clouds
Internet-Draft
Intended status: Standards Track
Expires: June 29, 2012

B. Khasnabish
ZTE USA
J. Chu
S. Ma
Y. Meng
ZTE
N. So
Verizon
P. Unbehagen
Avaya
M. Morrow
Cisco Systems [Switzerland] GmbH
M. Hasan
Cisco Systems

December 27, 2011

Cloud Reference Framework
draft-khasnabish-cloud-reference-framework-02.txt

Abstract

This document presents a cloud reference framework. In general, a cloud based system utilizes virtualized resources and applications. The reference framework is based on the survey of the SDOs and WGs that are focusing on cloud-based systems and services (draft-Khasnabish-cloud-sdo-survey). Both intra-cloud and inter-cloud reference frameworks are presented and the requirements of each layer are discussed.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 29, 2012.

Table of Contents

1. Introduction

We develop a general cloud reference framework. This reference framework describes basic functions in different layers to support the requirements of virtualized applications and services. This reference framework can be used to standardize a) features of functional elements and b) the interfaces between the functions.

Basically, the cloud reference framework includes

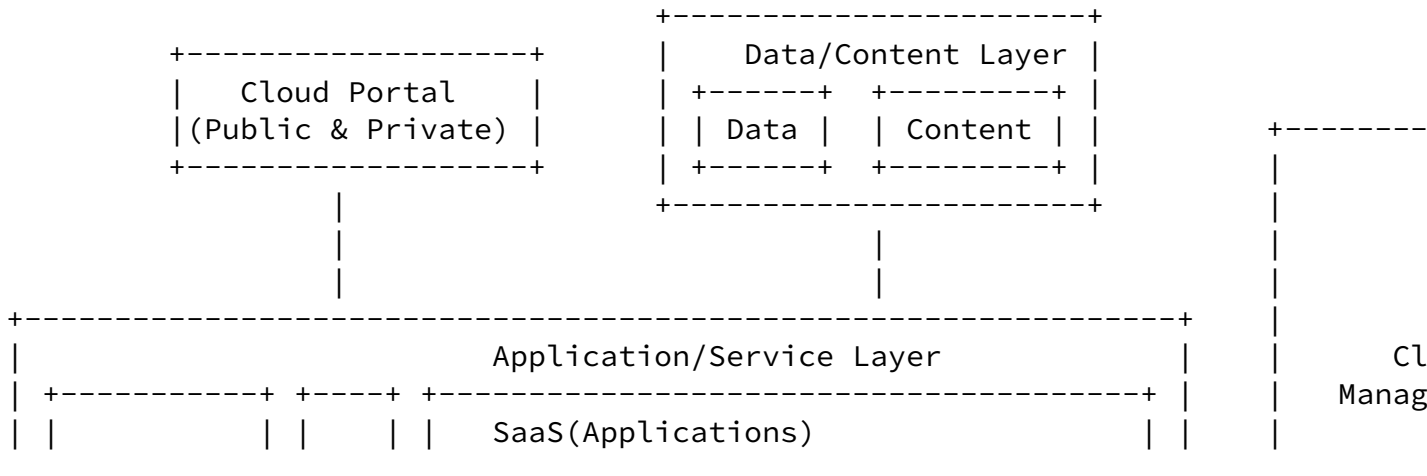
- Five horizontal layers
  - Data/Content Layer(DCL)
  - Application/Service Layer(ASL)
  - Resource Control Layer(RCL)
  - Resource Abstract and Virtualization Layer(RAVL)
  - Physical Resource Layer(PRL)
- One stacked vertical layer to support
  - Configuration management, registry, logging and auditing, security management, and service level agreement (SLA) management

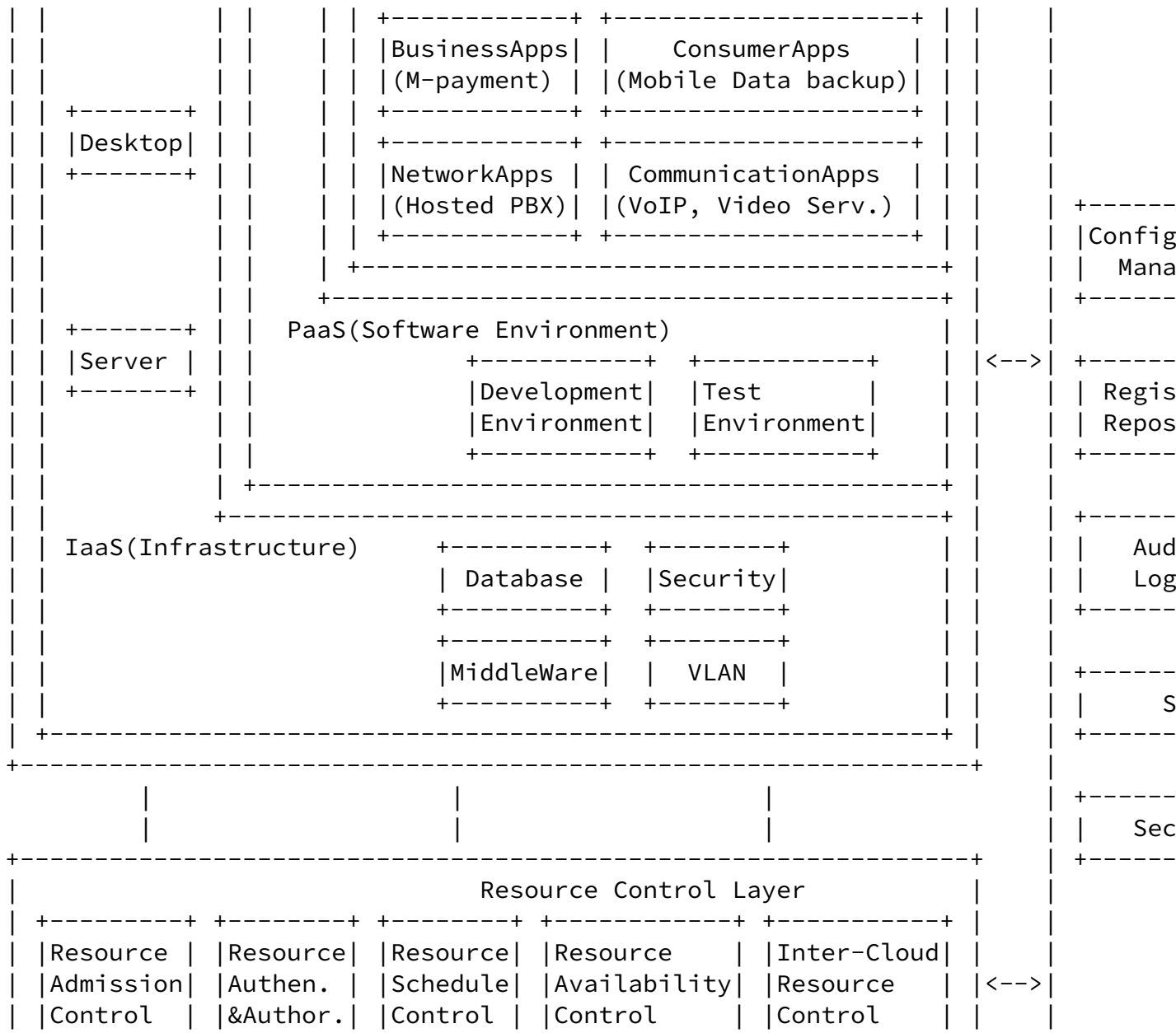
2. Terminology

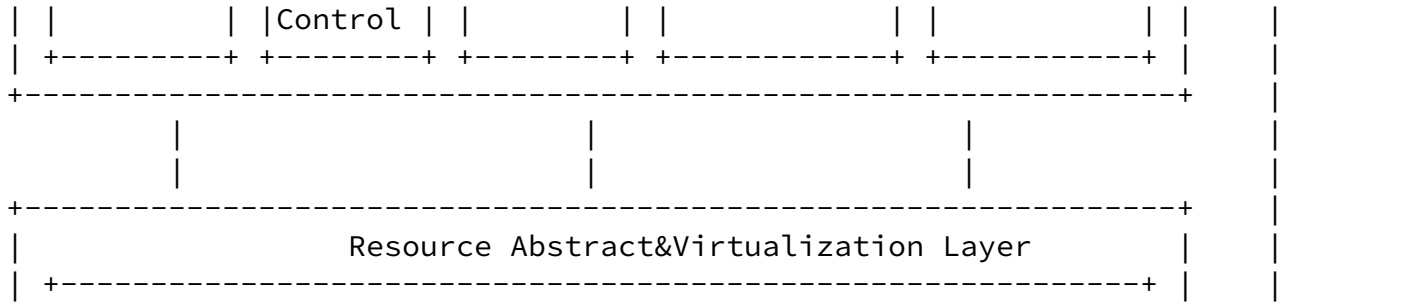
Clouds Discussion Archive:
http://www.ietf.org/mail-archive/web/clouds/current/maillist.html

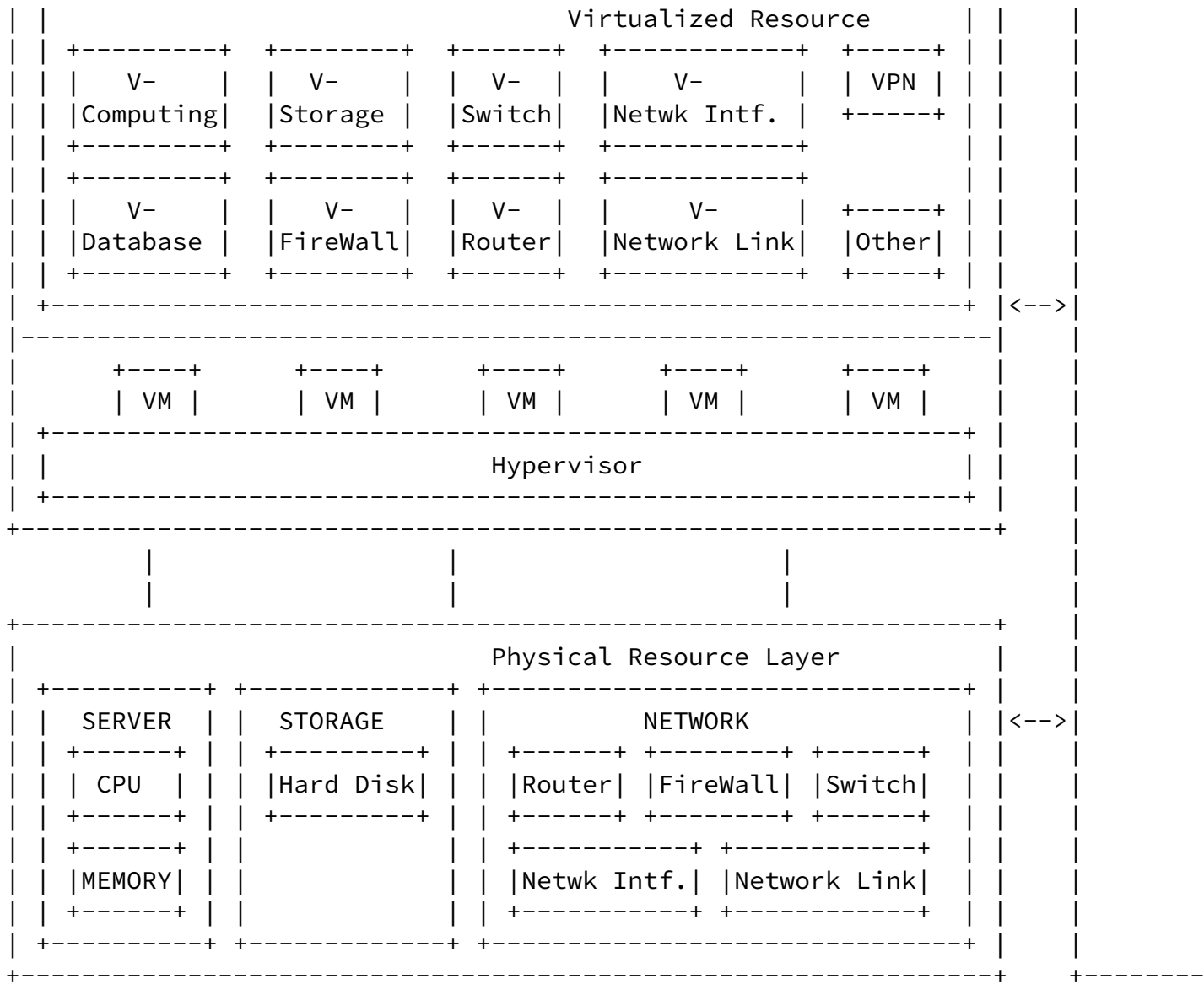
IETF Wiki Website for slides from Clouds bar BoFs:
http://trac.tools.ietf.org/area/app/trac/wiki/Clouds

3. Cloud Reference Framework




BusinessApps
(M-payment)
ConsumerApps
(Mobile Data backup)
Desktop
NetworkApps
(Hosted PBX)
CommunicationApps
(VoIP, Video Serv.)
Config
Mana
PaaS(Software Environment)
Server
Development
Environment
Test
Environment
Regis
Repos
IaaS(Infrastructure)
Database
Security
MiddleWare
VLAN
Aud
Log
S
Sec
Resource Control Layer
Resource
Admission
Control
Resource
Authen.
&Author.
Resource
Schedule
Control
Resource
Availability
Control
Inter-Cloud
Resource
Control


Control
Resource Abstract&Virtualization Layer



3.1. HORIZONTAL LAYERS

3.1.1. Application/Service Layer

Application/Service Layer defines the requirements of the basic functional entities based on the virtual resources needed to perform any tasks. The tasks are classified according to the 3 services

models IaaS, PaaS & SaaS. Some cloud services are illustrated as an

example of applications like:

- Server, desktop, database and VLAN for IaaS,
- Development environment and test environment for PaaS,
- Business, consumer, network and communication applications for SaaS.

The requirements the basic functional entities provided include the following characteristics and parameters of the virtual resources:

- Type of resources: CPU, memory, hard disk space, bandwidth, latency, jitter, and so on
- Amount of resources
- Nature of the resources: dedicated vs. shared, transport media exclusions, and so on
- Timing of the resources: scheduled vs. on-demand
- Duration of the Resources

3.1.2. Resources Control Layer

Resources Control Layer manages the virtual resources, ensuring that the resources are efficient, secure and reliable. With the interface of virtual resources, the layer integrates the resources as a whole supplied to upper layer. The layer has the following responsibilities:

- Resource security management. Resources must be accessed and owned by the right user, there are several function modules to fulfill this responsibility, include resource admission control, resource authentication and authorization control;
- Resource schedule control. The layer manages resources in form of resource pool. In a resource pool, the layer balances the virtual resources on a set of physical equipments to achieve higher hardware utilization. Virtual resources can be migrated between physical equipments if necessary, and also can be allocated according to user's priority grade.
- Inter-cloud resource control. Resources in a cloud can be shared with another cloud in some circumstances, so a cloud must control resources in other cloud, and supply cloud service to end users.

End users have no need to know where the resources are from.

- Resource availability control. The layer supports fault-tolerance on resources. It can allocate another copy of resources as a backup, and switch over when some faults raised.

3.1.3. Resources Abstraction and Virtualization Layer

Physical resources at the lowest level are the most complex to share among multiple users. There are several hardware details that don't need to visible to users, so we need a level of abstraction. In fact, these physical resources are abstracted first. The function of resources abstraction and virtualization layer is to convert physical resources to virtual resources. Virtual resources are contained in resource pool. Resources can be allocated to users from the resource pool, and released to resource pool when it's not needed.

Virtual resources are isolated from physical equipments, and have the features:

- Have all features as physical resources, resource users can't distinguish the difference between them;

- Can be allocated and released on demand;

- Support heterogeneous physical equipments, and supply a consistency view of resources to users;

- Support resource mobility, virtual resource can move from a physical equipment to another seamlessly;

There are several types of resources, such as computing resource, storage resource, database, bandwidth and network. According to the type of resource, there are different methods to realize virtualization. The variety function modules for virtualization are contained in Resources abstraction and virtualization layer. The layer has the following responsibilities:

- Through the interface of physical equipment to manage physical resource, mapping the virtual resources to physical resource;

- Supply the interface to upper layer to manage and access virtual resources;

- Hide the details of physical equipments, mask the difference between physical equipments.

3.1.3.1. Networking (Resources) Layer

Networking (Resources) layer converts and communicates network (LAN/MAN/WAN) capabilities and capacities(such as Bandwidth, ports, Latency matrices, Jitter matrices, Availability, Restoration capabilities, etc) into a set of resource pools that can be understood and used by the above layers. The resource pools include

- Virtual Switch
- Virtual Router
- Virtual Firewall
- Virtual Network Interface
- Virtual Network Link
- VPN

3.1.4. Physical Resources Layer

Physical Resources Layer include

- CPU
- Memory
- Hard Disk
- Network Interface Card
- Network Link
  - Ports
  - Bandwidth

3.2. VERTICAL LAYERS

3.2.1. Cloud Management Layer

Cloud Management Layer (CML) provides monitoring and administration of the cloud network platform to keep the whole cloud operating normally.

Key features of the Virtual System Management Layer include:

- Automatically deploying the cloud system based on the configuration data and policy
- Real-time monitoring and alerting of cloud status, resource usage and performance of cloud
- Reporting and charting of historical events and performance metrics
- Flexible IT management and operational status displays
- Authenticating/Authorizing the published cloud service registry
- Auditing the cloud environment to check whether its running smoothly
- Controlling the SLA implemented in the cloud system
- Maintenance concerned with performing repairs, upgrades and new nodes join into the Cloud
- Providing Security mechanism for the Cloud

Basically CML includes four Functions:

- Cloud Configuration Management
- Cloud Service Registry and Audit Management
- Cloud SLA Management
- Cloud Service Security Management

3.2.1.1. Cloud Configuration Management

Cloud Configuration Management (CCM) is responsible for establishing and maintaining the consistent performance of the Clouds system or product and its functional and physical attributes throughout its life-cycle. It mainly focuses on configuring the cloud system and retrieving the configuration information automatically. Requirements on Configuration Management are as follows:

- Provide efficient and reliable means to provision large amounts of configuration data. Current versions of provision configuration data are CLI, SNMP and NETCONF.

- Provide secure means to provision configuration data. The system must provide support for access control, authentication,

integrity-checking, replay- protection and/or privacy security services.

- Provide means to send feedback information to the management system. Feedback information include configuration data confirmation, network status and monitoring information, specific events, etc.

- Provide expiration time and effective time capabilities to configuration data. It is required that some configuration data items be set to expire, and other items be set to never expire.

- Provide facilities to help in tracing back configuration changes

- Be flexible and extensible to accommodate future needs. Configuration management data models are not fixed for all time and are subject to evolution like any other management data model.

- Leverage knowledge of the existing SNMP management infrastructure, such as the knowledge of and experience with MIBs and SMI.

- Basically, the CM includes CM database, CM policy, system change management and version management.

- Related protocol: CLI, SNMP, NETCONF

3.2.1.2. Cloud Service Registry/Repository

Service Registry/Repository provides management and governance capabilities that enable the published cloud service to be authenticated in the cloud system and accessed by service client. It facilitates storing, accessing and managing service information, called service metadata, so that the cloud service can be easily published, selected, invoked, enriched, governed and reused.

Requirements on Service Registry/Repository are as follows:

- Authentication & Authorization. Once a service is published by the service provider to the Cloud system, it should be authenticated to check the authority of the provider and the support capability of the Cloud. If the check is passed, the service is authorized and put into the repository, and the services and related metadata are classified into groups.

- Publication & Discovery. The authorized service is published in the Cloud system, and you can keep an accurate record of the deployed services in your repository platform. The user can find the service from the repository platform using the service

discovery engine. Cloud Service Registry/Repository is capable of a powerful query mechanism allows you to search and find the services that best fit the requirements of a given process.

- Service Access Control. The service repository enables dynamic and efficient access to services information by enabling selection of services based on service metadata.

- Optimize service usage. Service manage capability enables management of service metadata, as well as service interactions, dependencies and redundancies. You can classify services based on business objectives, manage policies for service usage and monitor how services are changed and versioned. This capability helps you optimize the use of services in cloud system by exchanging service metadata with runtime monitoring tools and operational data stores.

- Impact analysis. By maintaining relationships, Cloud Service

Registry/Repository has extensive support for analyzing the impact of service introduction, deletion or alteration.

- Service life cycle. By creating user-definable entities and customizing the service life cycle, you can configure Cloud Service Registry/Repository precisely according to your business needs. You can easily implement best practices for service life-cycle management with the ability to promote services and life-cycle validations.

- Policy support. You can publish policies that apply to services stored in Cloud Service Registry/Repository. These policies help you institute best practices in your Cloud deployment.

- Governance profile. To help you get started easily and quickly, Cloud Service Registry/Repository provides a welldefined service model that includes templates, associated life cycles, governance policies, a classification system, roles and perspectives.

3.2.1.3. Cloud Audit Management

Cloud Audit Management (CAM) is to provide an agent through which cloud providers and authorized consumers automate the Audit, Assertion, Assessment, and Assurance of the cloud infrastructure (IaaS), platform (PaaS), and application (SaaS) environments to reduce the risk. A common interface and namespace can be used by the CAM to facilitate these audit functions.

Requirements on CAM are as follows:

- A well-defined objective and scope tied to quality compliance and risk management processes

- Establish clear policies, procedures, and metrics. Audit management should incorporate defined policies, procedures, and metrics as performance benchmarks. These elements should be reviewed periodically for continuous improvement.

- Integrate essential quality management processes. An effective audit management system should automate the entire audit process and include integration of the following processes:

* Corrective and preventive actions

* Change control

* Non-conformance tracking and management

* Regulatory document/content management

* Custom reporting, analysis and analytics

* Training

* Compliance intelligence dashboard

3.2.1.4. Cloud SLA Management (CSM)

SLA is a part of a service contract where the level of service is formally defined between Cloud service providers and Cloud customers. Within the terms of their contracts, the SLA will have a technical definition, typical terms as MTTF (Mean Time To Failures), MTTR (Mean Time To Repair), ABA (Abandonment Rate), ASA (Average Speed to Answer), TSF (Time Service Factor), FCR (First Call Resolution), TAT (Turn Around Time), Uptime Agreements, various data rates, etc.

SM is to control the usage and receipt of resources from and by third parties. The strategy of CSM includes the negotiation of the contract and the monitoring of its realization in real-time. Thus, CSM encompasses the SLA contract definition (basic schema within QoS parameters), the SLA negotiation, the SLA monitoring, and the SLA enforcement.

SM also need define rate reductions and discounts that are applied when a service provider fails to meet the desired service parameters or does not fulfill an agreement.

Requirements on CSM are as follows:

o SLA template specification. when service provider publishes a new service, an SLA template which describes the contract type that goes with the resource usage will be specified. Such a template may be hard to define we propose to develop a skeleton of a

template with the corresponding write-up procedure.

- Negotiation. Service client and service providers have to agree on the terms of the SLA binding them and also with the consequences to violations.

- Resource Optimization. When the SLA processes the service access request from the service client, it also has to keep in mind the optimization of the usage of resources, and the QoS guaranteed in the SLA.

- Monitoring. Once the cloud system has started providing access to its resources, it should monitor the operating resources. The monitored information is then used to prove the QoS agreed within the SLA being satisfied.

- Re-negotiation. Some party of the contract may wish to change the resource usage policy while the system is running, in order to comply with a change in external conditions. In order to keep the behaviour of the process continuous, the agreed SLA need adjust to assure the process vitality after migration and resource shortage.

- Evaluation. Besides the running information is interested by the managers and users, other data like contract violations or global statistics are also needed in order to verify the SLA. Evaluation is the process of analyzing the previously monitored information. An evaluation daemon may be proposed, based on the monitoring tools developed.

- Accounting. The use of a resource generates an accounting sheet which describes the resources used and aligns them with the billing rules agreed in the SLA. This is a base to draft the real financial exchange, which can be in disfavour of the provider in case of failure to comply with the compromised QoS. This subject is very sensible, and the development of tools for such themes should not be taken lightly.

Related Language: WSLA, ITIL

3.2.1.5. Cloud Service Security Management

Cloud Service Security (CSS) provides a set of mechanisms (e.g. IP address filtering, message integrity & confidentiality, private key encryption, dynamic session key encryption, user authentication and

Service certification) to protect Cloud Services and their operating environment from damage.

Requirements on CSS are as follows

- Licensing. It is likely that your service is made up of many different components, most of which have some type of licensing agreement associated with them. You will need to review each of those agreements to determine if, or how, those licenses will be affected by deployment in a cloud. If your service uses a component that is licensed by CPU and you deploy it in a cloud environment designed to launch new instances and request more resources as load increases, for example, you could easily exceed your CPU license limit. You will need to understand how your licenses affect your ability to scale.

- Processing requirements and memory locks. If dynamic scalability is your main reason for looking to the cloud, then your application should be designed to take advantage of a parallel architecture. If the application is designed with multi-threaded code that allows processing to be split into small chunks, it's well-suited for use within the cloud. An application that is designed around single monolithic thread processing, on the other hand, will find it difficult to take advantage of the cloud's distributed nature.

- Communication protocol. The cloud is based on the Internet Protocol (IP), so for an service to be considered, it must use IP as its communication mechanism. While there are many protocols that can be run over IP, the IP layer can provide security mechanism to protect the security of the transmitted data.

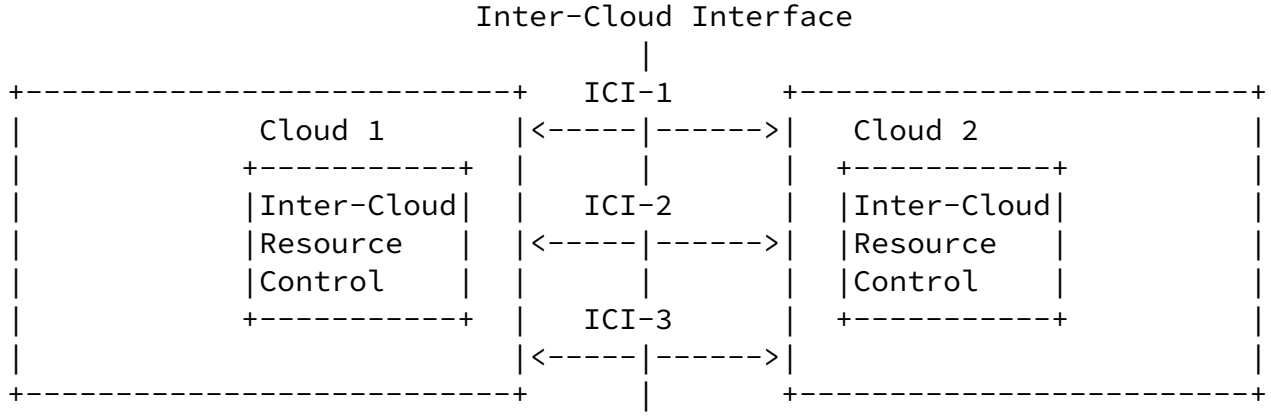
- Data security. The service needs to provide security at the data storage, processing and transmission stages. Data at rest must be protected by the service, that is the service must provide a mechanism to protect the data stored in the cloud. Data in transit needs to be protected either at the service or the transmission level. Most services choose the transmission level for protection and the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols are often used. Server to server communications need to ensure the security from one cloud instance to another cloud instance.

4. Inter-Cloud Framework

A Cloud Service Provider (CSP) can offer services using one or more date centers (DCs). These DCs can provide virtualized compute, storage, and networking resources on on-demand basis to the Cloud Service Consumers (CSC). Therefore, the DC infrastructure does not necessarily need to be a static entity as in a traditional DC. The infrastructure resources can span multiple CSPs and the entity that is offered to the consumer can be referred to as the Infrastructure as a Service (IaaS).

With the IaaS, a CSC can acquire and release resources on on-demand basis.

We therefore define an Inter-Cloud as a interconnction of clouds where two or more cloud service providers (any combination of Service-Provider-owned, private, public, etc.) can collaborate. The objective of the collaboration is to dynamically distribute the workloads based on mutually agreed upon service level agreement (SLA).



4.1. Inter-Cloud Requirements

Inter-cloud requirements may be articulated as follows:

- Provide a mechanism for resource search and discovery, to determine which serving cloud might have certain resources

available (including a match making mechanism).

- Provide a mechanism to authenticate participating entities.

- Provide a mechanism for requesting, controlling, and releasing resources between two clouds.

- Provide a secure transport channel between the interconnecting entities.

- Provide end-to-end isolation to support multitenancy.

- Provide a mechanism for monitoring, assuring, and troubleshooting across the interconnection.

- Provide a mechanism for defining the monitoring metrics such as Delay-Jitter-Loss. This may be useful for monitoring a flow such as TCP/UDP between IP prefix and a destination address across the interconnection.

4.2. Possible Inter-Clouds Interfaces

- Provisioning

- Signaling

- Control

- Monitoring

- Management

- Transport

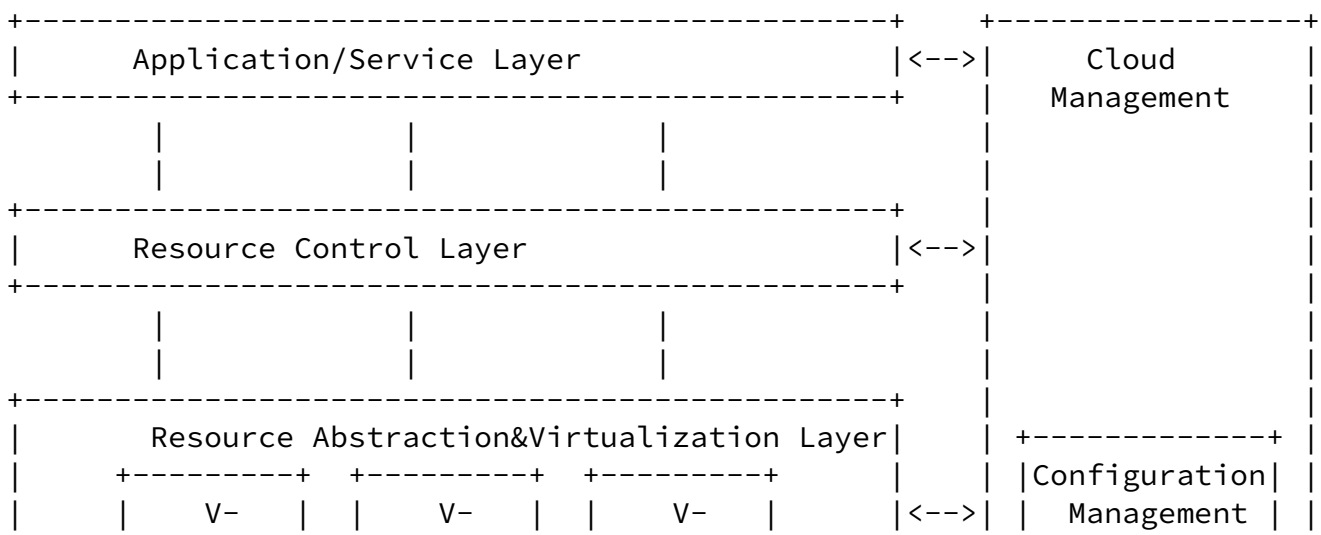
- Security

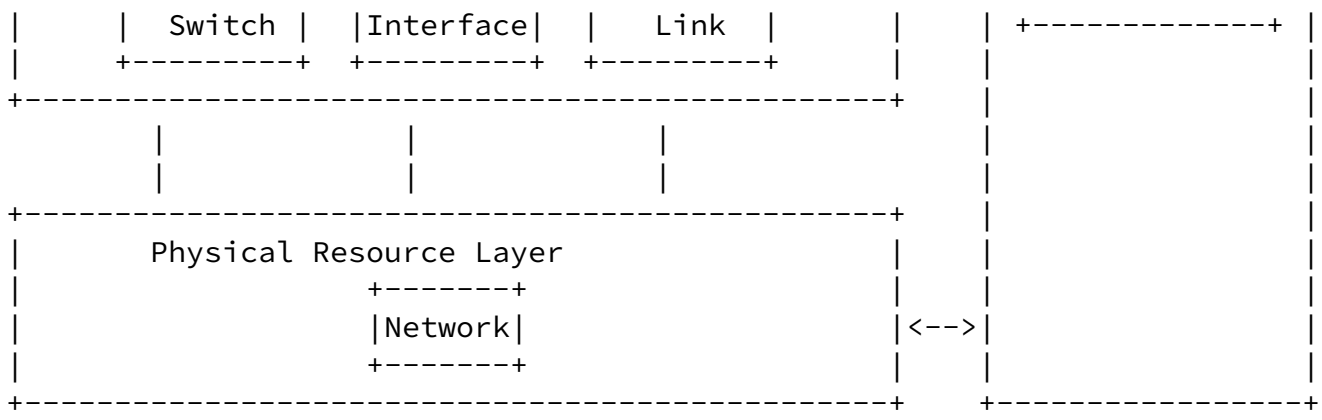
- Naming, Addressing and Translation (if/as needed)

5. Use Cases

5.1. Virtual Network Management

Configuration Management in VSML is responsible for creating and managing virtual network through the interface between the Configuration Manager and the Resources Abstraction&Virtualization Layer or Physical Resource Layer. This section is based on the information available in the following draft: draft-Okita-Clouds-VNM-model-for-PaaS-00, Okita-Clouds-VNM-model-for-PaaS-Sept10.pdf





5.2. Telecom Network Virtualization

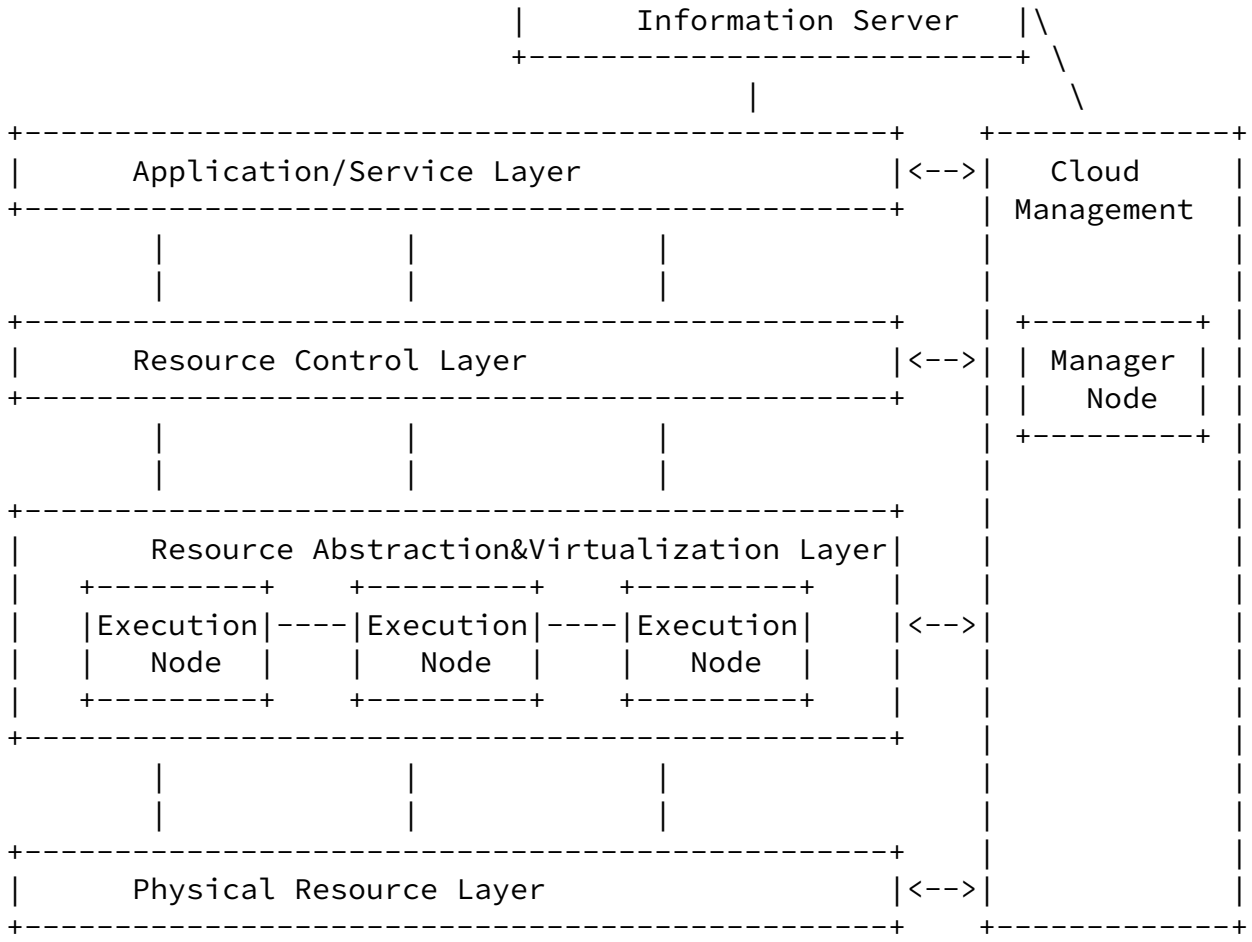
Telecom Network virtualization is the technology that enables the creation of logically isolated network partitions over shared physical network infrastructures so that multiple virtual telecom networks can simultaneously coexist over the shared infrastructures.

The objectives of telecom network virtualization is to

- scale telecom services on demand
- improve reliability and availability
- efficiently use infrastructure

In order to facilitate the deployment of telecom network virtualization, Manager Node provides control procedures such as creating Functional (Service) Entity operating on Execution Node, monitoring the status of Functional (Service) Entity and Execution Node, measuring the performance, retrieving deployment data from Infromation Server, and so on.

This section is based on the information available in the following draft: draft-Yokota-Clouds-Telecom-Net-Virtualization-00, Yokota-Clouds-Telecom-Net-Virtualization-Sept10.pdf



Manager Node manages the Execution Node and communicates with Information Server to get configuration data.

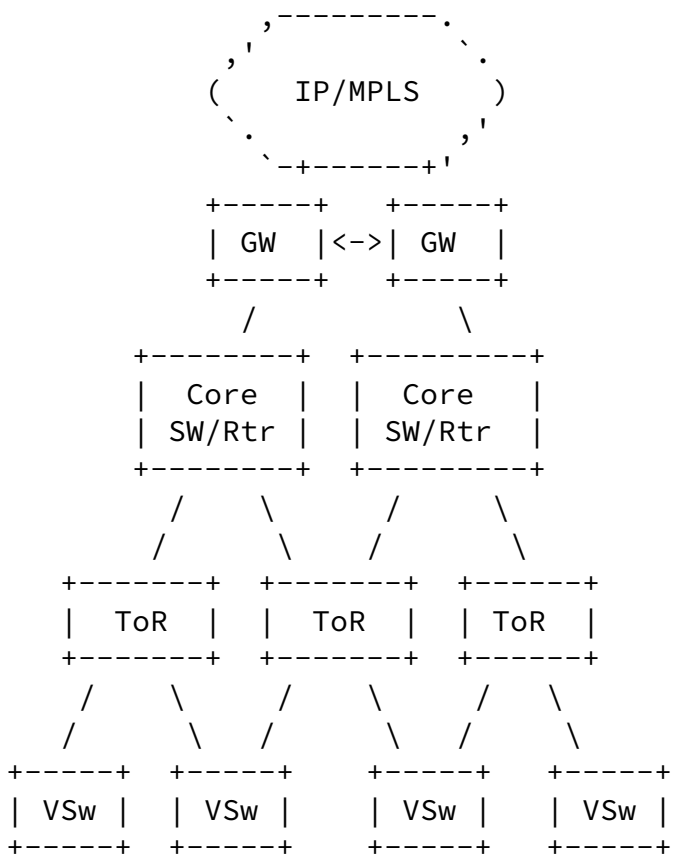
Execution Node is a physical or virtual machines on which target telecomm functions (software) are running. For example, in IMS, CSCF and HSS are candidates of functions.

Information Server (optional) is used for discovery and assignment of Execution Node for a session (e.g., P-CSCF at a UE's registration).

5.3. Virtual Data Center

Virtual Data Center (VDC) can be constructed base on the virtualized resources in cloud environment.

This section is based on the information available in the following draft: draft-bitar-datacenter-vpn-applicability-01.txt, draft-armd-datacenter-reference-arch-01.txt.



The following network components are present in a DC:

- VSw or virtual switch - software based Ethernet switch running inside the server blades. The individual VMs appear to a VSw as IP hosts connected via logical interfaces. The VSw may evolve to

support IP routing functionality.

- ToR or Top of Rack - software-based or hardware-based Ethernet switch aggregating all Ethernet links from the server blades in a rack representing the entry point in the physical DC network for

the hosts. ToRs may also perform routing functionality.

- Core SW (switch) - high capacity core node aggregating multiple ToRs. This is usually a cost effective Ethernet switch. Core switches can also support routing capabilities.

- DC GW - gateway to the outside world providing DC Interconnect and connectivity to Internet and VPN customers. In the current DC network model, this may be a Router with Virtual Routing capabilities and/or an IPVPN/L2VPN PE.

5.4. Security Framework for VDCS

Virtualized Data Center Services (VDCS) Security Framework is a reference framework to build secure and interoperable services on top of a virtualized infrastructure. A security framework and the associated requirements for Protocols, Profiles, Network Interfaces, Operations and Management, and Application Interfaces(APIs) need to be proposed in an environment where virtualized resources are shared among a variety of public and private subscribers/clients seamlessly.

The various applications and interworking protocols developed by the IETF MAY need to be extended or profiled to support the security requirements of virtualized services and infrastructure environment.

- Applications & Services: The most widely used protocol that is in use today for application & services development areas like HTTP have been considered for the applications in the virtualized environment. The protocol may have to be profiled or extended with significant changes to be ready to handle the security requirements in a virtualized environment.

- Infrastructure Operations & Management: The various security parameters related to operations and management of virtualized network resources in multiple administrative domains may need to be defined. The results of monitoring may need to be exchanged periodically to support the private and public virtualized domains and infrastructure in order to maintain the expected end-to-end security.

The above protocol extension and operations & management requirements can be implemented in current cloud reference framework (CRF) based on the security functionality provided by cloud management layer,

resource authentication and authorization mechanism, and services/ users admission control.

This section is based on the information available in the following draft: draft-karavettil-vdcs-security-framework-00.txt

6. Conclusion

We presented a high-level cloud reference framework. A few examples on utilization of the reference framework are also discussed.

7. Security Considerations

--[Editor's note] Will be added in future.

8. Acknowledgement

We thank T. Sridhar (thsridhar@gmail.com), Simon Leinen (simon.leinen@switch.ch) for comments on an earlier version of this document.

9. IANA Considerations

This document has no actions for IANA.

10. Normative references

[Cloud SDO]
Khasnabish, B., "draft-khasnabish-cloud-sdo-survey-02", June 2012.

[Cloud ServiceMobility]
Yokota, H., "draft-yokota-cloud-service-mobility-01", March 2011.

[DSP0004] DMTF, "Common Information Model (CIM) Infrastructure", May 2009.

[DSP1041] DMTF, "Resource Allocation Profile", June 2009.

[DSP1042] DMTF, "System Virtualization Profile", April 2010.

[DSP1057] DMTF, "Virtual System Profile", October 2009.

[DSP1059] DMTF, "Generic Device Resource Virtualization Profile", July 2009.

[ITU-T FGCC]
FGCC, "cloud-o-0046-funct_ref_arch", April 2011.

[ITU-T Y.2011]
ITU SG13, "Y.2011_General principles and general reference model for NGN", October 2004.

[Industry WorkItem]
Khasnabish, B.,
"draft-khasnabish-cloud-industry-workitems-survey-02",
June 2012.

[RFC2119] IETF, "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[RFC4741] IETF, "NETCONF Configuration Protocol", December 2006.

[UML] OMG, "Unified Modeling Language", September 2002.

[VDCS Security]
Karavettil, S.,
"draft-karavettil-vdcs-security-framework-00.txt",
June 2012.

[VNet Model]
Okita, H., "draft-okita-ops-vnetmodel-03", April 2011.

Authors' Addresses

Bhumip Khasnabish
ZTE USA
55 Madison Avenue, Suite 160
Morristown, NJ 07960
USA

Phone: +001-781-752-8003
Email: vumip1@gmail.com

Chu JunSheng
ZTE
No.50 Ruanjian Dadao Road, Yuhuatai District
Nanjing
China

Phone: +86-25-8801-4630
Email: chu.junsheng@zte.com.cn

Ma SuAn
ZTE
No.68 Zijinghua Rd,Yuhuatai District
Nanjing
China

Phone: +86-25-5287-8189
Email: ma.suan@zte.com.cn

Meng Yu
ZTE
No.50 Ruanjian Dadao Road, Yuhuatai District
Nanjing
China

Phone: +86-25-8801-4631
Email: meng.yu@zte.com.cn

Ning So
Verizon
2400 N. Glenville Dr.
Richardson, TX 75082
USA

Phone: +1-972-729-7905
Email: ning.so@verizonbusiness.com

Paul Unbehagen
Avaya
USA

Phone: +1-919-606-8845
Email: paul@unbehagen.net

Monique Morrow
Cisco Systems [Switzerland] GmbH
Richistrasse 7
CH-8304 Wallisellen
Switzerland

Phone:
Email: mmorrow@cisco.com

Masum Hasan
Cisco Systems
3675 Cisco Way
San Jose, California 95134
USA

Phone:
Email: masum@cisco.com