Project 1: Vodafone Private Cloud

1. Project Summary

1.1. Identification

Nature of project	Design and Deploy Private cloud Infrastructure
Location of project	Mumbai & Pune (Maharashtra)
Name of your employer	VMware

1.2. Role(s) and responsibilities in the project.

My Role :- Technical Domain Authority -Virtualization.

My Responsibilities

As part of this role, following were my responsibilities

1. Responsible for Architecting and designing highly available cloud platform
2. Responsible for Gathering, validating and documenting technical requirements for Private cloud.
3. Responsible for design of supporting Microsoft Infrastructure (Active Directory, DNS)
4. Responsible for design of Storage and Backup Infrastructure
5. Responsible for creating technical documents for server build, checklists and standardize naming conventions. Develop and present technical solutions and configurations for Private Cloud.
6. Single point of contact (SPOC) for Questions and problems related to the use and troubleshooting of the Cloud platform and dependent products. (SPOC) for Technical guidance concerning the business implications of selecting different technology in case solution doesn't meet the requirements. (SPOC) Interfacing with vendors, leadership and technical co-workers to develop, deploy, and document the solution.

2. Business Opportunity or Problem

The customer is a Telco company who wanted to offers physical, virtual, and cloud infrastructure to its development business units. Following are business requirement gathered during various meetings held with the customer:

- Enhance service portfolio by integrating the best products from physical, virtual, and cloud layers with automation, orchestration, and lifecycle management capabilities.
- Provide secure flexible and cost effective cloud infrastructure which may be provisioned and de-provisioned rapidly, in a secure environment
- Provide an underlying infrastructure upon which other "Infrastructure as a Service" will be presented and future services may be provided

3. Solution

Phase -I Assessment Phase

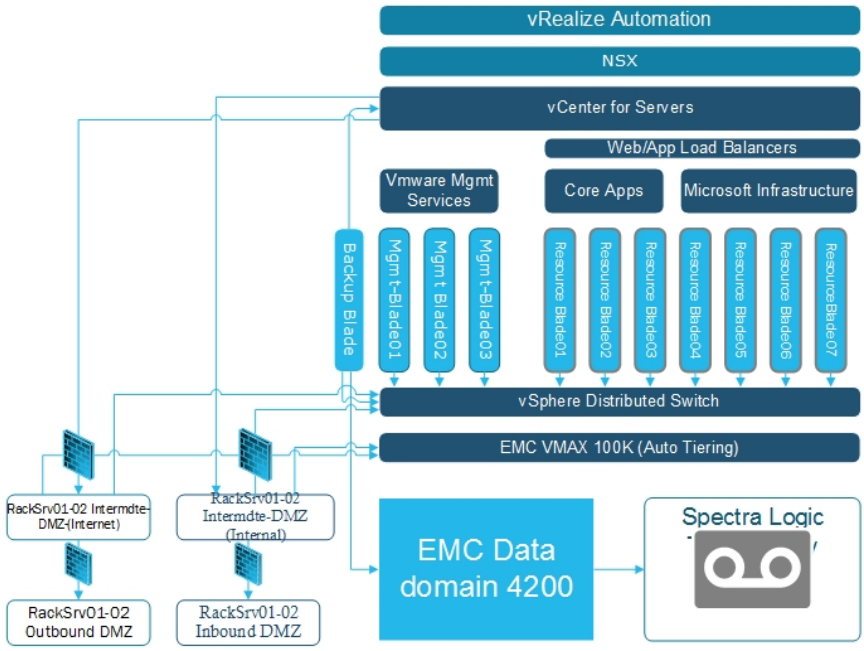
Following are my major contributions to the project

1. Understand business requirements, objectives, and use cases for the project.
2. Capture the business and technical requirements, constraints, and assumptions.
3. Conduct current state analysis of existing infrastructure and capacity planning exercise.
4. Lead Design sessions and interviews with the following subject matter experts: virtualization, storage, networking, and security. Translate business and technical requirements into logical and physical designs.

Business & Technical requirements were gathered during interaction with various stakeholders including Operations, Applications, Storage teams. In Assessment phase I, along with Network Architect I did the current state analysis of the IT Infrastructure. I built the current state architecture as the output of this exercise. I prepared Infrastructure Architecture diagram illustrating various integration points between functions/department. This phase helped me to build a conceptual model. In this phase along with requirements, I also identified constraints and risks. In absence of some information, I have documented assumptions in this design. Finally, in coordination with Network Architect requirements, assumptions were validated and refined. Output of this phase was logical architecture.

Phase -II Design Phase

In this phase the physical architecture and the details to operate the infrastructure was documented by me. Decisions on technology selection for the Private cloud, technology maturity comparison for the Private cloud and various components were documented in detailed. In this phase various technical design decisions are made and justified by me. Dedicated management layer was proposed to isolate production workload from impacting management activities. I have worked very closely with Network Architect to provide the Network ports required, the bandwidth required for Inbound and outbound traffic, management port and load balancing requirement for the environment. While sizing for the solution, 10% growth per year was considered for next 5 years.



Disk-based and tape-based Data protection solution was proposed. Tape based solution was the compliance requirement to keep data for 10 years. Data protection policy was proposed based on standard retention policy. I prepared Bill of Quantity for Compute, Storage, Backup. By working closely with customer's datacenter provided a Rack layout, power requirements.

Monitoring

Standard monitoring Baseline was proposed for monitoring of various components in the solution. Critical components e.g. Provisioning service, load balancer and for others, customized baseline was proposed by consulting with customer's Monitoring team. For load balancing health monitoring was enabled and integrated with monitoring and email system. Specific Provisioning service based on vRealize Automation Center (vRA) were configured for monitoring.

Naming Standards

The naming convention for various elements in the design has been standardized. This is extremely crucial as end users will be provisioning/decommissions virtual machines randomly. virtual machine naming convention should have sufficient information to identify to the department, owner, OS and application running on the VM

Virtual Machine Naming Convention

HRWINSQL01 (HR=Department, WIN=Windows, SQL=Database, NN=Two digit random number)

Storage Naming Convention

<Depart>Datastore# (i.e HR01_Datastore1, HR02_Datastore2, HR03 _Datastore1)

Local storage (hostname_local)

Network Port Naming Convention

The VLAN id for each VLAN that is required by the Guest OS. The Port group name should reflect the VLAN number:

- Front End = "FE_"+VLAN #
- Back End = "BE_"+VLAN#

The format to use is "FE_"+VLAN ID i.e. FE_1803, FE_2002.

Design Decisions

For every major section (Compute, Storage, Network) design decision matrix was created. Design decision matrix detailed out the decision made, design justification and any impact of it. Following is one of the major decision made in the project and justification

Decision Justification for selecting Blade Architecture

Design Decision	HP C7000 chassis & Blades
Justification	Agility is a must for cloud-based infrastructure, with blade infrastructure scaling is very easy. Centralized management of blades, 16 blades can be managed by a single interface. The solution will be co-located in 3rd party DC and is charged per Rack units, rather than a per server or blade. Total Rackspace in

	comparison with Rack server architecture is reduced by 25% and the cost is saved up to 35%. With 10% growth per year for next 5 years, Total Cost of Ownership is much more attractive. Blade architecture has deeper integration with virtualization, and better management tools can make them preferred choice
Impact/Implications	It is move from one architecture (Rack Server) to another (Blade Server). Extensive training is required for IT staff. Limited options when it comes to PCI/PCI Express slots or when adding more disk drives
Risks	Vendor Lock-in. Since the adoption is a strategic decision and not a tactical short-term purchase, it is considered as a Low risk. Maintenance of blade infrastructure needs careful planning. Appropriate training and shadowing are needed to mitigate this risk

We (Jointly with Network Architect) did the validation of the design. The Primary aim was to ensure all requirements are met and that constraints have adhered and risks are mitigated. Detailed PowerPoint presentation was presented to the customer. Snippets of PPT are shown below

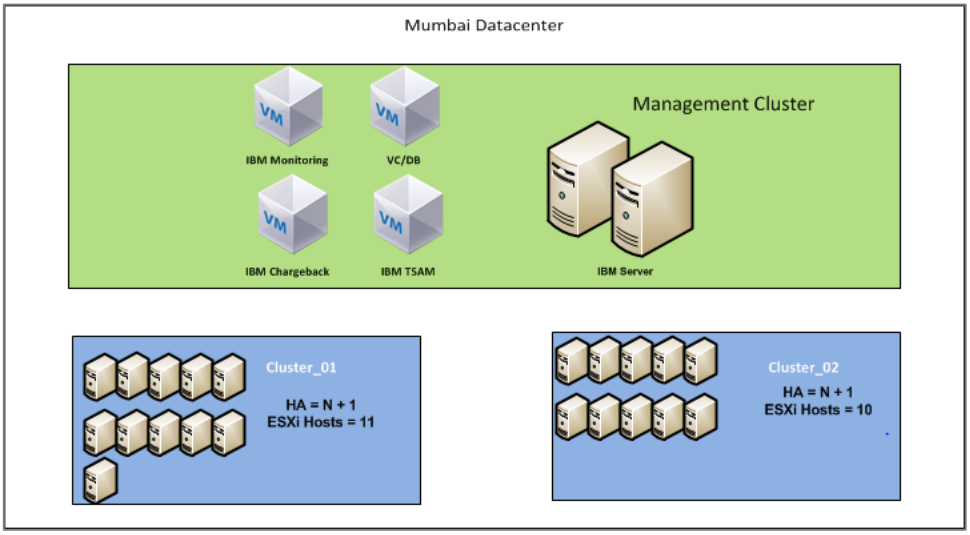


Figure 1 Logical Compute Design

Figure 2 Logical Network Design

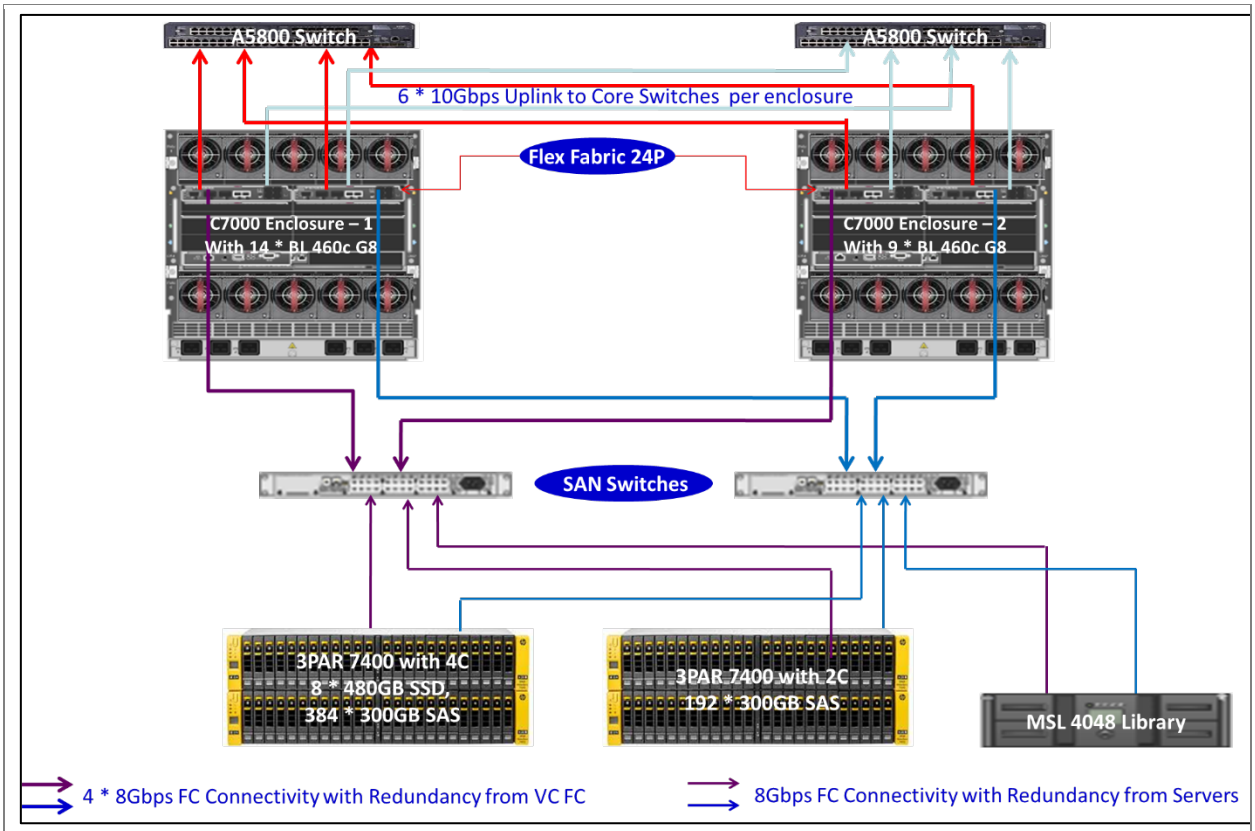


Figure 3 Physical Architecture (Compute, Storage, Network)

After a walk-through of Proposed design, 80% of the design was validated. Few changes in terms of choice of storage type, SAN fabric Speed, compute for management infrastructure was required to be changed to optimize the solution. New changes have been again reviewed with the customer upon agreement, design was frozen for next steps.

3.1. Design or problem solving methods used on this project.

VMware has their own design framework based on TOGAF. This design frame I learned in Course (VMware vSphere: Design Workshop [V5.x]) is been followed in all architecture and design I have proposed till the date. Phases are defined as 1) Assessment Phase, 2) Design Phase, 3) Deployment Phase, 4) Manage & maintain. As I progressed from one phase to another phase, requirements were validated, constraints were adhered except in phase:04 i.e. Manage and maintain. In Manage and Maintain phase it was operation who must ensure there is zero/minimal drift from implemented design. Any deviance from requirements/constraints were flagged as a risk.

3.2. Major deliverables of the project

Following are major deliverables in the project

1. Produced **Architecture Design Document** covering Project Requirements, Assumption, Constraints, Risks, Host Design, Cluster Design, Network Design, Storage Design, Automation & Orchestration Platform design, Virtual Machine Design, Defining Service Catalog, define a cost model
2. Created **Installation Guide** covering How to install guide. Interoperability matrix, Software Version, Bill of Quantity, Configuration (IP Address, Naming convention, 3rd party integration e.g. integration with Backup, CMDB system)
3. Created **Validation Guide** - Includes test plans for Availability, Manageability, Service Provisioning, Performance, Security, Hardware, software and operational test
4. Created **Operational Procedures** – Addressing Daily checks, weekly check, capacity planning
5. Contributed to **Risk Management –**for Risk identification with Risk Rating, mitigation plan (if any)
6. Contributed to **Implementation Plan –** for Project planning, validation of BOM post arrival, operational transformation plan.

4. Results

The Solution is implemented and in production. I was not responsible for implementation of this solution. But after the solution was implemented I had a task to cross verify the solution was implemented in line with proposed design. Any drift in the solution was updated in the design document with detailed justification.

4.1. *Assess the overall success or failure of the project*.

The Project was started with one primary goal which was to reduce service provisioning time. Service provisioning was not reduced to the expected level. This project is considered successful for provisioning of operating system, backup agent, Antivirus agent. However, not all application installation could be addressed using this solution. At least 60% provisioning time was reduced which was accepted by the customer as major achievement. The remaining 40% was due to the fact that integration between automation/orchestration tool and 3rd party tools was not matured during this implementation phase.

4.2. Lessons Learned

If I'm asked to redesign this project, I would consider the entire solution to be designed on Hyper-converged platform. Hyper-converged infrastructure will reduce the significant time required to install, configure Compute and Storage. During project implementation phase storage, network and compute gear arrived at different times. Unavailability of all of them in same time window delayed the project. Automation/Orchestration product was not mature enough to achieve an advanced level of automation which was thought initially. Vendor support was not skilled enough to provide right and timely support as the support cases filed resulted into bugs in the product. Hyper-converged based solution will not only provide low latency and High IOPS but makes scaling solution extremely easy as most hyper-converged solution provide block level scalability. In summary lesson learnt, POC for the integration with other components should have been done prior to selecting technology for private cloud

Project 2: Business Continuity & Disaster Recovery

5. Project Summary

5.1. Identification

Nature of project	Design and Deploy Business Continuity & Disaster Recovery Solution
Location of project	Abu Dhabi
Name of your employer	Injazat Data System

5.2. Role(s) and responsibilities in the project.

The Customer has commissioned Injazat to provide advisory services & Technology solution for IT Service Continuity solution (ITSC). As part of Business Continuity planning, Business Impact Analysis (BIA) was done by another team in Injazat. I was assigned Technical Architect -Infrastructure role to provide Technical solution which can meet the required RPO and RTO values for each service with a flexible, scalable design that introduces the ability to protect each system in accordance with the business value of both the data (as defined by RPO) and the service (as defined by RTO).

6. Business Opportunity or Problem

- The Injazat must develop a comprehensive workable ITSC solution
- The ITSC solution must cover all essential and critical infrastructure elements, systems, and networks, in accordance with key business activities and RPO/RTO are the underpinning reference.
- The ITSC solution must be designed to be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- The ITSC solution should be designed to be fully functional which will allow it run from DR site for minimum 30 days.

BIA report provided 25 Recovery Classes(RC). I grouped RC into similar sets of requirements in terms of RPO and RTO category (each had a scale from 1 to 5). Recovery Classes were defined as

RC Category	RPO/RTO Requirements
RC5	RPO Zero, RTO <4 Hours
RC5	RPO 1 Hour, RTO < 4 Hours
RC4	RPO 24 hours, RTO 4 Hours
RC3	RPO Read Only, RTO < 4 Hours
RC3	RPO Read Only, RTO < 24 Hours
RC3	RPO 24 hours, RTO < 24 Hours
RC3	RPO 48 hours, RTO < 24 Hours
RC2	RPO Read Only, RTO < 72 Hours
RC1	RPO Read Only, RTO < 120 Hours

The table below maps out how each category of RPO and RTO values (as captured during the BIA exercises) maps onto the corresponding Recovery Class.

Data Criticality	Highest	RPO 5	Zero data loss	**RC 3**	**RC 3**	**RC 4**		**RC 5**	**RC 5 CC&B/ External Entities**
		RPO 4	< 1 hour data loss	**RC 3**	**RC 3**	**RC 4**		**RC 4 SharePoint, SMS**	**RC 5 GIS, Maximo, MDM, SMS**
		RPO 3	< 24 hours data loss	**RC 2 EPPM, Primavera**	**RC 3**	**RC 3 Access Control, Aspen**		**RC 4 Laser Fiche**	**RC 4 AMR, EICT**
		RPO 2	< 48 hours data loss	**RC 2 ePost, Settlement**	**RC 2**	**RC 3**		**RC 4 BI**	**RC 4**
	Lowest	RPO1	None/ Read only	**RC 2 KIOSK**	**RC 2**	**RC 2**		**RC 4 BO**	**RC 4 DOC1**
				< 120 hours RTO 1 Lowest	< 72 hours RTO 2	< 48 hours RTO 3		< 24 hours RTO 4	< 4 hours RTO 5 Highest
			Service Criticality						

I provided solution to ensure following critical components are recovered in-line with RPO & RTO

1. Database (Microsoft, Oracle)
2. Infrastructure applications
3. Load balancing behaviour (for Intranet and Internet applications)

For the above items failure scenarios and the corresponding mitigation actions was provided and tabulated.

Traffic redirection to DR site using a load balancer and DNS forwarding was discussed in detailed with Network Architect. I calculated bandwidth calculation between Primary and Secondary Site and DR site was calculated using rate of change and Data to be transferred. Initial seeding data was proposed to be done within site.
Total 2 sites were considered. Near-DC (Secondary Site) where the customer can quickly failover which was at distance of 50 KM from the primary. The Third site (DR) where replication from Primary/Secondary will be done asynchronously. RC5 application (Zero RPO) were the only applications which were proposed to be failover to the secondary site. For RC5-RC4 applications, near site DR site was proposed. Data was also protected against logical corruption by providing a point in time feature to roll back to any given time at Primary and DR site.
RC3-RC2 application which has RTO/RPO greater than 24 hours, backup and restore solution was proposed. Backup data from Production site was proposed to be replicated to DR site daily. During DR event these would be last items to be restored. IP Address between Primary and DR site will be different. But IP Address between Primary and the secondary site will be retained post failover to ensure failover to secondary will be transparent. But failover to DR site will not be transparent, all services IP Address needs to be changed. The site will be failed over to DR site only when actual DR occurs or when DR drill is planned to be carried out. Disaster Recovery Plan will be referred for invoking DR.

6.1. Design or problem solving methods you used on this project.

The design approach was based on TOGAF framework but tuned to DR solution. This approach includes

1. **Assessment** – gathering key requirements to determine RPO and RTO for DR solutions
2. **Design** – Creating a DR Plan to meet business and Technical Requirements
3. **Deploy** – Stand up necessary infrastructure install, configure and Test solution
4. **Manage** – Test your DR plan as frequently as possible.

Disaster Recovery Plans (DRP) were built based on the categorization of RC. DRP plans included various critical information as for when to declare DR, whom to call during DR, contact details of all IT teams, how to invoke DR at compute, Storage and Network layer. Document the Priority of business-critical workloads and sequence they must be brought up. As 90% workload was virtualized, DRP plans were periodically updated using VMware SRM (DR Orchestration tool). DRP highlighted the various gaps in infrastructure e.g. Business user connected to DR site, IT Admins connectivity to DR site.

6.2. Major deliverables of the project that you were responsible for or contributed to.

- Conducted a Current State Assessment which established a baseline in terms of actual levels of resilience in each system, highlighted single points-of-failure, classified identified risks, and allocated owners to each one, and assessed the current level of service continuity maturity.
- Identified dependencies between systems and classified them by type to establish how to maintain the dependencies in failover scenarios.
- Specified the overall recovery strategy and defined which failure scenarios should be considered.
- Defined an architecture that addressed the failure scenarios and identified which kind of components would be needed in the solution design
- Sized Storage based on Application categorization. Provided overall effort required to build compute, storage platform in DR site
- Designed monitoring infrastructure for DR monitoring. As DR drills will be carried out every quarter and entire application set will run from DR for one month, monitoring platform was recommended
- Proposed to use DR compute facility for IT development work which aided in justifying investment in computing
- Contributed to Design of DMZ, internet connectivity for IT Admins and Business user during DR event
- As a part of lessons learned in previous projects Proof Of Concept was strongly recommended. Detailed POC success criteria were agreed with Vendor. Technology selection was made on the basis of success criteria met.

- Requested Bill Of Quantity (BOQ) for Storage, Servers, and Software (Hypervisor), Orchestration product for Monitoring of RTO/RPO violation. Post verification of BOQ, BOM was documented in Low Level Design Documented.
- Worked very closely with Vendor to agree of Professional Services required for implementing the storage solution. Statement of Work (SOW) was thoroughly reviewed and agreed with the Vendor.

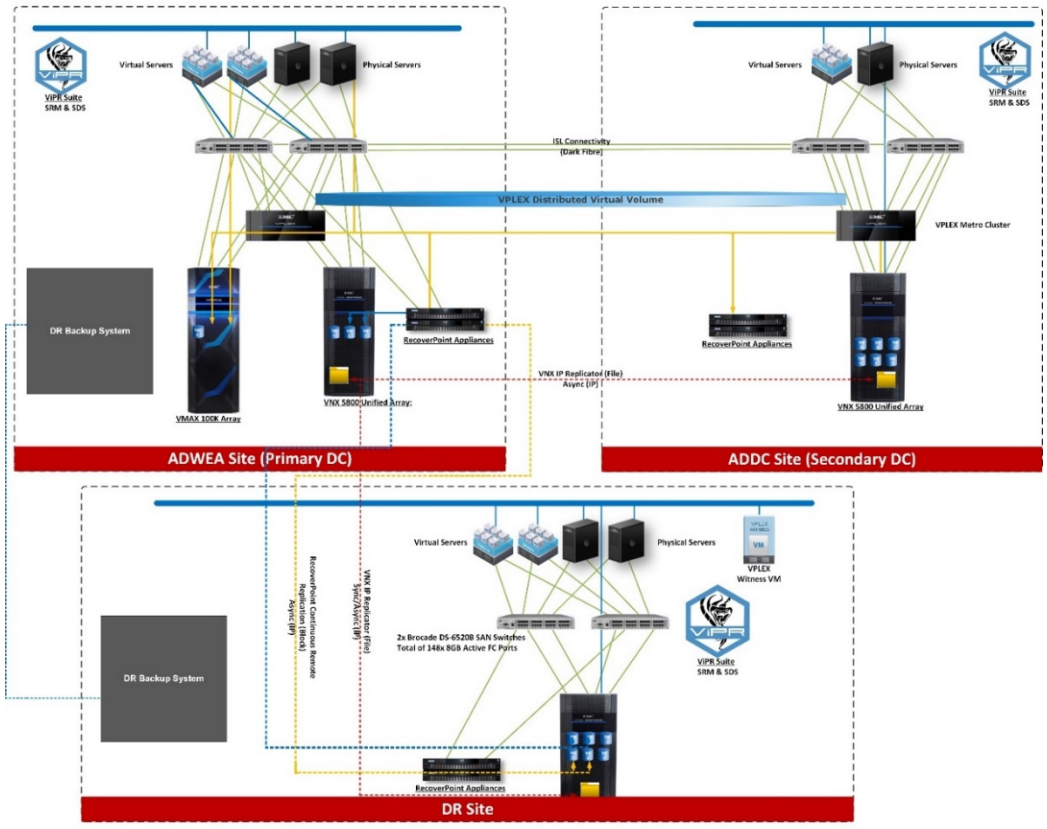


Figure 4 3DC Architecture

Project from 2019-2022

Migration from IBM infrastructure to Dell infrastructure Handling: approx. 600 VMs, 250 TB, 50 ESXi hosts

Timeframe: 6 month (2019)

Responsibility: Design, setup and configuration of 50 ESXi. Planning and testing, migration to 600 VMs

Technologies: vSphere, Dell VxRail, Windows 2016, Windows 2019, Dell SC Storage 5020 (active-active)

VDI for 600 users based on Windows 10

Description: about 600 desktops, 20 TB, 10 ESXi hosts, VMware Horizon 7.11

Timeframe: 6 month (2020)

Responsibility: Design, setup and configuration of VMware Horizon infrastructure. Planning and installation of servers in data centre.

Technologies: VMware Horizon, Dell, Windows 2019

Disaster recovery solution

Description: DR solution for 250 VMs, 50 TB, 25 ESXi Timeframe: 6 month (2020)

Responsibility: DR solution design based on Veeam Backup and Replication, RPO and RTO definition applications accordingly.

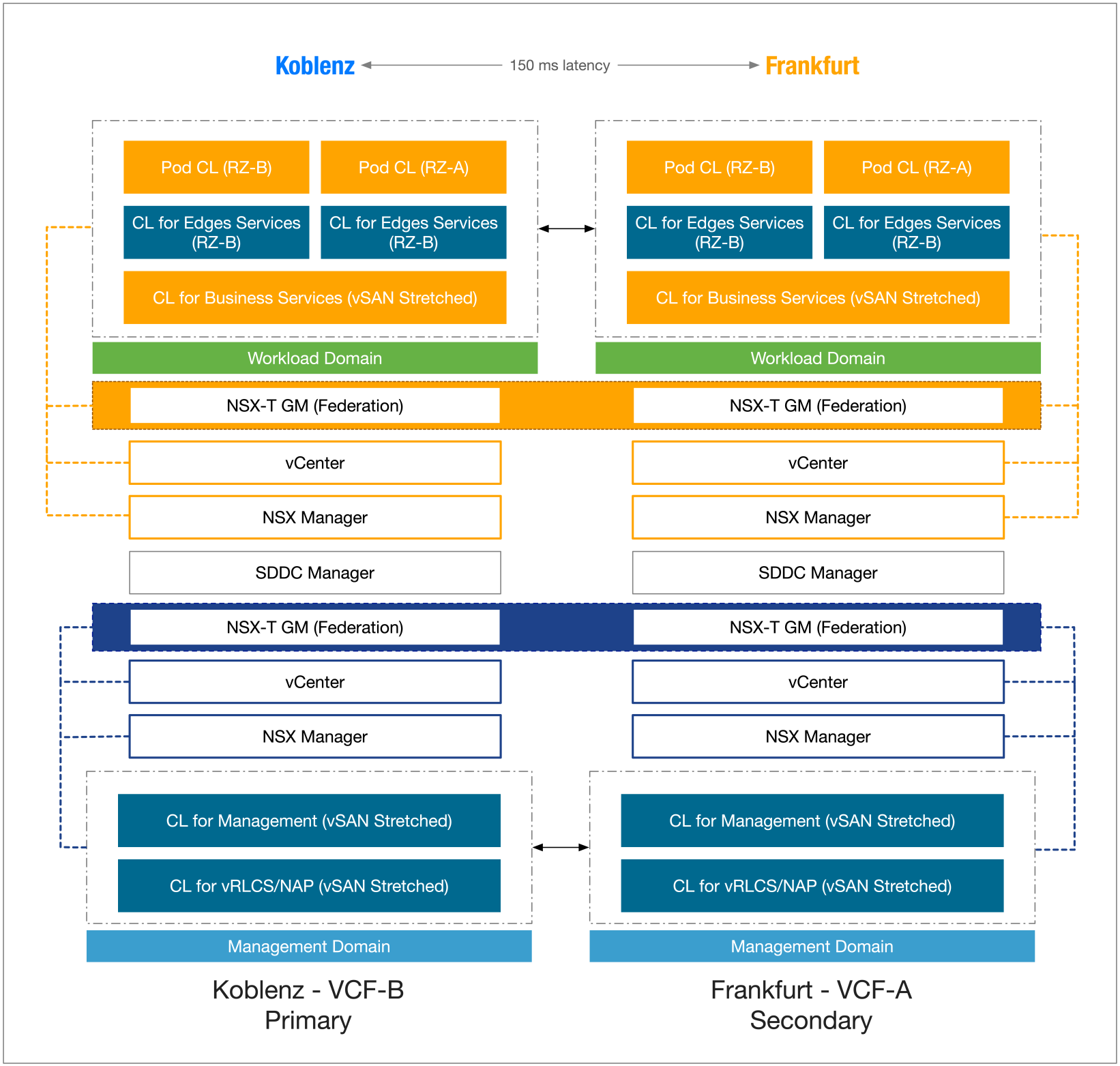
Technologies: Veeam Backup and Replication 10, vSphere 6.7, Dell, Windows 2019

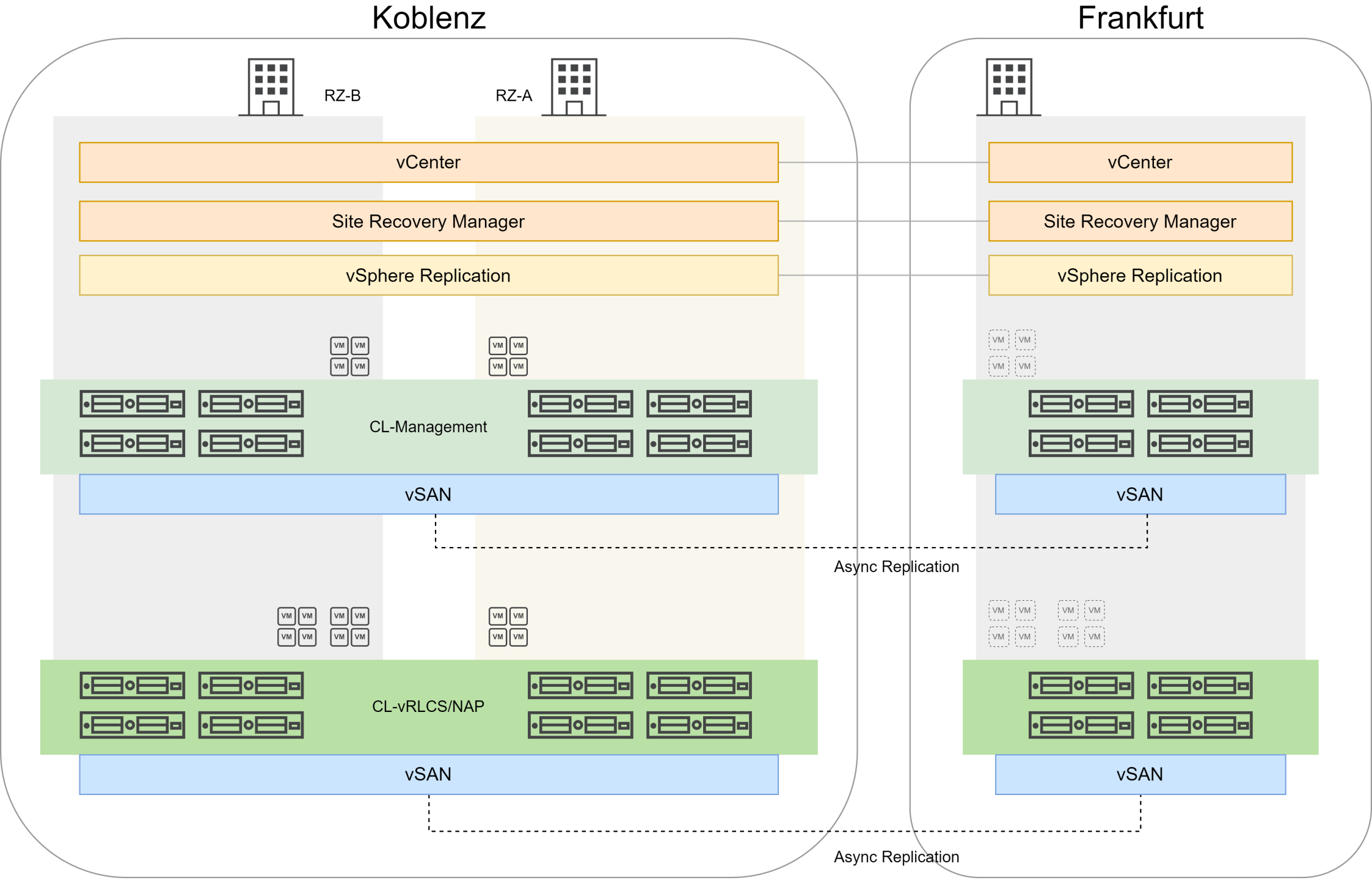
Migration from vSphere DVS Switch to Cisco ACI Handling: approx. 600 VMs, 50 ESXi hosts

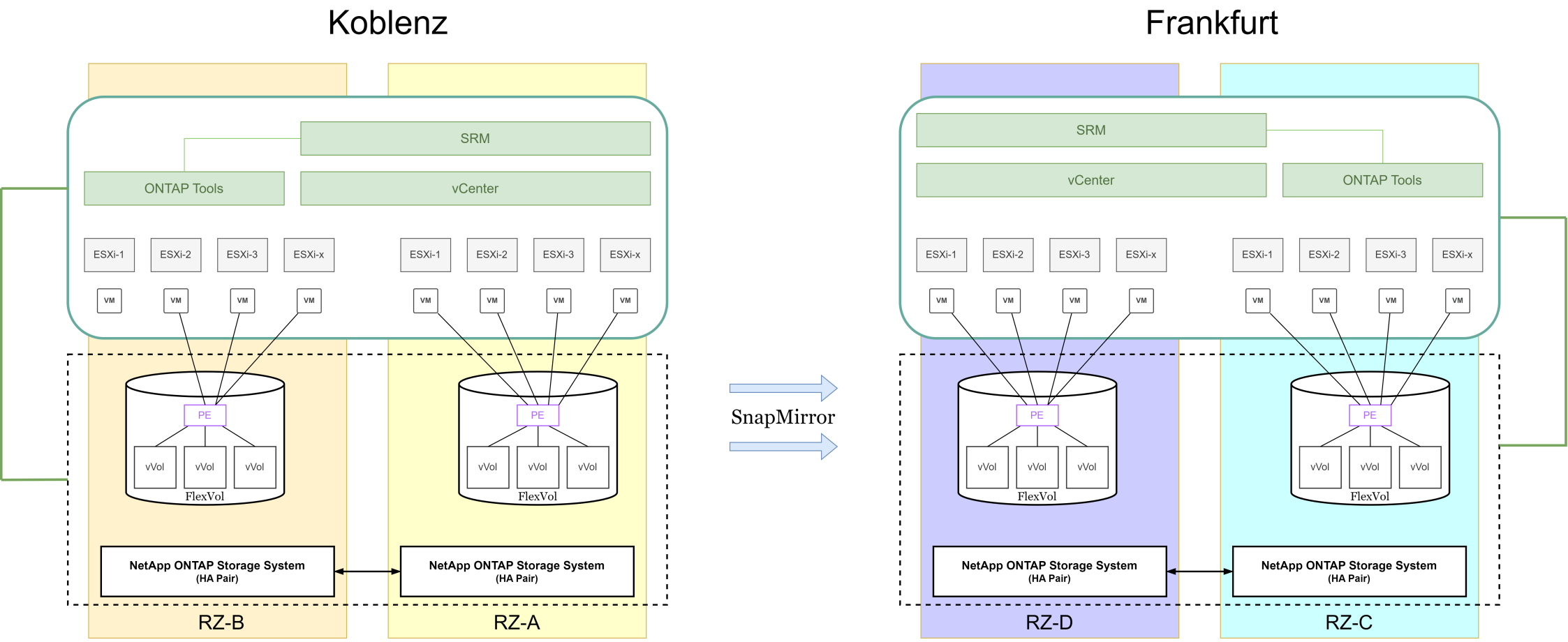
Timeframe: 3 month (2021)

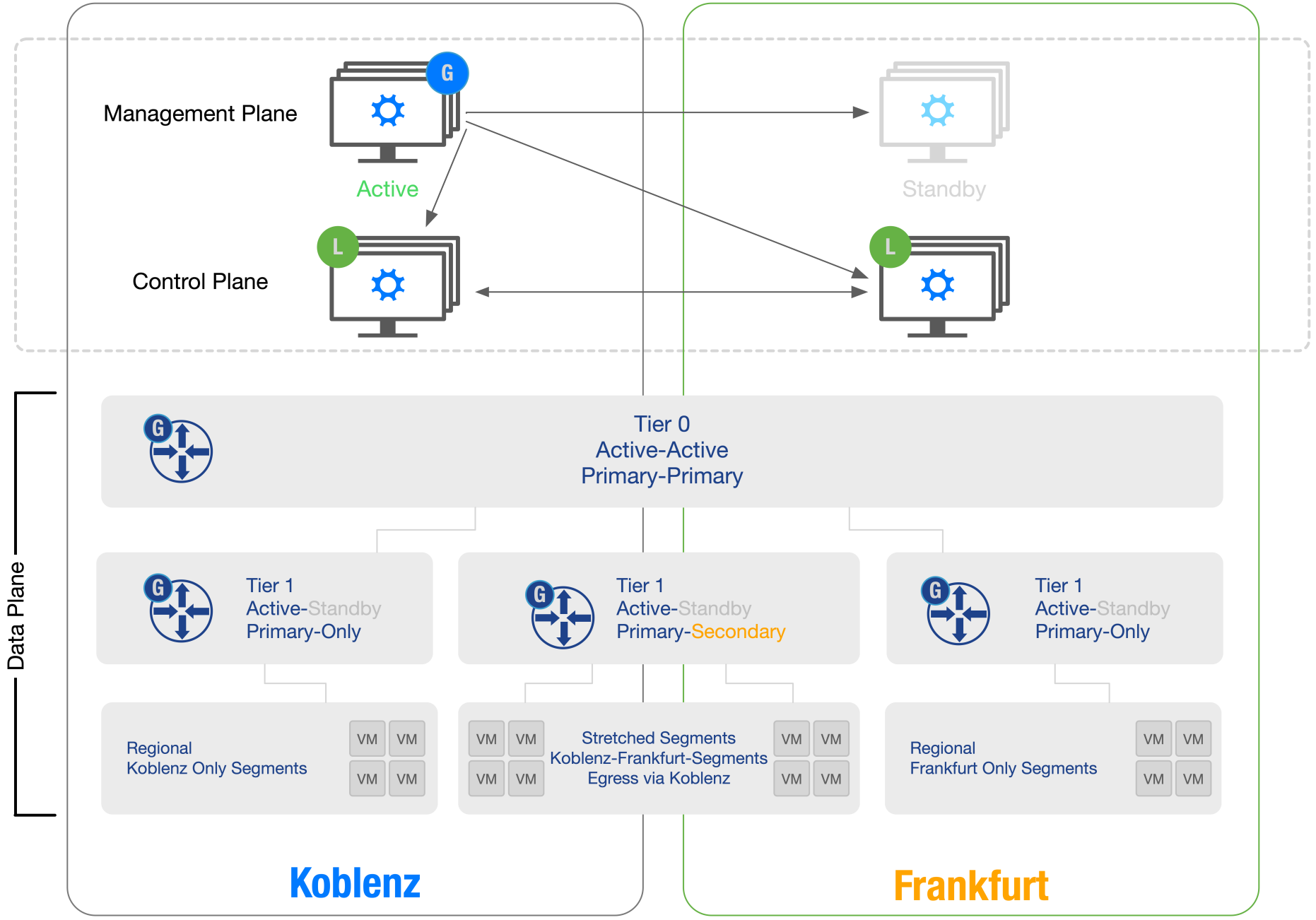
Responsibility: Migration from vSphere DVS Switch to Cisco ACI. Planning and testing the migration. Collaboration with network team

Technologies: ESXi 6.7


Koblenz
150 ms latency
Frankfurt
Pod CL (RZ-B)
Pod CL (RZ-A)
CL for Edges Services (RZ-B)
CL for Edges Services (RZ-B)
CL for Business Services (vSAN Stretched)
Pod CL (RZ-B)
Pod CL (RZ-A)
CL for Edges Services (RZ-B)
CL for Edges Services (RZ-B)
CL for Business Services (vSAN Stretched)
Workload Domain
Workload Domain
NSX-T GM (Federation)
NSX-T GM (Federation)
vCenter
vCenter
NSX Manager
NSX Manager
SDDC Manager
SDDC Manager
NSX-T GM (Federation)
NSX-T GM (Federation)
vCenter
vCenter
NSX Manager
NSX Manager
CL for Management (vSAN Stretched)
CL for vRLCS/NAP (vSAN Stretched)
CL for Management (vSAN Stretched)
CL for vRLCS/NAP (vSAN Stretched)
Management Domain
Management Domain
Koblenz - VCF-B
Primary
Frankfurt - VCF-A
Secondary


Koblenz
Frankfurt
RZ-B
RZ-A
vCenter
Site Recovery Manager
vSphere Replication
vCenter
Site Recovery Manager
vSphere Replication
VM
CL-Management
vSAN
vSAN
Async Replication
CL-vRLCS/NAP
vSAN
vSAN
Async Replication


Koblenz
Frankfurt
SRM
ONTAP Tools
vCenter
ESXi-1
ESXi-2
ESXi-3
ESXi-x
VM
PE
vVol
FlexVol
SnapMirror
NetApp ONTAP Storage System
(HA Pair)
RZ-B
RZ-A
RZ-D
RZ-C


Management Plane
Active
Standby
Control Plane
Data Plane
Tier 0
Active-Active
Primary-Primary
Tier 1
Active-Standby
Primary-Only
Tier 1
Active-Standby
Primary-Secondary
Tier 1
Active-Standby
Primary-Only
Regional
Koblenz Only Segments
VM
Stretched Segments
Koblenz-Frankfurt-Segments
Egress via Koblenz
Regional
Frankfurt Only Segments
Koblenz
Frankfurt