Cloud security and OpenStack
Primož Cigoj
Laboratorij za odprte sisteme in mreže
IJS-E5

www.kc-class.eu
Outline

• Cloud computing
  • General overview
  • Deployment and service models

• Security issues
  • Threats
  • CSA / NIST / ENISA
  • Data protection, privacy, cryptography, identity management

• OpenStack
  • Components overview
  • Security issues (identity provisioning, authentication, data protection)

• Conclusion and future work
Cloud computing

• Definitions:
  • Gartner “a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies”
  • NIST “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”

• Main characteristics:
  • Non-functional aspect (among the providers are very different)
    • flexibility, reliability, quality of service (QoS), availability, accessibility
  • Business aspect (an important reason for introducing cloud computing in business organizations)
    • reduce costs, pay-as-you-go model, return on investment (ROI), green IT
  • Technical aspect (realization of non-functional and financial aspects)
    • virtualization, several rental model, security, privacy and regulation compliance, self-service, automation, data management, APIs, software support, development, etc.
Deployment models

• Public cloud
  • services and facilities are available through the internet

• Private cloud
  • designed exclusively for a specific organization (local hosting)

• Hybrid cloud
  • composed of two or more different cloud infrastructure (linked together)
Service models

• Software as a Service (SaaS)
  • provide the consumer with the use of provider’s applications running on a cloud infrastructure

• Platform as a Service (PaaS)
  • a way to rent hardware, on which cloud customers are able to develop and implement applications

• Infrastructure as a Service (IaaS)
  • the consumer can implement any software, including operating system and applications

Present time = A lot of infrastructures:
  • Hyper-V, VMware, Nimbus, OpenStack, etc.
Problem definition

- The biggest obstacle for users in use of cloud is security!
- A popular approach is to create, publish and share server images with other users
- Trust model cloud provider & user is well-defined
  - Amazon is not going to hurt you :)
- What about image provider?
  - Users can create and share images too (blurry ????)
- What about data protection?
  - Admin can access our data, unencrypted data, etc.
Security issues

• When it comes to data hosting by external companies - it is an interesting, economic model, that induces security concerns. Security issues are known, discussed but not resolved entirely.

• CSA / NIST / ENISA

• Threats:
  • Abuse in use of cloud computing
  • Insecure interfaces and APIs
  • Malicious insiders
  • Shared technology issues
  • Data loss or leakage
  • Account or service hijacking
  • Unknown security profile
Data protection

• The main data protection risks:
  • loss of data by third-party service providers
  • unauthorized access to your data
  • malicious activities targeting your service provider (hacking, viruses)
  • poor internal IT security compromising data protection
  • deletion of data
Privacy

• Data storage => Where is located?
• Is the service provider owned or controlled by a foreign company?
• Destruction => What happens when the contract is terminated?
  • Is data destroyed or can be retrieved?
• Who is responsible for protecting privacy?
• Privacy breaches
• Risk management
Cryptography

• When it comes to data encryption, cloud providers still have a long road ahead.

• Alex Staomes, an iSec Partners researcher, claimed that cloud computing should be approached from the cryptographic angle.

• Security questions for cloud providers:
  • Data on write: Are files transferred to/from cloud servers encrypted by default?
  • Data at reset: Are files stored on cloud servers encrypted by default?
  • Data retention: If files on cloud servers are encrypted and there is a request from law enforcement to decrypt data, than what do you do?
Identity management

• Registration of identities
  • organizations that transfer their user accounts in the cloud must make sure to update the management of the user accounts

• Authentication
  • it is important the authentication of users should be managed and implemented in a trustworthy way (one time password or SSO - more protected; classic username and password approach - less protected)

• Authorization
  • specifies what rights every individual user account have in the cloud

• Federation of identities
  • is it possible to establish a single application (SSO)?

• Access control
  • access control requirements vary widely depending on whether the end-user is individual use or an organization.
OpenStack

• OpenSource platform to build private and public clouds.

• We will concentrate on the following:
  • Review of existing components
  • Authentication
  • Authorization
  • Recommendations
• Overview of versions
  • Austin (21. October 2010)
  • Bexar (3. Februar 2011)
  • Cactus (15. April 2011)
  • Diablo (22. September 2011)
  • Essex (5. April 2012)
  • Folsom (Fall 2012)
OpenStack

• **Components**
  
  • **OpenStack Compute (nova)**
    - Provision and management of large networks of virtual machines.
  
  • **OpenStack Object Storage (Swift)**
    - Create petabytes of reliable storage using standardized hardware.
  
  • **OpenStack Image Repository (Glance)**
    - Catalog and manage massive libraries of server images
# OpenStack – General overview

<table>
<thead>
<tr>
<th>DIABLO version</th>
<th>Authentication</th>
<th>Authorization</th>
<th>Issues</th>
<th>Suggestions for improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>keystone</td>
<td>Token</td>
<td>Simple password / unprotected passwords in novarc file</td>
<td>Password complexity / SSL</td>
</tr>
<tr>
<td>Object Storage</td>
<td>swAuth/tempAuth (keystone)</td>
<td>Token</td>
<td>Unprotected passwords/non-complex passwords</td>
<td>SSL / Password complexity and keystone usage</td>
</tr>
<tr>
<td>Image Service</td>
<td>Keypairs (key pairs)</td>
<td></td>
<td>Keys are publicly accessible, if not stored in the right location</td>
<td>Correct read/write permissions</td>
</tr>
</tbody>
</table>
OpenStack (Object Storage)

• User management is role based
  • Users are not granted to administrate any users themselves
  • Admin can add users to an account which he is allowed to administrate
  • Reseller admin has admin permissions on all of the accounts and cannot add other Reseller admins
  • Super admin is the most powerful user who can perform all user management procedures, including adding Reseller Admins
# OpenStack (Object Storage)

<table>
<thead>
<tr>
<th></th>
<th>devAuth</th>
<th>swAuth</th>
<th>tempAuth</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin (unprotected password)</strong></td>
<td><code>/etc/swift/auth-server.conf</code></td>
<td><code>/etc/swift/proxy-server.conf</code></td>
<td><code>/etc/swift/proxy-server.conf</code></td>
</tr>
<tr>
<td><strong>Users (unprotected passwords)</strong></td>
<td>SQLite DB</td>
<td>JSON-encoded text files</td>
<td><code>/etc/swift/proxy-server.conf</code></td>
</tr>
<tr>
<td><strong>Access to .conf and db files</strong></td>
<td>Anyone</td>
<td>Owner of .conf file</td>
<td>Owner of .conf file</td>
</tr>
<tr>
<td><strong>Used in Diablo version</strong></td>
<td>Dropped</td>
<td>Optional</td>
<td>Built-in</td>
</tr>
<tr>
<td><strong>Admin has access to all date of users</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Object Storage - Passwords

• Current user authentication is not in accordance with CSA
  • Password in plain text format
  • Minimal password length is not determined (only one character can be used)
  • Password complexity
• Weakness in tempAuth identified and reported to OpenStack community
• Solution?
  • Access rights
  • Python module hashlib
  • Encryption of super admin password in .conf file
  • Use of SSL
ObjectStorage – Portability of stored data

- Administrator has the possibility to retrieve authentication data of users
  - 1. step
  - 2. step

- Different types of administrators:
  - Super Admin, Reseller Admin, Admin
  - Reseller Admin
    - can obtain the URL address of existing users
    - can download or even delete files belonging to any user on any of the accounts

- Solution? Data encryption before transmission!
OpenStack - keystone

• OpenStack has recently added support for identity service Keystone

• Currently supports:
  • Authorization with tokens and authorization service
  • Connection with LDAP

• In future versions it will be possible to connect with:
  • OAuth (Open Authorization)
  • openID (Authentication mechanism)

• Data storage in SQLite DB or MySQL
The Keystone Identity Manager

1. Alice wants to launch a server
   - A Temporary Token is created
   - The Temporary Token is provided along the request

2. Alice requests all the tenants she has
   - A generic catalog is sent
   - The Temporary Token is provided along the request

3. Keystone provides Alice her list of Services
   - Keystone sends the Services the tenant has
   - The tenant token is provided
   - Alice determines the correct endpoint to launch a server
   - The token is provided along the request

4. The service verifies Alice's token
   - Is the Token correct?
   - Does it allow that service usage?

5. Keystone provides extra infos along the token
   - Alice's tenant is authorized to access the service
   - The token matches with the request
   - That token belong to the user Alice
   - The service validates the request against its own policy

6. The service executes the request
   - The service creates a new server

7. The server reports the status back to Alice
   - The server has been created
   - The server is reachable here
OpenStack (Tokens)

• Authorization (security token generation)
  • Security tokens in OpenStack play the same role as sessions identifiers for web applications
  • Tokens are stored in /etc/swift/account.ring.gz
  • Python UUID version 4 is used to generate tokens, which use
    • /dev/random (Ubuntu) as a source of randomness
OpenStack – Reliability

- Hazard perception?
  - Server load monitoring
  - CPU, memory etc.
- Isolation of infected
- Disabling access to an attacker
  - Network filtering (firewall)
  - Disabling user account
Recomendation

• ObjectStorage (Swift)
  • For development and testing is recommended to use tempAuth
  • For production is recommended to use swAuth or Keystone
• Password protection
• Data encryption
• Security portal (recently established)
• Subscribe to mailing list
Future work

• Cloud computing has many outstanding security concerns, some are technical, thus involving mechanisms for data processing, reliability, performance, etc.

• Therefore exploration does not STOP there and a lot of work can be done:
  • scripts for checking the security mechanisms for any deployment model in OpenStack (Swift part is done already)
  • SSL connections are set at the first install
  • Single-Sign-On for different cloud platforms and providers