International Journal of Advanced Information in Engineering Technology (IJAIET)
Vol.4, No.10, Oct 2017 ISSN: 2454-6933

TECHNIQUES OF vREALIZE AUTOMATION IN HYBRID CLOUD

Palakollu. Divya
Department of Computer Science and Engineering
Asst Professor at Samskruti College of Engineering and Technology
Cloud Computing

ABSTRACT

The vRealize Suite enables users to manage and provision assignments at scale, including computing, network, storage and application services in hybrid cloud environments. The platform's management capabilities for the software-defined data center and through two or more clouds. vRealize Automation as a single policy-driven portal delivers a true hybrid cloud. Initially, the two endpoints commit to be added to vRealize Automation. The local VMware vCenter Server that is keep the production cluster and the vCloud Director endpoint of the Virtual Private Cloud on vCloud Air.

INTRODUCTION

vRealize is the global leader in virtualization and cloud infrastructure software, the key enabling technologies for hybrid clouds. VMware is the common denominator among many of the most innovative organizations, successfully moving IT from rigid physical infrastructure to flexible, virtualized, and cloud environments. vRealize is behind some of the largest and highest strong cloud environments in the world, providing single insight into the paths IT and business teams are using cloud computing to convey new services, enter into new markets, get closer to customers, and make mobile employees more productive. Using this knowledge and the proven foundation of vSphere and the software-defined data center architecture, vRealize delivers the security, reliability, and performance for a hybrid cloud platform

vRealize MIGRATION STRATEGIES:

The highest challenge when forwarding workloads through public and private clouds is the coupling of the platform technology. That said, organizations highly spend in VMware should consider vCloud Air because it would make the transition between private and public more seamless

The vCloud Air interconnected partners circle, anyone who wants to own this thought of migration to the cloud for their clients, whether they are internal or external. The migration COE should be loaded with potential migration use cases and accept core service provider architectures presented within the vCAT-SP. The high-level transfer use cases are P2V (physical-to-virtual),V2V(virtual-to-virtual),V2C (virtualization-to-cloud), and C2C (cloud-to-cloud). Due to the separate combinations of tools available, this document provides a list of attributes for evaluating possibilities with the understanding that VMware customers, VMware service providers and their participants, as well as VMware itself will have more recommendations depending on criteria.

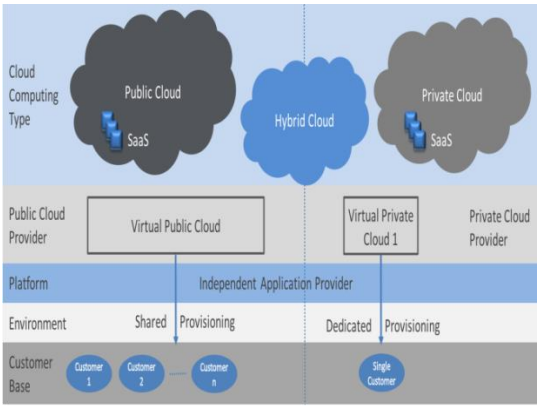

Fig 1.Migration strategies in cloud

The Categories For Transmission Of Data In Hybrid Cloud:

Replace: To discard an existing application and switch to a SaaS model

Refactor: To run an application on the cloud provider's infrastructure, requiring application code or configuration changes•

Revise: To modify or extend the existing codebase to modernize the application (changes range from minor to significant), then deploy to the cloud using rehosting or refactoring•

Rehost: Also referred to as "lift and shift," mass migration measure deploying an application to a different hardware environment, then changing the application's infrastructure configuration to support the cloud•

Rebuild: To fully redevelop or rearchitect an application on the cloud infrastructure provider's platform

TOOLS FOR MIGRATION

vCloud Connector

VMware vCloud adopter makes hybrid cloud migration simple. With vCloud adopter extend the logical circumferences of data centre by connecting vCloud Director stationed private and public clouds and maintain them with a unique interface. Use vCloud Connector to migrate the existing applications, workloads and templates to vCloud Air

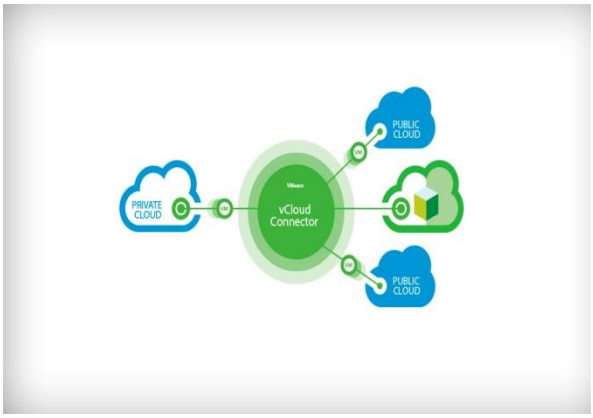

Fig 2.vCloud connector

Virtual Data Center Architecture

VMware framework virtualizes the entire IT framework including servers, storage and interconnections. It combine these different types of resources and presents a simple and same set of elements in the virtual environment. With VMware framework, IT resources can be managed like a shared utility and dynamically provisioned to different business units and projects without worrying about the underlying hardware differences and limitations.

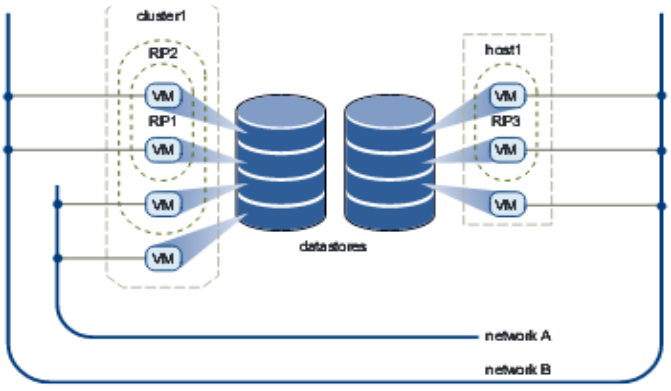

Fig 3. Virtual Data Center Architecture

VMware framework presents a simple set of virtual elements used to build a virtual data center.

- Computing and memory resources called Hosts, Clusters and Resource Pools
- Storage resources called Data stores
- Networking resources called Networks
- Virtual machines

A Host is the virtual statement of the computing and memory assets of a physical machine running ESX Server. When one or more physical machines are combined together to work and be maintaining as whole, the accumulated computing and memory assets form a Cluster. systems can be temporarily added or removed from a Cluster. Computing and memory assets from Clusters can be finely divided into a structure of assets Pools. Data stores are virtual statements of combinations of underlying physical storage resources in the data center. These physical storage resources can come from the local SCSI disks of the server, the Fiber Channel SAN disk arrays, the iSCSI SAN disk arrays, or Network Attached Storage (NAS) arrays. Inter connections in the virtual environment combined virtual machines to each other or to the physical inter connection outside of the virtual data center.

Virtual machines are designated to a particular Host, Cluster or Resource Pool and a Data store when they are created. A virtual machine takes assets like a physical appliance takes electricity. While in powered off, suspended, or idle state, it consumes no assets. Once powered-on, it consumes assets temporarily, using more as the workload increases or give back assets temporarily as the workload decreases.

Architecture Of vRealize Automation

vRealize Automation hold three main factors that can be classified as follows:

- vRealize Automation appliance: This is the main component, and is delivered as a virtual appliance in the Open Virtualization Format (OVF). Approximately, it hosts the web comprising the self-service portal. It also adds the Application Services and vRealize Orchestrator.

- vRealize Automation Infrastructure as a Service (IaaS): The installation files for the IaaS components are stored on the vRealize Automation appliance. The IaaS-fundamentals themselves must be installed on a Windows system and are responsible for the provisioning of IaaS resources. Therefore, the Windows machine must be able to communicate with hypervisors, cloud environments and physical hosts.

- Authentication Services: The Authorization as part of the vRealize Automation appliance.

Besides these core fundamentals, there are additional application which extend the functionality of vRealize Automation:

- vRealize Orchestrator: Just as the Authentication Services, the Orchestrator is running on the vRealize Automation appliance, but it can also be deployed as a stand-alone appliance. vRealize Orchestrator is VMware's central tool for all kinds of automation in the data centre. It is also the

preferred tool to extend vRealize Automation by any custom logic.

- vRealize Business Standard Edition:When it comes to costing, vRealize Business helps you to calculate the total costs of your data centre, to price any services, to compare the prices of private cloud service offerings with public cloud competitors or to generate reports about the money spent on these service offerings. vRealize Business Standard Edition is deployed as a stand-alone appliance and integrates into the vRealize Automation self-service portal.

- vRealize Code Stream: Technically, from vRealize Automation 6.2 onwards, the vRealize Automation applications also hosts. vRealize Code Stream – an automation tool that helps DevOps teams to build a release pipeline and provision new applications to a productive environment. However, technically present on the vRealize Automation application, it is a separate tool and is not part of the vRealize Automation or vRealize Suite licenses.
- n addition to these components, there is also the need for further software components. For the IaaS components, an instance of SQL Server is required. Microsoft Active Directory is needed as an authentication source for the Authentication Services.
- Many customers want to dynamically provision networks. In that case, VMware NSX can be used. In the recent versions, vRealize Automation has significantly enhanced its integration with VMware NSX to provide even more virtual networking and security capabilities.

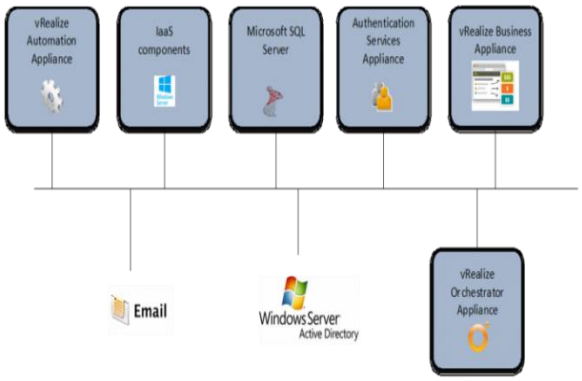

Fig 4.Logical overview of vRealize Automation components

vRealize Automation appliance

IaaS components

IaaS components must be installed on a Windows system and the most difficult ones to understand, install and manage. The following set of IaaS services and web sites are required to run a vRealize Automation environment:

- IaaS Website
- Model Manager
- vCloud Automation Center Manager Service
- IaaS MS SQL Server database
- Distributed Execution Manager
- vCloud Automation Center Management Agent
- A proxy agent (for communication with hypervisors)

IaaS Website

The IaaS website is depend on the *Internet Information Server* (IIS) and hosts the Model Manager as well as the management merge for the communication with the vRealize

Automation applications. The web performance varies significantly. All the stuff coming from the Linux appliance loads quite fast, while the Windows components take significantly more time to generate their content.

Model Manager

The model manger represents the IaaS components. Running within IIS, its basic jods are to encapsulate the Microsoft SQL Server database and provide access to the IaaS data via web services. For high-availability reasons, the model manager can have multiple instances that run on different hosts within the vRealize Automation environment

vCloud Automation Manager

The Manager duty is combines communication between agents and duplicate agents, the database, and SMTP. A minimum of single instance of the Manager Service component must be installed.

IaaS MS SQL database

As we have already discussed, IaaS uses a Microsoft SQL Server to store all of its data. Currently, only Microsoft SQL Server is supported. If you want to prepare for high-availability, you should consider implementing a Microsoft SQL Server failover cluster. While database mirroring or replication should be possible, VMware's 'preferred way' is to set up a cluster.

Distributed Execution Manager (DEM)

DEMs are in charge of talking to the model manager, fetch some work and then execute any workflow. From a technical perspective, there are two different kinds of DEMs:

- The DEM orchestrator communicates with the model manager and schedules the workflow execution. The DEM orchestrator only monitors the execution of the workflow, but does not do the work itself. As there is a lot of communication between the DEM agitator and the Model Manager, it is recommended to install the DEM agitator on, or 'near' to the Windows machine hosting the Model Manager. At any time, only one DEM agitator can be active within the vRealize Automation installation. For high-availability reasons, it is therefore always a good practice to have a failover system, which could become active in case of any failure.
- DEM workers are responsible for the execution of workflows. In contrast to DEM orchestrators, multiple workers can be active at the same time. This might be useful for scalability as well as for high-availability purposes. Because DEM workers interact with external resources, they should be installed as 'near' as possible to the system they are provisioning to. This means that a workflow can only be run by a way DEM worker which resides on a certain host. Technically, to run a workflow, a DEM worker will contact the model manager and download all the artefacts needed (e.g. some scripts) to run the code. DEM workers regularly contact the model manager and ask for new work.

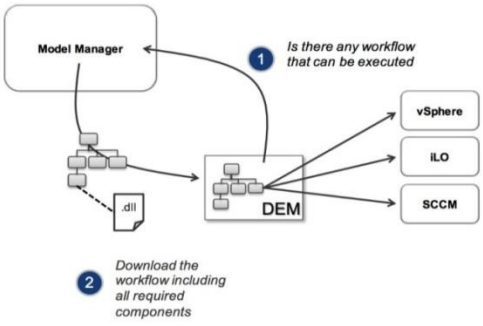

Fig 5. Distributed Execution Manager

Proxy agents

Virtualization proxy agents are used to interact with

hypervisors. They are responsible for the provisioning of a machine or for synchronizing hypervisor data with the vRealize database (e.g. importing virtual machine data from the hypervisor). Agents are installed as Windows services and must be installed and configured for every single virtualization environment. This means, if you want to address three different vCenter Servers, you must install three different agents. There are virtualization agents for vSphere, Hyper-V and XenServer.

Conclusion

This paper concludes that the main components are the vRealize Automation appliance and the IaaS components. Furthermore, there are also other components such as the Authentication Services, vRealize Orchestrator Altogether, they form the vRealize Automation environment. It is crucial to understand the roles of these different components in order to create a design for a vRealize deployment and begin with the installation. These automation capabilities deliver speed, reliability, responsiveness and consistency to the deployment; ongoing scaling; and deprovisioning of resources in the cloud environment

REFERENCES

1.Safwan Mahmud Khan and Kevin W. Hamlen,
"Hatman: Intra-cloud Trust Management for Hadoop", 2012 IEEE Fifth International Conference on Cloud Computing, 978-0-7695-4755-8/© 2012 IEEE DOI 10.1109/CLOUD.2012.64.

2. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: FromSingle to Multi-Clouds" 2012 45th Hawaii International Conference on System Sciences 978-0-7695-4525-7/12 © 2012 IEEE DOI 10.1109/-HICSS.2012.153

3. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing" 2012 International Conference on Computer Science and Electronics Engineering 978-0-7695-4647-6/12 © 2012 IEEE DOI 10.1109/ICCSEE.2012.193

4 O.Acii¸cmez. Yet another micro architectural attack:Exploiting I-cache. InACM Workshop on ComputerSecurity Architecture pages 11–18, October 2007.

5 O. Acii¸cmez, B. B. Brumley, and P. Grabher. Newresults on instruction cache attacks.InCryptographicHardware and Embedded Systems, CHES 2010, 12thInternational Workshop pages 110–124, August 2010.February 2007.

6 O. Acii¸cmez and J.-P. Seifert. Cheap hardware parallelism implies cheap security. In
Workshop on
Fault Diagnosis and Tolerance in Cryptography
, pages
80–91, September 2007.

7 M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H.
Katz, A. Konwinski, G. Lee, D. A. Patterson,
A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud Computing.Commun. AC, 53(4):50–58, 2010.

8 Celera Assembler.
http://wgs-assembler.sourceforge.net/.

9 E. Bangerter, D. Gullasch, and S. Krenn. Cache games– bringing access-based cache attacks on AES to practice. In32nd IEEE Symposium on Security and Privacy, 2011.

10 P. Barham, B. Dragovic, K. Fraser, S. Hand,T. Harris, A. Ho, R. Neugebauer, I. Pratt, andA. Warfield. Xen and the art of virtualization. In

19thACM Symposium on Operating Systems Principles, pages 164–177, 2003.

About Author

Palakollu Divya,
Assist. Professor
In Department of Computer Science and Engineering, Samskruti College Of Engineering and Technology, Ghatkesar, Hyderabad.