

Symantec Enterprise Vault™

Technical Note

Housekeeping for the Monitoring
database

8.0 or later

Symantec Enterprise Vault: Housekeeping for the Monitoring database

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated: 2013-01-15.

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Enterprise Vault, Compliance Accelerator, and Discovery Accelerator are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the *Third Party Software* file accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street, Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

<http://support.symantec.com>

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

<http://support.symantec.com>

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our Technical Support web page at the following URL:

<http://support.symantec.com>

Customer service

Customer service information is available at the following URL:

<http://support.symantec.com>

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Housekeeping for the Monitoring database

This document includes the following topics:

- [About housekeeping for the Monitoring database](#)
- [Assigning the roles and permissions to the Vault Service account](#)
- [Manually running the purge job SQL script file](#)

About housekeeping for the Monitoring database

If you do not assign some additional roles and permissions to the Vault Service account before you run the Enterprise Vault Configuration wizard for the first time, the wizard fails to create a SQL purge job for the Monitoring database history records. Upon completion, the Configuration wizard logs an event log error with the category "Monitoring Configuration Utility", and Event ID 41123. The error description begins as follows:

```
Monitoring Configuration Utility reported error: SQL Error at: --
```

The error description then lists the contents of a purge job SQL script file.

Without the SQL purge job, the history records for the Monitoring database continue to grow.

This technical note describes:

- How to assign to the Vault Service account the roles and permissions that are required to create the purge job. Ideally you should perform these steps before you run the Enterprise Vault Configuration wizard for the first time.

- How to manually create the SQL purge job if you did not assign the additional permissions before you ran the Enterprise Vault Configuration wizard for the first time.

Note: From Enterprise Vault 10.0.3, you can limit the Vault Service account's SQL privileges to increase database security. The Enterprise Vault databases contain a set of roles that enable you to assign to the Vault Service account only those SQL privileges that are required to run Enterprise Vault. However, if you limit the SQL privileges of the Vault Service account for normal daily operations, you may need to grant additional SQL privileges to the account for other tasks that require higher privileges.

For more information on using the SQL Server roles, see the following article on the Symantec Support website: <http://www.symantec.com/docs/HOWTO80670>.

Assigning the roles and permissions to the Vault Service account

Unless you assign the SQL system administrator (sysadmin) role to the Vault Service account, you must perform a number of steps to configure the Vault Service account.

In brief, you must do as follows:

- Add the Vault Service account as an msdb system database user.
- Grant the Vault Service account Select permissions on the msdb tables `sysjobs`, `sysjobschedules`, `sysjobobservers`, and `sysjobsteps`.
- If you use Microsoft SQL Server 2005 or later, assign the database role `SQLAgentUserRole` to the Vault Service account.

Follow the appropriate procedure for your version of Microsoft SQL Server.

Steps for Microsoft SQL Server 2000

- 1 On the SQL Server computer, start **Enterprise Manager** for SQL 2000.
- 2 Select the required SQL Server
- 3 Expand the **Databases** container and then expand the **msdb** container.
- 4 Right-click **Users**, and select **New Database User**.
- 5 In the **Login name** box, enter the domain and the user name of the Vault Service account, in the form `domain\user_name`.
- 6 In the **User name** box, enter a new user name.

- 7 Click **OK**.
- 8 Right-click the new user that you have just created, and then click **Properties**.
- 9 Click **Permissions**, and grant SELECT permission for the following objects:
 - sysjobs
 - sysjobschedules
 - sysjobservers
 - sysjobsteps
- 10 By default, the public role has execute permission on the following stored procedures. Grant execute permission on these procedures if it is not already granted:
 - sp_add_job
 - sp_add_jobschedule
 - sp_add_jobserver
 - sp_add_jobstep

Steps for Microsoft SQL Server 2005 and 2008

- 1 On the SQL Server computer, start SQL Server Management Studio.
- 2 Select the required SQL Server.
- 3 Browse to **Databases > System Databases > msdb > Security > Users**.
- 4 Right-click **Users**, and then click **New User**.
- 5 In the **User name** box, enter a new user name
- 6 In the **Login name** box, enter the domain and the user name of the Vault Service account, in the form `ddomain\user_name`.
- 7 Click **OK**.
- 8 Right-click the new user that you have just created, and then click **Properties**.
- 9 Add the following msdb tables to the list of securables, and then grant Select permission for them to the Vault Service account:
 - sysjobs
 - sysjobschedules
 - sysjobservers
 - sysjobsteps

- 10 Browse to **Databases > System Databases > msdb > Security > Roles > Database Roles**.
- 11 Right-click **SQLAgentUserRole**, and then click **Properties**.
- 12 On the **General** page, click **Add**, and then select the Vault Service account that you have just created.

Manually running the purge job SQL script file

Use the following procedure to manually create the SQL job to perform the purging of the Monitoring database history records.

Note: This procedure is only required if you did not assign the additional roles and permissions to the Vault Service account before you ran the Enterprise Vault Configuration wizard for the first time.

To run the purge job SQL script file

- 1 Make sure that you have set up the appropriate permissions for the Vault Service account.
See [“Assigning the roles and permissions to the Vault Service account”](#) on page 8.
- 2 Make sure that the status of the SQL Server Agent service is "Started" for the SQL Server that hosts the Enterprise Vault Monitoring database.
- 3 Start Query Analyzer for Microsoft SQL Server 2000, or SQL Server Management Studio for Microsoft SQL Server 2005 or 2008.
- 4 From the **File** menu, open the file **EVOMDB_7_PurgeJob.sql** in the Enterprise Vault installation folder, typically `C:\Program Files\Enterprise Vault`.
- 5 Press **F5**, or select **Query > Execute** to execute the SQL script.
After a short time, SQL Query Analyzer or SQL Server management Studio should indicate that the command completed successfully.