
EDB
Postgres for the AI Generation
EDB RDBA Security
www.enterprisedb.com

TABLE OF CONTENTS

EDB RDBA Security

This white paper provides an overview of the EDB Remote Database Administration (RDBA) security stance and the approach toward our customers.

The nature of the RDBA service requires our engineers to have access to customers' databases. But it is essential to understand that RDBA engineers would not need to - and do not - access the actual data in database tables. We don't read this data, we don't transfer it outside the customer environment, and we don't store it anywhere. We work with system and database metadata, database structure (including object names like tables and columns, but not the actual data within those) and logs, and we treat those in a safe and secure way as described further in this document.

We have implemented a set of policies and procedures to comply with security best practices and industry standards, that are confirmed by independent auditors (see below).

Overview

The following provides a brief description of RDBA service components, with a focus on security.

Database Access

Access to the customer's database is the cornerstone of RDBA service. To provide reliable and secure access to the customer environment, we have a dedicated Unified Access Infrastructure (UAI) as well as wrapping procedures and controls.

UAI is hosted using a certified vendor (see the Certification and Vendor Requirements section below), and the data there is protected both in transit and in rest (see the appropriate paragraphs).

UAI was also part of the SOC2 certification.

Connection Variants

Connection to various customer environments is flexible. From our end points (called hop boxes), we can connect directly, through proxies (jumphosts), use client-to-site VPNs, or use permanent site-to-site VPN tunnels.

Access and User Management

On the EDB side, we have applied access procedures to ensure that only staff who support the service offering in the customer environment have appropriate access and permissions.

On the customer side, we can work with either individual user accounts for our engineers or a shared account. While the first option is better from a security and compliance point of view, we understand that for some customers it might not be feasible to maintain separate accounts for our engineering team.

Please note that some security measures like password complexity or appropriate permissions in the customer environment are beyond our control and must be implemented according to your internal policies and requirements.

Monitoring

Monitoring is an essential part of the EDB RDBA service, as it allows our engineers to react to production incidents swiftly as well as providing the data for proactive work that can prevent those incidents and/or improve the customer's database performance.

Our monitoring system, called Sentinel, runs on a client-server architecture. The client is installed on the target host and is run periodically using cron. With every run, it collects the required data from both the database and operating system and sends it to the server-receiver. Our engineers can see the results in the GUI running on the server.

Network Security and Requirements

The network connection is always initiated from the target host toward the monitoring server, so no inbound traffic to the customer environment is required. The only requirement is to allow outgoing connection toward the monitoring server IPs (two are used to support high availability of the service). In case your database hosts don't have direct internet connection, the Sentinel monitoring agent can send the data through the proxy server.

Apart from the server-unique key that is used for proper identification with our monitoring schema, there is an application-level firewall on the monitoring server that allows it to receive payload from allowed hosts only.

Software Development Lifecycle (SDLC)

The Sentinel development team uses the Agile methodology to track and organize its development work. Development work is tracked in Sprint iterations. Testing for deploying features includes both automated smoke/regression for some parts of the code, plus basic verification by peers for any functionality or bug fix that is deployed to production. Smoke tests are to be triggered on most important commits, or manually whenever needed.

Sentinel SDLC has been reviewed by external auditors as part of our SOC2 Type 2 Audit.

Ticketing

The network connection is always initiated from the target host toward the monitoring server, so no inbound traffic to the customer environment is required. The only requirement is to allow outgoing connection toward the monitoring server IPs (two are used for HA reasons). In case your database hosts don't have direct internet connection, the Sentinel monitoring agent can send the data through the proxy server.

Apart from the server-unique key that is used for proper identification with our monitoring schema, there is an application-level firewall on the monitoring server that allows it to receive payload from allowed hosts only.

User Management

Access to the Portal is managed by EDB single-sign-on (SSO). EDB RDBA engineers are able to access all customers' tickets, while the customer-side technical contacts can see their company tickets only.

The user management at the customer side is fully in your control. Selected technical contacts gain the privileges of the Company Admin and they can further add or remove any other contacts from their company.

Tickets

The tickets usually contain customer metadata that is needed to describe and solve the issue. This metadata includes the host names and/or IP addresses, parts of configuration, log excerpts, query execution plans, etc.

It should be noted that the actual database data is never to be part of the ticket. If received in the ticket update, our engineers are trained to redact this and report a security incident.

Emails

As described above, the ticket updates can be viewed in the Portal with all appropriate access and security controls in place. However, the Portal can be set up to also send the ticket updates as emails. Every Portal user can enable or disable this feature for themselves.

We do not force encrypted email communications, so email exchanges are readable.

Therefore, any data that is considered sensitive but needs to be shared as part of the ticket can be added to a ticket update as an attachment. Attachments can be accessed from the Portal only after passing the authentication/authorisation check. In the emails, the attachment is visible as a link to the Portal.

Other Means of Communication

While the Portal remains the primary communication channel, and the only relevant one from an SLO perspective, we also welcome auxiliary means of communication that can be more flexible than ticket exchanges in certain situations. These include Slack channels, Zoom bridges, etc.

Data can only be shared through these supplementary channels upon agreement with the customer about the sensitivity of the data.

Certification and Vendor Requirements

The EDB RDBA service is SOC2 Type 2 certified.

For all vendors that are used for delivering the RDBA service, we require SOC2/ISO27001 certification or higher or adequate security measures.

Vulnerability Scans and Penetration Testing

Both EDB RDBA software and infrastructure undergo regular internal and external scans for relevant types of vulnerabilities. Any findings are processed through our internal vulnerability management procedures, which require applying patches or an equivalent remedy within a timeframe defined according to the severity of the finding.

Sentinel monitoring undergoes assessment by independent penetration testers, either in regular periods or when needed because of major changes. Any findings from the penetration testing are processed and remediated in accordance with our internal risk management policies and procedures.

Data Security

Encryption in Transit

Data traffic is encrypted using Transport Layer Security (TLS) v1.2 or greater. This covers the ticketing via the Portal, including attachments, monitoring data, etc.

Encryption at Rest

Servers involved in delivering RDBA services have all their partitions encrypted. Amazon S3 storage, where used, is encrypted as well using native object methods within the CSP. Our engineers' endpoint devices (laptops, desktops) have their drives encrypted as well.

Access Control

EDB RDBA engineers' access is managed according to our internal user and access policies and procedures, as well as the acceptable usage policy. Our staff needs to be logged into our internal VPN to be able to access our systems from their managed endpoint devices (laptops). multi-actor authentication (MFA) using biometrics is mandatory, ensuring the identity of the person trying to access the systems.

We have implemented audit-confirmed regular access control procedures, as well as standardized processes for onboarding/changing/leaving personnel.

Data Retention

As stated previously, EDB does not access or process the actual customer content within the database. There is, however, the metadata collected from the monitoring andstated in the tickets or in our internal documentation (e.g., technical contacts or connection guidelines).

This data is treated according to our internal data retention and disposal policies and procedures and is removed

Customer Database Security

Assessing our customer's database security is part of the Database Health Scan (DHS) that is done upon customer onboarding and again upon request or service agreement. The output of the DHS can contain various recommendations on how to improve the security measures, and those can be turned into proactive tasks in the RDBA service.

Specific questions or requirements from the customer regarding the database security are assessed by our engineers as well.

Tech Alerts

Whenever there is a serious vulnerability detected, either in the community PostgreSQL database and related tools or in the appropriate software developed by EDB, we send our customers a Tech Alert with the warning and proposed solutions. If you are directly affected, our staff will contact you with a remediation plan.

EDB

EDB provides a data and AI platform that enables organizations to harness the full power of Postgres for transactional, analytical, and AI workloads across any cloud, any time.

For more information, visit www.enterprisedb.com.