Evaluating IaaS security risks

This expert tip examines the risks organizations need to be aware of when evaluating IaaS solutions, and highlights the key architectural and process components of access management services that need to be considered in the cloud.

Sponsored By: ca technologies
Evaluating IaaS security risks

Table of Contents

Evaluating IaaS providers: security risks
Cloud computing access control: Access management services in the cloud
Resources from CA Technologies
Evaluating IaaS providers: security risks

By Joseph Granneman

There are many types of cloud-based infrastructures available today, ranging from Storage as a Service to full virtual server infrastructures. There is also a range of vendors looking to cash in on the latest cloud provider trends with an even wider range of capabilities. If there ever was a time for "buyer beware" in regard to cloud services, it's now. Let's examine some of the risks that should be considered when evaluating Infrastructure as a Service (IaaS) solutions.

Shared resources

One of the more obvious areas that should be evaluated with IaaS providers is performance. Cloud-based services derive their cost savings from scaling hardware and bandwidth across many different customers. In a SaaS solution, this is less critical than in an IaaS solution. For example, the bandwidth requirements for a cloud-based storage service are more demanding and require tighter tolerances than a hosted application service. One risk is that another customer monopolizes the system through large requests that leave your business suffocating for data. How does the cloud service provider divide up their resources among different customers?

Another issue that should be considered is also derived from the concept of shared resources. Not only is the performance of your cloud-based infrastructure at risk, but so is your data. Many IaaS providers utilize shared databases where the only separation between your data and your competitor’s data is a single field. What would be the impact to your business if your data was intermingled with another company’s data and breached?

IaaS providers are not just a boon for legitimate businesses looking for additional capacity or lower cost services. Criminals have also discovered that they can quickly and easily deploy services for DDOS attacks or malware command-and-control servers. There also could be servers that are offering content that is questionable or even illegal. What happens when your business is hosted on the same physical services as one of these illicit
services? The server could be overwhelmed with traffic, taking all of the other virtual
instances down with it. Or the servers could be confiscated due to a criminal investigation,
putting your data completely out of your control. It’s critical to understand how your virtual
servers will be deployed across the IaaS provider’s infrastructure and limit each server
instance to a single business process. It is also important to perform periodic backups of
these IaaS services locally or on a completely separate IaaS provider.

**Administration and management**

Administrative functions must be evaluated. It’s important to remember that cloud-based
infrastructure outsources administrative tasks such as system provisioning and hardware
maintenance to the cloud provider. These administrators will have access to your
confidential data and you may not have access to monitor what they have accessed. Even
Google reportedly had issues with rogue administrators accessing email and voice messages
of users without permission.

In addition, organizations need to consider the management of cloud-based infrastructure
services. If the IaaS provider doesn’t use some type of encryption for the management
interface, your virtual infrastructure could be accessible to anyone that captures your
unencrypted password off of the wire. Some IaaS providers create trusted connections
through the use of a secret API key that would also be vulnerable to a man-in-the-middle
attack if not encrypted. Procedures should be established for secure handling of these API
keys within your company as well; a Post-It note with a secret API key for an IaaS service
would provide anyone with access to your infrastructure...Use the same information security
standards that you would if the system was hosted internally: Encrypt all passwords and
API keys, limit administration to specific IP addresses, and require strong authentication for
administration.

Standardized procedures such as change control and server provisioning authorization are
also important in the daily operation of an IaaS implementation. This is no different than if
the servers were being housed internally at a corporate data center. These procedures are
critical to document the location of data and services as well as determine the risks and
appropriate mitigation strategies; they also provide a side benefit of helping to control
costs. Virtual servers and storage are typically priced on a pay-as-you-go model and the cost savings associated with utilizing IaaS could quickly evaporate without proper procedures and authorizations.

**Compliance complications**

It’s probably apparent that with all of the risks of using cloud-based infrastructure, compliance with SOX, HIPAA or PCI becomes very difficult. For example, HITECH requires electronic protected health information (ePHI) to be encrypted with algorithms defined in the FIPS-140 encryption standard... Since encryption causes higher server utilization, many IaaS providers will not offer this level of encryption by default. SOX requires data providence and data lineage, which is difficult to accomplish in the cloud. How do you verify all of the sources and the accuracy of the data when the servers are sharing bandwidth, CPUs, and even databases? Cloud providers won’t typically allow access to their firewall logs either or allow you to install an IDS or IPS as it would require sniffing network traffic, which is usually against the terms of service.

So with all of these potential risks, should companies pursue using IaaS providers? Yes, as long as they are aware of the risks and find an IaaS provider that can provide the level of segregation, encryption and contract terms required to meet their compliance and security requirements. Keep in mind, though, that information security doesn’t change in the cloud; the only difference is location of the data. If a company spends time to evaluate each IaaS vendor’s security capabilities and put the proper controls and procedures in place, it will be successful in deploying the promise of cloud-based infrastructure services.
cloud security.
can you see beyond the problem?
you can

The #1 issue for companies migrating to the cloud is identity and access management. But for the agile business, *know*-ing users is always better than *no*-ing them.

In fact, agile businesses, using our Content-Aware Identity and Access Management solutions, have been able to reduce security risk while improving productivity, access and efficiency. More effective compliance, reduced IT risk, broader, more secure customer and partner relationships.

That’s what happens when *no* becomes *know*. And security turns into agility.

To see how we can help make your business more agile and secure, visit ca.com
Cloud computing access control: Access management services in the cloud

By Philip Cox

Extending an organization’s access management services into the cloud is ad hoc, dependent on your cloud service provider, and rudimentary at best. However, with that said, there are some steps you can take to utilize cloud services as they become more mainstream:

• Ask your cloud service provider to support open standards for access management.
• Standardize and automate your user provisioning as much as possible.
• Create a centralized entitlement management mechanism within your organization.
• Extend policies and procedures regarding access management to include cloud services.

Let’s take a closer look at these steps, particularly the two key architectural and process components of access management services that need to be considered in the cloud:

• Entitlement (privilege) management: assignment and enforcement
• User provisioning and de-provisioning

Entitlement management

Organizations who want to utilize access management in the cloud will need to spend a significant amount of time ensuring their systems and applications have the ability to consume an externalized entitlement management service. In a nutshell, this means designing your application and systems to provide and consume eXtensible Access Control Markup Language (XACML) type information. XACML is the leading general purpose standard for describing policy management and access decisions. It describes a language as well as a processing environment model. The main purpose of XACML is to allow organizations to implement a common authorization standard across all systems and applications by providing a standardized language, a method of access control, and policy
enforcement. In contrast, Security Assertion Markup Language (SAML) is an open standard used for federated identity.

The key is that you will have to ensure your systems and applications can consume the XACML information, and that your IAM system can provide it.

The reason I stress XACML is that it is an open standard; you should be wary of spending significant amounts of resources to integrate into a cloud service provider’s proprietary entitlement management system. When it comes to the cloud, open is better.

However, I don’t know of an existing cloud service provider that supports the ability to have externalized entitlement management on a large scale. Meaning that while this is an admirable goal, the reality of cloud providers being able to consume or provide entitlement management is currently not practically feasible. For now, focus on providing the entitlement service and consume it with your own applications or systems. Think of this as an early frontier; as time passes, adoption of standards such as XACML will pave the way for a more universal entitlement management across cloud services.

**User provisioning**

Along with identity and entitlement management, user provisioning and de-provisioning are key elements of identity and access management services. User provisioning is the process of allocating users to systems and applications and effectively granting identities access to information and systems. In order to effectively utilize IAM in the cloud, you will need to have an efficient process for user creation and removal. This process of provisioning and de-provisioning will set the initial entitlements and link them to an identity.

You should look to see how your current provisioning process integrates Service Provisioning Markup Language (SPML) to make providing and consuming the service as seamless as possible with your cloud service provider. Like XACML, SPML is a standard, and utilizing it as the basis for your service provisioning will provide future benefits of interoperability you would not get if you integrate with proprietary cloud solution. Using SPML can allow you to standardize and automate much of the provisioning process, which is critical for a successful IAM operation in the cloud.
The need for standards

Standards for access management services are critical to ensure future cloud adoption. By using open standards -- as well as requiring cloud service providers to support them -- we set the foundation for a consistent and secure method of service offering and use. If the Internet has taught us anything, it is that the use of standards is the way to promote wide adoption and use of technology.
Resources from CA Technologies

CA Technology Brief: CA Point of View: Content Aware Identity & Access Management

Defending Against Insider Threats to Reduce your IT Risk

Cloud I.Am: Content-Aware IAM for the Cloud

About CA Technologies

CA is one of the world’s largest IT management software providers. Our software and expertise unify and simplify complex IT environments-in a secure way-across the enterprise for greater business results. We call this Enterprise IT Management (EITM)-our clear vision for the future of IT. It's how you can manage systems, networks, security, storage, applications and databases securely and dynamically. You can build on your IT investments, rather than replacing them, and do it at your own pace. Our more than 5,300 developers worldwide create and deliver IT management software that keeps our vision real. And we've taken our decades of experience solving complicated IT problems and developed practical paths for you to get from where you are today to where you want to be.