# Lifting and Shifting Enterprise Apps to the Cloud: 5 Rules to Follow (and 1 to Break)

Organizations considering moving enterprise applications to the public cloud should ensure that they also move the application delivery services their applications rely on in the data center. In addition, cloud migration presents an opportunity to...

White Paper

Organizations considering moving enterprise applications to the public cloud should ensure that they also move the application delivery services their applications rely on in the data center. In addition, cloud migration presents an opportunity to organize and rationalize security and access, gain visibility into cloud-based application traffic, and architect a strong disaster recovery plan.

## Introduction

For many organizations, moving enterprise applications to the public cloud can be a very attractive proposition. It enables them to dispose of the fixed costs and assets involved in running large-scale IT infrastructure, including expensive data centers packed with equipment of different generations and levels of supportability. While these servers are running the enterprise, they are also consuming power, making heat, and demanding expensive support contracts. Managing the lifecycle, maintenance, and physical housing of IT infrastructure demands skills, time, and budget that can detract from the overall mission of IT organizations: providing the applications that run the business.

Getting rid of this operational headache and financial drain in exchange for a new world where an old server or application can be retired with a simple API call often makes financial and operational sense. If you no longer need to manage the basic infrastructure that runs your IT, you can focus more on the security, performance, and availability of the applications that represent the real value IT brings to the enterprise.

But before you get to this nirvana of virtualized, maintenance-free infrastructure, you are going to have to work out the best way to move your applications into their new home. Migrating an application to the public cloud involves some choices. You can completely re-architect the application for a cloud environment, which can result in a sleek, streamlined user experience, but can often be a time- and labor-intensive process. Alternatively, you can simply pick up applications running in your data center and drop them into a public cloud without making large design or platform changes.

There are a number of good reasons to explore this "lift and shift" model: It's estimated to be about 10x cheaper[1], it's almost always a lot quicker, and in some cases it's simply not worth it to rewrite an application with a limited lifespan. But if you're going to have a successful "lift and shift" migration, there are a few rules you should follow—and one you are going to need to break.

## Rule #1: Treat Servers Like Cattle, Not Pets

We'll start with the one to break. The concept of treating servers like cattle is often seen as intrinsic to cloud architectures. If a server instance is functioning incorrectly, don't waste time fixing it—just kill it and redeploy. Don't upgrade operating systems or software; just deploy new instances and terminate the old ones. This is solid advice. But it can backfire if you are trying to move an application that was born and raised in the cosseted luxury of the data center into the cold, hard world of the public cloud.

Most enterprise applications were not designed with cloud architectures and methodologies in mind. They keep state locally, they take time to come online after the underlying server boots, and sudden shutdowns will probably result in inconsistent data. You need to treat them like the pampered pets they are, not like cattle.

Enterprise applications ported into cloud environments need much of the same care, management, and application delivery services (security, availability, and performance) that they receive in the data center. Even the basic load balancing services these applications require will be more complex than those needed by an application that was designed and born in the cloud. If you want your application to thrive in the cloud, you need to move its supporting infrastructure with it. Fortunately, most infrastructure components are now available in the public cloud of your choice—and you can reuse your organizational knowledge, skills, and even policies in the cloud.

## Rule #2: Move the Application, Not the Mess

The evolution of most enterprise IT follows a path that resembles a patch panel wiring rack. You know the one. It starts out beautiful, well designed, and perfectly executed. (Take a look at reddit.com/r/cableporn for some truly inspiring configurations.) Within a year, however, the necessities of time and urgency have resulted in a shortcut here, the use of the wrong color there ("red is for the DMZ, dammit!"). In three short years, the cabinet has degenerated into a Gordian knot of unlabeled, multicolored Ethernet cabling that just needs to be ripped out and reconfigured.

Moving to the cloud is your chance to get rid of that jumbled patch panel and take back control of security and access management. While you will need to move some of your infrastructure services along with the application, you should use this opportunity to rationalize, visualize, and organize your strategy of application and network access.

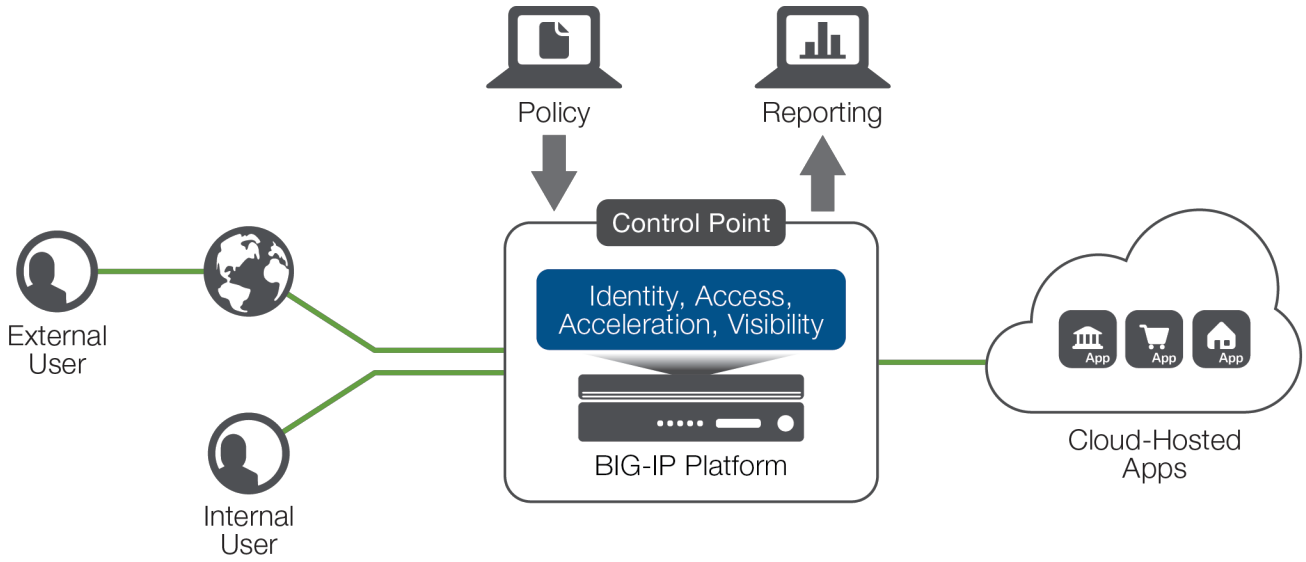


Figure 1: Add strategic control points to your cloud deployments.

## Rule #3: Hold On to Your Identity

Probably the most important control you can put in place is managing user identity in your cloud environments. As you move some applications to the cloud, retire some applications in favor of Software as a Service (SaaS) offerings, or rewrite some applications completely, you will need to make several key decisions about user identity management.

Running multiple identity services can be onerous, risky, and inefficient—and it can build back in some of the complexity you should be trying to eliminate. Identity management needs to be centralized, but access must be federated into all the required locations. Technology that integrates with your identity service (usually Microsoft Active Directory), and extends it into cloud and SaaS services using protocols like SAML and OAuth allows applications to authenticate users with a single source, rather than relying on local identity.

But just as applications have become more dispersed, so have users. Adding controls that identify a user's location and devices, combined with options for two-factor authentication and one-time passwords, can provide defense against social engineering and similar attempts to compromise your organization's information security.

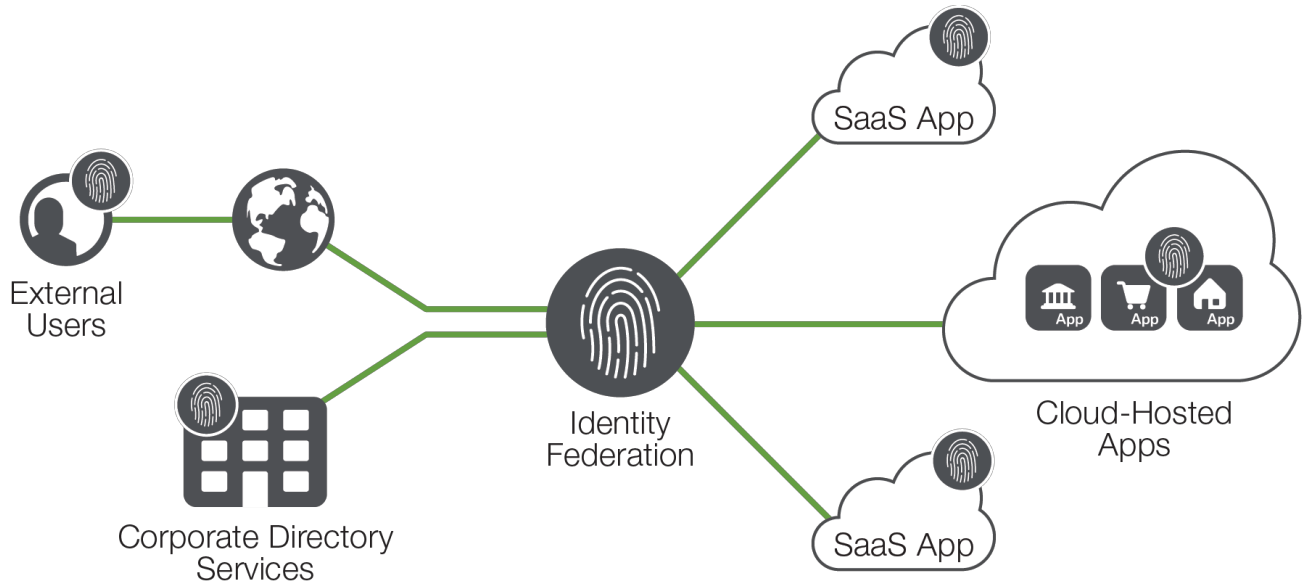


Figure 2: Federate identity to the cloud.

## Rule #4: Monitor to Cure "Cloud Anxiety"

Cloud environments abstract multiple layers of infrastructure away from your direct concern. This is a good thing, because now you don't have to service and support a physical infrastructure. However, this outsourcing of responsibility also comes with a ceding of direct control.

One of the things you will need to do to counteract this is monitor application performance more carefully. Adding in better monitoring that provides relevant and actionable information can make troubleshooting and capacity planning easier.

Another benefit can be the removal of some concerns within the business. Questions about security and performance in the cloud come partially from the multi-tenant and publicly connected aspects of the public cloud, but they also arise from the perceived loss of control. Adding in better monitoring of enterprise applications and behavior can significantly help in promoting this migration—and remove emotional barriers to cloud adoption.

## Rule #5: Stay Focused on DR/BC Strategies

Disaster recovery and business continuity (DR/BC) are mainstays of good data center infrastructure and application design. Using a public cloud does not remove your responsibility to keep applications running and secure. However, it does lower the barrier to entry for DR/BC services.

Before the availability of public cloud services, creating a physical disaster recovery location might have involved significant costs and lead times. Now, you can access infrastructure on another continent from a separate vendor using different underlying technology in a matter of minutes. But although the infrastructure may be far more readily available, creating a highly available application still requires significant planning and configuration.

While there is extensive documentation devoted to the topic of disaster recovery and cloud infrastructures, a good framework for planning and designing for DR/BC can be reduced to a few key decisions and concerns.

First, you're going to need to think about risk and return on investment (ROI). Is going for the ultimate multi-region, multi-vendor solution going to be worth the time and expense? While cloud services can lower the cost of acquisition, the operational costs of maintaining robust DR/BC services will still be there.

Second, you need to think about how you're going to store and distribute transactional data and keep it consistent. This is a well-understood problem, but is perhaps the hardest part of building geographically dispersed, highly available applications. Many solutions require high-bandwidth, low-latency connections between locations, or more esoteric designs such as an eventual consistency model that enterprise applications rarely embrace. Building low-latency connectivity between different cloud providers is not within the capability of most enterprises, but some options are becoming available.

The third key challenge is managing the access to your applications. For most active-active or active-DR designs, using DNS to direct traffic to the optimal data center based on availability, proximity, or performance represents the best balance of simplicity and functionality. This is especially true when you're considering a multi-cloud model in which you use different cloud vendors for your applications. Using network protocols such as BGP might also be an option, but that generally adds complexity and some risk. Another option might be to simply load balance or switch network traffic across clouds using equipment or services placed in locations outside the cloud, but near to it—which brings us to our final rule.

## Rule #6: Get Closer to the Cloud

Most midsize-to-large organizations migrating enterprise applications to the cloud will want to build secure private access into their cloud infrastructure. While running a VPN solution over public Internet may be appropriate for some, many organizations will use a more direct, dedicated connection to the cloud provider. These dedicated links delivered by service providers offer privacy, guaranteed bandwidth, and lower latency than public Internet connections—but they come at a price.

And if you need resilient connections to more than one cloud, you're going to have to provision multiple links. Or what if you need to connect your cloud to some infrastructure components, but your existing data centers are geographically or logically too far from the cloud network peering points?

Increasingly, organizations are considering colocating equipment in cloud-connected environments (commonly called cloud exchanges) that offer high-speed connections to multiple cloud providers. This allows you to host some of your IT assets extremely close to your cloud virtual infrastructure, which gives you private, low-latency connections between applications running in the cloud and infrastructure components such as storage or security appliances housed in the colocation center. In addition, this arrangement enables you to leverage existing IT equipment, and extend network and security controls into cloud infrastructure.

Finally, colocating in a cloud exchange lets you place controls at the nexus of your corporate data center, your cloud infrastructures, and the public Internet. You can extend or create the security policies that your business requires and achieve greater control and visibility of application data flows, improving your overall security posture and helping you rationalize and standardize access and security services.

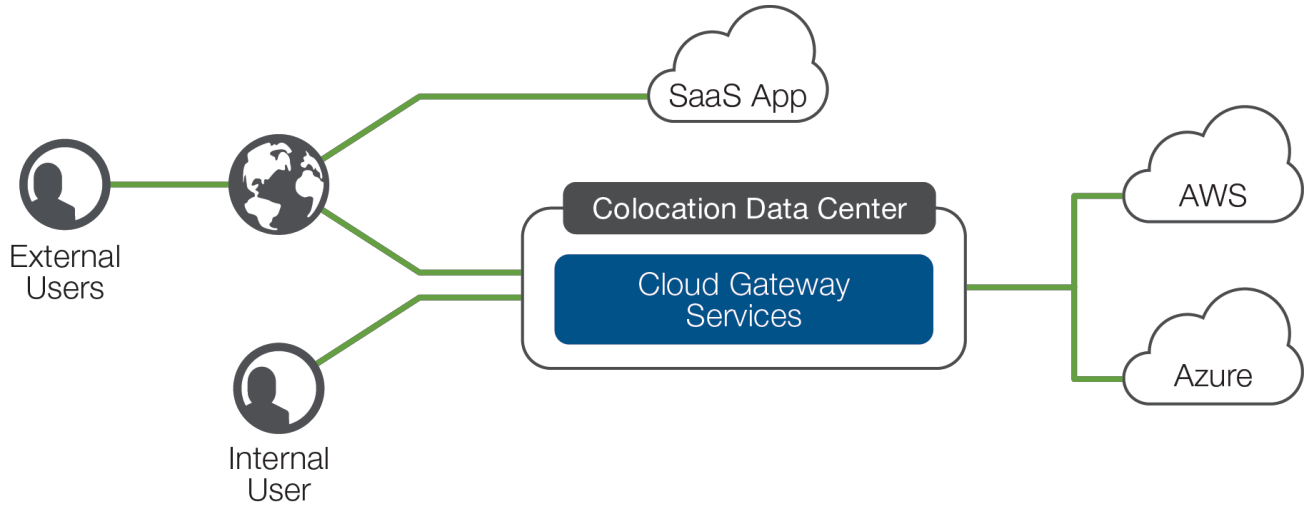


Figure 3: Colocating in a cloud exchange.

## Conclusion

Lifting and shifting enterprise applications to a public cloud can allow organizations to save money, increase flexibility, and move quickly into a cloud environment. Recognizing that enterprise applications still need a surrounding infrastructure, however, is critical to a successful migration.

Ensuring that the services your applications rely on for security, performance, and availability are present in the cloud will keep your traditional enterprise applications running and your users happy. Building in monitoring will enable you to spot problem areas quickly and help mitigate anxiety that application owners may feel as their services move to the cloud.

The act of lifting and shifting can also act as a catalyst to re-establish robust controls, rationalize access, and improve business continuity, which will increase the overall ROI of the migration. Finally, if you're leveraging multiple public clouds, consider the benefits of colocating in a cloud exchange, which can improve performance and allow you to standardize security and access policies from a single point of control.

[1] Knapp, Kristin, "The Means to the End," Modern Infrastructure, July/August 2015, http://docs.media.bitpipe.com/io_12x/io_125304/item_1181222/MI_JULY.pdf.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com