# Migrating Microsoft Workloads to Azure

\*\*\*This OpenHack is currently in preview.\*\*\*

During this OpenHack, your team will assess, migrate, modernize, and optimize existing on-premises applications hosted in Windows Server 2008 R2 and Microsoft SQL Server 2008 R2 as they move to Microsoft Azure in a secure way. While each migration is different, by working through this OpenHack your team will gain the knowledge necessary to perform migrations of applications and VMs that use legacy Windows operating systems to Azure, modernize applications by transitioning from IaaS to PaaS services, and begin to gain insights into application performance and behaviors and how to secure organizational secrets.

Any resemblance to actual scenarios, issues, or pain points that you are facing is \*not\* purely coincidental. The definitions of the challenges that will be presented to you during this event are inspired by real life.

## Context

Contoso Mortgage is a mortgage company that has grown organically and through the acquisition of other lenders and loan-servicing organizations. Over the years, Contoso Mortgage has seen not only its business grow, but also its on-premises presence in their private datacenter. Today, Contoso Mortgage has over 500 servers in their datacenter that are maintained by a lean infrastructure and application support team.

During a recent audit of their on-premises datacenter, several alarming findings were called out. The audit report found that many business-critical workloads for Contoso Mortgage are running on aging infrastructure that is rapidly approaching its end of support date, and in some cases, already past that date. These discoveries apply to both physical hardware and software such as operating systems and include workloads running on Windows Server 2008 R2. Contoso Mortgage also leverages virtualization within their datacenter, using Hyper-V as a hypervisor for many workloads. Even virtualized systems were found to be out of support or nearing the end of support during the audit. This is a matter of serious concern and Contoso Mortgage's management wants to take steps to mitigate the risk they are facing with immediate effect to bring themselves back into a supported state.

Contoso Mortgage has a longstanding relationship with Microsoft and is a current enterprise customer with an established Enterprise Agreement. Your team represents the migration project team for Contoso Mortgage. You have been tasked with evaluating the processes and tooling that can be used to assess, test, and eventually migrate the workloads to Microsoft Azure.

Public cloud computing is still a new concept to Contoso Mortgage's infrastructure and application support teams. While their existing applications are known to run on-premises, moving to a public cloud infrastructure is inherently complex due to the number of existing servers, applications, and the lack of knowledge around what it will take to move everything to Microsoft Azure. Also, Contoso Mortgage does not have access to the source code for many of its applications. This introduces risk as applications that are not well documented and cannot be updated to accommodate new platforms are migrated to the cloud.

To validate that Microsoft Azure will be able to accommodate Contoso Mortgage's existing servers and applications, a collection of servers has been identified by IT leadership and the business which are representative of Contoso's on-premises estate. While these servers are representative of the current on-premises estate, they are also an existing production system that is critical to the business.

Business drivers for this effort include:

- Limiting risk. While the applications selected for this migration effort are representative of Contoso Mortgage's on-premises estate, the are also production systems.

- Extend in a stable way. Without access to the source code, the applications cannot be easily modified and are considered stable today. Stability during and after the migration is critical and cannot come at the cost of modernization.

IT leadership's goals for this initial migration to Azure include:

- Validate the migration of workloads hosted on legacy Windows operating systems including Windows Server 2008 R2, and Windows Server 2012 R2, as well as systems hosted on Microsoft SQL Server 2008 R2, to take advantage of the additional time offered for vendor support.

- Modernize systems to improve availability and resiliency where possible within the timelines needed for rapid migration. While the overarching goal is to rehost existing systems, where meaningful improvements can be made, they should be.

- Investigate the potential modernization of application components by evaluating and eventually transitioning to platform services where possible \*after\* issues around vendor support have been addressed.

- Educate the business and Contoso Mortgage's management on the processes and tooling that can be used to eventually move the remaining servers to Microsoft Azure, drastically reducing their on-premises presence.

While each workload will undeniably be different due to different technologies and dependencies, the discovery in this exercise will help to instill a set of practices that can be used to move the remainder of Contoso Mortgage's on-premises estate into Microsoft Azure reliably and predictably.

## Architecture

Contoso Mortgage uses a pair of on-premises web applications to service loan applications today. The first application, \*\*Contoso Mortgage\*\*, is a public-facing website where customers can make requests for mortgages, check the status of their mortgage application, and learn more about the company's offerings. In addition to the public website, Contoso Mortgage also operates a website known as \*\*Contoso Mortgage Admin\*\*, that is only accessible to employees with domain credentials, where loan officers and other employees process customer mortgage applications.

Throughout the migration of these applications, downtime must be minimized to lessen the impact to Contoso Mortgage's customers. Where possible, Contoso Mortgage would like to adopt cloud principles and transition from traditional Infrastructure-as-a-Service (IaaS) to Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) offerings.

\*\*Your mission, should you accept it, is to not only migrate the existing applications to IaaS but also to prepare to modernize the applications by transitioning to PaaS services where possible, while keeping the applications functional.\*\*

The success of your team depends on your ability to perform the migrations and minimize the downtime of your applications.

### On-premises architecture

Contoso Mortgage currently hosts \*\*Contoso Mortgage\*\* and \*\*Contoso Mortgage Admin\*\* on various versions of Windows Server in virtual machines on Hyper-V. The virtual machines are on a single host. Each application consists of a web tier, an application (API) tier, and a shared data tier utilized by both the public-facing and employee-facing sites. Except for the shared data tier, each application tier resides on its own virtual machine.

The application tiers are segmented and constrained in communication through Windows Firewall. The web front ends are accessible over port 80 and 8080 to end-users and are not using SSL at this time. The application tier is only accessible over port 2901 by the respective application server, and the database tier is only accessible by the application tiers over port 1433.

The public-facing application, \*\*Contoso Mortgage\*\* (or \*\*CM\*\*), is an ASP.NET MVC web application with a Microsoft SQL Server backend that leverages forms-based authentication (FBA) for customer logins. The internal application, \*\*Contoso Mortgage Admin\*\* (or \*\*CMA\*\*), is also an ASP.NET MVC web application with a Microsoft SQL Server backend. \*\*CMA\*\* leverages integrated Windows authentication (IWA) to allow employees to access the site.

The following diagram shows the application server architecture:

![Application server architecture](images/application\_server\_architecture.png)

Each server in the production environment is domain-joined. Administrators of the environment do not connect from the public internet and access the guest virtual machines through an internal network. The following diagram shows the existing guests on the Hyper-V host.

![Hyper-V guest architecture](images/hyperv\_server\_architecture.png)

The current guests are as follows:

| Server name | Operating system | Purpose |

| ----------- | ---------------------- | --------------------------------------------------------------------------------------------------------- |

| \*\*cmad1\*\* | Windows Server 2012 R2 | Primary Active Directory Domain Controller |

| \*\*cmaweb1\*\* | Windows Server 2008 R2 | Web front-end for \*\*Contoso Mortgage Admin\*\* (Employee-facing) |

| \*\*cmaapp1\*\* | Windows Server 2008 R2 | Application front-end for \*\*Contoso Mortgage Admin\*\* (Employee-facing) |

| \*\*cmdb1\*\* | Windows Server 2008 R2 | Shared database server running SQL Server 2008 R2 for \*\*Contoso Mortgage\*\* and \*\*Contoso Mortgage Admin\*\* |

| \*\*cmid1\*\* | Windows Server 2016 | Non-provisioned server |

| \*\*cmweb1\*\* | Windows Server 2008 R2 | Web front-end for \*\*Contoso Mortgage\*\* (Customer-facing) |

| \*\*cmapp1\*\* | Windows Server 2008 R2 | Application front-end for \*\*Contoso Mortgage\*\* (Customer-facing) |

| \*\*cmvpn1\*\* | Windows Server 2016 | Hosts Routing and Remote Access Services (RRAS) |

- The server \*\*cmid1\*\* was created for a previous project at Contoso Mortgage, but was not used. It is a standard installation of Windows Server 2016 Datacenter and has no additional software or roles deployed. The server is currently \*not\* domain-joined.

- The server \*\*cmvpn1\*\* was created by Contoso Mortgage's Network Operations team to establish a site-to-site VPN between Azure and Contoso Mortgage's on-premises environment. While the server has been provisioned, domain-joined and the RRAS role has been installed, it has not yet been configured.

The Hyper-V host itself has 16 cores and 64GB of memory. All the guests are attached to the same internal switch, \*InternalNATSwitch\*. The following table shows the current allocations of CPU and memory across the existing guests and other configuration details.

| Server name | Virtual CPUs | Memory (GiB) | IP Address |

| ----------- | :----------: | :----------: | :---------: |

| \*\*cmad1\*\* | 1 | 4 | 192.168.0.2 |

| \*\*cmaweb1\*\* | 1 | 4 | 192.168.0.4 |

| \*\*cmaapp1\*\* | 1 | 4 | 192.168.0.5 |

| \*\*cmdb1\*\* | 2 | 8 | 192.168.0.3 |

| \*\*cmid1\*\* | 1 | 2 | 192.168.0.8 |

| \*\*cmweb1\*\* | 1 | 4 | 192.168.0.6 |

| \*\*cmapp1\*\* | 1 | 4 | 192.168.0.7 |

| \*\*cmvpn1\*\* | 1 | 2 | 192.168.0.9 |

The server \*\*cmad1\*\* also functions as a DNS server for all the VM guests. The following records are configured in the contosomortgage.local forward lookup zone. The application relies on these records to function (\*e.g.\* the web application \*\*Contoso Mortgage\*\* is explicitly configured to communicate with the application server at <http://api.contosomortgage.local>.)

| Name | Record type | Value |

| ------------ | :---------: | :----------: |

| \*\*adminapi\*\* | A | 192.168.0.5 |

| \*\*api\*\* | A | 192.168.0.7 |

### Cloud architecture

Contoso Mortgage currently has an existing Azure subscription and Azure Active Directory tenant. Within the tenant, there are only cloud users. Those cloud users are used to secure resources in Azure.

\*\*\*You are encouraged to use the provided logins and explore the existing infrastructure. Contoso Mortgage may already be using services which you can use as building blocks throughout this OpenHack.\*\*\*

--------------

## Cheat sheet

In this section, you will find a list of hints to help you get started with the technologies used during the Migration OpenHack.

### Obtaining the credentials of your team environment

1. Navigate to the \*\*OPEN HACK ENVIRONMENT\*\* tab.

2. The usernames and passwords provided can be used to access your Azure subscription.

### Connecting to the public-facing application

1. Navigate to the \*\*OPEN HACK ENVIRONMENT\*\* tab.

2. The usernames and passwords provided can be used to access your Azure subscription.

3. Search for the resource \*\*cmhostip\*\*. The FQDN of the resource can be used to access both the anonymous and Windows authenticated sites on port 80 and port 8080 respectively. The FQDN will be formatted as \*\*cmfinance\[unique string\].\[region\].cloudapp.azure.com\*\*. For example:

- Customer-facing site (\*\*Contoso Mortgage\*\*): \*\*cmfinancep24roka67fyjo.southcentralus.cloudapp.azure.com\*\*

- Employee-facing site (\*\*Contoso Mortgage Admin\*\*): \*\*cmfinancep24roka67fyjo.southcentralus.cloudapp.azure.com:8080\*\*

### Connecting to the Hyper-V host

1. Navigate to Azure and the \*\*openhackonpremrg\*\* resource group.

2. Select the virtual machine \*\*cmhost\*\*.

3. Use the public IP of the host to RDP to the server.

### Connecting to the Hyper-V guest virtual machines

RDP is enabled on each guest. The guests are accessible from the host through their private IP address.

#### Host credentials

The Hyper-V host, \*\*cmhost\*\*, can be accessed with the following credentials:

- Username: \*\*demouser\*\*

- Password: \*\*demo@pass123\*\*

A set of additional credentials is also provided if more than one user needs to connect to the host at the same time. The additional login names are:

- Username: \*\*demouser2\*\*

The password for all these accounts is:

- Password: \*\*demo@pass123\*\*

### Domain credentials

The virtual machines on the Hyper-V host that are domain-joined can be accessed with the following credentials:

- Username: \*\*CONTOSOMORTGAGE\\Administrator\*\*

- Password: \*\*demo@pass123\*\*

All the accounts in the domain share the same password (\*e.g.\* user accounts in the \*Azure Users\* OU):

- Password: \*\*demo@pass123\*\*

The virtual machines on the Hyper-V host that are non-domain-joined can be accessed with the following credentials:

- Username: \*\*.\\Administrator\*\*

- Password: \*\*demo@pass123\*\*

### Database credentials

The existing database instance has several accounts enabled.

- Administrative account

- Username: \*\*sa\*\*

- Password: \*\*demo@pass123\*\*

- Application account

- Username: \*\*financeUser\*\*

- Password: \*\*financeAdmin001!\*\*

### Application configuration

Each API server has two connection strings in the \*connectionStrings\* element of the \*\*web.config\*\* for the site:

```xml

<connectionStrings>

<add name="ContosoFinance" connectionString="Server=[databaseserver];Database=contosomortgagedb;User Id=[user id];Password=[password];MultipleActiveResultSets=False;Connection Timeout=30;" providerName="System.Data.SqlClient" />

<add name="ContosoIdentity" connectionString="Server=[databaseserver];Database=contosomortgageidentity;User Id=[user id];Password=[password];MultipleActiveResultSets=False;Connection Timeout=30;" providerName="System.Data.SqlClient" />

</connectionStrings>

```

Each web front end has an \*appSettings\* key called \*\*ApiBaseUrl\*\* in the \*\*web.config\*\* which defines the API server URL:

```xml

<appSettings>

<add key="webpages:Version" value="3.0.0.0" />

<add key="webpages:Enabled" value="false" />

<add key="ClientValidationEnabled" value="true" />

<add key="UnobtrusiveJavaScriptEnabled" value="true" />

<add key="ApiBaseUrl" value="http://[api url]:2901/" />

</appSettings>

```

## References

- <a href="https://go.microsoft.com/fwlink/?linkid=872689" target="\_blank">Migration Guide for Windows Server</a>

- <a href="https://www.microsoft.com/cloud-platform/windows-server-2008" target="\_blank">Prepare for Windows Server 2008 end of support</a>

## Glossary

### Infrastructure-as-a-Service

Infrastructure-as-a-Service (<a href="https://azure.microsoft.com/overview/what-is-iaas/" target="\_blank">IaaS</a>) is an instant computing infrastructure, provisioned and managed over the internet. It's one of the four types of cloud services, along with Software-as-a-Service (<a href="https://azure.microsoft.com/overview/what-is-saas/">SaaS</a>), Platform-as-a-Service (<a href="https://azure.microsoft.com/overview/what-is-paas/" target="\_blank">PaaS</a>), and <a href="https://azure.microsoft.com/overview/serverless-computing/" target="\_blank">serverless</a>.

IaaS quickly scales up and down with demand, letting you pay only for what you use. It helps you avoid the expense and complexity of buying and managing physical servers and other datacenter infrastructure. Each resource is offered as a separate service component, and you only need to rent a particular one for as long as you need it. A cloud computing service provider, such as Azure, manages the infrastructure, while you purchase, install, configure, and manage your software including operating systems, middleware, and applications.

### Platform-as-a-Service

Platform-as-a-Service (<a href="https://azure.microsoft.com/overview/what-is-paas/" target="\_blank">PaaS</a>) is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications. You purchase the resources you need from a <a href="https://azure.microsoft.com/overview/choosing-a-cloud-service-provider/" target="\_blank">cloud service provider</a> on a pay-as-you-go basis and access them over a secure Internet connection.

Like <a href="https://azure.microsoft.com/overview/what-is-iaas/" target="\_blank">IaaS</a>, PaaS includes infrastructure - servers, storage, and networking - but also middleware, development tools, data services, database management systems, and more. PaaS is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating.

PaaS allows you to avoid the expense and complexity of buying and managing software licenses, the underlying application infrastructure and middleware, or the development tools and other resources. You manage the applications and services you develop, and the cloud service provider typically manages everything else.

### Azure Active Directory

Azure Active Directory (<a href="https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-whatis" target="\_blank">Azure AD</a>) is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access the following resources:

- External resources, such as Microsoft Office 365, the Azure portal, and thousands of other SaaS applications.

- Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.