team
COMPUTERS

WHITEPAPER

Managed Hybrid Cloud Services

HYBRID CLOUD OVERVIEW

By the year 2025, 80% of the traditional/on-premise make-shift data centres will either migrate to public clouds or professionally managed data centres as per Gartner #1. The adoption of only public cloud platform might not address purposes of specific-need computing as that of Manufacturing 4.0, compliances related to R&D or that of a BFSI organization. The exponentially rising computing needs find a good addressal in hybrid cloud solution.

A hybrid cloud is a solution specific need for a mix of the on-premise infra, private cloud and public cloud. The workloads are moved across multiple clouds. Some of the important business drivers are listed as follows:

- Utility
- Cost optimization
- Security
- Reliability and
- Workload portability (particularly applications)

However, enterprises managing workloads across multiple clouds face dilemmas when it comes to manage a hybrid cloud setup. The skills that require to manage the magnitude of complexities involved in a hybrid cloud require industry best practices. There are multiple technical factors that need proper deliberation, expertise:

- Managed Scale-out/scale-up demands due to rising workloads
- Managed connectivities (e.g., Expressroute, Directconnect)
- Managed Security
- Managed Endpoints
- Managed Servicedesk and
- For CIO, availability of centralized Dashboards for all the services from different vendors are needed to monitor and measure SLAs for computing , connectivity, storage and backup. The configuration settings for a secured VPC (Virtual Private Cloud), VMs (including virtualization), vLANs, storages, backups have to be managed and supported with expertise on on-premise and clouds equally. Furthermore, when there are virtualization specific to platforms, it becomes imperative to look at not only present architectures but also agility in future.

Then there are problems which need prior planning with regards to identifying, moving, stabilizing and ongoing operational management. Here are some of the problems listed:

- **Security–**First & foremost is security. Since data will need to be accessed outside the enterprise, protection of personally identifiable information (PII) and other enterprise data calls for protection against any kind of security threats. The most secured cloud platform, whether we are using PaaS /SaaS, has to comply to the enterprise security policy.
- **Performance–**The complexity of data accessibility in a hybrid cloud far exceed the complexities involved in only public or only private cloud. The latency and performance being very important factors. For instance, address the resource-intensive workload requirements like that of SAP HANA accessibility.
- **Management & Governance –**The hybrid cloud usage adds to the challenge of maintaining visibility of cloud resources consistently and with least latencies, to manage

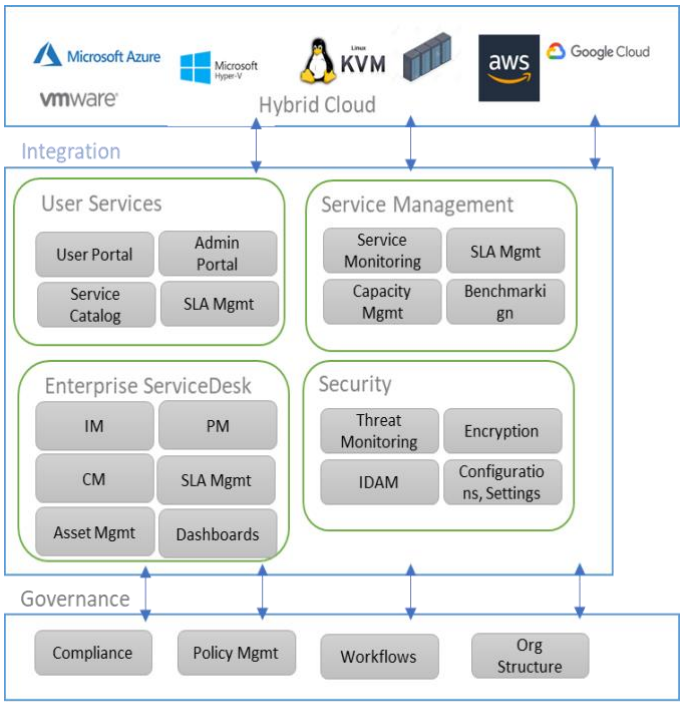
billings (e.g. chargebacks), and quality of service. As per another research by Gartner, most of the businesses running workloads on public clouds are overspending by 70%.

- **Compliance–**All standard, regulatory and statutory compliances need to be managed, controlled and audited against the internal security policies, industry mandates, standards and regulations.
- **Contractual obligation–**Enterprises often commit terms and conditions with a vendor for a lock-in initially under some perception. At a later time, moving out seems to be costly affair.

Managed Hybrid Cloud governance framework

There are multiple considerations that go into making a steady-state ready governance framework for a hybrid cloud.

I. **User Services:** For any request related to self-provisioning and enable self-service, where needed, a user portal is required. This should be rendered over the IP/intranet via browser/app. A catalogue of the available cloud services helps user covering all the essential cloud options and their offerings. The analytics and reporting helps into insight into the use of cloud services. At any point in time if user wants to know cloud services, consumption patterns, optimization suggestions to decrease cost, reduce risk, or increase service levels the same can be achieved by a set of users who are authorised to perform such functions. Clouds are obligated to fulfil the service levels of services as defined in the contracts. The status of the same should be referrable to measure the quality of service.



Managed Hybrid Cloud

II. **Service Management**: The service requests have to be simplified and resources managed for service levels of the business. Enabling the service level by the **Managed Hybrid Cloud Services Provider (MHCSP)** ensures agreed availability and performance service levels. One of the most critical component is monitoring and reporting for all the managed cloud services. The computing limitations of the on-premise Data Centres/ private clouds must be looked into for proper deliberations at all the times since it greatly affects the workload capacity planning from /to private clouds to public platforms and vice-versa. If the capacity information is not dealt with properly. Public cloud platforms provide capacity with infinite possibilities but there are costs associated. Further, in the absence of any capacity planning, workloads placement decisions can be impacted negatively resulting in resource-starved workloads and poor application response times.

III. **Governance** – The overall governance of the hybrid cloud in a complex environment becomes all the more critical. The ever-growing workloads with process & data compliances together call for an effective and performance driven governance. The main objective is to align the whole service framework to the organization policies. The policies can range from preventing the porting of confidential data to a public cloud to limiting the purchase options (on-demand, reserved, spot) for test servers to applying quotas for project spend and geographic placement of infrastructure and information. Policies are critical to enabling governance over the use of cloud services. Any breach of compliance should be taken on priority for avoiding any unexpected showstoppers to the business in future.

IV. **Security – The security policies are at the core of whatever we do today and thus very** imperative to protect data and devices from out of domain , in-domain and federated domains. The alignment of security to organization policies is a quintessential aspect. The data at rest and data in motion at all times have to be protected with encryption. This must also extend to Key Management and certificates with encryption capabilities. The role based access control is implemented using IDAM tools. The tools must be capable of defining entitlements for all roles including end users, cloud administrators, developers and managers.

Conclusion

There are many competent players in the industry who are managing the hybrid clouds and the multi-clouds as per the client expectations. The question is, are they also employing best practices for improving productivity and cost optimization. Then we have emerging areas such as SDDC, VDI, CaaS and IaaC. Then how does an enterprise selects the Managed Hybrid Cloud Services Provider?

The enterprise must look at following parameters:

1. Current expertise in managing virtualized workloads across multi-clouds.
2. Alliances / partnerships with the OEMs of the various sorts ranging from servers on the compute to the connectivities.
3. The client testimonials since that is the single source of truth for the level of competency a Managed Hybrid Cloud Services Provider claims.