Teradata VantageCloud Enterprise

Cloud Service Description and AWS Managed Application Addendum:

Blended Pricing

This Cloud Service Description applies to Teradata VantageCloud Enterprise featuring blended compute pricing options on all public cloud platforms where it is available. In addition, an Addendum to this Cloud Service Description exists for each cloud platform on which VantageCloud Enterprise operates. One or more addenda describing additional terms may be included. The terms within this Cloud Service Description apply to the latest Generally Available (GA) offerings. Orders effective prior to April 1, 2023, will reflect the changes in storage entitlement and pricing at the time of next Order renewal. If there are any conflicts between the terms of the Addenda and the provisions of this Cloud Service Description, then such Addenda-specific terms shall apply and take precedence over the conflicting provisions of this Cloud Service Description. Such Addenda specify the following:

- Subscription features
- Applications
- Supported connectivity options
- Supported instances
- Supported regions
- Pricing options
- Responsibilities
- Additional Terms

September 18, 2023

Table of Contents

1. Teradata VantageCloud Enterprise

Teradata VantageCloud Enterprise is Teradata's flagship analytic platform offering, which evolved from the industry-leading Teradata Database.

Teradata VantageCloud Enterprise is an enterprise data analytics platform for pervasive data intelligence that enables the Customer to perform advanced analytics in the cloud. With VantageCloud, the Customer can integrate analytic tools, languages, and engines to get insights from data. With VantageCloud, Teradata manages the performance, security, availability, and platform operations of the Vantage Data and Analytics platform as further described in this Cloud Service Description and applicable addenda.

2. Responsibilities

Teradata, the Customer, and the Cloud Service Provider (CSP) all have responsibilities for managing the Customer's VantageCloud system as summarized in the VantageCloud System Management table below.

VantageCloud Enterprise System Management	
Responsibility	**Responsible Party**
Hardware	Cloud Service Provider
Data Center / Hosting	Cloud Service Provider
Initial Data Migration	Customer ***Note:*** *Customer may hire Teradata to perform certain responsibilities under a Teradata Consulting engagement (sold separately).*
Environment Availability Monitoring – Operating System (OS) and Teradata software	Teradata
Software Patching and/or Upgrading	Teradata ***Note:*** *Third-Party Tools patching and/or upgrades require a Teradata Consulting engagement (sold separately).*
Premier Cloud Support (software)	Teradata
Cloud Platform Support	Cloud Service Provider
Database Administration / Operations • Database access security monitoring – managing VantageCloud security roles, passwords, and access rights • Maintaining VantageCloud structures, space, users, and jobs • Monitoring alerts, queries, access locks, and database performance • Analyzing database activity and priority of jobs/queries to identify performance tuning opportunities • Managing consumption and query performance	Customer ***Note:*** *Customer may hire Teradata to perform certain responsibilities under a Teradata Consulting engagement (sold separately).*
Operating System (OS) Administration / Operations • OS security monitoring • Volume encryption • OS user administration for Teradata personnel	Teradata
Network Administration / Operations • Restrictions / filtering of incoming traffic to VantageCloud environment	Teradata

VantageCloud Enterprise System Management	
Responsibility	**Responsible Party**
Cloud Environment Administration / Operations • Security monitoring of the VantageCloud environment • Cloud environment access management for Teradata personnel	Teradata
Backup and Restoration	Teradata – • Backup Support and Restore Requests per defined scope in Operational Services section Customer – • Sets up, changes, and manages the Backup Plans using self-service capability utilizing Vantage Console • Defines Backup Lifecycle and Storage Policy Management requirements • Resolves issues causing backup warnings and exceptions

3. VantageCloud Enterprise License Tiers

The following table shows the categories of features and functions available in the latest version of VantageCloud Enterprise for each license tier.

VantageCloud Enterprise License Tiers – Features and Functions			
Features and Functions	**Base**	**Advanced**	**Enterprise**
Customer Support Type	Premier Cloud	Premier Cloud	Premier Cloud
Elastic Performance on Demand (EPOD) ***Note:*** *Blended Pricing Option required.*		●	●
Vantage Unit Consumption for VantageCloud ***Note:*** *Available for applicable as-a-service deployment options only.*			●
Teradata Columnar	●	●	●
Teradata Intelligent Memory		●	●
Row-Level Security	●	●	●
Temporal	●	●	●
Workload Management		Teradata Integrated Workload Management (TIWM)	Teradata Active System Management (TASM)
Block Level Compression	●	●	●
Teradata Native Object Store	●	●	●

4. Analytics Database Feature Descriptions

This section describes the Teradata Analytics Database features that are available in the VantageCloud Enterprise license tiers.

4.1 Teradata Columnar gives the Customer the ability to store Customer Data in a table by column, instead of by row. In its simplest form, each column in the table becomes its own column partition.

4.2 Teradata Intelligent Memory identifies more frequently used data and places it in memory.

4.3 Row-Level Security allows the Customer to restrict data access on a row-by-row basis in accordance with Customer-site security policies.

4.4 Temporal tables store and maintain information with respect to time.

4.5 Workload Management can manage VantageCloud workload performance by monitoring system activity and by acting when pre-defined limits are reached.

a) TASM gives administrators the ability to prioritize workloads, tune performance, and monitor and manage workload and system health.

b) TIWM provides basic workload management capabilities (i.e., a subset of TASM) to Customers without full TASM.

4.6 Block Level Compression is a required data compression feature and is enabled by default.

4.7 Native Object Store (NOS) enables the Customer to use standard Teradata SQL and APIs to search and query CSV, JSON, and Parquet format datasets located on S3-compatible object store platforms. The Customer can also write data stored on VantageCloud to S3-compatible object store platforms.

5. Teradata Application Descriptions

This section describes the Teradata Applications that may be available with the Teradata VantageCloud Service. References to “Production Systems” are defined as all Customer Site IDs with System Use of “Production” in the Support Portal.

5.1 Teradata Viewpoint (Viewpoint) is a web-based operations management portal for VantageCloud systems. Viewpoint provides a framework to display web-based applications, known as portlets, that enable users across an enterprise to customize tasks and to display options for their specific business needs.

a) Viewpoint with Teradata VantageCloud runs in single-system mode. VantageCloud Customers run a single-system Viewpoint capable of monitoring and managing a single VantageCloud instance.

b) Viewpoint provides portlets for everyday management activities such as system and application administration, monitoring, and management with rewind capability, and Workload Management. Certain portlets that are available with Viewpoint for Teradata VantageCore are not available for VantageCloud since the functionality is provided through the Vantage Console or by Teradata (e.g., Backup and Recovery, Remote Console).

c) During the provisioning of VantageCloud in the Public Cloud, the Customer receives one (1) single-system Viewpoint for each VantageCloud system installed.

d) Teradata VantageCloud implementations use a limited SMTP service to complete provisioning and initial validations. If the Customer wants to receive VantageCloud system

email alerts configured in and generated by Viewpoint, the Customer must replace the limited SMTP solution from Teradata with an enterprise SMTP solution of its choosing.

5.2 Performance Data Collection Reporting (PDCR) is a data collection application that provides data related to database performance and workload utilization.

5.3 Teradata Data Lab enables self-service business intelligence and analytics by simplifying the provisioning and management of the analytic workspace within a data warehouse. By allocating that workspace, Data Lab provides lab users with easy access to critical information without moving or replicating data. Data Lab also gives them the flexibility to both self-provision the space and experiment with new data and theories. Teradata Data Lab is only available for Production Systems. Teradata Data Lab implementation support is available through Teradata Consulting for an additional fee.

5.4 Teradata Data Mover copies data and objects, such as statistics and tables, from one Teradata system to another. Reducing the complexities of data movement, Data Mover leverages built-in, underlying technologies in the Teradata system to enable automation, control, and process monitoring. One Data Mover instance (including software license and associated infrastructure) is included, and up to three additional instances may be purchased. Data Mover requires implementation on all instances by Teradata Consulting for an additional fee.

5.5 Teradata QueryGrid delivers data access, processing, and movement across systems in heterogeneous analytical environments. QueryGrid provides a means both to connect to a remote system and to retrieve or insert data using SQL. In this way, users can access multiple data sources without replicating data in the warehouse. QueryGrid also enables specialized processing engines, such as Analytics Database and Apache Hive for Hadoop, to act as one solution from a user's perspective. Specifically, core-enabling software links with processing engines to provide access to data and processing. The connectors then deliver bi-directional data movement and push-down processing across connected systems. QueryGrid requires implementation by Teradata Consulting for an additional fee.

5.6 Teradata Query Service is middleware that provides a REST API for connecting to VantageCloud. The Teradata Query Service lets Customers open database sessions, submit SQL queries, and access both responses and metadata through an Open API REST interface. Teradata Query Service enables self-service backup and restore and is mandatory for these features.

6. Optional Teradata VantageCloud Analytics Capabilities

Customer can opt for the following VantageCloud Analytic Capabilities, at no additional charge, via a VantageCloud Change Request:

6.1 Vantage Analytics Library (VAL) provides the data scientist with over fifty advanced analytic functions built directly into the Analytics Database. These functions support the entire data science process, including:

a) Exploratory data analysis

b) Data preparation and feature engineering

c) Hypothesis testing

d) Statistical and machine learning model building and scoring.

6.2 Bring Your Own Model (BYOM) consists of code and libraries that enable Data Scientists to predict (or score) machine learning models in standard interchange formats, such as PMML (Predictive Model Markup Language) and H2O MOJO (Model ObJect, Optimized), against data

in VantageCloud. The BYOM function can be invoked via SQL query, Python, and R languages to utilize the stored Machine Learning (ML) model to score Enterprise Feature Data and to predict the likelihood of a particular outcome.

6.3 Standard User-Defined Functions (UDF) let the Customer create a function by using code in SQL, C, C++, and Java that can be executed directly on the VantageCloud platform. The Customer can then bring to VantageCloud their customer UDF source code and binaries for C/C++ UDFs, as well as binaries and compiled code for Java UDFs. With this capability, the Customer can add functionality not natively supported by VantageCloud. Before deploying them on VantageCloud, however, the Customer should thoroughly test their UDFs for any unwanted effects of data stored in the system (e.g., performance, security, system availability, confidentiality, integrity).

6.4 Vantage Python and "R" Open Analytics. Teradata VantageCloud provides Python and "R" analytics in two forms: client and server-side analytics. The free, downloadable client Python library (teradataml) and the "R" library (tdplyr) enable users both to access business data in VantageCloud and to transform it into dataframes. Users can also use VantageCloud native functions to process them in-database. Meanwhile, server-side Python and "R" analytics give users the ability to run the Python/"R" scripts with the open-source analytic libraries where the data reside. VantageCloud Script Table Operator (STO) and ExecR capabilities enable partitioned data model training and scoring in parallel at high performance. With these VantageCloud capabilities, users no longer need to export data to another platform, thereby avoiding the added complexity and lower performance associated with that process.

7. VantageCloud Enterprise Support

Teradata provides integrated maintenance and support services for all VantageCloud Enterprise subscriptions, including defined coverage hours and response times, access to the Support Portal, Vantage Console, and other features. Support and Operational Services are provided in English; however, Support Tickets (Cases, Change Requests, and Service Requests) will have language translation capabilities based on Customer settings in the Support Portal.

7.1 Support Portal and Vantage Console. VantageCloud Enterprise Support and Operational Services are accessible through both the Support Portal and Vantage Console.

a) Support Portal. VantageCloud Support and Operational Services are accessible through the Support Portal (support.teradata.com), which is available 24 hours a day, 7 days a week, 365 days a year. The Support Portal gives the Customer self-service access to features such as Support Tickets, analytics, Customer dashboards, and Knowledge Articles.

b) Vantage Console (cloud.vantage.teradata.com) allows the Customer to use the web-based, self-service Vantage Console to monitor and manage VantageCloud systems. Depending on the Customer's order, available features may include:

i. View VantageCloud site metrics and utilization trends

ii. Scale VantageCloud compute power up or down, scale instances out or in, and stop or restart instances without affecting persistent storage (for applicable Blended Pricing options only)

iii. Track Vantage Unit consumption

iv. Set up and manage the Backup Lifecycle and Storage Policy

v. View network application IP addresses

vi. Administer Native Object Store (NOS) Policies

c) Account management for the Vantage Console has three main features:

i. Vantage Console access is controlled through the Support Portal for all users.

ii. Support Portal users with Admin rights will have the Site Super Admin role.

iii. Support Portal users without Admin rights will have Read-Only access.

7.2 Support Tickets. Customer can submit Support Tickets (i.e., Cases, Change Requests, and Service Requests) through the Support Portal, which is available 24 hours a day, 7 days a week, 365 days a year. Teradata uses best practices from the Infrastructure Technology Information Library (ITIL) for VantageCloud Support Tickets. The table below illustrates these options.

Support Ticket Types and Submission Options	
Support Ticket Types	**Support Ticket Submission Options**
Case	• Support Portal • Telephone (S1, S2 Cases only): 1-877-MY-TDATA, Option 3 • Automatic Case Creation: Generated by Teradata systems ***Note**: Additional global support telephone numbers are available via the Support Portal.*
Change Request	Support Portal
Service Request	Support Portal

a) A Case is a record to track customer issues, requests, and resolution activity.

i. When opening a Case in the Support Portal, the Customer must select a severity level based on the level of impact (see the Case Severity Levels table below).

ii. Teradata will respond to Cases based on the assigned Severity Level.

iii. Teradata also provides automated event management to monitor VantageCloud health and to create Cases.

iv. In some instances, Cases may be set to a State of “Awaiting Info.” When that happens:

a. The Case resolution duration pauses until the Customer responds.

b. If no response is received within 14 days, the Case closes automatically.

v. Once a solution has been provided in a Case, the State is set to “Resolved.” When that happens:

a. The Customer needs to review the update and either Accept or Reject the solution.

b. If the Customer does not respond within 14 days, the Case will close automatically.

Case Severity Levels		
Severity	**Impact**	**Description**
S1 (Critical)	The mission-critical Production System is down, corrupted, or severely degraded or is unusable and requires immediate attention to return the System to service.	Daily business is being critically impacted, causing revenue/risk exposure. Users are unable to perform primary functions; no workaround exists. Many users cannot access the system or login. ***Note**: For all S1 Cases, Teradata requires Customer engagement to provide the appropriate Support Levels. Teradata will default to contact the Primary Teradata Support Contact(s) and the Case submitter (if registered in the Support Portal). If the Case submitter or Primary Teradata Support Contact(s) are not available, Teradata will change the Case from S1 to S2 and respond accordingly.*
S2 (High)	The Production System is up and operational, but the issue has severe, ongoing, daily impact to operations; a non-mission critical System is down and requires expedited engagement and urgent resolution.	If not resolved, daily operations will be impacted. Many users are unable to perform primary functions; no workaround exists which significantly affects ability to sufficiently achieve business objectives. Many users are affected.
S3 (Medium)	The issue interferes with normal work efforts, but work can continue. System response / performance is degraded. Non-critical application functionality is not available.	Medium and manageable impact to business, with little revenue/risk impact. Users are unable to perform secondary functions without a sufficient short-term workaround. Several users are affected.
S4 (Low)	A minor issue exists; normal operations can continue. Functionality is impacted, but not down.	Issue has no business impact and low impact to operations. Additional research or information is needed to address a question. Impacts only a few users.
S5 (Planned)	No issue exists; normal operations can continue.	No business impact exists. Teradata uses this severity level for proactive, planned Cases.

b) A Change Request is a request to change something about a system. These changes can include the need to add, modify, configure, upgrade, or even decommission a site or discontinue use of a service component, application, or other associated elements.

   i. Customer can submit new “Normal” Change Requests and view existing Change Requests in the Support Portal.

   ii. Teradata can designate the Change Request as one of three types:

      a. Standard – Low risk, pre-approved change plans that follow a specified and repeatable procedure or work instruction. These changes do not require case-by-case approval.

      b. Normal – Changes without predefined plans that require both Customer approval and approval from the Teradata Cloud Change Advisory Board (i.e., a formal approval authority whose function is to control changes to the approved VantageCloud architecture).

c. Emergency – Unplanned changes necessary for service restoration. These changes require Customer approval and approval from the Teradata Cloud Change Advisory Board. An Emergency Change can only be created in one of the following situations:

- The Change is necessary to restore service and is recommended by Teradata Services SMEs during an S1 case investigation.
- The change must be for the same account as the Severity 1 case.
- A critical security vulnerability exists and, if not expeditiously corrected, could cause harm to the Cloud system and its Customers.

iii. Teradata will schedule the action taken in response to a Change Request in advance and will coordinate the date and time with both the Customer and the assigned Teradata resource.

c) Service Request has predefined and specific actions, services, or work activities that happen upon submission of the request. For example, the Service Request, "Create a Contact," on the Support Portal will allow the Customer to add a contact to the Customer's account. Some Service Requests, however, may need to go through an approval process or include tasks that must be completed by Teradata. Customers can submit new Service Requests and view existing Service Requests in the Support Portal.

7.3 Support Levels (i.e., Premier Cloud Support or Priority Service) define the types and standards of services to be offered.

a) Premier Cloud Support (included) provides integrated maintenance and support services for all VantageCloud Enterprise subscriptions with access to the Support Portal and Vantage Console, downloadable software, knowledge base searching, communities and forums, and other features. Premier Cloud Support coverage hours, Remote Response, and status update cadence are described in the Premier Cloud Support table below. Remote Response time is measured during Customer contracted hours of remote coverage by the interval between the Customer's initial contact (via electronic receipt of case or phone call) to Teradata and the first contact (via electronic receipt or phone call) with a Teradata representative.

<table>
<tr><th colspan="6">Premier Cloud Support</th></tr>
<tr><th></th><th>S1
(Critical)</th><th>S2
(High)</th><th>S3
(Medium)</th><th>S4
(Low)</th><th>S5
(Planned)</th></tr>
<tr><td>Case Coverage Hours</td><td>24 x 7</td><td colspan="3">9 standard business hours,
5 business days per week[1]</td><td>N/A</td></tr>
<tr><td>Remote Response</td><td>2 hours</td><td>2 hours[1]</td><td colspan="2">Next business day[2]</td><td>N/A</td></tr>
<tr><td>Customer Status Updates</td><td>Every hour</td><td>Every 6 hours[1]</td><td>Daily[1]</td><td>Weekly</td><td>N/A</td></tr>
<tr><td colspan="6">[1] Same business day: Monday – Friday (time zone of the Customer's address as set out in the Order)
[2] Next business day example: If the customer opens an S3 or S4 Case after 8 pm Friday, Teradata will respond after 9 am Monday.
Note: Support is provided in English only. Local language support is not provided for As-a-Service subscriptions.</td></tr>
</table>

b) Priority Service (sold separately) enhances Premier Cloud Support by providing Customers with increased VantageCloud Support coverage hours and accelerated response times for certain Case severities as described in the Priority Service table below.

Priority Service					
	S1 (Critical)	**S2 (High)**	**S3 (Medium)**	**S4 (Low)**	**S5 (Planned)**
Case Coverage Hours	24 x 7		9 standard business hours, 5 business days per week[1]		N/A
Remote Response	30 minutes		2 hours[1]	Next business day[2]	N/A
Customer Status Updates	Every hour	Every 6 hours[1]	Daily[1]	Weekly	N/A

[1] Same business day: Monday – Friday (time zone of the Customer's address as set out in the Order)

[2] Next business day example: If the customer opens an S3 or S4 Case after 8 pm Friday, Teradata will respond after 9 am Monday.

***Note**: Support is provided in English only. Local language support is not provided.*

8. VantageCloud Operational Services

Teradata provides both the initial System Provisioning and the day-to-day operational services for VantageCloud, including Access Management; System Monitoring and Telemetry; Upgrades and Maintenance; and Backup and Restoration Services.

8.1 System Provisioning

a) Teradata will provision and configure the VantageCloud system in accordance with an architecture design approved by both parties.

b) Teradata will configure the VantageCloud system to facilitate the Customer's network connectivity per the architecture design. This process may include collaborating with the Customer to perform a network handshake.

c) The Customer is responsible for configuring their infrastructure to connect to VantageCloud. This process may include:

i. Configuring the Customer's networks for all applications to connect to the VantageCloud system on appropriate ports and protocols.

ii. Configuring the Customer's infrastructure components and cloud services including, but not limited to, gateways, endpoints, access profiles, firewalls, DNS & proxy servers.

iii. Approving and maintaining outage windows to perform migrations, assessments, and network tests.

d) Teradata will notify the Customer of the VantageCloud Service Availability Date.

e) As of the Service Availability Date, the Customer is thereafter responsible for:

i. Registering to use the Support Portal and Vantage Console

ii. Retaining the DBC password

iii. Upgrading Teradata Tools and Utilities (TTU) software on all Customer devices that connect to VantageCloud

iv. Maintaining the Customer network connections to VantageCloud

8.2 Access Management (i.e., Support Role Assignment). The Customer is responsible for assigning and maintaining Support Portal and Vantage Console Customer roles as shown in the following table.

Support Portal and Vantage Console — Customer Roles and Functions	
Customer Roles	**Functions**
Support Portal Admin ***Note:*** *Teradata recommends assigning two or more Support Portal Admins.*	• Site Super Admin access to the Vantage Console • Approve all access requests • Grant site roles to customer contacts • Set up and manage the Backup Lifecycle and Storage Policy • Grant Secure Password Vault responsibilities
Cloud Service Owner	• Site Super Admin access to the Vantage Console • Set up and manage the Backup Lifecycle and Storage Policy
Change Control Contact	• Approve Change Requests • Approve maintenance schedules
Event Notification Contact	• Default Customer contact for both Teradata-owned Cases and Cases generated from system events • Notified and/or added to Case watchlists
Remote Access Contact	Support contact for system credentials
Primary Teradata Support Contact	Primary customer contact for escalations
Customer User	• Create, track, and manage Support Tickets • Read-Only Site access to the Vantage Console • View Backup Jobs

8.3 System Monitoring and Telemetry

a) Teradata Support Service tools and Performance Data Collection Reporting (PDCR) must be deployed upon provisioning and remain active for VantageCloud Support.

b) To remain active, Support Service tools (e.g., Viewpoint and PDCR) require database-level service accounts with default access rights.

c) If required for Teradata to provide support or troubleshooting access, the Customer must provide database and application-level credentials via Secure Password Vault or other approved / established mechanism for Teradata to fulfill service agreement responsibilities.

d) Teradata may modify the support tools to provide VantageCloud Support and Operational Services.

e) Teradata collects additional telemetry data to aid Teradata in detecting, troubleshooting, or resolving issues; gauging, analyzing, and optimizing performance and functionality; and providing feedback and recommendations related to the services that the Customer is receiving from Teradata. The data collected is further described in the telemetry collection and analytics guide available at docs.teradata.com. If Customer limits or interferes with Teradata collecting such information, Teradata will be unable to provide the security, operations, availability, billing, and other services that make up the Teradata Cloud Service as described herein.

f) To help them build their data and analytics strategy, the Customer has the option to share additional data with Teradata and to leverage available Industry Data Models and business value frameworks. This additional data collection can include:

i. Detailed performance metrics

ii. Usage metrics by user-id / customer-metadata

iii. Object usage - database, table, and column names metadata

iv. Obfuscated (non-PII) user information

8.4 Upgrades and Maintenance

a) Scheduled Downtime refers to all scheduled or Customer-approved outages of the VantageCloud System including planned maintenance, major upgrades, and system resize (growth or reduction).

b) Maintenance Windows are used by Teradata to perform service maintenance and include Scheduled Downtime. For instance, Teradata uses monthly service maintenance windows for regular service updates to maintain the currency of infrastructure, security, patches, and maintenance releases.

i. The Customer must identify a monthly Outage Maintenance Window (i.e., six hours) upon system installation, subject to availability of the outage window timeframe. This maintenance window will be used to perform activities that may require the system to be offline or otherwise require a database outage. Teradata will assign an outage maintenance window to Customers who do not identify an outage maintenance window.

ii. The Customer can optionally schedule maintenance not affecting availability during an additionally designated, non-outage maintenance window.

iii. The Customer can use a Change Request for ad-hoc maintenance needed outside of the monthly maintenance window.

c) Upgrades to the latest version of VantageCloud occur as new versions are released and are also used to patch the Operating System.

i. To minimize disruptions, the Customer and Teradata coordinate upgrade schedules. Teradata will inform the cloud service install base at least four months in advance for major version upgrades to VantageCloud so the Customer can test application compatibility and validate new versions. In addition to major versions, more frequent minor/patch releases will be made generally available to keep VantageCloud up to date. If these upgrades require a service outage, Teradata will install the upgrade during a planned maintenance window in coordination with the customer.

ii. To be eligible for the Availability Service Level Agreement (SLA) and to keep compliance with Security Standards, Customers are required to remain on either the latest generally available VantageCloud version (“N”) or one generally available version below the latest generally available VantageCloud version (“N-1”). "N" is determined by the maintenance version in Teradata's <major>.<minor>.<maintenance> versioning convention. For example, if the latest generally available VantageCloud version ("N") is 2.4.3, then one generally available version below that ("N-1") would be 2.4.2. Customer systems running older VantageCloud release versions will not be entitled to the committed Service Level Agreement. Software upgrades will occur during the monthly Outage Maintenance Window.

iii. As new versions are released, the Customer must upgrade Teradata Tools and Utilities (TTU) on all Customer devices that connect to VantageCloud to ensure compatibility and stability.

d) Service Disruption Notifications. In the event of a service disruption, a Case is either automatically created or the Customer can create a Case to report the disruption. Automatic notifications and updates regarding the Case are provided in accordance with the Service Levels set out in this Cloud Service Description and are sent to Customer users who have subscribed to such notifications. When Teradata becomes aware that a service disruption was caused by the Cloud Service Provider, Teradata will update the Case with appropriate information regarding such service disruption.

9. Data Protection

9.1 Data Protection Plans (Backup and Recovery). The Customer can create and manage Data Protection Plans using the Vantage Console. A Data Protection Plan defines the schedule, frequency, and retention policy for data backups using either Standard or Snapshot Backups.

a) "Data Protection Plan" refers to a defined set of rules used to perform system backups according to a predetermined schedule and lifecycle (retention) policy.

b) "Backup" refers to the execution of the Data Protection Plan.

c) A "Backup Job" is the term used to define the process of performing the Backup per the Data Protection Plan.

9.2 Backup Storage Pricing Options. The "Storage Pricing Options" section of this Cloud Service Description describes the available Backup Storage Pricing Options.

9.3 Configuring the Data Protection Plan. The Vantage Console enables the Customer to configure Data Protection Plans. Using self-service capabilities in the Vantage Console, the Customer can configure a Data Protection Plan by providing the following inputs:

a) Data Protection Plan name

b) Schedule (i.e., date, time, frequency)

c) Retention period (i.e., how many restore points to keep)

9.4 Backup Lifecycle and Storage Policy Management. The Customer can change or modify the Backup Lifecycle Policy via processes in the Vantage Console or Support Portal.

a) Backup Jobs are run as an automated process and will continue per the requested policy unless modified or cancelled.

b) Backup Jobs can be configured to run daily, weekly and/or monthly.

c) Older Backups will be deleted automatically per customer-defined lifecycle retention policy.

d) Backups are retained in the same cloud provider region where the Vantage Cloud instance is located.

e) If a Customer creates a backup policy, the Customer is solely responsible for managing that backup policy.

f) Through the Vantage Console, the Customer can perform the backup services shown in the Backup Services and Availability table below.

Backup Services	Availability in Vantage Console
Enable daily, weekly, or monthly backups	●
Disable scheduled Backup Jobs	●
View the status of upcoming and previously executed Backup Jobs	●
Sign up for weekly backup status reports by email	●
Enable auto-restart to re-run a failed Backup Job one time	●
Re-run Backup Jobs	●
Cancel in-progress Backup Jobs	●
Change default and custom backup schedules	●
Edit backup retention policies ***Note**: The Cloud Service Description (CSD) Addendum for the specific cloud platform provides the backup retention terms.*	●
Configure email alerts indicating the Backup Job's status (i.e., start, failure, completed successfully, completed with exception(s), completed with warning(s), and/or schedule changes)	●
Configure Backup Job priorities	●
Restore a full-system Snapshot Backup	●
Restore a Standard Backup to the same system	●
View backup storage utilization over time	●

g) The Customer may set completed backups as "do not delete" for an additional cost due to increased storage usage.

h) For encryption of Backups at rest, the Customer has the option to leverage customer-managed encryption keys in lieu of the default cloud provider-managed encryption keys.

i) Using the Vantage Console, the Customer can perform both standard and optional Backup policies either online or offline. Snapshots are always performed offline.

   i. Online backups contend for access for the objects being backed up and reduce available performance.

   ii. Offline backups usually complete in a shorter timeframe but block write access to objects until the backup job is complete.

j) Backups can be configured as Standard or Snapshot.

   i. Standard Backups can be configured to full, full delta, partial and/or partial delta incremental.

      a. Full and Full Delta Incremental. Full system (DBC All) standard backups can be executed either as Full or Full Delta Incremental jobs.

         - A Full Standard Backup is a complete copy of the system data (DBC All).
         - A Full Delta Incremental Standard Backup covers all the data that has changed since the previous full standard backup, regardless of type (i.e., Full vs. Full Delta Incremental).

      b. Partial Full and Partial Delta Incremental. Partial system standard backups can be either a Partial Full or a Partial Delta Incremental backup job.

- A Partial Full backup includes a subset of the data (e.g., databases, tables, views, etc.) from the overall system. A Partial Full backup is a complete copy of the targeted subset of the data.
- A Partial Delta Incremental backup includes only the data in the partial backup that has changed since the previous partial backup job was run. The first time a Partial Delta Incremental backup job is performed, it will always be a full copy of the targeted subset of data—only the subsequent backup jobs will be performed as an incremental backup.
- Partial backups can be used to split up full system backups into multiple smaller jobs that run at different times.

ii. Snapshot Backups are always full-system and have a limited effect on system availability while in progress.

a. Snapshot Backups can be performed either on an ad-hoc basis or configured to run according to a pre-defined schedule.

b. Incremental Snapshot Backups include only data that has changed since the previous Snapshot Backup was run.

9.5 Backup Support

a) Backup Jobs will initiate a Severity 3 Case Level on job "failure" and will include the status as "Failed." Failure is defined as unable to complete a Backup to its end point.

b) Teradata is responsible for investigating Backup Job failures and for resolving Backup Job failures that are under Teradata's control. Depending on the job failure error, the Customer may be responsible for fixing the root cause of the job failure.

c) Standard Backup Jobs can complete with exceptions and warnings that are reported in the Vantage Console.

d) Standard Backup Jobs completed with exceptions and/or warnings should not be considered as failed or unusable. To ensure Backup Jobs can complete within a reasonable timeframe, objects will be skipped (i.e., excluded) when multiple retries are unsuccessful or if the object is unavailable to backup. Those situations will be reported in the Vantage Console as an exception or warning. If a particular Backup Job continues to skip objects, the Customer should review the job schedule to see if the Backup Job can be rescheduled for a day/time when the affected object(s) will be available.

e) The Customer is responsible for monitoring the status of and configuring email alerts via the Vantage Console for all Backup Jobs, including exceptions and warnings. The Customer can set email alerts for Backup Job start, failure, completed successfully, completed with exception(s), completed with warning(s), and/or schedule changes.

f) The Customer is responsible for resolving exceptions and warnings.

g) If needed, the Customer can submit a Case in the Support Portal to request more information about any exceptions or warnings.

9.6 Restore Requests

a) Restores from a Snapshot Backup. The Customer may perform a self-service restore from the Vantage Console for Snapshot Backups. Snapshot Backups can only be used for full system restores to the point-in-time state from when the last Snapshot Backup was taken.

i. The configuration (e.g., instance type, size, and quantity; storage volume sizes; AMP configurations, etc.) of the VantageCloud system being used as a Snapshot Backup restoration target must match that of the source VantageCloud system from which that Snapshot Backup was taken. When the Snapshot Backup is

restored, it will initiate a reset of the full VantageCloud system, including ecosystem server metadata, where appropriate.

ii. Restores from Snapshot Backups will effectively overwrite existing system data with the last Snapshot Backup data. All data loaded / changed after the last Snapshot Backup was taken will be lost. This action is not reversible.

iii. Partial Restores from a Snapshot Backup are not possible (e.g., table-level restore).

b) Restores from a Standard Backup. The Customer can request a restore to the same system (e.g., Analytics Database tables, databases, and full system-level data) via either a self-service restore from the Vantage Console for a Standard Backup or a Change Request under Standard Backups on the Vantage Console or the Support Portal.

i. For Restores from a Standard Backup requested from a Change Request:

a. Restore jobs are performed manually by Teradata as a one-time operation (i.e., for the requested tables and/or databases) at the date and time agreed upon in the Change Request.

b. The Customer can request up to two (2) restores per month. The Customer must provide the following information in the Change Request:

- Object type(s) and object name(s)
- Standard Backup name and date (i.e., point-in-time)
- Restore maintenance window (i.e., date and time the restore should be implemented)

c. Change Requests for Restores will be designated as “Normal” unless “Emergency” S1 situation requirements are met.

ii. For all Restores from a Standard Backup:

a. A suitable Backup Job must be available to restore from the point-in-time that is requested.

b. Restores can only be applied to the same system from which the Backup Job was generated.

9.7 Additional Customer Responsibilities and Terms

a) The Customer is responsible for scheduling, monitoring, and correcting conflicts that may interfere with scheduled backups or restores (e.g., Data Integration (ETL), data loads, external queries, jobs/flows and queries).

b) The Customer can trigger Backup Jobs remotely using available API calls. The Customer is solely responsible for the use of APIs, including creation of scripts, setup of 3rd party scheduling tools, and managing conflicts between API-triggered backups and scheduled Standard and/or Snapshot Backups.

c) The Customer is responsible for Cron Jobs; these jobs are not supported by Teradata.

d) The Customer must keep Teradata Query Services enabled to take advantage of self-service Standard Backup features.

e) The Customer is responsible for ensuring that an appropriate Full Backup exists—either with a Snapshot Backup or with a full Standard Backup— to meet the Customer’s desired recovery point objective. The Customer can schedule the Full Backup either during System Provisioning or via the Vantage Console. These Backups will be used by Teradata to restore data and VantageCloud services in case of a system outage or hardware / software / OS induced data corruption that has rendered the database unusable and requires full

data restoration. Note that full system restores are performed only when needed to recover from a system outage or data loss/corruption event.

f) The Customer should not schedule concurrent or overlapping Backup Jobs due to possible performance degradation or prolonged job completion times.

g) The Customer is responsible for ensuring that retained Backups are capable of being restored.

10. Compute Pricing Options

Compute Pricing Options are available as described in the Cloud Service Description Addendum for the specific cloud platform.

11. Storage Pricing Options

11.1 Storage Types. Storage and related fee pricing options for VantageCloud Enterprise include Block Storage, Backup Storage, and Data Transfer (ingress/egress).

a) Block Storage is consumed based on the amount provisioned at any point during the contract term. Once increased, the Customer cannot decrease Block Storage.

b) Backup Storage

i. Standard Backup Storage is consumed based on the average storage capacity utilized at any point during each calendar month. Standard Backup Storage is a required purchase to store Standard Backups.

ii. Snapshot Backup Storage is consumed based on the actual total usage during each calendar month. Snapshot Backup Storage is a required purchase to store Snapshot Backups.

c) Data Transfer (Ingress and/or Egress) is consumed based on the actual total usage during each calendar month.

11.2 Storage Commitment. The Customer commits to an amount of Storage for a 12-month term or a 36-month term; there is no credit or refund for unused committed Storage.

a) For a 12-month order term, committed Storage purchased must be used in that 12-month term and unused Storage does not roll over. If the customer uses all of the committed Storage before the end of the 12-month term, the customer can pay for additional Storage at the on-demand rate invoiced monthly in arrears, or upon mutual agreement, the Customer can buy additional committed Storage for the balance of the order term and such committed Storage will expire at the end of the order term.

b) For a 36-month order term, the Customer will allocate a committed amount of Storage for each 12-month period during such order's term. The Customer will be invoiced for each 12-month commitment annually in advance. Committed Storage expires at the end of each 12-month period and does not roll over. If the Customer uses all the committed Storage before the end of a 12-month period, the Customer can pay for any additional Storage at the on-demand rate invoiced monthly in arrears, or upon mutual agreement, the Customer can buy additional committed Storage for either:

i. The balance of that 12-month period and such committed Storage will expire at the end of that 12-month period

ii. The balance of the Order's term, provided that each remaining full or partial 12-month period of the Order's term is increased by the same amount of Storage, with the partial period pro-rated appropriately.

c) In the absence of a Customer commitment, the Customer will be invoiced for the calendar month usage monthly in arrears at the on-demand rate stated in the Order.

d) At the end of a committed Order's term, unless customer has notified Teradata to shut down the Cloud Services or the parties otherwise mutually agree in writing, use of such system is converted to an On Demand Order (on a month-to-month term) at the then-current, on-demand Storage rate.

12. VantageCloud Security

VantageCloud Security includes the following features: Security Standards; Additional Audits or Reviews; Access Control; Security Re-Approval Process; Encryption; Secure Authentication; User Roles; Monitoring; and Vulnerability Management.

12.1 Security Standards. Teradata uses independent, industry-recognized auditors to annually audit the VantageCloud service for compliance with the following standards:

a) Health Insurance Portability and Accountability Act (HIPAA)

b) International Standards Organization (ISO/IEC 27001, 27017)

c) Payment Card Industry Data Security Standard (PCI DSS)

d) Service Organization Controls reports (SOC 1 Type 2, SOC 2 Type 2)

12.2 Additional Audits or Reviews. Any audits or reviews other than those listed in Section 12.1 (Security Standards) will only be allowed if expressly permitted in the Teradata Master Cloud Service Agreement.

12.3 Access Control

a) The Customer controls access to their Customer Data. Teradata treats all Customer Data as private and will only access it with specific permission from the Customer.

b) As part of its Access Protection Policy, Teradata requires its personnel to complete training and to sign security agreements before receiving system access.

c) Teradata enforces password complexity, stores, and transmits only encrypted password representations, and sets minimum and maximum lifetime restrictions on passwords. Teradata cannot view Customer Data without the Customer granting access–and Teradata never transfers Customer Data between countries unless instructed to do so by the Customer.

12.4 Security Re-Approval Process. Re-approval is a standard security operation to ensure that credentials and access rights are reviewed regularly. Teradata establishes a security re-approval process for Teradata personnel that consists of:

a) All access from remote devices to the cloud system is managed via VPN and Multi-Factor Authentication (MFA). Teradata logs all access to systems and sends the logs to a central server where they are protected from tampering. The logs are also correlated and analyzed.

b) Reviewing and approving account management actions

c) Monitoring account management operations for unauthorized actions

d) Disabling inactive accounts after 90 days

e) Disabling VantageCloud accounts after a Teradata user is transferred or terminated

f) Modifying role-based access when a Teradata user's system usage or need-to-know requirements change

12.5 Encryption

a) Teradata gives the Customer options for encrypting data-in-transit and data-at-rest. When enabled, data is encrypted in transit between Teradata and connecting client sessions. Data is also secure from public exposure as it traverses network segments in the Cloud Service Provider's infrastructure by implementing customer-selected connectivity options. Data-at-rest is stored in encrypted volumes in the Cloud Service Provider's storage.

b) Enhanced encryption solutions are also available from Teradata's third-party partners. Additional information is provided in the Cloud Service Description Addendum.

12.6 Secure Authentication. Teradata recommends the use of Federated Authentication / Single Sign-on (SSO) and can also provide optional support for Lightweight Directory Access Protocol (LDAP) as an authentication method. Teradata Database Authentication (TD2) is provided as a default database authentication method.

a) Federated Authentication/SSO: Teradata supports Federated Authentication/SSO. This capability is specific to Customers that have an identity provider (IdP), enables VantageCloud users to log on to the VantageCloud system and supported applications with a single set of their corporate credentials and enables them to move seamlessly between applications. These applications include Teradata Studio, Viewpoint, and certain third-party applications. The Customer Identity Provider can be integrated via the Vantage Console. This Federated Authentication/SSO offers the following features:

   i. Bring Your Own IdP (BYOIDP) - Customer can bring their own IdP to integrate with the VantageCloud native IdP. In this digital authentication approach, user identity is managed by the Customer's IdP.

   ii. Bring Your Own Multi-Factor Authentication (BYOMFA) - VantageCloud customer business users enrolled in MFA with their IdP can engage in that multi-level authentication flow.

   iii. Bring Your Own Third-Party Tool (BYOTT) - Customer can bring their own third-party Business Intelligence (BI) tools and participate in a secure single sign-on experience.

   iv. Federation Standard Protocols - VantageCloud Enterprise supports both SAML and OpenID Connect (OIDC) protocols. SAML is an XML-based open-standard for exchanging authentication and authorization data between applications. OIDC uses JSON Web Tokens (JWT) obtained through a standard OAuth 2.0 flow.

b) Teradata Database Authentication (TD2). Teradata provides the TD2 mechanism as a default for Teradata database authentication.

c) Lightweight Directory Access Protocol (LDAP). VantageCloud supports LDAP directory services integration over SSL/TLS (LDAPS). VantageCloud secure LDAP directory services integration for secure authentication is available by Teradata Consulting for an additional fee.

d) Kerberos. Teradata supports Kerberos single sign-on (SSO) secure user authentication between Customer domain users and a VantageCloud system where the Customer external directory service is designated as the Kerberos Key Distribution Center (KDC). This option does not require network connectivity between VantageCloud and the customer's external directory service.

12.7 User Roles. Designated users receive user IDs from Teradata with permission to access VantageCloud and its stored data. User types DBC (superuser), SYSDBA (VantageCloud management), and SECADM (security administration) receive TD2 authentication and default passwords, which the Customer is responsible for changing after the first use.

12.8 Monitoring. The VantageCloud security monitoring process collects and correlates relevant security policy events. VantageCloud systems are configured to log events such as failed login attempts, account creation, account removal, system policy changes, privileged access, IPS, etc. The logs are sent to the Security Information and Event Management system (SIEM), correlated, and analyzed in real time.

a) The SIEM database containing system logs is stored in a secure and tamper-proof area. Other events are audited, as appropriate, to monitor security-critical functions, respond to new threats, and to investigate potential security incidents.

b) Customer is responsible for performing scans on their own underlying infrastructure, applications, and database content.

12.9 Vulnerability Management. Teradata performs regular scans of the system and code to identify and remediate vulnerabilities in the software and operating systems. This is performed through a combination of static application security analysis and both network and application-level vulnerability assessments.

13. Pre-General Availability (GA) Offerings

Teradata may make available, and the Customer may choose to use, pre-general availability features for VantageCloud that are identified as “Limited Availability,” “Early Access,” “Preview,” “Alpha,” “Beta,” or a similar designation in related documentation or materials. Pre-General Availability offerings are not necessarily feature-complete, nor do they necessarily have technical support commitments. Unless otherwise stated by Teradata, Pre-General Availability features are intended for use in test environments only and should not be used to process personally identifiable data or data subject to legal or regulatory compliance requirements. Customer may provide feedback and suggestions to Teradata about pre-general availability offerings, and Teradata and its affiliates may use any feedback or suggestions provided without restriction and without obligation to the Customer. Pre-General Availability offerings may be changed, suspended, or discontinued at any time without prior notice to the Customer and are not covered by any Service Level Agreement.

14. Additional Services (Sold Separately)

Teradata has a wide variety of additional services (sold separately) for VantageCloud Customer needs, including:

14.1 Essential Success Service is an add-on to the Premier Cloud Support or Priority Service Support levels.

a) Essential Success Service is included for Analytics Database instances with greater than 70 TCores or 367,000 TCore-Hours.

b) Essential Success Service is included with the Vantage Units Consumption Pricing model.

c) Essential Success Service includes the following features:

i. Customer Support Plan. Teradata documents ongoing customer support processes (including roles and responsibilities) in a support plan that the Customer can access via the Support Portal.

ii. Assigned Service Management

a. Teradata will assign a Service Management resource to the Customer during onboarding.

b. For each Severity 1 Case, a Teradata representative conducts a "post-case" analysis that includes a closed loop corrective action plan. Teradata informs the customer of any changes in the product support policy permitted by, and in accordance with, this document, any order, or the agreement.

c. On an annual basis, the assigned Service Management resource will review the customer service offer to assess service coverage, determine how current services will satisfy any planned platform enhancements, and discuss future opportunities for developing the customer's relationship with Teradata.

iii. Service Advisory

a. Teradata will provide access to Teradata experts and resources to advise and assist the Customer with initial Support Portal onboarding, including Access Management and an overview of Support and Operational Services.

b. Teradata will provide ongoing Support and Operational Service Advisory via a Support Ticket in the Support Portal.

iv. Support Management

a. Teradata will provide resources to monitor and coordinate the delivery of Service Features to the Customer.

b. Teradata will provide resources to assist the customer with the escalation of Support Tickets.

c. Teradata will provide a resource to advise and coordinate during quarterly Customer Connections.

v. Service Report. Teradata will provide a Quarterly Service Report of service highlights, service recommendations, and services summary. Service Reports will be published in the Support Portal and can be reviewed during Customer Connections.

vi. Customer Connections. Teradata will conduct a virtual quarterly Customer Connection meeting, limited to 1-hour, for review of service reports and service performance.

vii. Viewpoint Configuration. Teradata will configure one (1) Teradata Viewpoint application using Teradata database administration best practices, including:

a. Standardized Portlets and Shared Pages for Customer Business Users, Developers, and DBAs

b. Standardized Database Alerts

c. System Monitoring and Telemetry, including Remote Connectivity, are required to provide this service feature

viii. Performance Data Collection Reporting (PDCR) Configuration

a. Teradata provides an initial standard configuration of the PDCR components.

b. Teradata will support one (1) maintenance activity for the PDCR configuration per year. This annual PDCR maintenance activity includes a PDCR review and, if necessary, an update to the configuration of the PDCR components, which may include an upgrade to the PDCR database and/or the migration of historical PDCR data.

c. Any Customer-initiated changes to the standard PDCR configuration are not in scope for annual maintenance activities. Support for customized configurations is available for an additional fee.

d. System Monitoring and Telemetry, including Remote Connectivity, are required to provide this service feature.

ix. Teradata Education Checkbook

a. Teradata provides one standard Education Checkbook allowance per Customer.

b. The checkbook can be used solely to purchase:

- a seat in a Teradata live public course, and/or
- a subscription to the entirety of Teradata University, and/or
- a voucher to sit for Teradata certification exams.

c. The checkbook allowance must be used during the initial VantageCloud Enterprise Service Term. Teradata may provide additional checkbook allowances for renewal terms

d. Canceling or rescheduling Education Checkbook purchases with less than 10 business days' notice will result in a full charge, including any instructor travel expenses

14.2 Optimize Success Service builds upon the Essential Success Services offering to engage additional tools, processes, and resources that are designed to improve the operation of the analytical ecosystem.

14.3 Backup Service Options refer to anything above and beyond the standard backup service listed above.

14.4 Performance Service Options not listed in the Cloud Service Description are available for Workload Management, Application Performance, Performance Data Analytics, and Capacity Management.

14.5 Database Administration and Operations Managed Services provides administration, operations, and production services for the Customer's Cloud ecosystem.

14.6 Migration Service Options assist the Customer during the migration to VantageCloud, including Data Migration, Viewpoint Migration, QueryGrid Migration, LDAP Migration.

Teradata VantageCloud Enterprise

Cloud Service Description: AWS Managed Application Addendum

Blended Pricing

This document supplements the Teradata VantageCloud Enterprise Cloud Service Description featuring blended compute pricing options.

September 18, 2023

Table of Contents

1. Teradata VantageCloud Enterprise as an AWS Managed Application

Teradata deploys VantageCloud Enterprise as an AWS Managed Application in a Customer-owned AWS account that is dedicated to host the infrastructure for VantageCloud as a Managed Application workload. This document supplements the Teradata VantageCloud Enterprise Cloud Service Description.

The Customer must provide administrator rights on the AWS account to Teradata using the AWS Identity and Access Management (IAM) service. Teradata needs rights to provision, operate, maintain, and upgrade the AWS instance based on Teradata's standard policies and procedures. The Customer has a view-only IAM role access to the AWS instance running Vantage and the resources in this AWS account. Customer might want to subscribe to a VantageCloud environment in an AWS account in the same AWS region as their data.

2. Responsibilities

The cloud service provider, Teradata, and the Customer all have responsibilities within a shared security model for the management of the VantageCloud system, as shown in the VantageCloud System Management table below.

VantageCloud System Management	
Responsibility	**Responsible Party**
Hardware	Customer (Cloud Service Provider)
Data Center / Hosting	Customer (Cloud Service Provider)
Initial Data Migration	Customer
System Availability Monitoring	Teradata (OS and Analytics Database software)
Software Patching/Upgrading	Teradata
Premier Cloud Support (software)	Teradata
Cloud Platform Support	Customer (Cloud Service Provider)
Database Administration / Operations • Database security monitoring – managing VantageCloud security roles, passwords, and access rights • Maintaining VantageCloud structures, space, users, and jobs • Monitoring alerts, queries, access locks, and database performance • Analyzing database activity and priority of jobs/queries to identify performance tuning opportunities • Managing consumption and query performance	Customer ***Note**: Teradata can take on some of these responsibilities with Teradata Database Administration and Operations Service (sold separately)*
Operating System (OS) Administration / Operations • OS security monitoring • Volume encryption • OS user administration for Teradata personnel	Teradata
Network Administration / Operations • Restrictions / filtering of incoming traffic to VantageCloud environment	Teradata/Customer*
Cloud Environment Administration / Operations • Security monitoring of the VantageCloud environment • Cloud environment access management for Teradata personnel	Teradata/Customer*

VantageCloud System Management	
Responsibility	**Responsible Party**
Backup and Restoration	Teradata – • Sets up the Default Backup Configuration • Backup Support and Restore Requests per defined scope Customer – • Backup Lifecycle and Storage Policy Management • Backup Support (for exceptions and warnings) per defined scope
** Because the Customer also holds privileged credentials to the account hosting the VantageCloud infrastructure, both Teradata and the Customer are responsible for securing their respective user credentials.*	

2.1 Teradata may add, change, or remove infrastructure to Vantage site as part of improvements and optimizations to the as-a-service offering. This change can be done by Teradata without consulting or notifying Customer under the following scenarios.

a) Permanent changes – Design updates, feature additions/ changes.

b) Temporary changes - Upgrades, root-cause analysis during failures etc.

2.2 Customer is responsible for facilitating a capacity reservation for the required AWS infrastructure within the provided account/subscription (if required). Failing to do so will void Teradata SLAs and/or result in suspension of service. Customer must maintain the capacity reservation for the duration of the VantageCloud subscription.

2.3 The availability of a service-level agreement (SLA) applies only to the Analytics Database software. The SLA does not apply to availability issues caused by AWS infrastructure components.

2.4 Teradata is responsible for certifying the environment to meet compliance with audits included within the VantageCloud Enterprise service.

2.5 Customer is prohibited from modifying the permissions on the account after they provide administrator rights to Teradata.

2.6 Customer is prohibited from accessing VantageCloud as an AWS Managed Application account and systems within the Account using means other than Teradata-approved access mechanisms or the view-only IAM role.

3. Working with AWS

Customer must add Teradata to all correspondence with AWS that affects the availability and stability of VantageCloud as a Managed Application system. Scenarios might arise where Teradata, the Customer, and AWS will need to work together to resolve issues. In such scenarios, Teradata is not responsible for any delays experienced in restoring the service.

4. Incident Resolution

The Customer must provide Teradata with AWS recommended Identity Access Management (IAM) permissions within the Customer AWS Managed Application account.

4.1 The IAM permissions should enable Teradata to:

a) Open, own, and edit incidents in the Customer's AWS account.

b) Receive updates made to the incidents as needed to restore or maintain service, stability, and performance of VantageCloud Enterprise as an AWS Managed Application systems.

4.2 Should Teradata request, the Customer will provide authorization (by email) to allow Teradata's AWS Technical Account Managers to:

a) Engage to resolve the incident.

b) Be able to access logs and other relevant details as available to the Customer's AWS Technical Account Managers.

4.3 The Customer will add Teradata's provided email address as an alternate contact for Operations and Security for the AWS Managed Application account

5. Access to VantageCloud by Teradata

Customer is responsible for procuring the cloud infrastructure. Teradata provides VantageCloud software and operational services; therefore, the availability service-level agreement (SLA) applies only to Teradata Analytics Database software.

5.1 If the Customer takes any of the following actions, they may void the availability SLA and security compliance such as Payment Card Industry Data Security Standard (PCI DSS), Service Organization Control (SOC), and so on.

a) Using the root user account to log on to the Managed Application account

b) Assuming IAM role into the managed app account from the master account

c) Revoking assumes role access for Teradata or modifying or using the AWSAccountAccessRole

d) Creating a new role or other mechanism that might provide the ability to change Teradata access permissions

e) Accessing the APIs of the services provided by Teradata in the managed application environment

f) Accessing or changing deployed resources like VPCs or VMs specifically for managed app in the Customer account

5.2 These actions might result in loss of the Teradata solution, including loss of Customer data. In such a scenario, the availability SLA won't be applicable, and Teradata is not responsible for any data loss that occurs.

5.3 If there is data or service loss, Teradata will attempt to restore data and service on a best effort basis using our backup restoration services or enhanced backup restoration services at an additional cost.

6. Compute Pricing Options

Pricing for VantageCloud Enterprise is available in three options: Fixed Capacity, Elastic Performance on Demand (EPOD), and Flexible Capacity. Each VantageCloud system can support only one pricing option. In this Section, "compute capacity" refers to the cloud computing infrastructure capability the Customer has procured from the Cloud Service Provider.

***Note**: VantageCloud Enterprise as a Managed Application is not offered in the Consumption Pricing model.*

6.1 Blended Pricing models refer to Fixed Capacity, Elastic Performance on Demand, and Flexible Capacity pricing constructs as indicated below.

a) Fixed Capacity consists of fixed baseline TCore purchased for the Cloud Service Term along with the option to obtain additional capacity for a variable term.

i. Fixed Capacity Baseline is measured in TCores. The Customer must order a fixed amount of compute capacity for the full Cloud Service Term and cannot reduce capacity below this level.

ii. Adjustable Capacity refers to additional CPU, memory, and I/O that can be added or removed on demand by using VantageCloud elasticity features during the Cloud Service Term (see table in Section 8 below). This additional capacity is billed in On Demand TCore-Hours monthly in arrears and is a function of: a) the number, type, and size of the provisioned Analytics Database compute instances; b) their respective TCore ratings; and c) the number of full or partial hours that the adjusted Analytics Database compute instances are provisioned. The computation of On Demand TCore-Hours also accounts for the Fixed Capacity Baseline ordered.

b) Elastic Performance on Demand (EPOD) refers to when Teradata provisions additional fixed compute capacity in the instance. The Customer starts by purchasing Committed EPOD TCore-Hours. When the Customer's processing uses the additional compute capacity in the instance, that usage consumes the EPOD TCore-Hours—first from any Committed EPOD TCore-Hours and then from On Demand TCore-Hours.

i. Fixed Capacity Baseline is measured in TCores. The Customer must order a fixed amount of compute capacity for the full Cloud Service Term and cannot reduce capacity below this level.

ii. Committed EPOD TCore-Hours are purchased at the beginning of each contract year in the Cloud Service Term and are consumed over that contract year. Unused EPOD TCore-Hours expire at the end of each contract year and do not roll over. If/when Committed EPOD TCore-Hours are fully consumed during a contract year, EPOD usage is then billed at the On Demand EPOD TCore-Hourly rate. EPOD is subject to a minimum annual purchase quantity of EPOD TCore-Hours based on the provisioned additional fixed compute capacity.

iii. On Demand EPOD TCore-Hours usage is billed at the On Demand EPOD TCore-Hourly rate if/when Committed EPOD TCore-Hours are fully consumed during a contract year. On Demand EPOD TCore-Hours are billed monthly in arrears.

iv. EPOD TCore-Hour Usage is measured by Teradata during each month of the Cloud Service Term by running a standard report that sums up both the time that the compute instance was processing and the TCore rating of each Analytics Database instance. That total is converted to TCore-Hours. Then, the Fixed Capacity Baseline TCore that the Customer purchased is deducted from the total. The remainder is the TCore-Hours used in that month.

c) Flexible Capacity allows the Customer to vary the compute capacity of the instance during the Cloud Service Term. Flexible Capacity is measured in both Committed TCore-Hours and On Demand TCore-Hours. ***Note: The Flexible Capacity compute pricing option will be discontinued effective October 1, 2023. Existing orders with Flexible Capacity compute pricing will be supported through December 31, 2026.***

i. Committed TCore-Hours are purchased at the beginning of each contract year in the Cloud Service Term and consumed over that contract year. Unused TCore-Hours expire at the end of each contract year and do not roll over. If/when Committed TCore-Hours are fully consumed during a contract year, Flexible Capacity is then billed at the On Demand TCore-Hourly rate. Flexible Capacity has a minimum annual commitment of 25,000 Committed TCore-Hours per Analytics Database instance. The rate of TCore-Hours drawn down from this annual commitment depends upon: a) the number, type, and size of the provisioned Analytics Database compute instances; b) their respective TCore ratings; and c) the number of full or partial hours that the Analytics Database compute instances are provisioned.

ii. On Demand TCore-Hours are billed monthly in arrears and reflect: a) the number, type, and size of the provisioned Analytics Database compute instances; b) their respective TCore ratings; and c) the number of full or partial hours that the Analytics Database compute instances are provisioned.

iii. The VantageCloud elasticity features (see table in Subscription Features section below) can be used to add and remove compute capacity of a VantageCloud instance as needed to meet workload requirements.

7. Subscription Features

The Cloud Service Description describes many of the features specified in this Cloud Service Description AWS Managed Application Addendum. The Cloud Service Features and Descriptions table shown below also summarizes the features.

Cloud Service Features and Descriptions	
Features	**Descriptions**
System Features (Included)	
Availability	24 x 7 availability service-level agreement (SLA of 99.9%) for the Analytics Database, measured and tracked monthly ***Note:*** *The 99.9% SLA applies only to the Teradata VantageCloud software and not the cloud infrastructure since that is deployed in the Customer's AWS account.* ***Note****: The availability SLA of 99.9% is not applicable to a disaster recovery event where the cloud provider availability zone or region is impacted. If VantageCloud is deployed in a cloud provider region that has multiple availability zones, Teradata will use reasonable efforts to deploy a new system in a secondary, unimpacted availability zone and restore from an existing backup to the secondary, unimpacted availability zone as part of our service.*
Onboarding Services	System provisioning and validation
System Monitoring	Infrastructure and operating system monitoring
System Maintenance	Software patches and version upgrades ***Note****: The monthly maintenance and upgrade process requires an AWS EBS Snapshot be taken for the component being upgraded. This will incur an additional AWS EBS Snapshot charge. The snapshots are subsequently deleted after the successful completion of an upgrade.*
System Backups	Default Backup Lifecycle Policy is zero full system Standard Backups and zero copies retained. Customer has the option of scheduling Standard Backups to be executed by Teradata daily, weekly, or monthly. Standard Backup storage must be purchased to support Standard Backups and to retain additional copies as needed. Snapshot Backup storage must be purchased as needed to support the required snapshot frequency and retention policy. Custom backup services (such as copying backups to multiple availability zones or regions for disaster recovery purposes) are purchased separately through Teradata Consulting and/or Teradata Services. ***Note:*** *Teradata backs up VantageCloud instances only as directed by the Customer.*

Cloud Service Features and Descriptions	
Features	**Descriptions**
Encryption	Data in Transit. Teradata provides Customer with choices for encryption of data at rest and in transit. When enabled, data is encrypted in transit between Teradata and connected client sessions. Data at Rest. AWS-managed Encryption Keys. By default, VantageCloud Data Store uses AWS-managed AWS KMS keys for encryption at rest. Customer may, optionally and where available, use Customer-managed AWS KMS keys to manage these keys themselves. Third-party Applications. As an enhanced security option, database administrators can leverage third-party partner software (sold separately) to encrypt and control access to individual rows and columns within the database
Elasticity Features (Available for Blended Pricing Only)	
VantageCloud Stop/Start	• Stop and restart VantageCloud instances without affecting persistent storage (subject to the cloud infrastructure availability). • Stop/Start will pause/resume the rate of TCore-Hour consumption when the VantageCloud instance is stopped/restarted. ***Note:*** *Available for Flexible Capacity pricing only.* ***Note****: Queries that are running when the VantageCloud instance is stopped are not automatically resumed and must be restarted after the VantageCloud instance is restarted.* ***Note****: VantageCloud Stop/Start alters the runtime state of Analytics Database only and does not extend to other components and services (and any associated fees) such as Applications, backups, network egress, etc.*
VantageCloud Scale Out/In	• Change number of Analytics Database node instances without affecting persistent storage (subject to the cloud infrastructure availability). • Scale Out/In will increase/decrease the rate of TCore-Hour consumption based on the number and size of the instances being added or removed to the VantageCloud system. ***Note****: Available for Fixed Capacity and Flexible Capacity pricing options only.* ***Note****: Scale Out/In operations result in the VantageCloud instances being restarted during which time Customer cannot submit queries and any running queries will need to be restarted.*
VantageCloud Scale Up/Down	• Change Analytics Database node instance sizes without affecting persistent storage (subject to the cloud infrastructure availability). • Scale Up/Down will increase/decrease the rate of TCore-Hour consumption. ***Note****: Available for Fixed Capacity and Flexible Capacity pricing options only.* ***Note****: Scale Up/Down operations result in the VantageCloud instances being restarted during which time Customer cannot submit queries and any running queries will need to be restarted.*
Elastic Performance on Demand (EPOD)	Add additional VantageCloud compute capacity without any downtime. EPOD capacity up to the baseline VantageCloud system size is possible. ***Note****: Available for the EPOD pricing option only.*
Elasticity Features (Available for all Pricing Options)	
Block Storage Expansion	Expand block storage after deployment at the system level via a new Order ***Note****: Block Storage Expansion operations result in the VantageCloud system being restarted during which time Customer cannot submit queries and any running queries will need to be restarted.* ***Note****: Block Storage Expansion is a one-way operation. Once increased, block storage capacity cannot be reduced.*
Self-Service Interfaces (Included)	
Service Portal	Submit incidents and other requests
Vantage Console	Monitor and manage systems, users, and tickets
Additional Fees (Required)	

Cloud Service Features and Descriptions	
Features	**Descriptions**
Standard Backup storage	Storage to persist standard backups is required for Standard Backups
Snapshot Backup storage	Storage to persist snapshot-based backups is required for Snapshot Backups
Additional Fees (Optional)	
Additional TCore-Hours	Additional TCore available on demand (Blended Pricing option required)
Teradata Success Services	Proactive operational support and service management
Priority Service	Increased incident support coverage hours and accelerated response times

8. Applications

This section describes various applications, including packaging options, that are either included with the VantageCloud subscription or that are sold separately.

8.1 Application Packaging Options Summary. This section describes various applications, including packaging options, that are either included with the VantageCloud subscription or that are sold separately, as shown in the Applications Packaging Options Summary table below.

Application Packaging Options Summary		
Package	**Availability**	**Details**
Cloud Foundation	Included	Included with VantageCloud Subscription.
A-la-Carte Teradata Applications	Sold separately	Alternative purchase option for Teradata applications on an individual application-by-application basis.
Third-Party Tools	Sold separately	• Customer may bring their own license for approved third-party partner tools (BYOL) that reside within the VantageCloud Enterprise as an AWS Managed Application environment. • Subject to an additional third-party software hosting fee.

8.2 Cloud Foundation (Included). Cloud Foundation bundles the foundational applications included with the VantageCloud subscription, as shown in the Cloud Foundation table below.

Cloud Foundation	
Application	**Details**
Teradata Analytics Database	Included with VantageCloud subscription.
Teradata Data Mover	• One instance included. • Requires implementation by Teradata Consulting for an additional fee. • VantageCloud Enterprise as an AWS Managed Application must be used as either a source or target.
Teradata Query Service	Included with VantageCloud subscription.
Teradata Viewpoint	One standard-size instance included with VantageCloud subscription.
Teradata Vantage Editor	Included with VantageCloud subscription and is part of console. ***Note:*** *Enablement requested by the Customer via Standard Change Request.*

8.3 A-la-Carte Teradata Applications (Sold Separately). For an additional fee, Teradata applications may be purchased individually.

A-La-Carte Teradata Applications	
Application	**Availability**
Teradata Data Lab	Available
Teradata Data Mover	• Available in one size • Requires implementation by Teradata Consulting for an additional fee. • VantageCloud Enterprise as an AWS Managed Application must be used as either a source or target. ***Note**: The first instance is included in Cloud Foundation. Up to three additional instances may be purchased.*
Teradata QueryGrid	• Available • Teradata Connectors for one VantageCloud system • Includes one instance of Teradata QueryGrid Manager per VantageCloud system. • Requires implementation by Teradata Consulting for an additional fee.
Teradata Viewpoint	• Available • One standard-size instance is included with Cloud Foundation.
Teradata Vantage Analyst	• Available ***Note:** Enablement requested by the Customer via Standard Change Request.*
Teradata Business Continuity Manager	• Available (Blended Compute pricing option only) • Must license all TCore for both production and hot standby systems to use the Business Continuity Manager

8.4 Third-Party Tools Descriptions (Sold Separately). For an additional fee, called the VantageCloud Third-Party Software Hosting Fee, Teradata will host approved and licensed third-party software as described in this section.

a) Third-Party Tools are available only through a bring-your-own-license (BYOL) model where the Customer is required to enter into a separate agreement directly with the third-party vendor to license, maintain, and support the Third-Party Tool for the duration of the Customer's VantageCloud subscription.

b) Customer is responsible for engaging the Third-Party Tool vendor for software maintenance and support. Teradata agrees to perform activities that are necessary for such maintenance and support of the Third-Party Tool software in a VantageCloud environment that require infrastructure or node-level access, but only as specifically described and directed by the Customer.

c) Service Availability. SLA commitments do not apply to the extent that Teradata reasonably determines a failure was caused by the Third-Party Tool software.

d) Customer is responsible for managing their own Third-Party Tool configurations, including application policies, passwords, and encryption keys.

Third-Party Tools Descriptions	
Third-Party Tool	**Details**
Protegrity	Protegrity develops enterprise data security software and provides scalable, end-to-end data security solutions. Protegrity Data Security Platform helps Teradata Customers secure sensitive data and comply with privacy regulations. Protegrity includes two components that pertain to VantageCloud: • Protegrity Database Protector for Teradata: Provides policy-based data encryption and tokenization capabilities for Analytics Database. • Protegrity Enterprise Security Administrator (ESA): Provides Customer with centralized, visual administration of data security policies, key management, auditing, and reporting. Protegrity ESA must be installed, hosted, and managed by the Customer, outside of the VantageCloud environment managed by Teradata. ***Note**: Customer must contract with Teradata Consulting to assist with implementation for an additional fee.*
Thales CipherTrust Protection for Teradata (CPT)	Thales develops enterprise data security software and provides scalable, end-to-end data security solutions. Thales CipherTrust Protection for Teradata helps Teradata Customers secure sensitive data and comply with privacy regulations. CipherTrust Protection for Teradata includes two components that pertain to VantageCloud: • CipherTrust Protection for Teradata: Provides encryption and decryption controls for securing sensitive columns in Analytics Database. • CipherTrust Manager: Provides Customer with centralized administration of data security policies, key management, auditing, and reporting. CipherTrust Manager must be installed, hosted, and managed by the Customer outside of the VantageCloud environment managed by Teradata. ***Note**: Customer must contract with Teradata Consulting to assist with implementation for an additional fee.*
Imperva SecureSphere	Imperva SecureSphere for Teradata database is a database activity monitoring (DAM) solution that provides real-time database protection and security. It helps Teradata Customers monitor and audit access to all sensitive data and helps Customers to satisfy compliance requirements. Imperva DAM reads database traffic from VantageCloud Analytics Database for monitoring, auditing, reporting, and alerting Customers. Imperva integrates with Teradata using an on-node agent installation that communicates to a management, rule-based command, and control console known as Imperva SecureSphere Management Server. Imperva SecureSphere Management Server must be installed, hosted, and managed by the Customer, outside of the VantageCloud environment managed by Teradata. ***Note**: Customer must contract with Teradata Consulting to assist with implementation for an additional fee.*
IBM Guardium	Guardium is a data protection and network monitoring tool from IBM. It provides a database activity monitoring system (DAM), which reads network traffic from the database for collection, aggregation, monitoring, reporting, and alerting on user activity on the integrated database. Guardium integrates with VantageCloud using an agentless "Guardium Exit Library" configuration that communicates to a rule-based management command and control console that is hosted and managed by the Customer, outside of the Teradata-managed VantageCloud environment. S-TAP/K-TAP integrations are not supported. Guardium Exit Library is the supported integration. ***Note**: Customer must contract with Teradata Consulting to assist with implementation for an additional fee.*
Dataguise	Dataguise is a provider of data-centric audit and protection (DCAP) solutions that discover sensitive data and secure it. DgSecure by Dataguise detects, protects, audits, and monitors sensitive data across the enterprise for data stored in VantageCloud by means of functions installed on the VantageCloud Analytics Database. ***Note**: Customer must contract with Teradata Consulting to assist with implementation for an additional fee.*

Third-Party Tools Descriptions	
Third-Party Tool	**Details**
SAS Embedded Process (SAS EP)	• SAS develops and markets a suite of analytics software, which helps access, manage, analyze and report on data to aid in decision-making. SAS Embedded Process helps bring to Teradata Customer advanced analytics capabilities through SAS code in Teradata VantageCloud without moving data out of VantageCloud. • SAS EP includes two components that pertain to VantageCloud: ○ SAS User-Defined Function (UDF) Server components: Includes SAS EP, SAS EP Support Functions, and the SAS Formats library. Installing or upgrading SAS EP is independent of VantageCloud. However, if these components are required. Teradata will install SAS UDF Server components for an additional fee. ○ SAS client-side software: Provides an interface that Customer can use to initiate function calls and analyze the results.

9. Supported AWS Connectivity Options

Connectivity for VantageCloud is described in the Supported AWS Connectivity Options table below.

Supported AWS Connectivity Options	
Connectivity Options	**Details**
AWS Transit Gateway (TGW)	• This is the recommended option • Customer must deploy the TGW in their account • The Customer uses a network transit hub to interconnect the VPCs and on-prem networks • For quotas or bandwidth details, click here.
VPN	• One virtual private network (VPN) connection • Standard connection speed up to 1.25 Gbps, subject to AWS published data rates for an AWS-managed VPN Virtual private gateway
AWS PrivateLink	• AWS PrivateLink is supported by an endpoint in a Customer VPC • Supports a connection speed of up to 25 Gbps
Direct Connect	• AWS Direct Connect allows the Customer to establish a dedicated network connection from their premises to the VantageCloud instance in AWS. • Using AWS Direct Connect, you establish a private connection between AWS and your datacenter, office, or colocation environment.
Direct Connect Gateway	• Customer must deploy the Direct Connect Gateway in their account • Teradata will support creating an association with Customer owned and managed Direct Connect Gateway • Teradata will invoice the Customer for egress traffic on Direct Gateway attachment. • Provides Hybrid connectivity option to the Customer with the flexibility of AWS Direct Connect Gateway • AWS Direct Connect gateway will give Customer ability to interface with VPCs in any AWS Region (except the AWS China Region), so Customer can use AWS Direct Connect connections to interface with VaaS site in more than one AWS Region

10. Supported AWS Instances

VantageCloud offers instance options based on Customer infrastructure and performance requirements. Instances are preconfigured with Teradata software, as shown in the Supported AWS Instances table below.

Supported AWS Instances					
Engine	**Instance Series**	**Instance Size**	**Instance Limit**	**TCore Per Instance**	**Key Attributes**
Analytics Database	R6i	XSmall 2	2-128	1.52	Separate compute and storage for elasticity Fallback for availability
		Small 3		3.03	
		Medium 2		6.06	
		Large 3		9.09	
		XLarge 7		12.11	
		XXLarge 8		18.17	
	R5	Small 1	2-128	2.96	
		Medium		5.14	
		Large 1		7.51	
		XLarge 1		10.29	
		XXLarge 1		15.03	
	R5b	Small 2	2-128	4.46	
		Large 2		8.91	
		XLarge 2		11.66	
		XLarge 3		12.46	
		XLarge 4		13.26	
		XLarge 5		13.37	
		XLarge 6		14.74	
		XXLarge 2		16.23	
		XXLarge 3		16.46	
		XXLarge 4		17.83	
		XXLarge 5		19.89	
		XXLarge 6		23.31	
		XXLarge 7		26.74	

11. Supported AWS Regions

VantageCloud is supported in the AWS Regions indicated in the Supported AWS Regions table below.

Supported AWS Regions	
Region Name	**Region**
North America	
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Canada (Central)	ca-central-1
South America	
South America (Sao Paulo)	sa-east-1
Asia Pacific	
AP (Mumbai)	ap-south-1
AP (Singapore)	ap-southeast-1
AP (Sydney)	ap-southeast-2
AP (Tokyo)	ap-northeast-1
AP (Seoul)	ap-northeast-2
Europe	
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
EU (London)	eu-west-2
EU (Paris)	eu-west-3
EU (Stockholm)	eu-north-1
EU (Milan)	eu-south-1
EU (Spain)	eu-south-2
EU(Zurich)	eu-central-2
Middle East	
Middle East (Bahrain)	me-south-1
Africa	
AF (Cape Town)	af-south-1