Veritas Enterprise Vault™ Technical Note

Using SQL Database Roles in Enterprise Vault, Compliance Accelerator, and Discovery Accelerator

10.0.3, 10.0.4, 11.0 and 11.0.1

VERITAS™

Veritas Enterprise Vault: Using SQL Database Roles in Enterprise Vault, Compliance Accelerator, and Discovery Accelerator

Last updated: 2016-06-13.

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

http://www.veritas.com/docs/000095758

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

http://www.veritas.com/docs/000001907

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

evdocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community

Contents

Chapter 1

About this guide

This chapter includes the following topics:

Introducing this guide

Version 10.0.3 of Enterprise Vault, Compliance Accelerator, and Discovery Accelerator introduced database roles that you can use to improve SQL database security.

This document describes how to revoke the SQL database permissions that the Vault Service account does not need, and how to use the database roles to grant only the permissions needed for normal daily operations, and additional permissions when they are required.

The installation and configuration of Enterprise Vault, Compliance Accelerator, or Discovery Accelerator must be complete before you use the procedures in this document.

Note the following:

- This document applies to Enterprise Vault 10.0.3 through 11.0.1 only. For earlier versions of Enterprise Vault, see the following page of the Veritas Support website:
  http://www.veritas.com/docs/000036365
- If you want to use Compliance Accelerator 12 with Enterprise Vault 11.0.1, or Discovery Accelerator 12 with Enterprise Vault 11.0 or 11.0.1, then it is important to read the 12-specific version of the *Using SQL Database Roles* document as well as this version for 10.0.3 through 11.0.1. Both versions of the document are available from the following page of the Veritas Support website:
  http://www.veritas.com/docs/000070503

Chapter 2

Using Enterprise Vault database roles

This chapter includes the following topics:

About Enterprise Vault database roles

The Enterprise Vault databases contain roles which you can use to increase the database security in your environment.

Standard Enterprise Vault installation and upgrade procedures do not use these roles. When you have completed the installation or upgrade of Enterprise Vault, the Vault Service account is the owner of all Enterprise Vault databases and has a high level of privilege on the SQL server.

Use the procedures in this chapter to do the following:

- Configure the Vault Service account with only the SQL privileges that are required for normal daily operations.
  See "Configuring the Vault Service account for normal operations" on page 9.
- Grant temporary additional SQL privileges to the Vault Service account for other tasks that require higher privileges.
  See "Configuring the Vault Service account for operations that require elevated privileges" on page 13.

Note: Before you use the procedures in this chapter, you must have completed the installation or upgrade of Enterprise Vault, and its configuration.

Table 2-1 lists the Enterprise Vault database roles and describes the purpose of each.

Table 2-1 Enterprise Vault database roles

Role	Used in these databases	For these operations
EVAdminRole	Directory Vault store Vault store group (fingerprint)	Assign the Vault Service account to EVAdminRole for all administrative operations, such as the creation of vault store partitions, and all EVSVR operations. Revoke the Vault Service account's membership of EVAdminRole when you have completed the administrative operations.
EVMonitoringOperator	msdb system database	Assign the Vault Service account to EVMonitoringOperator for all normal operations.
EVReportingRole	Audit Directory Monitoring Reporting Vault store Vault store group (fingerprint)	Assign the Vault Service account or the reporting user to EVReportingRole for all reporting operations. This allows the collection of the data required in Enterprise Vault reports.
EVRuntimeRole	Audit Directory Monitoring Reporting Vault store Vault store group (fingerprint)	Assign the Vault Service account to EVRuntimeRole for all normal operations.

Table 2-1 Enterprise Vault database roles *(continued)*

Role	Used in these databases	For these operations
EVUpgradeRole	Audit Directory Monitoring Vault store Vault store group (fingerprint)	Assign the Vault Service account to EVUpgradeRole before upgrading Enterprise Vault. Revoke the Vault Service account's membership of EVUpgradeRole when you have completed the upgrade.

The installation or upgrade of Enterprise Vault automatically creates these roles in the databases where they are required, except for the Enterprise Vault auditing database and the msdb system database.

The procedures in this chapter include the steps required to create the database roles in the auditing database and the msdb system database.

Configuring the Vault Service account for normal operations

Table 2-2 introduces the tasks you must complete to configure the Vault Service account with only the privileges it requires for normal daily operations.

Table 2-2 Configuring the Vault Service account for normal operations

Task	See this section for more details
Prepare to configure the Vault Service account	See "Preparing to configure the Vault Service account" on page 10.
Configure the Vault Service account's SQL login	See "Configuring the Vault Service account's SQL login" on page 10.
Upgrade the Enterprise Vault auditing database	See "Upgrading the audit database" on page 11.
Change ownership of the Enterprise Vault databases	See "Changing ownership of Enterprise Vault databases" on page 11.
Assign Vault Service account to EVRuntimeRole	See "Assigning the Vault Service account to EVRuntimeRole" on page 12.

Table 2-2 Configuring the Vault Service account for normal operations *(continued)*

Task	See this section for more details
Map the Vault Service account to the msdb system database	See "Mapping the Vault Service account to the msdb system database" on page 12.
Create the EVMonitoringOperator role in the msdb system database and assign Vault Service account	See "Creating EVMonitoringOperator in the msdb system database and assigning Vault Service account" on page 13.
Restart Enterprise Vault services.	See "Restarting Enterprise Vault services" on page 13.

Preparing to configure the Vault Service account

Before you complete the procedures in this chapter:

- Choose an account other than the Vault Service account under which to complete the procedures in the chapter. For example, you could use the SQL System Administrator (sa) account, or another privileged user that is assigned to the sysadmin fixed server role.
- Ensure that your Enterprise Vault backups are up to date. See "Backing up Enterprise Vault" in the*Administrator's Guide*.
- Stop all Enterprise Vault services.

Configuring the Vault Service account's SQL login

Use this procedure to take away the elevated SQL privileges that are assigned to the Vault Service account in a normal installation of Enterprise Vault, then assign only the reduced privileges that are required for normal daily operations.

To configure Vault Service account's SQL login

1. Connect to the SQL server using SQL Server Management Studio.
2. In **Object Explorer**, under **Security** > **Logins**, double-click the Vault Service account.
3. In the **Login Properties** dialog box, select the **Server Roles** page.
4. Under **Server roles**, clear the **dbcreator** and **sysadmin** options, check that only the **public** option is selected, and then click **OK**.
5. In **Object Explorer**, right-click the top-level server instance, and click **Properties**.

6. In the **Server Properties** dialog box, select the **Permissions** page.
7. Under **Logins or roles**, select the Vault Service account.
8. On the **Explicit** tab, select the **Grant** option for **Create any database**, **View server state**, and **Alter any login**, and then click **OK**.

Upgrading the audit database

In a new installation of Enterprise Vault 10.0.3 and later, the auditing database already contains the Enterprise Vault database roles. However, if you upgrade Enterprise Vault from a version earlier than 10.0.3, you must use this procedure to upgrade the auditing database.

To upgrade the auditing database

1. Connect to the SQL server using SQL Server Management Studio.
2. In **Object Explorer**, click **Databases** > **EnterpriseVaultAudit**.
3. From the **File** menu, click **Open** > **File**.
4. In the **OpenFile** dialog box, browse to the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`) and open `AuditDBRoles.sql`.
5. From the **Query** menu, click **Execute**, and wait for the script to complete.

Changing ownership of Enterprise Vault databases

After a normal installation or upgrade of Enterprise Vault, the Vault Service account owns all Enterprise Vault's databases. As a result, the Vault Service account is a member of the db_owner fixed database role, which is not required for normal daily operations.

Use the following procedure and run one of these queries against each Enterprise Vault database, to assign ownership to another privileged user. Choose the procedure that is appropriate for your version of SQL Server.

```
use EVDatabase
GO
ALTER AUTHORIZATION ON DATABASE:: EVDatabase TO [domain\privileged_user];
```

or

```
use EVDatabase
GO
EXECUTE sp_changedbowner 'domain\privileged_user'
```

where:

EVDatabase is the name of the Enterprise Vault database.

domain\privileged_user is the privileged user and the domain to which it belongs.

To change ownership of Enterprise Vault databases

1. Connect to the SQL server using SQL Server Management Studio.
2. Click **New Query** and then enter the query in the query editor window.
3. From the **Query** menu, click **Execute**, and then wait for the script to complete.
4. Repeat this procedure for all the other Enterprise Vault databases.

Assigning the Vault Service account to EVRuntimeRole

Use this procedure to assign the Vault Service account to EVRuntimeRole in all the Enterprise Vault databases. This grants the Vault Service account all the privileges it requires in Enterprise Vault databases for normal daily operations.

To assign the Vault Service account to EVRuntimeRole in all the Enterprise Vault databases

1. Connect to the SQL server using SQL Server Management Studio.
2. In **Object Explorer**, under **Security** > **Logins**, double-click the Vault Service account.
3. In the **Login Properties** dialog box, select the **Server Roles** page.
4. Check that only the **public** option is selected.
5. Select the **User Mapping** page.
6. For each Enterprise Vault database, do the following:
   - Under **Users mapped to this login**, select the **Map** option.
   - Under **Database role membership for**, select the **EVRuntimeRole** option.
7. Click **OK** to save the changes.

Mapping the Vault Service account to the msdb system database

Use this procedure to map the Vault Service account to the msdb system database.

To map the Vault Service account to the msdb system database

1. Connect to the SQL server using SQL Server Management Studio.
2. In **Object Explorer**, under **Security** > **Logins**, double-click the Vault Service account.

3 In the **Login Properties** dialog box, select the **User Mapping** page.

4 Select the **Map** option for the msdb system database.

5 Click **OK** to save the changes.

Creating EVMonitoringOperator in the msdb system database and assigning Vault Service account

Use this procedure to do the following:

- Create the EVMonitoringOperator role in the msdb system database.
- Assign the Vault Service account to the EVMonitoringOperator role.

To create the EVMonitoringOperator role and assign Vault Service account

1 Connect to the SQL server using SQL Server Management Studio.

2 Click **New Query** and then enter the following query in the query editor window:

```
USE MSDB
GO
CREATE ROLE EVMonitoringOperator AUTHORIZATION dbo
exec sp_addrolemember SQLAgentUserRole, EVMonitoringOperator
GRANT SELECT ON sysjobs TO EVMonitoringOperator
GRANT SELECT ON sysjobschedules TO EVMonitoringOperator
GRANT SELECT ON sysjobsteps TO EVMonitoringOperator
GRANT SELECT ON sysjobservers TO EVMonitoringOperator
EXEC sp_addrolemember N'EVMonitoringOperator', N'domain\vsa'
GO
```

where *domain\vsa* is the Vault Service account and the domain to which it belongs.

3 From the **Query** menu, click **Execute**, and then wait for the script to complete.

Restarting Enterprise Vault services

When you have completed these procedures, restart all the Enterprise Vault services.

Configuring the Vault Service account for operations that require elevated privileges

In addition to the SQL privileges that the Vault Service account requires for normal daily operations, you can assign temporary, elevated privileges for other operations such as Enterprise Vault upgrades.

Table 2-1 lists the Enterprise Vault database roles and describes the operations for which each is required. For example, for an Enterprise Vault upgrade, use the following procedure to assign the Vault Service account to the EVUpgradeRole.

To assign the Vault Service account to EVUpgradeRole

1. Stop all Enterprise Vault services.
2. Connect to the SQL server using SQL Server Management Studio.
3. In **Object Explorer**, under **Security** > **Logins**, double-click the Vault Service account.
4. In the **Login Properties** dialog box, select the **Server Roles** page.
5. Check that only the **public** option is selected.
6. Select the **User Mapping** page.
7. For each Enterprise Vault database, do the following:
   - Under **Users mapped to this login**, select the **Map** option.
   - Under **Database role membership for**, select the **EVUpgradeRole** option.
8. Click **OK** to save the changes.
9. Restart all Enterprise Vault services.

In this example, the Vault Service account must be assigned to EVUpgradeRole for the duration of the upgrade.

When the upgrade is complete, use the same procedure to revoke the assignment, by clearing the **EVUpgradeRole** option in step 7.

Chapter 3

Using Compliance Accelerator and Discovery Accelerator roles

This chapter includes the following topics:

About Compliance Accelerator and Discovery Accelerator database roles

Compliance Accelerator and Discovery Accelerator use databases roles which you can use to increase the database security in your environment.

Standard Compliance Accelerator and Discovery Accelerator installation and upgrade procedures do not use these roles. When you have completed the installation or upgrade, the Vault Service account is the owner of all Compliance Accelerator and Discovery Accelerator databases and has a high level of privilege on the SQL server.

Use the procedures in this chapter to do the following:

- Configure the Vault Service account with only the SQL privileges that are required for normal daily operations.
  See "Configuring the Vault Service account for normal operations" on page 17.

- Grant temporary additional SQL privileges to the Vault Service account for other tasks that require higher privileges.
  See "Configuring the Vault Service account for operations that require elevated privileges" on page 23.

Note: Before you use the procedures in this chapter, you must have completed the installation or upgrade, and subsequent configuration of Compliance Accelerator and Discovery Accelerator.

Table 3-1 lists the Compliance Accelerator and Discovery Accelerator database roles and describes the purpose of each.

Table 3-1 Compliance Accelerator and Discovery Accelerator database roles

Role	Used in these databases	For these operations
EVAdminRole	Discovery Compliance	Assign the Vault Service account to EVAdminRole for all administrative operations Revoke the Vault Service account's membership of EVAdminRole when you have completed the administrative operations.
EVAnalyticsOperator	msdb system database	Assign the Vault Service account for Analytics operations.
EVRuntimeRole	Compliance Configuration Custodian Manager Discovery	Assign the Vault Service account to EVRuntimeRole for all normal operations.
EVScheduledSearchOperator	msdb system database	Assign the Vault Service account to support scheduled searches.

Table 3-1 Compliance Accelerator and Discovery Accelerator database roles *(continued)*

Role	Used in these databases	For these operations
EVUpgradeRole	Compliance Configuration Custodian Manager Discovery	Assign the Vault Service account to EVUpgradeRole before upgrading Compliance Accelerator and Discovery Accelerator. Revoke the Vault Service account's membership of EVUpgradeRole when you have completed the upgrade.

The installation or upgrade of Compliance Accelerator and Discovery Accelerator automatically creates these roles in the databases where they are required, except for the msdb system databases. The procedures in this chapter include the steps required to create the database roles in the msdb system database.

Configuring the Vault Service account for normal operations

Table 3-2 introduces the tasks you must complete to configure the Vault Service account with only the privileges it requires for normal daily operations.

Table 3-2 Configuring the Vault Service account for normal operations

Task	See this section for more details
Prepare to configure the Vault Service account	See "Preparing to configure the Vault Service account" on page 18.
Configure the Vault Service account's SQL login	See "Configuring the Vault Service account's SQL login" on page 18.
Change ownership of the Compliance Accelerator and Discovery Accelerator databases	See "Changing ownership of Compliance Accelerator and Discovery Accelerator databases" on page 19.
Assign Vault Service account to EVRuntimeRole	See "Assigning the Vault Service account to EVRuntimeRole" on page 20.
Map the Vault Service account to the msdb system database	See "Mapping the Vault Service account to the msdb system database" on page 20.

Table 3-2 Configuring the Vault Service account for normal operations *(continued)*

Task	See this section for more details
Create the EVMonitoringOperator role in the msdb system database and assign Vault Service account	See "Creating EVScheduledSearchOperator in the msdb system database and assigning the Vault Service account" on page 20.
Create the EVAnalyticsOperator role in the msdb system database and assign Vault Service account	See "Creating EVAnalyticsOperator in the msdb system database and assigning the Vault Service account" on page 21.
Restart Compliance Accelerator and Discovery Accelerator services.	See "Restarting Compliance Accelerator and Discovery Accelerator services" on page 22.

Preparing to configure the Vault Service account

Before you complete the procedures in this chapter, do the following:

- Choose an account other than the Vault Service account under which to complete the procedures in the chapter. For example, you could use the SQL System Administrator (sa) account, or another privileged user that is assigned to the sysadmin fixed server role.
- Ensure that your backups are up to date.
- Stop all Compliance Accelerator and Discovery Accelerator services.

Configuring the Vault Service account's SQL login

Use this procedure to take away the elevated SQL privileges that are assigned to the Vault Service account in a normal installations of Compliance Accelerator and Discovery Accelerator, and then assign only the reduced privileges that are required for normal daily operations.

To configure the Vault Service account's SQL login

1. Connect to the SQL server using SQL Server Management Studio.
2. In **Object Explorer**, under **Security** > **Logins**, double-click the Vault Service account.
3. In the **Login Properties** dialog box, select the **Server Roles** page.
4. Under **Server roles**, clear the **dbcreator** and **sysadmin** options, then click **OK**.
5. In **Object Explorer**, right-click the top-level server instance, and click **Properties**.

6 In the **Server Properties** dialog box, select the **Permissions** page.

7 Under **Logins or roles**, select the Vault Service account.

8 On the **Explicit** tab, select the **Grant** option for **Create any database**, **View server state**, and **View any Definition**, and then click **OK**.

Changing ownership of Compliance Accelerator and Discovery Accelerator databases

After a normal installation or upgrade of Compliance Accelerator and Discovery Accelerator, the Vault Service account owns their databases. As a result, the Vault Service account is a member of the db_owner fixed database role, which is not required for normal daily operations.

Use the following procedure and run one of these queries against each Compliance Accelerator and Discovery Accelerator database, to assign ownership to another privileged user. Choose the procedure that is appropriate for your version of SQL Server.

```
use CADADatabase
GO
ALTER AUTHORIZATION ON
DATABASE:: CADADatabase TO [domain\privileged_user];
```

or

```
use CADADatabase
GO
EXECUTE sp_changedbowner 'domain\privileged_user'
```

where:

CADADatabase is the name of the Compliance Accelerator or Discovery Accelerator database.

domain\privileged_user is the privileged user and the domain to which it belongs.

To change ownership of Compliance Accelerator and Discovery Accelerator databases

1 Connect to the SQL server using SQL Server Management Studio.

2 Click **New Query** and then enter the query in the query editor window.

3 From the **Query** menu, click **Execute**, and then wait for the script to complete.

4 Repeat this procedure for all the other Compliance Accelerator and Discovery Accelerator databases.

Assigning the Vault Service account to EVRuntimeRole

Use this procedure to assign the Vault Service account to EVRuntimeRole in all the Compliance Accelerator and Discovery Accelerator databases. This grants the Vault Service account all the privileges it requires in the databases for normal daily operations.

To assign the Vault Service account to EVRuntimeRole in all the Compliance Accelerator and Discovery Accelerator databases

1. Connect to the SQL server using SQL Server Management Studio.
2. In **Object Explorer**, under **Security** > **Logins**, double-click the Vault Service account.
3. In the **Login Properties** dialog box, select the **Server Roles** page.
4. Check that only the **public** option is selected.
5. Select the **User Mapping** page.
6. For each Compliance Accelerator and Discovery Accelerator database, do the following:
   - Under **Users mapped to this login**, select the **Map** option.
   - Under **Database role membership for**, select the **EVRuntimeRole** option.
7. Click **OK** to save the changes.

Mapping the Vault Service account to the msdb system database

Use this procedure to map the Vault Service account to the msdb system database.

To map the Vault Service account to the msdb system database

1. Connect to the SQL server using SQL Server Management Studio.
2. In **Object Explorer**, under **Security** > **Logins**, double-click the Vault Service account.
3. In the **Login Properties** dialog box, select the **User Mapping** page.
4. Select the **Map** option for the msdb system database.
5. Click **OK** to save the changes.

Creating EVScheduledSearchOperator in the msdb system database and assigning the Vault Service account

Use this procedure to do the following:

- Create the EVScheduledSearchOperator role in the msdb system database. This role is required to support scheduled searches.
- Assign the Vault Service account to the EVScheduledSearchOperator role.

To create the EVScheduledSearchOperator role and assign the Vault Service account

1. Connect to the SQL server using SQL Server Management Studio.
2. Click **New Query** and then enter the following query in the query editor window:

```
USE [MSDB]
GO
if not exists
(select * from dbo.sysusers
where name = N'EVScheduledSearchOperator')
BEGIN
 CREATE ROLE EVScheduledSearchOperator  Authorization dbo
END
GO
GRANT SELECT ON sysjobs TO EVScheduledSearchOperator
GRANT SELECT ON sysjobschedules TO EVScheduledSearchOperator
GRANT SELECT ON sysjobsteps TO EVScheduledSearchOperator
GRANT SELECT ON sysschedules TO EVScheduledSearchOperator
GRANT EXECUTE ON sp_add_category TO EVScheduledSearchOperator
exec sp_addrolemember SQLAgentUserRole, EVScheduledSearchOperator
exec sp_addrolemember [EVScheduledSearchOperator], N'domain\vsa'
GO
```

   where *domain\vsa* is the Vault Service account and the domain to which it belongs.

3. From the **Query** menu, click **Execute**, and then wait for the script to complete.

Creating EVAnalyticsOperator in the msdb system database and assigning the Vault Service account

Use this procedure to do the following:

- Create the EVAnalyticsOperator role in the msdb system database. This role is required to support Analytics operations.
- Assign the Vault Service account to the EVAnalyticsOperator role.

To create the EVAnalyticsOperator role and assign the Vault Service account

1. Connect to the SQL server using SQL Server Management Studio.
2. Click **New Query** and then enter the following query in the query editor window:

```
USE [MSDB]
GO
if not exists
(select * from dbo.sysusers
where name = N'EVAnalyticsOperator')
BEGIN
 CREATE ROLE EVAnalyticsOperator Authorization dbo
END
GO
GRANT SELECT ON sysjobhistory TO EVAnalyticsOperator
GRANT SELECT ON sysjobs TO EVAnalyticsOperator
GRANT SELECT ON sysjobschedules TO EVAnalyticsOperator
GRANT SELECT ON sysjobsteps TO EVAnalyticsOperator
GRANT SELECT ON sysjobservers TO EVAnalyticsOperator
GRANT SELECT ON sysjobactivity TO EVAnalyticsOperator
GRANT SELECT ON sysschedules TO EVAnalyticsOperator
GRANT EXECUTE ON sp_add_category TO EVAnalyticsOperator
GRANT EXECUTE ON sp_add_job TO EVAnalyticsOperator
GRANT EXECUTE ON sp_add_jobschedule TO EVAnalyticsOperator
GRANT EXECUTE ON sp_add_jobserver TO EVAnalyticsOperator
GRANT EXECUTE ON sp_add_jobstep TO EVAnalyticsOperator
exec sp_addrolemember [EVAnalyticsOperator], N'domain\vsa'
GO
```

   where *domain\vsa* is the Vault Service account and the domain to which it belongs.

3. From the **Query** menu, click **Execute**, and then wait for the script to complete.

Restarting Compliance Accelerator and Discovery Accelerator services

When you have completed these procedures, restart all the Compliance Accelerator and Discovery Accelerator services.

Configuring the Vault Service account for operations that require elevated privileges

In addition to the SQL privileges that the Vault Service account requires for normal daily operations, you can assign temporary, elevated privileges for other operations such as Compliance Accelerator and Discovery Accelerator upgrades.

Table 3-1 lists the Compliance Accelerator and Discovery Accelerator database roles and describes the operations for which each is required. For example, for an Compliance Accelerator and Discovery Accelerator upgrade, use the following procedure to assign the Vault Service account to the EVUpgradeRole.

To assign the Vault Service account to EVUpgradeRole

1. Stop all Compliance Accelerator and Discovery Accelerator services.
2. Connect to the SQL server using SQL Server Management Studio.
3. In **Object Explorer**, under **Security** > **Logins**, double-click the Vault Service account.
4. In the **Login Properties** dialog box, select the **Server Roles** page.
5. Check that only the **public** option is selected.
6. Select the **User Mapping** page.
7. For each Compliance Accelerator and Discovery Accelerator database, do the following:
   - Under **Users mapped to this login**, select the **Map** option.
   - Under **Database role membership for**, select the **EVUpgradeRole** option.
8. Click **OK** to save the changes.
9. Restart all Compliance Accelerator and Discovery Accelerator services.

In this example, the Vault Service account must be assigned to EVUpgradeRole for the duration of the upgrade.

When the upgrade is complete, use the same procedure to revoke the assignment, by clearing the **EVUpgradeRole** option in step 7.