APOS Live Data Gateway

System Requirements, Scaling, and Security Notes

The APOS Live Data Gateway processes all data requests in memory, so the server configuration is very important for scalability and to meet service level requirements. While system requirements will vary between deployments according to scalability requirements and other variable, the following requirements and recommendations should be considered.

System Requirements

Hardware Requirements:

- Windows based Tomcat Server
- Architecture: 64-bit only
- Memory: 16 GB RAM minimum, 32GB RAM preferred
- CPU: 2 Core minimum, 4 Core preferred
- Disk Space: 20GB Minimum

Software Requirements:

- Apache Tomcat v8.5 or 9, configured with SSL Certificate for CORS
- Visual C++ redistributable for Visual Studio 2015
- Microsoft .NET Framework 4.0
- Java SE Runtime Environment 1.8 minimum Configuration Requirements
- The browser used by LDG users must support access to the SAP Analytics Cloud and to the Tomcat Servers.
- Tomcat Servers must be able to communicate with the data source you are connecting to.
- Database drivers required for connectivity must be installed on the Tomcat servers

System Scaling

Concurrent Connections Support Estimate

The actual number of supported connections will depend on the size and complexity of queries being executed, and the communication patterns of consuming application. However, a rough estimate for concurrent connection support is that the Live Data Gateway can support between 150 – 200 concurrent connections per server (based on hardware described above, with 32GB memory).

Web Farm Configuration / Load Balancing

The Live Data Gateway can be installed in a Tomcat Web Farm configuration so that you have multiple servers handling the requests. When the Live Data Gateway is installed on a Web Farm we recommend using a sticky sessions with your Load Balancer.

APOS Live Data Gateway

System Requirements, Scaling, and Security Notes

Security

Security Authentication

APOS Live Data Gateway is not focused on how a user logs into SAP Analytics Cloud, but is instead focused on how authentication happens to the data sources being connected to. APOS Live Data Gateway utilizes the data source security and authentication method, and leverages the existing security protocols of the database.

SSO Options

There are four options to consider for SSO. Options 1 and 2 can work with most data sources.

1. Use a single Pre-defined user account. This is the simplest approach that is very effective in scenarios where no row level security is required. In this scenario you could create connections/models based on a single pre-defined database user, and control access to those connections/models in SAC using the SAC security controls.
2. Have a user mapping strategy where all users and their credentials are stored in an encrypted file, and their SAC user profile is mapped to database authentication details.
3. Integrate with an identity provider solution, such as Kerberos. This identity provider approach relies on this being supported by both the target database and the Live Data Gateway. SSO deployment consulting is typically required to address the added deployment complexity.
4. Where we completely have SSO options turned OFF. In this scenario all users of these connections will be forced to enter technical username and passwords each time they wish to consume this connection.

External User Access

For the APOS Live Data Gateway configuration, it is critical that the SAP Analytics Cloud User has connectivity between their browser and the Tomcat server where Live Data Gateway is running. The most common use case scenario for User Access is where the SAC user is located within the organization firewall, where secure connectivity to the Live Data Gateway server (where Tomcat is installed) is easily accomplished. For external users who are located outside the firewall, they can establish secure connectivity with the Live Data Gateway through the use of a VPN connection. Where a VPN is not an option for external users, connection with Live Data Gateway can be accomplished through the use of Reverse Proxy technologies. The use of a Reverse Proxy requires that ports are opened in the organizational firewall, but the Reverse Proxy manages the security of this connection. Reverse Proxy utilization and configurations vary significantly across various organizations in order to meet that organizations security requirements, so there is no standard configuration for Live Data Gateway in its communication with the Reverse Proxy. The main consideration here is that end users outside of your network can access your reverse proxy server with the specified ports, that that server handles the request to the Tomcat server appropriately.