Cloud Core

Service Specification

Service Specification

Service Name:	Cloud Core
Service Level Hours:	24x7
Unit of Charge:	% of AWS and/or Azure Spend
Prerequisites:	Alert Logic (License)
Supported Cloud Platforms:	AWS and Azure
Product Code	CO-CORE-CORE
Version Number:	2.5.3
Status:	Release
Published Date:	November 2018

The Small Print

Definitions

The definitions for all capitalised terms used throughout this Service Specification are set out in the Cloudreach Cloud Operations Service Definitions and Interpretations 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

The Cloud Core Service delivered by Cloudreach provides the Customer with a fully monitored and managed IaaS/PaaS application stack based on both AWS and/or Azure cloud services.

Through the use of software agents provided by Cloudreach as deployed onto each Instance along with integrating AWS Cloudwatch and Azure Diagnostics, Cloudreach is able to monitor key services as well as automate execution of key maintenance and management tasks.

A summary of the key components of the Cloud Core Service are listed below:

Performance and Health - Infrastructure service critical events and metrics will be collected to detect trends with defined thresholds for alerting and performance analysis.

Automated backups - Block Level backups will be taken for Operating Systems and Database Engines with ad-hoc restores being submitted via Service Requests.

Patching - Both Operating System critical and security patches will be applied on a monthly basis with the ability to audit and report on the patches applied while maintaining compliance standards.

Maintenance - Cloudreach shall, when requested, deliver tasks through the Change Request process. These tasks cover the infrastructure to which an application resides. Inherent Operating System application issues will be dealt with via the Cloudreach Support desk.

Availability Monitoring - Operating Systems, Database Engines and service level checks will be carried out to ensure that critical components are in working order. These include Services or Daemons and response code checks on defined endpoints.

Commercial Governance - Cloudreach shall notify Customer by email of AWS-initiated scheduled maintenance or outage. Managed cloud billing, utilisation and billing insights, financial optimisation, governance and accountability are provided to ensure maximum control on cost and efficiency.

Threat and Vulnerability Management - Implement, report, amend rule/config, and tune deployed Threat Manager, Log Manager, Web Security Manager and AWS WAF and, monitor and respond to intrusions and vulnerabilities

Service Delivery Manager - Appointed individuals providing strategic business alignment, continuous service improvement, chaired proactive service reviews and business critical IT service management. Service Delivery Manager delivered remotely is included as part of Cloud Core. If the customer is requesting that the SDM is on-site and/or has specific dedicated number of hours or days a month, additional charges, including travel and expenses shall be applied. Customer's specific requirements will be captured during pre-sales and associated additional charges will be priced on application and reflected accordingly in the order form.

2. Cloud Infrastructure Performance and Health

Infrastructure service critical events and metrics will be collected to detect trends with defined thresholds for alerting and performance analysis.

2.1 Supported Operating Systems

Cloudreach supports the following Operating System versions:

Operating System Version	Comment
Windows Server 2008 R2 Service Pack 1/2-2016	Windows 2016 Nano is not supported at this time.
Ubuntu 14.04 - 18.04	Only the LTS edition is supported at this time. Canonical is expected to cease support for Ubuntu 14.04 in April 2019. Cloudreach shall stop support of this version on April 2019.
Debian 7 - 9	Debian is expected to cease support for version 7 on 31st of May 2018. Cloudreach shall stop support of this version on 31st May 2018. Debian is expected to cease support for version 8, April 2020. Cloudreach shall stop support of this version on April 2020.
Amazon Linux	Cloudreach supports all versions of Amazon Linux.
CentOS 6 - 7	CentOS is expected to cease support of these versions on 30th November 2020. Cloudreach shall stop support of these versions on 30th November 2020.
RedHat Enterprise	Cloudreach will support any RHEL version which is currently within Full Support. https://access.redhat.com/support/policy/updates/errata

2.2 Operating System Applications

- Programs and applications provided by Microsoft Windows and Linux distributions and included as part of the Windows Server and / or Linux operating system will be maintained by Cloudreach.
- Installation, updates, upgrades and support of third-party applications will be the sole responsibility of the Customer with the exception of applications outlined in (i) section 7.3.3 for which Cloudreach shall perform the tasks described in such section and in (ii) section 2.5.2 for which Cloudreach shall perform reactive monitoring only as described in such section.

2.3 AWS AMI & Azure Machine Image Access and Privileges

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.

The Customer shall inform Cloudreach of any changes to the Golden AMI in use of said resources outlined above to ensure that all Cloudreach monitoring and management tools continue to function effectively upon service redeployment.

2.4 Cloud Resource Health Check

Cloudreach will monitor the health of cloud resources outlined in the table below for each mutually agreed AWS and/or Azure Account and can raise an alert based on the event conditions defined in the table below. Cloudreach defined AWS and Azure health check metrics are based on a subset of available AWS CloudWatch and Azure Diagnostics metrics.

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

- Manage the response to the alert pursuant to the Incident Management Process.
- Send the alert based on the event conditions as:
    - an email to the Primary Contact as denoted during the Onboarding process.

2.4.1 Amazon Web Services Metrics

Cloud Resource	Health Check Metric	Health Check Event Condition
AWS ASG	Instance Count	When actual instances < Desired instance count
AWS ASG	Instance Count	Maximum Instance Level Reached
AWS ECS	Cluster CPU	Cluster CPU Reservation => 95%
AWS ECS	Cluster Memory	Cluster Memory Reservation => 95%
AWS ECS	Service Memory	Service Hard Memory Utilization => 150%
AWS EC2	CPUUtilization	Average greater than than 95% utilised for more than 5 consecutive minutes
AWS EC2	StatusCheckFailed	(sum) equal to or greater than 1 for more than 5 minutes
AWS ELB	HealthyHostCount	(average) less than 80% of total host count for more than 5 consecutive

		minutes
AWS ELB	HTTPCode_ELB_5XX	(percentage) greater than 10% of Sum Requests for 5 consecutive minutes
AWS ELB	SpilloverCount	(count) greater than 0 for 5 consecutive minutes OR ELB Surge Queue active greater than 100 connections queued
AWS RDS	CPUUtilization	(average) greater than 95% for more than 5 consecutive minutes
AWS RDS	QueueDepth	(average) greater than 2 for more than 5 consecutive minutes
AWS Cloudfront	5xxErrorRate	(average) greater than 5% for more than 5 consecutive minutes
AWS DynamoDB	SystemErrors	(count) greater than 2 for more than 5 consecutive minutes
AWS DynamoDB	ThrottledRequests	(count) greater than 2 for more than 5 consecutive minutes
AWS Redshift	CPUUtilization	(average) greater than 90% for more than 5 consecutive minutes
AWS Redshift	HealthStatus	(value) equal to 0 for more than 5 consecutive minutes
AWS Elasticsearch	ClusterStatus	(value) equal to yellow for more than 5 consecutive minutes
AWS Elasticsearch	ClusterStatus	(value) equal to red for more than 5 consecutive minutes
AWS Elasticsearch	CPUUtilization	(average) greater than 80% for more than 5 consecutive minutes
AWS Elasticsearch	JVMMemoryPressure	greater than 85% for more than 5 consecutive minutes
AWS Elasticsearch	FreeStorageSpace	Less than 20% for more than 5 consecutive minutes
AWS Elasticsearch	MasterCPUUtilization	(average) greater than 60% for more than 5 consecutive minutes
AWS Elasticsearch	MasterJVMMemoryPressure	greater than 85% for 5 consecutive minutes
AWS	CPUUtilization	(average) greater than 95% for more

Elasticache		than 5 consecutive minutes
AWS WorkSpaces	Unhealthy	(average) greater than 1 for 5 consecutive minutes
AWS WorkSpaces	ConnectionFailure	(average) ConnectionFailure greater than 50% (average) ConnectionAttempt for 5 consecutive minutes
AWS Storage Gateway	WorkingStoragePercentUsed	(average) greater than 95% for more than 5 consecutive minutes

2.4.2 Azure Metrics

Cloud Resource	Health Check Metric	Health Check Event Condition
Azure Virtual Machine	CPUPercentage	(average) greater than 95% for more than 5 consecutive minutes
Azure Virtual Machine	PercentAvailableMemory	(average) less than 5% for more than 5 consecutive minutes
Azure Virtual Machine	PercentUsedSwap	(average) greater than 5% for more than 5 consecutive minutes
Azure Virtual Machine	AverageReadTime AND/OR AverageWriteTime	(average) greater than 0.1 for more than 5 consecutive minutes
Azure WebApp	HTTP response code	(value) not equal to 200 for more than 1 consecutive minute
Azure ServiceBus	MessageCount	(count) greater than 0 for more than 5 consecutive minutes
Azure ServiceBus	SizeInBytes	(value) greater than 0 for more than 5 consecutive minutes
Azure SQL	cpu_percent	(average) greater than 95% for more than 5 consecutive minutes
Azure SQL	storage_percent	(average) greater than 90% for more than 5 consecutive minutes
Azure SQL	connection_failed	(count) greater than 0 for more than 5 consecutive minutes
Azure SQL	blocked_by_firewall	(count) greater than 0 for more than 5 consecutive minutes
Azure SQL	physical_data_read_percent	(average) greater than 95% for more than 5 consecutive minutes

All captured event data is retained by Cloudreach for at least 12 months.

2.5 Database Availability Check

Cloudreach shall monitor the status of engines (outlined in the table below) and will raise an alert based on the event conditions. Cloudreach defined health check metrics include a subset of available AWS CloudWatch and Azure Diagnostics metrics.

In the event that an alert is raised Cloudreach will manage the response to the alert in accordance with the Cloudreach Incident Management Process.

2.5.1 Metrics for AWS and Azure platform as a service database resources

Cloud Resource	Metric	Event Condition	Response
AWS RDS	CPUUtilization	(average) greater than 95% for more than 5 consecutive minutes	P2
AWS RDS	QueueDepth	(average) greater than 2 for more than 5 consecutive minutes	P2
AWS DynamoDB	SystemErrors	(count) greater than 2 for more than 5 consecutive minutes	P2
AWS DynamoDB	ThrottledRequests	(count) greater than 2 for more than 5 consecutive minutes	P2
AWS Redshift	CPUUtilization	(average) greater than 95% for more than 5 consecutive minutes	P2
AWS Redshift	HealthStatus	(value) equal to 0 for more than 5 consecutive minutes	P1
Azure SQL	cpu_percent	(average) greater than 95% for more than 5 consecutive minutes	P2
Azure SQL	storage_percent	(average) greater than 90% for more than 5 consecutive minutes	P2
Azure SQL	connection_failed	(count) greater than 0 for more than 5 consecutive minutes	P1
Azure SQL	blocked_by_firewall	(count) greater than 0 for more than 5 consecutive minutes	P1
Azure SQL	physical_data_read_percent	(average) greater than 95% for more than 5 consecutive minutes	P2

All captured event data is retained by Cloudreach for at least 12 months.

2.5.2 Metrics for hosted service database engines

Cloud Resource	Metric	Event Condition	Response
MSSQL	windows service	"Microsoft SQL Server Agent" equal to stopped "Microsoft SQL Server Engine" equal to stopped	P1
MSSQL	connection_check	read operation to mutually agreed table equal to not accepted	P1
MySQL	linux daemon	mysqld equal to stopped	P1
MySQL	connection_check	read operation to mutually agreed table equal to not accepted	P1
Oracle	windows service	Windows Service equal to stopped	P1
Oracle	windows service	OracleService<SID> equal to stopped	P1
Oracle	windows service	Oracle<SID>TNSListener equal to stopped	P1
PostgreSQL	connection_check	psql connection equal to connection refused	P1
PostgreSQL	connection_check	psql system table query equal to fail	P1
MongoDB	linux daemon	mongod/mongos equal to stopped	P1
MongoDB	connection_check	TCP port 27017 equal to connection refused	P1

All captured event data is retained by Cloudreach for at least 12 months.

2.6 Core Application Availability Check

Cloudreach shall monitor the status of core applications and will raise an alert based on the event conditions defined in the relevant table below.

In the event that an alert is raised, Cloudreach will manage the response to the alert in accordance with the Cloudreach Incident Management Process.

All captured event data is retained by Cloudreach for the time detailed in the data retention column.

Application	Metric	Event Condition	Response
Apache	linux daemon	apached equal to stopped, or httpd equal to stopped	P1
Apache	windows service	Apache service equal to stopped	P1
Apache	connection_check	TCP port unresponsive	P1
IIS	windows service	WWW service equal to stopped, or	P1

		WPA service equal to stopped, or RPC service equal to stopped, or FTP service equal to stopped, or SMTP service equal to stopped	
IIS	connection_check	TCP port unresponsive	P1
Tomcat	linux daemon	tomcat equal to stopped	P1
Tomcat	windows service	Tomcat7 equal to stopped	P1
Tomcat	http_check	http not equal to 200 response	P1
Tomcat	connection_check	TCP port unresponsive	P1
NGINX	linux daemon	nginxd equal to stopped	P1
NGINX	windows service	Nginx service equal to stopped	P1
NGINX	connection_check	TCP port unresponsive	P1
Web Server Generic	http_check	http(s) connection equal to refused, or http(s) response code greater than or equal to 500	P1
Web Server Generic	ssl_query	https certificate expiry less than or equal to 30 days	P3
PHPFPM	linux daemon	php-fpm equal to stopped	P1
PHPFPM	connection_check	TCP port 9000 connection equal to refused	P1
Varnish	linux daemon	varnishd equal to stopped	P1
Varnish	windows service	Varnish service equal to stopped	P1
Varnish	connection_check	TCP port unresponsive	P1
OpenVPN-AS	connection_check	TCP port 443 connection equal to refused, or TCP port 943 connection equal to refused	P1
OpenVPN-AS	ssl_query	https certificate expiry less than or equal to 30 days	P3
Sharepoint	Windows Service	Sharepoint Service is equal to stopped	P1
Sharepoint	Windows Service	ASP.NET Service is equal to stopped	P1
Sharepoint	Windows Service	AppFabric Service is equal to stopped	P1
Sharepoint	Windows Service	AppFabric Caching Service is equal to stopped	P1

Sharepoint	Windows Service	SPTimerV4 is equal to stopped	P1
Sharepoint	CPU Resource	If Utilisation is > 60% (Manual Override from MS-OS-ENT to ensure availability if a farm node dies)	P2
DFS	Windows Service	DFS-N Service is equal to stopped	P1
DFS	Windows Service	DFS-R Service is equal to stopped	P1

All captured event data is retained by Cloudreach for at least 12 months.

2.7 Database & Application Log Monitoring

Cloudreach shall monitor service logs and will raise an alert based on the event conditions defined in the relevant tables below. For the avoidance of doubt AWS and Azure platform as a service database resources are excluded.

In the event that an alert is raised, Cloudreach will manage the response to the alert in accordance with the Cloudreach Incident Management Process.

Customer may specify up to an additional 5 custom metrics during Onboarding of Customer services. For the avoidance of doubt, Customer custom metrics may result in an additional service charge.

All captured event data is retained by Cloudreach for at least 3 months.

Resource	Log Monitored	Event Condition	Response
Database Engine & Application	Application event log	Any Error and if Windows Eventcode = 1443, 1442, 1441, 1440, 1480.	P2
Windows Log	System OR Application OR Security	Critical	P1
Linux Log	Secure AND Message OR Auth AND Syslog	emergency OR alert OR critical	P1

2.8 Performance Monitoring

Cloudreach shall actively monitor the following resources and will raise an alert based on the event conditions defined in the relevant table below.

Resource	Threshold Triggers	Response
CPU:	100% Processor Time for greater than 3	P1
CPU:	80% Processor Time for greater than 3 minutes	P2
RAM:	10% Memory Available for greater than 3 minutes	P1
RAM:	20% Memory Available for greater than 3 minutes	P2

DISK:	10% Free Disk space available (All drives / volumes)	P1
DISK:	20% Free Disk space available (All drives / volumes)	P2
DISK:	100% IOP Usage for greater than 3 minutes	P1
DISK:	80% IOP Usage for greater than 3 minutes	P2
Network Interface:	ICMP Type 0: Echo Reply	P1
Custom Counters:	The Customer may specify up to 5 additional dimensions for integration into Cloudreach's existing monitoring tools during Onboarding of Customer services.	Mutually agreed during Onboarding of Customer services

All captured event data is retained by Cloudreach for at least 12 months.

Cloudreach shall monitor the performance of database engine(s) and infrastructure services. Cloudreach will raise an alert based on the event conditions defined in the relevant tables below. Cloudreach defined performance metrics include a subset of available AWS CloudWatch and Azure Diagnostics metrics.

In the event that an alert is raised Cloudreach will manage the response to the alert in accordance with the Cloudreach Incident Management Process.

2.9 Metric defined resources

Resource	Metric	Event Condition	Response
AWS DynamoDB	write capacity used %	Greater than 95% over five minutes	P2
AWS DynamoDB	read capacity used %	Greater than 95% over five minutes	P2
AWS RDS	CPU Utilisation	Greater than 95% for more than 5 minutes	P2
AWS RDS	Queue Depth	Greater than 2 for more than 5 minutes	P2
Redshift	WriteLatency	Trending activity only	Not applicable
Redshift	ReadLatency	Trending activity only	Not applicable
Apache	DNS resolution time	Trending activity only	Not applicable
Apache	http(s) connection time	Trending activity only	Not applicable
Apache	connection_check	http(s) response time greater than or equal to 10 seconds	P1

IIS	IIS / Web Application - Bytes Sent IIS / Web Application - Bytes Received IIS / Web Application - Connection Attempts IIS / Web Application - Current Anonymous Users W3SVC_W3WP - HTTP Requests Per Second	Trending activity only	Not applicable
IIS	connection_checks	W3SVC_W3WP response code equal to 500	P2
IIS	application_status	IIS - Current Blocked IO Requests, or IIS - Current Blocked Bandwidth bytes	P2
Tomcat	connection_check	http(s) response time greater than or equal to 10 seconds	P1
Tomcat	DNS resolution time	Trending activity only	Not applicable
Tomcat	HTTP connection time	Trending activity only	Not applicable
NGINX	connection_check	http(s) response time greater than or equal to 10 seconds	P1
NGINX	DNS resolution time	Trending activity only	Not applicable
NGINX	HTTP connection time	Trending activity only	Not applicable
Varnish	all varnishtop statistics	Trending activity only	Not applicable
PHPFPM	all server_status statistics	Trending activity only	Not applicable

All captured event data is retained by Cloudreach for at least 12 months.

3. Operating System Critical and Security Patching

Cloudreach shall perform the following Operating System patching where patches are made available by the Operating System provider.

- If Customer makes use of Golden AMIs as a source for infrastructure deployment Cloudreach will hold temporary Snapshots as a roll-back mechanism if required during critical/security patching periods.

Type	Frequency

Critical and Security Patching:	Monthly between 07:00 GMT Monday to 04:00 GMT Saturday, based on a mutually agreed schedule and Standard Change Request
Service Packs (Windows) or Distribution Upgrades (Linux):	On request by the Customer and subject to an additional charge.

4. Backup and Restore

4.1 AWS and Azure Backup / Restore

Cloudreach shall perform daily, weekly and monthly backups of the AWS EC2 and Azure Virtual Machine operating system Instances based on the default schedule and retention periods defined in the table below:

Backup	Schedule	Retention Period
Daily	02:00 UTC Monday to Sunday	7 days
Weekly	03:00 UTC every Sunday	4 weeks
Monthly	04:00 UTC on the first of every month	2 months

Customer may request alternative backup schedule and/or retention period during Onboarding of the Customer's services which shall be subject to approval by Cloudreach.

Instances are backed up based on the approach defined in the table below:

- All Incidents raised by the Cloudreach backup monitoring and configuration platform pertaining to 'backup failure' will automatically be assigned as a P2 Incident request and actioned by the Cloudreach CSD.

Cloud Platform	Backup Approach
AWS	Backups are performed by taking a Snapshot of AWS EC2 EBS volumes on a regular schedule as specified in the preceding table.
Azure	Backups are performed by taking full backups of each Azure Virtual Machine against a regular schedule defined by the Customer. By default the preceding table sets out the backup and retention periods.

Instances of Operating Systems can be restored on request by the Customer based on the approach defined in the table below:

- If required by the Customer, Cloudreach shall invoke an Operating System recovery approach against the Azure VMs or AWS EC2 instances within the supported account. The restore will be treated with P2 priority if it is service impacting.

- All requests raised by the Customer that are not identified as service impacting will be treated as P4 Service Requests.

Cloud Platform	Type	Recovery Approach
AWS	Instance or Full Volume	**Root Volumes**: Cloudreach shall create a new volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the current volume and replace with the newly created volume. **Additional Drives**: Cloudreach shall create a volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the volume and replace with the newly created volume or if requested attach the new volume at a different mount point. **Time:** Time scales depend on the size of the volume and any other file system factors such as encrypted file system implementations (e.g. BitLocker and ProtectV).
AWS	Individual file or files	**Individual Files:** Cloudreach shall create a new AWS EBS volume from a previous Snapshot depending on the date of the file to be retrieved. • For Linux: This EBS volume will be attached to the existing EC2 Instance and the file or folder moved over to the existing EC2 Instance file structure. • For Windows: This EBS volume will be attached to a new EC2 Instance and the file or folder moved over to the new EC2 Instance file structure. **Exclusions**: If the file is located in a protected volume where encryption or file security is in place, Cloudreach shall create a new Instance and attach the EBS volume to this Instance. Cloudreach shall extract the files / folders from this EBS volume and use cloud storage with encryption at rest to perform the backup and restore.
Azure	Instance or Full Volume	**Virtual Machine:** Cloudreach shall recover a chosen Azure Virtual Machine against an existing or retained application consistent backup from a previous recovery point as chosen by Customer. Upon system restore this will also restore all previous system dependent Azure services, installed applications, pre existing files and/or folders. Cloudreach shall reassign any pre existing Azure endpoints to the newly created Azure Virtual Machines to ensure continued connectivity upon successful restore. **Time** The time to execute a restore action is variable and dependent on the volume of data to be recovered from a backup.

4.2 Microsoft SQL Server hosted service database backup

Cloudreach shall perform full and differential backups plus 15 minute transaction log backups to locally attached storage for each hosted database engine in use as defined by the Customer.

Backup	Schedule	Retention Period
Full	Daily/Weekly if using differential backups	1 week
Differential (optional depending on size of database or Customer requirements)	As determined by Customer	1 week
Transaction Log	Every 15 minutes	1 day

4.3 MySQL hosted service database backup

Backup	Schedule	Retention Period
EBS Snapshot	Daily	1 week

4.4 PostgreSQL, Oracle, MongoDB, Cassandra and Couchbase hosted service database backup

Backup	Schedule	Retention Period
EBS Snapshot	Daily	1 week

- Cloudreach actively monitor all existing managed Instance backups for Incidents pertaining to 'backup failure'. If such an Incident is identified it will automatically be assigned as a P1 Incident and actioned by the CSD.
- If required by the Customer, Cloudreach shall invoke a recovery approach against the implemented database engine and respective configuration set up within the supported account as a P1 incident.
- All requests raised by the Customer not pertaining to an Incident relating to the reconfiguration of backup approach and/or retention periods will be treated as P4 Service Requests.

Customer may specify an alternative backup schedule and/or retention period during Onboarding of the Customer's services. Any changes made to the default approach taken by Cloudreach will incur additional costs subject to a new order form.

4.5 AWS RDS service database backup

For databases hosted on Amazon RDS, Cloudreach shall take additional copies of the RDS snapshots so that if the RDS Instance is terminated, Cloudreach can restore the RDS Instance.

- Cloudreach will automatically assign any backup related issues as P1 Incidents and action such Incidents via the CSD Incident Management Process.

4.6 File System Management

Cloudreach shall implement the following policies at Customer's request.

Object Scope	Responsibilities
System Files	• Cloudreach shall have full control over any protected file system objects which may be used by Operating System services. • Cloudreach shall ensure consistency between essential system files / folders / CAB / DLL files to ensure optimised performance and the essential running of the server environment. Microsoft Windows Only: • Cloudreach shall perform regular maintenance procedures using the Windows Server Disk Cleanup tool, Check Disk tool and System File Checker tool to maintain the health of the underlying Operating System.
User Space	• Cloudreach shall provide Customer with delegated access to files and folders which need to be maintained outside the scope of System Files. Only those Operating System privileges which are essential shall be granted.
Application Files or folders	• Cloudreach shall provide Customer with delegated access to Application Files and folders where Customer access is required to maintain the application. • Only those Operating System privileges which are essential shall be granted. • Customer shall follow the Change Management Process prior to implementing changes to application files or folders. • By default, Cloudreach is not responsible for the management or administration of Application Files or folders. Support for Application Files or folders may be provided by a separate service specification.

5. Security and Threat Management

For the avoidance of doubt, Customer acknowledges and agrees that the successful provision of the Security and Threat Management component of Cloud Core by Cloudreach is conditional upon Customer securing the necessary licences for the use of Alert Logic. Cloudreach shall have no obligation to provide Security and Threat Management as part of Cloud Core where Customer fails to obtain such licences.

5.1 Threat Management

As part of Threat Management, Cloudreach shall:

1. Respond to the intrusion types generated by the Alert Logic Threat Manager, Log Manager and Web Security Manager products, as defined in the table below, by raising an Incident via the Cloudreach Incident Management Process;
2. In response to identified Incidents, Cloudreach shall implement mutually agreed actions to the Customer's Cloud Platform where these actions are within the overall scope of this Service Specification and purchased by the Customer. Where actions are outside the overall scope of this Service Specification, Cloudreach shall notify the Customer in writing and no action will be taken at the time until Customer provides it's consent;

3. Provide a weekly review and monthly report with analysis to the Customer using data from Alert Logic and AWS Web Application Firewall (WAF), if deployed;
4. Perform AWS WAF rule amendments, if deployed;
5. Perform AWS WAF configuration tuning once per month;
6. Additional configuration tuning or review that may be required will be charged as DevOps on Demand and its applicable fees.

Intrusion Type	Description
Application attack	This Incident identifies attacks that target application-specific vulnerabilities. Alert Logic creates an application attack incident when an attacker attempts to compromise an application with a buffer overflow, race condition, directory traversal, SQL injection, cross-site scripting, /usr/bin/perl or other UNIX command attempts.
Brute force	This Incident identifies repeated authentication attempts and related activities. Alert Logic triggers a brute force incident when sufficient events indicate attempts to systematically compromise a system by brute-force guessing valid username and password combinations.
Denial-of-Service	This Incident, which includes denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks, identifies an attempt to make computer resources or services unavailable either temporarily or indefinitely.
Information leak	This Incident identifies generally successful reconnaissance attempts. Alert Logic creates an information leak incident when events indicate attempts at reconnaissance activities such as port scans used to identify open and closed ports, or obtaining information from a secure system.
Log policy	This Incident uses Log Manager log correlation policies to identify potential issues. Log Manager can create a log policy incident automatically based on selected correlated log messages and specifically defined conditions.
Misconfiguration	This Incident identifies a possible system misconfiguration. Alert Logic triggers a misconfiguration incident when events indicate that a system is incorrectly configured. Attackers can utilize the misconfiguration to compromise the system.
Policy violation	This Incident identifies activities that violate the acceptable use policies of most companies. These activities include viewing inappropriate material, peer-to-peer activity, and firewall policy changes.
Recon	This Incident identifies attempts to evaluate a target. Alert Logic creates a recon incident when events indicate reconnaissance activities against a network or set of hosts. The activities that trigger this Incident include gathering information about a server operating system, software versions, or the existence of debugging or demonstration scripts.
Suspicious activity	This Incident identifies activity not included in another category as set out in this table, and that requires further research. Alert Logic creates a suspicious activity incident when anomalous activities, which could indicate a compromise, occur.
Trojan activity	This Incident identifies activity that indicates a host is infected by a Trojan horse or other backdoor malware. Alert Logic creates a Trojan activity incident when events indicate a Trojan in the network. This type of malware acts as a legitimate program, but steals information or harms the system.

Worm activity	This Incident identifies hosts that display signs of worm infection. Alert Logic creates a worm activity incident when events indicate the traversing of a network worm.

Cloudreach shall respond to the Intrusions Types in accordance with the service levels outlined in the table below:

Threat Level	Examples	Incident Priority	Response Time
Critical	Successful data leakage; worm propagation; requires immediate remediation, or other post-compromise activity.	P1	30 Minutes
High	Aggressive penetration tests, large scale or long duration brute force attacks.	P2	30 Minutes
Medium	Brute-force or dictionary attacks; reconnaissance; failed web attack such as SQL injection, Apache Struts.	P3	1 Hour
Low	No threat, policy violation, authorised scans.	P4	1 Business Day

Cloudreach will not provide resolution times as part of Threat Management due to the varied nature of threats and the potential complexity of threat resolution.

Cloudreach shall perform daily checks to confirm the presence of the protected host in Alert Logic provided that the Customer appropriately tags the relevant Instances. The key value pair will be provided by Cloudreach during Onboarding.

Description	Incident Priority	Response Time
The host is not present in Alert Logic but is tagged with the appropriate key value pair	P4	1 Business day

5.2 Vulnerability Management

Cloudreach shall monitor the vulnerabilities generated by Alert Logic Cloud Insight and report any such vulnerabilities and configuration issues on a monthly basis as part of monthly reporting.

In response to identified vulnerabilities and/or configuration issues, Cloudreach shall implement mutually agreed actions to the Customer's Cloud Platform where these actions are within the overall scope of this Service Specification and purchased by the Customer. Where the actions fall outside of the overall scope of this Service Specification, Cloudreach shall inform the Customer in writing.

5.3 Endpoint Security

5.3.1 Event and Performance Monitoring

Cloudreach shall proactively monitor the anti malware software for alerts and respond to such alerts

as defined in the table below. Reports to generate these metrics will be created on a daily basis.

Endpoint Protection Metric	Event Condition	Response
Signature definitions date	If the current Signature definitions are not detected and the last definitions update is more than five days from current date.	P3
Signature definitions date	If the current Signature definitions are not detected and the last definitions update is more than ten days from current date.	P2
Engine version date	If running version of the engine is not equal to the latest version published by Endpoint Protection software and the published date for latest version is more than thirty days from current date.	P3
Virus/malware detection	Virus/malware is detected, automatically quarantined, including removal from the Instance, and reported within the daily Endpoint Protection application log report.	P3
Update service	If the Antivirus update service reports 'Running = False'.	P3

5.3.2 Regular Antivirus Maintenance Tasks

Cloudreach shall perform the following maintenance tasks as part of this Service Specification at no additional cost to the Customer.

Task	Description
On demand antivirus scans	Cloudreach will carry out a full antivirus scan by default at 01:00 GMT daily. Infected items will be automatically quarantined.
On Access scans	On access scans are setup by default. Infected items will be automatically quarantined.
Service Updates	Endpoint Protection application will be updated daily.
Signature/Definitions Update	Endpoint Protection application will check for Signature/definitions Updates on an hourly basis.
Reports	Upon request Cloudreach will provide the Customer with monthly reports for malware activity and update status.

Maintenance tasks not listed above but requested by the Customer may be subject to additional charges and/or a separately agreed Cloudreach order form.

5.3.3 Ad-hoc Antivirus Maintenance Tasks

Cloudreach shall perform the following ad-hoc maintenance tasks as part of this Service Specification at no additional cost to the Customer. These services will be delivered as a Standard Change.

Task	Description	Priority	Request Limit
On demand antivirus scans	Cloudreach will carry out an antivirus scan on request by the Customer.	P3	1 Per Month
Scanning frequency adjustments	Cloudreach will adjust the frequency of the current virus scan schedule.	P4	1 Per Month
Proactive scanning configuration	Cloudreach will modify the configuration for real time virus scanning to include or exclude specific files, folders and file extensions.	P4	1 Per Month
Scanning exclusions	Cloudreach will add folders/files/extension types to the exclusions. A Default list of exclusions is defined in Appendix B.	P4	1 Per Month
Retrieving quarantined file(s)	Cloudreach will retrieve and share quarantined files/folders on request from Customer.	P4	1 Per Month
Reports	Cloudreach will run reports as requested.	P4	1 per month

Maintenance tasks not listed above and requested by the Customer may be subject to additional charges and/ or may be delivered by a separately agreed Cloudreach order form.

5.4 Default Local Security Policy

Cloudreach will apply the following local security policy to an Instance at the request of the Customer:

Attribute	Setting
User Rights Management	• Backup and restore will be restricted to Cloudreach. • Access to shutdown the system from within the Instance will be restricted to Cloudreach. • Cloudreach will only be able to take ownership of files and folders and not the local administrator account.
Security Options	• The default administrative user will be renamed (in the interests of security the new name will not be defined in this Service Specification). • Cloudreach can specify the default logon banner for Customer to provide access notifications. Microsoft Windows Only: • The guest account will be explicitly disabled. • Anonymous SID/Name translations will be disabled.
Password Policy	• Password complexity requirements will be enabled. Microsoft Windows Only: • Account lockout policy will allow 5 failed login attempts and lock the account if breached for 30 minutes until it resets. • The minimum password length will be configured to 6 characters.

Windows Update	• Windows Updates will be defined in the local security policy and will connect to the Cloudreach Windows Server Update Services (WSUS) where patching and knowledge based articles will be approved or declined based on the specificity of the Customer systems/environment.
Linux Update Policy	• Linux will be updated based on the available packages in the repositories defined on the server. These updates are applied automatically (unless otherwise directed by Customer) but are limited to security updates only. **Exclusions:** • Due to the nature of security and non-security related updates in CentOS, patching will always include non-security related updates for this distribution.
Audit Policy	• Logon events, object access, process tracking and system events will be audited as part of the default service policy.

6 Service Levels

6.1 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.

6.2 Response and Resolution Times

The tables below show the response and resolution times for each Incident Priority. **"Response"** is defined as Cloudreach acknowledging the Incident by providing a reference number either electronically or verbally to the Customer as documented by Cloudreach.

"Resolution" is defined as Cloudreach providing a reasonable workaround or solution to the Incident and for the avoidance of doubt, the time for Resolution starts at the same time as the Response time.

Priority	Target Response Time	Target Resolution Time
P1	15 mins (24x7)	4 hours (24x7)
P2	30 mins (24x7)	8 hours (24x7)
P3	1 hour - (24x5)	24 hours (24x5)
P4	4 hours (24x5)	3 Business Days (24x5)

7 Support

7.1 Incident Management Guidelines

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 above (see "Incident Prioritisation" tables above)
    - The CSD can be accessed on a 24/7 basis to assist with all priority 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;
        - (iv) Customer's own ticketing system; or
        - (v) 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 requests made in a manner which does not comply with the Order Form.
    - CSD will use reasonable endeavours to find a work-around or solution to the Incident.

Customer Responsibilities

- Customer must log an Incident.
- 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.

7.2 IT Change Management

Cloudreach responsibilities:

- Cloudreach shall use reasonable endeavours to agree the IT Change Management process with the Customer.
- Cloudreach will only implement Change Requests to the Customer Cloud Platform which are in accordance with the IT Change Management process.
- Cloudreach shall only provide Customer with the credentials required to access the Customer Cloud Platform to complete work authorised through the IT Change Management process.

Customer responsibilities:

- Customer shall log all required changes made to the Customer Cloud Platform with Cloudreach using the mutually agreed IT Change Management Process.
- Customer shall provide Cloudreach with all necessary Public Cloud Environment and Private Cloud Environment services requested by Cloudreach in order to effect the Change Requests in accordance with the IT Change Management Process.

7.3 Maintenance Tasks

Cloudreach shall perform the following maintenance tasks as part of this Service Specification at no additional cost to Customer. These services will be delivered as a Standard Change Request and are subject to Cloudreach CSD's availability.

7.3.1 Compute Resources

Task	Description	Priority
Resize of Instance	Cloudreach shall change the size or type of EC2 instance to meet Customer performance or cost optimisation requirements.	P4
Increase Disk Storage Volumes	Cloudreach shall increase the size of existing disk storage volumes to support storage growth requirements.	P4
Add Additional Disk Storage Volumes	Cloudreach shall add additional disk storage volumes which will be integrated with the backup schedule defined above in section 4.	P4
Auto-Scaling Group Configuration	In addition to Incident Management, Cloudreach shall change auto-scaling group Min/Desired/Max values to meet Customer scaling requirements.	P4

7.3.2 Database Resources

Cloud Resource	Task	Description	Priority

AWS RDS	Configuration Management	Cloudreach shall change the size or type of RDS Instance to meet Customer performance or cost optimisation requirements. This excludes the creation and configuration of new Instances of RDS.	P4
Azure SQL	Configuration Management	Cloudreach shall change the size or type of Azure SQL Instance to meet Customer performance or cost optimisation requirements. This excludes the creation and configuration of new Instances of Azure SQL.	P4
Hosted database engines	Configuration Management	Cloudreach shall change the size or type of hosted database engine to meet Customer performance or cost optimisation requirements. This excludes the creation and configuration of new hosted database engine Instances..	P4

7.3.3 Other Infrastructure Resources

Cloud Resource	Task	Description	Priority
Apache	Configuration Management	Cloudreach shall update the configuration of an existing Instance of Apache on request by the Customer to meet Customer performance or cost optimisation requirements. This excludes the creation and configuration of new Instances of Apache or in the case of ASGs.	P4
IIS	Configuration Management	Cloudreach shall update the configuration of an existing Instance of IIS on request by the Customer to meet Customer performance or cost optimisation requirements. This excludes the creation and configuration of new Instances of IIS or in the case of ASGs.	P4
Tomcat	Configuration Management	Cloudreach shall update the configuration of an existing Instance of Tomcat on request by the Customer to meet Customer performance or cost optimisation requirements. This excludes the creation and configuration of new Instances of Tomcat or in the case of ASGs.	P4
NGINX	Configuration Management	Cloudreach shall update the configuration of an existing Instance of NGINX on request by the Customer to meet Customer performance or cost optimisation requirements. This excludes the creation and configuration of new Instances of NGINX or in the case of ASGs.	P4
PHPFPM	Configuration Management	Cloudreach shall update the configuration of an existing Instance of PHPFM on request by the Customer to meet Customer performance or	P4

		cost optimisation requirements. This excludes the creation and configuration of new Instances of PHPFM or in the case of ASGs.	
Varnish	Configuration Management	Cloudreach shall update the configuration of an existing Instance of Varnish on request by the Customer to meet Customer performance or cost optimisation requirements. This excludes the creation and configuration of new Instances of Varnish or in the case of ASGs	P4
OpenVPN-AS	Configuration Management	Cloudreach shall update the configuration of an existing Instance of OpenVPN-AS on request by the Customer to meet Customer performance or cost optimisation requirements. This excludes the creation and configuration of new Instances of OpenVPN-AS or in the case of ASGs.	P4

7.4 DevOps on Demand

DevOps on Demand should be used for a change, modification or creation of resources outside of the configuration of the environment from the time onboarding was completed, unless explicitly listed in the Standard Change list which will be provided upon request. The type of request or change for example are, creating new CloudFormation templates, updating Chef Cookbooks through to building new AWS or Azure resources.

The DevOps on Demand service is paid for on a hourly period basis and is available to during Business Hours only (9x5) This resource may be used to execute tasks to support the delivery of change within the Customer's Public Cloud Environment including, but not limited to:

- Non critical or urgent Operating System or application updates;
- Create & Update AWS CloudFormation templates;
- Create or update Chef cookbooks and recipes;
- Create & Update Azure resource manager templates;
- Implementation of financial optimisation recommendations / actions;
- Deployment cycle auditing and;
- Operational task automation.

7.4.1 DevOps On Demand Service Requests

- The Customer shall raise requests for DevOps On Demand by raising a call with the Service Desk via email, phone, or self-service portal;
- The Service Desk will triage Service Requests from Customer and assign such requests to Cloudreach's Core Operations team to review and prioritise;
- The Customer will receive a response to the Service Request within 1 Business Day. An estimate of effort and delivery date will be provided within 3 Business Days. There is no associated SLA Resolution Target for DevOps On Demand requests;
- Customer will communicate via email or telephone in a timely manner to answer questions and assist the Core Operations engineering team as appropriate.

7.4.2 DevOps On Demand Reporting

The Cloudreach Service Delivery Manager will include a summary of DevOps On Demand requests and number of hourly periods consumed during the previous month in the monthly service report.

7.4.3 DevOps On Demand Exceptions

For the avoidance of doubt, Cloudreach shall not perform any task which is not specifically detailed in this Service Specification, including but not limited to the following exclusions:

- Customer acknowledges that Cloudreach may not be able to act on every Service Request raised. Where Cloudreach is not able to act on the request, the Cloudreach Service Desk will notify the Customer;
- Examples of requests where Cloudreach may not be able to act include but are not limited to:
    - Requests which negatively impact the security of the Customer environment;
    - Application related changes where Cloudreach does not have the skills to implement change.

8 Service Delivery Management

The Service Delivery Manager (SDM) is responsible for delivering the service management outcomes associated with Managed Services provided by Cloudreach. The SDM provides the following services:

- ❏ **Business critical IT service management** – The SDM shall provide dedicated management of business-critical IT service management. They shall be the point of escalation and ensure the appropriate priority, resource, and associated governance is in place to progress to resolution.

- ❏ **Continuous service improvement** - The SDM shall implement a continuous service improvement plan. The plan shall cover recommendations, for example, on processes, procedures and run book improvements with action plan(s) mutually agreed with the Customer.

- ❏ **Proactive service reviews** - Owned by your dedicated service delivery manager focusing on business as usual reporting and identifying and driving improvements recommendations.

- ❏ **Strategic business alignment** - The SDM shall work with the Customer to ensure the operational services are delivered in line with the business objectives of the Customer. They shall also manage the business relations the Customer has with Cloudreach to enable delivery of services.

8.1 Service Review Meetings

The SDM will conduct a monthly service review and will chair a monthly service review meeting with the Customer at a time and place to be mutually agreed in advance by the parties. The agenda for the service review shall include:

- ❏ Review service report management summary and discuss any points including but not limited to Cloudreach or Customer actions

- ❏ Review Incidents, Problem(s), and Change Request(s) records, review performance and capacity issues identified (if applicable)
- ❏ Review status of existing, and any new mutually agreed, service improvement(s)

8.1.1 Service Reports

Cloudreach shall provide Customer with a monthly service report in Google Docs format or PDF .
The monthly service report shall include:

8.1.1.1 Management Summary

- ❏ Amazon Web Services (AWS), Microsoft Azure and/or Google Cloud Platform (GCP) performance summary: overall status plus availability and performance concerns, if any, on the following components: Cloud service availability, Instance CPU, memory, and network load
- ❏ AWS, Azure and/or GCP security: overall status plus any security concerns, if any, for the following components: Instances in VPC, Security Groups, 2 factor authentication
- ❏ Instance patching: overall status plus any security and compliance concerns
- ❏ Instance backups: overall status plus any business continuity concerns

8.1.1.2 Service Management

- ❏ Incident record summary including:
  - ❏ Current open Incident records and/or Service Requests
  - ❏ Recently closed Incident records and/or Service Requests
  - ❏ Summary of Incidents by priority and/or Service Requests
  - ❏ Summary of Incidents by component and/or Service Requests
- ❏ Problem record summary:
  - ❏ Current open problem records
  - ❏ Recently closed problem records
- ❏ Change Request record summary:
  - ❏ Pending Change Requests
  - ❏ Recently closed Change Requests
- ❏ SLA compliance summary
- ❏ Escalation Matrix
  - ❏ This lists the people and teams within Cloudreach and the customer organisation to contact and escalate an incident or an issue for example that remains unresolved at a support level

8.1.1.3 Performance Management

- ❏ Description of notable performance and/or capacity issues
- ❏ Performance charts from Cloudreach, AWS, Azure and/or GCP monitoring tools to support issues
- ❏ Information on cause of issue, if known
- ❏ Recommendations to remove or prevent future issues, if known

8.1.1.4 Infrastructure Management

- ❏ Infrastructure catalogue listing. AWS utilises EC2 to create and run virtual machines in the cloud and/or Azure and/or GCP Virtual Machine Instances managed by Cloudreach
- ❏ Summary of Instance backups for the previous reporting period. The default policy offered

is configured in the following 3 group policies: Daily, Weekly, and Monthly

8.2 Service Improvement Initiatives

- ❏ Cloudreach and / or Customer actions aimed at improving the quality and performance of the managed service
- ❏ The SDM shall implement a continuous service improvement plan that covers recommendations for example, on processes, procedures and run book improvements with action plan(s)is to be mutually agreed with the Customer
- ❏ Maintain and update Customer contact information
- ❏ Cloudreach will provide Customer with trending analysis in the quarterly and bi-annual service review meetings

8.3 Custom reports

Any service reporting that requires additional work to customise to Customer's requirements i.e. requires additional data to be collected and/or produced will be assessed and may be subject to additional charges

8.4 Service Review Timetable

Deliverable	Frequency
Introductions and Review of the Cloudreach Escalation Matrix Guideline	Kick Off
Conduct Monthly Service Review (Onsite or Remote)	Monthly
Provide Monthly Service Reports	Monthly
Provide Quarterly Service Report (trend reports for the quarter, analysis and recommendations)	Quarterly
Provide Annual Service Report (trend reports for the year, analysis and recommendations)	Annual

Appendix A - Cloudreach Windows Monitored Events

Application Events

Event Name	Event ID	Event Log Alert Level
Application Error (Requires Managed Application Infrastructure)	1000	Error
Application Hang (Requires Managed Application Infrastructure)	1002	Error
BSoD	1001	Error
Windows Error Reporting	1001	Informational
New MSI File installed	10,221,033	Informational
New Application Installed	903, 904	Informational
Updated Application	905, 906	Informational
Removed Application	907, 908	Informational
Application Package Updated	2	Informational

Audit Account Events

Event Name	Event ID	Event Log Alert Level
User Privileges updated	4728, 4732, 4756	Informational
Security Group Modification	4735	Informational
User Account Logon	4624	Informational
Failed User Logon	4625	Informational
Account Logged on with Explicit Credentials	4648	Informational
Basic Application Group Modifications	4783 - 4792	Informational
Distribution Group Modification	4744 - 4762	Security
Account Lockout	4740	Security

Certification Services Events

Event Name	Event ID	Event Log Alert Level
Certification modification has been modified	4868 - 4874	Informational
Certification Service has changes state	4875 - 4881	Informational

Extended Certification Messages	4882 - 5127	Informational

Event Log Services Events

Event Name	Event ID	Event Log Alert Level
Event Log was cleared	104	Informational
Audit Log was cleared	1102	Informational

Scheduled Task Events

Event Name	Event ID	Event Log Alert Level
A Scheduled task was created.	4698	Informational
A Scheduled task was deleted.	4699	Informational
A Scheduled task was enabled / disabled	4700 - 4701	Informational
A Scheduled task was updated	4702	Informational

System Services Events

Event Name	Event ID	Event Log Alert Level
Windows Service Fails or Crash Dumps	7022, 7023, 7024, 7026, 7031, 7032, 7034	Error
New Windows Service	7045	Informational
A new Service was installed in the system	4697	Informational
The System Time was changed	4616	Informational

Windows Update Events

Event Name	Event ID	Event Log Alert Level
Windows Update Failures	20, 24, 25, 31, 34, 35	Error
Hotpatching Failed	1009	Informational
Windows Update Installed	19	Informational

Kerberos Signing Events

Event Name	Event ID	Event Log Alert Level
A Kerberos authentication ticket (TGT) was requested	4768	Security
Kerberos pre-authentication failed	4771	Security

A Kerberos authentication ticket request failed	4772	Security
Kerberos success messages	4769, 4770, 4773	Security

Windows Firewall Events

Event Name	Event ID	Event Log Alert Level
Rule Added	2004	Informational
Rule Change	2005	Informational
Rule Deleted	2006, 2033	Informational
Failed with Group Policy	2009	Error
Service state has changed	5025, 5027, 5028, 5029, 5030, 5032, 5033, 5034, 5035, 5037	Informational

Kernel Signing Events

Event Name	Event ID	Event Log Alert Level
Invalid Image hash or a file	5038	Informational
Detected an Invalid page hash	6281	Informational

Local Security Policy Events

Event Name	Event ID	Event Log Alert Level
IPSec Settings have been changed	5040, 5041, 5042, 5043, 5044, 5045, 5046, 5047, 5048	Security

Object Modifications Events

Event Name	Event ID	Event Log Alert Level
A Scheduled task was modified	4698, 4699, 4700, 4701, 4702	Security
A Registry Key was modified	4657, 5039	Security
Object Deleted	4660	Security

Windows Processes Events

Event Name	Event ID	Event Log Alert Level
A Process was created	4688, 4696	Informational
A Process has exited	4689	Informational

Appendix B - Exclusions from on-demand and on-access Antivirus scans

Task	Exclusion (File Types)
On demand antivirus scans	ldf;mdf;ndf;bak;trn;adm;admx;adml;pol;aas;inf;ini;ins;
On Access scans	ldf;mdf;ndf;bak;trn;adm;admx;adml;pol;aas;inf;ini;ins; C:\Chef; C:\opscode
Built-In Exclusions	A list of exclusions maintained by the Endpoint Protection software is available on request.