**Migrating Azure SQL Managed Instance (MI) from CSP (Cloud Solution Provider) Tenant to an EA (Enterprise Agreement) Tenant**

Migrating Azure SQL Managed Instance (MI) from a CSP (Cloud Solution Provider) tenant to an EA (Enterprise Agreement) tenant is a complex and high-impact project that involves both technical and stakeholder management layers. Below is a breakdown that includes Scrum practices, stakeholder engagement strategies, and actionable steps with designated owners.

**Project Goal:**

Migrate Azure SQL MI from CSP Tenant A to EA Tenant B without downtime (or with minimal downtime), ensuring compliance, governance, and performance continuity.

|  |  |  |
| --- | --- | --- |
| Stakeholder | Role | Owner |
| Data Architect | Technical design & solutioning | Susanta Kumar |
| Product Owner | Business requirements, prioritization | Adnan Ali |
| Azure Admin | Platform provisioning, access | Basil Das and Pankaj Mandal |
| Network Engineer | Connectivity & VNet planning | Gaddiel Bryan |
| DBA / Data Engineer | SQL migration execution | Ahmad Khan/Asad Rehman |
| Security Officer | Governance, policies, compliance | Arnold Nzailu/Pratim Borah |
| Application Owner | Testing and validation | Reagan Ikie Sasa/Freddy |
| Vendor CSP Partner | Source tenant access/support | Pankaj Mandal |
| Microsoft TAM (if available) | EA support & escalation | Manar Alrifai |
|  |  |  |
|  |  |  |

**Migration Strategy Overview:**

Azure SQL Managed Instance cannot be moved directly between tenants. So, you must deploy a new MI in EA tenant and migrate the data using one of these options:

BACPAC export/import

Azure Data Migration Service (DMS) (recommended for minimal downtime)

**Scrum Practices in Migration Project:**

|  |  |
| --- | --- |
| Scrum Practice | Application to Migration |
| Sprint Planning | Plan iterations around phases like setup, connectivity, testing, cutover |
| Daily Stand-ups | Track blockers (e.g., firewall config, access delays) |
| Backlog Grooming | Refine tasks like VNet peering, DMS setup |
| Sprint Review | Demo migrated instance, test app connectivity |
| Retrospective | Review what went well or didn't (e.g., network delay) |
| Definition of Done (DoD) | New MI is live, monitored, backup configured, apps point to it |
|  |  |

**Steps, Action Owners, and Artifacts:**

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Description | Action Owner | Tools / Notes |
| 1. Tenant Assessment | Evaluate current CSP infra | Azure Admin | Azure Assessment Reports |
| 2. Provision Target MI | Deploy new SQL MI in EA tenant | Azure Admin | Use Azure Portal / ARM templates |
| 3. Networking | Configure VNet peering, NSGs | Network Engineer | ExpressRoute / VPN as needed |
| 4. Identity Access | AAD integration, RBAC setup | Azure Admin + Security Officer | Cross-tenant trust if needed |
| 5. Choose Migration Method | Pick DMS / replication etc. | Cloud Architect + DBA | Based on downtime requirements |
| 6. Setup Migration Tools | Provision Azure DMS or scripts | DBA | Azure DMS |
| 7. Data Migration Dry Run | Test performance & accuracy | DBA + App Owner | Validate data, latency |
| 8. App Configuration Testing | Redirect staging apps to new MI | App Owner | Test connection strings |
| 9. Production Cutover | Final sync & go-live | DBA + All Teams | Notify via change mgmt. |
| 10. Monitoring & Validation | Ensure metrics, performance | Azure Admin | Log Analytics, Alerts |
| 11. Post-Migration Review | Lessons learned, cleanup old infra | Business Analyst | Retrospective board |

**Sprint (Simplified):**

|  |  |  |
| --- | --- | --- |
| Backlog Item | Priority | Sprint |
| Setup EA Azure SQL MI | High | Sprint 1 |
| VNet peering setup | High | Sprint 1 |
| Data Migration Tool POC | Medium | Sprint 2 |
| Security & AAD setup | High | Sprint 2 |
| Dry Run Migration | High | Sprint 3 |
| App Layer Testing | Medium | Sprint 3 |
| Final Cutover | Critical | Sprint 4 |
| Documentation | Low | Sprint 4 |

**Stakeholder Communication Plan:**

|  |  |  |  |
| --- | --- | --- | --- |
| Communication | Frequency | Owner | Audience |
| Weekly Status Report | Weekly | Data Architect | All Stakeholders |
| Daily Standups | Daily | MS Team | Dev/Infra Team |
| Risk Updates | As needed | Security Officer | Security/Compliance |

**Security & Compliance Considerations:**

Ensure data encryption at rest/in transit

Role-based access control (RBAC) on new resources

Validate audit logs and diagnostics settings

Update Azure Policy to match EA governance standards

**Technical Actual Methods to do:**

To take a backup of your Azure SQL Managed Instance (MI) or other resources using Shared Access Signature (SAS) tokens to Azure Storage accounts and containers, you will typically perform the following steps. The SAS token is a secure way to grant limited access to storage resources without sharing your account key.

Here’s a general process for creating SAS tokens, storing backups in Azure Blob Storage, and automating backups with these SAS tokens:

Steps for Using SAS to Take Backup and Store in Azure Storage:

1. Generate SAS Token for Azure Storage Container

To upload backups (e.g., .bak files) to an Azure Storage container using a SAS token:

a. Azure Storage Account

Ensure that your Azure Storage Account and Container are already created.

b. Create a SAS Token

Azure Portal:

Navigate to your Storage Account.

Go to Containers and select the target container.

Select Shared Access Signature from the left menu.

Set the permissions for the SAS token (e.g., Write, List, Delete, etc.).

Set the expiry time for the token (e.g., 24 hours, 7 days).

Click Generate SAS and connection string.

Copy the SAS URL.

Allow to store the backup at EA tenant itself for easy restore

Let us try to minimize the outage.

Let us keep the server’s name, user id and password same as prod CSP at EA tenant.

**Planned Days:**

Below is our plan and we would be circulating to business stakeholders in advance for the outage etc.

* **Saturday:** Take backups of all databases.
* **Sunday:** Restore the databases in the new SQL MI environment, provided the backup completes on Saturday (subject to network latency).
* **Monday:** Testing of Change the connection setting/on-premises data gateway for some reports, dashboards, ETL processes, etc., to ensure there is no business impact on Tuesday.
* **Tuesday:** Confirm that all ETL processes are running smoothly on both the CSP and EA tenants. Similarly confirm for all reports/dashboard etc.
* **4-week windows for Production Migration:** Slowly we will redirect sources of all data & AI components in a four-week window period and once all are completed and tested then Tech Mahindra team will decommission CSP tenant.

**Conclusion:**

Please note that due to this transition, the entire Cloud Data & AI ecosystem Fabric (CRM dashboard/Lakehouse/ETL/Reports/others 110 + reports/all downstream like CRM/Infinity/Other applications dependent on Azure SQL MI) would be affected. Although we will ensure there is less impact, we might try to redirect everything to the new SQL MI ASAP. In case this activity is not complete on time and for any reason we may communicate to business about the downtime etc.