ACME Corporation
Cloud Migration Assessment

Executive Summary

At the request of ACME Corporation, iCorps performed a cloud migration assessment. This consisted of an examination of ACME Corporation's server and network infrastructure, collecting data about their use of Active Directory and domain services, as well as interviews around the company goals and challenges faced in their current environment.

iCorps has partnered with Microsoft to fund this cloud migration assessment. Microsoft's Azure cloud service presents one option in migrating ACME Corporation's services to a public cloud. Although Azure is presented prominently throughout the assessment, this output can be used with any cloud service – Azure, AWS, or Google Cloud.

A Migration Assessment looks at your current use of IT systems and determines how it can be best managed in a cloud environment. It is not in the scope of this document to look at reengineering the processes and services being used by the subject business to fit them into specific cloud services.

ACME Corporation currently has their server infrastructure housed with a third-party provider, Private Cloud Inc. Servers are managed by an outside Managed Service Provider (MSP) for patching and maintenance. They report that they have no issues with Private Cloud Inc. and in fact are happy with their services. Pricing is a-la-carte so it stays level with their needs, service is good and a lot of expenses (licensing, backups, anti-virus) are bundled in saving management overhead and vendor management time.

This engagement explores the options in public cloud infrastructure and looks at how the scalability and extensibility of Microsoft's Azure are a good option both as cost control and operationally.

Methods and Sources

iCorps Technologies conducted video conference interviews on January 1st and followed up with email questions and answers. In addition, iCorps was granted remote access via Team Viewer, to the ACME Corporation Active Directory and admin access to systems. During the remote session proprietary tools were used to collect data about the network, servers, and Active Directory.

Considerations

Some items are difficult to capture accurately because of impending change in the environment. It is understood that the 'CRM' application is being migrated to a SaaS product. Because the timeline of a cloud migration and the application migration may cross, and either's deadlines may slip, we present costs and migrations for pre-CRM migration that includes the web, database and test/QA servers, and post-CRM migration that does not.

Additional items to be addressed are ancillary services currently provided by Private Cloud Inc. Private Cloud Inc. is providing Windows licensing in the form of Windows Datacenter licenses, backup services and anti-virus for hosted virtual machines.

The decision to re-home your infrastructure services is not one to be taken lightly. There are many considerations to be made.

A major consideration is how much control of their environment ACME Corporation wishes to exert. ACME Corporation is currently in a hosted platform where changes are managed for them. Private Cloud Inc. manages licensing, back-ups, and anti-virus. They further use a Managed Service Provider (MSP) to monitor and manage patching and security.

The decision around how much direct management you should retain of your infrastructure and how much should be outsourced is an operational decision that is very personal. Some choose best in breed and prefer to have their internal staff manage vendors, and other choose to keep things in house and maintain direct management control. Neither is a better solution, just different.

Commented [JSL1]: political decision, how about operational decision

While it may seem that direct cost is the one driving factor in deciding the level of outsourcing to purchase, there are many hidden costs in moving away from managed services. Personnel costs in time to manage all the components being moved are real and while you may be staffed for it, the opportunity cost of what other tasks they are currently performing need to be accounted for.

That said, there are likely considerable cost savings to be found. ACME Corporation can also regain a large amount of control of their services by moving away from a full-service provider to a public cloud.

Recommendations

Based on the above, and the component level technical aspects in the body of this document, iCorp's recommendation is primarily a forklift move of your infrastructure from Private Cloud Inc. to Azure.

While there are many options in the components of your systems – Directory, database, virtual machines, and file storage – your complex use of AD, number of legacy applications and the sake of office resiliency make this the right choice.

Costs

We estimate that MRC for your current servers including the CRM software and without are below for both pay-as-you-go and for 1 year commitments on the VMS. The investment for iCorps to perform the migration for you as a service is approximately $23,000.

	Pay as you Go	1 Yr Commitment
MRC including CRM	$ 4,892.57	$ 4,177.20
MRC post CRM migration	$ 3,681.92	$ 3,275.36

Commented [JSL2]: seems very small is this become of the storage vs the vm discount?

Commented [JT3R2]: Probably, the details are in a spreadsheet in the teams site if you want to see how it breaks out.

Cloud Assessment

Appropriateness of Public Cloud

Given ACME Corporation's current hosting in a private cloud (Private Cloud Inc.), a move to a public cloud like Azure is highly appropriate.

Moving to a public cloud grants advantage

- Pricing – Public cloud infrastructure is typically less expensive than private cloud. This is tempered somewhat by more aggressive management by the private provider, but that is a double-edged sword.
- Control - Public cloud offers more control over all the aspects of your environment because they are mostly self-managed. You do not need to engage the provider to adjust resources or networking for your cloud services. Or to check on anti-virus portals, or to manage backup schedules
- Flexibility – Cost savings can be found by turning off machines when not in use in a public cloud. Azure charges by the hour for 'pay as you go' pricing which makes it useful to turn off Dev and QA servers when not in use.

Licensing Implications

Current licensing for ACME Corporation is a combination of owned (SQL) and subscription (Server Datacenter). The ability to continue with subscription licensing is possible using cloud services which maintains it as operating expense instead of a periodic capital expense.

In the pricing calculation we've included Windows licensing included in the virtual machine subscription. There are some minor savings that can be had by buying a copy of Windows Server Datacenter with Software Assurance which permits you to take a discount called 'BYOL' or bring your own license. But it only makes sense at the higher volume while you're keeping CRM in place.

With the CRM servers in place, the ROI is 24 months (Savings of $450 per month vs approximately $10,500 to purchase the license = payback in 23.8 months). With CRM being moved to SaaS, the ROI is extended to over 45 months and is beyond the point where it is worthwhile (<36 months, the lifetime of the Software Assurance without additional payments).

There is no achievable ROI on buying SQL vs buying rights in the virtual machine subscription.

AWS vs Azure

Comparing the two most prominent cloud providers can prove tricky because of differences in billing practices and terminology in describing their respective products.

However, comparisons exist by experts and can be found in sites like this: https://cloud.netapp.com/blog/azure-vs-aws-pricing-comparing-apples-to-apples-azure-aws-cvo-blg

In practice Azure has the advantage of price, and flexibility in how existing licenses can be leveraged and combined with embedded cloud licensing. Without a large infrastructure that you can leverage for savings at AWS, Microsoft's Azure is a clear leader on price.

Local AD Domain vs Azure Active Directory vs Azure Active Directory Domain Services

Local (on-premise) Active Directory has the advantage of being a full feature product. Its use at ACME Corporation is fully implemented and mature. While Azure Active Directory Domain Services has an expanding feature set, it has not yet reached the richness of the local version. It also complicates matters in branch offices when the inevitable network issues do occur.

Your current architecture is Active Directory Domain Services. You have redundancy at each location in a domain controller, domain name service (DNS), and copies of the policies that get applied to users and computers (Group Policy and logon scripts in SysVol). In the event of internet outages your local users can still authenticate to log on to their computers, be protected by the group policies that apply to them and have local name resolution to let them find site related resources like printers and scanners and local access or security systems.

Local AD provides a safety net in local domain controllers that can authenticate users and services in the event of a network outage versus relying on a vpn to reach the directory to find a local printer, for example.

Migrating to an Azure AD Domain Services (as a Service, AADDS) would necessitate eliminating the redundancy in on-prem services and has a hard requirement of VPN or ExpressRoute (a dedicated line that accesses Azure). There are 'as a service' analogs to DNS and a limited set of group policy attributes, but they require perpetual connections to work because they only reside on your Azure virtual network. DNS at your local offices would simply relay to the AADDS DNS across your VPN via conditional forwarding.

Azure AD is entirely inappropriate as a replacement for AD at ACME Corporation. You are currently using it in a hybrid fashion with your email and office subscriptions. Azure AD (without the DS) is an Identity as a Service offering that is intended strictly for access across the internet and does not have the domain services aspect of name services or the breadth of policy that can be applied. While it does allow some device management through Intune, it's really designed only for mobile and remote device use and managing authentication, and falls short of the granularity you use in your configuration including security log management, browser settings and domain based certificate authority transactions.

Because of how ACME Corporation uses group policy so extensively and how they already have local domain controllers for local authentication, it would be advisable to stick with the on-premise version currently used. This can be extended into Azure with a domain controller VM in their subscription.

Commented [JSL4]: Do you have a list of GPO? Could Intune manage the workstations? Create and manage group policy in Azure AD Domain Services | Microsoft Docs what about making computers Azure AD joined, and manage GPO, then moving them to 100 Azure AD and Intune?

Keep in mind this is about movign them to cloud vs why not.

Backup Considerations

Backups for ACME Corporation's implementation in Private Cloud Inc. consists of a limited number of daily copies at Private Cloud Inc. and copies sent to an office. This service is included in the Private Cloud Inc. package.

For backups, we've included our Guardian Service in this estimate. It is a virtual device from Datto that resides in your Azure tenant. It will keep backups for 1 year at a frequency that you set per server (unlimited retention is available). Management computers may only need daily backups, but your SQL server may need hourly (or more frequent) log backups. These would be configured after a risk analysis/data classification exercise.

Commented [JSL5]: I dont think this is approrate. if we move them to the cloud, guardian is not an option at all. We should be talking about azure backup and site recovery

Commented [JT6R5]: Ok, I'll reprice that way

Datto has the granular ability to restore whole VMs, individual SQL logs, individual AD objects, or any or all of a file system.

SQL

The majority of database services used at ACME Corporation is in the CRM database. There are other smaller databases for various pieces of software. The current version is 2012 R2.

Rehoming SQL is a developer task. The considerations are SQL version, software and client authentication and data connections and what business logic is handled by the database and what is coded in the application. Due to the sunsetting nature of CRM, and the varied nature of the very small databases remaining, the recommendation is to not attempt to convert these to one of the database-as-a-service offerings. The time and effort to do the testing, potential compatibility updates and migration far outweigh the benefit. At such small scale, the VM pricing is advantageous regardless.

Networking

ACME Corporation uses Meraki for SD Wan currently so this recommendation continues that relationship. The vMX100 virtual networking appliance creates a connection into Azure that is managed through the Meraki portal just like their other devices. Capabilities are just like their other offices and management and VPN configuration should feel familiar and comfortable.

The vMX100 is costed in two parts, the Meraki Cloud license and the Azure VM it runs in. Both are included in the cost estimate. Data egress costs are estimates, it is a difficult number to capture in advance. The estimate is based on a ~3x multiplier of the database and file storage volume.

Notes from Discovery

- Functional level of forest is 2008 R2, this can come up to 2012 R2 with your currently installed DCs
- Upgrade DCs to 2019 as part of integration with cloud will help with PowerShell compatibility with Azure and the licensing is included.
- Password policy resets lockout at 10 min, this is convenient but insecure
- Windows firewall are off with group policy and enforced
    - Let your anti-virus software turn off the Windows firewall and deploy its own. So, if a/v gets disabled by malware or a machine is overlooked in the deployment it will still have something
- Domain recycle bin is not enabled
- There are 129 enabled user accounts that haven't logged in for over 90 days. While the vast majority of these are service and resource accounts (conference rooms), there are a number that are users with non-expiring passwords

Migration to Public Cloud

Migration Strategy

In looking to migrate to Azure, timing will make many differences. The CRM application is being migrated to a SaaS service. If your confidence in that date is high, then it may be worth holding off on a cloud migration until that is complete to avoid spending resources on migrations that have a short shelf life. If those dates look like they might slip, then the cost savings in the new environment will compensate for the migration costs for the additional VMs that need to be moved.

For choosing how to migrate VMs, we determined whether to forklift (move the VM as is) or migrate to a new OS based on the operating system. Anything older than 2016 was slated to be migrated to a new OS.

There are opportunities to save some costs with licensing you have already. In order to qualify you must have software assurance. The cost savings are below the costs labeled 'BYOL Savings'. It may not be worthwhile to purchase licensing for this benefit if the CRM software servers will be short lived as it would take 42 months to recoup the cost of Datacenter licensing with software assurance.

To calculate the migration costs as a service from iCorps, we used 4 hours to forklift a server (not including upload time, we would set those up to copy overnight or over a weekend) and 8 to do a clean install and migrate data and services.

Server Matrix

"Servers"	Windows Server 2019	Azure Net New	B2MS 2 vCore/8 g Ram 128g SSD
1	Windows Server 2016 Datacenter	Azure Forklift	B2MS 2 vCore/8 g Ram 128g SSD
2	Windows Server 2019 Datacenter	Azure Forklift	B2MS 2 vCore/8 g Ram 128g SSD
3	Windows Server 2016 Datacenter	Azure Forklift	B2MS 2 vCore/8 g Ram 128g SSD
4	Windows Server 2019 Datacenter	Azure Forklift	B4MS 4 vCore/16 g Ram 512g SSD
5	Windows Server 2019 Datacenter	Azure Forklift	B2MS 2 vCore/8 g Ram 128g SSD
6	Windows Server 2012 R2 Datacenter	Azure Forklift	DS4 v2 8 Core/28 g Ram 2@ 512g SSD SQL
7	Windows Server 2012 R2 Datacenter	Azure Forklift	B4MS 4 vCore/16 g Ram 512g SSD x 80 hrs
8	Windows Server 2012 R2 Datacenter	Azure Forklift	B4MS 4 vCore/16 g Ram 512g SSD
9	Windows Server 2012 R2 Datacenter	Azure Forklift	B4MS 4 vCore/16 g Ram 512g SSD x 80 hrs
10	Windows Server 2019 Standard	Azure Forklift	B2MS 2 vCore/8 g Ram 128g SSD
11	Windows Server 2012 R2 Datacenter	Azure Install and Migrate	DS2 v3 2 Core/8 g Ram 2@ 128 g SSD SQL
12	Windows Server 2012 R2 Datacenter	Azure Install and Migrate	B4MS 4 vCore/16 g Ram 512g SSD x 80 hrs
13	Windows Server 2012 R2 Datacenter	Azure Install and Migrate	B4MS 4 vCore/16 g Ram 512g SSD x 80 hrs
14	Windows Server 2012 R2 Datacenter	Azure Install and Migrate	B4MS 4 vCore/16 g Ram 512g SSD
15	Windows Server 2012 R2 Datacenter	Azure Install and Migrate	B2MS 2 vCore/8 g Ram 128g SSD
16	Windows Server 2012 R2 Datacenter	Azure Install and Migrate	B4MS 4 vCore/16 g Ram 512g SSD
17	Windows Server 2012 R2 Datacenter	Azure Install and Migrate	B2MS 2 vCore/8 g Ram 128g SSD
18	Windows Server 2019 Standard	Denver On-Prem	

Commented [JSL7]: Why move this, Azure has its own cert services

19	Windows Server 2008 R2 Standard	Denver On-Prem
20	Windows Server 2012 R2 Datacenter	Merge into Azure DC
21	Windows Server 2012 R2 Datacenter	Merge into Azure DC
22	Windows Server 2012 R2 Datacenter	Off
23	Windows Server 2012 R2 Datacenter	Off
24	Windows Server 2008 R2 Standard	Off
25	Windows 10 Pro	Off
26	Windows Server 2008 R2 Standard	Off
27		Off
28	Windows 7 Professional	Off
29	Windows Server (R) 2008 Standard	Off
30	Windows Server 2012 R2 Datacenter	Upgrade into CLD-DC1
31	Windows Server 2008 R2 Standard	Windham On-Prem
32	Windows Server 2019 Standard	Windham On-Prem
33	Windows Server 2012 R2 Datacenter	Off

Azure Costs

Category	Pay-As-You-Go	1 Yr Reserved
vMX100 Meraki Licensing	$ 134.00	$ 134.00
vMX100 Azure VM (D2 v2, IP and disk)	$ 113.24	$ 113.24
Bandwidth/Data Egress 2T/mo	$ 176.00	$ 176.00

Compute & WAN Totals/mo incl CRM	$ 3,793.57	$ 3,078.20
Compute & WAN Totals/mo no CRM	$ 2,582.92	$ 2,176.36
Backup - iCorps Guardian	$ 1,099.00	$ 1,099.00
MRC including CRM	$ 4,892.57	$ 4,177.20
MRC post CRM migration	$ 3,681.92	$ 3,275.36
BYOL Discount (CRM)	$ 449.24	
BYOL Discount (Post-CRM)	$ 236.08	

Migration Expense

Type	Number	Hours/per	Total
Forklift Moves	10	4	40
Install and Migrate	7	8	56
Net New	1	8	8
		Hours	104
		Rate	$ 220.00
		Migration Costs	$ 22,880.00