

Migration Evaluator Agent — Case Study Document

Executive Summary

The **Migration Evaluator Agent** is a specialized automation solution developed by **UnifyCloud** to simplify, accelerate, and secure the migration of virtualized workloads from on-premises environments to **Microsoft Azure**.

The solution addresses one of the most critical modernization challenges faced by enterprises today — migrating legacy infrastructure and virtual machines (VMs) running on **Hyper-V** and **VMware vSphere** to Azure Infrastructure-as-a-Service (IaaS) in a secure, automated, and auditable manner.

This **purpose-built agent** reduces migration complexity through intelligent automation, including **machine scanning, compatibility validation, Azure resource generation, and VM deployment orchestration**. By eliminating manual effort and error-prone processes, it significantly shortens migration timelines, improves reliability, and ensures that each migrated workload adheres to Azure best practices for configuration, security, and governance.

The **Migration Evaluator Agent** supports both **Windows Server** and **Linux** workloads (Ubuntu, CentOS), providing cross-platform flexibility for diverse enterprise environments. It integrates seamlessly with Azure components such as **Azure AD Apps, Blob Storage, and Resource Groups**, leveraging secure authentication and encryption for all data transfers.

Ultimately, this solution empowers IT teams, Cloud Architects, and Migration Specialists to conduct **fast, repeatable, and scalable migrations** from virtualized on-premises systems to Azure — enabling organizations to accelerate their digital transformation journey while minimizing risk and cost.

Audience Personas

1. IT Infrastructure Administrator

Responsible for managing on-premises virtualization environments (Hyper-V or VMware).

- Needs a streamlined migration approach without manual scripting or configuration.
- Benefits from automatic VM scanning, validation, and resource mapping to Azure.
- Gains visibility and control through migration progress tracking and reporting.

2. Cloud Architect / Azure Migration Specialist

Leads the design and execution of cloud adoption or modernization initiatives.

- Requires a secure, repeatable, and scalable migration mechanism that adheres to Azure best practices.
- Uses the Migration Evaluator Agent to orchestrate migrations and validate post-deployment consistency.
- Relies on automation to reduce human error and ensure standardization across workloads.

3. Enterprise IT Manager / CIO

Oversees digital transformation and modernization strategies.

- Focused on cost efficiency, governance, and compliance during the migration process.
- Seeks to minimize downtime and resource dependency.
- Leverages reporting and validation results for executive oversight and audit readiness.

4. Security & Compliance Officer

Ensures adherence to corporate security and data protection policies.

- Evaluates the security posture of migration tools.
- Ensures that authentication mechanisms, data encryption, and Azure AD integration comply with standards.
- Uses the agent's controlled access model and audit trails to maintain compliance assurance.

Business Challenge

Many organizations running workloads on **Hyper-V** and **VMware vSphere** struggle to modernize due to the complexity and risk of migration. Traditional manual migration methods involve multiple disjointed steps — VM assessment, export/import, manual Azure configuration, and post-deployment validation — each prone to error, delay, or data inconsistency.

Common challenges include:

- **Manual and inconsistent processes** leading to extended migration timelines.
- **Complex Azure configuration requirements**, such as virtual network setup, NSGs, public IPs, and disk mappings.
- **Limited validation tools** to ensure migrated workloads perform as expected.
- **Security and compliance risks** due to inconsistent credential handling or lack of encryption.
- **Operational overhead** from coordinating between infrastructure, networking, and security teams.

Enterprises needed a unified, automated, and intelligent solution to **evaluate, validate, and execute migrations** efficiently while maintaining full compliance and control.

Solution Overview

The **Migration Evaluator Agent** is a **low-touch, automated migration accelerator** designed to streamline the movement of virtual workloads from **Hyper-V** and **VMware vSphere** environments to **Microsoft Azure IaaS**.

By combining automation, validation, and secure Azure integration, the solution removes the operational friction typically associated with large-scale migrations. It ensures consistent deployment configurations, preserves VM integrity, and provides post-migration verification to confirm readiness and accessibility.

Core Objectives:

- Automate discovery and evaluation of on-premises VMs.
- Generate Azure resource mappings automatically (VM size, storage, network, security).
- Ensure validated, policy-compliant deployment into Azure.
- Provide audit logs and progress tracking for transparency and governance.

Scope of Migration:

- **Source Platforms:** Hyper-V and VMware vSphere
- **Target Platform:** Microsoft Azure IaaS
- **Supported OS:** Windows Server, Ubuntu, Linux Distributions

This makes it applicable across enterprises modernizing hybrid or private cloud environments and standardizing workloads on Azure.

Architecture Overview

The **Migration Evaluator Agent** is built on a **modular architecture** consisting of four primary layers:

1. User Interface Layer

- The agent runs as a Windows application with administrative privileges.
- Provides an intuitive UI to initiate scans, validate resources, and trigger migrations.
- Displays real-time progress tracking, error logs, and validation results.

2. Orchestration Layer

- Powered by built-in automation routines.
- Handles scanning of source environments (Hyper-V or VMware).
- Executes validation checks — storage availability, guest service status, RDP/SSH accessibility.
- Generates Azure resource specifications and triggers deployment via secure APIs.

3. Data & Document Layer

- Stores validated VM configurations and metadata.
- Manages Azure resource mapping, including VM names, VNet, Subnets, NSG, NIC, and Disk configurations.

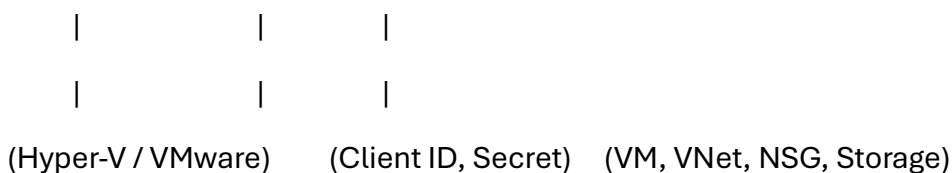
- Uses **Azure Blob Storage** for secure temporary storage during data transfer.
- **Azure Dataverse** (optional) can be leveraged for structured data tracking and reporting.

4. External Integration Layer

- Integrates with **Azure AD Applications** for authentication using **Client ID**, **Client Secret**, and **Tenant ID**.
- Deploys workloads to Azure subscriptions and resource groups securely.
- Ensures encrypted communication between on-premises and Azure environments.

Architecture Diagram (Conceptual):

[On-Prem Host] → [Migration Evaluator Agent] → [Azure AD Auth] → [Azure Subscription]



This architecture ensures modularity, scalability, and compliance with enterprise IT security standards.

Key Features & Capabilities

1. Multi-Platform Migration Support

- Enables migration from both Hyper-V and VMware vSphere environments.
- Supports Windows and Linux guest operating systems.

2. Automated VM Discovery

- Scans all available VMs within the host or vCenter environment.
- Retrieves configuration details including CPU, memory, disk size, and network adapters.

3. Resource Validation

- Ensures adequate storage, connectivity, and guest service availability before migration.
- Checks for RDP (Windows) or SSH (Linux) access readiness.

4. Azure Resource Generation

- Automatically maps VM specifications to Azure equivalents: VM SKU, NIC, VNet, Subnet, NSG, and Public IP.
- Allows custom naming conventions for enterprise consistency.

5. Secure Azure Deployment

- Uses Azure AD App credentials for authentication.

- Deploys directly into target subscriptions and resource groups.

6. Migration Logging and Progress Tracking

- Generates detailed logs for each migration phase.
- Supports audit, troubleshooting, and compliance reporting.

7. Cross-Platform Data Handling

- Transfers VM data securely via Azure Blob Storage.
- Supports encrypted transmission to prevent unauthorized access.

8. Post-Migration Validation

- Confirms VM deployment accuracy and service accessibility in Azure.
- Validates network, disk, and OS configurations post-migration.

Supported Platforms

Source Platform	Supported OS	Deployment Notes
Hyper-V	Windows Server, Ubuntu, Linux	Agent installed directly on host.
VMware vSphere	Windows Server, Ubuntu, Linux	Requires vSphere credentials and IP accessibility.

Prerequisites

- Windows machine with **Administrator rights**.
- Local storage capacity exceeding the total VM size.
- Stable network connectivity between on-premises and Azure.
- **Guest Services** enabled on all source VMs.
- **RDP (Windows)** or **SSH (Linux)** accessibility configured.
- Valid **Azure AD Application credentials**:
 - Client ID
 - Client Secret
 - Tenant ID
 - Blob Storage Connection String
 - Subscription ID
 - Resource Group Name

Migration Workflow

A. Hyper-V Migration

1. Agent Installation

- Install the Migration Evaluator Agent directly on the Hyper-V host.
- Launch with Administrator privileges.

2. Scan and Validate

- Automatically detects all VMs hosted on the Hyper-V machine.
- Performs validation of VM size, network configuration, and guest service availability.

3. Resource Generation

- Generates Azure resource definitions including VM names, IPs, VNet/Subnet mappings, NSG, NIC, and storage.
- Allows name customization and parameter overrides.

4. Azure Credential Configuration

- Input Azure AD App credentials (Client ID, Secret, Tenant ID, Subscription ID, Blob Storage Connection, Resource Group).

5. Migration Execution

- Initiates automated migration with real-time progress updates.
- Transfers data securely to Azure Blob Storage and provisions corresponding Azure VMs.

6. Post-Deployment Verification

- Validates RDP or SSH connectivity for the migrated machine.
 - Confirms alignment with Azure network and resource configurations.
-

B. VMware vSphere Migration

1. Agent Installation

- Install the agent on a Windows machine with sufficient storage.
- Run as Administrator.

2. Connection Setup

- Enter **vSphere credentials** (User ID, Password, vCenter/ESXi IP).
- Validate connectivity via ping and credential verification.

3. VM Scanning

- Discovers all accessible VMs from the vSphere environment.
- Checks accessibility and guest services status.

4. Validation and Preparation

- Validates available storage, RDP/SSH readiness, and guest service configuration.

5. Azure Resource Mapping

- Generates Azure configuration templates and allows custom name overrides.

6. Secure Deployment

- Provides Azure credentials for authentication and deployment.
- Initiates migration and tracks progress with detailed logging.

7. Post-Migration Review

- Confirms migrated VMs' accessibility and resource configuration in Azure.

Post-Migration Validation

After the migration process, the **Migration Evaluator Agent** automatically verifies:

- Proper configuration of **VNet**, **Subnets**, **NSGs**, **NICs**, and **Public IPs**.
- Disks are provisioned as per original VM configuration.
- For Windows machines: **RDP** is enabled and functional.
- For Linux machines: **SSH** access is validated.
- Guest services and network connectivity are tested for operational readiness.

This ensures that every migrated VM is **cloud-ready**, secure, and aligned with enterprise configuration standards.

Security & Compliance

The Migration Evaluator Agent enforces a **secure, role-based, and auditable** migration process through several built-in safeguards:

1. Azure AD Authentication

- Utilizes Azure Active Directory Application credentials (Client ID, Secret, Tenant ID) for authentication.
- Prevents credential exposure or hard-coded access keys.

2. Encrypted Data Transfer

- All data transmissions between on-premises and Azure occur via **Azure Blob Storage** with encryption in transit and at rest.

3. Administrator Privilege Limitation

- Requires administrative privileges only during scanning and migration initiation — reducing exposure risk.

4. Controlled Access

- Access limited to authenticated Azure subscriptions and specific resource groups.

5. Compliance Alignment

- Designed to align with **ISO 27001**, **SOC 2**, and **Azure Security Baseline** principles.

These security measures ensure the solution is enterprise-ready and compliant with stringent data governance standards.

Business Impact & Key Performance Indicators

1. Accelerated Migration Timelines

- Reduces end-to-end migration time by up to **60–70%** compared to manual approaches.
- Automates repetitive configuration and validation tasks.

2. Reduced Operational Costs

- Eliminates dependence on third-party migration consultants for standard workloads.
- Minimizes downtime and resource utilization costs.

3. Improved Accuracy and Consistency

- Automation ensures each migration follows the same validated process, minimizing configuration drift.

4. Enhanced Security and Compliance

- Integration with Azure AD ensures strong identity and access control.
- Encryption of all data streams meets enterprise compliance requirements.

5. Scalable and Repeatable Framework

- Supports bulk migrations with consistent performance.
- Enables IT teams to scale migration projects across business units.

Conclusion

The **Migration Evaluator Agent** represents a significant advancement in enterprise cloud migration automation. By integrating seamlessly with Azure and leveraging the Power of automation and secure authentication, it simplifies complex virtualization transitions into a standardized, repeatable, and auditable process.

For organizations pursuing **cloud modernization**, this solution not only accelerates migration velocity but also strengthens governance, compliance, and operational visibility.