
Cloud-Native Contrail Networking (CN2) General Presentation
Juniper Networks
2022/07
Juniper Networks
Driven by Experience™

CONFIDENTIALITY AND LEGAL NOTICE

This material contains information that is confidential and proprietary to Juniper Networks, Inc. Recipient may not distribute, copy, or repeat information in the document.

This statement of product direction sets forth Juniper Networks' current intention and is subject to change at any time without notice. No purchases are contingent upon Juniper Networks delivering any feature or functionality depicted in this presentation.

subject to a license agreement that describes program terms and conditions.

最新の状況などは公式のマニュアルをご確認ください。
また、内容は予告なしに変更になる場合があります。

技術詳細は公式ドキュメントを参照ください。
https://www.juniper.net/documentation/product/us/en/cloud-native-contrail-networking

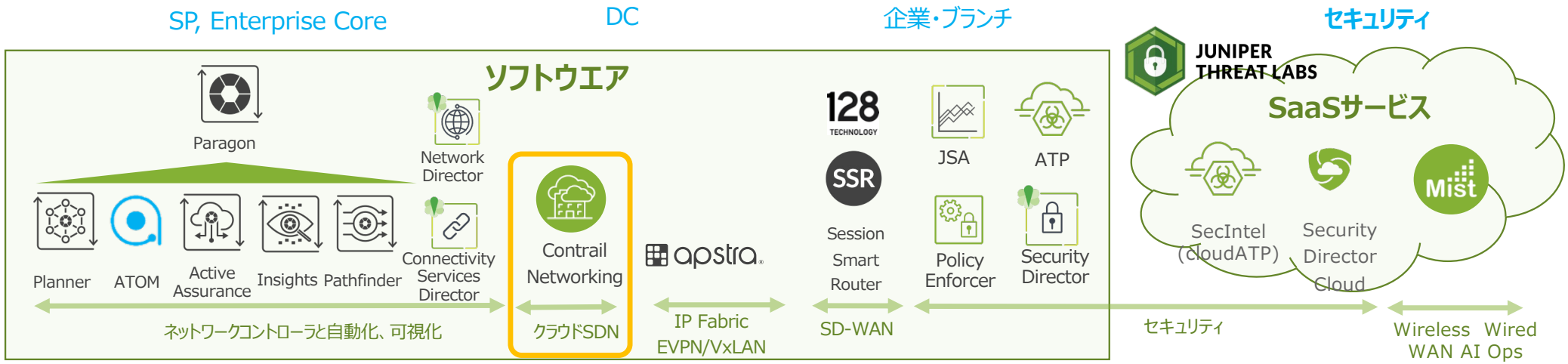
Agenda

- 製品ポートフォリオとSDN
- Kubernetesによるマイクロサービス
- Contrailについて
- 各種機能紹介 (Feature list)
- ユースケース
- 必要スペックやライセンス

Agenda

- 製品ポートフォリオとSDN
- Kubernetesによるマイクロサービス
- Contrailについて
- 各種機能紹介 (Feature list)
- ユースケース
- 必要スペックやライセンス

製品ポートフォリオ



Junos Evolved (vMX, vSRX, cSRX, cRPD)

ルーター

MXシリーズ　PTXシリーズ　ACXシリーズ

スイッチ

QFXシリーズ　EXシリーズ

Wi-Fi

MISTシリーズ

アプライアンス他

Junos Space

NFXシリーズ

セキュリティ

SRXシリーズ

TDD

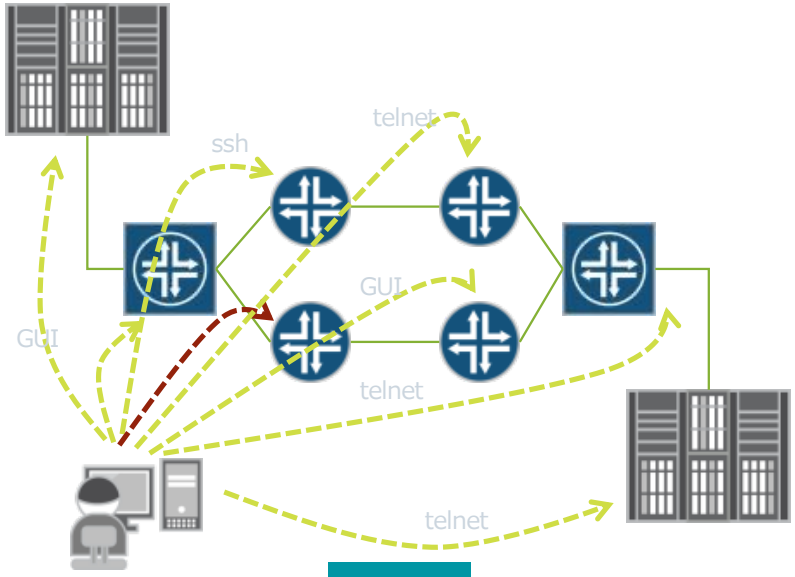
JSA

JATP

プロフェッショナルサービス（コンサルティング、設計、検証、導入）/ **アドバンスドサービス**（運用支援）

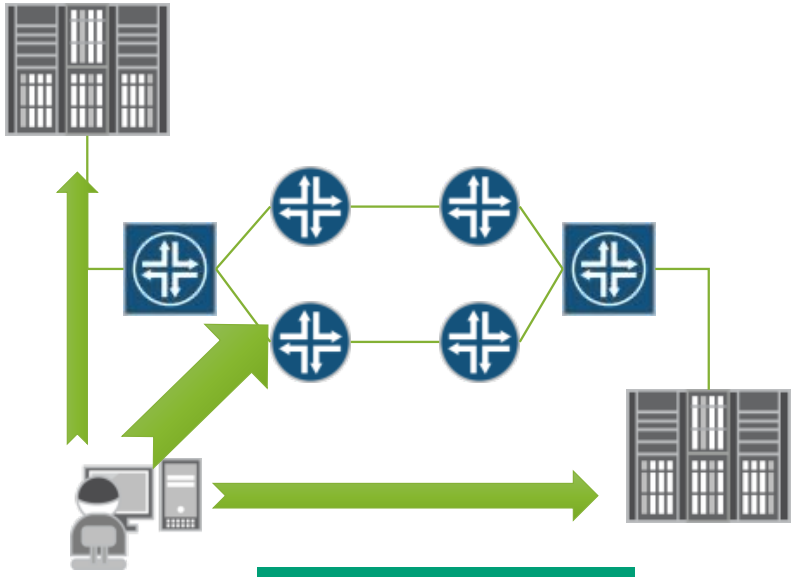
SDN (Software Defined Networking)

ネットワークの構成や機能の設定をソフトウェアによってプログラマブルに行い(Software Defined)、サーバーやストレージ、バーチャルマシン、バーチャルネットワークとの連携(Networking)を行う仕組み



従来

新規/ 追加等の作業で，個々の機器に対するアップデートが必要.



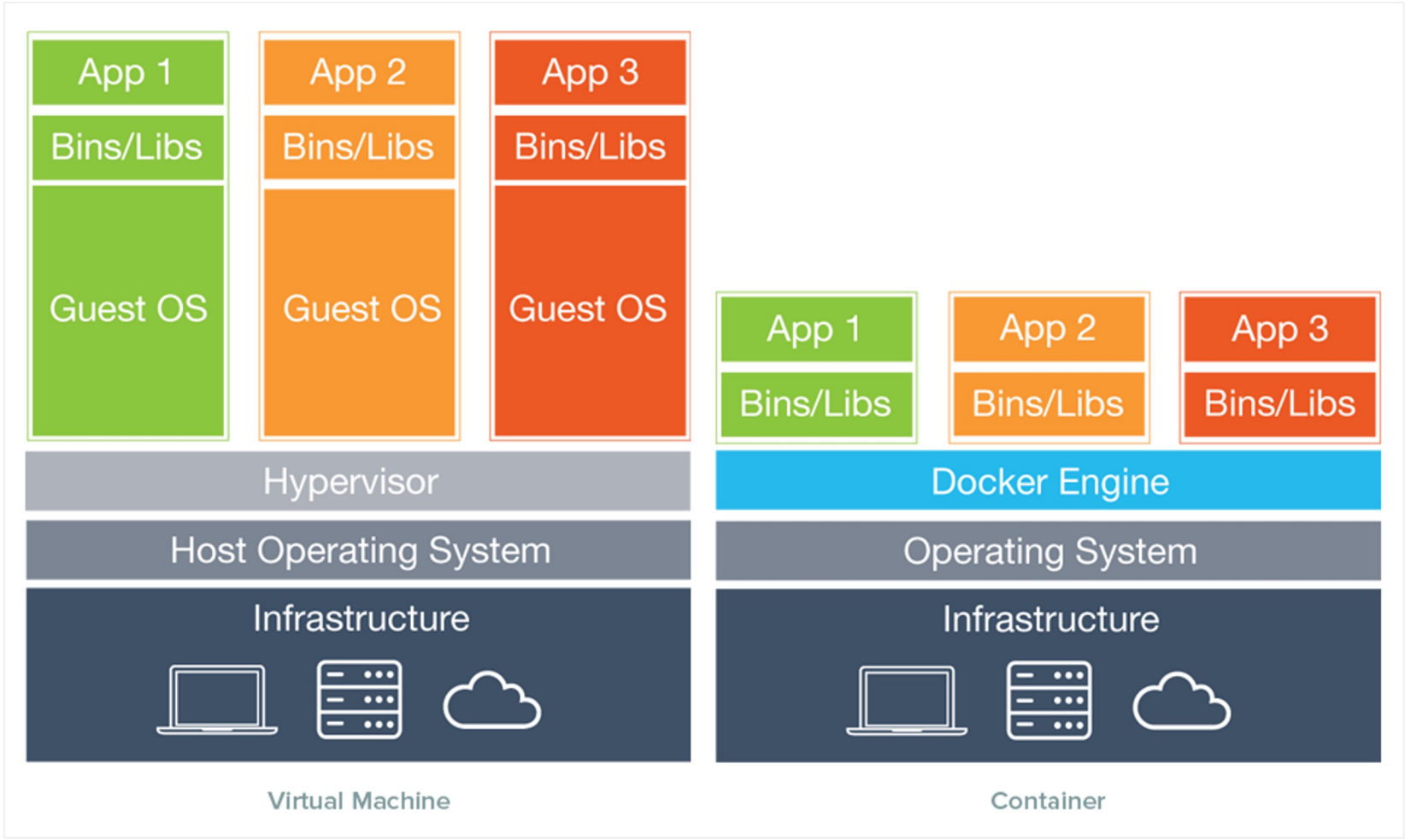
SDNになると…

一回の指示で，サーバからネットワーク全ての関連する内容が更新される.

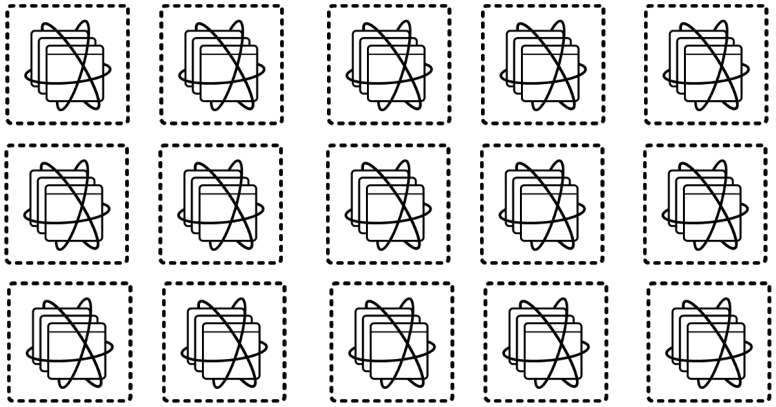
Agenda

- 製品ポートフォリオとSDN
- Kubernetesによるマイクロサービス
- Contrailについて
- 各種機能紹介 (Feature list)
- ユースケース
- 必要スペックやライセンス

CONTAINER OVERVIEW



CONTAINER ORCHESTRATION



CONTAINERIZED APPLICATIONS

kubernetes

MANAGE CONTAINERS SECURELY

MANAGE CONTAINERS AT SCALE

INTEGRATE IT OPERATIONS

ENABLE HYBRID CLOUD

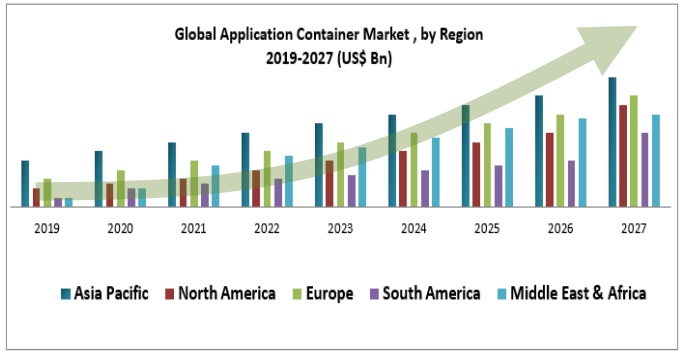
ITデプロイモデルの変化とコンテナ利用の増加

By 2026

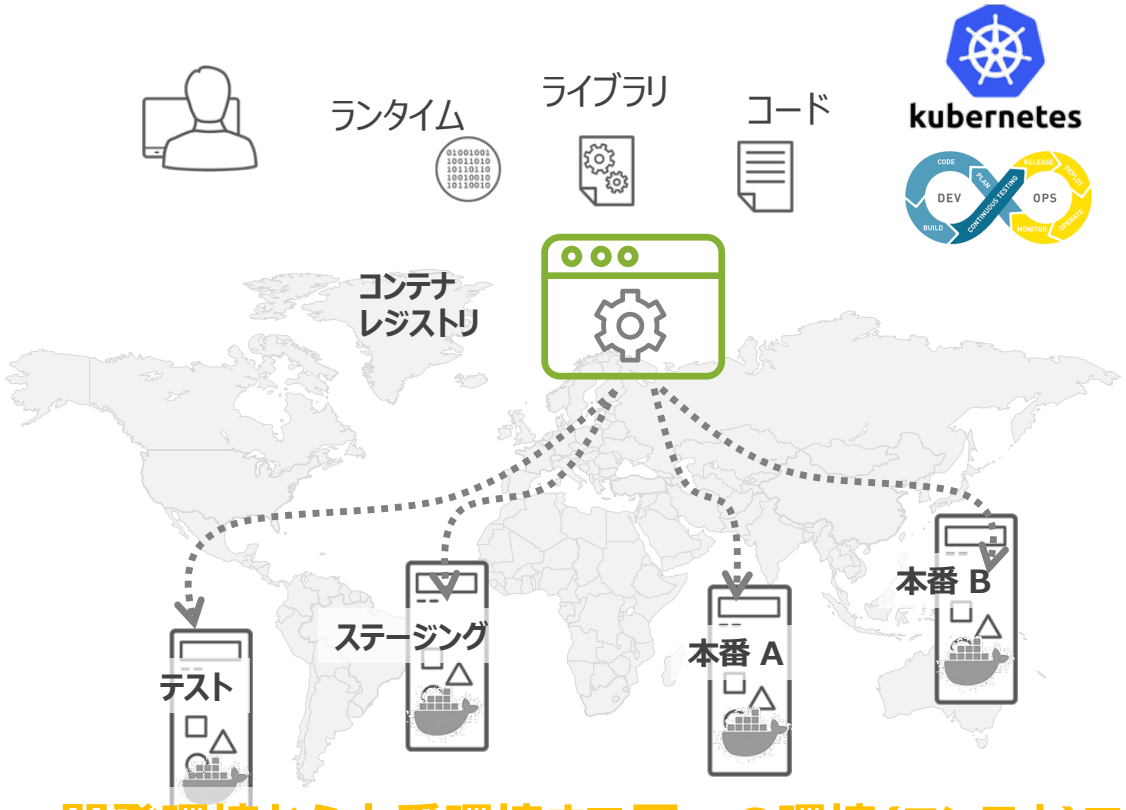
90 %

global organizations will be running containerized applications in production

** Source: Gartner*



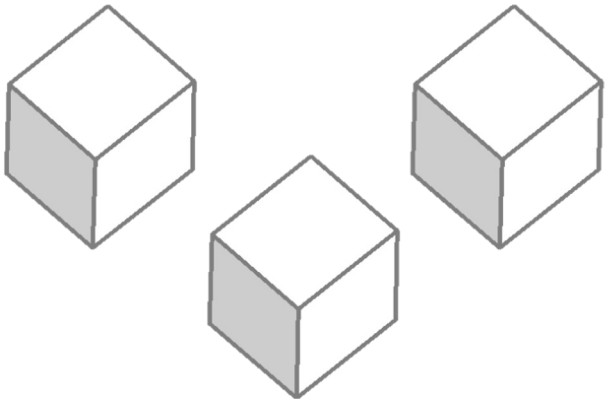
** Source: MMR*



開発環境から本番環境まで同一の環境(コンテナ)で
＊即座に＊ ＊どこでも＊ 利用するのが可能に。

MIND THE GAP

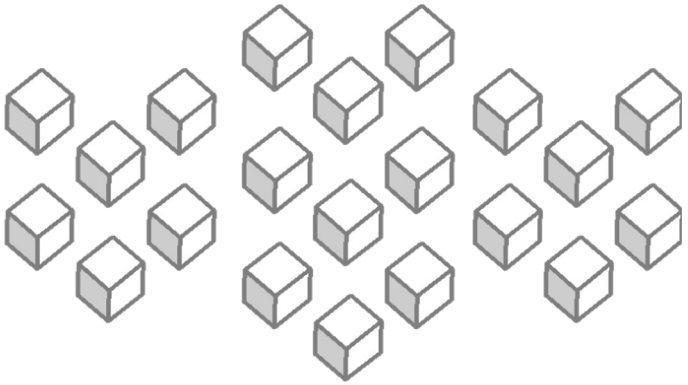
monolithic architecture
few interconnections



APIs talk a little

microservices means more NETWORK

microservices
many interconnections



APIs talk a lot… network becomes more important

KUBERNETES REACHES BEYOND CLOUD-NATIVE

Traditional Stack

Containers

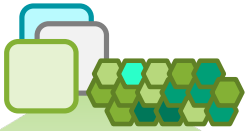
Optional VMs

Metal, private IaaS or public IaaS

Kubernetes is eating the Cloud!

Future Stack

Containers + VMs



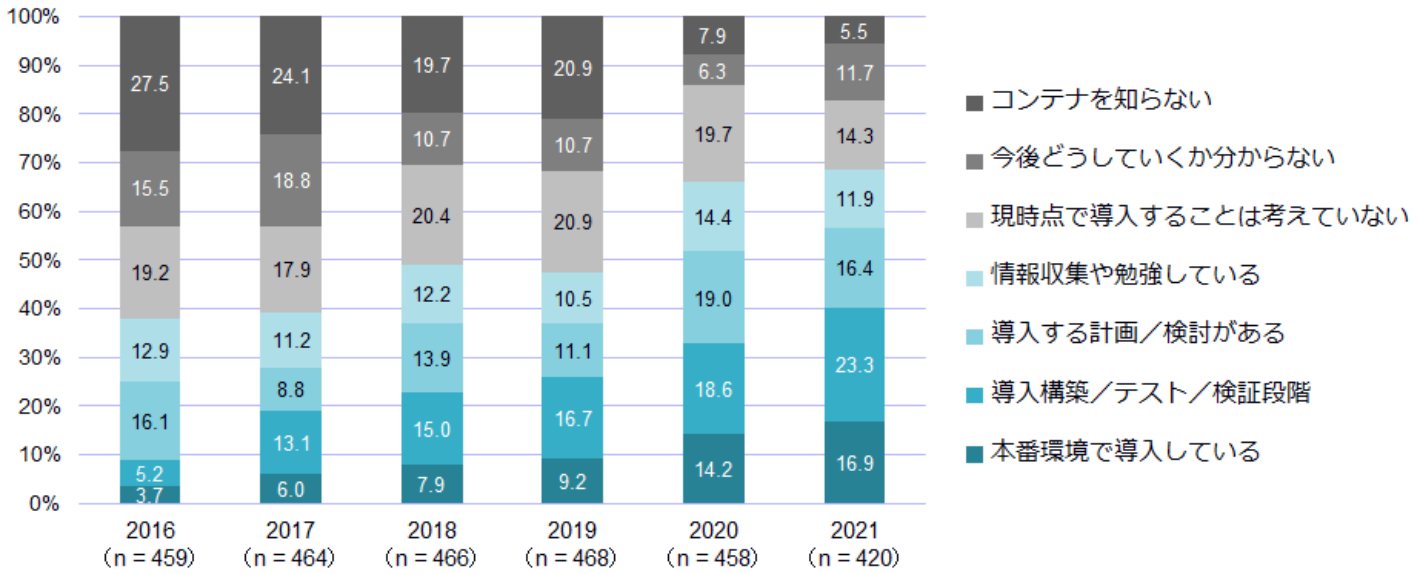
Many K8s distros +

includes KubeVirt

Kubernetes on metal or public IaaS

K8S 国内導入状況 – IDC Japan Report

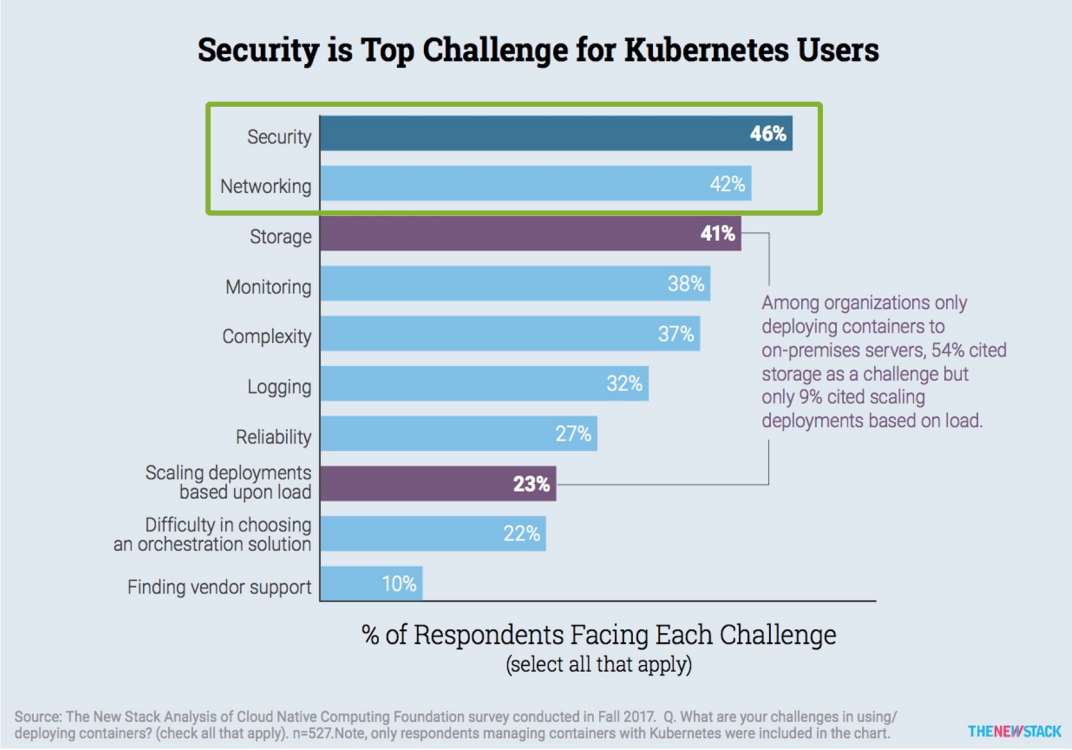
国内はコンテナの本格的な普及期へ

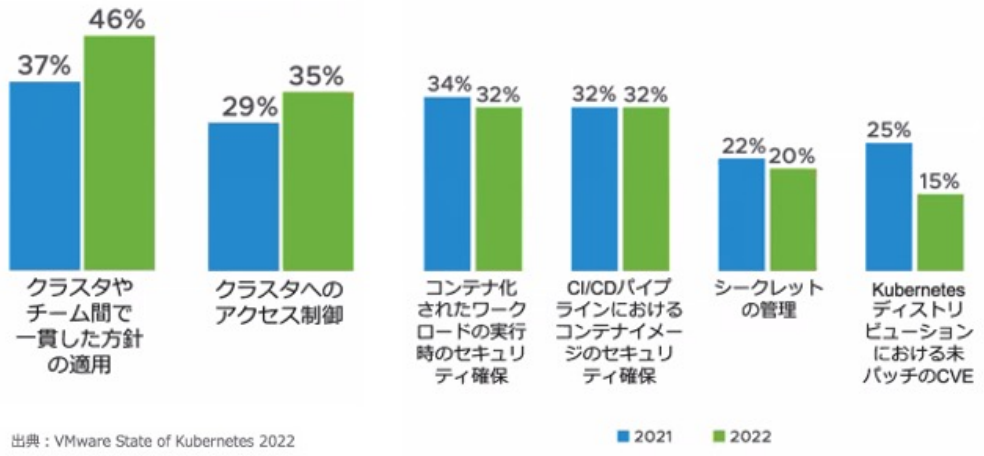


本番環境で使用している企業は*16.9%*となり、*2020*年調査から*2.7*ポイント上昇しました。さらに導入構築／テスト／検証段階にある企業は*23.3%*となり、*2020*年調査から*4.7*ポイント上昇しました。この*2*つを合わせた*40.2%*の企業がコンテナの導入を進めていることになり、国内はコンテナの本格的な普及期に入りました。これまでは*IT*サービス企業がコンテナの導入を牽引してきましたが、*2021*年調査ではサービス業、金融、製造など幅広い業種での導入が進んでいることが分かりました。様々な企業が*DX*（デジタルトランスフォーメーション）を進めていく中でアプリケーションのクラウドネイティブ化に取り組んでおり、コンテナ環境はその基盤としての採用が急速に進んでいます。

増加するコンテナ/k8s利用 と チャレンジ

Kubernatesの課題は、一貫した運用、セキュリティ、ネットワーク





出典：VMware State of Kubernetes 2022

KUBERNETES CNI

CNI: CNCFプロジェクトで管理されており、
Kubernetesで作成するPODにネットワークを提供

canal

flannel

PROJECT CALICO

weave net

Tungsten Fabric

Contiv

. . .

KubernatesではCNIの選択が必要

実装モデル(Overlay, Underlay, Routing)、POD/リソースのL2/L3接続、NetworkPolicyサポート、
ロードバランシングサポート、性能、運用管理など、ネットワーク要件に適したCNIを選択

Agenda

- 製品ポートフォリオとSDN
- Kubernetesによるマイクロサービス
- Contrailについて
- 各種機能紹介 (Feature list)
- ユースケース
- 必要スペックやライセンス

CONTRAILの進化

Contrailはお客さま･マーケットの期待にあわせて進化

2011

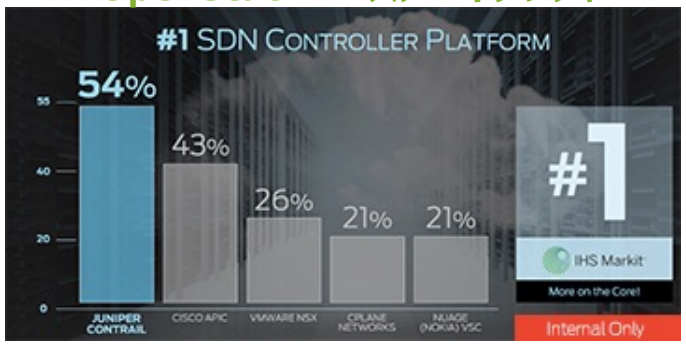
contrail systems

2013

Juniper買収

Open Contrail

OpenStackベースアーキテクチャ



OpenStack環境の No.1 SDN Controller

2018

Linux Fundation

Tungsten Fabric

Contrail Enterprise Multicloud

Underlay/Overlay/ Security/Cloud Connection含む 統合プラットフォーム

2021/2022

クラウドネイティブ アーキテクチャへ

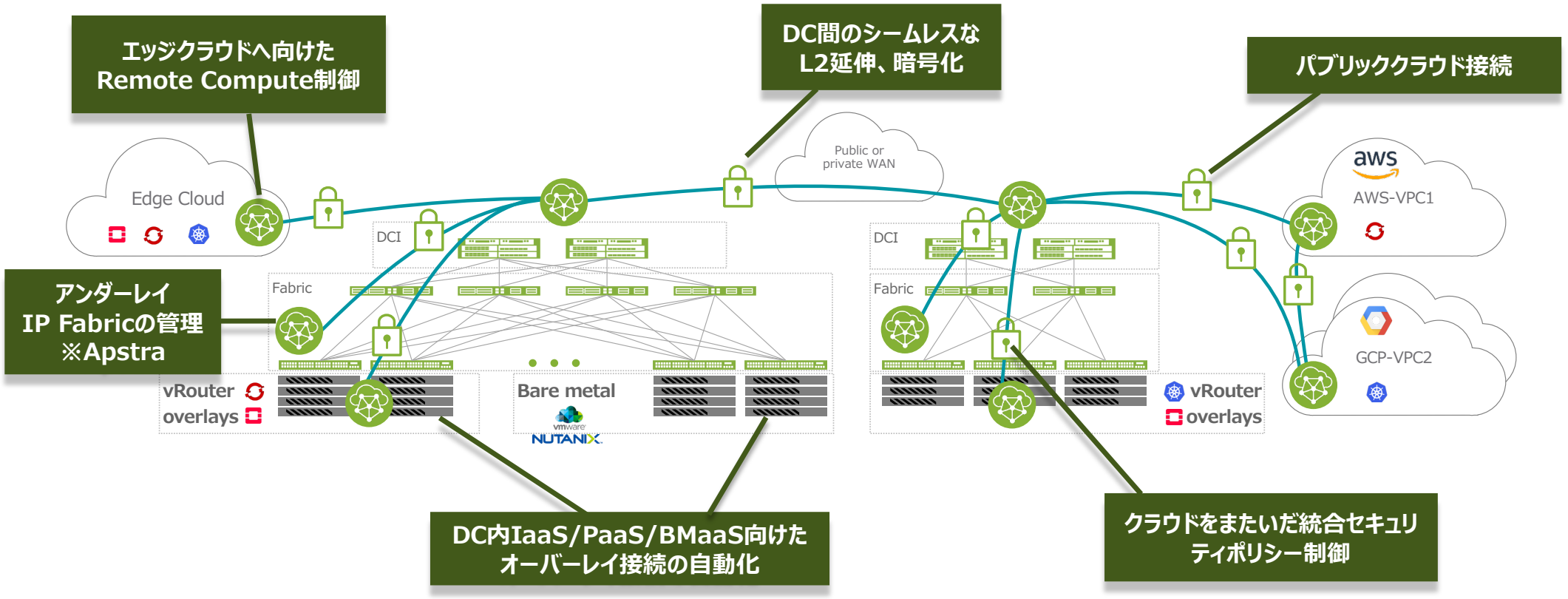
CN2 (Cloud Native Contrail Networking)

データセンタファブリック Apstraに継承

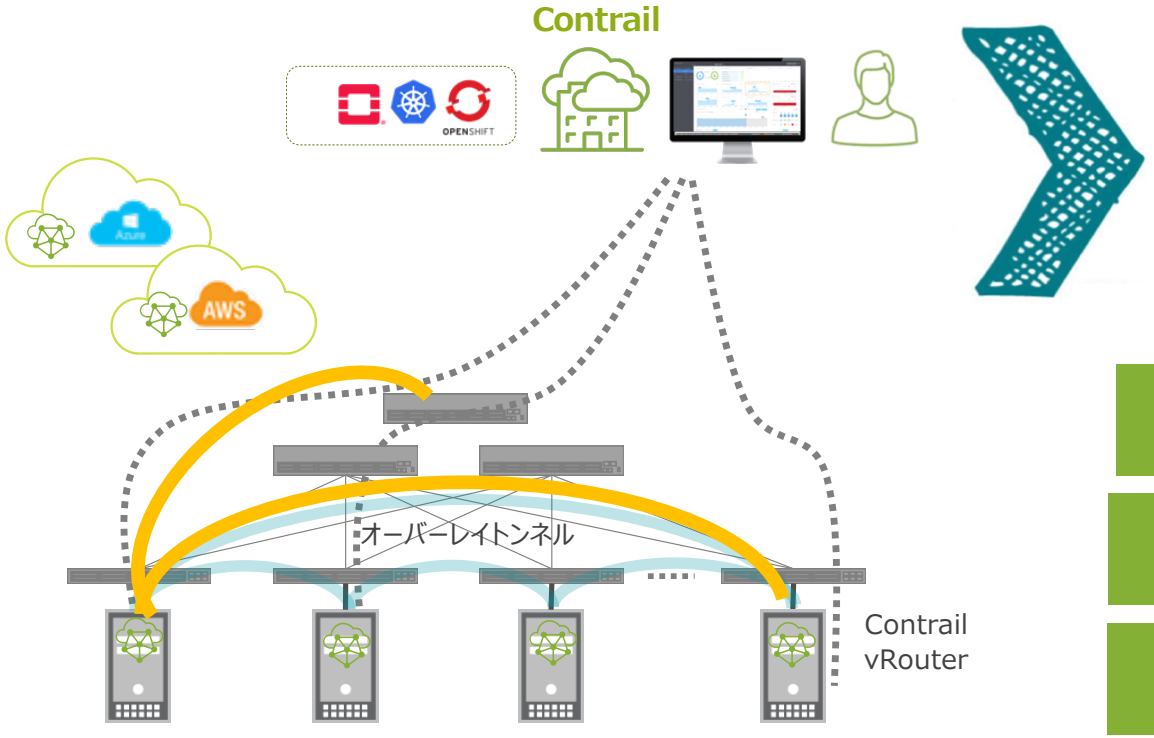
apstra

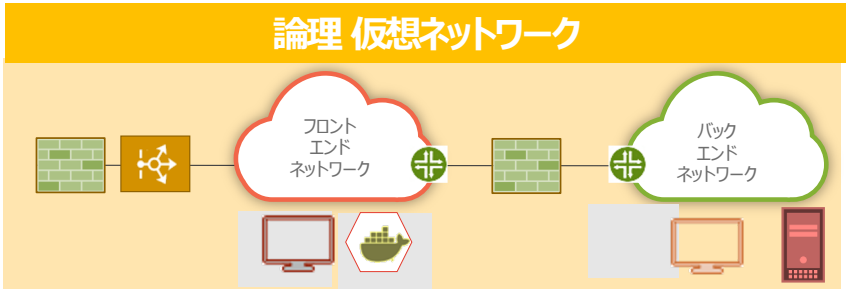
マルチ/ハイブリッドクラウドにおけるEND-to-END制御

クラウドのワークロードにおけるロケーション・ダイバーシティが進むことでネットワークや
セキュリティの重要度が増加



Contrail Networking概要





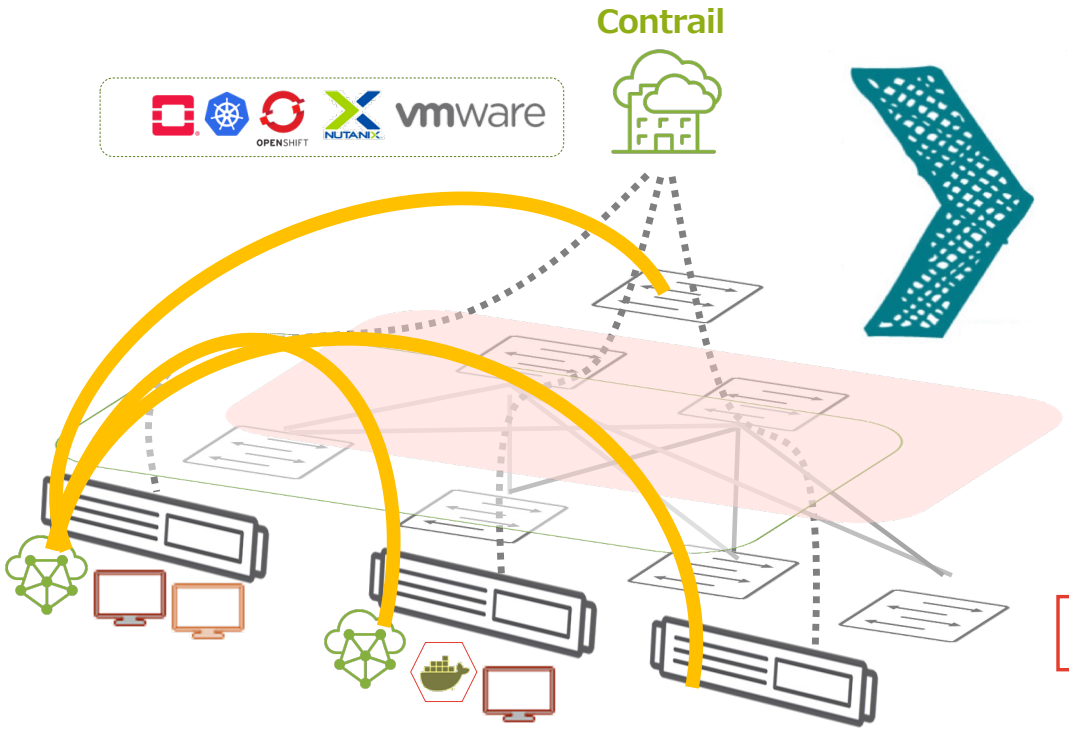
迅速で柔軟なネットワークサービス

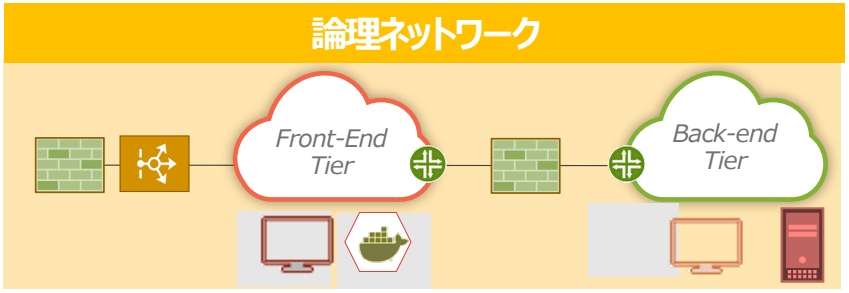
自動化・可視化・マルチテナント

オープン(非ハードウェア依存)

ソフトウェアオーバーレイベースの柔軟な仮想ネットワークを提供

仮想ネットワークに必要な様々なファンクションを提供





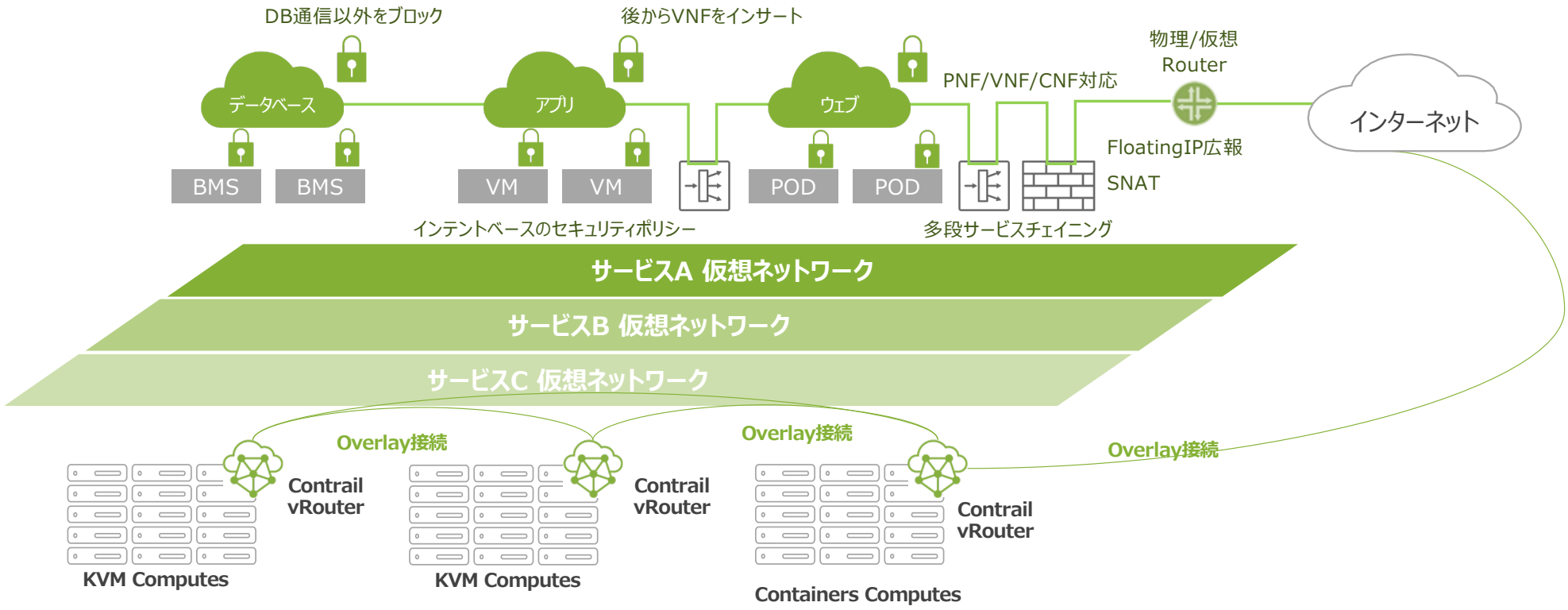
L2 VN　L3 VN　Security Policy　FW

LB　Service Chain.　QoS　IPAM DHCP　Monitoring　Analytics

ソフトウェアベースの柔軟な仮想ネットワークを提供

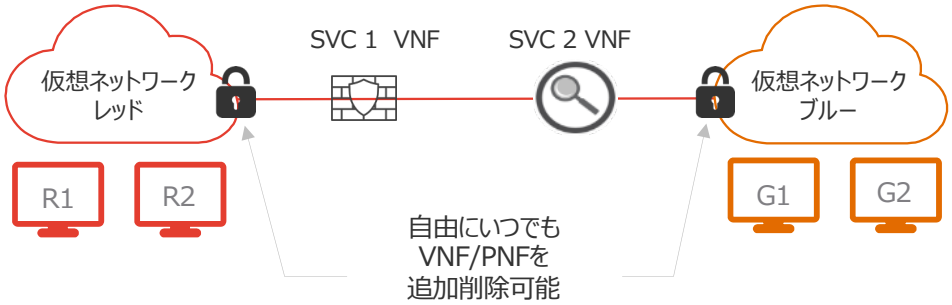
Contrailの仮想ネットワーク アーキテクチャ

- プラットフォームを跨った共通で柔軟なネットワーク＆セキュリティポリシー
- IPベースでない、サービスにタグ付けしたインテントベースのセキュリティポリシー

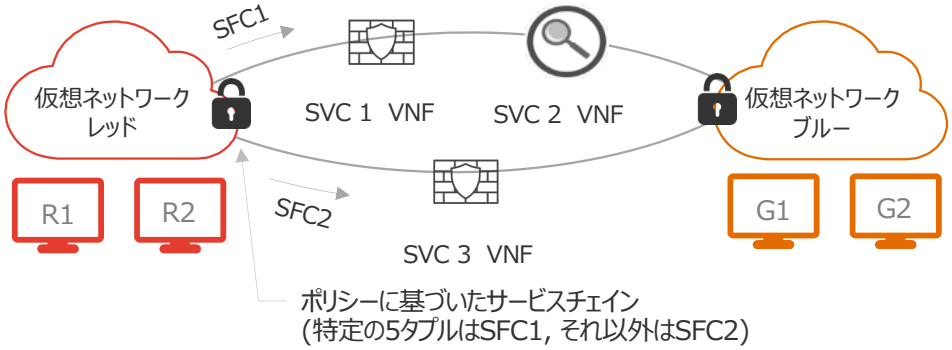


多様なサービスチェイニング ※(roadmap for CN2)

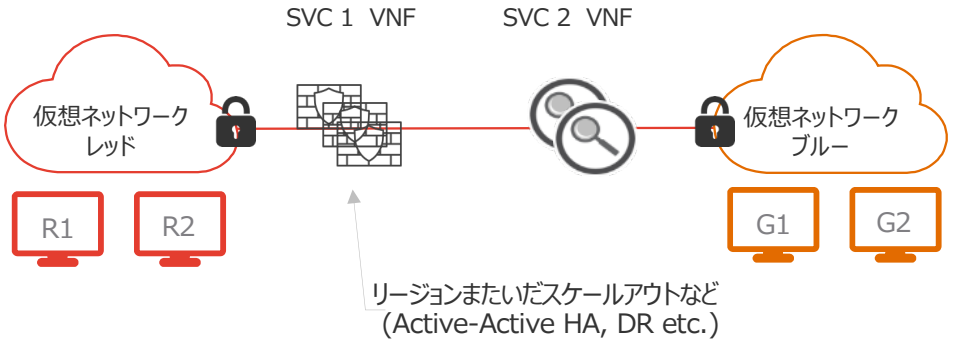
多段サービスチェニング (PNF, VNF, CNF)



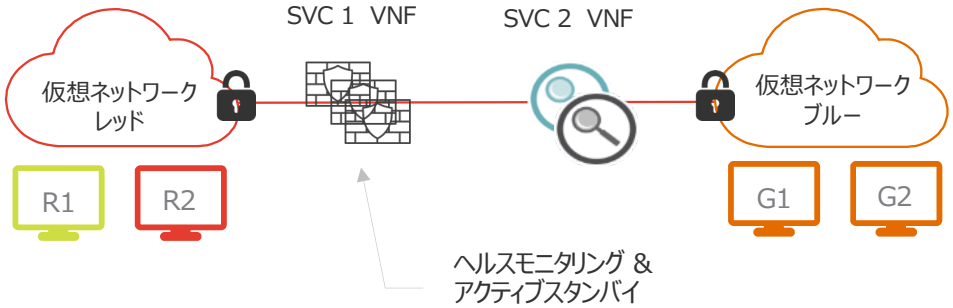
ポリシーベース・サービスチェイニング



スケール・アウト／スケール・イン (Active-Active HA)

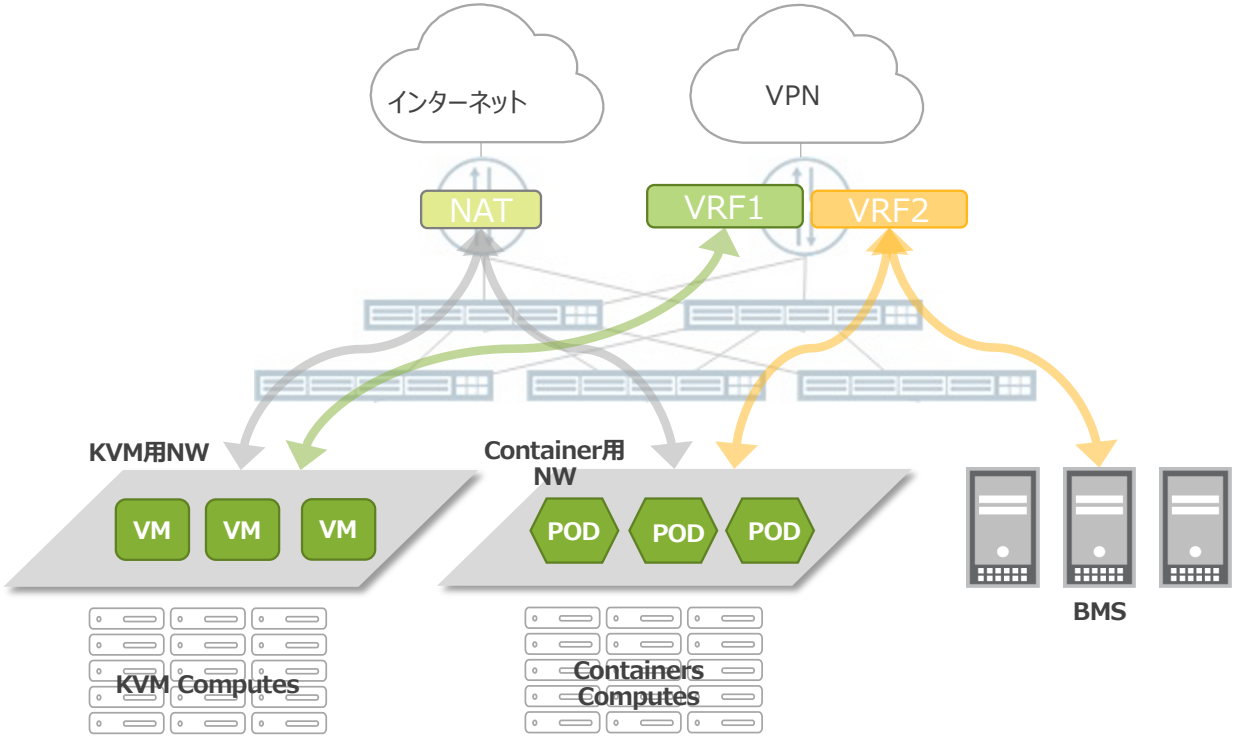


アクティブ・スタンバイ



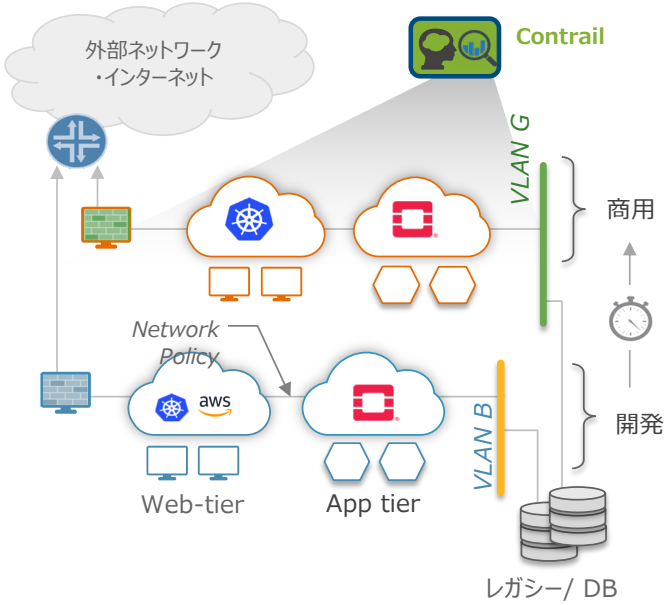
DC ハードウェア ゲートウェイ接続

- 外部接続には物理ルータを使用可能、ソフトウェアGWのボトルネックを解消
- 仮想ネットワークのVPN網への延伸、NATによるインターネット接続が可能



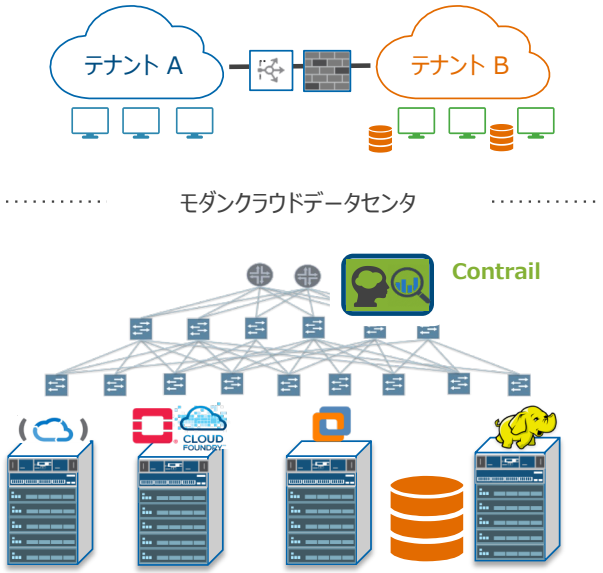
CONTRAIL メインセグメント

1. SaaS / IaaS /PaaS クラウド基盤
(Containers, Hybrid Cloud, BMS, …)



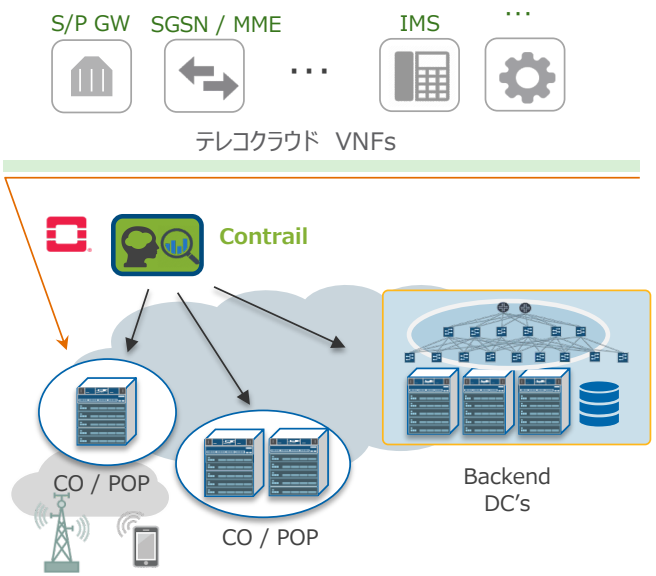
- コンテナ(K8s),プライベートクラウドへのインターコネクト, ベアメタル連携
- 自動化のためのAPI実装
- セキュリティポリシー& 可視化

2. Enterprise プライベートクラウド
(ITaaS, BMS, …)



- ベアメタル&アンダーレイ管理と自動化
- コンテナ、PaaSネットワーク管理
- ハイブリットクラウド対応

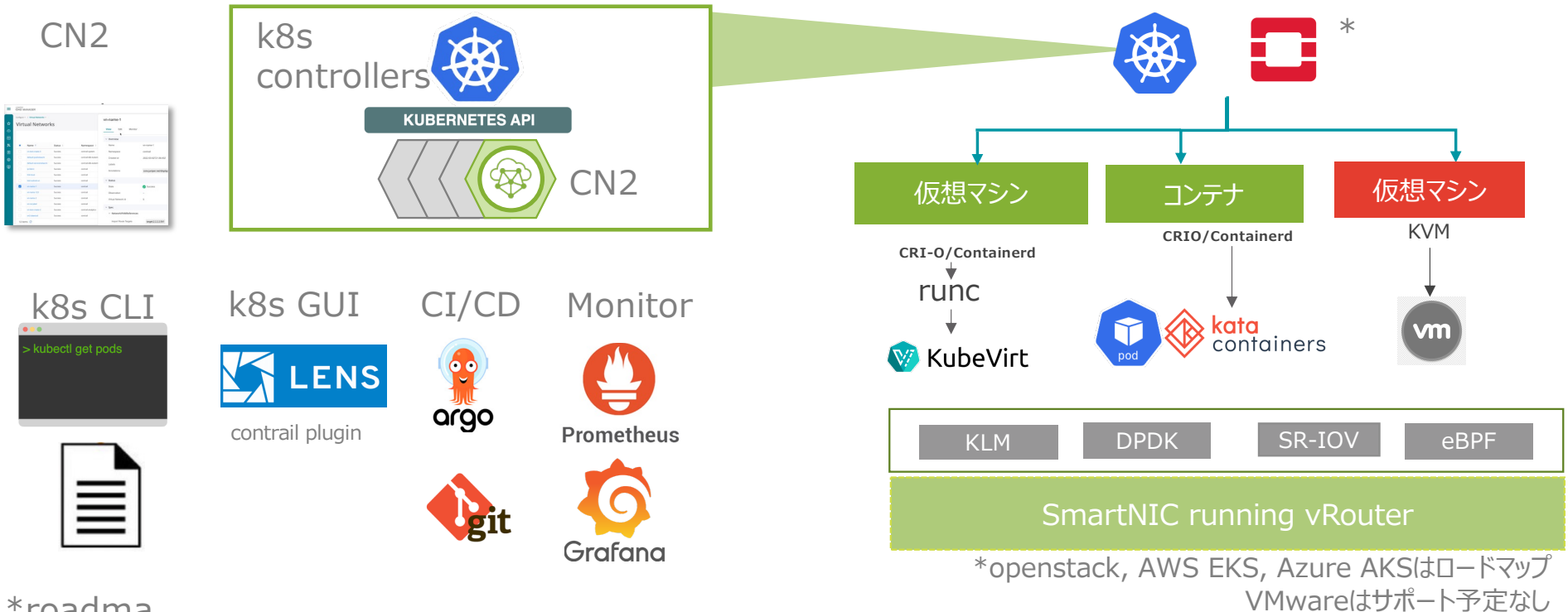
3. Telco / Cable テレコクラウド
(Telco / NFV Cloud, …)



- NFV基盤 and Edge Cloud
- テレコクラウドネットワーキング
- モビリティとGi-Lan VNFソリューション

Cloud-Native Contrail Networking (CN2) for k8s

コンテナオーケストレーション基盤のKubernates(k8s)に
最適な運用・機能の仮想ネットワークやファンクションを提供



クラウドネイティブ から K8s ネイティブ へ

Classic Contrail はマイクロサービスコンテナでしたが、

- 多くのユースケース(OpenStack、K8s、vSphere、ファブリック管理)がある
- 多くのコンポーネントもある (Docker, Cassandra, PostGRES, RabbitMQ, Zookeeper, AppFormix / Insights)
- 最初はOpenStack向けに作られ、次にK8s向けに作られた
- ライフサイクルマネージメントの長い道のりを歩んできた

Kubernetes ネイティブ化

- 設定データモデルにK8s CRD (Custom Resource Definition)、データベースにetcdを採用
- サービス連携とIAM/RBACのための Kubernetes API
- Kubectl CLI が使用でき、GitOps, CICD, Terraform, Infra as codeとの親和性がある

ネイティブのアナリティクスである Prometheus を使用

- 加えて、アナリティクスとテレメトリーとのフェデレーション

Contrail 最大のアップグレード

既存のユースケースとデータプレーンは残したままで

- 同じユースケース K8s, OpenShift, OpenStack, VMs, コンテナ, KubeVirt
- 同じデータプレーン：カーネル, DPDK, SmartNIC

OPENSHIFT RANCHER Amazon EKS

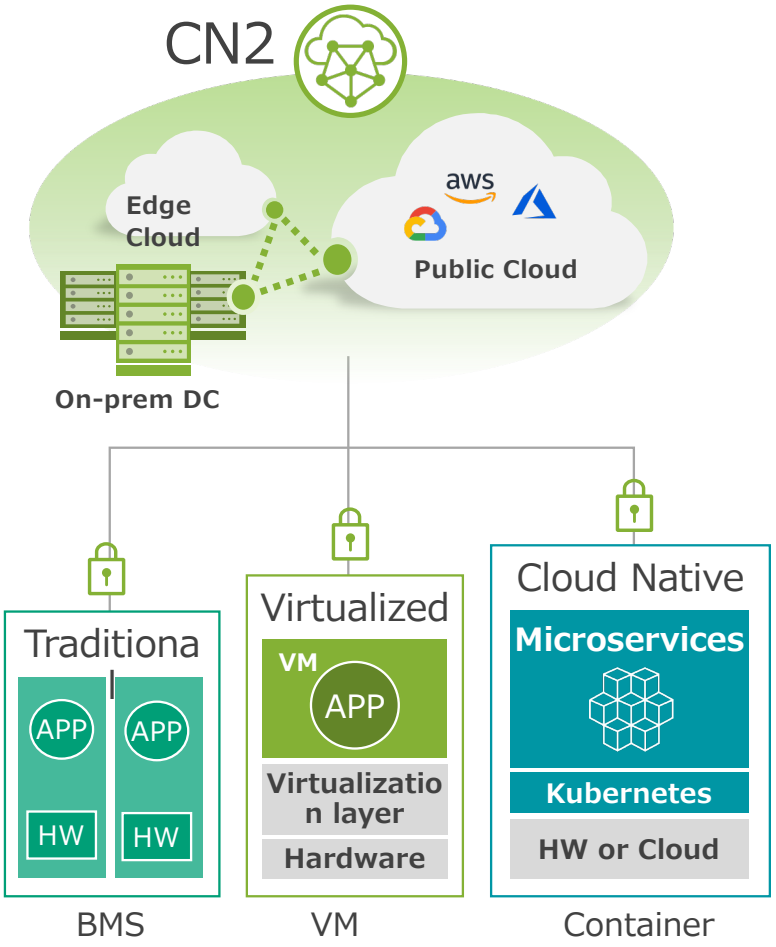
残りの部分を洗練させる

- 1つのGUIと1つの（新しい）CLI、そしてプラグインによる拡張性
- DCからEKS、リモートエッジまでどこでも対応可能

Agenda

- 製品ポートフォリオとSDN
- Kubernetesによるマイクロサービス
- Contrailについて
- 各種機能紹介 (Feature list)
- ユースケース
- 必要スペックやライセンス

CN2: CLOUD NATIVE CONTRAIL NETWORKING



クラウドネイティブネットワーキング

ハイブリッド・マルチクラウドでの一貫したネットワーク

K8S/OpenStack ハイブリッドSDN

※Future Support

Infrastructure investment protection and evolvable infrastructure

NetOps Driven Automation

GitOpsによるCI/CDパイプライン(Contrailパイプライン)

マルチクラスターフェデレーション

単一Contrail ControllerでK8Sマルチクラスター管理

ハイパフォーマンス

DPDK / SmartNIC対応

CN2の特徴(CN2新機能)

従来のContrail の機能

Advanced Networking

Advanced Security

- 柔軟な仮想ネットワーク(L2/L3, テナント分割)
- vRouterの高機能なファンクション (SNAT, QoS, IPAM, S-Chaining, BGP etc.)
- 動的で直感的なセキュリティポリシー
- ハードウェアゲートウェイ連携
- コンテナと非コンテナの仮想NWと一元管理

+

CN2による更なる強化

Extend-ops.

Multi-cluster

Automate

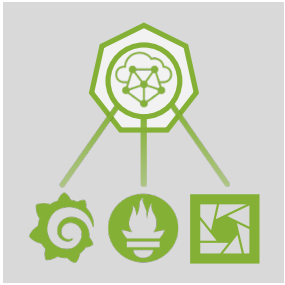
- K8s/DevOps/GitOpsとの高い親和性
- k8sマルチクラスター/フェデレーション※
- 容易な展開と評価(k8s deployer, test suites etc)※
- アドバンスドNW (cRPD, Apstra, SR-IOV etc)※
- 高パフォーマンス(smartNIC※, DPDK, eBPF※ etc)

※ roadmap

WHAT MAKES CONTRAIL UNIQUE

Advanced Networking

- Overlapping IP virtual networks
- Hub/spoke and mesh virtual networks topology
- Traffic mirroring and flow analytics
- Advanced routes and peering
- Multihoming uplinks (L2 or L3) + cRPD* w/ SR
- BGPaaS for 4G/5G workloads



Extends

- Prometheus collection and alert manager
- Grafana dashboards
- Lens Kubernetes GUI's Contrail plug-in

Advanced Security

- Multi-tenant and namespace network isolation
- Concise Contrail policies w/ groups/tags/rules
- Drop/deny alerting and visibility
- Service chaining transparent insertion of L7 NGFW and other network functions
- IPsec data plane encryption*

Spans

- Both OpenStack* and Kubernetes, many distros
- Private, public, and edge (remote compute)
- SmartNIC, DPDK and eBPF* forwarding
- Overlay and underlay/fabric forwarding
- Connects virtual workloads and metal/SRIOV

Better Federation and Multi-cluster

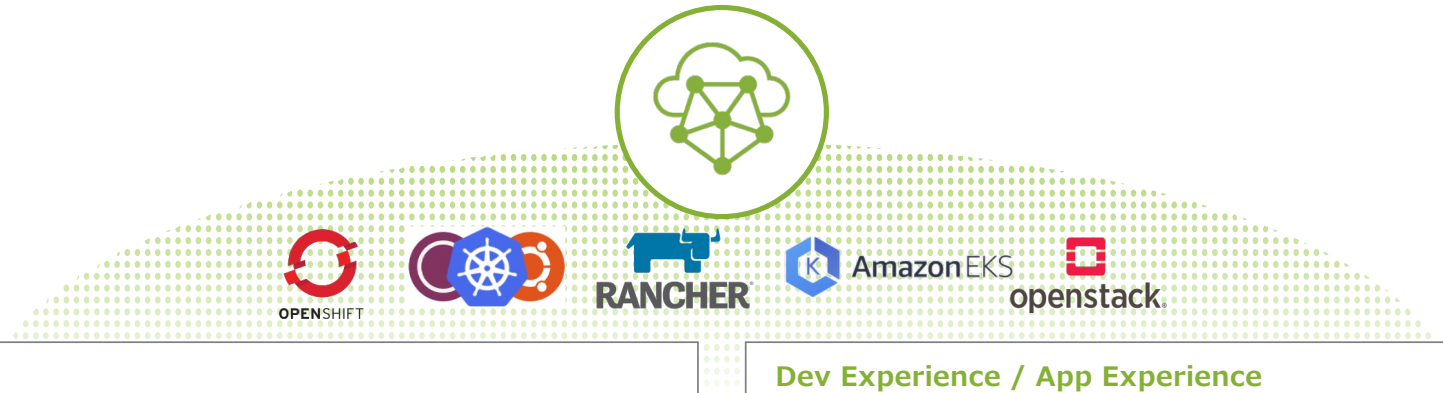
- One Contrail to many clusters CNI and analytics
- Edge/remote compute* model with worker nodes using local gateway
- KubeFed policy federation net/sec objects
- BGP cluster-to-cluster peering
- EVPN and BGP overlay to router peering

Automates

- Argo-based Contrail Pipelines for GitOps
- Validation and CICD with Juniper's test suite
- Easily extends DevOps "as-code" management repositories

* Roadmap for new or Contrail "Classic" feature parity in CN2

CN2 FEATURE-BENEFIT SUMMARY



Ops Experience

- Works with existing tools like kubectl, k9s, Prometheus, Grafana
- Extends existing GUIs: Lens GUI, OpenShift GUI
- Runs inside workloads cluster or in a separate controller cluster
- 1 SDN to rule all multicluster ops. Optional BGP+Kube federation
- Multi-tenancy for OpenStack and K8s namespaces

Dev Experience / App Experience

- Contrail Pipeline to automate infrastructure as code and CI/CD for your full-stack validation testing and ongoing config changes
- Overlapping networks for dev/test/stage/prod with same networks
- Troubleshoot with traffic mirroring and flow analytics
- Developers don't need to bother with policy rules, can use tags

Security

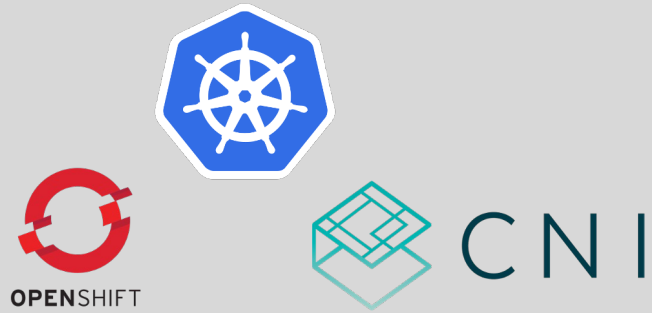
- Flexible micro-segmentation with K8s or Contrail-native policies
- Consolidate policy sprawl and overload with Contrail policy language
- Watch-and-learn mode of policy generation
- Service Chaining L7 Security Services with cSRX/vSRX
- Encrypt* traffic inside and between clusters

Connectivity:

- Virtual networks, load balancing, BGPaaS, remote/edge sites, federation
- High-performance / scale on physical routers/firewalls as gateways
- Data planes: k-mod, DPDK, SmartNIC, Multus and SRIOV compatible
- Connects VM and containers across OpenStack*, K8s, KubeVirt
- vRouter L2 and L3 multihoming

* Roadmap for parity with CN cluster

CHALLENGE OF SECURE NETWORKING FOR KUBERNETES



Kubernetes is the modern “kernel” for application architectures and container stacks

- For networking: CNI is the plug-in interface
- For security: namespaces, NetworkPolicy
- For load balancing: Ingress controller is the interface
- OpenShift is an open PaaS on top of Kubernetes

CNI is not enough

- CNI is generally used for pod networking only
- DNS is yet another add-on
- Inter-Service networking is done with proxies and IPtables
- Hard-to-impossible to get visibility into policy and blocked threats
- Multi-purpose clusters drive up resource efficiency, but are insecure without multitenancy, which CNI doesn’t provide

You get nothing by default

- Flannel CNI is quasi-defacto, but primitive and dead slow
- No NetworkPolicy
- No Ingress load balancing
- No Services load balancing
- No namespaces isolation on the network

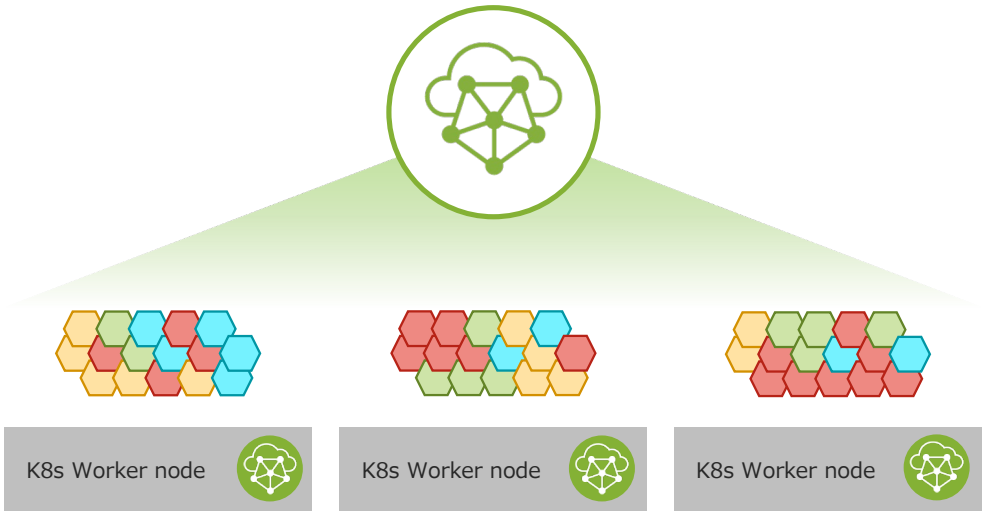
Writing security policy in Kubernetes is a pain

- Security policy as code is good, but developers may make mistakes
- NetworkPolicy objects have drawbacks of usability/complexity

Services meshes help, but aren’t a panacea

- Service mesh L7 policies don’t protect L3/L4 threats
- Enable service discovery between clusters, but not interconnect

SECURE KUBERNETES NETWORKING WITH CONTRAIL



Can run on any underlay IP network, even across distance

Can run on any compute infrastructure, anywhere

High-performance secure networking Kubernetes and OpenShift

Problems Solved!

Connect

- Namespaces are enabled with Contrail multitenancy or vNetworks
- Optionally assign anything its own vNet or IP e.g. overlap test/stage/prod
- DNS, Service and Ingress load balancing is portable and included
- No LB proxies and no upcharge or pay per use (unlike cloud LBs)
- Federate multiple clusters (Contrail controllers easily peer with BGP)
- Multiple interfaces per pod (with or without Multus)
- Container service chaining i.e. Juniper cSRX containerized NGFW
- Place bare-metal servers or VMs on same subnet

See

- Contrail visibility of all policies and threats, including blocked traffic
- Fits into existing observability tooling and K8s GUIs

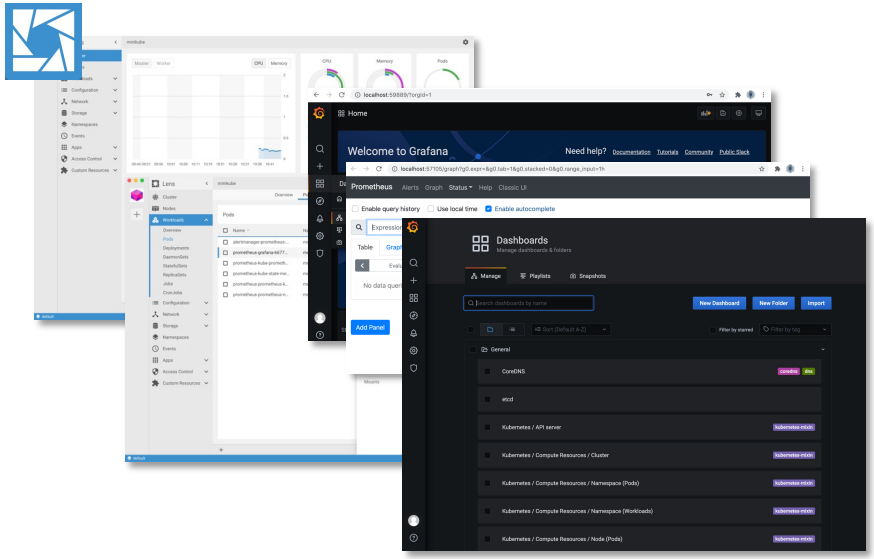
Secure

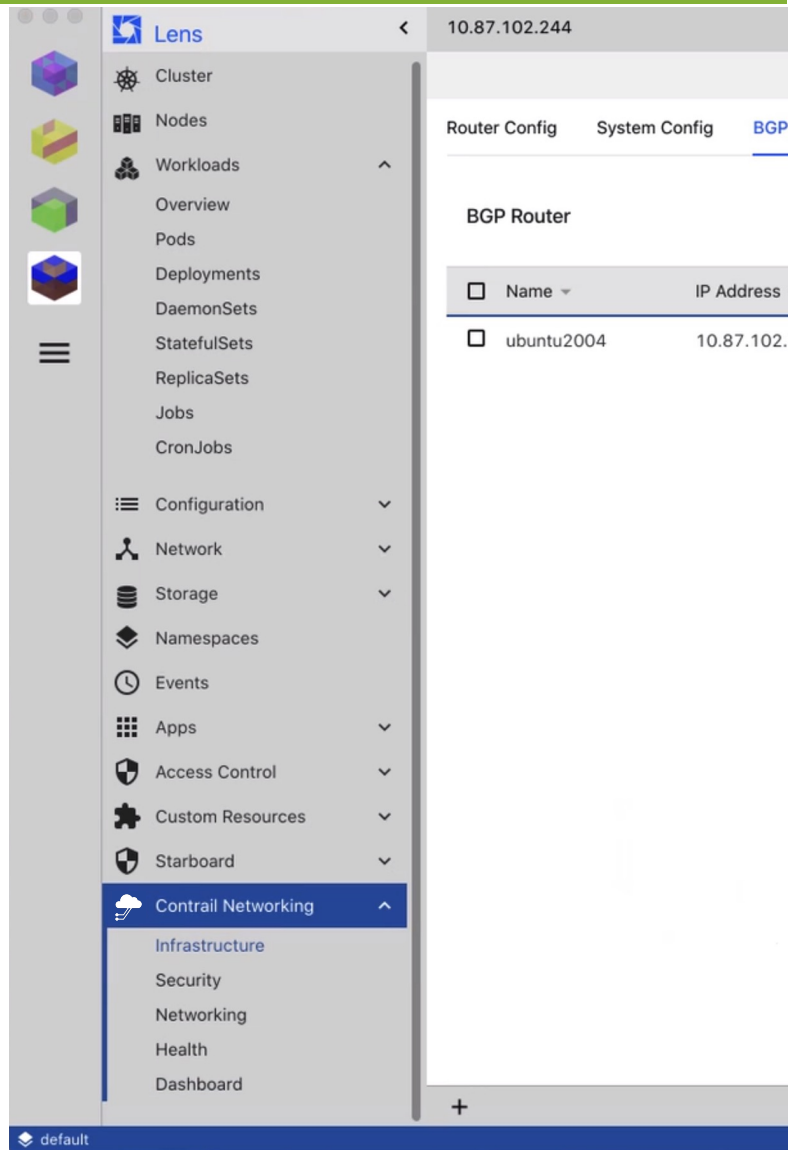
- Secure microsegments as both NetworkPolicy & Contrail policies
- Contrail can associate policy with arbitrary apps with K8s object tags
- Auto-generate policy with new watch-and-learn mode

Deliver… in automated lock-step with Kubernetes

Operations and Analytics in CN2

- Lens GUI w/ extensions for Contrail
- kubectl or k9s
- Any other tools supporting K8s API
- Contrail mixin for Prometheus and Grafana

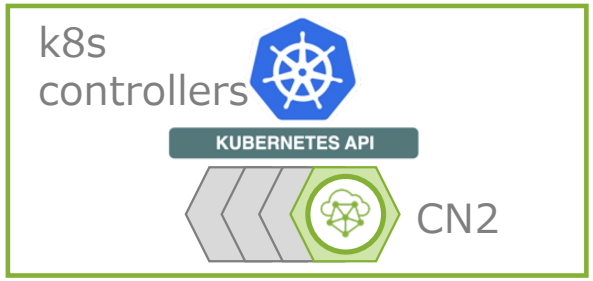




- GUI and analytics is fully optional. Works with standard Prometheus and Grafana to unify monitoring Contrail, Kubernetes, OpenStack and workloads
- Uses state-of-the-art telemetry, logging and time-series collection FluentD, Elastic Stack (Logging, Flows, Events), Prometheus, Grafana
- BYOA (Bring your own analytics) - CN2 will stream analytics data to your existing Prometheus/Elastic and other analytics collectors (DataDog, Splunk, GrafanaCloud, etc.)

CN2 changed to k8s operation

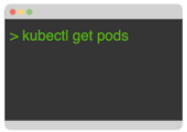
CN2リソースもk8sリソースとしてK8sオペレーション運用に
さまざまなエコシステムツールも利用可能



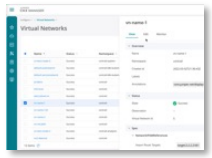
Contrail resources by k8s yaml

```
root@cn2u:~/github_cn2a/demo-manifest# cat stg-vn.yaml
apiVersion: core.contrail.juniper.net/v1alpha1
kind: Subnet
metadata:
  name: vn-stg-subnet
  namespace: stg
  annotations:
    core.juniper.net/display-name: vn-stg-subnet
spec:
  cidr: "192.168.100.0/24"
  defaultGateway: 192.168.100.1
---
apiVersion: core.contrail.juniper.net/v1alpha1
kind: VirtualNetwork
metadata:
  name: stg-vn
  namespace: stg
  annotations:
    core.juniper.net/display-name: Sample Virtual Network
    core.juniper.net/description:
      VirtualNetwork is a collection of end points (interface or ip(s) or MAC(s))
      that can communicate with each other by default. It is a collection of
      subnets whose default gateways are connected by an implicit router
spec:
  v4SubnetReference:
    apiVersion: core.contrail.juniper.net/v1alpha1
    kind: Subnet
    namespace: stg
    name: vn-stg-subnet
```

k8s CLI

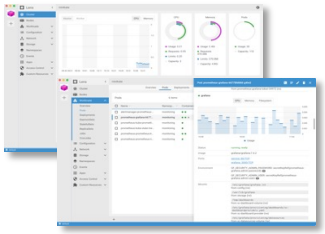


CN2



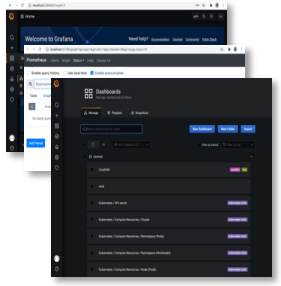
k8s GUI

contrail plugin



CI/CD

Monitor



CN2インストールと拡張の改善

Classic Contrail

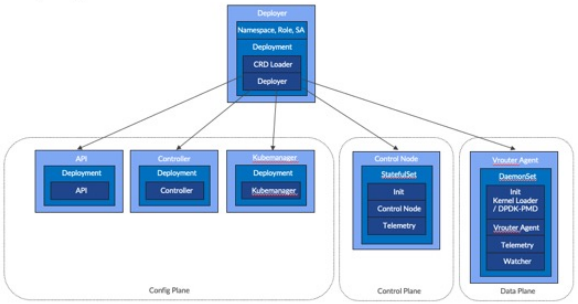
- 実行前チェックが不十分
  - Compute resources
  - DNS
  - Server reachability
- トラブルシューティングの複雑さ
  - Analytics components
  - Local log at each node
  - Docker install failure
- 実行後チェックが不十分
- 限定的なカーネルバージョンサポート

CN2 Install

- K8s custom resources
- Manifestを利用したシンプルインストール
- 実行前/後チェックツール
- K8s control planeの相互作用

K8sインストール後に以下コマンドでインストール実施
$ kubectl apply -f cn2-deployer.yaml

Deployment model

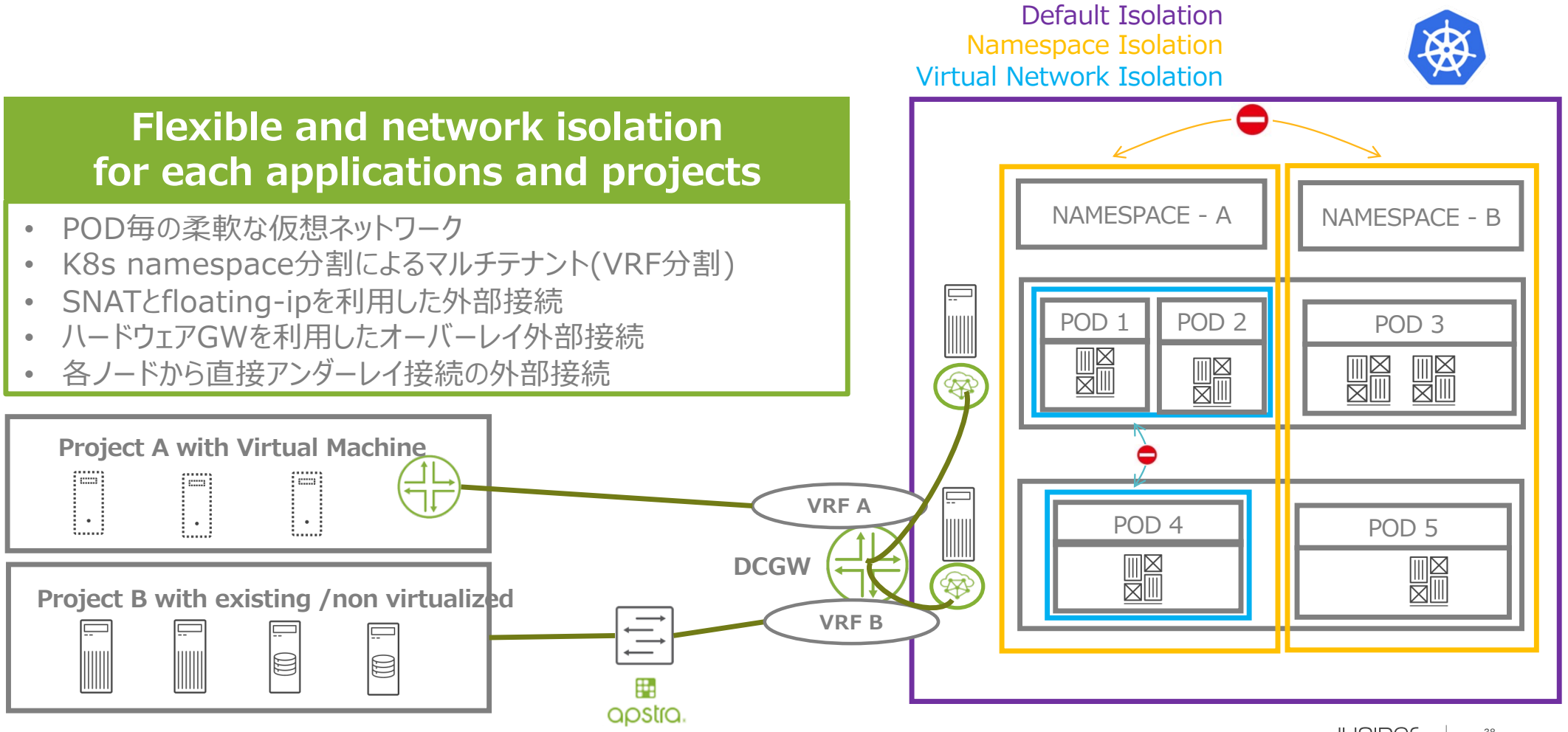


– クラウドネイティブネットワーキング

柔軟なネットワーク分割と相互接続

Flexible and network isolation for each applications and projects

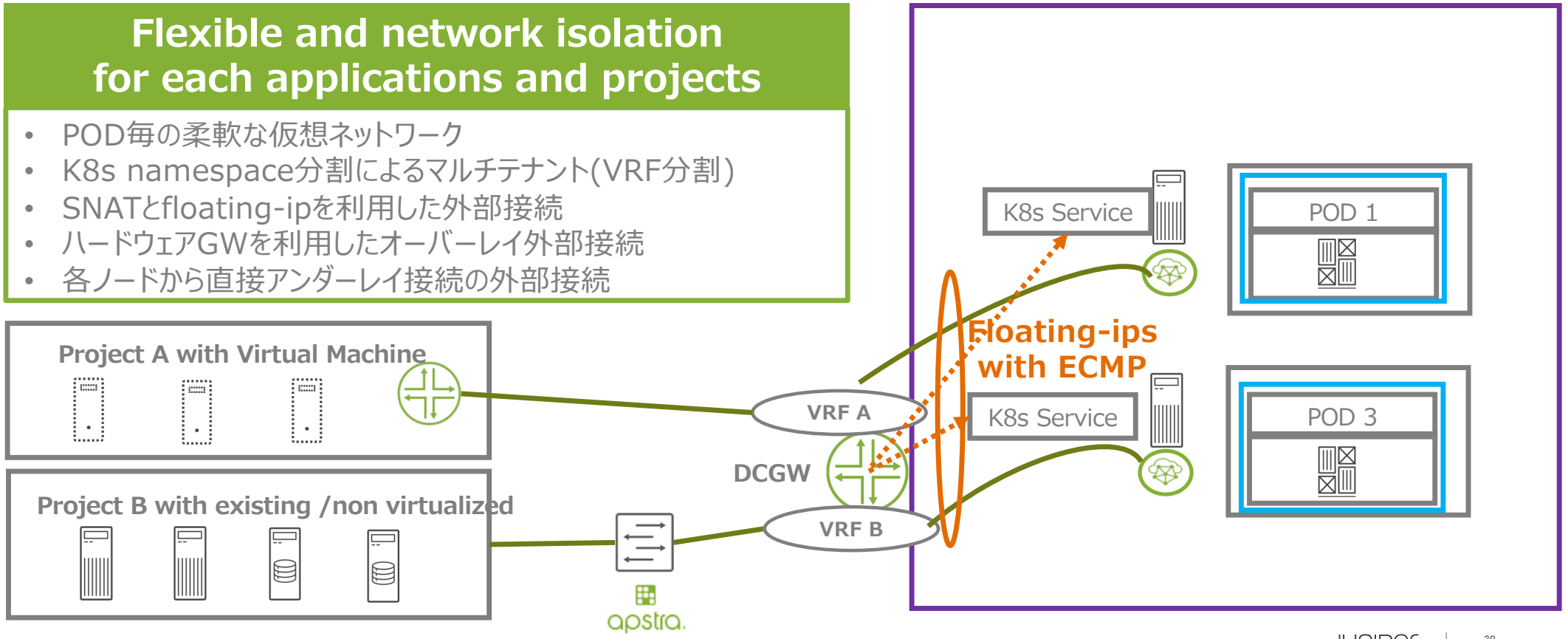
- POD毎の柔軟な仮想ネットワーク
- K8s namespace分割によるマルチテナント(VRF分割)
- SNATとfloating-ipを利用した外部接続
- ハードウェアGWを利用したオーバーレイ外部接続
- 各ノードから直接アンダーレイ接続の外部接続



柔軟なネットワーク分割と相互接続

Flexible and network isolation for each applications and projects

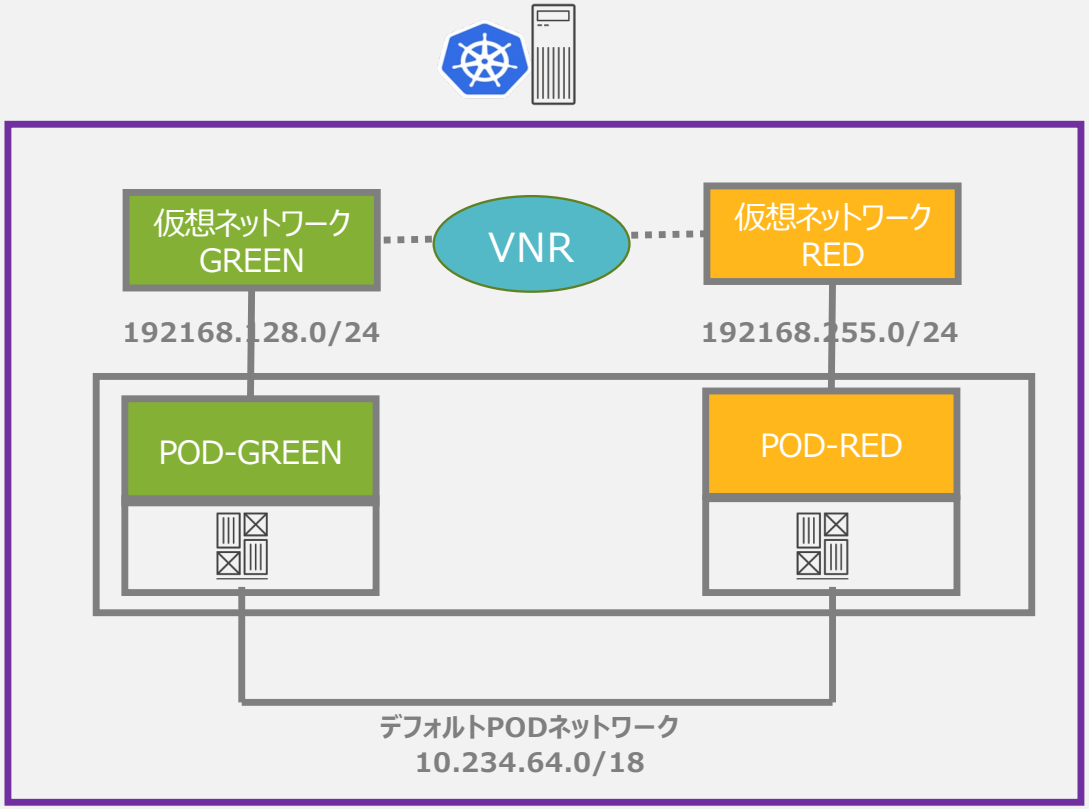
- POD毎の柔軟な仮想ネットワーク
- K8s namespace分割によるマルチテナント(VRF分割)
- SNATとfloating-ipを利用した外部接続
- ハードウェアGWを利用したオーバーレイ外部接続
- 各ノードから直接アンダーレイ接続の外部接続



PODマルチインタフェース

マルチインタフェースで接続も分割

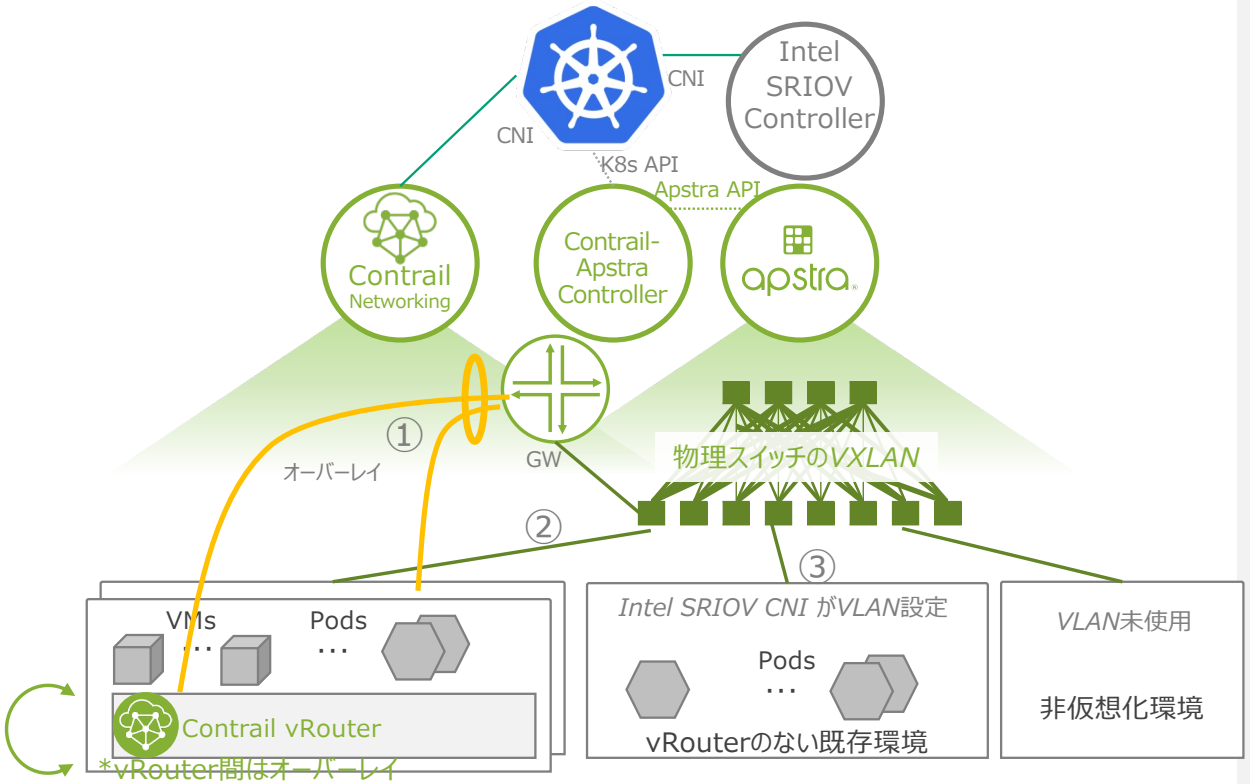
- 通常のPODは1インタフェースだが、複数インタフェースを利用可能に
- 利用ケース
  - 同一コンテナの別ネットワーク接続
  - データと管理のインタフェース分割
  - VNF/CNFの複数インタフェース
- 仮想ネットワーク(L2)をVNR:Virtual Network Router(L3)やRoute Targetにより相互接続可能に



VNR:Virtual Network Router

非仮想化環境/外部環境との相互通信

ゲートウェイを介した接続・非オーバーレイ・SR-IOV利用※
非仮想化環境との接続も柔軟



① オーバーレイゲートウェイ接続
ゲートウェイまでオーバーレイし、ハードウェアゲートウェイで多様な制御。

②アンダーレイ接続*(overlay-less)*
ワーカーノードから直接物理スイッチ接続。

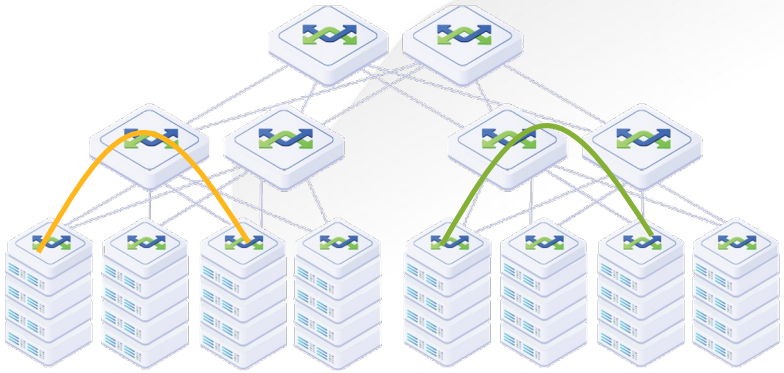
③SR-IOV/Apstra
SR-IOVを利用し、Apstra連携により必要なVLANを設定。

※ roadmap

参考：Juniper Apstraとは

- データセンタ物理ネットワークの自動構築/監視/診断
- マルチベンダ環境を一元管理

Juniper Apstra



JUNIPER NETWORKS　SONiC　ARISTA　cisco

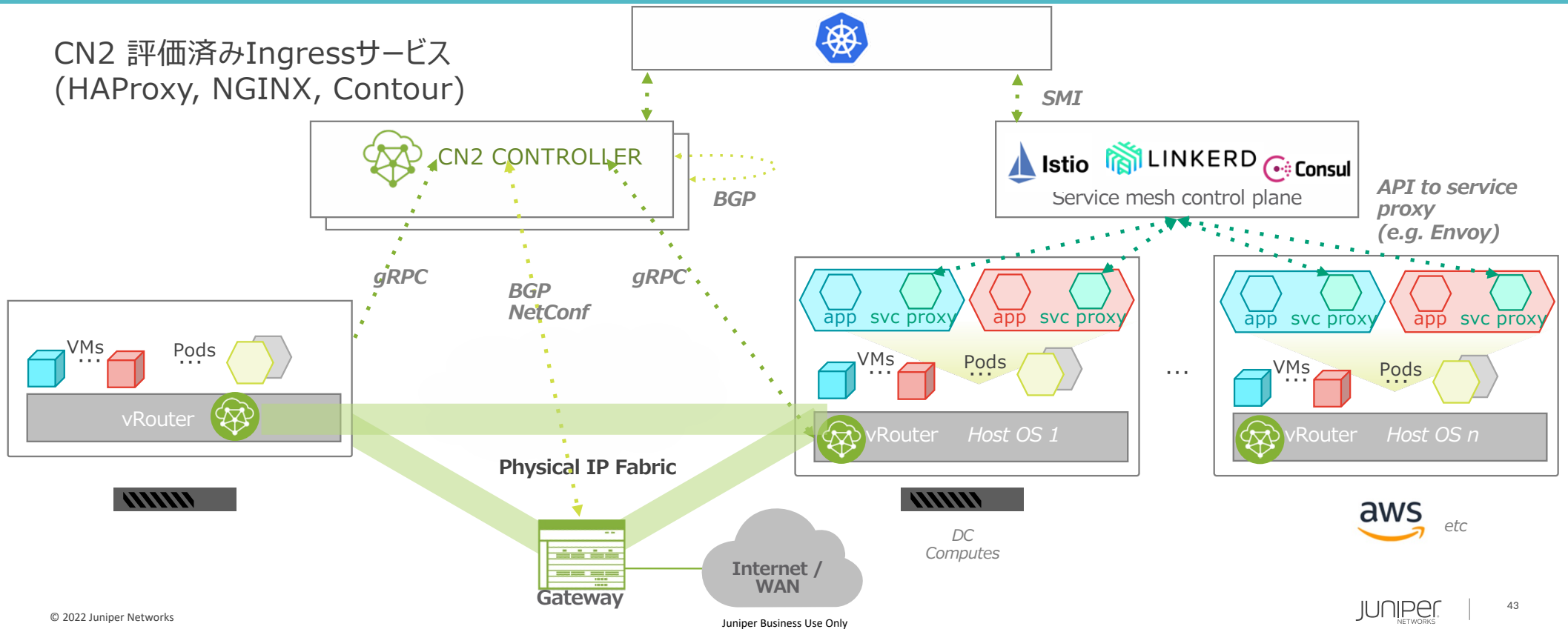
EVPN/VXLAN 標準アーキテクチャ利用

Extends-tool

※ roadmap

CN2 – L7 Ingress Service interaction

- CN2はL2-L4を提供し、Ingress(L7)と連携
- Service mesh連携の付加価値提供 ※



Juniper Business Use Only

– マルチクラスター

マルチクラスタ Kubernetesが広がるkubesprawl

K8sクラスタが広がるKubeSprawl(無秩序に拡大する)問題

Enterprise Kubernetes Multicluster

増加するk8sクラスタ：数十から数百のクラスタを扱うことも増えてきている

- 1 cluster 開発向け
- 1 cluster テスト向け
- 1 cluster ステージング向け
- 1 cluster 商用向け

✖

- チーム毎に1 cluster
- アプリケーション毎に1 cluster
- セキュリティ境界毎に1 cluster
- リージョン毎に1 cluster

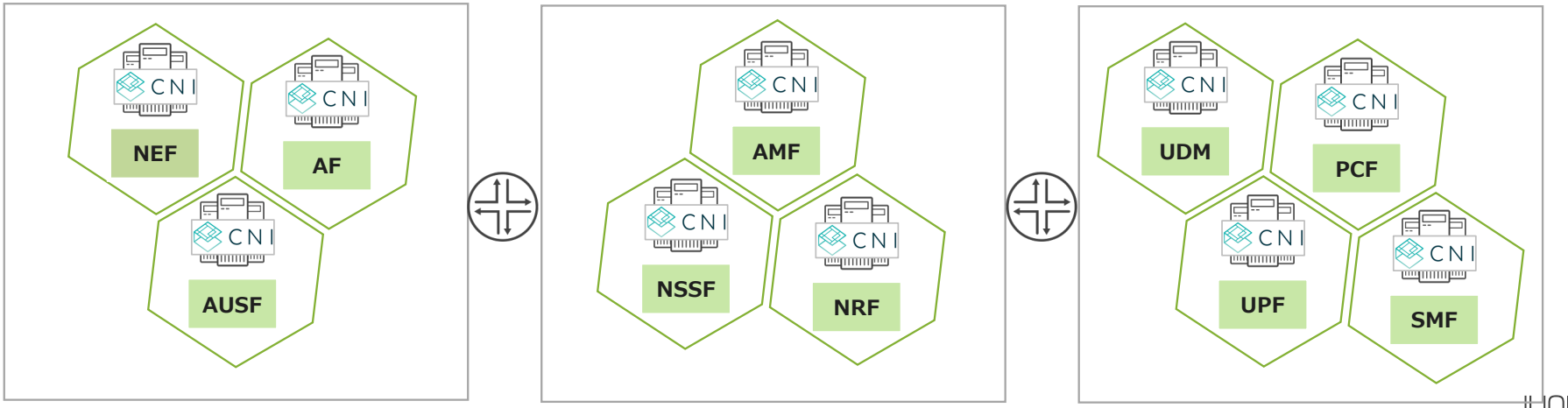
複雑さとオーバーヘッドの増加

複数バージョンで
セキュリティを確保

多数のアップグレード

観覧ツールの増加

サイロ化した
オブザーバ備リティ



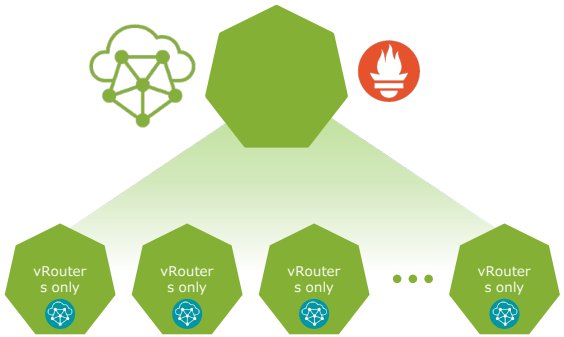
Multi-cluster

マルチクラスタ Kubernetesの簡素化

K8sクラスタが広がるKubeSprawl(無秩序に拡大する問題)の複雑さを低減

CN2 Multi cluster Solutions

統合的なネットワーク &セキュリティ



※*CN2* フェデレーションでクラスタ間の
経路交換・通信もサポート予定

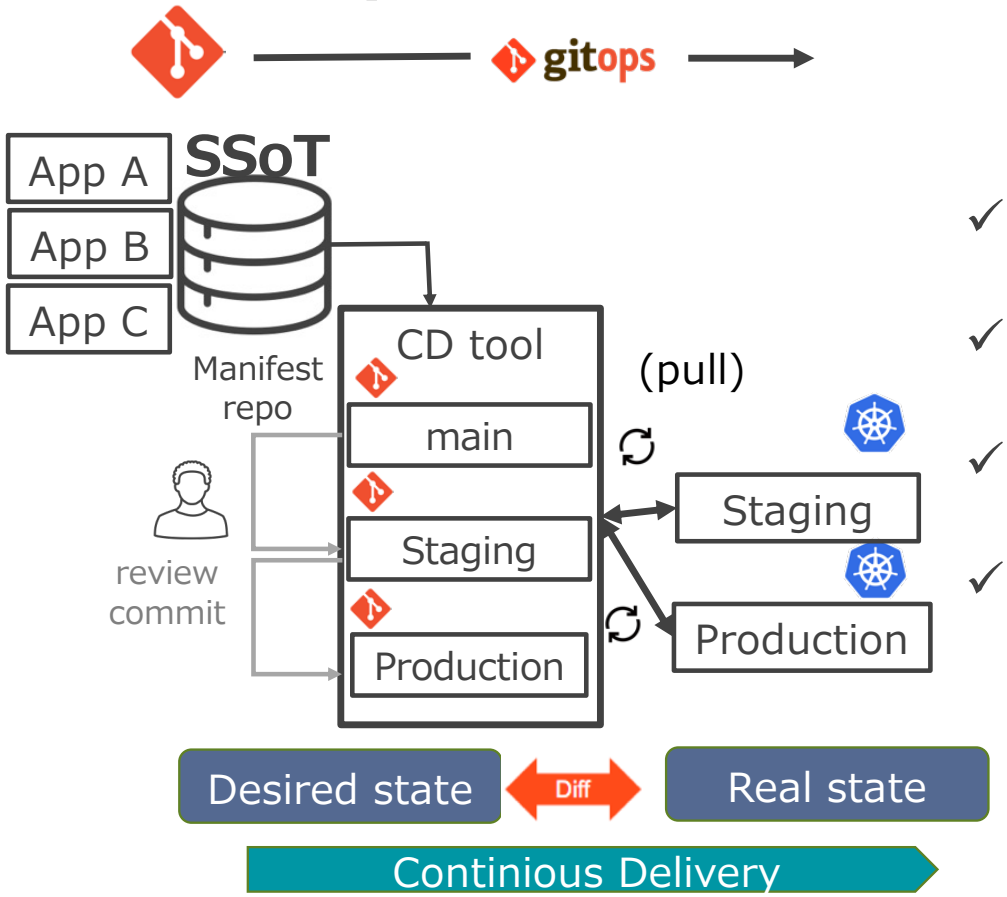
- セントラルクラスタの1つのCN2で
  多数のデータプレーンクラスタを管理
- NamespaceをRBACを利用しマルチテナント提供
- 各クラスタへのロードバランシング
- L3機能(VNR)で異なるクラスタの仮想ネットワークを
  相互接続
- BGPフェデレーションで外部や別クラスタとの連携

```
[centos@test1-central-cluster ~]$ kubectl get ns -A
NAME                                                              STATUS   AGE
aap-project-sut                                                   Active   6h27m
contrail                                                          Active   3h4m
contrail-analytics                                                Active   6h33m
contrail-deploy                                                   Active   3h4m
contrail-k8s-kubemanager-kubernetes-contrail                      Active   3h1m
contrail-system                                                   Active   3h3m
default                                                           Active   6h41m
isns-et-3-ip-fabric                                               Active   5h52m
km-distributed-cluster1-distributed-cluster1-aap-project-sut      Active   6h27m
km-distributed-cluster1-distributed-cluster1-contrail             Active   174m
km-distributed-cluster1-distributed-cluster1-contrail-analytics   Active   6h27m
km-distributed-cluster1-distributed-cluster1-contrail-deploy      Active   6h37m
km-distributed-cluster1-distributed-cluster1-contrail-system      Active   6h37m
km-distributed-cluster1-distributed-cluster1-default              Active   6h37m
km-distributed-cluster1-distributed-cluster1-isns-et-1-6d7690a2   Active   5h53m
km-distributed-cluster1-distributed-cluster1-kube-node-lease      Active   6h37m
km-distributed-cluster1-distributed-cluster1-kube-public          Active   6h37m
km-distributed-cluster1-distributed-cluster1-kube-system          Active   6h37m
km-distributed-cluster1-distributed-cluster1-multus-support       Active   5h33m
```

*Namespaceサンプル： Cluster-namespace*で論理分割

– CONTRAIL パイプライン

参考. GitOps with SSoT

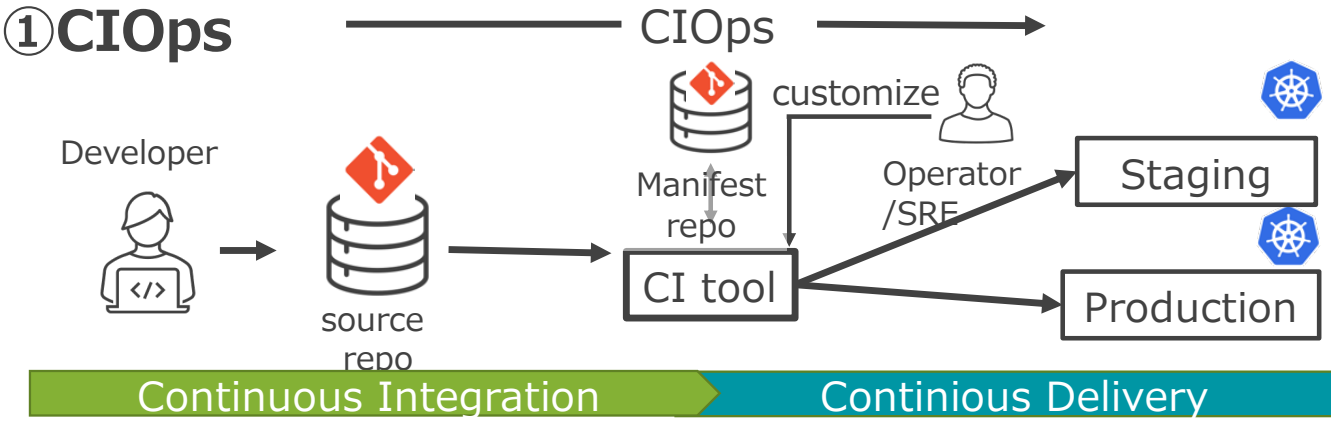


- ✓ GitOpsは2017年にWeaveworks が提唱
- ✓ Gitを SSoT としてアプリとインフラを宣言的に定義
- ✓ 宣言と実態の乖離があると、通知及び自動的に回復
- ✓ 生産性、安定性、信頼性、一貫性、セキュリティが向上

LINK : GitOps - Operations by Pull Request (weaveworks)
LINK : The History of GitOps (weaveworks)

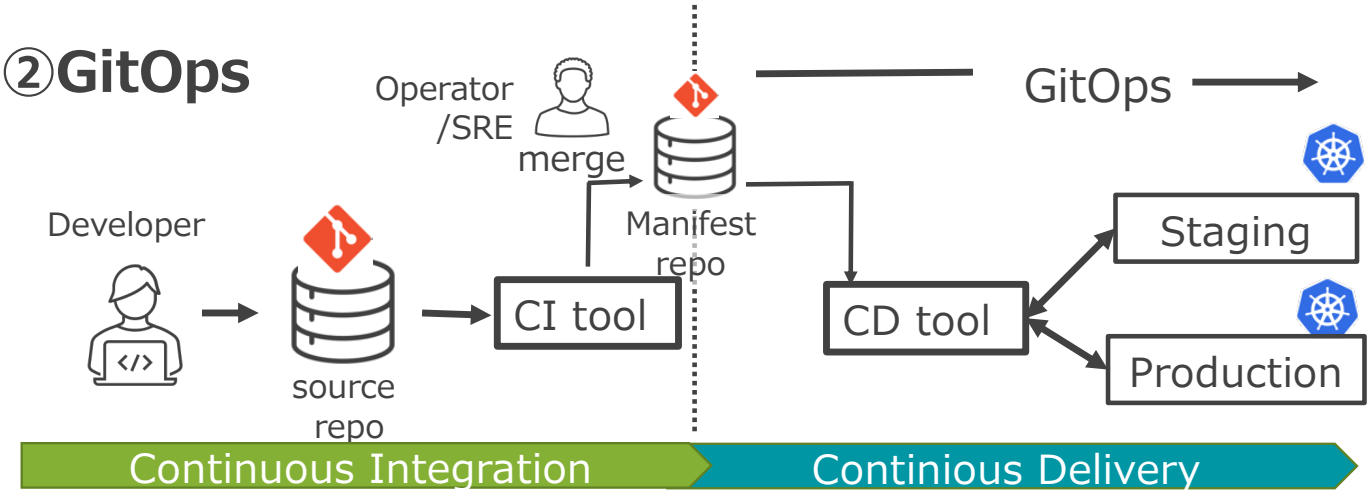
参考.Traditional CI/CDからContainer CI/CD(CIops, Gitops)

①CIOps



- ✓ CI ツールが直接デプロイ (push)
- ✓ CI ツールにデプロイする権限が必要 (セキュリティ課題)
- ✓ 開発者がデプロイ方法や運用を強く意識する必要がある。
- ✓ ロールバックや一貫性が保ちづらい

②GitOps

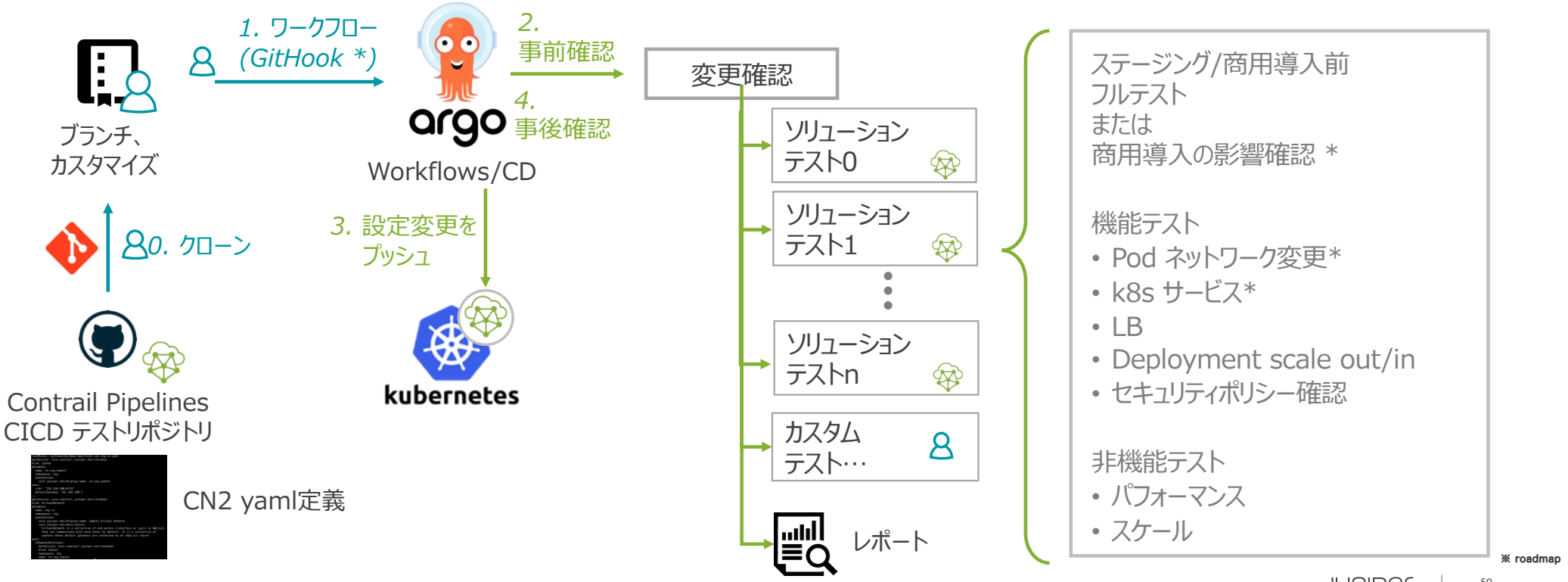


- ✓ CDツールがデプロイ (pull)
- ✓ CIとCDの権限の明確化と連携 (アプリ開発者(CI)とインフラオペレーター/SRE(CD)の分担と連携)

Extends-tool

Contrail Pipelines※を活用したGitOps

- 機能テスト、ミドルウェアテスト、アップグレードテスト、の自動化
- ArgoCDを利用したテストパーッケージの提供 ※



※ roadmap

Extends-tool

Next release plan

AUTOMATE RELIABILITY with CN2 and GitOps

- The test suites will automate to qualify Contrail with supported Kubernetes distribution
- Initial test cases are built around standard networking services and functionality, Ingress, Service Load balancing, VN creation, BGPaaS, etc.

Contrail Pipelines

ArgoCD

- Continuous Delivery, designed specifically for K8s; Already included in some distros like OpenShift
- Facilitates GitOps
  - Single source of truth and change reviews and tracking/auditing
  - Rollback to any previous state version
- Runs in cluster
  - More secure with user access only to Git
  - Tracks config drift: can overwrite manual changes or alert on them
- Group configs into Argo Applications and Application Projects
- Sequence config application with Argo workflows

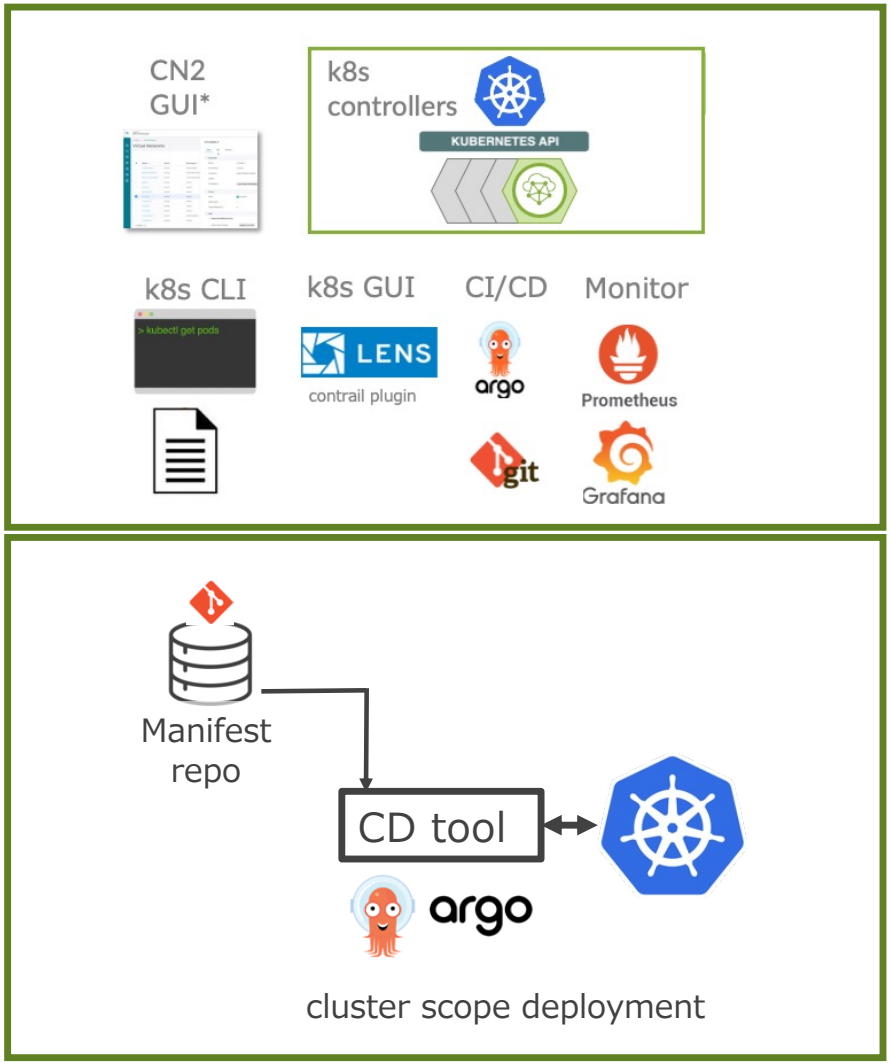
Contrail Test Suites

- Licensed and Juniper supported combo of our test packages with qualified Argo versions to automate:
  - Validate day-0 with unique distros, versions, infrastructure and middleware in cluster
  - Validate artifact change: upgrades of Contrail or other major components
  - Validate config changes: all Contrail configs as code and templatized for work with DevOps t
  - Run your unique scale/boundary testing cases
  - Create and easily template test / staging vs. production environments

CN2 オペレーションデモ動画

- ✓ **CN2 ベーシックオペレーション**
  - ✓ Contrail k8s API
  - ✓ CN2 マニフェストファイルサンプル
  - ✓ LENS GUI CN2プラグイン
- ✓ **CN2 with GitOps(最初の一歩)**
  - ✓ Argo CDによりGitからCN2リソースもデプロイ
  - ✓ Gitとk8sクラスタの差異を検知
  - ✓ 差異を自動修復

20220528-CN2-CODT.mp4



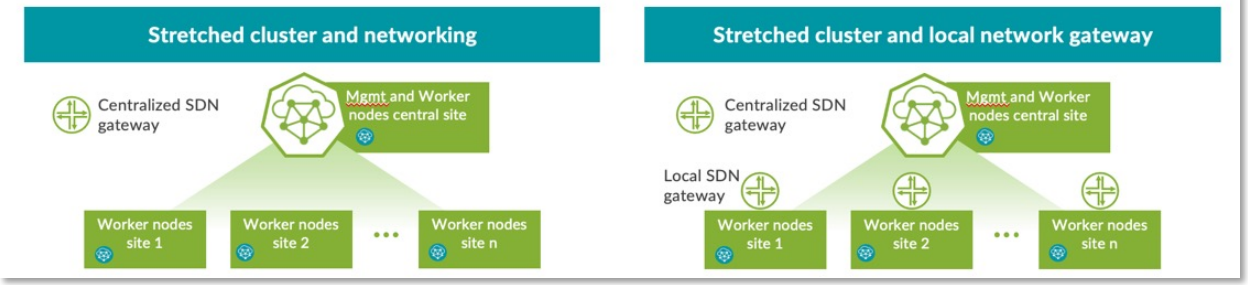
Agenda

- 製品ポートフォリオとSDN
- Kubernetesによるマイクロサービス
- Contrailについて
- 各種機能紹介 (Feature list)
- ユースケース
- 必要スペックやライセンス

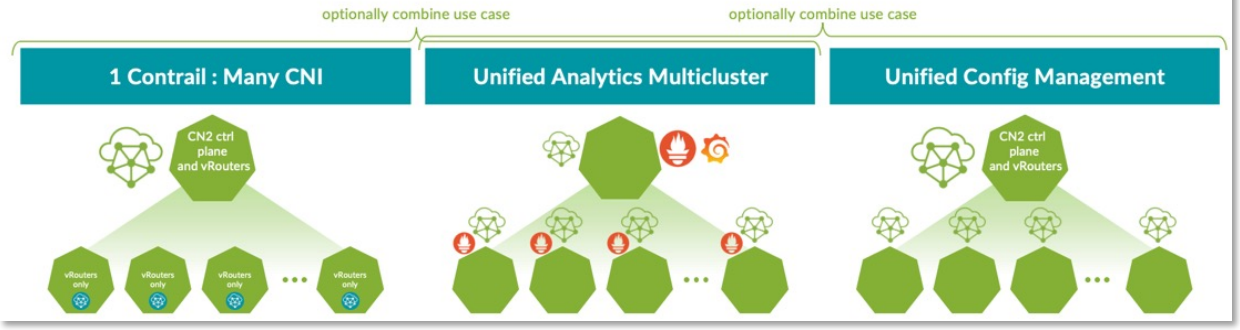
CN2のターゲットユースケース

・中大規模のk8sのネットワーク・セキュリティ課題を解決(大企業、事業者, サービス提供者 etc.)
・テレコクラウド、エッジクラウド、VNF/CNF, 5G RAN

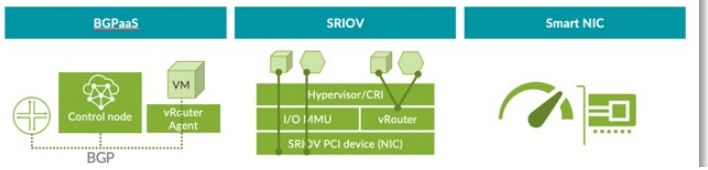
ユースケース: 拡大するシングルクラスターと集中/分散 GW



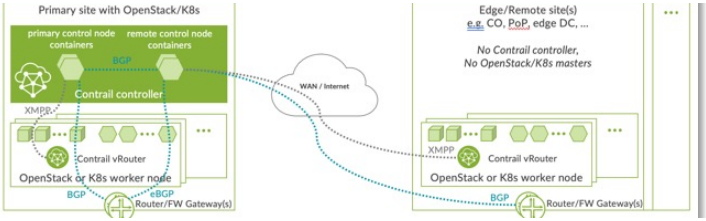
ユースケース: マルチクラスターの集中管理



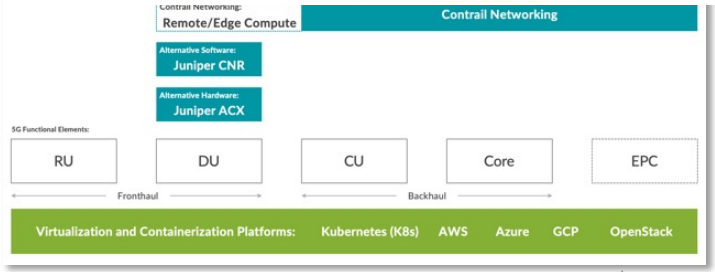
ユースケース: テレコクラウド



ユースケース: エッジクラウド/リモートノード

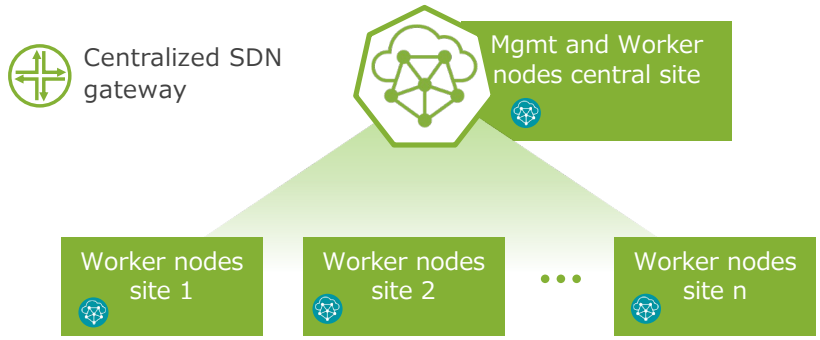


ユースケース: 5G RAN



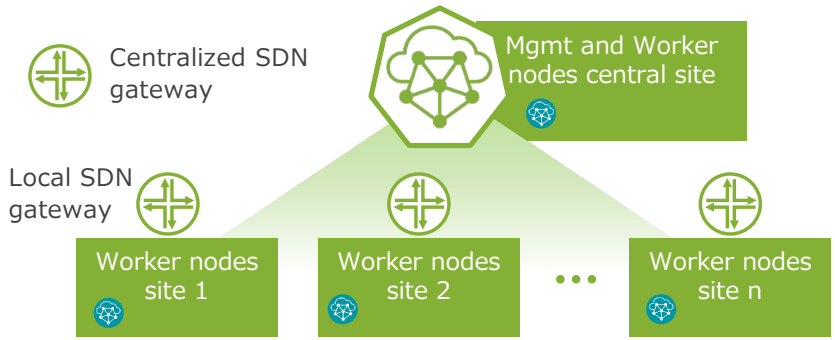
USE CASE: Wide-cluster - One Cluster, Multiple Sites

Stretched cluster and networking



- Central site runs K8s primary/mgmt nodes, etcd, Contrail controllers
- Distributed sites run K8s worker nodes only
- Central and distributed sites nodes all have vRouter
- No Contrail controller at remote site
- vRouter offers node-local gateway with underlay/fabric breakout too

Stretched cluster and local network gateway



- Each distributed site has its own local SDN gateway for ingress/egress into the overlay

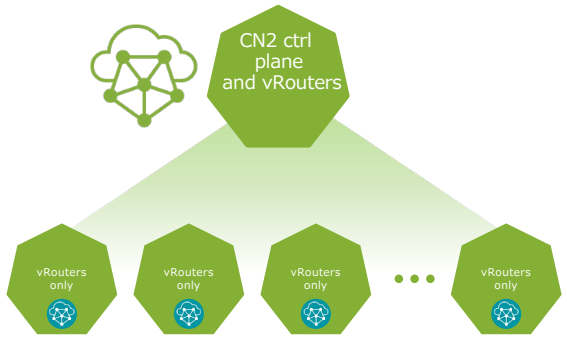
Next slide: Contrail's Remote/edge compute

USE CASE: Multi-cluster - Reduce and Wrangle K8s Sprawl

optionally combine use case

optionally combine use case

1 Contrail : Many CNI

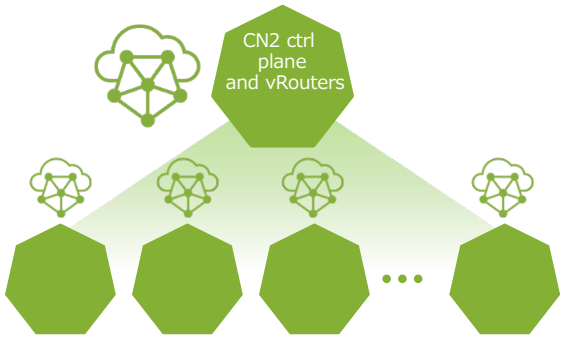


- Use one Contrail instance to serve as the CNI and load balancing for several K8s clusters and optionally an OpenStack cluster
- Reduces the number of Contrail controllers
- Lighter deployment for multicluster

Unified Analytics Multicluster

- Main cluster may or may not have workloads
- Federated Prometheus unifies telemetry and centralizes analytics through Grafana
- Main cluster uses Thanos and/or Cortex for analytics HA/storage and multi-tenant views
- Simplifies incident management, chatops, etc

Unified Config Management



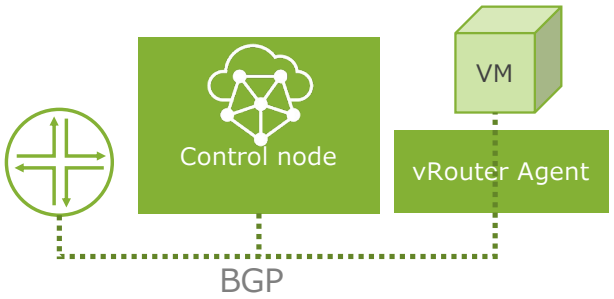
- Primary KubeFed cluster distributes all policy (Contrail included) to secondary clusters
- Unifies policy and control

Common across any deployment:

- Namespace RBAC/multitenancy improves cluster sharing
- BGP federation for extending network connectivity
- Lens GUI and K9s help with multicluster ops

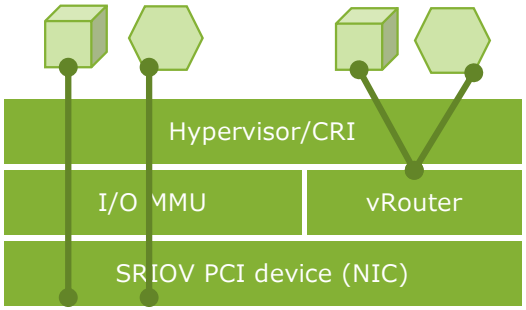
USE CASE: Telco Cloud 4G / 5G

BGPaaS



- Many telco VNFs are BGP speakers (e.g. 450 subinterfaces attached to a P-EGW instance)
- BGP speaker gets peered to Contrail controller/external peers to advertise routes
- vRouter agent accepts BGP connections from the VMs and proxy them to the control node

SRIOV



- SRIOV workloads can co-reside on the same server
- Multus+ Intel SRIOV plug-in in Kubernetes supports running with Contrail CNI
- CN2 interop with Apstra today; roadmap ‘22 automating Apstra with K8s SRIOV

apstra

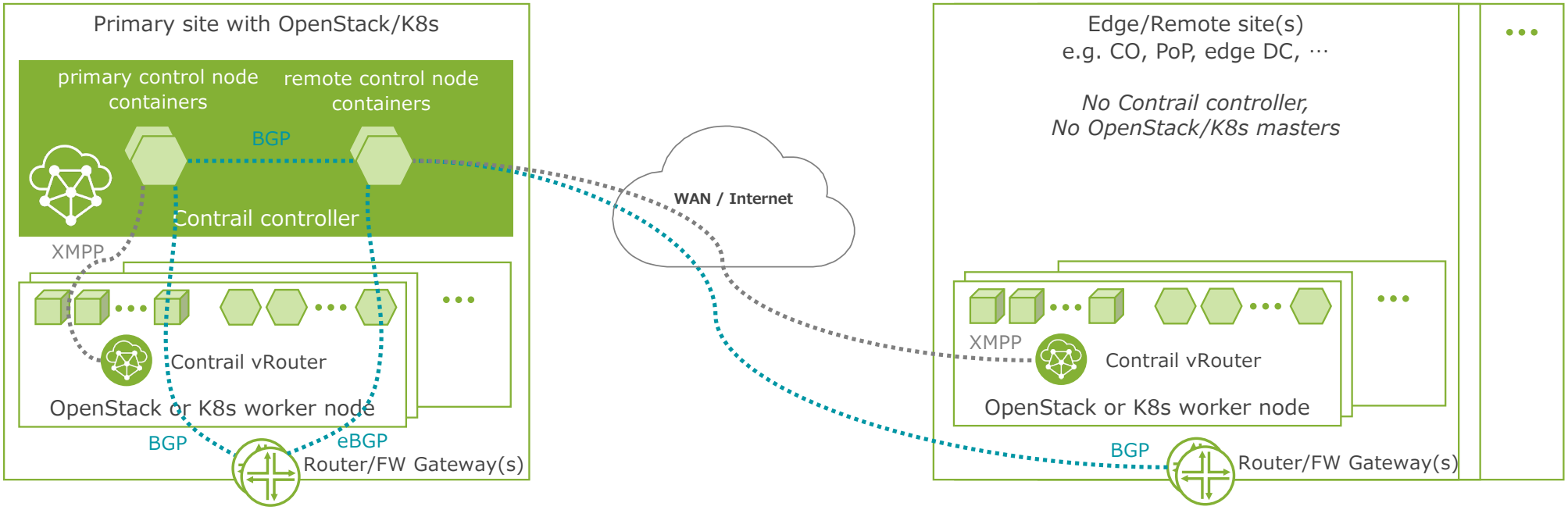
Smart NIC

- vRouter data plane offload support on
  - Mellanox / NVIDIA
  - Intel
  - Fungible (future)

Also frequently in use:

- Advanced networking (MAC learning, customer RTs, fat flows⋯)
- Service chaining
- DPDK data plane tested to 100Gbps

USE CASE: Edge Cloud / Remote Worker Nodes



- Workload orchestrator controllers and Contrail controller and their containers are distributed across several master/main nodes
- No primary site worker nodes are necessary (optional but shown)
- iBGP between control nodes and between their nodes and their site's gateway. eBGP between remote site's control nodes and main site's gateway

- Remote sites have a lighter footprint for worker/compute nodes only
- Remote sites do not have Contrail controllers nor workload orchestrators
- In primary site, only Contrail controller's "control nodes" are replicated per site: 2 remote control nodes per remote site

USE CASE: 5G RAN

- For clusters of one node containerized use JCNR
- For one node HW use ACX Series
- For 2+ node clusters use Contrail, with remote compute (no Contrail/K8s controller necessary)

- For larger clusters use Contrail with K8s
- Can interoperate/span SDN for K8s/OpenStack which is often the case for 5G/4G
- Contrail and K8s or OpenStack controllers here can manage remote/edge compute nodes and remote Contrail vRouters with local gateway

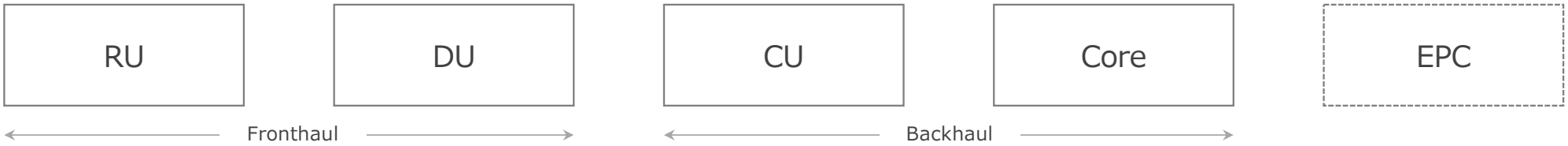
Contrail Networking:
Remote/Edge Compute

Contrail Networking

Alternative Software:
Juniper CNR

Alternative Hardware:
Juniper ACX

5G Functional Elements:



Virtualization and Containerization Platforms: Kubernetes (K8s) AWS Azure GCP OpenStack

Agenda

- 製品ポートフォリオとSDN
- Kubernetesによるマイクロサービス
- Contrailについて
- 各種機能紹介 (Feature list)
- ユースケース
- 必要スペックやライセンス

Supported Platform (22.1)

Contrail Networking Release		22.1
Orchestrator Platform		
Kubernetes	1.23.5	Ubuntu 20.04.3—Linux Kernel Version 5.4.0-97-generic Deployment Tool: Ansible
	1.22.3	Ubuntu 20.04.3—Linux Kernel Version 5.4.0-97-generic Deployment Tool: Ansible
Red Hat Openshift	4.8.39	RHEL CoreOS 4.8.39 — Linux 4.18.0-305.45.1.el8_4.x86_64 Deployment Tool: Redhat Openshift AI

System Requirement

Machine	CPU	RAM	Storage
Control Plane Nodes [1]	8	32 GB	400 GB
Worker Nodes[2]	4	16 GB	100 GB

CN2 LICENSING cloud-native / IaaS use cases

S-CN SKUs

License tiers (standard/advanced/premium; 1 is Contrail Networking without Contrail Pipelines; 2 is with Contrail Pipelines)

- **S-CN-S1-*** = standard tier, includes multi-tenant network overlays, service chaining for OpenStack or Kubernetes use cases, Insights
- **S-CN-A1-*** = advanced tier, adds DPDK and SmartNIC vRouter, BGPaaS, remote compute architecture
- **S-CN-P1-*** = premium tier, adds cRPD support with vRouter routing. cRPD sold separately
- **S-CN-S2-*** = S1 tier with Contrail Pipelines full CI/CD support and Contrail test suite
- **S-CN-A2-*** = A1 tier with Contrail Pipelines full CI/CD support and Contrail test suite
- **S-CN-P2-*** = P1 tier with Contrail Pipelines full CI/CD support and Contrail test suite

Class types (map to product integrations)

- **S-CN-*-C4-*** = Certified and integrated OpenStack (Red Hat RHOSP, Canonical/Juju)
- **S-CN-*-C3-*** = Red Hat OpenShift Operator integrated
- **S-CN-*-C2-*** = Pre-integrated K8s (Juju/Canonical, Rancher)
- **S-CN-*-C1-*** = Vanilla non-integrated or upstream Kubernetes. Integration may be self-tested with Contrail Pipelines tier

Duration terms

- **S-CN-*-C1-1** = 1 year of support and software subscription
- **S-CN-*-C1-3** = 3 years of support and software subscription
- **S-CN-*-C1-5** = 5 years of support and software subscription

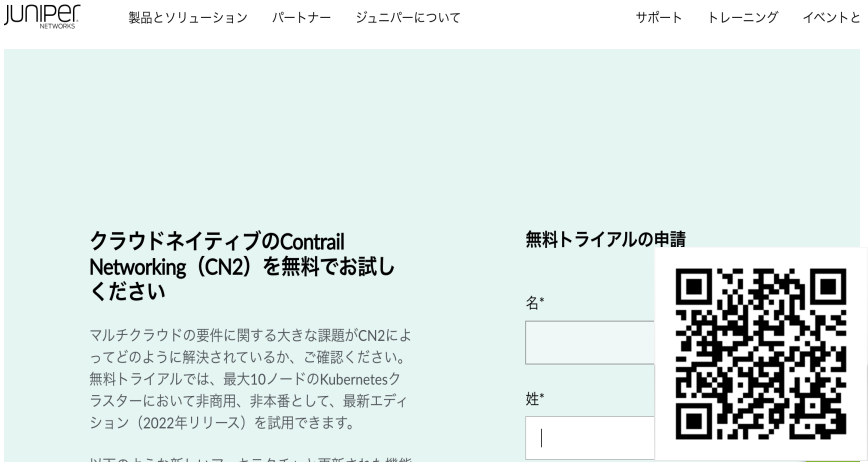
Examples *sold per vRouter compute node (controller node not licensed)*

- **S-CN-S1-C1-1** = standard tier license for 1 year for OpenStack
- **S-CN-S1-C2-5** = standard tier license for 5 years for for OpenShift
- **S-CN-S2-C2-5** = standard tier with Contrail Pipelines license for 5 years for for OpenShift
- **S-CN-A2-C3-1** = advanced tier with Contrail Pipelines license for 1 years Kubernetes integrations such as Canonical or Rancher
- **S-CN-A2-C4-1** = advanced tier with Contrail Pipelines license for 1 years Kubernetes integrations such as upstream K8s or Amazon EKS

Let’s Try CN2

Free Trial

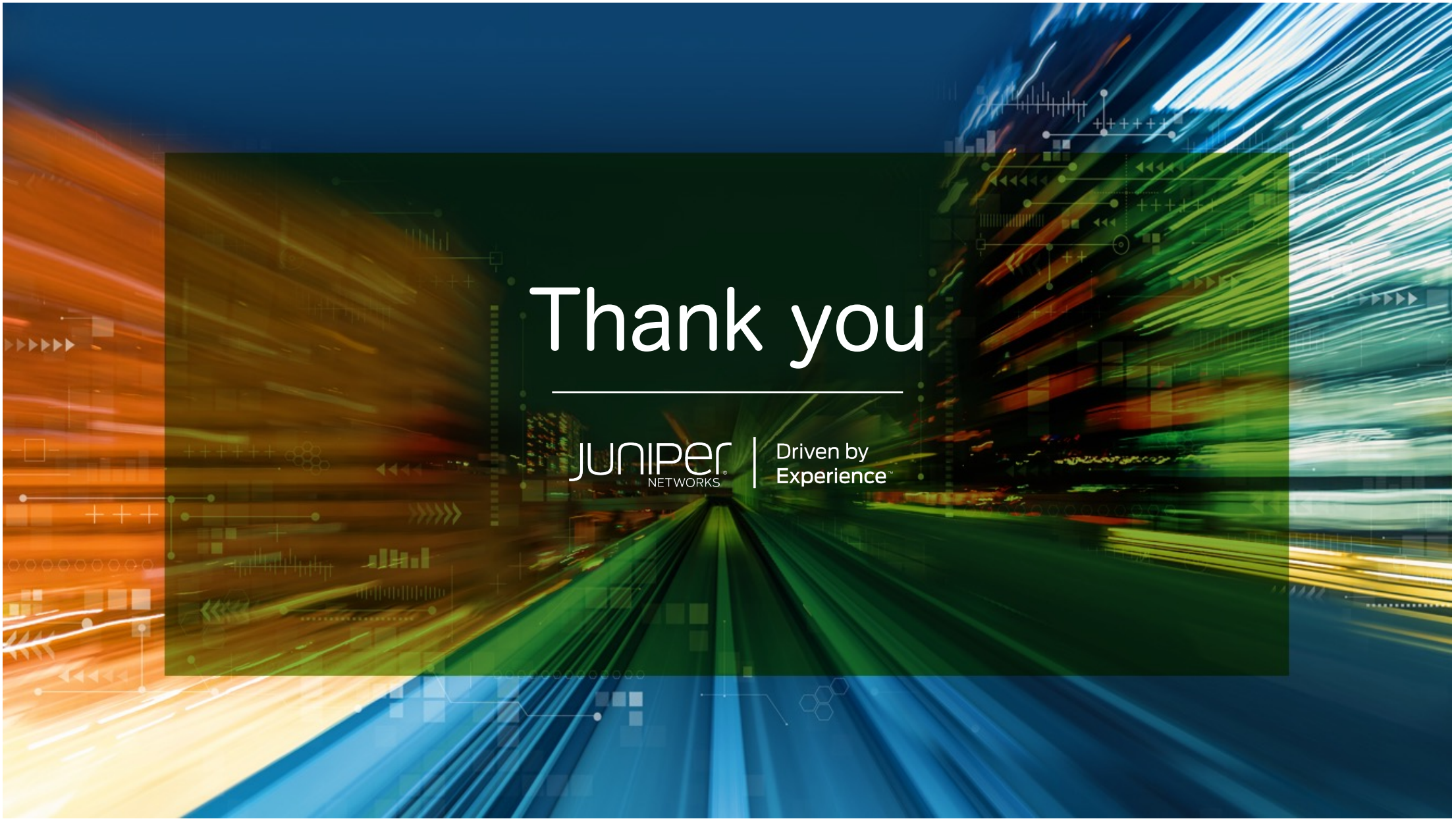
Minikube+CN2をMacBook上でトライアルも
https://www.juniper.net/jp/ja/forms/cn2-free-trial.html



Courseraオンデマンドトレーニング

現在は英語のみ/字幕あり
https://www.coursera.org/learn/juniper-contrail-networking

Minikube install guide
https://github.com/Juniper/contrail-networking/
User Guides, Install Guide, Support Platforms　※各ドキュメントは右側の言語選択で日本語表示可能
https://www.juniper.net/documentation/product/us/en/cloud-native-contrail-networking
※簡易ユーザーガイド(日本語)も作成・公開
https://www.juniper.net/jp/ja/local/solution-technical-information/software.html


Thank you
JUNIPER NETWORKS
Driven by Experience™