# Zilungele Cloud Services

# Overview

Zilungele Cloud Services is a VMware Cloud Provider partner providing Cloud services to Sub-Sahara Africa. Zilungele provides Shared and Dedicated Infrastructure-as-a-Service (IaaS), Object Storage, Desktop-as-a-Service, Endpoint Management, Managed Services, and Professional Services. Zilungele is Head-quartered in Johannesburg, South Africa where they have provided services over the past 12 years. Zilungele also has a presence in Luanda, Angola. ZCS has capitalized on the continent’s late entry into data center and inter-networking services. Providing its above-listed services to Financial Institutions, Governmental institutions, Non-Governmental Organizations (NGOs), Multi-National Organizations, as well as local small and mid-sized businesses in need of IT services to facilitate their business objective in a global economy.

Zilungele intends to extend its presence into Eastern and Western Africa with data centers in Nairobi, Kenya, Addis Abba, Ethiopia, Abuja, Nigeria & Dakar Senegal. ZCS plans to maximize their investment in the VMware Cloud Provider program by implementing an asset-heavy solution using the Cloud Provider Pod Stack which includes:

* vSphere
* vCloud Director
* NSX-T Datacenter
* vSAN
* Cloud Director Availability
* Etc…

The use of the VMware Cloud Provider Pod stack will allow ZCS to provide:

* Multi-Tenant Resource Pooling - create virtual data centers from common infrastructure to cater to heterogeneous enterprise needs
* Operational Visibility and Insights - refreshed dashboard and single pane of glass to provide centralized multi-tenant cloud management views
* Container-as-a-Service - onramp for enterprises leveraging flexible, on-demand containers and VMs in the same virtual data center and faster time-to-consumption for Kubernetes
* Data Center Extension and Cloud Migration - secure VM migration and data center extension
* Multi-Site Management - Stretch data centers across sites and geographies
* Data Protection and Availability - run simple DRaaS offerings that are compatible with enterprise environments

ZCS intends to begin this implementation in their Luanda, Angola Datacenter, and with the success of that implementation, replicate the roll-out in the new markets they are currently courting.

ZCS has 430 IaaS tenants in Angola 95% of whom leverage the shared IaaS solution. The remaining 5% subscribe either exclusively to their dedicated IaaS solution or a combination of both the shared and dedicated IaaS. The average Shared IaaS tenant runs 10 virtual machines. Clients with a dedicated Private cloud (IaaS) are provided a dedicated vSphere cluster with a minimum of 4 ESXi hosts configured with vSAN.

ZCS expects to increase its customer base by 200% over the next 18 months and needs a solution that will scale accordingly.

**Applications**

The majority of the applications running in ZCS’s IaaS solution are 3-tier applications. Because all of ZCSs’ customers are external to their data center they require HTTP and HTTPS access to their applications. For enhanced security and performance plus streamlined support, ZCS offers its customers access to their application via a VDI pool provided with VMware Horizon

**Infrastructure**

ZCS offers three compute tiers to its customers:

* Introductory Tier – Used to introduce prospective tenants to the ZCS solutions
  + Commodity Intel white-box servers
  + Dual 16-core 2.4 GHz
  + 128 GB RAM
  + Dual 10 Gb NIC
  + NFS Storage
* Standard Tier – Used for Shared IaaS Tenants
  + HP Synergy HCI Solution
  + Dual 24-core 2.4 GHz
  + 512 GB RAM
  + Dual 25 Gb
  + Mellanox SH2200 Switch Module
  + Up to 640 TB per 12000 Chassis
* Enhanced Tier – Used for Dedicated IaaS Tenants
  + HP DL 360
  + Dual 16-core 2.8 GHz
  + 128 GB RAM
  + Dual 25 Gb NIC
  + (4) 3.6 TB SSD
  + (2)1.2 TB SSD

# Project Scope

Below are the requirements obtained from the key stakeholders at Zilungele Cloud Services.

**Eric Moana, Chief Information Officer**

*Our increased expansion as an organization is key to our continued success. Our expansion will come in the form of additional service offerings (both Asset-heavy and Asset-light), entrance into new markets, partnerships with Hyperscale providers (Alibaba Cloud, Azure, AWS, etc…)*

|  |  |
| --- | --- |
| *Requirement Number* | *Requirement* |
| *Requirement 1* | *Security is paramount. We need to protect our tenants’ applications from internal and external threats.* |
| *Requirement 2* | *The solution must scale beyond 1500 tenants* |
| *Requirement 3* | *We must be able to provide integration with external security solutions for some of our tenants (Palo Alto, etc..)* |
| *Requirement 4* | *Tenants Should only have access and visibility to their applications and self-service provisioning and management, where necessary, but not to those of other tenants.* |
| *Requirement 5* | *Adhere to regulatory compliance in the markets we provide services and for the verticals we serve.* |

**Ava Masango, IT Director**

*As we continue to grow our company and subsequently our IT infrastructure by expanding our existing footprint and entry into new markets, we must keep our operations as centralized as possible. We use physical devices to provide network and security services. As we grow, we need to make better use of the VMware Cloud Provider Pod stack and move to a complete SDDC, providing us the agility in Tenant onboarding and management. We also want to take advantage of easy service monetization and 3rd party integration.*

*The majority of our customers use our Shared IaaS. Only a handful have a Dedicated IaaS. Some customers have workloads running in both the Shared IaaS and Dedicated IaaS.*

|  |  |
| --- | --- |
| *Requirement 6* | *Centralized Management is mandatory. The existing physical security mechanism is no longer scalable.* |
| *Requirement 7* | *For some of our customers with compliance requirements, we need to provide security via 3rd party appliances. We also need to provide endpoint protection for these tenants* |
| *Requirement 8* | *Our data center design uses the availability zone model. In each city where we provide services, we have 2 or more data centers within a 10-mile radius to account for site failures. The solution should allow for streamline mobility of tenant workloads without the need to reconfigure networking or security policies* |
| *Requirement 9* | *Reduce dependence on physical security appliances. Most network and security services should be deployed through software.* |
| *Requirement 10* | *Possible 3rd party integration. The security policies leveraged should be easily modifiable to seamlessly integrate 3rd party products. We need the flexibility to only license and deploy 3rd party security appliances as needed.* |
| *Requirement 11* | *All tenants will require access to shared services we provide (AD, DNS, NTP)* |
| *Requirement 12* | *Shared services must have a 99.99% uptime* |
| *Requirement 13* | *The security Posture of all workloads must remain consistent even as the move from site to site. This must happen without any additional administrative overhead* |

**Chaka Kgosi, Cloud Architect**

*Our three tiers of compute are organized in 3 different types of clusters tier-1 and tier-2 are used in our Shared IaaS solution and tier-3 exist as dedicated clusters per tenant. Most of the tenants with workloads in tier-3 need to consume external (non-nsx native) security services (IDS/IPS, Advanced L7 Firewall, etc…). Some of these Tier-3 customers may also have workloads running in tier-2 and thus need to have connectivity between their shared and dedicated virtual datacenters.*

*Most tier-2 customers do not need external security services, but we do offer these services to all customers (shared and dedicated)*

|  |  |
| --- | --- |
| *Requirement 14* | *We need to provide tenants in both our shared and dedicated IaaS solution access to enhanced security services if desired.* |
| *Requirement 15* | *The solution needs to scale beyond 1500 tenants with 5% or less of those tenants using our dedicated IaaS solution* |
| *Requirement 16* | *Due to security requirements, dedicated tenants cannot share T0 gateways with other tenants* |
| *Requirement 17* | *Dedicated IaaS tenants are provided access to both our VDI solution and site-to-site VPN as a value-added service* |
| *Requirement 18* | *Tenants must be isolated from one another. One tenant should not be allowed access to other tenants* |
| *Requirement 19* | *All tenants must have access to shared services provided by ZCS* |
| *Requirement 20* | *The solution must minimize administrative overhead* |
| *Requirement 21* | *Route-based VPN must be used for site-to-site VPN configuration from tenants’ dedicated IaaS and their on-premise datacenter* |

**Steven Waugh, Network Administrator**

|  |  |
| --- | --- |
| Requirement 22 | All Tenant applications need communication with Shared services provided by ZCS (AD, DNS, and NTP services, etc…). These services are running in the Physical infrastructure on bare metal servers. |
| Requirement 23 | Tenants should have external access to their applications on port 443. |
| Requirement 24 | Tenants with enhanced performance and security requirements will access their apps via a Horizon VDI running in a dedicated VDI cluster in the environment. This VDI pool is a shared (Floating) Pool and should be accessible to all users who have subscribed to the solution via their browser and the Horizon View Client |
| Requirement 25 | From the Shared VDI environment, admin users should have HTTP, HTTPS, SSH RDP, and VNC access to their virtual machines. |
| Requirement 26 | Future-proof the deployment for 3rd party guest introspection. We are looking at 3rd party guest introspection services. We need the infrastructure to be prepared for integrating the 3rd party product in the future. We also want the consultant to create a policy to consume this 3rd party product once it is deployed. |
| Requirement 27 | With potentially multiple virtual routers the solution should minimize the need to update BGP neighbor configuration every time a new T0 gateway is deployed |