

FTK - RDS ENVIRONMENT SETUP GUIDE

SEPTEMBER 2026

Table of Contents

About Exterro	3
Purpose of the Document.....	3
1 Creating a PostgreSQL RDS Instance	4
2 Initializing the Database	17
3 Maximizing AWS RDS Efficiency	19
4 RDS Database Migration: 14.x to 18.4.....	21
4.1 Upgrade PostgreSQL Engine in AWS RDS	21
4.2 Initialize the Database	22
4.3 Update Permissions via Configuration Tool	23
Contact Exterro	25

About Exterro

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 Data Risk Management 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.

Purpose of the Document

This guide provides users with the steps required for a successful AWS PostgreSQL RDS deployment.

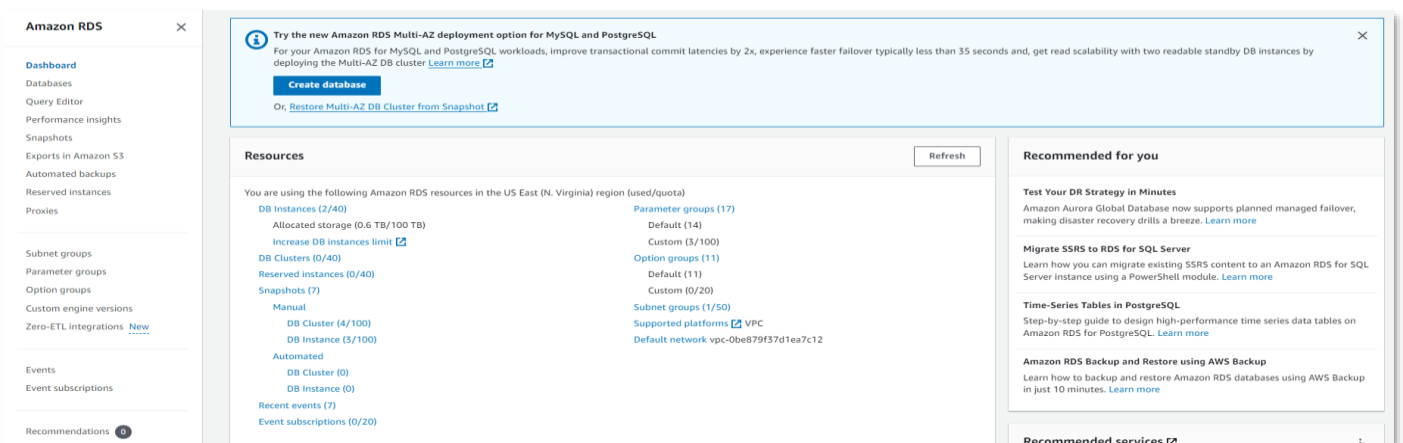
PostgreSQL RDS is a managed service from Amazon. As a managed service, RDS restricts users with certain roles from accessing the FTK application upon setting up the database using the DBConfig utility. For Forensic Tools to work with PostgreSQL RDS, you will need to perform certain operations that are not automatically performed by the DBConfig utility.

1 Creating a PostgreSQL RDS Instance

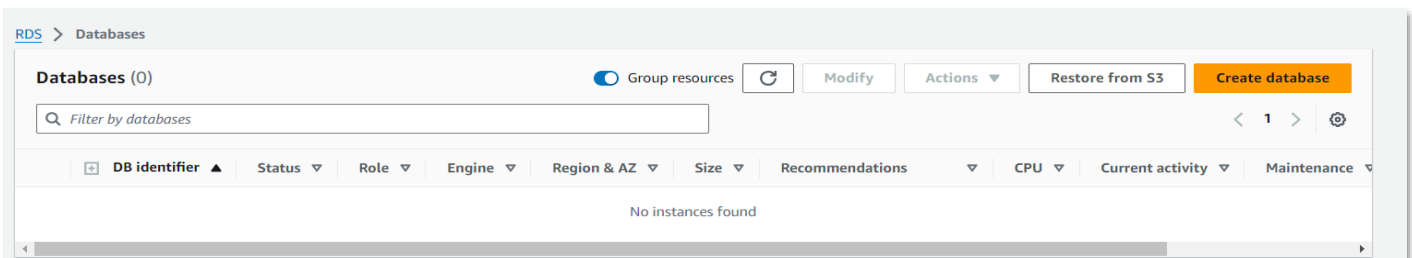
Follow these steps to set up a PostgreSQL RDS instance:

Steps:

1. Sign in to the **AWS Management Console** with your AWS account at <https://console.aws.amazon.com>.
2. Search **AWS RDS** and select the populated RDS service.
 - The Amazon RDS Management Console is displayed.



3. Click on **Databases** in the left pane.
 - The RDS Databases page is displayed.



4. Click the **Create database** button located in the top-right corner.

- The **Create database** pop-up is displayed.

RDS > Create database

Create database

Choose a database creation method [Info](#)

☒ **Standard create**
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

☐ **Easy create**
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

5. Choose the database creation method as **Standard create**.
6. Select **PostgreSQL** as the **Engine type**.

Engine options

Engine type [Info](#)

☐ Aurora (MySQL Compatible) 	☐ Aurora (PostgreSQL Compatible) 
☐ MySQL 	☐ MariaDB 
☒ PostgreSQL 	☐ Oracle 
☐ Microsoft SQL Server 	☐ IBM Db2 

7. Select the **Engine Version** to 14.x version. (The recommended version is **PostgreSQL 14.19**).

Engine version [Info](#)
View the engine versions that support the following database features.

▼ Hide filters

☒ Show versions that support the Multi-AZ DB cluster [Info](#)
Create a Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.

Engine Version
PostgreSQL ▼

8. Choose a sample template with the **Production** template being recommended.

Templates
Choose a sample template to meet your use case.

☒ **Production**
Use defaults for high availability and fast, consistent performance.

☐ **Dev/Test**
This instance is intended for development use outside of a production environment.

☐ **Free tier**
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

9. In the 'Availability and durability' section, select **Single DB instance** as the Deployment option.

Availability and durability

Deployment options [Info](#)
The deployment options below are limited to those supported by the engine you selected above.

☐ **Multi-AZ DB Cluster**
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

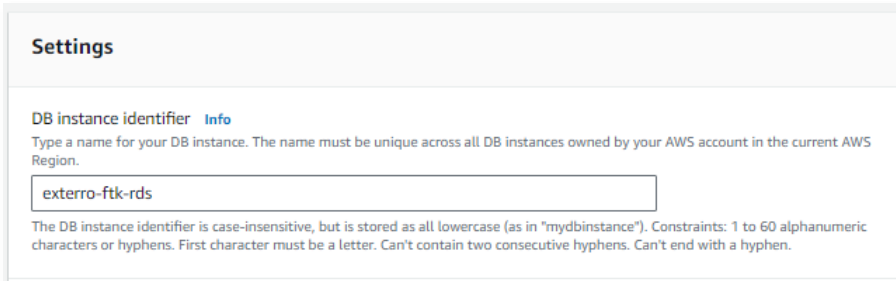
☐ **Multi-AZ DB instance**
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

☒ **Single DB instance**
Creates a single DB instance with no standby DB instances.

10. Provide the following details in the **Settings** section:

- **DB instance identifier:** Enter a unique name for the DB instance.

***Note:** Ensure that the name you choose is unique among all the DB instances associated with your AWS account.*



Settings

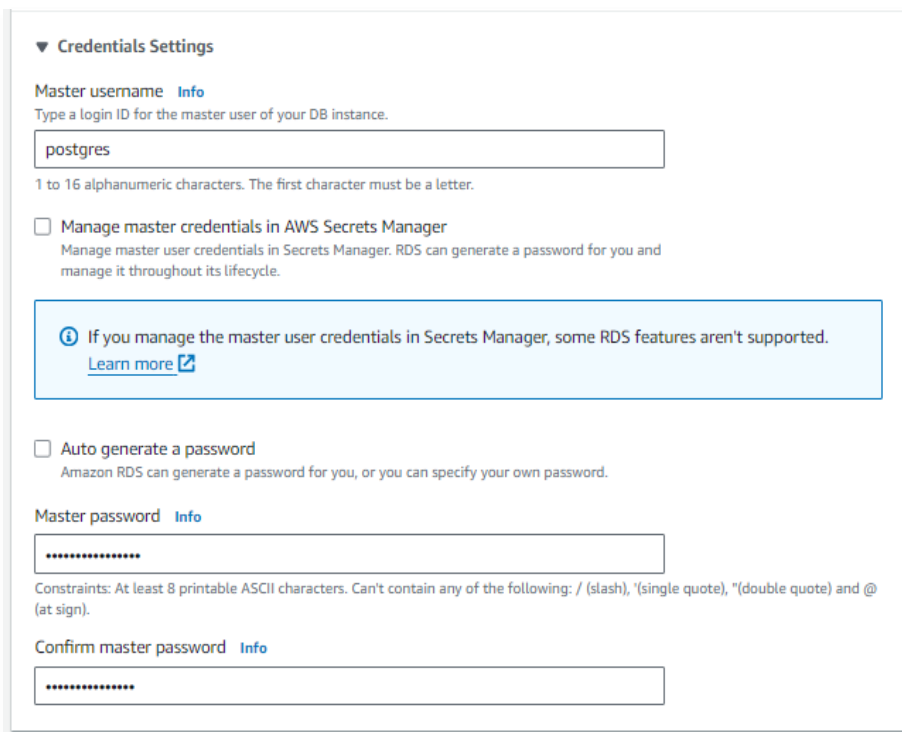
DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

exterro-ftk-rds

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

- **Master username:** Ensure the Master username is set to 'postgres'.
- **Master password:** Specify a password for the Master username.



▼ **Credentials Settings**

Master username [Info](#)

Type a login ID for the master user of your DB instance.

postgres

1 to 16 alphanumeric characters. The first character must be a letter.

☐ **Manage master credentials in AWS Secrets Manager**

Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

[Learn more](#)

☐ **Auto generate a password**

Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), ' (single quote), " (double quote) and @ (at sign).

Confirm master password [Info](#)

11. In the **Instance configuration** section, select the appropriate DB instance class based on performance requirements. It is recommended to utilize Memory-Optimized instances.

Note: Instance types can be changed at a later date if a reserved instance is not selected.

Specifications:

- Minimum Hardware Configuration: 16 GB, 4-core
- Recommended Hardware Configuration: 32 GB, 8-core
 - Users should consider at least 4GB/per core

Instance configuration
The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)

▼ Hide filters

☐ Include previous generation classes

☒ Standard classes (includes m classes)

☐ Memory optimized classes (includes r and x classes)

☐ Burstable classes (includes t classes)

db.m5.2xlarge
8 vCPUs 32 GiB RAM Network: 4,750 Mbps

12. Under the **Storage** section, select **General Purpose SSD (gp3)** as the Storage type.

- Refer to [Maximizing AWS RDS Efficiency](#).

Storage

Storage type [Info](#)
Provisioned IOPS SSD (io2) storage volumes are now available.

General Purpose SSD (gp3)
Performance scales independently from storage

Allocated storage [Info](#)
500 GiB
Minimum: 20 GiB. Maximum: 65,536 GiB

ⓘ After you modify the storage for a DB instance, the status of the DB instance will be in storage-optimization. Your instance will remain available as the storage-optimization operation completes.

[Learn more](#)

Note: Auto scaling for storage can be extended up to 65TB as per AWS guidelines.

▼ Storage autoscaling

Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

☒ **Enable storage autoscaling**
Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

Maximum storage threshold [Info](#)
Charges will apply when your database autoscales to the specified threshold

GiB

The minimum value is 550 GiB and the maximum value is 65,536 GiB

13. In the **Connectivity** section:

- As shown in the below image, select the **Compute resource** and **Network type** for the database.

Connectivity [Info](#) [G](#)

Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

☒ **Don't connect to an EC2 compute resource**
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

☐ **Connect to an EC2 compute resource**
Set up a connection to an EC2 compute resource for this database.

Network type [Info](#)
To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

☒ **IPv4**
Your resources can communicate only over the IPv4 addressing protocol.

☐ **Dual-stack mode**
Your resources can communicate over IPv4, IPv6, or both.

- Specify the **Virtual Private Cloud** (VPC) for the DB instance.

Note: This ensures that the RDS instance operates within a designated VPC, which should align with the VPC used by the Forensic Tools application.

- Select the required **DB subnet group**.

Note: The subnet group specifies the subnets and IP ranges available for use by the associated DB instance within the VPC.

Virtual private cloud (VPC) [Info](#)
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Default VPC (vpc-0be879f37d1ea7c12)
21 Subnets, 6 Availability Zones ▼

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group [Info](#)
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

postgres
2 Subnets, 2 Availability Zones ▼

- Set **Public access** as **No**.

Public access [Info](#)

☐ Yes
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

☒ No
RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

14. In the **VPC security group (firewall)** section, choose one or more VPC security groups to permit access to the database. Ensure that the security group rules are configured to allow the necessary incoming traffic from any EC2 instances running FTK Central, FTK Core, the Distributed Processing Manager, or the Processing Engine enabling seamless connection to the FTK application.

VPC security group (firewall) [Info](#)
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

☒ Choose existing
Choose existing VPC security groups

☐ Create new
Create new VPC security group

Existing VPC security groups

Choose one or more options ▼

ADDEV02_VPN_SG X Exterro_Dev X

15. Set the Availability Zone to 'No preference', as the chosen VPC and Subnet will automatically select the appropriate zone.

Availability Zone [Info](#)

No preference ▼

Note: The default settings for Proxy and Certificate Authority will be retained.

RDS Proxy
RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

☐ Create an RDS Proxy [Info](#)
RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see [Amazon RDS Proxy pricing](#).

Certificate authority - optional [Info](#)
Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-rsa2048-g1 (default)
Expiry: May 26, 2061 ▼

If you don't select a certificate authority, RDS chooses one for you.

16. In **Additional configuration**, set the **Database port** to **5432** (default for PostgreSQL).

▼ **Additional configuration**

Database port [Info](#)
TCP/IP port that the database will use for application connections.

5432

17. In the **Database authentication** section, opt for **Password authentication** to authenticate database users solely using database passwords.

Database authentication

Database authentication options [Info](#)

☒ Password authentication
Authenticates using database passwords.

☐ Password and IAM database authentication
Authenticates using the database password and user credentials through AWS IAM users and roles.

☐ Password and Kerberos authentication
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

18. In the **Monitoring** section, stick to the default settings. For the AWS KMS key, you can opt for the default option or select Customer Managed Keys (**CMK**) if preferred. In this case, CMK keys have been chosen. All other settings can remain as default.

Monitoring

☒ Turn on Performance Insights

Retention period for Performance Insights [Info](#)

7 days (free tier) ▼

AWS KMS key [Info](#)

AWS_EBS_CMK_KEYS ▼

Account
686428625652

KMS key ID
53ebdd0f-1b78-4e7d-883e-e6cf4ebef040

 You can't change the KMS key after enabling Performance Insights.

☒ Turn on DevOps Guru [Info](#)

DevOps Guru for RDS automatically detects performance anomalies for DB instances and provides recommendations.

Tag key

devops-guru-default

Tag value

rds-test

Cost per resource per hour
\$0.0042 [Amazon DevOps Guru pricing](#)

▼ **Additional configuration**

Enhanced Monitoring

☒ Enable Enhanced Monitoring

Enabling Enhanced Monitoring metrics are useful when you want to see how different processes or threads use the CPU.

Granularity

60 seconds ▼

Monitoring Role

default ▼

Clicking "Create database" will authorize RDS to create the IAM role rds-monitoring-role

19. In the **Additional Configuration** section, within the Database options:

- **Initial database name:** You are recommended to leave this field blank.

▼ **Additional configuration**

Database options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned on.

Database options

Initial database name [Info](#)

If you do not specify a database name, Amazon RDS does not create a database.

- **DB parameter group:** Select the DB parameter group that configures settings for this DB instance.
 - You can stick with the default value or create a parameter group tailored to the specific PostgreSQL version being.

DB parameter group [Info](#)

default:postgres14 ▼

- **Option group:** Opt for the default DB option group.

Option group [Info](#)

default:postgres-14 ▼

20. Configure the following settings in the 'Backup' section:

- **Enable automated backups:** Check this box to activate automated backups for the database.
- **Backup retention period:** Set the number of days for which the database will be automatically backed up. We recommend a retention period of 7 days.
- **Backup window:** Choose your preferred backup window to specify the start time (in UTC) and duration (in hours) for backups.
- **Enable Encryption:** If encryption of the volume and snapshot is necessary in Amazon RDS, enable this option. If selected, choose the appropriate Customer Master Key (CMK) for encryption.

Backup

☒ **Enable automated backups**
Creates a point-in-time snapshot of your database

Backup retention period [Info](#)
The number of days (1-35) for which automatic backups are kept.

days

Backup window [Info](#)
The daily time range (in UTC) during which RDS takes automated backups.

☒ Choose a window
☐ No preference

Start time **Duration**

: UTC hours

☒ Copy tags to snapshots

Backup replication [Info](#)

☐ Enable replication in another AWS Region
Enabling replication automatically creates backups of your DB instance in the selected Region, for disaster recovery, in addition to the current Region.

Encryption

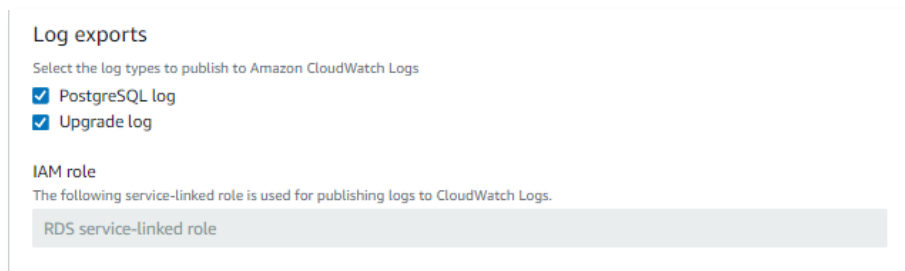
☒ **Enable encryption**
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

AWS KMS key [Info](#)

Account
686428625652

KMS key ID
53ebdd0f-1b78-4e7d-883e-e6cf4ebef040

21. Select the log types to be published to Amazon CloudWatch Logs. Select both PostgreSQL logs and Upgrade logs. Leave the IAM role setting as default.



Log exports

Select the log types to publish to Amazon CloudWatch Logs

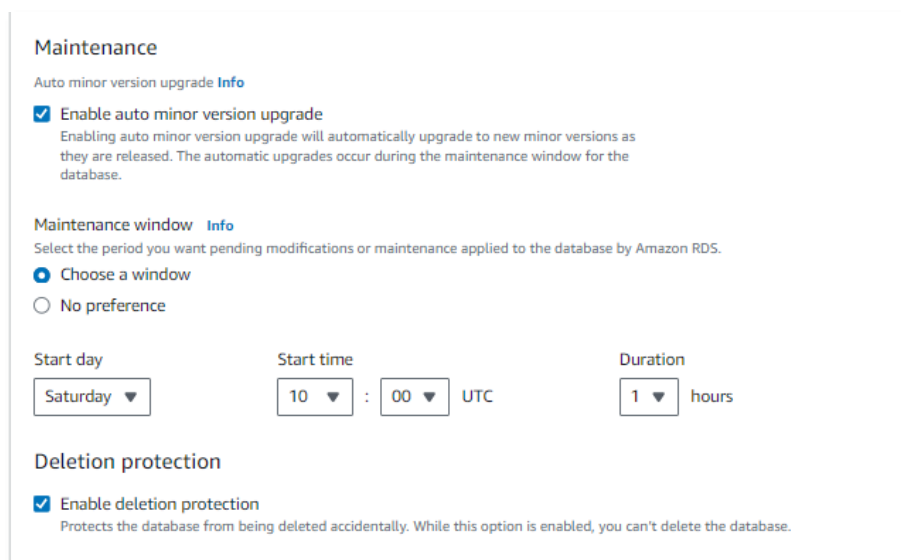
- ☒ PostgreSQL log
- ☒ Upgrade log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

22. Configure the following details in the **Maintenance window** section:
- **Enable auto minor version upgrade:** Select this option to automatically receive updates when they are available.
 - **Maintenance window:** Select your preferred time period for applying pending modifications or maintenance to the database by Amazon RDS.
 - **Enable deletion protection:** Select this option to prevent accidental deletion of databases.



Maintenance

Auto minor version upgrade [Info](#)

- ☒ **Enable auto minor version upgrade**
Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

☒ Choose a window

☐ No preference

Start day: Saturday ▼

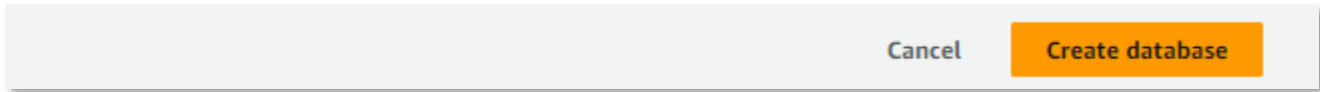
Start time: 10 ▼ : 00 ▼ UTC

Duration: 1 ▼ hours

Deletion protection

- ☒ **Enable deletion protection**
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

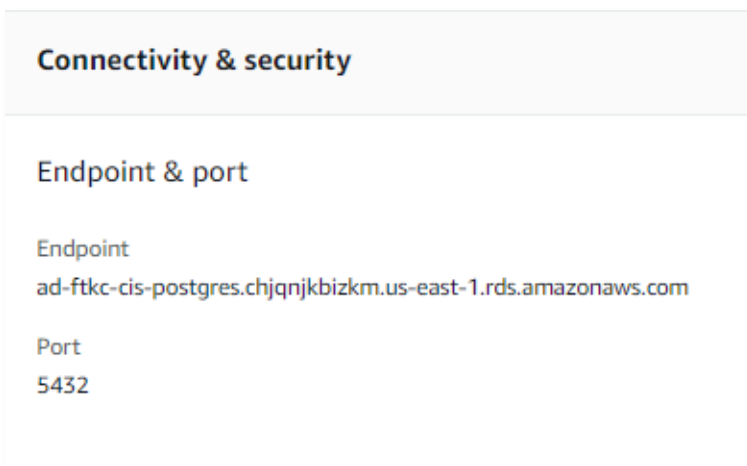
23. Click **Create database**.



Note: You are recommended to wait approximately 10 to 15 minutes for the database to become available.

	DB identifier ▲	Status ▼	Role ▼	Engine ▼	Region & AZ ▼	Size ▼
○	ad-ftkc-cis-postgres	✔ Available	Instance	PostgreSQL	us-east-1a	db.m5.2xlarge

24. Navigate to the database identifier name and click on it to access the **Endpoint** located under the **Connectivity & Security** tab.



2 Initializing the Database

Prerequisite:

Ensure the following environment variables are set on all the FTK/FTKC servers including the DPE and DPM machines when the database configured in DBConfig.exe is an SSL-enabled RDS PostgreSQL instance:

- ispostgresrdsconnection=true
- postgresdbtimeout=120
- usesecurepostgres=true

Steps:

1. Once the FTK application is installed, navigate to 'DBConfig.exe',

```
C:\Program Files\Accessdata\Forensic Tools\8.0\bin\DBConfig.exe
```

2. Right-Click and run **DBConfig.exe** as an **Administrator**.
3. Click on '**Add Configuration**'.
4. Enter **Postgres** within the '**Database Type**' field.
5. Enter the RDS endpoint and port within the '**Server Name: Port**' field.

```
Ad-ftkc-cis-postgres.axxxxxxxxxsd.us-east-1.amazonaws.com:5432
```

6. Enter the following options:

- **Create Database**
- **System User:** postgres
- **System Password:** Password set in **Step 10** of [Creating PostgreSQL RDS Instance](#) section.
- Select both the **Install WordNet** and **Cloud Install** checkboxes.
- **Application Admin:** Custom Value
- **Admin Password:** Custom Value

Database Information

Configuration Name: RDS PG

Database Type: Postgres

Server Name : Port: aws.RDS.PG.com

Database Name / SID: ADG

Database Schema: ADG7x1

Internal Authentication Mode: AccessData Default Password

☒ Create Database

System Authentication Mode: Database Authentication

System User: postgres

System Password:

☒ Install WordNet ☒ Cloud Install

Application Admin: Administrator

Admin Password: ...

Confirm Password: ...

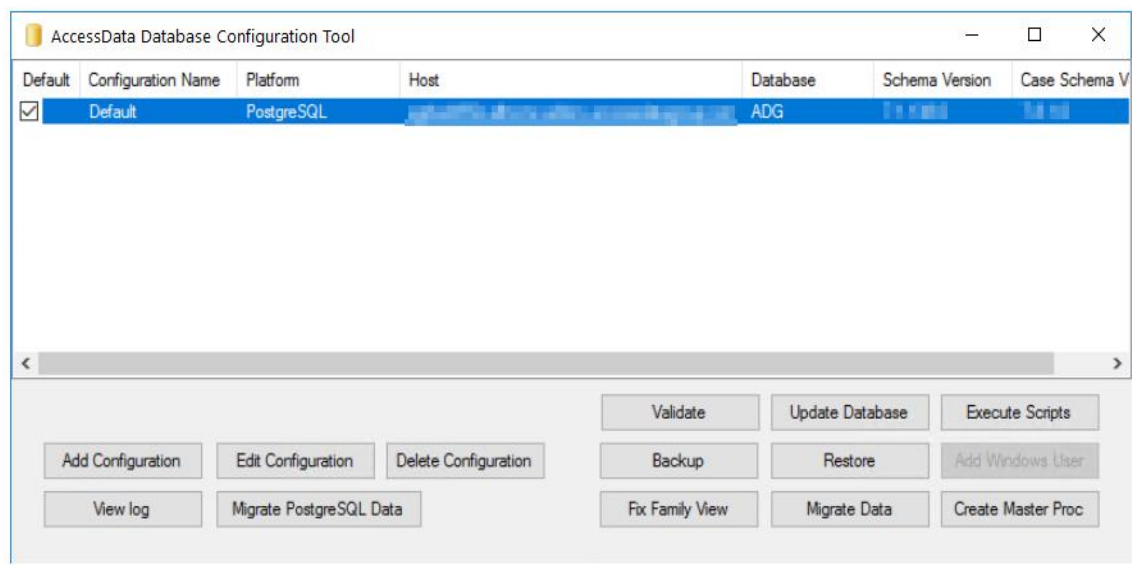
Transfer From...

Version: AccessData Database 7.1

Create Cancel

7. Click **Create**.

Note: Ensure the created **RDS Postgres** is listed in the 'Database Configuration Tool' window.



3 Maximizing AWS RDS Efficiency

a) Tailored Infrastructure Optimization:

- Infrastructure teams should customize settings to align with your specific needs, considering factors like concurrent usage, processing size, and any other unique requirements of your workload. This tailored approach ensures that your AWS RDS instance operates at its peak efficiency.

b) GP3 Flexibility and Cost Optimization:

- GP3 offers flexibility by allowing independent provisioning of storage, IOPS, and throughput. Moreover, it boasts a better price per GB compared to lower tiers, making it an attractive option for most users. This flexibility enables you to tailor your resource allocation precisely to match your workload requirements, optimizing both performance and cost-effectiveness.

c) Optimal Performance with GP3:

- For the best value-to-performance ratio, GP3 is Exterro's recommended choice. Unlike its predecessor GP2, which scales performance based on volume size, GP3 allows for direct adjustment of resources for improved performance without the need to increase storage size. This granular control empowers you to fine-tune your RDS instance to achieve optimal performance without unnecessary resource overhead.

- **Notes GP2 Vs GP3:**

- AWS provides (GP3 only) baseline values for IOPS and throughput, which serve as a starting point for your resource allocation.
- It is important to understand that GP2, disks under 400GB have baseline values of 3k IOPS and 125MB throughput, while GP3 disks 500GB+ utilize 12k IOPS and 500MB throughput.
- GP3 allows additional resources to be provisioned as needed, offering scalability and flexibility to accommodate changing demands.

d) Considerations on io1 and Cost-Benefit Analysis:

- While io1 offers higher throughput and IOPS in comparison to GP3, its significant cost increase may not always be justified. It's essential to conduct a thorough cost-benefit analysis to determine whether the performance gains justify the additional expense. This analysis should consider factors such as workload requirements, budget constraints, and potential performance bottlenecks to make an informed decision.

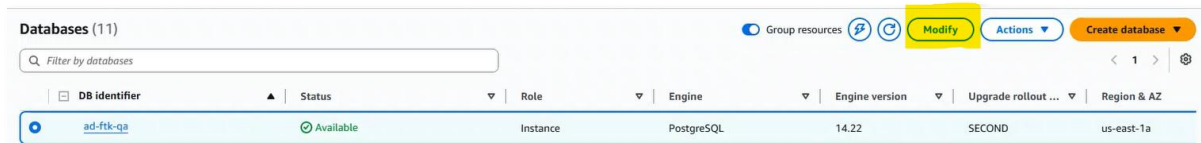
e) Usage Monitoring and Recommendations:

- Utilize RDS monitoring tools to track usage patterns and performance metrics continuously. By monitoring your RDS instance's performance closely, you can make adjustments accordingly.
- ***A recommended baseline for performance metrics includes 12k IOPS and a minimum throughput of 500MB/s***, which can serve as a starting point for optimization efforts. By following these comprehensive guidelines and leveraging the flexibility of AWS RDS, you can ensure that your infrastructure operates efficiently, effectively, and without any issues with resource allocation or performance optimization.

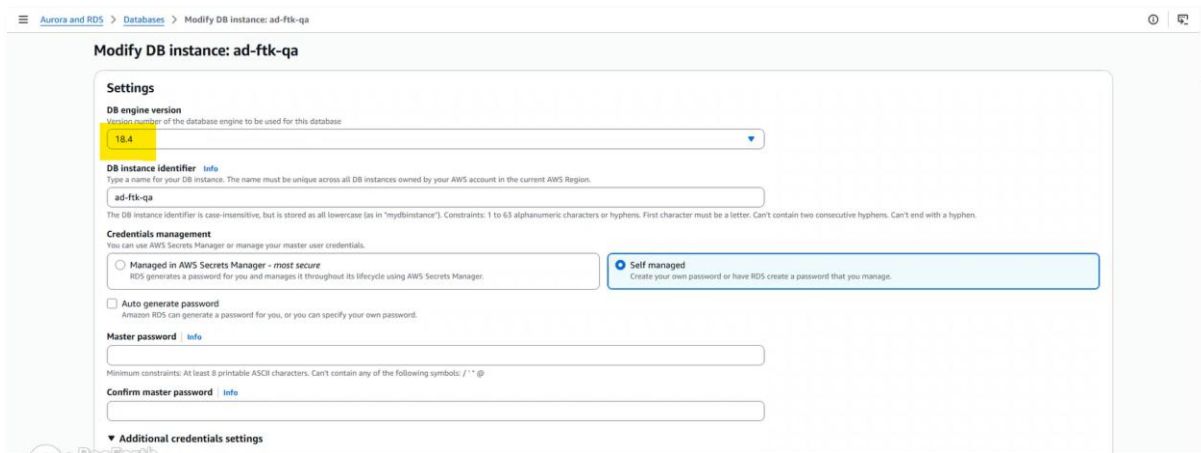
4 RDS Database Migration: 14.x to 18.4

4.1 Upgrade PostgreSQL Engine in AWS RDS

1. Log in to the **AWS Management Console** and navigate to the **RDS** section.



2. Select your existing PostgreSQL 14.x RDS instance and click **Modify**.
3. In the **DB engine version** drop-down menu, select **18.4**.



4. You can modify any optional parameters if necessary, then click **Continue**.

- Under **Schedule modifications**, select whether to apply changes immediately or during the next scheduled maintenance window.

Modify DB instance: ad-ftk-qa

Are you sure you want to upgrade your DB Instance?
 Once a DB instance has been upgraded, you cannot convert it back to the previous version. Please make sure you have tested both your database and your application with the new version before continuing. The upgrade will be applied either immediately (if you selected the Apply Immediately option) or during your next maintenance window (default). Please note that in either case, your database instance will have an availability impact for a few minutes as the upgrade is applied and your database instance is rebooted. For more information, see [major/minor version upgrade documentation](#).

Summary of modifications
 You are about to submit the following modifications. Only values that will change are displayed. Carefully verify your changes and choose **Modify DB Instance**.

Attribute	Current value	New value
Engine version	14.22	18.4
DB parameter group	postgresql-test-group	default.postgres18

Schedule modifications
When to apply modifications
☒ **Apply during the next scheduled maintenance window**
 Current maintenance window: September 12, 2025, 12:52 - 13:22 (UTC+05:30)
☐ **Apply immediately**
 The modifications in this request and any pending modifications will be asynchronously applied as soon as possible, regardless of the maintenance window setting for this database instance.

Cancel Back **Modify DB Instance**

- Click **Modify DB Instance** to start the upgrade process.

Note: Wait for the migration to finish until the confirmation banner appears: "Successfully modified [DB Instance Name]".

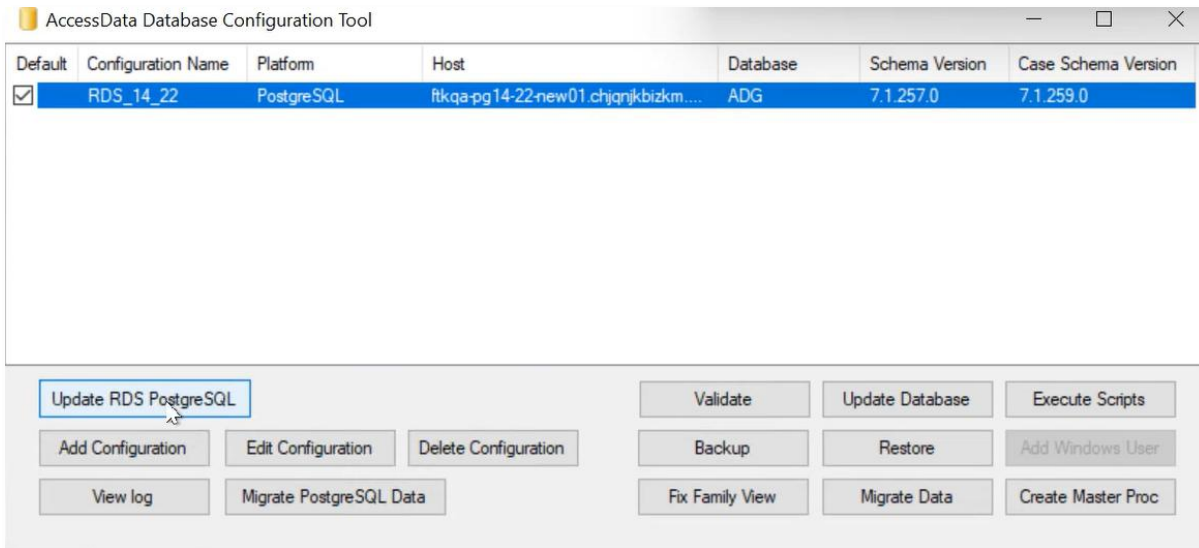
4.2 Initialize the Database

Follow the instructions provided in [Section 2: Initializing the Database](#) to initialize the database post-migration.

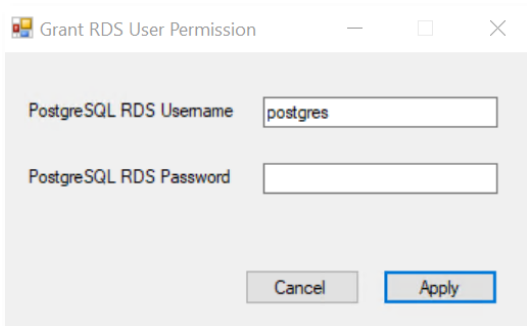
Note: Ensure the initialized database process completes without errors before moving to configuration.

4.3 Update Permissions via Configuration Tool

1. Open the **AccessData Database Configuration Tool**.
2. Confirm that the upgraded RDS PostgreSQL 18.4 database appears in the configuration list, then click to select it.
3. Click the **Update RDS PostgreSQL** button at the bottom-left of the window.

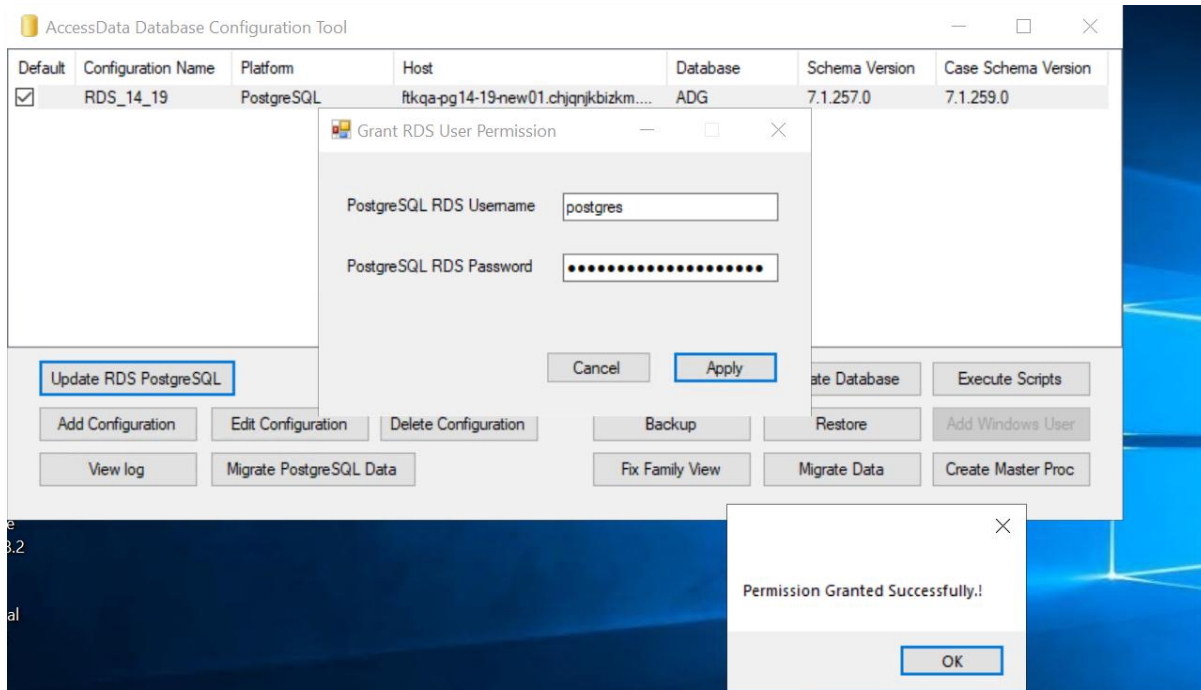


4. In the **Grant RDS User Permission** dialog box, enter the admin **PostgreSQL RDS Username** and **PostgreSQL RDS Password**.



5. Click **Apply**.

6. When the "Permission Granted Successfully.!" pop-up appears, click **OK**.



Note: Check that the pop-up confirms "Permission Granted Successfully.!" and close the window.

For any RDS upgrade queries or technical assistance, contact support at support@exterro.com.

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.**

2175 NW Raleigh St., Suite 110

Portland, OR 97210.

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 documentation for purposes of evaluating its functionality, or for any other competitive purposes.

If you have any questions, please contact Customer Support by email at support@exterro.com.