VMUG

user/con

the Netherlands

Automated Multi-Pod Micro-Segmentation with NSX

Who we are?

Toine Eetgerink

- Cloud Architect
- ITQ
- CMA/NSX/vSphere
- vconnectme.com
- @toine_eetgerink

Sam Vieillard

- Software engineer
- ITQ
- C#/TypeScript/CI/CD
- codevieillard.com
- @codevieillard

Krastin Krastev

- Network Guru
- ITQ
- NSX/Cisco
- @krasteff

Question for the audience

Can you automate micro segmentation over multiple sites?

Why?

To enable DevOps teams

NGINX

RabbitMQ

PHOTON™

Microsoft® SQL Server®

redis

Deliver secure networks

DevOps Team

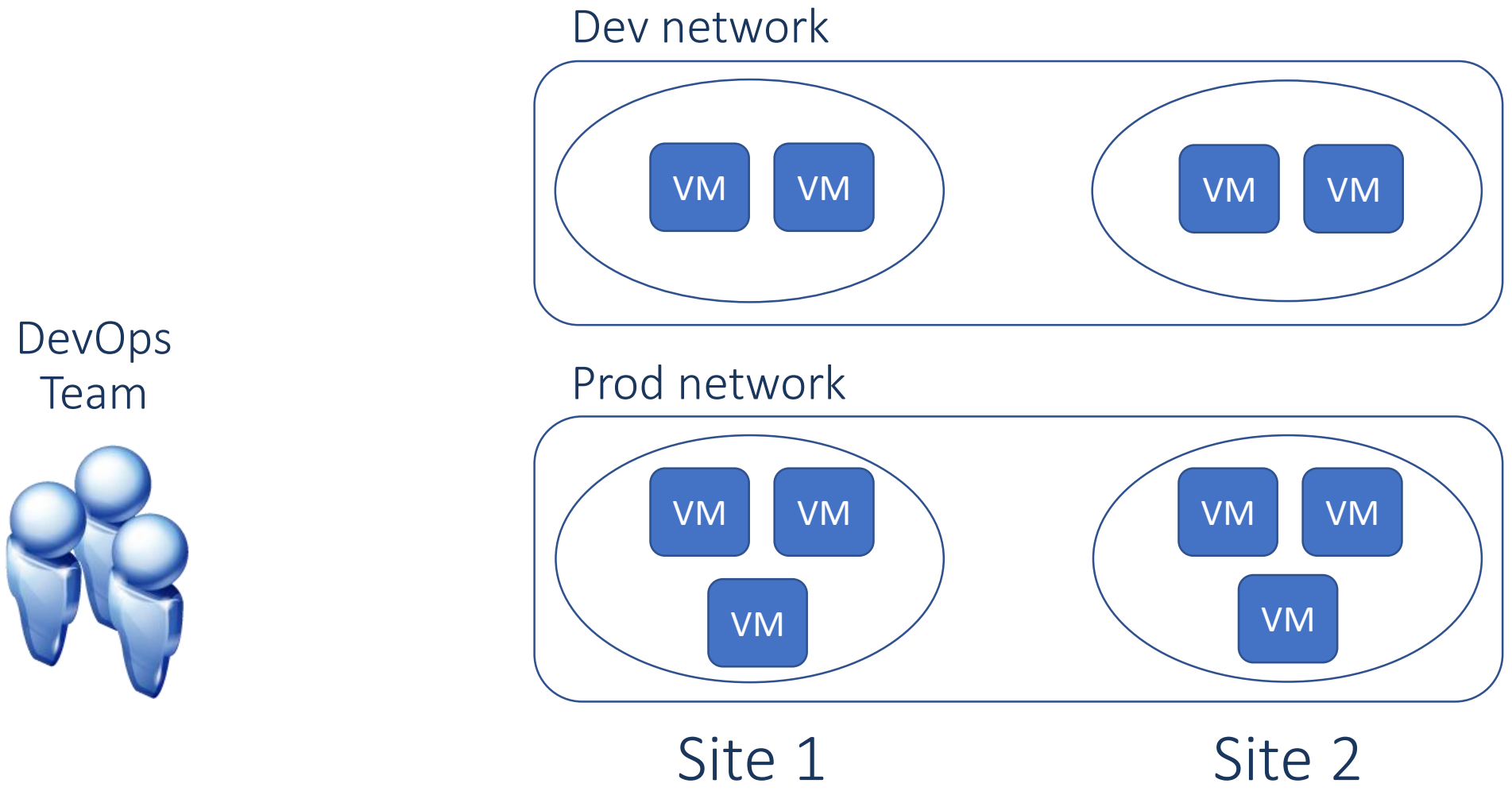
FISMA COMPLIANCE

PCI DSS COMPLIANT

HIPAA
Health Insurance Portability and Accountability Act

ISO International Organization for Standardization

Offer self-service capabilities



But what about?

Increasing the capacity within a datacenter?

Introducing a new datacenter?

Automation should be able to expand

Consume new resources as deployment target

The design

Design a scalable solution

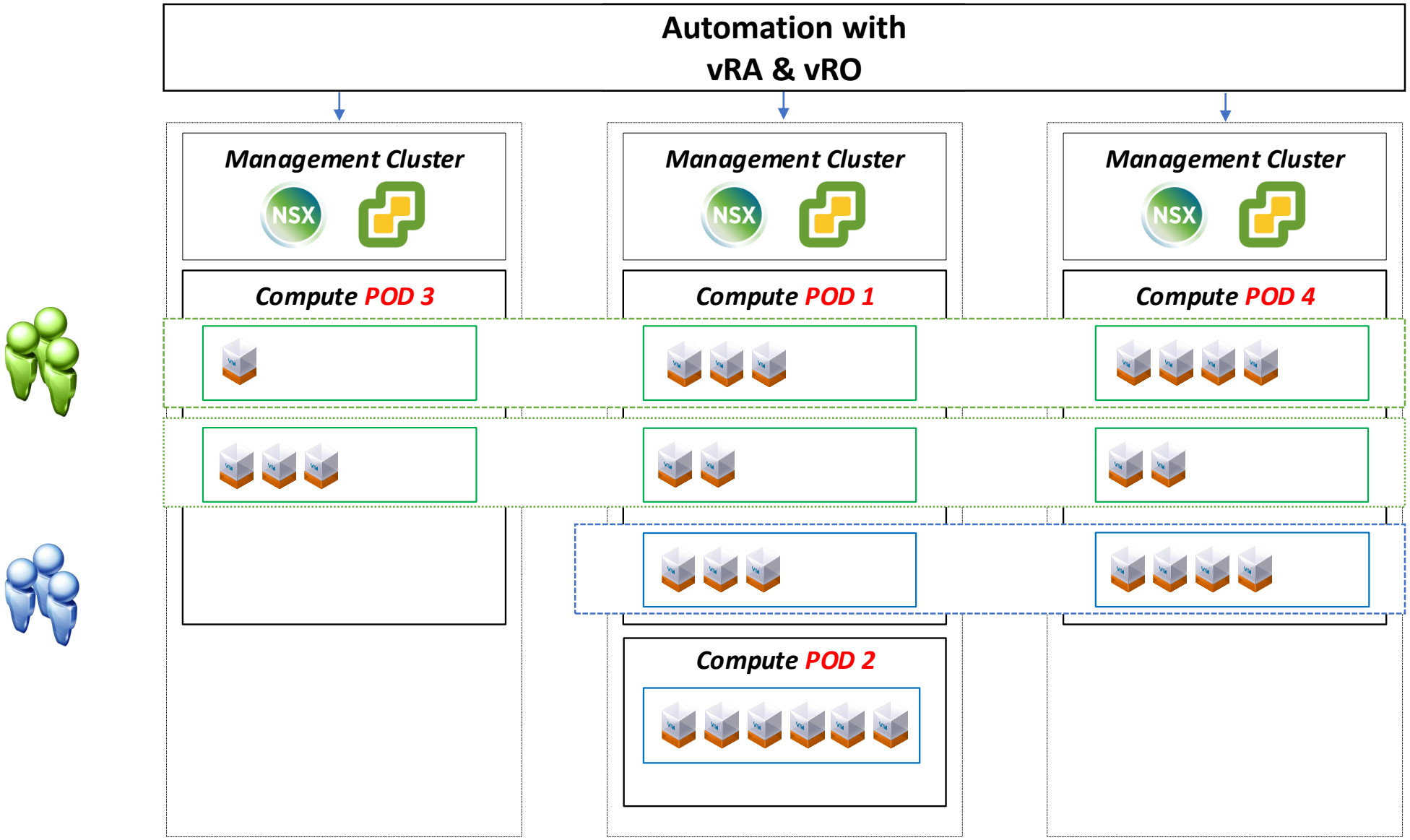
Combine available software systems

Implement consistent configuration over systems

Implement pod design

What does it look like?

What is a Pod and how do we define a pod?


Automation with
vRA & vRO
Management Cluster
NSX
Management Cluster
NSX
Management Cluster
NSX
Compute POD 3
Compute POD 1
Compute POD 4
Compute POD 2

What do we do with NSX?

Automation with vRA & vRO

Management Cluster

NSX

IPSet_UUID

SG_UUID

ST_UUID

Management Cluster

NSX

IPSet_UUID

SG_UUID

ST_UUID

LS_UUID_n

SG_UUID

IPSet_UUID

ST_UUID

LS_UUID_n

Management Cluster

NSX

IPSet_UUID

SG_UUID

ST_UUID

LS_UUID_n

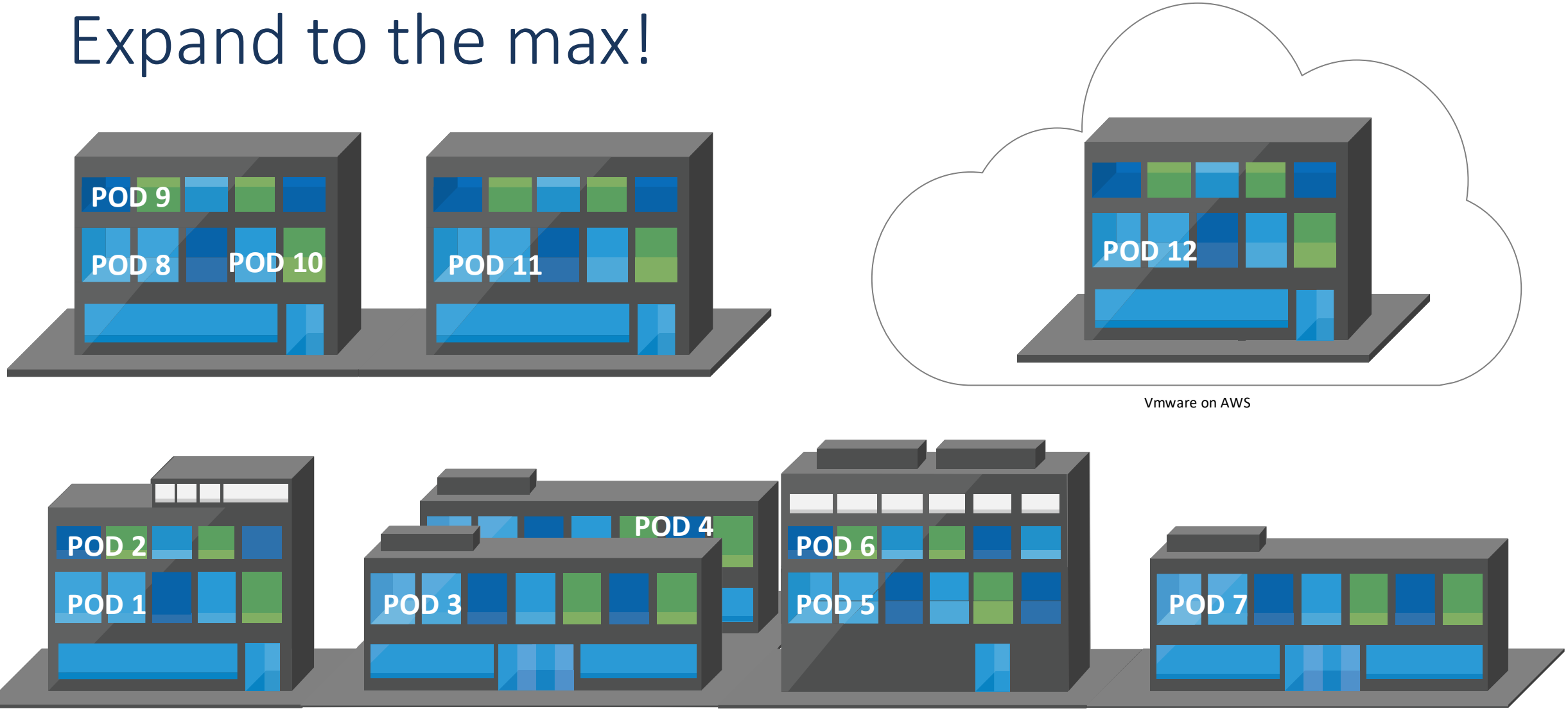
LS_UUID_n

SG_UUID

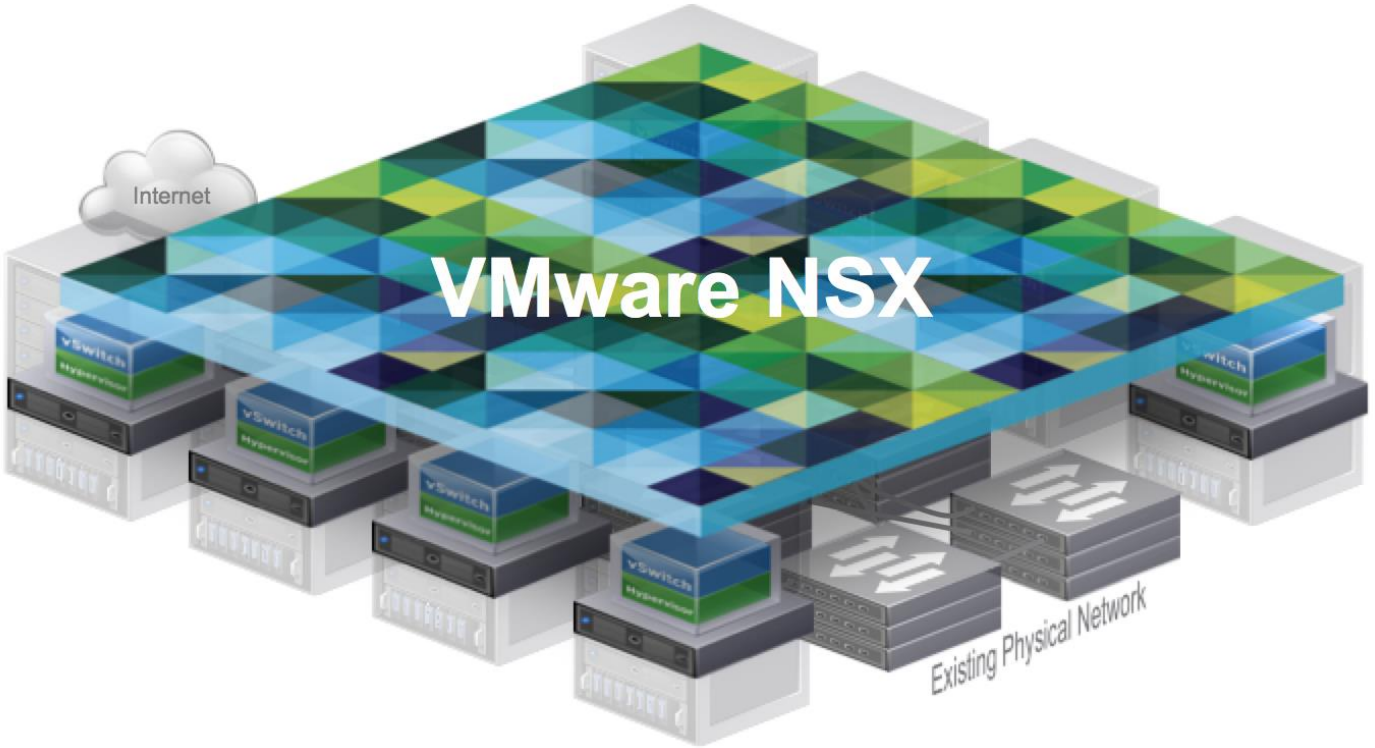
IPSet_UUID

ST_UUID

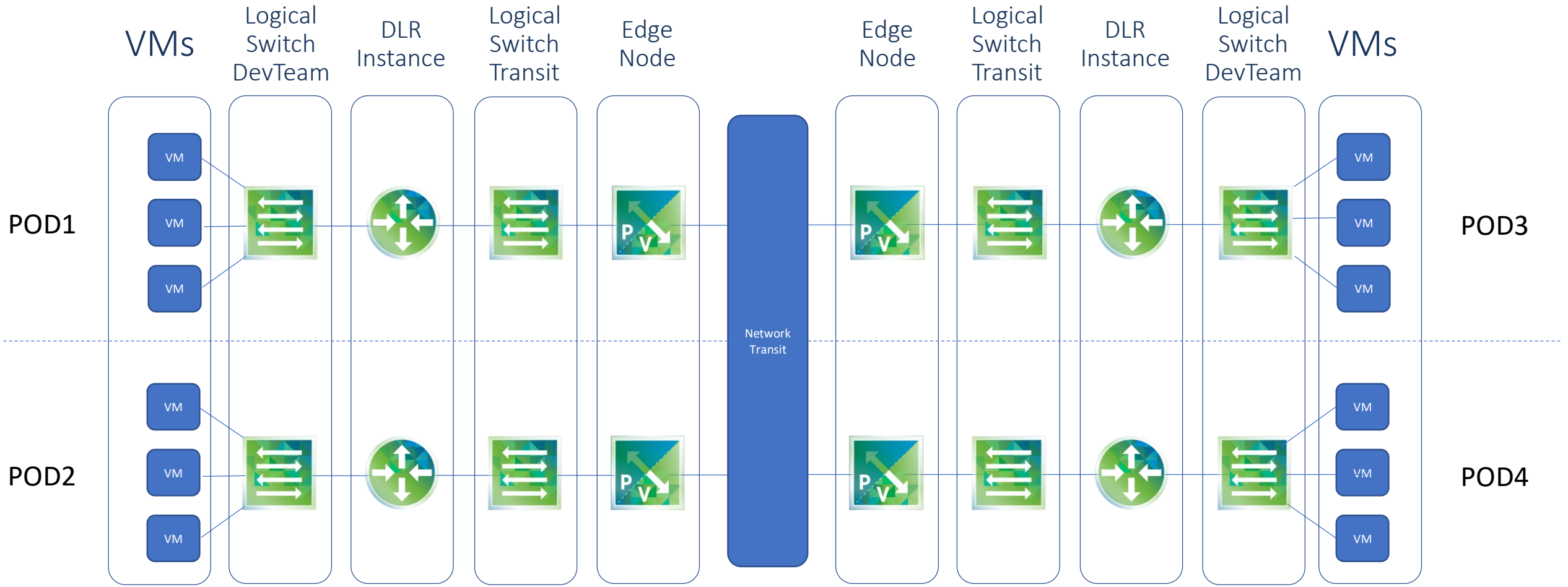
Expand to the max!



Traffic flow patterns in NSX



Cross-POD Network Path



And what about securing network traffic?

Traffic and Security

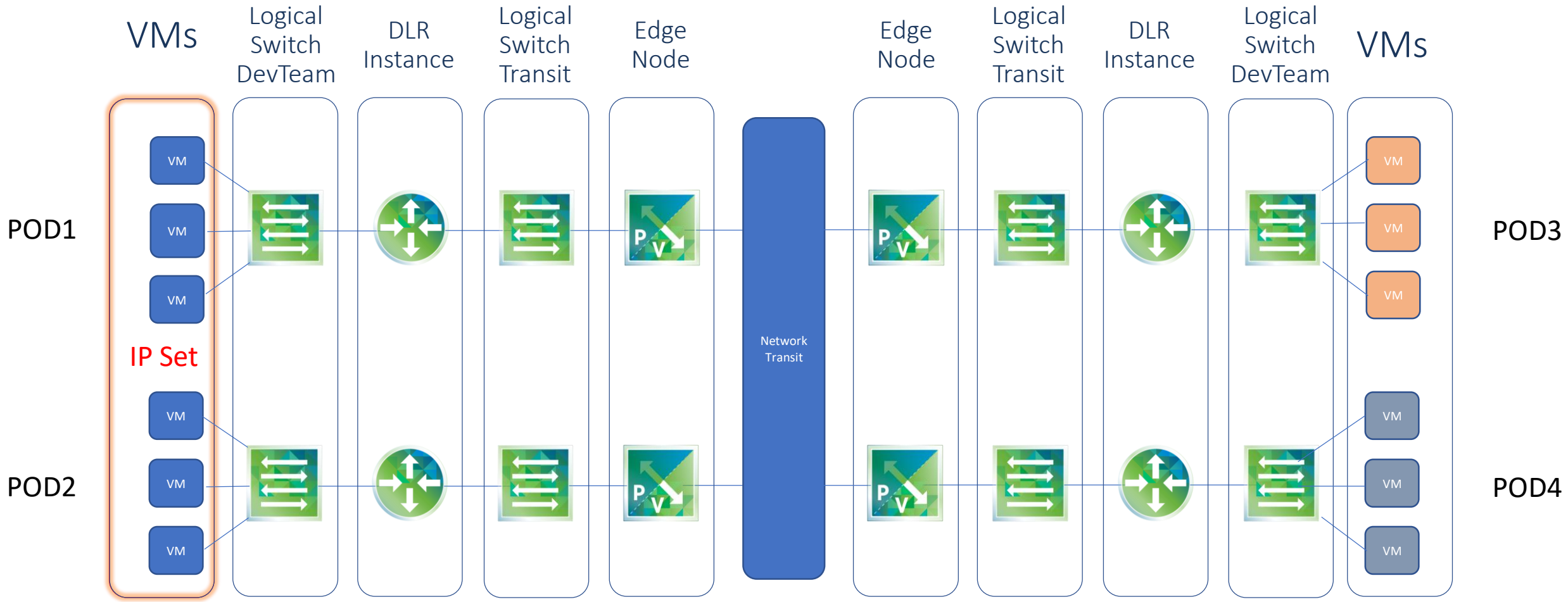
Firewall automation

All traffic local to the security group is allowed to flow through

Third Party integration possibilities

Source	Destionation	Protocol/Port	Action
ANY	SG_<UUID>	TCP/80	ALLOW
SG_<UUID>	ANY	TCP/3306	ALLOW
ANY	SG_<UUID>	ANY	DENT

Traffic and Security – Micro-segmentation perimeter



How do we automate this?

vRealize Automation for 1st and 2nd day operations

vRealize Orchestrator for customization and extensibility features

But we are implementing automation at scale

This requires a lot of custom coding

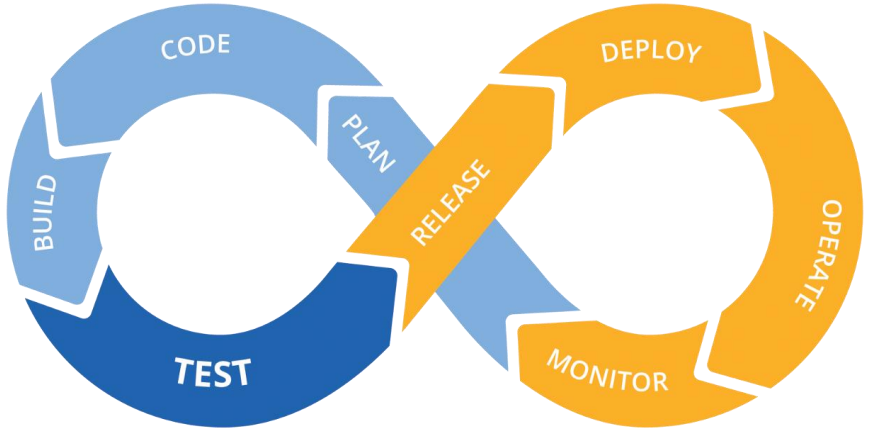
So?

Apply software development methodologies

Develop in an Integrated Development Environment

Version Control Software that scales to big teams

Leverage Continuous Integration and Continuous Delivery principles



Summarize principles

Continuous Integration

- Integrate small changes often
- Trigger builds on each release
- Automated testing

Continuous Delivery

- Release on business demand
- Automated release steps
- Rapid deployment

Right tool for the job

Move from scripting to programming

Complex projects require mature tooling

Integrate with proven technology

Use development Tools

vRealize DevTools

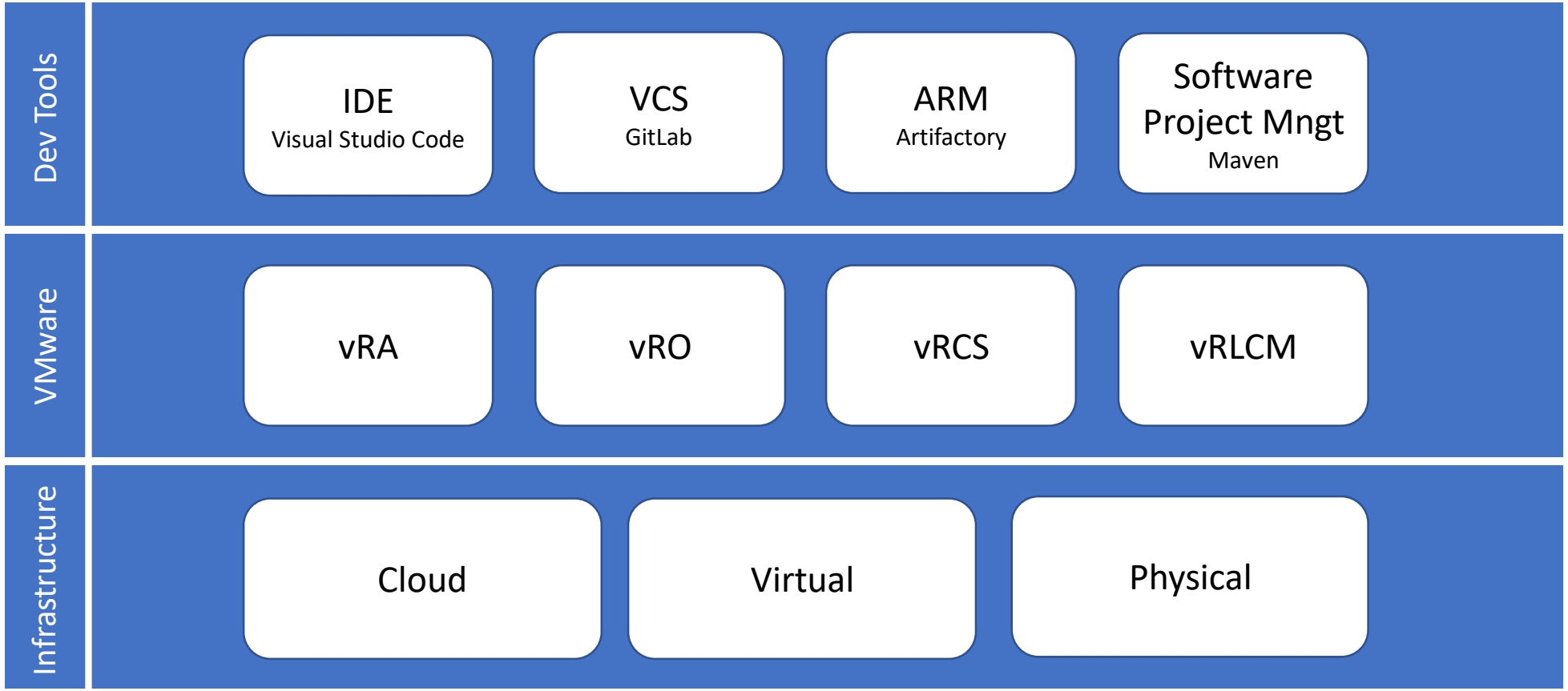
Utilizes TypeScript – a superset of JavaScript

Comes with unit-testing framework

Artifact and dependency management

Semantic versioning on packages

The big picture



Demo time!

Questions?

Thank you

VMUG user/con