PostgreSQL azure_superuser - common security questions

Last updated by | Juvenal Hernandez Carrillo | Sep 2, 2021 at 5:53 PM PDT

Contents

Issue

Suspected successful brute-force attack

- Customer has received an alert about a possibility of a malicious attack on the Postgres DB server, in the details, the system noticed Succeeded and Failed Logins from client ip: 127.0.0.1, using azure_superuser acccount.
- Customer wants to know about these alerts in Security Center, and if there was any attack on this DB server or confirmation of a false positive.
- Customer wants to understand how it is possible that the azure_superuser account was able to access their PostgreSQL.
- Customer would like to understand what the azure_superuser is capable of and if this account is capable of accessing their data.

Investigation/Analysis

After checking my telemetry I couldn't see any failed connections and it correlates with the metrics in azure portal.

Email reported at: 2021-08-31 16:24 UTC Activity start time: 2021-08-31 15:24 UTC

let ServerName = "fh-posql-prd-we-01";

MonLogin

| where server_name =~ ServerName or LogicalServerName =~ ServerName or logical_server_name =~ ServerName

```
| where TIMESTAMP > datetime('2021-08-31T15:24:00') and TIMESTAMP <= datetime('2021-08-31T18:24:00')

| where peer_address == "127.0.0.x"

| where event == "process_login_finish"

| where error <> 0
```

Mitigation

They are false positives due to regression we had. The deployment had been reverted, so there would no be more of those. This can be safely ignored.

RCA Template

A safe deployment of Threat Detection has upgraded a component with a minor version update of a Parquet data format library that is used in Big Data Analysis. The library had introduced an external regression that is exposed during concurrency situation, leading to data corruption: #122 : "Column data errors when writing string columns to individual parquets concurrently".

The data corruption lead to false positive alerts sent to customers on the 8/31/2021 in West Europe region.

Due to the complexity of this regression and its applicability only in high load situations, it started to affect only in West Europe region. Once detected, engineers have investigated the false positive and reverted to the previous deployment to mitigate the issue.

More Information about azure_superuser

Common questions from supportability about azure_superuser.

- If an external attack reveals the password for the azure_superuser account, is there an unauthorized login?
- Also, as a privileged user, are you aware that any action is possible if you are logged in?
- Is it possible to login user Databse using azure_superuser if attacker gets the password?
- Do we have any protections to prevent from getting password of azure_superuser?

Possible Answers:

(use carefully, for clarification purposes only)

This is a system account created by Microsoft to manage the server to conduct monitoring, backups operations, and other regular maintenance activites. These are automated task, meaning no human interaction login into the server.

Since Azure Database for PostgreSQL is a managed database service, users are not provided with superuser access. This is because modifying configuration files such as postgresql.conf has adverse effects on service availability and Data consistency. The Azure_superuser is owned by Microsoft and is responsible only to do periodic health checks, maintenance activities and backups operations. Azure super user does have access to the server to perform these activities automatically but it doesn’t have access to custom data. We do use this role to perform operations on behalf of the customers and also collect various stats and metrics that are required to investigate issues and keep the service running. Customers can always enable audit logs to see what is happening on their server.

On-call engineers may also use this account to access the server during an incident with certificate authentication and must request access using just-in-time (JIT) processes, all activity is monitored. So, there is no possibility to break-decipher the String password as it is not a regular account, having different method of authentication.

We should be clear the customer here that this user was built in for Microsoft use only, and the scenario mentioned here is not an option in Azure environment which is PCI DSS-compliant, as there are multiple levels of security, one level we had in Azure database for PostgreSQL is that we secure the data by encrypting data in-transit with Transport Layer Security. Encryption (SSL/TLS) is enforced by default.

Other level that the Connections to an Azure Database for PostgreSQL server are first routed through a regional gateway. The gateway has a publicly accessible IP, while the server IP addresses are protected, and every newly created Azure Database for PostgreSQL server has a firewall that blocks all external connections, though they reach the gateway, they are not allowed to connect to the server, so to be able to connect, you should have the password and also you should be whitelisted in the database firewall.

More information about admin user and superuser

While creating a server, you set up the credentials for your admin user. The admin user is the highest privilege user you have on the server. It belongs to the role azure_pg_admin. This role does not have full superuser permissions.

The PostgreSQL superuser attribute is assigned to the azure_superuser, which belongs to the managed service. You do not have access to this role.

An Azure Database for PostgreSQL server has default databases:

postgres - A default database you can connect to once your server is created. azure_maintenance - This database is used to separate the processes that provide the managed service from user actions. You do not have access to this database. azure_sys - A database for the Query Store. This database does not accumulate data when Query Store is off; this is the default setting. For more information, see the Query Store overview.

Maximum connections - The maximum number of connections per pricing tier and vCores are shown below. The Azure system requires five connections to monitor the Azure Database for PostgreSQL server.

Public Doc Reference (optional)

Please find more information about azure_superuser in the following links:

https://docs.microsoft.com/en-us/azure/postgresql/concepts-servers

https://docs.microsoft.com/en-us/azure/postgresql/howto-create-users

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause:
Azure/Azure Database for PostgreSQL single server/Security/Threat protection with Azure Defender

How good have you found this content?

🙂 🙁