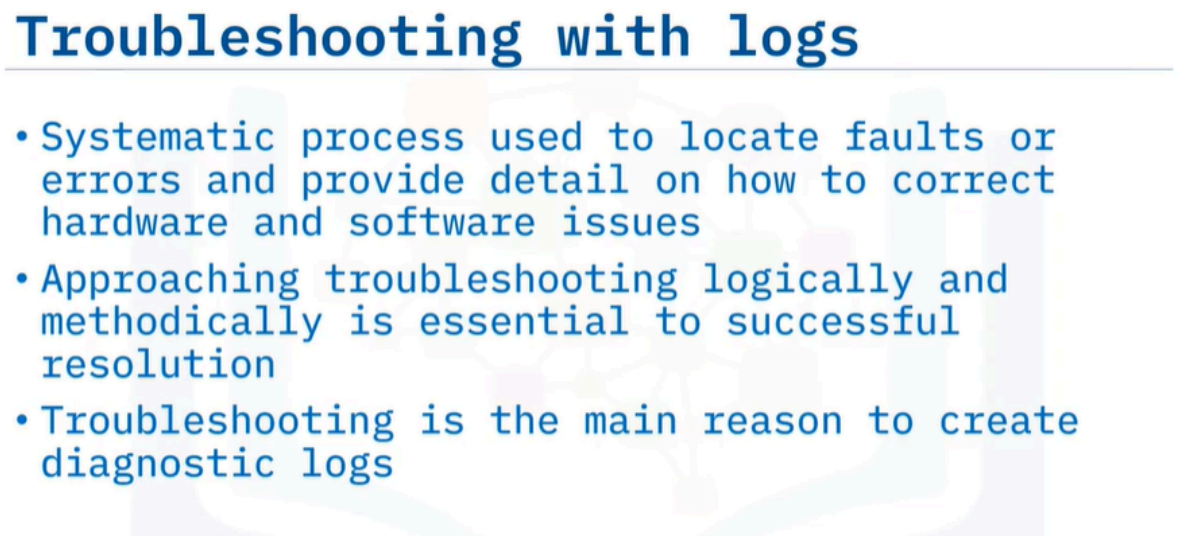
Using Logs for Troubleshooting

Sure! Let's talk about diagnostic logs and their purpose in troubleshooting.

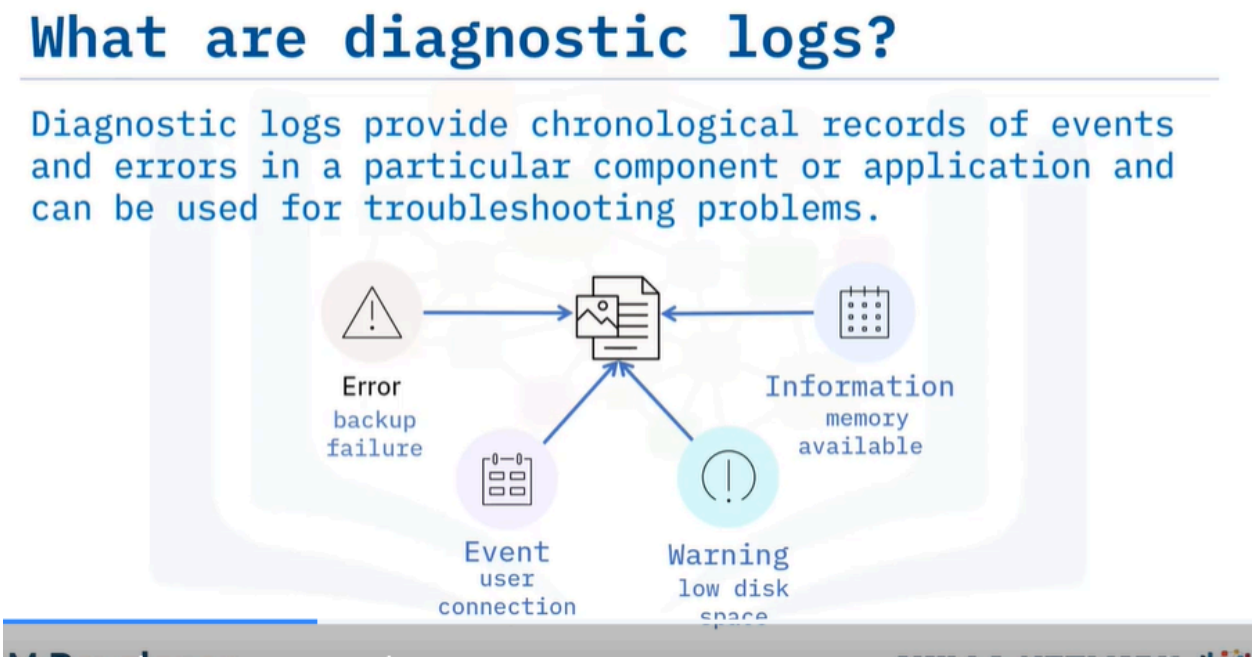
Diagnostic logs are like a diary for computer systems. They keep a record of important events, errors, and messages that happen within a system or application, such as a web server or a database. Imagine if your computer had a little notebook where it wrote down everything that went wrong or any important actions taken, like when a user connects or when a file is missing. This helps computer experts, like Database Administrators (DBAs), figure out what went wrong and how to fix it.

For example, if you were baking a cake and something went wrong, you might want to look back at your recipe and notes to see what happened. Similarly, when a computer has a problem, the diagnostic logs provide valuable information, like the time of the event, what type of issue it was (like an error or a warning), and where it occurred. This way, the experts can troubleshoot the issue systematically and get everything back on track!



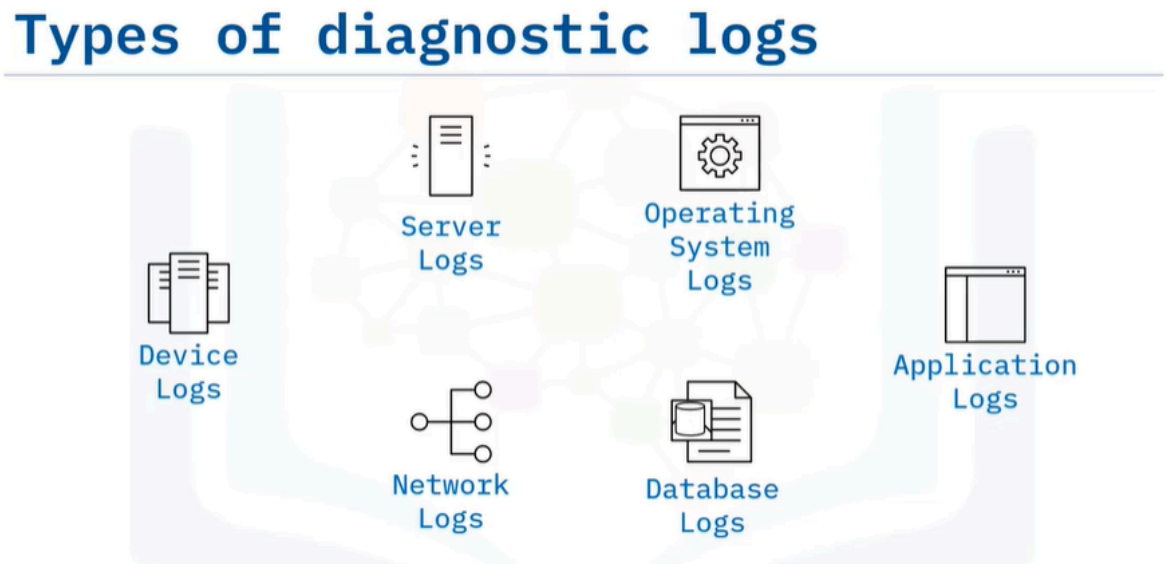
- Troubleshooting is a systematic process used to locate the cause of a fault in a computer system to provide details on correcting the relevant hardware and

software issues. Approaching troubleshooting using a logical and systematic approach is essential to a successful resolution. Troubleshooting is one of the main reasons people create logs. When a problem occurs, you'll want to diagnose it to understand why it happened and what the cause was.

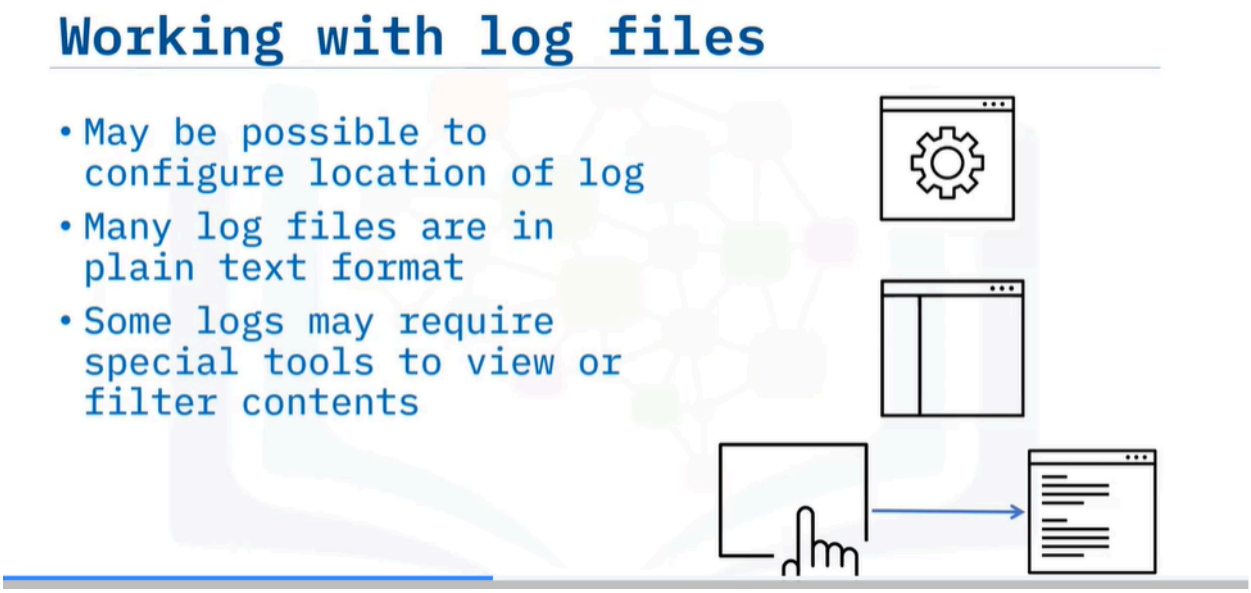


- A diagnostic log tracks what is happening in a system component or an application such as a web server or a database. It contains information about an event, or a problem encountered when processing requests. The diagnostic log is a record of significant events and errors in chronological order and is very useful for diagnosing or troubleshooting problems.
- For example, if a web server receives a request to load a file that is missing, this error and its details can be logged to the webserver log. The diagnostic logs are also sometimes referred to as troubleshooting logs, error logs, or event logs. It is essential to recognize that they may contain events, informational messages, warnings, or errors and their details.
- An event might be when a user connects to the database, or an informational message that includes information on a particular subsystem's status.

- Additional events may be a warning message that might indicate that disk space for the database volume is running low, or an error message may that contains details about a failed database backup operation.
- Some logs may have fewer or more categories of diagnostic messages such as FATAL and PANIC as additional classes of errors or may label them differently, for example, NOTE or NOTICE instead of Information.

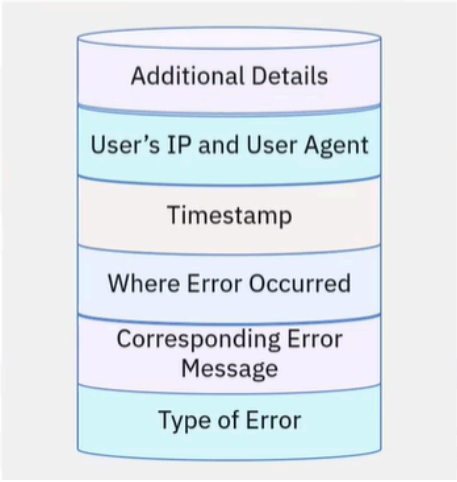


- A database administrator needs to be familiar with various types of diagnostic logs in the system. These include logs for server components, storage and other hardware devices, network, operating system, applications, and databases. While the systems administrator may monitor the other logs, the DBA needs to be intimately familiar with the database diagnostic logs, and review them frequently. These database diagnostic logs are generally separate from the database transaction logs or query logs.

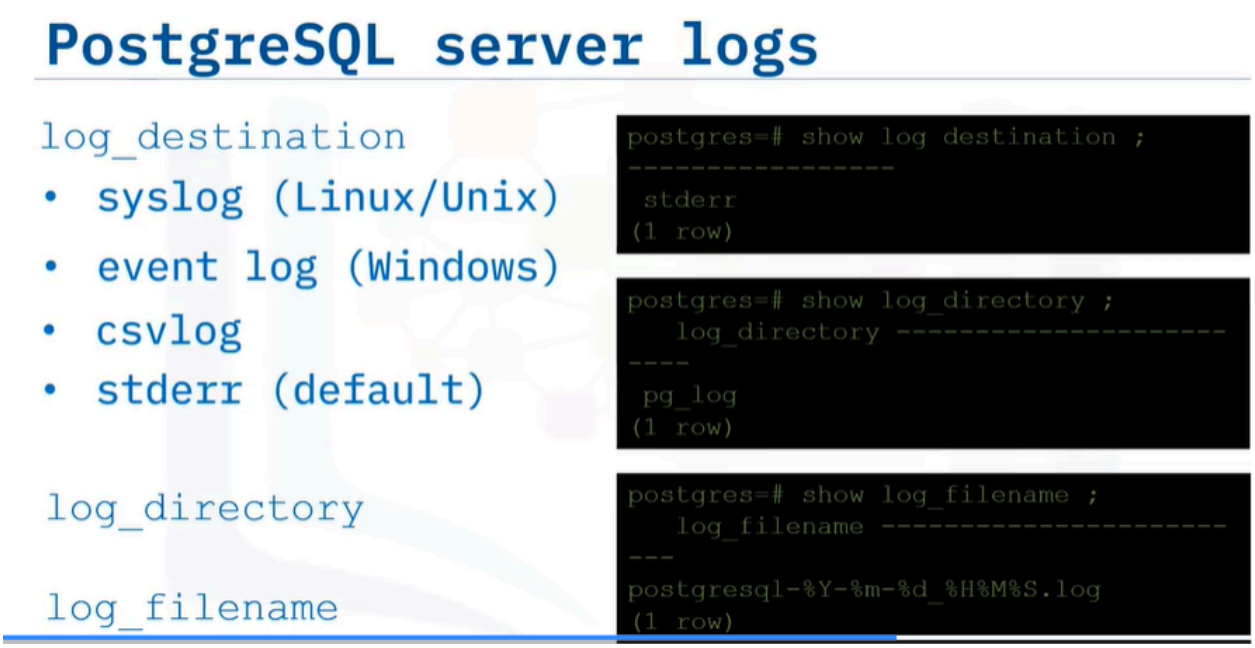


- In most cases, you can configure the location of the log files. However, certain logs, such as system log files, may have a fixed location. Many log files are recorded in plain text, and any text editor will do just fine to open them. For example, on a machine with a Windows operating system, double-clicking on a LOG file will open Notepad by default. However, some log files are machine-readable and may require particular viewers to see their contents.

Diagnostic log contents



- Diagnostic logs can contain a variety of information. Some typical components of messages in a diagnostic log include: The type and severity of issue – whether it is an event, informational, warning, or an error, The corresponding error code and message, The location, URL, or subsystem where the error occurred, A timestamp, The user's IP and user agent, And finally, any additional information depending on the event or error.



- the PostgreSQL database typically logs all events like startup and shutdown, errors, connection issues, and so on. You can configure the location where the log entries are stored using the log_destination parameter in the postgresql.conf: the syslog in case of Linux and Unix systems, the event log in case of Windows systems, to a CSVLOG file that you can easily import into a table and query the log entries using standard SQL statements, or to STDERR (short for standard error), which is the default and typically outputs to the console, but can be configured using log_directory parameter to specify a particular location – the default being pg_log. You can also select the format of the log_filename that names the log files based on a specific string pattern that can include a timestamp.

Summary

In this video, you learned that:

- A DBA needs to be familiar with many types of logs
- A database diagnostic log file contains timestamped informational messages, events, warnings, and errors
- Diagnostic logs are often text based but some may require special viewers
- Most databases provide settings for enabling and configuring diagnostic and error logging
- Some databases, like MySQL, include more than one diagnostic log