über eine gültige E-Mail-Adresse gesendet werden, werden von dieser Funktion generierte Nachrichten vom E-Mail-Eingangsserver von EMC zurückgewiesen. Der Avamar-Support weiß in diesen Fällen nicht, dass diese programmatisch generierten Meldungen zurückgewiesen wurden. Darüber hinaus werden programmatisch generierte Warnmeldungen an den Absender, dass diese Meldungen nicht gesendet werden konnten, niemals an Personen gesendet, die dieses Problem beheben könnten, da kein gültiges E-Mail-Konto zum Senden von E-Mails bekannt ist.

7. Speichern Sie die Änderungen und schließen Sie die Datei.
8. Starten Sie den MCS neu, indem Sie den folgenden Befehle eingeben:

   ```
   dpnctl stop mcsdpnctl start
   ```

9. Schließen Sie die Befehlsshell.

ConnectEMC

ConnectEMC ist ein Programm, das auf dem Avamar-Server ausgeführt wird und Informationen an den Avamar-Support sendet. ConnectEMC ist standardmäßig so konfiguriert, dass Warnmeldungen für eingetretene Ereignisse hoher Priorität sowie einmal täglich Berichte gesendet werden.

ConnectEMC ist in EMC Secure Remote Support (ESRS) integriert, sofern es installiert und betriebsbereit ist und der Avamar-Server über das Netzwerk darauf zugreifen kann. Zusätzliche Informationen zur Implementierung von ESRS erhalten Sie bei Ihrem Avamar-Vertriebsmitarbeiter.

ConnectEMC wird erstmalig während der Avamar-Serversoftwareinstallation konfiguriert. Mit Avamar Administrator haben Sie jedoch die Möglichkeit, ConnectEMC-Einstellungen nach Inbetriebnahme des Servers in Form von drei vom Benutzer konfigurierbaren Übertragungen zu managen:

- Primary transport
- Failover transport
- Notification transport

Beim Primary- und Failover-Transport werden Warnmeldungen für Ereignisse hoher Priorität bei ihrem Auftreten gesendet. Der Primary-Transport wird so lange verwendet, bis er fehlschlägt; dann wird der Failover-Transport verwendet.

Der Notification-Transport sendet unter bestimmten Bedingungen E-Mail-Benachrichtigungen an eine oder mehrere Kunden-E-Mail-Adressen.

Sie können außerdem steuern, ob der MCS ConnectEMC-Meldungen durch Aktivieren, Deaktivieren, Stoppen und Starten von ConnectEMC generiert und sendet.

Aktivieren und Deaktivieren von ConnectEMC

Wird ConnectEMC deaktiviert, generiert der MCS erst nach der erneuten Aktivierung von ConnectEMC wieder ConnectEMC-Nachrichten. Beenden Sie ConnectEMC, damit der MCS weiterhin ConnectEMC-Meldungen generieren kann, die Meldungen jedoch in die Warteschlange stellt.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage ConnectEMC** aus.

   Das Fenster **Manage ConnectEMC** wird angezeigt.
2. Geben Sie an, ob der MCS ConnectEMC-Meldungen generiert und sendet:
   - Um das Generieren von Meldungen durch den MCS zu stoppen, klicken Sie auf **Disable**.
   - Um das Generieren von Meldungen wieder zu starten, klicken Sie auf **Enable**.
   - Um weiterhin Meldungen zu generieren, diese jedoch in die Warteschlange zu stellen, klicken Sie auf **Stop**.
   - Um den Sendevorgang für Meldungen zu starten, klicken Sie auf **Start**.

   Wenn Sie ConnectEMC deaktivieren, werden Sie zur Eingabe eines Passworts aufgefordert.
3. Geben Sie ein gültiges Passwort ein und klicken Sie auf **OK**.

Bearbeiten von Primary- und Failover-Übertragungen

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage ConnectEMC** aus.

   Das Fenster **Manage ConnectEMC** wird angezeigt.
2. Wählen Sie im linken Bereich entweder **Primary Transport** oder **Failover Transport** aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Primary/Secondary Transport** wird angezeigt.
3. Wählen Sie den Übertragungstyp aus der Liste **Transport Type** aus:
   - **Email**
   - **FTP**
   - **HTTPS**

   Hinweis

   Für FTP- oder HTTPS-Übertragungen ist ein funktionsfähiges Secure Remote Support Gateway erforderlich.
4. (Nur E-Mail) Führen Sie nach der Auswahl von **E-Mail** die folgenden Schritte durch.
   a. Geben Sie im Feld **SMTP Host (Email Server)** den Hostnamen oder die IPv4-Adresse des Mailservers an.
   b. Geben Sie im Feld **E-Mail-Adresse** einen oder mehrere Empfänger dieser E-Mails an. Trennen Sie mehrere E-Mail-Adressen durch Kommata.
   c. Geben Sie im Feld **Email Sender Address** die E-Mail-Adresse an, von der die Nachricht gesendet werden soll.
   d. (Optional) Klicken Sie zur Konfiguration erweiterter Einstellungen auf **Advanced** und legen Sie anschließend die folgenden Einstellungen im Dialogfeld **Edit Advanced Email Settings** fest:

- **Wiederholungen** – Die Anzahl der Wiederholungsversuche, bevor eine Fehlermeldung ausgegeben wird. Die Standardeinstellung ist fünf Versuche.
- **Timeout** – Die Anzahl der Sekunden, bevor eine Meldung ausgegeben wird, dass die Zeit für diesen Vorgang überschritten wurde. Die Standardeinstellung ist 5 Minuten (300 Sekunden).
- **Description** – Eine Beschreibung dieser Übertragung, die im Fenster **Manage ConnectEMC** angezeigt wird. Die Standardbeschreibung ist `Email Transport`.
- **Email Subject** – Die Betreffzeile in der E-Mail. Die Standardbetreffzeile lautet `Avamar ConnectEMC Notification Email`.

  Ändern Sie die Betreffzeile der E-Mail nur auf Anforderung des Avamar-Supports. Avamar-Spamfilter können E-Mail-Nachrichten mit anderen Betreffzeilen zurückweisen.

e. Klicken Sie auf **OK**.

5. (Nur FTP) Führen Sie nach der Auswahl von **FTP** die folgenden Schritte durch.
   a. Geben Sie im Feld **IP Address** eine IPv4-Adresse ein.
   b. Geben Sie im Feld **Username** einen FTP-Benutzernamen ein. Die Einstellung hängt von der FTP-Serversoftware ab.
   c. Geben Sie im Feld **Passwort** das Passwort für den Benutzernamen an.
   d. (Optional) Klicken Sie zur Konfiguration erweiterter Einstellungen auf **Advanced** und legen Sie anschließend die folgenden Einstellungen im Dialogfeld **Edit Advanced FTP Settings** fest:
      - **Wiederholungen** – Die Anzahl der Wiederholungsversuche, bevor eine Fehlermeldung ausgegeben wird. Die Standardeinstellung ist fünf Versuche.
      - **Timeout** – Die Anzahl der Sekunden, bevor eine Meldung ausgegeben wird, dass die Zeit für diesen Vorgang überschritten wurde. Die Standardeinstellung ist 5 Minuten (300 Sekunden).
      - **Description** – Eine Beschreibung dieser Übertragung, die im Fenster **Manage ConnectEMC** angezeigt wird. Die Standardbeschreibung ist `FTP Transport`.
      - **FEP Folder** – Ein eindeutiger benutzerspezifischer UNIX-Pfad im ConnectEMC Front End Processor (FEP). Verwenden Sie den Ordnerspeicherort, der Ihnen vom Avamar-Support genannt wurde.
      - **FTP Port** – Ein IP-Port. Die Standardeinstellung ist Port 21.
      - **Mode** – Entweder „Active“ oder „Passive“. Die Standardeinstellung ist „Active“.

        Ändern Sie die Betreffzeile der E-Mail nur auf Anforderung des Avamar-Supports. Avamar-Spamfilter können E-Mail-Nachrichten mit anderen Betreffzeilen zurückweisen.

   e. Klicken Sie auf **OK**.
6. (Nur HTTPS) Führen Sie nach der Auswahl von **HTTPS** die folgenden Schritte durch.
   a. Geben Sie eine gültige URL für die Secure Remote Support-Startseite in das Feld **URL** ein.

Gültige URLs haben folgendes Format:

`https://home_name[:port]/target_directory`

home_name, *port* und *target_directory* stehen dabei für den Startseitennamen, den Datenport und das Zielverzeichnis.

Verwenden Sie die URL, die Sie vom Avamar-Support erhalten haben.

b. (Optional) Klicken Sie zur Konfiguration erweiterter Einstellungen auf **Advanced** und legen Sie anschließend die folgenden Einstellungen im Dialogfeld **Edit Advanced HTTPS Settings** fest:

- **Wiederholungen** – Die Anzahl der Wiederholungsversuche, bevor eine Fehlermeldung ausgegeben wird. Die Standardeinstellung ist fünf Versuche.
- **Timeout** – Die Anzahl der Sekunden, bevor eine Meldung ausgegeben wird, dass die Zeit für diesen Vorgang überschritten wurde. Die Standardeinstellung ist 5 Minuten (300 Sekunden).
- **Passphrase des privaten Schlüssels** – Die Passphrase, die der privaten Schlüsseldatei zugeordnet ist.
- **Private Schlüsseldatei** – Der Dateiname der privaten Schlüsseldatei.
- **Client Certificate** – Das zu verwendende Clientzertifikat. Die Standardeinstellung ist „Default“. Es wird dasselbe Zertifikat wie auf dem MCS verwendet. Geben Sie andernfalls den Dateinamen des Clientzertifikats ein.
- **Server CA Bundle** – Datei mit einer Liste der Stammzertifikate.
- **Verify Server Name** – Angabe, ob der Servername überprüft werden soll. Entweder „Yes“ oder „No“. Die Standardeinstellung ist „No“.

c. Klicken Sie auf **OK**.

Beispiele für Schlüsseldateien finden Sie in den Verzeichnissen `/opt/connectemc/certs/` und `https-privatekey.pem`. Beispiele für Clientzertifikate finden Sie in den Verzeichnissen `/opt/connectemc/certs/` und `https-cert.pem`. Beispiele für Stammzertifikatbündel finden Sie in den Verzeichnissen `/opt/connectemc/certs/` und `https-ca-cert.pem`.

7. Klicken Sie im Dialogfeld **Edit Primary/Secondary Transport** auf **OK**.

Bearbeiten der Notification-Übertragung

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage ConnectEMC** aus.

   Das Fenster **Manage ConnectEMC** wird angezeigt.

2. Wählen Sie **Notification Transport** aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Notification Transport** wird angezeigt.

3. Wählen Sie aus der Liste **Notification Type** eines der folgenden Elemente aus:

   - **On Success** – Informiert die Empfänger, dass eine Ereignisdatei erfolgreich an EMC übertragen wurde.
   - **On Failure** – Informiert die Empfänger, dass eine Ereignisdatei nicht erfolgreich an EMC übertragen wurde.

- **On Success or Failure** – Informiert die Empfänger darüber, dass ein Versuch unternommen wurde, eine Ereignisdatei an EMC zu übertragen – ungeachtet des Ergebnisses.
- **On All Failure** – Informiert die Empfänger, dass alle Versuche, eine Ereignisdatei an EMC zu übertragen, fehlgeschlagen sind.

4. Geben Sie im Feld **SMTP Host (Email Server)** den Hostnamen oder die IPv4-Adresse des Mailservers ein.
5. Geben Sie in das Feld **Email Address** einen oder mehrere Empfänger dieser E-Mails ein. Trennen Sie mehrere E-Mail-Adressen durch Kommata.
6. Geben Sie im Feld **Email Sender Address** die E-Mail-Adresse ein, von der die Benachrichtigung gesendet wird.
7. (Optional) Klicken Sie zur Festlegung erweiterter Einstellungen auf **Advanced** und legen Sie anschließend die Einstellungen im Dialogfeld **Edit Advanced Email Settings** fest:
   a. Geben Sie im Feld **Retries** die Anzahl der Wiederholungsversuche an, bevor eine Fehlermeldung ausgegeben wird. Die Standardeinstellung ist fünf Versuche.
   b. Geben Sie im Feld **Timeout** die Anzahl der Sekunden, bevor eine Meldung ausgegeben wird, dass die Zeit für diesen Vorgang überschritten wurde. Die Standardeinstellung ist 300 Sekunden (5 Minuten).
   c. Geben Sie im Feld **Description** eine Beschreibung der Übertragungsmethode an, die im Fenster **Manage ConnectEMC** angezeigt wird. Die Standardbeschreibung ist `Email Transport`.
   d. Geben Sie im Feld **Email Subject** die Betreffzeile für die E-Mail an. Die Standardbetreffzeile lautet `Avamar ConnectEMC Notification Email`.

      HINWEIS

      Ändern Sie die Betreffzeile der E-Mail nur auf Anforderung des Avamar-Supports. EMC Spamfilter können E-Mail-Nachrichten mit anderen Betreffzeilen zurückweisen.

   e. Wählen Sie aus der Liste **Email Format** das Format der E-Mail aus, ASCII oder HTML. Die Standardeinstellung ist ASCII.
   f. Legen Sie fest, ob an ConnectEMC gesendete Anhänge in die E-Mail-Benachrichtigung aufgenommen werden sollen, indem Sie das Kontrollkästchen **Include CallHome Data** aktivieren oder deaktivieren.
   g. Klicken Sie auf **OK**.
8. Klicken Sie im Dialogfeld **Edit Notification Transport** auf **OK**.

Testen von Übertragungen

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage ConnectEMC** aus.

   Das Fenster **Manage ConnectEMC** wird angezeigt.
2. Klicken Sie auf **Test**.

Überprüfen der Systemintegrität

Zum Überprüfen der Avamar-Serverintegrität müssen Sie sich zuerst vergewissern, dass ein überprüfter Serverprüfpunkt vorhanden ist.

Ggf. sollten Sie auch die Serverprotokolldateien sammeln und untersuchen, um sich zu vergewissern, dass während der Durchführung des Kontrollpunkts keine Fehler aufgetreten sind. Anweisungen finden Sie unter Anzeigen der Protokolldateien des Avamar-Servers auf Seite 313.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Server Management**.
3. Wählen Sie den Avamar-Servernamen im linken Bereich aus.
4. Überprüfen Sie, ob im Feld **Last validated checkpoint** ein aktuelles Kalenderdatum angezeigt wird.

KAPITEL 10

Kapazitätsmanagement

In diesem Kapitel werden folgende Themen behandelt:

Informationen zur Kapazitätsauslastung

Zeigen Sie Informationen zur Kapazitätsauslastung in Echtzeit für einen einzelnen Server in Avamar-Administrator oder für mehrere Server in Backup and Recovery Manager an.

In Avamar-Administrator stehen im Bereich **Capacity** des Avamar Administrator-Dashboards und auf der Registerkarte **Server Management** im Fenster **Server** Informationen zur Kapazitätsauslastung für einen einzelnen Avamar-Server zur Verfügung.

Informationen zur Kapazitätsauslastung für mehrere Server stehen über Backup and Recovery Manager zur Verfügung. Informationen zu dieser Funktion finden Sie in der Backup and Recovery Manager-Produktdokumentation.

Kapazitätsbegrenzungen und Schwellenwerte

In der folgenden Tabelle wird das Verhalten eines Avamar-Servers bei der Überschreitung verschiedener belegter Speicherschwellenwerte erläutert.

Tabelle 78 Kapazitätsbegrenzungen und Schwellenwerte

Speicherauslastung	Status	Beschreibung
Weniger als 75 %		Das System ist dafür ausgelegt, über ausreichend Kapazität zum Speichern zukünftiger Backups zu verfügen.
75 %		Überprüfen Sie die Speicherauslastung, um zu ermitteln, ob der Server über ausreichend Kapazität zum Speichern zukünftiger Backups verfügt.
80 %		Eine Pop-up-Benachrichtigung warnt Sie davor, dass 80 % der verfügbaren Speicherkapazität des Servers belegt sind. Überprüfen Sie die Speicherauslastung, um zu ermitteln, ob der Server über ausreichend Kapazität zum Speichern zukünftiger Backups verfügt.
90 %		Überprüfen Sie die Speicherauslastung, um zu ermitteln, ob der Server über ausreichend Kapazität zum Speichern zukünftiger Backups verfügt.

Tabelle 78 Kapazitätsbegrenzungen und Schwellenwerte (Fortsetzung)

Speicherauslastung	Status	Beschreibung
95 %		Der Server hat das Standardlimit für die Integritätsprüfung erreicht, d. h. die Menge der Speicherkapazität, die verwendet werden kann und gleichzeitig einen „fehlerfreien“ Server beibehält. Avamar schließt alle laufenden Backups ab, der Dispatcher beendet jedoch alle neuen Backupaktivitäten. Wenn Sie sich bei Avamar Administrator anmelden, wird eine Benachrichtigung angezeigt. Bestätigen Sie das Systemereignis, damit zukünftige Backupaktivitäten wieder aufgenommen werden. Sie können das Limit für die Integritätsprüfung anpassen, die Einstellung des Limits über 95 % wird jedoch nicht empfohlen. Anweisungen finden Sie unter Anpassen der Kapazitätsbegrenzungen und des Verhaltens auf Seite 328.
100 %		Der Server hat das schreibgeschützte Limit erreicht und wechselt automatisch in den schreibgeschützten Modus, um die Integrität der bereits auf dem Server gespeicherten Daten zu schützen. Falls ConnectEMC aktiviert wurde, wird ein Service-Request (SR) protokolliert. Besuchen Sie den Avamar-Support, um bestehende SRs für das System anzuzeigen. Durchsuchen Sie die Wissensdatenbank nach „Avamar User and OS Capacity Management solution esg118578.“

Kapazitätsprognose

Jeder Avamar-Server überwacht und analysiert fortlaufend die Rate, mit der die Speicherkapazität verbraucht wird, und prognostiziert, wie lange die Speicherkapazität zu dieser Rate verbraucht werden kann. Diese Prognose wird im Hintergrund ausgeführt.

Die Ergebnisse der Kapazitätsprognose für Avamar-Server und konfigurierte Data Domain-Systeme sind im Bereich „Capacity“ von Avamar-Administrator verfügbar. Weitere Informationen finden Sie unter Bereich „Capacity“ auf Seite 48.

Anpassen der Kapazitätsbegrenzungen und des Verhaltens

Bearbeiten Sie die Avamar-Administrator-Voreinstellungsdatei, um die Einstellungen anzupassen, mit denen die Kapazitätsbegrenzungen und das Systemverhalten gesteuert werden.

Bearbeiten von Kapazitätseinstellungen für Avamar-Administrator

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
2. Fahren Sie den Management Console Server (MCS) herunter, indem Sie den folgenden Befehl eingeben:

   ```
   dpnctl stop mcs
   ```
3. Wechseln Sie das Verzeichnis, indem Sie den folgenden Befehl eingeben:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```
4. Öffnen Sie `mcserver.xml` in einem Texteditor.
5. Suchen Sie nach dem Abschnitt `com.avamar.mc.mcsm` der Voreinstellungsdatei.
6. Bearbeiten Sie die folgenden Einstellungen.

Tabelle 79 Kapazitätseinstellungen in der Datei „mcserver.xml“

Einstellung	Beschreibung	Standardwert
`capErrPercent`	Wenn die Kapazitätsauslastung diesen Prozentsatz erreicht, ist das Kapazitätsstatussymbol rot.	95 %

Tabelle 79 Kapazitätseinstellungen in der Datei „mcserver.xml“ (Fortsetzung)

Einstellung	Beschreibung	Standardwert
capForecastDataDays	Menge der für die Prognose verwendeten historischen Kapazitätsauslastungsdaten	30 Tage
capForecastDataMinDays	Mindestmenge der für die Prognose erforderlichen historischen Kapazitätsauslastungsdaten	14 Tage
capForecastReachedDays	Wenn die prognostizierte Kapazität unter dieser Anzahl an Tagen liegt, beginnt Avamar-Administrator mit dem Generieren von Ereignissen, die eine Quittierung erfordern, und bei der Anmeldung werden Pop-up-Warnmeldungen angezeigt.	30 Tage
capMonitorIntervalMin	Diese Einstellung steuert, wie oft Avamar-Administrator die prognostizierte Kapazität prüft.	1 Tag (täglich)
capReachedPercentage	Wenn die Gesamtauslastung der Kapazität diesen Prozentschwellenwert erreicht, generiert Avamar-Administrator die Ereignisbenachrichtigung, dass das System voll ist.	95 %
capWarnPercent	Wenn die Kapazitätsauslastung diesen Prozentsatz erreicht, ist das Kapazitätsstatussymbol gelb.	80 %
hcMonitorIntervalMin	Diese Einstellung steuert, wie oft Avamar-Administrator eine Integritätsprüfung durchführt (d. h., wie oft überprüft wird, ob die belegte Kapazität das Limit für die Integritätsprüfung erreicht hat).	1 Tag (täglich)
hcOffsetROPercentage	Von der Serverbeschränkung durch Schreibschutz (100 %) abgezogener Prozentsatz, durch den sich das Limit für die Integritätsprüfung ergibt.	5 %
hcReminderIntervalMin	Diese Einstellung steuert, wie oft Avamar-Administrator	60 Minuten (jede Stunde)

Tabelle 79 Kapazitätseinstellungen in der Datei „mcserver.xml“ (Fortsetzung)

Einstellung	Beschreibung	Standardwert
	Ereignisse und Pop-up-Warnmeldungen ausgibt, sobald das Limit für die Integritätsprüfung erreicht wurde.	

7. Speichern Sie die Änderungen und schließen Sie die Datei.
8. Starten Sie den MCS und den Scheduler, indem Sie Folgendes eingeben:

```
dpnctl start mcs
dpnctl start sched
```

KAPITEL 11

Replikation

In diesem Kapitel werden folgende Themen behandelt:

Übersicht über die Avamar-Replikation

Der Avamar-Replikationsprozess kopiert Clientbackups von einem Avamar-Quellsystem auf ein Zielsystem.

Durch die Replikation wird der Verlust von Daten verhindert, wenn das Avamar-System ausfällt, da Kopien der Backups (Replikate) auf dem Zielsystem gespeichert werden.

Replikationstypen

Avamar unterstützt die Policy-basierte Replikation und die Befehlszeilenreplikation.

Policy-basierte Replikation
Die Policy-basierte Replikation bietet eine größere Kontrolle über den Replikationsprozess. Bei der Policy-basierten Replikation können Sie *Replikationsgruppen* in Avamar-Administrator erstellen, um die folgenden Replikationseinstellungen zu definieren:

- Mitglieder von Replikationsgruppen, entweder Domains oder Clients
- Prioritätsreihenfolge der Replikationsaufgaben
- Zu replizierende Backups, basierend auf der Aufbewahrungseinstellung oder dem Backupdatum
- Maximale Anzahl der für jeden Client zu replizierenden Backups
- Zielsystem für die Replikate
- Replikationsplanung
- Aufbewahrung von Replikaten

Replikation über die Befehlszeile
Die On-Demand-Replikation führen Sie über die Befehlszeile durch, indem Sie sich am Utility-Node anmelden und die Befehlszeilenoberfläche (CLI) `avrepl` verwenden. Die Replikation über die Befehlszeile bietet größere Kontrolle über den Replikationsprozess. Mit den Optionen für den Befehl `avrepl` werden die folgenden Replikationseinstellungen definiert:

- Zu replizierende Domains oder Clients
- Zu replizierende Backups, basierend auf:
  - Für das Backup verwendetes Plug-in
  - Aufbewahrungseinstellung für das Backup
  - Backupdatum
- Maximale Anzahl der für jeden Client zu replizierenden Backups
- Zielsystem für die Replikate
- Aufbewahrung von Replikaten

Replikationsplanung

Die Methode für die Planung von Replikationsaufgaben richtet sich nach dem verwendeten Replikationstyp. Für die Policy-basierte Replikation definieren Sie Planungen auf ähnliche Weise wie Backuppläne. Für die Befehlszeilenreplikation wird

kein Plan definiert, da eine Replikationsaufgabe manuell durch Ausführen des Befehls `avrepl` auf dem Utility-Node gestartet wird.

Definieren einer Planung für die Policy-basierte Replikation
Zum Konfigurieren von Planungen für die Policy-basierte Replikation wählen Sie **Extras** > **Planungen managen** aus, um das Fenster **Alle Planungen managen** zu öffnen. Definieren Sie in diesem Fenster einen Zeitplan für den automatischen Start der Replikationsaufgaben in täglichen, wöchentlichen oder monatlichen Intervallen. Es ist ebenfalls möglich, eine On-Demand-Planung zu erstellen, die nicht automatisch ausgeführt wird.

Die Planung umfasst eine Startzeit und eine Endzeit zur Angabe des Replikationsfensters.

Zeitzonenhinweise
Beachten Sie bei Verwendung von Avamar-Administrator zur Planung von Replikationsaufgaben, dass die Startzeit in der Zeitzone des Computers angezeigt wird, auf dem Avamar-Administrator ausgeführt wird. Die Startzeit wird nicht in der Zeitzone des Quellsystems oder in der Zeitzone des Zielsystems angezeigt.

Erwägen Sie beispielsweise die Verwendung von Avamar-Administrator in der Zeitzone PT mit einem Quellsystem in der Zeitzone ET. Das Quellsystem kompensiert die 3-Stunden-Differenz zwischen den beiden Zeitzonen. Eine Startzeit von 20:00 Uhr PT, die in Avamar-Administrator angegeben wird, bedeutet, dass das Quellsystem die Replikationsaufgabe um 23:00 Uhr ET beginnt.

Best Practices für die Replikationsplanung
Planen Sie Replikationsaufgaben für Zeiträume mit geringer Backupaktivität, damit die größtmögliche Anzahl von Clientbackups während jeder Replikationssitzung erfolgreich repliziert wird. Bei diesen Planungsüberlegungen wird der Tatsache Rechnung getragen, dass nur abgeschlossene Clientbackups repliziert werden.

Ziehen Sie bei der Policy-basierten Replikation die Größe jeder Replikationsgruppe in Betracht, sodass alle Backups während jeder geplanten Replikationsaufgabe erfolgreich repliziert werden. Wenn eine Gruppe so groß wird, dass die Backups nicht alle erfolgreich repliziert werden, bearbeiten Sie die Planung, sodass mehr Zeit zur Verfügung steht, oder teilen Sie die Gruppe in kleinere Gruppen auf, die separat ausgeführt werden.

Replikationsauthentifizierung

Geben Sie gültige Anmeldedaten für ein Konto auf dem Zielsystem an, wenn Sie die Policy-basierte Replikation konfigurieren. Geben Sie bei der Befehlszeilenreplikation gültige Anmeldedaten für das Avamar-Quellsystem und für das Zielsystem an der Eingabeaufforderung an.

Geben Sie für eine Policy-basierte Replikation die Anmeldedaten an, wenn Sie ein Zielsystem auf der Registerkarte **Destinations** im Fenster **Data Movement Policy** hinzufügen.

Zur Replikation über die Befehlszeile geben Sie das Benutzerkonto und das Passwort für das Zielsystem mithilfe der Optionen `--[replscript]dstid` und `--dstpassword` an. Verwenden Sie die Optionen `--[avtar]id` und `--password`, um das Benutzerkonto und das Passwort für das Quellsystem anzugeben.

Im Avamar-Quellsystem ist das Konto `repluser` das Standardkonto für die Replikation. Bei Verwendung des `repluser`-Kontos zur Replikation über die Befehlszeile lassen Sie die Option `--[avtar]id` im Befehl wegfallen und geben Sie das Passwort für das `repluser`-Konto mit der Option `--password` an. Im *Avamar –*

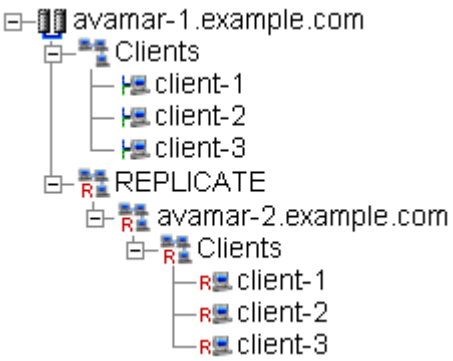
Produktsicherheitshandbuch finden Sie eine vollständige Liste der standardmäßigen Konten und Passwörter auf dem Avamar-Server.

Speicherort der Replikate auf einem Avamar-Zielsystem

Auf einem Avamar-Zielsystem sind Replikate in der Domain `REPLICATE` verfügbar. Diese Domain enthält eine Duplikatdarstellung der Clienthierarchie auf dem Avamar-Quellsystem.

In der folgenden Abbildung enthält das Avamar-Zielsystem `avamar-1.example.com` sowohl lokale Clients als auch Replikate vom Quellserver `avamar-2.example.com`.

Abbildung 16 Struktur einer Replikationsdomain – Beispiel



Alle Daten in der Domain `REPLICATE` sind schreibgeschützt. Sie können nur die folgenden Vorgänge für Replikate in der Domain `REPLICATE` durchführen:

- Ändern des Ablaufdatums des Replikats
- Anzeigen der Backupstatistiken
- Löschen eines Replikats

Replikate auf Quelle (Replicas at Source) auf Seite 334beschreibt die Funktion „Replicas at Source“, die das Management von Replikaten über den als Replikationsquelle fungierenden Avamar-Server anstelle der Domain `REPLICATE` des Zielsystems ermöglicht.

Replikate auf Quelle (Replicas at Source)

Mit der Funktion „Replicas at Source“ können Sie Replikate mithilfe einer Avamar-Administrator-Sitzung auf dem Avamar-Server, der die Replikationsquelle darstellt, anzeigen und managen.

Funktionen

Die Funktion „Replicas at Source“ ist in Avamar-Serverversion 7.2 und höher enthalten. Aktivieren der Funktion „Replikate auf Quelle“ auf Seite 338 beschreibt, wie die Funktion aktiviert wird.

In der folgenden Tabelle werden die Funktionen beschrieben, die „Replicas at Source“ auf dem Avamar-Quellserver bietet.

Tabelle 80 Über den Avamar-Quellserver verfügbare Funktionen von „Replicas at Source“

Funktion	Beschreibung
Replikate auf der Registerkarte „Restore“ anzeigen	Replikate werden zusammen mit Backups auf der Registerkarte **Restore** des Fensters

Tabelle 80 Über den Avamar-Quellserver verfügbare Funktionen von „Replicas at Source“ (Fortsetzung)

Funktion	Beschreibung
	Backup, Restore and Manage in Avamar-Administrator angezeigt.
Replikateinstellungen managen	Verwenden Sie Avamar-Administrator oder die Befehlszeilenoberfläche, um die folgenden Aktionen für ein Replikat durchzuführen: • Ablaufdatum ändern • Aufbewahrungseinstellung ändern • Delete • Validieren • Statistiken anzeigen
Von Replikat wiederherstellen	Wählen Sie mit den gleichen Methoden, die für Backups zur Verfügung stehen, ein Replikat aus und stellen Sie die Daten wieder her.
Regelmäßige Synchronisation	Das Avamar-Quellsystem führt in regelmäßigen Abständen eine Synchronisation mit jedem aktiven Zielsystem durch. Das Standardintervall zwischen Synchronisationen beträgt 12 Stunden. Kürzlich vorgenommenen Änderungen werden möglicherweise eine Zeit lang nicht berücksichtigt. Die Synchronisation umfasst die folgenden Aktionen: • Änderungen an Ablaufeinstellungen übernehmen • Änderungen an Aufbewahrungseinstellungen übernehmen • Lokale Auflistung löschen, wenn kein Replikat auf dem Remoteziel vorhanden ist • Lokale Auflistung hinzufügen, wenn ein nicht aufgelistetes Replikat auf dem Remoteziel gefunden wurde

Hinweis

Die Funktion „Replicas at Source“ unterstützt keine Replikate von Backups virtueller Maschinen.

Integration

Die Funktion „Replicas at Source“ in mehrere Avamar-Aufgaben integriert. Die Abschnitte, in denen diese Aufgaben erläutert werden, enthalten Informationen über die Integration der Funktionen „Replicas at Source“. Die folgende Tabelle bietet einen Überblick über die Integration der Funktionen „Replicas at Source“.

Tabelle 81 Beschreibungen der Integration der Funktionen von „Replicas at Source“ Avamar-Aufgaben

Aufgabe	Beschreibung
Remotezielmanagement	Verhindert das Löschen eines Remoteziels vom Avamar-Quellserver, wenn Replikate vom Avamar-Quellserver auf dem Zielsystem vorhanden sind. Umfasst eine Option zum Außerkraftsetzen, um das Löschen des Remoteziels zu erzwingen und alle Replikate des Quellservers vom Zielsystem zu löschen.
Restore	Replikate werden zusammen mit Backups auf der Registerkarte **Restore** des Fensters **Backup, Restore and Manage** in Avamar-Administrator aufgeführt. Wenn ein Backup auf dem Avamar-Quellsystem existiert und Replikate auf den Remotezielsystemen vorhanden sind, verwendet das Avamar-System das Backup für die Wiederherstellung.
Client stilllegen	Beim Stilllegen eines Clients bietet die Funktion „Replicas at Source“ weitere Wahlmöglichkeiten im Zusammenhang mit der Aufbewahrung und dem Ablauf von Replikaten.
Client löschen	Beim Löschen eines Clients bietet die Funktion „Replicas at Source“ eine Option, mit der auch die Replikate des Clients gelöscht werden können.
Serviceadministration	Fügt den externen Backupmanagerservice auf der Registerkarte **Services Administration** im Fenster **Administration** in Avamar-Administrator hinzu. Der Service umfasst die folgenden standardmäßigen Serviceaktionen: Starten, Beenden, Neustarten und Eigenschaften anzeigen. Wenn der externe Backupmanagerservice angehalten wird, verhindert Avamar-Administrator das Management von Replikaten durch „Replicas at Source“.
MCS	Der Datei `mcserver.xml` werden durch „Replicas at Source“ anpassbare Einstellungen hinzugefügt.
MCCLI	Der Ausgabe von `mccli backup show` werden durch „Replicas at Source“ Hostnamen- und Standortinformationen hinzugefügt. Zudem stellt „Replicas at Source“ die Option `--location` zur Verfügung, um Replikate zu ermitteln, wenn einer oder mehrere der folgenden Befehle ausgeführt werden:

Tabelle 81 Beschreibungen der Integration der Funktionen von „Replicas at Source“ Avamar-Aufgaben (Fortsetzung)

Aufgabe	Beschreibung
	• `mccli backup validate` • `mccli backup delete` • `mccli backup edit` • `mccli backup restore`

Aufbewahrung von Replikaten

Beim Replizieren von Backups gilt die Aufbewahrungseinstellung für das Backup auf dem Avamar-Quellsystem automatisch für das Replikat auf dem Zielsystem. Sie können die Aufbewahrungseinstellung für das Replikat jedoch ändern.

Festlegen der Aufbewahrungseinstellungen vor der Replikation
Geben Sie für die Policy-basierte Replikation eine andere Aufbewahrungseinstellung für Replikate auf der Seite **Expiration** an, wenn Sie die Replikationsgruppe konfigurieren.

Für eine Replikation über die Befehlszeile verwenden Sie die Option `--[avtar]expires`, um eine andere Aufbewahrungseinstellung für Replikate anzugeben.

Festlegen der Aufbewahrungseinstellungen nach der Replikation
Aktivieren Sie die Funktion „Replicas at Source“, um in einer Avamar-Administrator-Sitzung auf dem Avamar-Quellserver die Aufbewahrung von Replikaten auf dem Zielsystem festzulegen.

Oder melden Sie sich über Avamar-Administrator bei einem Avamar-Zielsystem an und ändern Sie das Ablaufdatum des Replikats manuell, nachdem die Replikation durchgeführt wurde. Ändern des Ablaufdatums für ein Backup auf Seite 143 bietet Anweisungen zum Ändern der Aufbewahrungseinstellungen für Backups. Diese Anweisungen gelten gleichermaßen für Replikate auf einem Avamar-System.

Replikation mit Data Domain-Systemen

Wenn ein Avamar-System Backups auf einem Data Domain-System speichert, verwendet die Avamar-Replikation DD Boost zum Kopieren von Backups vom ursprünglichen Data Domain-System und zum Erstellen von Replikaten auf einem anderen Data Domain-System.

Unterstützte Replikationskonfigurationen
In der folgenden Tabelle sind die unterstützten Replikationskonfigurationen für die Avamar-Replikation mit DD Boost aufgeführt.

Tabelle 82 Replikationskonfigurationen für die Avamar-Replikation mit DD Boost

Backupspeicher	Replikationsspeicher
Einzelnes Data Domain-System	Einzelnes Data Domain-System
Einzelnes Data Domain-System	Mehrere Data Domain-Systeme

Tabelle 82 Replikationskonfigurationen für die Avamar-Replikation mit DD Boost (Fortsetzung)

Backupspeicher	Replikationsspeicher
Mehrere Data Domain-Systeme	Einzelnes Data Domain-System
Mehrere Data Domain-Systeme	Mehrere Data Domain-Systeme

In einer Konfiguration, in der der Replikationsspeicher aus mehreren Data Domain-Systemen besteht, können Sie das System steuern, das die Replikate erhält, indem Sie eine Domain auf dem Avamar-Quellserver einem Data Domain-Zielsystem zuordnen. Legen Sie das Data Domain-System mit dem Standardziel fest. Avamar führt die Replikation zum Standardziel durch, wenn kein Data Domain-Zielsystem auf der Registerkarte **Storage Mapping** des Fensters **Data Movement Policy** in Avamar-Administrator angegeben ist.

Im *Avamar und Data Domain-System – Integrationshandbuch* erhalten Sie Anweisungen zur Speicherzuordnung und zum Angeben des standardmäßigen Data Domain-Zielsystems.

Replikationsdetails

Die folgenden Details gelten für die Avamar-Replikation mit Data Domain-Systemen:

- Die Datenübertragung während der Replikation erfolgt zwischen den Data Domain-Systemen, ohne zwischengeschaltete Bereitstellung.
- Bei der Replikation wird DD Boost zum Kopieren von Backups und zum Schreiben von Replikaten verwendet.
- Eine Data Domain-Replikationslizenz ist erforderlich.
- Keine Verwendung der Data Domain-Replikation.
- Die Replikation wird auf dem Avamar-Server konfiguriert und überwacht.
- Bei der Planung von Replikationsaufgaben wird nur die Avamar-Replikationsplanung verwendet.
- Es werden keine Data Domain-Administrationstools verwendet.

Aktivieren der Funktion „Replikate auf Quelle“

Die Funktion „Replicas at Source“ ist in Avamar-Serverversion 7.2 und höher enthalten. Zum Aktivieren dieser Funktion ändern Sie die Datei `mcserver.xml` und starten Sie dann den Remote Backup Manager Service.

Bevor Sie beginnen

Installieren Sie die Avamar-Serversoftware 7.2 oder höher oder führen Sie ein Upgrade auf diese Version durch.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. Stoppen Sie den MCS, indem Sie den folgenden Befehl eingeben:

   ```
   dpnctl stop mcs
   ```

3. Wechseln Sie mit folgendem Befehl das Arbeitsverzeichnis:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

4. Öffnen Sie `mcserver.xml` in einem Texteditor.
5. Legen Sie im Containerelement `repl` den Wert des Parameters `allow_dest_replica_management` auf **`true`** fest.

   Der Standardwert ist `false`.

6. Legen Sie im Containerelement `repl` den Wert des Parameters `show_external_backups` auf **`true`** fest.

   Der Standardwert ist `true`.

7. Legen Sie im Containerelement `repl` den Wert des Parameters `allow_manage_remote_backups_at_source` auf **`true`** fest.

   Der Standardwert ist `true`.

8. Speichern Sie die Änderung und schließen Sie die Datei.
9. Starten Sie den MCS und den Scheduler, indem Sie Folgendes eingeben:

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

10. Melden Sie sich bei Avamar-Administrator auf dem Avamar-Server an, der für die Clientbackups vorgesehen ist (Quellserver).
11. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

    Das Fenster **Administration** wird angezeigt.

12. Klicken Sie auf die Registerkarte **Services Administration**.
13. Klicken Sie mit der rechten Maustaste auf den **Remote Backup Manager Service** und wählen Sie **Start** aus.

Ergebnisse

Der Avamar-Server aktiviert die Funktion „Replicas at Source“.

Konfigurieren der Policy-basierten Replikation

Zur Vorbereitung der Policy-basierten Replikation müssen bestimmte Aufgaben durchgeführt werden.

Bevor Sie beginnen

Melden Sie sich bei Avamar-Administrator auf dem Avamar-Server an, der für die Clientbackups vorgesehen ist (Quellserver).

Die folgenden Schritte bieten Ihnen einen Überblick über die Reihenfolge der Aufgaben, die zum Konfigurieren der Policy-basierten Replikation durchgeführt werden müssen. Jeder Schritt wird in einem separaten Abschnitt, der sich mit der Aufgabe beschäftigt, näher erläutert.

Vorgehensweise

1. Fügen Sie in Avamar-Administrator ein Replikationsziel für jedes System hinzu, das Replikate vom Quellserver speichert (Zielsystem).

   Replikationsziele auf Seite 340 bietet Informationen zu Replikationszielen, darunter auch Angaben dazu, wie ein Zielsystem hinzugefügt wird.

2. Erstellen Sie in Avamar-Administrator tägliche, wöchentliche oder monatliche Zeitpläne für die Replikationsplanung.

   In Avamar ist das Erstellen einer Replikationsplanung identisch mit dem Erstellen einer Backupplanung. Planungen auf Seite 114 beschreibt Avamar-Planungen und Verfahrensweisen zu ihrer Erstellung.

3. Erstellen Sie in Avamar-Administrator eine oder mehrere Replikationsgruppen, um die Einstellungen für die Policy-basierte Replikation zu definieren.

   Replikationsgruppen auf Seite 343 bietet Informationen zu Replikationsgruppen, darunter auch Angaben dazu, wie eine Replikationsgruppe erstellt wird.

Replikationsziele

Fügen Sie Replikationsziele hinzu, um mit der Konfiguration der Policy-basierten Replikation auf einem Avamar-Server zu beginnen.

Stellen Sie Verbindungsinformationen für ein unterstütztes Datenspeichersystem zur Verfügung, um dieses als Replikationsziel hinzuzufügen.

Avamar unterstützt die Replikation auf andere Avamar-Systeme und auf Data Domain-Systeme über DD Boost. Ein Avamar-System kann auf ein anderes Avamar-System replizieren, auf dem eine andere Version der Avamar-Serversoftware ausgeführt wird. Die besten Ergebnisse werden jedoch mit der gleichen Serversoftwareversion erzielt.

Hinzufügen eines Avamar-Systems als Replikationsziel

Geben Sie Verbindungsinformationen für ein Avamar-System an, um es als Replikationsziel hinzuzufügen.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Data Movement Policy**Link zum Startprogramm.

   Das Fenster **Data Movement Policy** wird angezeigt.

2. Wählen Sie die Registerkarte **Destinations** aus.
3. Wählen Sie **Actions** > **New Destination** aus.

   Das Dialogfeld **New Replication Destination** wird angezeigt.

4. Geben Sie in das Feld **Name** einen Referenznamen für das Avamar-Zielsystem ein.
5. Wählen Sie im Feld **Destination server type** die Option **Replicate** aus.
6. Wählen Sie unter **Encryption** eine Verschlüsselungsstufe aus.

   Die ausgewählte Verschlüsselungsstufe gilt für die Übertragung von Replikationsdaten mit dem Avamar-Zielsystem. Die Standardeinstellung ist „High“ und sollte nur geändert werden, wenn die Quelle für die Verwendung von Authentifizierung konfiguriert ist und das Ziel keine Authentifizierung verwendet. In diesem Fall sollte „None“ festgelegt werden.

7. Geben Sie unter **Target server address** den DNS-Namen oder die IP-Adresse des Avamar-Zielsystems ein.
8. Geben Sie unter **Target server connection port** die Nummer des ausgehenden Ports auf dem Avamar-Quellsystem aus, die bei der Kommunikation mit dem Avamar-Zielsystem verwendet werden soll.

   Der standardmäßige Portwert ist 27000.

   Wenn Sie **High** unter **Encryption** auswählen, wird ein Offset für den Port festgelegt, damit Verbindungen über Firewalls zulässig sind. Der Standardoffset ist +2000. Eine manuelle Änderung ist möglich, indem Sie die `secured_port_offset`-Voreinstellung in `mcserver.xml` bearbeiten und dann den MCS neu starten.
9. Geben Sie unter **Target MCS connection port** die Nummer des eingehenden Ports auf dem Avamar-Zielserver ein, die für Datenverbindungen mit dem MCS auf dem Zielsystem verwendet werden soll.

   Der standardmäßige Portwert ist 28001.
10. Geben Sie unter **User ID on target server** einen Benutzernamen für ein Konto auf dem Avamar-Zielsystem ein, das über die Berechtigungen `backup` und `admin` verfügt.

    Normalerweise geben Sie **`repluser`** oder **`root`** ein.

    Hinweis

    Für einen Benutzer mit eingeschränktem Zugriff auf eine Domain unterhalb der Stammdomain (Mandantenzugriff) muss sowohl auf dem Avamar-Quellserver als auch auf dem Zielsystem die Avamar-Serverversion 7.2 oder höher ausgeführt werden.
11. Geben Sie unter **Password on target server** das Passwort für den Benutzernamen ein.
12. Klicken Sie auf **Verify Authentication**.

    Die Authentifizierung des Avamar-Quellsystems beim Avamar-Zielsystem erfolgt mit den angegebenen Einstellungen.

    Im Dialogfeld **Verifying Authentication** wird eine Ergebnismeldung angezeigt.
13. Klicken Sie im Dialogfeld **Verifying Authentication** auf **Close**.
14. Klicken Sie im Dialogfeld **New Replication Destination** auf **OK**.

Ergebnisse

Avamar-Administrator fügt das Replikationsziel der Liste auf der Registerkarte **Destinations** hinzu.

Bearbeiten eines Replikationsziels

Ändern Sie die Verbindungsinformationen für ein Replikationsziel.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Data Movement Policy**Link zum Startprogramm.

   Das Fenster **Data Movement Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Destinations**.

3. Wählen Sie das zu bearbeitende Replikationsziel aus.
4. Wählen Sie **Actions** > **Edit Destination** aus.

   Das Dialogfeld **Replication Destination** wird angezeigt.
5. Bearbeiten Sie die Einstellungen für das Replikationsziel.
6. Klicken Sie auf **OK**.

Ergebnisse

Avamar-Administrator ändert die Einstellungen des ausgewählten Replikationsziels.

Löschen eines Replikationsziel-Datensatzes

Sie können den Datensatz für ein Replikationsziel von einem Avamar-Quellsystem löschen.

Wenn „Replicas at Source“ aktiviert ist, prüft das Avamar-System, ob Replikate auf dem Replikationszielsystem vorhanden sind. Sind mit dem Avamar-Quellsystem verbundene Replikate vorhanden, verhindert Avamar-Administrator, dass der Datensatz des Replikationsziels gelöscht wird. Setzen Sie diese Einstellung außer Kraft, um den Replikationsziel-Datensatz selbst dann zu löschen, wenn Replikate vorhanden sind.

Wenn „Replicas at Source“ deaktiviert ist, prüft das Avamar-System vor dem Löschen des Replikationsziel-Datensatzes nicht, ob Replikate auf dem Replikationszielsystem vorhanden sind. Alle existierenden Replikate verbleiben auf dem Replikationszielsystem, bis sie ablaufen oder bis sie über die Zielsystemschnittstelle gelöscht werden.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Data Movement Policy**Link zum Startprogramm.

   Das Fenster **Data Movement Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Destinations**.
3. Wählen Sie den zu löschenden Replikationsziel-Datensatz aus.
4. Wählen Sie **Actions** > **Delete Destination** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
5. Klicken Sie auf **Yes**.

Replikate auf Quelle (Replicas at Source)	Result
Aktiviert	Das Avamar-System prüft, ob auf dem Replikationszielsystem Replikate vorhanden sind. Wenn dies nicht der Fall ist, wird der Replikationsziel-Datensatz gelöscht. Um zu verhindern, dass das Avamar-System prüft, ob Replikate vorhanden sind, und um den Replikationsziel-Datensatz selbst dann zu löschen, wenn Replikate auf dem Replikationszielsystem vorhanden sind, deaktivieren Sie die Option **Check for remote backups before deletion** und klicken Sie dann auf **Yes**.
Deaktiviert	Das Avamar-System löscht den Replikationsziel-Datensatz.

Replikationsgruppen

Replikationsgruppen ermöglichen Ihnen, die Einstellungen für Policy-basierte Replikation zu definieren.

Die Replikationsgruppenoption umfasst Folgendes:

- Die Domain- und Clientmitglieder der Replikationsgruppe
- Die zu replizierenden Backuptypen
- Die Anzahl der zu replizierenden Backups
- Den Zielserver
- Die Replikationsplanung
- Aufbewahrungsdauer replizierter Backups auf dem Zielserver

Sie können die Priorität in Bezug auf die zuerst zu replizierenden Backupdaten festlegen. Beim Definieren der Mitglieder der Replikationsgruppe wird durch die Reihenfolge, in der die Mitglieder in der Liste **Member(s)** aufgeführt sind, die Reihenfolge gesteuert, in der die Backupdaten repliziert werden.

Backupdaten für einen Client werden nur einmal repliziert, selbst wenn ein Client einzeln aufgelistet wird und auch ein Mitglied einer Domain in der Liste **Member(s)** ist.

Wenn ein einzelner Client eine höhere Priorität in der Liste **Member(s)** aufweist als die Domain, werden die Backupdaten für den einzelnen Client außerdem vor den Backupdaten der anderen Clients in der Domain repliziert.

Erstellen einer Replikationsgruppe

Bevor Sie beginnen

- Fügen Sie der Konfiguration auf dem Avamar-Quellserver einen Avamar-Zielserver hinzu.
- (Optional) Planen Sie, wann die Replikation für die Gruppe erfolgen soll. Anweisungen finden Sie unter Erstellen einer Planung auf Seite 117.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Data Movement Policy**Link zum Startprogramm.

   Das Fenster **Data Movement Policy** wird angezeigt.
2. Wählen Sie die Registerkarte **Groups** aus.
3. Wählen Sie **Actions** > **New Group** > **Replication** aus.

   Der Assistent **New Replication Group** wird mit der Seite **General** geöffnet.
4. Geben Sie im Feld **Replication group name** einen Namen für die Replikationsgruppe ein.
5. Legen Sie fest, ob die Replikation für die Replikationsgruppe aktiviert oder deaktiviert werden soll:
   - Aktivieren Sie das Kontrollkästchen **Disabled**, um die Replikation für die Replikationsgruppe zu deaktivieren.
   - Lassen Sie das Kontrollkästchen leer, um die Replikation für die Replikationsgruppe zu aktivieren.
6. Wählen Sie aus der Liste **Encryption method** die Verschlüsselungseinstellung für Datenübertragungen zwischen den Quell- und Zielservern aus.

Die genaue Verschlüsselungstechnologie und die Bitstärke für eine Verbindung sind von mehreren Faktoren abhängig, u. a. von der Serverplattform und der Avamar-Serverversion. Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.

7. Klicken Sie auf **Next**.

   Die Seite **Source** wird angezeigt.

8. Führen Sie die folgenden Schritte für die Mitglieder in einer Replikationsgruppe aus.

Mitglieder in der Replikationsgruppe	Schritte
Alle Clients	Wählen Sie **Replicate all client backups** aus.
Bestimmte Domains oder Clients	a. Wählen Sie **Choose specific client(s) and/or domain(s) to replicate** aus. b. Klicken Sie auf **Choose Membership**. Das Dialogfeld **Replication Group Membership** wird angezeigt. c. Aktivieren Sie die Kontrollkästchen neben den Domains oder Clients, die der Replikationsgruppe hinzugefügt werden sollen. Ausgewählte Mitglieder werden in der Liste **Member(s)** angezeigt. d. Legen Sie die Replikationspriorität für die Replikationsgruppenmitglieder fest, indem Sie die Reihenfolge steuern, in der Domains und Clients in der Liste **Member(s)** angezeigt werden. Markieren Sie die Mitglieder in der Liste und verschieben Sie sie in der Liste mithilfe der Pfeilschaltflächen. e. Um ein Mitglied aus der Replikationsgruppe zu entfernen, wählen Sie das Mitglied in der Liste **Member(s)** aus und klicken Sie dann auf **X**. f. Klicken Sie auf **Finish**.

9. Führen Sie die folgenden Schritte für den Typ der zu replizierenden Backups aus.

Typ der zu replizierenden Backups	Schritte
Alle Backups von allen Mitgliedern der Replikationsgruppe	Wählen Sie **Replicate all backups** aus.
Bestimmte Backups	a. Wählen Sie **Include/exclude backups by type, date, and more** aus. b. Klicken Sie auf **Change Filter**. Das Dialogfeld **Replication Filter Options** wird angezeigt.

Typ der zu replizierenden Backups	Schritte
	c. Wählen Sie den Typ der zu replizierenden Backups aus: **Daily**, **Weekly**, **Monthly**, **Yearly** oder **Not tagged**. Wählen Sie mindestens einen Backuptyp aus. d. Legen Sie die maximale Anzahl der zu replizierenden Backups für jeden Client fest, der ein Mitglied der Replikationsgruppe ist. Zum Replizieren aller Backups (kein Maximum) wählen Sie **No limit** aus. Zum Replizieren einer bestimmten Anzahl aktueller Backups für jeden Mitgliedsclient wählen Sie **backup(s)** aus und geben Sie dann die maximale Anzahl in der Liste an. e. Legen Sie die Datumsbeschränkungen der zu replizierenden Backups für jeden Client fest, der ein Mitglied der Replikationsgruppe ist. Um alle Backups ungeachtet des Backupzeitpunkts zu replizieren, wählen Sie **No Date Restrictions** aus. Um nur die Backups innerhalb eines aktuellen Zeitraums zu replizieren, wählen Sie „Last“ aus und legen Sie dann die zu berücksichtigenden zurückliegenden Tage, Wochen, Monate oder Jahre (unter **Day(s)**, **Weeks(s)**, **Month(s)** bzw. **Year(s)**) fest. Um nur die Backups innerhalb eines Datumsbereichs zu replizieren, wählen Sie **Range** aus und geben Sie in die Felder **From** Startdatum und -uhrzeit und/oder in die Felder **To** Enddatum und -uhrzeit ein. f. Klicken Sie auf **OK**.

10. Klicken Sie auf **Next**.

    Die Seite **Destination** wird angezeigt.

11. Wählen Sie den Zielserver aus der Liste **Where would you like to replicate backups to?** aus.

    Sie können auch einen Zielserver durch Auswahl von **New Destination** aus der Liste hinzufügen oder die Einstellungen für einen Zielserver bearbeiten, indem Sie einen Server in der Liste markieren und auf **Modify** klicken.

12. Klicken Sie auf **Next**.

    Die Seite **Expiration** wird angezeigt.

13. Legen Sie fest, wann die replizierten Backups auf dem Zielserver ablaufen sollen:

    - Damit die replizierten Backups gemäß des aktuell eingestellten Ablaufzeitpunkts ablaufen, wählen Sie **Keep current backup expiration** aus.

- Damit die replizierten Backups zu einem anderen Zeitpunkt als dem aktuell eingestellten Ablaufzeitpunkt ablaufen, wählen Sie **Set expiration by backup type** aus und legen Sie dann für jeden Backuptyp fest, wie viele Tage, Wochen, Monate oder Jahre dieser aufbewahrt werden soll.

  Wenn ein Backup mehreren Typen angehört, wird der Ablaufzeitpunkt für das replizierte Backup auf den Wert eingestellt, der für den Backuptyp mit der längsten Dauer festgelegt wurde. Wenn es sich bei einem Backup beispielsweise um ein tägliches und monatliches Backup handelt, wird der Ablaufzeitpunkt für das replizierte Backup auf den Wert eingestellt, den Sie für monatliche Backups angeben.

14. Klicken Sie auf **Next**.

    Die Seite **Schedule** wird angezeigt.

15. Wählen Sie die Replikationsplanung aus der Liste **How often would you like this replication to run?** aus.

    Sie können auch eine Planung durch Auswahl von **New Schedule** aus der Liste erstellen oder die Einstellungen für eine Planung durch Auswahl der Planung aus der Liste und Klicken auf **Modify** bearbeiten.

16. Klicken Sie auf **Next**.

    Die Seite **Order** wird angezeigt.

17. Wenn mithilfe poolbasierter Replikation mehrere parallele Replikationsbackups aus einer Data Domain-Quelle an einem Data Domain-Ziel ermöglicht werden sollen, wählen Sie **Replicate client backups in parallel** aus. Wählen Sie andernfalls **Default Mode** aus.

    a. Wählen Sie **Optimize Virtual Synthetic Replication (VSR)** aus, wenn das Replikations-Plug-in die VSR-Optimierung verwenden soll, sofern diese Optimierung unterstützt wird.

       Für die VSR-Optimierung ist erforderlich, dass unter **Replication order of client backups** die Option **Oldest backup to newest backup** aktiviert ist. Diese Option ist standardmäßig ausgewählt. Heben Sie die Auswahl dieser Option auf, wenn alle Reihenfolgeoptionen für die poolbasierte Replikation unabhängig vom Plug-in befolgt werden sollen.

    b. Wählen Sie unter **Replication order of client backups** eine der folgenden Optionen aus:

- **Oldest backup to newest backup**: Die Replikation beginnt mit dem ältesten Backup.
- **Newest backup to oldest backup**: Die Replikation beginnt mit dem neuesten Backup.

18. Klicken Sie auf **Next**.

    Die Seite **Overview** wird angezeigt.

19. Überprüfen Sie die Einstellungen für die Replikationsgruppe.
20. (Optional) Geben Sie Plug-in-Optionen für die Replikationsgruppe an:

    a. Klicken Sie auf **More Options**.

    b. Um ausschließlich Backups bestimmter Plug-ins zu replizieren, legen Sie den numerischen Plug-in-Deskriptor im Feld **Include plug-in specific backups** an.

Trennen Sie mehrere Einträge durch Kommata oder lassen Sie das Feld leer, um alle Backups zu replizieren. Numerische Plug-in-Deskriptoren auf Seite 359 enthält eine Liste der numerischen Plug-in-Deskriptoren.

c. Um Backups bestimmter Plug-ins von der Replikation auszuschließen, legen Sie den numerischen Plug-in-Deskriptor im Feld **Exclude plug-in specific backups** an.

   Trennen Sie mehrere Einträge durch Kommata oder lassen Sie das Feld leer, um alle Backups zu replizieren.

d. Wählen Sie in der Liste **Informational message level** die Ausführlichkeit der Informationsmeldungen in den Replikationsprotokolldateien aus:

   - Wählen Sie **No informationals** aus, um alle Informationsmeldungen zu unterdrücken, aber Fehler und Warnmeldungen in die Protokolldateien aufzunehmen.
   - Wählen Sie **Some informationals** aus, um neben Fehlern und Warnmeldungen auch einige Informationsmeldungen in den Protokolldateien bereitzustellen.
   - Wählen Sie **Many informationals** aus, damit die Protokolldateien neben Fehlern und Warnmeldungen auch zusätzliche Statusinformationen enthalten.
   - Wählen Sie **All informationals** aus, damit die Protokolldateien das Maximum an Informationen enthalten, einschließlich aller Informationsmeldungen, Fehler und Warnmeldungen.

e. Legen Sie fest, ob erweiterte Timing- und Deduplizierungsstatistiken in die Replikationsprotokolldateien aufgenommen werden sollen, indem Sie das Kontrollkästchen **Report advanced statistics** aktivieren oder deaktivieren.

f. Wählen Sie aus der Liste **Maximum concurrent processes** die maximale Anzahl der gleichzeitig zu replizierenden Clients aus.

g. Aktivieren Sie das Kontrollkästchen **Show Advanced Options**, um erweiterte Optionen festzulegen.

   Die erweiterten Optionen werden im Dialogfeld **More Options** in Rot dargestellt.

h. Um ausschließlich ein bestimmtes Backup zu replizieren, geben Sie die Sequenznummer des Backups im Feld **Backup sequence number** oder die Backupbezeichnung im Feld **Backup label** an. Geben Sie die vollständige Backupsequenznummer oder -bezeichnung an.

i. Um Backups zu replizieren, deren Bezeichnung mit einem bestimmten Muster übereinstimmt, geben Sie das Muster im Feld **Backup label pattern** an.

j. Legen Sie über die Liste **List contents being replicated** fest, wie viele Informationen über die replizierten Backups in die Replikationsprotokolldateien aufgenommen werden sollen:

   - **No file listing**
   - **List file names**
   - **List files and dates**

Seien Sie vorsichtig, wenn Sie Dateiinformationen in die Replikationsprotokolldateien aufnehmen. Die Replikationsperformance nimmt ab und die Größe der Protokolldateien kann immens sein.

k. Um zwecks Troubleshooting den maximalen Umfang von Informationen in Protokolldateien zu schreiben, aktivieren Sie das Kontrollkästchen **Enable debugging messages**.

Beim Replikationsprozess werden äußerst große Protokolldateien erzeugt.

l. Um die Netzwerkauslastung auf eine bestimmte Rate in Megabits pro Sekunde zu reduzieren, geben Sie den entsprechenden Megabitwert im Feld **Network usage throttle** an.

Geben Sie `0` (Null) an, um eine uneingeschränkte Netzwerkauslastung festzulegen. Legen Sie `0.772` fest, um 50 % einer T1-Leitung zu verwenden.

m. Wenn die poolbasierte Replikation für Data Domain-Systeme konfiguriert wird, wählen Sie unter **Client list ordering** die Reihenfolge für die Clientreplikation aus.

n. Wenn die poolbasierte Replikation für Data Domain-Systeme konfiguriert wird, geben Sie unter **Maximum number of Data Domain Replication Streams** die maximale Anzahl von avtar-Prozessen ein, die parallel gestartet werden können.

o. Klicken Sie auf **OK**.

21. Klicken Sie auf **Finish**.

Aktivieren und Deaktivieren einer Replikationsgruppe

Sie können eine Replikationsgruppe deaktivieren, um für diese Gruppe geplante Replikationen zu verhindern. Dieser Schritt erfolgt in der Regel, um das System in einen Zustand zu versetzen, der Wartungsaktivitäten unterstützt. Im Falle einer Deaktivierung einer Replikationsgruppe muss die Gruppe erneut aktiviert werden, um geplante Replikationen wieder aufnehmen zu können.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Data Movement Policy**Link zum Startprogramm.

   Das Fenster **Data Movement Policy** wird angezeigt.
2. Wählen Sie die Registerkarte **Groups** aus.
3. Wählen Sie die Replikationsgruppe aus.
4. Wählen Sie **Actions** > **Disable Group** aus.

   Ist die Gruppe deaktiviert, wird dies durch ein Häkchen neben **Disable Group** angezeigt. Wenn die Gruppe aktiviert ist, wird kein Häkchen angezeigt.
5. Klicken Sie in der Bestätigungsmeldung auf **Yes**.

Bearbeiten einer Replikationsgruppe

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Data Movement Policy**Link zum Startprogramm.

   Das Fenster **Data Movement Policy** wird angezeigt.
2. Wählen Sie die Registerkarte **Groups** aus.

3. Wählen Sie die zu bearbeitende Replikationsgruppe aus.
4. Wählen Sie **Actions** > **Edit Group** aus.

   Der Assistent **Edit Replication Group** wird angezeigt.
5. Bearbeiten Sie die Einstellungen für die Replikationsgruppe.

   Die Einstellungen stimmen mit den Einstellungen überein, die Sie beim Erstellen der Gruppe festgelegt haben.
6. Klicken Sie auf **OK**.

Löschen einer Replikationsgruppe

Wenn Sie eine Replikationsgruppe aus der Konfiguration auf dem Avamar-Quellserver löschen, verbleiben sämtliche bereits auf den Zielserver replizierte Daten für die Gruppe so lange auf dem Zielserver, bis die replizierten Backups ablaufen oder die Backups gelöscht werden.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Data Movement Policy**Link zum Startprogramm.

   Das Fenster **Data Movement Policy** wird angezeigt.
2. Wählen Sie die Registerkarte **Groups** aus.
3. Wählen Sie die zu löschende Replikationsgruppe aus.
4. Wählen Sie **Actions** > **Delete Group** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
5. Klicken Sie auf **Yes**.

Durchführen einer On-Demand-Replikation

Sie können bei Verwendung der Policy-basierten Replikation eine On-Demand-Replikation für eine Replikationsgruppe durchführen. Bei einer On-Demand-Replikation handelt es sich um eine einmalige Datenreplikation für die Replikationsgruppe. Es empfiehlt sich, eine On-Demand-Replikation als erste Replikation der Replikationsgruppe nach der Konfiguration der Policy-basierten Replikation durchzuführen. Führen Sie vor einer Systemwartung, vor Softwareinstallationen oder Softwareupgrades eine On-Demand-Replikation durch.

On-Demand-Replikationen lassen sich über das Fenster **Replication** oder das Fenster **Policy** starten.

Durchführen einer On-Demand-Replikation über das Replikationsfenster

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Data Movement Policy**Link zum Startprogramm.

   Das Fenster **Data Movement Policy** wird angezeigt.
2. Wählen Sie die Registerkarte **Groups** aus.
3. Wählen Sie die Replikationsgruppe aus.
4. Wählen Sie **Actions** > **Run Group Now** aus.

   Das Dialogfeld **On-Demand Replication Request** ist ein Indiz dafür, dass die Replikationsanforderung gesendet wurde.

5. Klicken Sie auf **Close**.

Durchführen einer On-Demand-Replikation über das Policy-Fenster

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Policy Management**.
3. Klicken Sie auf die Registerkarte **Groups**.
4. Wählen Sie die Replikationsgruppe aus der Liste aus.

   Replikationsgruppen werden mit dem Wert `Replication` in der Spalte **Type** für die Gruppe angezeigt.
5. Klicken Sie auf **Run**.

   Es wird eine Bestätigungsmeldung angezeigt.
6. Klicken Sie auf **Close**.

Durchführen einer Replikation über die Befehlszeile

Die `avrepl`-Befehlszeilenoberfläche (CLI) ermöglicht es Ihnen, Daten von einem Avamar-Quellserver auf einen Avamar-Zielserver zu replizieren.

Die `avrepl`-Binärdatei befindet sich im Verzeichnis `\usr\local\avamar\bin` auf dem Server-Utility-Node. Melden Sie sich als „Admin“ oder „Root“ an und führen Sie den Befehl von dort aus aus.

Befehlsreferenz

Die folgenden Themen dienen als Referenz für die vom Befehl `avrepl` unterstützten Vorgänge und Optionen.

Zusammenfassung

`avrepl --operation=replicate[`*`options`*`][`*`target`*`]`

Vorgänge

Für `avrepl` wird nur der Vorgang `--operation=replicate` unterstützt. Dabei werden Daten vom Avamar-Quellserver auf einen Avamar-Zielserver repliziert.

Optionen

Verwenden Sie die Optionen des Befehls `avrepl`, um das Replikationsverhalten zu steuern.

Kontooptionen

Kontooptionen für den Befehl `avrepl` ermöglichen die Angabe von Anmeldedaten, um zwecks Replikation eine Verbindung zum Avamar-Zielserver herzustellen.

Die folgenden Kontooptionen sind für den Befehl `avrepl` verfügbar.

Tabelle 83 Kontooptionen für den Befehl `avrepl`.

Option	Beschreibung
`--account=`*Speicherort* `--acnt=`*Speicherort* `--path=`*Speicherort*	Legt einen hierarchischen *Speicherort* auf dem Avamar-Zielserver fest. Diese Option verhält sich relativ zum aktuellen Startspeicherort, es sei denn, Sie geben einen Schrägstrich (`/`) als Präfix für die Pfadzuweisung an. In diesem Fall wird von einem absoluten Pfad ausgegangen. Das Standardkonto ist `REPLICATE`.
`--[replscript]dstaddr=`*destination_server*	Legt den DNS-Namen bzw. die IP-Adresse des Avamar-Zielservers fest. Eine Replikation zwischen Servern verschiedener Versionen wird unterstützt. Um ein optimales Ergebnis zu erzielen, vergewissern Sie sich jedoch, dass die Avamar-Serversoftware auf dem Zielserver mindestens über die gleiche oder eine neuere Version wie der Avamar-Quellserver verfügt.
`--[replscript]dstid=repluser`	Legt die Avamar-Benutzer-ID und -Domain zur Authentifizierung beim Avamar-Zielserver fest. **Hinweis** Das repluser-Konto ist das einzige Benutzerkonto, das bekanntermaßen auf allen Zielservern zuverlässig funktioniert.
`--dstpassword=`*password* `--dstap=`*password* `--dstpswd=`*password*	Legt das Passwort für das repluser-Konto auf dem Avamar-Zielserver fest.
`--[replscript]dstpath=`*domain*	Legt einen Speicherort (*domain*) auf dem Avamar-Zielserver zum Speichern der replizierten Quelldaten fest. Der Standardwert ist das Verzeichnis auf der obersten Ebene (`/`), in dem die replizierten Daten in einer neuen, für den Avamar-Quellserver benannten Domain gespeichert werden. Verwenden Sie diese Option mit der Option `--[replscript]srcpath`. Sie können diese Option nicht mit der Option `--[replscript]dpnname` verwenden.
`--[replscript]dstport=`*Port*	Legt den beim Verbinden mit dem Avamar-Zielserver zu verwendenden Datenport fest. Der Standardwert ist `27000`.
`--hfsaddr=`*Avamar_server* `--server=`*Avamar_server*	Legt den DNS-Namen bzw. die IP-Adresse des Avamar-Quellservers fest.
`--[avtar]id=`*user@auth*	Legt die Avamar-Benutzer-ID und das Authentifizierungssystem zur Authentifizierung beim Avamar-Quellserver fest. Der Standardwert ist `repluser`. Dabei handelt es sich um das standardmäßige Replikationsbenutzerkonto auf dem Avamar-Server. Zur Authentifizierung mit dem Avamar-Authentifizierungssystem geben Sie `avamar` für *auth* an. Beispiel: `--[avtar]id=jdoe@avamar`.
`--password=`*password*	Legt das Passwort für die Avamar-Benutzer-ID zur Authentifizierung auf dem Avamar-Quellserver fest.

Tabelle 83 Kontooptionen für den Befehl `avrepl`. (Fortsetzung)

Option	Beschreibung
`--ap=`*password* `--pswd=`*password*	

Protokollierungsoptionen

Protokollierungsoptionen für den Befehl `avrepl` ermöglichen zum einen die Angabe des Pfads und Dateinamens für die `avrepl`-Protokolldatei, zum anderen lässt sich steuern, wie viele Informationen vom Plug-in in die Protokolldatei geschrieben werden.

Die folgenden Protokollierungsoptionen sind für den Befehl `avrepl` verfügbar.

Tabelle 84 Protokollierungsoptionen für den Befehl `avrepl`.

Option	Beschreibung
`--[avtar]informationals=`*n*	Legt die Informationsebene für Statusmeldungen fest. *n* steht dabei für einen einstelligen Ganzzahlwert.
`--[avtar]noinformationals={true | false}`	Geben Sie `true` an, um alle Statusmeldungen zu deaktivieren.
`--[avtar]statistics={true | false}`	Geben Sie `true` an, um erweiterte Timing- und Deduplizierungsstatistiken in die Replikationsprotokolldateien aufzunehmen.
`--log=`*Datei* `--logfile=`*Datei*	Gibt den vollständigen Pfad und Dateinamen der Protokolldatei des `avrepl`-Plug-ins an.
`--nostdout={true | false}`	Geben Sie `true` an, um die Ausgabe an STDOUT zu deaktivieren. Falls Sie jedoch die Option `--log` oder `--logfile` verwenden, erfolgt die Ausgabe weiterhin in der Protokolldatei.
`--nowarnings={true | false}`	Geben Sie `true` an, um Warnmeldungen zu deaktivieren.
`--quiet={true | false}`	Geben Sie `true` an, um alle Meldungen zu unterdrücken. Diese Option entspricht der gleichzeitigen Verwendung von `--[avtar]noinformationals=true` und `--nowarnings=true`.
`--verbose` `--v`	Geben Sie `--verbose` oder `--v` an, um alle Meldungen zu aktivieren, einschließlich Status- und Warnmeldungen. Geben Sie zum Steuern der Ausführlichkeitsebene `--verbose=`*n* an. Der Standardwert ist `--verbose=6`.

Replikationsoptionen

Die Replikationsoptionen für den Befehl `avrepl` ermöglichen die Steuerung der Replikationsfunktionen, etwa die Auswahl der zu replizierenden Backups und die Aufbewahrungsdauer der replizierten Backups auf dem Zielserver.

Die folgenden Replikationsoptionen sind für den Befehl `avrepl` verfügbar.

Tabelle 85 Replikationsoptionen für den Befehl `avrepl`

Option	Beschreibung
`--[avtar]after=`*timestamp*	Legt fest, dass nur Backups, die dem Zeitstempel (*timestamp*) oder einem späteren Zeitpunkt entsprechen, repliziert werden sollen. Geben Sie als *timestamp* einen lokalen Zeitzonenwert im 24-Stunden-Format an und halten Sie sich dabei an die Syntax *jjjj-mm-tt hh:mm:ss*. Es ist möglich, *timestamp*-Teilwerte zu verwenden. Die Auflösung wird auf den letzten angegebenen Wert gekürzt. Beispiel: `2014-02` entspricht `2014-02-01 00:00:00`. Sie können diese Option auch mit `--[avtar]before=`*timestamp* verwenden, um einen Bereich von Gültigkeitsdaten zu definieren. Nur Backups, die innerhalb dieses Datumsbereichs erfolgt sind, werden repliziert.
`--[avtar]allsnapups={true | false}`	Der Standardwert ist `true`. Damit werden alle Backups repliziert. Bei Angabe von `false` wird nur das letzte Backup jedes Clients repliziert. Wenn Sie die Option `--[avtar]count` angeben, dann setzt die Option `--[avtar]count` die Option `--[avtar]allsnapups` außer Kraft. Nur die angegebene Anzahl der letzten Backups wird für jeden Client repliziert.
`--[avtar]before=`*timestamp*	Legt fest, dass ausschließlich vor *timestamp* erfolgte Backups repliziert werden sollen. Geben Sie als *timestamp* einen lokalen Zeitzonenwert im 24-Stunden-Format an und halten Sie sich dabei an die Syntax *jjjj-mm-tt hh:mm:ss*. Es ist möglich, *timestamp*-Teilwerte zu verwenden. Die Auflösung wird auf den letzten angegebenen Wert gekürzt. Beispiel: `2014-02` entspricht `2012-02-01 00:00:00`. Sie können diese Option auch mit `--[avtar]after=`*timestamp* verwenden, um einen Bereich von Gültigkeitsdaten zu definieren. Nur Backups, die innerhalb dieses Datumsbereichs erfolgt sind, werden repliziert.
`--[avtar]count=`*n*	Beschränkt replizierte Backups auf diese maximale Anzahl (*n*) zuletzt durchgeführter Backups jedes Clients.
`--[avtar]exclude-pluginid-list=`*list*	Schließt mit dem angegebenen Plug-in durchgeführte Backups aus, wobei es sich bei *list* um eine kommagetrennte Liste von Plug-in-IDs handelt.
`--[avtar]expires=`*{n | period | timestamp}*	Legt fest, wie lange replizierte Backups auf dem Zielserver aufbewahrt werden sollen: • Eine Anzahl von Tagen (*n*). • Ein Ablaufzeitraum (*period*), angegeben als eine bestimmte Anzahl von Tagen, Wochen, Monaten oder Jahren. Zur Angabe eines Zeitraums verwenden Sie einen der folgenden Werte: `days=`*n* `weeks=`*n* `months=`*n*

Tabelle 85 Replikationsoptionen für den Befehl `avrepl` (Fortsetzung)

Option	Beschreibung
	`years=`*n* *n* steht dabei für eine positive Ganzzahl. Geben Sie beispielsweise `--[avtar]expires=years=2` an, um replizierte Backups zwei Jahre lang auf dem Zielserver aufzubewahren. Außerdem entsprechen `--[avtar]expires=30` und `--[avtar]expires=days=30` einander. • Ein Zeitstempel (*timestamp*) für das Datum und die Uhrzeit, zu dem bzw. zu der das replizierte Backup abläuft. Geben Sie einen lokalen Zeitzonenwert im 24-Stunden-Format an und halten Sie sich dabei an die Syntax *jjjj-mm-tt hh:mm:ss*. Es ist möglich, *timestamp*-Teilwerte zu verwenden. Die Auflösung wird auf den letzten angegebenen Wert gekürzt. Beispielsweise ist `2014-02` gleich `2014-02-01 00:00:00`.
`--[avtar]pluginid-list=`*list*	Repliziert nur mit den angegebenen Plug-ins durchgeführte Backups, wobei es sich bei *list* um eine kommagetrennte Liste von Plug-in-IDs handelt.
`--[avtar]retention-type={daily | weekly | monthly | yearly | none}`	Repliziert nur Backups mit einem der folgenden Aufbewahrungstypen: • `daily` • `weekly` • `monthly` • `yearly` • `none` Bei Angabe von `none` werden nur die Backups ohne bestimmten Aufbewahrungstyp repliziert.
`--[replscript]dpnname=`*source_server* `--dpn=`*source_server*	Legt einen Namen zur Darstellung des Avamar-Quellservers (*source_server*) als Teil des Pfads für die replizierten Dateien in der `REPLICATE`-Domain auf dem Zielserver fest. Geben Sie den vollständig qualifizierten Domainnamen des Quellservers an. Sie können diese Option nicht mit den Optionen `--[replscript]dstpath` und `--[replscript]srcpath` verwenden.
`--[replscript]dstencrypt={ssl | tls}`	Aktiviert die Verschlüsselungsmethode für `avtar`, `avmaint` und `avmgr` auf dem Zielserver. Gültige Verschlüsselungsmethoden sind `ssl` und `tls`.
`--[replscript]srcpath=`*domain*	Legt einen Speicherort (*domain*) auf dem Avamar-Quellserver für den Replikationsstart fest. Nur Daten in diesem Speicherort werden repliziert. Die Standardeinstellung ist die Domain der obersten Ebene (`/`), mit der der gesamte Server repliziert wird. Verwenden Sie diese Option mit der Option `--[replscript]dstpath`. Sie können diese Option nicht mit der Option `--[replscript]dpnname` verwenden.

Tabelle 85 Replikationsoptionen für den Befehl `avrepl` (Fortsetzung)

Option	Beschreibung
`--backup-type=`*type*	Repliziert nur den angegebenen Backuptyp, wobei *type* einem der folgenden Werte entspricht: • `differential` • `differential_full` • `incremental` • `incremental_full` • `level0_full` • `synthetic_full`
`-- max-ddr-streams=`*n*	Legt die maximale Anzahl der parallel startbaren avtar-Prozesse mit dem Data Domain-Back-end-System als Ziel fest.
`--optimize-vsr={true | false}`	Diese Option wird mit `--vsr-plug-in-ids` verwendet. Wenn `--use-pool-based` auf „true“ festgelegt ist, bestimmt diese Option, ob die VSR-Optimierung (Virtual Synthetic Replication) mit Plug-ins verwendet werden soll, die Optimierung unterstützen. Die VSR-Optimierung erfordert die Reihenfolge von der ältesten zur neuesten Replikation, unabhängig von anderen Einstellungen. Die Standardeinstellung für diese Option ist „true“. Legen Sie diese Option auf „false“ fest, wenn alle Reihenfolgeoptionen für die poolbasierte Replikation unabhängig vom Plug-in befolgt werden sollen.
`--ordering-criterion=`*order*	Wenn `--use-pool-based` auf „true“ festgelegt ist, bestimmt diese Option die Reihenfolge, in der Backups repliziert werden. Verfügbare Werte sind: • `oldest-to-newest`: Die Replikation beginnt mit dem ältesten Backup zuerst. Wenn diese Option nicht angegeben wird, ist dies die Standardeinstellung. • `newest-to-oldest`: Die Replikation beginnt mit dem letzten Backup zuerst. • `largest-to-smallest`: Die Replikation beginnt mit dem größten Backup zuerst. • `smallest-to-largest`: Die Replikation beginnt mit dem kleinsten Backup zuerst.
`--use-pool-based={true | false}`	Bei „true“ wird der poolbasierte Replikationsmodus aktiviert, in dem bei der Replikation von einem Data Domain-Speichersystem zu einem anderen alle Clientbackups parallel repliziert werden.
`--vsr-plug-in-ids=`*plug-in-ids*	Wenn `--optimize-vsr` auf „true“ festgelegt ist, listet diese Option die Plug-in-IDs für Plug-ins auf, die die VSR-Optimierung (Virtual Synthetic Replication) verwenden sollen. Standardmäßig verwenden das NDMP- und das VMware-

Tabelle 85 Replikationsoptionen für den Befehl `avrepl` (Fortsetzung)

Option	Beschreibung
	Plug-in die VSR-Optimierung. Es werden keine anderen Plug-ins unterstützt.
`--within={days | weeks | months | years}=`*n*	Repliziert die Backups der letzten `days`, `weeks`, `months` oder `years`. *n* steht dabei für eine positive ganze Zahl. Geben Sie beispielsweise `--within=months=3` an, um drei Monate an Backups jedes Clients zu replizieren.

Reine Avamar-Optionen

Reine Avamar-Optionen ermöglichen den Zugriff auf erweiterte Funktionen, die normalerweise Avamar-Mitarbeitern vorbehalten sind. Eine falsche Anwendung dieser erweiterten Optionen kann zu Datenverlust führen. Wenn Unsicherheiten in Bezug auf diese Optionen bestehen sollten, wenden Sie sich an den Avamar-Support, um vor der Verwendung weitere Informationen zu erhalten.

Die folgenden reinen Avamar-Optionen sind für den Befehl `avrepl` verfügbar.

Tabelle 86 Reine erweiterte Avamar-Optionen für den Befehl `avrepl`

Option	Beschreibung
`--bindir=`*Pfad*	Gibt das Verzeichnis mit den Avamar-Binärdateien an. Der Standardwert ist `/usr/local/avamar/bin`.
`--[avtar]exp-delta={days | weeks | months | years}=`*n*	Ändert die Ablaufdaten replizierter Backups auf dem Zielserver der angegebenen Anzahl (*n*) von Tagen, Wochen, Monaten oder Jahren entsprechend. Der Wert kann entweder eine positive oder negative Ganzzahl sein. Geben Sie beispielsweise `--[avtar]exp-delta=days=-2` an, um das Ablaufdatum eines Backups auf dem Zielserver um zwei Tage zu verkürzen. Verwenden Sie `--[avtar]exp-delta` nicht mit `--[avtar]expires`.
`--[avtar]expiration-policy=`*type*`=`*period*	Repliziert Backups eines bestimmten Aufbewahrungstyps (*type*) innerhalb eines festgelegten Zeitraums (*period*), wobei *type* einem der folgenden Werte entspricht: • `dailies` • `weeklies` • `monthlies` • `yearlies` *period* entspricht dabei einem der folgenden Werte: • `days=`*n* • `weeks=`*n* • `months=`*n* • `years=`*n* *n* steht dabei für eine positive Ganzzahl. Geben Sie beispielsweise `--[avtar]expiration-policy=dailies=years=2` an, um zwei Jahre an täglichen

Tabelle 86 Reine erweiterte Avamar-Optionen für den Befehl `avrepl` (Fortsetzung)

Option	Beschreibung
	Backups für jeden Client zu replizieren. Die Option `--[avtar]expiration-policy` hat Vorrang vor `--[avtar]expires`.
`--[avtar]label=`*Name* `--f=`*Name*	Gibt die Bezeichnung der zu replizierenden Backups an. Trennen Sie mehrere Werte durch Kommata.
`--[avtar]label-pattern=`*Muster*	Repliziert Backups, deren Bezeichnung einem angegebenen Muster (*pattern*) entsprechen. Allgemeine glob-Operatoren (Platzhalter) wie Sternchen (*) und Fragezeichen (?) sind zulässig. Trennen Sie mehrere Muster durch Kommata, z. B. `----[avtar]label-pattern=temp, tmp`. Sie können die Option `----[avtar]label-pattern` mehrmals in einem Befehl angeben.
`--[avtar]sequencenumber=`*n* `--[avtar]labelnumber=`*n*	Gibt die Sequenznummer des zu replizierenden Backups an. Trennen Sie mehrere Einträge durch Kommata.
`--[avtar]throttle=`*n*	Steuert die Rate, mit der der zugrunde liegende `avtar`-Prozess Daten an den Server sendet. Bei Angabe dieser Option wird `avtar` nach dem Senden jedes Pakets angehalten, damit die Netzwerkauslastung die angegebene maximale Bandbreite in Megabit/Sekunde (Mbit/s) nicht überschreitet. Bei `--[avtar]throttle=5` wird beispielsweise die Hälfte einer 10-Mbit/s-Verbindung verwendet und `--[avtar]throttle=0.772` beschränkt die Auslastung auf die Hälfte eines T1-Links.
`--[replscript]exclude=`*Muster*	Schließt Domains oder Clients aus, die ein *pattern* aus der Replikation aufweisen. *pattern* steht dabei für ein übereinstimmendes Muster im Domain- bzw. Clientnamen. Allgemeine glob-Operatoren (Platzhalter) wie Sternchen (*) und Fragezeichen (?) sind zulässig. Geben Sie beispielsweise `--[replscript]exclude=spot` an, um Domains oder Clients auszuschließen, deren Namen das Muster `spot` beinhalten. Geben Sie `--[replscript]exclude=/clients/` an, um alle Clients in der `/clients`-Domain auszuschließen. Trennen Sie mehrere Muster durch Kommata, z. B. `--[replscript]exclude=spot, /clients/`. Sie können die Option `--[replscript]exclude` auch mehrmals in einem Befehl verwenden, um mehr als ein Muster anzugeben.
`--[replscript]forcecreate={true | false}`	Geben Sie `true` an, um die Erstellung aller Quellserverkonten auf dem Zielserver zu erzwingen, selbst wenn keine Daten für ein Konto in der Replikation enthalten sind. Der Standardwert ist `false`. Damit werden auf dem Zielserver ausschließlich Konten für die Clients erstellt, die Daten replizieren.
`--[replscript]force-move={1 | 0}`	Geben Sie `1` (true) an, um einen Wechsel zum Backupkonto des Zielservers zu erzwingen. Geben Sie `0` (false) an, wenn kein Wechsel erzwungen werden soll.

Tabelle 86 Reine erweiterte Avamar-Optionen für den Befehl `avrepl` (Fortsetzung)

Option	Beschreibung
`--[replscript]fullcopy={true | false}`	Geben Sie `true` an, um den kompletten *Root-to-Root*-Replikationsmodus durchzusetzen, der eine vollständige logische Kopie des gesamten Quellservers auf dem Zielserver erstellt. Die replizierten Daten werden nicht in die Domain `REPLICATE` kopiert, sondern direkt der Root-Domain hinzugefügt, so als ob Quellclients beim Zielserver registriert worden wären. Auf diese Weise replizierte Quellserverdaten sind auf dem Zielserver vollständig modifizierbar.
`--[replscript]globalcid={true | false}`	Geben Sie `true` an, damit während der Replikation globale Client-IDs (CIDs) verwendet werden. Globale CIDs werden in erster Linie verwendet, um nach einer Root-to-Root-Replikation schnelle Failover-Vorgänge zwischen Servern zu ermöglichen. Die Standardeinstellung ist `true`.
`--[replscript]reportonly={true | false}`	Geben Sie `true` an, um den reinen berichtsbezogenen Betriebsmodus durchzusetzen. Der rein berichtsbezogene Betriebsmodus wird zum Vorbestimmen der Speichermenge verwendet, die ggf. bei einer Replikationsaktivität auf einem Zielserver verbraucht wird. Hierzu wird der Replikationsjob ausgeführt, ohne dass Daten tatsächlich auf dem Zielserver gespeichert werden.
`--[replscript]restore={true | false}`	Geben Sie `true` an, um den Betriebsmodus für die Wiederherstellung durchzusetzen. Bei vorheriger Replikation eines Avamar-Quellservers auf einen Avamar-Zielserver können Sie `avrepl` über den Zielserver ausführen und diesen Befehl mit der Option `--[replscript]dpnname=`*original_source_server* angeben, um diese Daten auf einem Avamar-Server wiederherzustellen.
`--[replscript]small-client-mb=`*n*	Gibt den Schwellenwert in MB an, bis zu dem der Umfang neuer Daten für einen Client als „gering“ gilt. Die Standardeinstellung ist `128` MB an neuen Daten. Geben Sie `0` an, um diese Optimierung zu deaktivieren.
`--rechunk={disable | enable | default}`	Steuert, ob replizierte Daten zur Maximierung der Datendeduplizierung auf dem Zielserver neu in Blöcke aufgeteilt werden sollen. Verwenden Sie einen der folgenden Werte: • `disable` – Keine Neuaufteilung der Daten in Blöcke vor der Speicherung auf dem Zielserver • `enable` – Neuaufteilung der Daten in Blöcke vor der Speicherung auf dem Zielserver zur Maximierung der Datendeduplizierung • `default` – Automatische Neuaufteilung der Daten bei unterschiedlicher Aufteilung in Blöcke (Chunking) auf dem Quell- und Zielserver

Hilfeoption

Mit der Option `--help` wird eine Liste verfügbarer Optionen für den Befehl `avrepl` angezeigt:

```
avrepl --help
```

Versionsoption

Mit der Option `--version` wird die Softwareversion des Befehls `avrepl` angezeigt:

```
avrepl --version
```

Zielliste

Zur Replikation bestimmter Clients oder Avamar-Domains schließen Sie eine Liste der Clients und Domains am Ende des Befehls `avrepl` ein. Trennen Sie mehrere Einträge durch Leerzeichen.

Wenn Sie keine Liste angeben, umfasst die Replikation alle Clientbackups auf dem Avamar-Quellserver.

Numerische Plug-in-Deskriptoren

Manche Befehlsoptionen erfordern einen oder mehrere numerische Plug-in-Deskriptoren als Werte. Gültige numerische Plug-in-Deskriptoren sind in der folgenden Tabelle aufgeführt.

Tabelle 87 Numerische Plug-in-Deskriptoren

Deskriptor	Plug-in-Name
1000	Linux `avagent`
1001	Linux `avtar`
1002	Linux Oracle RMAN
1003	Linux NDMP
1009	Linux DB2
1014	Linux Lotus
1016	Linux VMware image
1019	Linux VMware File Level Restore (FLR)
1024	Linux extended retention
1025	Linux extended retention restore
1029	Linux Sybase
1030	Linux SAP
1034	Linux extended retention import
1035	Linux VDR Migration
1038	Linux VMware image restore
1039	Linux vApp image
2000	Oracle Solaris `avagent`

Tabelle 87 Numerische Plug-in-Deskriptoren (Fortsetzung)

Deskriptor	Plug-in-Name
2001	Oracle Solaris `avtar`
2002	Oracle Solaris RMAN
2009	Oracle Solaris DB2
2014	Oracle Solaris Lotus
2029	Oracle Solaris Sybase
2030	Oracle Solaris SAP
3000	Windows `avagent`
3001	Windows `avtar`
3002	Windows Oracle RMAN
3004	Windows Exchange message
3005	Windows Exchange database
3006	Windows SQL
3009	Windows DB2
3011	Windows Exchange 2007 database
3012	Windows Exchange 2007 web
3014	Windows Lotus
3015	Windows VSS
3016	Windows VMware image
3017	Windows MOSS
3018	Windows Exchange VSS
3019	Windows VMware File Level Restore (FLR)
3026	Windows MOSS VSS
3027	Windows Exchange Granular Level Restore (GLR)
3028	Windows MOSS Granular Level Restore (GLR)
3029	Windows Sybase
3030	Windows SAP
3032	Windows Hyper-V VSS
3033	Windows Hyper-V Granular Level Restore (GLR)
3036	Windows cluster file system
3041	Windows VMware Granular Level Restore (GLR)

Tabelle 87 Numerische Plug-in-Deskriptoren (Fortsetzung)

Deskriptor	Plug-in-Name
4000	HP-UX `avagent`
4001	HP-UX `avtar`
4002	HP-UX Oracle RMAN
4009	HP-UX DB2
4029	HP-UX Sybase
4030	HP-UX SAP
5000	IBM AIX `avagent`
5001	IBM AIX `avtar`
5002	IBM AIX Oracle RMAN
5009	IBM AIX DB2
5014	IBM AIX Lotus
5029	IBM AIX Sybase
5030	IBM AIX SAP
6000	Mac OSX `avagent`
6001	Mac OSX `avtar`
7003	NetApp NDMP
8003	EMC Celerra NDMP
10000	Novell NetWare `avagent`
10001	Novell NetWare `avtar`
10003	Novell NetWare NDMP
11000	FreeBSD `avagent`
11001	FreeBSD `avtar`
12000	SCO OpenServer `avagent`
12001	SCO OpenServer `avtar`
13000	SCO UnixWare `avagent`
13001	SCO UnixWare `avtar`
14003	EMC Isilon NDMP

CLI-Beispiele

Sehen Sie sich die `avrepl`-Befehlsbeispiele an, um Einzelheiten darüber zu erfahren, wie das Replikationsverhalten mithilfe von Optionen gesteuert werden kann.

Geben Sie die folgenden Optionen mit dem Befehl `avrepl` an:

Tabelle 88 Erforderliche Optionen für den Befehl `avrepl`

Option	Beschreibung
`--operation=replicate`	Befehlsvorgang für `avrepl`.
`--[replscript]dpnname=`*source_server*	Vollständig qualifizierter Domainname des Avamar-Quellservers.
`--[avtar]id=`*user@auth*	Benutzerkonto für den Avamar-Quellserver. Der Standardwert ist `repluser`. Um das `repluser`-Konto zu verwenden, können Sie `--[avtar]id` weglassen und für das `repluser`-Konto nur das Passwort mit der Option `--password` angeben.
`--password=`*password*	Passwort für das Benutzerkonto auf dem Avamar-Quellserver.
`--[replscript]dstaddr=`*destination_server*	Avamar-Zielserver.
`--[replscript]dstid=repluser`	Legt die Avamar-Benutzer-ID und -Domain zur Authentifizierung beim Avamar-Zielserver fest. **Hinweis** Das repluser-Konto ist das einzige Benutzerkonto, das bekanntermaßen auf allen Zielservern zuverlässig funktioniert.
`--dstpassword=`*password* `--dstap=`*password* `--dstpswd=`*password*	Legt das Passwort für das repluser-Konto auf dem Avamar-Zielserver fest.

Wenn die Firewall auf dem Zielserver installiert und aktiviert ist, geben Sie die Option `--[replscript]dstencrypt` mit der korrekten Verschlüsselungsmethode (`ssl` oder `tls`) an.

Replizieren aller Clientbackups

Mit dem folgenden Befehl werden alle Clientbackups vom Quellserver `avamar-1.example.com` auf den Zielserver `replication-server-1.example.com` repliziert. Das Benutzerkonto auf dem Quellserver ist `jdoe@avamar` (das `jdoe`-Benutzerkonto mit dem internen Avamar-Authentifizierungssystem) und das Passwort lautet `password`. Das Benutzerkonto auf dem Zielserver ist `repluser` und das Passwort lautet `password`.

```
avrepl --operation=replicate --
[replscript]dpnname=avamar-1.example.com --[avtar]id=jdoe@avamar --
password=password --[replscript]dstaddr=replication-
server-1.example.com --[replscript]dstid=repluser --
dstpassword=password --[replscript]dstencrypt=ssl
```

Replizieren von Backups für bestimmte Clients oder Domains

Mit dem folgenden Befehl werden alle Backups für die Clients `client1` und `client2` sowie für alle Clients in der Domain `domain3` repliziert.

```
avrepl --operation=replicate --
[replscript]dpnname=avamar-1.example.com --[avtar]id=jdoe@avamar --
password=password --[replscript]dstaddr=replication-
server-1.example.com --[replscript]dstid=repluser --
dstpassword=password --[replscript]dstencrypt=ssl client1 client2
domain3
```

Replizieren bestimmter Backuptypen
Mit dem folgenden Befehl werden alle kompletten Backups (Ebene 0), die nach dem 1. Februar 2014 durchgeführt wurden, für die Clients `client1` und `client2` repliziert.

```
avrepl --operation=replicate --
[replscript]dpnname=avamar-1.example.com --[avtar]id=jdoe@avamar --
ap=password --[replscript]dstaddr=replication-server-1.example.com --
[replscript]dstid=repluser --dstpassword=password --
[replscript]dstencrypt=ssl --[avtar]after=2014-02-01 --backup-
type=level0_full client1 client2
```

Überwachen von Replikationen

Überwachen Sie die Replikation, um sicherzustellen, dass sie erfolgreich abläuft und im Falle von Problemen ein Troubleshooting durchzuführen.

Dank der Funktion „Activity Monitor“ in Avamar-Administrator sind Sie in der Lage, Statusinformationen für On-Demand- und geplant durchgeführte Replikationsaktivitäten anzuzeigen.

Überwachen der Replikation in Avamar Administrator

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf den **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Eine Liste sämtlicher Aktivitäten wird angezeigt.

3. Um die Ergebnisse so zu filtern, dass ausschließlich Replikationsaktivitäten angezeigt werden, wählen Sie **Actions** > **Filter** aus.

   Das Dialogfeld **Filter Activity** wird angezeigt.

4. Wählen Sie aus der Liste **Type** die Option **All Replication Source & Destination** aus.

5. Klicken Sie auf **OK**.

6. Um Statistiken für eine Replikationsaktivität anzuzeigen, wählen Sie erst die Aktivität und dann **Actions** > **View Statistics** aus.

   Das Dialogfeld **Replicate Statistics** wird angezeigt. Auf der Registerkarte **Details** werden ausführliche Informationen aus der `v_repl_activities`-Datenbankansicht bereitgestellt. Die Registerkarte **Backups** enthält eine Liste der im Replikationsvorgang eingeschlossenen Backups. Auf der Registerkarte **Error** werden sämtliche während des Replikationsvorgangs aufgetretenen Fehler angezeigt.

7. Klicken Sie auf **Close**.

Abbrechen einer Replikationsaufgabe

Sie können eine Policy-basierte Replikationsaufgabe vor ihrem Abschluss jederzeit über die Funktion „Activity Monitor“ abbrechen. Der Abbruchvorgang kann 5 Minuten oder länger dauern. Die Replikation wird u. U. vor Abschluss des Abbruchvorgangs fertiggestellt.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Activity**Link zum Startprogramm.

   Das Fenster **Activity** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Activity Monitor**.

   Eine Liste sämtlicher Aktivitäten wird angezeigt.
3. Wählen Sie die Replikationsaufgabe in der Liste aus.
4. Wählen Sie **Actions** > **Cancel Activity** aus.

   Es wird eine Bestätigungsmeldung angezeigt.
5. Klicken Sie auf **Yes**.

Wiederherstellung mithilfe eines Replikats auf einem Zielsystem

Stellen Sie replizierte Daten von einem Client in der Domain `REPLICATE` eines Zielservers wieder her. Das Wiederherstellungsziel kann jeder Client sein, der Mitglied einer Domain auf dem Zielserver ist, einschließlich des Clients, der die Quelle des ursprünglichen Backups darstellt.

Verwenden Sie diese Methode, um Daten von einem Replikat wiederherzustellen, wenn der Avamar-Quellserver nicht verfügbar ist und wenn „Replicas at Source“ auf dem Avamar-Quellsystem nicht aktiviert ist.

Vorgehensweise

1. Registrieren und aktivieren Sie den Client, der das Wiederherstellungsziel darstellt, für den Avamar-Zielserver, der die replizierten Daten managt:

   a. Klicken Sie auf einem Windows-Client mit der rechten Maustaste auf das Avamar-Taskleistensymbol und wählen Sie dann **Manage** > **Activate Client** aus.

      Das Dialogfeld **Activate Client Setup** wird angezeigt.

   b. Geben Sie den Hostnamen des Avamar-Zielservers in das Feld **Administrator Server Address** ein.

   c. Geben Sie `28001` in das Feld **Administrator Server Port** ein.

   d. Geben Sie die Avamar-Domain für den Client in das Feld **Client Domain** ein.

   e. Klicken Sie auf **Activate**.

   Clientregistrierung auf Seite 59 bietet Anweisungen zu anderen Registrierungsmethoden. Sie können auch Avamar Client Manager verwenden, um Clients für den Zielserver zu aktivieren. Anweisungen finden Sie unter Verschieben eines Clients auf einen neuen Server auf Seite 425.

2. Klicken Sie in Avamar Administrator auf **Backup & Restore** Link zum Startprogramm.

   Das Fenster **Backup, Restore and Manage** wird angezeigt.

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

   Der Bereich links oben enthält eine Liste mit Domains.

4. Wählen Sie die Domain `REPLICATE` und dann den Hostnamen des Avamar-Quellservers aus.

5. Wählen Sie die Domain aus, die den Client enthält, der die Quelle des ursprünglichen Backups darstellt.

6. Wählen Sie den Client aus der Liste aus.

7. Klicken Sie auf die Registerkarte **By Date** oder die Registerkarte **By File/Folder** und wählen Sie die wiederherzustellenden Daten aus.

   Hinweis

   Wiederherstellen von Daten aus einem Backup auf Seite 208 stellt alternative Methoden zum Suchen eines Backups und Durchführen einer Wiederherstellung zur Verfügung.

8. Wählen Sie **Actions** > **Restore Now** aus.

   Das Dialogfeld **Restore Options** wird angezeigt.

9. Klicken Sie neben dem Feld **Restore Destination Client** auf **Browse**, navigieren Sie zu dem Client, der das Wiederherstellungsziel ist, und wählen Sie diesen aus.

   Wählen Sie keinen Client in der Domain `REPLICATE` als Wiederherstellungsziel aus. Wählen Sie einen Client aus, der in der Domain `clients` oder einer anderen Domain auf dem Avamar-Server aufgelistet ist.

10. Wählen Sie aus der Liste **Restore Plug-in** das für die Wiederherstellung zu verwendende Plug-in aus.

11. Wählen Sie in der Liste **Avamar encryption method** eine Verschlüsselungsmethode für Client-Server-Datenübertragungen während der Wiederherstellung aus.

    Hinweis

    Die Verschlüsselungstechnologie und die Bitstärke für eine bestimmte Client-/Serververbindung sind von einer Reihe von Faktoren abhängig, dazu gehören das Clientbetriebssystem und die Avamar-Serverversion. Informationen erhalten Sie im *Avamar – Produktsicherheitshandbuch*.

12. Wählen Sie entweder **Restore everything to a different location** oder **Restore everything to multiple locations** aus.

13. Klicken Sie unter der Liste **Items Marked for Restore** auf **Set Destination** und wählen Sie dann die Zielpfade für die wiederherzustellenden Daten aus.

14. Um bei dieser Wiederherstellung Plug-in-Optionen einzubeziehen, klicken Sie auf **More Options** und konfigurieren Sie dann die Einstellungen.

15. Klicken Sie im Dialogfeld **Restore Options** auf **OK**.

    Im Dialogfeld **Restore Request** wird angegeben, dass die Wiederherstellung begonnen hat.

16. Klicken Sie auf **Close**.
17. (Optional) Ändern Sie die Registrierung des Zielclients für die Wiederherstellung zurück in den Avamar-Quellserver.

    Führen Sie diesen Schritt durch, wenn der Avamar-Quellserver verfügbar ist.

MCS-Konfigurationsparameter zur Unterstützung von „Replikate auf Quelle“

Das MCS-Management von „Replikate auf Quelle“ wird über Konfigurationsparameter in `mcserver.xml` konfiguriert.

Ändern der Konfiguration der Funktion „Replikate auf Quelle“ auf Seite 368 beschreibt, wie `mcserver.xml` geändert wird. In der folgenden Tabelle werden die Parameter der Funktion „Replicas at Source“ in `mcserver.xml` beschrieben.

Tabelle 89 MCS-Konfigurationsparameter zur Unterstützung von „Replikate auf Quelle“

Behälter	Parameter	Standardwert	Beschreibung
`repl`	`external_sync_interval_minute`	`120`	Legt die Anzahl der Minuten zwischen den Vorgängen fest, in denen versucht wird, Replikatmetadaten vom Zielsystem mit der MCS-Datenbank auf dem Avamar-Quellsystem zu replizieren. Durch Festlegen des Parameters `get_backups_from_external_server` auf „true“ wird dieser Parameter außer Kraft gesetzt.
`repl`	`allow_dest_replica_management`	`false`	Legen Sie diesen Parameter auf **`true`** fest, um die Synchronisation der Replikatmetadaten zwischen dem Remotezielsystem und dem Avamar-Quellserver zuzulassen. Legen Sie den Parameter auf **`false`** fest, um die Synchronisation zu deaktivieren und die Funktion „Replikate auf Quelle“ zu deaktivieren.
`repl`	`get_backups_from_external_server`	`false`	Legen Sie diesen Wert auf **`true`** fest, um das Standardverhalten außer Kraft zu setzen und zu erzwingen, dass MCS Replikatmetadaten direkt vom Zielsystem bezieht. Standardmäßig bezieht MCS

Tabelle 89 MCS-Konfigurationsparameter zur Unterstützung von „Replikate auf Quelle“ (Fortsetzung)

Behälter	Parameter	Standardwert	Beschreibung
			Replikatmetadaten vom Zielsystem mittels periodischer Synchronisation. Diese Synchronisation schreibt die Metadaten in die lokale MCS-Datenbank auf dem Avamar-Quellsystem. Avamar-Administrator greift zur Bereitstellung von Replikatinformationen auf die lokale Datenbank zu.
repl	show_external_backups	true	Legen Sie diesen Parameter auf **true** fest, um die Auflistung von Replikaten auf der Registerkarte „Wiederherstellen“ zu aktivieren. Legen Sie den Parameter auf **false** fest, um die Auflistung von Replikaten auf der Registerkarte „Wiederherstellen“ zu deaktivieren.
ebms	ebms_home	lib/mcebms.war	Legt den Speicherort der Webarchivdatei für den externen Backupmanagerservice fest.
ebms	ebms_descriptor	/WEB-INF/web.xml	Legt den Speicherort der XML-Beschreibungsdatei für den externen Backupmanagerservice fest.
ebms	ebms_port	9090	Legt den eingehenden Port (Überwachungsport) für den externen Backupmanagerservice fest.
ebms	ebms_use_https	true	Legen Sie diesen Parameter auf **true** fest, um zu erzwingen, dass der externe Backupmanagerservice die SSL-/TLS-Verschlüsselung für die Kommunikation mit Zielsystemen verwendet.
mon	ebmsIntervalMinutes	720	Legt die Anzahl der Minuten zwischen den Vorgängen fest, mit denen der Status des Remote Backup Manager Services überprüft wird.

Tabelle 89 MCS-Konfigurationsparameter zur Unterstützung von „Replikate auf Quelle“ (Fortsetzung)

Behälter	Parameter	Standardwert	Beschreibung
mon	ebmsFailEventIntervalMinutes	120	Legt die Anzahl der Minuten zwischen veröffentlichten Aktualisierungen der stop-Ereignisse und fail-Ereignisse des Remote Backup Manager Services fest.
mon	ebmsMonitorTimeout	300	Legt die Anzahl der Minuten fest, nach denen versucht wird, den Status des Remote Backup Manager Services zu überprüfen.
repl	allow_manage_remote_backups_at_source	true	Legen Sie diesen Parameter auf **true** fest, um das Management von Replikaten auf dem Avamar-Quellserver zuzulassen. Das Management umfasst die folgenden Vorgänge: Löschen, Ablauf ändern und Aufbewahrung ändern. Legen Sie diesen Parameter auf **false** fest, um das Management von Replikaten auf dem Avamar-Quellserver zu deaktivieren.

Ändern der Konfiguration der Funktion „Replikate auf Quelle“

Zum Ändern der Konfiguration der Funktion „Replikate auf Quelle“ ändern Sie die Parameterwerte in der Datei „mcserver.xml“.

In diesem Thema wird beschrieben, wie Sie die Konfigurationsparameter der Funktion „Replicas at Source“ in der Datei „mcserver.xml“ ändern können. Eine Beschreibung der Konfigurationsparameter finden Sie hier: MCS-Konfigurationsparameter zur Unterstützung von „Replikate auf Quelle“ auf Seite 366.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```

2. Stoppen Sie den MCS, indem Sie den folgenden Befehl eingeben:

   ```
   dpnctl stop mcs
   ```

3. Wechseln Sie mit folgendem Befehl das Arbeitsverzeichnis:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```

4. Öffnen Sie `mcserver.xml` in einem Texteditor.
5. Suchen Sie das Containerelement des Parameters und suchen Sie innerhalb dieses Elements den Parameter.
6. Ändern Sie den Wert des Parameters.
7. Speichern Sie die Änderung und schließen Sie die Datei.
8. Starten Sie den MCS und den Scheduler, indem Sie Folgendes eingeben:

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

KAPITEL 12

Serverupdates und -hotfixes

In diesem Kapitel werden folgende Themen behandelt:

Übersicht über den Aktualisierungsprozess für die Avamar-Serversoftware

Avamar stellt regelmäßig Aktualisierungen und Hotfixes für die Avamar-Serversoftware bereit. Avamar speichert Aktualisierungs- und Hotfix-Pakete im EMC Repository. Mit dem Avamar Downloader Service können Sie die Installationspakete auf einen Avamar-Server oder einen lokalen Windows-Server herunterladen und die Pakete per Push-Vorgang auf einen Avamar-Server übertragen. Verwenden Sie dann Avamar Installation Manager, um die Pakete auf dem Avamar-Server zu installieren.

Bei Bedarf können Sie alte Installationspakete aus dem lokalen Repository auf dem Avamar-Server entfernen und diese dann ggf. über den Avamar Downloader Service erneut herunterladen.

Wenn kein Internetzugriff möglich ist, kopieren Sie die Pakete manuell in das Verzeichnis `/data01/avamar/repo/packages` auf dem Utility-Node oder dem Single-Node-Server, statt den Avamar Downloader Service zu verwenden. Verwenden Sie dann Avamar Installation Manager, um die Pakete auf dem Avamar-Server zu installieren.

Avamar Downloader Service

Vor Avamar-Version 7.3 wurde der Avamar Downloader Service auf einem separaten eigenständigen Microsoft Windows-Computer installiert. Ab Avamar-Version 7.3 ist der Downloader Service auch auf dem Avamar-Server verfügbar und in den Avamar Installation Manager integriert. Sie können entweder den Legacy-Downloader Service auf einem eigenständigen Microsoft Windows-Computer oder den neuen, in den Avamar Installation Manager integrierten Downloader Service verwenden.

Kundensupport installiert die Avamar Downloader Service-Software üblicherweise während der Installation bzw. während des Upgrades eines Avamar-Servers. Sie können den Avamar Downloader Service auch vom Avamar-Server herunterladen und die Software eigenhändig installieren.

Wenn sich der Avamar Downloader Service-Computer in einem privaten Netzwerk mit eingeschränktem Zugriff auf den EMC Repository-Server befindet, kann ein Proxyserver für die Kommunikation zwischen dem Avamar Downloader Service-Computer und dem EMC Repository-Server eingerichtet werden.

Sicherheit
Der Avamar Downloader Service verschlüsselt ausgehende Kommunikation an das EMC Repository mithilfe von SSL (Secure Socket Layer) über eine HTTP-Verbindung. Der Avamar Downloader Service überprüft jedes von ihm heruntergeladene Paket, um sicherzustellen, dass das Paket ordnungsgemäß signiert und übertragen wurde.

Legacy-Avamar Downloader Service

Der Legacy-Avamar Downloader Service-Computer ist ein eigenständiger Microsoft Windows-Computer mit Netzwerkzugriff auf Avamar-Websites im Internet und alle internen Avamar-Server.

Der Legacy-Avamar Downloader Service wird als Windows-Dienst zur Überwachung des EMC Repository ausgeführt. Mittels einer Desktopverknüpfung, eines Taskleistensymbols und der Befehle des Windows-Startmenüs kann auf die Legacy-Avamar Downloader Service-Benutzeroberfläche zugegriffen werden, sodass Sie den Downloader Service konfigurieren und das EMC Repository auf das Vorhandensein

von Installationspaketen prüfen können. Die Überwachungskomponente des Avamar Downloader Service beinhaltet Statusmeldungen für den Dienst.

Der Legacy-Avamar Downloader Service akzeptiert nur eingehende Anforderungen für Installationspakete von Avamar-Systemen, die sich auf einer Liste bekannter Systeme befinden.

Lokales Repository
Das Verzeichnis `C:\Program Files\EMC\Avamar Downloader Service \repository` auf dem Avamar Downloader Service-Computer dient als lokales Repository für den Download von Installationspaketen.

Hinweis

Benennen Sie die Clientinstallationspakete nicht um. Die Avamar-Push-Upgrademechanismen sind nicht mit umbenannten Paketen kompatibel.

Die Datei `manifest.xml` im lokalen Repository enthält eine Liste aller Server-, Client- und Workflowpakete, die derzeit aus dem EMC Repository heruntergeladen werden können.

AvInstaller und Avamar Installation Manager

Der AvInstaller-Prozess steuert den Prozess zum Herunterladen und Installieren für Installationspakete auf dem Avamar-Server. Mit Avamar Installation Manager können Sie den AvInstaller-Prozess managen.

Installation
Der Kundensupport installiert AvInstaller bei der Installation oder beim Upgrade eines Avamar-Servers. AvInstaller wird auf dem Utility-Node in einer Multi-Node-Umgebung bzw. auf dem Server in einer Single-Node-Umgebung installiert.

Lokales Repository
AvInstaller verwendet das Verzeichnis `/data01/avamar/repo/packages` auf dem Avamar-Utility-Node oder -Single-Node-Server als lokales Repository für heruntergeladene Installationspakete. AvInstaller managt darüber hinaus ein temporäres Verzeichnis, in das die Pakete während der Installation extrahiert werden.

Um zu ermitteln, ob neue Pakete verfügbar sind, lädt der Avamar Downloader Service automatisch einmal täglich die Manifestdatei aus dem EMC Repository herunter. Wenn der Legacy-Avamar Downloader Service verwendet wird, sendet er die aktualisierte Manifestdatei an das lokale Repository jedes bekannten Avamar-Systems. AvInstaller ruft aus der Manifestdatei aktuelle Informationen über alle Softwarepakete ab, die zum Herunterladen aus dem EMC Repository verfügbar sind.

Benutzeroberfläche
Verwenden Sie die Benutzeroberfläche von Avamar Installation Manager, um AvInstaller zu managen. Avamar Installation Manager wird automatisch mit AvInstaller installiert. Avamar Installation Manager bietet die folgenden Funktionen:

- Herunterladen von Softwarepaketen über den Avamar Downloader Service
- Installieren der Pakete auf dem Avamar-Server
- Anzeigen einer Liste der Softwarepakete im Repository des Avamar-Servers
- Um Speicher freizugeben, löschen Sie alte Installationspakete vom Avamar-Server.
- Anzeigen des Softwareinstallationsverlaufs für den Avamar-Server

Prüfen des Status des AvInstaller-Prozesses

So prüfen Sie den Status des AvInstaller-Prozesses:

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ssh-agent bashssh-add ~admin/.ssh/admin_key
2. Geben Sie **dpnctl status avi** ein.

   Die Ausgabe des Befehls `dpnctl status avi` entspricht in etwa dem folgenden Beispiel:

```
dpnctl: INFO: avinstaller status: up.
```

Beenden des AvInstaller-Prozesses

So beenden Sie den AvInstaller-Prozess:

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich für einen Single-Node-Server beim Server als Admin an und wechseln Sie dann zum Root-Benutzer, indem Sie **su -** eingeben.
   - Melden Sie sich für einen Multi-Node-Server beim Server als Admin an und wechseln Sie dann zum Root-Benutzer, indem Sie **su -** eingeben.
2. Geben Sie **avinstaller.pl --stop** ein.
3. Überprüfen Sie, ob der AvInstaller-Prozess beendet wurde, indem Sie Folgendes eingeben: **avinstaller.pl--test**.

   Die Ausgabe des Befehls `avinstaller.pl --test` entspricht in etwa dem folgenden Beispiel:

```
Avistart process:
INFO: AVI is not running.
```

Neustarten des AvInstaller-Prozesses

So starten Sie den AvInstaller-Prozess neu:

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich für einen Single-Node-Server beim Server als Admin an und wechseln Sie dann zum Root-Benutzer, indem Sie **su -** eingeben.

- Melden Sie sich für einen Multi-Node-Server beim Server als Admin an und wechseln Sie dann zum Root-Benutzer, indem Sie `su -` eingeben.

2. Geben Sie **`avinstaller.pl --start`** ein.
3. Überprüfen Sie, ob der AvInstaller-Prozess ausgeführt wird, indem Sie Folgendes eingeben: **`avinstaller.pl--test`**.

   Die Ausgabe des Befehls `avinstaller.pl --test` entspricht in etwa dem folgenden Beispiel:

```
Avistart process pid:
INFO: AVI is running.
```

Installieren und Konfigurieren des Avamar Downloader Service

Mit Avamar-Version 7.3 wird der Avamar Downloader Service im Rahmen des Avamar-Softwareinstallationsvorgangs installiert.

Verwenden des Legacy-Avamar Downloader Service auf Seite 382 enthält Informationen über die Installation und Konfiguration der Legacy-Avamar Downloader Service-Software auf einem eigenständigen Microsoft Windows-Rechner.

Konfigurieren des Avamar Downloader Service

Konfigurieren Sie den Avamar Downloader Service, bevor Sie ihn für den Download von Paketen vom EMC Repository-Server verwenden. Zu den Konfigurationsaufgaben zählen das Bereitstellen von Anmeldeinformationen für den Avamar-Support und das Festlegen der Proxyservereinstellungen.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und melden Sie sich bei Avamar Installation Manager an:

   a. Geben Sie die folgende URL ein:

      `https://Avamar-server/avi`

      Dabei steht *Avamar-server* für die IP-Adresse oder den auflösbaren Hostnamen des Avamar-Servers.

      Die Anmeldeseite von Avamar Installation Manager wird angezeigt.

   b. Geben Sie den Benutzernamen für das Avamar Administrator-Benutzerkonto im Feld **User Name** und das zugehörige Passwort im Feld **Password** ein.

   c. Klicken Sie auf **Login**.

2. Klicken Sie auf **Configuration**.

   Das Fenster **Configuration** wird angezeigt.

3. Geben Sie unter **Username** den Benutzernamen und unter **Password** das Passwort für den Avamar-Support an, die Sie zusammen mit der Avamar-Lizenz beim Produktkauf erhalten haben.
4. (Optional) Wählen Sie „Enable Proxy“ aus, um einen Proxyserver zu aktivieren, wenn der Downloader Service zum Passieren der Firewall bei der Kommunikation mit dem Avamar-Support einen Proxyserver erfordert. Geben

Sie den Hostnamen oder die IP-Adresse und die Portnummer für den Proxyserver an.

a. Geben Sie den Hostnamen oder die IP-Adresse und die Portnummer für den Proxyserver an.

b. Wenn der Proxyserver eine Authentifizierung erfordert, geben Sie unter **Username** den Benutzernamen und unter **Password** das Passwort für den Proxyserver ein.

5. Klicken Sie auf **Save**.

Herunterladen neuer Pakete aus dem EMC Repository

Sie können das EMC Repository auf neue Server-, Client- und Workflowpakete prüfen und die Pakete dann zur Installation herunterladen.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und melden Sie sich bei Avamar Installation Manager an:

   a. Geben Sie die folgende URL ein:

   `https://`*`Avamar-server`*`/avi`

   Dabei steht *Avamar-server* für die IP-Adresse oder den auflösbaren Hostnamen des Avamar-Servers.

   Die Anmeldeseite von Avamar Installation Manager wird angezeigt.

   b. Geben Sie den Benutzernamen für das Avamar Administrator-Benutzerkonto im Feld **User Name** und das zugehörige Passwort im Feld **Password** ein.

   c. Klicken Sie auf **Login**.

2. Klicken Sie auf **Configuration**.

   Das Fenster **Configuration** wird angezeigt.

3. Klicken Sie auf **Check for New Packages**.

   Das Dialogfeld **Check for New Packages** wird angezeigt und liefert Statusmeldungen. Der Avamar Downloader Service lädt die Manifestdatei vom EMC Repository-Server in das lokale Repository auf dem Windows-Server und auf Avamar-Server in der Liste bekannter Systeme herunter.

   Durch ein Häkchen neben einer Statusmeldung wird ein erfolgreicher Prozess angegeben. Durch ein X neben einer Statusmeldung wird ein fehlgeschlagener Prozess angegeben.

4. Um Details zu fehlgeschlagenen Prozessen anzuzeigen, doppelklicken Sie auf das X neben der Statusmeldung.

5. Klicken Sie im Dialogfeld **Check for New Packages** auf **Close**.

Herunterladen und Installieren von Paketen auf dem Avamar-Server

Verwenden Sie Avamar Installation Manager zum Herunterladen und Installieren von Softwarepaketen, Patches und Hotfixes.

Bevor Sie beginnen

Auf dem Computer müssen mindestens 2 GB RAM vorhanden sein.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und melden Sie sich bei Avamar Installation Manager an:
   a. Geben Sie die folgende URL ein:

      `https://Avamar-server/avi`

      Dabei steht *Avamar-server* für die IP-Adresse oder den auflösbaren Hostnamen des Avamar-Servers.

      Die Anmeldeseite von Avamar Installation Manager wird angezeigt.

   b. Geben Sie den Benutzernamen für das Avamar Administrator-Benutzerkonto in das Feld **User Name** und das zugehörige Passwort in das Feld **Password** ein.

   c. Klicken Sie auf **Login**.
2. Wenn für das Paket eine Schaltfläche **Download** angezeigt wird, klicken Sie darauf, um das Paket in das lokale Repository herunterzuladen.

   Nach Abschluss des Downloads wird die Schaltfläche **Download** durch eine Schaltfläche **Install** und eine Schaltfläche **Delete** ersetzt.
3. Um mit der Installation zu beginnen, klicken Sie auf **Install**.

   Die Hintergrundfarbe für das Paket wechselt zu Gelb und die Initiierung beginnt. Im Anschluss an den Initiierungsprozess wird die Seite **Installation Setup** angezeigt.
4. Machen Sie Angaben zur Installationskonfiguration.

   Für bestimmte Pakete ist die Angabe von Konfigurationsinformationen nicht erforderlich.
5. Um erweiterte Einstellungen festzulegen, wählen Sie **Show advanced settings** aus.
6. Klicken Sie auf **Continue**.

   Auf der Seite **Installation Progress** wird der Status der Installation angezeigt.

   HINWEIS

   Wenn Sie den Browser während der Installation eines Pakets schließen, wird die Installation zwar angehalten, aber nicht beendet. Zum Fortsetzen der Installation öffnen Sie ein Browserfenster und melden Sie sich bei Avamar Installation Manager an. Die Installation fährt an dem Punkt fort, an dem das Browserfenster geschlossen wurde.
7. Reagieren Sie auf alle installationsbezogenen Eingabeaufforderungen.

   Nach der Installation wird die Schaltfläche **Install** für Workflowpakete zur Schaltfläche **Run**. Die Schaltfläche **Run** ermöglicht eine erneute Ausführung des Workflowpakets.

Anzeigen einer Liste mit Installationspaketen auf dem Avamar-Server

Sie können eine Liste der Installationspakete im Repository auf einem Avamar-Server auf der Registerkarte **Repository** von Avamar Installation Manager anzeigen.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und melden Sie sich bei Avamar Installation Manager an:
   a. Geben Sie die folgende URL ein:

      `https://Avamar-server/avi`

      Dabei steht *Avamar-server* für die IP-Adresse oder den auflösbaren Hostnamen des Avamar-Servers.

      Die Anmeldeseite von Avamar Installation Manager wird angezeigt.
   b. Geben Sie den Benutzernamen für das Avamar Administrator-Benutzerkonto im Feld **User Name** und das zugehörige Passwort im Feld **Password** ein.
   c. Klicken Sie auf **Login**.
2. Klicken Sie auf **Repository**.

   Die Registerkarte **Repository** wird angezeigt.
3. (Optional) Um die Sortierreihenfolge der Pakete in der Liste umzukehren, klicken Sie auf eine Spaltenüberschrift.

Hochladen von Installationspaketen auf den Avamar-Server

Mit der Funktion **Package Upload** auf der Registerkarte **Repository** können Sie Pakete von der lokalen Festplatte oder einem anderen angeschlossenen Medium, z. B. einem Flash-Laufwerk, auf den Avamar-Server hochladen.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und melden Sie sich bei Avamar Installation Manager an:
   a. Geben Sie die folgende URL ein:

      `https://Avamar-server/avi`

      Dabei steht *Avamar-server* für die IP-Adresse oder den auflösbaren Hostnamen des Avamar-Servers.

      Die Anmeldeseite von Avamar Installation Manager wird angezeigt.
   b. Geben Sie den Benutzernamen für das Avamar Administrator-Benutzerkonto im Feld **User Name** und das zugehörige Passwort im Feld **Password** ein.
   c. Klicken Sie auf **Login**.
2. Klicken Sie auf **Repository**.

   Die Registerkarte **Repository** wird angezeigt.
3. Klicken Sie auf **Browse**, um ein Paket zum Hochladen auszuwählen.

Hinweis

Version 9 bis 11 des Browsers Internet Explorer unterstützt eine maximale Uploadgröße von 4 GB. Version 6 bis 8 unterstützt eine maximale Uploadgröße von 2 GB.

Nach Abschluss des Uploads wird das Paket automatisch in der Tabelle **Repository** aufgeführt.

Überschriften auf der Registerkarte „Repository“

Die im Repository eines Avamar-Servers vorhandenen Pakete werden auf der Registerkarte **Repository** von Avamar Installation Manager angezeigt. Das zuletzt installierte Paket wird unten in der Liste aufgeführt.

In der folgenden Tabelle sind die für jedes Paket eingeblendeten Informationen beschrieben.

Tabelle 90 Informationen auf der Registerkarte „Repository“

Überschrift	Beschreibung
FileName	Der Name des Pakets.
Status	Der Status des Pakets: • Waiting – Der AvInstaller-Service kopiert das Paket in das EMC Repository. • Checksum – Der AvInstaller-Service berechnet die Prüfsumme des Pakets. • Unsigning – Der AvInstaller-Service überprüft die Paketsignatur. • Extracting – Der AvInstaller-Service extrahiert das Paket aus dem tar-Archiv. • Accepted – Das Paket wird vollständig aus dem EMC Repository geladen und ist zur Installation bereit. • Abgelehnt – Das Paket wurde entweder wegen eines Übertragungsproblems abgelehnt oder es wurde zwar heruntergeladen, konnte jedoch auf das System in seinem aktuellen Zustand nicht angewendet werden.
Note	Kurze Beschreibung des Status
Last Updated	Datum und Uhrzeit der letzten Statusaktualisierung

Löschen von Paketen vom Avamar-Server

Nach erfolgreicher Installation eines Workflow-, Patch- oder Hotfix-Pakets wird das Paket vom AvInstaller-Service automatisch aus dem Repository auf dem Avamar-System gelöscht. Nicht installierte Pakete müssen manuell gelöscht werden.

Zugriffsbeschränkte Pakete können nur vom Kundensupport gelöscht werden.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und melden Sie sich bei Avamar Installation Manager an:
   a. Geben Sie die folgende URL ein:

      `https://Avamar-server/avi`

      Dabei steht *Avamar-server* für die IP-Adresse oder den auflösbaren Hostnamen des Avamar-Servers.

      Die Anmeldeseite von Avamar Installation Manager wird angezeigt.
   b. Geben Sie den Benutzernamen für das Avamar Administrator-Benutzerkonto in das Feld **User Name** und das zugehörige Passwort in das Feld **Password** ein.
   c. Klicken Sie auf **Login**.
2. Wählen Sie in der **Package List** ein Paket aus.
3. Klicken Sie neben dem Paket auf die Schaltfläche **Delete**.

   Es wird eine Bestätigungsmeldung angezeigt.
4. Klicken Sie auf **Yes**.

Anzeigen des Installationsverlaufs

Sie können einen Verlauf der Softwareinstallationen, -aktualisierungen und -Hotfixes für einen Avamar-Server auf der Registerkarte **History** des Avamar Installation Manager anzeigen.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und melden Sie sich bei Avamar Installation Manager an:
   a. Geben Sie die folgende URL ein:

      `https://Avamar-server/avi`

      Dabei steht *Avamar-server* für die IP-Adresse oder den auflösbaren Hostnamen des Avamar-Servers.

      Die Anmeldeseite von Avamar Installation Manager wird angezeigt.
   b. Geben Sie den Benutzernamen für das Avamar Administrator-Benutzerkonto im Feld **User Name** und das zugehörige Passwort im Feld **Password** ein.
   c. Klicken Sie auf **Login**.
2. Klicken Sie auf **History**.

   Die Registerkarte **History** wird angezeigt.
3. (Optional) Um die Sortierreihenfolge der Pakete in der Liste umzukehren, klicken Sie auf eine Spaltenüberschrift.
4. (Optional) Filtern Sie die Liste mit den Paketen, indem Sie einen Wert in der Liste **Show** auswählen.
5. (Optional) Um Details zu einem Paket in der Liste anzuzeigen, wählen Sie die Zeile für das Paket aus.

6. (Optional) Um die Protokolldatei für Pakete mit dem Status „Wird verarbeitet“ anzuzeigen, klicken Sie in der Tabelle **Details** auf **Logs**.
7. (Optional) Sie können die Protokollinformationen in eine Microsoft Excel- oder PDF-Datei exportieren, indem Sie auf **Export** klicken.

Verlaufsinformationen einer Installation

Verlaufsspalten

In der folgenden Tabelle sind die für jedes Paket auf der Registerkarte Avamar Installation Manager**Verlauf** angezeigten Informationen beschrieben.

Tabelle 91 Informationen auf der Registerkarte „Verlauf“

Überschrift	Beschreibung
Titel	Der Name des Pakets.
Version	Die Version der Avamar-Serversoftware.
Beschreibung	Eine kurze Beschreibung des Pakets.
Status	Der Status des Pakets: • Available – Das Paket ist im Manifest vorhanden und steht zum Download zur Verfügung. • Completed – Die Paketinstallation wurde abgeschlossen. • Processing – Derzeit wird ein Paket installiert. • Ready – Das Paket ist bereit zur Installation. • Removed – Das Paket wurde aus dem Avamar-Grid gelöscht.
Last Updated	Datum und Uhrzeit der letzten Statusaktualisierung für das Paket.

Detailspalten

In der folgenden Tabelle sind die in der Tabelle **Details** im unteren rechten Bereich der Registerkarte **Verlauf** angezeigten Informationen beschrieben.

Tabelle 92 Details auf der Registerkarte „Verlauf“

Spaltenüberschrift der Tabelle „Details“	Beschreibung
Status	Statusdetails für ein Paket: • Available – Das Paket ist im Manifest vorhanden und steht zum Download zur Verfügung. • Ready – Das Paket ist bereit zur Installation. • Deployed – Der Beginn der Installationsinitiierung.

Tabelle 92 Details auf der Registerkarte „Verlauf“ (Fortsetzung)

Spaltenüberschrift der Tabelle „Details“	Beschreibung
	• Deploying – Der Beginn der Paketbereitstellung. • Processing – Der Beginn der Paketinstallation. • Completed – Der Abschluss der Paketinstallation. • Removed – Die Entfernung des Pakets.
Last Updated	Das entsprechende Datum und die entsprechende Uhrzeit der Statusmeldung des Pakets.
Prot.	Zeigt die Schaltfläche **Logs** für Pakete mit dem Status Processing an. Klicken Sie auf **Logs**, um ein Fenster mit Details zu den im Rahmen der Paketinstallation durchgeführten Aufgaben zu öffnen.

Verwenden des Legacy-Avamar Downloader Service

In den folgenden Themen werden die Vorbereitung für die Installation, Konfiguration und Verwendung der Legacy-Avamar Downloader Service-Software auf einem Microsoft Windows-System sowie die Aktualisierung und Deinstallation der Software beschrieben.

Installationsanforderungen für den Legacy-Avamar Downloader Service

Der Legacy-Avamar Downloader Service ist als 32-Bit- oder 64-Bit-Anwendung verfügbar. Der Legacy-Avamar Downloader Service wird auf einem Microsoft Windows-Server mit Netzwerkzugriff auf den Avamar-Server installiert. Bei diesem System kann es sich um ein Desktop- oder Laptopsystem handeln.

In der folgenden Tabelle sind die Installationsanforderungen für den Computer aufgeführt, auf dem der Legacy-Avamar Downloader Service installiert wird.

Tabelle 93 Installationsanforderungen für den Legacy-Avamar Downloader Service

Software/Hardware	Anforderung
Betriebssystem	• Microsoft Windows Server 2012 (nur 64-Bit) • Microsoft Windows Server 2008 • Microsoft Windows 8 • Microsoft Windows 7 • Microsoft Windows Vista
Dateisystem	Beliebiges Dateisystem

Tabelle 93 Installationsanforderungen für den Legacy-Avamar Downloader Service (Fortsetzung)

Software/Hardware	Anforderung
Festplattenspeicher	Mindestens 12 MB
RAM	Mindestens 20 MB

Herunterladen der Legacy-Avamar Downloader Service-Software

Laden Sie die Legacy-Avamar Downloader Service-Software von der Seite EMC **Avamar Web Restore** auf dem Avamar-Server herunter.

Vorgehensweise

1. Melden Sie sich beim Windows-Hostsystem als Administrator an.
2. Geben Sie die URL des Avamar-Servers in den Webbrowser ein:

   https://*Avamar-server*

   Dabei steht *Avamar_server* für den Hostnamen des Avamar-Systemnetzwerks (wie im DNS angegeben) bzw. die IP-Adresse.

   Die Avamar-Seite **Avamar Web Restore** wird angezeigt.
3. Klicken Sie auf **Downloads**.

   Die Liste **Downloads** wird angezeigt.
4. Klicken Sie auf **+** neben der Plattformüberschrift für den Windows-Computer.
5. Klicken Sie auf **+** neben der Betriebssystemüberschrift für den Windows-Computer.
6. Klicken Sie auf den Link für **AvamarDownloaderService-windows-*platform-version*.exe**.

   Hierbei gilt:

   - *platform* ist der Typ der Windows-Plattform (32- oder 64-Bit).
   - *version* ist die Version der Avamar-Serversoftware.

   Über ein Dialogfeld werden Sie aufgefordert, die Datei auszuführen oder zu speichern.
7. Speichern Sie die Installationsdatei in einem temporären Verzeichnis.

Installieren der Legacy-Avamar Downloader Service-Software

Vorgehensweise

1. Melden Sie sich beim Windows-Hostcomputer als Administrator an.
2. Navigieren Sie zu dem Verzeichnis, das die Datei `AvamarDownloaderService-windows-`*`platform-version`*`.exe` enthält, und doppelklicken Sie dann auf die Datei, um den Installationsvorgang zu starten.

   Der Konfigurationsassistent wird mit der Begrüßungsseite geöffnet.
3. Klicken Sie auf **Next**.

   Die Seite **Destination Folder** wird angezeigt.

4. Legen Sie den Ordner für die Avamar Downloader Service-Installation fest:
   - Klicken Sie auf **Next**, um den Standardordner, `C:\Program Files\EMC\Avamar Downloader Service`, zu übernehmen.
   - Um einen anderen Ordner festzulegen, klicken Sie auf **Change** und navigieren Sie dann zum gewünschten Ordner. Klicken Sie dann auf **Next**.

   Die Seite **Ready to install Avamar Downloader Service** wird angezeigt.
5. Klicken Sie auf **Install**.

   Die Seite **Installing Avamar Downloader Service** mit dem Fortschritt der Installation wird angezeigt. Nach abgeschlossener Installation wird die Seite **Completed the Avamar Downloader Service Setup Wizard** angezeigt.
6. Klicken Sie auf **Finish**.

   Während der Installation wird der Systemsteuerung und der Taskleiste ein Avamar Downloader Service-Symbol hinzugefügt. Bei der Installation wird `AvamarDownloaderService` ebenfalls zu den Windows-Diensten hinzugefügt.

Aktivieren von HTTPS

Die HTTPS-Funktion muss auf dem Microsoft Windows-Computer aktiviert sein, der den Legacy-Avamar Downloader Service hostet. Unter bestimmten Umständen ist HTTPS möglicherweise bereits auf dem Computer aktiviert. Wenn dies nicht der Fall ist, führen Sie die folgenden Schritte auf dem Computer aus.

Vorgehensweise

1. Wählen Sie **Control Panel** > **Windows Firewall** > **Advanced settings** aus.

   Die Konsole **Windows-Firewall with Advanced Security** wird angezeigt.
2. Klicken Sie im Navigationsbereich auf **Outbound Rules**.
3. Klicken Sie im Bereich **Actions** auf **New Rule**.

   Der **New Outbound Rule Wizard** wird angezeigt.
4. Wählen Sie **Port** aus und klicken Sie dann auf **Next**.
5. Wählen Sie **Specific remote ports** aus, geben Sie in das Textfeld den Wert „443“ ein und klicken Sie auf **Next**.
6. Klicken Sie auf **Allow the connection** und klicken Sie dann auf **Next**.
7. Übernehmen Sie die Standardeinstellungen und klicken Sie auf **Next**.
8. Geben Sie einen Namen für die ausgehende Regel (z. B. „Avamar Downloader Service“) an und klicken Sie auf **Finish**.

   Der **New Outbound Rule Wizard** wird angezeigt.
9. Klicken Sie im Bereich „Outbound Rules“ mit der rechten Maustaste auf die vorher erstellte ausgehende Regel (diese sollte sich in der Liste an oberster Position befinden) und wählen Sie **Properties** aus.

   Das Fenster **Properties** wird angezeigt.
10. Wählen Sie die Registerkarte **Programs and Services** aus.
11. Klicken Sie auf **Settings**.
12. Wählen Sie **Apply to this service** aus.
13. Wählen Sie in der Liste der Services Avamar Downloader Service aus und klicken Sie auf **OK**.

14. Klicken Sie auf **Apply** und anschließend auf **OK**.
15. Schließen Sie die Konsole **Windows Firewall with Advanced Security**.

Konfigurieren des Legacy-Avamar Downloader Service

Konfigurieren Sie den Avamar Downloader Service, bevor Sie ihn für den Download von Paketen vom EMC Repository-Server verwenden. Zu den Konfigurationsaufgaben zählen das Überprüfen der Verbindung, das Zusammenstellen einer Liste bekannter Systeme und die Angabe von Proxyservereinstellungen.

Bevor Sie beginnen

Installieren Sie die Avamar Downloader Service-Software.

Vorgehensweise

1. Klicken Sie auf dem Avamar Downloader Service-Computer mit der rechten Maustaste auf das Avamar Downloader Service-Taskleistensymbol und wählen Sie **Configure Service** aus.

   Der Konfigurationsassistent für den Avamar Downloader Service wird mit der Begrüßungsseite geöffnet.
2. (Optional) Um die lokale Version der Datei `manifest.xml` zu verwenden, wählen Sie **Disable Internet access. Use only local files** aus.

   Verwenden Sie diese Option, wenn der Avamar Downloader Service-Computer über das Internet keine Verbindung mit dem EMC Repository herstellen kann.
3. Klicken Sie auf der Begrüßungsseite des Konfigurationsassistenten auf **Next**.

   Die Seite **Avamar-Anmeldedaten**Avamar wird angezeigt.
4. Geben Sie auf dieser Seite den **Benutzernamen** und das **Passwort** (sowie die Passwortbestätigung) für den Avamar-Support an, die Sie zusammen mit der Avamar-Lizenz beim Produktkauf erhalten haben, und klicken Sie dann auf **Next**.

   Die Seite **Proxy Configuration** wird angezeigt.

   Hinweis

   Um die Avamar-Anmeldedaten zu einem späteren Zeitpunkt zu bearbeiten, öffnen Sie das Fenster **Show Advanced Settings**, indem Sie mit der rechten Maustaste auf das Taskleistensymbol klicken und **Show Advanced Settings** auswählen.
5. (Optional) Geben Sie den Hostnamen oder die IP-Adresse und die Portnummer für den Proxyserver sowie die Avamar-Anmeldedaten an: **Username**, **Password** und **Confirm Password**.

   Geben Sie Proxyserverinformationen an, um einen Proxyserver als Mittler für Anforderungen vom Avamar Downloader Service-Computer an den EMC Repository-Server zu verwenden. Auf dieser Seite können Sie auch **Use Authentication** auswählen.

   Verwenden Sie einen Proxyserver beispielsweise dann, wenn sich der Avamar Downloader Service-Computer in einem privaten Netzwerk befindet und der Zugriff auf den EMC Repository-Server eingeschränkt ist.
6. Klicken Sie auf **Next**.

   Die Seite **Avamar Systems** wird angezeigt.

7. Klicken Sie auf **Add**.

   Das Dialogfeld **Avamar Downloader Service – Add Known System** wird angezeigt.

8. Geben Sie den Hostnamen, den Benutzernamen und das Passwort für einen Avamar-Server an:

   a. Geben Sie in das Feld **Hostname** die IP-Adresse oder den Hostnamen für den Avamar-Server ein.

   b. Geben Sie im Feld **Username** die Zeichenfolge `root` ein, um den Root-Benutzer des Linux-Betriebssystems anzugeben.

   c. Geben Sie in die Felder **Password** und **Confirm Password** das Passwort für den Root-Benutzer ein.

9. Klicken Sie auf **OK**.

   Wenn der Hostname nicht im Zuge des Konfigurationsprozesses aufgelöst werden kann, wird eine Informationsmeldung angezeigt. Klicken Sie auf **Yes**, um das System hinzuzufügen. Klicken Sie auf **No**, um den Vorgang abzubrechen. Es ist möglich, der Liste bekannter Systeme Systeme mit nicht auflösbaren Hostnamen, etwa Offlinesysteme, hinzuzufügen.

10. Fügen Sie weitere Avamar-Server hinzu.

11. Nachdem alle Avamar-Server hinzugefügt wurden, klicken Sie auf **Next**.

    Die Seite **Review Configuration** wird angezeigt.

12. Überprüfen Sie die Details der Konfiguration und klicken Sie auf **Finish**.

Weitere Erfordernisse

Führen Sie bei Bedarf den Konfigurationsassistenten erneut aus, um den Hostnamen, die IP-Adresse oder die Portnummer für einen Proxyserver bzw. die Liste bekannter Systeme zum Hinzufügen und Entfernen von Avamar-Servern zu bearbeiten.

Aktualisieren der Legacy-Avamar Downloader Service-Software

Mit dem Avamar Downloader Service können Sie nach Aktualisierungen der Avamar Downloader Service-Software suchen und die Aktualisierungen herunterladen und installieren.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol für den Avamar Downloader Service und wählen Sie **Check for Updates** aus.

   Wenn eine Aktualisierung verfügbar ist, wird die Meldung `Update is ready to install` angezeigt.

   Sind keine Aktualisierungen verfügbar, wird die Meldung `Your software is up to date` angezeigt.

   Das Dialogfeld **Avamar Downloader Service Updater** wird angezeigt.

2. Wenn eine Aktualisierung verfügbar ist, klicken Sie auf **Install**.

   Der Einrichtungsassistent für den Avamar Downloader Service wird angezeigt.

3. Befolgen Sie die Eingabeaufforderungen, um den Assistenten zu durchlaufen, und installieren Sie den neuen Software-Build.

Deinstallieren des Legacy-Avamar Downloader Service

Deinstallieren Sie den Avamar Downloader Service über die Windows-Konsole **Programs**.

Vorgehensweise

1. Schließen Sie auf dem Avamar Downloader Service-Computer alle laufenden Anwendungen.
2. Öffnen Sie die Windows-Konsole **Programs** über die **Systemsteuerung**.
3. Wählen Sie in der Spalte **Name** Avamar Downloader Service aus.
4. Klicken Sie auf **Uninstall**.

Ergebnisse

Während der Deinstallation werden alle Dateien, einschließlich des Inhalts des Dateicaches, der Konfigurationselemente und der Windows Registry-Einträge für den Avamar Downloader Service entfernt.

Herunterladen neuer Pakete aus dem EMC Repository

Sie können das EMC Repository auf neue Server-, Client- und Workflowpakete prüfen und die Pakete dann zur Installation herunterladen.

Bevor Sie beginnen

Stellen Sie sicher, dass der Status des Avamar Downloader Service entweder `OK` oder `Waiting for configuration` ist. Andernfalls ist die Prüfung auf neue Pakete nicht möglich.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol Avamar Downloader Service und wählen Sie **Check for New Packages** aus.

   Das Dialogfeld **Check for New Packages** wird angezeigt und liefert Statusmeldungen. Der Avamar Downloader Service lädt die Manifestdatei vom EMC Repository-Server in das lokale Repository auf dem Windows-Server und auf Avamar-Server in der Liste bekannter Systeme herunter.

   Durch ein Häkchen neben einer Statusmeldung wird ein erfolgreicher Prozess angegeben. Durch ein X neben einer Statusmeldung wird ein fehlgeschlagener Prozess angegeben.
2. Um Details zu fehlgeschlagenen Prozessen anzuzeigen, doppelklicken Sie auf das X neben der Statusmeldung.
3. Klicken Sie im Dialogfeld **Check for New Packages** auf **Close**.

Anzeigen einer Liste der zum Download verfügbaren Pakete

Die Datei `manifest.xml` im Repository-Ordner auf dem Avamar Downloader Service Downloader Service-Computer enthält eine Liste der Softwarepakete, die zurzeit zum Download aus dem EMC Repository zur Verfügung stehen.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol Avamar Downloader Service und wählen Sie **Open Repository** aus.

Windows Explorer wird geöffnet und zeigt den Ordner `C:\Program Files \EMC\Avamar Downloader Service\repository` mit der Datei `manifest.xml` an.

2. Öffnen Sie `manifest.xml`, um die Paketinformationen anzuzeigen.

   Paketnamen haben die Dateierweiterung `.avp` und werden in den Tags `<filename>` angezeigt.

Überprüfen der Verbindung mit dem EMC Repository

Nachdem Sie die Verbindungseinstellungen für das Repository bearbeitet haben oder nachdem ein Paketdownload fehlgeschlagen ist, müssen Sie überprüfen, ob der Avamar Downloader Service-Computer eine Verbindung zum EMC Repository-Server herstellen kann.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol Avamar Downloader Service und wählen Sie **Run Diagnosis** aus.

   Der Status des Prozesses wird im Dialogfeld **Run Diagnosis** angezeigt. Durch ein **X** neben einer Statusmeldung wird auf ein Problem mit der Netzwerkverbindung hingewiesen. Klicken Sie auf das **X** neben den Fehlern, um im Dialogfeld **Error Information** weitere Informationen hierzu aufzurufen.

   Das Dialogfeld **Run Diagnosis** wird angezeigt und der Prozess zum Prüfen der Netzwerkverbindung wird automatisch gestartet.

2. (Optional) Um den Verifizierungsprozess vor seinem Abschluss zu beenden, klicken Sie auf **Stop System Check**.
3. Klicken Sie nach Abschluss der Verifizierung auf **Close**.

Überwachen des Avamar Downloader Service-Status

Die Überwachungskomponente von Avamar Downloader Service wird automatisch gestartet, wenn Sie sich am Avamar Downloader Service-Computer anmelden. Verwenden Sie die Überwachungskomponente, um den Status des Avamar Downloader Service anzuzeigen.

Vorgehensweise

- Um den Status aus der Überwachungskomponente anzuzeigen, bewegen Sie die Maus über das Avamar Downloader Service-Taskleistensymbol.

  Daraufhin wird ein Fenster mit einer Statusmeldung angezeigt.

  In der folgenden Tabelle sind die Statusmeldungen der Avamar Downloader Service-Überwachungskomponente aufgeführt.

  Tabelle 94 Statusmeldungen der Avamar Downloader Service-Überwachungskomponente

Statusmeldung	Beschreibung
Avamar Downloader Service	Standardmäßige Statusmeldung.
Authentication Failure with the EMC Repository	Grundlegender HTTP-Authentifizierungsfehler.
Authentication Failure with one or more „Known Systems“	Grundlegender HTTP-Authentifizierungsfehler, darunter:

Tabelle 94 Statusmeldungen der Avamar Downloader Service-Überwachungskomponente (Fortsetzung)

Statusmeldung	Beschreibung
	■ Fehler bei Kommunikation mit dem EMC Repository ■ SSL(Secure-Socket-Layer-)Handshake-Fehler ■ Unterbrochene HTTP-Verbindung ■ HTTP NAK (Negatively Acknowledged Message)
Failed communication with one or more „Known Systems“	Mögliche Ursachen: ■ SSL-Handshake-Fehler ■ Unterbrochene HTTP-Verbindung ■ HTTP NAK
Failed file download from the EMC repository	Dateiübertragung wurde abgebrochen.
Failed file transfer to one or more known systems	Dateiübertragung wurde abgebrochen.
Network Error	HTTPS-Browsereinstellungen verhindern, dass der Avamar Downloader Service Dateien von der Avamar-Online-Support-Website anfordert.
Out of space	Der Dateicache des Avamar Downloader Service ist voll. Entfernen Sie Dateien aus dem lokalen Repository, um Festplattenspeicher freizugeben.
Running.	Der Dienst wird ausgeführt und kommuniziert mit allen bekannten Systemen und dem EMC Repository.
Socket failure on host computer	Mögliche Ursachen: ■ Der Hostcomputer verfügt nicht mehr über Socket-Ressourcen. ■ Ein Bindungsproblem im Zusammenhang mit der NIC. ■ Deadlock-Bedingung innerhalb von Winsock.
Waiting for configuration	Der Avamar Downloader Service wurde installiert, aber nicht konfiguriert.

Stoppen und Starten der Avamar Downloader Service-Überwachungskomponente

Die Avamar Downloader Service-Überwachungskomponente wird automatisch gestartet, wenn Sie sich am Avamar Downloader Service-Computer anmelden.

Vorgehensweise

- Zum Beenden der Überwachungskomponente klicken Sie mit der rechten Maustaste auf das Taskleistensymbol für den Avamar Downloader Service und wählen Sie dann **Exit** aus.
- Zum Starten der Überwachungskomponente öffnen Sie das **Start**-Menü von Windows und wählen Sie den Befehl **All Programs** > **Avamar Downloader Service *Version*** > **Avamar Downloader Service Monitor** aus.

Troubleshooting bei Problemen mit Avamar Downloader Service

Häufig auftretende Probleme im Zusammenhang mit dem Avamar Downloader Service können Sie beheben.

Paketdownload schlägt fehl
SYMPTOM: Der Utility-Node oder der Single-Node-Server kann nicht auf den Windows-Hostcomputer zugreifen und beim Download eines Pakets wird eine dem folgenden Beispiel ähnliche Meldung angezeigt:

```
The selected package cannot be downloaded.
```

LÖSUNG: Fügen Sie der Datei `/etc/hosts` auf dem Utility-Node eine Zeile mit der IP-Adresse, dem vollständig qualifizierten Domainnamen und dem Kurznamen des Avamar Downloader Service-Computers hinzu.

BEISPIELEINTRAG: `10.6.172.50 avamar-1.example.com avamar-1`

Temporäre IPv6-Adressen führen zu fehlgeschlagenem Paketdownload
SYMPTOM: Der Avamar Downloader Service kann ein Paket nicht herunterladen und zeigt Fehler vom Typ `connection refused` an.

MÖGLICHE URSACHE: Bei allen Betriebssystemen werden temporäre IPv6-Adressen verwendet. Die Fehler `connection refused` sind auf die Verwendung temporärer IPv6-Adressen zurückzuführen. Windows Vista, Windows 2008 Server oder neuere Windows-Versionen nutzen standardmäßig temporäre IPv6-Adressen.

LÖSUNG: Blockieren Sie als Workaround für dieses Problem temporäre IPv6-Adressen auf dem Avamar Downloader Service-Computer. Geben Sie jeden der folgenden `netsh`-Befehle an der Eingabeaufforderung des Avamar Downloader Service-Computers ein. Geben Sie jeden `netsh`-Befehl in einer separaten Zeile ein.

```
netsh interface ipv6 set privacy state=disabled store=activenetsh
interface ipv6 set privacy state=disabled store=persistentnetsh
interface ipv6 set global randomizeidentifiers=disabled
store=activenetsh interface ipv6 set global
randomizeidentifiers=disabled store=persistent
```

KAPITEL 13

Avamar Client Manager

In diesem Kapitel werden folgende Themen behandelt:

Überblick über Avamar Client Manager

Avamar Client Manager ist eine webbasierte Managementanwendung, die zentrale Avamar-Clientverwaltungsfunktionen für größere Unternehmen bereitstellt. Avamar Client Manager vereinfacht das Management einer großen Anzahl von Avamar-Clients.

Avamar Client Manager funktioniert mit Avamar-Clients auf einem unterstützten nativen Betriebssystem und Avamar-Clients auf einem unterstützten Betriebssystem, das auf einer virtuellen VMware-Maschine ausgeführt wird. Avamar Client Manager funktioniert nicht mit Avamar-Clients über ein virtuelles Center, eine virtuelle Maschine oder virtuelle Proxykonfigurationen. Die Avamar Client Manager-Benutzeroberfläche zeigt unterstützte Avamar-Clients an und blendet alle nicht unterstützten Clients aus.

Verbindungssicherheit

Für die sichere Datenübertragung zwischen einem Computer und dem Avamar-Server wird eine sichere Verbindung über HTTPS hergestellt.

Bei dieser Form des HTTP-Protokolls werden Meldungen vor dem Senden verschlüsselt und beim Empfang entschlüsselt. HTTPS wird für alle Übertragungen von Anmeldedaten und für alle Datenübertragungen bei Registrierungs- und Aktivierungsvorgängen verwendet.

Alle Zugriffsversuche auf den Avamar-Server mithilfe der Benutzeroberfläche über das Standard-HTTP-Protokoll werden an HTTPS umgeleitet, um reine Textübertragungen zu verhindern.

Apache-Webserver-Authentifizierung

Die Avamar Client Manager-Benutzeroberfläche verwendet nur sichere Webseiten. Außerdem wird eine Authentifizierungswarnung in Webbrowsern angezeigt, die auf diese Seiten zugreifen, es sei denn, Sie installieren ein vertrauenswürdiges Public-Key-Zertifikat auf dem Apache-Webserver. Diese Option wird mit Avamar bereitgestellt.

Im *Avamar – Produktsicherheitshandbuch* wird beschrieben, wie Sie ein vertrauenswürdiges Public-Key-Zertifikat für den Apache-Webserver erhalten und installieren können.

Bearbeiten des Timeout-Zeitraums von Sitzungen

Wenn eine Sitzung 72 Stunden oder länger ohne eine Interaktion zwischen Webbrowser und Avamar Client Manager-Server ausgeführt wurde, wird die Sitzung von Avamar Client Manager beendet. Durch die automatische Sitzungszeitüberschreitung bleibt die Sicherheit der Ressourcen gewahrt, auf die über Avamar Client Manager zugegriffen werden kann. Sie können den Timeout-Zeitraum verlängern oder verkürzen.

Wenn eine Avamar Client Manager-Sitzung beendet wird, schließen Sie das Fenster oder die Registerkarte des Webbrowsers, in dem bzw. auf der die Sitzung ausgeführt wurde, und starten Sie dann Avamar Client Manager neu. Eine Avamar Client Manager-Sitzung wird nicht beendet, während eine Commit-Aufgabe ausgeführt wird.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell:
    a. Melden Sie sich beim Server als Administrator an.

b. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie **su -** eingeben.

c. Laden Sie für einen Multi-Node-Server den OpenSSH-Schlüssel rootid, indem Sie Folgendes eingeben:

ssh-agent bashssh-add /root/.ssh/rootid

2. Beenden Sie den EM Tomcat-Server, indem Sie Folgendes eingeben: **dpnctl stop emt**.
3. Öffnen Sie die folgende Datei in einem Texteditor:

   /usr/local/avamar-tomcat/webapps/aam/WEB-INF/web.xml

4. Ändern Sie den Wert des session-timeout-Tag auf einen neuen Wert in Minuten.

   Das folgende Beispiel zeigt das session-timeout-Tag mit dem Standardwert von 4320 Minuten (72 Stunden):

```
<session-config>
   <session-timeout>4320</session-timeout>
</session-config>
```

5. Speichern und schließen Sie die Datei.
6. Starten Sie den EM Tomcat-Server, indem Sie Folgendes eingeben: **dpnctl start emt**.

Erhöhung des JavaScript-Timeout-Zeitraums

Die Avamar Client Manager-Benutzeroberfläche verwendet JavaScript zum Durchführen zahlreicher Aufgaben. Mitunter erfordert ein Skript der Avamar Client Manager-Benutzeroberfläche mehr Zeit zum Abschließen, als es der Standard-Zeitüberschreitungswert des Webbrowsers für das Skript zulässt.

Wenn dieser Schritt eintritt, wird eine Meldung angezeigt und das Skript gestoppt. Sie können auf „Continue“ klicken, damit das Skript den Vorgang abschließen kann.

Erhöhen Sie den Timeout-Zeitraum des Skripts, um zu verhindern, dass diese Meldung angezeigt wird. Die Schritte sind abhängig vom Webbrowser.

Erhöhung des JavaScript-Timeout-Zeitraums in Internet Explorer unter Windows

Vorgehensweise

1. Öffnen Sie einen Registrierungseditor, zum Beispiel Regedt32.exe.
2. Öffnen Sie den folgenden Registrierungsschlüssel:

   HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Styles

   Wenn der Schlüssel nicht existiert, erstellen Sie ihn.

3. Erstellen Sie unter dem Schlüssel einen DWORD-Wert namens MaxScriptStatements.
4. Geben Sie als DWORD-Wert 20.000.000 an.

   Diese Zahl spiegelt die Anzahl der Skriptanweisungen wider.

5. Starten Sie den Webbrowser neu.

Erhöhung des JavaScript-Timeout-Zeitraums in Firefox

Vorgehensweise

1. Geben Sie **about:config** in die Adressleiste des Browsers ein.

   Daraufhin wird eine Warnmeldung angezeigt.
2. Klicken Sie auf **Ich werde vorsichtig sein, versprochen!**.

   Das Fenster mit den Einstellungen wird geöffnet.
3. Geben Sie unter **Filter** die Zeichenfolge **dom.max_script_run_time** ein.

   Die Einstellung zur Skriptlaufzeit wird angezeigt.
4. Doppelklicken Sie auf die Einstellung.

   Das Dialogfeld **Geben Sie einen integer-Wert ein** wird angezeigt.
5. Geben Sie 30 ein und klicken Sie auf **OK**.
6. Starten Sie den Browser neu.

Avamar Client Manager – Konfigurationseigenschaften

Normalerweise müssen keine Änderungen an der Standardkonfiguration von Avamar Client Manager vorgenommen werden. Manche Eigenschaften können jedoch an eine bestimmte Bereitstellungsanforderung angepasst werden.

Die Avamar Client Manager-Eigenschaften sind in der Datei `/usr/local/avamar/etc/acm.properties` angegeben.

In der folgenden Tabelle finden Sie Informationen zu den Eigenschaften.

Tabelle 95 Avamar Client Manager-Konfigurationseigenschaften

Eigenschaft	Beschreibung	Standardwert
activation.retry.attempts	Die Anzahl der Versuche, einen Client zu aktivieren, bevor die Aktivierung fehlschlägt.	24
activation.retry.frequency.minutes	Die Anzahl der Minuten zwischen den Clientaktivierungsversuchen.	120
move.getactivities.retry.attempts	Anzahl der Prüfungen, um zu bestimmen, ob ein Client inaktiv ist (sodass er verschoben werden kann).	7
move.getactivities.frequency.seconds	Anzahl der Sekunden zwischen Prüfungen zur Bestimmung, ob ein Client inaktiv ist (sodass er verschoben werden kann).	5
move.queue.error.codes	Legt eine kommagetrennte Liste von Fehlercodes fest, die bestimmen, ob eine fehlgeschlagene Verschiebeaufgabe der Warteschlange hinzugefügt wird. Eine Verschiebung wird nur dann der Warteschlange hinzugefügt, wenn ihr Fehlschlagen einen dieser Fehlercodes erzeugt. Verwenden Sie den Wert none, um zu verhindern, dass alle fehlgeschlagenen Verschiebeaufgaben in die Warteschlange aufgenommen werden. Verwenden Sie den Wert	22271, 22280, 22282, 22295, 30006, 30012, 30016, 30017, 30019

Tabelle 95 Avamar Client Manager-Konfigurationseigenschaften (Fortsetzung)

Eigenschaft	Beschreibung	Standardwert
	`empty`, um alle fehlgeschlagenen Verschiebeaufgaben der Warteschlange hinzuzufügen.	
`move.retry.attempts`	Legt fest, wie oft eine fehlgeschlagene Verschiebeaufgabe wiederholt wird.	24
`move.retry.frequency.minutes`	Legt die Zeitspanne zwischen den erneuten Versuchen in Minuten fest.	120
`orgu.name.append.domain`	Legt fest, ob die im Bereich **Client Information** angezeigten Clients der Benutzeroberfläche nur mit dem Hostnamen des Clients oder mit den vollständig qualifizierten Domainnamen angezeigt werden. Der Standardwert zeigt den vollständig qualifizierten Domainnamen für jeden Client an.	true
`toolbar.displaytime.client`	Bestimmt, ob die in Avamar Client Manager angezeigte Zeit die Zeitzone des Hostcomputers des Webbrowsers oder die Zeitzone des Avamar-Servers verwendet. Der Standardwert entspricht der Zeitzone des Hostcomputers des Webbrowsers.	true
`upgrade.freeform.flags`	Stellt eine Möglichkeit zur Verfügung, um Schlüssel-/Werte-Flags für ein Upgrade von Arbeitsaufträgen zu übergeben. Der Wert stellt eine kommagetrennte Liste von KV-Paaren dar. Beispiel: `upgrade.freeform.flags=key1=val1,key2=val2,key3=val3`	Kein Standardwert

Ändern einer Avamar Client Manager-Konfigurationseigenschaft

Vorgehensweise

1. Öffnen Sie eine Befehlsshell:
   a. Melden Sie sich beim Server als Administrator an.
   b. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie **`su -`** eingeben.
   c. Laden Sie für einen Multi-Node-Server den OpenSSH-Schlüssel rootid, indem Sie Folgendes eingeben:

      `ssh-agent bashssh-add /root/.ssh/rootid`

2. Wechseln Sie das aktuelle Arbeitsverzeichnis, indem Sie den folgenden Befehl eingeben:

   `cd /usr/local/avamar/etc`

3. Öffnen Sie die Avamar Client Manager-Eigenschaftendatei, `acm.properties`, in einem Texteditor.

4. Bearbeiten Sie den Wert der Eigenschaft.
5. Speichern und schließen Sie die Datei.
6. Starten Sie den EM Tomcat-Server neu, indem Sie Folgendes eingeben:

```
dpnctl stop emt
dpnctl start emt
```

Starten von Avamar Client Manager

Starten Sie Avamar Client Manager durch Eingabe der URL Avamar Client Manager in einem Webbrowser. Avamar Client Manager kann auch in Backup and Recovery Managergestartet werden.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und geben Sie die folgende URL ein:

   https://*Avamar_server*/aam

   Dabei steht *Avamar_server* für den auflösbaren Hostnamen oder die IP-Adresse des Avamar-Servers, auf dem der Avamar Client Manager-Prozess ausgeführt wird.

2. Geben Sie im Feld **User Name** den Benutzernamen eines Administratorkontos auf dem Avamar-Server ein.
3. Geben Sie unter **Password** das Passwort des Kontos ein.

Ergebnisse

Avamar Client Manager wird mit dem Abschnitt **Server Summary** der Seite „Übersicht“ geöffnet.

Anmeldeseite

Über die Anmeldeseite wird der Zugriff auf die Benutzeroberfläche von Avamar Client Manager eingeschränkt, indem ein Benutzername und ein Passwort eingegeben werden müssen.

Die Anmeldeseite authentifiziert den Benutzernamen und das Passwort durch einen Vergleich mit Administratorkonten, die auf dem Avamar-Server registriert sind. Avamar Client Manager gestattet nur den Zugriff für Konten mit Administratorrechten auf den Avamar-Server, auf dem der Avamar Client Manager-Prozess läuft.

Nach einer erfolgreichen Anmeldung wird die Benutzeroberfläche des Avamar Client Manager mit dem Abschnitt **Serverübersicht** der Übersichtsseite geöffnet.

Allgemeine Tools

Avamar Client Manager verfügt über verschiedene Tools, die auf mehr als einer Seite verwendet werden können.

Verwenden Sie diese Tools, um Unterstützung bei den folgenden Aufgaben zu erhalten:

- Hinzufügen eines Avamar-Servers
- Entfernen eines Avamar-Servers
- Ändern der Einstellungen für einen Avamar-Server

- Auswählen eines zu verwendenden Avamar-Servers
- Filtern der Übersicht einer Seite
- Anzeigen von im Kontext relevanten Details
- Exportieren von Informationen einer Seite
- Aktivieren von Sprechblasenmeldungen

Hinzufügen eines Avamar-Servers

Fügen Sie den Avamar-Server zu Avamar Client Manager hinzu, um das Management der Avamar-Clients eines Avamar-Servers zu ermöglichen.

Bevor Sie beginnen

Ermitteln Sie die folgenden Informationen:

- Den auflösbaren Hostnamen oder die IP-Adresse des Avamar-Servers
- Den eingehenden RMI-Port auf dem Avamar-Server
- Das Passwort für das MCUser-Benutzerkonto auf dem Avamar-Server

Vorgehensweise

1. Navigieren Sie zum Abschnitt **Serverübersicht** der Übersichtsseite.
2. Klicken Sie auf **Server hinzufügen**.

   Das Fenster **Server hinzufügen** wird angezeigt.
3. Geben Sie unter **System name (or) IP** den auflösbaren Hostnamen oder die IP-Adresse des Avamar-Servers ein.
4. Geben Sie in das Feld **Port** den eingehenden RMI-Port für den Avamar-Server ein.

   In dem Feld wird der Standardwert 9443 angezeigt. Übernehmen Sie den Standardwert unverändert, es sei denn, auf dem Avamar-Server wird ein nicht standardmäßiger Port verwendet.
5. Geben Sie in das Feld **MCUser Passwort** das Passwort für das MCUser-Konto auf dem Avamar-Server ein.
6. Klicken Sie auf **Save**.

Ergebnisse

Avamar Client Manager prüft die Werte und fügt den Avamar-Server hinzu.

Entfernen eines Avamar-Servers

Entfernen Sie den Avamar-Server aus Avamar Client Manager, um das Management der Avamar-Clients auf einem Avamar-Server zu beenden.

Vorgehensweise

1. Navigieren Sie zum Abschnitt **Serverübersicht** der Übersichtsseite.
2. Wählen Sie die zu entfernenden Avamar-Server aus.

   Der Avamar-Server, der den Avamar Client Manager-Prozess hostet, kann nicht entfernt werden.
3. Klicken Sie auf **Server entfernen**.

   Ein Warndialogfeld wird angezeigt.

4. Klicken Sie auf **Yes**.

Ergebnisse

Avamar Client Manager entfernt die ausgewählten Avamar-Server aus der Gruppe der gemanagten Server.

Ändern der Einstellungen für einen Avamar-Server

Änderungen auf einem Avamar-Server am eingehenden RMI-Port oder an dem Passwort für das MCUser-Benutzerkonto verhindern das Management des Avamar-Servers durch Avamar Client Manager. Bearbeiten Sie die gespeicherten Einstellungen für den Avamar-Server, um das Management durch Avamar Client Manager wieder zu aktivieren.

Bevor Sie beginnen

Ermitteln Sie die folgenden Informationen:

- Den neuen eingehenden RMI-Port auf dem Avamar-Server
- Das neue Passwort für das MCUser-Benutzerkonto auf dem Avamar-Server

Vorgehensweise

1. Unterbrechen Sie alle Aktivitäten auf dem Avamar-Server.

   Unterbrechen und Wiederaufnehmen von Serveraktivitäten auf Seite 243 beschreibt, wie Aktivitäten auf dem Avamar-Server unterbrochen werden.

2. Navigieren Sie zum Abschnitt **Serverübersicht** der Übersichtsseite.
3. Wählen Sie einen Avamar-Server aus.
4. Klicken Sie auf **Server bearbeiten**.

   Das Fenster **Server bearbeiten** wird angezeigt.

5. Geben Sie in das Feld **Port** den eingehenden RMI-Port auf dem ausgewählten Avamar-Server ein.
6. Geben Sie in das Feld **MCUser Passwort** das Passwort für das MCUser-Konto auf dem ausgewählten Avamar-Server ein.
7. Klicken Sie auf **Save**.

Ergebnisse

Avamar Client Manager prüft die Werte und richtet das Management des Avamar-Servers wieder ein.

Auswählen eines Servers

Über das Feld für die Serverauswahl lassen sich Informationen für einen bestimmten Server anzeigen und verwenden.

Bevor Sie beginnen

Erweitern Sie den **Navigationsbereich** auf der linken Seite der Benutzeroberfläche, damit das Feld für die Serverauswahl oben im Bereich sichtbar wird. Navigieren Sie zu einer Seite, auf der das Feld für die Serverauswahl in einem aktiven, auswählbaren Status angezeigt wird.

Vorgehensweise

1. Klicken Sie im Feld für die Serverauswahl auf das Pfeilsymbol.

   Sollte das Feld für die Serverauswahl nicht angezeigt werden, erweitern Sie den **Navigationsbereich** auf der linken Seite der Benutzeroberfläche. Wenn das

Feld für die Serverauswahl keine Relevanz für die aktuelle Seitenansicht hat, ist es abgeblendet, d. h., es ist weder aktiv noch auswählbar.

2. Wählen Sie aus der Liste der Server einen Server aus.

   Die Seitenansicht wird aktualisiert und es werden Informationen über den Server und seine Aufgaben angezeigt.

Filter

Avamar Client Manager verfügt über ein breites Angebot an Filtern.

Verwenden Sie einen Filter, um zu ermitteln, welche Objekte in der Liste auf der aktuellen Seite angezeigt werden. Filter lassen sich bei verschiedenen Objekten einsetzen. Der Objekttyp und die verfügbaren Filter sind vom Kontext der Seite abhängig. In Avamar Client Manager können die folgenden Objekttypen gefiltert werden:

- Server
- Clients
- Policies
- Gruppen
- Aufgaben
- Protokolleinträge

Filter für den aktuellen Kontext werden in der Leiste „Filters“ oben auf der Seite angezeigt.

Suchen nach Namen

Um nach Objekten durch Abgleich einer Suchzeichenfolge mit Objektnamen zu suchen, verwenden Sie das Suchfeld.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** über eines der folgenden suchfähigen Felder verfügt:

- User name
- Client name
- Group name
- Domain name

Beschränken Sie mithilfe eines Suchvorgangs die Liste auf Objekte mit denselben oder ähnlichen Namen.

Vorgehensweise

1. Klicken Sie auf den Pfeil neben dem suchfähigen Feld.

   Daraufhin wird ein Feld für die Texteingabe angezeigt.

2. Geben Sie in das Feld zur Texteingabe eine Suchzeichenfolge ein.

   Avamar Client Manager vergleicht die von Ihnen eingegebene Suchzeichenfolge mit den Namen der Objekte und nimmt übereinstimmende Objekte in die Liste auf. Objekte stimmen überein, wenn ein Teil des Namens die Suchzeichenfolge enthält.

3. Klicken Sie auf das Lupensymbol.

Ergebnisse

Avamar Client Manager aktualisiert die Liste und es werden nur Objekte mit Namen, die der Suchzeichenfolge entsprechen, angezeigt.

Beispiel 1 Suchen nach Benutzernamen

Um alle Clients einzuschließen, die über einen Benutzer mit dem Zeichen „eng“ im Benutzernamen verfügen, geben Sie `*eng*` in das Texteingabefeld ein.

Weitere Erfordernisse

(Optional) Um die Suchzeichenfolge zu entfernen und alle Objekte anzuzeigen, klicken Sie auf **X** neben dem Texteingabefeld.

Regeln zu Suchzeichenfolgen

Die Suchzeichenfolge besteht aus einem oder mehreren Zeichen, die Sie in ein bestimmtes Suchfeld eingeben. Avamar Client Manager vergleicht die Suchzeichenfolge mit allen Objektnamen. Wenn die Suchzeichenfolge mit dem Namen eines Objekts vollständig oder teilweise übereinstimmt, wird von Avamar Client Manager der Name des Objekts den Ergebnissen hinzugefügt.

Eine Suchzeichenfolge ist folgenden Regeln unterworfen:

- Sie darf höchstens 24 Zeichen lang sein.
- Es kann ein Sternchen (*) als Platzhalter für 0 oder mehr Zeichen verwendet werden.
- Sie darf nicht mit einem Punkt beginnen.
- Sie darf keines der in der Spalte „Zeichen“ der folgenden Tabelle aufgeführten Zeichen enthalten:

  Tabelle 96 In Suchzeichenfolgen unzulässige Zeichen

Zeichen	Name	Unicode
/ [a]	Schrägstrich	002F
:	Doppelpunkt	003A
;	Semikolon	003B
?	Fragezeichen	003F
"	Anführungszeichen	0022
<	Kleiner-als-Zeichen	003C
>	Größer-als-Zeichen	003E
\	Umgekehrter Schrägstrich	005C
,	Komma	002c
~	Tilde	007E
!	Ausrufezeichen	0021
@	@-Zeichen	0040
#	Nummernzeichen	0023
$	Dollarzeichen	0024

Tabelle 96 In Suchzeichenfolgen unzulässige Zeichen (Fortsetzung)

Zeichen	Name	Unicode
%	Prozentzeichen	0025
^	Zirkumflex-Akzent	005E
|	Senkrechter Strich	007C
&	Kaufmännisches Und-Zeichen	0026
'	Apostroph	0027
`	Graviszeichen	0060
(	Öffnende Klammer	0028
)	Schließende Klammer	0029
{	Geschweifte Klammer links	007B
}	Geschweifte Klammer rechts	007D
[	Eckige Klammer links	005B
]	Eckige Klammer rechts	005D

a. Ausnahme bei diesem Ausschlusskriterium: Der Schrägstrich ist im Filter „Domain Name“ auf der Seite „Policies“ zulässig.

Verwenden des Filters „Activity Type“

Verwenden Sie den Filter „Activity Type“, um eine Liste auf einen Aktivitätstyp zu beschränken.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** die Option **Aktivitätstyp** enthält.

Vorgehensweise

1. Klicken Sie in der Leiste **Filters** auf den Pfeil neben **Activity Type**.

   Daraufhin wird eine Auswahlliste mit den folgenden Werten angezeigt: **Backup** und **Restore**.

2. Wählen Sie einen Wert aus.

   Wählen Sie **Backup** aus, um ausschließlich Backupaufgaben in die Liste aufzunehmen. Wählen Sie **Restore** aus, um ausschließlich Wiederherstellungsaufgaben in die Liste aufzunehmen.

   Wählen Sie beispielsweise im Abschnitt **Idle Clients** der Seite **Clients** als Filter für **Activity Type** die Option **Backup** aus. Avamar Client Manager beschränkt die Liste auf Clients ohne Backupaktivität während des definierten Zeitraums.

Ergebnisse

Avamar Client Manager filtert die Ergebnisse mithilfe des von Ihnen ausgewählten Aktivitätstyps.

Verwenden des Filters „Client Status“

Verwenden Sie den Filter „Client Status“, um der Liste Clients mit dem festgelegten Clientstatus hinzuzufügen.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** die Option **Clientstatus** enthält.

Vorgehensweise

1. Klicken Sie in der Leiste **Filters** auf den Pfeil neben **Client Status**.

   Daraufhin wird eine Auswahlliste mit den Clientstatus für alle Clients in diesem Kontext angezeigt.

2. Wählen Sie einen Status aus.

   Wählen Sie beispielsweise im Abschnitt **Add Clients** der Seite **Clients** die Option **Activation Failure** für den Filter **Client Status** aus. Avamar Client Manager beschränkt die Liste auf registrierte Computer mit mindestens einem fehlgeschlagenen Aktivierungsversuch.
   Avamar Client Manager aktualisiert die Liste. In der Liste werden ausschließlich Einträge mit dem ausgewählten Clientstatus angezeigt.

3. (Optional) Wiederholen Sie die Schritte, um zusätzliche Status auszuwählen.

Ergebnisse

Avamar Client Manager aktualisiert die Liste. In der Liste werden ausschließlich Einträge mit dem ausgewählten Clientstatus angezeigt.

Verwenden des Filters „Failure Criteria“

Verwenden Sie den Filter „Failure Criteria“, um zu definieren, welche Clients von Avamar Client Manager in die Liste fehlgeschlagener Clients aufgenommen werden.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** die Option **Fehlerkriterien** enthält.

Vorgehensweise

1. Klicken Sie in der Leiste **Filters** auf den Pfeil neben **Failure Criteria**.

   Daraufhin wird eine Auswahlliste mit den folgenden Werten angezeigt: **At least one activity failed**, **All activities failed** und **Last activity failed**.

2. Wählen Sie einen Wert aus.

   Über den von Ihnen ausgewählten Wert wird festgelegt, welche Clients von Avamar Client Manager in die Liste fehlgeschlagener Clients aufgenommen werden. Avamar Client Manager schließt nur diejenigen Clients ein, die dem ausgewählten Aktivitätsstatus entsprechen.

   Wählen Sie beispielsweise **Last activity failed** aus. Avamar Client Manager aktualisiert die Liste und schließt nur Clients ein, deren letzte Aktivität fehlgeschlagen ist. Bei der fehlgeschlagenen Aktivität kann es sich um ein Backup oder eine Wiederherstellung handeln.

Ergebnisse

Avamar Client Manager aktualisiert die Liste. In der Liste werden nur die Clients angezeigt, deren Aktivitätsstatus mit dem ausgewählten Wert übereinstimmt.

Verwenden des Betriebssystemfilters

Verwenden Sie den Betriebssystemfilter, um eine Liste auf Clients mit bestimmten Betriebssystemen zu beschränken.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** die Option **BS** enthält.

Vorgehensweise

1. Klicken Sie in der Leiste **Filters** auf den Pfeil neben **OS**.

   Daraufhin wird eine Liste der Betriebssystemversionen aller Clients in diesem Kontext angezeigt.

2. Wählen Sie eine Betriebssystemversion aus.

   Avamar Client Manager aktualisiert die Liste. Nur Clients mit der ausgewählten Betriebssystemversion werden in der Liste angezeigt.

3. (Optional) Wiederholen Sie die Schritte, um zusätzliche Betriebssystemversionen auszuwählen.

Ergebnisse

Avamar Client Manager aktualisiert die Liste. Nur Clients mit der ausgewählten Betriebssystemversion werden in der Liste angezeigt.

Verwenden des Filters „Period“

Verwenden Sie den Filter „Period“, um die Kalenderdatumsgrenzen der angezeigten Ergebnisse zu definieren.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** die Option **Periode** enthält.

Vorgehensweise

1. Klicken Sie in der Leiste **Filters** auf den Pfeil neben **Period**.

   Daraufhin wird eine Auswahlliste mit den folgenden Werten angezeigt: **Before**, **After** und **On**.

2. Wählen Sie einen Wert aus.
3. Klicken Sie auf den Pfeil neben dem ausgewählten Wert.

   Daraufhin werden ein Feld für die Datumseingabe und ein kleines Kalendersymbol angezeigt.

4. Klicken Sie auf das Kalendersymbol, navigieren Sie zu einem bestimmten Datum und klicken Sie dann auf das Datum.

   Geben Sie als Alternative ein Datum im Format m/t/jj in das Feld für die Datumseingabe ein und klicken Sie dann auf das Lupensymbol.

   Avamar Client Manager aktualisiert die Liste. In der Liste werden ausschließlich Einträge innerhalb des angegebenen Zeitraums angezeigt.

5. (Optional) Verfeinern Sie die Ergebnisanzeige, indem Sie diese Schritte mit anderen Werten wiederholen.

Ergebnisse

Avamar Client Manager aktualisiert die Liste. In der Liste werden ausschließlich Einträge innerhalb des angegebenen Zeitraums angezeigt.

Verwenden des Filters „Status“

Verwenden Sie den Filter „Status“, um eine Liste auf Einträge mit bestimmten Status zu beschränken.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** die Option **Status** enthält.

Vorgehensweise

1. Klicken Sie in der Leiste **Filters** auf den Pfeil neben **Status**.

   Daraufhin wird eine Auswahlliste mit allen Status für alle Einträge in diesem Kontext angezeigt.

2. Wählen Sie einen Status aus.

   Avamar Client Manager aktualisiert die Liste. In der Liste werden ausschließlich Einträge mit dem ausgewählten Status angezeigt.

3. (Optional) Wiederholen Sie die Schritte, um zusätzliche Status auszuwählen.

Ergebnisse

Avamar Client Manager aktualisiert die Liste. In der Liste werden ausschließlich Einträge mit den ausgewählten Status angezeigt.

Verwenden des Filters „Status Code“

Verwenden Sie den Filter „Status Code“, um eine Liste auf Einträge mit bestimmten Statuscodes zu beschränken.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** die Option **Statuscode** enthält.

Vorgehensweise

1. Klicken Sie in der Leiste **Filters** auf den Pfeil neben **Status Code**.

   Daraufhin wird eine Auswahlliste mit den Statuscodes für alle Einträge in diesem Kontext angezeigt.

2. Wählen Sie einen Statuscode aus.

   Avamar Client Manager aktualisiert die Liste. In der Liste werden ausschließlich Einträge mit dem ausgewählten Statuscode angezeigt.

3. (Optional) Wiederholen Sie die Schritte, um zusätzliche Statuscodes auszuwählen.

Ergebnisse

Avamar Client Manager aktualisiert die Liste. In der Liste werden ausschließlich Einträge mit den ausgewählten Statuscodes angezeigt.

Verwenden des Filters „Success Criteria“

Verwenden Sie den Filter „Success Criteria“, um zu definieren, welche Clients von Avamar Client Manager in die Liste erfolgreicher Clients aufgenommen werden.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** die Option **Erfolgskriterien** enthält.

Vorgehensweise

1. Klicken Sie in der Leiste **Filters** auf den Pfeil neben **Success Criteria**.

   Daraufhin wird eine Auswahlliste mit den folgenden Werten angezeigt: **At least one activity successful**, **All activities successful** und **Last activity successful**.

2. Wählen Sie einen Wert aus.

   Über den von Ihnen ausgewählten Wert wird festgelegt, welche Clients von Avamar Client Manager in die Liste erfolgreicher Clients aufgenommen werden. Avamar Client Manager nimmt nur diejenigen Clients auf, die dem ausgewählten Aktivitätsstatus entsprechen.

   Wählen Sie beispielsweise **Last activity successful** aus. Avamar Client Manager aktualisiert die Liste und nimmt nur Clients mit einem erfolgreichen Backup- oder Wiederherstellungsvorgang auf.

Ergebnisse

Avamar Client Manager aktualisiert die Liste. In der Liste werden nur die Clients angezeigt, deren Aktivitätsstatus mit dem ausgewählten Wert übereinstimmt.

Verwenden des Filters „Version“

Verwenden Sie den Filter „Version“, um eine Liste auf Clients mit bestimmten Versionen der Avamar-Clientsoftware zu beschränken.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste **Filter** die Option **Version** enthält.

Vorgehensweise

1. Klicken Sie in der Leiste **Filters** auf den Pfeil neben **Version**.

   Daraufhin wird eine Auswahlliste mit den Avamar-Clientsoftwareversionen für alle Clients in diesem Kontext angezeigt.

2. Wählen Sie eine Version aus.

   Avamar Client Manager aktualisiert die Liste. Nur Clients mit der ausgewählten Softwareversion werden in der Liste angezeigt.

3. (Optional) Wiederholen Sie die Schritte, um zusätzliche Softwareversionen auszuwählen.

Ergebnisse

Avamar Client Manager aktualisiert die Liste. Nur Clients mit den ausgewählten Softwareversionen werden in der Liste angezeigt.

Anzeigen von Details

Verwenden Sie den Bereich **Details**, um kontextrelevante Details anzuzeigen.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die den Bereich **Details** oder die Leiste **Details** auf der rechten Seite enthält.

Vorgehensweise

1. Klicken Sie rechts auf der Seite auf die Leiste **Details**.

   Der Bereich **Details** wird erweitert.

2. Wählen Sie ein Objekt unter **Summary** aus.

   Der Objekttyp ist vom Seitenkontext abhängig. Bei einem Objekt kann es sich um einen Client oder eine Gruppe handeln. Sie können mehrere Objekte auswählen.

   Ausführliche Informationen für das ausgewählte Objekt werden im Bereich „Details“ angezeigt.
3. (Optional) Verwenden Sie bei Auswahl von mehr als einem Objekt die Steuerelemente für die Seitennavigation unten im Bereich „Details“, um Informationen für jedes ausgewählte Objekt anzuzeigen.

Exportieren von Daten

Mithilfe der Exportfunktion lässt sich die ausgewählte Zusammenfassung in Form einer Excel-Tabelle herunterladen.

Bevor Sie beginnen

Navigieren Sie zu einer Seitenansicht, die in der Seitenleiste die Option **Export** enthält.

Vorgehensweise

1. Klicken Sie in der Seitenleiste auf **Export**.

   Avamar Client Manager schließt alle Informationen aus der Zusammenfassung in die exportierten Daten ein.

   Der Webserver überträgt die Excel-Datei mit den zusammenfassenden Informationen per Push-Vorgang auf den Browser.
2. Speichern Sie die Datei lokal.
3. Verwenden Sie eine Anwendung, die Excel-formatierte Tabellen lesen kann, um die Datei zu öffnen.

Einstellen der pro Seite zulässigen Einträge

Erhöhen Sie die Anzahl der in Übersichtslisten zulässigen Einträge.

Standardmäßig beschränkt Avamar Client Manager seine Übersichtslisten auf 25 Einträge pro Seite. Wenn die Anzahl der Einträge das pro Seite zulässige Limit an aktuellen Einträgen überschreitet, werden die Einträge auf zwei oder mehr Seiten angezeigt. Sie können das Limit für die pro Seite zulässigen Einträge erhöhen, um die Arbeit mit vielen Einträgen zu vereinfachen.

Vorgehensweise

1. Klicken Sie unten in der Avamar Client Manager-Statusleiste auf **Entries Per Page**.

   Daraufhin wird eine Auswahlliste angezeigt.
2. Klicken Sie auf eine Zahl in der Liste.

Ergebnisse

Avamar Client Manager legt die ausgewählte Zahl als das neue Limit fest und aktualisiert die Seite.

Anzeigen von Sprechblasenmeldungen

Aktivieren Sie Sprechblasenmeldungen, um kurze Hilfemeldungen für verschiedene Elemente der Benutzeroberfläche anzuzeigen.

Vorgehensweise

1. Wählen Sie unten in der Avamar Client Manager-Statusleiste die Option **Show Tooltips** aus.
2. Bewegen Sie den Zeiger über ein Benutzeroberflächenelement mit Sprechblasenmeldung.

   Die folgenden Elemente weisen u. U. Sprechblasenmeldungen auf:

   - Diagramm-/Tabellenabschnitte des Dashboard
   - Steuerelemente
   - Spaltenüberschriften

Übersicht

Die Seite „Overview“ bietet Zugriff auf übergeordnete Informationen zum Management von Avamar-Clients. Außerdem bietet sie Tools für die Verwaltung von Avamar-Servern.

Wählen Sie im Menü auf der linken Seite der Seite „Overview“ Folgendes aus:

- **Server Summary**
  Wählen Sie **Server Summary** aus, um Informationen über den ausgewählten Avamar-Server anzuzeigen, einen Avamar-Server hinzuzufügen, einen Avamar-Server zu entfernen oder die Einstellungen für einen Avamar-Server zu bearbeiten.
- **Dashboard**
  Wählen Sie **Dashboard** aus, um Informationen über die Clientbackups für den ausgewählten Avamar-Server anzuzeigen.

Server Summary

Der Abschnitt **Server Summary** der Seite „Overview“ enthält Spalten mit Informationen über die von Avamar Client Manager gemanagten Avamar-Server.

Filtern Sie diese Informationen mithilfe der in der Leiste „Filters“ verfügbaren Filter. Ändern Sie die für die Liste verwendete Sortiermethode, indem Sie auf eine Spaltenüberschrift klicken.

Klicken Sie in jeder der folgenden Spalten auf einen Wert ungleich Null, um einen ausführlicheren Bericht über die Informationen der jeweiligen Spalte zu erhalten:

- Active Clients
- Idle Clients
- Successful Clients
- Failed Clients

Spalten der Seite Server Summary

In der folgenden Tabelle werden die Spalten beschrieben, die im Abschnitt **Serverübersicht** der Übersichtsseite verwendet werden.

Tabelle 97 Spalten auf der Seite „Serverübersicht“

Spalte	Beschreibung
Server	Hostname oder IP-Adresse des Avamar-Servers.
Version	Version der auf dem Avamar-Server installierten Version der Avamar-Serversoftware
Total Clients	Gesamtanzahl der beim Avamar-Server registrierten Clients. Enthält keine stillgelegten Clients.
Active Clients	Gesamtanzahl der Clients mit Aktivität (Backup oder Wiederherstellung) im angegebenen Zeitraum.
Idle Clients	Gesamtzahl der Clients ohne Backupaktivität im angegebenen Zeitraum.
Successful Clients	Gesamtanzahl der Clients mit einem Backupstatus, der dem im Filter **Successful Backups** festgelegten Wert entspricht. Umfasst ebenfalls den durchschnittlichen Zeitaufwand für diese Backups.
Failed Clients	Gesamtanzahl der Clients mit fehlgeschlagenen Backups während des angegebenen Zeitraums.
Clients with Restore	Gesamtanzahl der Clients mit Wiederherstellungsaktivität (erfolgreich oder nicht erfolgreich) im angegebenen Zeitraum.

Dashboard

Der Abschnitt **Dashboard** der Übersichtsseite liefert eine grafische Snapshot-Ansicht des ausgewählten Servers.

Im Dashboard werden Informationen in Form von Bereichen bereitgestellt, die Sie erweitern, reduzieren oder löschen können, um die benötigte Ansicht zu erstellen.

Verwendungstipps:

- Reduzieren oder erweitern Sie einen Bereich, indem Sie in der Titelleiste des Bereichs auf das Pfeilsymbol klicken.
- Setzen Sie das Dashboard auf seine Standardansicht zurück, indem Sie die Seite im Webbrowser neu laden.

Einstellen des Zeitraums für einen Bereich

Legen Sie den Zeitraum für einen Bereich fest, um zu definieren, für wie viele Tage Daten angezeigt werden.

Bevor Sie beginnen

Navigieren Sie zum Abschnitt **Dashboard** der Übersichtsseite, wobei eines oder mehrere der folgenden Fenster angezeigt werden: **Analysieren**, **Backupbericht** und **Backuptrend**.

Vorgehensweise

1. Klicken Sie in einem Bereich im Feld „Period“ auf das Pfeilsymbol.

   Das Feld „Period“ ist in den folgenden Bereichen verfügbar:

   - Analysieren
   - Backup Report
   - Backup Trend

   Die Zeitraumliste wird angezeigt.
2. Wählen Sie einen Zeitraum aus.

   Zur Auswahl stehen die folgenden Optionen:

   - Last 24 hours
   - Last 7 days
   - Letzte 30 Tage

   Avamar Client Manager aktualisiert den Bereich mit den Daten für den ausgewählten Zeitraum.

Bereich „Client“

Im Bereich **Client** wird in einem Tortendiagramm die Gesamtzahl potenzieller Clients für den ausgewählten Server dargestellt. Anhand von Farben wird der Prozentsatz für die jeweilige Gesamtanzahl der Clients wie folgt angezeigt:

- Aktiviert
  Grün steht für den Prozentsatz der Clients, die der ausgewählte Server aktiviert hat.
- Nicht aktiviert
  Rot steht für den Prozentsatz der Clients, die der ausgewählte Server registriert, aber nicht aktiviert hat.
- Frei
  Grau steht für den Prozentsatz nicht verwendeter Clientverbindungen, die auf dem ausgewählten Server verfügbar sind.

Bereich „Server“

Im Bereich **Server** werden über eine Tabellenansicht Informationen über den ausgewählten Server zur Verfügung gestellt.

Tabelle 98 Serverinformationen im Bereich „Server“

Spalte	Beschreibung
Node Type	Legt den Node-Typ des Servers fest: „Single“ oder „Multi“
Active Backup	Anzahl der ausgeführten Backups
Backup in Queue	Anzahl der Backups in der Serverwarteschlange, die auf ihre Ausführung warten
Replication	Aktueller Status des Replikations-Cron-Jobs:

Tabelle 98 Serverinformationen im Bereich „Server“ (Fortsetzung)

Spalte	Beschreibung
	• Running • Not running
Status	Aktueller Status des Management Console Server(MCS)-Systems des Servers: • Aktiv • Down

Bereich „Backup Trend“

Im Bereich **Backuptrend** wird über ein Liniendiagramm die Größe der gesicherten Daten zu bestimmten Points-in-Time eines definierten Zeitraums dargestellt. Die X-Achse steht für Points-in-Time über den ausgewählten Zeitraum. Die Y-Achse steht für die Größe der Daten im Backup zum jeweiligen Point-in-Time.

Die zwischen den gezeichneten Punkten gezogene Linie gibt den Backuptrend an, also die Veränderung bei den im Laufe der Zeit gesicherten Daten.

Bereich „Client Type“

Im Bereich **Clienttyp** wird für die ausgewählten Server in einem Balkendiagramm die Anzahl der aktivierten Clients aus den folgenden Kategorien angezeigt:

- Regular
  Alle aktivierten Clients, die zu keiner der drei anderen Kategorien passen
- vMachine
  Gastclients. Die virtuellen Computer, die über die auf dem Hostcomputer ausgeführte Avamar-Clientsoftware gesichert wurden.
- Proxy
  Proxy-VM-Clients. Clients, die Avamar für VMware-Image-Backups und -Wiederherstellungen verwenden.
- vCenter
  Avamar-Clients, die die vCenter-Managementinfrastruktur durch das Sichern von vCenter-Hosts schützen.

Bereich „Analyze“

Im Bereich **Analysieren** wird mit einem Balkendiagramm die Anzahl der Clients dargestellt, die sich während des ausgewählten Zeitraums jeweils in den folgenden Status befinden:

- Erfolgreich
  Clients mit mindestens einem erfolgreichen Backup
- Fehlgeschlagen
  Clients mit Backupaktivität, aber ohne erfolgreiche Backups
- Leerlauf
  Clients ohne Backupaktivität

Bereich „Backup Report“

Im Bereich **Backupbericht** wird über ein Balkendiagramm die Anzahl der während des ausgewählten Zeitraums gestarteten Backups mit den folgenden Ergebnissen dargestellt:

- Erfolgreich
  Erfolgreich abgeschlossene Backups; mit oder ohne Fehler
- Fehlgeschlagen
  Backups, die nicht abgeschlossen werden konnten
- Abgebrochen
  Backups, die vor dem Abschluss abgebrochen wurden

Bereich „Client Queues“

Im Bereich **Clientwarteschlangen** wird über ein Balkendiagramm die Anzahl der Clients in den folgenden Warteschlangen angezeigt:

- Upgrade
- Move to server
- Activation

Bereich „Storage Capacity“

Im Bereich **Speicherkapazität** wird über ein Tortendiagramm die Gesamtspeicherkapazität des ausgewählten Servers dargestellt. Die farbigen Stücke stehen für Folgendes:

- Verwendet
  Rot steht für den Anteil des Speichers, der Daten enthält.
- Freie Kapazität
  Grün steht für den Anteil des Speichers, der nicht belegt und damit verfügbar ist.

Bereich „Backup Health“

Im Bereich **Backupintegrität** wird über ein Balkendiagramm die Anzahl der Clients dargestellt, die Backupdaten über einen bestimmten Zeitraum aufbewahrt haben. Dabei werden die folgenden Zeiträume verwendet: 1 Tag, 30 Tage, 60 Tage und 90 Tage.

Die X-Achse des Balkendiagramms steht für den Zeitraum, über den Avamar die Daten aufbewahrt hat, die Y-Achse für die Anzahl der Clients.

Clients

Die Seite „Clients“ stellt Informationen und Tools zum Arbeiten mit Avamar-Clients bereit.

Über diese Seite ist Folgendes möglich:

- Auswählen der Computer in der Domain des Unternehmens und Hinzufügen dieser Computer als Avamar-Clients
- Anzeigen ausführlicher Informationen über die einzelnen Clients
- Verschieben, Stilllegen und Löschen von Clients
- Ändern der Gruppenzuordnungen eines Clients

- Durchführen von Upgrades der Avamar-Software auf dem Client

Um zwischen den Abschnitten der Seite „Clients“ zu navigieren, wählen Sie aus den Optionen des Menüs auf der linken Seite aus.

Client- und Servertools

Avamar Client Manager stellt verschiedene Tools für das Management von Avamar-Clients und Avamar-Servern bereit.

Ein Tool wird nur dann angezeigt, wenn es für den Kontext relevant ist. Vom Tool durchgeführte Änderungen gelten für den ausgewählten Client und den ausgewählten Server. Starten Sie ein Tool, indem Sie auf die zugehörige Befehlsschaltfläche klicken.

Erstellen einer Avamar-Domain

Erstellen Sie eine Avamar-Domain, um der Administrationshierarchie eines Avamar-Servers eine Verzweigung hinzuzufügen.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die **Create Domain** enthält: entweder im Dialogfeld **Add New Clients** oder im Dialogfeld **Client Move**.

Vorgehensweise

1. Wählen Sie im Bereich **Domain** den Speicherort für die neue Domain.

   Um die neue Domain direkt unterhalb der Root-Domain zu platzieren, wählen Sie das Serversymbol aus. Um die neue Domain unterhalb einer anderen Domain zu platzieren, wählen Sie diese Domain aus.

2. Klicken Sie auf **Create Domain**.

   Das Dialogfeld **New domain** wird angezeigt.

3. Geben Sie unter **New Domain Name** einen Namen für die Domain ein.

   In Avamar sind die folgenden Zeichen in Domainnamen unzulässig: `=~!@$^%(){}[]|,`;#\/:*?<>'"&+`

4. (Optional) Geben Sie die entsprechenden Informationen in den Feldern **Contact**, **Phone**, **Email** und **Location** ein.
5. Klicken Sie auf **OK**.

Ergebnisse

Avamar Client Manager fügt dem ausgewählten Server die neue Domain hinzu und die neue Domain wird im Bereich **Domain Selection** angezeigt.

Anzeigen der Gruppenzuordnungen eines Clients

Um die für einen Client geltenden Policies zu ermitteln, zeigen Sie die Gruppen an, die den Client enthalten.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste „Aktionen“ die Option **Gruppenzuordnungen** enthält.

Die Gruppenzuordnungen eines Clients legen das Backup-Dataset, die Backupplanung und die Backupaufbewahrungsfrist des Clients fest.

Vorgehensweise

1. Wählen Sie einen Client aus.

2. Klicken Sie auf **Group Associations**.

Ergebnisse

Das Dialogfeld **Groups for Client** wird mit aufgeführten Clientgruppen angezeigt.

Hinzufügen von Gruppenzuordnungen zu einem Client

Um die Policies einer Gruppe auf einen Client anzuwenden, fügen Sie dem Client die Gruppenzuordnung hinzu.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste „Aktionen“ die Option **Gruppenzuordnungen** enthält.

Bei dieser Aufgabe wird eine Zuordnung zwischen einem Client und einer Gruppe erstellt. Der Avamar-Server wendet die Policies der Gruppe auf den Client an.

Vorgehensweise

1. Wählen Sie einen Client aus.
2. Klicken Sie auf **Group Associations**.
3. Klicken Sie im Dialogfeld **Groups for Client** auf **Add Groups**.

   Das Dialogfeld **Add Groups for Client** wird angezeigt.
4. Wählen Sie eine Gruppe aus.

   Sie können mehrere Gruppen auswählen.
5. Klicken Sie auf **Add**.

Ergebnisse

Avamar Client Manager fügt dem Client die Gruppenzuordnungen hinzu.

Erstellen einer Gruppe

Um einen neuen Satz Policies zwecks Zuweisung zu Clients zur Verfügung zu stellen, erstellen Sie eine Gruppe mit den Policies. Der Befehl „Create Group“ ist beim Hinzufügen eines Clients zu einer Gruppe und beim Verschieben eines Clients in eine neue Domain oder auf einen neuen Server verfügbar.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die **Create Group** enthält: entweder im Dialogfeld **Add Groups** oder im Dialogfeld **Client Move**.

Vorgehensweise

1. Klicken Sie auf **Create Group**.

   Im Dialogfeld **Client verschieben** wird die Schaltfläche durch Auswahl einer Domain aktiviert.

   Das Dialogfeld **Create Group in Domain** wird angezeigt.
2. Geben Sie unter **Group Name** einen Namen für die neue Gruppe ein.

   In Avamar sind die folgenden Zeichen in Gruppennamen unzulässig: `=~!@$^%()
   {}[]|,`;#\/:*?<>'"&+`
3. (Optional) Wählen Sie **Enable** aus, um geplante Backups von Clients zu aktivieren, die der Gruppe zugewiesen werden.

   Deaktivieren Sie dieses Kontrollkästchen, um geplante Backups von Clients zu deaktivieren, die Sie der Gruppe zuweisen.

4. Wählen Sie unter **Dataset** ein Dataset für die Gruppe aus.
5. Wählen Sie unter **Schedule** eine Planung für die Gruppe aus.
6. Wählen Sie unter **Retention Policy** eine Aufbewahrungs-Policy für die Gruppe aus.
7. Klicken Sie auf **OK**.

Ergebnisse

Avamar Client Manager erstellt die Gruppe in der ausgewählten Domain.

Entfernen von Gruppenzuordnungen von einem Client

Damit die Policies einer Gruppe nicht mehr auf einen Client angewendet werden, entfernen Sie die Gruppenzuordnung von dem Client.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, die in der Leiste „Aktionen“ die Option **Gruppenzuordnungen** enthält.

Bei dieser Aufgabe wird die Zuordnung zwischen einem Client und einer Gruppe entfernt. Bei Abschluss dieser Aufgabe gelten die Policies der Gruppe nicht länger für den Client.

Vorgehensweise

1. Wählen Sie einen Client aus.
2. Klicken Sie auf **Group Associations**.
3. Wählen Sie im Dialogfeld **Groups for Client** eine Gruppe aus.

   Sie können mehrere Gruppen auswählen.
4. Klicken Sie auf **Remove**.

Ergebnisse

Avamar Client Manager entfernt die Zuordnung zwischen dem Client und den ausgewählten Gruppen.

Außerkraftsetzen von Gruppen-Policy-Einstellungen für einen Client

Um die auf einen Client angewendeten Policies zu ändern, setzen Sie die Policies seiner Gruppe außer Kraft.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, in der **Details anzeigen/bearbeiten** in der Leiste **Aktionen** und der Client in der Clientliste angezeigt werden.

Vorgehensweise

1. Wählen Sie einen Client aus.
2. Klicken Sie in der Leiste **Actions** auf **View/Edit Details**.

   Das Dialogfeld **Clientdetails** wird angezeigt.
3. Wählen Sie die Registerkarte **Advanced** aus.

   Die Einstellungen zum Außerkraftsetzen von Policies werden mit dem aktuell angezeigten Status des Clients angezeigt.
4. Ändern Sie den aktuellen Status des Clients, indem Sie Einstellungen auswählen oder aufheben.

5. Klicken Sie auf **OK**.

Ergebnisse

Avamar Client Manager ändert die Gruppen-Policy-Einstellungen für den Client.

Einstellungen zum Außerkraftsetzen von Gruppen-Policies

Um eine auf einen Client angewendete Policy zu ändern, verwenden Sie eine der Einstellungen zum Außerkraftsetzen von Policies.

In der folgenden Tabelle werden die Einstellungen zum Außerkraftsetzen von Policies auf der Registerkarte **Advanced** des Dialogfelds **Client Details** beschrieben.

Tabelle 99 Einstellungen auf der Registerkarte „Advanced“ des Dialogfelds „Client Details“

Einstellung	Beschreibung
Override group retention	Hiermit können Sie einem Client eine von der Gruppeneinstellung abweichende Aufbewahrungseinstellung zuweisen. Weisen Sie nach der Auswahl dieser Option eine Aufbewahrungseinstellung zu, indem Sie sie aus der Liste **Select an existing retention policy** auswählen.
Select an existing retention policy	Liste verfügbarer Aufbewahrungseinstellungen, die einem Client zugewiesen werden können. Um diese Liste zu verwenden, wählen Sie zunächst **Override group retention** aus.
Disable all backups	Deaktiviert alle Backups des Clients. Benutzer können Daten nach wie vor wiederherstellen.
Aktiviert	Versetzt einen registrierten Client in einen aktivierten Status. Wenn Sie diese Einstellung aufheben, können Benutzer weder Backups noch Wiederherstellungen durchführen.
Allow client-initiated backups	Ermöglicht Benutzern, Backups vom Client zu starten.
Allow file selection for client-initiated backups	Ermöglicht Benutzern, Dateien auszuwählen, die in die vom Client gestarteten Backups aufgenommen werden sollen. Die Ausschlussliste für das Dataset der Gruppe hat keine Gültigkeit.
Allow client to add to dataset	Ermöglicht Benutzern, Ordner zu den Datasets der Clientgruppen hinzuzufügen. Diese Einstellung ist folgenden Regeln unterworfen: • Der Avamar-Server filtert die hinzugefügten Daten anhand der Ausschluss- und Einschlussliste der Gruppe. • Die hinzugefügten Daten sind in jedem geplanten und On-Demand-

Tabelle 99 Einstellungen auf der Registerkarte „Advanced“ des Dialogfelds „Client Details“ (Fortsetzung)

Einstellung	Beschreibung
	Backupvorgang für jede dem Client zugewiesene Gruppe vorhanden. • Benutzer müssen Zugriff auf die Avamar-Client-Webbenutzeroberfläche haben, um Ordner hinzuzufügen oder zu entfernen.
Allow client to override daily group schedules	Ermöglicht Benutzern, eine von der Startzeit für ihre Gruppe abweichende Startzeit für geplante Backups auszuwählen. Voraussetzungen: • Fügen Sie der „Override Schedule“ des Avamar-Servers Zeiteinträge hinzu. • Weisen Sie der Clientgruppe eine tägliche Planung zu. • Räumen Sie Benutzern Zugriff auf die Avamar-Client-Webbenutzeroberfläche ein, damit sie eine neue Planung auswählen können.
Allow client to override retention policy on client-initiated backups	Weist clientinitiierten Backups die unter **Vorhandene Aufbewahrungs-Policy auswählen** angegebene Aufbewahrungs-Policy zu. Voraussetzungen: • Aktivieren Sie **Override group retention**. • Aktivieren Sie **Allow client-initiated backups**.

Anzeigen zusammenfassender Informationen über einen Client

Verwenden Sie „Client Details“, um Informationen über einen Client und seine Benutzer anzuzeigen.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, in der **Details anzeigen/bearbeiten** in der Leiste **Aktionen** und der Client in der Clientliste angezeigt werden.

Vorgehensweise

1. Wählen Sie einen Client aus.
2. Klicken Sie in der Leiste **Actions** auf **View/Edit Details**.

   Das Dialogfeld **Clientdetails** wird angezeigt.
3. Wählen Sie die Registerkarte **Summary** aus.

Ergebnisse

Daraufhin werden Informationen über den Client angezeigt. Eine Liste der mit dem Client verknüpften Benutzer wird ebenfalls aufgerufen.

Ändern des Clientnamens auf dem Server

Wenn Sie den Hostnamen eines Computers ändern, müssen Sie auch den Namen ändern, der vom Avamar-Server verwendet wird, um den Computer als Avamar-Client zu identifizieren.

Bevor Sie beginnen

Ändern Sie den Hostnamen auf dem Computer und in DNS, bevor Sie diese Aufgabe durchführen. Navigieren Sie zu einer Ansicht, in der **Details anzeigen/bearbeiten** in der Leiste **Aktionen** und der Computer in der Clientliste angezeigt werden.

Vorgehensweise

1. Wählen Sie einen Client aus.
2. Klicken Sie in der Leiste **Actions** auf **View/Edit Details**.

   Das Dialogfeld **Clientdetails** wird angezeigt.
3. Wählen Sie die Registerkarte **Summary** aus.
4. Geben Sie unter **Clientname** den neuen Hostnamen für den Computer ein.
5. Klicken Sie auf **OK**.

Ergebnisse

Avamar Client Manager ersetzt den alten Hostnamen durch den neuen Hostnamen für den Avamar-Client auf dem Avamar-Server.

Anzeigen des Backupverlaufs eines Clients

Um zu ermitteln, ob ein Avamar-Server einen Client wie erwartet gesichert hat, rufen Sie den Backupverlauf des Clients auf.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, in der **Details anzeigen/bearbeiten** in der Leiste **Aktionen** und der Client in der Clientliste angezeigt werden.

Vorgehensweise

1. Wählen Sie einen Client aus.
2. Klicken Sie in der Leiste **Actions** auf **View/Edit Details**.

   Das Dialogfeld **Clientdetails** wird angezeigt.
3. Wählen Sie die Registerkarte **Backups** aus.
4. Wählen Sie unter **From** das Startdatum des anzuzeigenden Zeitraums aus.
5. Wählen Sie unter **To** das Enddatum des anzuzeigenden Zeitraums aus.
6. (Optional) Wählen Sie **On-demand backups** aus.

   Aktivieren Sie diese Option, um vom Benutzer initiierte Backups in die Ergebnisse aufzunehmen. Deaktivieren Sie diese Option, um solche Backups auszuschließen.
7. (Optional) Wählen Sie **Scheduled backups** aus.

   Aktivieren Sie diese Option, um Backups, mit denen eine Gruppenplanung beginnt, in die Ergebnisse aufzunehmen. Deaktivieren Sie diese Option, um solche Backups auszuschließen.

Ergebnisse

Eine Liste der Clientbackups, die mit den Filtereinstellungen übereinstimmen, wird angezeigt.

Anzeigen der installierten Plug-ins eines Clients

Zeigen Sie die auf einem Avamar-Client installierten Avamar-Plug-ins an, um die Art der in den Backups enthaltenen Daten ermitteln zu können.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, in der **Details anzeigen/bearbeiten** in der Leiste **Aktionen** und der Client in der Clientliste angezeigt werden.

Vorgehensweise

1. Wählen Sie einen Client aus.
2. Klicken Sie in der Leiste **Actions** auf **View/Edit Details**.

   Das Dialogfeld **Clientdetails** wird angezeigt.
3. Wählen Sie die Registerkarte **Plug-ins** aus.

Ergebnisse

Die auf diesem Client installierten Plug-ins werden angezeigt.

Löschen eines Clients von einem Server

Um die Datensätze und Backups eines Clients von einem Avamar-Server zu entfernen, löschen Sie den Client vom Server.

Bevor Sie beginnen

Navigieren Sie zu einer Ansicht, in der der Client in der Clientliste und die Option **Löschen** in der Leiste **Aktionen** angezeigt wird.

Wenn Avamar Client Manager einen Client von einem Avamar-Server löscht, werden alle Aktivitäten im Zusammenhang mit diesem Client gestoppt, die Backups des Clients gelöscht und alle Datensätze des Clients aus der Datenbank des Servers entfernt.

Vorgehensweise

1. Wählen Sie einen Client aus.
2. Klicken Sie auf der Leiste **Aktionen** auf **Löschen**.
3. Geben Sie im Dialogfeld **Bestätigen** Ihr Passwort ein.

   Verwenden Sie das Passwort des bei Avamar Client Manager angemeldeten Kontos.
4. Klicken Sie auf **OK**.

   Das Dialogfeld **Alert** wird angezeigt.
5. Klicken Sie auf **OK**.

Ergebnisse

Avamar Client Manager führt einen Prozess im Hintergrund aus, mit dem alle Informationen und Daten des Clients vom Server entfernt werden.

Hinzufügen von Clients

Der Abschnitt **Add Clients** stellt Informationen und Tools bereit, mit denen Sie die Computer im Unternehmen als Avamar-Clients registrieren und aktivieren können.

Verwenden Sie den Abschnitt **Clients hinzufügen**, um Informationen über die Computer im Unternehmen zu importieren. Importieren Sie die Informationen von einem unterstützten LDAP-Benennungssystem oder aus einer CSV-Datei.

Filtern Sie nach dem Importieren die Informationen nach Clientstatus und Clientname, um die Auswahl potenzieller Avamar-Clients zu unterstützen.

Verwenden Sie Avamar Client Manager, um die ausgewählten Computer bei einem Avamar-Server zu registrieren und zu aktivieren. Für den Abschluss des Aktivierungsprozesses sind die Installation der Avamar-Clientsoftware auf dem Computern und der Zugriff auf Avamar-Clientprozesse vom Server aus erforderlich. Der normale Workflow sieht vor, dass die Clientsoftware auf einem Computer installiert wird, bevor er zur Aktivierung ausgewählt wird.

Bereitstellen von Informationen über den Verzeichnisdienst

Sie können den Verzeichnisdienst eines Unternehmens verwenden, um Avamar Client Manager Informationen über die Computer bereitzustellen, die potenzielle Avamar-Clients sind.

Verwenden Sie einen unterstützten Verzeichnisdienst, der Informationen über die potenziellen Avamar-Client-Computer enthält. Avamar Client Manager richtet eine Abfrage an den Verzeichnisdienst, um Informationen über Clients und, sofern verfügbar, Organisationseinheiten des Verzeichnisdiensts wie Verzeichnisdomains und Verzeichnisgruppen abzurufen.

Bevor Sie die Verzeichnisdienstmethode zum Abrufen von Informationen über Computer in einer Domain verwenden können, müssen Sie Avamar Client Manager für die Verwendung des Verzeichnisdiensts konfigurieren.

Für die Verzeichnisdienstmethode ist Folgendes erforderlich:

- TCP/IP-Zugriff auf den Verzeichnisdienst von dem Server aus, auf dem Avamar Client Manager ausgeführt wird.
- Kontoinformationen für ein Benutzerkonto mit Lesezugriff auf den Verzeichnisdienst
- Name der Verzeichnisdienstdomain für die zu importierenden Computer

Importieren von Informationen aus einem Verzeichnisdienst

Um das Hinzufügen von Computern als Avamar-Clients vorzubereiten, importieren Sie Informationen über die Computer aus dem Verzeichnisdienst.

Bevor Sie beginnen

Gehen Sie folgendermaßen vor:

- Konfigurieren Sie Avamar Client Manager für die Verwendung des Verzeichnisdiensts.
- Beziehen Sie einen Benutzernamen sowie die zugehörige Domain und das entsprechende Passwort für ein Konto mit Lesezugriff auf den Verzeichnisdienst.
- Halten Sie den Namen der Verzeichnisdienstdomain der Computer bereit, die importiert werden.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Clients** > **Add Clients**.
2. Klicken Sie in der Leiste **Actions** auf **New Clients**.

   Das Dialogfeld **Client Information Source** wird angezeigt.
3. Wählen Sie **Active Directory** aus.
4. Wählen Sie unter **User Domain** die Domain des Kontos aus, über das Sie auf den Verzeichnisdienst zugreifen.

   Informationen zum Hinzufügen von Verzeichnisdienstdomains zu dieser Liste finden Sie im Administrationshandbuch.
5. Geben Sie unter **User Name** den Namen des Kontos ein.
6. Geben Sie unter **Password** das Passwort des Kontos ein.
7. Wählen Sie unter **Directory Domain** den Namen der Verzeichnisdienstdomain für die zu importierenden Computerinformationen aus.
8. Klicken Sie auf **OK**.

Ergebnisse

Avamar Client Manager importiert die Informationen aus dem Verzeichnisdienst.

Weitere Erfordernisse

Verwenden Sie die importierten Computerinformationen, um Computer als Clients eines Avamar-Servers auszuwählen und zu aktivieren.

Bereitstellen von Informationen über CSV-Dateien

Sie können eine kommagetrennte Datei (CSV) verwenden, um Avamar Client Manager Informationen über die Computer bereitzustellen, die potenzielle Avamar-Clients sind.

Erstellen Sie die CSV-Datei manuell oder anhand der Ausgabe eines Systemmanagementtools wie Microsoft System Center Configuration Manager oder Microsoft Systems Management Server.

Sie können die Ausgabe, die ein Systemmanagementtool während der Installation der Avamar-Clientsoftware auf einer Gruppe von Computern generiert, zum Erstellen der CSV-Datei verwenden. Es werden jedoch nur diejenigen Clients in Avamar Client Manager angezeigt, auf denen die Avamar-Clientsoftware erfolgreich installiert wurde.

Während des Hochladens einer CSV-Datei prüft Avamar Client Manager die Datei auf eine ordnungsgemäße Formatierung und bricht im Falle eines festgestellten Problems das Hochladen ab.

CSV-Dateiformat

Eine korrekt formatierte CSV-Datei berücksichtigt die folgenden Regeln:

- Es müssen mindestens zwei Zeilen vorhanden sein.
- Die Werte sind nur durch ein Komma voneinander getrennt.
- Die erste Zeile der Datei muss aus den wörtlichen Namen jedes Wertetyps bestehen.
  Der Name für den ersten Wert lautet `Hostname`. Der Name für den zweiten Wert lautet `Group`.
- Die zweite Zeile und alle darauffolgenden müssen über mindestens einen Wert verfügen und dürfen höchstens zwei Werte umfassen.
- Die Formatierungsregeln setzen einen ersten Wert, bestehend aus einem gültigen Hostnamen für einen Computer und einem nachgestellten Komma, voraus.

- Der zweite Wert ist zwar optional, aber wenn Sie diesen einschließen, muss es sich dabei um den logischen Gruppennamen des Verzeichnisdiensts für den Computer handeln.
  Wird kein zweiter Wert für einen Computer angegeben, führt Avamar Client Manager den Computer in der hierarchischen Anzeige auf Root-Ebene auf.
- Verwenden Sie für den zweiten Wert einen Schrägstrich (/), um die Hierarchieebenen des logischen Gruppennamens des Verzeichnisdiensts voneinander zu trennen.

Wenn Sie die Clientliste mithilfe eines Tabellenkalkulationsprogramms erstellen oder bearbeiten, fügen Sie bei dem Versuch, kommagetrennte Werte zu erstellen, kein Komma mit dem Wert hinzu. Das Hinzufügen eines Kommas zu dem Wert innerhalb des Tabellenkalkulationsprogramms kann eine falsch formatierte Datei zur Folge haben. Wenn Sie die Clientliste im Editor als CSV-Dateityp speichern, fügt der Editor die Kommatrennzeichen im Rahmen des Dateikonvertierungsprozesses hinzu. Zum Prüfen der Formatierung können Sie die Clientliste in einem Texteditor öffnen.

Beispiel einer korrekt formatierten Clientlistendatei
In einem Texteditor wird eine korrekt formatierte Clientlistendatei wie im folgenden Beispiel dargestellt.

```
Hostname,Group
User1-desktop.Acme.corp.com,acme.corp/USA/MA
User1-laptop.Acme.corp.com,acme.corp/USA/CA/SFO
User2-desktop.Acme.corp.com,acme.corp/Engineering
User3-desktop.Acme.corp.com,
User4-desktop.Acme.corp.com,
```

In der ersten Zeile werden die wörtlichen Namen jedes Wertetyps aufgeführt.

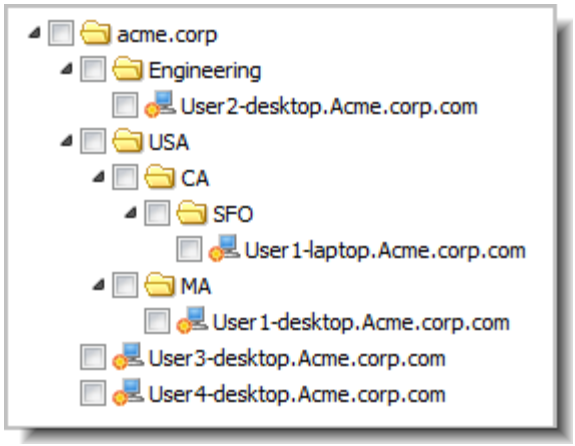
Die zweite Zeile enthält den Hostnamen `User1-desktop.Acme.corp.com`, das trennende Komma und die Gruppe `acme.corp/USA/MA`.

Die dritte Zeile enthält den Hostnamen `User1-laptop.Acme.corp.com`, das trennende Komma und die Gruppe `acme.corp/USA/CA/SFO`.

Die vierte Zeile enthält den Hostnamen `User2-desktop.Acme.corp.com`, das trennende Komma und die Gruppe `acme.corp/Engineering`.

Die fünfte und sechste Zeile enthalten nur die Hostnamen `User3-desktop.Acme.corp.com` und `User4-desktop.Acme.corp.com`, jeweils durch ein Komma getrennt. Die Formatierungsregeln setzen ein Komma voraus, selbst in Fällen ohne eine Gruppe. In den Zeilen werden keine Gruppen aufgelistet, sodass beide Hostnamen auf Root-Ebene der hierarchischen Anzeige angezeigt werden.

Abbildung 17 Anzeige nach dem Upload der beispielhaften CSV-Datei



Hochladen von Informationen in eine CSV-Datei

Um das Hinzufügen von Computern als Avamar-Clients vorzubereiten, laden Sie Informationen über die Computer in Form einer kommagetrennten Datei (Comma-Separated Values, CSV) hoch.

Bevor Sie beginnen

Erstellen Sie eine ordnungsgemäß formatierte CSV-Datei und machen Sie sie auf dem zum Navigieren im Internet verwendeten Computer verfügbar.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Clients** > **Add Clients**.
2. Klicken Sie in der Leiste **Actions** auf **New Clients**.

   Das Dialogfeld **Client Information Source** wird angezeigt.
3. Wählen Sie **CSV File** aus.
4. Klicken Sie auf **Browse**.

   Das Dialogfeld **Choose File to Upload** wird angezeigt.
5. Wechseln Sie zur CSV-Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**.
6. Klicken Sie im Dialogfeld **Client Information Source** auf **OK**.

Ergebnisse

Avamar Client Manager lädt die Informationen aus der CSV-Datei hoch.

Weitere Erfordernisse

Verwenden Sie die hochgeladenen Computerinformationen, um Computer als Clients eines Avamar-Servers auszuwählen und zu aktivieren.

Activation

Die Aktivierung umfasst die Änderung der Beziehung zwischen einem Computer und einem Avamar-Server, um dem Server das Management der Backups des Computers zu ermöglichen.

Die Beziehung durchläuft die in der folgenden Tabelle gezeigten drei Status.

Tabelle 100 Beziehungsstatus während der Clientaktivierung

Status	Beschreibung
Keine Beziehung	Der Computer ist dem Server unbekannt. Computer in diesem Status werden unter **Add Clients** angezeigt, wenn die Computerinformationen erstmalig zu Avamar Client Manager hinzugefügt werden.
Registriert	Avamar Client Manager hat die Informationen über den Computer zur Datenbank des Avamar-Servers hinzugefügt. Computer in diesem Status werden unter **Registered Clients** angezeigt, nachdem Avamar Client Manager den Aktivierungsprozess gestartet und die Registrierung beim Avamar-Server abgeschlossen hat. Der geänderte Status dieser Computer wird ebenfalls unter **Add Clients** angezeigt.
Aktiviert	Auf dem Computer ist die Avamar-Clientsoftware installiert und wird ausgeführt. Die Clientsoftware und der Server kommunizieren miteinander und haben zwecks Verifizierung ihrer Identität einen Chiffrierschlüssel ausgetauscht. Computer in diesem Status werden nach abgeschlossener Aktivierung unter **Activated Clients** angezeigt. Der geänderte Status dieser Computer wird ebenfalls unter **Add Clients** und **Registered Clients** angezeigt.

Ein Computer, der sich im Aktivierungsprozess befindet, wird auf der Seite **Queues** unter **Activation** aufgeführt. Avamar Client Manager versucht so lange, einen Computer alle 2 Stunden zu aktivieren, bis der Vorgang erfolgreich war oder das Limit von 24 Versuchen erreicht wurde. Beim Abschluss des Prozesses entfernt Avamar Client Manager den Computer aus dieser Anzeige und fügt auf der Seite **Logs** unter **Activation** einen Eintrag hinzu.

Aktivieren von Computern für die Ausführung des Backupmanagements

Um das Backupmanagement eines Clients zu ermöglichen, aktivieren Sie ihn bei einem Avamar-Server.

Bevor Sie beginnen

Installieren Sie die Avamar-Clientsoftware auf den Computern, die aktiviert werden, und importieren Sie Informationen über die Computer von einem Verzeichnisdienst oder aus einer CSV-Datei.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf Clients **Clients** > **Add Clients**.

   Daraufhin wird eine hierarchische Ansicht der Computer im Unternehmen angezeigt. Avamar Client Manager erzeugt diese Ansicht anhand der von Ihnen importierten Informationen.

2. Navigieren Sie in der Hierarchie oder durchsuchen Sie sie, um die zu aktivierenden Computer zu finden.

3. Wählen Sie jeden zu aktivierenden Computer aus.

   Um alle Computer in einem Ordner auszuwählen, erweitern Sie den Ordner, um die Computer anzuzeigen. Wählen Sie dann den Ordner aus.

4. Klicken Sie auf **Activate**.

   Das Dialogfeld **Server – Domain Selection** wird angezeigt.

5. Erweitern Sie die Auflistung für einen Server und wählen Sie eine Avamar-Domain aus.

   Avamar Client Manager weist die Computer dem ausgewählten Server und der ausgewählten Domain während der Aktivierung zu.

6. Klicken Sie auf **Next**.

   Das Dialogfeld **Server – Group Selection** wird angezeigt.

7. Wählen Sie eine Gruppe oder mehrere Gruppen aus.

   Avamar Client Manager weist die Computer der ausgewählten Gruppe bzw. den ausgewählten Gruppen während der Aktivierung zu.

8. Klicken Sie auf **Finish**.

Ergebnisse

Avamar Client Manager sendet die Aktivierungsaufgabe an die Warteschlange.

Weitere Erfordernisse

Um den Status des Aktivierungsprozesses zu ermitteln, prüfen Sie den Abschnitt **Activation** der Seite **Queues**. Prüfen Sie nach Abschluss des Prozesses den Abschnitt **Activation** der Seite **Logs**, um den endgültigen Status festzustellen.

Registrierte Clients

Clients, die von einem Avamar-Server registriert, aber nicht aktiviert wurden, werden im Abschnitt **Registered Clients** angezeigt.

Verwenden Sie den Abschnitt **Registrierte Clients**, um Clients auszuwählen und die folgenden clientbezogenen Aufgaben durchzuführen:

- Aktivieren
- Löschen
- Zuordnen zu Gruppen
- Anzeigen und Bearbeiten von Details
- Hinzufügen und Entfernen von Einstellungen zum Außerkraftsetzen von Gruppen

Aktivieren eines registrierten Clients

Um das Backupmanagement eines registrierten Clients zu aktivieren, dessen Aktivierung bei der Registrierung fehlgeschlagen ist, aktivieren Sie den Client über den Abschnitt **Registrierte Clients**.

Bevor Sie beginnen

Installieren Sie die Avamar-Clientsoftware auf den zu aktivierenden Computern.

Wenn die Aktivierung eines Computers als Client eines Avamar-Servers fehlschlägt, wird der Computer dennoch von Avamar Client Manager beim Server registriert. Beheben Sie ggf. Probleme, die die Aktivierung verhindern. Versuchen Sie dann erneut, den registrierten Client zu aktivieren.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Clients** > **Registered Clients**.
2. Wählen Sie jeden zu aktivierenden Client aus.
3. Klicken Sie auf **Activate**.

Ergebnisse

Avamar Client Manager sendet die Aktivierungsaufgabe an die Warteschlange.

Weitere Erfordernisse

Um den Status des Aktivierungsprozesses zu ermitteln, prüfen Sie den Abschnitt **Activation** der Seite **Queues**. Prüfen Sie nach Abschluss des Prozesses den Abschnitt **Activation** der Seite **Logs**, um den endgültigen Status festzustellen.

Aktivierte Clients

Clients, die für den ausgewählten Avamar-Server aktiviert sind, werden im Abschnitt **Activated Clients** angezeigt.

Verwenden Sie den Abschnitt **Aktivierte Clients**, um die folgenden Aufgaben durchzuführen:

- Verschieben des Clients auf einen anderen Server
- Verschieben des Clients in eine andere Avamar-Domain
- Stilllegen eines Clients
- Löschen eines Clients
- Managen der Gruppenzuordnungen eines Clients
- Anzeigen und Bearbeiten von Clientdetails
- Hinzufügen und Entfernen von Einstellungen zum Außerkraftsetzen von Gruppen

Verschieben eines Clients auf einen neuen Server

Um einen Avamar-Client über einen neuen Avamar-Server zu managen, verschieben Sie die Registrierung, die Aktivierung und die Backups des Avamar-Clients auf den neuen Server.

Bevor Sie beginnen

Gehen Sie folgendermaßen vor:

- Fügen Sie den Zielserver zu Avamar Client Manager hinzu, wie in Hinzufügen eines Avamar-Servers auf Seite 397 beschrieben.
- Wählen Sie einen Client aus, der bei einem Server mit Version 5.0.1.31 oder höher der Avamar-Serversoftware aktiviert ist.
- Initialisieren Sie für einen Client, der bei einem Avamar-Server vor Version 6.x aktiviert ist, den MCS-Prozess auf diesem Server vollständig.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Clients** > **Activated Clients**.
2. Wählen Sie einen Client aus.

   Wählen Sie keinen NDMP-Client aus. Wählen Sie keinen Client mit Backups auf einem Data Domain-Server aus.
3. Klicken Sie in der Leiste **Actions** auf **Move**.

   Der Bereich **Domain Selection** des Dialogfelds **Client Move** wird angezeigt.
4. Wählen Sie oben im Bereich **Domain Selection** den Avamar-Server aus der Serverauswahlliste aus, der das Ziel des Verschiebevorgangs ist.

   Die Domains des Zielservers werden im Bereich **Domain Selection** angezeigt.
5. Wählen Sie die Zieldomain im Bereich **Domain Selection** aus.

6. Klicken Sie auf **Next**.

   Der Bereich **Group Selection** des Dialogfelds **Client Move** wird angezeigt.

7. Wählen Sie eine Zielgruppe aus.

   Sie können optional mehrere Zielgruppen auswählen. Avamar Client Manager fügt den Client allen ausgewählten Gruppen hinzu.

8. Wählen Sie im Bereich **Group Selection** unter **Replicate Existing Backups** einen Wert aus.

Option	Beschreibung
Alle	Replizieren Sie alle Backups des Clients auf den Zielserver.
Letztes	Replizieren Sie nur das letzte Backup.
Keins	Replizieren Sie keine Backups.

   Nach einer Replikation sind die Backups über den Zielserver verfügbar.

9. (Optional) Gehen Sie unter **Delete From Source** wie folgt vor:
   - Wählen Sie die Option, mit der sämtliche Backups des Clients vom Quellserver entfernt werden.
   - Deaktivieren Sie die Option, um die Quellserverregistrierung des Clients in die MC_RETIRED-Domain des Quellservers zu verschieben und Kopien der Clientbackups auf dem Quellserver aufzubewahren.
10. Klicken Sie auf **Finish**.

    Das Dialogfeld **Confirm Replication Authentication** wird angezeigt.

11. Geben Sie unter **Source Server** das Passwort für das repluser-Konto auf dem Quellserver ein.
12. Geben Sie unter **Target Server** das Passwort für das repluser-Konto auf dem Zielserver ein.
13. Klicken Sie auf **OK**.

Ergebnisse

Über einen im Hintergrund ausgeführten Prozess verschiebt Avamar Client Manager den Client auf das ausgewählte Ziel.

Verschieben eines Clients in eine andere Avamar-Domain

Um die administrative Beziehung zwischen einem Avamar-Client und einem Avamar-Server zu ändern, können Sie den Client in eine andere Avamar-Domain verschieben.

Bevor Sie beginnen

Wählen Sie einen Client aus, der bei einem Server mit Version 6.x oder höher der Avamar-Serversoftware aktiviert ist.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Clients** > **Activated Clients**.
2. Wählen Sie einen Client aus.
3. Klicken Sie in der Leiste **Actions** auf **Move**.

   Das Dialogfeld **Client Move** wird angezeigt.

4. Wählen Sie im Bereich **Domain Selection** des Dialogfelds **Client Move** die Zieldomain aus.

5. Klicken Sie auf **Next**.

   Der Bereich **Group Selection** wird im Dialogfeld **Client Move** angezeigt.

6. Wählen Sie eine Zielgruppe aus.

   Sie können optional mehrere Zielgruppen auswählen. Avamar Client Manager fügt den Client allen ausgewählten Gruppen hinzu.

7. Klicken Sie auf **Finish**.

   Eine Warnmeldung wird angezeigt.

8. Klicken Sie auf **OK**.

Ergebnisse

Über einen im Hintergrund ausgeführten Prozess verschiebt Avamar Client Manager den Client auf das ausgewählte Ziel.

Stilllegen eines Clients

Legen Sie den Avamar-Client still, um die Erstellung von Backups eines Avamar-Clients zu beenden. Avamar Client Manager bewahrt Backups auf, die zum Zeitpunkt der Stilllegung vorhanden sind, sodass Sie diese bei Bedarf wiederherstellen können.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Clients** > **Activated Clients**.
2. Wählen Sie einen Client aus.

   Sie können mehrere Clients auswählen. Die von Ihnen ausgewählte Aufbewahrungs-Policy-Einstellung gilt für alle ausgewählten Clients.

3. Klicken Sie in der Leiste **Actions** auf **Retire**.

   Das Dialogfeld **Retire Client** wird angezeigt.

4. Wählen Sie eine der Optionen unter **Select Retention Policy** aus.

Option	Beschreibung
Retire client and retain backups with existing expiration date	Der Avamar-Server bewahrt die Backups während der bestehenden Aufbewahrungsfrist auf.
Retire client and retain all backups indefinitely	Der Avamar-Server bewahrt die Backups so lange auf, bis sie manuell gelöscht werden.
Retire client and reset backup expiration date	Der Avamar-Server bewahrt die Backups bis zu dem unter „New Expiration Date“ festgelegten Datum auf.

5. Wenn Sie im vorherigen Schritt **Retire client and reset backup expiration date** ausgewählt haben, dann legen Sie nun ein Datum unter **New Expiration Date** fest.

   Das Dialogfeld **Confirm** wird angezeigt.

6. Klicken Sie auf **Yes**.

   Das Dialogfeld **Alert** wird angezeigt.

7. Klicken Sie auf **OK**.

Ergebnisse

Über einen im Hintergrund ausgeführten Prozess legt Avamar Client Manager den ausgewählten Client still.

Failed Clients

Clients mit erfolgloser Backup- oder Wiederherstellungsaktivität werden im Abschnitt **Fehlgeschlagene Clients** angezeigt.

Verwenden Sie den Abschnitt **Fehlgeschlagene Clients**, um die folgenden Aufgaben durchzuführen:

- Löschen eines Clients
- Managen der Gruppenzuordnungen eines Clients
- Anzeigen und Bearbeiten von Clientdetails
- Hinzufügen und Entfernen von Einstellungen zum Außerkraftsetzen von Gruppen

Verwenden Sie beim Arbeiten mit fehlgeschlagenen Clients die in der folgenden Tabelle beschriebenen Filter.

Tabelle 101 Filter für fehlgeschlagene Clients

Filter	Beschreibung
Period	Legt den Zeitraum fest, den Avamar Client Manager untersucht.
Activity Type	Legt den Aktivitätstyp fest, den Avamar Client Manager untersucht.
Failure Criteria	Definiert den von Avamar Client Manager verwendeten Fehlerschwellenwert.

Idle Clients

Aktivierte Avamar-Clients, die über einen angegebenen Zeitraum keinerlei Aktivität aufweisen, werden im Abschnitt **Idle Clients** angezeigt.

Geben Sie beim Arbeiten mit Clients im Leerlauf über den Filter **Period** den Zeitraum an, den Avamar Client Manager auf Aktivitäten überprüfen soll, und legen Sie über den Filter **Activity Type** den Aktivitätstyp fest.

Verwenden Sie den Abschnitt **Clients im Leerlauf**, um die folgenden Aufgaben durchzuführen:

- Löschen eines Clients
- Managen der Gruppenzuordnungen eines Clients
- Anzeigen und Bearbeiten von Clientdetails
- Hinzufügen und Entfernen von Einstellungen zum Außerkraftsetzen von Gruppen

Clientupgrade

Der Abschnitt **Upgrade Clients** stellt Informationen und Tools bereit, mit denen Sie Upgrades und Hotfixes auf Avamar-Clients anwenden können.

Verwenden Sie den Abschnitt **Clientupgrade**, um die folgenden Aufgaben durchzuführen:

- Herunterladen eines Upgradepakets auf einen Server
- Auswählen eines Upgradepakets
- Anwenden des Pakets auf ausgewählte Clients
- Entfernen eines Upgradepakets vom Server

Anforderungen in Bezug auf den Abschnitt Upgrade Clients

Gehen Sie wie folgt vor, bevor Sie den Abschnitt **Upgrade Clients** von Avamar Client Manager verwenden:

- Installieren Sie für jeden Client bzw. jedes Plug-in die minimal erforderliche Clientversion, die in der Kompatibilitätstabelle für Avamar-Push-Clientupgrades im *Avamar Kompatibilitäts- und Interoperabilitätsmatrix* angegeben ist. Sie erhalten die neueste Version dieses Dokuments beim Avamar-Support unter http://compatibilityguide.emc.com:8080/CompGuideApp.

  Hinweis

  Die Verwendung der Funktion „Upgrade Clients“ zum Durchführen von Upgrades der Avamar-Clientsoftware auf Windows-Cluster-Nodes wird nicht unterstützt. Im *Avamar for Windows-Server – Benutzerhandbuch* wird das Durchführen von Upgrades der Avamar-Clientsoftware auf Windows-Cluster-Nodes beschrieben.

- Installieren und konfigurieren Sie den Avamar Downloader Service und führen Sie ihn aus. Der Avamar Downloader Service ruft die von der Upgradefunktion benötigten Client- und Plug-in-Pakete ab. Dieser Service bezieht die Pakete und stellt sie per Push-Vorgang auf dem Subsystem des Avamar Data Server (GSAN) bereit. Nach der Paketaktualisierung in GSAN werden die Pakete im Fenster **Select Package** von Avamar Client Manager angezeigt und Upgrades können durchgeführt werden.

Mehrere Systembereitstellungen

Bei Avamar-Bereitstellungen, die mehr als ein Avamar-System umfassen, können mithilfe von Avamar Client Manager – ausgeführt auf einem der Avamar-Systeme (managendes System) – die mit anderen Avamar-Systemen (gemanagten Systemen) verbundenen Clients gemanagt werden.

Die gemanagten Systeme müssen folgende Anforderungen erfüllen:

- Das gemanagte System wurde Avamar Client Manager auf dem Managementsystem hinzugefügt.
  Das Hinzufügen gemanagter Systeme zu Avamar Client Manager auf dem Managementsystem stellt dem Managementsystem die für die Unterstützung von Clientupgrades auf den gemanagten Systemen benötigten Informationen bereit.
- Das gemanagte System führt eine „Näherungsversion“ der Avamar-Software aus, bei der es sich ganz einfach um eine Version handelt, die nicht mehr als zwei Versionen älter ist als das managende System.

Die Anforderung, dass es sich um eine Näherungsversion handeln muss, sorgt dafür, dass alle für Clients auf den gemanagten Systemen erforderlichen Pakete durch das Managementsystem bereitgestellt werden können.

Führen Sie zwecks voller Upgradeunterstützung für mit Avamar-Systemen verbundenen Clients, die keine Näherungsversion besitzen, Avamar Client Manager auf diesen Systemen aus.

Herunterladen von Upgrade- und Hotfix-Paketen

Verwenden Sie Avamar Client Manager, um Upgrade- und Hotfix-Pakete auf einen Avamar-Server herunterzuladen.

Bevor Sie beginnen

Gehen Sie folgendermaßen vor:

- Installieren und konfigurieren Sie den Avamar Downloader Service und den AvInstaller-Dienst. Im Administrationshandbuch finden Sie Informationen über diese Aufgaben.
- Wählen Sie einen Avamar-Server aus.

Laden Sie vor dem Anwenden eines Upgrade- oder Hotfix-Pakets auf einen Avamar-Client das Paket auf den mit dem Avamar-Client verbundenen Avamar-Server herunter.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Clients** > **Upgrade Clients**.
2. Klicken Sie in der Leiste **Actions** auf **Select Package**.

   Das Dialogfeld **Upgrade Client** wird angezeigt.
3. Klicken Sie in der Spalte **Status** für das Paket auf **Download**.

   Der Status des Pakets muss `Available` lauten.

Ergebnisse

Avamar Client Manager beginnt mit dem Herunterladen. Eine Fortschrittsleiste wird angezeigt. Nach dem Herunterladen aktualisiert Avamar Client Manager den Paketstatus der Reihe nach auf die folgenden Werte: `Waiting`, `Processing` und `Ready`.

Auswählen eines Upgradepakets

Wählen Sie ein Upgrade- oder Hotfix-Paket aus, das auf Avamar-Clients angewendet werden soll.

Bevor Sie beginnen

Gehen Sie folgendermaßen vor:

- Installieren und konfigurieren Sie den Avamar Downloader Service und den AvInstaller-Dienst. Im Administrationshandbuch finden Sie Informationen über diese Aufgaben.
- Wählen Sie einen Avamar-Server aus.
- Laden Sie das Upgrade- oder Hotfix-Paket auf den ausgewählten Avamar-Server herunter.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Clients** > **Upgrade Clients**.
2. Klicken Sie in der Leiste **Actions** auf **Select Package**.

   Das Dialogfeld **Upgrade Client** wird angezeigt.
3. Wählen Sie ein Paket aus.

   Um ein Paket auswählen zu können, muss dieses den Status **Ready** aufweisen.

4. Klicken Sie auf **Select**.

   Das Dialogfeld **Upgrade Client** wird angezeigt.

Ergebnisse

Die Avamar-Clients, die für das Upgrade bzw. den Hotfix geeignet sind, werden angezeigt.

Weitere Erfordernisse

Wählen Sie Clients aus und wenden Sie das Upgrade- oder Hotfix-Paket auf sie an.

Anwenden des Upgradepakets

Wählen Sie die Avamar-Clients aus und wenden Sie das Upgrade- oder das Hotfix-Paket an.

Bevor Sie beginnen

Wählen Sie ein Upgrade- oder ein Hotfix-Paket aus. Zeigen Sie die Liste der Avamar-Clients an, die für das ausgewählte Paket geeignet sind.

HINWEIS

Die Anwendung eines Upgrades auf einen Avamar NDMP Accelerator Node (Accelerator Node) führt dazu, dass der Accelerator Node die Ausführung von Backups einstellt. Nach dem Upgrade wird der Accelerator Node gestartet und NDMP-Backups werden normal abgeschlossen.

Vorgehensweise

1. Wählen Sie aus der Liste der Avamar-Clients, die für das Upgrade bzw. Hotfix geeignet sind, einen Client aus.

   Sie können mehrere Clients auswählen.

2. Klicken Sie in der Leiste **Actions** auf **Upgrade**.

Ergebnisse

Avamar Client Manager beginnt mit dem Durchführen des Upgrades der ausgewählten Clients. Das Upgrade wird im Hintergrund ausgeführt.

Weitere Erfordernisse

Verfolgen Sie den Fortschritt des Upgrades im Abschnitt **Upgrade** der Seite **Queues** nach. Zeigen Sie den endgültigen Status des Upgrades im Abschnitt **Upgrade** der Seite **Logs** an.

Löschen von Upgrade- und Hotfix-Paketen

Verwenden Sie Avamar Client Manager, um Upgrade- und Hotfix-Pakete von einem Avamar-Server zu löschen.

Bevor Sie beginnen

Wählen Sie einen Avamar-Server mit einem nicht benötigten Upgrade- oder Hotfix-Paket aus.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Clients** > **Upgrade Clients**.
2. Klicken Sie in der Leiste **Actions** auf **Select Package**.

   Das Dialogfeld **Upgrade Client** wird angezeigt.

3. Wählen Sie ein Paket aus.

   Sie können nur Pakete mit dem Status **Ready** löschen.

4. Klicken Sie auf **Delete**.

Ergebnisse

Avamar Client Manager entfernt das ausgewählte Paket vom Avamar-Server.

Policies

Die Seite „Policies“ ermöglicht den Zugriff auf Gruppen-Policy-Aufgaben und Informationen.

Die Seite „Policies“ enthält eine Übersicht über jede Gruppen-Policy auf dem ausgewählten Avamar-Server.

Verwenden Sie die Seite „Policies“, um die folgenden Aufgaben durchzuführen:

- Hinzufügen von Clients zu einer Gruppe
- Entfernen von Clients aus einer Gruppe
- Anzeigen der Details der Dataset Policy, Aufbewahrungs-Policy und Planungs-Policy einer Gruppe

Hinzufügen von Clients zu einer Gruppe

Um die Policies einer Gruppe auf ausgewählte Clients anzuwenden, fügen Sie die Clients der Gruppe hinzu.

Nach Abschluss dieser Aufgaben wurden die ausgewählten Clients einer Gruppe zugeordnet. Der Avamar-Server wendet dann die Policies der Gruppe auf die ausgewählten Clients an.

Vorgehensweise

1. Klicken Sie auf **Policies** > **Groups**.
2. Wählen Sie eine Gruppe aus.
3. Klicken Sie auf **Edit Group Members**.

   Das Dialogfeld **Edit Group Members** wird angezeigt.

4. Klicken Sie auf **Add**.

   Das Dialogfeld **Add Clients to Group** wird angezeigt.

5. Wählen Sie einen Client aus.

   Sie können mehrere Clients auswählen.

6. Klicken Sie auf **Add**.

Ergebnisse

Avamar Client Manager fügt die Clients zur Gruppe hinzu.

Entfernen von Clients aus einer Gruppe

Um die Policies einer Gruppe von ausgewählten Clients zu entfernen, entfernen Sie die Clients aus der Gruppe.

Bei dieser Aufgabe wird die Zuordnung zwischen ausgewählten Clients und einer Gruppe aufgehoben. Nach Abschluss dieser Aufgabe gelten die Policies der Gruppe nicht länger für die ausgewählten Clients.

Vorgehensweise

1. Klicken Sie auf **Policies** > **Groups**.
2. Wählen Sie eine Gruppe aus.
3. Klicken Sie auf **Edit Group Members**.

   Das Dialogfeld **Edit Group Members** wird angezeigt.
4. Wählen Sie einen Client aus.

   Sie können mehrere Clients auswählen.
5. Klicken Sie auf **Remove**.

Ergebnisse

Avamar Client Manager entfernt die Clients aus der Gruppe.

Anzeigen der Dataset-Policy einer Gruppe

Verwenden Sie den Gruppeneintrag auf der Seite „Policies“, um Details der Dataset-Policy der Gruppe anzuzeigen.

Vorgehensweise

1. Wählen Sie einen Avamar-Server aus.
2. Klicken Sie auf **Policies** > **Groups**.

   Daraufhin wird eine Übersicht der Gruppen auf dem ausgewählten Server angezeigt.
3. Klicken Sie im Eintrag einer Gruppe in der Spalte **Dataset** auf den Namen der Dataset-Policy.

Ergebnisse

Die Details der Dataset-Policy für die ausgewählte Gruppe werden in einem Dialogfeld angezeigt.

Anzeigen der Aufbewahrungs-Policy einer Gruppe

Verwenden Sie den Gruppeneintrag auf der Seite „Policies“, um Details der Aufbewahrungs-Policy der Gruppe anzuzeigen.

Vorgehensweise

1. Wählen Sie einen Avamar-Server aus.
2. Klicken Sie auf **Policies** > **Groups**.

   Daraufhin wird eine Übersicht der Gruppen auf dem ausgewählten Server angezeigt.
3. Klicken Sie für einen Gruppeneintrag in der Spalte **Retention** auf den Namen der Aufbewahrungs-Policy.

Ergebnisse

Die Details der Aufbewahrungs-Policy für die ausgewählte Gruppe werden in einem Dialogfeld angezeigt.

Anzeigen der Planungs-Policy einer Gruppe

Verwenden Sie den Gruppeneintrag auf der Seite „Policies“, um Details der Planungs-Policy der Gruppe anzuzeigen.

Vorgehensweise

1. Wählen Sie einen Avamar-Server aus.
2. Klicken Sie auf **Policies** > **Groups**.

   Daraufhin wird eine Übersicht der Gruppen auf dem ausgewählten Server angezeigt.
3. Klicken Sie für einen Gruppeneintrag in der Spalte **Schedule** auf den Namen der Planungs-Policy.

Ergebnisse

Die Details der Planungs-Policy für die ausgewählte Gruppe werden in einem Dialogfeld angezeigt.

Queues

Die Seite **Queues** ermöglicht den Zugriff auf die Aktivitätswarteschlangen von Avamar Client Manager.

Auf der Seite **Queues** wird eine Übersicht der aktiven und anstehenden Avamar Client Manager-Aufgaben für den ausgewählten Avamar-Server dargestellt. Aufgaben werden je nach Art der Aufgabe in verschiedenen Abschnitten angezeigt:

Tabelle 102 Aufgabenarten auf der Seite „Warteschlangen“

Aufgabenart	Navigationspfad	Beschreibung
Activation	**Queues** > **Activation**	Anzeigen aktiver und anstehender Aufgaben im Zusammenhang mit der Clientaktivierung
Delete	**Queues** > **Delete**	Anzeigen aktiver und anstehender Aufgaben im Zusammenhang mit der Entfernung von Clients von Avamar-Servern
Move	**Queues** > **Move**	Anzeigen aktiver und anstehender Aufgaben im Zusammenhang mit dem Verschieben von Clients zwischen Avamar-Servern
Retire	**Queues** > **Retire**	Anzeigen von aktiven und anstehenden Aufgaben im Zusammenhang mit dem Stilllegen von Avamar-Clients.
Upgrade	**Queues** > **Upgrade**	Anzeigen von aktiven und anstehenden Aufgaben im Zusammenhang mit dem Upgrade der Software auf Avamar-Clients

Verwenden Sie die Seite **Queues**, um die folgenden Aufgaben durchzuführen:

- Anzeigen der Details von aktiven und anstehenden Aufgaben
- Abbrechen von Aufgaben

Abbrechen einer Aufgabe

Brechen Sie eine anstehende Aufgabe ab, um deren Ausführung zu verhindern.

Sie können die Ausführung einer Aufgabe stoppen, indem Sie die Aufgabe abbrechen, während sie sich im Status „Pending“ befindet.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Queues** > ***task_queue***. Dabei bezeichnet *task_queue* den Abschnitt der Seite „Warteschlangen“ für die Art der Aufgabe, die abgebrochen werden soll.

   Um etwa eine Clientaktivierung abzubrechen, klicken Sie auf **Queues** > **Activation**.
2. Wählen Sie eine Aufgabe aus.
3. Klicken Sie auf **Cancel**.

   Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **OK**.

Ergebnisse

Avamar Client Manager entfernt die Aufgabe aus der Warteschlange, bricht die Aufgabe ab und fügt dem Protokoll einen Eintrag hinzu.

Protokolle

Die Seite „Logs“ ermöglicht den Zugriff auf die Protokolle von Avamar Client Manager.

Die Seite „Logs“ bietet eine Übersicht über die Avamar Client Manager-Protokolle. Protokolleinträge werden je nach Art der Aufgabe, durch die der Eintrag erzeugt wurde, in verschiedenen Abschnitten angezeigt.

Tabelle 103 Aufgabenarten auf der Seite „Protokolle“

Aufgabenart	Navigationspfad	Beschreibung
Activation	**Logs** > **Activation**	Anzeigen von Protokolleinträgen im Zusammenhang mit der Clientaktivierung
Löschen	**Logs** > **Delete**	Anzeigen von Protokolleinträgen im Zusammenhang mit dem Entfernen von Clients von Avamar-Servern
Move	**Logs** > **Move**	Anzeigen von Protokolleinträgen im Zusammenhang mit dem Verschieben von Clients zwischen Avamar-Servern
Retire	**Logs** > **Retire**	Anzeigen von Protokolleinträgen im Zusammenhang mit der Stilllegung von Avamar-Clients
Upgrade	**Logs** > **Upgrade**	Anzeigen von Protokolleinträgen im Zusammenhang mit dem Durchführen von Upgrades der Software auf Avamar-Clients

- Activation
  Klicken Sie auf **Logs** > **Activation**, um Protokolleinträge im Zusammenhang mit der Clientaktivierung anzuzeigen.
- Löschen
  Klicken Sie auf **Logs** > **Delete**, um Protokolleinträge im Zusammenhang mit dem Entfernen von Clients von Avamar-Servern anzuzeigen.

- Move
  Klicken Sie auf **Logs** > **Move**, um Protokolleinträge im Zusammenhang mit dem Verschieben von Clients zwischen Avamar-Servern anzuzeigen.
- Retire
  Klicken Sie auf **Logs** > **Retire**, um Protokolleinträge im Zusammenhang mit der Stilllegung von Avamar-Clients anzuzeigen.
- Upgrade
  Klicken Sie auf **Logs** > **Upgrade**, um Protokolleinträge im Zusammenhang mit dem Durchführen von Upgrades der Software auf Avamar-Clients anzuzeigen.

Verwenden Sie die Seite „Logs“, um die folgenden Aufgaben durchzuführen:

- Anzeigen von Protokolleinträgen
- Anzeigen des Clientprotokolls für Upgrades
- Löschen aller Protokolleinträge in einem Abschnitt

Anzeigen des Clientprotokolls nach dem Durchführen eines Upgrades eines Avamar-Clients

Zeigen Sie das lokale Protokoll des Avamar-Clients nach einem abgeschlossenen Upgradeversuch an.

Bevor Sie beginnen

Verwenden Sie Avamar Client Manager, um ein Upgradepaket oder einen Hotfix auf einen Avamar-Client anzuwenden.

Durch das Anzeigen des lokalen Protokolls eines Avamar-Clients können Details zu den Ursachen eines fehlgeschlagenen Clientupgrades geliefert werden.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Logs** > **Upgrade**.
2. Klicken Sie rechts auf der Seite auf die Leiste **Details**.

   Der Bereich **Details** wird erweitert.
3. Wählen Sie unter „Summary“ einen Protokolleintrag für das Clientupgrade aus.

   Ausführliche Informationen für den ausgewählten Protokolleintrag werden im Bereich **Details** angezeigt.
4. Klicken Sie im Bereich **Details** unter „Log“ auf **View Log**.

Ergebnisse

Das Fenster **Upgrade Log** wird geöffnet und das lokale Protokoll des Clients wird im Fenster angezeigt.

Weitere Erfordernisse

(Optional) Markieren und kopieren Sie Informationen aus dem lokalen Protokoll des Clients. Fügen Sie die kopierten Informationen in einen Texteditor ein.

Löschen aller Protokolleinträge in einem Abschnitt

Avamar Client Manager stellt eine Methode bereit, mit der Sie alle Protokolleinträge aus einem Aufgabenabschnitt der Seite „Logs“ entfernen können.

Bevor Sie beginnen

Schließen Sie mindestens eine Aufgabe ab, die zu einem Protokolleintrag in einem der Aufgabenabschnitte der Seite „Logs“ führt.

Vorgehensweise

1. Klicken Sie im Menü auf der linken Seite auf **Logs** > ***task_log***, wobei *task_log* für einen Abschnitt der Seite „Protokolle“ steht.

   Um z. B. alle Upgradeeinträge zu löschen, klicken Sie auf **Logs** > **Upgrade**.
2. Klicken Sie auf **Clear All**.

   Das Dialogfeld **Alert** wird angezeigt.
3. Klicken Sie auf **Yes**.

Ergebnisse

Avamar Client Manager entfernt alle Protokolleinträge für den ausgewählten Abschnitt.

KAPITEL 14

Avamar Desktop/Laptop

In diesem Kapitel werden folgende Themen behandelt:

Überblick über Avamar Desktop/Laptop

Avamar Desktop/Laptop ist eine Version der Avamar-Clientsoftware für Windows und Macintosh, die erweiterte Funktionen für Enterprise-Desktop- und -Laptopcomputer hinzufügt. Zahlreiche Avamar Desktop/Laptop-Funktionen sind ebenfalls auf unterstützten Linux-Computern verfügbar.

Clientinstallation und -management
In einer Unternehmensumgebung kann Avamar Desktop/Laptop mithilfe von Systemmanagementtools wie Microsoft Systems Management Server 2003 (SMS) per Push-Vorgang auf Windows- sowie Macintosh-Desktop- und -Laptopcomputern installiert werden.

Die Avamar Desktop/Laptop-Software kann auch lokal durch Starten des Installationsassistenten installiert werden.

Nach der Clientinstallation ist eine Aktivierung, ein Upgrade, eine Analyse und das Management der Clients über die Webbrowser-Benutzeroberfläche von Avamar Client Manager möglich.

Benutzerauthentifizierung
Avamar Client Manager-Benutzer werden durch einen Active Directory- oder OpenLDAP-vorgabenkonformen Verzeichnisdienst des Unternehmens authentifiziert, mit oder ohne Kerberos-Verschlüsselung. Benutzer können auch mithilfe der integrierten Avamar-Authentifizierung oder einer Kombination aus Avamar- und LDAP-Authentifizierung authentifiziert werden. NIS-Authentifizierung wird ebenfalls unterstützt.

Die Pass-Through-Authentifizierung versetzt Benutzer in die Lage, ohne Verwendung des Anmeldebildschirms auf die Webbenutzeroberfläche zuzugreifen. Es wird ein sicherer Benachrichtigungsmechanismus verwendet, um Benutzer basierend auf den Informationen vom Clientcomputer zu authentifizieren. Mittels Pass-Through-Authentifizierung können Administratoren Nicht-Domainbenutzern die Wiederherstellung von Dateien auf ihrem lokalen Konto auf dem Computer ermöglichen.

Benutzeroberflächen
Die Avamar Desktop/Laptop-Funktionen sind über zwei Benutzeroberflächen verfügbar:

- Die lokale Clientbenutzeroberfläche wird bei der Installation von Avamar Client für Windows bzw. Avamar Client für Mac OS X auf dem Clientcomputer installiert. In der Clientbenutzeroberfläche von Windows-Computern wird ein Avamar-Symbol im Infobereich („Taskleiste“), bei Mac-Computern in der Menüleiste angezeigt. Klicken Sie unter Windows mit der rechten Maustaste auf das Symbol bzw. klicken Sie unter Mac auf das Symbol, um das Clientmenü zu öffnen, über das auf die Backup-, Wiederherstellungs- und Programmeinstellungen sowie die Protokolle zugegriffen werden kann.
- Über die Webbrowser-Benutzeroberfläche (Webbenutzeroberfläche) lassen sich ein On-Demand-Backup bzw. eine On-Demand-Wiederherstellung starten, die Backup- und Wiederherstellungsaktivität für einen Clientcomputer anzeigen oder andere Backupeinstellungen für einen Clientcomputer konfigurieren.

Backup
Benutzer können ein On-Demand-Backup mit nur einem Klick im Clientmenü starten oder für ein interaktives On-Demand-Backup die Webbenutzeroberfläche aufrufen. Das Verhalten von On-Demand-Backups lässt sich u. a. durch folgende Optionen anpassen:

- Zulassen der benutzerseitigen Erstellung von On-Demand-Backupsätzen
- Beschränken der Gesamtanzahl der täglich pro Clientcomputer durchführbaren Backups
- Ändern der Aufbewahrungs-Policy für On-Demand-Backups
- Deaktivieren von On-Demand-Backups

Führen Sie geplante Backups aller Avamar Desktop/Laptop-Clients durch. Bei täglich geplanten Backups können Sie Benutzern erlauben, eine andere Startzeit für ihre Backups aus einer von Ihnen erstellten Liste verfügbarer Zeiten auszuwählen. Das System führt das Backup so bald wie möglich nach der ausgewählten Zeit aus.

Außerdem können Sie zulassen, dass Benutzer den Quelldaten Ordner hinzufügen, definiert durch die Gruppen, zu denen ein Client gehört. Die Ordner umfassen sowohl On-Demand-Backups als auch geplante Backups für den Client.

Wiederherstellung
Benutzer können nach wiederherzustellenden Ordnern, Dateien und Dateiversionen suchen bzw. dorthin navigieren und eine Wiederherstellung am ursprünglichen Speicherort oder an einem neuen Speicherort auf demselben Computer durchführen. Benutzer können Daten mit demselben Namen oder mit einem neuen Namen wiederherstellen.

Wenn Benutzer Daten am ursprünglichen Speicherort unter demselben Namen wiederherstellen, werden im Zuge des Wiederherstellungsprozesses alle aktuellen lokalen Dateiversionen mit den wiederhergestellten Dateien überschrieben. Dieser Wiederherstellungstyp ist nützlich, wenn die aktuellen lokalen Versionen Fehler enthalten oder Probleme mit beschädigten Daten aufweisen.

Benutzer können die Dateien auch an einem neuen Speicherort oder mit einem neuen Namen oder mit beiden Möglichkeiten wiederherstellen, um ein Überschreiben der aktuellen lokalen Dateiversionen zu vermeiden.

Domainbenutzer können Dateien von jedem Windows- oder Mac-Computer, auf dem sie über ein Benutzerprofil verfügen, auf dem Windows- oder Mac-Computer wiederherstellen, bei dem sie angemeldet sind.

Wenn sich umfangreiche Wiederherstellungsaufgaben auf die Netzwerkperformance auswirken, können Sie die von den Benutzern wiederherstellbare Datenmenge beschränken.

Benutzer dürfen nur jeweils eine Wiederherstellungsaufgabe initiieren. Zusätzliche Anforderungen werden blockiert und dem Benutzer wird eine entsprechende Meldung angezeigt. Sie können dieses Verhalten ändern, damit Benutzer mehrere Wiederherstellungsaufgaben starten können.

Aktivitätsverlauf
Die Seite **History** der Webbenutzeroberfläche liefert Statusangaben der letzten 14 Tage zu den Wiederherstellungs- und Backupaufgaben eines Clientcomputers sowie Listen mit den während dieses Zeitraums gesicherten Ordnern und Dateien. Domainbenutzer mit einem Benutzerprofil auf dem Quellcomputer können den Aktivitätsverlauf für den Quellcomputer von einem anderen Computer aus anzeigen.

Anforderungen für Avamar Desktop/Laptop

Bei der Entscheidung über die Merkmale der Bereitstellung eines Avamar-Systems, das am besten für die Unterstützung von Desktop- und Laptopclients eines Unternehmens geeignet ist, sollten Sie mit Avamar Vertriebsmitarbeitern

zusammenarbeiten. Die Umgebung muss die Anforderungen aus folgenden Bereichen erfüllen.

In diesem Handbuch ist eine Beschreibung der Anforderungen eines Avamar-Systems zur Unterstützung von Desktops und Laptops für alle Unternehmen leider nicht möglich. Der Leitfaden ist aufgrund der zahlreichen Unterschiede in der Desktop- und Laptoptopologie für jedes Unternehmen vorhanden.

Clientcomputeranforderungen

Avamar-Clientcomputer mit Avamar Desktop/Laptop müssen die in den folgenden Abschnitten angegebenen Mindestanforderungen erfüllen.

Betriebssystemanforderungen

Für Avamar Desktop/Laptop-Clientcomputer ist ein Windows-, Mac- oder Linux-Betriebssystem erforderlich, das für die Verwendung mit dem Avamar-Client unterstützt wird. Der *Avamar Kompatibilitäts- und Interoperabilitätsmatrix* unter http://compatibilityguide.emc.com:8080/CompGuideApp enthält eine vollständige und aktualisierte Liste.

Windows Server-, Mac OS X Server- und Linux-Computer, die die Anforderungen aus dem *Avamar Backup Clients – Benutzerhandbuch* erfüllen, werden als Clients der Serverklasse unterstützt. Generell funktionieren die Avamar Desktop-/Laptop-Erweiterungen für Computer der Serverklasse genauso wie für Desktop- und Laptopcomputer. Zu den Unterschieden gehören u. a.:

- Auf einem Computer der Serverklasse wird durch Klicken auf **Back Up Now** im Menü **Client** oder in der **Backup**erinnerung ein Backup des dem Computer individuell zugewiesenen Dataset gestartet.

  Um das Dataset, das einem Computer zugewiesen ist, anzuzeigen oder zu bearbeiten, verwenden Sie Avamar-Administrator zum Bearbeiten der Policy-Einstellungen für den Client. Anweisungen finden Sie unter Außerkraftsetzen von Gruppen-Policy-Einstellungen für einen Client auf Seite 137.
- Die Avamar Desktop/Laptop-Funktion zum Deaktivieren von Backups für Computer im Akkubetrieb steht für Computer der Serverklasse nicht zur Verfügung.

  Backups sind auf Computern der Serverklasse immer aktiviert.
- Nachdem lokal gestartete Wiederherstellungen auf Windows- und Macintosh-Computern der Serverklasse deaktiviert wurden, kann eine Wiederherstellung nur mithilfe von Avamar-Administrator durchgeführt werden.

  Benutzer mit lokalen Administratorrechten auf dem Computer der Serverklasse sind jedoch in der Lage, Backups auf einem anderen Computer wiederherzustellen.

Hardwareanforderungen

In der folgenden Tabelle sind die Hardwareanforderungen für Avamar Desktop/Laptop-Clientcomputer aufgeführt.

Tabelle 104 Avamar Desktop/Laptop-Hardwareanforderungen

Kategorie	Anforderung
CPU	1 GHz
RAM	1 GB
Festplattenspeicher	Für die Softwareinstallation sind mindestens 250 MB permanenter Festplattenspeicher

Tabelle 104 Avamar Desktop/Laptop-Hardwareanforderungen (Fortsetzung)

Kategorie	Anforderung
	erforderlich. Für die Snapshot-Technology und Systemstatusbackups ist möglicherweise zusätzlicher Speicherplatz erforderlich.
Netzwerkschnittstelle	Eine der folgenden: • 10BaseT oder höher, mit den neuesten Treibern für die Plattform konfiguriert • IEEE 802.11a/b/g, mit den neuesten Treibern für die Plattform konfiguriert

Unterstützte Avamar-Plug-ins

Avamar Desktop/Laptop unterstützt Backups und Wiederherstellungen mit den folgenden Avamar-Dateisystem-Plug-ins:

- Windows
- Mac
- Linux

Avamar Desktop/Laptop bietet keine Unterstützung für Anwendungs-Plug-ins oder Dateisystem-Plug-ins anderer Betriebssysteme.

Portanforderungen

Der TCP-Datenport muss eine bidirektionale Kommunikation mit dem Avamar-Server ermöglichen.

Webbrowseranforderungen

Der für die Avamar Desktop/Laptop-Benutzeroberfläche verwendete Webbrowser muss JavaScript-aktiviert sein und weitere Anforderungen erfüllen.

In der folgenden Tabelle werden unterstützte Webbrowser aufgeführt.

Tabelle 105 Unterstützte Webbrowser fürAvamar Desktop/Laptop

Betriebssystem	Unterstützte Webbrowser
Windows	• Windows Internet Explorer • Mozilla Firefox
Macintosh	Apple Safari
Linux	Mozilla Firefox

Hinweis

Browser, die die Avamar-Software verwenden, müssen die TLS 1.2-Verschlüsselung unterstützen.

Verwenden Sie eine der Umgebungsvariablen in der folgenden Tabelle, um den Webbrowser zu starten.

Tabelle 106 Umgebungsvariablen zum Starten eines Webbrowsers in Avamar Desktop/Laptop

Browser	Umgebungsvariable
KDE	`kfmclient`
GNOME	`gnome-open`
Others	`BROWSER`

Netzwerkanforderungen

Das Netzwerk in einer Avamar Desktop/Laptop-Umgebung muss die in der folgenden Tabelle angegebenen Anforderungen erfüllen.

Tabelle 107 Avamar Desktop/Laptop-Netzwerkanforderungen

Kategorie	Anforderung
Protokoll	TCP/IP.
Router	Muss das Routing von TCP-Paketen zwischen dem Avamar-Server und jedem Clientcomputer ermöglichen.
Firewalls	Müssen die bidirektionale Kommunikation zwischen dem Avamar-Server und jedem Clientcomputer über den TCP-Datenport 28002 ermöglichen.
Benennungssystem	Muss Verbindungen zwischen jedem Client und dem Avamar-Server ermöglichen, z. B. in Situationen, in denen sich die IP-Adresse aufgrund eines DHCP- und VPN-Zugriffs ändert.

Installation der Avamar-Clientsoftware

Die empfohlene Methode zur Installation der Avamar-Clientsoftware auf einer großen Anzahl von Windows- oder Mac-Computern ist die Verwendung eines Systemmanagementtools. Ein Systemmanagementtool kann innerhalb kurzer Zeit eine Remote-Push-Installation der Software auf einer großen Anzahl von Computern vornehmen.

Ein Systemmanagementtool kann häufig eine Liste von Computern erzeugen, auf denen die Software erfolgreich installiert ist. Sie können diese Liste in Avamar Client Manager verwenden, um Computer zu registrieren und zu aktivieren.

Sie können Avamar Client für Windows mithilfe verschiedener Optionen zur automatischen Installation installieren.

HINWEIS

Benennen Sie die Clientinstallationspakete nicht um. Die Avamar-Push-Upgrademechanismen sind nicht mit umbenannten Paketen kompatibel.

Unterstützte Systemmanagementtools

Die Remoteinstallation wurde getestet und mithilfe der folgenden Systemmanagementtools genehmigt:

- Microsoft Systems Management Server 2003 (SMS) auf Windows-Computern
- SMS mit Quest Management Xtensions for SMS von Quest-Software auf Macintosh-Computern

Sie können möglicherweise auch andere Systemmanagementtools, wie die in der folgenden Aufstellung genannten Tools, für eine Remote-Push-Installation der Avamar-Clientsoftware verwenden:

- Microsoft System Center Configuration Manager 2007
- IBM Tivoli Management Framework
- HP OpenView ServiceCenter
- Symantec Altiris
- Apple Remote Desktop

Die Systemmanagementtools weisen Unterschiede auf. Die erforderlichen Schritte zur Push-Installation von Software auf mehreren Computern hängen vom jeweiligen Tool ab. Sehen Sie in der Dokumentation für das Tool nach, um die erforderlichen Schritte zur Durchführung dieser Aufgaben zu erfahren.

Push-Installation auf Windows-Computern

Vorgehensweise

1. Kopieren Sie das Installationsprogrammpaket für Avamar Client für Windows an einen Speicherort, auf den das Systemmanagementtool zugreifen kann.
2. Konfigurieren Sie das Systemmanagementtool so, dass es das richtige Installationsprogrammpaket auf die einzelnen Computer kopiert.
3. Legen Sie die Computer fest, auf denen die Software installiert werden soll.
4. Geben Sie einen Startbefehl für die Installation an, der folgendes Format verwendet:

   msiexec /qn /I "*path_to_MSI_pkg*" SERVER=*server* DOMAIN=*domain* GROUP="*groups*" UICOMPONENT={0|1} PROGRESSBAR={true|false} BALLOONMESSAGE={true|false} BACKUPREMINDER=*days*

   In der folgenden Tabelle finden Sie Details zu den Argumenten für den Installationsstartbefehl.

Tabelle 108 Befehlsargumente für den Start der Push-Installation

Argument	Beschreibung
"*path_to_MSI_pkg*"	Gibt den vollständigen Pfad zum Speicherort des Installationsprogrammpakets relativ zum Stammverzeichnis des Computerdateisystems an.
SERVER=*server*	Gibt die IP-Adresse oder den vollständig qualifizierten Domainnamen des dem Client zugewiesenen Avamar-Servers an. Wenn dieses Argument ausgelassen wird oder falsch

Tabelle 108 Befehlsargumente für den Start der Push-Installation (Fortsetzung)

Argument	Beschreibung
	ist, wird der Client zwar erfolgreich installiert, aber nicht aktiviert.
DOMAIN=*domain*	Gibt die Avamar-Domain für den Client an. Der Pfad muss mit einem Schrägstich als Pfadzeichen (Unicode 002F: /) beginnen. Der Standardwert ist /clients.
GROUP=*groups*	Gibt eine kommagetrennte Liste mit Avamar-Backupgruppen für den Client an. Stellen Sie an den Beginn des Pfads jeder Gruppe einen Schrägstrich als Pfadzeichen (Unicode 002F: /) und setzen Sie den Gruppenpfad in gerade Anführungszeichen. Beispiel: GROUP="/clients/text,/clients/admin". Der Standardwert ist "/Default Group".
UICOMPONENT={0|1}	Gibt an, ob der Avamar-Client mit der Standard-GUI (1) oder als Agent-Prozess ohne Benutzeroberfläche (0) aktiviert werden soll. Bei Angabe von 0 werden alle übrigen Optionen ignoriert.
PROGRESSBAR={true|false}	Gibt an, ob das Fortschrittsfenster während der Durchführung von Aufgaben auf dem Client eingeblendet (true) oder ausgeblendet (false) werden soll.
BALLOONMESSAGE={true|false}	Gibt an, ob Sprechblasenmeldungen während der Durchführung von Aufgaben auf dem Client eingeblendet (true) oder ausgeblendet (false) werden sollen.
BACKUPREMINDER=days	Legt fest, nach wie vielen Tagen nach dem letzten Backup eine Backuperinnerung angezeigt werden soll. Mögliche Werte für die Angabe der Tage sind die Zahlen 1 bis 7 und Never. Der Standardwert ist 3.

Benutzer können die von UICOMPONENT, PROGRESSBAR, BALLOONMESSAGE und BACKUPREMINDER festgelegten Werte ändern, indem sie die Optionen im Clientmenü der Clientbenutzeroberfläche verwenden. Die Werte lassen sich ebenfalls während eines Upgrades ändern.

5. Starten Sie den Installationsprozess des Systemmanagementtools.

Push-Installation auf Macintosh-Computern

Vorgehensweise

1. Kopieren Sie das Installationsprogrammpaket für Avamar Client für Mac OS X an einen Speicherort, auf den das Systemmanagementtool zugreifen kann.
2. Konfigurieren Sie das Systemmanagementtool so, dass es das richtige Installationsprogrammpaket auf die einzelnen Computer kopiert.

3. Legen Sie die Computer fest, auf denen die Software installiert werden soll.
4. Geben Sie folgenden Installationsstartbefehl an:

   /usr/sbin/installer -pkg "*path_to_install_pkg*" -target *install_location*

   Dabei steht *path_to_install_pkg* für den vollständigen Pfad zum Speicherort des Installationsprogrammpakets, relativ zum Stammverzeichnis des Computerdateisystems. *install_location* steht für den Speicherort, an dem die Software zu installieren ist. In der Regel handelt es sich bei *install_location* um das Stammverzeichnis, das Root (/). Es ist jedoch jedes lokale Volume zulässig.

5. Starten Sie den Installationsprozess des Systemmanagementtools.

Weitere Erfordernisse

Nach der Avamar Client für Mac OS X-Installation ist ggf. ein Neustart mancher Clients erforderlich. Eine Änderung der Größeneinstellung für die Datenverarbeitung, die auf diesen Computern vorgenommen wird, führt dazu, dass diese Clients neu gestartet werden. Während der Installation ermittelt das Installationsprogramm, ob die Größe für die Datenverarbeitung geringer als 96 MB ist. Für eine optimale Performance von Avamar Client für Mac OS X ist eine Größe für die Datenverarbeitung von mindestens 96 MB erforderlich.

Falls die Größe für die Datenverarbeitung geringer als 96 MB ist, ändert das Installationsprogramm sie auf 96 MB und zeigt eine Erinnerung zum Neustart an. Wenn Sie die Meldung länger als 30 Sekunden geöffnet lassen, ohne auf eine Schaltfläche zu klicken, um sofort oder zu einem späteren Zeitpunkt neu zu starten, wird die Erinnerung ausgeblendet und nach zwei Stunden erneut eingeblendet.

Wenn Sie sich für einen Neustart des Computers entscheiden, der Neustartprozess aber unterbrochen wird, wird die Erinnerung nicht wieder angezeigt. Sie müssen den Computer neu starten, damit die Größenänderung für die Datenverarbeitung abgeschlossen werden kann.

Lokale Clientinstallation

Sie können die Avamar Desktop/Laptop-Software durch Start einer grafischen Installationsoberfläche lokal installieren. Nach der Installation ist der Computer bereit für die Registrierung und Aktivierung auf einem Avamar-Server.

Um eine lokale Installation durchzuführen, können Sie das Clientinstallationsprogramm über den Downloadlink herunterladen. Wenn der Downloadlink deaktiviert ist, müssen Sie das Clientinstallationsprogramm mithilfe einer anderen Dateiübertragungsmethode auf den Computer übertragen.

Die lokale Installation hat einige Nachteile:

- Sie ist sehr zeitaufwendig, wenn sie auf Tausenden Computern einzeln durchgeführt wird.
- Sie stellt keine Liste bereit, die zur Aktivierung und Registrierung von Computergruppen in Avamar Client Manager verwendet werden kann.

Im *Avamar Backup Clients – Benutzerhandbuch* finden Sie weitere Informationen zur lokalen Installation, zum Upgrade und zur Deinstallation von Avamar Desktop/Laptop.

Deinstallieren der Avamar-Clientsoftware

Wenn Sie die Avamar-Clientsoftware von einem Clientcomputer deinstallieren, werden geplante Backups für den Client nicht mehr ausgeführt. Sie können keine Backups mehr auf dem Client wiederherstellen, nachdem Sie die Software deinstalliert haben.

Wenn Sie die Avamar-Clientsoftware deinstallieren, können Sie die Backups für den Client aufbewahren oder löschen:

- Um die Backups für den Client beizubehalten, damit Sie die Backups auf einem anderen Client wiederherstellen können, legen Sie den Client durch die Verwendung des Avamar Administrator still.
- Um die Backups für den Client zu löschen, löschen Sie den Client durch die Verwendung des Avamar Administrator.

Löschen Sie den Client oder setzen sie den Client außer Kraft, bevor oder nachdem Sie die Avamar-Clientsoftware deinstallieren.

Deinstallieren unter Windows

Vorgehensweise

1. Öffnen Sie in Windows **Add or Remove Programs** oder das Applet **Programs and Features**.
2. Wählen Sie aus der Liste derzeit installierter Programme den Eintrag **Avamar for Windows** aus.
3. Klicken Sie auf **Remove**.

   Es wird eine Bestätigungsmeldung angezeigt.
4. Klicken Sie auf **Yes**.

Deinstallieren auf Macintosh

Vorgehensweise

1. Öffnen Sie eine Terminal-(shell-)Sitzung.
2. Melden Sie sich als Administrator an.

   Der Deinstallationsbefehl erfordert Root-(Superuser-)Berechtigungen. Der Befehl `sudo` wird verwendet, um den Befehl mit Root-Berechtigungen auszuführen. Ein Administratorkonto oder ein anderes unter `sudoers` aufgeführtes Konto wird von `sudo` benötigt.
3. Führen Sie den Deinstallationsskript aus, indem Sie folgenden Befehl eingeben:

   `sudo /usr/local/avamar/bin/avuninstall.sh`

Avamar Desktop/Laptop-Benutzerauthentifizierung

Avamar Desktop/Laptop schützt Backupdaten durch Authentifizierung von Benutzern und Durchsetzung von Zugriffsrechten. Avamar Desktop/Laptop verwendet einen separaten Serverprozess auf dem Avamar-System, um eine Authentifizierung über interne und externe Methoden zu ermöglichen. Zu jeder Avamar-Systeminstallation gehört der Avamar Desktop/Laptop-Serverprozess.

Pass-Through-Authentifizierung

Die Pass-Through-Authentifizierung verwendet verschlüsselte Kanäle, um auf die Benutzeranmeldedaten von einem Clientcomputer zuzugreifen und ihnen

Dateieigentumsrechte zuzuweisen. Das Betriebssystem des Clientcomputers bezieht die Benutzeranmeldedaten während der Anmeldung bei dem Computer oder mithilfe der Common Access Card(CAC)-Technologie.

Avamar Desktop/Laptop führt die Pass-Through-Authentifizierung auf transparente Weise durch. Benutzer können Dateien sichern und wiederherstellen, ohne den Avamar Desktop/Laptop-Anmeldebildschirm anzeigen zu müssen.

Bei Avamar Desktop/Laptop ist die Pass-Through-Authentifizierung standardmäßig aktiviert. Sie ist auf Benutzer von Windows- und Mac-Computern beschränkt. Außerdem können Windows-Benutzer mit lokalen Administratorrechten ohne eine zusätzliche Anmeldung Dateien wiederherstellen, deren Eigentumsrechte bei einem anderen Benutzer des Computers liegen.

Die Pass-Through-Authentifizierung wird bei der LDAP-Authentifizierung und NIS-Authentifizierung unterstützt.

Aktivieren des Zugriffs durch lokale Benutzer zwecks Pass-Through-Authentifizierung

Sie können Avamar Desktop/Laptop so konfigurieren, dass ein Zugriff durch lokale Benutzer über die Pass-Through-Authentifizierung zugelassen wird. Ein lokaler Benutzer ist ein Benutzer, der über ein Konto auf einem lokalen Computer anstatt über ein Domainkonto authentifiziert wird.

Wenn ein Zugriff durch lokale Benutzer aktiviert ist, können lokale Benutzer auf die Webbenutzeroberfläche des Avamar-Clients, um die ihnen gehörenden Daten auf dem authentifizierenden Computer wiederherzustellen.

Für einen Zugriff durch lokale Benutzer ist die Pass-Through-Authentifizierung auf einem Windows- oder Mac-Computer Voraussetzung. Standardmäßig ist der Zugriff durch lokale Benutzer deaktiviert.

Hinweis

Eine Aktivierung des Zugriffs durch lokale Benutzer gilt für alle mit dem Server verknüpften Clients und Backups. Bevor Sie den Zugriff durch lokale Benutzer aktivieren, berücksichtigen Sie die daraus entstehenden Sicherheitsrisiken im Kontext der Organisation. Die lokale Benutzerauthentifizierung ist per se unsicherer als die Domainauthentifizierung.

Um den Zugriff durch lokale Benutzer für die Pass-Through-Authentifizierung zu aktivieren, heben Sie die Auskommentierung der Eigenschaft `allowLocalUsers` in der Datei `dtlt.properties` auf dem Avamar-Server auf und stellen Sie den zugehörigen Wert auf `true` ein, indem Sie `#allowLocalUsers=false` zu `allowLocalUsers=true` ändern.

Deaktivieren der Pass-Through-Authentifizierung

Sie können die Pass-Through-Authentifizierung deaktivieren und die Einstellungen so vornehmen, dass sich alle Benutzer über den Avamar Desktop/Laptop-Anmeldebildschirm anmelden müssen. Konfigurieren Sie bei deaktivierter Pass-Through-Authentifizierung eine andere Authentifizierungsmethode für Windows- und Mac-Benutzer.

Um die Pass-Through-Authentifizierung zu deaktivieren, stellen Sie den Wert der Eigenschaft `userLoginRequired` in der Datei `dtlt.properties` auf dem Avamar-Server auf `true` ein.

LDAP-Authentifizierung

Konfigurieren Sie Avamar Desktop/Laptop für die Verwendung eines unterstützten LDAP-Verzeichnisdiensts zur Authentifizierung von Benutzern anhand der Benutzernamen und Passwörter des Verzeichnisdiensts.

Der Authentifizierungsprozess nutzt standardmäßig Kerberos in einer SASL-Bindung (Simple Authentication and Security Layer). Alternativ können Sie den Authentifizierungsprozess so konfigurieren, dass Nur-Text in einer einfachen Bindung verwendet wird. Bei der Pass-Through-Authentifizierung wird nur die SASL-Bindung unterstützt. Nur-Text in einer einfachen Bindung ist mit der Pass-Through-Authentifizierung nicht kompatibel.

Bei der LDAP-Authentifizierung melden sich Benutzer beim Clientcomputer mit einem über einen Domainverzeichnisdienst authentifizierten Domainkonto an. Zur Verwendung eines lokalen Kontos aktivieren Sie den Zugriff durch lokale Benutzer.

Um die Sicherheit für die Benutzerdaten zu erhöhen, ermittelt Avamar Desktop/Laptop den Domainbenutzernamen eines Windows- oder Mac-Benutzers vom Clientcomputer und zeigt ihn dann in einem schreibgeschützten Feld auf dem Anmeldebildschirm von Avamar Desktop/Laptop ein.

Hinweis

Verwenden Sie kein Root-Konto auf einem Mac-Rechner, um Dateien aus Backups wiederherzustellen.

Konfigurieren der LDAP-Authentifizierung für Avamar Desktop/Laptop

Um Avamar Desktop/Laptop so zu konfigurieren, dass Benutzer über einen unterstützten LDAP-Verzeichnisdienst mit Kerberos in einer SASL-Bindung oder mit Nur-Text in einer einfachen Bindung authentifiziert werden, bearbeiten Sie die LDAP-Konfigurationsdatei.

Bevor Sie beginnen

- Konfigurieren Sie Avamar mit Informationen über den Verzeichnisservice. Anweisungen finden Sie unter Hinzufügen von Informationen für einen unterstützten LDAP-Verzeichnisdienst auf Seite 79.
- Vergewissern Sie sich, dass die Konfiguration des Avamar Desktop-/Laptop-Servers die zur Trennung der Authentifizierung verwendeten Domainkomponenten korrekt beschreibt.
- Bei Verwendung von Kerberos in einer SASL-Bindung ist darauf zu achten, dass es sich bei dem Kerberos-Bereich für die LDAP-Benutzerauthentifizierung von Macintosh-Rechnern um den standardmäßigen Kerberos-Bereich handelt.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **LDAP Management**.
3. Klicken Sie auf **Edit LDAP file**.
4. Bearbeiten oder erstellen Sie im Textbereich den Schlüssel `user-login-module`:
   - Um Kerberos in einer SASL-Bindung anzugeben, legen Sie `user-login-module=kerberos` fest.

- Um Nur-Text in einer einfachen Bindung anzugeben, legen Sie `user-login-module=ldap` fest.

Kerberos ist der Standardwert. Avamar Desktop/Laptop geht von diesem Wert aus, wenn der Schlüssel fehlt.

5. Klicken Sie auf **Save**.
6. Klicken Sie auf **Close**.

Ändern des Kerberos-Verschlüsselungstyps

Bei Verwendung der LDAP-Authentifizierung mit Kerberos müssen Sie ggf. den Kerberos-Verschlüsselungstyp ändern.

Avamar Desktop/Laptop nutzt standardmäßig den MIT-Kerberos-Verschlüsselungstyp „DES cbc mode with CRC-32“ für die Kommunikation mit LDAP-Servern. Bei diesem Verschlüsselungstyp kann es zu einem Konflikt mit einem Schlüsselverteilungscenter (Key Distribution Center, KDC) in der Active Directory-Umgebung kommen. In diesem Fall wird die Meldung `KDC has no support for encryption type` angezeigt. Um dieses Problem zu beheben, entfernen Sie den angegebenen Verschlüsselungstyp aus der Konfigurationsdatei `krb5.conf`, sodass das Schlüsselverteilungscenter den Verschlüsselungstyp auswählen kann.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **LDAP Management**.
3. Klicken Sie auf **Edit KRB5 file**.
4. Suchen Sie im Textbereich nach den folgenden Einträgen:

```
[libdefaults]
default_tgs_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
default_tkt_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
```

5. Kommentieren Sie die folgenden Einträge aus:

```
[libdefaults]
#default_tgs_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
#default_tkt_enctypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
```

6. Klicken Sie auf **Save**.
7. Klicken Sie auf **Close**.

NIS-Authentifizierung

Sie können Avamar Desktop/Laptop so konfigurieren, dass Linux-Benutzer über das Unternehmens-NIS authentifiziert werden.

Bei Verwendung der NIS-Authentifizierung müssen alle Clientcomputer denselben statischen, auflösbaren, vollständig qualifizierten NIS-Domainnamen verwenden.

Außerdem müssen Benutzer über korrekt konfigurierte Benutzerkonten in der NIS-Domain verfügen.

Anweisungen zum Konfigurieren der NIS-Authentifizierung finden Sie unter Hinzufügen von Informationen für einen unterstützten LDAP-Verzeichnisdienst auf Seite 79.

Avamar-Authentifizierung

Sie können Avamar Desktop/Laptop so konfigurieren, dass Benutzer mithilfe der Avamar-Authentifizierung authentifiziert werden. Dabei werden interne Avamar-Domaininformationen verwendet.

Die Avamar-Authentifizierung arbeitet mit Benutzern, die sich auf der Avamar-Root-Ebene, auf Avamar-Domain-Ebenen oder Avamar-Subdomain-Ebenen authentifizieren. Bei diesem Mechanismus wird mit der Überprüfung auf Subdomain-Ebene begonnen. Wird der Benutzername auf dieser Ebene gefunden, wird der Authentifizierungsprozess fortgesetzt. Wird der Benutzername nicht gefunden, wird die nächste Ebene geprüft. Dieser Vorgang wird so lange fortgesetzt, bis der Benutzername gefunden oder die Avamar-Root-Ebene ohne Auffinden des Benutzernamens erreicht wurde.

Wenn beispielsweise der Anmeldecomputer `123abc.example.com` mit der `/clients/mountain`Avamar-Subdomain aktiviert ist, dann überprüft der Mechanismus das Avamar-System in der folgenden Reihenfolge, bis der Benutzername gefunden wird:

1. `/clients/mountain` (Subdomain der Aktivierung)
2. `/clients` (nächste Ebene)
3. `/` (root)

Bei der Avamar-Authentifizierung müssen Clientcomputer über einen statischen, auflösbaren, vollständig qualifizierten Domainnamen verfügen. Außerdem müssen Benutzer über ein lokales oder Domainanmeldekonto für den Clientcomputer verfügen und ein Konto in der Avamar-Domain muss mit dem Clientcomputer verknüpft sein.

Avamar Desktop/Laptop wendet die dem Avamar-Benutzerkonto zugewiesene Rolle an, wenn über die Avamar-Authentifizierung Zugriff zum Konto gewährt wird. Benutzer können nur die Vorgänge durchführen, die gemäß ihrer Rolle zulässig sind. Die einzige Ausnahme: Benutzer mit der Rolle **Restore only operator** können ein Backup von Avamar Desktop/Laptop starten.

Konfigurieren der Avamar-Authentifizierung

Sie können ein Avamar-System so konfigurieren, dass die Avamar-Authentifizierung über die Registerkarte „LDAP-Management“ von Avamar Administrator erfolgt.

Bevor Sie beginnen

Fügen Sie Listen auf Domainebene Avamar-Benutzerdatensätze hinzu. Anweisungen finden Sie unter Hinzufügen eines Benutzers zu einem Client oder einer Domain auf Seite 101.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Administration** Link zum Startprogramm.

   Das Fenster **Administration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **LDAP Management**.

3. Klicken Sie auf **Edit LDAP file**.
4. Bearbeiten oder erstellen Sie den Schlüssel `user-login-module`:
   - Um die Avamar-Authentifizierung und alle anderen konfigurierten und aktivierten Authentifizierungsmethoden zu verwenden, legen Sie `user-login-module=mix` fest.
   - Um die Avamar-Authentifizierung und alle anderen konfigurierten und aktivierten Authentifizierungsmethoden außer LDAP zu verwenden, legen Sie `user-login-module=avamar` fest.
5. Geben Sie in den Textbereich das folgende Schlüssel-/Wertpaar ein:

   avamar-authentication-domains=/*domain1*,/*domain2*,/*domain3*,/...**

   Dabei sind *domain1*, *domain2* und *domain3* Avamar-Domainnamen, die in einer kommagetrennten Liste kombiniert werden. Jeder Domainname muss mit dem Stammpfadbezeichner beginnen: `/`.

   Beispiel: Verwendung der Avamar-Authentifizierung für die folgenden Domains:

   /
   /clients/accounting
   /clients/shipping

   Geben Sie das folgende Schlüssel-/Wertepaar ein:

   avamar-authentication-domains=/,/clients/accounting,/clients/shipping
6. Klicken Sie auf **Save**.
7. Klicken Sie auf **Close**.

Gemischte Authentifizierung

In einer Umgebung können Sie mehrere Authentifizierungsmethoden verwenden.

Wenn Sie mehrere Authentifizierungsmethoden zulassen, erfolgt der Authentifizierungsprozess in der nachstehend angegebenen Reihenfolge:

1. Benutzer auf einem Client in einer Avamar-Domain werden mithilfe der Avamar-Authentifizierung authentifiziert.
2. Benutzer, die nicht bei einem Client in einer Avamar-Domain angemeldet sind, werden mithilfe der Pass-Through-Authentifizierung authentifiziert.
3. Linux-Benutzer, die nicht bei einem Client in einer Avamar-Domain angemeldet sind, werden durch NIS authentifiziert.
4. Bei Aktivierung der gemischten Authentifizierung und LDAP-Konfiguration werden Benutzer, die nicht bei einem einer bestimmten Avamar-Domain zugewiesenen Client angemeldet sind, durch LDAP authentifiziert.

Avamar Desktop/Laptop-Benutzeroberflächen

Die Avamar Desktop/Laptop-Funktionen sind über die Client- und Webbenutzeroberfläche verfügbar.

Clientbenutzeroberfläche

Die lokale Clientbenutzeroberfläche wird bei der Installation von Avamar Client für Windows bzw. Avamar Client für Mac OS X auf dem Clientcomputer installiert. In der

Clientbenutzeroberfläche von Windows-Computern wird ein Avamar-Symbol im Infobereich („Taskleiste“), bei Mac-Computern in der Menüleiste angezeigt. Klicken Sie unter Windows mit der rechten Maustaste auf das Symbol bzw. klicken Sie unter Mac auf das Symbol, um das Clientmenü zu öffnen, über das auf die Backup-, Wiederherstellungs- und Programmeinstellungen sowie die Protokolle zugegriffen werden kann.

In der folgenden Tabelle sind die in der Clientbenutzeroberfläche verfügbaren Funktionen aufgeführt.

Tabelle 109 Funktionen der Avamar Desktop/Laptop-Clientbenutzeroberfläche

Clientmenübefehl	Beschreibung
Back Up Now	Startet ein mit nur einem Klick durchführbares On-Demand-Backup.
Back Up ...	Startet ein interaktives On-Demand-Backup.
Restore ...	Startet eine interaktive Wiederherstellung.
Settings > Show Backup Reminder (days)	Steuert, wann eine Backuperinnerung angezeigt wird, um Sie darauf hinzuweisen, dass der Computer seit einem bestimmten Zeitraum, zwischen einem und sieben Tagen, nicht mehr gesichert wurde. Sie können die Erinnerung deaktivieren, indem Sie **Never** auswählen.
Settings > Show Progress Bar	Steuert, ob das Fenster **Progress** während eines Backups angezeigt wird. Über das Fenster **Progress** können Backups abgebrochen und angehalten oder zugehörige Protokolle angezeigt werden.
Settings > Show Balloon Messages	Steuert, ob auf unterstützten Windows-Computern eine Sprechblasenmeldung zum Systemstatus in der Nähe des Avamar-Symbols angezeigt wird.
Settings > Back Up On Battery Power	Steuert, ob bei Akkubetrieb des Computers geplante Backups oder On-Demand-Backups für den Computer durchgeführt werden können.
Settings > Back Up On Wireless	Steuert, ob geplante Backups oder On-Demand-Backups für den Computer durchgeführt werden können, wenn der Computer lediglich drahtlos mit dem Netzwerk verbunden ist.
Languages	Ermöglicht die Auswahl der Sprache für die Clientbenutzeroberfläche.
Manage > Activate Client	Aktiviert den Client, sodass eine eindeutige ID für den Client bereitgestellt und der Client mit einem bestimmten Avamar-Server verbunden wird.
Manage > View Console	Öffnet die Clientkonsole, die Zugriff auf lokale Statusdatensätze für Aufgaben, das Agent-

Tabelle 109 Funktionen der Avamar Desktop/Laptop-Clientbenutzeroberfläche (Fortsetzung)

Clientmenübefehl	Beschreibung
	Protokoll, das Konsolenprotokoll und das Arbeitsauftragsprotokoll bietet.
Manage > Create ZIP File of Logs	Erstellt eine ZIP-Datei mit den von Administratoren für die Diagnose von Backup- und Wiederherstellungsproblemen benötigten Protokollen.
(Nur unter Mac) Client Agent Tasks	Stoppt den Backup-Agent-Prozess bzw. startet diesen neu.
(Nur unter Mac) Logs	Bietet Zugriff auf das Agent-Protokoll, das Konsolenprotokoll und die Funktionen zum Erstellen einer ZIP-Datei mit den von Administratoren für die Diagnose von Backup- und Wiederherstellungsproblemen benötigten Protokollen.
About	Stellt Versions-, Server- und Urheberrechtsinformationen für Avamar Desktop/Laptop bereit.
Help	Startet die Onlinehilfe für Avamar Desktop/Laptop, wenn der Client auf einem Avamar-Server aktiviert wird.
Exit	Fährt den Avamar-Client herunter.

Webbenutzeroberfläche

Über die Webbrowser-Benutzeroberfläche (Webbenutzeroberfläche) lassen sich ein On-Demand-Backup bzw. eine On-Demand-Wiederherstellung starten, die Backup- und Wiederherstellungsaktivität für einen Clientcomputer anzeigen oder andere Backupeinstellungen für einen Clientcomputer konfigurieren.

In der folgenden Tabelle sind die Hauptelemente der Webbenutzeroberfläche beschrieben.

Tabelle 110 Funktionen der Avamar Desktop/Laptop-Webbenutzeroberfläche

Element	Beschreibung
Avamar Desktop-/Laptop-Logo	Sie können das Avamar-Logo und das Desktop-/Laptop-Logo oben links auf der Webbenutzeroberfläche austauschen, um die Webbenutzeroberfläche umzubenennen.
Menü „Settings“	Das Menü „Settings“ oben rechts auf der Webbenutzeroberfläche ermöglicht die Steuerung der Konfigurationseinstellungen der Webbenutzeroberfläche, darunter Folgendes: • Aktivierung/Deaktivierung von Sprechblasenmeldungen

Tabelle 110 Funktionen der Avamar Desktop/Laptop-Webbenutzeroberfläche (Fortsetzung)

Element	Beschreibung
	• Sprache der Webbenutzeroberfläche • Anzahl der auf den Seiten **Search**, **Browse** bzw. **History** anzuzeigenden Einträge • Die während einer Wiederherstellung angezeigte Standardseite • Verwendung/Nichtverwendung der vollständigen Webbenutzeroberfläche oder des reinen Durchsuchenmodus, bei dem lediglich die Seiten **Search** und **History** angezeigt werden
Das Symbol „Refresh“	Aktualisiert die Seite der Webbenutzeroberfläche.
Menü „Help“	Bietet Zugriff auf die Avamar Desktop/ Laptop-Onlinehilfe und auf Informationen zur Softwareversion.
Seite „Search“	Ermöglicht die Suche nach wiederherzustellenden Dateien und Ordnern auf dem Clientcomputer.
Seite „Browse“	Ermöglicht die Navigation zu wiederherzustellenden Dateien und Ordnern auf dem Clientcomputer.
Seite „Backup“	Bietet Informationen über die Backupgruppen, denen der Client zugewiesen ist, sowie zum nächsten geplanten Backup. Außerdem können Sie hierüber ein On-Demand-Backup des Clients durchführen, indem Sie die Gruppen-Policies für die Gruppen verwenden, denen der Client zugewiesen ist. Wenn die Schaltfläche **Add Data** auf der Seite **Backup** aktiviert ist, ist es Benutzern möglich, den Gruppen-Datasets Ordner für geplante Backups und On-Demand-Backups hinzuzufügen.
Seite „History“	Stellt Informationen zur Backup- und Wiederherstellungsaktivität auf dem Computer für die letzten 14 Tage zur Verfügung. Dazu gehören: • Status der Backupaktivität und für jedes Backup eine Auflistung der übertragenen Dateidaten • Status der Wiederherstellungsaktivität
Statusleiste	Zeigt das Datum und die Uhrzeit des letzten und nächsten geplanten Backups sowie das

Tabelle 110 Funktionen der Avamar Desktop/Laptop-Webbenutzeroberfläche (Fortsetzung)

Element	Beschreibung
	Ergebnis des letzten Backups an. In der Statusleiste werden Informationen der letzten 14 Tage angezeigt. Wenn das letzte Backup mehr als 14 Tage zurückliegt, wird die Statusleiste in der Meldung `No backups found` angezeigt. Auf den Seiten **Browse** und **Search** werden jedoch ggf. Dateien angezeigt, wenn die der Gruppe für den Client zugewiesene Aufbewahrungs-Policy eine Frist von mehr als 14 Tagen aufweist.

Eingeschränkte Benutzeroberfläche

Der Avamar-Server zeigt einem Client eine eingeschränkte Version der Webbenutzeroberfläche an, wenn die Anzahl der Dateien und Verzeichnisse in einem Clientbackup einen Wert von etwa 4 Millionen überschreitet oder wenn nicht ausreichend Speicher für Avamar Desktop/Laptop zugewiesen ist.

Große Anzahl von Dateien und Verzeichnissen in einem Clientbackup
Die genaue Anzahl von Dateien und Verzeichnissen, die die Ursache für diese Änderungen sind, hängt von dem verfügbaren Arbeitsspeicher des Avamar-Servers ab.

Es gibt keine Obergrenze hinsichtlich der Anzahl von Dateien und Verzeichnisse, die in einem Backup enthalten sein können.

Unzureichende Speicherzuweisung
Die eingeschränkte Version der Webbenutzeroberfläche wird auch für alle Clients angezeigt, die auf den Avamar-Server zugreifen, wenn der Arbeitsspeicher, der zum Erfüllen der aktuellen Avamar Desktop/Laptop-Anforderungen erforderlich ist, die für Avamar Desktop/Laptop zugewiesene Speichermenge überschreitet.

Indem Benutzer dazu aufgefordert werden, sich am Ende ihrer Sitzung von der Webbenutzeroberfläche abzumelden, lässt sich dieses Problem vermeiden.

Beschreibung der eingeschränkten Webbenutzeroberfläche
Die eingeschränkte Version der Webbenutzeroberfläche weist folgende Änderungen auf:

- Die Seiten **Search** und **History** werden in der Webbenutzeroberfläche nicht angezeigt.
- Dateiversionen stehen auf der Seite **Browse** nicht zur Verfügung.
- Die Wiederherstellung ist nur für Benutzer mit lokalen Administratorrechten auf dem Computer zulässig. Nicht-Administrator-Benutzer können keine Dateien wiederherstellen, auch nicht diejenigen, die ihnen lokal auf Computern der Serverklasse gehören.
- Es wird kein Limit für die Wiederherstellungsdatengröße durchgesetzt.

Apache-Webserver-Authentifizierung

Zum Schutz der Benutzersicherheit zeigen Webbrowser eine Authentifizierungswarnung an, wenn auf eine sichere Webseite zugegriffen wird, es sei denn, der Webserver stellt ein vertrauenswürdiges Public-Key-Zertifikat zur Seite bereit. Die Avamar Desktop/Laptop-Webbenutzeroberfläche nutzt ausschließlich sichere Webseiten und diese Warnung wird in Browsern angezeigt, über die auf diese

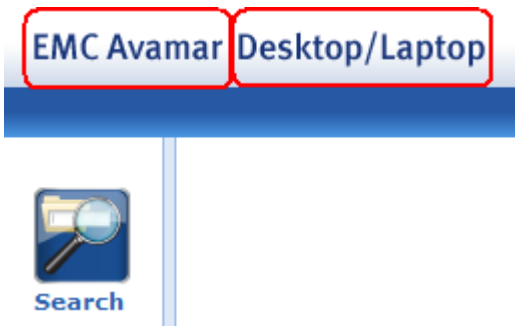
Seiten zugegriffen wird. Installieren Sie ein vertrauenswürdiges Public-Key-Zertifikat auf dem mit Avamar bereitgestellten Apache-Webserver, um die Warnung zu verhindern.

Im *Avamar – Produktsicherheitshandbuch* wird beschrieben, wie Sie ein vertrauenswürdiges Public-Key-Zertifikat für den Apache-Webserver erhalten und installieren können.

Umbenennen der Webbenutzeroberfläche

Sie können die Webbenutzeroberfläche des Avamar-Clients umbenennen, indem Sie die zwei Logografiken in der linken oberen Ecke der Benutzeroberfläche ersetzen.

Abbildung 18 Ersetzbare Grafiken auf der Webbenutzeroberfläche des Avamar-Clients



Vorgehensweise

1. Erstellen Sie zwei Ersatzgrafiken mit der Bezeichnung `ProductNameAvamar.png` und `ProductNameDTLT.png`.

   Die Ersatzgrafiken müssen folgende Anforderungen erfüllen:

   - Als Dateiformat ist Portable Network Graphic (`.png`) erforderlich.
   - Der Hintergrund muss transparent sein, damit der Hintergrundverlauf hinter dem Grafiktext und den Abbildungen erkennbar ist.
   - `ProductNameAvamar.png` Muss 97 Pixel breit und 18 Pixel hoch sein.
   - `ProductNameDTLT.png` Muss 128 Pixel breit und 18 Pixel hoch sein.

2. Öffnen Sie eine Befehlsshell:

   a. Melden Sie sich beim Server als Administrator an.

   b. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie `su -` eingeben.

   c. Laden Sie für einen Multi-Node-Server den OpenSSH-Schlüssel rootid, indem Sie Folgendes eingeben:

   ```
   ssh-agent bashssh-add /root/.ssh/rootid
   ```

3. Wechseln Sie mit folgendem Befehl das Arbeitsverzeichnis:

   ```
   cd /usr/local/avamar-tomcat-7.0.59/webapps/dtlt/images/banner
   ```

4. Erstellen Sie Backupkopien der Originalgrafiken, indem Sie die folgenden Befehle eingeben:

   ```
   cp ProductNameAvamar.png ProductNameAvamar.png_origcp
   ProductNameDTLT.png ProductNameDTLT.png_orig
   ```

5. Verschieben Sie die neuen Logos als `ProductNameAvamar.png` und `ProductNameDTLT.png` in das aktuelle Arbeitsverzeichnis.
6. Sollten die neuen Grafiken nicht angezeigt werden, löschen Sie die zwischengespeicherten Kopien zuvor im Webbrowser angezeigter Dateien und aktualisieren Sie die Seite.

Ändern des Ports für die Webbenutzeroberfläche

Der Zugriff auf die Webbenutzeroberfläche erfordert eine HTTPS-Kommunikation zwischen dem Avamar-Server und dem Webbrowser des Clients. Wenn ein Benutzer ein Backup oder eine Wiederherstellung über das Avamar-Clientmenü anfordert, wird der standardmäßige Webbrowser auf dem Client dazu aufgefordert, den Avamar-Server auf Port 443, dem standardmäßigen HTTPS-Port, zu kontaktieren. Auf dem Avamar-Server wird die ursprüngliche Anforderung an Port 443 an Port 8443, den HTTPS-Port für die Webbenutzeroberfläche, umgeleitet. Sie können den ursprünglichen Kontaktport ändern, indem Sie die Konfigurationsdatei `avscc.cfg` auf dem Client und die Apache-SSL-Konfigurationsdatei auf dem Server bearbeiten.

Vorgehensweise

1. Bearbeiten Sie die Datei `avscc.cfg` auf dem Clientcomputer, um die neue Portnummer zu verwenden:
   a. Öffnen Sie `avscc.cfg` in einem Texteditor.

      Bei Windows-Clients befindet sich die Datei im Verzeichnis `%SystemDrive%\Program Files\avs\var`. Bei allen anderen Clients befindet sich die Datei im Verzeichnis `/usr/local/avamar/var`.

      Wenn `avscc.cfg` unter diesem Speicherort nicht vorhanden ist, erstellen Sie die Datei.

   b. Fügen Sie die folgende Zeile in die Datei ein:

      `--dtlt-port=`*n*

      Dabei steht *n* für die Nummer des ursprünglichen Kontaktports.

   c. Speichern und schließen Sie `avscc.cfg`.
   d. Starten Sie den Client neu.
2. Bearbeiten Sie die Apache-SSL-Konfigurationsdatei auf dem Avamar-Server:
   a. Öffnen Sie eine Befehlsshell und melden Sie sich als Administrator bei einem Single-Node-Server oder bei dem Utility-Node eines Multi-Node-Servers an.
   b. Öffnen Sie die Apache-SSL-Konfigurationsdatei in einem Texteditor.

      Bei Red Hat Enterprise Linux ist die Datei `/etc/httpd/conf.d/ssl.conf`. Bei SuSE Linux Enterprise Server ist die Datei `/etc/apache2/vhosts.d/vhost-ssl.conf`.

   c. Navigieren Sie zur HTTPS-Port-Listening-Richtlinie und ändern Sie `Listen 443` zu `Listen`*n*. Dabei steht *n* für die Nummer des ursprünglichen Kontaktports.
   d. Speichern und schließen Sie die Datei.
   e. Starten Sie den Apache-Serverprozess neu, indem Sie **`apachectl restart`** eingeben.

Ändern des Timeout-Werts des sicheren Tokens

Avamar Desktop/Laptop enthält ein temporäres sicheres Token als Teil der URL, über die eine Backup- oder Wiederherstellungssitzung in einem Clientwebbrowser gestartet wird. Der Clientwebbrowser muss eine HTTPS-Verbindung zum Avamar-Server herstellen, bevor das Token abläuft oder die Sitzung zurückgewiesen wird und das Backup bzw. die Wiederherstellung nicht fortgesetzt werden kann. Sie können den standardmäßigen Timeout-Wert von 20 Sekunden bearbeiten.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell und melden Sie sich mittels einer der folgenden Methoden an:
   - Melden Sie sich bei einem Single-Node-Server als Administrator beim Server an.
   - Bei einem Multi-Node-Server:
     a. Melden Sie sich als Administrator beim Utility Node an.
     b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```
2. Stoppen Sie den MCS, indem Sie den folgenden Befehl eingeben:

   ```
   dpnctl stop mcs
   ```
3. Wechseln Sie mit folgendem Befehl das Arbeitsverzeichnis:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs
   ```
4. Öffnen Sie `mcserver.xml` in einem Texteditor.
5. Bearbeiten Sie in Abschnitt `<node name="dtlt">` den Wert `<entry key="expire_data_after_secs" value="20" /> from 20` so, dass dieser den neuen Timeout-Wert in Sekunden widerspiegelt.
6. Speichern Sie die Änderung und schließen Sie die Datei.
7. Starten Sie den MCS und den Scheduler, indem Sie Folgendes eingeben:

   ```
   dpnctl start mcs
   dpnctl start sched
   ```

Erzwingen der clientseitigen Verwendung der alternativen Methode zum Durchsuchen von Dateien

Die Webbenutzeroberfläche des Avamar-Clients nutzt betriebssystemspezifische Services zum Durchsuchen von Dateien auf dem Clientcomputer, um Benutzern eine Dateimanageroberfläche für die Auswahl von zu sichernden und wiederherzustellenden lokalen Dateien und Ordnern bereitzustellen. Wenn diese Services jedoch nicht verfügbar sind, weil der Client NAT verwendet oder der Port 28002 auf dem Client durch eine Firewallregel blockiert ist, wird eine alternative Methode zum Durchsuchen von Dateien angeboten. Sie können festlegen, dass Clients die alternative Methode zum Durchsuchen von Dateien verwenden müssen.

Ein Grund für eine solche Änderung ist die Unterstützung von Wechselmedien. Die Standardmethode zum Durchsuchen von Dateien bietet im Gegensatz zur alternativen Methode keine Unterstützung für Wechselmedien.

Die alternative Methode verwendet ein Java-Applet, um Dienste zum Durchsuchen von Dateien bereitzustellen. Wenn die Standarddienste nicht verfügbar sind und der

Benutzer die alternative Methode zulässt, wird das Java-Applet geladen. Beim Laden des Applets werden dem Benutzer u. U. Authentifizierungswarnungen zum Websitezertifikat des Avamar-Servers und zur digitalen Signatur des Java-Applets angezeigt. Bestätigen Sie diese Warnungen. Ansonsten wird das Applet nicht geladen.

Nach dem Laden des Applets wird die Webseite automatisch aktualisiert, sodass die Webbenutzeroberfläche des Avamar-Clients das Applet verwenden kann. Der Benutzer muss die Aufgabe nach der Aktualisierung der Seite neu starten.

Um zu erzwingen, dass Clients die alternative Methode zum Durchsuchen von Dateien verwenden, fügen Sie die Eigenschaft `useAppletToBrowseLocalFile` der Datei `dtlt.properties` auf dem Avamar-Server hinzu und stellen Sie sie auf den Wert `true` ein.

Backup mit Avamar Desktop/Laptop

Avamar Desktop/Laptop bietet verschiedene Methoden zum Starten eines Clientbackups.

In der folgenden Tabelle werden die Methoden zum Starten eines Clientbackups sowie die jeweils für die Methode verfügbaren Optionen beschrieben.

Tabelle 111 Beschreibungen der Methoden zum Starten eines Avamar Desktop/Laptop-Clientbackups

Methode	Beschreibung	Optionen	Dataset
Geplant	Der Avamar-Server sichert den Client automatisch gemäß der für die Gruppe des Clients festgelegten Planung.	• Vom Benutzer ausgewählte Backupzeit • Daten hinzufügen	Das für die geplante Gruppe angegebene Dataset oder das dem Computer zugewiesene Dataset. Wenn **Daten hinzufügen** aktiviert ist, enthält das Dataset auch Ordner, die der Benutzer hinzugefügt hat.
Einfachklick	Der Avamar-Server übernimmt ein Backup des Clients in eine Warteschlange, wenn ein Benutzer auf dem Client auf **Back Up Now** klickt.	• Daten hinzufügen	Das Dataset für jede Gruppe, die dem Computer zugeordnet ist, oder das dem Computer zugewiesene Dataset. Wenn **Daten hinzufügen** aktiviert ist, enthält das Dataset auch Ordner, die der Benutzer hinzugefügt hat.
Interaktiv	Der Benutzer klickt auf **Sichern** und die Webbenutzeroberfläche wird angezeigt. Der Benutzer wählt unter den verfügbaren Start- und Datenoptionen und klickt auf der Seite **Backup** auf **Jetzt sichern**. Der Avamar-Server fügt das Backup der Backupwarteschlange auf dem Avamar-Server hinzu.	• Daten hinzufügen • On-Demand-Backupsatz	Das Dataset der Gruppe, die der Benutzer aus den Gruppen auswählt, die dem Client zugewiesen sind. Wenn **Daten hinzufügen** aktiviert ist, enthält das Dataset auch Ordner, die der Benutzer hinzugefügt hat. Wenn **Jetzt auswählen** (Option für On-Demand-Backupsatz) aktiviert ist, enthält das Dataset nur die vom Benutzer ausgewählten Dateien und Ordner.

Geplante Backups

Führen Sie geplante Backups von Avamar Desktop/Laptop-Clientcomputern wie Backups anderer Avamar-Clientcomputer in der Umgebung durch. Erstellen Sie Datasets, Planungen, Aufbewahrungs-Policies und Gruppen für die Backups mithilfe von Avamar-Administrator.

Benutzern werden die Gruppen, die mit einem Avamar Desktop/Laptop-Client verbunden sind, auf der Seite **Backup** der Webbenutzeroberfläche angezeigt.

Die nächste geplante Backupzeit für jede mit einem Avamar Desktop/Laptop-Client verbundene Gruppe wird ebenfalls auf der Seite **Backup** angezeigt. Normalerweise bestimmt die Policy der Gruppe die geplante Startzeit für die Backups dieser Gruppe. Bei einzelnen Avamar Desktop/Laptop-Clients können Sie es Benutzern gestatten, eine andere Startzeit für die geplanten Backups ihrer Clients auszuwählen.

Zulassen der benutzerseitigen Auswahl einer Startzeit für geplante Backups

Ermöglichen Sie Benutzern eines Avamar Desktop/Laptop-Clients, eine Startzeit für die geplanten Backups des Clients auszuwählen, die von der Startzeit abweicht, die über die Gruppen-Policy zugewiesen wurde.

Wenn Sie diese Funktion für einen Avamar Desktop/Laptop-Client aktivieren, können Benutzer aus einer Liste vom Administrator definierter Uhrzeiten wählen, die auf der Seite **Backup** der Webbenutzeroberfläche angezeigt werden. Die ausgewählte Startzeit gilt für alle nachfolgenden geplanten Backups für den Client.

Um Lücken bei der Datensicherheit zu verhindern, verwenden Avamar Desktop/Laptop-Clients weiterhin die vom Benutzer ausgewählte Startzeit für das Backup, selbst wenn Sie diese Zeit aus der Planung **Tägliche Planung außer Kraft setzen** entfernen. Wenn sich der Benutzer das nächste Mal an der Webbenutzeroberfläche anmeldet, fordert Avamar Desktop/Laptop den Benutzer zur Auswahl einer neuen Startzeit auf der Seite **Backup** auf.

Der Avamar-Server ordnet der Gruppe des Clients eine vom Benutzer ausgewählte Startzeit zu. Durch das Entfernen des Clients aus einer Gruppe wird auch die vom Benutzer ausgewählte Startzeit für diesen Client entfernt.

Vorgehensweise

1. Vergewissern Sie sich, dass der Client einer Gruppe angehört, die eine tägliche Planung verwendet.
2. Fügen Sie mithilfe von Avamar-Administrator der Planung **Tägliche Planung außer Kraft setzen** Zeiteinträge hinzu.

   Um der Planung **Tägliche Planung außer Kraft setzen** Zeiteinträge hinzuzufügen, führen Sie die unter Bearbeiten der Startzeiten für Clientaußerkraftsetzungen von Gruppenplanungen auf Seite 120 beschriebene Aufgabe aus.

   Hinweis

   Override Daily Schedule zeigt die Zeitwerte für die Zeitzone des Avamar-Servers an. Avamar Desktop/Laptop verwendet die Zeitzone des Clients, wenn die Zeiten angezeigt werden, die auf der **Backup**-Seite zu sehen sind.

3. Aktivieren Sie mithilfe von Avamar-Administrator die Option **Außerkraftsetzen der täglichen Planung der Gruppe zulassen** für den Client.

Außerkraftsetzen von Gruppen-Policy-Einstellungen für einen Client auf Seite 137 enthält Anweisungen für die Einstellung **Allow override of group's daily schedule**.

Option „Daten hinzufügen“

Für geplante Backups und On-Demand-Backups können Benutzer Ordner angeben, die in den Gruppen-Policy-basierten Backups eines Avamar Desktop/Laptop-Clientcomputers berücksichtigt werden sollen.

Wenn die Option „Daten hinzufügen“ aktiviert ist, erstellt Avamar Desktop/Laptop Backup-Datasets für den Clientcomputer, indem die vom Benutzer ausgewählten Ordner dem Dataset jeder Gruppe, zu der der Avamar Desktop/Laptop-Clientcomputer gehört, hinzugefügt werden. Avamar Desktop/Laptop wendet die Aus- und Einschlüsse in der Dataset-Policy jeder Gruppe auf die vom Benutzer angegebenen Ordner an.

Verwenden Sie Avamar-Administrator, um diese Option zu aktivieren. Außerkraftsetzen von Gruppen-Policy-Einstellungen für einen Client auf Seite 137 bietet Anweisungen für die Verwendung von Avamar-Administrator zum Aktivieren der Option **Allow additions to source data**.

Nachdem Sie die Option „Daten hinzufügen“ aktiviert haben, können Benutzer Ordner hinzufügen, indem sie auf der Seite **Backup** der Webbenutzeroberfläche auf **Daten hinzufügen** klicken und die Ordner auswählen.

Backups mit nur einem Klick

Benutzer können ein On-Demand-Backup auf einem Avamar Desktop/Laptop-Clientcomputer mit einem einzigen Klick auf die Schaltfläche **Jetzt sichern** im Clientmenü oder im Dialogfeld mit der Backuperinnerung starten.

Die Daten, die in einem mit nur einem Klick durchführbaren Backup enthalten sind, sind vom Betriebssystem des Clientcomputers abhängig. In der folgenden Tabelle sind die Daten beschrieben, die für bestimmte Betriebssysteme eingeschlossen werden. Wenn die Option „Daten hinzufügen“ aktiviert ist, fügt Avamar Desktop/Laptop auch vom Benutzer ausgewählte Ordner zu den im Backup berücksichtigten Daten hinzu.

Tabelle 112 Datasets für mit nur einem Klick durchführbare On-Demand-Backups

Betriebssystem	Im Backup enthaltene Daten
• Windows • Mac	Dataset für jede Gruppe, zu der der Client gehört
• Linux • Windows Server • Mac OS X Server	Dem Computer zugewiesenes Dataset

Interaktive Backups

Interaktive Backups bieten Benutzern die Möglichkeit, eine dem Client zugeordnete Backupgruppe auszuwählen und den Client mithilfe der Gruppeneinstellungen zu sichern. Wenn On-Demand-Backupsätze aktiviert sind, bieten interaktive Backups Benutzern auch die Möglichkeit, stattdessen nur ausgewählte Dateien und Ordner zu sichern.

Gruppenauswahl
So führen Sie ein interaktives Backup einer einzigen Gruppe durch:

1. Wählen Sie **Back Up...** im Clientmenü.
2. Wählen Sie die Backupgruppe auf der Seite **Backup** der Webbenutzeroberfläche.
3. Klicken Sie auf **Back Up Now**.

Wenn ein Benutzer ein interaktives Backup einer Gruppe ausführt, werden alle der ausgewählten Gruppe zugeordneten Policies auf das Backup angewendet.

Ein interaktives Backup einer Gruppe unterscheidet sich von einem Einfachklick-Backup, da in einem interaktiven Backup einer Gruppe nur die ausgewählte Gruppe gesichert wird.

Datei- und Ordnerauswahl
Um es Benutzern zu ermöglichen, ohne Berücksichtigung der dem Client zugewiesenen Gruppen-Policies ausgewählte Dateien auf einem Avamar Desktop/Laptop-Client zu sichern, aktivieren Sie On-Demand-Backupsätze. Nach der Aktivierung von On-Demand-Backupsätzen können Benutzer auf Windows-, Mac- und Linux-Computern, die Avamar Desktop/Laptop-Clients sind, Sätze von Ordnern und Dateien erstellen, die über On-Demand-Backups gesichert werden sollen. Benutzer können mehrere Sätze erstellen, die Sätze zur Wiederverwendung speichern und ein auf einem Satz basierendes Backup an die Backupwarteschlange auf dem Avamar-Server senden.

Bei Verwendung von On-Demand-Backupsätzen werden die Daten, die gesichert werden, nicht gemäß den Gruppen-Policies geändert, die dem Avamar Desktop/Laptop-Client zugeordnet sind.

Der Avamar-Server kann so konfiguriert werden, dass die Anzahl der On-Demand-Backupsatz-Backups, die von einem Avamar Desktop/Laptop-Client gestartet werden kann, begrenzt ist.

Um Backupdaten in Data Domain zu speichern, beachten Sie die folgenden Informationen:

- Wenn ein Data Domain-System für den Avamar-Server konfiguriert wurde, werden On-Demand-Backups im GSAN gesichert.
- Wenn ein einziges Data Domain-System für den Avamar-Server konfiguriert wurde, werden On-Demand-Backups in Data Domain gesichert.
- Wenn mehrere für den Avamar-Server konfigurierten Data Domain-Systeme vorhanden sind, werden On-Demand-Backups an das Data Domain-System gesendet, das über mehr verfügbaren Speicherplatz verfügt.

Zulassen der benutzerseitigen Erstellung von On-Demand-Backupsätzen

Sie können Benutzern auf Windows-, Mac- und Linux-Clients, die Avamar Desktop/Laptop verwenden, das Erstellen von On-Demand-Backupsätzen ermöglichen.

Vorgehensweise

1. Aktivieren Sie die Einstellung **Allow file selection on client initiated backups** in Avamar-Administrator. Anweisungen finden Sie unter Außerkraftsetzen von Gruppen-Policy-Einstellungen für einen Client auf Seite 137.
2. Ändern Sie den Wert des Schlüssels `allowUserInititedBackupsFileSelection` in der Datei `dtlt.properties` auf dem Avamar-Server zu `true`.
3. Benutzer erstellen On-Demand-Backupsätze:

a. Klicken Sie auf dem Avamar Desktop/Laptop-Clientcomputer mit der rechten Maustaste auf das Avamar-Symbol und wählen Sie **Back Up...** aus.

   Die Webbenutzeroberfläche wird mit der Seite **Backup** geöffnet.

b. Klicken Sie unter **Select folders and files to backup** auf **Select Now**.

   Das Dialogfeld **On-Demand Backup Sets** wird angezeigt.

c. Wählen Sie die zu sichernden Ordner und Dateien aus und klicken Sie auf **OK**.

d. Um den Backupsatz zur Wiederverwendung zu speichern, geben Sie unter **Save backup set as** einen Namen für den Backupsatz ein und klicken Sie dann auf **Save**.

e. (Optional) Um den Avamar-Server anzuweisen, ein Backup des On-Demand-Backupsatzes zu der Backupwarteschlange hinzuzufügen, klicken Sie auf **Start Backup** und dann auf **OK**.

4. So weisen Benutzer den Avamar-Server an, ein Backup eines gespeicherten On-Demand-Backupsatzes zur Backupwarteschlange hinzuzufügen:

   a. Klicken Sie auf dem Avamar Desktop/Laptop-Clientcomputer mit der rechten Maustaste auf das Avamar-Symbol und wählen Sie **Back Up...** aus.

      Die Webbenutzeroberfläche wird mit der Seite **Backup** geöffnet.

   b. Klicken Sie unter **Select folders and files to backup** auf **Select Now**.

      Das Dialogfeld **On-Demand Backup Sets** wird angezeigt.

   c. Wählen Sie unter **Load Backup Set** den Backupsatz aus.

   d. Klicken Sie auf **Start Backup** und dann auf **OK**.

Einstellen einer Einschränkung bei On-Demand-Backups

Legen Sie einen Grenzwert für die Anzahl der On-Demand-Backupsatz-Backups fest, die ein Benutzer der Aufgabenwarteschlange des Avamar-Servers hinzufügen kann.

Standardmäßig verwendet der Avamar-Server die folgenden Regeln für On-Demand-Backupsatz-Backups:

- In der Aufgabenwarteschlange sind nicht mehrere On-Demand-Backupsatz-Backups von einem Client gleichzeitig zulässig.
- Ein On-Demand-Backupsatz-Backup kann nicht gestartet werden, während ein Backup für den Client ausgeführt wird.
- Es gibt keine Begrenzung für die Anzahl der On-Demand-Backupsatz-Backups eines Clients, die ein Benutzer der Aufgabenwarteschlange hinzufügen kann.

Um einen Grenzwert für die Anzahl der On-Demand-Backupsatz-Backups festzulegen, die täglich für Avamar Desktop/Laptop-Clientcomputer durchgeführt werden können, legen Sie die Eigenschaft `restrictBackupsPerDay` in der Datei `dtlt.properties` auf dem Avamar-Server fest.

In der folgenden Tabelle werden die verfügbaren Werte beschrieben.

Tabelle 113 Unterstützte Werte für die Eigenschaft `restrictBackupsPerDay`

Wert	Beschreibung
`false`	Es gibt keine spezifische Einschränkung bezüglich der Anzahl von On-Demand-

Tabelle 113 Unterstützte Werte für die Eigenschaft `restrictBackupsPerDay` (Fortsetzung)

Wert	Beschreibung
	Backupsatz-Backups, die erfolgreich an einem Tag ausgeführt werden können. In der Standardeinstellung ist keine Begrenzung vorhanden.
0	Benutzer können keine On-Demand-Backupsatz-Backups ausführen.
n	Es können nicht mehr als *n* On-Demand-Backupsatz-Backups für einen Client pro Tag durchgeführt werden. *n* ist hier eine positive Ganzzahl kleiner oder gleich 100. Ein Tag ist von Mitternacht bis Mitternacht in der Zeitzone für den Avamar-Server definiert.

Der angegebene Wert gilt für alle auf dem Avamar-Server aktivierten Clients. Alle erfolgreich abgeschlossenen Backups für alle Benutzer auf einem Avamar Desktop/Laptop-Clientcomputer fließen in die Gesamtanzahl der pro Tag erlaubten Backups ein.

Hinweis

Dieser Grenzwert gilt nur für Backups, denen ein vom Benutzer erstellter On-Demand-Backupsatz zugrunde liegt.

Deaktivieren von On-Demand-Backups

Sie können verhindern, dass Benutzer On-Demand-Backups von Avamar Desktop/Laptop-Clientcomputern durchführen. Diese Einstellung gilt sowohl für Einfachklick-On-Demand-Backups als auch für interaktive On-Demand-Backups.

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Policy**Link zum Startprogramm.

   Das Fenster **Policy** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Clients**.
3. Deaktivieren Sie On-Demand-Backups für einen Client oder mehrere Clients.

Anzahl der Clients	Schritte zum Deaktivieren von On-Demand-Backups
Eins	a. Wählen Sie den Client aus und klicken Sie auf **Edit**. b. Deaktivieren Sie im Dialogfeld **Edit Client** die Option **Allow client initiated backups**. c. Klicken Sie auf **OK**.
Zwei oder mehr Clients	a. Wählen Sie die Clients aus und klicken Sie auf **Edit**. b. Ändern Sie im Dialogfeld **Edit Multiple Clients** die Einstellung für **Allow client initiated backups** zu **No**. c. Klicken Sie auf **Apply Change**.

Anzahl der Clients	Schritte zum Deaktivieren von On-Demand-Backups
	d. Klicken Sie auf **OK**.

Ändern der Aufbewahrungs-Policy für On-Demand-Backups

Mit der Policy „End User On Demand Retention“ wird die Aufbewahrung der Daten für On-Demand-Backups gesteuert. Sie können die Policy End User On Demand Retention auf einem Avamar-Server mithilfe von Avamar-Administrator ändern. Die Änderung gilt für alle On-Demand-Backups, die von einem für diesen Server aktivierten Client initiiert wurden. allerdings nur für nach dieser Änderung durchgeführte On-Demand-Backups.

Vorgehensweise

1. Wählen Sie in Avamar Administrator den Befehl **Tools** > **Manage Retention Policies** aus.

   Das Fenster **Manage All Retention Policies** wird angezeigt.
2. Wählen Sie **End User On Demand Retention** aus der Liste aus und klicken Sie auf **Edit**.

   Das Dialogfeld **Edit Retention** wird angezeigt.
3. Geben Sie unter **Retention period** eine Zahl ein und wählen Sie eine Zeiteinheit aus („days“, „weeks“, „months“ oder „years“).
4. Klicken Sie auf **OK**.

Wiederherstellen mit Avamar Desktop/Laptop

Die folgenden Themen liefern Informationen zur Durchführung von Wiederherstellungen und zur Steuerung wiederherstellungsbezogener Einstellungen in Avamar Desktop/Laptop.

Suchen nach wiederherzustellenden Daten

Avamar Desktop/Laptop-Benutzer können über die Webbenutzeroberfläche entweder zu wiederherzustellenden Ordnern, Dateien und Dateiversionen navigieren oder nach diesen suchen.

Navigieren zu wiederherzustellenden Daten
Wählen Sie im Menü auf der linken Seite die Option **Browse** aus, um die Backups für einen Clientcomputer in einer Baumstruktur anzuzeigen, in der Sie navigieren können, um nach wiederherzustellenden Ordnern und Dateien zu suchen.

Um zu einem bestimmten Backup und nicht zu allen Backups für den Client zu navigieren, verwenden Sie zur Auswahl des Datums und der Uhrzeit des Backups die Optionen **Backup Date** und **Time**.

Suchen nach wiederherzustellenden Daten
Wählen Sie in der Webbenutzeroberfläche aus dem Menü auf der linken Seite die Option **Search** aus, um nach bestimmten wiederherzustellenden Ordnern und Dateien zu suchen. Geben Sie zum Starten einer Suche eine Suchzeichenfolge in das Suchfeld ein und klicken Sie auf **Search**. Die Ergebnisse werden während der Ausführung der Suche angezeigt und eine Fortschrittsanzeige gibt Informationen über die Dauer der Suche an.

Die von Ihnen im Suchfeld angegebene Suchzeichenfolge darf maximal 255 Zeichen lang sein und kann in Groß- und Kleinschreibung eingegeben werden. Zu den unterstützten Platzhalterzeichen gehören das Sternchen (*), um null oder mehr Zeichen darzustellen, und das Fragezeichen (?), um ein Zeichen darzustellen.

Die Zeichenfolge wird mit den Namen aller Ordner und Dateien in den Backups für den Clientcomputer verglichen. Wenn der Name eines Ordners bzw. einer Datei ganz oder teilweise mit der Zeichenfolge übereinstimmt, wird der Ordner- bzw. Dateiname in den Suchergebnissen angezeigt.

Auswählen einer Dateiversion

Die Backups für einen Clientcomputer umfassen mehr als eine Version von zahlreichen Dateien, die gesichert werden. Wenn eine Datei gesichert und anschließend bearbeitet wird, enthält das nächste Backup eine neue Version dieser Datei. Jede Version wird für die vom Avamar Administrator festgelegte Aufbewahrungsfrist aufbewahrt.

Die Anzahl der Versionen einer Datei in den Clientbackups ist von vielen Faktoren abhängig, z. B.:

- der Aufbewahrungsdauer der gesicherten Daten,
- der Häufigkeit von Backups und
- der Bearbeitungshäufigkeit der Datei.

Wenn mehrere Versionen einer Datei in den Backups für einen Client vorhanden sind, wird beim Navigieren zu oder Suchen nach wiederherzustellenden Daten neben dem Dateinamen ein Versionssymbol angezeigt. Um eine andere Version der Datei als die letzte Version auszuwählen, klicken Sie auf das Versionssymbol und wählen Sie dann die Version aus. Legen Sie anschließend fest, ob die vorhandene Datei auf dem Clientcomputer überschrieben oder ob die Dateiversion mit einem neuen Namen wiederhergestellt werden soll.

Wiederherstellungstypen

Avamar Desktop/Laptop-Benutzer können Daten am ursprünglichen Speicherort oder an einem neuen Speicherort auf demselben Computer wiederherstellen. Benutzer können Daten mit demselben Namen oder mit einem neuen Namen wiederherstellen.

Wenn Benutzer Daten am ursprünglichen Speicherort unter demselben Namen wiederherstellen, werden im Zuge des Wiederherstellungsprozesses alle aktuellen lokalen Dateiversionen mit den wiederhergestellten Dateien überschrieben. Dieser Wiederherstellungstyp ist nützlich, wenn die aktuellen lokalen Versionen Fehler enthalten oder Probleme mit beschädigten Daten aufweisen.

Benutzer können die Dateien auch an einem neuen Speicherort oder mit einem neuen Namen oder mit beiden Möglichkeiten wiederherstellen, um ein Überschreiben der aktuellen lokalen Dateiversionen zu vermeiden.

Domainbenutzer können Dateien von jedem Windows- oder Mac-Computer, auf dem sie über ein Benutzerprofil verfügen, auf dem Windows- oder Mac-Computer wiederherstellen, bei dem sie angemeldet sind. Sie können das Wiederherstellen von einem anderen Rechner deaktivieren, indem Sie den Wert der Eigenschaft `disableRestoreFromAlternateComputer` in der Datei `dtlt.properties` des Avamar-Servers auf `true` setzen. Diese globale Eigenschaft wirkt sich auf alle Clients aus.

Einschränkung bei der Wiederherstellung unter Linux und Mac

Linux- und Mac-Benutzer ohne Schreibberechtigung für den Stammordner können nicht mit Avamar Desktop/Laptop ihre vollständige Verzeichnisstruktur am ursprünglichen Speicherort wiederherstellen. Das Betriebssystem interpretiert diese

Art von Wiederherstellung als unbefugten Schreibversuch im Stammordner und verhindert sie daher.

Der Wiederherstellungsversuch einer vollständigen Verzeichnisstruktur schlägt fehl, wenn die folgenden Bedingungen erfüllt sind:

- Der Benutzer meldet sich bei einem Mac- oder Linux-Computer mit einem Benutzerkonto an, das über keine Schreibberechtigung für den Stammordner verfügt.
- Der Benutzer meldet sich mit der Avamar-Authentifizierungsmethode bei der Avamar Desktop/Laptop-Webbenutzeroberfläche an.
- Der Benutzer wählt auf der Avamar Desktop/Laptop-Seite „Browse“ die vollständige Verzeichnisstruktur aus.
- Der Benutzer wählt keinen neuen Speicherort für die Wiederherstellung aus.

Workarounds

Um diese Einschränkung zu umgehen, verwenden Sie eine der folgenden Methoden für die Wiederherstellung:

- Stellen Sie die vollständige Verzeichnisstruktur an einem neuen Speicherort wieder her.
- Stellen Sie weniger als alle Dateien in der Verzeichnisstruktur wieder her.

  Entfernen Sie beispielsweise eine Datei aus dem Ordner, die sich in der Hierarchie des Wiederherstellungssatzes am weitesten unten befindet. Das Wiederherstellen von weniger als allen Dateien funktioniert, weil das Betriebssystem die nachfolgende Wiederherstellung als eine Reihe von Schreibvorgängen in Ordnern unterhalb des Stammordners interpretiert.

Wiederherstellungsanforderungen

Um von einem anderen Computer wiederherzustellen, überprüfen Sie vor einer Wiederherstellung die Berechtigungsanforderungen und die Anforderungen.

Wiederherstellungsberechtigungen

Zu welchen Daten Benutzer navigieren können bzw. welche Daten Benutzer suchen und wiederherstellen können, hängt von den Kontoberechtigungen zur Benutzeranmeldung ab.

Wenn Benutzer nach wiederherzustellenden Daten suchen bzw. diese durchsuchen, werden die angezeigten Ergebnisse auf Grundlage der aktuellen Anmeldedaten und der von diesem Clientcomputer gesicherten Daten gefiltert. In der folgenden Tabelle finden Sie Details zur Filterung.

Tabelle 114 Avamar Desktop/Laptop-Filterung bei Datenwiederherstellungen

Datentyp	Filterung unter Windows	Filterung unter Mac
Ordner	Es werden alle Ordner angezeigt, für die der angemeldete Benutzer Eigentümer oder Mitglied einer Gruppe mit entsprechenden Eigentumsrechten ist. Außerdem werden alle Ordner angezeigt, die Ordner oder	Es werden alle Ordner angezeigt, für die der angemeldete Benutzer eine Leseberechtigung hat: entweder als Eigentümer oder aufgrund der Gruppen- oder anderer Berechtigungen für den Ordner.

Tabelle 114 Avamar Desktop/Laptop-Filterung bei Datenwiederherstellungen (Fortsetzung)

Datentyp	Filterung unter Windows	Filterung unter Mac
	Dateien enthalten, für die der Benutzer Rechte hat.	
Dateien	Es werden alle Dateien angezeigt, deren Eigentümer der angemeldete Benutzer ist.	Es werden alle Dateien angezeigt, deren Eigentümer der angemeldete Benutzer ist.

Wenn die Benutzer nach wiederherzustellenden Daten suchen, erfolgen die folgenden Aktionen:

- Ordner, für die der Benutzer keine Eigentumsrechte besitzt, werden im Dateisystempfad für Ordner angezeigt, für die der Benutzer Eigentumsrechte hat. Durch diese Option wird eine genauere Darstellung des Dateisystems auf dem Computer ermöglicht.
- Es wird ein abgeblendetes Kontrollkästchen neben den Ordnern angezeigt. Die Ordner werden nicht wiederhergestellt, wenn Sie einen Ordner oder eine Datei wiederherstellen, dessen bzw. deren Pfad diese Ordner enthält.

Benutzer sind nur dann in der Lage, Daten wiederherzustellen, wenn ihre Anmeldedaten Betriebssystem-Schreibberechtigungen für den Wiederherstellungsspeicherort gewähren. Damit Daten mit demselben Pfad und Namen wie die Daten auf dem Clientcomputer wiederhergestellt werden, muss der Benutzer durch die Anmeldedaten als Eigentümer der vorhandenen Daten authentifiziert werden, bevor die Wiederherstellung fortgesetzt wird.

Um Dateien unter Windows wiederherzustellen, muss das Anmeldekonto in den lokalen Sicherheitseinstellungen über das Benutzerrecht `Restore files and directories` verfügen. Dieses Benutzerrecht wird standardmäßig Konten zugewiesen, die Mitglieder der Gruppe „Administratoren“ oder „Backupoperatoren“ sind. Weisen Sie dieses Recht einem Konto zu, das nicht Mitglied einer dieser Gruppen oder einer anderen Gruppe mit diesem Benutzerrecht ist. Erst dann ist es einem Benutzer möglich, das Konto zum Wiederherstellen von Daten zu verwenden.

Anforderungen für die Wiederherstellung von einem anderen Computer

Damit von einem anderen Computer aus wiederhergestellt werden kann, müssen die Anforderungen in der folgenden Tabelle erfüllt sein.

Tabelle 115 Anforderungen für die Wiederherstellung von einem anderen Computer mit Avamar Desktop/Laptop

Kategorie	Anforderung
Betriebssystem	• Windows-Betriebssystem • Mac-Betriebssystem **Hinweis** Wiederherstellungen zwischen Windows- und Mac-Computern werden unterstützt.
Kontotyp	Domain

Tabelle 115 Anforderungen für die Wiederherstellung von einem anderen Computer mit Avamar Desktop/Laptop (Fortsetzung)

Kategorie	Anforderung
Profil	Sowohl Quell- als auch Zielcomputer verfügen über ein lokales Profil für das Domainkonto des Benutzers. **Hinweis** Ein lokales Profil für ein Domainkonto wird automatisch bei der ersten Anmeldung des Benutzers am Computer erstellt.
Avamar-Client	Version 7.0 oder höher ist sowohl auf der Quelle als auch auf dem Ziel installiert.
Avamar-Server	Sowohl Quelle als auch Ziel sind auf demselben Avamar-Server aktiviert und auf dem Server wird Avamar 7.0 oder höher ausgeführt.
Backup	Es liegt mindestens ein qualifizierendes Backup vor. Ein qualifizierendes Backup ist ein erfolgreich abgeschlossenes Backup, bei dem folgende Bedingungen erfüllt sind: • Avamar Desktop/Laptop 7.0 oder höher wurde auf dem Quellcomputer installiert. • Auf dem Quellcomputer wurde ein lokales Profil für das Domainkonto des Benutzers erstellt.

Standardmäßig können Benutzer mit lokalen Administratorrechten auf einem Windows-Quellcomputer zum Zeitpunkt eines Backups beliebige Dateien von diesem Quellcomputer auf einem Zielcomputer wiederherstellen, und zwar ungeachtet der Dateieigentumsrechte. Sie können dieses Verhalten ändern, um den Zugriff auf die Dateien zu beschränken, die den Benutzern gehören. Um den Dateizugriff für Windows-Administratoren zu beschränken, ändern Sie den Wert der Eigenschaft `checkAlternateComputerOwnership` in der Datei `dtlt.properties` auf dem Avamar-Server in `true`.

Wiederherstellungslimits

Die Datenmenge in einer einzigen Wiederherstellungsaufgabe und die Anzahl gleichzeitiger Wiederherstellungsaufgaben für einen Clientcomputer können eingeschränkt werden.

Limit der Wiederherstellungsdatengröße
Für Avamar Client-Benutzer gibt es in der Regel kein Limit hinsichtlich der Datenmenge, die im Rahmen einer einzigen Aufgabe wiederhergestellt wird. Diese Standardeinstellung ermöglicht es einem Benutzer, ein komplettes Backup über eine einzige Aufgabe wiederherzustellen. Äußerst umfangreiche Wiederherstellungsaufgaben können zu einer unerwünschten Belastung des Netzwerks führen. Legen Sie ein Limit für die Wiederherstellungsdatengröße fest, um

die von diesen umfangreichen Wiederherstellungsaufgaben verursachte Netzwerklast zu steuern.

Wenn Sie ein Limit festlegen, können einzelne Benutzer nicht mehr als das Limit einer Wiederherstellungsaufgabe wiederherstellen. Benutzer müssen Dateien, die das Limit überschreiten, in mehreren Aufgaben wiederherstellen, die das Limit nicht überschreiten, oder die Wiederherstellung muss von einem Administrator durchgeführt werden.

HINWEIS

Das Limit der Wiederherstellungsdatengröße gilt nicht für Clients der Serverklasse (Clients mit einem sehr großen Backup-Dataset).

Um ein Limit für die Wiederherstellungsdatengröße festzulegen, heben Sie die Auskommentierung des Schlüssels `limitRestoreSize` in der Datei `dtlt.properties` auf dem Avamar-Server auf und geben Sie den Wert für die Beschränkung der Datengröße in MB an.

Limit der Wiederherstellungswarteschlange

Die Webbenutzeroberfläche des Avamar-Clients minimiert Netzwerk- und Serverlasten, indem sie Wiederherstellungsanforderungen für Clients blockiert, bei denen sich bereits eine Wiederherstellungsaufgabe in der Warteschlange befindet. Benutzer, die eine neue Wiederherstellung starten, während noch eine andere Aufgabe ansteht, erhalten eine Nachricht, dass die Anforderung blockiert wird. Nach Abschluss der anstehenden Aufgabe können Benutzer eine neue Wiederherstellungsaufgabe initiieren. Sie können dieses Verhalten ändern, damit Benutzer mehrere Wiederherstellungsaufgaben starten können. Die Änderung gilt für alle Clients des Avamar-Servers.

Um das Limit der Wiederherstellungswarteschlange zu entfernen, ändern Sie den Wert der Eigenschaft `disallowMultipleRestores` in der Datei `dtlt.properties` auf dem Avamar-Server in `false`.

Wiederherstellen replizierter Backups

Sie können einen Avamar-Client mit den Avamar Client Manager-Replikationsbefehlen zu einem neuen Avamar-Server verschieben. Wenn Sie einen Client verschieben, werden die Backups für den Client auf dem neuen Server repliziert. Avamar Desktop/Laptop muss replizierte Backups indexieren, bevor sie in der Webbenutzeroberfläche durchsucht oder gesucht werden können.

Wenn sich ein Benutzer über die Webbenutzeroberfläche beim Client anmeldet, nachdem der Client verschoben wurde, wird das Dialogfeld **Replicated Backups Available** angezeigt. Der Benutzer kann entweder die Indizierung der replizierten Backups starten oder das Dialogfeld ohne Start der Indizierung schließen. Schließt der Benutzer das Dialogfeld ohne Indexierung, wird ein Warnmeldesymbol in der Bannerleiste der Webbenutzeroberfläche angezeigt. Dem Benutzer ist es ebenfalls möglich, die Indizierung über das Warnmeldesymbol zu starten.

Bei der Indexierung handelt es sich um eine einmalig durchgeführte Aufgabe für einen Computer, der auf einen neuen Server verschoben wurde. Sie wird in derselben Sitzung ausgeführt, in der sie auch gestartet wird. Anschließend sendet Avamar Desktop/Laptop dem Webbrowser einen Befehl zum Aktualisieren. Die Daten von den replizierten Backups werden in der Webbenutzeroberfläche angezeigt.

Verlauf der Backup- und Wiederherstellungsaktivität des Clients

Die Seite **History** der Avamar Desktop/Laptop-Webbenutzeroberfläche bietet eine Aufzeichnung der Backup- und Wiederherstellungsaktivität auf dem Clientcomputer im Verlauf von 14 Tagen.

Im Abschnitt **Activity History** der Seite **History** finden Sie Informationen zu den Backups und Wiederherstellungen der letzten 14 Tage. Zudem werden Links zu detaillierteren Informationen über die Backups zur Verfügung gestellt. Zu den Informationen gehören das Ergebnis der Aktivität, das Startdatum und die Startzeit, die Dauer der Aktivität, die Datenmenge und die ID des Arbeitsauftrags. Klicken Sie auf die Aktivitätsbezeichnung für ein Backup, um eine Liste der Dateien im Dataset für das Backup anzuzeigen.

Um den Backupverlauf für einen anderen Computer anzuzeigen, wählen Sie den entsprechenden Computer aus der Liste aus. Die unter Anforderungen für die Wiederherstellung von einem anderen Computer auf Seite 470 beschriebenen Anforderungen müssen erfüllt sein, bevor der Backupverlauf für einen anderen Computer angezeigt werden kann.

Bearbeiten von Avamar Desktop/Laptop-Parametern

Mit der Avamar Desktop/Laptop-Eigenschaftendatei `dtlt.properties` können Sie Parameter ändern, die sich auf die Funktionen aller Avamar Desktop/Laptop-Clients auswirken, die eine Verbindung zum Avamar-Server herstellen. Die Datei befindet sich auf dem Avamar-Server im folgenden Verzeichnis: `/usr/local/avamar/etc/dtlt.properties`.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell:
   a. Melden Sie sich beim Server als Administrator an.
   b. Ändern Sie den Benutzer zum Root-Benutzer, indem Sie `su -` eingeben.
   c. Laden Sie für einen Multi-Node-Server den OpenSSH-Schlüssel rootid, indem Sie Folgendes eingeben:

      ```
      ssh-agent bashssh-add /root/.ssh/rootid
      ```

2. Wechseln Sie in das Verzeichnis `/usr/local/avamar/etc`, indem Sie den folgenden Befehl eingeben:

   ```
   cd /usr/local/avamar/etc
   ```

3. Öffnen Sie `dtlt.properties` in einem Texteditor.
4. Erstellen oder bearbeiten Sie die Parameter.
5. Speichern und schließen Sie die Datei.

Avamar Desktop/Laptop-Parameter

In der folgenden Tabelle sind die Parameter aufgeführt, die in der Datei `dtlt.properties` verfügbar sind.

Tabelle 116 Avamar Desktop/Laptop-Parameter

Parameter	Beschreibung
allowLocalUsers	Aktiviert und deaktiviert den Zugriff durch lokale Benutzer für die Pass-Through-Authentifizierung. Heben Sie die Auskommentierung des Parameters auf, indem Sie das Zeichen # vor dem Parameter entfernen. Legen Sie den Wert dann auf true fest, um den Zugriff durch lokale Benutzer für die Pass-Through-Authentifizierung zu aktivieren. Verwenden Sie den Standardwert false, um den Zugriff durch lokale Benutzer für die Pass-Through Authentifizierung zu deaktivieren.
allowServerRestores	Aktiviert oder deaktiviert lokal gestartete Wiederherstellungen auf Computern der Serverklasse. Verwenden Sie den Standardwert true, um Wiederherstellungen auf Rechnern der Serverklasse zuzulassen, oder legen Sie false fest, um Wiederherstellungen auf Rechnern der Serverklasse zu unterbinden.
allowUserInititedBackupsFileSelection	Aktiviert oder deaktiviert die Funktion, dass Benutzer Sets von Ordnern und Dateien zum Sichern in On-Demand-Backups erstellen können. Um auswählbare Backupsätze zu ermöglichen, aktivieren Sie die Einstellung **Allow file selection on client initiated backups** für den Client in Avamar Administrator und legen Sie dann den Wert des Parameters allowUserInititedBackupsFileSelection auf true fest. Verwenden Sie den Standardwert false, um auswählbare Backupsätze zu deaktivieren.
checkAlternateComputerOwnership	Steuert, ob Benutzer mit lokalen Administratorrechten beliebige Dateien vom Quellcomputer oder nur eigene Dateien wiederherstellen können. Geben Sie true an, um lokale Administratoren auf die Wiederherstellung eigener Dateien zu beschränken, oder stellen Sie den Standardwert false ein, damit lokale Administratoren beliebige Dateien vom Quellcomputer wiederherstellen können.
disableRestoreFromAlternateComputer	Aktiviert oder deaktiviert die Wiederherstellung von einem anderen Computer. Geben Sie true an, um die Wiederherstellung von einem anderen Computer zu deaktivieren, oder stellen Sie den Standardwert false ein, um die Wiederherstellung von einem anderen Computer zu aktivieren.
disallowMultipleRestores	Steuert, ob Benutzer gleichzeitig mehrere Wiederherstellungsaufgaben für einen Clientcomputer starten können. Legen Sie false fest, um mehrere gleichzeitige Wiederherstellungen zuzulassen, oder verwenden Sie den Standardwert true, um mehrere gleichzeitige Wiederherstellungen zu verhindern.
limitRestoreSize	Steuert, ob die in einer einzigen Aufgabe wiederhergestellte Datenmenge eingeschränkt werden soll. Um einen Grenzwert festzulegen, heben Sie die Auskommentierung des

Tabelle 116 Avamar Desktop/Laptop-Parameter (Fortsetzung)

Parameter	Beschreibung
	Parameters `limitRestoreSize` auf und geben Sie die Beschränkung für die Datengröße in MB an. Das Standardlimit beträgt 500 MB.
`maxDirectoryDepth`	Gibt die Anzahl der verschachtelten Unterordner in jeder hierarchischen Baumstruktur eines Backups an, die der Avamar Desktop/Laptop-Server während der Indizierung durchläuft. Der Standardwert ist `3000`.
`restrictBackupsPerDay`	Steuert, ob die Anzahl der vom Clientcomputer an einem Tag durchführbaren On-Demand-Backups eingeschränkt ist. Falls ja, wird auch der Maximalwert festgelegt. Verwenden Sie den Standardwert `false`, wenn die Anzahl der an einem Tag erfolgreich ausführbaren On-Demand-Backups nicht eingeschränkt werden soll. Geben Sie den Wert `0` an, um On-Demand-Backups auf dem Clientcomputer zu deaktivieren. Um die Anzahl der an einem Tag erfolgreich ausführbaren On-Demand-Backups einzuschränken, legen Sie den Grenzwert als positive ganze Zahl kleiner als oder gleich 100 fest.
`useAppletToBrowseLocalFile`	Steuert, ob Benutzer die betriebssystemspezifischen Dienste zum Durchsuchen von Dateien auf dem Clientcomputer oder die alternative Methode zum Durchsuchen von Dateien verwenden. Legen Sie `true` fest, damit Benutzer die betriebssystemspezifischen Dienste zum Durchsuchen von Dateien verwenden können, oder stellen Sie `false` ein, um durchzusetzen, dass Benutzer die alternative Methode zum Durchsuchen von Dateien einsetzen. Der Standardwert ist `false`.
`userLoginRequired`	Aktiviert und deaktiviert die Pass-Through-Authentifizierung. Verwenden Sie den Standardwert `false`, um die Pass-Through-Authentifizierung zu aktivieren, oder `true`, um die Pass-Through-Authentifizierung zu deaktivieren.

Speicherorte der Clientprotokolle

Lokale Protokolle auf Clientcomputern liefern Informationen zu Backup- und Wiederherstellungsvorgängen sowie zu Funktionen der Benutzeroberfläche.

Verfügbare Protokolle

In der folgenden Tabelle werden die auf Clientcomputern verfügbaren Protokolle aufgeführt.

Tabelle 117 Verfügbare Clientprotokolle

Protokolltyp	Protokolldateiname	Beschreibung
Arbeitsauftrag	*workorder_name*.log, wobei *workorder_name* für den vollständigen Namen einer Aufgabe steht	Liefert detaillierte Informationen über eine bestimmte Aufgabe.

Tabelle 117 Verfügbare Clientprotokolle (Fortsetzung)

Protokolltyp	Protokolldateiname	Beschreibung
Agent	`avagent.log`	Liefert Informationen über den Status sämtlicher Backup- und Wiederherstellungsaktivitäten auf dem Computer.
Konsole	`avscc.log`	Liefert Informationen über die Performance der Benutzeroberfläche. Für jeden Benutzer auf einem Computer wird ein Konsolenprotokoll erstellt.

Der Zugriff auf diese Protokolle erfolgt über die Clientbenutzeroberfläche. Der Zugriff kann auch direkt erfolgen.

Protokollspeicherorte auf Windows-Computern

Auf Windows-Computern stehen die Protokolle über die Pfade in der folgenden Tabelle zur Verfügung.

Tabelle 118 Pfade zu Protokollen auf Windows-Computern

Protokoll	Pfad
Arbeitsauftrag	`%SystemDrive%\Program Files\avs\var\clientlogs\`
Agent	`%SystemDrive%\Program Files\avs\var\`
Konsole	`%APPDATA%\Avamar\`

Protokollspeicherorte auf Linux- und Mac-Computern

Auf Linux- und Mac-Computern stehen die Protokolle über die Pfade in der folgenden Tabelle zur Verfügung.

Tabelle 119 Pfade zu Protokollen auf Linux- und Mac-Computern

Protokoll	Pfad
Arbeitsauftrag	`/usr/local/avamar/clientlogs`
Agent	`/var/avamar/`
Konsole	Linux: `$HOME/` Mac: `$HOME/.avamardata/`

KAPITEL 15

Data Domain-Systemintegration

In diesem Kapitel werden folgende Themen behandelt:

Überblick über die Data Domain-Systemintegration

Es ist möglich, Avamar-Backups auf einem oder mehreren Data Domain-Systemen zu speichern und anschließend eine nahtlose Wiederherstellung der Daten aus diesen Backups durchzuführen.

Sie können Dateisystem- und Anwendungsdaten auf einem Data Domain-System sichern. Die Speicherung von Avamar-Backups auf einem Data Domain-System wird für Umgebungen mit großen Datenbanken und einer hohen Änderungsrate empfohlen. Speichern Sie die folgenden Typen von Backups stattdessen auf dem Avamar-Server:

- Backups von Dateisystemen
- Backups von virtuellen Maschinen
- Backups von Remotestandorten
- Backups von Datenbanken mit niedrigen Änderungsraten

Beim Speichern von VMware-Image-Backups auf einem Data Domain-System können Sie eine verloren gegangene oder beschädigte virtuelle Maschine über die Funktion für den Sofortzugriff praktisch unmittelbar aus dem Backup starten.

Sie können auch Avamar-Prüfpunkte für einen Single-Node-Server oder Avamar Virtual Edition- (AVE-)Server auf einem Data Domain-System speichern.

Integration von Avamar in Data Domain

DD OS-Software führt die Deduplizierung von Daten auf einem Data Domain-System durch. Die Data Domain Boost- (DD Boost-)Bibliothek stellt eine Schnittstelle für ein Avamar-System zur Verfügung, um auf der Quelle deduplizierte Daten an ein Data Domain-System zu senden.

Avamar verwendet die DD Boost-Bibliothek über eine API-basierte Integration, um auf Verzeichnisse, Dateien und sonstige Elemente im Data Domain-Dateisystem zuzugreifen und mit ihnen zu arbeiten. Durch die DD Boost-API erhält ein Avamar-System eine Schnittstelle zu einigen Eigenschaften und Funktionen des Data Domain-Systems. Diese Schnittstelle bietet einem Avamar-System die Möglichkeit, die in Data Domain-Systemen gespeicherten Backup-Images zu steuern. Avamar wird außerdem in die Lage versetzt, Wartungsaktivitäten zu managen und die Replikation auf Data Domain-Remotesysteme zu steuern.

DD Boost ist auf den Backupclients und dem Avamar-Utility-Node oder einem Avamar-Single-Node-System installiert. DD Boost wird automatisch bei der Installation der Avamar-Client- oder -Serversoftware installiert.

Sie können festlegen, ob bestimmte Backup-Datasets auf einem Avamar-Server oder einem Data Domain-System gespeichert werden.

Bei Auswahl eines Avamar-Servers als Backupziel führt der Avamar-Client auf den einzelnen Hosts eine Verarbeitung der Deduplizierungssegmente durch. Der Avamar-Client sendet die Backupdaten und die zugehörigen Metadaten an den Avamar-Server.

Wenn Sie ein Data Domain-System als Backupziel auswählen, werden die Backupdaten an das Data Domain-System übertragen. Gleichzeitig sendet der Avamar-Client die zugehörigen Metadaten zur Speicherung an den Avamar-Server. Durch die Metadaten kann das Avamar-Managementsystem Wiederherstellungsvorgänge direkt vom Data Domain-System aus durchführen, ohne zunächst die wiederhergestellten Daten auf dem Avamar-System bereitzustellen.

Der Prozess der Datenwiederherstellung ist für den Backupadministrator transparent. Der Backupadministrator nutzt die gleichen Avamar-Recovery-Prozesse, die für aktuelle Avamar-Implementierungen nativ sind.

Dateisystembackups in einem Data Domain-System

Avamar unterstützt Data Domain-Systemspeicher der Dateisystembackups für die folgenden Betriebssysteme:

- Windows und Windows-Server
- IBM AIX
- HP-UX (nur IA-64, erfordert ONCPlus-Bibliotheksversion 11.31.06 oder höher)
- Solaris (für Solaris 10 auf SPARC ist die clientseitige Deduplizierung deaktiviert und die Deduplizierung wird auf dem Data Domain-System durchgeführt)
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)
- Mac 10.8, 10.9 und 10.10

Nur 64-Bit-Betriebssysteme werden unterstützt. Die *Avamar Kompatibilitäts- und Interoperabilitätsmatrix* auf http://compatibilityguide.emc.com:8080/CompGuideApp enthält aktualisierte Clientkompatibilitätsinformationen, einschließlich einer kompletten Liste von unterstützten Betriebssystemversionen und Service Packs.

Anwendungsbackups auf einem Data Domain-System

Sie können die Backups der Anwendungsdaten von einer der folgenden Avamar-Plug-ins auf einem Data Domain-System speichern:

- Avamar-Plug-in für DB2
- Avamar-Plug-in für Exchange VSS
- Avamar-Plug-in für Hyper-V VSS
- Avamar-Plug-in für Lotus Domino
- Avamar-Plug-in für Oracle
- Avamar-Plug-in für SAP mit Oracle
- Avamar-Plug-in für SharePoint VSS
- Avamar-Plug-in für Sybase ASE
- Avamar-Plug-in für SQL Server

Außerdem können Sie VMware-Image-Backups und Backups mit dem Avamar NDMP Accelerator auf einem Data Domain-System speichern.

Data Domain Cloud Disaster Recovery

Die Data Domain Cloud Disaster Recovery- (Cloud DR-)Lösung vereinfacht die Disaster Recovery für virtuelle Maschinen vor Ort durch Bereitstellung der Möglichkeit zur Wiederherstellung von VMs in der Cloud.

Cloud DR verwendet Avamar-Software vor Ort und Data Domain-Speicher vor Ort zum Replizieren von Backups von Daten auf virtuellen Maschinen in die Public Cloud und zum Durchführen einer Disaster Recovery von Produktionsumgebungen durch das Wiederherstellen der vollständigen VM als eine Instanz der Amazon Web Services Elastic Compute Cloud (EC2).

Im *Avamar und Data Domain-System – Integrationshandbuch* finden Sie weitere Informationen zur Verwendung von Avamar mit Data Domain Cloud Disaster Recovery.

VMware-Sofortzugriff

Beim Speichern von VMware-Image-Backups auf einem Data Domain-System können Sie verloren gegangene oder beschädigte virtuelle Maschinen über die Funktion für den Sofortzugriff aus dem Backup starten.

Beim Sofortzugriff wird ein VM-Image-Backup in einer temporären NFS-Share auf dem Data Domain-System bereitgestellt. Danach können Sie die virtuelle Maschine mit vSphere Client einschalten und einen vMotion-Vorgang der virtuellen Maschine auf einen Datenspeicher im vCenter initiieren. Wenn der vMotion-Vorgang abgeschlossen ist, sind die wiederhergestellten Dateien der virtuellen Maschine nicht mehr auf dem Data Domain-System vorhanden. Danach können Sie die NFS-Share auf dem Data Domain-System mithilfe von Avamar Administrator löschen.

Hinweis

Wenn Sie den Sofortzugriff verwenden, führen Sie die virtuelle Maschine nicht über längere Zeiträume auf dem Data Domain-System hinweg aus. Wenn die virtuelle Maschine auf dem Data Domain-System ausgeführt wird, wird die Performance möglicherweise aufgrund des Workflows beeinträchtigt.

Sie können eine virtuelle Maschine auch in der Produktionsumgebung statt über den Sofortzugriff wiederherstellen. Die Avamar-Software nutzt Changed Block Tracking (CBT), um den Recovery-Prozess erheblich zu beschleunigen.

Im *Avamar for VMware – Benutzerhandbuch* erfahren Sie weitere Details zum Sofortzugriff und zur Wiederherstellung von Image-Backups.

Cloud-Tiering

Wenn Sie Avamar-Backupdaten auf einem Data Domain-System speichern, können Sie die Backups auch für Cloud-Tiering konfigurieren.

Die Unterstützung für Data Domain Cloud Tier wurde mit Avamar 7.4 initiiert. DD Cloud Tier verschiebt Daten von einer Data Domain in die Cloud. Sie können über Avamar-Administrator Cloud-Tiering konfigurieren, um Avamar-Backups von der Data Domain in die Cloud zu verschieben und eine nahtlose Recovery dieser Backups durchzuführen.

Die Unterstützung für Data Domain Cloud Tier Disaster Recovery wurde mit Avamar 7.5 initiiert. Sie können Backups aus der Cloud im Falle des Ausfalls eines Data Domain-Systems wiederherstellen und auch einen Avamar-Server aus der Cloud wiederherstellen.

Im *Avamar und Data Domain-System – Integrationshandbuch* finden Sie weitere Informationen zum Cloud-Tiering mit Data Domain.

Kontrollpunkte auf einem Data Domain-System

Sie können Avamar-Prüfpunkte für einen Single-Node-Server oder Avamar Virtual Edition- (AVE-)Server auf einem Data Domain-System mit DD OS 5.3 oder höher speichern. Bei Prüfpunkten handelt es sich um systemweite Backups des Avamar-Servers, die zum Zweck der Disaster Recovery erstellt werden.

Die Speicherung von Prüfpunkten auf einem Data Domain-System wird für Umgebungen empfohlen, die nicht die folgenden Optionen umfassen:

- Replikation an einen sekundären Avamar-Server
- Umgebungen, in denen Mehrheit der Clientbackups auf einem Data Domain-System gespeichert sind

Um die Speicherung von Prüfpunkten auf einem Data Domain-System zu konfigurieren, aktivieren Sie beim Hinzufügen oder Bearbeiten des Data Domain-Systems in Avamar Administrator das Kontrollkästchen **Use as target for Avamar Checkpoint Backups**.

Setzen Sie sich mit Mitarbeitern der Avamar Professional Services in Verbindung, um Unterstützung beim Rollback des Avamar-Servers auf einen Prüfpunkt auf einem Data Domain-System zu erhalten.

Data Domain-Systemstreams

Jedes Data Domain-System hat einen weichen Grenzwert für die maximale Anzahl von Verbindungs- und Datenstreams, die bei unveränderter Performance gleichzeitig unterhalten werden können. Die Anzahl der Streams hängt vom jeweiligen Data Domain-Systemmodell ab.

Konfigurieren Sie können die maximale Anzahl der von Avamar verwendbaren Streams, wenn Sie dem Avamar-Server ein Data Domain-System hinzufügen. Der Avamar-Server nutzt den Backupstreamwert, um die Anzahl gleichzeitiger Backup- bzw. Wiederherstellungsjobs zu begrenzen.

Wenn das Data Domain-System vollständig gegenüber dem Avamar-Server dediziert ist, handelt es sich bei dem in Avamar Administrator eingegebenen Streamwert möglicherweise um die maximale Anzahl der vom Data Domain-Systemmodell unterstützten Streams. Wenn das Data Domain-System gemeinsam mit anderen Drittanbieteranwendungen oder einem anderen Avamar-Server genutzt wird, sollte eine Teilmenge der Streamanzahl zugewiesen werden.

Jeder Avamar-Backupclient, der Multistreambackups unterstützt, kann zur Verwendung der korrekten Streamanzahl (normalerweise basierend auf der Anzahl der Datenbanken) konfiguriert werden. Dieser Schritt erfolgt per Multistreaming-Konfiguration, wenn der Avamar-Backupjob konfiguriert wird. Die Streams werden bei Abschluss des Backup- oder Wiederherstellungsvorgangs freigegeben. Die Anzahl der zugewiesenen Streams sollte von der Anzahl und dem Typ der Avamar-Clients abhängig sein, die Daten zum etwa selben Zeitpunkt sichern.

Replikation mit Data Domain-Systemen

Wenn ein Avamar-System Backups auf einem Data Domain-System speichert, verwendet die Avamar-Replikation DD Boost zum Kopieren von Backups vom ursprünglichen Data Domain-System und zum Erstellen von Replikaten auf einem anderen Data Domain-System.

Unterstützte Replikationskonfigurationen

In der folgenden Tabelle sind die unterstützten Replikationskonfigurationen für die Avamar-Replikation mit DD Boost aufgeführt.

Tabelle 120 Replikationskonfigurationen für die Avamar-Replikation mit DD Boost

Backupspeicher	Replikationsspeicher
Einzelnes Data Domain-System	Einzelnes Data Domain-System
Einzelnes Data Domain-System	Mehrere Data Domain-Systeme
Mehrere Data Domain-Systeme	Einzelnes Data Domain-System

Tabelle 120 Replikationskonfigurationen für die Avamar-Replikation mit DD Boost (Fortsetzung)

Backupspeicher	Replikationsspeicher
Mehrere Data Domain-Systeme	Mehrere Data Domain-Systeme

In einer Konfiguration, in der der Replikationsspeicher aus mehreren Data Domain-Systemen besteht, können Sie das System steuern, das die Replikate erhält, indem Sie eine Domain auf dem Avamar-Quellserver einem Data Domain-Zielsystem zuordnen. Legen Sie das Data Domain-System mit dem Standardziel fest. Avamar führt die Replikation zum Standardziel durch, wenn kein Data Domain-Zielsystem auf der Registerkarte **Storage Mapping** des Fensters **Data Movement Policy** in Avamar-Administrator angegeben ist.

Im *Avamar und Data Domain-System – Integrationshandbuch* erhalten Sie Anweisungen zur Speicherzuordnung und zum Angeben des standardmäßigen Data Domain-Zielsystems.

Replikationsdetails

Die folgenden Details gelten für die Avamar-Replikation mit Data Domain-Systemen:

- Die Datenübertragung während der Replikation erfolgt zwischen den Data Domain-Systemen, ohne zwischengeschaltete Bereitstellung.
- Bei der Replikation wird DD Boost zum Kopieren von Backups und zum Schreiben von Replikaten verwendet.
- Eine Data Domain-Replikationslizenz ist erforderlich.
- Keine Verwendung der Data Domain-Replikation.
- Die Replikation wird auf dem Avamar-Server konfiguriert und überwacht.
- Bei der Planung von Replikationsaufgaben wird nur die Avamar-Replikationsplanung verwendet.
- Es werden keine Data Domain-Administrationstools verwendet.

Monitoring und Reporting des Data Domain-Systemstatus

Avamar kann mithilfe von Simple Network Management Protocol (SNMP) Daten für die Integritätsüberwachung, Systemwarnmeldungen und Kapazitätsberichte auf einem Data Domain-System sammeln und anzeigen.

SNMP ermöglicht es, die Data Domain-Aktivitäten, -Ereignisse, -Kapazität und -Systemstatus auf dieselbe Weise zu überwachen wie die Aktivitäten, Ereignisse, Kapazität und den Systemstatus für den Avamar-Server. Konfigurieren Sie SNMP-Einstellungen, wenn Sie der Avamar-Konfiguration ein Data Domain-System hinzufügen.

Im *Avamar-Berichte – Handbuch* finden Sie weitere Informationen über die Erstellung von Berichten. Um das System zu analysieren, führen Sie die Berichte aus.

Im *Avamar und Data Domain-System – Integrationshandbuch* finden Sie weitere Informationen über die Überwachung des Systemstatus für ein Data Domain-System.

Sicherheit durch Data Domain-Systemintegration

In den folgenden Abschnitten werden Details zum Thema Sicherheit bei Verschlüsselung und Benutzerzugriff in einer Avamar-Umgebung mit Data Domain beschrieben.

Verschlüsselung

Die DD Boost-Bibliothek unterstützt die Datenverschlüsselung zwischen dem Avamar-Client und dem Data Domain-System für DD OS 5.5 oder neuer. Die DD Boost-

Bibliothek unterstützt nicht die Datenverschlüsselung zwischen dem Avamar-Client und dem Data Domain-System für DD OS 5.4.

Backups vom Avamar-Client auf den Avamar-Server sind immer komprimiert und verschlüsselt.

Benutzerzugriff
Seien Sie vorsichtig, wenn Sie Benutzern Zugriff auf das Data Domain-System gewähren. Autorisieren Sie einen Benutzer niemals für den Zugriff auf das Data Domain-System und das manuelle Löschen der Daten.

Datenmigration auf ein angebundenes Data Domain-System

Backupdaten können nicht direkt vom Avamar-Server auf ein angebundenes Data Domain-System migriert werden.

Um für einen Avamar-Client statt des Avamar-Servers das Data Domain-System als Backupziel zu verwenden, bearbeiten Sie das Dataset so, dass das Data Domain-System verwendet wird. Starten Sie die Durchführung von Backups auf das Data Domain-System. Wenn das Backupziel auf das Data Domain-System geändert wird, ist die Durchführung eines kompletten Backups erforderlich.

Im Anschluss an ein erfolgreiches Backup auf das Data Domain-System können vorherige Backups vom Avamar-Server gelöscht werden.

Vorbereiten auf Hinzufügen eines Data Domain-System

Bevor Sie der Avamar-Konfiguration ein Data Domain-System hinzufügen, installieren und konfigurieren Sie sowohl den Avamar-Server als auch das Data Domain-System. Achten Sie darauf, dass die Umgebung die Systemanforderungen erfüllt, und erstellen Sie ein DD Boost-Benutzerkonto auf dem Data Domain-System.

Systemanforderungen für eine Data Domain-Systemintegration

Vergewissern Sie sich, dass die Umgebung die erforderlichen Systemanforderungen erfüllt, bevor Sie der Avamar-Konfiguration ein Data Domain-System hinzufügen.

In der folgenden Tabelle sind die Anforderungen für das Data Domain-System aufgeführt.

Tabelle 121 Data Domain-Systemanforderungen

Merkmal oder Spezifikation	Anforderung zur Verwendung mit Avamar
Data Domain Operating System (DD OS)	DD OS 5.3 oder höher
DD Boost	DD Boost 2.6 oder höher

Tabelle 121 Data Domain-Systemanforderungen (Fortsetzung)

Merkmal oder Spezifikation	Anforderung zur Verwendung mit Avamar
	Hinweis Die DD Boost-Software ermöglicht Backupservern die Kommunikation mit Speichersystemen, ohne dass Data Domain-Systeme hierzu eine Bandemulation durchführen müssen. DD Boost umfasst zwei Komponenten: eine Komponente, die auf dem Backupserver ausgeführt wird, und eine Komponente, die auf dem Data Domain-System ausgeführt wird. Im Kontext von Avamar ist die Komponente, die auf dem Backupserver (DD Boost-Bibliotheken) ausgeführt wird, im Avamar-Client integriert. Die DD Boost-Software ist ein optionales Produkt, für das eine Lizenz erforderlich ist, damit es auf dem Data Domain-System betrieben werden kann.
Data Domain-Gerätetyp	Avamar bietet Unterstützung für alle Data Domain-Systeme, die die Ausführung der erforderlichen DD OS-Version unterstützen.
Data Domain-Dateisystem	Aktivieren Sie das Data Domain-Dateisystem (Data Domain File System, DDFS) entweder über Data Domain System Manager oder die Befehlszeilenoberfläche. Nachdem Sie die Dateisystemvorgänge aktiviert haben, kann es bis zu 10 Minuten dauern, bis Avamar Administrator den Status des Data Domain-Systems korrekt wiedergibt. Die Verzögerung wird geringfügig ausgedehnt, wenn das Data Domain-System die Option „DD Extended Retention“ verwendet. Führen Sie keine Backups, Wiederherstellungen oder Systemwartungsvorgänge durch, bevor der Status in Avamar Administrator korrekt angezeigt wird. Andernfalls schlagen Backups, Wiederherstellungen oder Systemwartungsvorgänge ggf. fehl.
DD Boost	Aktivieren Sie DD Boost auf dem Data Domain-System. Beim Aktivieren von DD Boost wird DD Boost zur bevorzugten Verbindungsmethode für DD Boost-aktivierte Clients. Diese Methode ist zwar für Clients, die DD Boost-Funktionen nutzen können, akzeptabel, sie kann jedoch auch eine Performanceverschlechterung anderer Clients bedeuten. Angemessene Sorgfalt und eine effektive Datensammlung sind der Schlüssel

Tabelle 121 Data Domain-Systemanforderungen (Fortsetzung)

Merkmal oder Spezifikation	Anforderung zur Verwendung mit Avamar
	zur Vermeidung solcher Interaktionen. Dies gilt insbesondere während der Durchführung von Upgrades.
DD Boost-Benutzerkonto	Die DD Boost-Bibliothek nutzt einen eindeutigen Anmeldekontonamen, der auf dem Data Domain-System erstellt wurde. Dieser Kontoname ist als das DD Boost-Konto bekannt. Pro Data Domain-System existiert nur ein DD Boost-Konto. Wenn das Konto umbenannt und/oder das Passwort geändert wird, müssen diese Änderungen sofort durch Bearbeitung der Data Domain-Konfigurationsoptionen im Avamar-System aktualisiert werden. Bleibt eine Aktualisierung der DD Boost-Kontoinformationen aus, kann dies zu Integritätsprüfungsfehlern oder Backup- und Wiederherstellungsproblemen führen. Das DD Boost-Konto muss über Administratorrechte verfügen.

Kapazitätsanforderungen

Bewerten Sie Backupspeicheranforderungen sorgfältig, wenn Sie die Menge der auf dem Data Domain-System und dem Avamar-Server zu speichernden Daten berechnen. Fügen Sie Schätzungen von Daten hinzu, die von anderen Servern an das Data Domain-System gesendet werden.

Wenn das Data Domain-System seine maximale Speicherkapazität erreicht, sind auf das Data Domain-System so lange keine weiteren Backups möglich, bis zusätzliche Kapazität hinzugefügt wurde bzw. bis alte Backups gelöscht wurden.

Anforderungen bei Verwendung anderer Backupprodukte

Data Domain-Systeme können Backup- und Archivierungssoftware von Drittanbietern verwenden. Der Avamar-Server geht nicht davon aus, dass er die alleinigen Eigentumsrechte am Data Domain-System besitzt. Achten Sie auf eine angemessene Dimensionierung, wenn das System zusammen mit anderen Softwareprodukten verwendet wird.

Der Avamar-Server verwendet nicht die nativen Snapshot- und Replikationsfunktionen des Data Domain-Systems. Die Replikation erfolgt über die DD Boost-SDK-Bibliothek anhand von Kopier- und Cloningvorgängen. Allerdings greifen andere Produkte von Drittanbietern möglicherweise auf die nativen Snapshot- und Replikationsfunktionen des Data Domain-Systems zurück. In diesem Fall umfasst ein Snapshot des gesamten Data Domain-Systems oder eine Replikation eines gesamten Data Domain-Systems die Avamar-Daten.

Netzwerkanforderungen

Der Avamar-Server und alle Data Domain-Systeme müssen sich im selben lokalen Netzwerk befinden. Verbinden Sie den Avamar-Server und Data Domain-Systeme

nicht über ein WAN (Wide Area Network). Konfigurationen, die auf ein WAN zurückgreifen, werden nicht unterstützt.

Sie können die Avamar-Replikation über ein WAN nutzen, um Daten von Avamar-Quellservern und Data Domain-Quellsystemen auf Avamar-Zielserver und Data Domain-Zielsysteme zu replizieren.

Vergewissern Sie sich vor der Integration eines Data Domain-Systems in einen Avamar-Server davon, dass die verfügbare Netzwerkbandbreite ausreichend ist. Stellen Sie sicher, dass die Netzwerkinfrastruktur mehr Bandbreite bereitstellt als die für den maximalen Durchsatz des Data Domain-Systems geforderte Bandbreite. Dieser Schritt dient dazu, den maximal verfügbaren Durchsatz auf einem Data Domain-System (für Wiederherstellungen, Backups auf Ebene 0 und nachfolgende inkrementelle Backups nach einem Backup auf Ebene 0) zu erhalten.

Die Netzwerkkonfiguration muss außerdem die folgenden Anforderungen erfüllen:

- Weisen Sie jedem Data Domain-System einen vollständig qualifizierten Domainnamen (Fully Qualified Domain Name, FQDN) zu.
- Verwenden Sie bei der Registrierung eines Data Domain-Systems keine IP-Adressen anstelle von Hostnamen. Diese Aktion kann die Möglichkeit einschränken, optimierten Duplizierungsverkehr exklusiv über eine registrierte Schnittstelle weiterzuleiten.
- Vergewissern Sie sich, dass DNS auf dem Data Domain-System korrekt konfiguriert ist.
- Vergewissern Sie sich, dass die DNS-Vorwärts- und Rückwärtssuche (Forward und Reverse Lookup) zwischen dem Avamar-Server, dem Data Domain-System sowie allen Backup- und Wiederherstellungsclients funktioniert.
- Verwenden Sie Hostdateien, um Hostnamen in nicht routbare IP-Adressen aufzulösen.
- Erstellen Sie keine sekundären Hostnamen zum Verknüpfen mit alternativen oder lokalen IP-Schnittstellen.

Anforderungen von NTP

Der Avamar-Server, das Data Domain-System und alle AvamarClients müssen denselben Network Time Protocol- (NTP-)Server verwenden.

Anforderungen an die Portverwendung und Firewalls

Um die Kommunikation zwischen Avamar und den Data Domain-Systemen zu ermöglichen, lesen und implementieren Sie die in den folgenden Dokumenten genannten Anforderungen an die Portverwendung und Firewalls. Diese sind beim Avamar-Support verfügbar:

- *Avamar – Produktsicherheitshandbuch*
- *Port-Anforderungen für den Zugriff auf Data Domain-Systeme über eine Firewall (Technischer Hinweis)*

Erstellen eines DD Boost-Benutzerkontos

Bevor der Avamar-Konfiguration ein Data Domain-System hinzugefügt werden kann, muss das Data Domain-System vorbereitet werden, indem DD Boost aktiviert und ein DD Boost-Benutzerkonto für den Avamar-Server erstellt wird. Diese Aktion wird ausgeführt, um auf das Data Domain-System für Backups und Wiederherstellungen (und Replikation, falls zutreffend) zuzugreifen.

Denken Sie bei einer Änderung des DD Boost-Kontonamens oder -Passworts nach der Kontoerstellung daran, die Data Domain-Systemkonfiguration in Avamar Administrator

zu bearbeiten. Anderenfalls schlagen alle Backups, Wiederherstellungen und Wartungsaktivitäten fehl.

Vorgehensweise

1. Deaktivieren Sie DD Boost auf dem Data Domain-System, indem Sie sich bei der Data Domain-Befehlszeilenoberfläche als Administrator anmelden und den folgenden Befehl eingeben:

   ```
   ddboost disable
   ```

2. Erstellen Sie das DD Boost-Benutzerkonto mit Administratorberechtigungen, indem Sie den folgenden Befehl eingeben:

   ```
   user add username role admin
   ```

   Dabei steht *username* für den Benutzernamen des neuen Kontos.

3. Legen Sie das neue Konto als DD Boost-Benutzer fest, indem Sie den folgenden Befehl eingeben:

   ```
   ddboost set user-name username
   ```

   Dabei steht *username* für den Benutzernamen des Kontos.

4. Geben Sie den folgenden Befehl ein, damit DD Boost die Änderungen zulässt:

   ```
   ddboost enable
   ```

Hinzufügen eines Data Domain-Systems

Vorgehensweise

1. Klicken Sie in Avamar Administrator auf **Server**Link zum Startprogramm.

   Das Fenster **Server** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Server Management**.
3. Wählen Sie **Actions** > **Add Data Domain System** aus.

   Das Dialogfeld **Add Data Domain System** wird angezeigt.

4. Geben Sie auf der Registerkarte **System** die Data Domain-Systeminformationen an:

   a. Geben Sie in das Feld **Data Domain System Name** den vollständig qualifizierten Domainnamen des Data Domain-Systems ein.

   Hinweis

   Verwenden Sie keine IP-Adresse bzw. keinen sekundären Hostnamen, die bzw. der mit alternativen oder lokalen IP-Schnittstellen verbunden ist. Dies kann die Fähigkeit von Avamar zur Weiterleitung optimierten Deduplizierungsdatenverkehrs einschränken.

   b. Geben Sie in das Feld **DDBoost User Name** den Benutzernamen des DD Boost-Kontos für Avamar ein, mit dem zwecks Backup-, Wiederherstellungs- und Replikationsvorgängen auf das Data Domain-System zugegriffen werden soll.

   c. Geben Sie in das Feld **Password** das Passwort für das Konto ein, das Avamar für den Zugriff auf das Data Domain-System zwecks Backup-, Wiederherstellungs- und Replikationsvorgängen verwendet.

d. Wiederholen Sie Ihre Eingabe im Feld **Verify Password**, um das Passwort zu bestätigen.

e. Falls mehr als ein Data Domain-System mit Avamar verbunden ist, können Sie ein Data Domain-System festlegen, das als Standardreplikationsspeicher dienen soll. Wählen Sie **Use system as default replication storage** aus, falls es sich bei diesem System um den Standardreplikationsspeicher handelt.

f. Um Prüfpunkte für einen Avamar-Single-Node-Server oder Avamar Virtual Edition- (AVE-)Server auf dem Data Domain-System und nicht auf dem Avamar-Server zu speichern, aktivieren Sie das Kontrollkästchen **Use as target for Avamar Checkpoint Backups**.

g. Klicken Sie auf **Verify**, um die maximale Anzahl der vom Data Domain-System unterstützten Streams anzuzeigen.

h. Legen Sie die maximale Anzahl an Streams fest, die Avamar zu einem bestimmten Zeitpunkt zur Durchführung von Backups und Wiederherstellungen verwenden kann:

- Um eine definierte Streamanzahl festzulegen, geben Sie die entsprechende Anzahl im Feld **Max used by Avamar** ein.
- So geben Sie die maximale Anzahl von Streams an, die auf dem Prozentsatz der Gesamtanzahl der unterstützten Streams basieren:
  a. Geben Sie den Prozentsatz in das Feld **Max used by Avamar** ein.
  b. Wählen Sie die das Kontrollkästchen **As percentage of the max limit** aus.

Berücksichtigen Sie sowohl die maximale Anzahl der vom Data Domain-System unterstützten Streams sowie das Vorhandensein etwaiger anderer Anwendungen, die mithilfe von Streams Daten an das Data Domain-System senden bzw. von dort empfangen.

Wenn beim Schreiben bzw. Lesen vom Data Domain-System sämtliche verfügbaren Streams verwendet werden, werden Backup- oder Wiederherstellungsanforderungen so lange von Avamar in die Warteschlange gestellt, bis ein oder mehrere Streams verfügbar werden.

5. Zum Konfigurieren von SNMP klicken Sie auf die Registerkarte **SNMP**.

   Die SNMP-Konfiguration ermöglicht Avamar, Daten zur Überwachung der Systemintegrität, zu Systemwarnmeldungen sowie zu Kapazitätsberichten zu sammeln und anzuzeigen.

6. Überprüfen Sie die SNMP-Konfiguration:

   - Im Feld **Getter/Setter Port Number** wird der Port auf dem Data Domain-System aufgeführt, über den SNMP-Objekte empfangen bzw. festgelegt werden. Der Standardwert ist 161.
   - Im Feld **SNMP Community String** wird der von Avamar für schreibgeschützten Zugriff auf das Data Domain-System verwendete Community-String aufgeführt.
   - Im Feld **Trap Port Number** wird der Trap-Port auf dem Avamar-Server aufgeführt. Der Standardwert ist 163.

7. Um die Cloud-Tiering-Funktion zu konfigurieren, klicken Sie auf die Registerkarte **Tiering**.

   Avamar-Software verwendet Cloud-Tiering, um Avamar-Backupdaten von einem Data Domain-System in die Cloud zu verschieben.

8. Klicken Sie auf **OK**.

   Eine Fortschrittsmeldung wird angezeigt.

9. Klicken Sie nach Abschluss des Vorgangs auf **Close**.

Ergebnisse

Wenn der Avamar-Konfiguration ein Data Domain-System hinzugefügt wird, erstellt Avamar für den Avamar-Server ein MTree-Verzeichnis auf dem Data Domain-System. „Mtree“ bezieht sich auf das innerhalb des DD Boost-Pfads erstellte Verzeichnis. Data Domain-Systeme unterstützen maximal 100 Mtree-Verzeichnisse. Nach dem Erreichen dieses Grenzwerts ist es nicht mehr möglich, der Avamar-Konfiguration das Data Domain-System hinzuzufügen.

ANHANG A

Befehlsshell-Serveranmeldungen

In diesem Anhang werden folgende Themen behandelt:

Benutzerkonten

Die folgenden Benutzerkonten werden häufig für Systemadministrations- und -wartungsaufgaben verwendet:

- root
- admin

Das Benutzerkonto „admin“ erfordert eine Authentifizierung über Secure Shell (SSH).

Starten von Befehlsshellsitzungen

Melden Sie sich über SSH als Administratorbenutzer am Avamar-Server oder am Utility-Node an. Diese Aktion wird für Wartungsaufgaben und die Konfiguration des Avamar-Systems ausgeführt.

Bevor Sie beginnen

Hinweis

Kryptografische Änderungen in Avamar 7.5.1 erfordern die Verwendung von PuTTY 0.7 oder höher und WinSCP 5.11.1 (Build 7725) oder höher.

Vorgehensweise

- Um eine Befehlsshellsitzung auf einem Single-Node-Server zu starten, öffnen Sie eine Befehlsshell und melden Sie sich beim Server als „admin“ an.
- So starten Sie eine Befehlsshellsitzung auf einem Multi-Node-Server:
  a. Öffnen Sie eine Befehlsshell und melden Sie sich beim Utility-Node als „admin“ an.
  b. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie die folgenden Befehle eingeben:

     ```
     ssh-agent bashssh-add ~admin/.ssh/admin_key
     ```

  c. Wenn Sie nach der `admin_key`-Passphrase gefragt werden, geben Sie sie ein und drücken Sie die **Enter**.

Wechseln zwischen Benutzer-IDs

Sie können den Benutzer einer Befehlsshellsitzung durch Eingabe von **`su`** zu „root“ wechseln und durch Eingabe von **`exit`** zur vorherigen Anmelde-ID zurückkehren. Wenn Sie während einer Befehlsshellsitzung zum Benutzer „admin“ wechseln, müssen Sie auch den admin-OpenSSH-Schlüssel laden.

Vorgehensweise

1. Wechseln Sie zum Benutzerkonto „admin“ und zur Anmeldeshell, indem Sie **`su - admin`** eingeben.
2. Wenn Sie nach dem Passwort gefragt werden, geben Sie das admin-Passwort ein und drücken Sie die **Enter**.
3. Laden Sie den admin-OpenSSH-Schlüssel, indem Sie Folgendes eingeben:

   ```
   ssh-agent bashssh-add ~admin/.ssh/admin_key
   ```

Hinweis

Um das aktive Benutzerkonto (Benutzer-ID) einer Shell-Sitzung zu bestimmen, geben Sie **whoami** ein.

Verwenden von sudo

In Avamar Data Stores ab der 4. Generation werden admin-Benutzerkonten automatisch der sudoers-Datei hinzugefügt. Dadurch können Administratorbenutzer eine begrenzte Zahl an Befehlen ausführen, die anderweitig eine Betriebssystem-Root-Berechtigung erfordern würden.

Hinzufügen des sudo-Präfixes zu Befehlen

Statt den Benutzer mithilfe des Befehls su zu „root“ zu ändern, können admin-Benutzer Befehle direkt ausgeben, die Root-Berechtigungen erfordern. Hierzu muss jedem Befehl das Präfix sudo hinzugefügt werden.

Mit dem folgenden Befehl wird beispielsweise MyPackage.rpm installiert:

```
sudo rpm -ivh MyPackage.rpm
```

Wenn Sie nach dem Passwort gefragt werden, geben Sie es ein und drücken die **Enter**.

Sie werden ggf. regelmäßig zur erneuten Eingabe des admin-Passworts aufgefordert, wenn Sie anderen Befehlen das Präfix sudo hinzufügen.

ANHANG B

Plug-in-Optionen

In diesem Anhang werden folgende Themen behandelt:

Festlegen von Plug-in-Optionen

Mit Plug-in-Optionen können Sie bestimmte Aktionen für On-Demand-Backups, Wiederherstellungen und geplante Backups steuern. Welche Plug-in-Optionen verfügbar sind, hängt vom Vorgangstyp und vom Plug-in-Typ ab.

Legen Sie in Avamar Administrator Plug-in-Optionen für On-Demand-Backup- und Wiederherstellungsvorgänge oder zur Erstellung eines Dataset für ein geplantes Backup fest. Plug-in-Optionen werden über die Steuerelemente (Textfelder, Kontrollkästchen, Optionsfelder usw.) der grafischen Benutzeroberfläche (GUI) festgelegt. Geben Sie eine Option und den zugehörigen Wert in die Felder **Enter Attribute** und **Enter Attribute Value** ein.

HINWEIS

Die Avamar-Software prüft oder validiert die von Ihnen in die Felder **Enter Attribute** und **Enter Attribute Value** eingegebenen Informationen nicht. Die Werte in den Feldern **Enter Attribute** und **Enter Attribute Value** setzen Einstellungen außer Kraft, die Sie mithilfe der GUI-Steuerelemente für die Optionen festlegen.

Backup-Optionen

Die angezeigten Backupoptionen hängen vom Plug-in-Typ ab.

Im folgenden Abschnitt werden die Backupoptionen für die folgenden Plug-ins beschrieben:

- AIX-Dateisystem
- FreeBSD-Dateisystem
- HP-UX-Dateisystem
- Linux-Dateisystem
- Macintosh-Dateisystem
- NetWare-Dateisystem
- SCO OpenServer-Dateisystem

Backupoptionen für das Avamar-Plug-in für Microsoft Windows sind im *Avamar for Windows-Server – Benutzerhandbuch* verfügbar. Backupoptionen für Anwendungs-Plug-ins wie SQL Server und SharePoint VSS sind im Benutzerhandbuch zum jeweiligen Plug-in verfügbar.

In den folgenden Tabellen werden die Optionen beschrieben, die verfügbar sind, wenn Sie ein On-Demand Backup durchführen oder wenn Sie für aufgeführte Dateisystem-Plug-ins ein Dataset für geplante Backups konfigurieren.

Tabelle 122 Backup-Plug-in-Optionen

Option	Beschreibung
Store backup on Data Domain system	(Nur AIX, HP-UX, Linux und Macintosh) Speichert das Backup auf einem konfigurierten Data Domain-System statt auf dem Avamar-Server. Um das Backup auf einem Data Domain-System zu speichern,

Tabelle 122 Backup-Plug-in-Optionen (Fortsetzung)

Option	Beschreibung
	aktivieren Sie das Kontrollkästchen und wählen Sie dann das Data Domain-System aus der Liste aus.
Verschlüsselungsmethode für das Data Domain-System	(Nur AIX, HP-UX, Linux und Macintosh) Legt die Verschlüsselungsmethode für Datenübertragungen zwischen dem Client und dem Data Domain-System fest.
Backup-Bezeichnung	Weist dem Backup diese beschreibende Bezeichnung zu.

Tabelle 123 Backup-Plug-in-Optionen für SMS-Authentifizierung (nur NetWare)

Option	Beschreibung
Server login ID	(Nur NetWare) Legt den Benutzernamen für die SMS-Anmeldung fest, zum Beispiel CN=admin.O=HOSTNAME_CTX.
Server password	(Nur NetWare) Legt das Passwort für den Benutzernamen für die SMS-Anmeldung fest.
Snapshot stored-on pool	(Nur NetWare) Legt den Poolnamen fest, in dem der Snapshot gespeichert ist.

Tabelle 124 Backup-Plug-in-Optionen für Protokollierung

Option	Beschreibung
List backup contents	Legt fest, wie viele Informationen zu den Backup-Inhalten in den Protokolldateien enthalten sein sollen. Die Informationen enthalten Folgendes: • No file listing • List file names • List files and dates
Informational message level	Legt fest, wie viele Informationsmeldungen in den Protokolldateien enthalten sein sollen. Zu dieser Option gehört Folgendes: • No informationals – Unterdrückt alle Informationsmeldungen; Fehler und Warnungen sind allerdings in den Protokolldateien enthalten. • Some informationals – In den Protokolldateien sind einige Informationsmeldungen enthalten. • Many informationals – In den Protokolldateien sind zusätzliche Statusinformationen enthalten.

Tabelle 124 Backup-Plug-in-Optionen für Protokollierung (Fortsetzung)

Option	Beschreibung
	• All informationals – Das Höchstmaß an Informationen wird bereitgestellt. Alle Informationsmeldungen, Fehler und Warnungen sind in den Protokolldateien enthalten.
Report advanced statistics	Legt fest, ob erweiterte Timing- und Deduplizierungsstatistiken in die Protokolldateien geschrieben werden sollen.
Debugging-Meldungen aktivieren	Legt fest, ob das Höchstmaß an Informationen in die Protokolldateien geschrieben werden soll, was zu großen Protokolldateien führt.

Tabelle 125 Backup-Plug-in-Optionen für Durchlaufen des Dateisystems

Option	Beschreibung
Do not traverse any mounts	Gibt an, ob während des Backups Mount-Punkte durchlaufen werden.
Traverse fixed-disk mounts	Gibt an, ob während des Backups ausschließlich Mount-Punkte von Dateisystemen mit Festplatten durchlaufen werden.
Traverse fixed-disk and remote network mounts	Gibt an, ob während des Backups sowohl Festplatten- als auch NFS-Netzwerk-Mount-Punkte durchlaufen werden.
Force traversal of specified file system type(s)	Akzeptiert eine kommagetrennte Liste von einem oder mehreren Dateisystemtypen (z. B. nfs, ext2, jfs, xfs), die während dieses Backups nicht durchlaufen werden sollten.

Tabelle 126 Backup-Plug-in-Optionen für Prä-Skripts

Option	Beschreibung
Run user-defined script at beginning of backup	Führt ein benutzerdefiniertes Skript zu Beginn der Backupsitzung aus. Das Skript muss sich unter `/usr/local/avamar/etc/scripts` befinden.
Abort backup if script fails	Gibt an, ob das Backup gestoppt wird, wenn das Skript einen Statuscode zurückgibt, der nicht gleich Null ist.

Tabelle 127 Backup-Plug-in-Optionen für Post-Skripts

Option	Beschreibung
Run user-defined script at end of backup	Führt ein benutzerdefiniertes Skript am Ende der Backupsitzung aus. Das Skript muss sich unter `/usr/local/avamar/etc/scripts` befinden.
Exit process with script failure exitcode	Gibt an, ob `avtar` statt mit einem standardmäßigen `avtar`-Beendigungscode mit dem Beendigungscode des Skripts beendet werden soll.

Tabelle 128 Backup-Plug-in-Clientcacheoptionen

Option	Beschreibung
Check client-side caches and report inconsistencies	Bei Aktivierung wird kein Backup durchgeführt. Stattdessen führt Avamar eine Validierungsprüfung des clientseitigen Caches beim Avamar-Server durch.
Check and repair client-side caches	Bei Aktivierung wird kein Backup durchgeführt. Stattdessen führt Avamar eine Validierungsprüfung des clientseitigen Caches beim Avamar-Server durch und behebt Inkonsistenzen.
Maximum client file cache size (MBs)	Gibt die maximale Cachegröße der Clientdatei in MB an. Mit einem negativen Wert wird ein Bruchteil des RAM angegeben. Ein Wert von „-8“ bedeutet etwa, dass dem Cache der Clientdatei höchstens 1/8 des physischen RAM zugeordnet werden sollte.
Maximum client hash cache size (MBs)	Gibt die maximale Client-Hash-Cachegröße in MB an. Mit einem negativen Wert wird ein Bruchteil des RAM angegeben. Ein Wert von „-8“ bedeutet etwa, dass dem Client-Hash-Cache höchstens 1/8 des physischen RAM zugeordnet werden sollte.

Tabelle 129 Erweiterte Backup-Plug-in-Optionen

Option	Beschreibung
Client-side flag file	Gibt den Pfad zu einer Flag-Datei mit zusätzlichen Optionseinstellungen auf dem Client an.
Network usage throttle (Mbps)	Legt eine Einstellung fest, die die Netzwerkauslastung auf eine bestimmte, in Megabit/Sekunde angegebene Rate reduziert. Beispiel: 0 = keine Einschränkung, 50 % von T1 = 0,72.

Tabelle 129 Erweiterte Backup-Plug-in-Optionen (Fortsetzung)

Option	Beschreibung
Directly connect to all server nodes	Legt fest, ob mehrere Verbindungen zum Server hergestellt werden. Mehrere Verbindungen können zur Verbesserung der Backupperformance führen.

Wiederherstellungsoptionen

Welche Wiederherstellungsoptionen verfügbar sind, ist vom Plug-in-Typ abhängig.

Im folgenden Abschnitt werden die Backupoptionen für die folgenden Plug-ins beschrieben:

- AIX-Dateisystem
- FreeBSD-Dateisystem
- HP-UX-Dateisystem
- Linux-Dateisystem
- Macintosh-Dateisystem
- NetWare-Dateisystem
- SCO OpenServer-Dateisystem

Wiederherstellungsoptionen für das Avamar-Plug-in für Microsoft Windows sind im *Avamar for Windows-Server – Benutzerhandbuch* verfügbar.
Wiederherstellungsoptionen für Anwendungs-Plug-ins wie SQL Server und SharePoint VSS sind im Benutzerhandbuch zum jeweiligen Plug-in verfügbar.

In der folgenden Tabelle werden die Optionen beschrieben, die verfügbar sind, wenn Sie eine Wiederherstellung mithilfe der aufgeführten Dateisystem-Plug-ins durchführen.

Tabelle 130 Plug-in-Wiederherstellungsoptionen

Option	Beschreibung
Overwrite existing files	Steuert das Verhalten für den Fall, dass die wiederherzustellende Datei vorhanden ist. Wählen Sie eine der folgenden Optionen aus: • Never • Always • Generate New Name • If Modified • If Newer
Verschlüsselungsmethode für das Data Domain-System	Wenn das Backup auf einem Data Domain-System gespeichert wurde, wählen Sie die Verschlüsselungsmethode für Datenübertragungen zwischen dem Data Domain-System und dem Client aus.

Tabelle 131 Wiederherstellungs-Plug-in-Optionen für SMS-Authentifizierung (nur NetWare)

Option	Beschreibung
Server login ID	(Nur NetWare) Legt den Benutzernamen für die SMS-Anmeldung fest, zum Beispiel CN=admin.O=HOSTNAME_CTX.
Server password	(Nur NetWare) Legt das Passwort für den Benutzernamen für die SMS-Anmeldung fest.

Tabelle 132 Wiederherstellungs-Plug-in-Optionen für Protokollierung

Option	Beschreibung
List backup contents	Legt fest, wie viele Informationen zu den Backup-Inhalten in den Protokolldateien enthalten sein sollen. Die Informationen enthalten Folgendes: • No file listing • List file names • List files and dates
Informational message level	Legt fest, wie viele Informationsmeldungen in den Protokolldateien enthalten sein sollen. Zu dieser Option gehört Folgendes: • No informationals – Unterdrückt alle Informationsmeldungen; Fehler und Warnungen sind allerdings in den Protokolldateien enthalten. • Some informationals – In den Protokolldateien sind einige Informationsmeldungen enthalten. • Many informationals – In den Protokolldateien sind zusätzliche Statusinformationen enthalten. • All informationals – Das Höchstmaß an Informationen wird bereitgestellt. Alle Informationsmeldungen, Fehler und Warnungen sind in den Protokolldateien enthalten.
Report advanced statistics	Legt fest, ob erweiterte Timing- und Deduplizierungsstatistiken in die Protokolldateien geschrieben werden sollen.
Debugging-Meldungen aktivieren	Legt fest, ob das Höchstmaß an Informationen in die Protokolldateien geschrieben werden soll, was zu sehr großen Protokolldateien führt.

Tabelle 133 Wiederherstellungs-Plug-in-Optionen für Prä-Skripts

Option	Beschreibung
Run user-defined script at beginning of restore	Führt ein benutzerdefiniertes Skript zu Beginn der Wiederherstellungssitzung aus. Das Skript muss sich unter `/usr/local/avamar/etc/scripts` befinden.
Abort restore if script fails	Wenn das Skript einen Statuscode zurückgibt, der nicht gleich Null ist, geben Sie an, ob die Wiederherstellung gestoppt werden soll.

Tabelle 134 Wiederherstellungs-Plug-in-Optionen für Post-Skripts

Option	Beschreibung
Run user-defined script at end of restore	Führt ein benutzerdefiniertes Skript am Ende der Wiederherstellungssitzung aus. Das Skript muss sich unter `/usr/local/avamar/etc/scripts` befinden.
Exit process with script failure exitcode	Gibt an, ob `avtar` statt mit einem standardmäßigen `avtar`-Beendigungscode mit dem Beendigungscode des Skripts beendet werden soll.

Tabelle 135 Wiederherstellungs-Plug-in-Clientcacheoptionen

Option	Beschreibung
Check client-side caches and report inconsistencies	Bei Aktivierung wird keine Wiederherstellung durchgeführt. Stattdessen führt Avamar eine Validierungsprüfung des clientseitigen Caches beim Avamar-Server durch.
Check and repair client-side caches	Bei Aktivierung wird keine Wiederherstellung durchgeführt. Stattdessen führt Avamar eine Validierungsprüfung des clientseitigen Caches beim Avamar-Server durch und behebt Inkonsistenzen.
Rebuild client-side caches from most recent backup	Es werden keine Daten wiederhergestellt. Bei Aktivierung nutzt Avamar den Inhalt des letzten Backups, um den clientseitigen Dateicache neu zu erstellen.

Tabelle 136 Erweiterte Wiederherstellungs-Plug-in-Optionen

Option	Beschreibung
Do not descend into subdirectories	Legt fest, ob nur das angegebene oberste Verzeichnis, ausschließlich Unterverzeichnissen, wiederhergestellt werden soll.

Tabelle 136 Erweiterte Wiederherstellungs-Plug-in-Optionen (Fortsetzung)

Option	Beschreibung
Recreate original path beneath target directory	Legt fest, ob der ursprüngliche Pfad zu Dateien und Verzeichnissen unterhalb des angegebenen Zielverzeichnisses neu erstellt werden soll. Wenn Sie beispielsweise `/usr/MyDir/MyFile` unter `/tmp` wiederherstellen und Sie diese Option auswählen, lautet der vollständige Pfad zur wiederhergestellten Datei wie folgt: `/tmp/usr/MyDir/MyFile`.
Directly connect to all server nodes	Legt fest, ob mehrere Verbindungen zum Server hergestellt werden. Unter bestimmten Bedingungen können mehrere Verbindungen zu Performance-Verbesserungen bei Wiederherstellungen führen.

GLOSSAR

A

Accelerator Der Avamar NDMP Accelerator (Accelerator) ist ein spezieller Avamar-Server-Node, der bei Verwendung im Rahmen eines Avamar-Systems das Backup und die Wiederherstellung von Network Attached Storage(NAS)-Systemen mittels NDMP (Network Data Management Protocol) ermöglicht.

Aktivierung Der Prozess, bei dem die Client-ID (CID) an den Client zurückgegeben wird, wo sie im Clientdateisystem in einer verschlüsselten Datei gespeichert wird.

Siehe auch Clientaktivierung

Aufbewahrung Die Zeiteinstellung zum automatischen Löschen von Backups auf einem Avamar-Server. Für Backups, die nicht von einem Avamar-Server gelöscht werden sollten, kann eine dauerhafte Aufbewahrung eingestellt werden. Die Aufbewahrung ist eine dauerhafte und wiederverwendbare Avamar-Policy, die benannt und mit mehreren Gruppen verbunden werden kann.

Authentifizierungssystem Ein Benutzername- und Passwortsystem, das verwendet wird, um Benutzerzugriff auf den Avamar-Server zu gewähren. Avamar unterstützt ein eigenes internes Authentifizierungssystem (avs) sowie mehrere externe Authentifizierungssysteme (OpenLDAP, Windows Active Directory, NIS und SMB).

Avamar Administrator Eine grafische Managementkonsolen-Softwareanwendung, die über einen unterstützten Windows- oder Linux-Clientcomputer die Remoteadministration eines Avamar-Systems ermöglicht.

Avamar Client Ein Computer oder eine Workstation, auf dem bzw. der Avamar-Software ausgeführt wird und über den bzw. die per Netzwerkverbindung Zugriff auf den Avamar-Server erfolgt. Die Avamar Client-Software besteht aus einem *Client-Agent* und einem oder mehreren *Plug-ins*.

Avamar-Dateisystem (AvFS) Eine durchsuchbare virtuelle Dateisystemansicht des normalerweise nicht zugänglichen Avamar-HFS. Das Avamar-Dateisystem bietet schreibgeschützten Zugriff auf alle auf einem Avamar-Server gespeicherten Backups – bis hinunter zur Ebene der einzelnen Dateien. Dadurch kann ein Avamar-Server als langfristiger historischer, strategischer Onlinedatenspeicher für das Unternehmen verwendet werden, zusätzlich zu einem Backup- und Wiederherstellungs-Repository.

Avamar Downloader Service Ein Windows-basiertes Dateiverteilungssystem, das Softwareinstallationspakete für Avamar-Systeme bietet.

Avamar Installation Manager Eine Webschnittstelle zum Managen von Installationspaketen.

Avamar-Server Die Serverkomponente des Avamar-Client-/-Serversystems. Der Avamar-Server ist ein fehlertolerantes System mit hoher Verfügbarkeit, das Backups von allen geschützten Clients effizient speichert. Außerdem stellt er die für Datenwiederherstellungen, Clientzugriff und Remote-Systemadministration erforderlichen Prozesse und Dienste zur Verfügung. Der Avamar-Server wird als verteilte Anwendung über mehrere vernetzte Speicher-Nodes hinweg ausgeführt.

Avamar Web Access Eine browserbasierte Benutzeroberfläche, die zum Wiederherstellen von Dateien auf einem Client Zugriff auf den Avamar-Server bietet.

AvInstaller Ein Back-end-Dienst, der Paketinstallationen ausführt und meldet.

B

Backup Eine Point-in-Time-Kopie der Clientdaten, die als einzelne Dateien, ausgewählte Daten oder als komplettes Backup wiederhergestellt werden können.

C

Client-Agent Ein plattformspezifischer Softwareprozess, der auf dem Client ausgeführt wird und mit dem Management Console Server (MCS) sowie mit allen auf diesem Client installierten Plug-ins kommuniziert.

Clientaktivierung Der Prozess, bei dem die Client-ID (CID) an den Client zurückgegeben wird, wo sie im Clientdateisystem in einer verschlüsselten Datei gespeichert wird.

Siehe auch Aktivierung

Clientregistrierung Der Prozess, bei dem eine Identität für den Avamar-Server erstellt wird. Wenn Avamar den Client erkennt, wird eine eindeutige Client-ID (CID) zugewiesen, die während der *Clientaktivierung* an den Client zurückgegeben wird.

Siehe auch Registrierung

ConnectEMC Ein Programm, das auf dem Avamar-Server ausgeführt wird und Informationen an den Support von Avamar sendet. ConnectEMC ist standardmäßig so konfiguriert, dass Warnmeldungen für eingetretene Ereignisse hoher Priorität sowie einmal täglich Berichte gesendet werden.

D

Dataset Eine Policy, die einen Satz aus Dateien, Verzeichnissen und Dateisystemen für jede unterstützte Plattform definiert, die in einer Clientgruppe in Backups eingeschlossen bzw. aus diesen ausgeschlossen sind. Ein Dataset ist eine dauerhafte und wiederverwendbare Avamar-Policy, die benannt und mit mehreren Gruppen verbunden werden kann.

DNS Domain Name Server. Ein dynamischer und verteilter Verzeichnisdienst für die Zuweisung von Domainnamen für spezifische IP-Adressen.

Domain Eine Funktion in Avamar Administrator, die zur Organisation einer großen Anzahl von Clients in benannte Steuerungs- und Managementbereiche verwendet wird.

E

Email Home Eine optionale Funktion, die das Profil mit den Ereignissen hoher Priorität sowie die Benachrichtigungsplanung nutzt, um regelmäßig Serverfehler- und Statusmeldungen an den Support von Avamar zu senden.

EMC Repository Ein Repository, das Serverinstallationspakete, Clientinstallationspakete und Manifestdateien umfasst. Das Repository befindet sich im EMC Netzwerk. Jeder EMC Kunde verfügt über ein Downloadcenter, das die verfügbaren Dateien enthält. Ausgehende Kommunikation vom Avamar Downloader Service zum EMC Repository wird über eine HTTP-Verbindung mithilfe von SSL verschlüsselt.

EM Tomcat-Server (EMT) Der Avamar EM Tomcat-Server (EMT) stellt wichtige Services bereit, die zur Anzeige von Avamar-Systeminformationen erforderlich sind, und bietet einen Mechanismus zum Managen von Avamar-Systemen mithilfe eines Standardwebbrowsers. Der EMT kommuniziert außerdem direkt mit dem MCS.

ESRS Sicherer EMC Remote Support.

G

Gruppe Eine Organisationsstufe in Avamar Administrator für einen oder mehrere Avamar Clients. Alle Clients in einer Avamar-Gruppe verwenden dieselben Gruppen-Policies, einschließlich *Dataset*-, *Planungs*- und *Aufbewahrungs-Policy*.

Gruppen-Policy Die *Dataset*-, *Planungs*- und *Aufbewahrungs-Policy* für alle Clients in einer Avamar-Gruppe.

H

HFS Hash File System (Hash-Dateisystem). Der Content-Addressed-Storage-Bereich im Avamar-Server, der zur Speicherung von Clientbackups verwendet wird.

HFS-Kontrolle Eine Avamar-Hash-Dateisystemkontrolle (HFS-Kontrolle) ist ein interner Vorgang, bei dem die Integrität eines bestimmten Kontrollpunkts validiert wird. Wenn ein Kontrollpunkt eine HFS-Kontrolle bestanden hat, kann er als zuverlässig genug betrachtet werden, um ein Serverrollback durchzuführen.

J

JRE Java Runtime Environment.

L

LAN Local Area Network.

LOFS Loopback File System.

Lokales Repository Das Verzeichnis `/data01/avamar/repo/packages` auf dem Utility-Node oder Single-Node-Server. Dieses Verzeichnis enthält die aktuelle Manifestdatei aus dem EMC Repository. Der Avamar Downloader Service stellt Pakete aus dem EMC Repository per Push-Vorgang im lokalen Repository bereit. Falls an einem Kundenstandort kein Internetzugriff möglich ist, können Pakete manuell in das lokale Repository kopiert werden.

M

MAC-Adresse Media Access Control-Adresse. Eine eindeutige Hardwareadresse, die in der Regel auf der niedrigsten Ebene in einen Hardwareaufbau integriert ist und die jedes Gerät in einem Netzwerk eindeutig identifiziert.

Manifestdatei Eine XML-Datei, in der alle derzeit zum Download aus dem EMC Repository bereitstehenden Server-, Client- und Workflow-Pakete aufgeführt sind.

MCS Management Console Server. Das Serversubsystem, das eine zentrale Administration (Planung, Überwachung und Management) des Avamar-Servers ermöglicht. Der MCS führt außerdem die serverseitigen Prozesse aus, die von *Avamar Administrator* verwendet werden.

Modul Avamar 1.2.0- und frühere Avamar-Multi-Node-Server verwendeten eine synchrone 2-Modul-RAIN-Architektur, in der die Nodes in zwei separaten Geräteschränken gleichmäßig auf separate virtuelle LANs verteilt wurden. Der Begriff „Modul“ ist ein logisches Konstrukt, das diese Architektur beschreibt und unterstützt. (Ältere Avamar-Multi-Node-Server bestanden aus einem primären und einem sekundären Modul.) Diese Legacy-Systeme werden weiterhin unterstützt. Neuere Avamar-Multi-Node-Server nutzen hingegen eine Einzelmodularchitektur. Avamar Administrator stellt zwar „detaillierte Modulinformationen“ bereit, doch entspricht ein Modul logisch betrachtet dem gesamten Server.

N

NAT Network Address Translation.

NDMP Network Data Management Protocol. Ein offenes Protokoll, mit dem Daten von einem NAS-System auf einen Backupserver verschoben werden.

NFS Network File System (Netzwerkdateisystem).

NIS Network Information Service (Netzwerkinformationsdienst). Ein externes Authentifizierungssystem, das für die Anmeldung bei einem Avamar-Server verwendet werden kann.

Node Ein vernetztes Speichersubsystem, das sowohl Verarbeitungsleistung als auch Festplattenspeicher bietet und mit Avamar-Software ausgeführt wird

NTP Network Time Protocol. Steuert die Zeitsynchronisation eines Client- oder Servercomputers mit einer anderen Referenzzeitquelle.

O

ODBC Open DataBase Connectivity. Eine Standardmethode für den Datenbankzugriff, die unabhängig von dem zur Datenverarbeitung eingesetzten Datenbankmanagementsystem (DBMS) den Zugriff auf beliebige Daten von jeder Anwendung aus ermöglicht.

OpenLDAP Open Lightweight Directory Access Protocol. Ein externes Authentifizierungssystem, das für die Anmeldung bei einem Avamar-Server verwendet werden kann.

P

Pakete Avamar-Softwareinstallationsdateien, Hotfix-Patches und Betriebssystem-Patches, die im EMC Repository zur Verfügung stehen. Es gibt drei Pakettypen:

- Client – eine Version des Avamar-Dateisystems bzw. der Anwendungsbackupsoftware
- Server – eine neue Version der Avamar-Serversoftware, ein Service Pack oder ein Patch für Betriebssystem, MC oder Avamar-Server
- Workflow – ein Paket, das Vorgänge wie das Hinzufügen oder Austauschen eines Node ausführt

Paketdateien weisen die Dateierweiterung `.avp` auf.

PAM Pluggable Authentication Module. Eine Linux-Bibliothek, mit deren Hilfe ein lokaler Systemadministrator festlegen kann, wie die Benutzerauthentifizierung bei den einzelnen Anwendungen durchgeführt wird.

Plan Die Möglichkeit, die Häufigkeit sowie die tägliche Start- und Endzeit für Backups von Clients in einer Gruppe zu steuern. Ein Plan ist eine dauerhafte und wiederverwendbare Avamar-Policy, die benannt und mit mehreren Gruppen verbunden werden kann.

Plug-in Avamar Client-Software, mit der bestimmte Daten erkannt werden, die auf diesem Client gespeichert sind.

Plug-in-Optionen Während des Backups bzw. der Wiederherstellung zur Steuerung der Backup- oder Wiederherstellungsfunktion festgelegte Optionen.

Policy Ein Satz von Regeln für Clientbackups, die benannt und auf mehrere Gruppen angewendet werden können. Gruppen verfügen über Datasets, Planungen und Aufbewahrungs-Policies.

R

RAIN Redundant Array of Independent Nodes. Eine flexible, fehlertolerante Architektur, dank der ein Avamar-Server seine Verfügbarkeit sowie den Datenspeicher aufrechterhalten kann, wenn in einem Avamar-Modul einzelne Nodes ausfallen.

RDMS Relationales Datenbankmanagementsystem.

Registrierung Der Prozess, bei dem eine Identität für den Avamar-Server erstellt wird. Wenn Avamar den Client erkennt, wird eine eindeutige Client-ID (CID) zugewiesen, die während der *Clientaktivierung* an den Client zurückgegeben wird.

Siehe auch Clientregistrierung

replication Die Replikation ist eine optionale Funktion, die es einem Avamar-System ermöglicht, schreibgeschützte Kopien seiner Daten auf einem Remotesystem zu speichern. Bei den replizierten Daten kann es sich um Replikate von Clientbackups und Kopien von Avamar-Systemdaten handeln. Die Replikation unterstützt die Disaster Recovery des Avamar-Systems.

Replikat Replizierte Kopie eines Backups

Rollen Eine Einstellung in Avamar Administrator, die steuert, welche Vorgänge jeder Benutzer auf dem Avamar-Server durchführen darf. Die Rollen werden für jeden Benutzer einzeln zugewiesen.

S

Speicher-Node Ein Node auf dem Avamar-Server, der Datenspeicher bereitstellt.

SSH Secure Shell. Ein Dienstprogramm für die Remote-Anmeldung, das eine Authentifizierung über verschlüsselte Sicherheitsschlüssel vornimmt, statt zur Eingabe von Passwörtern aufzufordern. Dadurch wird verhindert, dass Passwörter ungeschützt netzwerkübergreifend verwendet werden.

Systemmigration Ein geplanter Vorgang, bei dem alle sich auf dem Avamar-Quellserver befindenden Daten durch vollständige „Root-zu-Root“-Replikation auf einen neuen Zielserver kopiert werden. Wenn globale Client-IDs (globale CIDs) verwendet werden, können zuvor auf dem Quellserver gesicherte Clients weiter transparent ausgeführt werden, ohne sich bei dem neuen Zielserver erneut anmelden zu müssen.

T

TFTP Trivial File Transfer Protocol. Eine Version des TCP/IP-FTP-Protokolls, das über keine Verzeichnis- oder Passwortfunktionen verfügt.

U

Utility-Node Bei skalierbaren Avamar-Multi-Node-Servern führt ein einziger Utility-Node wichtige interne Dienste für den Server aus. Zu diesen Diensten zählen u. a. MCS, cronjob, Domain Name Server (DNS), externe Authentifizierung, Network Time Protocol (NTP) und Webzugriff. Da Utility-Nodes eigens auf die Ausführung dieser wichtigen Dienste ausgerichtet sind, können sie nicht zum Speichern von Backups verwendet werden.

V

VLAN Virtual Local Area Network oder VLAN.

Vollständige Replikation Bei einer Root-to-Root-Replikation wird eine komplette logische Kopie des gesamten Quellsystems auf dem Zielsystem erstellt. Die replizierten Daten werden nicht in die Domain REPLICATE kopiert. Stattdessen werden sie der Root-Domain hinzugefügt, so als hätten sich Quellclients beim Zielsystem registriert. Auf diese Weise replizierte Quellserverdaten sind außerdem auf dem Zielsystem vollständig modifizierbar. Diese Replikationsmethode wird in der Regel zur Systemmigration (von einer kleineren zu einer größeren Avamar-Konfiguration mit ggf. mehreren Nodes) oder für einen Systemwechsel (zum Beispiel im Falle einer Disaster Recovery) verwendet.

W

Wiederherstellung Ein Vorgang, bei dem ein oder mehrere Dateisysteme, Verzeichnisse, Dateien oder Datenobjekte aus einem Backup abgerufen und an einen bestimmten Speicherort geschrieben werden.