
# Infrastructure Reliability Essentials

## Service Specification

# Service Specification

| | |
|---|---|
| Service Name: | Infrastructure Reliability Essentials |
| Service Level Hours: | Refer to section 1.1 |
| Unit of Charge: | Fixed fee based on tier. |
| Prerequisites: | Deployment Checklist<br>Up to 100 Resources (VM's and Endpoints) Service Limit |
| Supported Cloud Platforms: | AWS, Azure and GCP |
| Product Codes: | CO-MONITORING-AS-A-SERVICE<br>CO-REMEDIATION |
| Version Number: | 1.0 |
| Status: | LIVE |
| Published Date: | June 2020 |

# The Small Print



# Definitions

The definitions for all capitalised terms used throughout this Service Specification are set out in the Cloud Operations Service Definitions document which forms a part of this Service Specification and the Cloudreach Order Form to which this Service Specification relates.

# Table of Contents

# 1. Service Overview

Infrastructure Reliability Essentials is a managed service for Amazon Web Services (AWS), Microsoft Azure Public Cloud and Google Cloud Platform (GCP). The service will manage the availability and accessibility of the Customer's environment(s) in these public clouds. It will provide operational support services of Customer's environments and support Resources at a Platform Level that are controllable by the Cloud Service Provider's (CSP) console or APIs.

Infrastructure Reliability Essentials is suited to up to 100 Resources (Service Limit). Customer and Cloudreach will agree to the applicable revision to the Services Scope and Charges if Customer requires support for >100 Resources s (which may include replacing Reliability Essentials Services with the Infrastructure Reliability Service).

A summary of the key features of Infrastructure Reliability Essentials are listed below:

**Onboarding** - Cloudreach will assign a Service Transition team member to manage the project of onboarding Customer environment into Infrastructure Reliability Essentials. During the initial phase of onboarding, Cloudreach will assess the time needed to onboard the environment based on the complexity and intricacies involved with onboarding. Please note that Cloudreach will only perform onboarding of Customers Environments during Business Hours.

**Monitoring as a Service (Tier 1)** - The service will monitor the availability and accessibility of the Customer's environments.. Cloudreach will monitor IAAS and PAAS services at the Platform Level by ingesting metrics which are available by default in the corresponding CSP's monitoring service (i.e. AWS Cloudwatch, Azure Monitor, GCP Stackdriver). Cloudreach shall define alerting for these metrics based on the best practices for the corresponding CSP service and Customer requirements. The performance metrics will also be collected to detect trends with defined thresholds for alerting and performance analysis.

In addition to this, Cloudreach will provide automated notification for any public websites (HTTP endpoints) so that Cloudreach can respond to and inform you if a website becomes unavailable. Cloudreach will carry out a HTTP check on the specified public endpoints gathered during onboarding and detect bad response codes (e.g 404).

**Remediation (Tier 2)** - Alongside the services delivered in Tier 1, Cloudreach will provide hands on intervention and resolution of incidents captured through **Monitoring-aaS**. Cloudreach will assist Customers with resolving issues with the service or resource at Platform level, with the focus of providing availability and accessibility of the resource and service within Customer environments.

| Service | Tier 1 | Tier 2 | Infrastructure Reliability* |
|---|---|---|---|
| Platform Availability Management | ✔ (partial) | ✔ | ✔ |
| Incident notification | ✔ | ✔ | ✔ |
| Endpoint Monitoring (Public HTTP) | ✔ | ✔ | ✔ |
| Platform Level Incident Resolution | | ✔ | ✔ |

| | | | |
|---|---|---|---|
| VM Level monitoring | | | ✔ |
| Patching | | | ✔ |
| Backups | | | ✔ |
| Threat and Vulnerability Management | | | ✔ |
| FinOps | | | ✔ |

*The latest version of the full Infrastructure Reliability service is available here

## 1.1 Service Levels

| Services | Applicable Tier(s) | Service Level Hours |
|---|---|---|
| Onboarding | Tier 1<br>Tier 2 | Business Hours (9x5)<br>(*PDT time zone if the Customer is based in NA and GMT time zone if the Customer is based in EEA*) |
| Platform Availability Management | Tier 1<br>Tier 2 | 24x7 |
| Service Management Support (P1 and P2 Incidents) | Tier 2 | |
| Service Management Support (P3 and P4 Incidents) | Tier 2 | 24x5 |

# 2. Operating Systems Supported

Cloudreach supports the following Operating System versions:

| Operating System Version | Comment |
|---|---|
| Windows Server 2012 and onward | On January 14, 2020, Microsoft will be officially ending its support for Windows Server 2008 R2 editions. Cloudreach shall stop support of this version on January 14, 2020.<br><br>Windows 2016 Nano is not supported at this time. |
| Ubuntu | Only the LTS editions are supported at this time.<br><br>Cloudreach will support any LTS (Long Term Support) versions which are currently within vendor support.<br><br>For a list of supported LTS versions and their end-of-life date please visit https://wiki.ubuntu.com/Releases<br><br>Please note that within an LTS version of Ubuntu, Canonical releases multiple “patch versions” of the LTS distribution. Different patch versions may contain different kernel |

| | |
|---|---|
| | revisions, with varying support (and security patching availability), which may end before the end of life of the LTS distribution. Cloudreach recommends that Customers always opt in for the patch version that uses a kernel version which is supported throughout the lifecycle of the LTS distribution, as otherwise Customer may miss out on some security patches until the kernel is upgraded. Kernel upgrades are not part of the monthly patching schedule performed by Cloudreach.<br><br>For further information please see https://wiki.ubuntu.com/Kernel/Support |
| Debian | Cloudreach will support any LTS versions which are currently within vendor support.<br><br>For a list of supported LTS versions and their end-of-life date please visit https://wiki.debian.org/LTS/ |
| Amazon Linux | Cloudreach will support any LTS versions which are currently within vendor support.<br><br>For a list of supported versions and their end-of-life date please visit https://aws.amazon.com/amazon-linux-ami/faqs/ |
| CentOS | Cloudreach will support any major version which are currently within vendor support.<br><br>For a list of the currently supported versions and their end-of-life date please visit https://wiki.centos.org/About/Product |
| RedHat Enterprise | Cloudreach will support any RHEL version which is currently within vendor's Full Support.<br><br>For a list of the currently supported versions and their end-of-life date please visit https://access.redhat.com/support/policy/updates/errata |

## 2.1 LTS version support

Cloudreach may require to update & test the set of tooling to ensure that it works as expected with new versions of Operating Systems. For that reason, at times, Cloudreach may not be able to support new LTS versions of Operating Systems as soon as they are released.

In the case of OS vendors making changes that require Cloudreach to adjust the tooling, Cloudreach reserves the right to take up to 6 months to make all necessary changes to support new LTS releases.

With regards to Operating Systems end of support, Cloudreach will provide support until such date or extension thereof, from the OS vendors.

# 3. Onboarding

## 3.1 Onboarding Terms

Once the service is ready for onboarding, Cloudreach will assign a Service Transition team member to manage the project of onboarding Customer environment into Infrastructure Reliability Essentials.

During the initial phase of onboarding, Cloudreach will assess the time needed to onboard the environment based on the complexity and intricacies involved with onboarding.

Please note that Cloudreach will only perform onboarding of Customers Environments during Business Hours.

## 3.2 Deployment Checklist

In order to deliver the Infrastructure Reliability Essentials service, Cloudreach needs to have access to the Customer's Environment(s) in the form of network, API and system level access. This enables Cloudreach's operational teams to provide the various management services within the Customer's Environment where configuration, maintenance, troubleshooting and service management are required. For example, in the case of incident resolution and service management within Tier 2 Services, Cloudreach may need to deploy its management tools in the event the customer does not have bastion or VPN access configured for VM's .

The level of access required by Cloudreach is determined by the relevant service tier requested by the customer. For example, with Tier 1 access is limited to a read only role for the purposes of our monitoring tool (SignalFX) capturing platform metrics and a read only role for Cloudreach engineers to troubleshoot incidents.

The Deployment Checklist also details the policies that the Customer needs to comply with for the duration of the contract. This also details the access information required for the Customer's chosen public cloud platform such as network address(es), accounts/subscriptions and logins, authentication and permissions. This is a prerequisite for Cloudreach to deliver Infrastructure Reliability Essentials to the Customer. The necessary documentation will be made available before and at the time of onboarding the environments to be taken under Cloudreach management.

Here's an example:

If AWS ASG or Azure Scale Sets exist within Customer's Cloud Platform, then the Customer shall provide Cloudreach with relevant access to implement the required integration and deployment tools as made available per the AWS ASG or Azure Resource Groups services. (i.e. User data for an AMI that is used with an ASG launch configuration). Customer shall be responsible for limiting Cloudreach's access to only the specific data, information or other Customer material which is required for the purposes of carrying out the implementation.

# 4. Platform Availability Management

Cloudreach will monitor the health of cloud resources for each mutually agreed AWS, Azure and/or GCP Account and can raise an alert based on the event conditions denoted in our preconfigured thresholds determined in accordance with 4.2.2.1 . Cloudreach

defined AWS and Azure health check metrics are based on a subset of available AWS CloudWatch, Azure Monitor Diagnostics and GCP Stackdriver metrics.

In the event an alert is raised, Cloudreach shall provide Incident Notification (under Tier 1) and Incident Resolution (if the Customer has purchased Tier 2) in accordance with the Incident Management Process.

## 4.1 Monitoring Methodology

### 4.1.1 Data Residency

All monitoring data collected by Cloudreach will be stored on servers hosted in the EU region.

### 4.1.2 Data Collection

For CSP native monitoring services (i.e. AWS CloudWatch), data will be collected from an external 3rd party tooling provider via API requests to the appropriate CSP service. As part of the onboarding process, a service account role and relevant permissions will need to be created in Customer environments to allow this collection.

Frequency of collection is configurable, with default being every 5 minutes. Over time, older data might be aggregated for performance reasons.

### 4.1.3 Data Retention

Monitoring data will be retained for 13 months.

## 4.2 Scope of “Supported” and “Monitored”

This section provides an explanation of what Cloudreach means in relation to supporting and monitoring CSP services.

### 4.2.1 Scope of “Supported”

#### 4.2.1.1 Best Practice Guidance

Cloudreach holds expert level knowledge of this service and leverages this to provide guidance and advice to Customers. Engineers will be able to advise Customer on changes to the service that are inline with the best practice guidelines provided by the vendor and discuss details and intricacies of the service with Customers.

#### 4.2.1.2 Configuration Management

Where **Remediation (Tier2)** is purchased, Cloudreach will perform changes to the service at Platform Level, using either CSP’s provided GUI or API to execute the change. The focus of any changes to be carried out will be to resolve incidents related to resource/service.

##### 4.2.1.2.1 Out of Scope: Configuration Management

Please note that within the Infrastructure Reliability Essentials service, Cloudreach will only perform Platform Level support and will not provide Resource Level administration. An example of this is an RDS service, where Cloudreach will ensure that the database is running correctly (i.e. monitoring CloudWatch metrics).

However, within Infrastructure Reliability Essentials, Cloudreach will not provide any service that interacts with the data inside the database (i.e. altering tables, modifying data, creating SQL users).

#### 4.2.1.3 Service Troubleshooting

Where **Remediation (Tier2)** is purchased, Cloudreach will assist Customers with troubleshooting issues with the service or Resource at Platform Level, with the focus of providing availability and accessibility of the resource and service within Customer environments.

An example of an issue, where Cloudreach can assist, could be a problem with an application connecting to the database. In such an instance, Cloudreach would be able to review the network connectivity & health of the database to establish the cause of the connectivity issue where related to the platform infrastructure. With this in mind, within Infrastructure Reliability Essentials service, Cloudreach would not look to investigate any issues with the data at the Resource Level once inside the database (i.e. query performing slowly).

#### 4.2.1.4 Out of Scope: Support Boundaries

- For services that are not “supported” in the below tables, Cloudreach will endeavour to work with the Customer and CSP Support team, leveraging CSP’s in-house skills and documentation to deliver guidance for this service.
- For avoidance of doubt, Infrastructure Reliability Essentials will support existing resources, rather than provision net new resources unless necessary in support of existing infrastructure.

### 4.2.2 Scope of “Monitored”

#### 4.2.2.1 Service Monitoring

Cloudreach shall integrate with Cloud Service Provider native monitoring tooling to provide monitoring service to Customers. In most cases, Cloudreach will perform API calls (either directly or via 3rd party tooling) to collect various metrics from CSP Monitoring service (i.e. AWS CloudWatch) and will ingest those metrics into a monitoring platform, where further analysis will be performed to identify problems and patterns within Customer environments.

Cloudreach is utilising the following API services to collect Metrics Data:

- AWS Cloudwatch
- Azure Monitor
- GCP StackDriver

During onboarding, Cloudreach will apply a baseline of monitoring metrics to effectively monitor the Cloud environment. Cloudreach can configure custom platform alerting on a case by case basis as agreed during onboarding. Custom monitoring is limited up to 10 metrics.Cloudreach will configure the monitoring alerts to the needs of the Customer environment(s), focusing on monitoring key components which indicate that the platform is available and accessible. Cloudreach will only perform monitoring of the services which are critical for the health & availability of the Environment.

Once onboarding is completed, Cloudreach monitoring software will monitor the Customer environment(s). Cloudreach will receive notifications and investigate events in accordance with the defined monitoring alerting. If appropriate, Cloudreach will raise a

support case and contact the Customer primary contact(s) to inform them of the details of the support case.

Cloudreach reserves the right to disable or modify a specific monitoring or alerting configuration on notice to the Customer, if deemed necessary by Cloudreach in order to preserve an accurate and effective alerting signal.

## 4.3 Supported & Monitored CSP Services

The list of Supported and Monitored CPS services shall be amended to reflect changes that the CSPs make to their services. Cloudreach will reflect these changes accordingly.

### 4.3.1 AWS-native - Supported & Monitored

In the table below is a list of AWS services which publish metrics to CloudWatch, with indication of support and monitoring capabilities within Infrastructure Reliability Essentials.

| Service | Namespace | Supported | Monitored |
|---|---|---|---|
| Amazon API Gateway | AWS/ApiGateway | | ✔ |
| AppStream 2.0 | AWS/AppStream | | ✔ |
| AWS Billing and Cost Management | AWS/Billing | | ✔ |
| Amazon CloudFront | AWS/CloudFront | ✔ | ✔ |
| Amazon CloudSearch | AWS/CloudSearch | | ✔ |
| Amazon CloudWatch Events | AWS/Events | ✔ | ✔ |
| Amazon CloudWatch Logs | AWS/Logs | ✔ | ✔ |
| AWS CodeBuild | AWS/CodeBuild | | ✔ |
| Amazon Cognito | AWS/Cognito | | ✔ |
| Amazon Connect | AWS/Connect | | ✔ |
| AWS Database Migration Service | AWS/DMS | | ✔ |
| AWS Direct Connect | AWS/DX | ✔ | ✔ |
| Amazon DynamoDB | AWS/DynamoDB | ✔ | ✔ |
| Amazon EC2 | AWS/EC2 | ✔ | ✔ |
| Amazon EC2 Spot Fleet | AWS/EC2Spot | ✔ | ✔ |
| Amazon EC2 Auto Scaling | AWS/AutoScaling | ✔ | ✔ |
| AWS Elastic Beanstalk | AWS/ElasticBeanstalk | ✔ | ✔ |
| Amazon Elastic Block Store | AWS/EBS | ✔ | ✔ |
| Amazon Elastic Container Service | AWS/ECS | ✔ | ✔ |
| Amazon Elastic File System | AWS/EFS | ✔ | ✔ |

| | | | |
|---|---|---|---|
| Amazon Elastic Inference | AWS/ElasticInference | | ✔ |
| Elastic Load Balancing | AWS/ApplicationELB | ✔ | ✔ |
| Elastic Load Balancing | AWS/ELB | ✔ | ✔ |
| Elastic Load Balancing | AWS/NetworkELB | ✔ | ✔ |
| Amazon Elastic Transcoder | AWS/ElasticTranscoder | | ✔ |
| Amazon ElastiCache for Memcached | AWS/ElastiCache | ✔ | ✔ |
| Amazon ElastiCache for Redis | AWS/ElastiCache | ✔ | ✔ |
| Amazon Elasticsearch Service | AWS/ES | | ✔ |
| Amazon EMR | AWS/ElasticMapReduce | | ✔ |
| AWS Elemental MediaConnect | AWS/MediaConnect | | ✔ |
| AWS Elemental MediaConvert | AWS/MediaConvert | | ✔ |
| AWS Elemental MediaPackage | AWS/MediaPackage | | ✔ |
| AWS Elemental MediaTailor | AWS/MediaTailor | | ✔ |
| Amazon FSx for Lustre | AWS/FSx | | ✔ |
| Amazon GameLift | AWS/GameLift | | ✔ |
| AWS Glue | AWS/Glue | | ✔ |
| AWS CloudHSM | AWS/CloudHSM | | ✔ |
| Amazon Inspector | AWS/Inspector | | ✔ |
| AWS IoT | AWS/IoT | | ✔ |
| AWS IoT Analytics | AWS/IoTAnalytics | | ✔ |
| AWS IoT Things Graph | AWS/ThingsGraph | | ✔ |
| AWS Key Management Service | AWS/KMS | ✔ | ✔ |
| Amazon Kinesis Data Analytics | AWS/KinesisAnalytics | | ✔ |
| Amazon Kinesis Data Firehose | AWS/Firehose | | ✔ |
| Amazon Kinesis Data Streams | AWS/Kinesis | | ✔ |
| Amazon Kinesis Video Streams | AWS/KinesisVideo | | ✔ |
| AWS Lambda | AWS/Lambda | ✔ | ✔ |
| Amazon Lex | AWS/Lex | | ✔ |
| Amazon Machine Learning | AWS/ML | | ✔ |
| Amazon Managed Streaming for Kafka | AWS/Kafka | | ✔ |
| Amazon MQ | AWS/AmazonMQ | | ✔ |

| | | | |
|---|---|---|---|
| Amazon Neptune | AWS/Neptune | | ✔ |
| AWS OpsWorks | AWS/OpsWorks | ✔ | ✔ |
| Amazon Polly | AWS/Polly | | ✔ |
| Amazon Redshift | AWS/Redshift | | ✔ |
| Amazon Relational Database Service | AWS/RDS | ✔ | ✔ |
| Amazon Route 53 | AWS/Route53 | ✔ | ✔ |
| Amazon SageMaker | AWS/SageMaker | | ✔ |
| AWS Shield Advanced | AWS/DDoSProtection | ✔ | |
| Amazon Simple Email Service | AWS/SES | ✔ | ✔ |
| Amazon Simple Notification Service | AWS/SNS | ✔ | ✔ |
| Amazon Simple Queue Service | AWS/SQS | ✔ | ✔ |
| Amazon Simple Storage Service | AWS/S3 | ✔ | ✔ |
| Amazon Simple Workflow Service | AWS/SWF | ✔ | ✔ |
| AWS Step Functions | AWS/States | ✔ | ✔ |
| AWS Storage Gateway | AWS/StorageGateway | ✔ | ✔ |
| Amazon Textract | AWS/Textract | | ✔ |
| Amazon Translate | AWS/Translate | | ✔ |
| AWS Trusted Advisor | AWS/TrustedAdvisor | ✔ | ✔ |
| Amazon VPC | AWS/NATGateway | ✔ | ✔ |
| Amazon VPC | AWS/TransitGateway | ✔ | ✔ |
| Amazon VPC | AWS/VPN | ✔ | ✔ |
| AWS WAF | AWS/WAF | ✔ | ✔ |
| Amazon WorkSpaces | AWS/WorkSpaces | ✔ | ✔ |
| Glacier | N/A* | ✔ | N/A* |
| VPC | N/A* | ✔ | N/A* |
| CloudFormation | N/A* | ✔ | N/A* |
| CloudTrail | N/A* | ✔ | N/A* |
| Config | N/A* | ✔ | N/A* |
| Systems Manager | N/A* | ✔ | N/A* |
| Trusted Advisor | N/A* | ✔ | N/A* |
| Personal Health Dashboard | N/A* | ✔ | N/A* |

| | | | |
|---|---|---|---|
| IAM | N/A* | ✔ | N/A* |
| Organizations | N/A* | ✔ | N/A* |
| Key Management Service | N/A* | ✔ | N/A* |
| Certificate Manager | N/A* | ✔ | N/A* |

* Services marked with N/A under monitoring are already managed-natively by the CSP and monitoring of these services is either not possible or not necessary.

### 4.3.2 Azure-native - Supported & Monitored Services

In the table below is a list of Azure services that publish metrics to Azure Monitor service, with indication of support and monitoring capabilities within Infrastructure Reliability Essentials. Where there are no metrics to collect and therefore no monitoring performed, Cloudreach provides best practice, configuration and troubleshooting services.

| Namespace | Supported | Monitored |
|---|---|---|
| Microsoft.AnalysisServices/servers | | ✔ |
| Microsoft.ApiManagement/service | ✔ | ✔ |
| Microsoft.Automation/automationAccounts | ✔ | ✔ |
| Microsoft.Batch/batchAccounts | | ✔ |
| Microsoft.Cache/redis | ✔ | ✔ |
| Microsoft.CognitiveServices/accounts | | ✔ |
| Microsoft.Compute/virtualMachines | ✔ | ✔ |
| Microsoft.Compute/virtualMachineScaleSets | ✔ | ✔ |
| Microsoft.Compute/virtualMachineScaleSets/virtualMachines | ✔ | ✔ |
| Microsoft.ContainerInstance/containerGroups | ✔ | ✔ |
| Microsoft.ContainerService/managedClusters | ✔ | ✔ |
| Microsoft.CustomerInsights/hubs | | ✔ |
| Microsoft.DataFactory/datafactories | | ✔ |
| Microsoft.DataFactory/factories | | ✔ |
| Microsoft.DataLakeAnalytics/accounts | | ✔ |
| Microsoft.DataLakeStore/accounts | | ✔ |
| Microsoft.DBforMariaDB/servers | ✔ | ✔ |
| Microsoft.DBforMySQL/servers | ✔ | ✔ |
| Microsoft.DBforPostgreSQL/servers | ✔ | ✔ |
| Microsoft.Devices/IotHubs | | ✔ |
| Microsoft.Devices/provisioningServices | | ✔ |
| Microsoft.DocumentDB/databaseAccounts | ✔ | ✔ |

| | | |
|---|---|---|
| Microsoft.EventGrid/topics | ✔ | ✔ |
| Microsoft.EventGrid/eventSubscriptions | ✔ | ✔ |
| Microsoft.EventGrid/extensionTopics | ✔ | ✔ |
| Microsoft.EventHub/namespaces | ✔ | ✔ |
| Microsoft.EventHub/clusters | ✔ | ✔ |
| Microsoft.HDInsight/clusters | | ✔ |
| Microsoft.Insights/AutoscaleSettings | | ✔ |
| Microsoft.Insights/Components | | ✔ |
| Microsoft.KeyVault/vaults | ✔ | ✔ |
| Microsoft.Kusto/Clusters | | ✔ |
| Microsoft.LocationBasedServices/accounts | | ✔ |
| Microsoft.Logic/workflows | ✔ | ✔ |
| Microsoft.NetApp/netAppAccounts/capacityPools/Volumes | | ✔ |
| Microsoft.NetApp/netAppAccounts/capacityPools | | ✔ |
| Microsoft.Network/networkInterfaces | ✔ | ✔ |
| Microsoft.Network/loadBalancers | ✔ | ✔ |
| Microsoft.Network/dnszones | ✔ | ✔ |
| Microsoft.Network/publicIPAddresses | ✔ | ✔ |
| Microsoft.Network/applicationGateways | ✔ | ✔ |
| Microsoft.Network/virtualNetworkGateways | ✔ | ✔ |
| Microsoft.Network/expressRouteCircuits | ✔ | ✔ |
| Microsoft.Network/expressRouteCircuits/peerings | ✔ | ✔ |
| Microsoft.Network/connections | ✔ | ✔ |
| Microsoft.Network/trafficManagerProfiles | ✔ | ✔ |
| Microsoft.Network/networkWatchers/connectionMonitors | ✔ | ✔ |
| Microsoft.Network/frontdoors | ✔ | ✔ |
| Microsoft.NotificationHubs/Namespaces/NotificationHubs | ✔ | ✔ |
| Microsoft.OperationalInsights/workspaces | ✔ | ✔ |
| Microsoft.PowerBIDedicated/capacities | | ✔ |
| Microsoft.Relay/namespaces | | ✔ |
| Microsoft.Search/searchServices | | ✔ |
| Microsoft.ServiceBus/namespaces | ✔ | ✔ |
| Microsoft.SignalRService/SignalR | | ✔ |

| | | |
|---|---|---|
| Microsoft.Sql/servers/databases | ✔ | ✔ |
| Microsoft.Sql/servers/elasticPools | ✔ | ✔ |
| Microsoft.Sql/managedInstances | ✔ | ✔ |
| Microsoft.Storage/storageAccounts | ✔ | ✔ |
| Microsoft.Storage/storageAccounts/blobServices | ✔ | ✔ |
| Microsoft.Storage/storageAccounts/fileServices | ✔ | ✔ |
| Microsoft.Storage/storageAccounts/queueServices | ✔ | ✔ |
| Microsoft.Storage/storageAccounts/tableServices | ✔ | ✔ |
| Microsoft.StreamAnalytics/streamingjobs | | ✔ |
| Microsoft.TimeSeriesInsights/environments | | ✔ |
| Microsoft.TimeSeriesInsights/environments/eventsources | | ✔ |
| Microsoft.Web/serverfarms | | ✔ |
| Microsoft.Web/sites (excluding functions) | | ✔ |
| Microsoft.Web/sites (functions) | | ✔ |
| Microsoft.Web/sites/slots | | ✔ |
| Microsoft.Web/hostingEnvironments/multiRolePools | | ✔ |
| Microsoft.Web/hostingEnvironments/workerPools | | ✔ |

Within Azure CSP, Cloudreach is not able to support or monitor “Classic” Azure services from previous generation of Azure Platform.

For resources that offer different service tiers, Cloudreach requires that Customers opt in for a tier that supports Azure Monitor metrics. For example: Load Balancer, “Basic” tier does not report health metrics to Azure Monitor

### 4.3.3 GCP-native - Supported & Monitored

In the table below is a list of GCP services with indication of support and monitoring capabilities within Infrastructure Reliability Essentials. Where there are no metrics to collect and therefore no monitoring performed, Cloudreach provides best practice, configuration and troubleshooting services.

| ServiceNamespace | Supported | Monitored |
|---|---|---|
| Compute Products | | |
| Compute Engine: Virtual Machines, Disks, Network | ✔ | ✔ |
| App Engine: Managed App Platform | ✔ | ✔ |
| Kubernetes Engine: Managed Kubernetes/Containers (GCP platform level) | ✔ | ✔ |
| Cloud Functions: Event-driven serverless functions | ✔ | ✔ |
| Storage Products | | |

| | | |
|---|---|---|
| Cloud Storage: Object Storage and Serving | ✔ | ✔ |
| Nearline: Archival Occasional Access Storage | ✔ | |
| Coldline: Archival Rare Access Storage | ✔ | |
| Persistent Disk: VM-attached Disks | ✔ | |
| Cloud Filestore: Managed NFS Server | ✔ | ✔ |
| Database Products | | |
| Cloud Bigtable: Petabyte-scale, low-latency nonrelational | | ✔ |
| Cloud Datastore: Horizontally Scalable Document DB | ✔ | ✔ |
| Cloud Firestore: Strongly-consistent Serverless Document DB | ✔ | ✔ |
| Cloud Memorystore: Managed Redis | ✔ | ✔ |
| Cloud Spanner: Horizontally Scalable Relational DB | | ✔ |
| Cloud SQL: Managed MySQL and PostgreSQL | ✔ | ✔ |
| Data and Analytics Products | | |
| Cloud Dataflow: Stream/batch data processing | | ✔ |
| Cloud Pub/Sub: Global Real-time Messaging | ✔ | ✔ |
| Google BigQuery: Data Warehouse/Analytics | | ✔ |
| Networking Products | | |
| Carrier Peering: Peer through a carrier | ✔ | |
| Direct Peering: Peer with GCP | ✔ | |
| Dedicated Interconnect: Dedicated private network connection | ✔ | ✔ |
| Partner Interconnect: Connect on-premises network to VPC | ✔ | |
| Cloud CDN: Content Delivery Network | ✔ | |
| Cloud DNS: Programmable DNS Serving | ✔ | |
| Cloud Load Balancing: Multi-region Load Distribution | ✔ | ✔ |
| Cloud NAT: Network Address Translation Service | ✔ | |
| Cloud Router | ✔ | ✔ |
| IPsec VPN: Virtual private network connection | ✔ | ✔ |
| Internet of Things Products | | |
| Cloud IoT Core: Device Management and ingest data | | ✔ |
| Identity and Security Products | | |
| Access Transparency: Audit Cloud Provider Access | ✔ | |
| Cloud IAM: Resource Access Control | ✔ | |
| Cloud Key Management Service: Hosted Key Management Service | ✔ | |

| | | |
|---|---|---|
| Management Tools Products | | |
| Cloud APIs: APIs for Cloud Services | | ✔ |
| Stackdriver Logging: Centralized Logging | ✔ | ✔ |
| Stackdriver Monitoring: Infrastructure and Application Monitoring | ✔ | ✔ |
| Mobile Products (Firebase) | | |
| Firebase database | | ✔ |

### 4.3.4 Out of Scope: Virtual Machine Hosted Applications

Customer hosted applications such as databases, network and web servers will only be monitored for health and performance of underlying infrastructure that they are running on.

# 5. Endpoint Monitoring

Cloudreach will provide automated alerting for any public websites (HTTP Endpoints) as mutually agreed during onboarding.

The Endpoint Monitoring service will carry out a HTTP check on the agreed endpoint and detect a bad response code (e.g 404). Following receipt of a bad response code, Cloudreach will, dependent on the service agreed, provide Incident Notification (if Tier 2 is purchased andIncident Resolution (if Tier 2 is purchased) in accordance with the Incident Management Process.

# 6 Platform Level Incident Resolution

As part of Remediation (Tier 2), Cloudreach will provide troubleshooting, Support and Incident Resolution to ensure the availability and accessibility of the Customer's environment(s) in the Public Cloud in accordance with the Incident Management Process, as relevant. This section covers the service management Cloudreach will provide to the Customers as part of Infrastructure Reliability Essentials - Remediation.

# 7 Incident Management Process

### 7.1.1 Incident Management Guidelines

#### 7.1.1.1 Cloudreach Responsibilities

Cloudreach shall adhere to the following guidelines as part of the Incident Management Process:

- All Incidents raised by Customer will be logged with Cloudreach and will be categorised as per the Priority table below (see "Incident Prioritisation" tables above)
    - The CSD can be accessed on a 24/7 basis to assist with P1 and P2 Incidents relating to the Customer Cloud Platform and troubleshooting issues in the

manner set out below. An Incident can be logged by the Customer or Cloudreach either through:
    - (i) emailing Cloudreach at support@cloudreach.com;
    - (ii) calling [UK] 0800 612 2966, [Overseas] +44 207 183 3991 or [US/Canada] (212) 335-0700;
    - (iii) the web by logging in to support.cloudreach.com using login details provided by Cloudreach during the onboarding process; or
    - (iv) mutually agreed automated event process.

  - For P1 Incidents specifically, the CSD can be accessed on a 24/7 basis only by telephone through the numbers as set out above. For the avoidance of doubt, P1 Incidents cannot be raised by email or through the CSD web portal.
- Customer can access CSD only by a designated Customer employee ("Support Engineer") raising an Incident.
- Cloudreach is under no obligation to respond to Incidents made in a manner which does not comply with this section.
  - CSD will use reasonable endeavours to find a work-around or solution to the Incident.

#### 7.1.1.2 Customer Responsibilities

- Incidents must be logged by Customer in accordance with this section.
- When logging an Incident, Customer will provide to Cloudreach the following diagnostic information:
  - Detailed description of the issue
  - Customer Incident number
  - If available and reproducible, step by step instructions to reproduce the reported Incident
  - If available, date and time (and timezone) when Incident occurred
- Following the logging of an Incident, Customer shall be available via email or telephone to answer questions and assist the CSD as appropriate.
- Customer shall provide telephone or email access to the End User to facilitate troubleshooting Incidents.
- Customer shall provide access to End User support tools or permit Cloudreach to use their support tools to facilitate troubleshooting Incidents.
- Customer shall, within 5 working days of a request from Cloudreach, provide CSD staff access to all required Customer systems in order to enable Cloudreach to provide the Services detailed in the Order Form.

### 7.1.2 Incident Notification

In the event that an alert is raised, Cloudreach shall:

- Prioritise in accordance with the Incident Prioritisation requirements in 7.1.2.1.
- Send the alert in accordance with the Incident Response Timelines in 7.1.2.2 on the event conditions as an email to the Primary Contact as denoted during the Onboarding process.

#### 7.1.2.1 Incident Prioritization

The following tables outline the prioritization of Incidents and the description of each

Priority Level.

| Priority Level | Type of issue |
|---|---|
| P1 - Critical Impact | Total loss of service, no workaround available. |
| P2 - High Impact | Functional but degraded critical service or total loss for a service which supports a critical service. No work around available. |
| P3 - Medium Impact | Non critical service which is partially impacted and not functioning as intended. |
| P4 - Low Impact | Minor issue contained to a small group. A work around or alternative service is available. |
| P5 - Very Low | Impact and urgency are negligible and do not need to be resolved to improve or restore service, or general technical guidance. |

### 7.1.2.2 Incident Response Timelines

The table below show the response times for each Incident Priority. For the purpose of this clause:

- "Response" is defined as Cloudreach acknowledging the Incident by (i) providing a Cloudreach reference number either electronically or verbally to the Customer and (ii) assigning a priority to the Incident.
- SLA for Response times start ticking when an Incident is logged by a Customer (either by phone, email or through the CSD web portal) or when Cloudreach is alerted of a service impact via its monitoring system.

| Priority | Target Response Time |
|---|---|
| P1 | 30 mins (24x7) |
| P2 | 1 hour (24x7) |
| P3 | 4 hour (24x5) |
| P4 | 8 hours (24x5) |
| P5 | Reasonable endeavours |

## 7.1.2 Incident Resolution

Where Customer has purchased Platform Level Incident Resolution as part of Remediation (Tier 2), in the event that an alert is raised, in addition to following the Incident Notification process, Cloudreach shall:

- Complete the steps described in part 6 to remediate incidents at the Platform Level. Where, as part of troubleshooting, an incident is identified to require Resource Level remediation, the Customer will be notified.
- Inform the customer of steps taken to resolve the issue, and confirm that the issue is resolved before closing the associated ticket in the Cloudreach ticketing tool.

# 8. Offboarding and handling of customer data

The table below details the type of customer information that Cloudreach requires for the provision of the services and how such information is handled upon termination of a customer service contract.

| Data | Type of data | Retention Period | Format / method of transfer or deletion (if applicable) |
|---|---|---|---|
| Customer Personnel Email Address | Identity contact | Duration of contract | Deletion from internal systems |
| Customer Personnel Phone Number | Identity contact | Duration of contract | Deletion from internal systems |
| Customer Personnel Name | Identity contact | Duration of contract | Deletion from internal systems |
| Customer Personnel Title | Identity contact | Duration of contract | Deletion from internal systems |
| Chef data | Monitoring | Duration of contract | Deletion from internal systems |
| Performanc e data | Monitoring | 13 months | Deletion from internal systems |
| Log data | Monitoring | 13 months | Deletion from internal systems |
| Trace data | Monitoring | 13 months | Deletion from internal systems |
| Access credentials to CSP | Access | Duration of contract | Deletion of Cloudreach roles from CSP |
| Switch role | Access | Duration of contract | Cloudreach or customer will remove switch role access and this includes any individual IAM accounts in the customer account |
| PEM keys | Access | 10 business days after contract termination | Deletion from internal systems |
| AMI snapshots | Backup | Per the agreed retention policy | Deletion from AWS console, unless customer wishes to retain these |
| WSUS data | Monitoring | Duration of contract | Deletion from WSUS and reset of registry keys |

| | | | |
|---|---|---|---|
| Alert Logic data | Monitoring | 13 months | Deletion of customer tenant post contract termination |
| Cylance data | Monitoring | 13 months | Deletion of customer tenant post contract termination |
| Source Code | Customer IP | Duration of contract | Deletion of any customer source code from internal systems or transfer ownership of repositories if applicable |