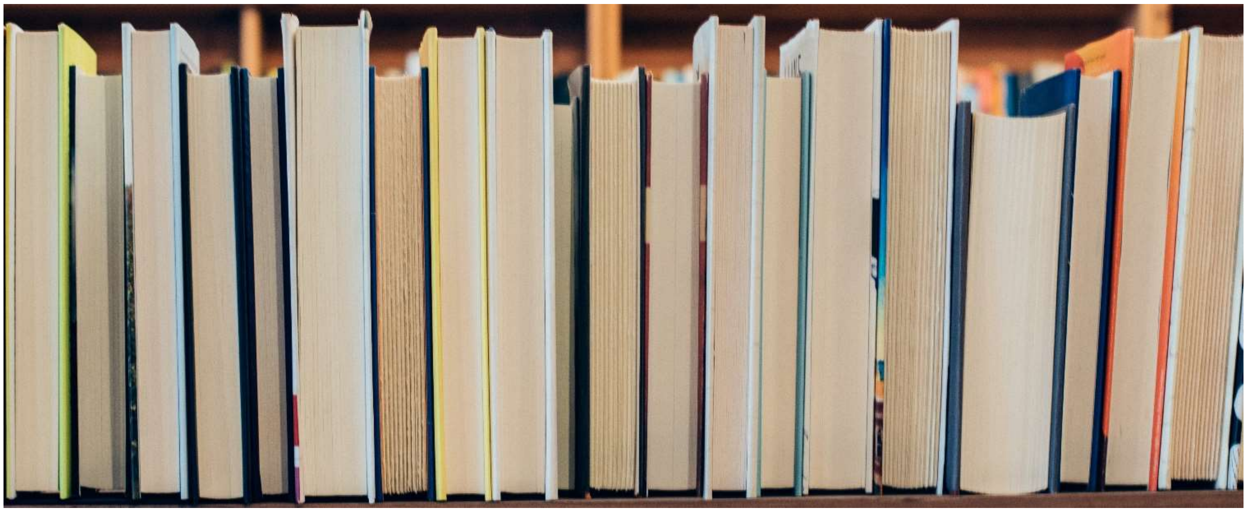
FAQ

Ensemble Virtualization Frequently Asked Questions (FAQ)



ADVA’s Ensemble virtualization suite comprises a portfolio of industry-leading components for supporting network functions virtualization (NFV), universal CPE (uCPE) and edge computing solutions. The portfolio is called ADVA Ensemble for Network Virtualization. The following frequently asked questions and associated answers provide an overview of the Ensemble virtualization platform and the associated benefits.

NFV primer, market drivers and key use cases

Q: What are NFV and SDN, and what is the difference?

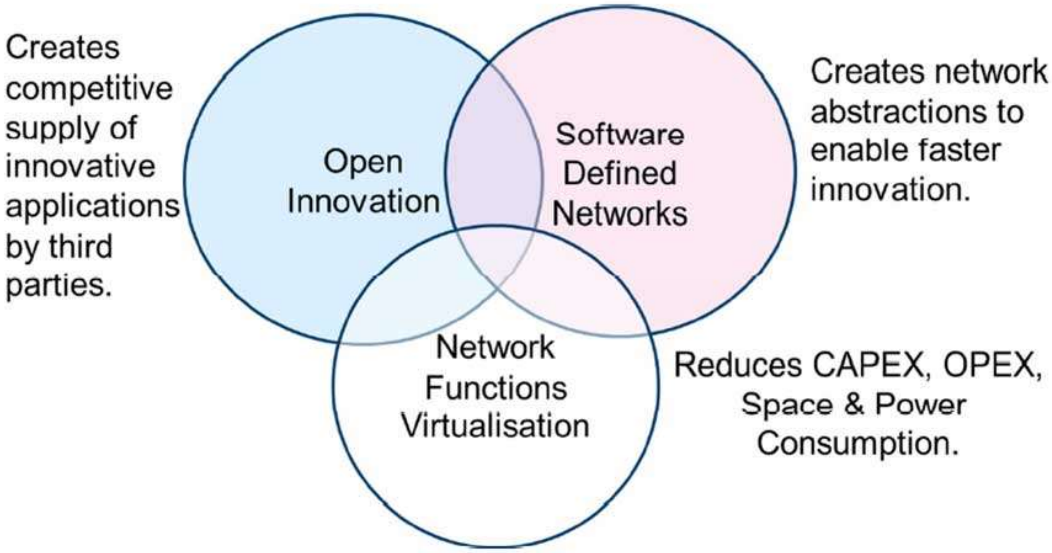
A: Software-defined networking (SDN) got its start on campus networks. As researchers were experimenting with new protocols, they were frustrated by the need to change the software in the network devices each time they wanted to try a new approach. As a result, they came up with the idea to make the network device behavior programmable, allowing them to be controlled by a central element. This led to a formalization of the principle elements that define SDN today:

- Separation of control and forwarding functions
- Centralization of control
- Ability to program the behavior of the network using well-defined interfaces

Network functions virtualization (NFV) is a means to enable telco operators to leverage the benefits of the cloud, including:

- Replacing closed appliances with software running on open, commercial-off-the-shelf (COTS) servers as shown below
- Reduction of capital expense (CAPEX), operating expense (OPEX), hardware footprint, and power
- Construction of services from interchangeable components provided by an ecosystem of hardware and software suppliers
- New commercial models including usage-based and shared-risk/shared-reward
- New methods of working such as agile development and DevOps

The original ETSI NFV white paper included this diagram showing the intersection of SDN and NFV:


Creates competitive supply of innovative applications by third parties.
Open Innovation
Software Defined Networks
Creates network abstractions to enable faster innovation.
Network Functions Virtualisation
Reduces CAPEX, OPEX, Space & Power Consumption.

More info:

- ETSI NFV white paper
- NFV and SDN: What's the Difference?
- NFV and SDN: What's the Difference Two Years Later?
- Cloudifying the Communications Network

Q: What are network appliances and why should I move away from them?

A: Network appliances typically include routers, firewalls, WAN Optimization and SD-WAN endpoints, Wi-Fi controllers, DPI devices, etc. An appliance is characterized by the tight integration between software features delivered on purpose-built hardware from a single supplier. As a result, network appliances are typically closed solutions, such that if a service provider wants to change between network application vendors, this requires changing out not only the software application vendor but expensive network appliance hardware as well. Additionally, most network appliance vendors will not allow service provides to run "foreign applications" on the device. This type of vendor lock-in encompasses all the attributes that operators are trying to move away from with the push for cloud-centric solutions.

More Info:

- Don't Use Hardware Appliances for SD-WAN
- Open hosting for virtualized SD-WAN
- Cloudifying the Communications Network

Q: What are "white boxes", and why do people want to use them?

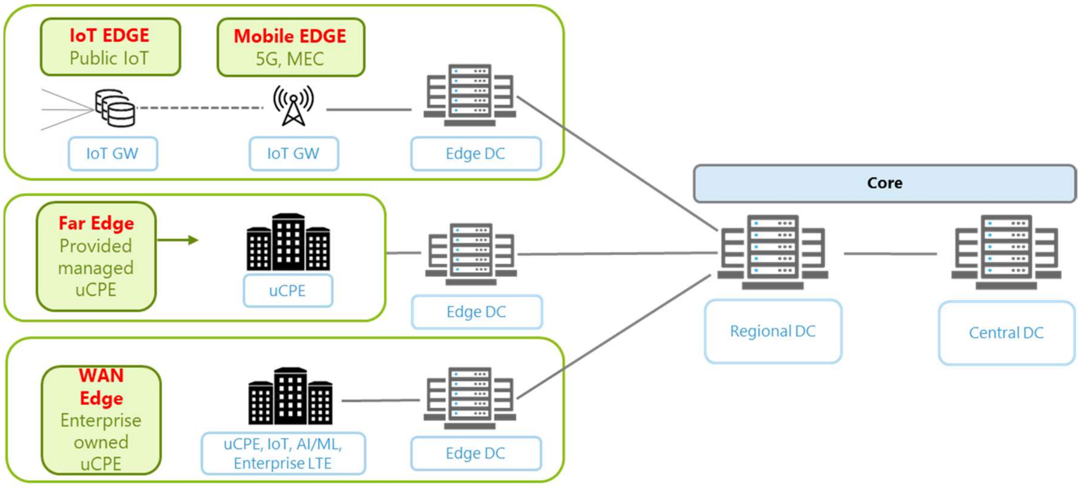
A: White box is a term that denotes a generic and open computing platform, offered by a wide variety of hardware manufacturers that can be used to run a wide variety of applications – networking or otherwise. One of the key benefits of using a white box is that the primary features of the hardware platform will be consistent across suppliers. White boxes are desirable for the following reasons:

- They decouple hardware from software, enabling best-of-breed choices in both
- They allow customers to deploy other enterprise applications in the same computing footprint as their telco services
- They enable operators to ride the broader hardware innovation curve
- They allow for choice in hardware suppliers enabling more price competition
- They simplify operations in locations that have onerous import restrictions by allowing for local procurement of compatible hardware platforms

Today, we are in the midst of a white box “super-cycle”. Functional disaggregation is the norm in the enterprise and the cloud, and we are now seeing the same thing happing in networking and communications – especially with the rise of the edge computing phenomena. It is anticipated that this disaggregation wave will dominate the networking and communications space for the next decade or more, supported by maturing hardware and software ecosystem. As the capabilities of the white box and software frameworks continue to evolve to support virtualization and containerized cloud native architectures, we will continue to see a wide range of networking capabilities are moving away from purpose-built appliances and onto white boxes operational models:

- White box server
- White box switching
- White box optical
- White box hybrid

These enabling technologies can be leveraged at various locations in the network – from the “far edge” or “WAN edge” at the customer premises, to the service provider edge where IoT, multi-access edge compute, and micro data center resources are deployed.



More info:

- What is Universal CPE?
- Understanding the Use of Universal CPE
- Why Service Providers Need Universal CPE (page 10)
- Universal Customer Premises Equipment

Q: What are the benefits of NFV to the end user?

A: End users may not care about NFV, but NFV-based services do bring them benefits. Here are some examples:

- NFV can provide consolidation of a stack of appliances down into one server. This saves space and power at the end user location.
- Sofware-centric services can be deployed in real-time, which gives end users control over their telecom services and faciliates reduced support costs and faster time to market/revenue for service providers.
- NFV allows services to be deployed on white box uCPE devices via zero-touch provisioning (ZTP) requiring little-to-no end user intervention. This go-to-market model enables the acceleration of service activation with local sourcing/sparing of servers and/or bring-your-own-device models. E.g. – services can be activated almost immediately rather than waiting for days or weeks.
- NFV facilitates moving from appliances to software, enabling new applications that were not previously possible. See "Q: What are the key use cases for Ensemble?" below for examples of new use cases being deployed today!

More info:

- Why Do Customers Care About NFV? (video)
- Software and Support Optimize SD-WAN for Enterprises

Q: Can NFV meet telco performance requirements?

A: Yes. With the aid of more efficient VNFs and optimized infrastructure like Ensemble Connector, operators can deploy virtualized systems that meet both performance and cost requirements.

Today, the Ensemble Connector datapath replaces standard Open vSwitch (OVS) and delivers improved throughput, latency and jitter leveraging data acceleration technologies such as DPDK and SR-IOV. Moving forward, we will be expanding our support for other acceleration technologies such as PCI Passthrough, multi-queue KVM and multi-core datapath. Additionally, Connector will support application level accelerators for thing such as encryption with the enablement of AES-NI (supported today) and QAT (roadmap feature).

More info:

- Open vSwitch is No Match for ADVA Ensemble Connector Performance
- Performance and Low Cost Enable NFV and SDN

Q: Is IT/network convergence realistic?

A: IT/network convergence is realistic; it is happening now, and NFV is the path. NFV was invented by service providers to bring the benefits of the cloud to the telco network. NFV is often characterized as being about replacing appliances with software running on COTS servers, but it is much more than that. Here's what operators are doing to fully realize the benefits of the cloud:

- They are moving from single-vendor solutions (whether appliances or single-vendor applications running bare metal) to multi-vendor systems.
- They are moving from static configurations to dynamically orchestrated virtual network functions (VNFs) and container network functions (CNFs) on standard NFV infrastructure, i.e. COTS server, Linux, KVM, OpenStack, Docker, Kubernetes, OpenShift, etc.
- They are embracing new methods of working, such as agile development and DevOps. This includes partnering with both suppliers and customers to accelerate development and deployment cycles.
- They are seeking to provide their customers with converged cloud/connectivity solutions. This requires virtualized networking and security solutions.
- They are looking to treat the network as a platform with fungible resources so as to enable a new class of dynamic services and new technologies such as 5G, edge compute, private tenant space hosting and IoT.
- They are looking to radically increase automation to reduce time to service and human errors, as well as to enable automatic resolution of most network failures.

The barriers and risks include:

- Acquiring the necessary IT and cloud computing skills within the service provider through training and/or hiring.
- Changing organizations to reflect the new realities of operation, i.e. breaking down internal silos.
- Building out new virtual infrastructure while maximizing the use of the existing network.
- Driving new revenues quickly to justify the capital outlay.

This migration is just getting underway, but operators see it as necessary to support their future strategies and more importantly, their end customers are now demanding these kinds of solutions. Embarking on this technology evolution will enable operators to move much more quickly, drive new services and cut costs. The risks are manageable given leadership and vision.

More Info:

- Staffing and Organizing for Telco Innovation – Part 1
- Staffing and Organizing for Telco Innovation – Part 2
- Staffing and Organizing for Telco Innovation – Part 3
- Network Modernization Means Operator Innovation (Page 10)
- Service Providers are Changing for the Cloud
- Network Virtualization Simplified
- Cloudburst (page 32)

Q: What are the key use cases for Ensemble?

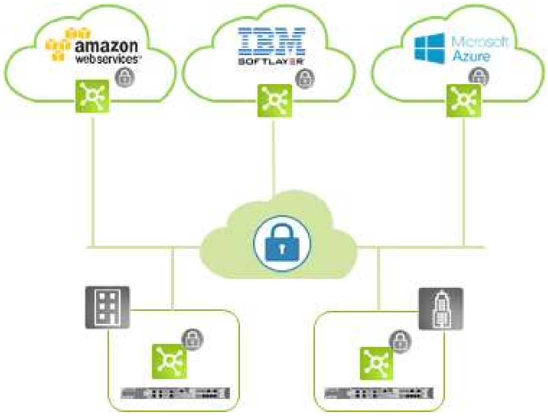
A: Here are some of the leading use cases:

Universal CPE (uCPE). With uCPE, service providers can realize the true value of NVF. They can replace a stack of network appliances with best of breed applications software running on a standard COTS server. Doing so accelerates service innovation and enables dynamic services for end users.

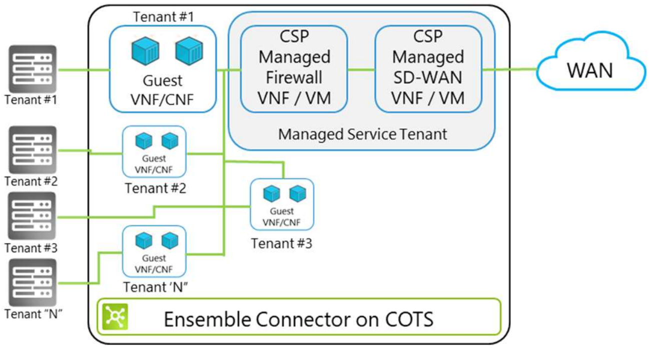
SD-WAN. Managed SD-WAN is a tremendous revenue opportunity for service providers. With Ensemble Connector, service providers can deploy software SD-WAN VNFs on COTS servers rather than old-fashioned closed appliances. With our integrated ZTP capabilities, we can deliver SD-WAN services to end customers with little to no end-user intervention ("power to packets"). And since the SD-WAN application is running as a VNF, the end customers have the flexibilty to swap out SD-WAN vendors or add additional functionality (like UTM firewall, WAN optimization, etc.) with the push of a button.

See "**Error! Reference source not found.**" below for more information.

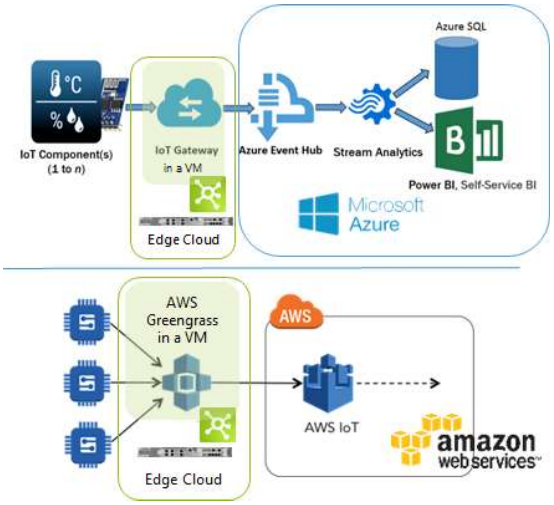
Secure cloud connectivity. The virtualization of network functions has many benefits, but the biggest is enabling applications that were not possible before. With secure cloud connectivity, the virtualization of encryption functions enables end-to-end security, all the way from the customer site to a public cloud provider. Doing so makes hybrid cloud applications secure and suitable for mission-critical applications.



Customer tenant applications and edge computing. One of the key benefits of NFV is the ability to deploy a variety of workloads onto standard, commodity COTS servers. Leveraging this, Ensemble provides the ability for service providers to enable new revenue opportunities by offering their enterprise customers managed micro-cloud services on the same uCPE COTS server (or compute cluster) as they are providing their managed networking services. In this scenario, enterprise customers can run any user managed IT workload in a dedicated VM or container "tenant space" on the uCPE device. In uCPE deployments, the tenant space application supports single customer tenant hosting applications that are integrated into the managed networking services.



This same concept can be extended to the service provider edge where multi-tenant "edge compute" infrastructure can be offered. In this case, private IT workloads from multiple end-customers can be hosted on a common NFV infrastructure platform – all while maintaining workload isolation and security. Ensemble provides options for how these enterprise managed applications can be networked into the service provider managed networking service chain as well as how these applications are managed either locally or via a provider owned customer portal.



Internet of Things (IoT). IoT is getting a lot of interest, and uCPE/edge computing is the perfect vehicle for delivery of IoT functionality to the edge of the network. Both managed IoT services and enterprise-owned deployments require deployment of an IoT gateway close to the managed devices.

The uCPE-hosted approach can benefit a wide variety of verticals, especially medical, industrial and energy applications.

ADVA Ensemble provides options for deploying and managing IoT gateways from leading supliers, whether running in a VM or in a container.

IT/OT convergence. Manufacturers have a tough job ensuring the safe and secure operation of their infrastructure. The task is complicated by an array of factors, from balancing cost to supporting emerging technologies. The Ensemble suite is the ultimate tool kit to help utilities address these challenges. Ensemble solutions enable advances in networking, operations and choice, bringing the power of the cloud to manufacturing.

Manufacturers currently deploy a variety of appliances to monitor and control their operations. These appliances are usually sold and serviced by a single supplier, creating vendor lock-in. Even worse, those solutions may be obsolescent or not available in all regions. Running each application on its own device drives excessive cost, power consumption and space. Finally, closed solutions are not conducive to support new innovations such as IoT or custom applications.

With Ensemble, manufacturers can achieve IT/OT convergence by hosting multiple applications on the same server, including:

- IoT: including gateways from AWS and Azure
- Networking: VPN, SD-WAN, MPLS VPNs, LTE and WSAN
- Security: encryption, IDS/IPS, firewall/UTM, SCADA and DDOS
- PaaS: custom or third-party applications

More Info:

- Verizon Adds Ensemble to Its Virtual Network Services uCPE Solution
- Verizon uCPE Case Study
- Universal Customer Premises Equipment
- Realizing the Value of NFV with Universal Customer Premises Equipment (uCPE) (webinar)
- Don’t Use Hardware Appliances for SD-WAN
- Open hosting for virtualized SD-WAN
- Orchestrated virtualized multi-vendor SD-WAN services
- Virtualised encryption: How it could be the killer app for NFV – and help with GDPR too
- Securing zero touch for uCPE deployments

- Using the Cloud to Secure the Cloud
- Security is a many-layered thing
- Meet Anna and the future of virtualized encryption in the cloud
- Ensemble solutions for utilities
- Ensemble solutions for manufacturing
- Ensemble solutions for satellite operators
- Ensemble solutions for retail and small/medium business

Q: Does Ensemble have an SD-WAN solution?

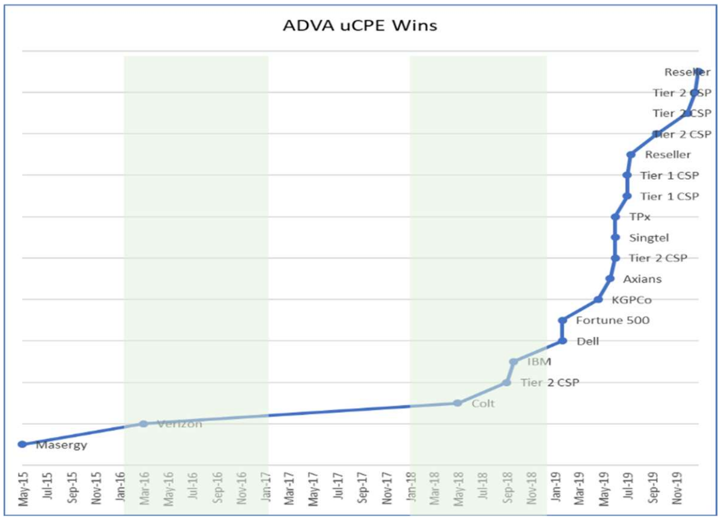
A: Yes, but not specifically a SD-WAN VNF. Ensemble Connector is an open virtualized networking platform for deploying and managing virtual SD-WAN and other NFV services at scale. The Ensemble Connector platform enables service providers to deploy any best-of-breed SD-WAN function as a software application, and do so in an automated and virtualized fashion, consistent with their forward-looking architectures. With this approach, service providers can deliver new and more flexible VPN and hybrid WAN services to their customers at a lower cost and with more features than today's service offerings. What's more, Ensemble Connector comes with a rich feature set for connecting off-net customers through the internet or wireless networks.

More Info:

- Don't Use Hardware Appliances for SD-WAN
- Open hosting for virtualized SD-WAN

Q: Does Ensemble have live deployments?

A: Yes. The NFV/uCPE market has passed through the "trough" of the hype cycle and we are seeing significant traction in service provider adoption of uCPE solutions. As a matter of fact, NFV/uCPE solutions are asked for by name in half of enterprise RFPs to service providers. The figure below shows the rate at which ADVA is winning new NFV business. Clearly, ADVA's Ensemble suiteis the market winner – delivering the right product at the right point in the cycle.



More Info:

Verizon

- No Shortcuts to NFV Success
- Verizon Adds Ensemble to Its Virtual Network Services uCPE Solution
- Verizon uCPE Case Study
- The Real Innovators of Networking: Chad Thompson, Verizon

- Realizing the Value of NFV with Universal Customer Premises Equipment (uCPE) (webinar)

Colt

- Colt builds new global uCPE solution on Ensemble Connector
- uCPE: Revolutionising the Network Edge with Colt (webinar)
- Speed, Economy and Efficiency: Advantages of uCPE for Service Delivery (webinar)

TPX

- TPx Selects ADVA for Edge Device Innovation

Dell

- Dell EMC Puts the "U" in Universal Customer Premises Equipment at the Network Edge
- ADVA and Dell EMC deliver open uCPE solution

IBM

- IBM Agile Lifecycle Manager and ADVA universal CPE

Masergy

- The Real CTOs of NFV: Tim Naramore, Masergy
- Real-World NFV, Real Lessons Learned

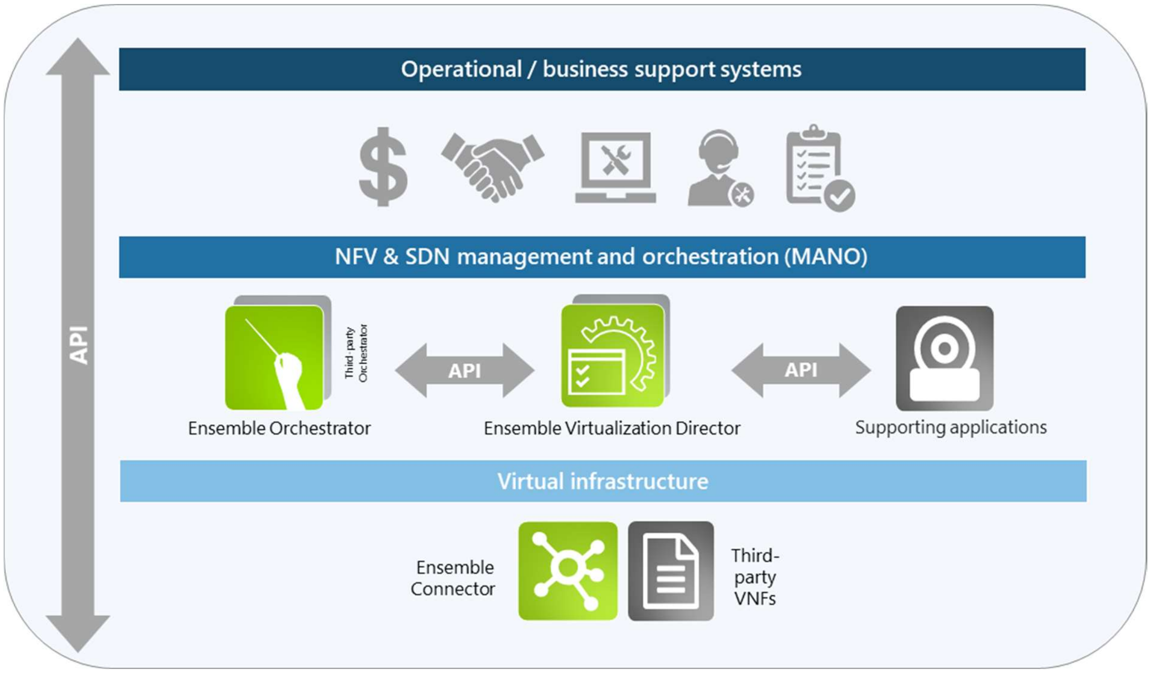
DartPoints

- The Real CTOs of NFV: Satya Baddipudi, DartPoints
- Bringing the Cloud to a Business Near You

ADVA Ensemble virtualization architecture and components

Q: What products comprise the Ensemble for Network Virtualization portfolio?

A: The Ensemble virtualization software portfolio enables service providers and enterprises to realize the benefits of the cloud by replacing closed appliances with their choice of software that can be hosted anywhere in the network on their choice of open hardware. The Ensemble software portfolio is made up of three distinct product components – Ensemble Connector, Ensemble Orchestrator and Ensemble Virtualization Director. The high-level architecture of these three components is shown in the figure below.



The Ensemble components are designed to work together using open and standard application programming interfaces (APIs). However, the solution has also been designed to be functionally decomposable enabling each of the components to be deployed separately, allowing service providers to integrate various Ensemble components with best of breed orchestration or management tools. This openness and deployment flexibility allows service providers to take advangage of key Ensemble benefits while still leveraging a best-of-breed multi-vendor environment. In short, Ensemble enables choice in:

Hardware suppliers

- White box, gray box, branded
- Compute, memory, networking and storage
- Features (hardware accelerators, redundancy, networking, wireless connectivity, etc.)

Software suppliers

- “App store model” provides ability to change application suppliers as needed to support business requirements (features, cost, etc.)

Deployment location

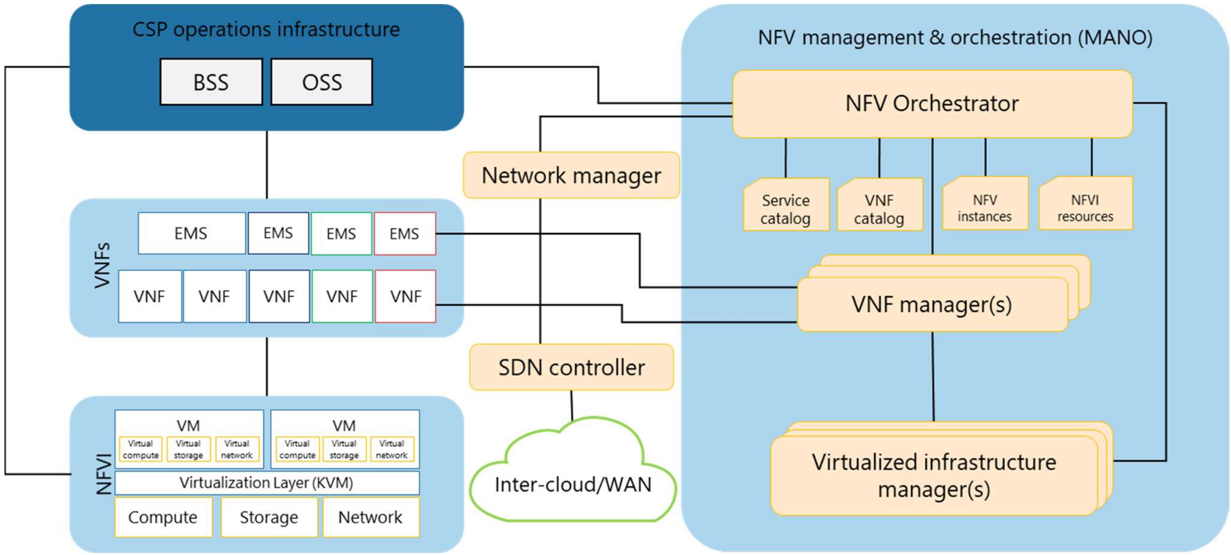
- Public cloud / data center / central office / edge cloud
- Customer premises
- Any combination of the above

More info:

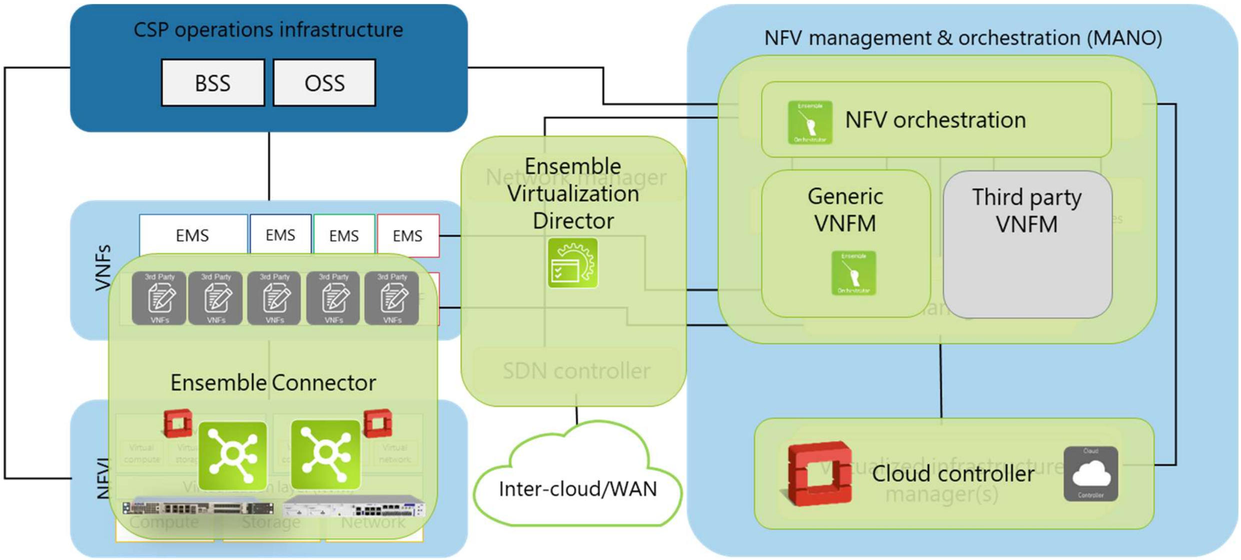
- Network virtualization overview page
- Ensemble Explained (video)
- Ensemble Connector – NFV Infrastructure (NFVI) operating system and VNF hosting platform
- Ensemble Orchestrator - ETSI MANO NFV orchestrator and VNF manager
- Ensemble Virtualization Director – NFVI management and operations system, and SDN Controller
- Ensemble Harmony Ecosystem – Partner program for NFV hardware, software, and services suppliers

Q: How do the Ensemble components fit into the ETSI NFV architecture?

A: The first diagram below shows the generic ETSI NFV reference architecture.



The second diagram below overlays the Ensemble solution components (green shaded boxes) on top of the ETSI NFV architecture. Ensemble provides functionality that supports key management and orchestration features, the virtual infrastructure manager (cloud manager) and virtualization hosting layer running on the NFV infrastructure.



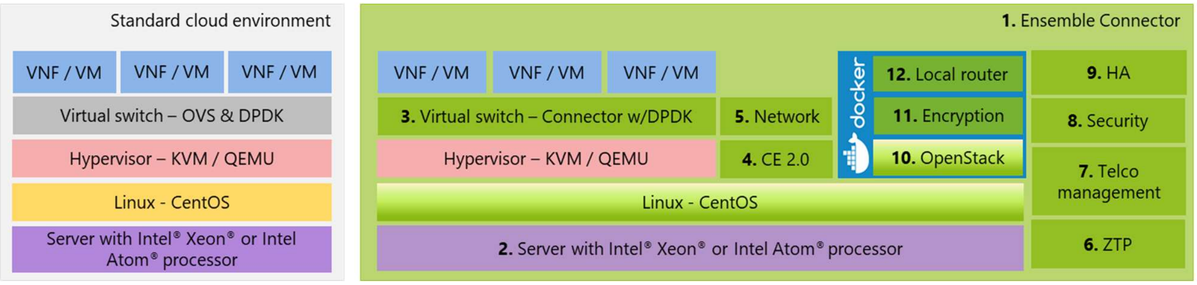
Q: What is Ensemble Connector?

A: The award-winning Ensemble Connector delivers the industry's first and most advanced pure-play virtualization platform designed to simplify the deployment and management of uCPE and edge computing solutions. Ensemble Connector is an open software framework running on standard COTS servers and providing a scalable, high-performance network operating system. It is capable of hosting a wide array of third party VNFs and CNFs, which enable the service provider to offer a wide array of new revenue generating services.

Ensemble Connector includes standard NFV infrastructure (NFVI) components such as Linux, KVM, Docker, and OpenStack. It runs on standard COTS servers as well as on ADVA's enhanced server platforms, including the FSP 150 ProVMe and XG304u.

A high-level block diagram of Ensemble Connector is shown below.

1. Integrated OS with open interfaces
2. Choice of NFVI hardware platforms
3. Accelerated vSwitch
4. Carrier Ethernet 2.0
5. Embedded L3 Networking incl. LTE
6. Zero touch provisioning (ZTP)
7. Telco management
8. Platform security
9. High availability
10. Embedded cloud (OpenStack)
11. Encryption engine
12. Local router



More info:

- Ensemble Connector product page
- Ensemble Connector data sheet
- Ensemble Connector Explained (video)

Q: What are the benefits of Ensemble Connector?

A: Ensemble Connector improves on a standard NFVI platform (such as stock Linux and OpenStack) with the following features, as shown below:

1. **Improved virtual switching –** Ensemble Connector's forwarding performance delivers improved throughput, latency and jitter when compared with open vSwitch (OVS).
2. **Virtualized Carrier Ethernet 2.0 (CE 2.0) –** Ensemble Connector provides standard CE 2.0 functions in software. This enables a single COTS server to host not only standard VNFs, but also to present a CE 2.0 UNI on any of the server's Ethernet ports thereby eliminating the need for an external NID.
3. **Improved networking –** Ensemble Connector can support a variety of advanced networking applications at Layer 2 or 3, including support for LTE access.
4. **Zero touch provisioning (ZTP)** – With Ensemble Connector, service providers can ship an un-configured server to a customer site and then provision it securely without a technician. This includes both the NFVI network operating system as well as the VNFs and associated service chains.

Embedded cloud – Embedded cloud places a self-contained OpenStack cloud on the edge node, enabling cloud-native deployments without the issues created by separating the OpenStack controller from its agents. See '

5. Q: What is embedded cloud aka "cloud in a box?"' for more info.
6. **Integrated OS with open interfaces** – Ensemble Connector provides a unified platform with open, standard APIs (REST & NETCONF) to facilitate simplify deployment of 3rd party VNFs as well as integration with northbound management platforms, including MANO and OSS/BSS.
7. **Device scalability** – Ensemble Connector supports a wide array of standard COTS servers, ranging from low-cost Intel® Atom®-based devices all the way up to multi-socket Intel® Xeon® blade servers.
8. **Telco management –** Ensemble Connector provides sophisticated deployment features such as automated ZTP, embedded cloud, NETCONF/YANG, Ansible, REST, SNMP, SSH, Y.1731, TWAMP, etc.
9. **High availability (HA) –** Ensemble Connector provides intrinsic HA features such as dual home routing and micro-cloud with multiple servers. It can also host VNFs with HA features such as HSRP or VRRP.
10. **Security** – Ensemble Connector provides for security at multiple levels: commissioning, virtualization, management, and user connections.
11. **Encryption** – Ensemble Encryption delivers robust, low-cost, software-based network protection, giving customers fully-secured cloud access with none of the performance issues of IPSec and with the ability to address Layer 2, 3, and 4 connectivity.
12. **Local router** – In addition to the Layer 2/Carrier Ethernet functionality embedded in Ensemble Connector's datapath, it also supports advanced Layer 3 options that provide additional flexibility for deploying Ensemble Connector into a wide variety of access networking configurations.

For more information on these benefits, please see the Key Ensemble Features section below.

Q: What is Ensemble Orchestrator?

A: Our award-winning Ensemble Orchestrator provides a scalable and economical solution for NFV orchestration. Ensemble Orchestrator is compliant with the ETSI NFV MANO architecture, and it provides both an NFV orchestrator (NFVO) and a generic VNF manager (VNFM).

Automated service creation

Our Ensemble Orchestrator helps providers and operators achieve greater profitability through policy-driven automation for quick and reliable service creation, activation, and assurance.

Single-point management

Ensemble Orchestrator provides a single point of entry for end-to-end network service and VNF lifecycle management. It handles VNF onboarding, service design, service deployment and VNF/service operations and management.

Seamless integration

Ensemble Orchestrator features cloud management, service orchestration, and networking capabilities as well as seamless operation across the various existing IP and virtual networks when integrated with our Ensemble Virtualization Director.

Ensemble Orchestrator is feature rich:

- Full lifecycle management including VNF onboarding, service design, service deployment, as well as VNF/service operations and generic/vendor-provided VNF management
- Powerful service editing capability providing ability to dynamically change deployed NFV services while minimizing impact to the end customer
- Service designer GUI and APIs for building NFV services
- Day-0 and Day-N configuration for VNFs including support for integration with VNF managers
- Dynamic tracking of cloud resources and advanced VNF placement algorithms
- Supports cross-cloud VNF service chaining
- Multi-tenancy and per-tenant quota management
- Scalable and highly available architecture

More info:

- Ensemble Orchestrator product page
- Ensemble Orchestrator data sheet
- Ensemble Orchestrator Explained (video):
- NFV orchestration demands openness and flexibility
- Orchestration for NFV Needs Scale and Resiliency
- Making MANO Easy

Q: What is Ensemble Virtualization Director?

A: Ensemble Virtualization Director provides a single pane of glass for managing NFV operations. Ensemble Virtualization Director provides a multi-layer architecture that delivers:

Core components

- Fault management
- Performance monitoring
- Security
- Provisioning
- Inventory
- Nodal discovery
- Topology discovery

Services

- uCPE device provisioning
- Service topology visibility
- End-to-end service management
- Service troubleshooting
  - Service fault monitoring
  - Service assurance
- Telemetry integration

Application Extensions

- Open API architecture
- Custom and third-party applications

Ensemble Virtualization Director hosts native and third-party, multi-layer network and service management applications. It features an open, extensible, YANG-based, model-driven architecture providing a software framework that supports custom application development in Scala/Java and Python.

Ensemble Virtualization Director features industry standard interfaces, including web, CLI, SNMP, CSV, REST, NETCONF, and RESTconf.

More info:

- Ensemble Director Explained (video)

Q: What are the benefits of the Ensemble management and orchestration products?

A: Ensemble Orchestrator and Ensemble Virtualization Director provide a perfect option for customers looking for a packaged end-to-end NFV solution. The Ensemble MANO products offer numerous benefits, including:

- ZTP automation platform
  - Versatile enough to handle single cloud, multi-cloud automated NFV service turn up
  - Supports integration with third party orchestration systems
  - Supports easy integration with VNF managers for building VNF Day-1 configurations
- NFV Service Designer UI
- Build NFV service and configure VNF service-chaining
- Rich set of VNF onboarding options
- Integrated view of both NFVI (hardware and platform) and VNF fault/performance data

- Built-in troubleshooting tools and service visualization

Q: What is the Ensemble Harmony Ecosystem?

A: ADVA's ecosystem of hardware and software vendors along with technology and services partners who are focusing on accelerating automation and virtualization initiatives at the telco edge and the customer premises.

We believe the success of NFV is built around a strong and open ecosystem of partners. Service providers are quickly moving out of the proof of concept stage and into live deployments and as a result, the list of hardware platforms and 3rd party VNFs that need to be supported continues to grow each day.

The Ensemble Harmony partner program is a pillar of the open environment. We believe this is essential for the realization of software-defined services. It enables service providers to select best-of-breed components and avoid single vendor proprietary systems, while also decreasing their project risks and accelerating deployments.

More info:

- Ensemble Harmony Ecosystem web page
- Ensemble Harmony Ecosystem Explained (video)

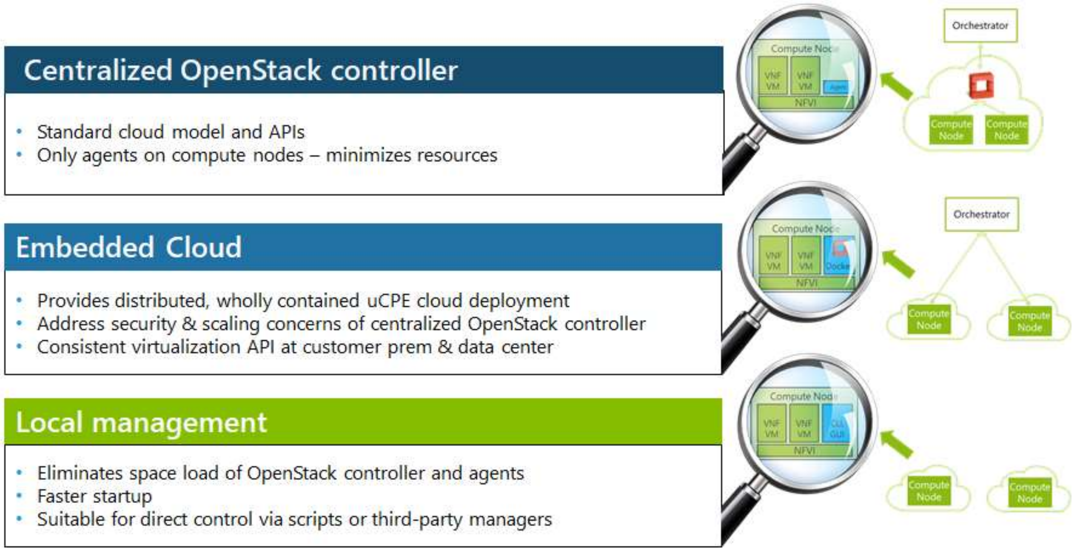
Key Ensemble features and benefits

Q: What is embedded cloud aka "cloud in a box?"

A: Operators see many benefits to NFV. In short, the goal is to bring the advantages of the cloud to telco operators. One of the big benefits is the wide array of available support software, including Linux, kernel-based virtual machine (KVM), Open vSwitch and OpenStack. These software packages provide a base of well-known functionality upon which operators can build innovative new virtualized services.

However, the telco network is not the same as the data center, so cloud-centric solutions may not transfer directly. Operators are concerned about OpenStack regarding its scalability and resiliency. How do we enable virtualized services to be deployed at scale when using OpenStack?

One way is to move from a centralized mode to a distributed mode. In a distributed mode, each compute node has an instance of OpenStack controller creating a "cloud in a box" as shown below. In addition, Ensemble also supports centralized and standalone models.



Centralized OpenStack controller

- Standard cloud model and APIs
- Only agents on compute nodes – minimizes resources

Embedded Cloud

- Provides distributed, wholly contained uCPE cloud deployment
- Address security & scaling concerns of centralized OpenStack controller
- Consistent virtualization API at customer prem & data center

Local management

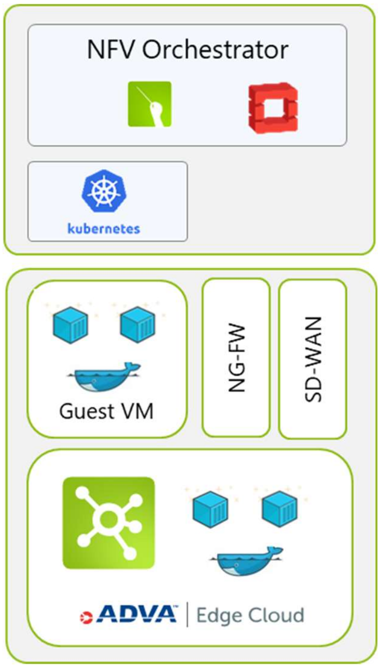
- Eliminates space load of OpenStack controller and agents
- Faster startup
- Suitable for direct control via scripts or third-party managers

In the case of Ensemble Connector, we run the OpenStack controller in a Docker container and can limit its footprint to a fraction of a CPU core, if required.

More info:

- Can Cloud in a Box Address OpenStack Issues?
- What Is Cloud in a Box? (video)

Q: Does Ensemble Connector support containers?



A: Yes. Container operation is supported today, and Ensemble Connector provides the ability to integrate containers with existing VNFs.

Ensemble Connector supports two different container operational models:

- Native container applications hosted within Connector
- Guest containers hosted by a VM running on Connector

Native containers offer all the value of reduced footprint, but they required Linux kernel alignment with Connector and possibly other functions that share the same container. In contrast, guest containers are hosted in a guest VM that supports multiple containers operating in one host OS. In the guest container model, the resulting sandbox offers greater security and flexibility for container selection.

Regardless of the container operational model selected, both can be service chained with each other and with traditional VNFs, and orchestrated with OpenStack or Kubernetes

Q: What sort of networking is available as part of the base Ensemble Connector operating system?

A: Ensemble Connector provide a datapath application that is responsible for all physical network interfaces on the NFVI device. The datapath can process data from all interfaces at line rates. To ensure that flows to VNFs are within specified limits, a variety of tunneling and overlay options support traffic shaping for Layer 2 and Layer 3 traffic. The system shapes traffic by either of these methods:

- Virtual machine managing the interface, the preferred solution
- Networking services within the Ensemble datapath

Layer 2 Traffic

The basic Layer 2 forwarding construct in Connector is called a service. As Connector receives traffic, it classifies the traffic using a set of rules and segments that traffic into streams that belong to the service. The basic service types supported include:

- **E-Line service** – is a point-to-point Ethernet service that connects two interfaces so that all packets that ingress on either interface transfer directly to the other interface.
- **E-LAN service** – is a point-to-multi-point Ethernet service where a virtual learning Layer 2 bridge governs forwarding among the ports. E-LAN services can have two or more service ports connected to the bridge.
- **E-Tree service** – is a rooted multi-point service that connects several UNIs, and which provides sites with hub and spoke multi-point connectivity. Each UNI is either a designated root or a designated leaf. A root UNI can communicate with other root UNIs or any leaf UNI. A leaf UNI can only communicate with a root UNI.
- **E-Flow service** – provides three service ports where each port is designated either as root, VNF, or Connector using the service port attribute settings. The root service port is the WAN, the VNF service port leads to the VNF service chain and is thus a vport, and the Connector service port is typically an IP

interface that is part of a VRF. The three service port attributes indicate the function of the service port and affect the handling of packets.

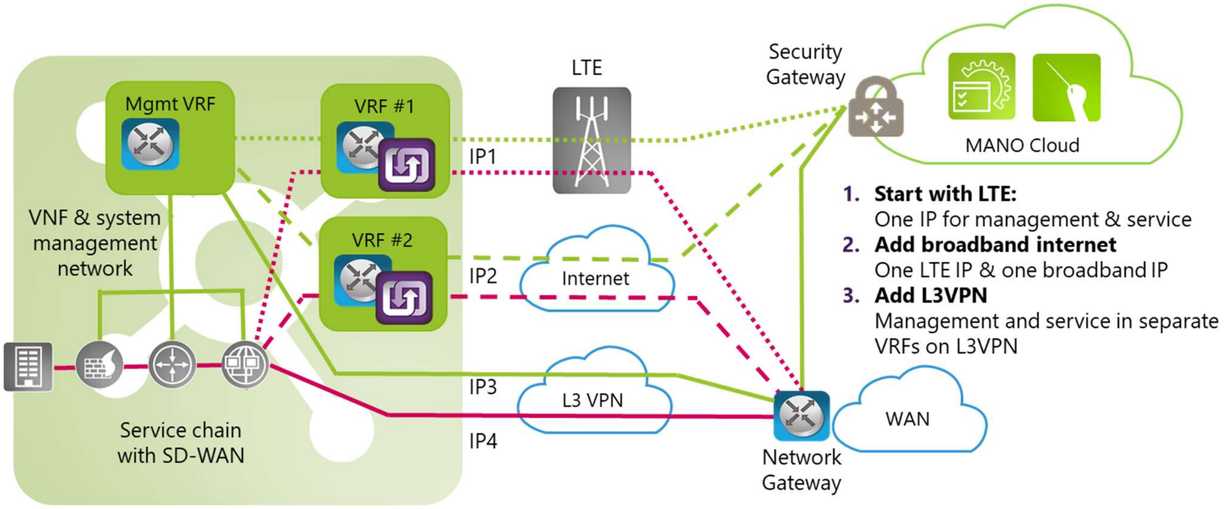
Layer 3 Traffic

Connector supports Layer 3 packet forwarding through VRFs. Similar to the Layer 2 service model, Connector can contain many VRF instances, each of which is a unique and independent forwarding entity that uses independent route and ARP tables. You control the interfaces through which packets ingress or egress the VRF by explicitly configuring those interfaces as a member of a specific VRF. The VRF accepts packets and forwards them based on the routing table as configured and updated by dynamic routing protocols such as BGP.

After the VRF accepts the packets, it further verifies the Layer 3 destination addresses. If the Layer 3 destination, for example, is an IP destination address and matches any of the IP addresses configured in the VRF, Connector recognizes the packet as addressed to the VRF as an end station. In that case the packet processing by higher layer protocols occurs locally. These higher-level protocols can include matching to tunnel interfaces in the VRF (matching protocol, tunnel ID, and so on), ICMP handling, or other higher layer protocols configured or operating within that VRF instance context.

For those packets with a destination address that does not match any addresses in the VRF, the VRF forwards the packets according to the VRF route table. The route table lookup results in an egress interface and possibly an explicit next-hop IP address. The software then uses the next-hop address and the VRF ARP table to construct the Layer 2 header. The software then applies the header to the packet prior to forwarding it to the egress interface.

Ensemble Connector also provides an integrated Network Address and Port Translation (NAPT) and DHCP server within a VRF context. A single interface within the VRF can act as the NAT boundary. You can use the integrated DHCP server to provision IP addresses for attached clients. You can use the NAT and DHCP functions together or separately.



1. **Start with LTE:**
   One IP for management & service
2. **Add broadband internet**
   One LTE IP & one broadband IP
3. **Add L3VPN**
   Management and service in separate VRFs on L3VPN

Q: What capabilities are available as part of the Ensemble Connector local router feature?

A: The Local Router feature provides customers with the following key capabilities:

- VRFs managed under Connector API umbrella
- Integrated with Connector OS
- Requires no additional cores
- Scale (per Connector)
  - 100 VRFs
  - 50 L2/L3 VPNs
  - 42 IPsec VPNs
  - 1 BGP instance
  - 16 BGP peers

<u>Routing Rules</u>

- Static
- BGP

<u>Tunnels</u>

- L3VPN
- L2VPN
- IPsec
- IPv4inv6

<u>Protocols</u>

- NAT, NAT-T
- DHCP client
- DHCP server
- IP Pass-through

<u>Network Resiliency</u>

- Hybrid WAN Failover

Customers will need to enable the Local Router Feature when they want to support any of the following networking capabilities:

- Any tunneled solution (L2VP, L3VPN, IPsec, IPv4inv6)
- Hybrid WAN Failover
- Any VRF for the data path

Q: What is IP Pass-through and what benefits does it provide within the local router feature?

A: IP pass through provides the ability to share a single public IP address with both Ensemble Connector management and a VNF service chain. To set up an IP pass through service, you must use the E-Flow Layer 2 service type. Connector management applications can then run using the same WAN port and public IP address that the VNF chain uses. By using the E-Flow type service, selected

Connector traffic is redirected from the WAN port to Connector management. All other traffic is directed to the VNF service chain. The VNF can then implement NAT, IPSec, routing protocols, and other applications, which are unknown to Ensemble Connector.

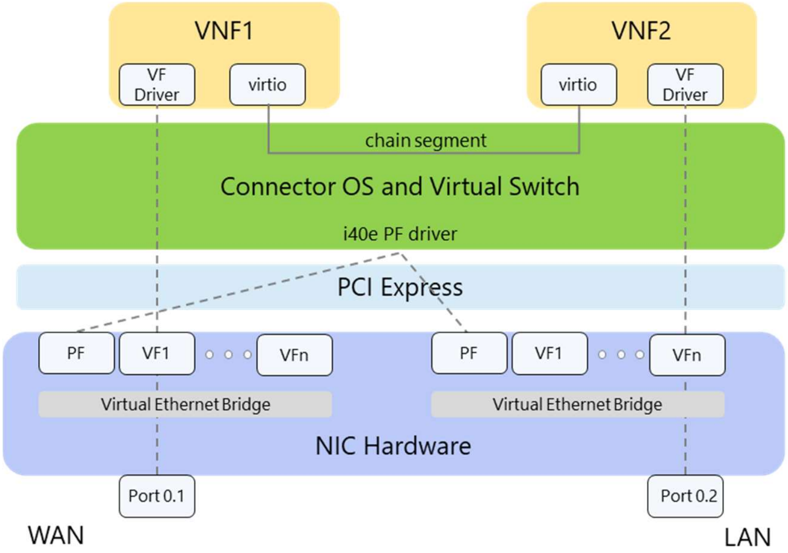
An access control list (ACL) and an exact-match hash table identify the packet's process flow based on its ingress port and Layer 2, 3, and 4 header fields. These fields include network prefixes and Layer 4 port ranges.

<u>Benefits</u>

- IP Pass-through eliminates NAT processing of SD-WAN traffic and enables direct SD-WAN client-client traffic flows
- Because NAT is no longer required, it allows line rate traffic throughput of SD-WAN traffic while still sharing single WAN
- IP Pass-through also enables use cases with dedicated servers (i.e., mail, web) behind Connector because they can now be reached from the public side at known IP/port addresses.

Q: How does Ensemble Connector provide SR-IOV support?

A: SR-IOV provides a mechanism to transfer user traffic directly between appropriately enabled NICs and the VNF through the server PCIE bus. The benefit of SR-IOV is that end-to-end service chain bandwidth can be increased without increasing CPU or RAM footprint requirements for the Ensemble Connector datapath.



It is important to know that the Ensemble Connector vSwitch datapath is bypassed on the traffic segments that use SR-IOV. In that case, Ensemble Connector datapath features such as local router, IP Pass-through, etc. will not be available on those interfaces

Connector implements a physical function (PF) driver that is associated with a set of properly enabled SR-IOV NICs. NIC PF compatibility is assured through ADVA verification of Connector on the documented NIC firmware. The VNF must implement the appropriate virtual function (VF) driver to speak directly to the NIC. NIC PF compatibility guidance are the responsibility of the VNF supplier.

The following hardware and drivers are supported in the initial release of the Ensemble Connector SR-IOV feature.

Hardware Verified NICS: Intel X710 and X722
Networking The NIC grooms management and service chain traffic via VLAN tags. VLAN tagging is mandatory into SR-IOV.
Hardware Settings SR-IOV must enabled Each 10G interface on the X710 NIC must have SR-IOV enabled
Drivers and Firmware Linux i40e: 2.10.19.82 (in Connector OS) NIC firmware: x710 - 6.80 and x722 - 4.10

Q: Can you define the interfaces on which SR-IOV is applied?

A: Yes. At the time of orchestration, the user can elect to use SR-IOV on WAN or LAN or both.

Q: Why would you choose to only apply SR-IOV to only one of the interfaces?

A: As mentioned above, SR-IOV bypasses the Connector vSwitch, which means Connector vSwitch features are removed from that segment– including IP Pass-through, Layer 2 frame counts, etc. In this case, the VNF must provide these functions. Where Connector WAN-side features are required, users may apply SR-IOV only to the LAN side traffic.

Q: How does a user select SR-IOV?

A: The day-1 configuration defines selected ports for SR-IOV. The Ensemble Connector API exposes VF resource availability to northbound orchestration platforms and the orchestration platform can configure the binding of the port when building the service chain is instantiated (normal for virtio, direct for SR-IOV).

Q: Are there VNF dependencies for leveraging Connector SR-IOV capabilities?

A: Yes. The VNF must provide a VF Driver and it must be compatible with the NIC PF functions that set up SR-IOV.

Q: What native wireless (LTE) capabilities does Ensemble Connector provide?

A: LTE interfaces in Ensemble Connector provide wireless layer 3 (IP) connectivity to the Internet. You can provision up to 16 LTE interfaces and you assign LTE interfaces to VRFs within Connector.

Connector uses PDP profiles to establish a data connection with a mobile network. When a connection is initiated, Connector automatically determines the PDP profile to use based on the MCC and MNC information contained on the SIM card of the modem (values uniquely assigned to a mobile operator within a specific country). A PDP profile specifies one or more Access Point Names (APNs) for Connector to use when dynamically establishing that data connection. You can configure up to 100 PDP profiles, each of which can contain up to 16 APNs. Ensemble Connector attempts to use each APN listed in the PDP profile until a connection is successfully established. Connector also supports logic to back-off retry attempts to prevent Connector from breaching the Internet of Things (IoT) connection guidelines

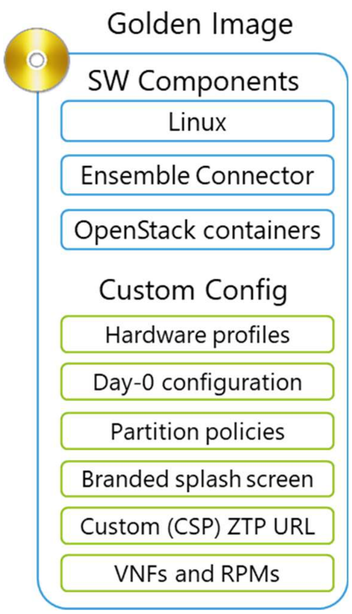
When you provision an LTE interface for dynamic modem detection, Ensemble Connector attempts to automatically identify a suitable, connected modem and then configures the discovered modem. This process is fully automated and in general, the modem does not need to be physically present when you apply the LTE interface configuration. This allows the user to install the modem later and the system will automatically recognize that the modem has been added (dynamic plug-and-play).

Ensemble Connector works with modems by many different manufacturers using different control protocols including MBIM, QMI, and Hays-AT. The primary supported wireless technology is 3GPP, both LTE and LTE-A. Although many modems can use the older GSM (2G) or UMTS/HSPA (3G) technology, data throughput over those connections will be limited.

Ensemble Connector also provides several ways to help identify the root cause of problems related to the SIM and mobile account, radio signal strength, or the modem itself.

Q: What are Golden Images and why are they important?

A: A golden image provides a standard Ensemble Connector ISO that includes enough customer specific configuration information to enable the automated zero touch deployment process. Golden images contain the following key items:



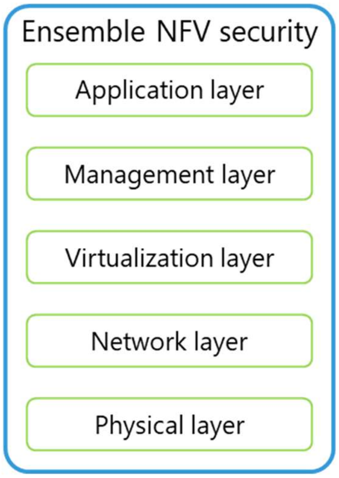
- Ensemble Connector software
  - Embedded Linux OS
  - Management and datapath applications
  - OpenStack Containers (if leveraging an OpenStack cloud model)

- Customer-specific configuration files
  - Hardware profiles – defines detailed configuration of hardware vendors and models that the operator intends to deploy
  - Day-0 configuration – defines the pre-deployment configuration parameters
  - Partition policies – based on specific hardware profiles and deployment use cases, this will define how the storage resources are configured
  - Branded splash screen – the splash screen is used during the ZTP process to provide feedback to the end user regarding the status of system initialization
  - Custom ZTP URL – defines how to access service provider specific management domain
  - VNFs and RPMs – allows for pre-staging of VNF images as well as ability to execute custom applications or scripts after ZTP is complete

Customers must engage ADVA professional services for the creation of Ensemble Connector golden images. Note, typically a customer will only require a single golden image for their network, although there are certain scenarios where more than one golden image will be required.

Q: How does Ensemble address security requirements for uCPE?

A: Ensemble provides a systematic approach to NFV security by addressing security at multiple levels as shown in the figure.



<u>Physical and Network Layer Security</u>

- Support virtual networking including E-LAN, E-Tree and multiple secure VRFs:
  - Separation between tenants is ensured by VLAN isolation
  - Each VRF is a unique and isolated forwarding entity that uses independent route and ARP tables for isolation
- Management network secured by interfacing into standard security gateways using IKE
- Management firewall protection allowing firewall profiles to be assigned to all types of physical/logical interfaces

- Prevents unwanted VNF data plane connectivity into the carrier management network

Virtualization Layer Security

- Safeguard against VM escape – protecting one VM from another
- Prevention of rogue management system connectivity to hypervisor
- Support for VNF attestation via checksum validation to confirm running VNF matches stored image

Management Layer Security

- Use of HTTPS on APIs and UIs
- Support for role-based access across multiple privilege levels controls access to available commands
- Root operating system login blocked on Ethernet and serial ports
- SSH key-based login options to eliminate password exposure
- RADIUS & TACACS+ authentication options

Application/Solution Layer Security

- Use of two-factor authentication at customer sites
- Encryption of management and user tunnels
- Encryption of locally stored passwords

Q: What service activation and service assurance features does Ensemble Connector provide?

A: Ensemble Connector provides native capabilities to support service activation and service assurance, including:

Service activation

- Smart Layer 2 loopbacks (ingress and egress)
- Y.1731 Ethernet loopback supported

Service Assurance

- Y.1731/802.1ag with up and down MEPs (up to 100)
- Link OAM (802.3ah)
- TWAMP reflector for Layer 3 testing

Connector also provides performance management (PM) reporting via 15-minute binned counters

- Interface RMON PM
- Interface Rx/TX PMs on Ethernet flows
- Per service CoS queue PM
- Y.1731 service OAM
- Tunnel latency, loss, throughput

Additionally, Ensemble Connector supports “embedded” 3rd party Service Activation and Service Assurance tools from partners such as EXFO, Spirent and Viavi. These test applications can be automatically instantiated during service activation, perform initial service qualification (“born-on certificate”) and then be spun down to release those compute resources for use by other VNFs.

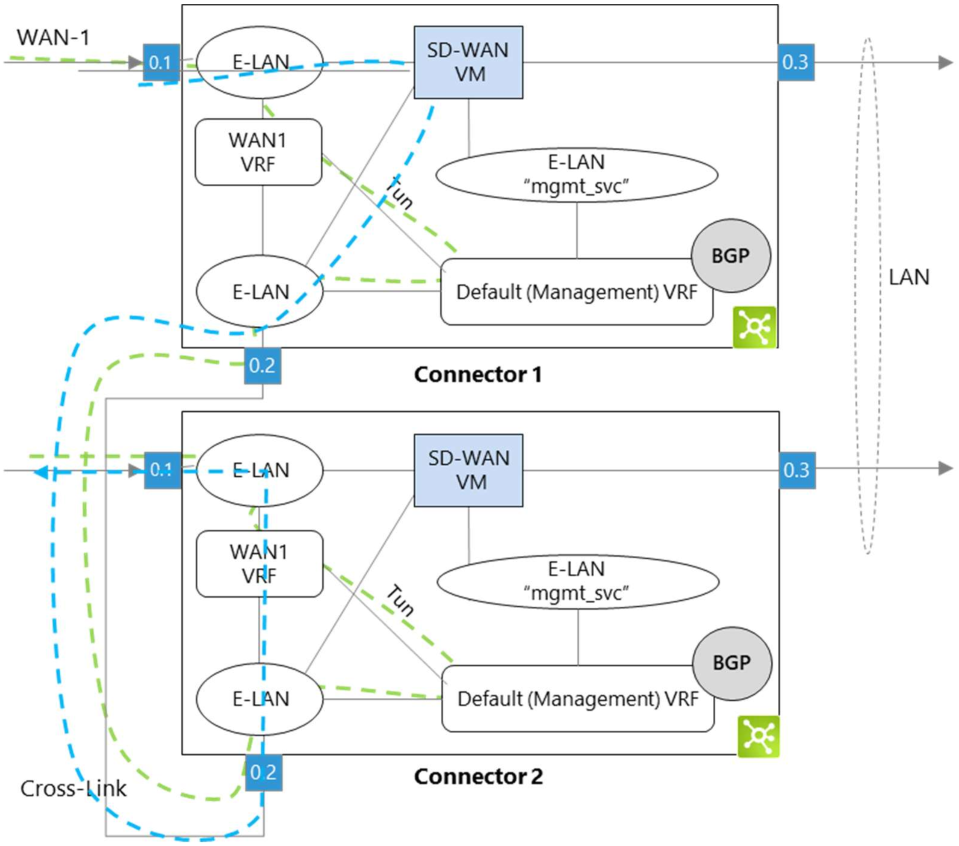
Q: How does Ensemble Connector support service resiliency?

A: Supporting high availability requires a redundant uCPE device to be deployed at a customer site. The second device needs to be configured with the same Ensemble Connector software version, virtual infrastructure, VNFs and service chain.

To maintain resiliency within the service chain, all VNFs in the service chain should support high availability synchronization. Ensemble Connector has been designed to provide flexible networking for high availability synchronization between VNFs of redundant service chain instances, thereby providing resiliency to the overall service.

The figure below shows how Ensemble Connector supports a hybrid WAN service with network and node failure protection. This is provided with the following enabling Connector technologies:

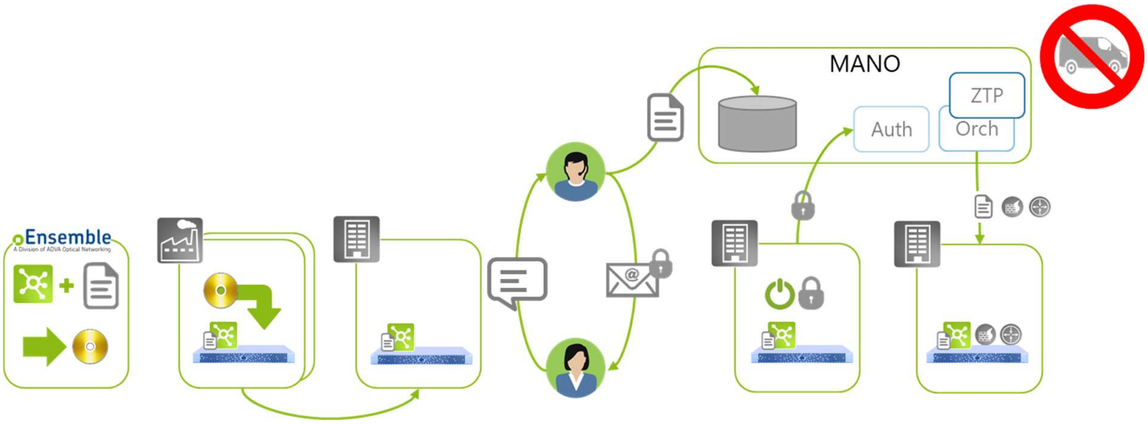
- E-Flow service with IP Pass-through
- BGP Dynamic Routing
- Link Loss forwarding



Q: What is ZTP and why is it so important.

A: Zero touch provisioning (ZTP) is a set of tools and procedures that enable the automated deployment of remote Ensemble Connector instances across a network with minimal or no user intervention. With ZTP you can:

- Apply a completely user-defined static configuration to all MaestrOS components.
- Obtain an initial IP address over a defined infrastructure using DHCP.
- Use the port query feature to identify available access network options when external cabling or connectivity is unknown.
- Access an authentication scheme that uses two-factor authentication and X.509 certificates with a remote authentication server. Exchange of critical customer provisioning data occurs only after a valid certificate is presented to both the authentication server and Ensemble Connector.
- Download customer specific day-1 CPE configuration with end-customer, site specific provisioning.
- Instantiate 3rd party VNFs or containers and setup target service chains.
- When applicable, integrate with external VNF managers to automatically provision dy-1 configuration of VNFs.
- Customize the commissioning utility to provide the initial configuration, scripts, and processes.
- Invoke your own user-supplied scripts for more customized operations.



With Ensemble ZTP, an entire branch site can be deployed ("power to packets") with little or zero interaction required from either the end customer or a service technician.

Q: What sort of fault information is provided by Ensemble Virtualization Director?

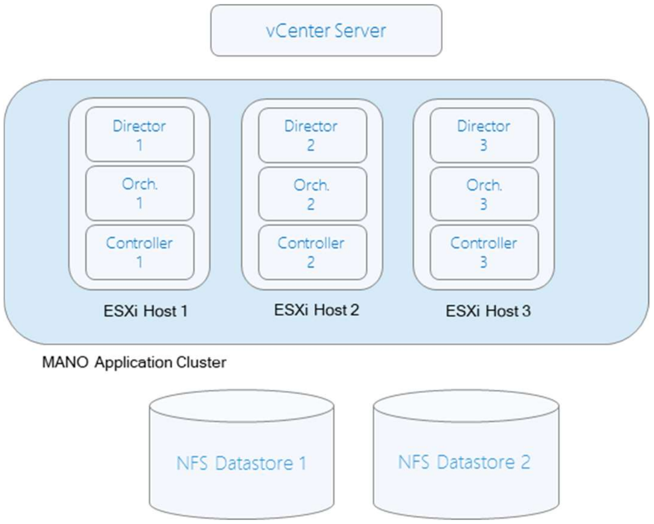
A: Ensemble Virtualization Director provides a framework to collect faults and alarms from all Ensemble components. Fault information includes:

- Dynamic current alarm count display
- Current alarm summary table
- Powerful alarm filtering/search
- Event browser maintains complete history of raise/clear events
- Correlation between raise/clear events
- Alarm acknowledgment, latching alarms and commenting function
- Log browser
- Connector Inventory view showing status and configuration details of each instance
- Connector status page
- Service topology
- Northbound API and reporting
- Publish subscribe model

- Syslog
- Troubleshooting tools and drill-down options

Q: How does Ensemble MANO support resiliency?

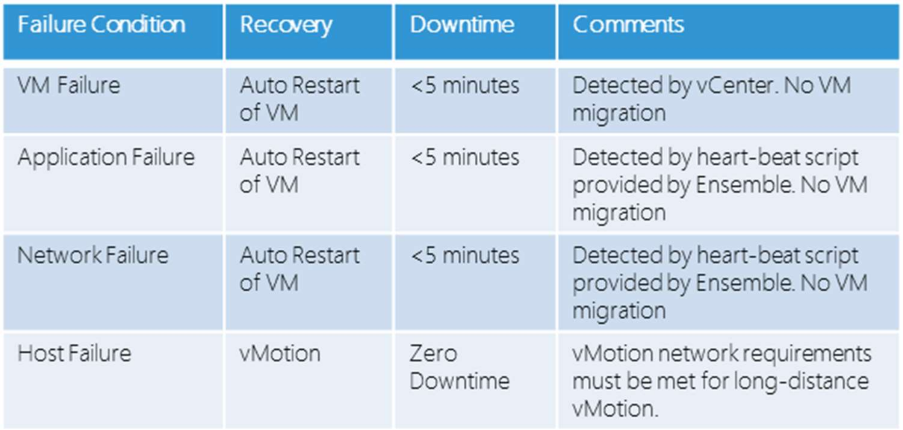
A: System resiliency can be expressed in terms of high availability (HA) and fault tolerance. High availability refers to avoiding loss of service by minimizing downtime. It is described in terms of a system's uptime, as a percentage of total running time. Fault tolerance refers to continuing operating without interruption when one or more components fail. Fault tolerant systems use backup components that automatically take the place of failed components, ensuring no loss of service.



The Ensemble MANO components (Orchestrator and Virtualization Director) provide options for both highly available and fault tolerant configurations. Native, application level high availability is provided through the deployment of application clusters whereas fault tolerance is provided by application resource distribution leveraging native VMware HA tools such as vMotion and vSphere Replication.

For HA deployments, the application cluster will consist of three instances of each application deployed on separate ESXi hosts as shown in the figure. These clusters will be deployed in an Active-Standby configuration where at any point in time, one instance is active and the other two instances are in hot-standby mode. The virtual IP, which drives communication between each MANO cluster and north-bound/south-bound applications, will be owned by the active cluster instance upon initial configuration. Upon failure of a host, application or VM, the remaining 2 instances will continue to run, and the VIP will be taken over by one of the active instances.

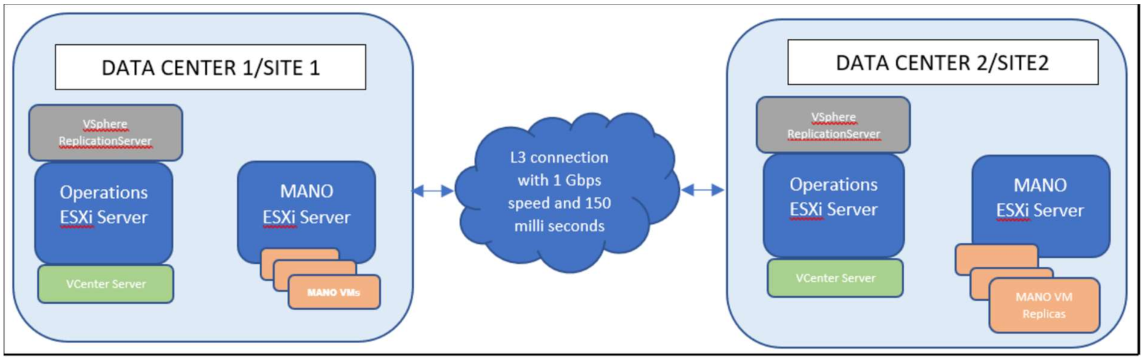
Ensemble MANO components also support native HA via application clustering within an OpenStack based deployment. For fault tolerant deployments, Ensemble MANO components leverage VMware vMotion to migrate running VMs from one physical server to another without scheduling downtime and disrupting business operations. When an Ensemble MANO cluster has vMotion enabled, the vSphere distributed resource scheduler will make the initial placement recommendations for fault tolerant virtual machines and then manage the movement of those VMs during cluster load re-balancing. A high-level view of expected behavior for a variety of failure conditions is shown in the table below.



Failure Condition	Recovery	Downtime	Comments
VM Failure	Auto Restart of VM	<5 minutes	Detected by vCenter. No VM migration
Application Failure	Auto Restart of VM	<5 minutes	Detected by heart-beat script provided by Ensemble. No VM migration
Network Failure	Auto Restart of VM	<5 minutes	Detected by heart-beat script provided by Ensemble. No VM migration
Host Failure	vMotion	Zero Downtime	vMotion network requirements must be met for long-distance vMotion.

For vMotion fault tolerance, the advantage is that there is little downtime. But there is high requirement on network bandwidth between redundant servers, so the solution tends to be more expensive to deploy.

Another option supported by Ensemble MANO is to use vSphere Replication for disaster recovery (DR). VMware vSphere Replication is a DR solution that allows you to replicate virtual machines on the same vCenter Server instance or to other instances within the same site, across sites An example deployment topology of a site to site replication of virtual machines is shown below.

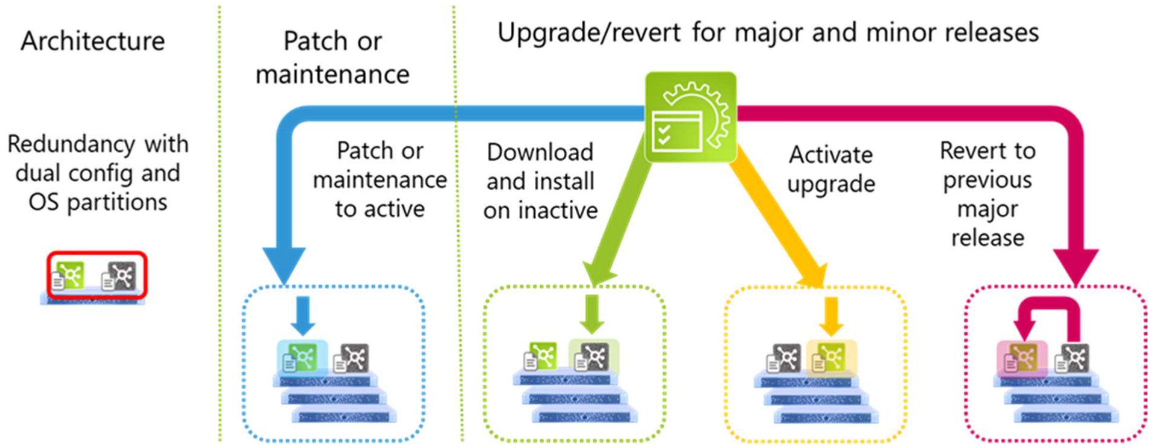


For vSphere fault tolerance, the advantatge is that it's very cost efficient and will support multi-geo deployments architectures. However, in this solution, there will be several minutes of downtime before the next instance is functional.

Within the native AWS deployment model, the options are more limited. Currently, no native HA is supported in AWS configurations. However, Ensemble MANO does leverage tools such as CloudWatch available in AWS to monitor VMs and auto-restart the application when issues arise. We can also leverage Amazon EBS snapshots for backup and disaster recovery, which works across regions to provide multi-geo fault tolerance.

Q: How does Ensemble process Connector software upgrades?

A: There are two general types of upgrades: full software upgrades, which can be major or minor upgrades, and maintenance or patch upgrades. Major and minor Connector upgrade images contain a full OS update, including the latest CentOS release an all the latest security and critical fixes. During major and minor upgrades, the necessary files are delivered to the non-active partition and require a reboot to activate. You can revert to the previous image for these upgrades. Maintenance upgrade images provide minor updates and bug fixes to Connector software. A maintenance update does not contain a full OS upgrade and is installed on the current active partition. Due to nature of the installation, a maintenance update is irreversible and cannot be undone.


Architecture
Redundancy with dual config and OS partitions
Patch or maintenance
Patch or maintenance to active
Upgrade/revert for major and minor releases
Download and install on inactive
Activate upgrade
Revert to previous major release

Release Type	Description	Delivered to Partition	Activation Requires	Reversion
Major	Complete Connector package, significant new feature content, delivered to non-active partition	Non-active	Reboot	Yes. Boot to previous partition
Minor	Complete Connector package, modest new feature content, delivered to non-active partition	Non-active	Reboot	Yes. Boot to previous partition
Maintenance	Complete Connector package, bug fix, delivered to active partition	Active	May or may not require reboot	No
Patch	Targeted software package delivered to active partition	Active	May or may not require reboot	No

Q: What lessons has Ensemble learned from working with service providers?

A: We are fortunate to have worked with several operators and large enterprises on NFV deployments for almost three years. As a result, we have increased our knowledge and experience with NFV. Some of the key reasons our customers pick up are highlighted below:

- True multi-platform hardware support
  - Multiple COTS suppliers – Dell, Lanner, Advantech, Lenovo, HPE, Supermicro, Silicom
- Open platform
  - Multitude of onboarded VNFs
  - Open, standard cloud components such as Linux, KVM, and OpenStack provide the flexibility to deploy a fully multi-vendor environment

- Scalable software
  - From small Intel Atom® servers, up to large multi-socket Xeon® servers
  - Upcoming support for ARM servers
- Operational simplicity
  - Zero touch provisioning: Empowers an operator to ship an unconfigured COTS server to a customer site and commission it automatically – including VNFs
  - Embedded cloud: Solves the problems of deploying OpenStack in the distributed telco network
  - LTE wireless support: Turn-up sites that don't yet have wireline connectivity, as well as provide an economical means of resilient access
- Telco-grade manageability
  - Fault, performance, configuration, inventory, and topology support for NFVI
- Our products work!

More info:

- Real-World NFV, Real Lessons Learned
- Ensemble Continues to Make NFV Easy – and Cloudy

Ensemble virtualization and NFV economics

Q: Does the NFV business case work for service providers?

A: Yes. The NFV hardware and software market has matured greatly over the last few years. In general, the prices for both hardware and software have come down to the point that virtualized services can be deployed on white box COTS servers at a capital cost below that of the equivalent appliances. Additionally, using software-centric functions has significantly lowered operational expenses while enabling innovation, all without changing the deployed hardware. Operational costs have also improved as NFV management, operations, and automation tools have continued to mature.

ADVA has developed tools to help service providers evaluate the potential total cost of ownership and return on investment that can be achieved by investing in NFV. We are happy to share these tools upon request.

More info:

- Hard Truths about Software Licensing for NFV
- Optimizing Profitability with Pure-Play NFV
- The Business Value of Software-Defined Networking (page 18)
- The Real Reason to Deploy NFV: New Revenue

Q: What is the Ensemble virtualization pricing strategy?

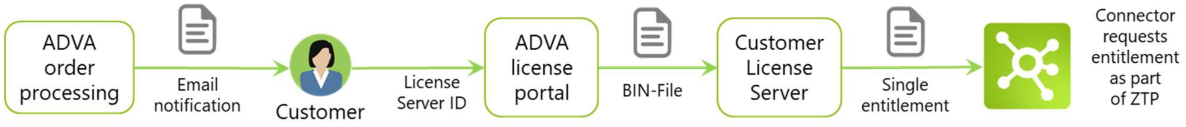
A: The Ensemble components have been part of live deployments for over three years. As a result, we have a very good understanding of the varying commercial models required by service providers to be successful in this market. The Ensemble team has defined a flexible set of pricing models to meet these needs. These models include:

- Perpetual licensing allows the service provider to deploy an instance of Ensemble software forever, for a given software revision, feature level, performance, etc.
  - Perpetual licenses are typically not "node locked" meaning that the license is transferrable from one hardware device to another – if the service provider deploys an enterprise license server (ELS) and the license is properly returned to the license server.
  - ADVA's strategy allows customers who maintain active support agreements to perform feature constant software upgrades to new revision levels - at no additional cost.
- Subscription licensing provides all the aforementioned perpetual licensing benefits but for a single low monthly fee.
  - Typically, annual support and maintenance is included with the subscription price for the duration.
  - The subscription model will include a minimum duration – e.g., 2 – 3 years.
  - Subscription models allow customers to perform feature constant software upgrades to new revision levels - at no additional cost.
- Both of the above models are built around a "pay as you grow" strategy that minimizes up-front charges and defers licensing fees based on time and usage

In short, we can define a model that makes sense for both the service provider and Ensemble.

Q: How is Ensemble licensed?

A: Ensemble Connector simplifies the solution licensing into a single structure. The Ensemble Connector operating system (OS) and embedded cloud are licensed through a common license structure. As a software-based solution, it is imperative that ADVA can manage the distribution and usage of its software products to ensure that all deployed instances are covered under appropriate commercial terms. The license structure is intended to be simple and non-service affecting.



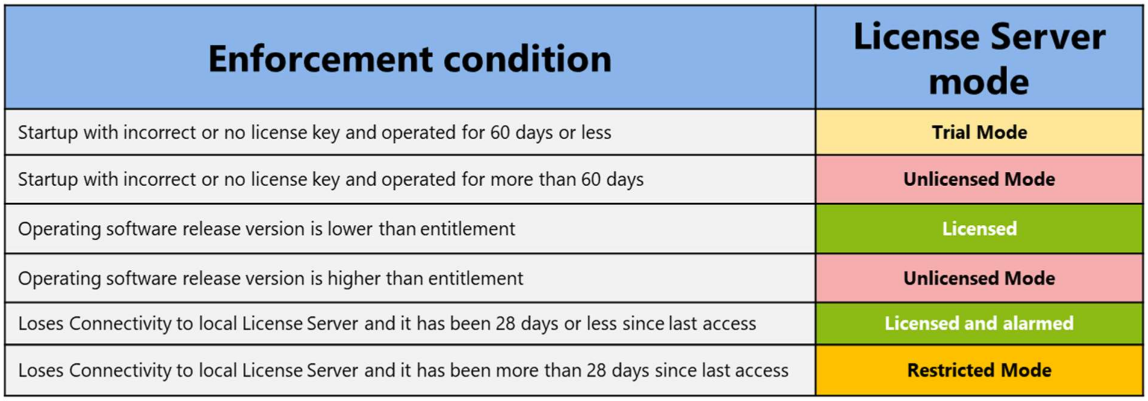
Ensemble Connector licenses are controlled by an enterprise license server (provided by ADVA at no additional cost). The customer can deploy one or more license server instances depending on their management network architecture and need for license server resiliency.

Software Entitlements are files that contain one or more Activation IDs (or license keys), which represent a particular "licensed feature". Entitlements are procured directly from ADVA via a purchase order. The license keys are bound and activated against a specific/target License Server deployed within the customer's management domain. The License Server requires an IP connection to all managed network elements via data communications network (DCN). The License Server is responsible for the following:

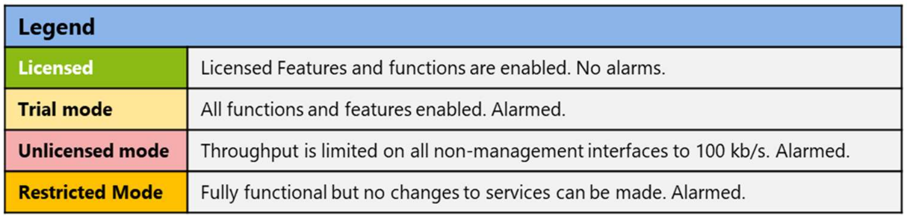
- Tracks the total number of available and used licenses
- Tracks devices to which the licenses are leased

A network element retrieves a license from this server in a similar way a computer leases an IP address from a DHCP server

Licenses can be applied during device staging or as part of initial field deployment through the ZTP process. During ZTP, Ensemble Connector will communicate with the target License Server provided as part of the day-0 configuration. After license delivery, Ensemble Connector will cache the license locally ensure that the solution works without an active License Server connection for a certain duration. The behavior of the solution in various "licensing modes" is described in the tables below.



Enforcement condition	License Server mode
Startup with incorrect or no license key and operated for 60 days or less	Trial Mode
Startup with incorrect or no license key and operated for more than 60 days	Unlicensed Mode
Operating software release version is lower than entitlement	Licensed
Operating software release version is higher than entitlement	Unlicensed Mode
Loses Connectivity to local License Server and it has been 28 days or less since last access	Licensed and alarmed
Loses Connectivity to local License Server and it has been more than 28 days since last access	Restricted Mode



Legend	
Licensed	Licensed Features and functions are enabled. No alarms.
Trial mode	All functions and features enabled. Alarmed.
Unlicensed mode	Throughput is limited on all non-management interfaces to 100 kb/s. Alarmed.
Restricted Mode	Fully functional but no changes to services can be made. Alarmed.

In volume deployment, this can be automated through the customer OS. In this method, the customer OS reads the device ID of the Ensemble Connector instance. The customer OS then provides it to the ADVA portal and obtains a pre-purchased license through portal APIs opened to the customer OS. The customer OS then applies the node-locked license to the Ensemble Connector instance.

More info:

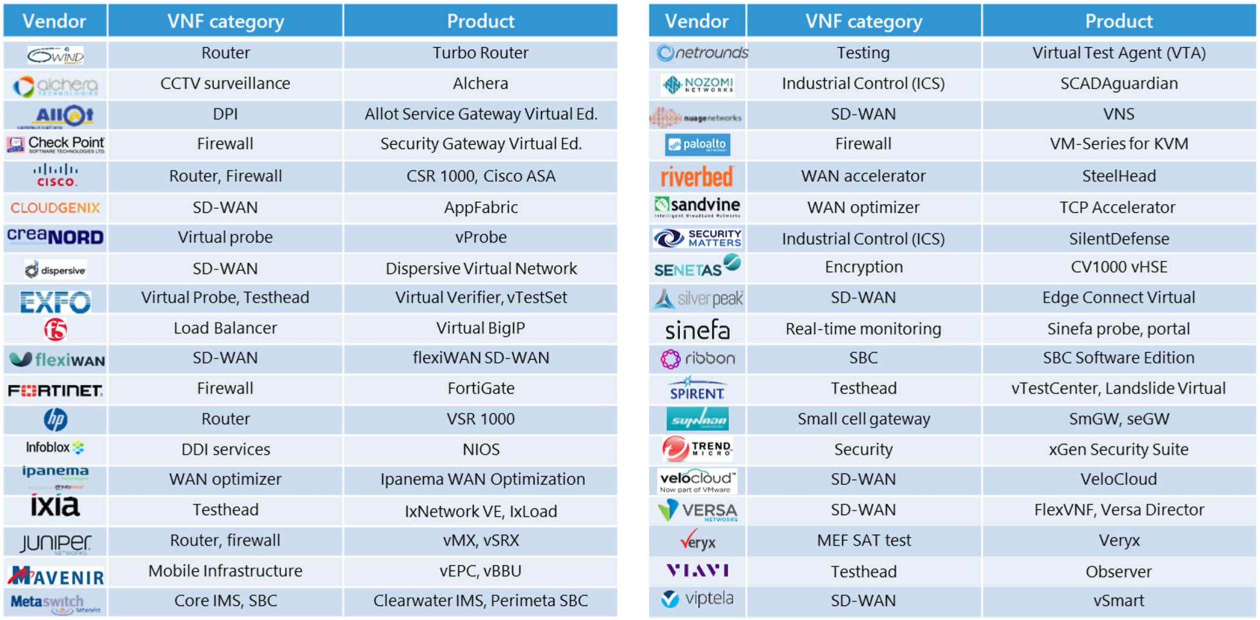
- Hard Truths about Software Licensing for NFV

Ensemble Harmony ecosystem and strategic partnerships

Q: What VNFs does Ensemble provide?

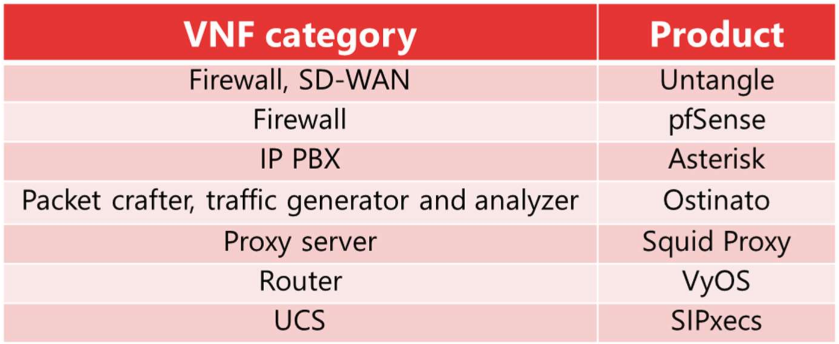
A: In general, ADVA does not sell VNFs. Ensemble provides an open architecture for NFV that enables a wide array of third-party VNFs to be easily deployed. The figure below shows a subset of the currently onboarded VNFs. This list includes both commercial and open source VNFs.

Third-party vendors



Vendor	VNF category	Product
6WIND	Router	Turbo Router
alchera	CCTV surveillance	Alchera
Allot	DPI	Allot Service Gateway Virtual Ed.
Check Point	Firewall	Security Gateway Virtual Ed.
Cisco	Router, Firewall	CSR 1000, Cisco ASA
CLOUDGENIX	SD-WAN	AppFabric
creaNORD	Virtual probe	vProbe
dispersive	SD-WAN	Dispersive Virtual Network
EXFO	Virtual Probe, Testhead	Virtual Verifier, vTestSet
f5	Load Balancer	Virtual BigIP
flexiWAN	SD-WAN	flexiWAN SD-WAN
FORTINET	Firewall	FortiGate
hp	Router	VSR 1000
Infoblox	DDI services	NIOS
ipanema	WAN optimizer	Ipanema WAN Optimization
ixia	Testhead	IxNetwork VE, IxLoad
Juniper	Router, firewall	vMX, vSRX
MAVENIR	Mobile Infrastructure	vEPC, vBBU
Metaswitch	Core IMS, SBC	Clearwater IMS, Perimeta SBC
netrounds	Testing	Virtual Test Agent (VTA)
NOZOMI NETWORKS	Industrial Control (ICS)	SCADAguardian
nuage networks	SD-WAN	VNS
paloalto	Firewall	VM-Series for KVM
riverbed	WAN accelerator	SteelHead
sandvine	WAN optimizer	TCP Accelerator
SECURITY MATTERS	Industrial Control (ICS)	SilentDefense
SENETAS	Encryption	CV1000 vHSE
silver peak	SD-WAN	Edge Connect Virtual
sinefa	Real-time monitoring	Sinefa probe, portal
ribbon	SBC	SBC Software Edition
SPIRENT	Testhead	vTestCenter, Landslide Virtual
sunwave	Small cell gateway	SmGW, seGW
TREND MICRO	Security	xGen Security Suite
velocloud Now part of VMware	SD-WAN	VeloCloud
VERSA NETWORKS	SD-WAN	FlexVNF, Versa Director
Veryx	MEF SAT test	Veryx
VIAVI	Testhead	Observer
viptela	SD-WAN	vSmart

Open source VNF library



VNF category	Product
Firewall, SD-WAN	Untangle
Firewall	pfSense
IP PBX	Asterisk
Packet crafter, traffic generator and analyzer	Ostinato
Proxy server	Squid Proxy
Router	VyOS
UCS	SIPxecs

3rd party platform integration

Supplier	Product category	Ensemble component integrated
Amdocs	Orchestration	Ensemble Connector
NetCracker	Orchestration	Ensemble Connector, Virtualization Director & Orchestrator
Ericsson	Orchestration	Ensemble Connector
Cloudify	Orchestration	Ensemble Connector
IBM	Orchestration	Ensemble Connector & Orchestrator
ONAP	Orchestration	Ensemble Connector & Orchestrator
Adtran	Adtran Operating System	Ensemble Orchestrator
Allot	NetXplorer EMS	Ensemble Orchestrator
Wind River	Titanium Server	Ensemble Orchestrator

Q: What does on-boarding mean?

A: On-boarding is the process of integrating a VNF with the NFV infrastructure (Ensemble Connector) and MANO (Ensemble Orchestrator). During the on-boarding process, Ensemble Orchestrator is provisioned with the information it needs to instantiate and operationalize a VNF type on a remote compute node (either standalone or within a service chain).

On-boarding a new VNF involves specification of the "VNF Type", where a wide variety of VNF configuration and operating parameters are defined, including:

- VNF flavors and optimizations for virtual resources (CPU, RAM, storage, etc.)
- Day-0 initialization options
  - Config drive
  - Cloud-init
  - Metadata
  - SSH scripts
- Network parameters (cidr, gateway ip, link ip) variables
- High availability profiles
- Auto-scaling profiles
- Configuration scripts tied to lifecycle events such as boot, edit, and delete scripts as well as "day-N" scenarios
- Fault remediation policies

This process can be performed by the Ensemble team, but it can also be done by the operator or third-party contractor.

Q: Does Ensemble provide an app store for VNFs?

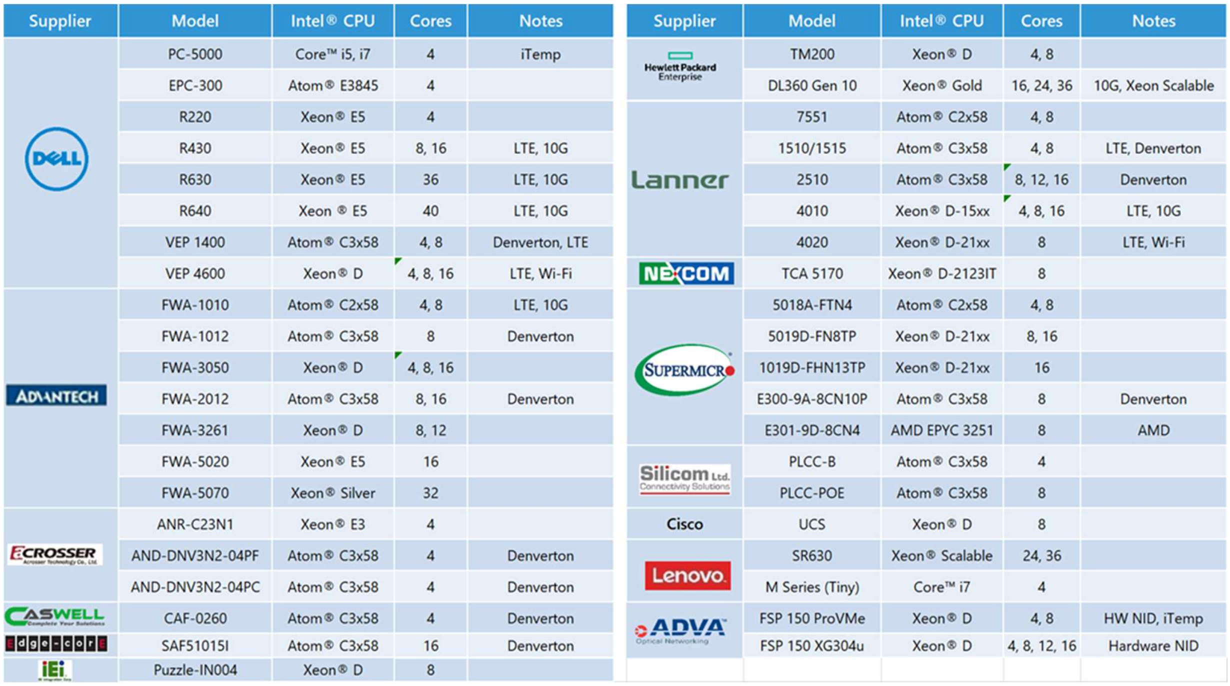
A: Not today. Most of our customers want to acquire VNFs directly from the suppliers. However, Ensemble does provide for ease of use with its Harmony program and large portfolio of onboarded VNFs.

More info:

- Ensemble Harmony Ecosystem web page
- Ensemble Harmony Ecosystem Explained (video)

Q: What COTS servers does Ensemble Connector currently support?

A: Connector supports the industry's largest portfolio of white box vendors. Leveraging our relationship with Intel® as well as Ensemble Connector's flexible and configurable software architecture, we can easily on-board new hardware models within the Intel® Atom and Xeon processor familes.



Supplier	Model	Intel® CPU	Cores	Notes
DELL	PC-5000	Core™ i5, i7	4	iTemp
	EPC-300	Atom® E3845	4	
	R220	Xeon® E5	4	
	R430	Xeon® E5	8, 16	LTE, 10G
	R630	Xeon® E5	36	LTE, 10G
	R640	Xeon ® E5	40	LTE, 10G
	VEP 1400	Atom® C3x58	4, 8	Denverton, LTE
	VEP 4600	Xeon® D	4, 8, 16	LTE, Wi-Fi
ADVANTECH	FWA-1010	Atom® C2x58	4, 8	LTE, 10G
	FWA-1012	Atom® C3x58	8	Denverton
	FWA-3050	Xeon® D	4, 8, 16	
	FWA-2012	Atom® C3x58	8, 16	Denverton
	FWA-3261	Xeon® D	8, 12	
	FWA-5020	Xeon® E5	16	
	FWA-5070	Xeon® Silver	32	
ACROSSER Acrosser Technology Co., Ltd.	ANR-C23N1	Xeon® E3	4	
	AND-DNV3N2-04PF	Atom® C3x58	4	Denverton
	AND-DNV3N2-04PC	Atom® C3x58	4	Denverton
CASWELL Complete Your Solutions	CAF-0260	Atom® C3x58	4	Denverton
Edge-corE	SAF51015I	Atom® C3x58	16	Denverton
iEi	Puzzle-IN004	Xeon® D	8	

Supplier	Model	Intel® CPU	Cores	Notes
Hewlett Packard Enterprise	TM200	Xeon® D	4, 8	
	DL360 Gen 10	Xeon® Gold	16, 24, 36	10G, Xeon Scalable
Lanner	7551	Atom® C2x58	4, 8	
	1510/1515	Atom® C3x58	4, 8	LTE, Denverton
	2510	Atom® C3x58	8, 12, 16	Denverton
	4010	Xeon® D-15xx	4, 8, 16	LTE, 10G
	4020	Xeon® D-21xx	8	LTE, Wi-Fi
NEXCOM	TCA 5170	Xeon® D-2123IT	8	
SUPERMICRO	5018A-FTN4	Atom® C2x58	4, 8	
	5019D-FN8TP	Xeon® D-21xx	8, 16	
	1019D-FHN13TP	Xeon® D-21xx	16	
	E300-9A-8CN10P	Atom® C3x58	8	Denverton
	E301-9D-8CN4	AMD EPYC 3251	8	AMD
Silicom Ltd. Connectivity Solutions	PLCC-B	Atom® C3x58	4	
	PLCC-POE	Atom® C3x58	8	
Cisco	UCS	Xeon® D	8	
Lenovo	SR630	Xeon® Scalable	24, 36	
	M Series (Tiny)	Core™ i7	4	
ADVA Optical Networking	FSP 150 ProVMe	Xeon® D	4, 8	HW NID, iTemp
	FSP 150 XG304u	Xeon® D	4, 8, 12, 16	Hardware NID

Q: Can we replace appliances with COTS hardware plus proprietary software?

A: Yes. Leading operators like Masergy, Verizon, Colt, TPx and CenturyLink are already deploying virtualized services built on software VNFs running on COTS servers. By doing so, they can leverage the benefits of cloud technologies, as described above.

Q: What is the relationship between ADVA and Intel®?

A: ADVA and Intel have a broad relationship, as follows:

- ADVA is a member of Intel Network Builders. More specifically, ADVA is a member of the Leaders Board within the Winners' Circle of selected Intel partners.
- Ensemble Connector is also an approved software component for Intel Select Solutions for uCPE.

Finally, Connector runs on a wide variety of platforms powered by Intel Architecture processors. See "

- Q: What COTS servers does Ensemble Connector currently support?" for more information.

Q: What is the relationship between ADVA and Dell EMC?

A: Dell resells Ensemble Connector software pre-installed on the Dell EMC VEP 1400 and VEP 4600 servers. These servers are optimized for uCPE applications.

Q: What is the relationship between ADVA and Lanner?

A: ADVA resells a variety of Lanner servers, enabling our customers to get a combined hardware/software solution from a single supplier.