exterro®
Data Risk Management

FTK - RDS ENVIRONMENT SETUP GUIDE

SEPTEMBER 2026

Table of Contents

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.

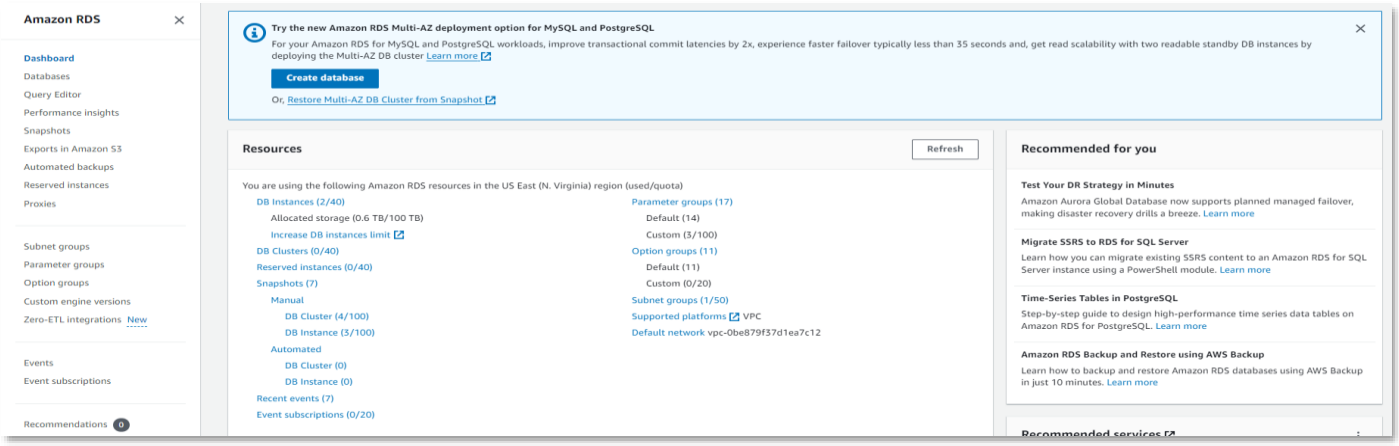
PostgreSQL RDS is a managed service from Amazon. As a managed service, RDS restricts users with certain roles from accessing the FTK application upon setting up the database using the DBConfig utility. For Forensic Tools to work with PostgreSQL RDS, you will need to perform certain operations that are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

1 Creating a PostgreSQL RDS Instance

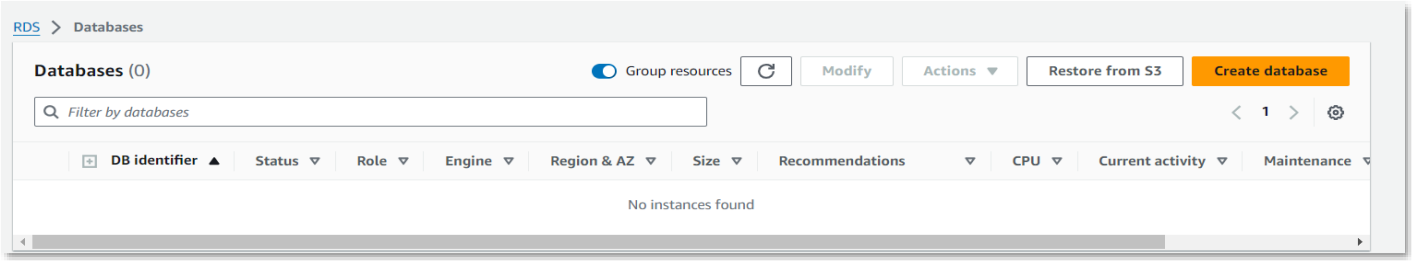
Follow these steps to set up a PostgreSQL RDS instance:

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.

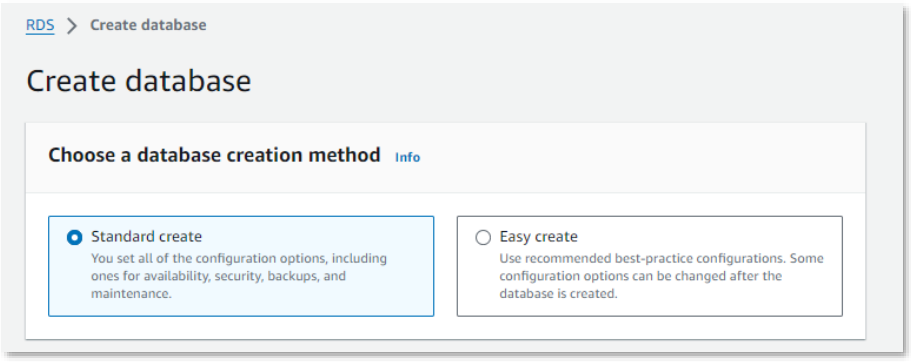


3. Click on **Databases** in the left pane.
   - The RDS Databases page is displayed.

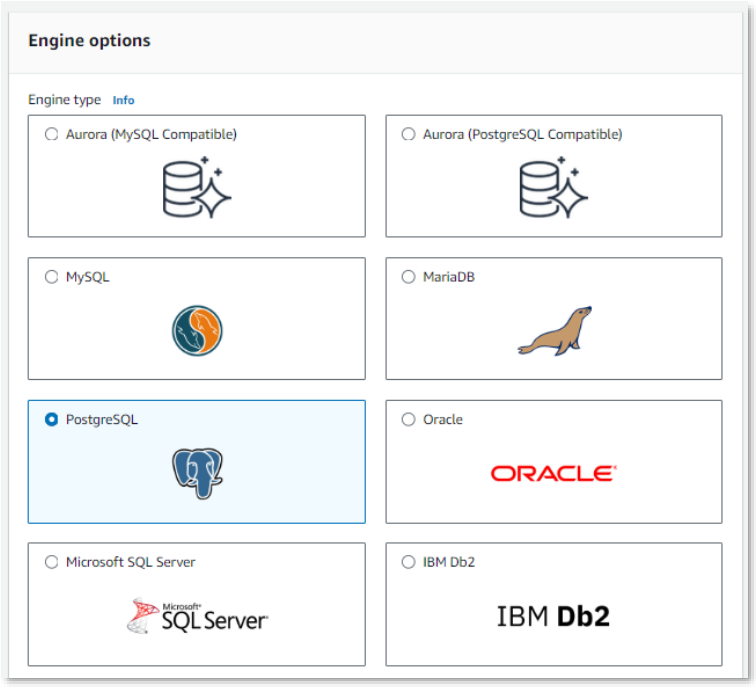


4. Click the **Create database** button located in the top-right corner.

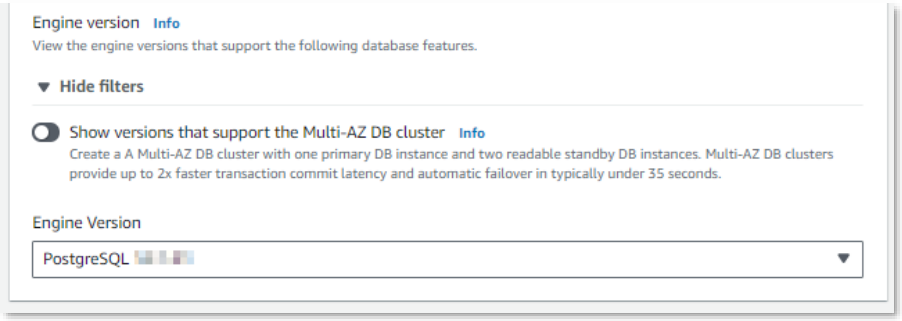
- The **Create database** pop-up is displayed.



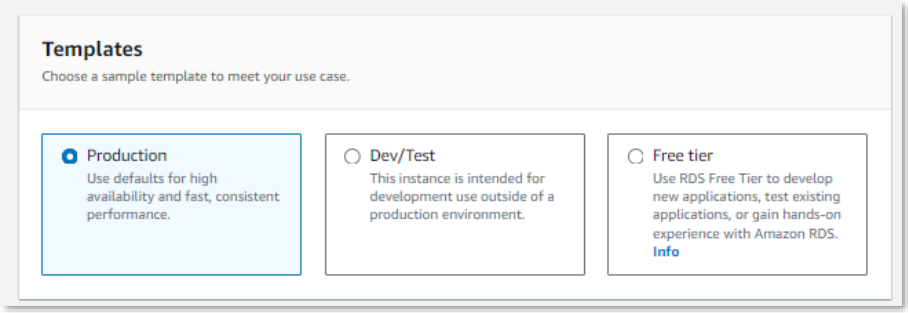
5. Choose the database creation method as **Standard create**.
6. Select **PostgreSQL** as the **Engine type**.



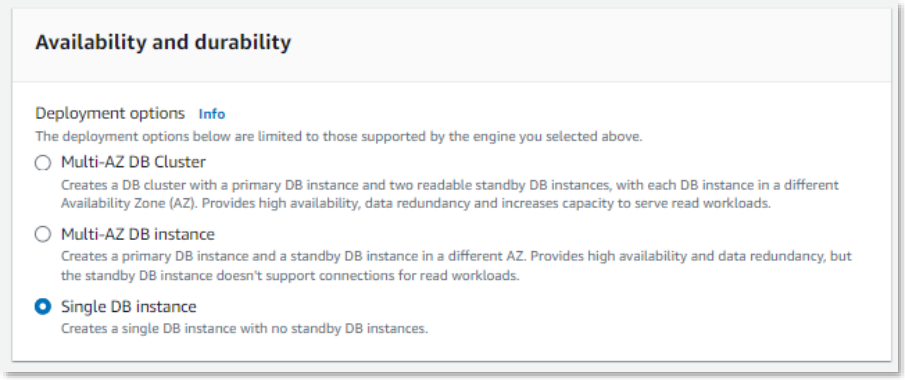
7. Select the **Engine Version** to 14.x version. (The recommended version is **PostgreSQL 14.19**).



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



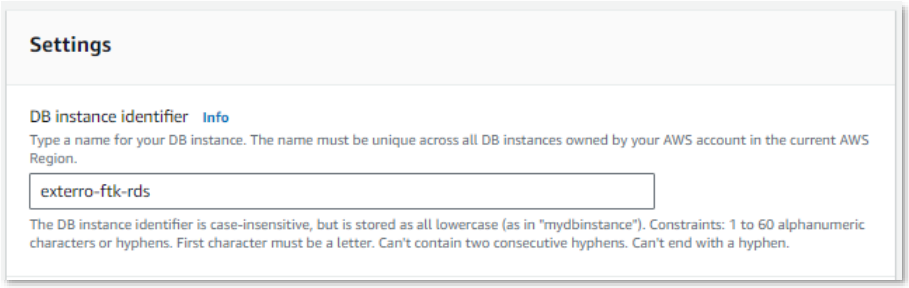
9. In the 'Availability and durability' section, select **Single DB instance** as the Deployment option.



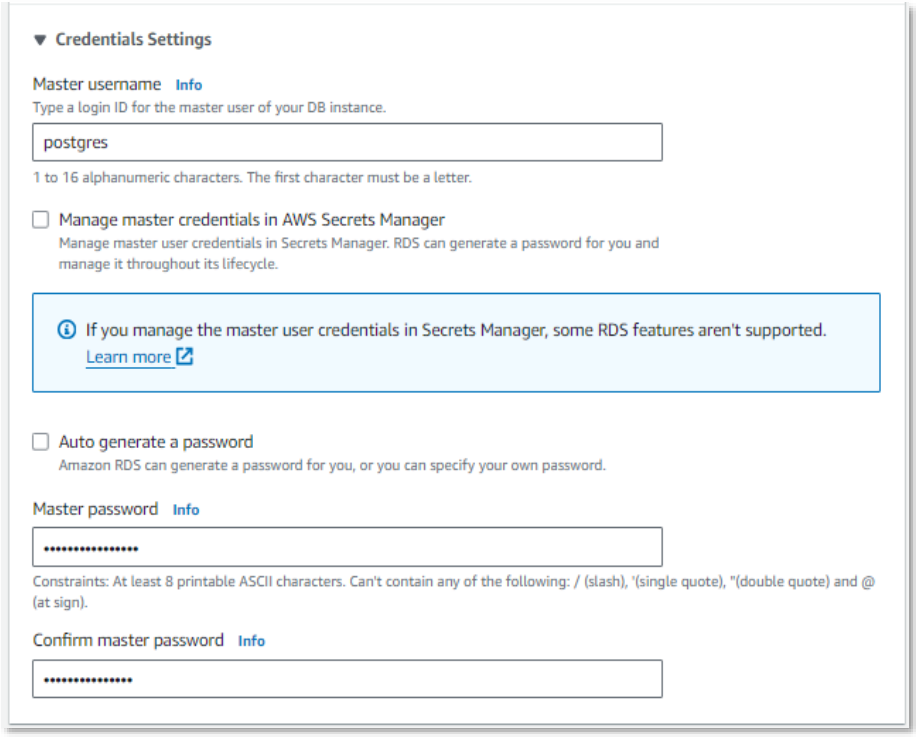
10. Provide the following details in the **Settings** section:

- **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.*



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

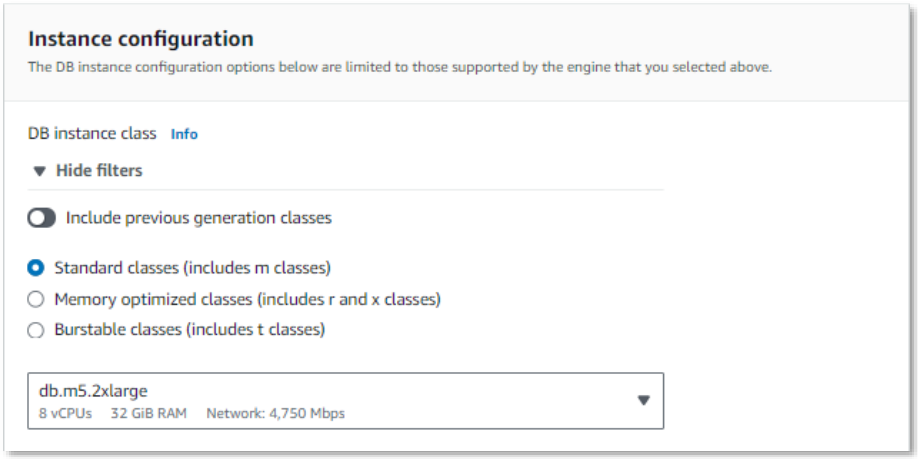


11. In the **Instance configuration** section, select the appropriate DB instance class based on performance requirements. It is recommended to utilize Memory-Optimized instances.

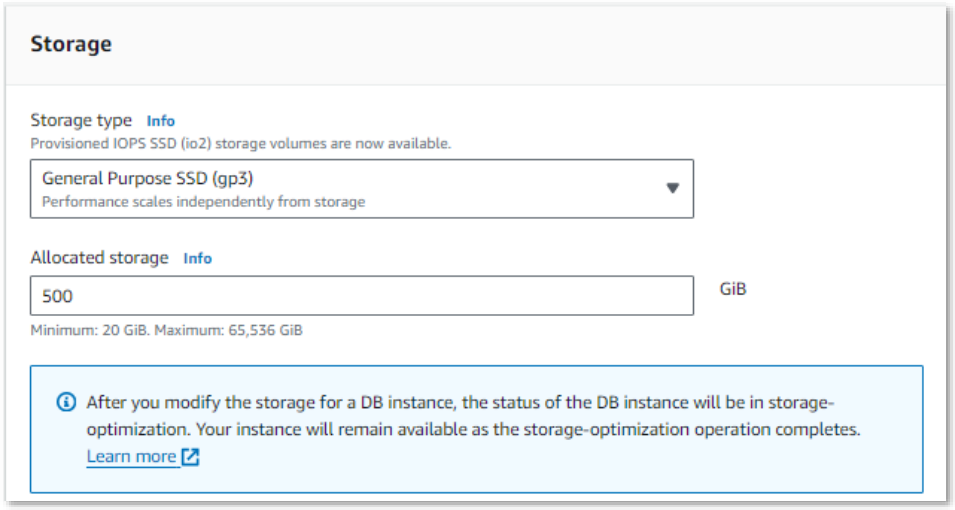
    ***Note**: Instance types can be changed at a later date if a reserved instance is not selected.*

    Specifications:

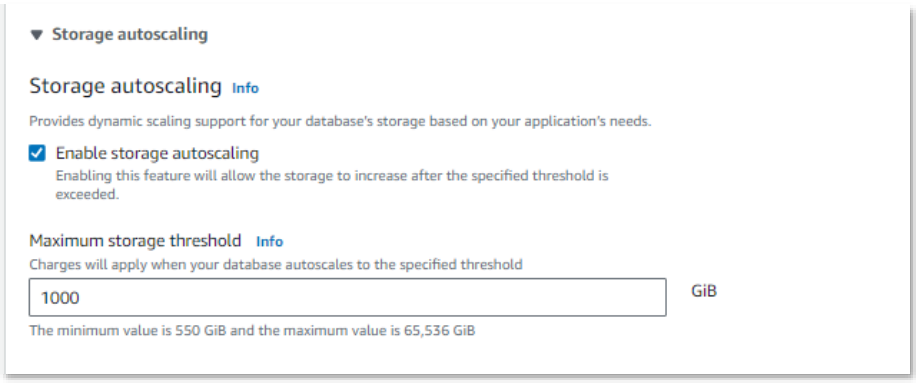
    - Minimum Hardware Configuration: 16 GB, 4-core
    - Recommended Hardware Configuration: 32 GB, 8-core
        - Users should consider at least 4GB/per core



12. Under the **Storage** section, select **General Purpose SSD (gp3)** as the Storage type.
    - ***Refer to** [Maximizing AWS RDS Efficiency]*.

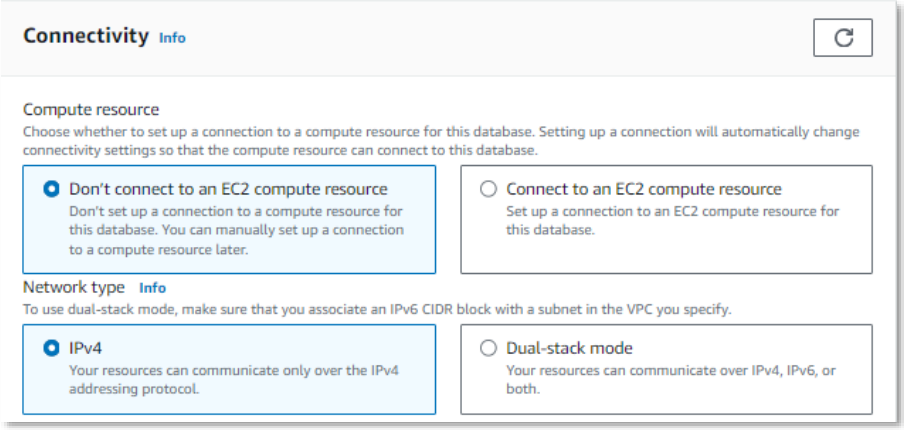


***Note**: Auto scaling for storage can be extended up to 65TB as per AWS guidelines.*



13. In the **Connectivity** section:

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

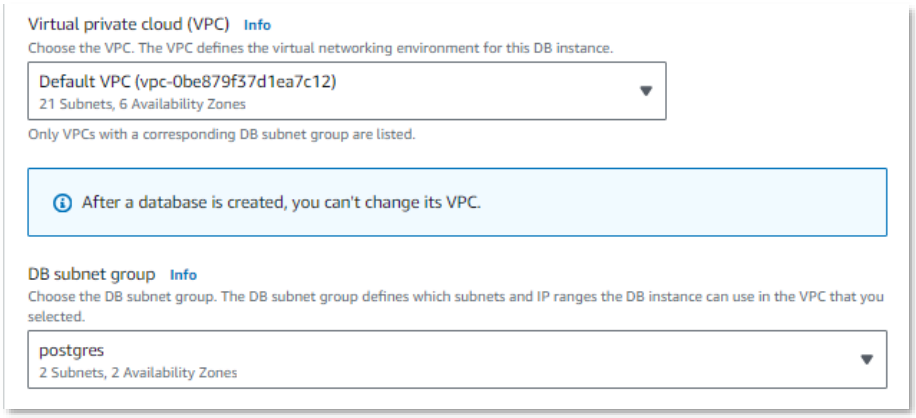


- Specify the **Virtual Private Cloud** (VPC) for the DB instance.

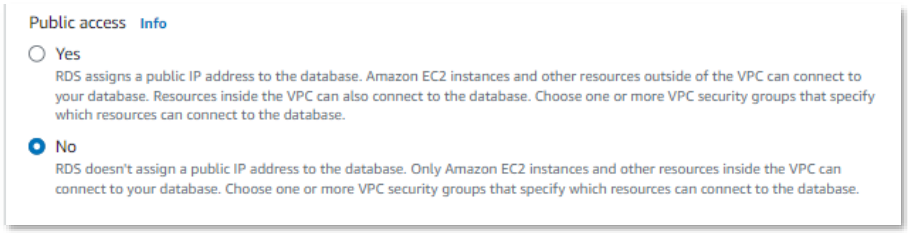
  ***Note:** This ensures that the RDS instance operates within a designated VPC, which should align with the VPC used by the Forensic Tools application.*

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

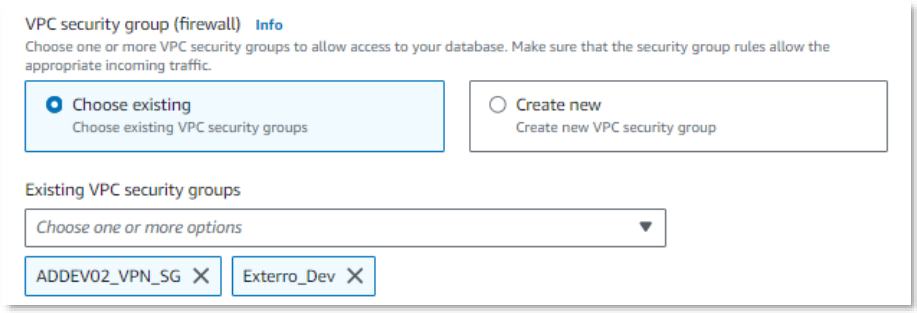
  Note: *The subnet group specifies the subnets and IP ranges available for use by the associated DB instance within the VPC.*



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

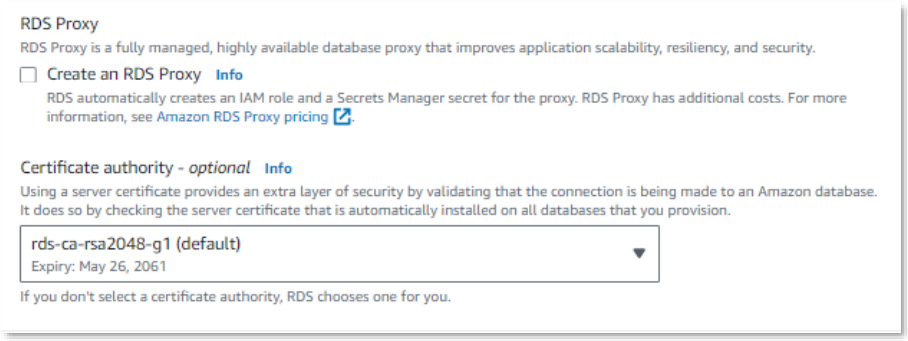


14. In the **VPC security group (firewall)** section, choose one or more VPC security groups to permit access to the database. Ensure that the security group rules are configured to allow the necessary incoming traffic from any EC2 instances running FTK Central, FTK Core, the Distributed Processing Manager,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

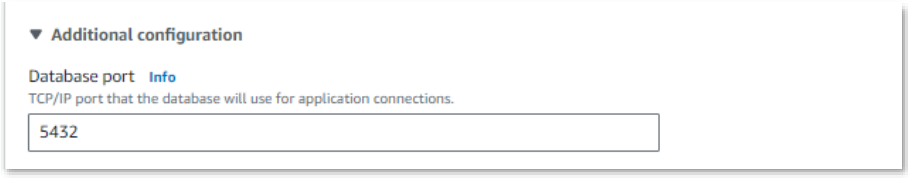


15. Set the Availability Zone to 'No preference', as the chosen VPC and Subnet will automatically select the appropriate zone.

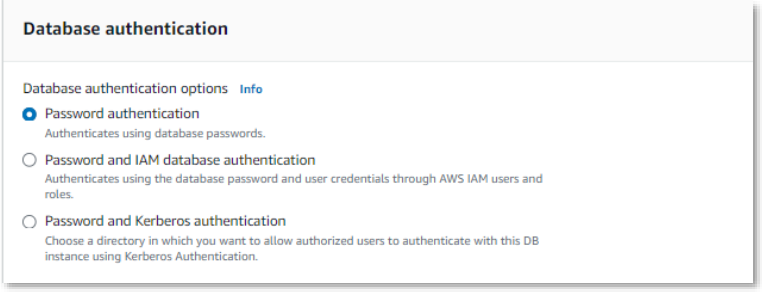
***Note**: The default settings for Proxy and Certificate Authority will be retained.*



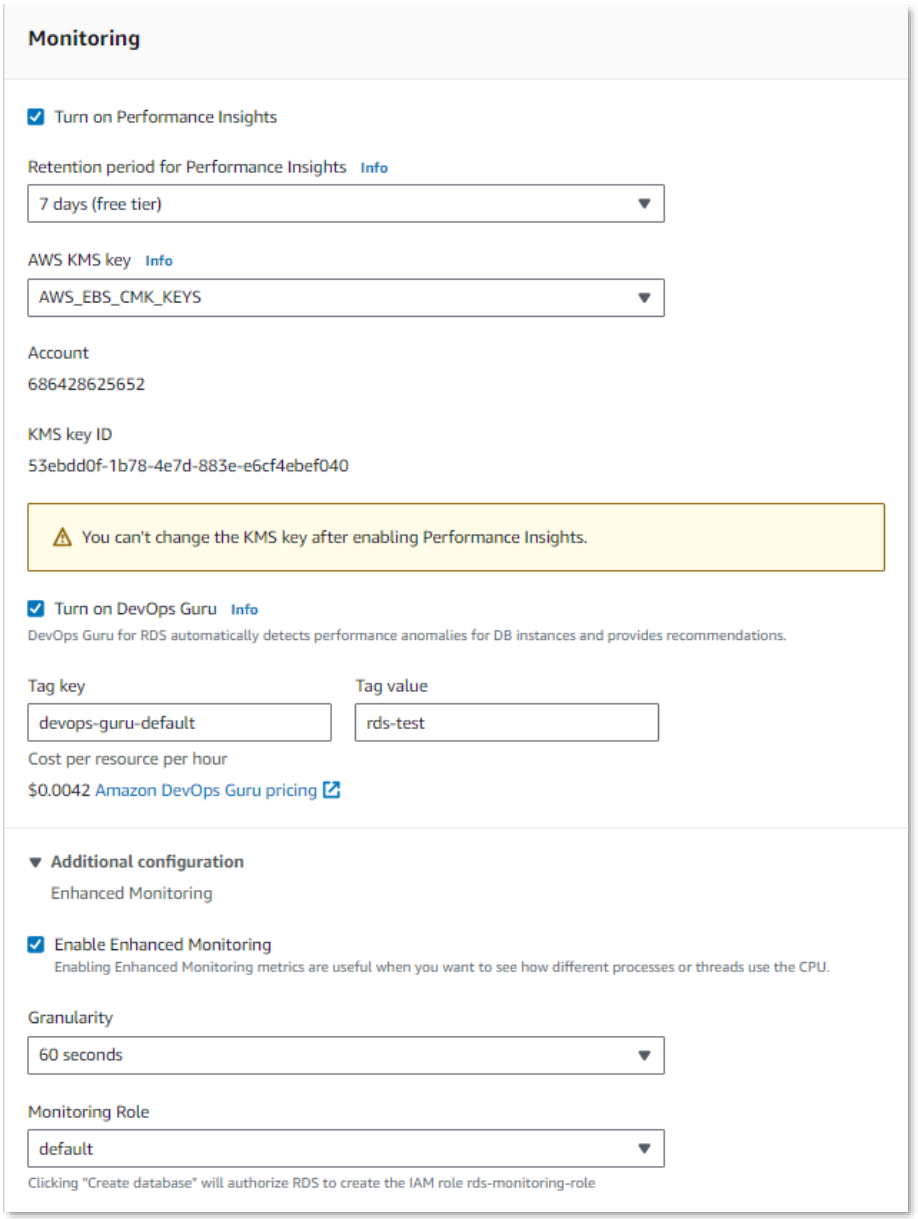
16. In **Additional configuration,** set the **Database port** to **5432** (default for PostgreSQL).



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

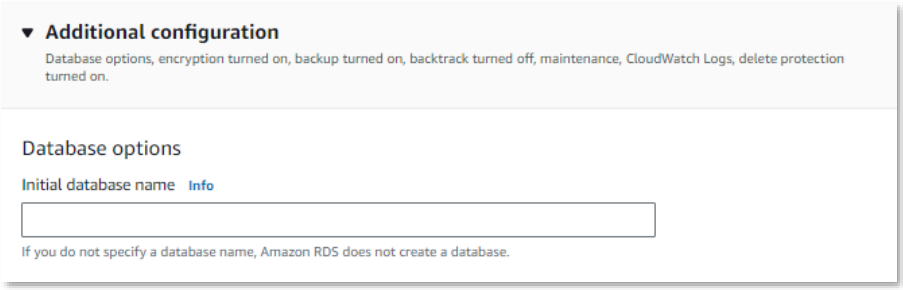


18. In the **Monitoring** section, stick to the default settings. For the AWS KMS key, you can opt for the default option or select Customer Managed Keys (**CMK**) if preferred. In this case, CMK keys have been chosen. All other settings can remain as default.



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

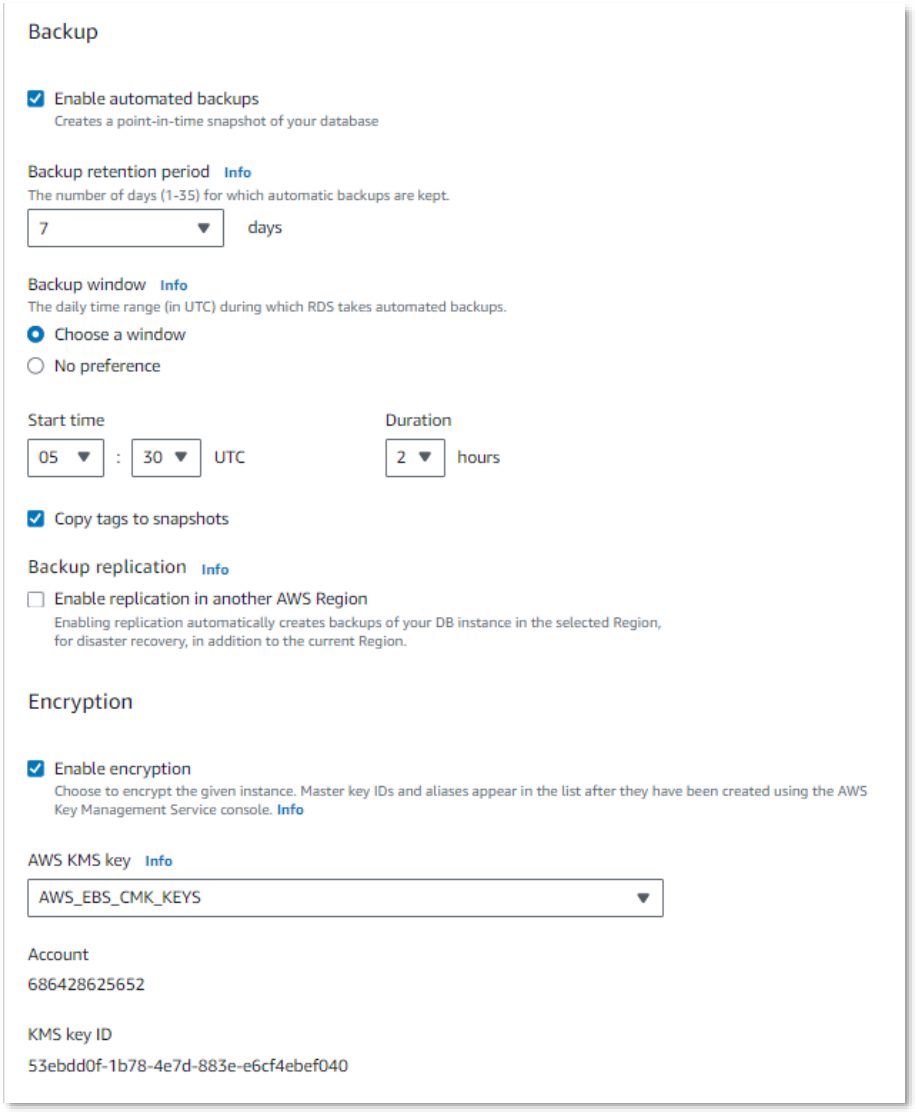
- **Initial database name**: You are recommended to leave this field blank.



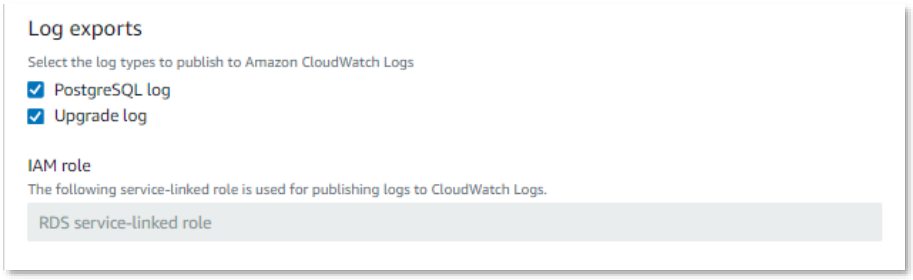
- **DB parameter group**: Select the DB parameter group that configures settings for this DB instance.
    - You can stick with the default value or create a parameter group tailored to the specific PostgreSQL version being.

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

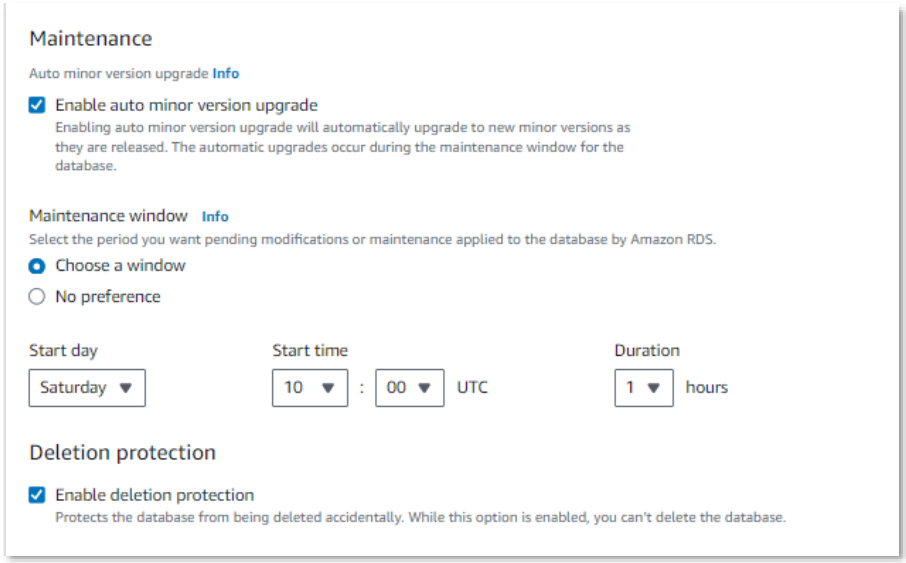
20. Configure the following settings in the 'Backup' section:
    - **Enable automated backups**: Check this box to activate automated backups for the database.
    - **Backup retention period**: Set the number of days for which the database will be automatically backed up. We recommend a retention period 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.



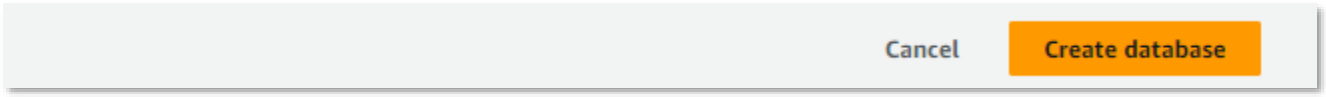
21. Select the log types to be published to Amazon CloudWatch Logs. Select both PostgreSQL logs and Upgrade logs. Leave the IAM role setting as default.



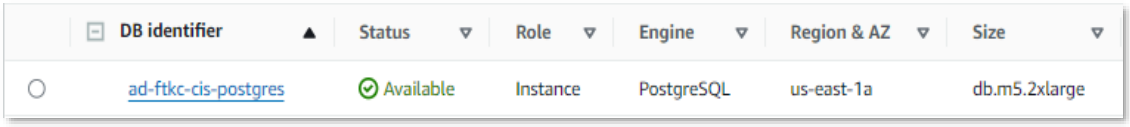
22. Configure the following details in the **Maintenance window** section:
    - **Enable auto minor version upgrade**: Select this option to automatically receive updates when they are available.
    - **Maintenance window**: Select your preferred time period for applying pending modifications or maintenance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



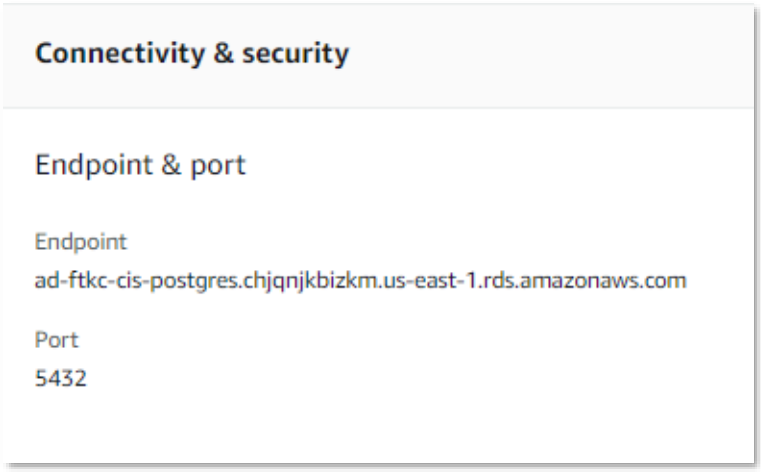
23. Click **Create database**.



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



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:

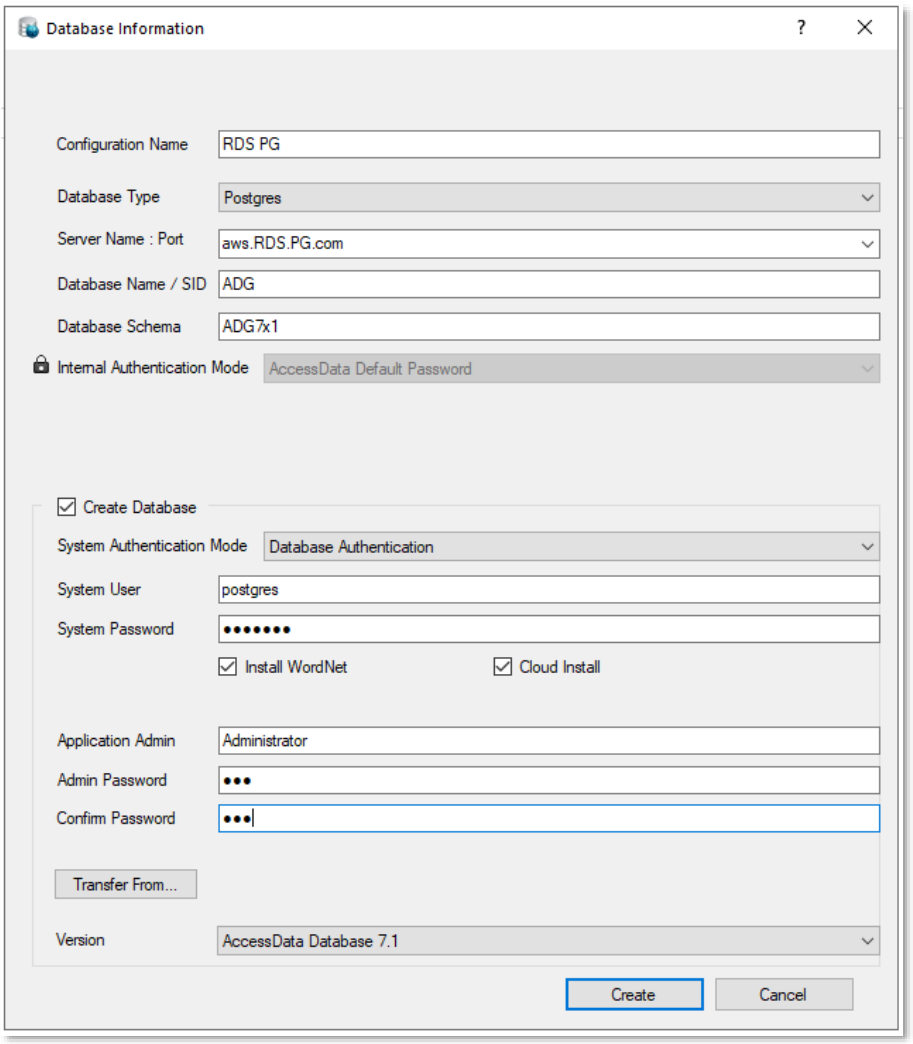
1. Once the FTK application is installed, navigate to 'DBConfig.exe',

   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.

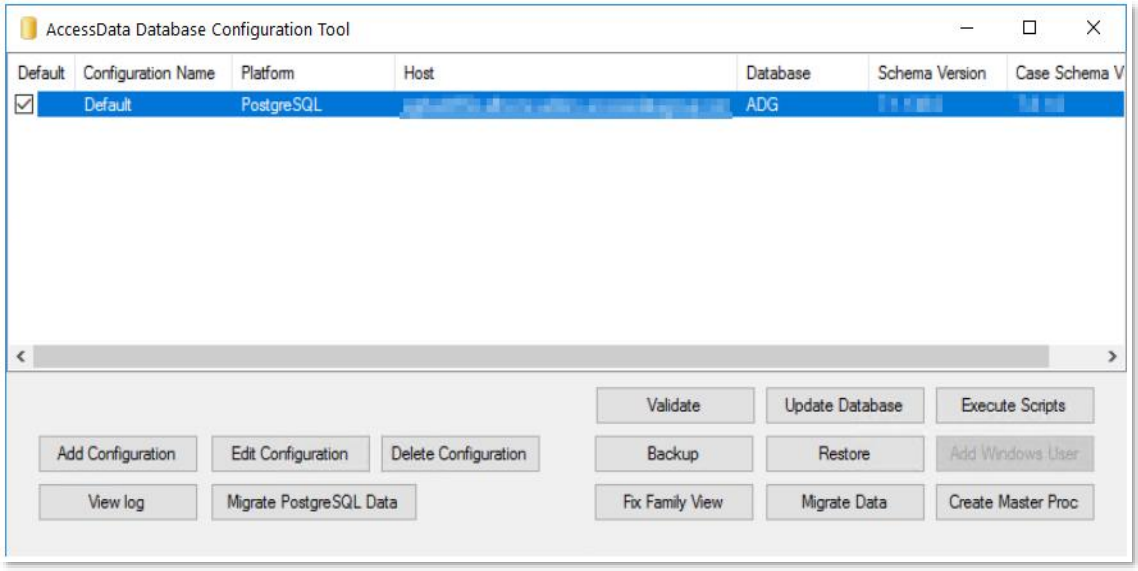
   Ad-ftkc-cis-postgres.axxxxxxxxsd.us-east-1.amazonaws.com:5432

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



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:

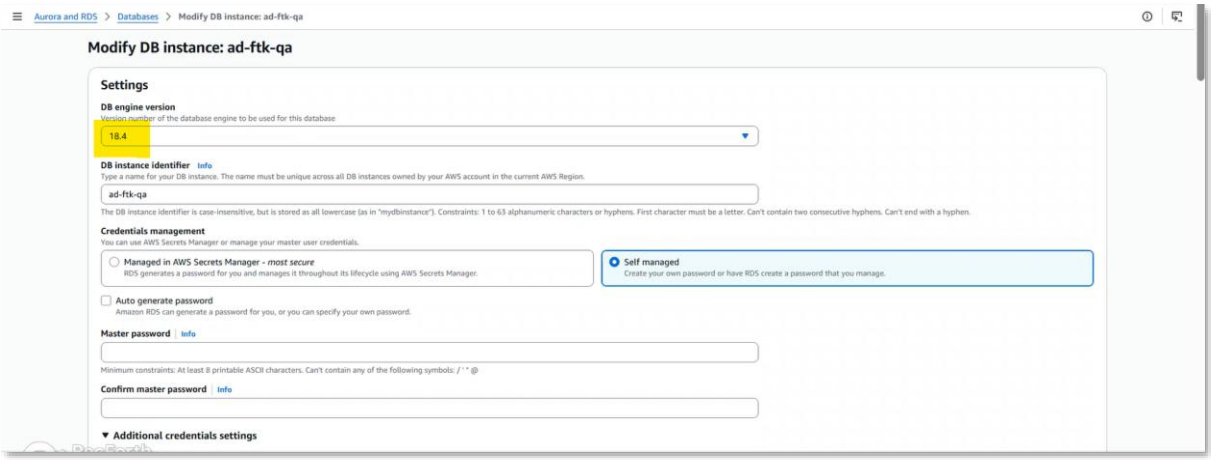
- Utilize RDS monitoring tools to track usage patterns and performance metrics continuously. By monitoring your RDS instance's performance closely, you can make adjustments accordingly.
- ***A recommended baseline for performance metrics includes 12k IOPS and a minimum throughput of 500MB/s***, which 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

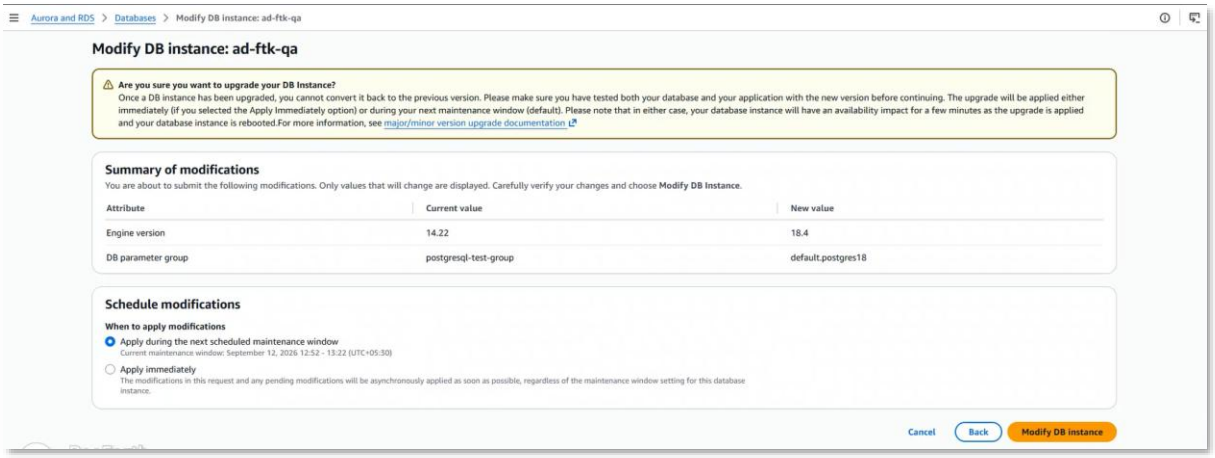
1. Log in to the **AWS Management Console** and navigate to the **RDS** section.

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**.

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



6. 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]".*

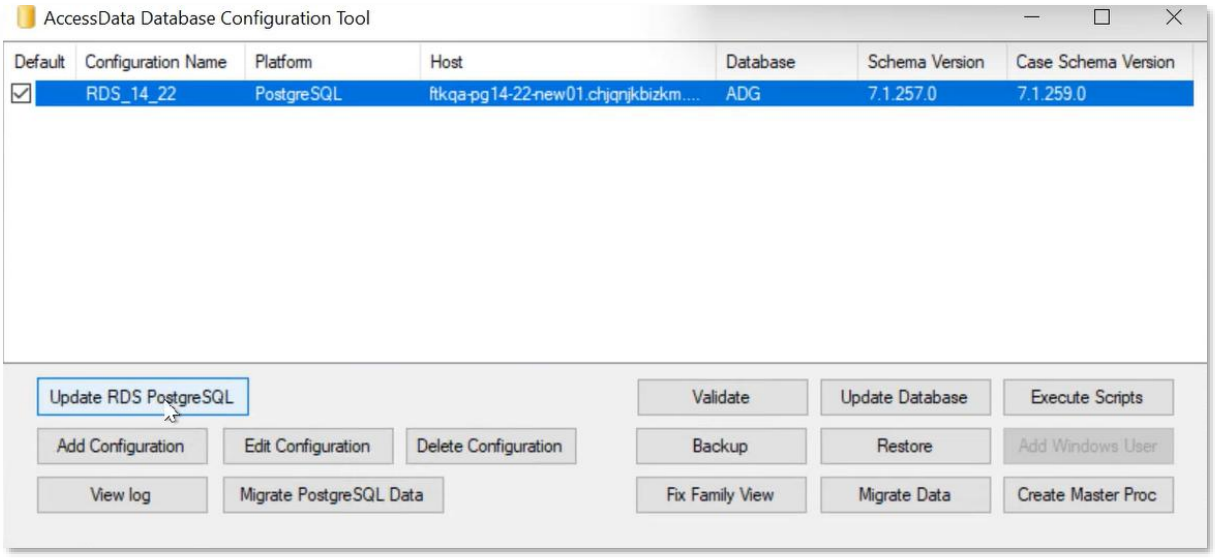
4.2 Initialize the Database

Follow the instructions provided in *Section 2: Initializing the Database* to initialize the database post-migration.

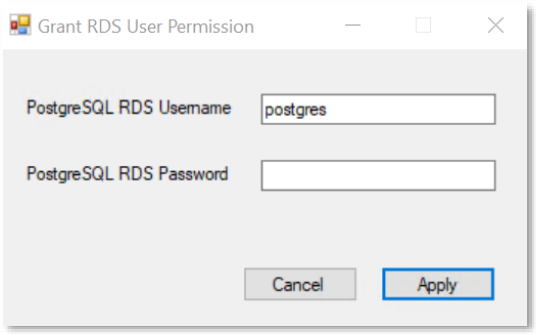
***Note**: Ensure the initialized database process completes without errors before moving to configuration.*

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.

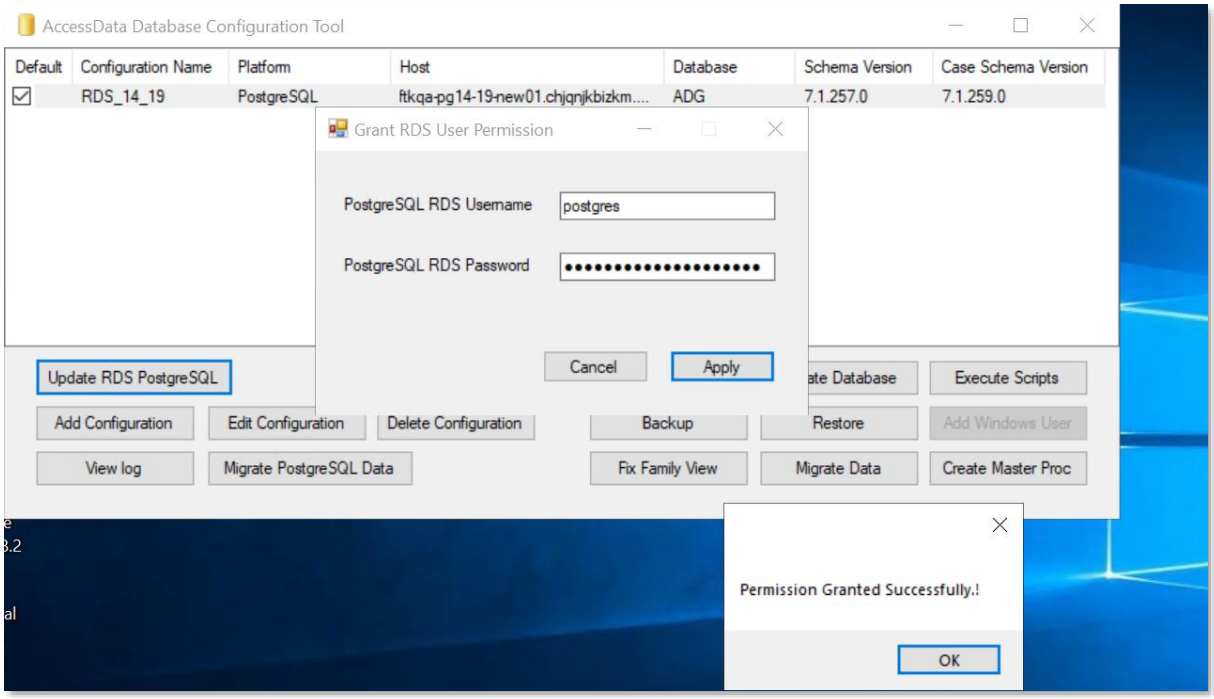


4. In the **Grant RDS User Permission** dialog box, enter the admin **PostgreSQL RDS Username** and **PostgreSQL RDS Password**.



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