TD SYNNEX | Services

Cloud Express (CX)

Statement of Services

Contents

1 Introduction

This Statement of Service is an extension of the Managed-Service Agreement (MSA) with the purpose to define the entitlements specific to Cloud Express that are either not defined or different to those listed within the MSA.

Whilst the MSA defines two different service levels, Enhanced and Managed, Cloud Express is only available within the Manage set of entitlements.

Cloud Express is a 24 x 7 service where TD SYNNEX covers all aspects of management and administrative activities of your Public Cloud IaaS (Infrastructure as a Service). The service is designed to help TD SYNNEX's Partners with the shared responsibility model associated with the management and administration of Public Cloud. The service is available for AWS and Azure services. The service includes monitoring, alerting, full problem troubleshooting and remediation.

This document provides Partners with detailed information about the entitlement and operational aspects of how the service is provided, and the associated add-ons that are available to purchase.

2 Service Scope

Services	Included in Cloud Express Service	Service Components
Platform Monitoring and Management	✓	Tenant & Consumption Dashboard
		Assets status
		Security Status
		Cost Optimisation & Forecasting
		Alert Management
		Monthly Recommendations (Cost, Security, Stability)
IaaS Monitoring and Management	✓	Virtual Machine monitoring and management
		Patch Management
		Security Monitoring & Management (Next Gen EDR + SOC)
		Storage Monitoring & Management
		Backup Monitoring & Management
Cloud Service Management	✓	Incident Management
		Change Management
		Problem Management
		Service Request Management
		Service Reporting
Exclusions	X	Resource deployment or implementation
		Operating System upgrade
		Hardware Issues
		Support for 3rd party applications

2.1 Platform Monitoring and Management

TD SYNNEX use native and 3rd party tools (e.g. Cloud Interconnect) to provide the IaaS monitoring and management services. The Proactive Monitoring and Management of Virtual Machines optimises availability and performance of the environment.

The service includes:

- 24*7 Proactive Monitoring of AWS/Azure Virtual Machines and Network resources

- Monitoring the environment for the following
  - Uptime
  - Health
  - Performance
  - Security
- Realtime CPU, Memory, Disk Utilization and Threshold Monitoring
- Realtime monitoring of critical related services and processes leveraging 3rd party tooling (e.g. ConnectWise) to ensure uptime and respond to any issues that occur.
- Deploy and manage automated tasks for environment management
- Critical alert and event notifications delivered to the Partner in case of any system generated event or user generated tickets. Note that this can be adjusted to the Partner requirements and can include less critical alerts on demand.
- Managing and remediating any alerts generated from the system
- Troubleshooting and remediation of system and user generated Incidents and Problems
- Addressing Service Requests related to the environment
- Change Management to accommodate recommended changes in the environment

2.2 Virtual Machine Monitoring and Management

VM Monitoring and Management ensures the operational integrity and high availability of your virtualised compute resources resident in Azure or AWS.

Supported Operating Systems:

Operating System	Linux	RedHat, Amazon Linux, Linux SUSE (versions SLE 12 SP4,SLE 15, SLE 15 SP1), Centos, Debian, Ubuntu (versions currently supported by Azure/AWS)
	Windows	Windows Servers (versions currently supported by Azure/AWS)

Note: VM's created with ARM templates can not be monitored under the cloud express service

2.3 Patch Management

TD SYNNEX manages and deploys operating system patches and critical updates to protect against vulnerabilities. This practice includes the following:

- Patch policy creation for virtual servers
- Patch pilots roll out and testing
- Patch deployment (Scheduled and On-demand)
- Patch compliance reporting
- CVSS Scoring of scope virtual machines (Common Vulnerability Scoring System)

VM scheduled downtimes are confirmed by the Partner during the Onboarding. This schedule is then used for any scheduled patching after specific patches have been approved / pre-approved by the Partner.

When a Zero-Day Vulnerability patch has been released TD SYNNEX validated the authenticity and applicability and within two (2) business days sends a notification supported by recommendations to Partner requesting action to address the issue.

2.4 Security Monitoring & Management

Cloud Express includes several essential security management services using the embedded cloud native tools for foundation level monitoring, and/or 3rd party tooling (e.g. SentinelOne Platform) for an advanced level of monitoring for vulnerabilities. The range of services provided within Cloud Express include:

- Advanced End point Detection Platform (EDR)
- 24 x 7 Security Operations Center (for partners who do not have an existing next gen AV solution)
- Ransomware Protection & Assurance for scoped machines

- AI based Malware detection
- Infected & Compromised machines are automatically fixed and taken off-line
- Security Policy management in Azure Security Center or AWS Security hub
- Monitoring and reporting any in scope resource security health issues.
- Managing visibility and recommendations of missing patches on Virtual Machines
- Periodic and proactive updates of rulesets for effective threat detection.
- Monitoring install status and update status of any Non-Microsoft AV or EDR Solutions
- AV monitoring and Compliance

2.4.1 Anti-virus monitoring and compliance

- Anti-Virus/Anti-malware (AV) updates are provided automatically based on the set schedule every day. Any failure in AV updates will generate a Sev3 alert, following which TD SYNNEX will notify Partner in accordance with the appropriate SLA response.
- If there is an issue with updates failing due to license or subscription issues or any other reason outside TD SYNNEX's control, TD SYNNEX will notify the Partner in order to seek resolution. Please note that resolution of all AV issues cannot be guaranteed as this has to be remediated by the AV platform owner (Master server) which is not in the scope of the Cloud Managed service.

Additionally, TD SYNNEX will perform a Partner's standard operating procedure (SOP), defined during the Onboarding phase for the remediation of AV update issues on the managed servers. TD SYNNEX may be limited in reporting these types of issues in accordance with the stated SLA due to the potential inconsistency of AV updates.

> ***Note:*** *Partners / End Customers must have a valid maintenance or licenses from the AV vendor. Expiry of licenses places limits on AV management. Failure by customer to resolve reported issues in a timely manner will constrain TD SYNNEX's ability to ensure AV updates are current.*
>
> ***Note:*** *Where a Partner does not subscribe to the native security centre offering TD SYNNEX will provide the above using 3rd party tooling (e.g. SentinelOne).*

2.5 Storage Monitoring and Management

TD SYNNEX Cloud Express service monitors and manages the following services as part of Cloud Storage:

- Azure Storage: Blob, table, file & queue
- AWS Storage : S3, EBS, Glacier, EFS

The scope of activities in managing cloud storage include:

- Monitoring storage health, capacity, availability and performance to ensure the operational integrity of cloud based storage.
- 24x7 proactive troubleshooting of access, capacity and performance issues.
- Providing insight and recommendations on storage access policies as part of the monthly and quarterly service review meetings.

Note: *Application Specific Storage performance issues are not included in the standard scope of Cloud Express.*

2.6 Backup Monitoring and Management

TD SYNNEX will setup and monitor backup services for the full VM workloads thereby ensuring their operational integrity.

This service ensures continuous proactive monitoring of the backups running in AWS or Azure Backup, to deliver continuous and unimpacted services.

TD SYNNEX will monitor the backups running on AWS or Azure, utilizing native Backup tools to capture the Realtime status of Backups, failures and success ratios.

- TD SYNNEX will setup and configure Backups in accordance with the Partner's backup schedule or the default backup schedules (See Appendix) as appropriate

Backup Monitoring includes:

- 24*7 Backup Status Monitoring

- Backup Success and Failure Alerts
- Backup Jobs Management
- Test Restores Every Month
- OnDemand Restores
- Incidents (such as failures) related to backups
- Ad hoc backup requests can be made by raising a service request with the TD SYNNEX service desk
- Any failure of a daily backup will trigger an alert, which will be remediated by the TD SYNNEX engineer

2.7 Cloud Network Management

TD SYNNEX's Cloud Express service provides the monitoring and management of Cloud native network components including:

- Azure: vNet, NSG, load balancer, gateway, VPN, Azure firewall, Express Route.
- AWS: VPC, ELB, VPN, Direct Connect

TD SYNNEX will:

- Monitor the above cloud network resources to help ensure their availability, connectivity and performance.
- Troubleshoot issues related to connectivity and performance.

Note: *The Cloud Express service does not include any on-premise network connectivity monitoring and troubleshooting as standard but these additions can be made available as additional service options.*

2.8 Cloud Environment Management

2.8.1 Certificate Management

Cloud Express helps Partners manage the challenges of certificate management for cloud resources. The service includes:

- The export and import of secure socket layer (SSL) certificates within Partner / End Customer subscriptions.
- Managing SSL certificate validity and reporting on potential expiry in advance.

2.8.2 Azure / AWS Subscription Organisation Management

Cloud Express subscription management includes:

- IAM user and group management – Providing or revoking users and group access to authorised resources and service levels.
- Providing resource-group (Azure)/tag-based (AWS) billing breakdown.

Note: *Service available only if billing access is provided to the TD SYNNEX team and appropriate resource group tagging is enabled.*

2.9 Cloud Directory Services

The service includes:

- Availability – Checks the availability of Active Directory.
- Response Time – Get the response time of the Active Directory.

2.10 Cloud Optimisation

TD SYNNEX services will help customers to optimise their Cloud resources by providing monthly recommendations around the following:

- Cost
- Security
- Reliability

- Operational Excellence
- Performance

TD SYNNEX uses native functionality and 3rd party tools to share these recommendations and associated reports with the Partners.

2.11 Out of Scope Services

Any services which are not explicitly covered in the above sections will be deemed as out of scope. Optionally such services can be provided on a bespoke-pricing basis.

The following list of service activities are specifically excluded from the scope of Cloud Express IaaS management service for Azure / AWS:

- Applications monitoring and management
- Azure/AWS technical architect support
- License management Windows, Remote Desktop Services Client Access Licenses

2.12 Optional SQL on VM Managed Services

Provides management and support to Partners for SQL Database instances on Azure and AWS. Cloud Express is a pre-requisite to this service.

- 24x7 monitoring, alert filtering and prioritisation of incidents
- Configuration of DB Backups and retention policies
- Validation of backup-failures
- User management (Example – User creation, deletion, update and permissions)
- Backup test restorations
- Monitoring database resources (CPU percentage, Storage percentage, Storage used, Storage limit, Compute unit limit, Compute Unit percentage, Memory percent, IO percent, Total active connections, Total failed connections.
- Microsoft / AWS support escalation and coordination as required.
- In the event of an outage we will work closely with end customers to restore the cloud instance from the latest/golden image available from the backup repository.

SQL on VM Managed Services		
Services	**Service Components**	**Inclusions**
Performance Monitoring	DTU Usage Monitoring	√
	Read/Write Monitoring	√
Resource Monitoring	CPU Monitoring	√
	I/O Monitoring	√
	Storage Monitoring	√
	Blocking Queries	√
	Deadlock Monitoring	√
	Active Sessions	√
	Failed Connections	√
Capacity Management	Capacity Recommendations	√
Azure Database Support	Incident Management	√
	Service Request Management	√
	Microsoft / AWS Tier 3 Escalations	√
	Reporting	√
Exclusions	Assessment, Deployment, Implementation or Migration	X
	DBA Related Requests	X

	Support for Applications linked with Database	X

2.13 Optional Disaster Recovery as a Service (DRaaS)

DRaaS offers management and support to Partners for the planning and execution of disaster recovery to a secondary site in Microsoft Azure. DRaaS is only available on Azure and for VMs that are under the management of the Cloud Express Service; we support Azure Virtual Machines deployed from one Azure Site replicated to another Azure site. The add-on ensures the underlying infrastructure can support End Customer DR plans and includes on-going replication and configuration changes to a secondary Azure site as well as quarterly testing. Cloud Express is a pre-requisite to this service. The service de-risks the common scenario of a business' DR policy not being effectively supported and leverages cloud based Microsoft Azure platform to minimise the costs and risks associated with creating and maintaining a DR-ready infrastructure.

Service scope:

- DR Design – Defines the Microsoft Azure DR redundancy strategy with orchestration, replication policies and sync frequency for server groups, providing a high level architecture diagram for DR solution.
- Implementation of the DR design
- 24 x 7 monitoring of Cloud DR resources and replication health status
- Cloud DR orchestration – Manages the replication policy setting for all Azure workloads – server, storage and networking components.
- DR Readiness – Manages Microsoft Azure DR Readiness consistency and readiness checks quarterly including quarterly redundancy and failover test.
- Incident resolution
- Service Delivery Management
- Vendor Support Co-ordination

2.13.1 Roles and responsibilities during DR Activities

During Disaster Recovery and Recovery Readiness testing TD SYNNEX will be responsible for ensuring the VMs and supporting infrastructure are replicated to the secondary site. Partner / End Customer will be responsible for verifying applications, databases and integration with third parties are up and working as expected on the secondary site. The table below outlines the responsibilities of these parties for delivering the managed DRaaS add-on:

Tasks for Delivering DRaaS	TD SYNNEX Services	Partner / End Customer
Azure Disaster Recovery Setup and Operations		
Evaluate End Customer Requirements	R, A	C, I
High Level DR Architecture (scope limited to context of replication of virtual machines only)	R, A	C, I
Architecture sign-off for implementation	C, I	R, A
Azure subscription and support contract	C, I	R, A
Azure Disaster Recovery plan creation	R, A	C, I
Azure Disaster Recovery sign-off for implementation	C, I	R, A
Onboarding	R, A	C, I
Operations and monitoring	R, A	C, I
Change management: Notification of changes to the primary site	C, I	R, A
Change management: Replication of change to secondary site	R, A	C, I
Azure Disaster Recovery testing		
Azure Disaster Recovery execution sign-off	C, I	R, A
Initiate failover to secondary site	R, A	C, I
VPN: Verify and troubleshoot VPN access is available to secondary site	R, A	C, I
DNS changes (if any) related to DR	C, I	R, A
Network: verify and troubleshoot related infrastructure	R, A	C, I

Network Security Group: verify and troubleshooting	R, A	C, I
VMs: verify connectivity (reachable through network infrastructure, ability to login)	R, A	C, I
Applications: Verify and troubleshoot any application related issues	C, I	R, A
Databases: Verify and troubleshoot any application related issues	C, I	R, A
3rd Party API integrations: Verify and troubleshoot any integration	C, I	R, A
DR Failover completion acceptance	C, I	R, A
Sign off to fail back to primary	C, I	R, A
Primary site completion acceptance	C, I	R, A

RACI: **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed

2.13.2 DRaaS Recovery Point and Time Objectives

Recovery Time Objective (RTO) refers to the amount of time a server can be unavailable without causing significant damage to the business.

RTO is not simply the time between loss and recovery but also accounts for the steps IT must take to restore the server and its data.

Recover Point Objective (RPO) refers to the company's loss tolerance or the amount of data that can be lost before significant harm to the business occurs. The objective is expresses as a time measurement from the loss event to the most recent preceding backup.

For example, if all or most of the End Customer data is regularly backed up in scheduled 24-hour increments, then the maximum loss is the data collected between the last backup and the loss event, to a maximum of 24 hours.

Recommended RPO threshold from fifteen minutes to two hours based on available bandwidth and workload.

DR Environment	Target RPO
Azure to Azure	Minimum 15 minutes to 2 hours

Note: *Minimum Recommended Bandwidth is 50 Mbps. If lower bandwidth is available, the ROP time will increase.*

DR Environment	Target RTO
Azure to Azure	2 hours

Note: *Above DRaaS RPO/RTOs will be achieved as per Microsoft best practices. However, RTO may also change based on the complexity of extended infrastructure services like Azure firewall, network appliances, Site to site VPN, Virtual Network Gateway, Traffic Manager, Load Balancer, Application Gateway. If these additional components adversely affect the target RPO/RTO the actual RPO/RTO will be made clear at the time of implantation of the service.*

2.13.3 DRaaS Exclusions / Out of Scope

The following is a list of activities that are out of scope of the DR service:

Area	Out of Scope
Monitoring	• Customisations to monitoring templates
SQL Server	• Granular DB level transactions (Setting up Always On availability group)
3rd Party Vendor Escalations	• Line of business app vendors
Software licenses	• All license management is the responsibility of the Partner • Microsoft Support Contract
Automation	• Custom scripts implementation
Third party Backup or Storage	• Managing 3rd party backups or storage
Network and VPN connectivity	• Monitoring and management of network and VPN cloud connectivity

Service Requests	• Service Requests (SRs) for resources that are outside of the scope of the service. Onboarding additional servers to the service will be managed through the standard on-boarding service, all other SRs will be managed as T&M professional services.

2.13.4 DRaaS Delivery Reporting

Quarterly service reports are generated by TD SYNNEX. The Service Delivery Manager (SDM) will ensure regular communication with the Partner for service delivery management reviews:

Quarterly Operational Service Review / Report

- Response SLAs
- Alerts and Tickets Trends
- Test Failover Success Rate
- Failover Requests
- Service Requests for DR plan update

2.13.5 DRaaS Onboarding

Onboarding includes:

- Environment assessment
- DR Solution Architecture as per application server dependencies
- Orchestration Design with Server Protection Groups
- DR Architecture Design Report
- Failover Configuration
- Implementation Plan
- Consumption cost estimates for Azure

2.13.6 DRaaS Change Management

There are two types of change:

- **Standard Changes**: Changes where scope falls within the defined scope of the service (managed as Service Requests). For example:
    - Virtual Machines
        - VM instance creation / deletion
        - Creation, encryption of volumes
        - Virtual disk creation / deletion
        - Creation or modification of Security Groups
        - Auto Scaling groups creation and autoscaling policy configuration changes
    - Storage
        - Storage account creation and providing permissions
        - Storage policy creation / modification
        - Creating / modifying file share storage
        - Mapping shares to instances with ACLs
    - Network
        - Network creation, modification or deletion vNET
        - Subnet creation, modification or deletion
        - Creation / Modification or deletion of VPN connections

Note: *It is important for the Partner / End Customer to notify TD SYNNEX of any changes made to the environment outside of the virtual machines (changes to the network, security groups, VPN, etc.) as soon as they occur in order to ensure the secondary site is modified (if/when required). This helps to ensure all systems operate properly in the event of failover and failover testing. This requirement doesn't extend to changes at the system level (within the VM) as these will be handled automatically via replication. Failure to do so could result in failures in the event of failover to the secondary site. Because Cloud Express is a pre-requisite for DRaaS TD SYNNEX will sync environment changes to the primary environment that are made as part of Cloud Express*

automatically to the secondary site and it will not be necessary for the End Customer/Partner to make a secondary request to sync these changes to the secondary site.

- Non-Standard Changes: Changes where the scope of the change does not fall within the defined scope of the service, handled as Complex Changes.

3 Ordering and Billing

3.1 Pricing and Ordering

Partner shall provide to TD SYNNEX the environment details and service requirement, including quantities.

Based on above, TD SYNNEX shall provide to the Partner a quote or offer which will include Partner, End Customer and pricing details.

Elements of the Managed Service that are priced:

1. Cloud Express: Monthly Per Virtual Machine Fee based on maximum active number of Virtual Machines during the period; once a VM is no longer active then they will fall out of scope with the next month's billing cycle.
2. Monthly White Label Fee (Optional): Monthly fee to offer Partner White Labelling of the service
3. Azure SQL Instance database management add-on is charged monthly based on number of databases under management.
4. DRaaS add-on is charged based on the monthly per server replicated fee. This ongoing monthly fee is charged based on the number of servers with active replications in a given month, once a server is no longer actively being replicated it will fall out of scope of the service and the following month's billing cycle. In addition to the monthly service fee there is an assessment and setup fee that is equal to three month's of the monthly recurring fee. TD SYNNEX will charge a minimum monthly fee equivalent to the cost of 5 (five) servers.

For the current Price List, please contact your TD SYNNEX representative.

Appendix 1: Pre-Requisites

The following section provides the list of pre-requisites that are required to allow TD SYNNEX to onboard the Partner and/or End Customer to the Cloud Express service, and to then deliver the service based on the entitlement described within this SOS.

- Delegated Admin Privileges to the End Client's admin centre
- Admin access of cloud Portal

Partner should have ability to provide remote access to the End Customer environment, if required during the onboarding project.

For White Labelled services add on

- Partner to provide IVR recordings & call opening scripts to provide White Labelled phone service
- Partner to allow Zendesk system in their mailing system by allowing SPF & DNS to send emails on behalf of their domain & setup a mailbox for incoming & outgoing communication
- Partner to provide their logos & any specific branding requirements.
- For Domain mapping , partner will have to make certain DNS redirection entries in their DNS portal , for us to redirect the Zendesk system to their website domain.
- Partner to share documented process of managing third party escalations.
- Partner to share documented scripts & templates that they would like us to embed in our system for email notifications & standard responses.

Appendix 2 Standard Changes

The following is a list of typical standard changes performed within Cloud Express.

1. IAM
    a. User creations, user policy changes
    b. Role creations
    c. Group creation and group policies
    d. IAM user permissions
2. Virtual Machines
    a. VM instances creation
    b. Modify VM instance properties (type of VM)
    c. Creation, encryption of volumes
    d. Image creation
    e. Creation of security groups
    f. Auto Scaling groups creation and autoscaling policy configuration changes
3. Storage
    a. Storage account creation and providing permissions
    b. Storage policy creation
    c. Creating file share storage
    d. Mapping shares to instances with ACL's
4. Network
    a. Network creation (VPC/vNET)
    b. Subnet creation
    c. Creation of Route Tables and Networks ACLs
    d. Internet and NAT gateway creation
    e. Create VPN connections
5. Certificates
    a. Import/Renew certificates to resources

Appendix 3 Glossary

- **"DR"** means Disaster recovery
- **"DRaaS"** means Disaster Recovery as a Service as described and defined in this document.
- "**Escalation**" means when a support ticket is moved to a higher priority within the services operational management model or a ticket is passed to the Vendor for additional support.
- **"Failover DR Test"** means testing of the process of backing up a given server.
- **"IaaS environment"** means the association of cloud technologies that together form the basis of the scope of services managed within Cloud Express
- **"Vendor"** means Original Equipment Manufacturer and is used in this document to reference Manufacturer of the hardware equipment or software to which the Service applies.
- **"On-premise"** means virtual machines or systems that are located in an on-site data center and not in the cloud.
- **"SDM"** means **"Service Delivery Manager"**, Tech Data's main point of contact for managing the in-life performance of the service
- **"TD SYNNEX engineer"** means technical engineer who is performing services set out in this document
- **"VM"** or **"Virtual Machine**" means the different types (known as instances) of computing configurations provided within the IaaS cloud service.

Appendix 4 Default Backup Schedule

Virtual Backup Types	**Retention**
Daily (Monday to Saturday)	1 Week (7 Copies Available)
Weekly (Sunday) (Optional)	4 Weeks (4 Copies Available)
Monthly (Last Day of every month) (Optional)	One Month (1 Copy Available)

*Daily backups are configured by default with defined schedules whereas for optional configuration i.e., Weekly & Monthly schedules will be based on Partner explicit requirement