One Identity Manager 8.1

Administrationshandbuch für die Datenarchivierung

Legende

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

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

WICHTIG, HINWEIS, TIPP, MOBIL, or VIDEO: Ein Informationssymbol weist auf Begleitinformationen hin.

One Identity Manager Administrationshandbuch für die Datenarchivierung
Aktualisiert - März 2019
Version - 8.1

Inhalt

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 One Identity Manager History Database übertragen. Diese One Identity Manager History Database stellt somit das Veränderungsarchiv dar. In der One Identity Manager History Database erfolgen statistische Auswertungen, die die Darstellungen von Trends oder Verläufen vereinfachen. Die Auswertung der historischen Daten erfolgt über die TimeTrace-Funktion oder über Berichte.

Inbetriebnahme einer One Identity Manager History Database

Bei der Inbetriebnahme einer History Database 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 One Identity Manager History Database zu erstellen.

Die Einrichtung einer Arbeitsumgebung für eine One Identity Manager History Database umfasst folgende Schritte:

- Einrichten einer administrativen Arbeitsstation
- Erstellen und Migrieren der One Identity Manager History Database
- Installieren und Konfigurieren eines One Identity Manager Service für die One Identity Manager History Database
- Bekanntgeben der Quelldatenbank
- Einrichten des Archivierungsverfahrens

Detaillierte Informationen zum Thema

- Einrichten einer administrativen Arbeitsstation auf Seite 14
- Berechtigungen für die One Identity Manager History Database auf Seite 5

- Hinweise zum Einsatz mehrerer SQL Server auf Seite 12
- Hinweise zur Nutzung der integrierten Windows-Authentifizierung auf Seite 14
- Installieren und Aktualisieren einer One Identity Manager History Database auf Seite 16
- Quelldatenbank in der One Identity Manager History Database bekanntgeben auf Seite 16
- Einrichten des Archivierungsverfahrens auf Seite 18

Berechtigungen für die One Identity Manager History Database

Für den Einsatz einer einer One Identity Manager History Database werden folgende Benutzer unterschieden.

Installationsbenutzer

Der Installationsbenutzer wird für die initiale Installation einer One Identity Manager History Database mit dem Configuration Wizard benötigt. Für den Installationsbenutzer müssen eine SQL Server Anmeldung und ein Datenbankbenutzer mit den folgenden Berechtigungen zur Verfügung gestellt werden.

SQL Server:

- Mitglied der Serverrolle **dbcreator**

  Die Serverrolle wird nur benötigt, wenn die Datenbank durch den Configuration Wizard erstellt wird.
- Mitglied der Serverrolle **securityadmin**

  Diese Serverrolle wird für die Erstellung der SQL Server Anmeldungen benötigt.
- Berechtigung **view server state** und Berechtigung **alter any connection** mit der Option **with grant option**

  Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.
- Berechtigung **alter any server role**

  Die Berechtigung wird benötigt, um die Serverrolle für den administrativen Benutzer zu erzeugen.

msdb-Datenbank:

- Berechtigung **Select** mit der Option **with grant option** für die Tabellen `dbo.sysjobs`, `dbo.sysjobschedules` und `dbo.sysjobactivity`

  Die Berechtigungen werden zum Ausführen und Überwachen von Datenbankschedules benötigt.
- Berechtigung **alter any user**

Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

master-Datenbank:

- Berechtigung **alter any user**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

- Berechtigung **Execute** mit der Option **with grant option** für die Prozedur `xp_readerrorlog`

  Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.

One Identity Manager History Database:

- Mitglied der Datenbankrolle **db_owner**

  Diese Datenbankrolle wird nur benötigt, wenn bei der Installation des Schemas mit dem Configuration Wizard eine vorhandene Datenbank verwendet werden soll.

Administrativer Benutzer

Der administrative Benutzer wird durch Komponenten des One Identity Manager verwendet, die Berechtigungen auf Serverebene und Datenbankebene benötigen, beispielsweise der Configuration Wizard, der DBQueue Prozessor oder der One Identity Manager Service.

Für den administrativen Benutzer werden während der Installation einer One Identity Manager History Database mit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMAdminRole_<DatabaseName>**
  - Berechtigung **alter any server role**

    Die Berechtigung wird benötigt, um die Serverrolle für den Konfigurationsbenutzer zu erzeugen.

  - Berechtigung **view any definition**

    Die Berechtigung wird benötigt, um die SQL Server Anmeldungen für den Konfigurationsbenutzer und den Endbenutzer mit den entsprechenden Datenbankbenutzern zu verbinden.
- SQL Server Anmeldung **<DatabaseName>_Admin**

- Mitglied der Serverrolle **OneIMAdminRole_<DatabaseName>**
- Berechtigung **view server state** und Berechtigung **alter any connection** mit der Option **with grant option**

  Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.

msdb-Datenbank:

- Datenbankrolle **OneIMRole_<DatabaseName>**
  - Mitglied der Datenbankrolle **SQLAgentUserRole**

    Die Datenbankrolle wird zum Ausführen von Datenbankschedules benötigt.
  - Berechtigung **Select** für die Tabellen `dbo.sysjobs`, `dbo.sysjobschedules` und `dbo.sysjobactivity`

    Die Berechtigungen werden zum Ausführen und Überwachen von Datenbankschedules benötigt.
- Datenbankbenutzer **OneIM_<DatabaseName>**
  - Mitglied der Datenbankrolle **OneIMRole_<DatabaseName>**
  - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

master-Datenbank:

- Datenbankrolle **OneIMRole_<DatabaseName>**
  - Berechtigung **Execute** für die Prozedur `xp_readerrorlog`

    Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.
- Datenbankbenutzer **OneIM_<DatabaseName>**
  - Mitglied der Datenbankrolle **OneIMRole_<DatabaseName>**
  - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

One Identity Manager History Database:

- Datenbankbenutzer **Admin**
  - Mitglied in Datenbankrolle **db_owner**

    Die Datenbankrolle wird benötigt, um eine Datenbank mit dem Configuration Wizard zu aktualisieren.
  - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

Konfigurationsbenutzer

Der Konfigurationsbenutzer kann Konfigurationsaufgaben innerhalb des One Identity Manager ausführen, beispielsweise mit dem Designer arbeiten. Konfigurationsbenutzer benötigen Berechtigungen auf Serverebene und Datenbankebene.

Für Konfigurationsbenutzer werden während der Installation einer One Identity Manager History Database mit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMConfigRole_<DatabaseName>**
  - Berechtigung **view server state** und Berechtigung **alter any connection**

    Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.
- SQL Anmeldung **<DatabaseName>_Config**
  - Mitglied der Serverrolle **OneIMConfigRole_<DatabaseName>**

One Identity Manager History Database:

- Datenbankrolle **OneIMConfigRoleDB**
  - Berechtigungen **Create Procedure**, **Delete**, **Select**, **Create table**, **Update**, **Checkpoint**, **Create View**, **Insert**, **Execute**, **Create function** auf die Datenbank
- Datenbankbenutzer **Config**
  - Mitglied der Datenbankrolle **OneIMConfigRoleDB**
  - Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_Config** verbunden.

Endbenutzer

Endbenutzer erhalten nur Berechtigungen auf Datenbankebene, um beispielsweise Aufgaben mit dem HistoryDB Manager zu erfüllen.

Für Endbenutzer werden während der Installation einer One Identity Manager History Database mit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- SQL Anmeldung **<DatabaseName>_User**

One Identity Manager History Database:

- Datenbankrolle **OneIMUserRoleDB**
  - Berechtigungen **Insert**, **Update**, **Select**, **Delete** auf ausgewählte Tabellen der Datenbank
  - Berechtigung **View Definition** auf die Datenbank
  - Berechtigungen **Execute** und **References** für einzelne Funktionen, Prozeduren und Typen
- Datenbankbenutzer **User**

- Mitglied der Datenbankrolle **OneIMUserRoleDB**
- Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_User** verbunden.

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.

Erweiterte Konfiguration für die Datenübernahme

Für die Datenübernahme gibt es folgende Szenarien:

- Szenario 1: One Identity Manager History Database und One Identity Manager-Datenbank befinden sich auf einem Datenbankserver.
- Szenario 2: One Identity Manager History Database und One Identity Manager-Datenbank befinden sich auf verschiedenen Datenbankservern. Der Verbindungsserver wird durch den One Identity Manager Service der One Identity Manager History Database erzeugt.
- Szenario 3: One Identity Manager History Database und One Identity Manager-Datenbank befinden sich auf verschiedenen Datenbankservern. Es wird ein Verbindungsserver bereitgestellt.

Szenario 1:

HINWEIS: Wenn Sie mit dem **sa** arbeiten, sind keine weiteren Schritte erforderlich.

Wenn Sie mit abgestuften Berechtigungen auf Serverebene und Datenbankebene arbeiten, erstellen Sie im Designer in der One Identity Manager-Datenbank einen Datenbankbenutzer für die Datenübernahme.

Um den Datenbankbenutzer in der One Identity Manager-Datenbank einzurichten

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Datenbankserverberechtigungen | Datenbankserver-Anmeldungen**.
2. Klicken Sie und erfassen Sie folgende Informationen:

   Anmeldename: SQL Server Anmeldung des Benutzers, mit dem die Prozessverarbeitung in der History Database (`DialogDatabase.ConnectionString`) erfolgt.

   Datenbankbenutzer: Name des Datenbankbenutzers.
3. Wählen Sie den Tabreiter **Datenbank- oder Serverrolle** und weisen Sie die Rolle **Datenbank: Rolle für Datenarchivierung** zu.
4. Speichern Sie die Änderungen.

Der DBQueue Prozessor erzeugt in der One Identity Manager-Datenbank die Datenbankrolle **OneIMHistoryRoleDB** und den Datenbankbenutzer. Der Datenbankbenutzer wird mit der SQL Server Anmeldung verbunden und in die Datenbankrolle aufgenommen.

Szenario 2:

HINWEIS: Wenn Sie mit dem **sa** arbeiten, sind keine weiteren Schritte erforderlich.

Wenn Sie mit abgestuften Berechtigungen auf Serverebene und Datenbankebene arbeiten, sind zusätzliche Berechtigungen zum Erstellen eines Verbindungsservers und für die Datenübernahme erforderlich.

- Um einen Verbindungsserver zu erstellen, benötigt der Benutzer, mit dem die Prozessverarbeitung in der History Database (`DialogDatabase.ConnectionString`) erfolgt, die folgenden Berechtigungen auf Serverebene:
  - Berechtigung **alter any linked server**

    Die Berechtigung wird zum Erstellen und Löschen eines Verbindungsservers benötigt. Der Verbindungsserver ermöglicht die Ausführung verteilter Abfragen.
  - Berechtigung **alter any login**

    Die Berechtigung wird zum Erstellen und Löschen einer Zuordnung von Anmeldenamen auf dem lokalen Server und einem Anmeldenamen auf dem Verbindungsserver benötigt.
- Erstellen Sie auf dem Datenbankserver, auf dem die One Identity Manager-Datenbank liegt, eine SQL Server Anmeldung für die Datenübernahme.
- Erstellen Sie im Designer in der One Identity Manager-Datenbank einen Datenbankbenutzer.

Um den Datenbankbenutzer in der One Identity Manager-Datenbank einzurichten

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Datenbankserverberechtigungen | Datenbankserver-Anmeldungen**.
2. Klicken Sie und erfassen Sie folgende Informationen:

   Anmeldename: SQL Server Anmeldung für die Datenübernahme.

   Datenbankbenutzer: Datenbankbenutzer.
3. Wählen Sie den Tabreiter **Datenbank- oder Serverrolle** und weisen Sie die Rolle **Datenbank: Rolle für Datenarchivierung** zu.
4. Speichern Sie die Änderungen.

Der DBQueue Prozessor erzeugt in der One Identity Manager-Datenbank die Datenbankrolle **OneIMHistoryRoleDB** und den Datenbankbenutzer. Der Datenbankbenutzer wird mit der SQL Server Anmeldung verbunden und in die Datenbankrolle aufgenommen.

Szenario 3:

- Erstellen Sie auf dem Datenbankserver, auf dem die One Identity Manager-Datenbank liegt, eine SQL Server Anmeldung für die Datenübernahme.
- Erstellen Sie im Designer in der One Identity Manager-Datenbank einen Datenbankbenutzer.

  Um den Datenbankbenutzer in der One Identity Manager-Datenbank einzurichten

  1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Datenbankserverberechtigungen | Datenbankserver-Anmeldungen**.
  2. Klicken Sie und erfassen Sie folgende Informationen:

     Anmeldename: SQL Server Anmeldung für die Datenübernahme.

     Datenbankbenutzer: Datenbankbenutzer.
  3. Wählen Sie den Tabreiter **Datenbank- oder Serverrolle** und weisen Sie die Rolle **Datenbank: Rolle für Datenarchivierung** zu.
  4. Speichern Sie die Änderungen.

  Der DBQueue Prozessor erzeugt in der One Identity Manager-Datenbank die Datenbankrolle **OneIMHistoryRoleDB** und den Datenbankbenutzer. Der Datenbankbenutzer wird mit der SQL Server Anmeldung verbunden und in die Datenbankrolle aufgenommen.
- Richten Sie den Verbindungsserver ein und referenzieren Sie die SQL Server Anmeldung für die Datenübernahme.

  Um einen Verbindungsserver bereitzustellen, wird empfohlen, die SQL Prozeduren `sp_addlinkedserver`, `sp_setNetname` und `sp_addlinkedsrvlogin` zu nutzen.

- Halten Sie den Namen des Verbindungsserver bereit. Diesen benötigen Sie bei Bekanntgabe der Quelldatenbank in der One Identity Manager History Database.
- Aktivieren Sie in der One Identity Manager History Database den Konfigurationsparameter **HDB | UseNamedLinkedServer**.

Hinweise zum Einsatz mehrerer SQL Server

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

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

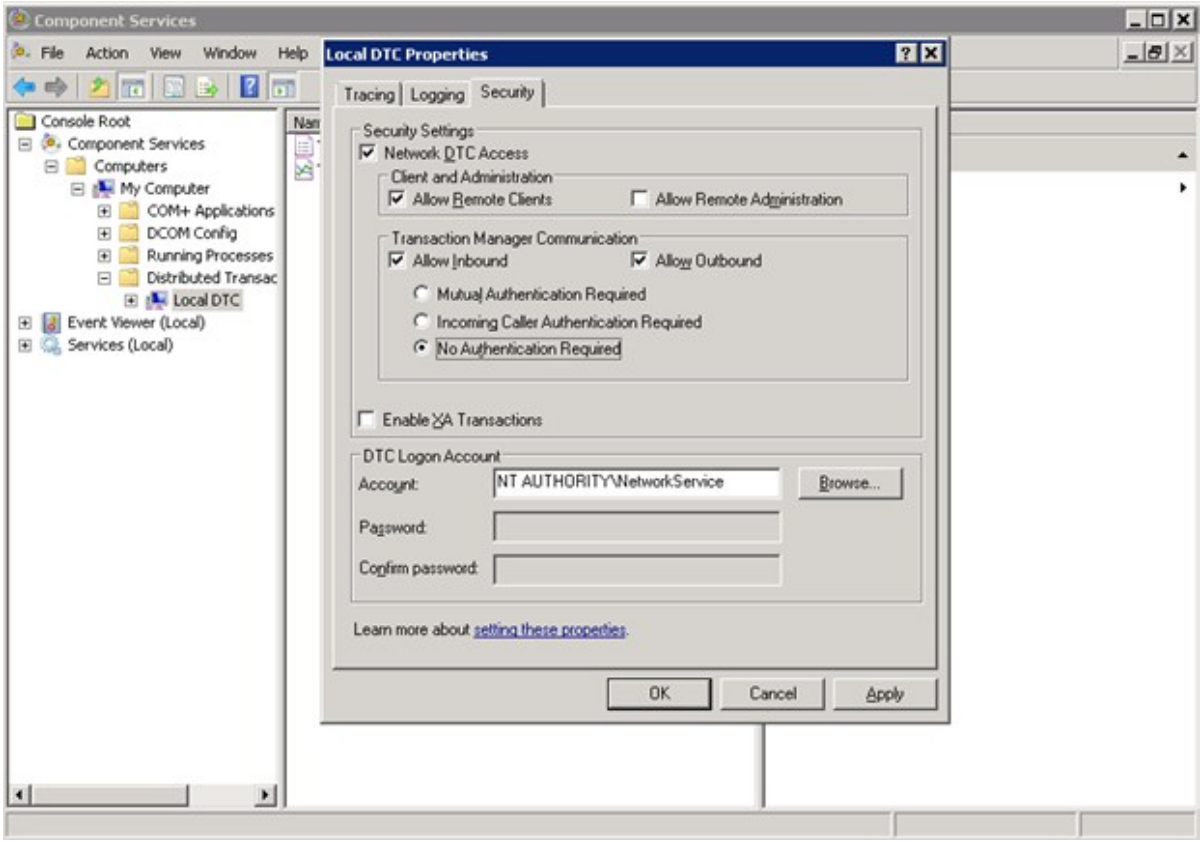
- Start der Dienste **Microsoft Distributed Transaction Coordinator**(DTC), **RPC Client** und **Security Accounts Manager**
- Für die Netzwerkkommunikation zwischen den Servern prüfen Sie die Einstellungen der Firewall und passen Sie bei Bedarf die Einstellungen entsprechend der Empfehlungen des eingesetzten 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 One Identity Manager History Database 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
```

Hinweise zur Nutzung der integrierten Windows-Authentifizierung

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

- Für das Benutzerkonto richten Sie auf dem Datenbankserver eine SQL Server Anmeldung ein. Befinden sich One Identity Manager History Database 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 Berechtigungen für die One Identity Manager History Database auf Seite 5.

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

- Das Benutzerkonto des One Identity Manager 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 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>
  ```

Einrichten einer administrativen Arbeitsstation

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

Auf einer administrativen Arbeitsstation sollten Sie mindestens folgende Werkzeuge installieren:

- HistoryDB Manager
- Job Queue Info
- Configuration Wizard
- Designer

Auf der Arbeitsstation, auf der die Installation und Aktualisierung des One Identity Manager History Database Schemas gestartet wird, müssen zusätzlich die folgenden Voraussetzungen erfüllt sein:

- Installation des Configuration Wizard
- Zugriff auf die Installationsquellen

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

Die Erstinstallation der One Identity Manager History Database-Werkzeuge auf den Arbeitsstationen nehmen Sie mit dem Installationsassistenten vor.

Um die Komponenten zu installieren

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Wechseln Sie auf den Tabreiter **Andere Produkte,** wählen Sie den Eintrag **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 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 One Identity Manager History Database 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 One Identity Manager History Database Schemas starten.

7. Um den Installationsassistenten zu beenden, klicken Sie **Ende**.
8. Schließen Sie das Autorun Programm.

Installieren und Aktualisieren einer One Identity Manager History Database

One Identity Manager-Datenbank und One Identity Manager History Database müssen den gleichen Versionsstand haben.

Die Installation und Aktualisierung einer One Identity Manager History Database ist ähnlich der Installation einer One Identity Manager-Datenbank. Die One Identity Manager History Database richten Sie mit dem Configuration Wizard ein. Der Configuration Wizard führt die folgenden Schritte aus.

1. Installieren des One Identity Manager History Database Schemas in eine Datenbank.

   Der Configuration Wizard kann eine neue Datenbank erstellen und das Schema installieren. Alternativ kann das Schema in eine bereits bestehende Datenbank installiert werden.
2. Erstellen der erforderlichen SQL Server Anmeldungen und Datenbankbenutzer mit den Berechtigungen für den administrative Benutzer, Konfigurationsbenutzer und Endbenutzer.
3. Erstellen der administrativen Systembenutzer und Rechtegruppen.
4. Installieren und Konfigurieren des One Identity Manager Service mit direktem Zugriff auf die One Identity Manager History Database für die Verarbeitung von SQL Prozessen.

Ausführliche Informationen zu den Systemvoraussetzungen, zur Installation und Aktualisierung einer Datenbank finden Sie *One Identity Manager Installationshandbuch*.

Quelldatenbank in der One Identity Manager History Database bekanntgeben

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

Um die Quelldatenbank bekanntzugeben

1. Starten Sie den HistoryDB Manager und geben Sie die Verbindungsdaten an.
2. Wählen Sie die Kategorie **Historie | Basisdaten | Quelldatenbanken**.
3. Wählen Sie in der Ergebnisliste die Quelldatenbank aus und bearbeiten Sie die Stammdaten.

Tabelle 1: 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`
	HINWEIS: Wenn Sie einen Verbindungsserver bereitstellen, tragen Sie den Namen des Verbindungsservers ein. Weitere Informationen finden Sie unter Erweiterte Konfiguration für die Datenübernahme auf Seite 9.

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 Service. Für den Einsatz dieses Authentifizierungsverfahrens sind bestimmte Installationsvoraussetzungen zu beachten. Weitere Informationen finden Sie unter Installieren und Aktualisieren einer One Identity Manager History Database auf Seite 16.
Datenbankbenutzer	SQL Server Anmeldung des Benutzers für die Datenübernahme.

Eigenschaft	Bedeutung
	Diese Angabe ist nur erforderlich, wenn sich One Identity Manager History Database und One Identity Manager-Datenbank auf unterschiedlichen Servern befinden und kein Verbindungsserver bereitgestellt wird. Weitere Informationen finden Sie unter Erweiterte Konfiguration für die Datenübernahme auf Seite 9.
Kennwort	Kennwort zur SQL Server Anmeldung. Diese Angabe ist nur erforderlich, wenn sich One Identity Manager History Database und One Identity Manager-Datenbank auf unterschiedlichen Servern befinden und kein Verbindungsserver bereitgestellt wird. Weitere Informationen finden Sie unter Erweiterte Konfiguration für die Datenübernahme auf Seite 9.
Beginn und Ende der Aufzeichnungen	Diese Datumsangaben werden beim Import der Aufzeichnungen automatisch gesetzt und aktualisiert.

4. Speichern Sie die Änderungen.

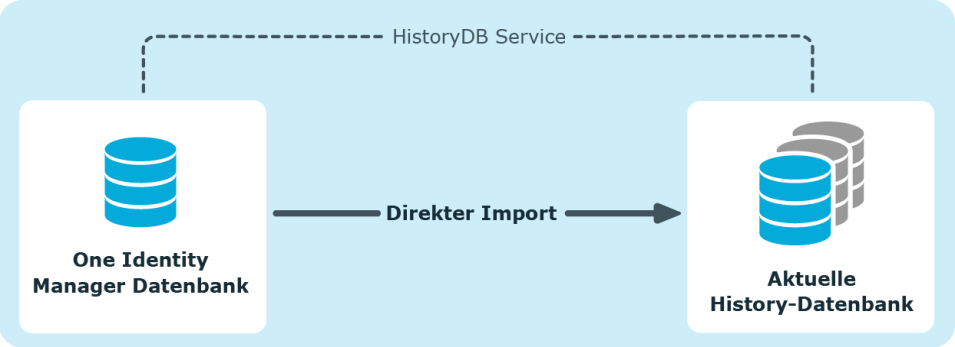
Einrichten des Archivierungsverfahrens

Alle im One Identity Manager protokollierten Aufzeichnungen werden zunächst in der One Identity Manager-Datenbank gespeichert. Der Anteil der historisierten Daten am Gesamtvolumen einer One Identity Manager-Datenbank sollte maximal 25 % betragen. Anderenfalls kann es zu Performance-Problemen kommen. Die Aufzeichnungen sollten in regelmäßigen Abständen aus der One Identity Manager-Datenbank entfernt und archiviert werden.

Um die aufgezeichneten Daten 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 One Identity Manager History Database 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 One Identity Manager History Database 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 eine One Identity Manager History Database



Für die direkte Übernahme in eine History Database 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 One Identity Manager History Database 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 in eine One Identity Manager History Database sind in beiden Datenbanken - der One Identity Manager-Datenbank und der One Identity Manager History Database - 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 2: Zulässige Werte des Konfigurationsparameters Common | ProcessState | ExportPolicy

Wert	Bedeutung
HDB	Die Daten werden nach Ablauf einer festgelegten Zeitspanne direkt in eine One Identity Manager History Database 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 3: Konfigurationsparameter für die Behandlung der aufgezeichneten Datenänderungen

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

Tabelle 4: Konfigurationsparameter für die Behandlung der Prozessinformationen

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

Tabelle 5: Konfigurationsparameter für die Behandlung der Prozesshistorie

Konfigurationsparameter	Bedeutung
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.
Common | ProcessState |	Mit diesem Konfigurationsparameter wird die maximale

Konfigurationsparameter	Bedeutung
JobHistory | LifeTime	Aufbewahrungszeit für Aufzeichnungen aus der Prozesshistorie in der Datenbank festgelegt.

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 One Identity Manager History Database 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 One Identity Manager History

Zeitpunkt	Prozessinformationen	Prozesshistorie	Datenänderungen
			Database übernommen und anschließend in der One Identity Manager-Datenbank gelöscht.

Beispiel 2

Die Aufzeichnungen werden direkt in eine One Identity Manager History Database 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 One Identity Manager History Database übernommen und anschließend in der One Identity Manager-Datenbank gelöscht.

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.
- Prüfen Sie im Designer den Wert der Konfigurationsparameters **Common | ProcessState | PackageSizeHDB**. Dieser Parameter legt die maximale Anzahl der, in die History Database zu übertragenden, Prozessgruppen fest. Der Standardwert ist **10000**.

One Identity Manager History Database:

- Geben Sie die One Identity Manager-Datenbank in der One Identity Manager History Database als Quelldatenbank bekannt.
- Der Import wird in regelmäßigen Abständen durch den One Identity Manager Service der One Identity Manager History Database ausgeführt. Konfigurieren und aktivieren Sie im Designer den Zeitplan **Prozessinformationen direkt importieren**.

Verwandte Themen

- Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank auf Seite 19
- Quelldatenbank in der One Identity Manager History Database bekanntgeben auf Seite 16

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.
- 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 Prozessor aus der One Identity Manager-Datenbank gelöscht.

Bei großen Datenmengen können Sie zur Performance-Optimierung die Menge der zu löschenden Objekte pro Operation und Verarbeitungslauf des DBQueue Prozessor festlegen. Die Festlegung für die einzelnen Bereiche treffen Sie über Konfigurationsparameter.

Tabelle 6: Konfigurationsparameter für das Löschen der aufgezeichneten Datenänderungen

Konfigurationsparameter	Bedeutung
Common | ProcessState | PropertyLog | Delete	Der Konfigurationsparameter erlaubt die Konfiguration des Löschverhaltens für aufgezeichnete Datenänderungen.
Common | ProcessState | PropertyLog | Delete | BulkCount	Der Konfigurationsparameter enthält die Anzahl der Einträge, die in einer Operation gelöscht werden sollen.
Common | ProcessState | PropertyLog | Delete | TotalCount	Der Konfigurationsparameter enthält die Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen.

Tabelle 7: Konfigurationsparameter für das Löschen der Prozessinformationen

Konfigurationsparameter	Bedeutung
Common | ProcessState | ProgressView | Delete	Der Konfigurationsparameter erlaubt die Konfiguration des Löschverhaltens für Prozessinformationen .
Common | ProcessState | ProgressView | Delete | BulkCount	Der Konfigurationsparameter enthält die Anzahl der Einträge, die in einer Operation gelöscht werden sollen.
Common | ProcessState | ProgressView | Delete | TotalCount	Der Konfigurationsparameter enthält die Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen.

Tabelle 8: Konfigurationsparameter für das Löschen der Prozesshistorie

Konfigurationsparameter	Bedeutung
Common | ProcessState | JobHistory | Delete	Der Konfigurationsparameter erlaubt die Konfiguration des Löschverhaltens für die Prozesshistorie.
Common | ProcessState |	Der Konfigurationsparameter enthält die Anzahl der

Konfigurationsparameter	Bedeutung
JobHistory | Delete | BulkCount	Einträge, die in einer Operation gelöscht werden sollen.
Common | ProcessState | JobHistory | Delete | TotalCount	Der Konfigurationsparameter enthält die Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen.

Tabelle 9: Konfigurationsparameter für das Löschen von Prozessstatus-Einträge

Konfigurationsparameter	Bedeutung
Common | ProcessState | Delete	Der Konfigurationsparameter erlaubt die Konfiguration des Löschverhaltens für die Einträge zum Prozessstatus.
Common | ProcessState | Delete | BulkCount	Der Konfigurationsparameter enthält die Anzahl der Einträge, die in einer Operation gelöscht werden sollen.
Common | ProcessState | Delete | TotalCount	Der Konfigurationsparameter enthält die Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen.

Verwandte Themen

- Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank auf Seite 19

Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen besuchen Sie https://www.oneidentity.com/company/contact-us.aspx oder rufen Sie + 1-800-306-9329 an.

Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

Index