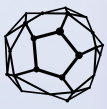
Cloud Security is a First Principle:

Elements of Private Cloud Security



nebula

Nebula.com

Table of Contents

Why the Security Minded are Drawn to Private Cloud Deployments

Cloud computing carries an attractive value proposition for many enterprises, thanks to the higher levels of scalability, flexibility and efficiency it can provide an IT organization.

However, there remains a great divide in the degree of trust that IT professionals place in public versus private clouds. The ISACA, the global nonprofit IT organization, in its annual IT Risk/Reward Barometer survey[1], found that IT professionals were cautious of public clouds but enthusiastic about private. "69 percent believe that the risk of using public clouds outweighs the benefit," ISACA reports. "Opinions of private clouds are the opposite—the majority (57 percent) believes the benefit outweighs the risk."

The value of on-premises private clouds was also underscored by a recent eWEEK survey[2] that found private cloud deployments to be on the rise, growing at a rate faster than even hybrid clouds, in a drastic shift from recent years The survey also found that "65 percent of IT decision makers say they use or plan to use a private cloud deployment model for internal purposes or for application inside value chains. Plus, 36 percent of respondents say they are now running a private cloud, with 29 percent planning to use a private cloud."

On-premises private clouds are especially attractive to a range of organizations, from the SMB to the enterprise, because of the inherent security, control, and compliance benefits that come from managing your own infrastructure. Many organizations, especially (but certainly not limited to) those in the public sector and financial industries are under pressure, from within or without, to harden their systems, maximize access controls, and reduce the risk of intrusion or data breach.

The security-minded IT professional knows that it's very difficult to lock down and apply controls and countermeasures to a system that isn't designed to be secure from first principles.

Because security is such a strong driver for the deployment of on premise private clouds, the security-minded IT professional should take a close look to ensure that any private cloud solution incorporates elements that ensure the long-term security of the system. This paper provides a guide on the security features that are essential for a private cloud infrastructure.

1 Cybersecurity, Private Clouds, Privacy: ISACA Issues Guidance on Top 2013 Trends
2 Running Your On-Premise Cloud Like a Business: 10 Key Steps to Take

Security is the Driver Behind Private Clouds

When IT professionals talk about security, it is generally a catch-all term for a trio of concerns: confidentiality, integrity, and availability. Confidentiality means that data is only viewable by the correct parties. Integrity means that your data is never altered, accidentally or otherwise. And availability means that the system is designed to be running and useful as much as possible. Protecting confidentiality, integrity, and availability is best accomplished through a comprehensive, multi-layered approach to security, which we'll examine in this paper.

How to Find a Solution that is Secure by Design

The simple fact is that creating a private cloud from scratch is a complex undertaking. With the right talent, you can certainly create your own on-premises private cloud, but in the process of assembling a best-of-breed solution you will be pulling together servers, switches, storage devices and other elements—each with its own set of configuration variables.

There are many vendors and technologies on the market, all promising an ideal path to meet these challenges and provide a frictionless path to the private cloud.

The right candidate for deployment will be one designed and created with security in mind. Ideally, you want a private cloud solution designed with layers of security as a crucial design element. In short, you want a solution created by security-minded engineers intent on making their system—at every juncture of design and execution—as impervious to attack as possible.

Elements of a securely-designed private cloud should include:

- Well defined security domains
- Verified boot
- Hardened API endpoints
- Hardened Kernel Hypervisors
- Security update management
- Strong instance protection
- Entropy

Well Defined Security Domains

A private cloud can be thought of as a collection of security domains, each comprised of users, applications, servers or networks that share common trust requirements and expectations within the system. Typically a security domain has the same authentication and authorization requirements and users.

From a design standpoint, you need to be very careful about how one security domain bridges to another. For example, if a bad actor gained access to your external security domain, you would want to have a secure design that would prevent them from bridging to the control plane domain. From a best practices standpoint, access to domains should be granted on a least-privileged basis so that only those who need to access the domain can, and once in the domain their rights for the domain are restricted to just what they need to accomplish in their job.

There are many ways in which to design the security domains of a private cloud, but when evaluating a private cloud solution, one should look for critically important basics such as:[3]

- **Management Domain.** The management security domain (sometimes referred to as the control plane) is where services interact. Access to this domain should be highly restricted and monitored, as the networks in this domain transport confidential data such as provisioning orders, configuration parameters, usernames, and passwords. The command and control traffic of the management domain necessitates strong integrity requirements.
- **External Domain.** The external domain refers to anything external to the private cloud. Usually this is the corporate network, or via a web dashboard, the Internet. Because such networks are by definition beyond the cloud, from a design perspective they should all be considered untrusted, meaning that any data that transits this domain with confidentiality or integrity requirements should be protected using compensating controls such as encryption.
- **Instance Domain.** The instance domain consists of a network reserved for communication between instances. Every instance comes up on the instance network, which allows the instances to talk to each other. Optionally, you can give an instance a network address that allows it to also talk on the external network, but to conserve your external network IP addresses, your cloud architecture can instead designate one instance as a gateway for communicating out to the Internet, that relays information as needed to other instances.
- **Data Network.** The data security domain refers to the network that handles data access between the domains and storage. Much of the data that crosses this network has high integrity and confidentiality requirements and depending on deployment-type there may be also be strong availability requirements. The trust level of this network is heavily dependent on deployment decisions.

3 OpenStack Security Guide

As noted earlier, special attention should be paid to the security of bridges. Any component that bridges security domains with different trust levels or authentication requirements must be carefully configured. These bridges are often the weak points in network architecture. A bridge should always be configured to meet the security requirements of the highest trust level of any of the domains it is bridging. In many cases the security controls for bridges should be a primary concern due to likelihood of attack.

As a best practice, consider securing a bridge to a higher standard than any of the domains it resides within. For example, with an API endpoint, an adversary could potentially target the API endpoint from the public domain, leveraging it in the hopes of compromising or gaining access to the management domain.

Verified Boot

Provisioning of nodes should incorporate validation using a Trusted Platform Module (TPM) for verified boot. This helps detect malicious modifications to firmware, boot loaders, kernels, and other low-level software. The TPM can use embedded credentials along with measurements of the running firmware and software to attest – or prove to a remote system – that this code is correct. These constructs allow more complete validation of cloud nodes before they are permitted to join the cloud, which raises the bar for an attacker. Leveraging hardware to validate node security greatly enhances the overall cloud security.

Hardened API Endpoints

A well-designed private cloud can be protected through the use of security-enhanced protocols for the API endpoints. This enables use of a customer-supplied server certificate and private key so organizations can enjoy the security of a completely encrypted and authenticated environment. Dashboard communications, which typically involve contact with the control plane and other critical security domains, should also be protected.

Although secure socket layer (SSL) is often associated with protecting HTTP connections, it is broadly applicable to any type of network connection. Transport layer security (TLS), an updated version of SSL, provides even better security and should be used when possible. As a best practice, every cloud should use SSL/TLS to help protect interactions. HTTP strict transport security (HSTS) is also strongly recommended as it will forces clients to only use a secure connection, helping to mitigate SSL-stripping man-in-the-middle attacks.

Hardened Kernel Hypervisors

An additional layer of security is gained through the use of hardened kernel hypervisors and device drivers, significantly limiting the potential attack surface.

Security Update Management

In the ever changing threatscape that immerses the Internet, it is safe to assume that critical security vulnerabilities will be discovered in the hypervisor. With this in mind, it is important to be able to quickly and reliably update the hypervisor to a new version. And, of course, to actively monitor the appropriate information sources for announcements about updates to the software.

When contemplating a private cloud deployment, you should look for strong internal practices from a vendor committed to providing complete lifecycle protection. This means a commitment to continual testing and a proactive program in place for detecting potential weaknesses, alerting cloud managers, and swiftly releasing well-tested, digitally signed, updates for effortless installation.

Strong Instance Protection

Strong instance protection, including use of SELinux mandatory access controls and hardened QEMU deployments, mitigate instance escape attacks and cross-user security concerns.

Entropy

A private cloud should provide high quality and sufficient entropy to support robust random number generation for all running instances.

About Nebula

Nebula is dedicated to enabling all businesses to easily, securely, and inexpensively deploy large private cloud computing infrastructures. The company has developed a hardware appliance that allows any business to easily build a massive private computing cloud from hundreds or thousands of inexpensive computers.

Nebula's goal is to ignite a new era of global innovation by making big data and large scale computing accessible to every business in the world. We believe that the proliferation of data will fuel an "information revolution" across all industries, and will be enabled by democratizing web-scale cloud technology.

Nebula is privately held and venture-funded by Kleiner Perkins Caufield & Byers and Highland Capital Partners. Other investors include Google's first investors, Andy Bechtolsheim, David Cheriton, and Ram Shriram.

Nebula, Inc.
215 Castro St, 3rd Floor
Mountain View, CA 94041
(650) 539-9900
Nebula.com