

Cloud Service Overview

Cloud.config





Contents

1. Service Overview

3

4

7

8

9

2. Cloud Transformation

2.1 Service Levels

3. Service Level Agreement

4. Monitoring

5. Incident Management and Support

6. Cosnumption monitoring and invoicing (cloud.config Portal)

7. Security and Governance

8. Business Continuity / Disaster Recovery

9. Azure Service Matrix

11



1. Service Overview

cloud.config allows companies to take advantage of the power of Microsoft Azure as well as the expertise of FIXER to tailor the cloud environment to business needs. This makes it possible for businesses to focus on value

creation from core competencies while assuring that their cloud is optimized for performance, cost management, governance and security.

cloud.config delivers the essential services and support that provide flexibility to grow and adapt cloud services according to business needs. This process begins with an assessment of the current state and builds up a roadmap given business strategy and goals.

The cloud.config process:

Assessment & Architecture		Operation			Optimization
Implementation Plan	Environment Architecture	24/7/365 Monitoring	Primary Incident Response	Technical Account Manager	cloud.config portal
Confirm client requests and plan	Speedy architecting of Azure	Automatic monitoring of clients`	Confirmation of normal	Technical Account Manager	A dedicated tool to check Azure
Azure architecture accordingly.	environment relying on the	environment, incident reporting	operation as first response to	(TAM) to assist resolving tickets	consumption and cost, provided
Proposal for optimal system	expertise of professionals in the	via email.	incident.	submitted by clients, including	to aid clients in cost optimization

configuration and	cloud.config team.			for troubleshooting, technical	and billing management.
implementation notes.				quality assurance, etc.	
Customized quotation	n based on client needs	Basic Service Level	Optional Service	Optional Service	Optional Tool

In addition, FIXER offers a range of services to assist with the smooth operation of a client's business in financial, security, and administrative respects.

Payments-on-behalf-of client	DeepSecurity	Domain Registration	SSL Certificate Management
Payment on behalf of client for	Implementation and management	Total support for website domain,	Total support from generation of
cloud consumption to Microsoft &	of security solution DeepSecurity	from purchase to setup.	CSR to purchase of SSL certificate
Issuing invoice to client at later	to detect & prevent intrusions.		
date.			



2. Cloud Transformation

FIXER specializes in cloud transformation. This is the process by which the cloud is fitted to a specific business objective and architected for growth potential. Depending on an organization's needs this can include migration to the cloud, architecture validation, architecting for growing demand or new business functions, agile cloud deployment, as well as disaster recovery. FIXER provides services that range from the assessment of current environments, Azure migration, and managed services using a combination of industry-standard tools and proprietary FIXER tools.





Veean

octifio











FIXER診断ツール	CLOUD MANAGEMENT	CLOUD MANAGEMENT
//////////////////////////////////////	Jdynatrace	e 🧊dynatrace
Assessment	Migration	Managed Services
L&S Phase 1	L&S Phase 2 L&S Pha	se 3



2.1 Service Levels

Clients can choose service levels corresponding to their needs.

Free	Standard	Enterprise
Hyper Monitoring Service	Hyper Monitoring Service	Hyper Monitoring Service
✓ 24/7 Automated Monitoring (Zabbix)	 ✓ 24/7 Automated Monitoring (Zabbix) ✓ 24/7 Automated Monitoring (DeepSecurity) 	 24/7 Automated Monitoring (Zabbix) 24/7 Automated Monitoring (DeepSecurity) 24/7 Automated Monitoring (Akamai)
Expert Engineer Access		24/7 Automated Monitoring (AzureMonitor, Datadog
✓ Private Access Screen	Expert Engineer Access	Dynatrace, etc.)
Multiple Insights ✓ Operating Status Report (English ver.)	 Private Access Screen Primary Troubleshooting Technical Account Manager Multiple Insights Operating Status Report (English ver.) 	 Expert Engineer Access Private Access Screen Primary Troubleshooting Technical Account Manager BCDR (RPO 15 min, RTO 1 hr) *3 Multiple Insights Operating Status Report (Japanese ver.) Optimization proposal (including latest Azure use cases) Regular report meeting Support various audits

Monitoring & response levels are defined as follows:

- 24/7/365 Automated Monitoring (included with all service agreements)
 - o Using custom FIXER templates, incidents are classified into 5 categories of severity and automatically reported via email to clients.
- Incident First Response
 - o FIXER implements primary restoration measures for incidents according to the standard operating procedure (SOP) and reports to clients via email.
- Advisory Consulting
 - o Specialist engineer available to assist with root cause detection of incidents, reconfiguration of processes & servers as needed. Submission of monthly reports. (Engineer availability: weekdays 10:00 19:00 JST)
- Technical Account Manager (TAM)
 - o Detailed monitoring of cloud environment & performance with consideration of business impacts. Analysis of root cause for all incidents. Reconfiguration of processes & servers as needed. Monthly hands-on meeting to report on activity, latest Azure news, use cases, and answer any requests. (24/7





	Availability		Support Team		
	Workday daytime*	24/7/365	Dedicated Service Engineer	System Operations Manager	Consultant
24/7/365 Monitoring					
Primary Incident Response					
Advisory					
Technical Account Manager					

Each service level is supported by a team making sure that clients' requests and incidents are managed as per their Service Level Agreement.



3. Service Level Agreement

The cloud.config services are delivered according to the Service Level Agreements (SLA) and Service Level Objectives (SLO).

Services provided using Microsoft Azure Platform default to Microsoft's SLA, as do network uptime and server availability.

(For details, see: https://azure.microsoft.com/support/legal/sla/)

The SLA also governs the level of access and the response time of our experts.

At the highest level, SLAs define and establish response times for incidents, events, and root cause resolution. More information on the handling of incidents, escalation and response times of experts is provided in the Incident Management section below.

Priority Level	Time to Start Processing (Decide the responsible person)	Validation
P1 - Highest	< 30 Minutes	< 4 Hours
P2 - High	< 60 Minutes	< 1 Day
P3 - Middle	< 4 Hours	< 7 Days
P4 - Low	< 1 Day	< 2 Weeks
P5 - Lowest	< 7 Days	< 1 Month



4. Monitoring

cloud.config employs a combination of Azure-native monitoring tools as well as FIXER's purpose-built monitoring suite (part of the cloud.config Management System) to give visibility into the status of cloud deployments. Virtual

machine availability and infrastructure configurations are monitored and logged 24/7 with proven tools & processes.

As soon as FIXER's 24/7 monitoring tool detects any anomaly in a client's service(s) and/or infrastructure, it automatically triggers the following:

a. Automated phone calls to the responsible service desk personnel as per a pre-defined service call matrix.

b. An incident entry to FIXER's ITSM service desk tool.



FIXER's automated monitoring process ensures proactive incident management support for its clients.

Application-level monitoring with Dynatrace.



5. Incident Management and Support

Incidents are events where service has been interrupted and the restoration thereof is the primary objective. When an incident occurs, cloud.config supported by FIXER's expert staff will discern and address root causes in a timely and prioritized manner. Incidents are classified according to business impact and urgency. This process is

governed by the SLA and relies on the cloud.config Management System to make sure incidents are handled consistently for optimal service.

Incident Types & Definition

Event	Description
Irregularity / Trouble	 Irregular functioning of hardware/software or message output deviating from normal operation Notices of threshold exceeding or irregular flags that do not revert to normal Other events judged interruptions by the operations team
Operational mistake / incorrect response	• Operational mistakes or incorrect replies made by the operational team to clients

Security Incident	Detection of cyber attack Oetection of data breach
Complaint	• Receipt of complaint from client as defined by operational manual

 \bigcirc



Incident Priority



		configurations		
1. No external impact.	P5 - Lowest	P5 - Lowest	P4 - Low	P3 - Middle
2. Some impact on business operations. Light external impact.	P5 - Lowest	P4 - Low	P4 - Low	P3 - Middle
3. Impact on multiple business operations. External impact.	P4 - Low	P3 - Middle	P3 - Middle	P2 - High
4. Wide disruption of regular business activities. Large external impact.	P4 - Low	P3 - Middle	P2 - High	P1 - Highest

Severe Incidents: Severe incidents are those with a "P2 - High" or "P1 - Highest" priority rating. Reporting of

severe incidents follows the below rules. According to agreements in the SLA/SLO, the primary response to severe incidents is as follows:

Reporting at the occurence of severe incidents

Reporter	Reporting to	Timing	
Discoverer of the incident	Responsible person for service management provision	Immediately upon discovery	
Responsible person for service management provision	Administrator for service management	Within 30 minutes of discovery	

The responsibility for handling severe incidents lies with the responsible person for service management provision.

Management of incidents is escalated according to priority levels in keeping with protocols set out in the SLA.

In addition to the handling of incidents, service requests are handled using ticketing in the cloud.config Management System outlined above.



6. Consumption monitoring and invoicing (cloud.config Portal)

The cloud.config Portal is a FIXER original tool that provides granular insight into service consumption via intuitive dashboards and visualizationsg.



Cloud.config

The cloud.config Portal is highly customizable and allows administrators to provision access privileges for a variety of users, including both internal stakeholders as well as customers.

Alerts can be set to easily track budgets, keeping users informed of important consumption events and ensure usage limits are not crossed.

Consumption patterns can be analyzed to identify ways in which to optimize costs for particular business objectives or deployments.

Consumption can be split into multiple accounts and invoices can be generated directly from within the cloud.config Portal for simple, speedy and accurate billing of customers.



12



7. Security & Governance

It is important for organizations to strike a balance between leveraging the flexibility of Azure and ensuring control through security and governance.

cloud.config makes it easy for organizations to set security and governance policies and maintain enforcement as cloud deployments become increasingly sophisticated. By centralizing the administration of policies, operational consistency is maintained across an organization. This supports automation and helps to avoid reduce uncontrolled consumption leading to cost savings.

Security is managed through the proven Deep Security solution produced by Trend Micro, delivering robust protection for Azure environments with the simplicity of a single agent. Fully integrated with Microsoft Azure, Deep Security is easy to scale and provides continuous compliance while preventing data breaches and business disruptions.



For governance, resource tagging is enforced under cloud.config. FIXER provides assistance in managing resource groups and resource tagging, as well as governance reviews to assess Azure resource usage and provide best-practice guidance.

13



8. Business Continuity / Disaster



FIXER has a protocol in place for the management of unforeseen external shocks to promote business continuity and to facilitate disaster recovery, including the creation of Azure Recovery Service vault (RSV) and backup policies to FIXER's standards.

In addition to redundancy in Azure availability zones, FIXER has multiple physical locations to mitigate the operational impact of natural disasters.



2	Universal Kids	なぎさテラス 4階	
3	金沢事業所	石川県金沢市広岡2-13-37 ST金沢ビル 3階	
4	名古屋事業所	愛知県名古屋市中区栄2-2-23 アーク白川公園ビルディング 6階	
5	四日市事業所	三重県四日市市安島1-2-27 ジェックsビル 7階 「クラウド オペレーションセンター(サブ)」	
6	クラウドAIスクール	三重県四日市市安島1-2-29 MIZUTANIビル 1階	
7	FIXER Technologies, Inc.	717 Market St STE100, San Francisco CA 94103	and the second of the second o



9. Azure service matrix

Azure Service

Supported

Compute - Infrastructure	
Azure Virtual Machines -Linux	
Azure Virtual Machines -Scale Sets	
Azure Virtual Machines -Windows	
Azure Managed Disks	
Compute - Application Services	
Azure App Service	
Azure Container Service (AKS)	
Azure Functions	
Azure Logic Apps	
Azure Notification Service	
Azure Service Fabric	
Azure Service Fabric Mesh	
Azure Web Apps	
Networking	
Application Gateway	
Azure CDN	

Azure DDoS Protection	
Azure DNS	
Azure Express Route	
Azure Firewall	



Azure Service	Supported
Networking	
Azure Front Door	

Azure Load Balancer	
Azure Network Watcher	
Azure Traffic Manager	
Azure VPN	
Network Security Groups	
Virtual Network Endpoints	
Virtual Network TAP	
Virtual Network(VNET)	
Wob Application Firowall	
Storage	
Storage Azure Archive Storage	
Storage Azure Archive Storage Azure Blob Storage	
Storage Azure Archive Storage Azure Blob Storage Azure File Storage	
Storage Azure Archive Storage Azure Blob Storage Azure File Storage	
Storage Azure Archive Storage Azure Blob Storage Azure File Storage Azure Queue Storage Data Platform	
Storage Azure Archive Storage Azure Blob Storage Azure File Storage Azure Queue Storage Data Platform Azure Cosmos DB	

Azure SQL Database	
Azure SQL Database for MySQL	
Azure SQL Database for Postgre SQL	

Cloud.config

Azure Service	Supported
Management Tools	
Azure Advisor	
Azure Alerts	

Azure Automation	
Azure Backup	
Azure Blueprint	
Azure Database Migration	
Azure Migrate	
Azure Monitor	
Azure Policy	
Azure Resource Manager	
Azure Service Health	
Azure Site Recovery	
Azure Update Management	
Azure VM In-Guest Configuration	
Security	
Azure Active Directory & Identity	
Azure Key Vault	
Azure Security Center	
Analytics	
Azure Event Grid	
Azure Event Hub	
Azure Machine Learning	
Azure Stream Analytics	