Dell™ One Identity Manager 7.1.3

Administrationshandbuch für die Datenarchivierung

Legende

△ **VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.**

⚠ **WARNUNG: Das Symbol WARNUNG weist auf mögliche Personen- oder Sachschäden oder Schaden mit Todesfolge hin.**

ⓘ **WICHTIG**, **HINWEIS**, **TIPP**, **MOBIL**, oder **VIDEO:** Ein Informationssymbol weist auf Begleitinformationen hin.

One Identity Manager Administrationshandbuch für die Datenarchivierung
Aktualisiert: November 2017
Version: 7.1.3

Inhalt

1

Archivierung der Datenänderungen

Alle im One Identity Manager erfassten Datenänderungen werden zunächst in der One Identity Manager-Datenbank gespeichert. Historische Daten der One Identity Manager-Datenbank werden in zyklischen Abständen in eine History-Datenbank übertragen. Diese History-Datenbank stellt somit das Veränderungsarchiv dar. In der History-Datenbank erfolgen statistische Auswertungen, die die Darstellungen von Trends oder Verläufen vereinfachen. Die Auswertung der historischen Daten erfolgt über die TimeTrace-Funktion oder über Berichte.

Installieren des HistoryDB-Archivsystems

Bei der Inbetriebnahme des HistoryDB-Archivsystems sollten Sie Perfomanceüberlegungen berücksichtigen. Abhängig vom Datenvolumen der One Identity Manager-Datenbank, den für die Archivierung aufzuzeichnenden Daten und deren Änderungshäufigkeit kann es erforderlich sein, in gewissen Zeitabständen (beispielsweise jährlich, quartalsweise oder monatlich) weitere History-Datenbanken zu erstellen.

Die Einrichtung einer Arbeitsumgebung für das HistoryDB-Archivsystem umfasst folgende Schritte:

- Einrichten einer administrativen Arbeitsstation

  Weitere Informationen finden Sie unter Einrichten einer administrativen Arbeitsstation auf Seite 4.
- Erstellen und Migrieren der History-Datenbank

  Weitere Informationen finden Sie unter Installieren und Konfigurieren einer History-Datenbank auf Seite 11.
- Installieren und Konfigurieren eines One Identity Manager History Service auf einem Server

  Weitere Informationen finden Sie unter Installieren und Konfigurieren eines Servers auf Seite 12.

Einrichten einer administrativen Arbeitsstation

Die Systemvoraussetzungen für die Installation der HistoryDB-Werkzeuge auf einer administrativen Arbeitsstation und die erforderlichen Berechtigungen sind im Dell One Identity Manager Installationshandbuch beschrieben.

Auf einer administrativen Arbeitsstation sollten Sie mindestens folgende Werkzeuge installieren:

- HistoryDB Manager
- Job Queue Info

- Configuration Wizard
- Designer

Die Erstinstallation der HistoryDB-Werkzeuge auf den Arbeitsstationen nehmen Sie mit dem Installationsassistenten vor.

Um die Komponenten zu installieren

1. Führen Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager-Installationsmediums aus.
2. Wechseln Sie auf den Tabreiter **Andere Produkte,** wählen Sie den Eintrag "Dell™ One Identity Manager History Database" und klicken Sie **Installieren**.
3. Der Installationsassistent wird gestartet. Auf der Startseite wählen Sie die Sprache für den Installationsassistenten aus und klicken Sie **Weiter**.
4. Auf der Seite **Einstellungen für die Installation** legen Sie die Daten zur Installationsquelle und Installationsziel fest.
    - Wählen Sie unter **Installationsquelle** das Verzeichnis mit den Installationsdateien.
    - Wählen Sie unter **Installationsverzeichnis** das Verzeichnis, in das die Dateien der One Identity Manager History Database installiert werden sollen.
    - Klicken Sie **Weiter**.
5. Auf der Seite **Maschinenrolle zuordnen** legen Sie die Maschinenrollen und die Installationspakete fest und klicken Sie **Weiter**.

    HINWEIS: Die zu den One Identity Manager Modulen passenden Maschinenrollen sind aktiviert. Bei Auswahl einer Maschinenrolle werden alle untergeordneten Installationspakete mit ausgewählt. Sie können einzelne Installationspakete abwählen.
6. Auf der letzten Seite des Installationsassistenten können Sie verschiedene Programme für die weitere Installation starten.
    - Um die Installation des HistoryDB Schemas auszuführen, starten Sie den Configuration Wizard und folgen Sie den Anweisungen des Configuration Wizard.

        HINWEIS: Führen Sie diesen Schritt nur auf der Arbeitsstation aus, auf der Sie die Installation des HistoryDB Schemas starten.
7. Um den Installationsassistenten zu beenden, klicken Sie **Ende**.
8. Schließen Sie das Autorun Programm.

Voraussetzungen für den Betrieb einer History-Datenbank

Wenn Sie eine History-Datenbank erstmals installieren, richten Sie zuvor eine initiale Datenbank ein. Die Systemvoraussetzungen dafür sind im Dell One Identity Manager Installationshandbuch beschrieben.

Hinweise zum Einsatz mehrerer SQL Server®

> **HINWEIS:** Befinden sich History-Datenbank und One Identity Manager-Datenbank auf verschiedenen Servern werden nur gleiche Versions- und Patchstände von Betriebssystem und Datenbanksystem unterstützt.

Befinden sich History-Datenbank und One Identity Manager-Datenbank auf verschiedenen Datenbankservern sind auf beiden Servern folgende Voraussetzungen für die Datenübernahme zu gewährleisten:

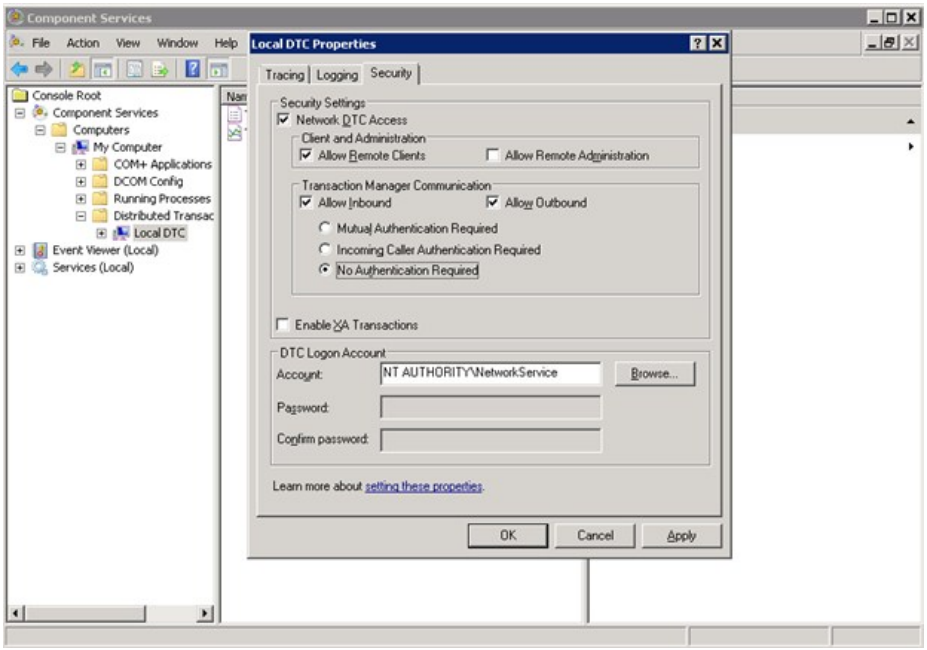
- Start der Dienste „Microsoft Distributed Transaction Coordinator“(DTC), „RPC Client“ und „Security Accounts Manager“
- Für die Netzwerkkommunikation zwischen den Servern prüfen Sie die Einstellungen der Firewall und passen Sie bei Bedarf die Einstellungen entsprechend der Empfehlungen des eingesetzten Betriebssystems an. Weitere Informationen finden Sie in der Dokumentation zum eingesetzten Betriebssystem.

In den DTC-Sicherheitseinstellungen sollten folgenden Einstellungen aktiviert sein:

- DTC-Netzwerkzugriff (Network DTC Access)
- Remoteclients zulassen (Allow Remote Clients)
- Eingehende zulassen (Allow Inbound)
- Ausgehende zulassen (Allow Outbound)
- Kein Authentifizierung erforderlich (No Authentication Requiered)

Die Sicherheitseinstellungen konfigurieren Sie in der Microsoft Management Console im Snap-In Komponentendienste.

Abbildung 1: Konfiguration der DTC-Sicherheitseinstellungen



Werden große Datenmengen von der One Identity Manager-Datenbank in die History-Datenbank übertragen, sollte auf dem Datenbankserver, der die One Identity Manager-Datenbank hält, das Timeout für Remoteabfragen erhöht werden. Die Standardeinstellung ist 600 Sekunden, was einer Wartezeit von zehn

Minuten entspricht. Ist die Wartezeit abgelaufen, wird die Datenübertragung abgebrochen. Das Timeout für Remoteabfragen sollte sich am Ausführungsintervall das Zeitplans zur Datenübernahme orientieren.

Das Timeout für Remoteabfragen können Sie mit folgendem Statement abfragen:

```
select * from sys.configurations where name like '%remote query timeout%'
```

Um das Timeout für Remoteabfragen zu ändern, verwenden Sie folgendes Statement:

```
exec sp_configure 'remote query timeout (s)',<new value>
RECONFIGURE WITH OVERRIDE
```

Wobei:

```
<new value> = Neuer Timeout-Wert in Sekunden
```

Datenbankbenutzer unter SQL Server®

ⓘ **HINWEIS:** Als Standardsprache für Datenbankbenutzer ist "English" auszuwählen.

Die Berechtigungen der Datenbankbenutzer können nach zwei Benutzertypen unterschieden werden:

- Endbenutzer

  Endbenutzer, die beispielsweise nur mit dem Web Portal arbeiten, müssen nur Mitglied der Datenbankrolle „basegroup“ sein.

- Administrative Benutzer

  Administrative Benutzer benötigen die nachfolgend aufgeführten Berechtigungen. Hierbei kann zwischen Berechtigungen für die Installation und Berechtigungen für den laufenden Betrieb unterschieden werden.

Um die Funktionen der HistoryDB in vollem Umfang zu nutzen, werden folgende Berechtigungen benötigt.

Tabelle 1: Berechtigungen für Datenbankbenutzer unter SQL Server®

Berechtigung	Für Datenbank	Benötigt für Installation	Benötigt für laufenden Betrieb	Benötigt für
Serverrolle „dbcreator“*		x	-	Erzeugen der Datenbank.
Serverrolle „processadmin“		-	x	Aktivität von Verbindungen prüfen und gegebenenfalls schließen der Verbindung.
Datenbankrolle „db_owner“	History-Datenbank	x	x	Erzeugen der Datenbank. Betreiben der Datenbank.
Datenbankrolle „basegroup“**	History-Datenbank	-	x	Interne Berechtigungsrolle für Datenbankobjekte.
Berechtigung „Execute“	Master	x	x	Starten des SQL Server Agent.
Datenbankrolle „SQLAgentUserRole“	msdb	-	x	Ausführen von Datenbankschedules.
Datenbankrolle „db_Datareader“	msdb	-	x	Lesen und Ändern von Datenbankschedules.

Berechtigung	Für Datenbank	Benötigt für Installation	Benötigt für laufenden Betrieb	Benötigt für
Datenbankrolle „SQLAgentOperatorRole“	msdb	x	x	Definieren von Datenbankschedules.
Berechtigung „Connect“	tempdb	x	x	Prüfen, ob Einzelbenutzermodus während der Verbindung erforderlich ist.

*) Die Berechtigung ist nur erforderlich, wenn die Datenbank durch den Configuration Wizard erstellt wird.

**) Die Datenbankrolle „basegroup“ wird während der initialen Schemainstallation der History-Datenbank standardmäßig angelegt.

HINWEIS: Wird das Benutzerkonto des Datenbankbenutzers erst nach der Migration der Datenbank gewechselt, dann muss der neue Datenbankbenutzer nachträglich als Eigentümer der Datenbankschedules eingetragen werden. Ansonsten kommt es zu Fehlermeldungen bei der Ausführung der Datenbankschedules.

Zusätzliche Berechtigungen für die Datenübernahme

Befinden sich History-Datenbank und One Identity Manager-Datenbank auf einem Datenbankserver erfolgt die Datenübernahme mit dem Datenbankbenutzer, unter dem die History-Datenbank läuft. Dieser Datenbankbenutzer benötigt zusätzlich Zugriff auf die One Identity Manager-Datenbank.

- Datenbankrolle „db_owner“ für die One Identity Manager-Datenbank

Befinden sich History-Datenbank und One Identity Manager-Datenbank auf verschiedenen Datenbankservern wird mit dem Datenbankbenutzer, unter dem die History-Datenbank läuft, eine Verbindung zur One Identity Manager-Datenbank erzeugt. Folgende Berechtigungen werden zusätzlich benötigt:

- Serverberechtigung „ALTER ANY LINKED SERVER“

  Erstellen und Löschen eines Verbindungsservers. Der Verbindungsserver ermöglicht die Ausführung verteilter Abfragen.

- Serverberechtigung „ALTER ANY LOGIN“

  Erstellen und Löschen einer Zuordnung von Anmeldenamen auf dem lokalen Server und einem Anmeldenamen auf dem Verbindungsserver.

- Serverrollen „setupadmin“ und „sysadmin“

  Aufbau und Löschen einer Verbindung zwischen Datenbankservern.

Die anschließende Datenübernahme erfolgt mit einem Datenbankbenutzer, der Zugriff auf die One Identity Manager-Datenbank besitzt. Folgende Berechtigungen werden benötigt:

- Datenbankrolle „db_owner“ für die One Identity Manager-Datenbank

Hinweise zur Nutzung der integrierten Windows® Authentifizierung

Die integrierte Windows® Authentifizierung kann für den One Identity Manager Service und die Webanwendungen uneingeschränkt genutzt werden. Für die Fat-Clients kann die integrierte Windows Authentifizierung genutzt werden. Die Nutzung von Windows® Gruppen zur Anmeldung wird unterstützt. Zur Sicherstellung der Funktionalität wird jedoch dringend die Nutzung einer SQL Server® Anmeldung empfohlen.

Um die integrierte Windows® Authentifizierung einzusetzen

- Richten Sie für das Benutzerkonto auf dem Datenbankserver eine SQL Server® Anmeldung ein.
- Tragen Sie als Standardschema „dbo“ ein.
- Weisen Sie der SQL Server Anmeldung die benötigten Berechtigungen zu. Weitere Informationen finden Sie unter Tabelle 1 auf Seite 7.

Hinweise zur Nutzung der integrierten Windows® Authentifizierung

Wird die integrierte Windows® Authentifizierung genutzt, erfolgt die Datenübernahme mit dem Benutzerkonto des One Identity Manager History Service.

- Für das Benutzerkonto richten Sie auf dem Datenbankserver eine SQL Server® Anmeldung ein. Befinden sich History-Datenbank und One Identity Manager-Datenbank auf verschiedenen Servern, richten Sie die SQL Server® Anmeldung auf beiden Datenbankservern ein.
- Weisen Sie der SQL Server Anmeldung die benötigten Berechtigungen für die Datenübernahme zu. Weitere Informationen finden Sie unter Datenbankbenutzer unter SQL Server® auf Seite 7.

Befinden sich History-Datenbank, One Identity Manager History Service und One Identity Manager-Datenbank auf verschiedenen Servern sind weitere Voraussetzungen zu erfüllen:

- Das Benutzerkonto des One Identity Manager History Service benötigt einen Service Principal Name (SPN) für die Authentifizierung. Dieser kann über folgenden Kommandozeilen erstellt werden:

  ```
  SetSPN -A HTTP/<Vollständiger Domänenname> <Domäne>\<Benutzerkonto>
  ```

- Das Benutzerkonto des One Identity Manager History Service muss für Delegierungen freigeschaltet sein und Kerberos zur Authentifizierung verwenden.

  Setzen Sie dazu in der Microsoft Management Konsole für Active Directory® Benutzer- und Computer auf dem Tabreiter **Delegierungen** die Option **Benutzer bei Delegierungen aller Dienste vertrauen (nur Kerberos)** (Trust this user for delegation to any service (Kerberos only).

- Der SQL Server® Dienst benötigt einen Service Principal Name zur Authentifizierung. Diesen können Sie über folgenden Kommandozeilenaufruf prüfen:

  ```
  SetSPN -L <Name des Datenbankservers>
  ```

Hinweise zum Einsatz mehrerer Oracle Server

Befinden sich History-Datenbank und One Identity Manager-Datenbank auf verschiedenen Servern werden nur gleiche Versions- und Patchstände von Betriebssystem und Datenbanksystem unterstützt.

Datenbankbenutzer unter Oracle® Database

Für die Nutzung der Datenbank sollte ein eigener Datenbankbenutzer eingerichtet werden. Den Datenbankbenutzer können Sie über den Configuration Wizard erzeugen oder manuell erstellen.

ⓘ **HINWEIS:** Die verwendeten Datenbankbenutzer müssen die Berechtigungen direkt erhalten. Bei der Zuweisung von Berechtigungen über Datenbankrollen kann es bei der Ausführung von Datenbankabfragen, aufgrund von Berechtigungseinschränkungen, zu Oracle Fehlermeldungen kommen.

Berechtigungen für Oracle® Database Installationen

Um die Funktionen der HistoryDB in vollem Umfang zu nutzen, werden für Oracle® Database Installationen die folgenden Berechtigungen benötigt.

Tabelle 2: Berechtigungen für Datenbankbenutzer

Berechtigung	Benötigt Für
GRANT ALTER SESSION TO <user>	Einstellungen der eigenen Benutzersitzung ändern.
GRANT ANALYZE ANY TO <user>	Die Berechtigung wird zum Ausführen der Prozedur `DBMS_STATS.FLUSH_DATABASE_MONITORING_INFO` während der Statistikberechnungen verwendet. Sollen keine Statistiken ermittelt werden, kann auf diese Berechtigung verzichtet werden.
GRANT CONNECT TO <user>	Datenbank verbinden.
GRANT CREATE JOB TO <user>	Datenbankschedules erzeugen.
GRANT CREATE PROCEDURE TO <user>	Schemaobjekte erzeugen.
GRANT CREATE SEQUENCE TO <user>	Schemaobjekte erzeugen.
GRANT CREATE SYNONYM TO <user>	Schemaobjekte erzeugen.
GRANT CREATE TABLE TO <user>	Schemaobjekte erzeugen.
GRANT CREATE TRIGGER TO <user>	Schemaobjekte erzeugen.
GRANT CREATE TYPE TO <user>	Schemaobjekte erzeugen.
GRANT CREATE VIEW TO <user>	Schemaobjekte erzeugen.
GRANT EXCEUTE ON DBMS_PIPE TO <user>	Kommunikation der einzelnen Verarbeitungsschritte mit der Hauptroutine des DBQueue Prozessor im Parallelbetrieb.

Berechtigung	Benötigt Für
GRANT EXECUTE ON DBMS_CRYPTO TO <user>	Zugriff auf Paket für allgemeine Verschlüsselungsroutinen.
GRANT EXECUTE ON DBMS_LOCK TO <user>	Nutzung der Sleep-Methode bei der Weiterschaltung der Verarbeitung im DBQueue Prozessor, zum Beispiel zum Warten auf Beenden einzelner Verarbeitungsschritte.
GRANT SELECT ON GV_ $OSSTAT TO <user>	Informationen zu aktuellen Serverversion auslesen.
GRANT SELECT ON GV_ $SESSION TO <user>	Informationen der aktuellen Sitzungen auslesen. Diese Berechtigung wird unter anderem dazu benötigt, die Datenbank in der Einzelbenutzermodus zu schalten.

Zusätzliche Berechtigungen für die Datenübernahme

Die Datenübernahme erfolgt mit dem Datenbankbenutzer, unter dem die History-Datenbank läuft. Dieser Datenbankbenutzer benötigt zusätzlich Zugriff auf die One Identity Manager-Datenbank über einen Datenbank-Link (Database Link). Der Datenbank-Link sollte von einem Datenbank-Administrator zur Verfügung gestellt werden. Der Datenbank-Link muss einmalig erzeugt werden.

Installieren und Konfigurieren einer History-Datenbank

Die Installation und Konfiguration der Datenbank erfolgt mit dem Configuration Wizard. Der Ablauf ist im Dell One Identity Manager Installationshandbuch beschrieben.

Auf der Arbeitsstation, auf der die Schemainstallation gestartet wird, müssen zusätzlich die folgenden Voraussetzungen erfüllt sein:

- Installation des Programms „Configuration Wizard“

  Die Installation des Programms erfolgt mit dem Installationsassistenten. Wählen Sie dazu im Installationsassistenten die Maschinenrolle "Workstation" und das Installationspaket "Configuration".

- Zugriff auf die Installationsquellen

  HINWEIS: Wenn Sie die Installationsquellen auf ein Ablageverzeichnis kopieren, müssen Sie sicherstellen, dass die relative Verzeichnisstruktur erhalten bleibt.

HINWEIS: Die HistoryDB-Werkzeuge auf dieser Arbeitsstation aktualisieren Sie nicht über die automatische Softwareaktualisierung, sondern über den Installationsassistenten.

Installieren und Konfigurieren eines Servers

Der Dienst „One Identity Manager History Service“ sorgt für die Datenübernahme aus der One Identity Manager-Datenbank in die History-Datenbank.

Die Systemvoraussetzungen für die Installation der One Identity Manager History Service auf einem Server und die erforderlichen Berechtigungen sind im Dell One Identity Manager Installationshandbuch beschrieben.

Die Erstinstallation des One Identity Manager History Service auf dem Server nehmen Sie mit dem Installationsassistenten vor. Die Installation und Konfiguration des One Identity Manager History Service erfolgt analog zum One Identity Manager Service. Der Ablauf ist im Dell One Identity Manager Installationshandbuch beschrieben.

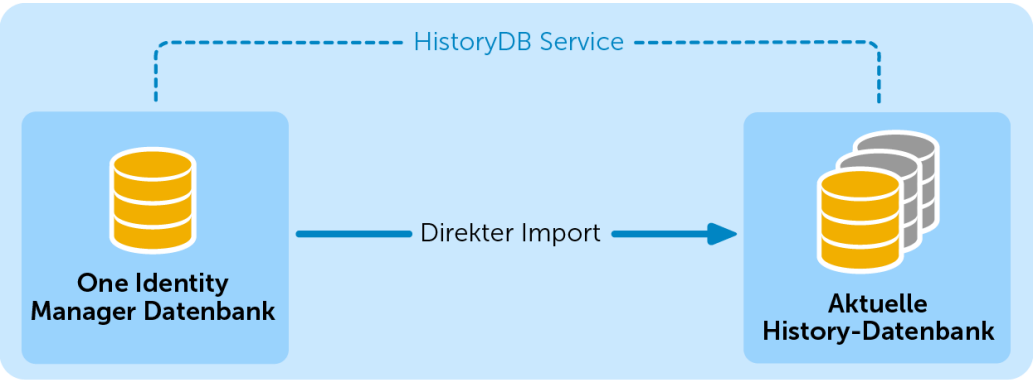
Einrichten des Archivierungsverfahrens

Im One Identity Manager werden verschiedene Verfahren zur Nachverfolgung von Änderungen genutzt. Dazu zählen die Aufzeichnung von Datenänderungen, die Aufzeichnung von Prozessinformationen und die Aufzeichnung von Meldungen in der Prozesshistorie. Der Anteil der historisierten Daten am Gesamtvolumen einer One Identity Manager-Datenbank sollte maximal 25 % betragen. Anderenfalls kann es zu Performance-Problemen kommen.

Um die aufgezeichneten Daten der einzelnen Teilbereiche in regelmäßigen Abständen aus der One Identity Manager-Datenbank zu entfernen, werden folgende Verfahren angeboten:

- Die Daten können direkt aus der One Identity Manager-Datenbank in eine History-Datenbank übernommen werden. Dieses ist das Standardverfahren für die Datenarchivierung. Wählen Sie dieses Verfahren, wenn die Server auf denen die One Identity Manager-Datenbank und die History-Datenbank liegen einander sehen.
- Die Daten werden ohne Archivierung nach einer festgelegten Zeitspanne aus der One Identity Manager-Datenbank gelöscht.

Abbildung 2: Übernahme der Aufzeichnungen in das HistoryDB-Archivsystem



Für die direkte Übernahme in eine History-Datenbank werden in der One Identity Manager-Datenbank alle Aufzeichnungen, die von einer Aktion ausgelöst wurden, anhand einer ID-Nummer, der GenProcID, zu einer Prozessgruppe zusammengefasst. Nach erfolgreichem Export werden die exportierten Prozessgruppen mit den zugehörigen Aufzeichnungen aus der One Identity Manager-Datenbank gelöscht.

Für die direkte Übernahme in eine History-Datenbank müssen folgende Bedingungen erfüllt sein:

- Der Teilbereich der Aufzeichnungen ist für den Export konfiguriert.
- Die Aufbewahrungszeit aller Aufzeichnungen, die zu einer Prozessgruppe gehören, ist abgelaufen, unabhängig davon ob der Teilbereich zum Export gekennzeichnet ist.
- Es gibt keine aktiven Prozesse mit der GenProcID der Prozessgruppe in der DBQueue, in der Jobqueue oder als geplante Operationen.
- Es gibt für die auslösende Aktion mindestens eine Aufzeichnung in dem Teilbereich, der exportiert werden soll.

Für die Archivierung der Aufzeichnungen sind in beiden Datenbanken - der One Identity Manager-Datenbank und der History-Datenbank - Konfigurationen vorzunehmen.

Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank

Die Auswahl des grundlegenden Verfahrens treffen Sie über die Einstellung des Konfigurationsparameters „Common\ProcessState\ExportPolicy“. Ist der Konfigurationsparameter deaktiviert, verbleiben die Daten in der One Identity Manager-Datenbank. Ist der Konfigurationsparameter aktiviert, dann wird das gewählte Verfahren angewendet.

Tabelle 3: Zulässige Werte des Konfigurationsparameters „Common\ProcessState\ExportPolicy“

Wert	Bedeutung
HDB	Die Daten werden nach Ablauf einer festgelegten Zeitspanne direkt in eine History-Datenbank übernommen.
NONE	Die Daten werden nach Ablauf einer festgelegten Zeitspanne aus der One Identity Manager-Datenbank gelöscht.

Für jeden Teilbereich der Aufzeichnungen können Sie nach der Auswahl des grundlegenden Verfahrens separat festlegen, ob die Daten exportiert oder gelöscht werden. Die Festlegung für die einzelnen Bereiche treffen Sie über Konfigurationsparameter.

Tabelle 4: Konfigurationsparameter für die Behandlung der Prozessinformationen

Konfigurationsparameter	Bedeutung
Common\ProcessState\ProgressView\LifeTime	Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit für Prozessinformationen in der Datenbank festgelegt.
Common\ProcessState\ProgressView\IsToExport	Die Prozessinformationen sollen exportiert werden. Ist der Konfigurationsparameter nicht aktiv, werden die Informationen nach Ablauf der Aufbewahrungszeit gelöscht.

Tabelle 5: Konfigurationsparameter für die Behandlung der Prozesshistorie

Konfigurationsparameter	Bedeutung
Common\ProcessState\JobHistory\LifeTime	Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit für Aufzeichnungen aus der Prozesshistorie in der Datenbank festgelegt.
Common\ProcessState\JobHistory\IsToExport	Die Informationen in der Prozesshistorie sollen exportiert werden. Ist der Konfigurationsparameter nicht aktiv, werden die Informationen nach Ablauf der Aufbewahrungszeit gelöscht.

Tabelle 6: Konfigurationsparameter für die Behandlung der aufgezeichneten Datenänderungen

Konfigurationsparameter	Bedeutung
Common\ProcessState\PropertyLog\LifeTime	Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit für aufgezeichnete Datenänderungen in der Datenbank festgelegt.
Common\ProcessState\PropertyLog\IsToExport	Die aufgezeichneten Datenänderungen sollen exportiert werden. Ist der Konfigurationsparameter nicht aktiv, werden die Informationen nach Ablauf der Aufbewahrungszeit gelöscht.

Festlegen der Aufbewahrungszeiten

Die Aufzeichnungen werden, abhängig vom gewählten Archivierungsverfahren, nach Ablauf der Aufbewahrungszeiten aus der One Identity Manager-Datenbank exportiert oder gelöscht. Für die Teilbereiche, deren Aufzeichnungen exportiert werden, sollte eine längere Aufbewahrungszeit gewählt werden, als für die Teilbereiche, deren Aufzeichnungen gelöscht werden.

ⓘ **HINWEIS:** Wenn Sie keine Aufbewahrungszeiten festlegen, werden die Aufzeichnungen dieser Teilbereiche täglich innerhalb der tägliche Wartungsaufträge des DBQueue Prozessors aus der One Identity Manager-Datenbank gelöscht.

Die Aufzeichnungen werden erst exportiert, wenn die Aufbewahrungszeiten aller Teilbereiche abgelaufen ist und keine weiteren aktiven Prozesse für die Prozessgruppe (GenProcID) in der DBQueue, der Prozesshistorie oder als geplante Operation existieren.

Beispiel 1

Die Aufzeichnungen werden direkt in eine History-Datenbank übernommen. Für die einzelnen Teilbereiche wurden folgende Konfigurationen gewählt:

Konfiguration	Prozessinformationen	Prozesshistorie	Datenänderungen
Daten exportieren	Nein	Nein	Ja
Aufbewahrungszeit	3 Tage	4 Tage	5 Tage

Daraus ergibt sich folgender Ablauf:

Zeitpunkt	Prozessinformationen	Prozesshistorie	Datenänderungen
Tag 3	Daten werden in der One Identity Manager-Datenbank gelöscht.	Keine Aktion.	Keine Aktion.
Tag 4	-	Daten werden in der One Identity Manager-Datenbank gelöscht.	Keine Aktion.
Tag 5	-	-	Daten werden in die History-Datenbank übernommen und anschließend in der One Identity Manager-Datenbank gelöscht.

Beispiel 2

Die Aufzeichnungen werden direkt in eine History-Datenbank übernommen. Für die einzelnen Teilbereiche wurden folgende Konfigurationen gewählt:

Konfiguration	Prozessinformationen	Prozesshistorie	Datenänderungen
Daten exportieren	Ja	Nein	Ja
Aufbewahrungszeit	3 Tage	4 Tage	5 Tage

Daraus ergibt sich folgender Ablauf:

Zeitpunkt	Prozessinformationen	Prozesshistorie	Datenänderungen
Tag 3	Keine Aktion, da die Aufbewahrungszeit noch nicht in allen Teilbereichen abgelaufen ist.	Keine Aktion.	Keine Aktion.
Tag 4	Keine Aktion, da die Aufbewahrungszeit noch nicht in allen Teilbereichen abgelaufen ist.	Daten werden in der One Identity Manager-Datenbank gelöscht.	Keine Aktion.
Tag 5	Daten werden exportiert und anschließend gelöscht.	-	Daten werden in die History-Datenbank übernommen und anschließend in der One Identity Manager-Datenbank gelöscht.

Bekanntgeben der Quelldatenbank in der History-Datenbank

Für die Datenübernahme geben Sie in der History-Datenbank die zu verwendende One Identity Manager-Datenbank bekannt. Nutzen Sie den HistoryDB Manager um den Zugriff auf die Quelldatenbanken einzurichten.

Um die Quelldatenbank bekanntzugeben

- Starten Sie den HistoryDB Manager und geben Sie die Verbindungsdaten an.
- Wählen Sie die Kategorie **Historie | Basisdaten | Quelldatenbanken**.

- Wählen Sie in der Ergebnisliste die Quelldatenbank aus.
- Bearbeiten Sie die Stammdaten.

Tabelle 7: Daten für Quelldatenbank

Eigenschaft	Bedeutung

Server	Name des Datenbankservers, auf dem sich die One Identity Manager-Datenbank befindet. Der Servername kann in der One Identity Manager- Datenbank über folgendes Statement abgefragt werden:
	`select @@SERVERNAME`
	Wenn der Server über einen bestimmten Port erreichbar ist kann dieser folgendermaßen übergeben werden.
	`Servername, Port`

Datenbank	Name der One Identity Manager-Datenbank.
Datenbank-ID	Datenbank-ID der One Identity Manager-Datenbank. Diese Kennung entspricht der UID des Datenbankeintrages in der One Identity Manager-Datenbank. **HINWEIS:** Verbinden Sie sich mit dem Object Browser auf die One Identity Manager-Datenbank und kopieren Sie aus der Tabelle `DialogDatabase` und den Wert der Spalte `UID_Database`. Diesen Wert fügen Sie im Eingabefeld **Datenbank-ID** ein.
Integrierte Windows® Authentifizierung verwenden	Wird die integrierte Windows® Authentifizierung genutzt, erfolgt die Datenübernahme mit dem Benutzerkonto des One Identity Manager History Service. Für den Einsatz dieses Authentifizierungsverfahrens sind bestimmt Installationsvoraussetzungen zu beachten. Lesen Sie dazu den Abschnitt Voraussetzungen für den Betrieb einer History-Datenbank auf Seite 5.
Datenbankbenutzer	Datenbankbenutzer, mit dem der Zugriff auf die Quelldatenbank erfolgt. Befinden sich History-Datenbank und One Identity Manager-Datenbank auf einem Server, ist diese Angabe nicht erforderlich. Der Zugriff erfolgt mit dem Datenbankbenutzer unter dem die History-Datenbank läuft. Befinden sich History-Datenbank und One Identity Manager-Datenbank auf verschiedenen Servern, geben Sie hier den Datenbankbenutzer der One Identity Manager-Datenbank an, mit dem die Datenübernahme durchgeführt werden soll. Beachten Sie die unter Datenbankbenutzer unter SQL Server® auf Seite 7 beschriebenen Berechtigungen.
Kennwort	Kennwort des Datenbankbenutzers.
Beginn und Ende der Aufzeichnungen	Diese Datumsangaben werden beim Import der Aufzeichnungen automatisch gesetzt und aktualisiert.

- Speichern Sie die Änderungen.

Konfigurieren der Datenbanken für die direkte Archivierung

One Identity Manager-Datenbank:

- Aktivieren Sie im Designer den Konfigurationsparameter "Common\ProcessState\ExportPolicy" und tragen Sie den Wert `HDB` ein.
- Konfigurieren Sie die Teilbereiche für den Export und legen Sie die Aufbewahrungszeiten fest. Weitere Informationen finden Sie unter Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank auf Seite 13.
- Prüfen Sie im Designer den Wert der Konfigurationsparameters "Common\ProcessState\PackageSizeHDB". Dieser Parameter legt die maximale Anzahl der, in die History-Datenbank zu übertragenden, Prozessgruppen fest. Der Standardwert ist 10000.

History-Datenbank:

- Geben Sie die One Identity Manager-Datenbank in der History-Datenbank als Quelldatenbank bekannt. Weitere Informationen finden Sie unter Bekanntgeben der Quelldatenbank in der History-Datenbank auf Seite 15.
- Der Import wird in regelmäßigen Abständen durch den One Identity Manager History Service ausgeführt. Konfigurieren und aktivieren Sie im Designer den Zeitplan „Prozessinformationen direkt importieren“.

Direktes Löschen der Aufzeichnungen in der One Identity Manager-Datenbank

Sollen die Aufzeichnungen einzelner Teilbereiche für einen gewissen Zeitraum in der One Identity Manager-Datenbank gehalten werden, jedoch keine spätere Archivierung erfolgen, dann haben Sie folgende Möglichkeiten:

- Um einen einzelnen Teilbereich von der Archivierung auszuschließen, konfigurieren Sie diesen Teilbereich nicht für den Export, sondern legen nur den Aufbewahrungszeitraum fest. Weitere Informationen finden Sie unter Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank auf Seite 13.
- Um alle Teilbereiche ohne Archivierung direkt zu löschen, legen Sie die Aufbewahrungszeiten fest. Aktivieren Sie im Designer den Konfigurationsparameter „Common\ProcessState\ExportPolicy“ und tragen Sie den Wert `NONE` ein.

Die Aufzeichnungen werden nach Ablauf der Aufbewahrungszeit durch den DBQueue Prozessor aus der One Identity Manager-Datenbank gelöscht. Zusätzlich werden alle Einträge für ausgelöste Aktionen gelöscht, zu denen es keine Aufzeichnungen in den Teilbereichen gibt.

ⓘ **HINWEIS:** Wenn Sie keine Aufbewahrungszeiten festlegen, werden die Aufzeichnungen dieser Teilbereiche innerhalb der täglichen Wartungsaufträge des DBQueue Prozessors aus der One Identity Manager-Datenbank gelöscht.

Über Dell

Dell berücksichtigt die Wünsche seiner Kunden und liefert auf der ganzen Welt innovative Technologien, Geschäftslösungen und Dienstleistungen, die anerkannt und geschätzt werden. Weitere Informationen finden Sie unter www.quest.com.

Kontaktaufnahme zu Dell

Bei Fragen zum Kauf von Dell Produkten oder anderen Fragen besuchen Sie http://quest.com/company/contact-us.aspx oder rufen Sie +1 949 754 8000 an.

Technische Supportressourcen

Der technische Support steht Kunden, die Dell-Software mit einem gültigen Wartungsvertrag gekauft haben, und Kunden zur Verfügung, die über eine Testversion verfügen. Das Support Portal ist unter https://support.quest.com/ erreichbar.

Das Support Portal stellt Selbsthilfetools bereit, mit denen Sie Probleme schnell und eigenständig lösen können – 24 Stunden am Tag, 365 Tage im Jahr. Darüber hinaus ermöglicht das Portal über ein Online-Serviceanforderungssystem auch direkten Zugang zu unseren Produktsupporttechnikern.

Das Portal bietet folgende Möglichkeiten:

- Erstellen, Aktualisieren und Verwalten von Serviceanforderungen (Supportfälle)
- Anzeigen von Knowledge Base-Artikeln
- Erhalten von Produktbenachrichtigungen
- Herunterladen von Software. Testsoftware finden Sie unter http://quest.com/trials.
- Anzeigen von Videos zur Vorgehensweise
- Teilnahme an Communitydiskussionen
- Chatten mit einem Supporttechniker

Index