EGERTON UNIVERSITY

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

ACMP 473: GRID AND CLOUD COMPUTING

CLOUD INFRASTRUCTURE REFERENCE MODEL

GROUP 3: CONTROL LAYER

Members

Alfred Arusei- S13/02619/20

Venessa Mutende- S13/02589/20

Nicole Kipkorir - S13/02609/20

Joy Wanjiku - S13/02580/20

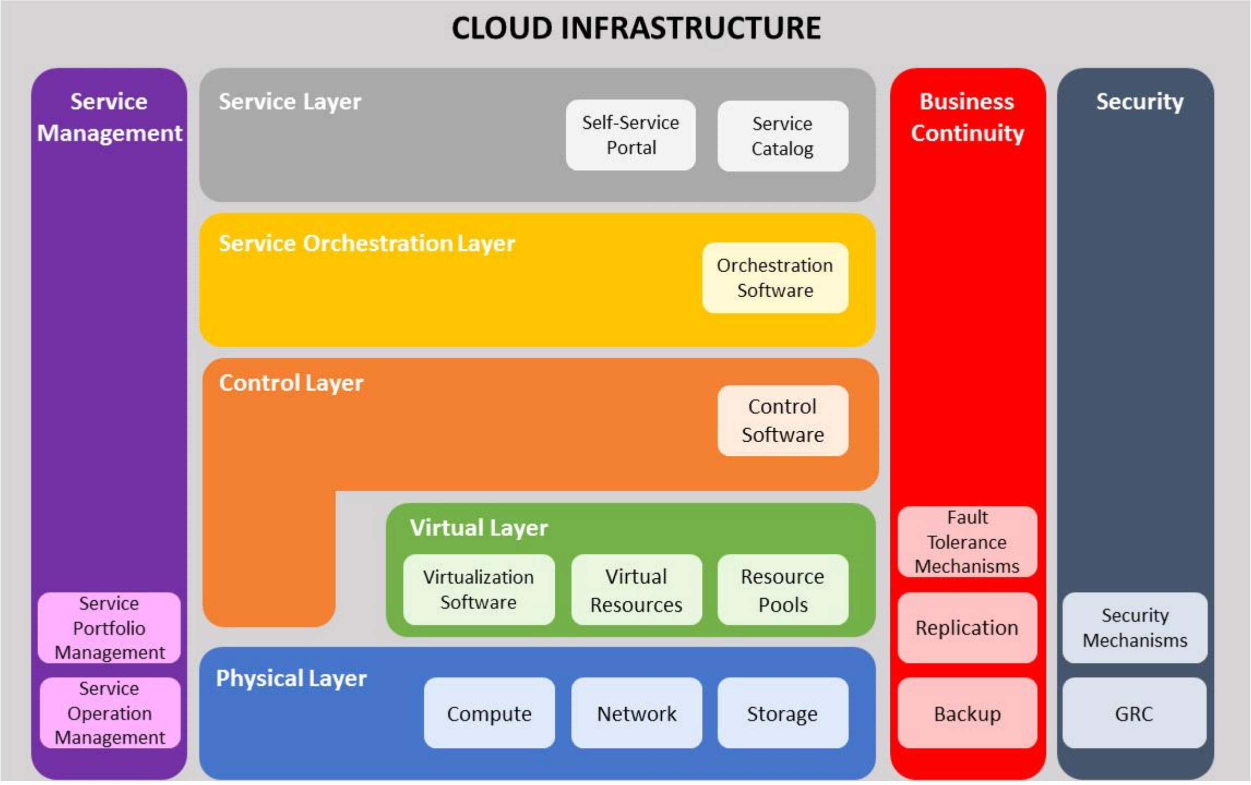
Kefa Nathan – S13/02621/20

Ian Mwendwa -S13/02326/19

Module: Control Layer

Objectives.

1. Description of the control layer and its key functions.
2. Description of the control software and its types.
3. Software-defined approach for managing IT infrastructure.
4. Resource optimization techniques.



The control layer—highlighted in the figure above with the orange color - enables to manage and control the cloud infrastructure.

Description of the Control Layer and its Key Functions.

The control layer includes control software that are responsible for managing and controlling the underlying cloud infrastructure resources and enable provisioning of IT resources for creating cloud services. Control layer can be deployed on top of the virtual layer or on top of the physical layer. This layer receives request from the service and orchestration layers, and interacts with the underlying virtual and physical resources for provisioning IT resources. For example, when a consumer initiates a service request (a VM instance with 4 GB RAM and 500 GB storage), based on the workflow defined by the orchestration layer for this service, the control layer provisions the required resources from the resource pool to fulfill the service request. This layer also exposes the resources (physical and/or virtual) to and supports the service layer where cloud services interfaces are exposed to the consumers.

The key functions of the control layer includes:

- Enables resource configuration and resource pool configuration
- Enables resource provisioning
- Executes requests generated by service layer
- Exposes resources to and supports the service layer
- Collaborates with the virtualization software and enables
- Resource pooling and creating virtual resources
- Dynamic allocation of resources
- Optimizing utilization of resources

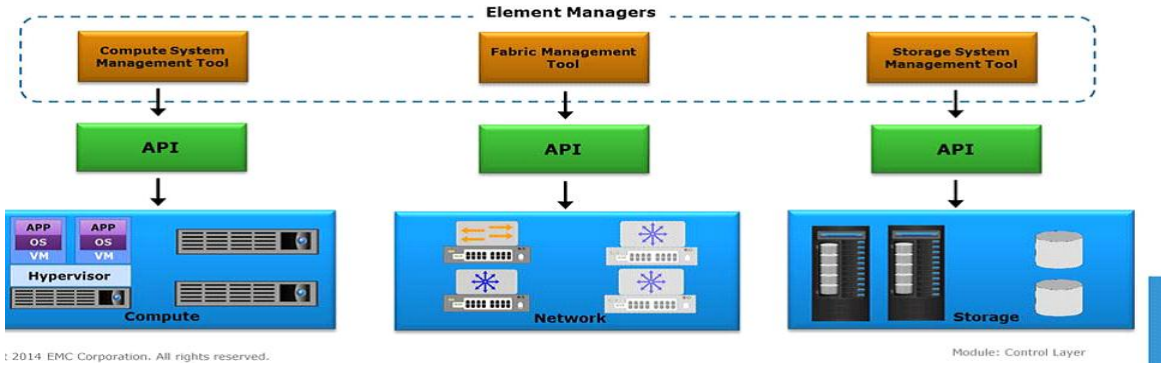
Control Software and its Types

The control software ties together the underlying physical resources and their software abstraction to enable resource pooling and dynamic allocation of resources. It provisions resources for services and provides information about provisioned or consumed resources by service instances to the cloud portal and billing system. Before configuring the cloud resources, the control software should discover all the underlying resources in order to know the total available resources in the environment for service provisioning. This also provides a complete view of all the resources in the cloud environment and enables to centralize management of IT resources.

The two types of control software are element manager and unified manager.

Element Manager -:

Infrastructure component vendors may provide the element managers as built-in or external software to configure those components or elements. For example, storage vendors offer element manager along with the storage system to configure and make the storage resources available for the applications or services. Similarly, network and compute systems are managed using network and compute management software, respectively. The figure below depicts how various element managers are involved in managing the infrastructure components independently. Typically the underlying infrastructure is managed from element manager through either graphical user interface (GUI) or command line interface (CLI).

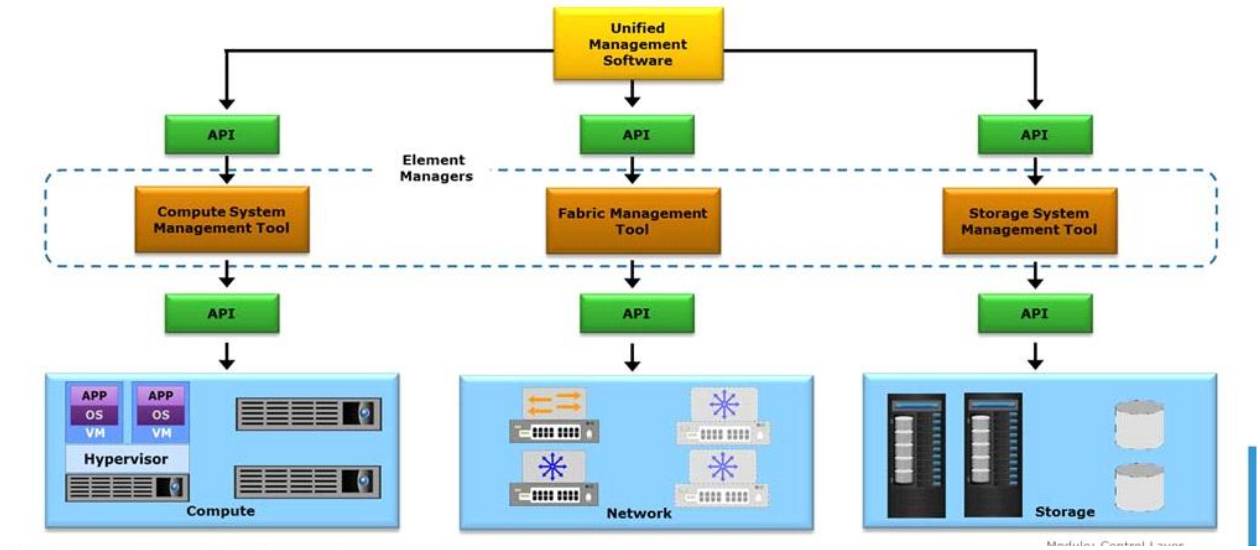


Tasks Performed by Element Manager.

- Enables to perform initial component configurations such as zoning, RAID levels and allows to modify them.
- Allows to expand resource capacity by detecting the newly added resources and adding them to an existing pool.
- Enables to identify the problem and performing troubleshooting.
- Monitors the infrastructure components for performance, availability, capacity and security.

Unified Manager-:

Unified manager provides a single management interface to manage cloud infrastructure resources and provisioning resources for services. Unified manager interacts with all standalone infrastructure elements through the elements' native APIs. It discovers and collects information on configurations, connectivity, and utilization of cloud infrastructure elements. Unified manager compiles this information and provides a consolidated view of infrastructure resources wherever they reside. In addition, unified manager identifies the relationships between virtual and physical elements for easy management. It provides a topology or a map view of infrastructure, which enables an administrator to quickly locate and understand the interconnections of infrastructure.



Tasks performed by Unified Manager.

- Exposes APIs that can be integrated with the orchestration layer to automate resource provisioning for cloud services.
- Enables adding or removing infrastructure resources to an already provisioned service.
- Provides a dashboard showing resource configuration and utilization. This enables administrators to perform monitoring, reporting, and route cause analysis.
- Perform compliance check during resource configurations by creating configurations policies which are applied to the resources consumed by a service instance.

Software-defined approach for managing IT infrastructure.

1. Access Control and Authentication: Implement robust access control and authentication mechanisms to ensure that only authorized personnel can make changes to the infrastructure. Utilize role-based access control (RBAC) to define permissions.

2. Audit and Logging: Enable comprehensive auditing and logging to track changes and activities within the software-defined

infrastructure. This helps in identifying unauthorized or suspicious actions.

3. Security Policies: Define and enforce security policies using software-defined tools and solutions. This includes firewall rules, security groups, and policies for software-defined networking and security.

4. Automation Control: Be mindful of automation scripts and orchestration workflows. Maintain control over these automation processes to prevent unintended changes or breaches.

5. Version Control: Use version control systems for configuration files and scripts to track changes and revert to known, stable states if necessary.

6. Change Management: Establish a formal change management process for any modifications to the software-defined infrastructure. This should include testing and validation before deploying changes into production.

7. Security Testing: Regularly conduct security assessments, vulnerability scans, and penetration testing to identify and address potential weaknesses in the infrastructure.

8. Backup and Disaster Recovery: Implement robust backup and disaster recovery solutions to ensure data and configuration can be restored in case of errors or security incidents.

9. Compliance and Governance: Ensure that your software-defined infrastructure complies with relevant regulations and standards, and establish governance practices to maintain control and compliance.

10. Training and Education: Continuously train and educate IT staff on best practices for maintaining control over software-defined infrastructure and security.

Benefits of Software Defined Approach.

Improves business agility by minimizing resource provision in time to get new services up and running.

Provides cost efficiency.

It helps cloud service providers to provide the most efficient and scalable cloud solutions.

Allows to create new innovative services using the underlying resources.

Provides a central point of access to all management functions.

Resource optimization techniques.

Resource Optimization is the process of allocating available resources in the most efficient manner to achieve desired goals. The key goals of resource optimization are controlling utilization of resources and preventing service instances from monopolizing the resources.

The key resource (compute, storage, and network) optimization techniques enables to optimize resource utilization, improve performance, and ensure meeting the service levels. Most of these techniques allow cloud administrators to set policies for managing resources effectively based on the requirements. Some of the techniques provide the capability to overcommit (more capacity is allocated than is actually available) CPU, memory, and storage resources to avoid frequent provisioning of resources, or to reduce disruption to application availability when adding new resources.

Compute

Hyper-threading

Memory page sharing

Dynamic memory allocation

VM load balancing across hypervisors

Server flash-cache

Storage

Virtual storage provisioning

Storage pool rebalancing

Storage space reclamation

Automated storage tiering

Cache tiering

Dynamic VM load balancing across storage volumes

Network

Balancing client workload across nodes

Network storm control

Quality of Service (QoS)

Traffic shaping

Link aggregation

NIC teaming

Multi-pathing

CONCLUSION

In summary, the control layer plays an important role in safeguarding the security, accessibility, and integrity of foundational resources and data. Employing a software-defined approach to manage IT infrastructure not only enhances business agility by expediting service deployment and driving cost-efficiency but also empowers cloud service providers to deliver highly scalable solutions. This approach encourages the creation of innovative services while consolidating management functions into a central point of access. Furthermore, resource optimization proves helpful in regulating resource utilization and averting the monopolization of resources by service instances.

REFERENCES.

Younis, Y.A., Kifayat, K. and Merabti, M., 2014. An access control model for cloud computing. Journal of Information Security and Applications, 19(1), pp.45-60.

Spring, J., 2011. Monitoring cloud computing by layer, part 1. IEEE Security & Privacy, 9(2), pp.66-68.

Yan, Q., Yu, F.R., Gong, Q. and Li, J., 2015. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE communications surveys & tutorials, 18(1), pp.602-622.

Almorsy, M., Grundy, J. and Müller, I., 2016. An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.