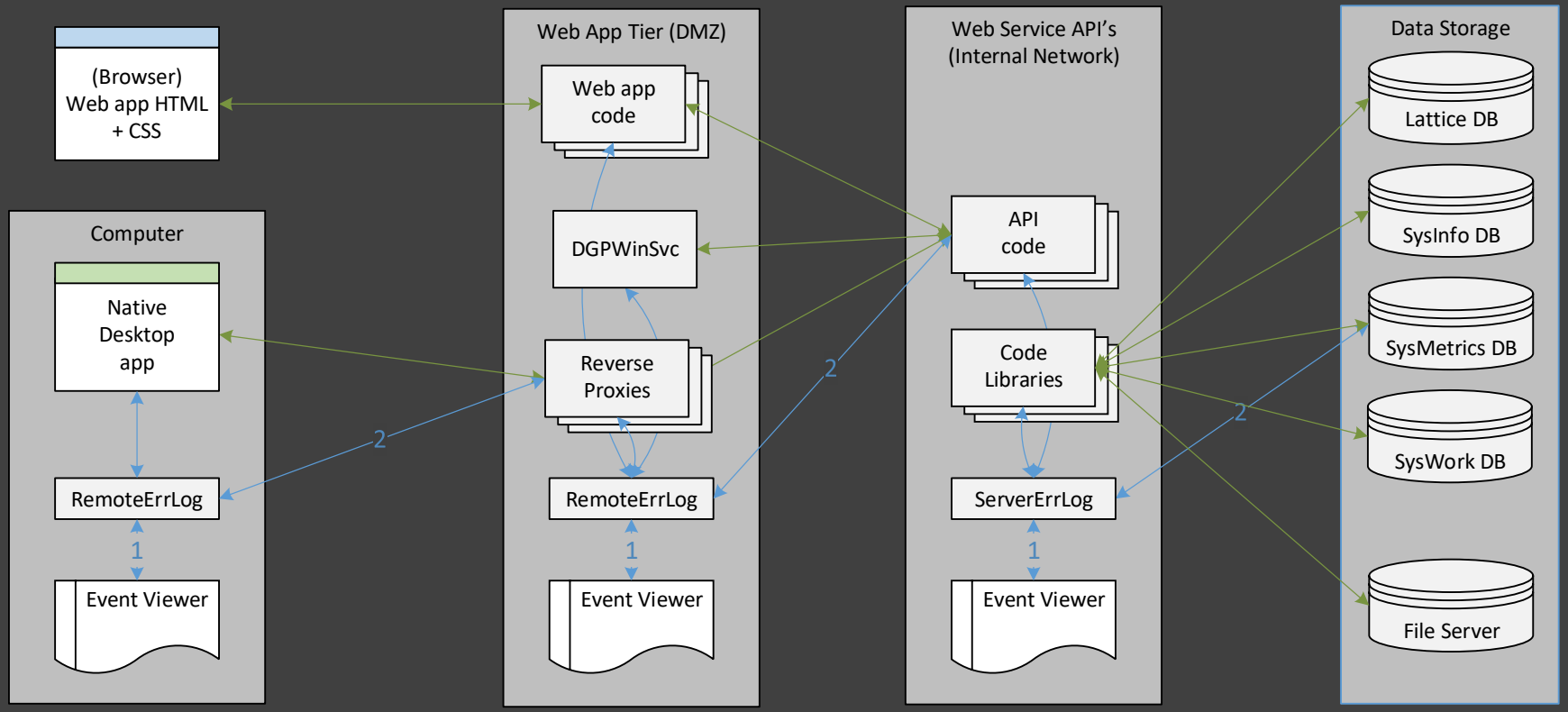
DGP Logging



Logging in DGP systems is handled by two classes: the RemoteErrLog class and the ServerErrLog class.

They both follow the same two steps:

1. Write the message to the Event Viewer
2. Write the message to the DGPError table in the SysMetrics database

© 2021 Alan Rahn All Rights Reserved

The difference between the two classes is that the RemoteErrLog class runs outside of the internal network, and therefore must call an API method to write to the DGPError table. The ServerErrLog runs on the internal network, and uses an ADO.NET call to write directly to the DGPErrors table.

Note: the diagram above shows the classes separate from the applications to highlight the data flows, but the classes are obviously incorporated into the applications in practice.

Writing to an Event Log is very easy to do, as long as that log already exists. The DGP apps and services write to the Event Log that is specified as the EventSource and EventID specified in their respective .config files.

Custom event logs can be created using the Utility under the Help menu. Creating a new custom Event Log using the Lattice UI requires Lattice be run as an administrator, which is difficult in certain environments.

If a custom Event Log has not yet been created, DGP will by default use the ".NET Runtime" Event Log with an EventID of "1000". That log is guaranteed to be present for computers running the .NET framework, and is very seldom used in practice. This can be changed to use a custom event log and event ID at any time by changing the .config file key values.

Tools such as Splunk are the preferred way to constantly scan the various Event Logs and notify administrators whenever exceptions or errors occur.

Remote Monitoring

In addition, each native app can be used as a remote monitor of the functionality in the location they connect to. User accounts that are members of the RemoteMonitor role will call an API method to save the performance measurements that are shown in the status bar at the bottom of the Lattice UI. This acts as a heartbeat mechanism, but also measures end-to-end performance over time. Once again, tools such as Splunk are recommended to notify administrators when performance-related events of interest occur and are logged as part of the remote monitoring functionality.

© 2021 Alan Rahn *All Rights Reserved*