MICROSTRATEGY CLOUD ENVIRONMENT SERVICE GUIDE

GUIDELINES FOR INTERACTING WITH MICROSTRATEGY CLOUD SUPPORT

Update published May 2020

MicroStrategy
Intelligence Everywhere

Table of Contents

1. Overview

The MicroStrategy Cloud Environment ("MCE" or "MCE Service") is a Platform-as-a-Service ("PaaS") delivery model designed to allow businesses to consume the MicroStrategy Analytics and Mobility platform in a single tenant architecture.

MCE offers a distributed compute architecture using various components provided by the cloud infrastructure vendors of either Microsoft Azure or Amazon Web Services. At the core of the solution are MicroStrategy Analytics and Mobility, components that provide users with a secure, scalable, and resilient business intelligence enterprise application platform.

It 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 predefined configuration. Once provisioned, users can develop, tailor, and manage the application components to meet their respective needs.

Based on this operating model, customers control the Analytics and Mobility application stack, while MicroStrategy maintains the supporting cloud-based infrastructure. "MCE Service" means the MicroStrategy Cloud Environment service, a platform-as-a service offering that we manage on your 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 you; and (b) the Cloud Environment, Cloud Support, and Cloud Infrastructure you have purchased for use with such Products.

2. Cloud Platform

Standard Support for the "Cloud Platform" version of our Products is provided with your license for such Products pursuant to your contract with MicroStrategy and our Technical Support Policies and Procedures.

3. Cloud Application Support

Under "Cloud Application Support" (or "Cloud Support"), our Cloud Support engineers will provide ongoing support to you to help you maximize the performance and agility—and minimize the cost—of your MicroStrategy Cloud Platform deployment, including environment configuration, environment and application optimization, enterprise data warehouse integration, authentication (SSO/LDAP) and application integration. If a support issue is logged and it has been determined through the diagnosis

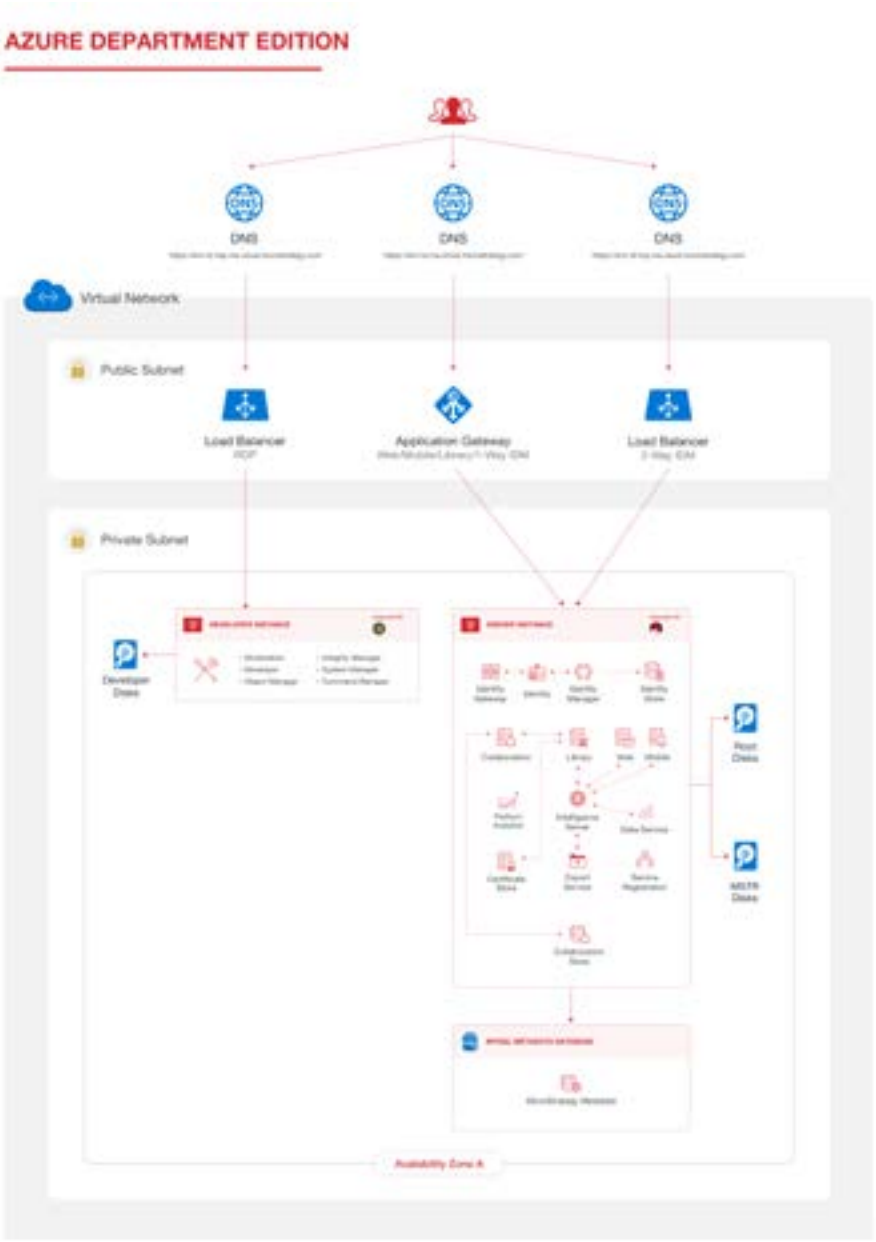
that the Root Cause Analysis of the stated issue was due to a customer-specific customization of the MicroStrategy application, then the customer will be given the option to apply the Cloud Application Support hours in the successful resolution of the stated issue. It should be noted that we will not charge for the diagnosis of the issue, but we will highlight the options for the customer and the customer can then decide whether they wish to apply Cloud Application Support hours to fix the issue. If it is a production outage issue, MicroStrategy reserves the right to fix the issue on behalf of the customer without a pre-authorization of the utilization of the stated hours.

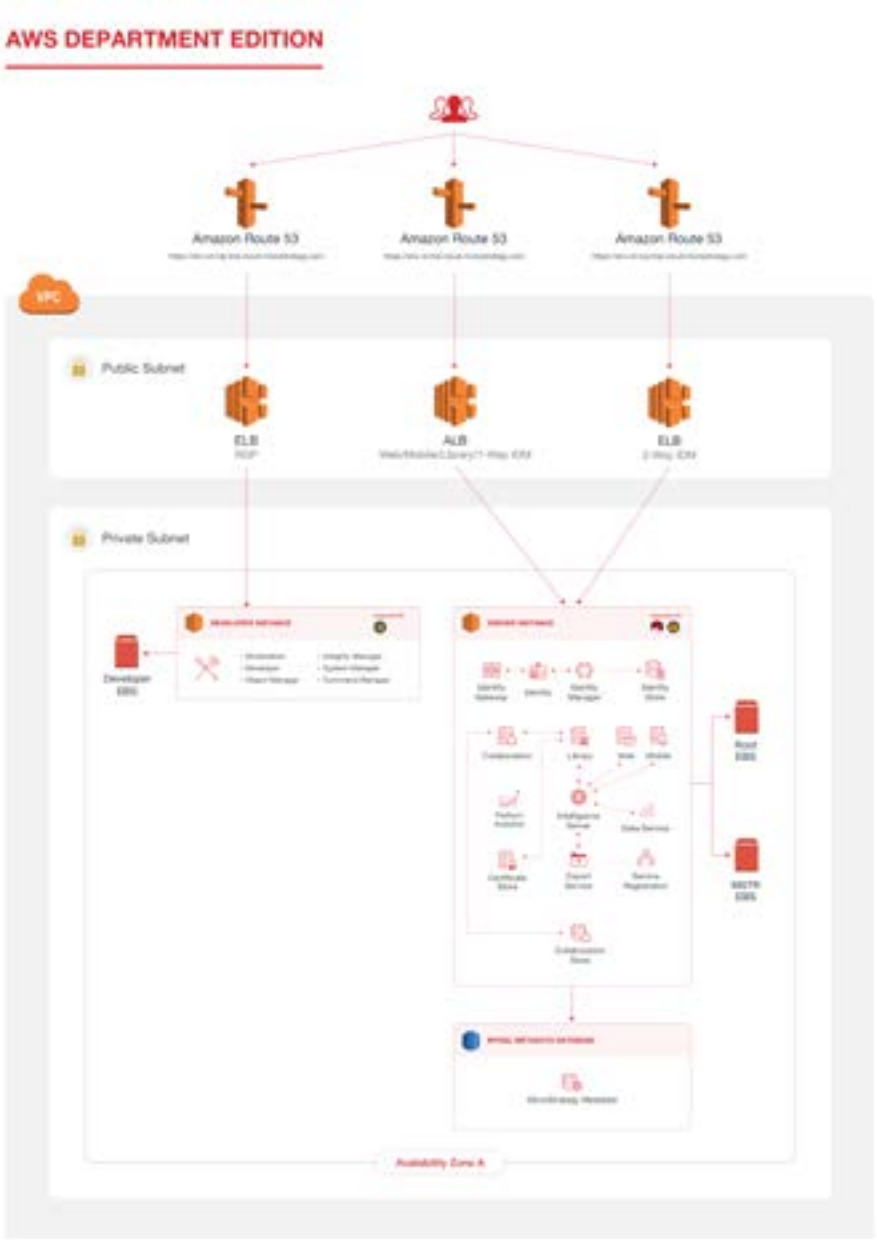
4. Cloud Infrastructure

MCE offers 2 types of single tenant platform architectures and they have been built based on application performance and security best practices.

4.1 Department Architecture

Department Architecture consists of a single server node for MicroStrategy Intelligence Server, Web, Mobile, Collaboration, and Identity. There is a distributed database for the MicroStrategy metadata and statistics. Department architectures can scale to tens of thousands of end users.

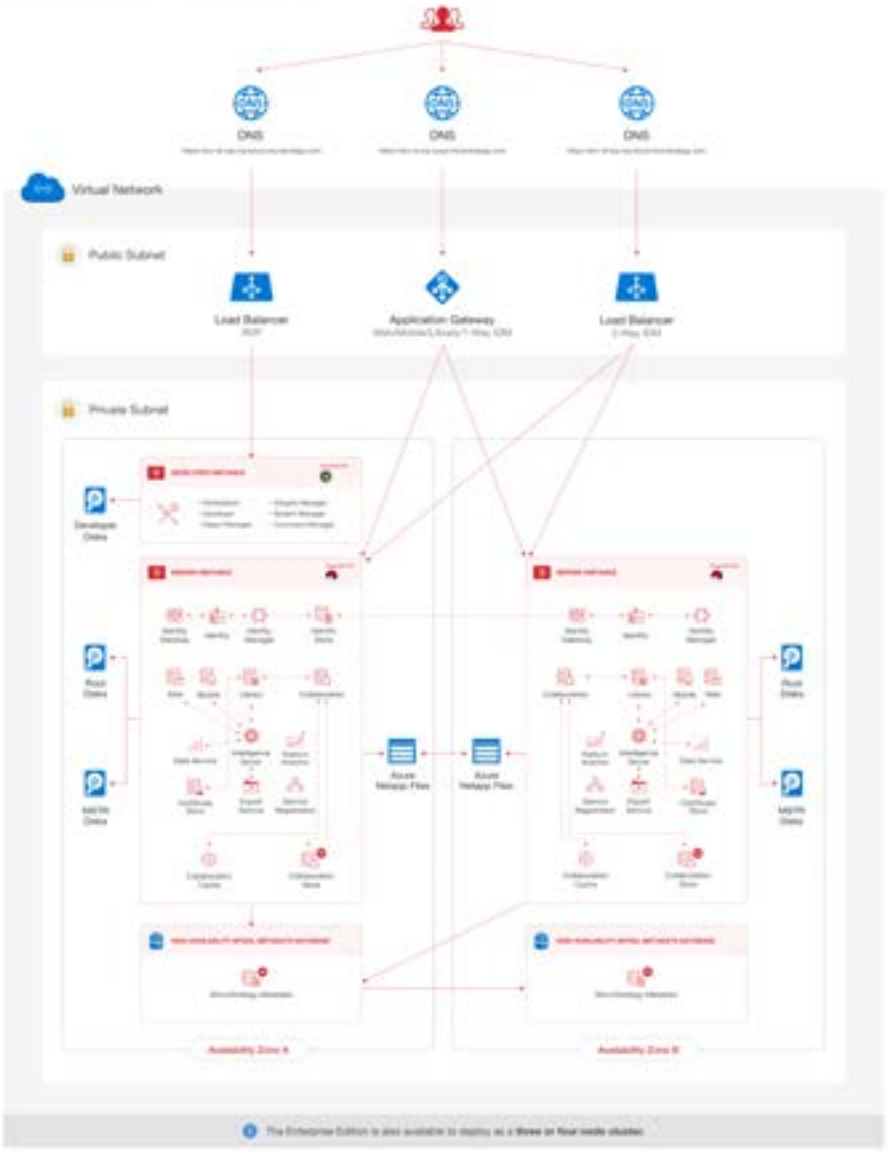


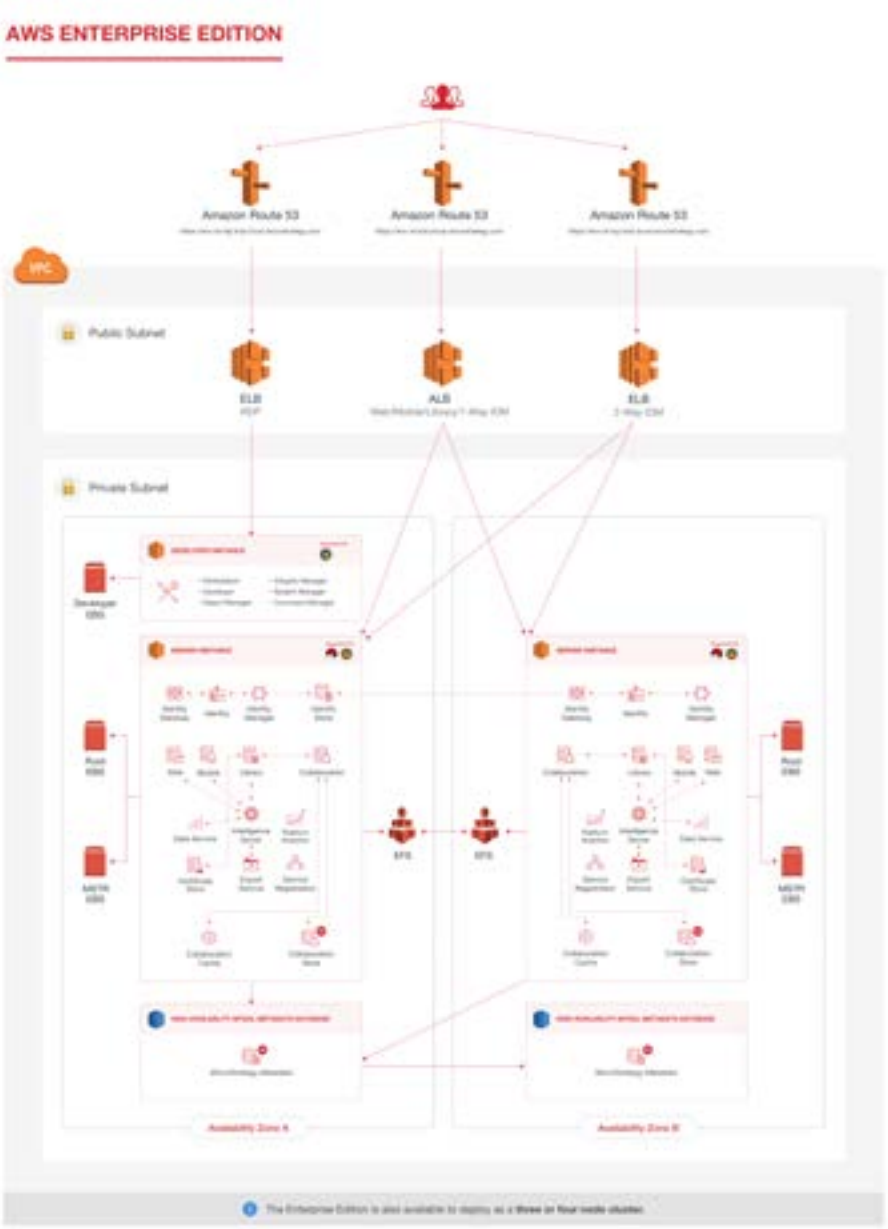


4.2 Enterprise Architecture

Enterprise Architecture consists of a two to eight node highly available cluster for MicroStrategy Intelligence Server, Web, Mobile, Collaboration, and Identity. There is a distributed and highly available database for the MicroStrategy Metadata and Statistics. Enterprise architectures can scale to hundreds of thousands of end users.

AZURE ENTERPRISE EDITION




AWS ENTERPRISE EDITION
Amazon Route 53
Amazon Route 53
Amazon Route 53
VPC
Public Subnet
ELB
ALB
ELB
Private Subnet
EFS
EFS
Availability Zone A
Availability Zone B

5. Cloud Environment

We will maintain one or more production and/or non-production environments for the total number of nodes purchased in an order, in each case by providing the following:

5.1 Availability

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

5.2 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 Environment will cover all support with regard to diagnosis of the RCA. It will also cover product defects, security updates, operating system updates, and changes. If an RCA was determined to be specific to a customer-specific customization, any customer-desired resolution of the issue would be considered Cloud Application Support (Section 3).

5.3 24/7 Cloud Helpdesk

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

5.4 24/7 Monitoring and Alerting

Key system parameters are tagged and monitored. MicroStrategy has alerts on CPU utilization, RAM utilization, disk space, and application-specific performance counters. A full list can be provided upon request from the Cloud Operations team. We provide alerts that will be monitored and if they break 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.

5.5 Backups

Daily backups are performed for all customer systems, including system state, metadata, customizations, and performance characteristics. MicroStrategy retains five consecutive days of backups.

5.6 Platform Analytics/Enterprise Manager

MicroStrategy Platform Analytics is set up for all MicroStrategy 2019 or later versions and maintained to allow for instant access to system performance metrics. Enterprise Manager is the precursor product for Platform Analytics. MicroStrategy will monitor the data repository and/or cube memory requirement of the Enterprise Manager and/or Platform Analytics database with the standard being Platform Analytics. In the event the space availability is less than 20%, MicroStrategy will purge older data from the Enterprise Manager and/or 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 could have a corresponding cost to the customer. If a customer opts to increase the data repository and/or cube memory requirements, they will either necessitate a change order or will be billed in arrears for the overage per the terms of the contract. An estimate of costs to make any change can always be requested from our Cloud Support team.

5.7 Maintenance

Maintenance windows are scheduled on a monthly basis 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. Customer systems should include a process to pause and restart the applications and related data load routines planned around maintenance activities. When it is necessary to execute emergency maintenance procedures, MicroStrategy will notify customer 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 maintenance windows. However, if emergency maintenance work is required, we will use commercially reasonable efforts to give 72 hour notice before applying a remedy.

5.8 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.

5.9 Updates and Upgrades

For each Product license, we will deliver to you, at your request, an Update at no charge as part of a Technical Support Services subscription. Updates will not include new products that we market separately. Upgrades or a major version change are completed in a parallel environment and this additional node would be at additional cost to the customer and covered within the customer's ordering agreement with MicroStrategy.

5.10 Security

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

5.10.1 Service Organization Controls (SOC)

SOC over the security, availability, and processing integrity of a system and the confidentiality and privacy of the information processed by the system.

5.10.2 Health Insurance Portability and Accountability Act (HIPAA)

Controls designed to protect health information.

5.10.3 Privacy Shield

MicroStrategy has certified compliance with the EU–U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of European Union personal information transferred to the United States.

5.10.4 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.

5.10.5 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.

5.10.6 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union.

5.11 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.

6. 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:

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

6.1 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.

6.2 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.

6.3 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

6.4 Service Credits Procedure

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.

7. Terms Applicable to Processing Personal Data

This Section 7 will apply only to the extent there is no other executed agreement in place regarding the same subject between MicroStrategy and the customer ("Customer" or "customer") and shall be considered a Data Protection Agreement (DPA).

7.1 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 Services relating to the processing of personal data and privacy, including, without limitation, the General Data Protection Regulation (EU) 2016/679.

The terms "Data Controller," "Data Processor," "Data Subject," "Supervisory Authority," "process," "processing," and "personal data" shall be construed in accordance with their meanings as defined under Applicable Data Protection Law.

"Customer's Group" shall include and mean the Customer and any subsidiary, subsidiary undertaking, and holding company of Customer.

"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) to a country outside the EEA (as it is made up from time to time) of personal data which is undergoing processing or which is intended to be processed after transfer.

"MCE Service" means the MicroStrategy Cloud Environment service, a platform-as-a service offering that we manage on your 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 you; and (b) the Additional PaaS Components (as defined in the MicroStrategy Cloud Environment Service Terms section below) you have purchased for use with such Products.

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

7.2 Data Processing

MicroStrategy will process, as a Data Processor, the personal data that is uploaded or transferred to the MCE Service as instructed by Customer or provided by Customer as Data 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 Customer's Group, to process Customer Data during the term of this DPA as a Data 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:

a. Process Customer Data only on documented instructions from Customer (unless MicroStrategy or the relevant Sub-Processor (see Section 7.4 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);
b. Immediately inform the Customer in writing if, in its reasonable opinion, any instruction received from them infringes any Applicable Data Protection Law;
c. Ensure that any individual authorized to process Customer Data complies with Section 7.2a) above;
d. 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 7.3 will continue to apply to retained Customer Data.
e. In the event that you provide us with access to Personal Information as such is defined in Title 1.81.5 California Consumer Privacy Act of 2018 ("CCPA"), the following additional terms of this DPA will apply. The terms "Business," "Personal Information," and "Service Provider" shall be construed in accordance with their meanings as defined in the CCPA. As a Service Provider, we will use Personal Information that is transferred to us by you as a Business in accordance with your documented instructions. You authorize us to use Personal Information during the term of this Agreement for the purpose set out in Section 7.2. MicroStrategy will not sell Personal Information, retain, use, or disclose Personal Information 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 hereby certifies that it understands and will comply with the aforementioned restrictions.

7.3 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 law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends MicroStrategy a demand for Customer Data, MicroStrategy will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, MicroStrategy may provide basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, MicroStrategy will give Customer reasonable notice of the demand to allow 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, and

imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection, and data security.

7.4 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 7.4. Except as set forth in this Section 7.4, 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 and; (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. MicroStrategy will remain responsible to Customer for performance of the Sub-Processor's obligations.

7.5 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. The adequate safeguard MicroStrategy has in place for transfers from the EU to the US is the EU–U.S. Privacy Shield Framework. MicroStrategy Incorporated and MicroStrategy Services Corporation have certified compliance with the EU–U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of EU personal information transferred to the United States. Where MicroStrategy makes an

International Transfer, it shall do so via the use of the EU-U.S. Privacy Shield Framework, which will apply to all transfers between MicroStrategy EU entities and MicroStrategy U.S. entities and third parties used by MicroStrategy as part of the provision of the MCE Services. Any transfers from the United States to any third-party countries will be considered an "onward transfer" under the EU-U.S. Privacy Shield Framework. Where MicroStrategy makes an onward transfer, it will ensure a contract is in place with that party which satisfies the onward transfer accountability requirements of the EU-U.S. Privacy Shield Framework.

In respect of other International Transfers, 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 such International Transfer unless such applicable laws prohibit notice to Customer on public interest grounds; or
3. Otherwise lawfully permitted to do so by Applicable Data Protection Law.

7.6 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 backu p 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.

7.7 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 7.7. 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 7.7 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.

7.8 Audit

MicroStrategy will allow for and contribute to audits, including 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 7.4(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 7.5a), 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 clauses.

7.9 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.

7.10 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.

7.11 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 90 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 0520