Is the cloud in your future?

Why and how to plan your cloud migration

Introduction

For many organizations, a move to the cloud is inevitable. According to one survey of North American businesses, 95 percent of respondents said their organizations have migrated critical applications and IT infrastructure to the cloud over the past year.[1] Another survey reported that respondents anticipate 80 percent of their infrastructure will be on cloud within an average of 14 months.[2]

What is driving this push toward the cloud? Organizations recognize that the cloud can deliver a range of important benefits, from increased flexibility and scalability to a shift in the cost model from capital expenditures to operating expenses.

Unfortunately, too many migration teams dive in before they completely understand the scope of the work. Without sufficient preparation, they often run into significant issues that result in stalled projects and costly rework.

Should your organization migrate applications to the cloud? And if so, how do you start your cloud journey?

Before undertaking a migration to cloud, keep the following considerations top of mind:

- Is the cloud right for your business?
- Which applications should you migrate?
- What is the right approach for each application migration?
- How will you secure each application and its data?
- How will you manage and maintain the application after migration?

By fully evaluating your options and taking the time to complete the planning process, you can improve your odds for a successful migration and maximize the benefits of the cloud.

Stages of a successful cloud migration

1. Evaluate your options
2. Plan early and thoroughly for your unique business case
3. Migrate
4. Continue innovating on cloud
5. Operate and maintain

For more details about these stages, including use cases, visit ibm.com/cloud/migration

Is the cloud right for your business?

Why move your applications to the cloud? Running applications on the cloud gives you greater agility because it offers IT resources on demand. On-premises solutions require additional steps to consume similar resources.

You can also reduce capital expenditures and avoid buying new servers to run your applications, instead shifting to an operating expenses model in which you pay as you go. In addition, you can scale up (or back) while paying only for what you use. You can accommodate short-term usage spikes without having to buy new servers and then leaving them underutilized when demand ebbs.

Moreover, you can take advantage of the latest hardware technologies without having to purchase new equipment. As your cloud provider upgrades its hardware, your applications benefit.

In most cases, you can also enhance security. The cloud can offer a number of security options throughout the stack, from physical hardware and networking to software and people.

There's enormous value in migrating your applications to the cloud, but the advantages can be difficult to explain to stakeholders who don't work closely with your organization's technology. Learn more about how your organization can benefit from migrating one or more applications to the cloud. Then come back to this white paper and learn how to plan a successful migration.

Will this application be better on the cloud?

Cloud migration can be a time- and resource-intensive process. Be sure there is a real benefit to hosting your applications on the cloud before you move them. Evaluate every application in your portfolio and ask: "Will this perform better, be more secure or be more effective in the cloud?"

If the initial answer is "no," consider whether any parts of the application could benefit from being on the cloud. You could replace those parts with a third-party Software-as-a-Service (SaaS) offering. For example, you could replace a homegrown mail server or a clunky on-premises database with a cloud equivalent to support an otherwise on-premises application.

Moving parts of an application to the cloud can help with short-term scaling. You might have an application with low utilization during some parts of the year and heavy utilization during other parts of the year. You can benefit from cloud scaling, which enables you to add or remove cloud computing resources as you need them. The replacement approach may initially cost more, but partnering with an established cloud vendor can provide stability and reliability, and reduce the migration and maintenance burden on IT.

Determining when cloud is not the answer

If no part of the application gets a boost from the cloud, don't force the issue. You may have some applications that contain very sensitive information or have specific usage or compliance restrictions that are better suited to on-premises environments. For example:

- Applications that require a USB key or dongle
- Applications that need to be used in environments where Internet access is not available or used on air-gapped networks
- Data sets with legal requirements to stay on-premises

You don't have to relegate these applications to a permanent on-premises existence. As the security, performance and economy of the public cloud improves, there will be fewer reasons to leave an application on-premises.

Which applications should you migrate?

Before beginning any migration, understand what you're moving and why. Your overarching cloud migration strategy should be based on how many applications you intend to move: Are you moving a single application or shared resource, such as a database or mail server? A cluster of related applications? Your entire portfolio?

Look beyond your current goals. You might be migrating a single application today, but intend to eventually lift everything to the cloud. Though migrating more applications at once increases the effort, performing a single migration with all your applications that share services or data saves rework and limits incompatibility. You'll help ensure all of the applications function as expected in the cloud when they're deployed at the same time.

Single application migration

You might decide to move a single shared resource to the cloud to take advantage of performance scalability while keeping the rest of your portfolio on premises. As you create your hybrid environment, map how users and other applications interact with the application to avoid breaking workflows. You'll also avoid a clumsy migration with absent data sources, unfulfilled dependencies or confusing new access protocols.

When migrating a single application, you have two primary options for managing data transfer in the resulting hybrid environment. Use a VPN to create a secure line between your cloud application and your on-premises portfolio. Or use a secured API to automatically read and write data between the two platforms. Adopting single sign-on federation will let users seamlessly connect in the new environment.

Linked application migration

If you need to migrate a suite of applications or a set based around a single workflow, your biggest challenge is managing the order in which you roll out your applications to limit dependency issues. It might seem safest to hold rollover until you've migrated all the applications, but doing so isn't always possible.

If you need to retire on-premises applications fast, start with the application that has the largest number of dependencies and work your way to those with the fewest. This approach will reduce the amount of rework, as the number of shared services to migrate will shrink until all are hosted on the cloud.

Full portfolio migration

When you're moving applications to the cloud, your biggest challenge is minimizing downtime. You're balancing risk tolerance with speed. Profiling your application portfolio is crucial for determining which applications will benefit most from the cloud and should get resource priority, and which are less strategic and can be rehosted to save cost and effort. Careful testing prior to cutover should reduce the overall risk of a mass migration. But be prepared with a contingency plan in case any dependencies are missed.

American Airlines: Lifting legacy software to the cloud

Challenge: American Airlines wanted a stable, cost-efficient way to expand its digital presence, meeting customer expectations for instant access to information.

Solution: American Airlines migrated existing applications—running on end-of-service-life infrastructure platforms—to VMware HCX on IBM Cloud™, gaining immediate technological and economic efficiencies. Over time, the airline will leverage these efficiencies and replace the legacy applications with new, cloud-native applications exhibiting a microservices architecture.

Benefit: American Airlines reduced costs, accelerated application development and improved end customer response times.

Learn more

What is the right approach for each application migration?

One size does not fit all when it comes to migrating applications and data to the cloud—there are many paths and cloud services options. First, you'll need to decide how much of the back-end infrastructure you want to support: Will you use an Infrastructure-as-a-Service (IaaS) solution or a Platform-as-a-Service (PaaS) solution? Next, you will develop a separate migration strategy for each application in your portfolio, choosing the right approach based on the application's unique needs.

Back-end support

Moving an application to the cloud can mean using an IaaS solution to replace on-premises servers, using a PaaS solution to replace the operating system and server software to virtualize your application, or both.

Infrastructure-as-a-Service solution

An IaaS solution offers a fully hosted cloud environment in which the provider is responsible for all the server maintenance and provisioning. Your application is hosted in a secure data center and your server allocation automatically scales to provide more power as needed. IaaS solutions are often pay-as-you-go: Instead of purchasing racks of servers and paying for the upkeep (whether you're using the equipment or not), you pay only for the resources actually used. This approach is especially suited to applications with seasonal or irregular use.

Because IaaS providers regularly upgrade their servers to the latest models, you can take advantage of cutting-edge technology without having to continuously purchase new equipment. Using new, well-maintained systems can also help you maintain high uptime. Remember: If the IaaS provider goes down, so does your application.

Think Research: Working smarter, not harder

Challenge: Think Research, a company that develops knowledge-based tools and leading clinical content for doctors, needed a way to reduce the time and complexity of managing its IT infrastructure.

Solution: Think Research adopted IaaS and PaaS solutions from IBM.

Benefit: By offloading day-to-day maintenance tasks to the IBM Cloud teams, the Think Research DevOps team can refocus on building better tools. The result is faster solution development.

Watch the video

Platform-as-a-Service solution

A PaaS solution manages your operating system and all server software, taking day-to-day operating environment maintenance off your staff's to-do list. It can be deployed on an on-premises server or (most commonly) in conjunction with an IaaS solution.

For on-premises PaaS deployments, you select the hardware. You maintain control over performance, patching, security and uptime. This approach can accelerate deployment and help you control costs.

A good PaaS offering should enable you to share services and implement upgrades better than older platforms. If you take this approach, be certain your application's hypervisor is compatible with the PaaS platform. If it isn't, you might need to redesign your application for the cloud. The hypervisor—also known as a virtual machine (VM) monitor—is a key process that creates and runs VMs. The hypervisor enables a single host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing. This approach helps increase system utilization and IT availability because the VMs are hardware-independent and can be moved easily between different servers. Check with your provider for their compatible virtualizations or use an industry-standard hypervisor from a vendor such as VMware.

Container-as-a-Service solution

Alternatively, instead of using VMs with a hypervisor, you can use application containers that leave all host-level management to the platform provider.

Each container stores a single application and all the necessary software to run it. This approach creates isolation at the application level, preventing one resource-hungry application from affecting others.

Containers simplify deployment and testing. You can easily copy the container without having to reconfigure it, and you can send ready-to-run applications directly to the cloud.

Containers offered by IBM Cloud Kubernetes Service can also provide a deeper level of security than traditional cloud or on-premises hosting (Figure 1). Container-level activity monitoring limits administrators to interact only with authorized applications. That limitation reduces the risk of a rogue administrator compromising data while automated encryption keeps your data safe from prying eyes.

The right container approach can also help you enhance performance. For example, IBM enables you to run application containers on bare metal. Running applications without a hypervisor or operating system helps maximize processing resources available for the application.

There are, however, potential drawbacks to the container approach. For example, because each application exists in a self-contained environment, any updates or patches need to be deployed to each container. When using a container approach, solutions such as Docker (an integral part of IBM Cloud Kubernetes Service) schedule and deploy updates to multiple containers.

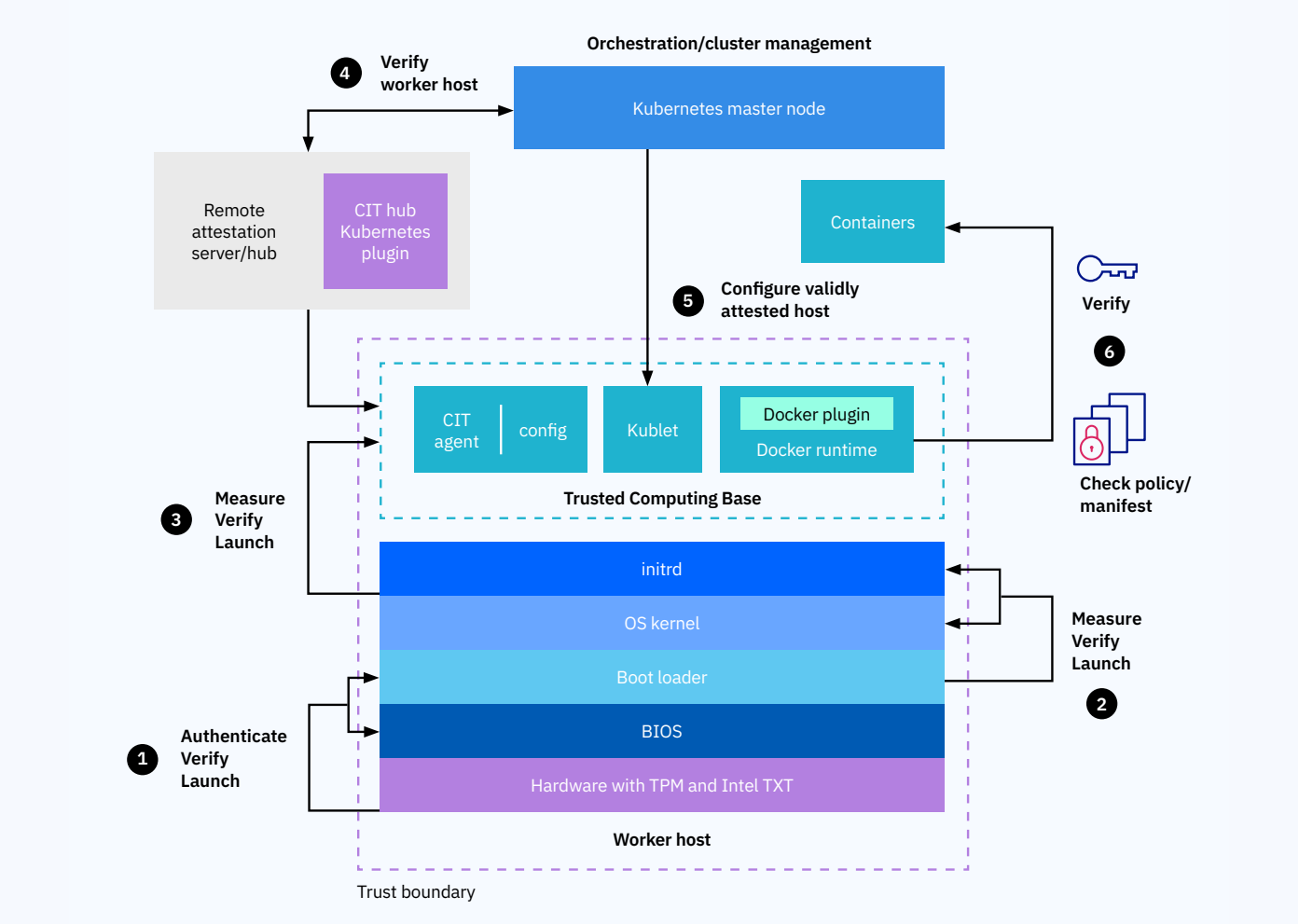


Figure 1. IBM Cloud Kubernetes Service provides a hardware-rooted chain of trust for container security. Because it is driven by security policies, the entire container platform automatically and only runs hosts and containers in known good states. The chain of trust is integral in addressing one of the major objections to cloud migration: a perceived lack of security. For more about container security, read the IBM white paper.

Hosted public cloud

You can also opt to host your application in a public cloud data center. A hosted public cloud solution provides many of the benefits of the public cloud: scalable performance, remote accessibility, data loss prevention, and total control over security and hardware.

Many enterprises manage a public/private hybrid deployment, running applications on premises and scaling out to the public cloud to address short-term demand, control costs or consolidate data center environments.

Application readiness

Can the application be moved as-is, or should it be refactored for the cloud? Some applications are cloud-ready, built with microservices designed to maximize the value of the cloud without requiring application changes. For other applications, you must decide how much effort you're willing to invest to move the application into the cloud and begin benefiting from the cloud's scalability and extensibility.

Move the application "as-is"

The major advantage to moving the entire application to a virtual environment without refactoring is speed. There's no need to delay migration for development time. Many cloud services can automate the deployment process, making it simple to rehost several applications.

A move to the cloud holds many benefits. A public cloud data center is often better maintained and more secure than an internal enterprise data center. It can also provide significantly more control around issues such as disaster recovery. For example, IBM Cloud provides "secure slicing," which automatically splits your data among three data centers for more reliable recovery, without charging to rehost the data in three data centers. Even the most inefficient application can benefit from this advantage.

OSRAM: Heightening agility in an ever-shifting industry

Challenge: OSRAM needed a more agile IT infrastructure that could keep up with the competition in a highly competitive marketplace.

Solution: Working with IBM, the company migrated its new and legacy applications to the cloud. OSRAM engaged IBM® Services to reduce the support burden on its in-house IT staff.

Benefit: Since the migration, OSRAM experienced seven-digit annual savings and several competitive new business wins. It also gained peace-of-mind from 24x7 infrastructure support.

Learn more

The downside: An application that isn't cloud-ready will use more compute resources. If you're using a cloud provider with a pay-as-you-go model, rehosting too many legacy applications can be a costly proposition. You'll want to refactor your resource-hogging applications as soon as possible.

Rewrite or refactor the application

If you have the time and resources, you can rewrite or refactor all or part of the application. Older, legacy applications would likely benefit if you start from scratch, giving you the opportunity to introduce new features and modernize the application. Other applications need only minor changes to take full advantage of the cloud, either by replacing specific services with SaaS offerings or changing the application to better manage its resources.

This method gives your application the full benefit of cloud computing but introduces additional steps prior to migration. You need more developers, designers and architects to optimize the software for the cloud—but the potential payoff is high.

To provide the extra support you might need, IBM offers a comprehensive application design service through the IBM Cloud Garage. This service is designed to guide your application from concept to deployment in fewer than eight weeks and provide training resources so your team can maintain your newly cloud-ready applications.

Replace the application

At this stage, it might make sense to re-evaluate whether you want to move the current version of the application to the cloud at all. Many applications considered critical can be replaced with preconfigured SaaS offerings from the same (or similar) vendor. While this might initially carry a higher cost, it is often offset by the lower costs of development, hosting and migration—and the faster time to value.

How will you secure each application on the cloud?

Some chief privacy officers and chief information officers are apprehensive about cloud security. Sending sensitive data offsite, to a third-party data center, can seem to add risks.

Nonetheless, many cloud solutions are just as safe or safer than on-premises deployments. As part of your cloud migration planning, consider digital security, data security, authentication tools and access restrictions.

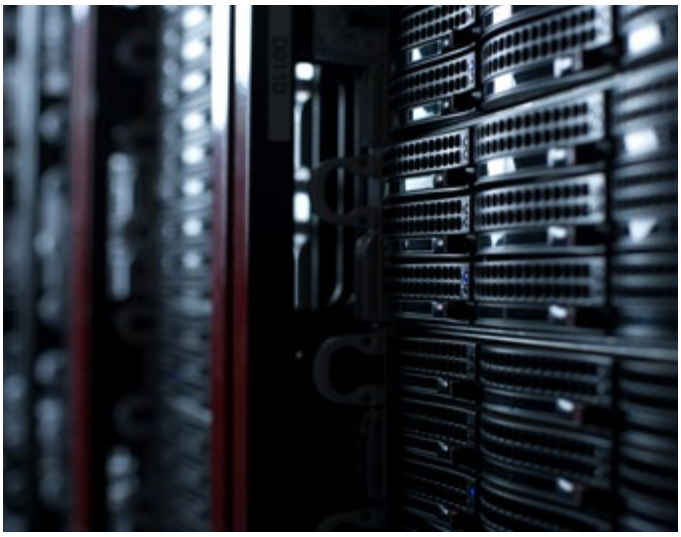
1. Digital security

It's vital to protect your applications from digital intrusion, especially as your data transmits to remote devices. Most public cloud providers possess security and compliance capabilities that exceed what organizations can do locally.

For example, IBM Cloud offers security at three layers: physical, networking and software. This multilayered approach avoids a single point of failure. Intrusion detection and prevention systems extending the boundaries to the Internet create a barrier against external threats. Encryption and protection technologies that work below the operating system, such as Intel Trusted Execution Technology (Intel TXT) and the Trusted Platform Module (TPM), help protect your data from unauthorized access or tampering, even at the BIOS level.

2. Data security

Maintaining strict data privacy standards sometimes requires additional assurance. A bring-your-own-key (BYOK) security approach offers one answer. With BYOK, you generate, manage and store your own encryption keys. The cloud service provider passes your keys to your application to encrypt, and decrypts data for your end users, but never has access to the keys or your data directly. This approach adds a layer of security and limits data access to your enterprise.



IBM Cloud offers Key Protect to provide customer-managed encryption (Figure 2). You import your own encryption keys into your application using the Key Protect API to encrypt and decrypt your data without exposing your keys to IBM. These keys are FIPS 140-2 Level 2 and are irrevocably destroyed upon delete, helping ensure your data is secure on your server. In addition to providing peace of mind, maintaining full control over your encryption keys is a necessary component of CISO audits.

IBM Cloud also uses Transport Layer Security/Secure Sockets Layer (TLS/SSL) protocol to protect data in transit. This capability helps prevent interception of your valuable data.

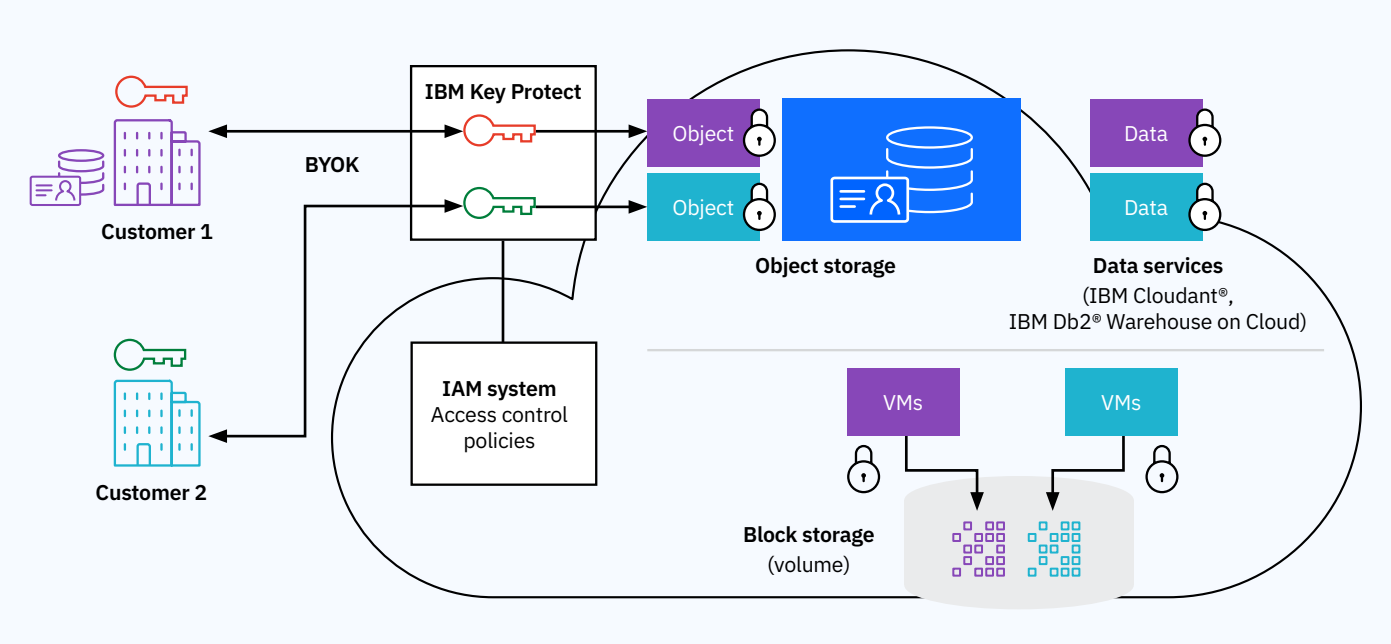


Figure 2. Architecture of a BYOK solution with Key Protect cloud-based security service.

3. Authentication tools

When your application is no longer restricted to a specific machine used on premises, access control becomes even more important. You must be able to accurately authenticate a user without noticeably slowing down the workflow. Two-factor authentication that uses both a physical device (like an authentication phone app or a dongle) and a password makes unauthorized access even more difficult. Single sign-on protocols allow shared identity federation, so users can access multiple sites using the same login without revealing the actual identity credentials to each site.

4. Access restrictions

Moving from on-premises environments to the cloud means that your employees can now access your applications—and the associated data—remotely. Though the data is safe on the cloud servers, you'll need to bolster security to protect data on your employees' devices.

In addition to implementing full-disk encryption, you should consider building and enforcing policies about which devices can access your cloud applications. Review and adjust administrators' access as well: Limiting the number of people who can enter the cloud environment at administrator levels helps reduce the risk of accidental (or malicious) activities affecting everyone's data and applications.

How will you manage and maintain the application after migration?

The best cloud migration and development strategies account for maintenance after deployment. With careful planning, a cloud deployment can streamline your IT and system administrator workloads. It is important to know that cloud applications scale, patch and upgrade differently from on-premises applications. Understanding these differences before you migrate will simplify your post-implementation workflows.

Cloud performance management

Scalability is one of the key reasons organizations migrate applications to the cloud. With a traditional, on-premises environment, adding processing resources requires you to buy, configure and install new servers. With IaaS deployments, you can expand your resources dynamically, allowing you to accommodate unexpected server demand.

Though the scaling happens behind the scenes, it's still important to maintain visibility over your application performance to minimize expected usage spikes and identify critical bugs that might lead to application downtime. The easiest way to keep tabs on your remote applications is through a cloud services monitor. Cloud vendors should provide tools to track and predict usage spikes, processing inefficiencies and crashes so you can maintain high availability and low usage costs.

Application upgrades and patches

Hosting your applications on the cloud simplifies the lift needed to keep them running at peak performance. But no matter how well designed your application, eventually you'll need to change, improve or fix something.

Some organizations prefer to offload platform, server and even application maintenance to a cloud service provider. If you choose that path, you'll need to consider the amount of control your organization wants to exert over your applications when choosing a cloud service implementation:

- **SaaS:** No control over patching or update. The service provider handles all maintenance.
- **PaaS:** You can apply patches to your application and upgrade servers, but you do not have access to the operating system or hypervisor.
- **IaaS:** You can apply patches to your application, to the operating system and to the hypervisor, but you can't make any changes to the servers.

Outside SaaS implementations, the cloud offers a great advantage for post-deployment maintenance. An on-premises application can be installed on hundreds, if not thousands, of computers across your organization. But an application on the cloud is a single installation accessed by multiple users. When you deploy a new version of the application, all users get that new version automatically.

However, this approach requires immense attention during patches or upgrades. Because the cloud application is unavailable to all users at the same time, patching or upgrading can potentially shut down your entire operation.

The easiest method to maintain your cloud software without significant downtime is to create a new deployment with the updated version, instead of trying to apply a patch to the cloud-hosted version. This approach can dramatically speed up testing and improve performance while helping to ensure that users all access the latest and greatest version. You can cut over to the new version as soon as it's deployed. If you're using application containers, remember to patch or deploy each container separately even if the fix applies to more than one application, unless you're using a management system like Docker or Istio.

Adjusting to the cloud

In many cases, a cloud migration requires some changes to workflows, IT policies and business practices. Consider these tips for migrating your enterprise to "cloud thinking" when you migrate your applications to the cloud:

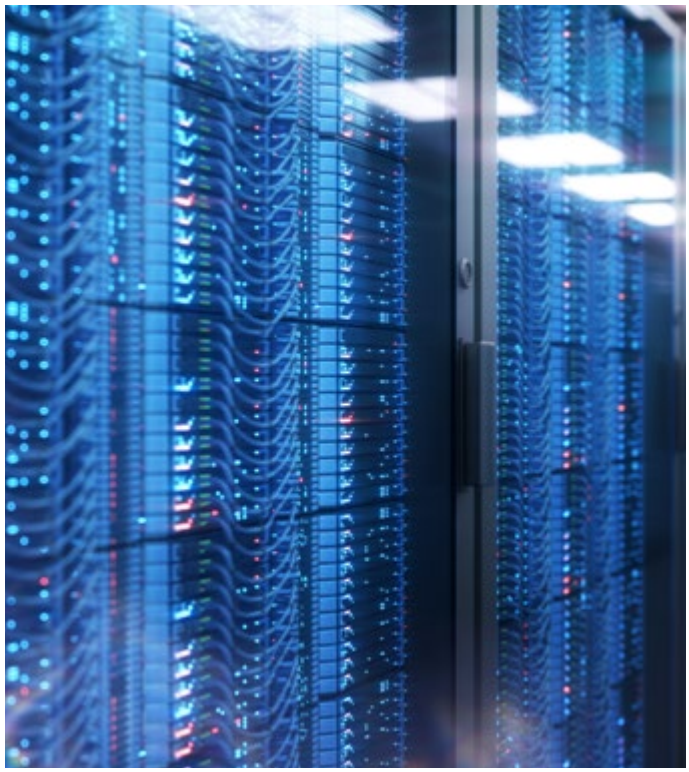
- **Be visible:** Form a migration team to act as a focal point for progress reports and inbound questions. Having an accessible "face" of the project will help keep the migration work in perspective.
- **Demonstrate value:** Score an early win in your migration by identifying and deploying your low-hanging fruit: applications that migrate with minimal development effort and can demonstrate the benefits of cloud computing.
- **Address concerns:** People unfamiliar with the cloud often overestimate security concerns or workflow disruptions. Demonstrating the security measures in place can put these worries to rest.
- **Minimize disruption:** Schedule your rollout to limit the impact on workflow. Sales kickoff is the wrong time to migrate your CRM; the end of the fiscal year is the wrong time to replace your financial software. If possible, deploy all your applications before retiring your on-premises implementation. That way you can test how your applications work together and provide a seamless experience for your users.
- **Get help:** IBM Services can provide resources and consulting to prepare your organization for a smooth migration.

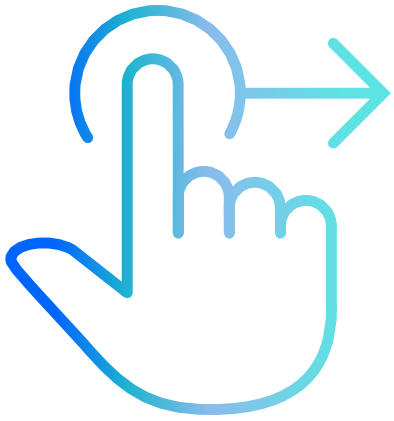
What's next?

Now that you've developed your migration plan, it's implementation time. Assemble your migration team and execute the identified strategy for each of your applications. Migrate the applications you can, replace the ones you can't. Migrate the easiest applications first to build momentum and demonstrate the value of the cloud, then work on progressively more difficult migrations.

Whether you're transferring your applications to the cloud, developing new cloud-ready applications or replacing your legacy software with a SaaS solution, you'll need a blend of trusted technology, tools, expertise and services to complete the migration.

From the time-sharing mainframes of the 1960s to the high-performance infrastructure and APIs of today, IBM has been a trusted partner in cloud computing for decades. IBM Services can help you design, develop and execute plans around even the most complicated deployment scenarios. Visit the IBM Cloud site to explore IaaS, PaaS and SaaS migration options.





For more information

To learn more about cloud migration and related technologies and services from IBM, visit: ibm.com/cloud

Stay connected

IBM Cloud Blog

Follow us

@IBMcloud
Facebook

Connect with us

LinkedIn
YouTube

IBM Cloud
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
August 2018

[1] SolarWinds, "IT Trends Report: Portrait of a Hybrid IT Organization," North America 2017; http://it-trends.solarwinds.com/reports/2017/portrait-of-a-hybrid-it-organization/north-america.pdf.

[2] McAfee, "Navigating a Cloudy Sky: Practical Guidance and the State of Cloud Security," April 2018; https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-security-report.html.