IBM Common SQL Engine

Gain flexibility and protect your data management investments

IBM

Stop paying the price for flexibility. Protect your data management investment with the Common SQL Engine and IBM Hybrid Data Management.

Your organization's data needs can change rapidly. In response, smart organizations have adopted hybrid data management strategies with flexible deployment capabilities. These include cloud and on-premises deployments, as well as relational and data lake infrastructure implementations to house and analyze both structured and unstructured data.

However, these flexible deployment capabilities typically require the ability to rewrite or otherwise restructure the queries, applications and management schemes that use this diverse data. If you want to change a database deployment, vendor or format, you might have to rewrite your applications, license new software or both.

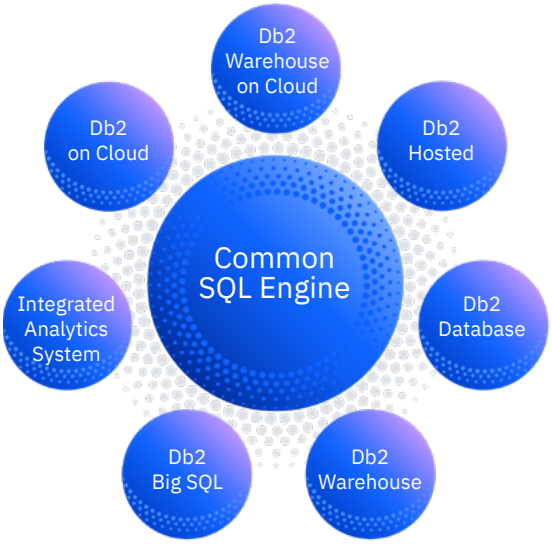
If you choose IBM® hybrid data management offerings, the Common SQL Engine protects your data management investment. The Common SQL Engine is part of a comprehensive IBM strategy for flexibility and portability—one that includes application compatibility, strong data integration and flexible licensing. The Common SQL Engine includes an Oracle Application Compatibility layer, allowing Oracle applications to integrate with the IBM Db2® family of offerings, as well as the IBM Integrated Analytics System. Typically, more than 98 percent of existing Oracle application code can run as-is.

Query and application compatibility

You can be confident that once you write a query, it will work across the Db2 family of offerings, including databases, data warehousing and open-source Hadoop. It is also compatible with the IBM Integrated Analytics System and existing IBM PureData® for Analytics (Netezza®) offerings. With the Common SQL Engine, you can change your data infrastructure as needed without worrying about application compatibility or license costs.

Although the Common SQL Engine is the heart of query and application compatibility, this compatibility extends beyond data repositories and analytic applications — it includes security, governance, management, data movement and other applications as well.

The IBM Common SQL Engine is designed to help your applications just work on cloud or on-premises, with transactional, warehouse or data lake repositories.



Write once, run anywhere with the Common SQL Engine

Data integration and virtualization

Comprehensive and valuable insights usually draw on different types of data from different repositories, so application compatibility isn't much use without data integration. Fortunately, the Common SQL Engine includes built-in data virtualization services to help ensure you can access data from all your data sources. These virtualization services apply to the Db2 family of offerings, including IBM Db2, IBM Db2 Warehouse, IBM Db2 Big SQL and others; as well as IBM Integrated Analytics System and PureData for Analytics. They also extend to non-IBM data sources such as Oracle, Teradata, and Microsoft SQL Server; cloud sources such as Amazon Redshift; and open-source solutions such as Hive.

Because of the robust application compatibility and data integration enabled by the Common SQL Engine, you can write a query without necessarily needing to know where the queried data resides. As part of a single query you could pull data from an IBM data store such as Db2 and join it with data from a non-IBM data source. This feature is particularly powerful as part of a data lake architecture because it allows you to choose the optimal place to store your data without having to worry about how to query it later.

Learn more

Stop paying the price for flexibility. Protect your data management investment with the Common SQL Engine and IBM Hybrid Data Management.

Dive deeper into each of the offerings with a free trial or schedule time to speak with one of our data management experts about your questions for free.

© Copyright IBM Corporation

IBM Corporation
New Orchard Road, Armonk, NY 10504
Produced in the United States of America
April 2020

IBM, the IBM logo, ibm.com, Db2, and PureData are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information”at www.ibm.com/legalcopytrade.shtml

Netezza®, is a registered trademark of IBM International Group B.V., an IBM Company.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS ”WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.