IDaaS

Identity-as-a-Service best practices

An expert guide from the Cloud Best Practices Network

http://CanadaCloud.biz

Table of Contents

Building GovCloud Services, Part 1 – Solutions Matrix Model

The objective of this guide is to introduce and explain Cloud Best Practices, as defined by the American standards organization NIST, and how these might be applied in Canada to recreate a Canadian version including aspects like security and privacy policies.

Via their 'GC Community Cloud' program the Canadian Government is defining their localization of these models. You can download the PPT and other materials from this section.

It is also to showcase local expertise and vendor products who are available to enhance and implement these best practices. This provides them the ideal context to explain their innovations and value-add services.

Solutions Matrix Model

Fundamentally the NIST cloud models are based on two key design methods of 'Service Models' (IaaS, PaaS and SaaS) and Deployment Models (Private/Hybrid/Community/Public Cloud).

This makes this matrix of different options possible, that can be used by agencies to determine which specific configuration is correct for them, based on their information security requirements.

		CLOUD SERVICE MODELS		
DEPLOYMENT MODELS		Software as a Service (SaaS)	Platform as a Service (PaaS)	Infrastructure as a Service (IaaS)
	Private			
	Community	X	X	
	Public		X	
	Hybrid			

Business Use Cases

Then in addition to this matrix NIST is organizing a catalogue of 'Business Use Cases'.

These package up these combinations and apply them to specific use case scenarios, such as Email hosting, E-Discovery and IT Service Management, amongst others, and are therefore forming a best practices library that other agencies can then reuse for procuring the same services.

The use case states what configuration of Service and Deployment models are needed. For example the E-Discovery scenario says that the service is required on a SaaS basis (Software as a Service) and implemented via a Community Cloud model.

Telco Cloud Services

The IDaaS model offers in-house implementation or alternatively you can source it as a managed service from a third-party provider.

For example this Verizon news piece highlights that they recently launched an IDaaS offering, one that has been certified for levels 1, 2 and 3 class of service. This basically means that the security checks applied at the sign-on process becoming increasingly more sophisticated, using 2, 3 and 4-factor authentication methods.

The greater the security at the username/password sign-on process for users, the more that Identity provider can guarantee the person is who they say they are. This then provides a keystone for enabling more secure services, ideal for better online automation of government workflows, like filing tax returns as the news release highlights.

Cloud Identiy & Security Best Practices

Naturally the security of information hosted in Cloud systems is of paramount importance, and luckily the Cloud best practices in these areas are now fully maturing to cope the wide array of areas that need covered.

There are various industry authorities in this area including NIST, such as the Cloud Security Alliance, which stipulates a program of best practices.

Canada is also active in the development of key Cloud resources relevant to this trend.

Recently they published their '**ITSS Security Domains & Zones**' documentation that stipulates the security models required to implement their 'GC Community Cloud' program, as we have documented here.

PaaS and Cloud Security

The roles of both PaaS and Cloud Security are explained through their overlap, in that security is often an area that an organization expects to be enforced in a common and standardized manner.

PaaS also has an objective of this common standardization, which includes but is not limited to security, also encompassing application servers and middleware.

This is explained through analyzing the NIST 'Business Use Cases'.

Cloud	Enterprise
SaaS	Applications (SAP, Oracle BS)
PaaS	Middleware (DB, ESB, App Srvr)
IaaS	Virtualization / Hardware / OS

In these documents they describe the need for a set of 'common building blocks' that correspond with the PaaS layer of the Cloud stack, what NIST describe as 'cross-cutting'. These are described in the following way in the use cases:

"In addition, the initial public platforms will benefit from being able to operate on the community cloud infrastructure, and visa-versa. To that end, the following interoperability requirements are needed:

1. ***Authentication and identity management interoperability will be required so that users of multiple target clouds can maintain consistent identity and role based access across multiple cloud implementations.***
2. *Virtual machine management interoperability will be required so that platforms running in multiple cloud implementations can be stopped, started, terminated and otherwise operated through a consistent interface.*
3. *Billing and reporting interoperability will be helpful to allow for meaningful comparisons of costs and benefits across multiple cloud implementations.*

8.3. Portability

Static virtual machine portability is required so that the maintained platform images can be freely migrated between cloud implementations without the need for parallel development or maintenance. Dynamic VM portability, where running machines are migrated in flight is not required."

Cloud Identity and Security Best Practices

A key backbone to our program is the combination of 'Cloud Identity and Security Best Practices', referring to the intersection between Cloud Computing and Identity Management technologies.

The importance of this is illustrated through the NIST Business Use Cases. For example the E-Discovery use case describes both a need for common Identity Management as well as data sharing between different Cloud-hosted applications, like the e-discovery application being able to audit another providers hosted email. These secure data sharing mechanisms will be facilitated by common, standards-based PaaS layer components, and it also achieves compliance with multiple government mandates.

A great example is this recent press release from NASA, about their use of 'PIV' technologies to secure their move to Google apps.

By securing the user authentication process to Cloud apps like Google they are putting in place one key foundation for ensuring ultra-robust Cloud Security, demonstrating one part of the relationship between the Cloud and Identity Management.

It also demonstrates healthy portions of political compliance too. By adopting Google they are demonstrating progress against their Cloud First requirements, and simultaneously doing the same for this Whitehouse directive requiring agencies to begin accepting signin credentials from external sites, a principle known as 'federated identity'.

This federation is achieved through best practice frameworks such as the Kantara Initiative, which provides a means of stipulating differing user security levels ranging from 1 through 4, referring to the number of factors used in the authentication process, and also to build 'Trusted Services', a network of providers to then accept these credentials and provide access to the user.

As well as their own in-house standards for identity authentication ITSG-31 here the Government of Canada has also standardized on(and contributed to) Kantara. Their specific implementation is defined in this document. (53-page PDF).

Virtualization and Identity Security

As highlighted recently the Canadian Government published their '**ITSS Security Domains & Zones**' documentation that stipulates the security models required to implement their 'GC Community Cloud' program, as we have documented here.

It builds on their previous reference documents, ITSG-22, Baseline Security Requirements for Network Security Zones and ITSG-38, Network Security Zoning, which describe WAN (Wide Area Network) level approaches to sharing networks the same way.

This same principle is applied higher up the stack, across virtualization, servers and storage, and hence in essence describes best practices a logical architecture for segregating 'Cloud Security Zones', linking each Cloud area (IaaS, PaaS, SaaS) to a security infrastructure component, and describing how the computing environments will be integrated with their wide area networks and access control systems, through a Cloud Services Access Layer and a Cloud Peering Layer..

Fundamentally this defines the required **Virtualization Security,** meaning the seperation of Virtual Machine environments in the same way vLANs seperate networks, so that agency customers can be

ensure their applications are logically entirely seperate from those of other agencies. Only then will they move to multi-tenant Cloud environments.

VMware Horizon Application Manager

An example of a vendor technology that can be used to implement Cloud Identity and Security Best Practices is the Horizon Application Manager from VMware.

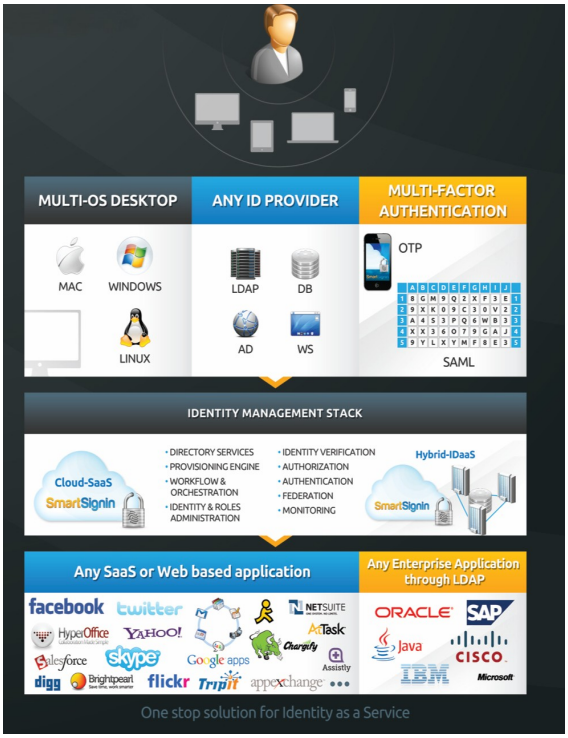
As this article explains the Cloud itself has a user authentication process, for users and admin to sign on to the actual environment, such as vCloud in this case and it may not be as robust as you need or as compliance dictates.

Therefore the principles of Identity Management, increasing the security of these user authentication procedures, can be applied to Clouds too, both internally and importantly externally. It will likely become a key mechanic required for "secure Cloud outsourcing", especially to government.

Hence Cloud Identity Management includes this sign-on process, and then the role it plays as a secured single sign-on across the applications that the Cloud is used to run. This function of interconnecting different systems this way is known as 'Federation', as described in the diagram above.

Smart Signin

Other similar solutions include SmartSignin, an example of a home-grown Canadian venture specializing in this field.



SmartSignin is based on a joint venture with the University of Toronto, to leverage a unique new security algorithm to make online user security more robust while also easier to use.

SmartSignin offers a platform to implement Cloud and Identity security best practices through:

- A "cookie-less" approach to web security.
- Support for multiple devices and multi-factor authentication modes
- Cloud SaaS sign-in to any web based application
- Hybrid IDaaS model for enterprise single sign-on to apps like SAP and Oracle

Authors

Neil McEvoy, Founder, Cloud Best Practices Network

Neil McEvoy is a senior executive, consultant and communicator specializing in adoption of innovative new technologies for enhanced business effectiveness and accelerated social change. He is a subject matter expert in cutting edge technologies such as Identity 2.0, Cloud Computing, Big Data and the Semantic Web, and as the Founder of the Cloud Best Practices Network (cloudbestpractices.net) works to organize a community of industry pioneers, experts and consultants and communicators to help distil these into easily repeatable business models.

Contact Neil: neil.mcevoy@l5consulting.net