

# 에티버스 VMware 클라우드 아키텍처 가이드

- VCF Unified Experience

에티버스 SDI사업분부

# **Etevers VMware Cloud Standard Architecture Guide**

Version v1.0.3, 2025-05-29

# Table of Contents

현사 .....	2
제사 .....	3
서문 .....	4
문서의 목적 .....	4
프로젝트에 대해 .....	5
저자 서문 .....	6
1. 소개 .....	8
1.1. EVCS .....	9
1.1.1. EVCS Architecture .....	10
1.1.2. EVS Architecture .....	11
1.2. Broadcom Value Pack .....	13
1.3. Orbrium .....	15
1.3.1. Orbrium 연동체 개념 .....	16
2. 공통 인프라스트럭처 .....	20
2.1. 네트워킹 .....	22
2.1.1. 스위치 (하드웨어) .....	22
2.1.2. 대역폭 .....	22
2.1.3. MTU .....	23
2.1.4. 라우터 .....	23
2.1.5. Domain Name System .....	25
2.1.6. NTP .....	29
2.2. Network Attached Storage .....	31
2.3. Object Storage Service .....	32

2.3.1. Data Services Manager .....	32
2.4. 보안 .....	33
2.4.1. 인프라스트럭처 보안 .....	33
2.4.2. 신원 관리 .....	39
3. 클라우드 서비스 인프라스트럭처 .....	42
3.1. 병합 아키텍처 모델 .....	43
3.2. 동서 트래픽 .....	45
3.2.1. Multitenancy .....	45
3.2.2. NSX Overlay Transport network .....	46
3.2.3. NSX Overlay network .....	46
3.3. 북남 트래픽 .....	48
3.3.1. NSX Edge Clusters .....	48
3.3.2. Gateway Load Balancer .....	51
3.3.3. Global Server Load Balancing (GSLB) .....	52
3.4. 작업서 그리고 JSON .....	53
3.4.1. Planning and Preparation Workbook .....	53
3.4.2. Deployment Parameter Workbook .....	53
3.4.3. 서버 사양 계산 .....	54
3.4.4. JSON .....	54
4. ETVS 클라우드 서비스 용어 .....	57
4.1. 물리 인프라스트럭처 용어 .....	58
4.1.1. 지리적 영역 .....	58
4.1.2. 가용 영역 .....	58
4.1.3. 클러스터 .....	59
4.2. 논리 인프라스트럭처 용어 .....	60

4.2.1. Virtual Privater Cloud . . . . .	60
4.2.2. Segment . . . . .	60
4.2.3. Segment Peering . . . . .	60
4.2.4. Access IP . . . . .	60
4.2.5. Block Disk . . . . .	60
4.2.6. 프로젝트 . . . . .	61
4.2.7. DBaaS . . . . .	61
부록 A: 클라우드 빌드 . . . . .	63
A.1. Cloud Builder . . . . .	64
A.1.1. Management Domain Networks . . . . .	64
A.1.2. Management Domain ESXi Hosts . . . . .	65
A.1.3. vSphere Distributed Switch Profile . . . . .	65
A.1.4. NSX Host Overlay Network - Static IP Pool in NSX . . . . .	66
A.1.5. Existing Infrastructure Details . . . . .	66
A.1.6. License Keys . . . . .	67
A.1.7. vSphere Infrastructure . . . . .	67
A.1.8. NSX . . . . .	68
A.1.9. SDDC Manager . . . . .	68
A.1.10. JSON 커스터마이즈 . . . . .	69
A.2. VCF Installer . . . . .	70
부록 B: BVP Deploy & Manage . . . . .	72
부록 C: Orbrium Installation . . . . .	73
참고 문헌 . . . . .	74

에티버스 VMware 클라우드 스탠다드 아키텍처 가이드

CC BY 4.0

- <https://creativecommons.org/licenses/by/4.0/deed.ko>

편집: 에티버스 SDI사업본부

저자: 장혜천, 박하림, 우승민, 정수윤, 오예빈

표지: 백지은

VMware 및 VMware by Broadcom은 Broadcom의 등록 상표입니다.

여기에 언급된 다른 모든 제품 및 회사 이름은 각 소유자의 상표이거나

등록 상표입니다.

# 현사

우리는 모두 꿈꾸는 것들을 현실로 만들기 위해 열심히 달려가고 있습니다. 하지만 그 방법은 쉽지 않을 수 있다는 것을 잘 알고 있습니다.

때로는 지식의 부족으로 잘못된 길로 들어서며, 시간의 제약에서 원하는 만큼의 성과를 보지 못할 수도 있고, 서로 다른 방향을 바라보는 이상을 최대한 조율하여 실현 가능한 목적지에 도달해야 합니다.

모든 힘든 일을 넘어 이 결과를 낼 수 있도록 전폭적인 지원과 도움을 주신 브로드컴 및 에티버스의 모든 분께 감사의 말씀을 드립니다.

– 장혜천

# 제사

Yesterday we obeyed kings and bent our necks before emperors. But today we kneel only to truth, follow only beauty, and obey only love.

— Kahlil Gibran, The Vision: Reflections on the Way of the Soul

# 서문

## 문서의 목적

본 문서는 소프트웨어 정의 데이터 센터 (software-defined data center, SDDC) 및 클라우드 관리 포털 (Cloud Management Portal, CMP)를 제공하는 Broadcom의 VMware Cloud Foundation (VCF) 솔루션을 다룬다.

VCF의 설계 고려 사항을 이해한 파트너와 고객의 엔지니어에게 Orbrium Cloud Portal의 운영을 위한 포괄적인 개관 제공을 목적으로 한다.

- 사전 설계에 기반하여 Etevers Virtualization Standard (EVS) 및 Etevers VMware Cloud Standard (EVCS) 아키텍처의 SDDC 토폴로지를 구현한다.
- EVCS 아키텍처의 SDDC 토폴로지 환경에 Orbrium을 구현한다.

## **프로젝트에 대해**

에티버스 D&N SDI사업본부는 국내 최초의 VMware 한국 총판으로서 소프트웨어 정의 데이터 센터 솔루션 및 보안 솔루션을 공급하고 있다.

이 프로젝트는 구 VMware Korea 전인호 지사장의 리더십에서 시작하였으며, Broadcom 김정환 부사장 및 오용원 부사장이 이어받아 완료하였다.

에티버스 D&N부문 김범수 대표와 SDI사업본부 이정현 본부장은 VMware Cloud Management Business Unit 장혜천 상무를 영입하여 프로젝트의 정신적 승계하였고, 프라이빗 클라우드 서비스로서의 프레임워크 기술 구현을 시작하였다.

VMware by Broadcom의 Commercial & Partners Sales 팀 리더인 이형직 전무는 에티버스의 프로젝트를 전폭 지지 및 커머셜 티어를 위한 채널 비즈니스 강화로서 적극 추진하였으며, 한국 부사장 임원석 부사장 및 오용원 부사장은 이를 전사적 프로젝트로서 인수하고 Broadcom Customer Experience Services와 연계하여 전체 고객 만족을 위한 비즈니스 모델인 VCF Unified Experience (VUE)로 재설계하였다.

# 저자 서문

"클라우드"라는 것을 단순히 기술 구현의 문제로 접근할 때, 우리는 많은 어려움을 겪게 됩니다. 근원적으로 가장 큰 어려움은 "클라우드"라는 것의 실체와 정의가 없다는 것입니다. 많은 사람들이 클라우드를 기술적인 요소로 접근하지만, 정확히 클라우드를 정의할 단위 기술은 존재하지 않습니다.

사실상 클라우드는 하드웨어, 소프트웨어, 컴퓨팅, 네트워크, 스토리지, 운영체제, 소프트웨어, 보안, 알고리즘, API, 운영 방법론, 비즈니스 서비스 등을 서로 하나로 묶어놓은 "연동체" 개념으로 보아야 합니다.

그렇기에 단순히 몇몇 기술이나 사람으로 거대한 "연동체" 개념을 설계하고 운영하기란 쉽지 않은 일입니다.

만약 클라우드를 "연동체" 개념으로 바라본다면, 우리가 먼저 생각해 보아야 할 것들은 다음과 같을 것입니다.

- 연동을 통해 이루고자 하는 목표가 무엇인가?
- 목표를 이루기 위해 어떠한 요소들을 연동할 것인가?
- 여러 요소를 어떠한 방법으로 연동할 것인가?

사실 이 부분에서 VMware는 물리적인 많은 부분을 논리적인 요소로 바꿔주며, 여러 인프라 기술 간에 효과적인 연동을 통해 많은 답을 주고 있습니다.

그렇기에 많은 사람들이 VMware 제품을 구입하면 클라우드를 구축한다는 오해가 만연한 것도 사실입니다.

무수히 수행되었던 클라우드 구축 목표에서 VMware는 클라우드를 구축하기 위한 훌륭한 재료일 수 있었으나, 최종적으로 앞선 질문에 대한 결론이 부족하여 원하던 만큼의 성과가 이루어진 사례가 소수인 점도 사실입니다.

VUE (VMware Unified Experience)는 VMware 생태계를 활용하여 최종적으로 위의 질문에 답하기 위한 최종적인 방법들을 제공합니다.

EVCS (Etevers VMware Cloud Standards)를 통해 VMware 생태계를 활용하여 표준 논리 구성을 완성하고,

BVP (Broadcom Value Pack)를 통해 표준 클라우드 운영 방안을 수행하고,

Orbrium을 통해 최종 완성된 클라우드 경험을 제공합니다.

VUE를 통하여 많은 분이 클라우드 경험을 완성하기를 소원합니다.

– 장혜천

# Chapter 1. 소개

VCF는 VMware by Broadcom의 SDDC 제품을 모두 모아 소프트웨어 정의 인프라스트럭처 중앙 관리 소프트웨어인 SDDC Manager를 통해 프라이빗 클라우드 인프라스트럭처를 구현하는 솔루션이다.

VCF Unified Experience는 제조사-총판-리셀러의 상생협력 체제로서, Broadcom의 업무 기술 방법론과 절차를 표준화하여 고객 경험을 향상시키는 기술 비즈니스 모델인 상생협력 체제이다.

프라이빗 클라우드의 상용 표준화를 구현하기 위한 3종의 업무 모델을 가지고 있다.

1. Etevers VMware Cloud Standard
2. Broadcom Value Pack
3. Orbrium

## 1.1. EVCS



EVCS는 국내 환경 특성에 맞춘 손쉬운 VCF 표준 설계안을 제공하며, 모든 파트너의 기술 이행 표준화를 돋고자 하였다.

VCF로 구현하는 SDDC 두 인프라스트럭처 환경을 가진다.

- 지원 인프라스트럭처
- 클라우드 서비스 인프라스트럭처

### 1.1.1. EVCS Architecture

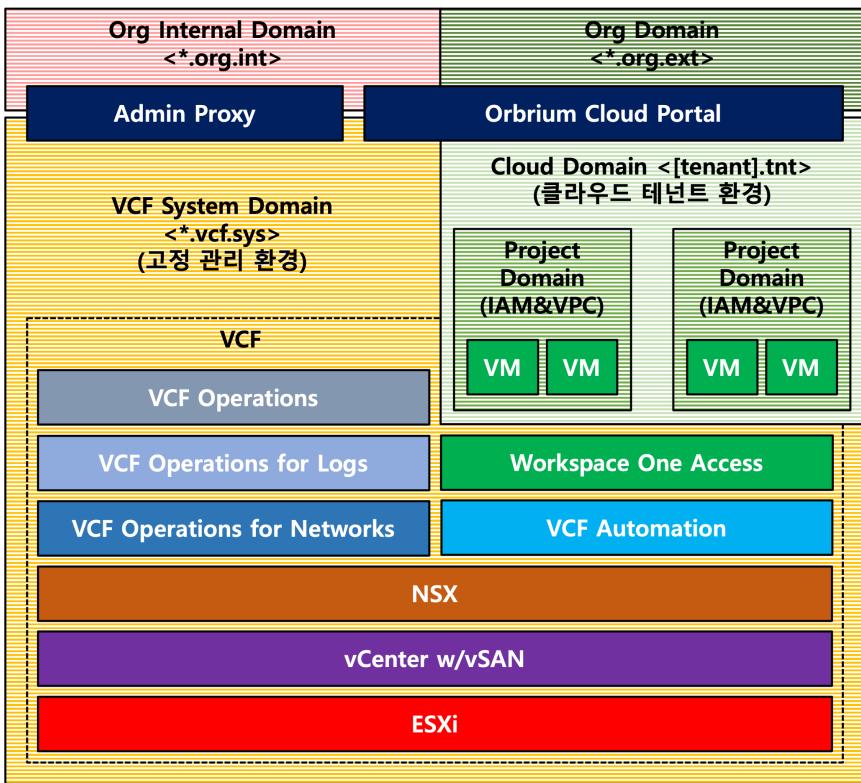


그림 1. EVCS 스택

EVCS는 VCF의 클라우드 서비스 인프라스트럭처를 위한 아키텍처이다. Broadcom CXS의 상용 클라우드 구현 방안을 따라 BVP 및 Orbrium을 배포할 SDDC 구조이다.

### 1.1.2. EVS Architecture

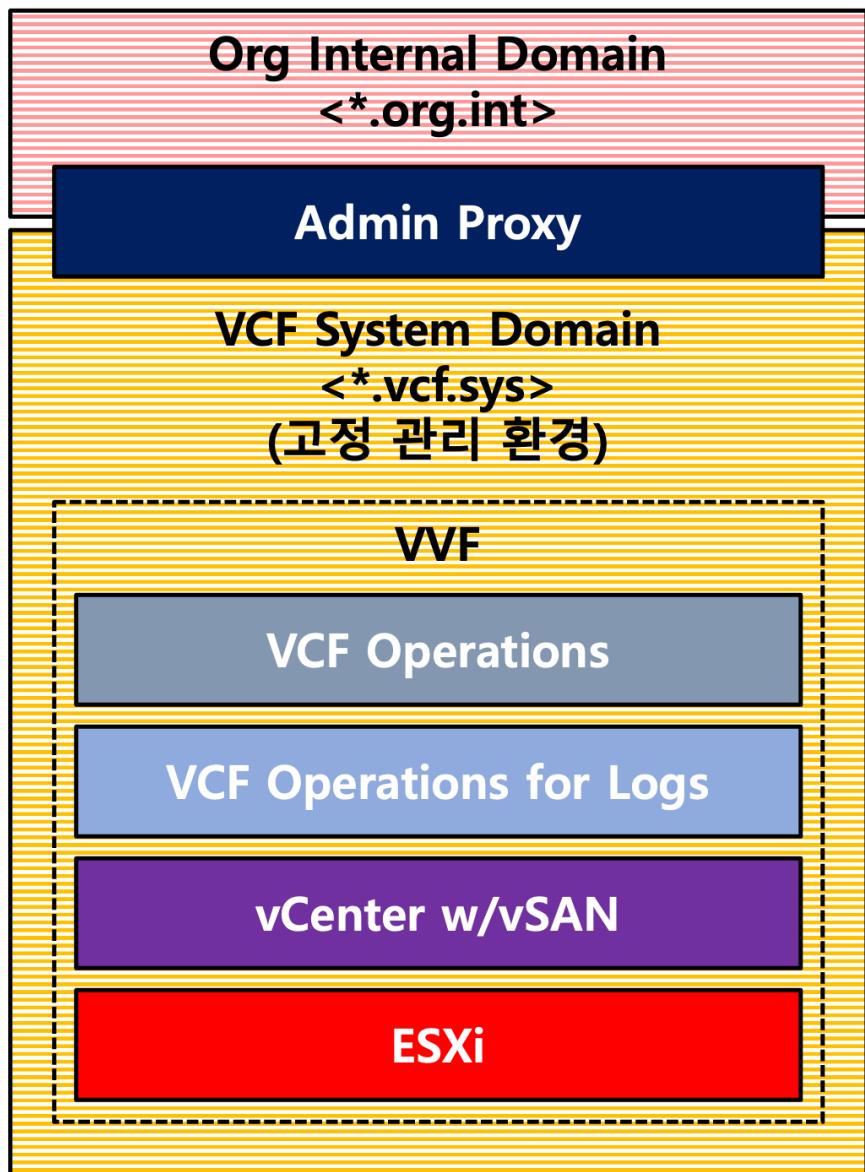


그림 2. EVS 스택

EVS는 VCF의 지원 인프라스트럭처 환경을 위한 아키텍처이다. SDDC 및 클라우드 구현에 수반되는 전통 인프라스트럭처 시스템의 가상화 데이터 센터 구조이다.

EVS는 VMware vSphere Foundation (VVF) 솔루션<sup>[1]</sup>을 따르며, vSphere 설계는 VCF와 동일한 구성을 권한다.



VCF 9부터 VVF 및 VCF 환경을 배포 및  
라이프사이클 관리를 통합할 것으로 알려졌다.  
그러므로 각 인프라스트럭처의 vSphere 환경 구성이  
서로 동일한 VMware Validated Solutions 지침을  
따름이 유리하다.

필요 서비스만 살피면 지원 인프라스트럭처의 구현은 가상화 데이터 센터 여부와는 무관하나, EVS의 추종을 권장한다.

## 1.2. Broadcom Value Pack



BVP는 Broadcom Customer Experience Services (이하 Broadcom CXS) 조직에서 제공하는 클라우드 인프라 서비스를 위한 부가 서비스이다.

상용 클라우드 표준에 맞추어 리소스 프로비저닝을 자동화하기 위해 미리 구성된 템플릿을 제공한다. 템플릿은 6개의 기본 범주로 구성하였으며, 사용자가 다양한 사용 사례에 맞게 서비스를 빠르고 효율적으로 구성할 수 있다. 사용자는 이러한 템플릿을 활용하여 VCF 환경 전반에 인프라 구성 요소 배포를 자동화/간소화할 수 있다.<sup>[2]</sup>

1. Compute
2. Network
  - a. VPC
  - b. Access IP
  - c. Load Balancer
  - d. Segment
  - e. Segment Peering
3. Storage
  - a. Block Disk
  - b. Network File System

4. Security
  - a. Distributed Firewall
5. Container
  - a. Kubernetes Cluster
  - b. Kubernetes Namespace
6. Database
  - a. PostgreSQL
  - b. MySQL

## 1.3. Orbrium



Orbrium은 BVP의 방안에 맞춘 API 프레임워크를 기반으로 하여, 클라우드 사용성 표준화를 내세운 클라우드 이용자 포털이다.

Identity Manager와 연동한 별도의 엔터프라이즈 환경의 통합 인증 기능을 제공하며, 승인 및 권한 제어를 통한 운영 절차 확립을 제공한다.



클라우드 주문을 실현하는 마법의 구슬 orb이 있는 공간 rium을 뜻한다. 클라우드 구축과 서비스 제공을 어렵게 만들었던 다양한 요소를 Orbrium 통하여 체계성을 가지며 접근할 수 있다.

EVS 및 EVCS 아키텍처 환경에서의 사용과 Admin Proxy 구현에 대해 기술 지원을 제공한다.

### 1.3.1. Orbrium 연동체 개념

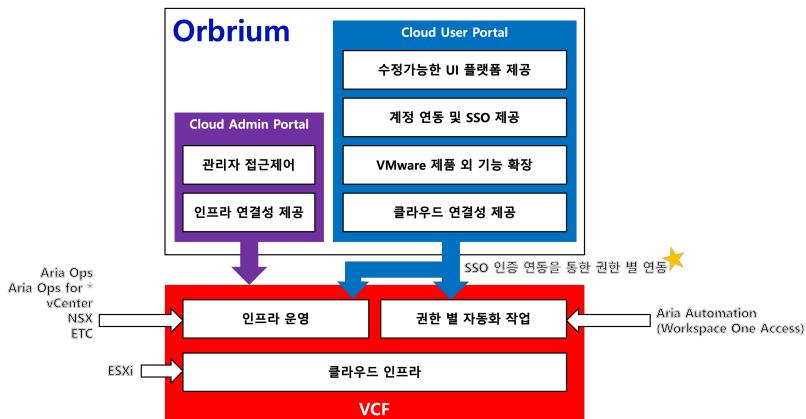


그림 3. Orbrium 연동체 개념

#### Admin Proxy

지원 인프라 스트럭처와 클라우드 서비스 인프라스트럭처 사이에는 웹 애플리케이션 프록시 서버가 위치한다. 클라우드 서비스 인프라스트럭처를 대상으로한 정보 노출 및 접근 통제 역할이다.

#### Orbrium Cloud Portal

EVS, EVCS 그리고 Admin Proxy를 포함한 연동체 역할을 하는 클라우드 사용자 포털이다.

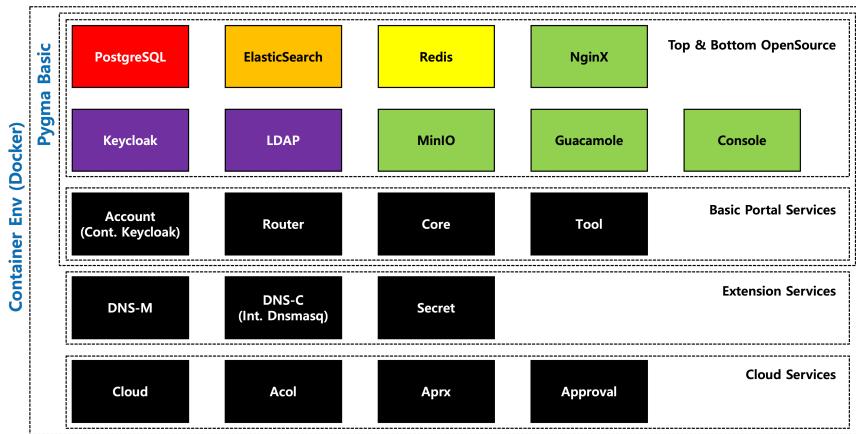


그림 4. Orbrium Cloud Portal의 서비스 컴포넌트

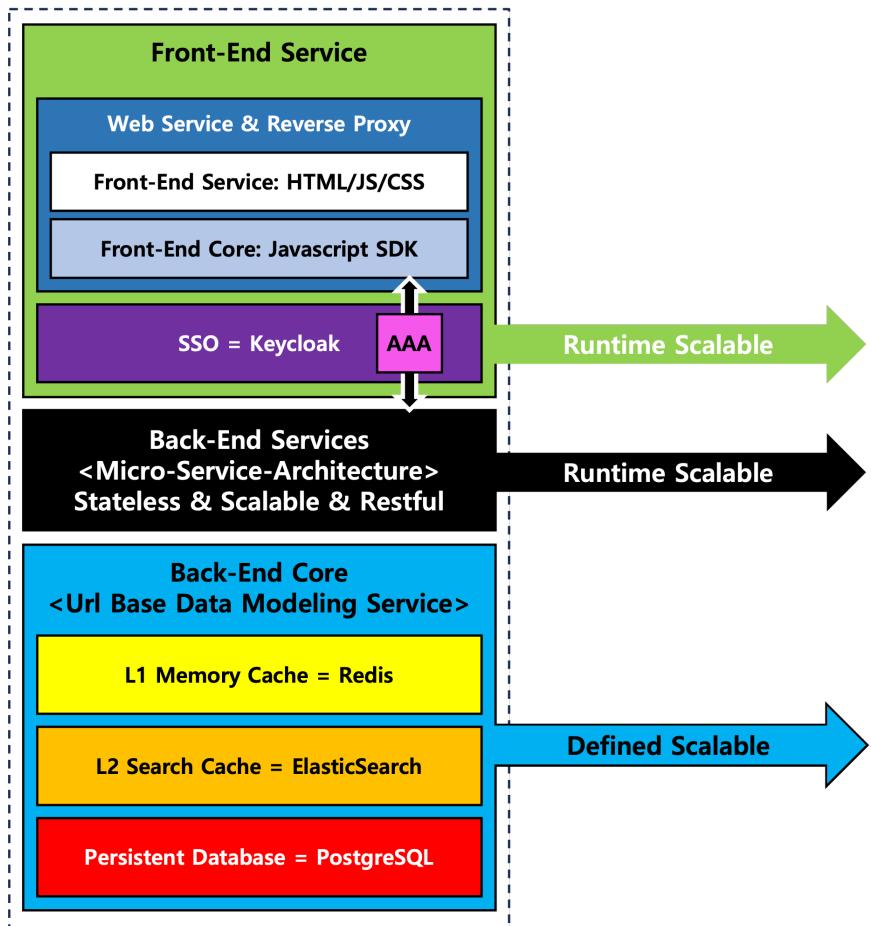


그림 5. Orbrium Cloud Portal 서비스 스택

[1] VMware by Broadcom. (2024). What Is VSphere Foundation? Broadcom Tech Docs Portal. <https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vsphere-foundation/5-2/vvf-getting-started-5-2/what-is-vsphere-foundation.html>

[2] Moon, S. (2025). Broadcom Value Pack (BVP) Package. GitHub. <https://github.com/etevers-vcs/broadcom-value-pack>

# Chapter 2. 공통 인프라스트럭처

공통 인프라스트럭처는 EVCS에서 정의하는 표현이다.

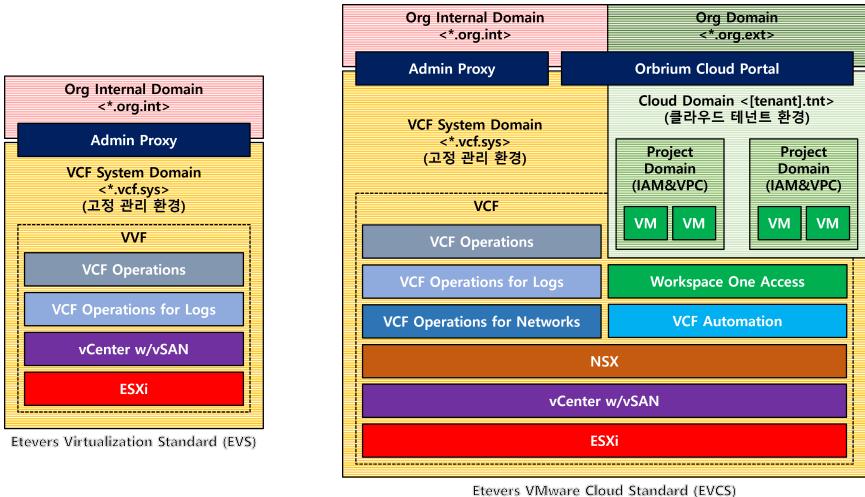


그림 6. EVS & EVCS 스택

지원 인프라스트럭처는 클라우드 서비스 인프라스트럭처처럼 vSphere 기반 환경을 갖출 수 있으며, 기반을 통합하여 설계 및 유지보수 업무 절차를 통합한다. 이를 '공통 인프라스트럭처' 환경으로 정의한다.

공통 인프라스트럭처 환경은 언더레이어 네트워크에 기반하며, 다양한 하드웨어 스택과 밀접한 업무 연관성을 갖추고 있다.

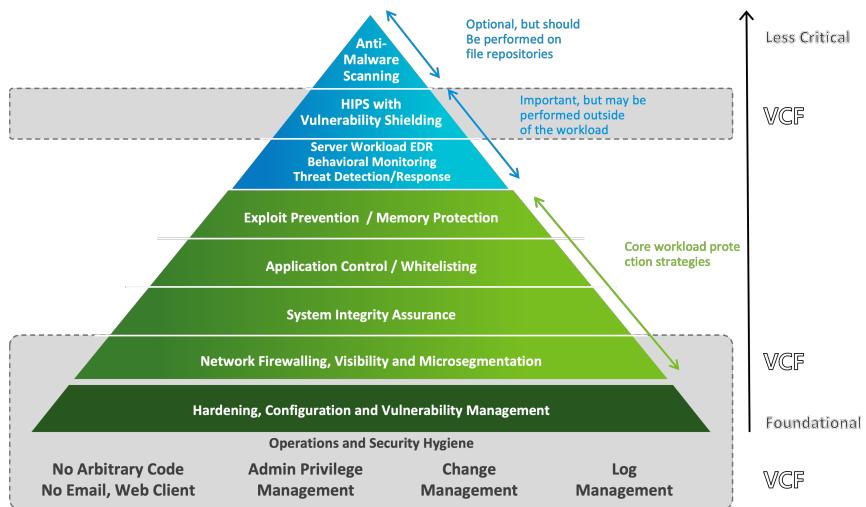


그림 7. 워크로드 보호 통제 계층과 VCF의 역할<sup>[1]</sup>

또한 사이버보안으로서 워크로드 보호 통제 계층을 고려하여 설계한다.

## 2.1. 네트워킹

VMware Validated Solutions에서 네트워크 서비스는 이중화를 기반으로 한다. EVCS도 이를 따른다.



PoC 등을 위해 L3 스위치 구성으로 이중화 인식을 시킬 수 있다.

### 2.1.1. 스위치 (하드웨어)

L2 스위치를 쓰는 경우, 적어도 하기의 국제 표준 프로토콜을 지원해야 한다.

- IEEE 802.1Q (VLAN, trunking)
- 이더넷 프레임 9038 바이트 이상의 Jumbo Frame

네트워크 이중화의 경우, STP 연결 설계를 해야 한다.

- IEEE 802.1d (STP)
- IEEE 802.1w (RSTP)
- IEEE 802.1s (MSTP, default)



Beacon Probing<sup>[2]</sup>은 최후의 수단이며, 실현 및 관리에 어려움이 있다.

### 2.1.2. 대역폭

네트워크 인터페이스 카드는 기본 10Gbps 이상으로 선택한다.

VCF는 10Gbps 미만 대역폭을 허용하지 않으며, 이전의 여러 1Gbps pNIC을 활용한 vSphere 기능별 트래픽 분할 방법론은 불가하다.

vSAN ESA와 같은 NVMe 기반 고속 HCI 스토리지 서비스를 구현한다면 스토리지 네트워크는 개념 증명 기준 25Gbps 이상으로 하며, 프로덕션의 경우 100Gbps를 기본으로 한다.

### 2.1.3. MTU

TCP/IP의 기본값인 MTU 1500 byte는 문제해결에 유연하게 대처할 수 있어야 하는 하이퍼바이저 및 관리 네트워크에 사용한다.

하이퍼바이저를 제외한 VCF 환경에서의 기본 MTU 값은 9000 바이트이다. 네트워크 스위치의 지원 사양에 따라 증감할 수 있다.

### 2.1.4. 라우터

L3 단계에서는 라우터의 역할과 트래픽 경로에 대한 이해를 필요로 한다.

라우터는 BGP 다이나믹 라우팅 프로토콜 사용하여 네트워크를 광고 및 재유통할 수 있어야 한다.

NSX는 BGP/OSPFv2 지원하고, 국내에서는 OSPF가 더 익숙할 수도 있겠으나, VCF의 SDDC Manager를 통한 Edge Cluster를 배포는 BGP를 사용한다.

#### 하드웨어 (스위치/라우터)

상기 사항과 네트워크 패킷 흐름을 고려하여 적절하게 구성한다.

#### 소프트웨어 (L3/L4/L7)

L3 이상의 언더레이어 네트워크는 가상화를 통해 소프트웨어화 구현할 수 있으나, 추가 설계를 고려해야 한다.



PoC 등의 특수한 상황에서의 네트워크 구현에 쓰일 수 있다.

L3의 경우, 고가의 스위치 가격에서 벗어날 여지가 있으나, 박스 단위의 스로우풋 보장이 없이 유연한 운영을 전제한다. 기업 문화에 따라 적용 및 유지보수에 어려운 요소를 포함한다.

L3의 경우, 이중화를 반드시 구현한다. 게이트웨이 접근 문제 시 전체 데이터 센터 전체 장애로 번질 수 있다. 스페이 높은 X86 서버 특성상 네트워크 박스보다 유지보수 리스크가 크다.

하이퍼바이저 단위의 망 혼용 관리 규정이 있거나, 별도의 언더레이 엣지 클러스터 구축 시의 비용 차이가 박스 장비 교체에 비해 크게 다르지 않을 수 있다.

Edge Cluster 전용의 vSphere Cluster를 별도로 운영하는 엔터프라이즈에서 고려하거나, 역으로 평시 트래픽이 높지 않은 않은 VVF 환경하에 고려할 수 있다.

#### 가상화 소프트웨어 라우터 구성 시,

- 소프트웨어 라우터만을 위한 포트 그룹을 만든다.
- 포트 그룹은 하이퍼바이저 호환 수준인 Ephemeral (no binding) 수준으로 구성한다.
- 라우터가 트래픽을 추적 및 집계할 수 있도록 promiscuous mode를 허용한다.
- 라우터가 작성하는 트래픽에 대한 오인이 발생하지 않도록 forged transmits을 허용한다.

#### 가상화 소프트웨어 라우터 이중화 구성 시,

- 이중화를 위한 시리얼 네트워크 포트 그룹을 만든다.

- 전통 네트워크 장비 이중화는 필연적으로 MAC 주소 위조가 발생하므로, 소프트웨어 라우터를 연결한 모든 포트 그룹에 MAC address changes를 허용한다.

## Distributed Port Group - Edit Settings | Trunk-SFOS

General	Promiscuous mode	Accept ▾
Advanced	MAC address changes	Accept ▾
VLAN	Forged transmits	Accept ▾
<b>Security</b>		
Traffic shaping	<b>MAC Learning</b>	
Teaming and failover	Status	Disabled ▾
Monitoring	Allow unicast flooding	Enabled ▾
Miscellaneous	MAC limit	4096
	MAC limit policy	Allow ▾

그림 8. 소프트웨어 라우터를 위한 포트 그룹 구성 예시



경우에 따라서는 소프트웨어 라우터의 OS에 따라  
점보 프레임을 제대로 다룰 수 있는 커널을 가졌는지  
살펴야 한다.

### 2.1.5. Domain Name System

지원 인프라스터럭처 및 클라우드 서비스 인프라스터럭처 양측에서  
DNS 서버를 구현해야 한다.

Cross-Origin Resource Sharing (CORS) 체크는 모던 서비스 간  
연결의 기본이며, 클라우드 인프라스트럭처 또한 이에 대한 준수를  
요한다.

최상위 도메인과 2단계 도메인의 정의하여 그리고 Fully Qualified Domain Name (FQDN)과 Uniform Resource Identifier (URI) 사용해 통신하기 위함이다.

Open Source를 활용할 경우, 다양한 소프트웨어를 통해 직접 구현할 수 있다. 예를 들면 하기와 같다.

- DNS: Unbound, Dnsmasq or et cetera

VMware가 지원하는 Microsoft Active Directory 사용할 경우, DNS 서버가 기본 동작한다.

- DNS: Active Directory Domain Services

## Top-level domain

최상위 도메인은 .com, .one, .network, .local과 같은 접미사 도메인이며, 용도 등을 나타내는 데 쓰인다.

조직 도메인을 고를 때는 IANA가 선언한 특수 용도 도메인 이름<sup>[3]</sup>을 피하여 고유한 접미사를 선택한다.



.local 접미사도 RFC 규약에 의해 mDNS를 위한 용도와 목적이 있다. 자동 할당 시에 임시로 사용되는 도메인이다. 규약에 집착하는 앱의 경우, 통신에 문제가 없어도 고의로 특수 용도 도메인에 거절하여 방해하는 사례가 흔하다. 호스트에.local 사용 시, 타 서비스와의 통신에 사용하지 말 것.

## Second-level domain

2단계 도메인은 최상위 도메인 앞에 기입하며, 조직 이름 등으로 널리 쓰인다.

각 인프라스트럭처 환경의 이름에 사용한다.

## Fully Qualified Domain Name

정규화 도메인 이름은 호스트 (인스턴스) 간 고유한 전체 도메인 이름이다.

FQDN은 특정 도메인으로 이동하는 트래픽을 허용하거나 거부하는 방화벽 규칙에 쓰일 수 있다.<sup>[4]</sup>

## Public DNS

인터넷에 노출하는 외부 네임 서버이다. ICANN에서 제공하는 일반 최상위 도메인 (generic top-level domain, gTLD)을 사용한다.

## ORG DNS

gTLD를 사용하는 조직 내부의 네임 서버이다. 조직원이 인터넷과 동일한 도메인으로 사내망을 통해 접속하여 이용함으로써 패킷이 밖으로 흐르는 요소를 막는다. 예상치 못한 부하나 패킷 감청으로부터 보안을 지키기 위한 기본 영역이다.



온프레미스의 경우, 외부에 서버를 노출 시키는 Web Application Firewall이 함께한다.

## ORG Internal DNS

EVS 지원 인프라스트럭처가 사용하는 조직 내부의 Admin Proxy 네임 서버이다.

클라우드 사용자는 Admin Proxy에 접근하며 계류하는 영역이다.

ORG Internal Domain에서는 Cloud System Domain의 클라우드 서비스 인프라스트럭처의 아이피를 확인할 수 없으며, Reverse Proxy에서

인가한 프로토콜 및 포트를 통해 접근만 할 수 있다.

고유한 최상위 도메인 및 2단계 도메인을 서비스한다.

### Cloud System DNS

EVCS 클라우드 서비스 인프라스트럭쳐가 사용하는 조직 네임 서버이다.

각 연결 호스트 간의 실제 모든 아이피를 서비스한다.



VMware by Broadcom은 Planning and Preparation Workbook은 ORG Internal Domain의 2단계 도메인을 공유하여 서브도메인을 선택하도록 권하고 있다. 이는 Private CA의 중간 인증 기관 (Intermediate CA)에서 SSL 인증서를 발급하는 설계로 보인다.

EVCS에서는 고유한 최상위 도메인 혹은 2단계 도메인으로 선택한다.

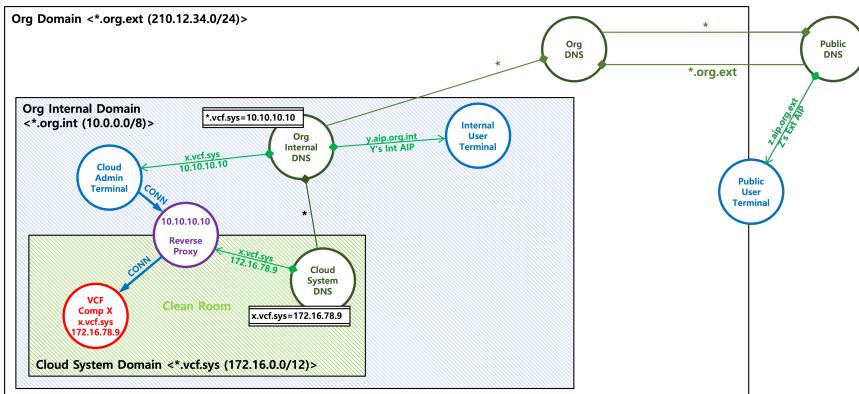


그림 9. 용도 별 DNS 위치

## 2.1.6. NTP

vCenter를 포함해 서버 간 역할에 있어 순차 오동작이 없도록 하려면 모든 서버의 시간을 동기화하여야 한다.

Open Source를 활용할 경우, 다양한 소프트웨어를 통해 직접 구현할 수 있다. 예를 들면 하기와 같다.

- NTP: NTPD

VMware가 지원하는 Microsoft Active Directory 사용할 경우, 하기의 기능을 켜 구현할 수 있다.

- NTP: Windows Time Services



Microsoft Active Directory는 도메인 컨트롤러 그룹 정책을 한 번만 편집하여 기능을 켠다.<sup>[5]</sup> 이후에는 도메인 커트롤러를 만들 때마다 자동으로 NTP 서버가 동작한다.



NTP 서버를 가상 머신으로 구현할 경우, VMware Tools 및 Open VM Tools의 기본 기능인 호스트와의 시간 동기화 기능을 끈다.<sup>[6]</sup>

## Edit Settings | et-dc1-win2025

Virtual Hardware    VM Options    Advanced Parameters

> General Options    VM Name: et-dc1-win2025

> VMware Remote Console Options    Expand for VMware Remote Console settings

> Encryption    Expand for encryption settings

▼ VMware Tools

**Power Operations**

- ▷ Power On / Resume VM
- Shut Down Guest (Default) ▾
- Suspend (Default) ▾
- Restart Guest (Default) ▾

Tools Upgrades

Check and upgrade VMware Tools before each power on

**Synchronize Time with Host** ⓘ

Synchronize at startup and resume (recommended)

Synchronize time periodically

**Run VMware Tools Scripts**

After powering on

After resuming

Before suspending

Before shutting down guest

그림 10. vCenter에서 시간 동기화 옵션을 비활성화한 화면

## **2.2. Network Attached Storage**

SDDC Manager, vCenter, NSX Manager의 구성 백업/복원을 위해 네트워크 결합 스토리지를 구현한다.

## 2.3. Object Storage Service

데이터베이스 정보 저장/백업/복원을 위해 오브젝트 스토리지 서비스 (OSS) 구현을 고려한다.

OSS의 구현은 선택사항이다. 현재 EVCS 환경에 OSS의 구현을 고려할 요소는 크게 두 가지이다.

1. Orbrium Cloud Portal에서의 프록시 사용
2. Data Services Manager (DSM) 사용

### 2.3.1. Data Services Manager

현재 DSM은 VCF에 번들 공급할 뿐, 기본 배포 구성에서 제외하였다. VCF 9 카탈로그로 미뤄볼 때 차기 버전에서 통합될 것으로 예측하였다.

DSM은 OSS를 사용하여 동시에 서비스한다.

1. 기 구축한 OSS와 연결하여 데이터베이스 관리 정보 저장
2. 기 구축한 OSS와 연결하여 데이터베이스 백업/복원
3. MinIO AIStor 라이선스 통한 vCenter 통합<sup>[7]</sup>

## 2.4. 보안

클라우드 서비스 운영은 인프라스트럭처 보안은 물론 신원 및 접근 관리에 대한 기본 설계를 요한다.

### 2.4.1. 인프라스트럭처 보안

기존의 vSphere 환경 설계 및 구현 시에 익숙한 요소이다.

- 추상화를 통한 격리
- 네트워크 격리 및 네트워크 트래픽 제어
- 통신 암호화

#### 추상화를 통한 격리

가상화 기술의 기본 보안 요소로서, VCF 솔루션을 도입하여 기본 충족한다 볼 수 있으나, 보안 규정 수준에 따라 Trusted Platform Module (TPM) 기술을 활용한 VM 키 관리와 스토리지 퍼포먼스의 균형을 고려하여 하드웨어 추가 설계를 고려한다.

#### 네트워크 격리 및 네트워크 트래픽 제어

네트워크 격리는 VLAN을 사용하여 구현하는 네트워크 간섭 사고 및 공격을 방지하기 위한 기본 격리 시나리오이다.

- 하이퍼바이저 네트워크
- 관리 네트워크
- vMotion 네트워크
- Overlay Tunnel End Point (TEP) 네트워크
- Intelligent Platform Management Interface (IPMI) 네트워크

- 백업 네트워크
- 기타

네트워크 트래픽 제어는 규정을 준수하는 각 네트워크와 어떠한 수단을 통하여 어느 정도 통신할 지에 대한 이중화 시나리오이다.

- 물리 네트워크 인터페이스 카드 (pNIC)
- 가상화 스위치 포트 그룹
- Quality of Service (QoS)

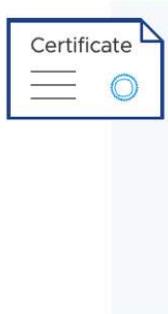
pNIC의 필요 수량에 따라 x86 서버의 프로세서 다중화 및 유닛 크기에 영향을 미치므로 공급하는 하이퍼바이저 설계와 병행해야 한다.

## 통신 암호화

SSL/TLS 인증서는 서버와 클라이언트 간의 통신에 비밀을 보장하고 감청을 방지하는 종단 간 암호화 기술이다.

SSL/TLS 인증서 발행처를 인증 기관 (CA)라 하며, 유형과 목적에 따라 나눌 수 있다.

SSL/TLS 인증서를 통한 통신 암호화는 기본 업무 절차 중 하나이다. CA는 가능한 한 통일해야 한다. 전체 인프라스트럭처 및 애플리케이션에 걸쳐 신뢰 등록해야 할 인증서를 줄이기 위함이다.



<b>Certificate</b>	
<u>Country</u>	: Two uppercase letters only (Example: US)
<u>Name</u>	: FQDN of the vCenter Server ( <b>Subject Alternate Name</b> )
<u>Organization</u>	: Company Name
<u>OrgUnit</u>	: Department name within the organization (Example: IT)
<u>State</u>	: The state/province where your company is located
<u>Locality</u>	: The city where your company is located.
<u>IPAddress</u>	: IP Address of vCenter Server (optional)
<u>Email</u>	: Email Address
<u>Hostname</u>	: <b>FQDN of vCenter Server</b>

그림 11. SSL/TLS 인증서 생성 시 기재 항목.<sup>[8]</sup>

또한 SSL/TLS 인증서는 암호화 사설 키의 유출을 고려하여 발급 시의 이용 기한이 정해져 있다. 인증 기한 도달 전 교체하지 않으면 통신이 정지하며 업무의 정지를 유발한다.

이를 해결하기 위해 인프라스트럭처 관리 조직은 Root CA를 만들고 인증서 발급을 중앙 관리하도록 해야 하며, 보안 규정 요소에 따라 중간 인증 기관 (Intermediate CA)을 통해 유연한 SSL/TLS 인증서 발급 및 관리를 구현하도록 설계해야 한다.

통신 암호화는 네트워크 격리와 함께 VCF 배포 전에 고려해야 할 사안 중 하나이다.



SSL/TLS 인증서의 유효 기간 국제 표준은 지속 짧아지고 있으며, 자동화를 권장하고 있다. 2029년까지 49일 단위 재발급을 구현해야 한다. Apple의 경우, 서버 인증서가 표준 기한을 지키지 않으면 OS가 앱을 일시 정지한다.<sup>[9]</sup> CA의 루트 인증서가 신뢰 상태여도 발생하며, 이러한 표준을 지키지 않은 모든 서버 인증서를 서비스 이용자가 직접 개별 허용해야 한다.

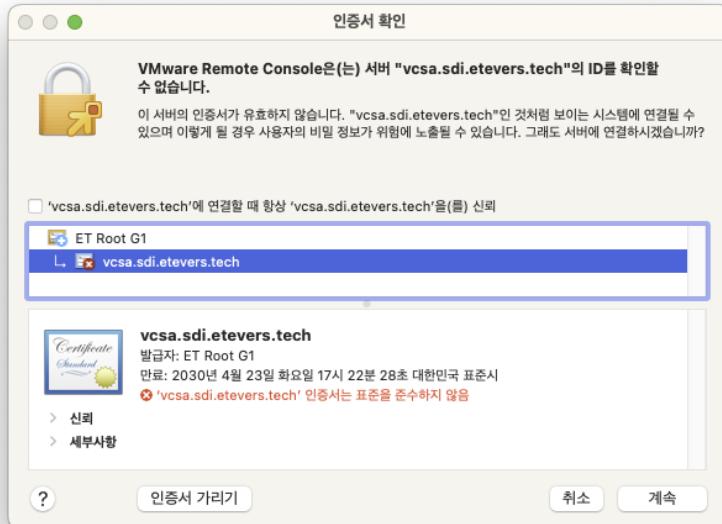


그림 12. 사설 인증 기관이 평의를 위해 인증서 기한을 임의로 늘렸을 때 Apple의 OS에서의 메시지

#### Public CA 및 Private CA



Public CA는 국제 기관 및 기업간 조율에 의해 신용하기로 결정하여, 이들의 인증서는 컴퓨터 운영체제 또는 웹 브라우저에 기본 포함한다. Private CA는 누구나 직접 SSL/TLS 인증서를 발행하고 암호화 키를 관리할 수 있는 OpenSSL기술을 활용한 사설 CA를 뜻한다.

#### Root CA 및 Intermediate CA



Root CA는 최초의 CA이며, Intermediate CA는 Root CA로부터 SSL 인증서를 발급할 권한을 부여받은 2차 CA다.

## vCenter Server Appliance

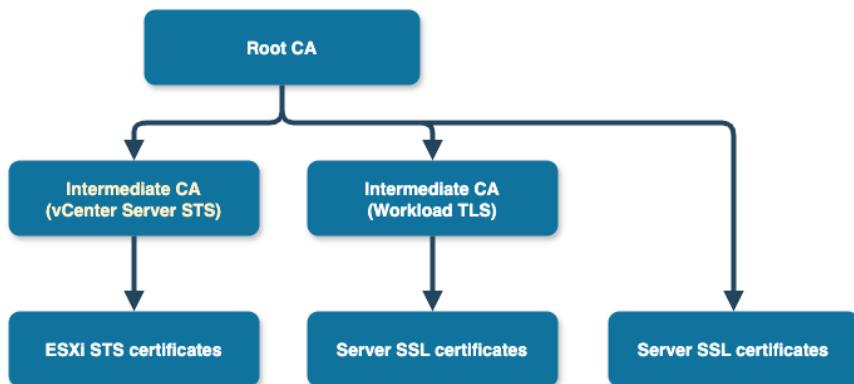
vCenter 기본 배포 시, Root CA인 VMware Certificate Authority (VMCA)를 생성하며 크게 두 목적을 위해 CA를 사용한다.

1. vSphere Client 및 VMware Remote Console 등 VI Admin 접근을 위한 HTML 및 API 통신
2. 하이퍼바이저 중앙 관리 통신 (vCenter Security Token Service)

## SDDC Manager

SDDC Manager 배포 후, VCF 솔루션의 SSL/TLS 인증서 통합을 위한 Private CA를 생성하거나, Active Directory Certificate Services (ADCS)에 인증서 요청 및 발급을 통합할 수 있다.

### CA 트리 시나리오



조직의 인증서 관리 규정을 일괄 적용해야 할 경우에는 vCenter STS의 인증서를 중간 인증 기관 CA로 교체하여 관리하도록 구성한다.



VMware by Broadcom은 vCenter Server STS 인증서의 교체를 지양하도록 권고한다.<sup>[10]</sup>

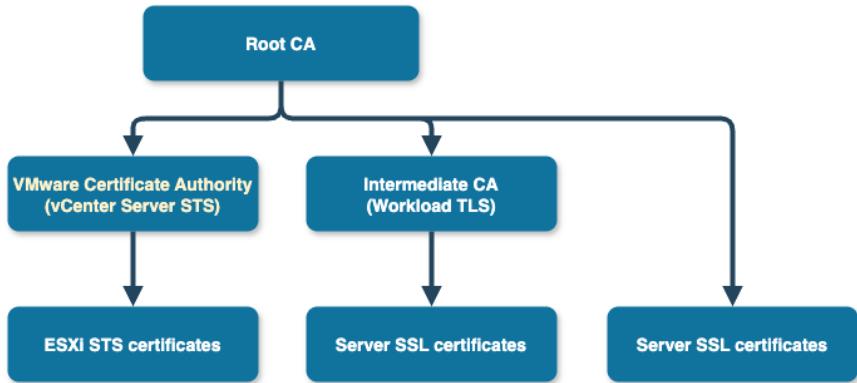


그림 14. CA 트리 시나리오 2 - Root CAT와 하이퍼바이저 인증서 분리

일반 배포 시나리오이며, vCenter Server STS 인증서만 vCenter가 관리하도록 두고, vSphere Client의 SSL/TLS 인증서만 통합한다.

## 2.4.2. 신원 관리

통신 암호화 고려와 함께, 추후의 클라우드 인프라스트럭처 신원 관리를 고려한다.

Open Source를 활용할 경우, 다양한 소프트웨어를 통해 직접 구현할 수 있다. 예를 들면 하기와 같다.

- LDAP: OpenLDAP (LightLDAP 비권장)
- CA: OpenSSL
- OIDC: Authentik, Apache Keycloak or et cetera

VMware가 지원하는 Microsoft Active Directory 사용 시, 하기의 기능을 통해 구현할 수 있다.

- LDAP: Active Directory Domain Services
- CA: Active Directory Certificate Services
- OIDC: Active Directory Federation Services

### LDAP

LDAP은 관문을 담당하는 공통 인프라스트럭처에서 구현하여 조직에 디렉터리 서비스를 제공한다.

클라우드 서비스 인프라스트럭처의 경우, 별도 구축 없이 지원 인프라스트럭처에 아웃바운드 접근하여 LDAP 신원 및 접근 관리를 수행한다.

### OIDC Single Sign-On

현대 웹앱 서비스에 신원 및 접근 관리로 역할 기반 접근 통제 (Role based Access Control, RBAC)를 구현할 때는 LDAP을 넘어서 OAuth

2.0을 적용한 OpenID Connect (OIDC) 기술이 널리 쓰인다. Aria Suite Lifecycle에 포함된 Identity Manager (Identity Manager) 또한 이런 기술을 접목하기 위해 제작되었다.

그러나 Identity Manager의 용도와 활용에 대해 고민해야 한다.

1. Identity Manager의 제작 목적이 인프라스트럭처 관점의 VMware Cloud Management Portal (CMP) 관리에 초점이 맞추어 있는 점
2. End User Computing Division의 분사 (Omnissa)로 인해 Identity Manager를 대체하는 새 소프트웨어의 개발이 필요한 점

그런므로 OIDC 또한 관문을 담당하는 공통 인프라스트럭처에서 별도로 구현하여 조직에 통합 서비스를 제공토록 한다.

- [1] Macdonald, N., & Croll, T. (2020). Market Guide for Cloud Workload Protection Platforms. Gartner. <https://www.gartner.com/en/documents/4003465>
- [2] What Is Beacon Probing? (2025). Broadcom. <https://knowledge.broadcom.com/external/article/324536/what-is-beacon-probing.html>
- [3] Special-Use Domain Names. (2024). Internet Assigned Numbers Authority. <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml>
- [4] VMware by Broadcom. (2025)FQDN. Broadcom Tech Docs Portal. <https://techdocs.broadcom.com/kr/ko/vmware-cis/cloud/vmware-cloud-on-aws/SaaS/fqdn.html>
- [5] FoW. (2025). Active Directory Domain Services 컨트롤러 서버의 NTP 서버 켜기. Netsphere ONE. <https://netsphere.one/@FoW/114254578621689598>
- [6] Deji. (2016). Completely Disable Time Synchronization for Your VM. VMare Blogs. <https://blogs.vmware.com/apps/2016/01/completely-disable-time-synchronization-for-your-vm.html>
- [7] Minio. (2025). VMware Object Storage Solutions & Integration. MinIO. <https://min.io/solutions/vmware>
- [8] VTSP - VMware Cloud Foundation 5.1 (2024) for Partners. (2024). Learning@Broadcom. <https://brocade.csod.com>
- [9] 신뢰할 수 있는 인증서에 대한 향후 제한 사항에 관하여. (2023). Apple Support. <https://support.apple.com/ko-kr/102028>
- [10] Replace a VCenter Server STS Certificate Using the Command Line. (2025). Broadcom Tech Docs Portal. <https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/replace-an-sts-certificate.html>

# Chapter 3. 클라우드 서비스 인프라스트럭처

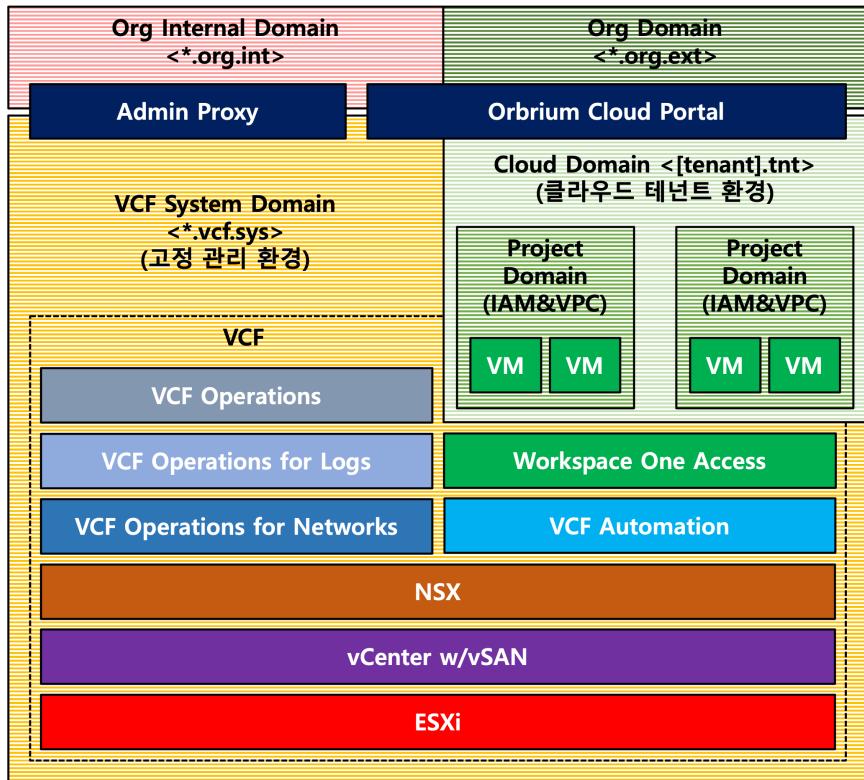


그림 15. EVCS 스택

### 3.1. 병합 아키텍처 모델

VCF 솔루션의 자원 사용 단위는 셋으로 구분한다. 병합 아키텍처 모델은 이러한 자원 할당을 클러스터 내 자원 풀로 구분하여 통제한다.

EVCS는 보다 폭 넓은 파트너 및 국내 환경을 고려하여 병합 클러스터 (consolidated cluster) 아키텍처를 골자로 하였다.



그림 16. 병합 아키텍처 예시 [1]

1. VCF 솔루션 관리
2. 워크로드

### 3. NSX Edge

최초의 VCF 데이터 센터는 병합 클러스터로 설계하고, 워크로드 클러스터 등을 추가하여 서비스의 안정성을 확장하는 방향으로 운영한다.

## 3.2. 동서 트래픽

### 3.2.1. Multitenancy

클라우드 이용자에게 고유한 서비스 영역 가치를 전달하려면 멀티테넌시가 필수이며, NSX가 서비스를 제공한다. VCF에서 NSX를 사용하여 멀티테넌시를 구현하는 방법론은 크게 두 가지이다.

#### NSX Virtual Private Cloud

NSX Virtual Private Cloud (VPC)는 프로젝트 단위의 테넌트 정의를 제공한다. VCF의 최신화 멀티테넌시 모델이다.

기본 NSX 인프라스터럭처의 복잡성을 숨김으로서 퍼블릭 클라우드 환경과 유사한 간소화된 네트워킹 및 보안 서비스 소비 모델을 제공한다.

#### Virtual Private Zone

Virtual Private Zone (VPZ)는 VCF Automation에서 테넌트 정의를 제공한다. vRealize Automation부터 이어진 멀티테넌시 모델이다. VCF Automation VPZ는 Automation Assembler 사용하여 이미지 및 플레이버 매핑을 구성할 때 멀티테넌시를 제공한다.

EVCS 5.2 및 Orbirum은 VCF Automtion VPZ를 사용하며, 클라우드 서비스 구현 시, 용어를 VPC로 통일한다.



vRealize Automation VPZ와 혼용할 수 있지만  
구성을 변경할 수 없으므로 VCF Automation  
VPZ과의 클라우드 서비스 구현 호환성을 고려해야  
한다.

### **3.2.2. NSX Overlay Transport network**

NSX Manager 및 오버레이 전송 네트워크는 VCF 최초 배포 시에 함께 펼치므로, 배포 전 패브릭을 설계한다. TEP 네트워크와 호스트는 고유한 VLAN과 아이피를 할당한다.

[VCF Overlay Networks] | images/VCF-Overlay-Networks.gif

그림 17. VCF 논리 네트워크.<sup>[2]</sup>

### **3.2.3. NSX Overlay network**

오버레이 네트워크를 설계한다. NSX 오버레이 네트워크는 북남 트래픽인 NSX Edge Cluster 배포를 반드시 선행해야 하므로 NSX 외부 라우터의 준비와 설계를 병행한다.

EVCS는 기본 오버레이 네트워크를 4종으로 정의한다.

1. Application Virtual Network
2. EVCS Private Network
3. EVCS Private Network
4. EVCS vSphere with Kubernetes Network

#### **Application Virtual Network**

SDDC Manager 통제 환경하에서 최초의 NSX 오버레이 네트워크는 반드시 프라이빗 클라우드 플랫폼을 위한 Application Virtual Network (AVN)이다.

- Aria Suite Lifecycle
- Identity Manager
- VCF Automation

- VCF Operations
  - VCF Operations for Networks
  - VCF Operations for Logs

프라이빗 클라우드 플랫폼의 컴포넌트 유형마다 고가용성 및 멀티 리전 지원 여부가 다르다. 유연한 구현 및 상황 대응을 고려해야 하므로 오버레이 네트워크에 배포하는 설계를 두고 있다.

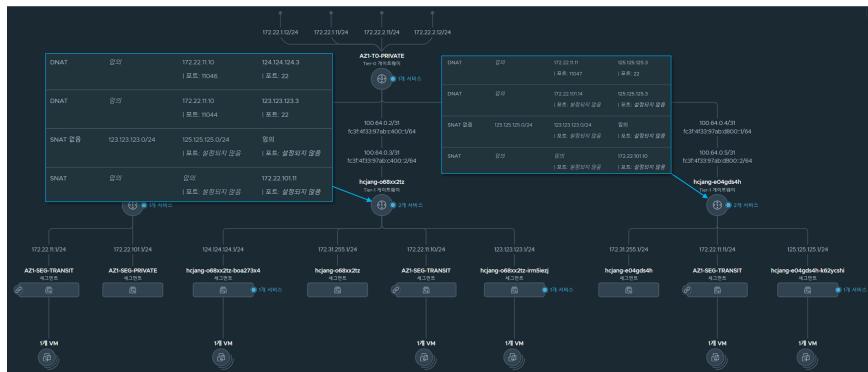
EVCS Public Network

Orburn이 통제하는 일반 워크로드 오버레이 네트워크이다.

**EVCS Private Network**

Orbirum이 통제하는 폐쇄 워크로드 오버레이 네트워크이다

EVCS 통해 구현한 VPC 예



# EVCS vSphere with Kubernetes Networks

Orbirum이 통제하는 Tanzu 워크로드 네트워크이다. SDDC Manager를 통해 선언한다.

## 3.3. 북남 트래픽

### 3.3.1. NSX Edge Clusters

VCF는 NSX Edge 클러스터는 A NSX EDGE 클러스터와 외부 라우터의 연결은 Active-Active 동작하도록 논리적 메시 구성하여 배포한다.

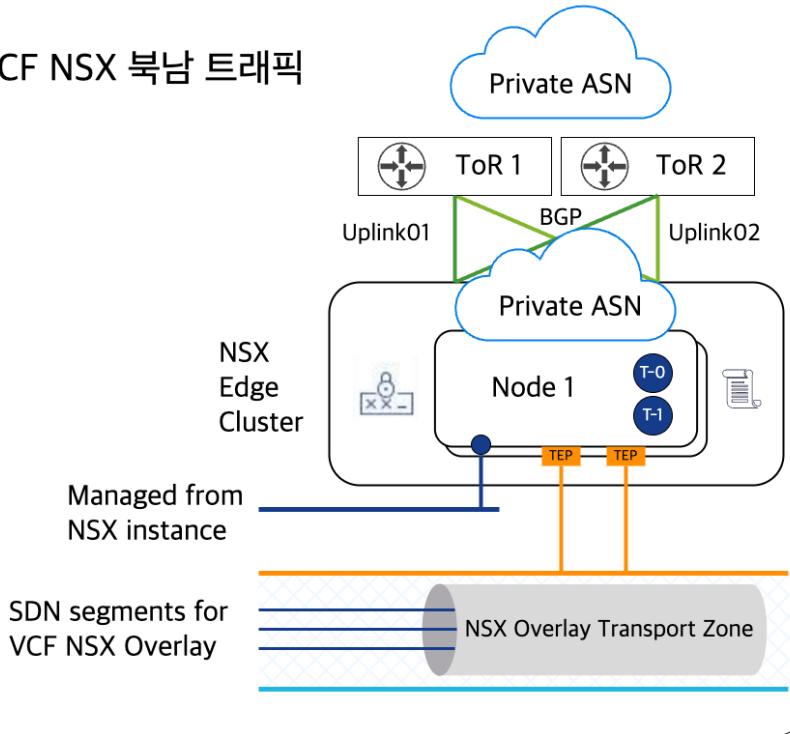


시험 환경의 경우, 한 대의 외부 라우터에 두 대 분의 네트워크 구성을 하여도 NSX에서는 이중화 구성으로 인식시킬 수 있다.

VCF 환경의 모든 NSX 오버레이 네트워크는 동일한 네트워크 구조의 NSX Edge 클러스터를 갖는다.

VCF 환경에서의 NSX Edge 클러스터 토플로지

## VCF NSX 북남 트래픽



한 대의 NSX Edge를 배포에 요구하는 네트워크 정보

- Edge Node 1: Edge Node Name (FQDN)
- Edge Node 1: Management IP (CIDR)
- Edge Node 1: Management Gateway
- Edge Node 1: Edge TEP 1 IP (CIDR)
- Edge Node 1: Edge TEP 2 IP (CIDR)
- Edge Node 1: Edge TEP Gateway
- Edge Node 1: Edge TEP VLAN
- Edge Node 1: Cluster
- Edge Node 1: Cluster Type

- Edge Node 1: First Uplink VLAN
- Edge Node 1: First Uplink Interface IP (CIDR)
- Edge Node 1: Peer IP (CIDR)
- Edge Node 1: ASN Peer
- Edge Node 1: BGP Peer Password
- Edge Node 1: Second Uplink VLAN
- Edge Node 1: Second Uplink Interface IP(CIDR)
- Edge Node 1: Peer IP (CIDR)
- Edge Node 1: ASN Peer



Autonomous System Number (ASN)에도 사설 영역이 있다. 64512-65534.

## Application Virtual Network

프라이빗 클라우드 플랫폼을 위한 2차 관리 네트워크이므로 NSX Edge 클러스터의 부하량이 상대적으로 적다.

기본 Medium 사이징 이상으로 배포하고 필요에 따라 스케일을 고려한다.

## 워크로드 네트워크

프로덕션 워크로드 VM의 트래픽은 Tier-1 게이트웨이와 Tier-0 게이트웨이를 수시로 거치거나 언더레이어 네트워크에 요청 및 응답하므로 부하량을 고려한 배포를 해야 한다.

기본 Large 사이징 이상으로 배포하고 필요에 따라 수시로 스케일을 고려한다.



한 번 배포한 NSX Edge 클러스터의 사이징은 SDDC Manager에서 변경할 수 없으며, CLI workaround 작업이 필요할 수 있다. SDDC Manager는 NSX Overlay 네트워크를 NSX Edge 클러스터와 동시에 취급하므로, 배포 전 예상 설계를 신중히 한다.

### 3.3.2. Gateway Load Balancer

VMware 클라우드 인프라스트럭처 문서는 Gateway Load Balancer (이하 GWLB)를 직접 언급하지 않았으나, Broadcom이 직접 공급하는 NSX를 위한 로드 밸런서는 두 종이다.

1. NSX Load Balancer
2. Avi Load Balancer

#### NSX Load Balancer

NSX에 기본 포함하여 제공하는 로드 밸런싱 기능이며, Tier-1 Gateway의 네트워크 서비스를 위한 기본 기능을 제공한다. L7 가상 서버에만 쿠기 영속성을 쓸 수 있다.

EVCS 5.2는 NSX 로드 밸런서만 사용한다.

Orbrium에서의 사용 (검토 필요)

로드 밸런서는 보통 인라인 또는 원암 모드로 배포한다. 원암 모드에는 Source NAT (SNAT) 구성이 필요하다.

Tier-1 게이트웨이에 위치하며 세그먼트의 통신 경로 조정하는 Arm 구성이며, Orbrium 전체 동작에 있어서는 Two Arm 구성이다.

## **Avi Load Balancer**

Avi Load Balancer (ALB)는 vSphere 언더레이와 NSX 오버레이 펼칠 수 있다. 단 컨트롤러당 하나의 네트워크 인프라스트럭처에 배포함이 표준 모델이다.

VCF의 경우, NSX 오버레이 네트워크 인프라스트럭처에 펼친다. 마찬가지로, SDDC Manager를 사용하여 배포 및 사용한다.

### **3.3.3. Global Server Load Balancing (GSLB)**

Global Server Load Balancing (GSLB)는 백본 네트워크를 거쳐 조직 도메인에 위치하며 외부와 통신하고 나아가서는 리전 간의 애플리케이션 고가용성을 위한 통신을 중개한다.

고객의 철학/유형/규제 등에 따라 설계와 구현이 상이한 영역이며, EVCS 5.2는 가이드하지 않는다.

## 3.4. 작업서 그리고 JSON

앞서 다른 컴포넌트 설계를 마친 후에 VMware by Broadcom이 제공한 작업서에 설계를 기입하고 서버 사양을 확정한다.

### 3.4.1. Planning and Preparation Workbook

Planning and Preparation Workbook은 Broadcom Tech Docs Portal<sup>[3]</sup>에서 내려받을 수 있다. Microsoft Excel을 이용하여 설계를 마친 VCF 구성을 기입할 수 있는 정밀 양식 파일이다.

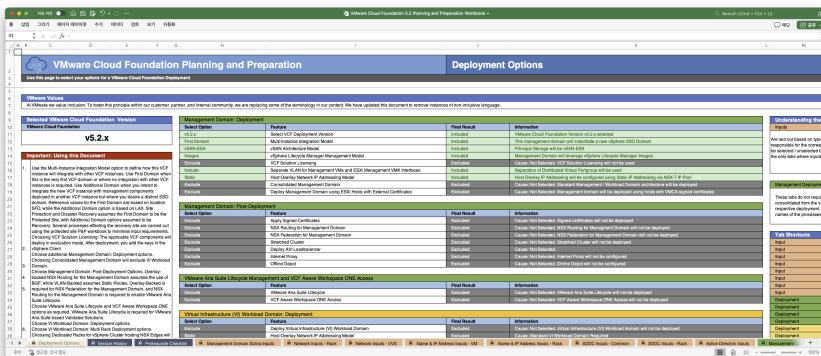


그림 18. Planning and Preparation Workbook 화면

### 3.4.2. Deployment Parameter Workbook

Deployment Parameter Workbook은 Broadcom Support Portal에서 제품과 함께 내려받을 수 있다. Microsoft Excel을 이용하여 설계를 마친 VCF 구성을 기입할 수 있는 간이 양식 파일이다.

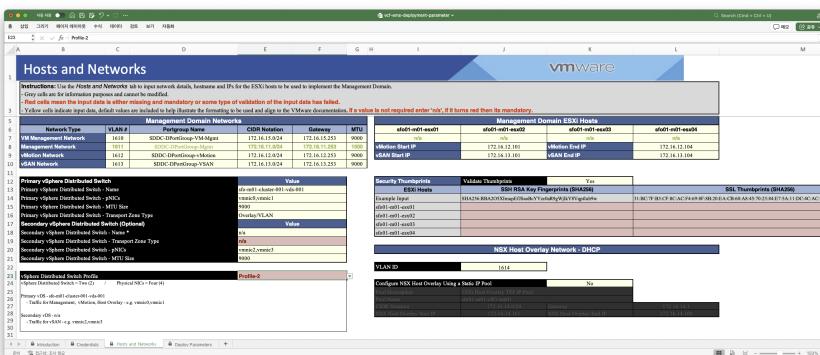


그림 19. Deployment Parameter Workbook 화면

### 3.4.3. 서버 사양 계산

VCF 설계 시에, VMware by Broadcom이 권장하는 하이퍼바이저 호스트별 CPU/MEM 사양의 가이드를 받을 수 있다. Planning and Preparation Workbook에서 모든 설계를 마치면 이를 적용 시의 권장 사양이 Management Domain Sizing Inputs 시트에 '표시'된다.

### 3.4.4. JSON

상기 두 스프레트시트 중 하나를 택일하여 구성 값을 넣으면 JSON 산출 시트에 Cloud Builder에 넣을 수 있는 JSON 스크립트를 작성해 준다. 스프레드시트의 가이드를 그대로 따를 경우, 하이퍼바이저 서버의 하드웨어 구성도 스프레트시트에 따라 설계 및 공급받아야 한다.

```
(-) vcf-ecs-20250116-v2.json x
age > SynologyDrive-ET-Colleague-Broadcom > 2024-05 SDIBD-587 Etevers Cloud Standard > 04 프로덕션 VCF 구축 > (?) vcf-ecs-20250116-v2.json [ ] dvsSpecs
126
127     "dvsSpecs": [
128
129         {
130             "id": "9000",
131             "networks": [
132                 ],
133             "nsxtSwitchConfig": [
134                 {
135                     "transportTypes": [
136                         {
137                             "name": "AZ1-TZ-OVERLAY",
138                             "transportType": "OVERLAY"
139                         },
140                         {
141                             "name": "AZ1-TZ-VLAN-DATA",
142                             "transportType": "VLAN"
143                         }
144                     ]
145                 }
146             ],
147             "clusterSpec": [
148                 {
149                     "clusterName": "CL1",
150                     "clusterRvMode": null,
151                     "clusterImageEnabled": false,
152                     "vmFolders": [
153                         {
154                             "MANAGEMENT": "FD-AZ1-MGMT",
155                             "NETWORKING": "FD-AZ1-NSX",
156                             "EDGENODES": "FD-AZ1-EDGE"
157                         }
158                     ],
159                     "resourcePoolSpecs": [
160                         {
161                             "id": "9000"
162                         }
163                     ]
164                 }
165             ]
166         }
167     ]
168 }
```

그림 20. VCF 설계 JSON

JSON 파일을 직접 트윅할 때는 VMware by Broadcom 정규 문서를 참조하여 작성한다.



VCF 설계 및 검정을 마치지 않고 서버를 발주하면  
사업 이행에 사고가 발생할 수 있다.

EVCS에서는 Deployment Parameter Workbook의 양식을 응용하여 작성한 JSON을 국내 실정에 맞는 네트워크 인터페이스 카드와 VMKernel 구성을 트윅하여 사용한다.

파트너의 VCF 설계를 돋기 위해 추후 GUI 웹 앱 형식의 EVCS-JSON Editor를 제공할 계획이다.

- [1] Broadcom. (2025). VMware Cloud Foundation Architecture. Broadcom Tech Docs Portal. <https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-5-2-and-earlier/5-2/getting-started-with-vcf-5-2/cloud-foundation-architecture.html>
- [2] VTSP - VMware Cloud Foundation 5.1 (2024) for Partners. (2024). Learning@Broadcom. <https://brocade.csod.com>
- [3] VMware by Broadcom. (2025). Planning and Preparation Workbook. Broadcom Tech Docs Portal. <https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-5-2-and-earlier/5-2/planning-and-preparation-workbook-5-2.html>

# Chapter 4. ETVS 클라우드 서비스 용어

EVCS 아키텍처를 통해 구현한 인프라스트럭처는 클라우드 사용자에게 산업 표준에 준하는 공통 용어로 가치를 전달하고자 하였다.

## 4.1. 물리 인프라스트럭처 용어

VCF 솔루션으로 구성 및 구분한 컴퓨트/스토리지 자원의 공통 표현 양식이다.

리전은 별도의 지리적 영역이며, 가용 영역은 리전 내에 있는 여러 격리된 위치이다.<sup>[1]</sup>

### 4.1.1. 지리적 영역

Region 1 = SDDC Management Plane = SDDC Manager

**Multi Region** 구분

- 지역적으로 거리가 있는 컴퓨팅 영역
- 특수 목적으로 제한된 사용 목적이 있는 컴퓨팅 영역

그림 21. Region

격리된 위치라 함은 데이터 센터의 필수 요소 전력/컴퓨트/스토리지/네트워크 등을 독립한 빌딩 블록으로서 동작하도록하여 지리적 영역 내 영향도를 분리하였음을 뜻한다.

Orbrium이 정의하는 가용 영역은 워크로드 도메인 내에서 NSX의 오버레이 네트워크 도메인으로 구분한 영역이다.

### 4.1.2. 가용 영역

Availability Zone 1 = Workload Domain = vCenter & NSX Pair = Overlay Domain 1

**Multi Availability Zone** 구분

- 가용성 확보를 위해 독립된 공간/배전/네트워크 를 구성하는 컴퓨팅 영역

그림 22. Availability Zone

DRS/HA 통해 익숙한 하이퍼바이저 클러스터는 클라우드 인프라스트럭처 관점에서도 여전히 유요한 배치 전략이다.

클러스터는 하드웨어의 구동 체계 등에 따라 하이퍼바이저 팜을 구성할

수 있는 호스트의 묶음이다.

Orbrium이 정의하는 클러스터는 컴퓨터 유형 단위 하이퍼바이저 팜에 NSX 오버레이 네트워크 도메인을 서비스할 수 있는 클러스터다.

#### 4.1.3. 클러스터

Availability Zone 2 = Workload Domain = vCenter & NSX Pair = Overlay Domain 2

Compute Type 1 = Cluster

Compute Type/Version 구분

- 동일 작업 명세가 가능한 영역
- 장비 도입 시기, 도입 환경에 따른 장비간 차이별 묶음

Compute Type 2 = Cluster

그림 23. Cluster

## 4.2. 논리 인프라스트럭처 용어

### 4.2.1. Virtual Private Cloud

Orbirum에서 프로젝트 단위로 할당하는 고유한 사설 네트워크이다.

### 4.2.2. Segment

VPC 내에서 분리된 네트워크 영역으로, IP 주소의 범위를 의미한다.

### 4.2.3. Segment Peering

네트워크가 특정 기능을 담당하는 세그먼트로 나뉘어 관리될 때, 이러한 두 세그먼트 간의 연결을 Segment Peering이라고 한다. 하나의 VPC 내부의 세그먼트 간 연결뿐만 아니라, 서로 다른 VPC 간의 연결도 포함한다.

### 4.2.4. Access IP

Access IP는 VPC 바깥과 통신하기 위해 VM에 부여하는 NAT 아이피이다.

Access IP는 용도와 목적에 따라 사설/공인 유형 모두가 될 수 있다. 제공하는 Access IP의 유형은 BGP를 통해 NSX Edge Cluster에 연결하는 영역 나름이다.

### 4.2.5. Block Disk

vSAN의 iSCSI target 기능을 사용하여 디스크를 마운트하여 사용하는 기능이다. VM에 Block Disk를 연결하여 저장 장치(HDD, SSD)처럼 사용하는 기능을 뜻한다.

#### **4.2.6. 프로젝트**

Virtual Machine, VPC, 스토리지 등의 리소스를 프로젝트라는 하나의 그룹 단위로 관리할 수 있도록 제공한다. 용도에 맞춰 프로젝트를 생성하고 관리한다.

#### **4.2.7. DBaaS**

별도의 하드웨어 또는 소프트웨어 설치 구성 없이 데이터베이스를 서비스 형식으로 제공하는 서비스이다. Orbrium에서는 VMWare Data Services Manager를 통해 데이터베이스를 생성할 수 있도록 제공한다. Data Services Manager에서는 오픈소스 데이터베이스인 PostgreSQL과 MySQL를 지원한다.

[1] 리전 및 영역. (n.d.). Amazon Elastic Compute Cloud 사용자 가이드.  
[https://docs.aws.amazon.com/ko\\_kr/AWSEC2/latest/UserGuide/using-regions-availability-zones.html](https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/using-regions-availability-zones.html)

# 부록 A: 클라우드 빌드

VCF를 배포하기 위해서는 전용 소프트웨어 어플라이언스인 Cloud Builder에 작업서를 업로드하여 검정을 진행하고 반드시 통과해야한다.

클라우드 빌드를 활용한 배포 과정은 전체 과정 중 일부이다.

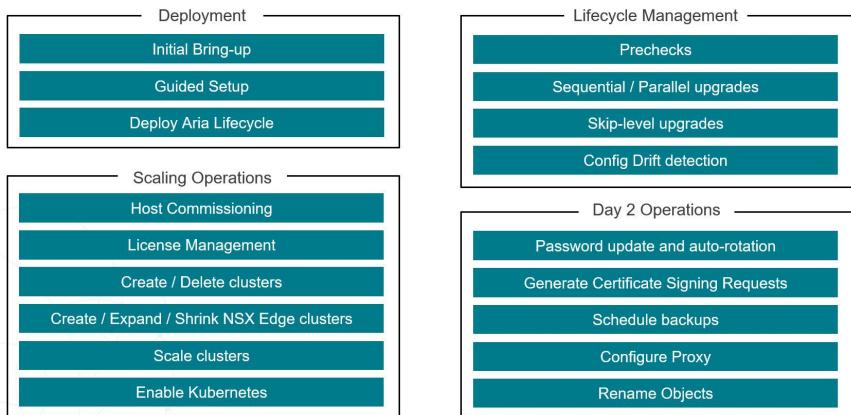


그림 24. VCF 배포 작업흐름.<sup>[1]</sup>

해 부록은 Deployment Parameter WorkbookDeployment Parameter Workbook을 기준으로 하였다.

## A.1. Cloud Builder

Cloud Builder Appliance (Cloud Builder) 통해 VCF 5.2 솔루션을 구현한다. Cloud Builder는 VCF의 첫 번째 클러스터를 만들고 SDDC Manager가 통제하는 VMware 솔루션을 배포할 때 쓰인다. 이후에는 쓰지 않는다.

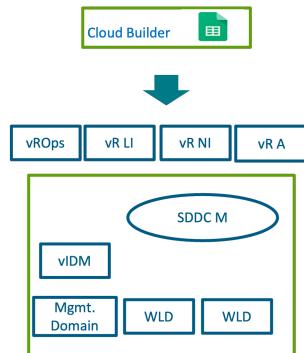


그림 25. VCF Deployment in VCF 5.2

▶ [videos/Dc6xygJDzjs.mp4](#) (video)

Cloud Builder Appliance 배포 예

클라우드 서비스 인프라스트럭처의 설계 중 동서 트래픽 각 오버레이 네트워크는 Cloud Builder에 쓰이지 않는다. VCF 배포 작업이 완료된 후 SDDC Manager에서 추가 작업을 진행한다.



4.3. 에서 언급한 명명 규칙에 따라 모든 객체의 이름을 지정하였다.

### A.1.1. Management Domain Networks

Management Domain Networks					
Network Type	VLAN #	Portgroup Name	CIDR Notation	Gateway	MTU
VM Management Network	1001	MGMT-SYS	172.21.1.0/24	172.21.1.1	9000
Management Network	1011	MGMT-VIRT-AZ1	172.21.11.0/24	172.21.11.1	1500
vMotion Network	1012	DATA-FUNC-AZ1	172.21.12.0/24	172.21.12.1	9000
vSAN Network	1013	DATA-VSAN-AZ1	172.21.13.0/24	172.21.13.1	9000

## A.1.2. Management Domain ESXi Hosts

Management Domain ESXi Hosts			
esxi1-cl1-az1	esxi2-cl1-az1	esxi3-cl1-az1	esxi4-cl1-az1
172.21.11.11	172.21.11.12	172.21.11.13	172.21.11.14
vMotion Start IP	172.21.12.11	vMotion End IP	172.21.12.99
vSAN Start IP	172.21.13.11	vSAN End IP	172.21.13.99

Security Thumbprints	Validate Thumbprints	No	SSL Thumbprints (SHA256)
ESXi Hosts	SSH RSA Key Fingerprints (SHA256)		
Sample Input	SHA256:BBAD01XmugE73BwBYY6e@9yWjA1YVgqslbw		E1:BC:7E:13:C1:BC:AC:19:49:8F:3D:3D:FA:CB:6B:AF:45:70:23:88:17:5A:11:1K:4C:9C:94:AD:23:FF:10:7A
esxi1-cl1-az1			
esxi2-cl1-az1			
esxi3-cl1-az1			
esxi4-cl1-az1			

Validate Thumbprints 값을 Yes로 선택할 경우, ESXi 호스트의 SSH 팽거프린트와 SSL Thumbprints를 사전 검증하는 보안 기능이 활성화된다.

Cloud Builer에 SSH로 접근하여 호스트의 Thumbprints를 확인하여 값을 넣어준다.

No를 선택할 경우, 위의 과정을 진행하지 않고 배포된다.

## A.1.3. vSphere Distributed Switch Profile

Primary vSphere Distributed Switch	Value
Primary vSphere Distributed Switch - Name	VDS-MGMT
Primary vSphere Distributed Switch - pNICs	vmnic5,vmnic4
Primary vSphere Distributed Switch - MTU Size	9000
Primary vSphere Distributed Switch - Transport Zone Type	VLAN
Secondary vSphere Distributed Switch (Optional)	Value
Secondary vSphere Distributed Switch - Name *	VDS-DATA
Secondary vSphere Distributed Switch - Transport Zone Type	Overlay/VLAN
Secondary vSphere Distributed Switch - pNICs	vmnic1,vmnic0
Secondary vSphere Distributed Switch - MTU Size	9000

vSphere Distributed Switch Profile	Profile-3
vSphere Distributed Switch = Two (2) / Physical NICs = Four (4)	
Primary vDS - VDS-MGMT - Traffic for Management, vMotion, vSAN - e.g. vmnic5,vmnic4	
Secondary vDS - VDS-DATA - Traffic for Host Overlay - e.g. vmnic1,vmnic0	

vSphere Distributed Switch Profile은 1~3번을 선택할 수 있다.

Profile-1의 경우, 하나의 vDS를 통해 관리, vMotion, vSAN, Host Overlay 네트워크를 선언한다.

Profile-2, Profile-3의 경우, 2개의 vDS를 사용하는 것은 동일하나 기본 vDS와 보조 vDS의 역할이 다르다.

Profile-2의 기본 vDS는 관리, vMotion, Host Overlay 네트워크를 선언하고, 보조 vDS는 vSAN 네트워크를 선언한다. Profile-3의 기본 vDS는 관리, vMotion, vSAN 네트워크를 선언하고, 보조 vDS는 Host Overlay 네트워크를 선언한다.



Deployment Parameter Workbook 스프레드시트는 두 개의 vDS만 선언할 수 있다. 용도 별 세분화를 위해 추가 vDS가 필요하다면 최종 과정에서 JSON 커스터마이즈 작업을 수행한다.

#### A.1.4. NSX Host Overlay Network - Static IP Pool in NSX

NSX Host Overlay Network - Static IP Pool in NSX					
VLAN ID	1014				
Configure NSX Host Overlay Using a Static IP Pool		Yes			
Pool Description	ESXi Host Overlay TEP IP Pool				
Pool Name	VTEP-IP-POOL-AZ1				
CIDR Notation	172.21.14.0/24	Gateway	172.21.14.1		
NSX Host Overlay Start IP	172.21.14.11	NSX Host Overlay End IP	172.21.14.99		

#### A.1.5. Existing Infrastructure Details

Infrastructure	Value
DNS Server #1	172.21.1.2
DNS Server #2	172.21.1.3
NTP Server #1	172.21.1.2
NTP Server #2	172.21.1.3

DNS Zone	Value
DNS Zone Name	sys.sdi

Enable Customer Experience Improvement Program (“CEIP”)	No
Enable FIPS Security Mode on SDDC Manager	No

FIPS Security Mode의 경우, 미국 공공기관에서 요구되는 보안

규정이므로 한국에서는 사용하지 않는다.

### A.1.6. License Keys

License Now	No
ESXi	
vSAN	
vCenter Server	
NSX	

라이선스란을 비워두면, Cloud Builder에서 제공하는 임시 라이선스가 자동으로 들어가므로 최초 배포 시 필수 사항은 아니다. 배포 후, 별도로 기입해도 문제가 발생하지 않는다.

### A.1.7. vSphere Infrastructure

	Hostname	IP Address
vCenter Server Hostname and IP Address	vcsal-az1	172.21.1.11
<b>vCenter Server Appliance Size (Default Small)</b>	large	
<b>vCenter Server Appliance Storage Size</b>	default	

vCenter Server Appliance Size의 경우, 사용자 환경에 따라서 VMware에서 요구하는 기준에 맞추어 선택한다. (공식 문서 참고)  
<https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/vcenter-server-installation-and-setup-8-0/deploying-the-vcenter-server-appliance/vcenter-server-appliance-requirements.html>

	Value
vCenter Datacenter and Cluster	
Datacenter Name	AZ1
Cluster Name	CL1
Enable vLCM Cluster Image	No
Cluster EVC Setting	n/a

	Value
<b>vSphere Datastore</b>	
vSAN Datastore Name	DS-VSAN
Enable vSAN Deduplication and Compression	No
Enable vSAN-ESA	No
Path to HCL JSON File	n/a

vLCM 클러스터 이미지 관리 방식을 선택하지 않을 시

1. Baseline Profile 패치만 가능하며 vLCM 클러스터 이미지 관리 전환 불가능
2. vSAN ESA 배포 불가능

Select the VCF Architecture to be deployed:	Value
vSphere Resource Pools	RP-SDDC-MGMT
Resource Pool SDDC Management	RP-USER-EDGE
Resource Pool User Edge	RP-USER-VM
Resource Pool User VM	

VCF Architecture deploy 타입을 Standard로 선택 시, 관리 도메인과 워크로드 도메인을 물리적으로 분리하여 각각 별도의 클러스터를 사용한다.

Consolidated로 선택 시, 관리 도메인과 워크로드 도메인을 하나의 클러스터, 그리고 하나의 vCenter에서 함께 운영한다.

## A.1.8. NSX

NSX Management Cluster	Hostname	IP Address
NSX Management Cluster VIP	nsx-az1	172.21.1.15
NSX Virtual Appliance Node #1	nsx1-az1	172.21.1.16
NSX Virtual Appliance Node #2	nsx2-az1	172.21.1.17
NSX Virtual Appliance Node #3	nsx3-az1	172.21.1.18
NSX Virtual Appliance Size (Default Medium)	medium	

## A.1.9. SDDC Manager

SDDC Manager	Value
SDDC Manager Hostname	sddc
SDDC Manager IP Address	172.21.1.19
Network Pool Name	ECS
Cloud Foundation Management Domain Name	AZ1

### A.1.10. JSON 커스터마이즈

Workbook에서 선택한 옵션을 커스터마이즈하여 사용해야 할 때가 있다. 너무 간이하거나, 너무 정밀한 workbook

Cloud Builder에 workbook을 업로드한 후에, SSH로 접속하여 추출해 만들어진 JSON 파일을 다운로드하여 편집한다.

편집을 마친 후에는 Cloud Builder에 JSON 파일을 업로드한다.

## A.2. VCF Installer

VCF 9 릴리스 시에 VCF Installer가 Cloud Builder를 대체할 것으로 알려져 있다. [2] EVCS 5.2는 다루지 않는다.

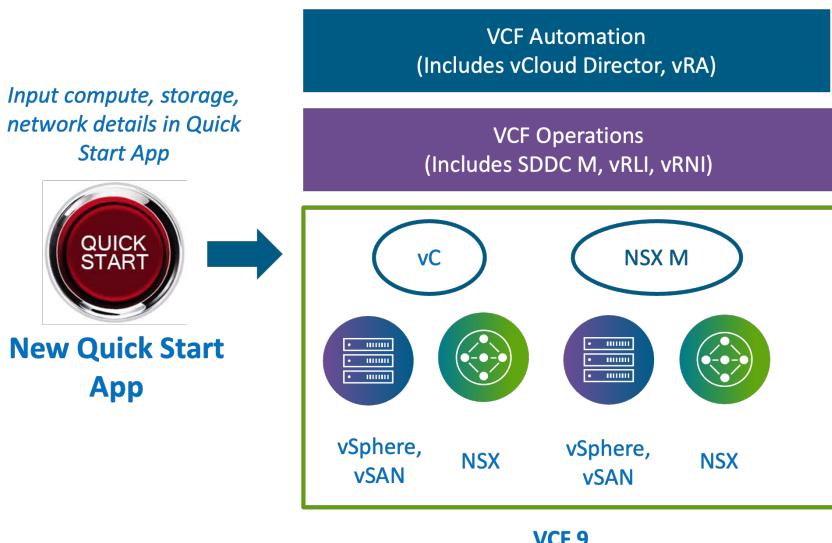


그림 26. VCF Deployment in VCF 9

▶ [videos/H0mz4JM6nk4.mp4](#) (video)

VCF Installer 시연 영상

- [1] VTSP - VMware Cloud Foundation 5.1 (2024) for Partners. (2024). Learning@Broadcom. <https://brocade.csod.com>
- [2] Shimkhada, R. (2024). Simplified Lifecycle Management for VMware Cloud Foundation and VMware vSphere. VMware. <https://www.vmware.com/explore/video-library/video/6360758785112>

# 부록 B: BVP Deploy & Manage

- ▶ [videos/nqDJu\\_5mIX4.mp4](#) (video)

EVCS with VCF Automation Settings

- ▶ [videos/Y7Wm50\\_oJ7w.mp4](#) (video)

BVP Installation

- ▶ [videos/oBICro6ZZHM.mp4](#) (video)

VMware Identity Manager Settings

# 부록 C: Orbrium Installation

▶ [videos/MXcu-ZJCQw8.mp4](#) (video)

Orbrium Installation

# 참고 문헌

박하림, & 김태호. (2021). 클라우드워크로드보호 핸드북: Carbon Black Cloud. 넷스피어퍼블리셔. <https://play.google.com/store/books/details?id=34QxEAAAQBAJ>

Amazon Elastic Compute Cloud 사용자 가이드. (2025). Amazon Web Services. [https://docs.aws.amazon.com/ko\\_kr/AWSEC2/latest/UserGuide/using-regions-availability-zones.html](https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/using-regions-availability-zones.html)

VMware Cloud Foundation (5.2). (2025). Broadcom Tech Docs Portal. <https://techdocs.broadcom.com/content/dam/broadcom/techdocs/us/en/pdf/vmware/vcf/vcf-52/vmware-cloud-foundation-5-2-and-earlier-5-2.pdf>

VMware Validated Solutions (1.0). (2025). Broadcom Tech Docs Portal. <https://techdocs.broadcom.com/content/dam/broadcom/techdocs/us/en/pdf/vmware/vcf/vvs/vmware-validated-solutions-1-0.pdf>

VMware Cloud Foundation as a Service. (2025). IBM Cloud. <https://cloud.ibm.com/media/docs/pdf/vmware-service/nl/ko/vmware-service.pdf>

New GTLD Collision Occurrence Management Proposal. (2013). ICANN. <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-1-07oct13-en.pdf>

VTSP - VMware Cloud Foundation 5.1 (2024) for Partners. (2024). Learning@Broadcom. <https://brocade.csod.com>

클라우드 컴퓨팅 이해. (2023). Red Hat. <https://www.redhat.com/ko/topics/cloud-computing>

<https://www.redhat.com/ko/topics/cloud-computing>