# Table of Contents

Overview ......................................................................................................................... 4

1  Prerequisites ............................................................................................................... 4

2  Create a Failover Cluster .......................................................................................... 5
   2.1  Install the Failover Clustering feature ................................................................. 5
   2.2  Run cluster validation tests ............................................................................... 12
   2.3  Create the failover cluster ................................................................................. 17

3  Install & Configure MSSQL ...................................................................................... 21
   3.1  Install MSSQL ................................................................................................... 21
   3.2  Set the Default MSSQL Backup Location ........................................................... 22
   3.3  Enable Named Pipes .......................................................................................... 25
   3.4  Configure MSDTC ............................................................................................. 26
   3.5  Initialize the Databases ..................................................................................... 28

4  Configure AlwaysOn ................................................................................................. 30
   4.1  Enable AlwaysOn Availability .......................................................................... 30
   4.2  Back Up the Primary ADG Database ................................................................ 32
   4.3  Delete the Secondary ADG Database ................................................................. 35
   4.4  Create the Availability Group ............................................................................ 37
   4.5  Granting Permissions to the Availability Group and Creating Triggers .......... 43

5  Configure FTK Central ............................................................................................... 44
   5.1  Update the ServerList Table ............................................................................. 44
   5.2  Update the Database Configuration Utility ....................................................... 45
Overview

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Legal GRC platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world’s largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

1 Prerequisites

1. One server to act as SQL Primary Replica.
2. One server to act as SQL Secondary Replica.
3. All servers must be running the same version of Windows Server and have all current updates.
4. All servers must be running the same version of MSSQL Enterprise 2016/2017/2019.
5. All servers must be members of the same Active Directory domain.
6. The SQL Server Agent service must be set to Automatic Startup Type on all servers.
7. A domain-level service account.
2. **Create a Failover Cluster**

2.1 **Install the Failover Clustering feature**

1. On the Primary Replica, start Server Manager.

2. On the **Manage** menu, select **Add Roles and Features**.
3. On the **Before you begin** page, select **Next**.

Before you begin

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:

Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default
4. On the **Select installation type** page, select **Role-based or feature-based installation**, and then select **Next**.
5. On the **Select destination server** page, select the server where you want to install the feature, and then select **Next**.
6. On the Select server roles page, select Next.
7. On the **Select features** page, select the **Failover Clustering** check box.
8. To install the failover cluster management tools, select **Add Features**, and then select **Next**.
   i. If prompted to add additional required features, click **Add Features**.

9. On the **Confirm installation selections** page, select **Install**.

10. When the installation is completed, select **Close**.
   i. If prompted, reboot the server.

11. Repeat this procedure on the Secondary Replica.
2.2 Run cluster validation tests

1. On the Primary Replica, start Server Manager.
2. On the **Tools** menu, select **Failover Cluster Manager**.
3. In the Failover Cluster Manager pane, under Management, select Validate Configuration.

5. On the Select Servers or a Cluster page, add the names (NetBIOS or FQDN) of the Primary and Secondary Replica. When you are finished, select Next.
6. On the Testing Options page, select Run all tests (recommended), and then select Next.

7. On the Confirmation page, select Next.

8. Wait for the tests to complete.
9. On the **Summary** page, do one of the following:

- If all tests indicate Success, check the **Create the cluster now using the validated nodes** check box, and then select **Finish**.

- If any tests indicate Warnings, select **View Report** to view the details and determine if any issues must be corrected. You can either correct those items and retry later, or to continue anyway, check the **Create the cluster now using the validated nodes** check box, and then select **Finish**.

- If any tests indicate Failures, select **View Report** to view the details and determine what issues must be corrected. You will need to correct those items and retry later.
2.3 Create the failover cluster

1. In the Create Cluster Wizard, on the Before You Begin page, select Next.

2. On the Access Point for Administering the Cluster page, do the following:
   i. In the Cluster Name box, enter the name that you want to use to administer the cluster. Before you do, review the following information:
      a. During cluster creation, this name is registered as the cluster computer object (also known as the cluster name object or CNO) in AD DS. If you specify a NetBIOS name for the cluster, the CNO is created in the same location where the computer objects for the cluster nodes reside. This can be either the default Computers container or an OU.
      b. To specify a different location for the CNO, you can enter the distinguished name of an OU in the Cluster Name box. For example: CN=ClusterName, OU=Clusters, DC=Contoso, DC=com.
c. If a domain administrator has prestaged the CNO in a different OU than where the cluster nodes reside, specify the distinguished name that the domain administrator provides.

ii. Select one or more unique static IP addresses for the failover cluster. Select the check box next to each network that you want to use for cluster management. Select the **Address** field next to a selected network, and then enter the IP address that you want to assign to the cluster. This IP address (or addresses) will be associated with the cluster name in Domain Name System (DNS) and is not related to the IP addresses of the servers in the cluster.

*Note: The Cluster will typically use the same method of address assignment as the Replica Servers. If the servers are configured to use DHCP, the Cluster will be automatically set to use DHCP. If the servers are configured with static IPs, you will be prompted to assign a static IP to the Cluster.*

iii. When you are finished, select **Next**.
3. On the **Confirmation** page, review the settings. By default, the **Add all eligible storage to the cluster** check box is selected. Leave this checked and select **Next** to create the failover cluster.
4. On the **Summary** page, confirm that the failover cluster was successfully created. If there were any warnings or errors, view the summary output or select **View Report** to view the full report.

5. Select **Finish**.

6. To confirm that the cluster was created, verify that the cluster name is listed under **Failover Cluster Manager** in the navigation tree.

7. After the cluster name successfully replicates in DNS, if you select **All Servers** in Server Manager, the cluster name should be listed as a server with a **Manageability** status of **Online**.
3 Install & Configure MSSQL

Note: If MSSQL is already installed, the following steps should still be reviewed to verify if the MSSQL is configured appropriately.

3.1 Install MSSQL


1. Install MSSQL on both the Primary and Secondary replica servers.
   i. The SQL Server Agent service’s Startup Type should be set to Automatic.
   ii. The SQL Server Database Engine service should be set to run under the service account.
   iii. Set MSSQL to use Mixed Mode Authentication.

![Database Engine Configuration](image-url)
iv. The service account should have the ‘sysadmin’ role in both MSSQL instances.

2. Install SQL Server Management Studio on either the Primary Replica or another server that can see both the Primary and Secondary Replica.

3.2 Set the Default MSSQL Backup Location

1. Open SQL Server Management Studio.
2. Connect to the Primary Replica.
3. In the left pane, right-click the server/instance name (top node in the list) and select Properties.
4. In the Server Properties dialog, select the Database Settings page on the left.

5. Under Database default locations, browse to and select a default Backup path.

Note: The selected path must always have sufficient space to store backups for all future databases.

6. Click OK.

7. Repeat this procedure on the Secondary Replica.
3.3 Enable Named Pipes

1. On the Primary Replica, open SQL Server Configuration Manager.
2. In the left pane, expand SQL Server Network Configuration.
3. Select the Protocols entry for your SQL instance.
4. In the right pane, right-click Named Pipes and select Enable.

5. In the left pane, click SQL Server Services.
6. In the right pane, right-click the SQL Server service for your SQL instance and select Restart.

7. Repeat this procedure on the Secondary Replica.
3.4 Configure MSDTC

1. On the Primary Replica, open **Component Services**.
2. In the left pane, expand **Component Services**.
3. Expand **Computers**.
4. Expand **My Computer**.
5. Expand **Distributed Transaction Coordinator**.
6. Right-click **Local DTC** and select **Properties**.
7. Configure the options under the **Security** tab as shown below, then click **OK**.

8. Repeat this procedure on the Secondary Replica.
3.5 Initialize the Databases

1. On the FTK Central application server, launch the **AccessData Database Configuration Tool**, typically located at 
   ‘C:\Program Files\AccessData\Forensic Tools\<version>\bin.DBConfig.exe’, as the service account.

   ![Database Configuration Tool](image)

2. Click **Add Configuration**.

3. In the **Database Type** dropdown, select **MSSQL**.

4. Enter the **Server Name** and **Port** of the Primary Replica, using a colon between the server/instance name and port. If your database is using the default port, you do not need to specify a port here.

5. Do not change the **Database Name / SID** and **Database Schema** fields from their default values.

6. If you’d like to set a custom password for Forensic Tools to use when communicating with the database, click the lock next to **Internal Authentication Mode** and select **Database Authentication**.

   **Note:** Using Database Authentication with MSSQL also allows you to select whether to enforce the Windows/domain password policy.
7. Check **Create Database**.
8. Set **System Authentication Mode** to **Windows Authentication**.
9. Check **Install WordNet**.
10. Choose a username and password for your initial Forensic Tools administrator.
11. Leave the **Version** dropdown set to its default value.
12. Click **Create**.
13. After database creation completes, highlight the new entry in the list and click **Delete Configuration**.

14. Repeat this procedure, making sure to use the same settings and passwords, to initialize the Secondary Replica.

## 4 Configure AlwaysOn

### 4.1 Enable AlwaysOn Availability

1. On the Primary Replica, open **SQL Server Configuration Manager**.
2. In the left pane, select **SQL Server Services**.
3. In the right pane, right-click the **SQL Server** service for your SQL instance and select **Properties**.
4. Under the **Always On Availability Groups** tab, check **Enable Always On Availability Groups** and click **OK**.

5. In the right pane, right-click the **SQL Server** service for your SQL instance and select **Restart**.

6. Repeat this procedure on the Secondary Replica.
4.2 Back Up the Primary ADG Database

1. Open SQL Server Management Studio.
2. Connect to the Primary Replica.
3. In the left pane, expand Databases.
4. Right-click the **ADG** database and select **Tasks** then **Back Up**.

5. In the **Database** dropdown, select **ADG**.

6. In the **Backup type** dropdown, select **Full**.

7. In the **Back up to** dropdown, select **Disk**.
8. Add one of more locations for the resulting BAK file, then click **OK**.
4.3 Delete the Secondary ADG Database

1. Open SQL Server Management Studio.
2. Connect to the Secondary Replica.
3. In the left pane, expand Databases.

4. Right-click the ADG database and select Delete.
5. Check **Close existing connections**, then click **OK**.
4.4 Create the Availability Group

1. Open SQL Server Management Studio.
2. Connect to the Primary Replica.
3. In the left pane, expand Always On High Availability.
4. Right-click Availability Groups and select New Availability Group Wizard.
5. On the Introduction page, click Next.
6. On the Specify Options page, do the following:
i. In the **Availability group name** field, create a unique name for your availability group.

ii. In the **Cluster type** dropdown, select *Windows Server Failover Cluster*.

iii. Check **Database Level Health Detection**.

iv. Click **Next**.
7. On the **Select Data Synchronization** page, check the **ADG** database and click **Next**.

![New Availability Group](image)

**Select Databases**

<table>
<thead>
<tr>
<th>Introduction</th>
<th>Specify Options</th>
<th>Select Databases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify Replicas</td>
<td>Select Data Synchronization</td>
<td>Validation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Status</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADG</td>
<td>336.0 MB</td>
<td>Meets prerequisites</td>
<td></td>
</tr>
</tbody>
</table>

- ReportServer  
- ReportServerTemp...

8. On the **Specify Replicas** page, do the following:

i. Open the **Replicas** tab.

ii. Click **Add Replica** and specify your Secondary Replica.

iii. Check the **Automatic Failover** box for both replicas. This also sets the **Availability Mode** to **Synchronous Commit**.

iv. For both replicas, in the **Readable Secondary** dropdown, select **Yes**.

v. Open the **Listener** tab.

vi. Select **Create an availability group listener**.

vii. In the **Listener DNS Name** field, create a unique name for your listener. This name will be associated with the listener in Domain Name System (DNS) and is not related to the names of the servers/instances in the availability group or of the failover cluster.

viii. In the **Port** field, choose what port your listener will be on. This port is unique to the listener and not related to ports on the involved servers.

ix. Select a unique static IP addresses for the listener. This IP address will be associated with the listener in Domain Name System (DNS) and is not related to the IP addresses of the servers in the availability group or of the failover cluster.
Notes:

- You will need to ensure that any involved firewalls are set to allow traffic to the chosen listener’s IP and port.
- The Listener should typically use the same method of address assignment as the Replica Servers. If the servers are configured to use DHCP, you should set the Listener's Network Mode set to ‘DHCP’. If the servers are configured with static IPs, you should set the Listener’s Network Mode to ‘Static IP’ and assign a static IP to the Listener.

x. Click Next.
9. On the **Select Data Synchronization** page, select **Automatic Seeding** and click **Next**.

![Select Initial Data Synchronization](image)

**Select your data synchronization preference.**

- **Automatic seeding**
  SQL Server automatically creates databases for every selected secondary replica. Automatic seeding requires that the data and log file paths are the same on every SQL Server instance participating in the availability group.

- **Full database and log backup**
  Starts data synchronization by performing full database and log backups for each selected database. These databases are restored to each secondary and joined to the availability group. Make sure the file share is accessible to all replicas and is mounted to the same directory on all Linux replicas.

  Specify the file share path in Windows format:

  ![File share path input field]

  Specify the file share location in Linux format:

  ![File share location input field]

- **Join only**
  Starts data synchronization where you have already restored database and log backups to each secondary server. The selected databases are joined to the availability group on each secondary.

- **Skip initial data synchronization**
  Choose this option if you want to perform your own database and log backups of each primary database.
10. On the **Validation** page, confirm the checks were successful and click **Next**.

11. On the **Summary** page, click **Finish**.
4.5 Granting Permissions to the Availability Group and Creating Triggers

1. Open SQL Server Management Studio.
2. Click New Query.
3. Paste the contents of CreateJobAndTriggers.sql file into the query window.
4. Modify the contents below:
   - **@ServiceAccount** – Account that has permissions to access the replica.
   - **@AGname** – Availability Groups name (refer the ‘Specify Options’ point of Create the Availability Group section).
   - **@Password** – Password required to access the replica.
5. Click Execute.
6. Repeat this procedure for the Secondary Replica.
5 Configure FTK Central

5.1 Update the ServerList Table

1. Open SQL Server Management Studio.
2. Connect to the listener.
3. Click New Query.
4. Paste the contents of UpdateServerList.sql into the query window.
5. Modify the @ListenerName variable to be the name of your Availability Group’s Listener (created in the 8th point of Create the Availability Group section).
6. Modify the @ListenerPort variable to be the port of your Availability Group’s Listener (created in the 8th point of Create the Availability Group section).
7. Click Execute.
5.2 Update the Database Configuration Utility

1. On the FTK application server, launch the AccessData Database Configuration Tool, typically located at "C:\Program Files\AccessData\Forensic Tools\<version>\bin.DBConfig.exe", as the service account.

2. Click Add Configuration.

3. In the Database Type dropdown, select MSSQL.

4. Enter the name and port of the Listener (created in the 8th point of Create the Availability Group section) in the Server Name field, using a colon between the server/instance name and port.
5. Do not change the **Database Name / SID** and **Database Schema** fields from their default values.

6. If you selected **AccessData Default Password** when initializing the databases with DBConfig (created in the 6th point of Initialize the Databases section), leave the **Internal Authentication Mode** as **AccessData Default Password** here. However, if you set a custom password, click the lock next to **Internal Authentication Mode** and select **Database Authentication** to enter your custom password.

   **Note:** Using Database Authentication with MSSQL also allows you to select whether or not to **enforce the Windows/domain password policy**.

7. Click **Connect**.
6 Performing Failovers

6.1 Manual Failover

1. Open SQL Server Management Studio.
2. Connect to the listener.
3. In the left pane, expand Always On High Availability.
4. Expand Availability Groups.
5. Right-click your availability group and click Failover.
6. On the **Introduction** page, click **Next**.

7. On the **Select New Primary Replica** page, select the Secondary Replica and click **Next**.

8. On the **Summary** page, click **Next**.

9. On the **Results** page, verify that the failover was successful without any errors.

10. Repeat this procedure to return to using the original primary/secondary replica setup.

### 6.2 Automatic Failover

*Note: You can also refer the Microsoft’s Automatic Failover section.*

1. Open **SQL Server Management Studio**.

2. Connect to the listener.

3. In the left pane, expand **Always On High Availability**.

4. Expand **Availability Groups**.
5. Right-click your availability group and click **Properties**.

6. In the **Availability Replica Properties** dialog box, select the **Failover mode** drop-down list to change the failover mode to **Automatic**.
Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro.
For usage questions, please check with your organization’s internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:
Exterro, Inc.
4145 SW Watson Ave., Suite 400
Beaverton, OR 97005.
Telephone: 503-501-5100
Toll Free: 1-877-EXTERRO (1-877-398-3776)
Fax: 1-866-408-7310

General E-mail: info@exterro.com
Website: www.exterro.com

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Exterro, Inc. The trademarks, service marks, logos or other intellectual property rights of Exterro, Inc and others used in this documentation ("Trademarks") are the property of Exterro, Inc and their respective owners. The furnishing of this document does not give you license to these patents, trademarks, copyrights or other intellectual property except as expressly provided in any written agreement from Exterro, Inc.
The United States export control laws and regulations, including the Export Administration Regulations of the U.S. Department of Commerce, and other applicable laws and regulations apply to this documentation which prohibits the export or re-export of content, products, services, and technology to certain countries and persons. You agree to comply with all export laws, regulations and restrictions of the United States and any foreign agency or authority and assume sole responsibility for any such unauthorized exportation.
You may not use this documentation if you are a competitor of Exterro, Inc, except with Exterro Inc’s prior written consent. In addition, you may not use the