IBM Technology

G-Cloud 15
IBM - Guardium Data Security Center

Service Definition Document

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

IBM Guardium Data Security Center

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order. Upon acceptance of Client's order, this Service Description and the Cloud Services Agreement found at http://www.ibm.com/terms/csa (or equivalent agreement for Cloud Services between the parties) applies to Client's use of the Cloud Services.

1. Cloud Service

IBM Guardium Data Security Center is a software-as-a-service data security platform that allows Client access to modules of capabilities for monitoring and reporting on activity in their hybrid cloud environment and take action to mitigate risk. As part of the offering IBM provides 24x7 monitoring of the infrastructure that runs the solution and applies the latest software and platform patches whenever they are available.

IBM Guardium Data Security Center SaaS uses IBM Security Verify for Single Sign-On (SSO), multi-factor authentication, and identity lifecycle controls for all IBM Guardium Security Center user types.

IBM Guardium Data Security Center is hosted and runs on the Amazon Web Services (AWS) cloud environment using a number of AWS services.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Guardium Data Security Center

IBM Guardium Data Security Center is entitled through packs of 100 Resource Units that can be allocated across the included modules. Unused Resource Units do not roll over to the next month.

Upon request, Client is authorized to use a separate tenant provisioned for non-productive use, including but not limited to testing functionality and technology, restricted to use with two (2) concurrent data source connections. Resource Unit allocation is not required to access the modules on the non-production tenant.

a. **IBM Guardium DDR**

IBM Guardium DDR provides Clients with a full view of the threat landscape, finding risk inside the noise, streamlining response both internally and externally to the Security Operations Center (SOC), through altering mechanisms that support data security as well as risk analytics and threat mitigation. With IBM Guardium DDR Clients can process data from IBM Security Guardium Data Protection as well as activity data streamed directly from any supported data source. IBM's analytics engine will profile the data collected from Client's data sources and make recommendations as to the risk level of potential threats.

Add-on storage is required, and Client must obtain entitlements either on a subscription or pay per use basis to support the volume of data being collected and the retention of that data in 5 GB increments. This entitlement applies to the aggregated amount of storage for the production and non-production tenants associated with a subscription.

1 Asset : 200 Resource Units

The following modules, formerly part of IBM Guardium Data Security Center, are no longer available in this Cloud Service. Any Asset entitlements previously allocated to these modules will be added back to the Client's available Resource Unit balance upon their subscription renewal date.

- IBM Guardium AI Security
- IBM Guardium Data Compliance
- IBM Guardium DSPM

1.1.2 IBM Guardium Data Security Center Trial

Client is authorized to use a Trial Cloud Service for IBM Guardium DDR.

The Trial Cloud Service is available for a 14-day trial period for the purpose of evaluating its functionality and technology, at no cost. A Trial Cloud Service may only provide a limited set of features and function; therefore, use in a production environment or for commercial purposes is not recommended or supported. Any such use is solely at Client's own risk. The generally available Cloud Service may be ordered at any

time. Client may only participate in a trial for a Trial Cloud Service one time. If Client wishes to continue with the Trial Cloud Service upon expiration of the trial period, Client will need to submit an order for the generally available Cloud Service offering. IBM is under no obligation to offer migration capabilities or services.

For IBM Guardium DDR, the Trial Cloud Service is limited to use with two (2) data source connections.

1.2 Optional Services

1.2.1 IBM Guardium Data Security Center Add-On Storage

IBM Guardium Data Security Center Add-On Storage allows Clients to store the data they collect, analyze, and report on from any IBM Guardium Data Security Center modules. Client must obtain entitlements either on a subscription or pay per use basis to support the volume of data being collected and the retention of that data in 5 GB increments. For pay per use, storage usage is measured at the end of each month and rounded up to the next increment of 5 GB and billed accordingly.

1.3 Acceleration Services

1.3.1 IBM Expert Labs Configure and Assist Guardium (8 hours)

IBM Expert Labs Services are remotely delivered services that provide Client access to subject matter expertise (SME) resources and supporting information for IBM Guardium Data Security Center.

Expert Labs Services are delivered in English language only, unless mutually agreed with Client, and do not replace the role of the IBM Support organization which should continue to be the point of contact for technical problems. Each Engagement provides Client 8 hours of assistance with one or more of the following focus areas:

- Discuss Cloud Service intended use cases, scope, regions.
- Discuss prerequisites (for example: firewalls, permissions, roles, accounts)
- Assist with access to relevant environments or systems (for example: accounts, SaaS applications, Guardium Data Protection environment)
- Configure, deploy module components (for example: Guardium Data Protection Datamart)
- Discuss module use cases, functionality and assist with configuration (for example: discovery process, policy config, reports and audit processing needs)
- Discuss data detection & response (DDR) expectations
- Deploy dashboards, reports and audit processing needs
- Review alerting and actions
- Discuss or configure integrations

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

Link(s) to the applicable Data Sheet(s):

IBM Guardium Data Security Center	https://www.ibm.com/terms/?id=2F572F80BA6C11ECBDA1ED9610150DDC
IBM Common Service Mesh	https://www.ibm.com/terms/?id=503882A8505045C1802C09E0B315F6CC

IBM Guardium Data Security Center does not commit to full implementation of the requirements included within the IBM Data Security and Privacy Principles, as referenced in the base Cloud Service terms and the Data Processing and Protection Data Sheet.

IBM Common Service Mesh is a common service that enables the generative AI functionality contained in the Cloud Service.

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/support/pages/node/731179.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at https://www.ibm.com/support/home/pages/support-guide/.

Technical support is not applicable for Trial Cloud Services.

3.2.1 Optional Support Offerings

Additional support options are available for this Cloud Service. If Client selects to order an optional support offering, the terms defined in the Optional Support Offerings Service Description at https://www.ibm.com/terms/?id=i126-9789 will apply to the support offering specified in Client's TD.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Engagement is a professional or training service related to the Cloud Services.
- Gigabyte (GB) is 2 to the 30th power bytes of data processed by, analyzed, used, stored, or configured in the Cloud Services.
- Resource Unit (RU) is an independent measure of a resource managed by, processed by, or related to the use of the Cloud Service. Usage of each module requires the specified number of RU entitlements to this Cloud Service subscription as measure by the following ratio table:

Module	Ratio
Guardium DDR	1 Asset : 200 RU

- Asset is a uniquely identified tangible resource or item of value to be accessed, scanned or managed by the Cloud Services.

Module	Asset definition
Guardium DDR	Each unique data source (including but not limited to text file, cloud provider data store, database server, IP address, host name)

4.2 Remote Services Charges

A remote service will expire 90 days from purchase regardless of whether the remote service has been used.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at https://www.ibm.com/acs apply.

5.1 Enabling Software

IBM Guardium DDR include use of the following Enabling Software; IBM Security Guardium Aggregator Software Appliance, IBM Security Guardium Collector Software Appliance, and IBM Security Guardium Data Protection for Databases. Enabling Software may only be deployed and configured (i) as collectors and central managers, and (ii) solely to collect and send data activity information to the IBM Guardium Data Security Center Cloud Service. Client is not required to obtain entitlements for Enabling Software.

Enabling Software	Applicable License Terms (if any)
IBM Security Guardium Collector Software Appliance	https://www.ibm.com/terms/?id=L-XGQT-L279Y2
IBM Security Guardium Aggregator Software Appliance	https://www.ibm.com/terms/?id=L-NVAD-N2M65F
IBM Security Guardium Data Protection for Databases	https://www.ibm.com/terms/?id=L-DLUU-PPA2PL

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content or that otherwise identify Client. IBM may however use Content and other information that results from Content in the course of managing and providing the Cloud Service provided that any data subject to applicable privacy regulations will be rendered into a form that no longer constitutes personal data. IBM will use Client's Content and other information that results from Content, excluding personal data, only for research, testing, and offering development. IBM may share threat identifiers and other security information embedded in Client personal data for threat detection and protection purposes. The provisions of this section will survive the termination or expiration of the transaction.