digital space

AWS Managed Service

G-Cloud 15 Service Definition

Contents

1. Service summary

Digital Space will fully monitor and support your AWS infrastructure for a fixed percentage of your AWS costs. Digital Space is a top scoring AWS Managed Services Partner and was the first partner in Europe to gain the AWS Government Competency. All Digital Space support staff are UK government Security Cleared. Our Managed Service includes 24/7 monitoring which is visible to you through our Cloud Monitoring Portal. This portal also enables you to self-serve features such as backup schedules and automated switch-on and switch-off, instance and workspace stop / starts. Additionally, you can raise tickets and service requests and track the progress of both to conclusion.

2. Features & benefits

Top-scoring, independently audited managed service	This results in high quality services that are regularly audited and updated
Our pro-active monitoring predicts issues before you notice them	Pro-active incident resolution saves time and reduces unscheduled outages
We use an ITIL V4 approach	Integrates easily with your service desk
We hold ISO27001, ISO27017, ISO20000, ISO9001 and ISO14001	Staff and process security is already in place.
All technical staff are UK Government Security Cleared	Peace of mind that your environment is in safe and trusted hands
Our AWS Public Sector competency means we talk your language	We can work as an extension of your team.
Our percentage-based pricing makes budgeting easy	You can easily calculate the impact of changes in your estate
Our secure portal lets you monitor & manage your services	Monitor and configure elements of your workloads, raise and track service requests and incidents. The secure portal is included for free.
Secure by design	Our AWS-accredited expert consultants will work with you to define your infrastructure requirements and design a solution to meet your needs. Our engineers will then implement the solution and manage any migrations into AWS. Once live, our support teams will manage your environment in accordance with your selected service tier. We follow best practices throughout the lifecycle of a service.

3. Why choose Digital Space?

Cloud	Digital Space has more than twelve years' experience in providing Cloud solutions as an AWS Advanced Partner, a Microsoft Gold Partner and an IBM Gold Partner. It also has its own UK-based private Cloud and so is able to offer hybrid and multi-Cloud services that meet all needs from basic co-location, through to full public Cloud.
Connectivity	Cloud requires reliable connectivity and Digital Space is able to provide that through its own networking and connectivity business which includes a dedicated national network as well as the ability to provide everything from mobile connectivity to PWAN and SD-WAN solutions.
Security	Digital Space Cloud solutions have security built-in via the use of architectural patterns and technical staff who are Security Cleared but we also have partners who are security experts and can offer everything from Security Operations Centre as a service to ethical hacking and penetration tests.
Managed Service	Digital Space is expert in providing managed services and has held the AWS Managed Service Partner accreditation which involves regular external audits for more than 9 years. We also hold the following accreditations: ISO27001 – Information Security ISO27017 – Cloud Security ISO 20000 – IT Service management ISO14001 – Environmental management ISO9001 – Quality Management Our experience in this area means that we can either run services for you, making use of our automated Cloud monitoring services and Security Cleared experts, or implement services that can be easily managed and then train your team in how to provide that service themselves. Migrating your workloads to AWS allows you to innovate quickly by having compute infrastructure ready as required, enabling you to respond more quickly to shifting business conditions.
Public sector	Digital Space is experienced in working with the public sector including managing critical national infrastructure for central government, deploying artificial intelligence services for the NHS and delivering Cloud migrations for a wide range of organisations. This experience means that we understand your drivers and focus and are better able to supply your needs.
Innovation	In addition to a wide range of infrastructure engineers and architects, we also have developers who create innovative solutions on Cloud platforms.

4. Detailed service offering

Digital Space offers 3 levels of public Cloud managed service which provide increasing levels of support. The following table describes each service element, and a second table details which service elements are included in each level by default.

Each level includes the services that were provided at the previous level and adds additional ones.

Note that the Advanced level services listed below are an example of what can be provided but the detail of what Advanced Level means for each customer will be agreed with them before the service is delivered as it is typically specific to their environment and processes.

Services are provided between 09:00 and 17:00 on UK business days.

Digital Space can extend the hours of any of these services to be 24/7 and 365 days a year if required.

Service Element descriptions

Service Element	Detail
Incident Management & Service Desk	We provide a single point of contact via telephone, email and Web that enables named contacts at the customer and its suppliers to: 1. Raise Service Requests 2. Report Service Incidents 3. Raise Requests for Change 4. Track the progress of all the 'Tickets' above We ensure that all Tickets are prioritised, responded to and resolved in line with the categories and service level agreements listed below. We escalate issues to AWS where appropriate. Resolution time SLAs are provided in the 'Service Levels' section later in this document.
Infrastructure Management	This involves the following activities: 1. Ensuring that the infrastructure component of services works as planned and meets or exceeds AWS SLAs 2. Monitoring of and response to standard and custom metrics (see list of these below) 3. Engaging with the AWS Business Support Team as necessary to resolve technical issues for the customer. 4. Response to and management of AWS infrastructure event notifications e.g. degradation of hardware

Service Element	Detail
	Provision of Probable Root Cause Analysis reports for Priority 1Service Incidents
Access Control – General	Unless otherwise agreed with the customer, controlling access to the environments using: 1. Secure bastions 2. Multi Factor Authentication (MFA) 3. Role-based access control and policy-based identity and access management 4. Overlay networks
Access Control – Active Directory	Where required by the customer, manage Windows Active Directory services including: • Group policy construction & management • Schema changes • Debugging
Access Control – 3rd Parties	Control access for the customer's suppliers, ensuring that the customer authorises all user access
Endpoint Security	Manage and maintain anti-virus, malware and web reputation software on EC2 instances
External Internet Connectivity	Manage connectivity to the Internet
External Network Connectivity	Manage connectivity to any other networks agreed with the customer e.g. PSN, HSCN.
Secure Content Delivery Management	Control access to the services from the Internet using the following technologies as agreed with the customer: 1. Content delivery networks e.g. CloudFront 2. Web application firewall 3. Geo-fencing 4. Web threat management
Proactive Monitoring	Proactively monitor metrics and logs to automatically raise alerts when tolerances are breached. Details of metrics and alerts are provided below. Provide the ability for the customer to request provision of additional metrics, alerts, and reports via the RFC process. Note that provision of additional metrics, alerts or reports is charged at 3 days of T&M using

Service Element	Detail
	our SFIA rates where we agree that it is possible to provide what the customer has requested. Reports are only available at OS level or above as delivery requires use of our CMaaS portal which is only provided at that level and above.
Dynamic Reporting	Provide a secure, online CMaaS (Cloud Monitoring as a Service) portal that enables the customer and their selected suppliers to view and report on all the monitoring data listed below, along with any other custom metrics that are agreed. Access to the portal uses Multi-Factor Authentication (MFA).
Business Continuity & Disaster Recovery	Ensure that the service conforms to AWS best practices where the customer has approved their use including: 1. Load balancing 2. Provision of a mechanism to manage automated snapshots (backups) 3. Self-healing infrastructure Infrastructure as Code - the ability to re-build environments rapidly using templates
Backup management	We provide automated scheduled backups as wellas ad hoc backups via request to our service desk or via the CMaaS portal.
Infrastructure security management	Ensure, unless otherwise agreed with the customer, that their infrastructure conforms with the NCSC 14 Cloud Security Principles listed here: https://www.ncsc.gov.uk/guidance/implementing-Cloud-security-principles The defence layers should provide: 1. Implementation of standards-based system (infrastructure and OS) hardening to meet IT Health Check (ITHC) requirements 2. Support for ITHC execution by third parties commissioned by the customer and remediation to support Government Information Security accreditation requirements 3. Management and timely update of anti-Malware real-time protection using a leading Anti-Malware technology vendor 4. Implementation of Intrusion Detection Systems (IDS) based on modern open-source standards 5. Implementation of Intrusion Prevention Systems (IPS) based on modern open-source standards

Service Element	Detail
	6. Provision of near real time Cloud API malicious activity detection 7. Provision of near real time Identity and Access Management (IAM) malicious activity detection 8. Provision of near real time log analytics, from any source, for suspicious and anomalous behaviour 9. Controlling outbound internet access using managed whitelists 10. 'Detection at the edge' using AWS Cloud based services including GuardDuty and WAF or similar 11. Provision of automated environment defence in response to detected/suspected security threats 12. Near real-time, secure reporting on events and incidents Automatic URL redirection to static, safe, S3-backed websites in the event of specific attack vectors being detected
OS level support & patch management	We support and manage operating systems running on AWS servers including all versions of AWS Linux, CentOS and Windows supported by AWS. Where possible, we use AWS System Manager and Patch Manager to orchestrate patch windows based on tags. Where automation is not possible, our engineers will manually patch your instances
Landing Zone management	Management of AWS Landing Zone including some automation of services e.g. Guard Duty, CloudWatch, CloudWatch logs, Config/Rules.
Project and Change management	Work with the customer to align with its change control processes. Run a regular internal change advisory board (CAB) to respond to customer change requests and have the capability to call ad hoc CAB meetings to respond to emergency change requests. This CAB will safeguard environments by providing technical review and governance. Integrate internal CAB with the customer CAB / Technical Review Board as required. Project manage changes and integrate with customer processes, adopting different approaches (Agile, PRINCE2) where required on a per-project basis. Provide project management capability that is trained in both PRINCE2 and Agile.

Service Element	Detail
	Note that changes and associated design, specification and project management will be charged for separately using our SFIA rates.
Application deployment	Work with the customer and its suppliers to: 1. Manage the application deployment process / pipeline 2. Assist with application testing Provide the above regardless of the application / orchestration technology
Third-party engagement	Engage with multiple third-party suppliers to provide a single interface and help the customer keep things simple. Manage complex relationships through proactive engagement with multiple third-party suppliers.
Cost Management	Proactively monitor Cloud service utilisation and performance metrics to look for opportunities to reduce cost. The frequency of our recommendations will scale with the value of your infrastructure. Recommendations will be presented at least annually. We have FinOps qualified staff who specialise in enabling you to manage and reduce Cloud costs. We consider a number of approaches to achieve savings including the following: **Managed Run-time hours** - Switching infrastructure off based on service delivery requirements e.g. for a service running only 9 - 5 this represents ~76% cost reduction versus 24 by 7 operations **Right Sizing** - Using performance metrics including CPU usage, Network traffic, Memory etc. to identify when a service (server, Lambda function) is oversized and make recommendations to reduce the provisioned capacity and associated cost **Reserved Instances** - Analysis of the delivery hour requirements of a service e.g. 9 - 5, 24 by 7, identification of the underlying infrastructure and recommendations to purchase Reserved Instances (RI's) or Savings Plans to significantly lower cost based on commitment type **Re-platforming** – Moving workloads from Windows to Linux or from a self-managed to AWS managed one to reduce costs while maintaining or improving up-time **Storage optimisation** – Automatically moving file and object storage to cheaper services where access is infrequent

Service Element	Detail
	New Services - Introduction of new, or improved, AWS services e.g. new instance types, also offer the potential for lower cost (and typically improved performance).
Architecture & security consulting	Provide an effective design service for turning customer requirements into practical solutions that use AWS best practice and are secure. Note that Digital Space will respond to Requests for Change with written proposals within 10 working days for all changes other than large or complex projects that require significant investigation or weeks of implementation work. Architecture and security work to investigate and define changes is chargeable separately using our SFIA rates. Proactively suggest how new technologies / approaches may be used to improve service outcomes and / or reduce costs e.g. raising how the use of serverless technologies may enable the customer to deliver services more cheaply / effectively.
Service review	Provide regular (quarterly for Infrastructure & Operating System Level and monthly for Advanced Level) Service Review meetings that cover the following topics: 1. Progress on actions from the last meeting 2. Progress on proposals & new build work 3. Review of the last month's support report & KPIs 4. Discussion of any issues 5. Discussion of plans for change and implications for existing services 6. Quality assurance questions

Service Element distribution

	Infrastructure	Operating System	Advanced
Service Description	Ensures that Cloud infrastructure and services run as designed and configured.	Same as Infrastructure level but includes patching and maintenance of operating systems	As OS level but includes additional security processes. Can also include other disciplines not covered so far
Service Element	**Infrastructure**	**Operating System**	**Advanced**
Incident Management & Service Desk			
Infrastructure Management			
Access Control – General			
Access Control – Active Directory			
Access Control – 3rd Parties			
Endpoint Security			
External Internet Connectivity			
External Network Connectivity			
Secure Content Delivery Management			
Proactive Monitoring			
Dynamic Reporting			
Business Continuity & Disaster Recovery			
Backup management			
Infrastructure security management			
OS level support & patch management			
Landing Zone management			
Project and Change management			

	Infrastructure	Operating System	Advanced
Application deployment			
Third-party engagement			
Self-service elements			
Cost Management			
Architecture & security consulting			
Service review			

5. Service Levels

Incidents are categorised using the table below:

Category	Explanation
P1- Critical	Where a Service is down or does not function at all, and there is no circumvention for the problem; a significant number of users (over 40%) are affected, or a production business system is inoperable
P2 - High	Where a component of the Service is not performing, creating a significant operational impact (affecting over 10% of users)
P3 - Medium	Where a component of the Service is not performing as documented or is providing unexpected results; where there are problems that can be worked around; or where there is moderate or minor operational impact causing inconvenience
P4 - low	Where there are usage questions; requests for clarification of documentation, suggestions; or requests for new product features and enhancements

Service levels in terms of response and resolution targets for each of the priorities above are listed below:

Category	Explanation	
P1- Critical	< 10 minutes	< 2
P2 - High	< 30 minutes	< 4
P3 - Medium	< 30 minutes	< 8
P4 - low	< 1day	< 32

In addition to Incidents, you can raise tickets requesting changes. These tickets do not fall under the SLA for Incidents. The two types of change are listed in the table below:

Type of Change	Explanation & SLA
Requests for Change (RFC)	A request for a change requires us to understand what the user's objective is in requesting the change and to determine what needs to happen in order to deliver that change while maintaining the security and resilience of the existing service. This typically requires us to spend time contacting the user and discussing the technical implications of the change. Unless otherwise agreed, we will respond to RFCs within 10 working days with a proposal for the work and the timing of the change. Implementing RFCs will involve additional professional services costs.
Service Requests	A Service Request is a user request for information or advice, or for a standard change (a pre-approved change that is low risk, relatively common and follows a procedure) or for access to an IT service. Addition, removal and changes to user accounts driven by people joining, moving and leaving is a typical example of a service request. Details of which activities qualify as Service Requests will vary with each service - please request these from your Account Manager Unless otherwise agreed, we will action Service Requests using the SLA for Low priority incidents listed above.

6. Monitoring & alerts

Severities

Events listed in the tables below are only monitored if the services that produce those events exist within the customer's environment i.e. Tomcat or OSSEC logs will only be captured if there is a Tomcat or OSSEC service within the customer's environment. The severity column in the tables shows how Digital Space classifies each event. All events are reported in the monitoring dashboard that is viewed by Digital Space, but Major and Critical events automatically cut tickets on the Digital Space service desk which means they always result in human review and action. The table defines each Severity level. The following tables

Monitoring Severity Level	Explanation
Critical	Immediate intervention required as the alert could affect the service. We automatically create a support ticket when a critical alert is triggered.
Major	An alert that does not require immediate intervention but will get worse unless something is done. We also use this for state changes in critical infrastructure e.g. a change in a single VPN tunnel that might be a sign that the VPN could fail.
Minor	Used for alerts that are negative but have occurred with a lower frequency or at a lower level than would trigger a Major alert. The reason that we log these is so that we can track a pattern of alerts when performing root cause analysis.
Warning	Alerts that are of potential interest but have not yet hit "Minor" i.e. they indicate that action may need to be taken if the alert occurs more than three consecutive times. Alerts that do not breach this threshold will return to a clear condition after three consecutive "no issue" polls.
Clear	Shows that something is being monitored but that there are no issues

Infrastructure Health

Event Type	Explanation	Severity
Application logs (eg; MarkLogic, Tomcat)	WARNING level messages ERROR level messages CRITICAL level messages	Minor Major Critical
CPU Utilisation	>70% utilisation	

Minor

Event Type	Explanation	Severity
	>80% utilisation	Major
	>90% utilisation	Critical
Memory Utilisation	>70% utilisation	Minor
	>80% utilisation	Major
	>90% utilisation	Critical
ELB (Elastic Load Balancer) Health	>1 unhealthy instance	Major
CloudFront Health	4xx and 5xx errors >20% at any time	Critical
Disk Utilisation	>70% utilisation	Minor
	>80% utilisation	Major
	>90% utilisation	Critical
Status Checks	System reachability failure	Major
	Instance reachability failure	Major
	System AND Instance reachability failures	Critical
VPN / DirectConnect health	<2 tunnels available	Warning
	Tunnel status change	Minor
	1tunnel failure	Major
	>=2 tunnel failures	Critical
Anti-Malware alerts	Error status	Minor
	3 consecutive Error states	Major
	Anti-Malware Alert	Critical
Windows Event Logs	ERROR level messages	Major
	CRITICAL level messages	Critical
	Error codes 1058, 1073, 18204, 3041, 1105, 1006, 1030	Minor
AWS Service status	Service degraded	Critical
	Service down	Critical
Trusted Advisor	Status: Green	Clear
	Status: Yellow	Minor
	Status: Red	Critical
	Unattached volumes	Major

Event Type	Explanation	Severity
	Untagged instances	Major
Simple Email Service) Bounce Rate	Bounce rate >6% in 24 hour period Permanent email Bounces	Major Warning
AWS Health	Events with a status of Open Events with a status of Upcoming	Major Major
AWS Config	Beyond a default set of deployed Config rules, we can create / deploy additional rules as required. Compliant rules Non-compliant rules	 Clear Major
AWS CloudTrail	Unauthorised API calls Login without MFA Root account usage IAM user / group / role / policy changes CloudTrail configuration changes Login failures Disabled Customer Managed Keys S3 policy changes Config service changes Security Group changes Network ACL changes Network gateway changes Routing table changes VPC changes General List / Describe commands User-specific List / Describe commands	Major Major Critical Major Major Major Major Major Major Major Major Major Major Major Clear Major

Access Control

Event Type	Explanation	Severity
AWS Console Logins	Successful login, no MFA set Successful login, unknown IP 3 consecutive login failures Root account login	Warning Major Critical Critical
Server logins (Windows, Linux)	Unsuccessful login 3 consecutive login failures Use of "break-glass" account	Warning Major Critical
Web Application logins	Unsuccessful login 3 consecutive login failures	Warning Critical
ELB (Elastic Load Balancer) Health	>1 unhealthy instance	Major
CloudFront Health	4xx and 5xx errors >20% at any time	Critical
Disk Utilisation	>70% utilisation >80% utilisation >90% utilisation	Minor Major Critical
Status Checks	System reachability failure Instance reachability failure System AND Instance reachability failures	Major Major Critical
VPN / DirectConnect health	<2 tunnels available Tunnel status change 1tunnel failure >=2 tunnel failures	Warning Minor Major Critical
Anti-Malware alerts	Error status 3 consecutive Error states Anti-Malware Alert	Minor Major Critical

Security

Event Type	Explanation	Severity
AWS Security Groups	Security Group changes	Major
AWS Instance State Changes	Launched Started Stopped Terminated	Critical Major Major Critical
AWS components with unrestricted access	Unrestricted Internet-facing Security Groups	Critical
AWS S3 - public buckets	Unrestricted publicly available buckets	Critical
GuardDuty	Recon Behaviour Unauthorised Access	Major Major Critical

7. OS level portal

Customers of this service have access to the Digital Space service portal (customer space). There are two areas of interest.

ServiceHub is a platform from where you can open Incidents, raise Service Requests and track the progress of these and also on any orders raised on your behalf.

Additionally, you can see an overview of current Service Status, plus any upcoming planned maintenance or other scheduled outages.

Cloud Monitoring provides insights (from an AWS perspective) into the current security statis of your AWS domains, allowing you to prioritise mediation any findings from Security Hub, so ensuring that your environment is secure.

This platform also provides a highly granular breakdown of your spend over time, helping you to better understand where there may be opportunities to save money.

8. Complementary services

Business Continuity	Digital Space Backup as a Service Digital Space Disaster Recovery as a Service Digital Space Microsoft 365 native Backup as a Service Digital Space Microsoft Teams Backup as a Service
Communications	Digital Space 8x8 Cloud PBX Digital Space 8x8 Hosted PBX Digital Space 8x8 Meetings Collaboration Digital Space 8x8 Video Conferencing Digital Space 8x8 Voice for Microsoft Teams Digital Space Hosted Mitel Cloud (Flex)
Contact Centre	Digital Space 8x8 CCaaS (Contact Centre as a Service) Digital Space 8x8 Cloud Contact Centre Digital Space 8x8 Contact Centre Digital Space 8x8 CPaaS (Contact Platform as a Service) Digital Space 8x8 UCaaS (Unified Communications as a Service) Digital Space 8x8 Unified Communications Digital Space 8x8 XCaaS (Experience Communications as a Service) Digital Space Amazon Connect Administrative Extensions Digital Space Cloud Contact Centre (Amazon Connect) Digital Space Cloud Contact Centre Managed Service Digital Space Cloud Contact Centre Migration
Migration	Digital Space Cloud Migration Digital Space SAP to Cloud Migration Digital Space EPR (Electronic Patient Record) Cloud Migration Digital Space Housing Management System Migration Digital Space Microsoft 365 Discovery Digital Space Microsoft 365 Migration
Platform	Digital Space AWS Managed Service Digital Space Azure Managed Service / Platform Digital Space Cloud Architecture, Design and Build Services Digital Space Cloud Solution Brokerage & Implementation Digital Space Data & GenAI Assessment Digital Space Desktop as a Service (virtual desktops /VDI) Digital Space FinOps & Cloud Cost Optimisation Digital Space Licensing Assessment Digital Space Managed VMware Cloud on AWS Digital Space Managed VMware Cloud on Azure Digital Space Private Cloud Managed Service Digital Space Well Architected Review
Security	Digital Space Cyber (Security) Maturity Assessment (CMA) Digital Space Cyber Essentials and Cyber Essentials Plus Digital Space DDoS Mitigation Digital Space Managed Security Monitoring (SIEM) Digital Space Managed Security Operations Centre (SOC) Digital Space Penetration Testing

9. Copyright