MICROSTRATEGY CLOUD ENVIRONMENT SERVICE GUIDE

Update published July 2021

MicroStrategy
Intelligence Everywhere

Table of Contents

1. Overview

The MicroStrategy Cloud Environment service ("MCE" or "MCE Service") is a platform-as-a-service ("PaaS") offering that MicroStrategy manages on its customers' behalf in an Amazon Web Services or Microsoft Azure environment that includes access to, collectively, (a) the "Cloud Platform" version of MicroStrategy software products (an optimized version of the MicroStrategy software platform built specifically for deployment in an Amazon Web Services or Microsoft Azure environment) licensed by the customer; (b) Cloud Support, as described below; and (c) Cloud Architecture, as described below. MicroStrategy's PaaS delivery model is designed to allow businesses to consume the MicroStrategy Analytics and Mobility platform in a single tenant architecture without the need to deploy and manage the underlying infrastructure.

MCE offers a distributed compute architecture using cloud-native services provided by either Microsoft Azure or Amazon Web Services. As this technology evolves, MicroStrategy continually incorporates new services that allow for increased availability, security, or performance to ensure the latest architecture is available to our customers. At the core of the solution are MicroStrategy Analytics and Mobility, a secure, scalable, and resilient business intelligence enterprise application platform.

MCE also includes the elements needed to operate, access, and manage the intelligence architecture. Users are provisioned with their own dedicated intelligence architecture based on a reference architecture. Once provisioned, users can develop, tailor, and manage the application components to meet their respective needs.

Based on this operating model, customers administer and control the Analytics and Mobility solution while MicroStrategy maintains the supporting cloud-based infrastructure.

2. Cloud Support

As an MCE Service customer, you will receive "Cloud Application Support" ("Cloud Support") in which our Cloud Support engineers will provide on-going support over your MCE Service term to assist in maximizing the performance and agility—and minimizing the cost— of your MicroStrategy Cloud Platform deployment. Cloud Support includes environment configuration (setting up customer accounts in a selected VPC or VNET), enterprise data warehouse integration (including modifying the MicroStrategy configuration for data warehouse connections and opening up any connectivity for external data warehouses), authentication (SSO/LDAP), and application integration (creating connectivity for Office Plugin). Additionally, Standard Support for the Cloud Platform version of MicroStrategy Products is provided with the licenses for such Products pursuant to your contract with MicroStrategy and our Technical Support Policies and Procedures, except that all MCE customers are entitled to four Support Liaisons (as defined in the Technical Support Policies and Procedures).

If a production outage issue occurs, MicroStrategy reserves the right to fix the issue on behalf of the customer without pre-authorization. If a support issue is logged and determined through the diagnosisthat the Root Cause Analysis (RCA) that the stated issue is due to a customer-specific customization of the MicroStrategy application, the Support team will provide the customer with available options to resolve issue. These solutions may require the purchase of MicroStrategy Professional Services for additional assistance depending on the complexity of the issue.

3. Cloud Architecture

The Cloud Architecture offered as part of the MCE Service is an optimized reference architecture providing enterprise-grade data design and governance, and consists of (a) the Cloud infrastructure and architecture components required to run your PaaS environment, configured through either the Enterprise MCE Architecture or High-Availability MCE Architecture constructs detailed below, and (b) Cloud Environment Support, the support services and components needed to successfully run the infrastructure and architecture components of the MCE Service offering. Additionally, all MCE customers will receive up to 500 GB per month of data egress at no additional charge.

3.1 Cloud Infrastructure

Our MCE Service offers two types of single tenant platform architectures built based on industry best practices for security, compliance, and availability. The building blocks of these PaaS components are (i) the Cloud Architecture Standard Offering, which includes a base infrastructure package and optional additional nodes; and (ii) the Cloud Architecture Small Offering, which includes a base infrastructure package and is available for purchase by certain small to medium sized customers with less complex requirements. Both Cloud Architecture Offerings include 24x7x365 system monitoring and alerting, daily backups for streamlined disaster recovery, and annual compliance checks and security certifications. These offerings are procured on your behalf from Microsoft Azure or Amazon Web Services to host the MicroStrategy Cloud Platform in a MicroStrategy Cloud Environment and will be operated out of a mutually determined data center location.

A. The Cloud Architecture Standard Offering is a fully managed cloud environment with separate metadata servers, load balancers, firewalls, data egress, and other services to ensure ease of use that consists of a base infrastructure package with the option to purchase incremental, additional nodes as needed.

I. The base infrastructure package in the Standard Offering includes the following components:

- one (1) production node with up to 512 GB RAM (24x7 availability)

- one (1) non-production development node with up to 64 GB RAM (minimum 12x5 availability)
- one (1) non-production utility node with up to 32 GB RAM (24x7 availability)

II. Additional nodes are available to purchase as an add-on to the base infrastructure package. Each additional node purchased is for use in either production or non-production environments and includes up to 512 GB RAM (24x7 availability). A customer may purchase additional nodes to create a clustered production instance (inclusive of a high-performance file system) or for use as separate, standalone environments for quality assurance or development.

B. The Cloud Architecture Small Offering is one fully managed cloud environment with a metadata server, load balancers, firewalls, data egress, and other services to ensure ease of use that consists of a base infrastructure package only. The base infrastructure package in the Small Offering includes the following components:

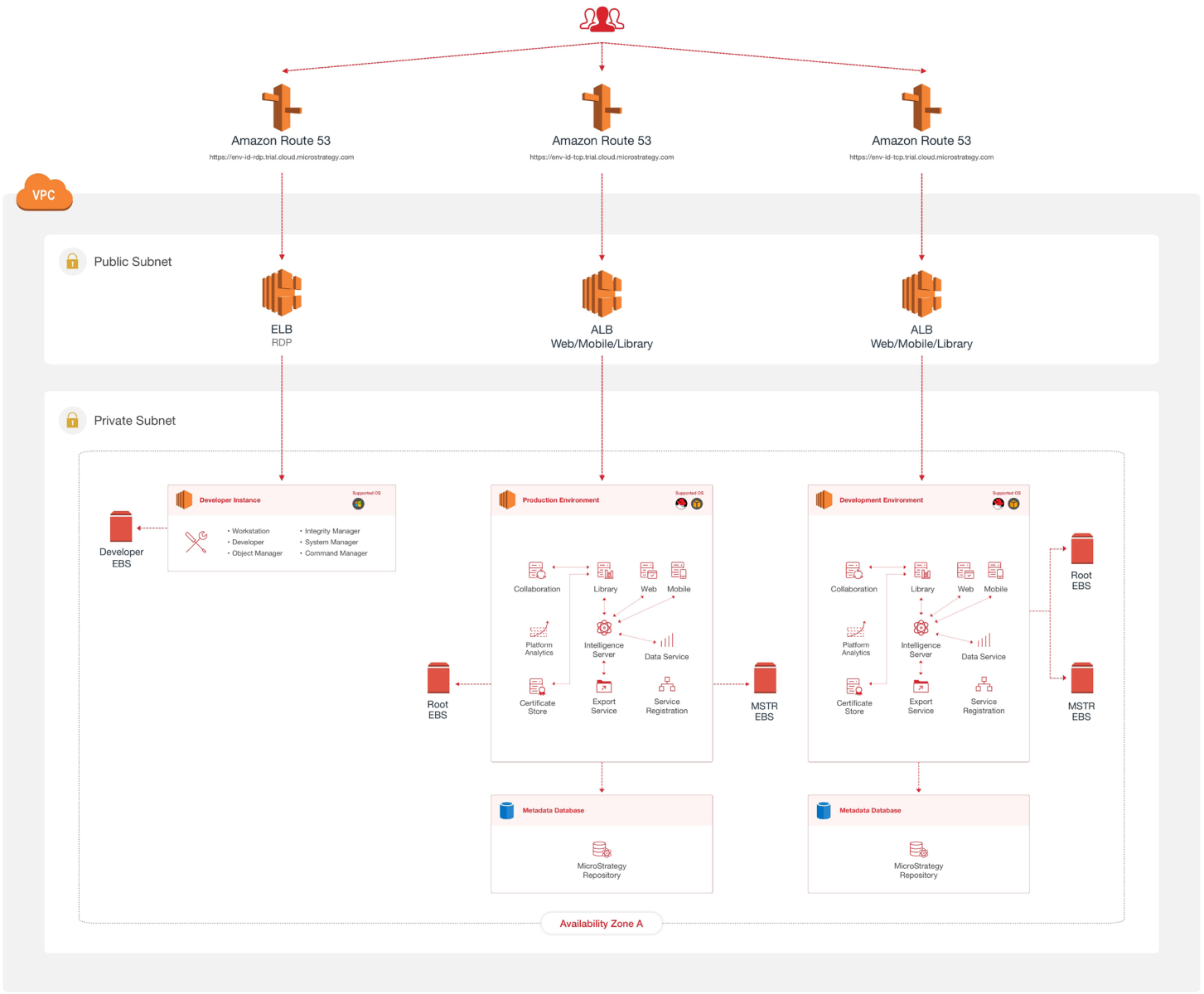
I. one (1) production node with up to 128 GB RAM (24x7 availability)

II. one (1) non-production utility node with up to 16 GB RAM (24x7 availability)

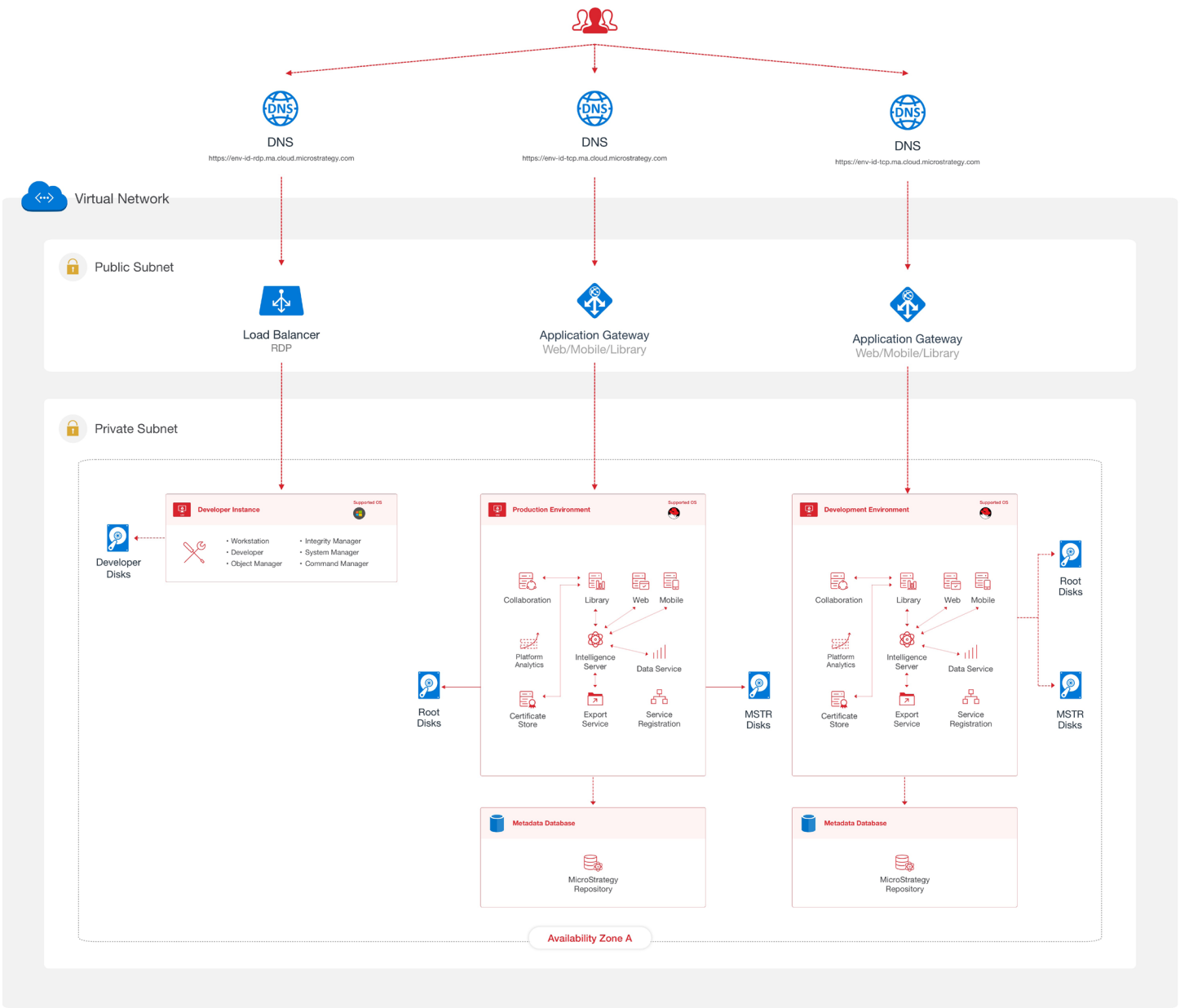
3.1.2 Enterprise MCE Architecture

Customers who purchase the Standard Cloud offering – base infrastructure package only – receive access to MicroStrategy's Enterprise MCE Architecture which consists of one Production node, one Development node, and one Utility node from either Microsoft Azure or Amazon Web Services as demonstrated in the diagrams below. Each node consists of a single server node for MicroStrategy Intelligence Server, Web, Library, Mobile, and Collaboration. There is a distributed database for the MicroStrategy metadata and statistics. The Enterprise MCE Architecture can scale to thousands of end users.

MICROSTRATEGY CLOUD ENVIRONMENT



MICROSTRATEGY CLOUD ENVIRONMENT



3.1.3 High-Availability MCE Architecture

MicroStrategy's High-Availability MCE Architecture consists of the Enterprise MCE Cloud Architecture plus additional nodes beyond the base package including, but not limited to, a clustered Production node, one Development node, and one Utility node for MicroStrategy Intelligence Server, Web, Library, Mobile, and Collaboration. There is a distributed and highly available database for the MicroStrategy metadata and statistics. The High-Availability MCE Architecture can scale to hundreds of thousands of end users.

3.2 Cloud Environment Support

As part of the Cloud Architecture offering, we will provide Cloud Environment Support to you by maintaining one or more production and/or non-production environments for the total number of nodes purchased as part of an MCE Service subscription, by providing the following:

3.2.1 Availability

The standard availability for production nodes will be 24x7 and for non-production nodes is a minimum of 12x5 in the customer's local time zone. These parameters may be changed based upon mutual agreement.

3.2.2 Root Cause Analysis (RCA)

For production outages, an RCA is generated by the Cloud Support team. For other P1 cases (outside of a production outage) that are logged, an RCA can be requested by the customer. Customers will receive the RCA report within 10 business days of the production outage or the requested RCA. The final analysis is conducted during business hours on the Eastern Time Zone to allow for management and peer approvals before formal communication of the stated issues.

Cloud Support will cover all support regarding diagnosis of the RCA. It will also cover product defects, security updates, operating system updates, and changes. As noted in Section 2, if an RCA determines an issue to be created by a customer-specific customization, MicroStrategy will provide options outside of Cloud Support, such as Professional Services engagements, to remedy the issue.

3.2.3 24/7 Cloud Helpdesk

For Production Node outages where system restoration is paramount, all alerts are sent to a global team for prompt resolution.

3.2.4 24/7 Monitoring and Alerting

Key system parameters are tagged and monitored. MicroStrategy has alerts on CPU utilization, RAM utilization, disk space, application-specific performance counters, VPN Tunnel, and ODBC warehouse sources monitoring. A full list can be provided upon request from the Cloud Support team. We provide alerts that will be monitored and if they exceed pre-defined thresholds, they are acted upon by the global helpdesk. System performance is logged over time to give the customer and Cloud Support team the ability to maintain a performant cloud platform.

3.2.5 Backups

Daily backups are performed for all customer systems, including system state, metadata, customizations, and performance characteristics. MicroStrategy retains five consecutive days of backups. Backups are dispersed across a region to ensure single points of failure (for example, a single cloud datacenter).

3.2.6 Platform Analytics

MicroStrategy Platform Analytics is set up for all MicroStrategy 2019 or later versions and maintained to allow for instant access to system performance metrics. MicroStrategy will monitor the MCE Service based data repository and/or cube memory requirement of the Platform Analytics database. In the event the space availability is less than 20%, MicroStrategy will purge older data from the MCE Service based Platform Analytics database in 30-day increments until the disk availability is below the 80% capacity threshold. The amount of data that the customer chooses to keep may have a corresponding cost to the customer. Contact your Account team for a cost estimate to modify the MCE Service, including increases to the data repository and/or cube memory requirements.

3.2.7 Maintenance

Maintenance windows are scheduled monthly to allow for third-party security updates to be applied to the MCE platform. During these scheduled interruptions, the MCE systems may be unable to transmit and receive data through the provided services. Customers should plan to create a process that includes the pause and restart of applications, rescheduling subscriptions, and including but not limited to, related data load routines. When it is necessary to execute emergency maintenance procedures, MicroStrategy will notify customer specific support liaisons via email as early as possible - identifying the nature of the emergency and the planned date and time of execution. Customers will normally receive a minimum of two weeks advance notification for planned maintenance windows. However, if emergency maintenance work is required, we will use commercially reasonable efforts to give 72-hour notice before applying a remedy.

3.2.8 Quarterly Service Reviews

The assigned designated Support Engineer for your MCE will conduct the Quarterly Service Reviews (QSR) with the business and technical contacts on a regular cadence.

3.2.9 Availability

The MCE Service is architected to withstand the failure of an individual service or process to achieve availability. This is achieved by utilizing underlying application features and building on best practices such as clustering along with the advantage AWS and Azure allow through the splitting of a particular Region into multiple Availability Zones ("AZ") to withstand AZ wide failure.

3.2.10 Disaster Recovery

Standard Disaster recovery routines allow for backups and system state data with storage spanning AZ's. The use of multiple AZ's creates a physical separation of data between the machines storing production and back-up environments. Paid Professional Services are available for customers in which specific automation and routines are configured so all customer data is collected and copied to an alternate region.

3.2.11 Updates and Upgrades

For each Product license, we will deliver to you, at no charge and at your request, an Update as part of the Technical Support Services subscription. Major version updates are completed in a free parallel environment for up to 30 days to allow for customer testing. Updates will not include any new, separately marketed products.

3.2.12 Security

Various security tools are employed to perform penetration testing and remediation, system event logging, and vulnerability management. The MCE Service maintains a high security posture in accordance with the following security standards:

3.2.12.a Service Organization Controls (SSAE-18)

SSAE-18 is the service organization auditing standard maintained by the AICPA. It evaluates Service Organization Controls over the security, availability, and processing integrity of a system and the confidentiality and privacy of the information processed by the system. Our MCE Service maintains a SOC2 Type 2 report.

3.2.12.b Health Insurance Portability and Accountability Act (HIPAA)

Controls designed to protect health information.

3.2.12.c Payment Card Industry Data Security Standards (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information. MCE maintains a SAQ-D for Service Providers.

3.2.12.d International Organization for Standardization (ISO 27001-2)

International Organization for Standardization (ISO 27001-2) is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance.

3.2.13 Cloud Shared Services Components

As part of the MCE Service's platform architecture and in support of the Cloud Environment, we incorporate other solutions to assist in the management, deployment, and security of the infrastructure, and to complete operational tasks. These include management and detection response solutions, cloud security posture management solutions, application/infrastructure monitoring, alerting and on call management solutions, and workflow and continuous integration tools.

4. Service Availability

MCE offers a service level agreement of 99.9% for clustered production environments and 99% service level for signal node non-clustered production environments. Availability is calculated per calendar month as follows:

$$\left[\left(\frac{\text{TotalMinutes*\# of Production Instances}-\text{Unavailability}}{\text{TotalMinutes*\# of Production Instances}}\right)*100\right]$$

4.1 Service Definition

"Total Minutes": the total number of minutes in a calendar month.

"Production Instance": an MCE Intelligence Architecture that users are running in production, in support of an operational business process.

"Unavailability": for each Production Node, the total number of minutes in a calendar month during which (1) the Production Node(s) has no external connectivity; (2) the Production Node(s) has external connectivity but is unable to process requests (i.e., has attached volumes that perform zero

read-write IO, with pending IO in the queue); or (3) all connection requests made by any component of the Production Node(s) fail for at least five consecutive minutes. "Unavailability" does not include minutes when the MCE is unavailable due to issues related to applications built on the MicroStrategy software platform, including project, report, and document issues; migration problems related to user design; ETL application problems; improper database logical design and code issues; downtime related to scheduled maintenance; downtime experienced as a result of user activity; general internet unavailability; and other factors out of MicroStrategy's reasonable control.

"Total Unavailability": the aggregate unavailability across all Production Nodes.

For any partial calendar month during which customers subscribe to the MCE, availability will be calculated based on the entire calendar month, not just the portion for which they subscribed.

4.2 Service Remedies

If the availability standard of 99.9% (for clustered Production Nodes) and 99% (for non-clustered Production Node) is not met in any given calendar month, customers may be eligible for a Service Credit, according to the definitions below. Each Service Credit will be calculated as a percentage of the total fees paid by customers for the MCE Service, managed by MicroStrategy within the calendar month that a Service Credit has been accrued. This is the exclusive remedy available to customers in the event MicroStrategy fails to comply with the service level requirements set forth in the availability designed in Section 4.

4.3 Service Credits

Clustered Production Node:

- Availability less than 99.9% but equal to or greater than 99.84%: 1% Service Credit
- Availability less than 99.84% but equal to or greater than 99.74%: 3% Service Credit
- Availability less than 99.74% but equal to or greater than 95.03%: 5% Service Credit
- Availability less than 95.03%: 7% Service Credit

Non-Clustered Production Node:

- Availability less than 99% but equal to or greater than 98.84%: 1% Service Credit

- Availability less than 98.84% but equal to or greater than 98.74%: 3% Service Credit
- Availability less than 98.74% but equal to or greater than 94.03%: 5% Service Credit
- Availability less than 94.03%: 7% Service Credit

4.4 Service CreditsProcedure

To receive a Service Credit, customers must submit a MicroStrategy case on or before the 15th day of the calendar month following the calendar month in which the Service Credit allegedly accrues that includes the following information: (a)the words "SLA Credit Request" in the "Case Summary/ Error Message" field; (b) a detailed description of the event(s) that resulted in unavailability; (c) the dates, times, and duration of the unavailability; (d) the affected system or component ID(s) provided to customers by MicroStrategy during onboarding and Intelligence Architecture delivery activities; and (e) a detailed description of the actions taken by users to resolve the unavailability. Once MicroStrategy receives this claim, MicroStrategy will evaluate the information provided and any other information relevant to determining the cause of the Unavailability (including, for example, information regarding the availability performance of the Intelligence Architecture, third-party software or services, dependencies on customer-hosted or subscribed software or services, operating system, and software components of the MCE). Thereafter, MicroStrategy will determine in good faith whether a Service Credit has accrued and will notify customers of its decision. If MicroStrategy determines that a Service Credit has accrued, then at its discretion, it will either (1) apply the Service Credit to the next MCE Service invoice sent or (2) extend the MCE Service Term for a period commensurate to the Service Credit amount. Customers may not offset any fees owed to MicroStrategy with Service Credits.

5. Terms Applicable to Processing Personal Data

This Section 5 will apply only to the extent there is no other executed agreement in place regarding the same subject between MicroStrategy and the customer ("Customer"), including any order(s) and/or a master agreement between the customer and MicroStrategy (collectively, the "Governing Agreement"), and shall be considered a Data Protection Agreement (DPA).

5.1 Definitions

"Applicable Data Protection Law" shall include and mean all applicable laws and regulations where these apply to MicroStrategy, its group and third parties who may be utilized in respect of the performance of the MCE Service relating to the processing of personal data and privacy, including, without limitation, the General Data Protection Regulation (EU) 2016/679 and the California Consumer Protection Act

(Cal. Civ. Code §§ 1798.100 et. seq.) (CCPA). The terms "Controller," "Business," "Processor," "Data Subject," "Service Provider," "Supervisory Authority," "process," "processing," and "personal data" shall be construed in accordance with their meanings as defined under Applicable Data Protection Law.

"Customer Group" shall include and mean Customer and any affiliate, subsidiary, subsidiary undertaking and holding company of Customer (acting as a Controller) accessing or using the MCE Service on Customer's behalf or through Customer's systems or who is permitted to use the MCE Service pursuant to the Governing Agreement between Customer and MicroStrategy, but who has not signed its own Order Form with MicroStrategy.

"International Transfer" shall include and mean a transfer from a country within the European Economic Area (EEA) (including the UK following its exit from the European Union (EU) and Switzerland (a country not in the EEA or the EU) of personal data which is undergoing processing or which is intended to be processed after transfer to a country or territory to which such transfer is prohibited or subject to any requirement to take additional steps to adequately protect personal data.

"MCE Service" means the MicroStrategy Cloud Environment service, a platform-as-a service offering that we manage on the Customer's behalf in an Amazon Web Services or Microsoft Azure environment that includes access to, collectively: (a) the "Cloud Platform" version of our Products (an optimized version of the MicroStrategy software platform built specifically for deployment in an Amazon Web Services or Microsoft Azure environment) licensed by the Customer; and (b) the Additional PaaS Components (as defined in the MicroStrategy Cloud Environment Service Terms section below) Customer has purchased for use with such Products.

"Standard Contractual Clauses" means those clauses comprised within the European Commission Decision (C (2010)593) of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, as may be updated, supplemented, or replaced from time to time under Applicable Data Protection Law and which are incorporated by reference herein forming part of this DPA and a copy of which can be accessed at https://www.microstrategy.com/licensing, subject to the provisions of Section 5.5 below.

"Sub-Processor" shall include and mean any third party appointed by MicroStrategy to process personal data.

5.2 Data Processing

MicroStrategy will process, as a Processor, the personal data that is uploaded or transferred to the MCE Service as instructed by Customer or provided by Customer as Controller (collectively, "Customer Data") in accordance with Customer's documented instructions. Customer authorizes MicroStrategy, on its own behalf and on behalf of the other members of the Customer Group, to process Customer Data during the term of this DPA as a Processor for the purpose set out in the table set forth below.

Customer Data in relation to MCE Service

Subject matter of processing	Storage of data, including without limitation personal data, provided by Customer for its business purpose
Duration of processing	MCE Service Term
Nature of processing	Storage, back-up, recovery, and processing of Customer Data in connection with the MCE Service
Purpose of processing	Provision of the MCE Service
Type of personal data	The Customer Data uploaded for processing through the MCE Service
Categories of data subject	Employees of the Customer and Customer's customers, prospects, business partners and vendors, and employees or agents of the Customer, including those who have been authorized to use the MCE Service

The parties agree that this DPA is Customer's complete and final documented instruction to MicroStrategy in relation to Customer Data. Additional instructions outside the scope of this DPA (if any) require prior written agreement between MicroStrategy and Customer, including agreement on any additional fees payable by Customer to MicroStrategy for carrying out such instructions. Customer shall ensure that its instructions comply with all rules and regulations applicable in relation to Customer Data, and that the processing of Customer Data in accordance with Customer's instructions will not cause MicroStrategy to be in breach of Applicable Data Protection Law. MicroStrategy will not process Customer Data outside the scope of this DPA.

MicroStrategy will:

1. Process Customer Data only on documented instructions from Customer (unless MicroStrategy or the relevant Sub-Processor (see Section 5.4 below) is required to process Customer Data to comply with applicable laws, in which case MicroStrategy will notify Customer of such legal requirement prior to such processing unless such applicable laws prohibit notice to them on public interest grounds);
2. Immediately inform the Customer in writing if, in its reasonable opinion, any instruction received from them infringes any Applicable Data Protection Law;
3. Ensure that any individual authorized to process Customer Data complies with Section 5.2a) above;
4. At the option of Customer, delete or return to Customer all Customer Data after the end of the

provision of the MCE Service, relating to processing, and delete any remaining copies. MicroStrategy will be entitled to retain any Customer Data which it has to keep in order to comply with any applicable law or which it is required to retain for insurance, accounting, taxation, or record keeping purposes. Section 5.3 will continue to apply to retained Customer Data.

MicroStrategy will not "sell" Customer Data as that term is defined in the CCPA, nor will it retain, use, or disclose Customer Data for any purpose other than for the specific purpose of performing the services specified in the Governing Agreement, or as otherwise permitted by the CCPA or its implementing regulations. MicroStrategy certifies that it understands the restrictions and obligations under the CCPA, including the restrictions and obligations in the previous sentence, and will comply with CCPA. In addition, MicroStrategy will comply with any applicable amendments to the CCPA or its regulations.

5.3 Confidentiality

MicroStrategy will not disclose Customer Data to any government or any other third party, except as necessary to comply with the law or a valid and binding order of a government or law enforcement agency (such as a subpoena or court order). If a government or law enforcement agency sends MicroStrategy a demand for Customer Data, MicroStrategy will attempt to redirect the government or law enforcement agency to request that data directly from the Customer. As part of this effort, MicroStrategy may provide Customer's basic contact information to the government or law enforcement agency. If compelled to disclose Customer Data to a government or law enforcement agency, then MicroStrategy will give the Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy, unless MicroStrategy is legally prohibited from doing so. MicroStrategy restricts its personnel from processing Customer Data without authorization by MicroStrategy, and imposes appropriate contractual obligations upon its personnel, including, as appropriate, relevant obligations regarding confidentiality, data protection and data security. If the Standard Contractual Clauses apply, nothing in this section 5.3 varies or modifies the Standard Contractual Clauses, including without limitation the obligations within clause 5(a).

5.4 Sub-Processing

Customer authorizes MicroStrategy to engage its own affiliated companies for the purposes of providing the MCE Service. In addition, Customer agrees that MicroStrategy may use Sub-Processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf. The MicroStrategy websites at https:// community.microstrategy.com/s/article/GDPR-Cloud-Sub-Processors list its Sub-Processors that are currently engaged to carry out specific processing activities on Customers' behalf. Before MicroStrategy engages any new Sub-Processor to carry out specific processing activities,

MicroStrategy will update the applicable website. If Customer objects to a new Sub-Processor, MicroStrategy will not engage such Sub-Processor to carry out specific processing activities on Customer's behalf without Customer's written consent. Customer hereby consents to MicroStrategy's use of Sub-Processors as described in this Section 5.4. Except as set forth in this Section 5.4, or as otherwise authorized, MicroStrategy will not permit any Sub-Processor to carry out specific processing activities on Customer's behalf. If MicroStrategy appoints a Sub-Processor, MicroStrategy will(i) restrict the Sub-Processor's access to Customer Data only to what is necessary to provide the MCE Service to Customer and will prohibit the Sub-Processor from accessing Customer Data for any other purpose; (ii) will enter into a written agreement with the Sub- Processor; (iii) to the extent the Sub-Processor is performing the same data processing services that are being provided by MicroStrategy under this DPA, impose on the Sub-Processor substantially similar terms to those imposed on MicroStrategy in this DPA; and iv) comply with the Standard Contractual Clauses, which separately contain obligations in respect of the terms to be imposed in respect of an onward transfer of Personal Data to a Sub-Processor. MicroStrategy will remain responsible to Customer for performance of the Sub-Processor's obligations.

5.5 Transfers of Personal Data by Region

With respect to Customer Data containing personal data that is uploaded or transferred to the MCE Service, Customer may specify the geographic region(s) where that Customer Data will be processed within MicroStrategy's Sub-Processor's network (e.g., the EU-Dublin region). A Sub-Processor will not transfer that Customer Data from Customer's selected region except as necessary to maintain or provide the MCE Service, or as necessary to comply with a law or binding order of a law enforcement agency.

To provide the MCE Service, Customer acknowledges and confirms MicroStrategy may make International Transfers of Customer Data including onward transfers to its affiliated companies and/or Sub-Processors. Where those International Transfers occur, the Standard Contractual Clauses shall apply. The Customer agrees that by signing this DPA (or continuing to use the MCE Services) it will be deemed to have entered into and executed the Standard Contractual Clauses with MicroStrategy (as data importer), and the Standard Contractual Clauses shall be deemed incorporated into this DPA. The Customer agrees to be bound by its obligations under the Standard Contractual Clauses. The Customer acknowledges that there may be instances where the contracting MicroStrategy entity or entities executing the Governing Agreement and DPA may differ from the MicroStrategy entity (data importer) named in the Standard Contractual Clauses.

This may occur for example where the MicroStrategy entity signing the Governing Agreement and DPA is based within the EEA or Switzerland (and is thus not an offshore processor, importing the personal

data for the purposes of the Standard Contractual Clauses), and Customer Data is being shared onwards with another MicroStrategy entity who is based outside of the EEA.

In the event that the form of the Standard Contractual Clauses is changed or replaced by the relevant authorities under Applicable Data Protection Law from time to time, MicroStrategy shall have the right to review any new form of Standard Contractual Clauses and, if acceptable, will update the form of Standard Contractual Clauses on MicroStrategy's website within sixty (60) days of the effective date of any such new form at https://www.microstrategy.com/us/terms. The Standard Contractual Clauses disclosed on MicroStrategy's aforementioned website, as amended from time to time, are deemed to be incorporated into the Governing Agreement between Customer and MicroStrategy. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if MicroStrategy has adopted an alternative recognized compliance standard for the lawful transfer of personal data outside the EEA (including the UK following its exit from the EU) or Switzerland, to protect the Customer Data.

With respect to other International Transfers, (outside of those covered by the Standard Contractual Clauses) MicroStrategy will only make a transfer of Customer Data if:

1. Adequate safeguards are in place for that transfer of Customer Data in accordance with Applicable Data Protection Law, in which case Customer will execute any documents (including without limitation Standard Contractual Clauses) relating to that International Transfer, which MicroStrategy or the relevant Sub-Processor reasonably requires it to execute from time to time; or
2. MicroStrategy or the relevant Sub-Processor is required to make such an International Transfer to comply with applicable laws, in which case MicroStrategy will notify Customer of such legal requirement prior to International Transfer unless applicable laws prohibit notice to Customer on public interest grounds; or
3. Otherwise lawfully permitted to do so by Applicable Data Protection Law.

5.6 Security of Data Processing

MicroStrategy has implemented and will maintain appropriate technical and organizational measures, including, as appropriate:

1. Security of the MicroStrategy network;
2. Physical security of the facilities;
3. Measures to control access rights for MicroStrategy employees and contractors in relation to the MicroStrategy network; and

4. Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by MicroStrategy.

Customer may elect to implement appropriate technical and organizational measures in relation to Customer Data, directly from MicroStrategy's Sub-Processor. Such appropriate technical and organizational measures include:

1. Pseudonymization and encryption to ensure an appropriate level of security;
2. Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services provided by Customer to third parties;
3. Measures to allow Customer to backup and archive appropriately to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident;and
4. Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

5.7 Security Breach Notification

MicroStrategy will, to the extent permitted by law, notify Customer without undue delay after becoming aware of any actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Data by MicroStrategy or MicroStrategy's Sub-Processor(s) (a "Security Incident"). If such a Security Incident is caused by a violation of the requirements of this DPA by MicroStrategy, MicroStrategy will make reasonable efforts to identify and remediate the cause of such breach, including steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Customer agrees that an unsuccessful Security Incident will not be subject to this Section 5.7. An unsuccessful Security Incident is one that results in no actual unauthorized access to Customer Data or to any of MicroStrategy's or MicroStrategy's Sub-Processor's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-in attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents; and MicroStrategy's obligation to report or respond to a Security Incident under this Section 5.7 is not, and will not, be construed as an acknowledgment by MicroStrategy of any fault or liability of MicroStrategy with respect to the Security Incident.

Notification(s) of Security Incidents, if any, will be delivered to Customer by any means MicroStrategy selects, including via email. It is Customer's responsibility to ensure that they provide MicroStrategy with accurate contact information and secure transmission at all times.

The information made available by MicroStrategy is intended to assist Customer in complying with their obligations under Applicable Data Protection Law in respect of data protection impact assessments and prior consultation.

5.8 Audit

MicroStrategy will allow for and contribute to audits (including those under the Standard Contractual Clauses where these apply), which shall include inspections, conducted by Customer or other auditors mandated by Customer, provided that they give MicroStrategy at least 30 days' reasonable prior written notice of such audit and that each audit is carried out at their cost, during business hours, at MicroStrategy nominated facilities, and so as to cause minimum disruption to MicroStrategy's business and without Customer or its auditor having any access to any data belonging to people other than Customer's. Any materials disclosed during such audits and the results of and/or outputs from such audits will be kept confidential by Customer. Such audits shall be performed not more than once every 12 months, and Customer shall not copy or remove any materials from the premises where the audit is performed.

Customer acknowledges and agrees (having regard to Section 5.4(iii)) that in respect of MicroStrategy's auditing rights of its Sub-Processor providing infrastructure services for the MCE Service, such Sub-Processor will use external auditors to verify the adequacy of security measures including the security of the physical data centers from which the Sub-Processor provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or other such alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third-party security professionals at the Sub-Processor's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be the Sub-Processor's confidential information or otherwise be made available subject to a mutually agreed upon non- disclosure agreement covering the Report ("NDA"). MicroStrategy will not be able to disclose such Report to Customer without permission from the Sub-Processor. At Customer's written request during the exercise of its audit rights under this section, MicroStrategy will request the permission of the Sub-Processor to provide Customer with a copy of the Report so that Customer can reasonably verify the Sub-Processor's compliance with its security obligations. The Report will constitute confidential information and the Sub-Processor may require Customer to enter into an NDA with them before releasing the same.

If the Standard Contractual Clauses apply under Section 5.5a), then Customer agrees to exercise its audit and inspection right by instructing MicroStrategy to conduct an audit as described in this section, and the parties agree that notwithstanding the foregoing, nothing varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or data subject's rights under those Standard Contractual Clauses.

5.9 Independent Determination

Customer is responsible for reviewing the information made available by MicroStrategy and its Sub- Processor relating to data security and making an independent determination as to whether the MCE Service meets Customer's requirements and legal obligations as well as Customer's obligations under this DPA.

5.10 Data Subject Rights

Taking into account the nature of the MCE Service, Customer can utilize certain controls, including security features and functionalities, to retrieve, correct, delete, or restrict Customer Data. MicroStrategy will provide reasonable assistance to Customer (at Customer's cost) in:

1. Complying with its obligations under the Applicable Data Protection Law relating to the security of processing Customer Data;
2. Responding to requests for exercising Data Subjects' rights under the Applicable Data Protection Law, including without limitation by appropriate technical and organizational measures, insofar as this is possible;
3. Documenting any Security Incidents and reporting any Security Incidents to any supervisory authority and/or Data Subjects;
4. Conducting privacy impact assessments of any processing operations and consulting with supervisory authorities, Data Subjects, and their representatives accordingly; and
5. Making available to Customer information necessary to demonstrate compliance with the obligations set out in this DPA.

5.11 Return or Deletion of Customer Data

Due to the nature of the MCE Service, MicroStrategy's Sub-Processor provides Customer with controls that Customer may use to retrieve or delete Customer Data. Up to the termination of the master agreement between Customer and MicroStrategy ("Governing Agreement"), Customer will continue to have the ability to retrieve or delete Customer Data in accordance with this section. For 30 days following that date, Customer may retrieve or delete any remaining Customer Data from the MCE Service, subject to the terms and conditions set out in the Governing Agreement, unless (i) it is prohibited by law or the order of a governmental or regulatory body, (ii) it could subject MicroStrategy or its Sub-Processors to liability, or (iii) Customer has not paid all amounts due under the Governing Agreement. No later than the end of this 90-day period, Customer will close all MicroStrategy accounts. MicroStrategy will delete Customer Data when requested by Customer through the MCE Service controls provided for this purpose.

COLL-2149 0721