Design considerations and Guiding Principles for Implementing Cloud Security

William Stearns

Security Analyst

CloudPassage

In a nutshell…

- How do *Cloud Servers* differ from *Data Center Servers*?
- How do the differences affect:
  - Program design
  - Security
  - Setup, configuration, and maintenance

Who's responsible

Backups	You and/or Cloud Provider
Data Confidentiality	You
Applications	You
OS	You
Virtualization layer	Cloud Provider
Hardware	Cloud Provider
Availability	Cloud Provider

First, similarities

- All(*) are virtual machines
  - Effectively no additional security considerations from virtual machine vs bare metal
- Same OS's, server applications
- Still need to
  - Lock down configuration
  - Firewall ports
  - Shut off services

Transient nature of Cloud Servers

- Lifespan: as little as hours
- Launched based on network/application load
  - Easy to launch, manually and automatically
  - Easy and quick to destroy

Effect of transient nature

- Can't depend on local storage
  - Destroyed when VM destroyed
  - Serious performance issues on shared media
  - Network too, to a lesser degree
- Instead: SQL, File server, API
- No(*) need for backups of Cloud servers
- Tougher for long running jobs
  - Better to break into smaller bites
  - Regular checkpointing

Identical servers in a group

- Similar role => similar VMs
  - Base OS
  - Packages installed
  - Running services
  - Configuration changes
  - Local accounts

Effect of Identical machines

- More dependence on automated setup, configuration
  - Chef, puppet, rightscale, others
- Less dependence on local user accounts
  - And fewer manual changes
  - Manual changes at 3am?
  - Fewer end-user tools
- Canary: deltas between servers
  - Or between server and master image

Patching

- Base image fully patched before clone
  - Fully/almost fully patched cloud servers at launch
- Options
  - Instead of patching running machine, only patch base
    - Test base image after patching, before use
    - Rollout new cloud servers, retire the old ones
  - Patch immediately at launch
    - Delay before VM productive, no time to test patch

Less control over Cloud Network

- Network segmentation
  - Easy in data center, tough in Cloud
- Cloud servers: little or no external protection

Effect of exposed servers

- Less dependence on Network security measures
  - Network firewalls
  - NIDS/NIPS
- Instead, use Host-based tools
  - Host-based firewalls
  - HIDS/HIPS
- Lock down access to test/development

Firewall good news

- Toughest part of firewalls: managing *user* outbound connections
  - Very few user tasks: simpler outbound firewall
- Cloud servers with specific task
  - (Instead of older servers running multiple daemons)
  - Simpler inbound firewall

Data privacy

- VPN/encrypted links
- Encrypted storage for sensitive data
  - How do you enable at boot? ☹

Monitoring

- No logged-in users to notify
- All monitoring must be automatic and routed
  - CPU, memory, network usage
  - Listening ports
  - Disk less important as local disk less used
- Post-install configuration checks
  - Configuration and user data set up the way you want them?
  - Regression testing
  - Report and/or alert

File Integrity Monitoring

- Look for modified files that shouldn't be
  - Less end-user fingers in Cloud Servers, good
- Multiple baselines
  - Useful during switchover to new code/VM/data

Logging

- Centralize logs, not local storage
- Centralized analysis/SIEM
  - Abnormal behaviour
  - Malicious activity
  - Local system logins (rare, if at all)
- Means no more dependence on log directories/windows events that may disappear

Tools need to

- Be portable
  - Cloud provider has awesome security feature
  - What happens when they go down and you need to migrate?
  - What happens when they become more expensive than competitors?
- Be cloud Aware
  - Can they handle regular churn?
  - Do they start automatically and run from minute 1?
  - Can they be licensed on machines that may only exist for an hour?
- Provide an API

Questions?

- William Stearns
- wstearns@cloudpassage.com
- http://blog.cloudpassage.com