TRANSPUTEC

Service Type	NOSQL Databases in the cloud

Transputec is a reseller of AWS and Azure cloud NOSQL services offering necessary support services for the implementation and ongoing support thereof.

Service Description:
Our service aims to provide end-to-end solutions for provisioning NoSQL databases on both AWS and Azure platforms. This includes initial setup, configuration, deployment, and subsequent support and maintenance for optimal performance and reliability.

Service Features:

- **Platform Agnostic Approach:** We cater to both AWS and Azure platforms, ensuring flexibility and compatibility with clients' existing infrastructure or preferences.
- **Consultation and Assessment:** We conduct a thorough consultation and assessment of clients' requirements and existing infrastructure to determine the most suitable NoSQL database solution and platform.
- **Database Selection:** Based on the assessment, we assist clients in selecting the appropriate NoSQL database technology such as Amazon DynamoDB, Amazon DocumentDB, Azure Cosmos DB, or others, considering factors like scalability, performance, and cost-effectiveness.
- **Architecture Design:** We design the database architecture tailored to clients' specific needs, ensuring optimal performance, scalability, and high availability.
- **Deployment and Configuration:** Our team handles the deployment and configuration of NoSQL databases on AWS or Azure infrastructure, following best practices and security guidelines.
- **Data Migration:** If required, we assist in migrating existing data from on-premises or other cloud platforms to the newly provisioned NoSQL databases.
- **Performance Tuning:** We continuously monitor and fine-tune the database performance to ensure optimal efficiency and responsiveness.
- **Backup and Disaster Recovery:** Implementation of robust backup and disaster recovery strategies to safeguard clients' data against unforeseen events or outages.
- **Security Implementation:** Implementation of security measures such as encryption, access control, and compliance with industry standards to protect clients' data from unauthorized access or breaches.
- **24/7 Support:** We provide round-the-clock support and monitoring to promptly address any issues, ensure system uptime, and provide timely assistance to clients.

Implementation Process:

- **Initial Consultation:** We conduct an initial consultation with the client to understand their requirements, budget, and timeline.
- **Assessment and Planning:** We assess the existing infrastructure and determine the appropriate NoSQL database technology and platform.

- **Architecture Design:** Our team designs the database architecture, considering scalability, performance, and high availability requirements.

- **Deployment and Configuration:** We deploy and configure the NoSQL databases on the chosen platform, following best practices and security guidelines.
- **Data Migration** (if applicable): If required, we assist in migrating existing data to the new NoSQL databases.
- **Performance Tuning:** We monitor and optimize the database performance to ensure efficient operation.
- **Backup and Disaster Recovery Setup:** Implementation of backup and disaster recovery strategies to protect clients' data.
- **Security Implementation:** Implementation of security measures to safeguard data integrity and confidentiality.
- **Testing and Validation:** We conduct thorough testing and validation to ensure the system meets the client's requirements and performance expectations.
- **Handover and Support:** Upon successful implementation, we provide training, documentation, and ongoing support to the client.

Services Overview

24x7 Monitoring

Our 24x7 monitoring service uses advanced tools and technologies to continuously monitor your AWS and Azure cloud infrastructure. We track key performance indicators, system health, and usage patterns to identify potential issues before they become problems. This proactive approach helps to maintain high availability and performance of your cloud services.

24x7 Support

Our 24x7 support service ensures that help is always available when you need it. Our team of certified cloud experts is ready to assist with any issues or queries you may have, no matter the time of day. We offer multiple channels for support, including phone, email, and live chat, ensuring that you can reach us in the way that is most convenient for you.

Regular Patching

Regular patching is crucial for maintaining the security and performance of any cloud service. Patching of vendor own infrastructure is undertaken by the vendor with any interruption being provided with advance warning. Transputec own patching of own systems is schedule and we manage the patching process to minimise disruption to your operations. Our team ensures that all patches are tested and compatible with your systems before deployment.

24x7 Security Management

Our 24x7 security management service provides comprehensive protection for your cloud infrastructure. We use advanced threat detection tools and conduct regular security audits to identify and mitigate potential risks. In the event of a security incident, our team responds swiftly to contain the threat and minimise damage.

Scalability Services

Our scalability services ensure that your cloud infrastructure can adapt to changes in demand. We use auto-scaling and other techniques to dynamically adjust resource allocation based on real-time demand. This ensures that your services can handle peak loads without over-provisioning resources, helping to maintain performance while controlling costs.

Reporting and Relationship Management

Our reporting and relationship management service keeps you informed about the status and performance of your cloud services. We provide regular reports detailing usage, performance, security, and cost metrics. Our team works closely with you to understand your business needs and ensure our services are aligned with your goals.

Onboarding and offboarding process

As an ISO 27001 organisation we have clear and repeatable processes for these activities. These are designed with a focus on user-centricity, aims to streamline the process of onboarding and offboarding clients to Microsoft and AWS cloud services.

Leveraging the robust and scalable infrastructure of the vendor platforms, our onboarding and operational readiness process, ensures a seamless transition for clients, whether they are just beginning their cloud journey or choosing to migrate their services.

The onboarding process is designed to be intuitive and efficient, reducing the time and resources required for clients to start benefiting from our services. Similarly, the offboarding process ensures that clients can safely and securely migrate their data and services away if they choose to do so.

Our commitment to flexibility, security, and customer satisfaction sets us apart, and we believe our tried and tested methodologies will greatly enhance the client experience in the cloud environment.

Service Constraints (if applicable)

- The suite of services that are provided by the vendor – these can be modified or withdrawn at the vendors timelines, we will endeavour to communicate any such service impacting changes as soon as possible.
- Any such pricing changes will be communicated in line with vendor guidelines.
- Transputec will act as master payer for each of the vendor services and will invoice the client directly based upon the agreed payment schedules.
- By paying for said vendor services, the client will be accepting the vendors terms and conditions for use of such services.

Service Levels

All services provided by Transputec and Microsoft and AS are 24x7x365.

After sales support

Transputec provide a complete cloud managed service 24x7x365, for details of the services provided please see the service descriptions above.

Technical requirement

Not applicable although the vendor may change or withdraw advertised services either globally or for specific geo-locations.

Outage and Maintenance periods

Where relevant and if site and service resilience is not implemented, then Transputec will carry out monthly maintenance periods to patch relevant services, optimise configuration or resolve any underlying non-time critical request or issues. These will be generally carried out, outside of normal UK working hours unless agreed otherwise.

Data Storage , DR/BCP

All data will be stored in the agreed geo-locations (availability zones, sites as relevant) as defined as part of the overall architecture design. Our designs will be based around the Well Architected Framework for each vendor.
For resilience we can design and provide to suit your needs:

- Azure Site Recovery & Availability zones
- AWS Availability zones
- Third party data backup's
- Vendor native backup's
- Managed by ISO27001 support teams.

Access to data (upon exit)
AWS and Azure have specific protocols in place to manage data access for clients upon exit of their services.
AWS Data Access Management Upon Exit:

- AWS provides a rich set of tools and capabilities for managing access. Users can authenticate with multi-factor authentication (MFA), federate using an external identity provider, and obtain temporary credentials with limited permissions.
- When a client decides to exit AWS, they may request Microsoft technical support to export the organization's Microsoft Managed Key (MMK) and all associated artifacts in the form of a Trusted Publishing Domain (TPD).
- This TPD file can then be imported into a clean installation of Active Directory Rights Management Services[2]. Afterwards, this (on-premises) AD RMS cluster can be used to license content protected with the MMK through the AIP service from any Windows client that is configured with special redirections in the registry.

Azure Data Access Management Upon Exit:

- Access to customer data by Microsoft operations and support personnel is denied by default. When access to data related to a support case is granted, it is only granted using a just-in-time (JIT) model using policies that are audited and vetted against Azure's compliance and privacy policies.
- Azure has established internal records-retention requirements for back-end data. Customers are responsible for identifying their own record retention requirements.
- If a client decides to exit Azure, they can request the export of the Microsoft Managed Key as part of a TPD file. This TPD file can then be imported into a clean installation of Active Directory Rights Management Services[5]. Afterwards, this (on-premises) AD RMS cluster can be used to license content protected with the MMK through the AIP service from any Windows client that is configured with special redirections in the registry.

In both cases, accessing previously protected content after a cloud exit is limited to users on Windows machines in the Intranet. This setup allows administrators with AD RMS super user privilege to access and optionally unprotect any content. Regular end users are capable of consuming content protected explicitly for them as well as content labelled with predefined permissions granting them access.

Security
Amazon Web Services (AWS) and Microsoft Azure both prioritise security in their cloud services, offering a wide array of tools and capabilities to ensure the protection of user data and applications.

Transputec will leverage these relevant tools and any suitable third-party services to ensure you have “security by design” as the core principle of the service model.
AWS provides a secure cloud infrastructure with over 300 security services and features[1]. It offers tools for increasing privacy and controlling network access, such as network firewalls, connectivity options, and DDoS mitigation. AWS also provides automatic encryption for all data flowing across its global network. It protects the infrastructure of the cloud, including hardware, software, and networking that run AWS services. AWS also has a team of more than 3,500 global cybersecurity experts working together to help safeguard business assets and data.

Azure, on the other hand, provides multi-layered security across physical data centres, infrastructure, and operations. It offers built-in security controls and unique threat intelligence to help identify and protect against rapidly evolving threats. Azure’s infrastructure is designed from facility to applications for hosting millions of customers simultaneously, providing a trustworthy foundation upon which businesses can meet their security requirements. Azure also provides configurable security options and the ability to control them, allowing users to customize security to meet the unique requirements of their organization’s deployments.

Both AWS and Azure provide a secure foundation and give users built-in security tools and intelligent insights to help rapidly improve their security posture in the cloud.