White Paper

Cisco Elastic Services Controller: Simplify and Automate the Virtualized Environment

Executive Summary

As service providers try to keep up with the rapid pace of change today, they are turning to network functions virtualization (NFV) to be agile and more responsive to customer needs. By virtualizing a range of network functions, they are seeking to accelerate the delivery of new services, scale them elastically with demand, and replace manual tasks with automated, repeatable processes. In practice, however, most NFV management tools used today fall short of this ideal. They are often complex, requiring domain-specific knowledge, custom automations, and manual operations.

The Cisco® Elastic Services Controller (ESC) provides a comprehensive lifecycle management platform for NFV. It provides end-to-end capabilities to automate various tasks such as deploying, monitoring, and elastically scaling virtualized functions, and make them available as business-level service, not just as a collection of virtual machines. In short, it makes the promise of NFV - end-to-end automation, agility, and simplicity - a reality in your business.

Virtualization Trends and Challenges

Business success is increasingly dictated by agility: the ability to respond quickly to change, bring new services to market fast, and do it all within an IT environment that is simple and inexpensive to operate. But for service providers, as well as a growing number of enterprises, the traditional network architecture can present significant barriers.

In the traditional network model, most services are tied to specialized hardware appliances. As a result, lead times for implementing a new service for a customer - deploying the appliances, configuring them, provisioning the service - can take weeks or even months. Scaling services is also a complex, manual effort, meaning that organizations can miss business opportunities because they can't respond quickly enough to demand. And, since the network is designed to handle peak loads, ongoing operational costs are higher than they should be, with most resources typically sitting idle.

Disconnected Virtualization Capabilities and Business Processes

For all of these reasons, service providers and enterprises are looking to virtualize many network functions to make their environments more agile, scalable, and easier to manage. A variety of virtualized network function management (VNFM) tools are now available to manage a wide range of VNFs. But most of these tools are designed around managing virtualized workloads - not around delivering services. They are great at instantiating virtual machines. But when it comes to provisioning or monitoring those virtual machines in the context of delivering a service to a customer (for example, monitoring the health and performance of a service inside a virtual machine to comply with a service-level agreement [SLA]), you're largely on your own. You typically have to rely on manual processes and a patchwork of custom scripts developed on a per-customer or per-application basis.

Meeting Modern NFV Requirements

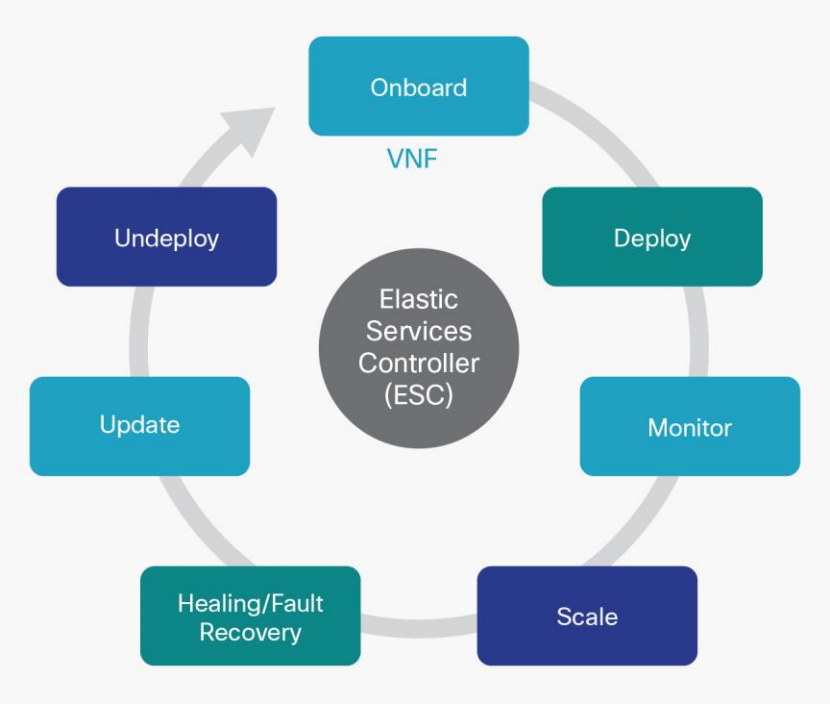
What you need is a VNF management platform built around your business and services, not just virtualization tasks. You need a solution that provides:

- **Services agility,** with the ability to dynamically deploy, monitor, and scale VNFs, so you can onboard new applications faster
- **Simplified operations,** with an open and extensible architecture that abstracts away NFV complexity and lets you provision services with reusable data models
- **Lower OpEx and optimized resource consumption** by automating VNF monitoring, elastic scaling, and service recovery
- **Accelerated innovation,** with the ability to integrate with any standards-based VNF, orchestration or assurance system, or custom applications

The Solution: Cisco Elastic Services Controller

The Cisco Elastic Services Controller (ESC), a key product in the Cisco NFV Orchestration portfolio, provides a comprehensive lifecycle management platform for NFV. By design it is built as an open and modular system. Cisco ESC default integrates with Cisco Network Service Orchestrator using Netconf-Yang APIs, or ESC can be deployed standalone. Cisco NSO and ESC together provides comprehensive VNF and Service lifecycle management capabilities for both physical and virtual environment. Drawing on industry standards and open APIs, you can control the full lifecycle of all your virtualized resources, whether using Cisco or third-party VNFs and management tools, and retain choice to use best-of-class industry solutions (refer to Figure 1).

Figure 1. Cisco ESC VNF Lifecycle Services

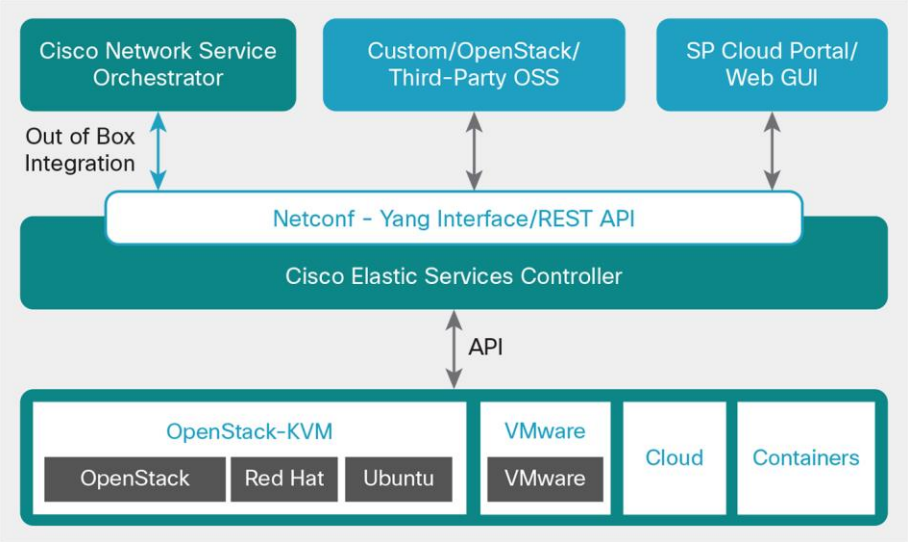


The following sections provide more details about key attributes and capabilities.

A Standards-Based, Model-Driven Solution

Cisco ESC provides advanced VNF lifecycle management capabilities through an open, standards-based platform that conforms to the ETSI NFV framework. By conforming to industry standards and exposing well-defined APIs, it can interoperate with any standards-based VNF infrastructure (VNFI) or NFV orchestration (VNFO) system(Figure 2).

Figure 2. Cisco ESC Modularity



Likewise, Cisco ESC lifecycle management capabilities are data model-directed (VNF Descriptor, or VNFD), supporting the Yang data model and NETCONF interfaces. So you can define data models once using an XML template - for example, a virtualized firewall service template - and use them over and over again for multiple deployments.

The following is a sample excerpt of XML for a Cisco Cloud Services Router CSR 1000V (CSR 1000V) virtual router:

```
<name>vCSR</name>
          <bootup_time>300</bootup_time>
          <recovery_wait_time>0</recovery_wait_time>
          <disk>
            <src>file://cisco/images/csr/csr1000v-universalk9.03.13.01.S.154-
3.S1-ext.qcow2</src>
            <disk_format>qcow2</disk_format>
            <container_format>bare</container_format>
            <serial_console>true</serial_console>
            <disk_bus>virtio</disk_bus>
          </disk>
          <vm_flavor>
            <vcpus>2</vcpus>
            <memory_mb>4096</memory_mb>
            <root_disk_mb>0</root_disk_mb>
            <ephemeral_disk_mb>0</ephemeral_disk_mb>
            <swap_disk_mb>0</swap_disk_mb>
          </vm_flavor>
```

In the configuration example, we specify the time the VNFM will wait for the virtual machine to boot before it raises a recovery event. It also defines the image that will be used to instantiate this VNF in the virtual infrastructure manager (VIM) (<disk> section). Finally, it defines the flavor for the virtual machine (<vm_flavor> section).
Note that we can incorporate multiple flavors in the same VNFD, permitting designers to select between various sizes during service design (for example, small, medium, or large). The flavors are created dynamically in the VIM during the onboarding (publishing) of a service definition.

These capabilities are agnostic to the underlying device. Whether the service encompasses a Cisco Cloud Services Router (CSR) or a virtualized firewall or security appliance from a third-party vendor, or contains a combination of virtual machines within a service, you can use the same tools to automate and accelerate deployment, provisioning, and scaling.

Cisco ESC abstracts away the complexities of multihypervisor environments from the user. It is designed as hypervisor-agnostic, so you can take advantage of these capabilities in the industry's most dominant virtual infrastructure management systems, including OpenStack, containers, or VMware environments.

VNF Lifecycle Management

Cisco ESC manages the complete lifecycle of a VNF. Triggered by a northbound request, Cisco ESC instantiates virtual machine to facilitate the requirements of a VNF service. The requester can specify all of the characteristics (for example, vCPU, memory, disk, monitoring KPIs, and more) typically associated with spinning up and managing a virtual machine in an XML template.

When a VNF is deployed, Cisco ESC applies "day-zero" configuration for a new service. Typically configuration includes credentials, licensing, connectivity information (IP address, gateway), and other static parameters to make the new virtual resource available to the system. It also activates licenses for the new VNFs.

The solution enables advertisement of newly created virtual machines using custom mechanisms like BGP, DNS, and RADIUS to alert the rest of the system that new VM is now available and ready for service. Similarly, it can unregister these advertisements when the virtual machine is no longer active (for example, in response to a failure event, or when a virtual machine is decommissioned when demand falls below a threshold you define).

Cisco ESC combines and automates all of these previously manual processes, so you can deploy new virtual services much faster and more easily. You can improve both service velocity and revenue by responding to new service requests more quickly. And you improve OpEx by using only the resources that you need at a given time, and elastically scaling back VNFs when they're not needed.

Managing Single or Coupled VNFs

Your business processes aren't designed around instantiating virtual machines, but around delivering services - potentially involving multiple virtual machines working together or implemented in a specific way. For example, in some cases you might need to implement a single virtual machine such as a Cisco CSR for a specific application. In others, the service may involve a group of virtual machines that have interdependency. You may be deploying multiple virtual machines that need to be on the same host. Or, you may need to spin up a group of linked virtual machines in a particular startup order to create a composite virtual service.

In a typical virtualized environment, instantiating multiple interdependent virtual machines involves complex, manual processes, meaning it can take days or even weeks to bring up a new service. Cisco ESC can provide lifecycle management capabilities for virtual machines individually or in groups. So whether a new service involves a single virtual machine or a group of composite VNFs operating together and/or in sequence, it automates the entire process, so you can deliver the new service in hours or minutes.

Out-of-the-Box Support for Multivendor VNFs

With Cisco ESC, you can onboard any new VNF type as long as it meets the prerequisites for supporting it in an OpenStack environment. For example in Openstack environment, Cisco ESC supports QCOW2 image format and config drive support for the VNF bootstrap mechanism.

Cisco ESC makes it easy. You just define the XML template for the new VNF type to onboard the VNF with ESC. The platform also provides out-of-the-box monitoring support for new VNF types with SNMP MIBs, ICMP Ping, and custom application monitoring methods.

Together, these capabilities help increase your service velocity and agility by allowing you to quickly integrate the service VNFs - regardless of where they are developed - into your elastic virtual infrastructure.

VNF Licensing

Another core task in virtualized environments that typically requires manual processes is activating the license for the VNF. Cisco ESC simplifies this process.

It enables Cisco Smart Licensing configurations in the VNF, Cisco's new "pay-as-you-go" licensing model, on supported VNFs. With Smart Licensing, instead of having to manually activate licenses for each virtual machine, the virtual machine registers itself with a centralized licensing server on boot-up, tracks how the resource is used, and bills on a consumption basis.

This setup provides important flexibility for elastic environments, allowing you to expand and contract as needed, in a completely automated fashion, while paying only for the resources you actually consume. When used in conjunction with Cisco Network Service Orchestrator (NSO), Cisco ESC also supports automated static license management with the use of customization features.

Transactions Resume and Rollback

Repeatability is an essential ingredient for business agility. After you've defined a virtualized service, you should be able to deploy it over and over again, hundreds or thousands of times, with a click of a button. But there's always a possibility that something will go wrong. If you're relying on bespoke scripts to automatically deploy a service 100 times and you identify a problem on the 50th, that situation can be a significant problem. Undoing previous operations can be incredibly complex and time-consuming.

Cisco ESC provides a transaction-based system to simplify these processes, and offers advanced rollback and resume features. So in the previous example, you can easily roll back the first 50 operations, or you could program Cisco ESC to start from the 51st operation and complete the remaining deployments.

Advanced Health and Service Monitoring, Recovery, and Elasticity

In addition to instantiating virtual machines, Cisco ESC also monitors virtual machines for health and performance. It engages a number of capabilities built into the platform to gather information from the virtual machine, analyze it to determine the health of the system, and take defined or custom actions in response to thresholds or events that you define.

These automated capabilities are extremely important in virtualized environments, where decisions must be made quickly. And they are essential to enabling elastic scalability. So for example, if performance is degrading on a service, the system can automatically react to that situation by instantiating a new virtual machine to increase capacity. Or, if virtual machines have gone idle as demand has dropped, the system can power them down to conserve resources and power.

Virtual-Machine Health and Service Monitoring

Cisco ESC integrates with the host hypervisor, whether KVM/OpenStack or VMware, to monitor the health of virtual machines. It tracks performance metrics such as CPU use, memory consumption, and other core parameters. It also provides an elaborate framework to monitor service performance-related metrics and other key parameters that you define.

The solution can interface with element managers to determine whether service-related metrics (for example, capacity, load bursts, or number of concurrent sessions) are operating within expected thresholds and time periods. In this way, it allows you to monitor the health of the actual services within the VNF - not just the virtual machine itself. So for example, if you've deployed a Cisco CSR virtual routing instance, you can monitor both the overall health of the virtual machine and the individual VPN sessions inside the VNF.

Agentless Monitoring

Most management systems now in the market require an agent to be deployed in the VNF itself to monitor its health. But this approach has distinct disadvantages in real-world NFV environments, including:

- **Slow time to market:** If every VNF you use needs to have an agent integrated before it can be deployed, the process can add considerable time to deployments.
- **Need for revalidation/re-certification:** Integrating an agent inside a VNF often affects its performance and stability, meaning the VNF may need to be revalidated or certified again by the VNF vendor.
- **Potential support concerns:** It's not uncommon for service providers to use a VNF from one vendor and an orchestration system and agent from another. If there is a problem after integrating the agent inside the VNF, who is responsible for fixing it? This lack of clear accountability poses a serious business risk when operationalizing NFV environments.
- **Potential resource and TCO impact:** An agent is likely to increase the footprint (such as CPU and memory requirements) of the VNF in order to maintain optimal performance, resulting in increased TCO for the overall solution.
- **Scalability limitations:** If you're integrating agents into many different VNFs from an array of vendors, you may have a harder time scaling your environment.

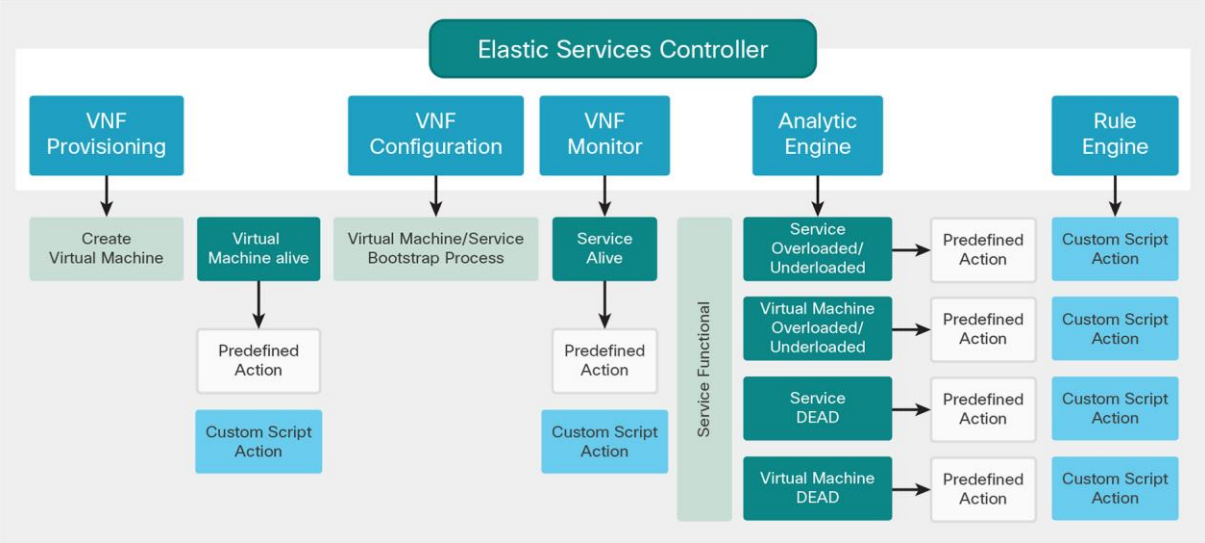
Cisco ESC eliminates all of these concerns by supporting a VNF deployment model that requires no agent at all. Unlike other management platforms, it allows you to continuously monitor the health and performance of your VNFs without introducing added complexity or business risk.

With its agentless mode of operations, Cisco ESC can monitor CPU or memory use to track VNF performance. It can also use other protocols such as SNMP, or even custom scripts if you need to monitor something more specific that CPU- or memory-based monitoring wouldn't reveal.

Customizations: Monitoring and Rules

Cisco ESC builds on its monitoring capabilities by providing an analytics engine to identify problems and events that require action, and a rules engine to define rules and thresholds (Figure 3). Together, these engines automate and accelerate the response of the system to specific conditions or events. Cisco ESC provides a customizable environment to enable monitoring of specialized VNFs out of the box. It can tie back monitoring events into its workflow to trigger the appropriate custom- or system-defined actions.

Figure 3. End-to-End Monitoring with Customizable Analytics and Rules



Cisco ESC provides a northbound API that allows it to integrate with Cisco Network Service Orchestrator (NSO)-enabled by Tail-f, or a third-party orchestration system, to notify the system when a threshold has been crossed or an event identified, such as an unreachable virtual machine. Or, you can define these rules within Cisco ESC itself, and use integrated healing and recovery capabilities of Cisco ESC without an orchestrator.

The solution provides the intelligence to handle both simple and complex rules. A simple rule could be that when a service goes live, advertise its availability to the rest of the system. A more complex rule could define a series of actions in response to a particular event. For example, if resources are getting overloaded, you can direct the system to automatically scale up, scale out, and notify the orchestrator.

All of this intelligence and automation translates to improved service agility. You can realize the full promise of NFV to enable on-demand service delivery and elastic scaling, and more easily meet SLAs.

Integrating with Orchestration and Virtualization Platforms

As an open, standards-based platform, Cisco ESC exposes a northbound interface to integrate with NFV orchestration systems. The solution is completely programmable using a well-defined northbound REST API. It also supports NETCONF and Yang data models “out of the box” to integrate easily with a wide range of Cisco solutions, as well as third-party orchestration and assurance systems. And it supports a wide range of API protocols, both northbound (web portal, NETCONF, REST, CLI) and southbound (OpenStack REST API, SNMP, Gangila, CLI). Through its northbound API, Cisco ESC can notify any system that has subscribed to the events manager of the solution, making it easy to orchestrate and automate even highly complex provisioning scenarios.

Scalability and High Availability

Cisco ESC is a highly scalable system, supporting up to 1,000 virtual machines per ESC instance, with the option to deploy multiple instances. The solution also supports high-availability deployments.

Cisco ESC Use Cases

Cisco ESC provides unmatched intelligence and automation when using Cisco VNFs. But unlike many VNFM tools, Cisco ESC is an open, interoperable platform that can support any vendor’s standards-based VNF and, as a result, virtually any NFV use case or deployment.

The following sections provide some examples of how organizations can use Cisco ESC to accelerate services and simplify their operations.

Cisco vMS 1.0, Cloud VPN

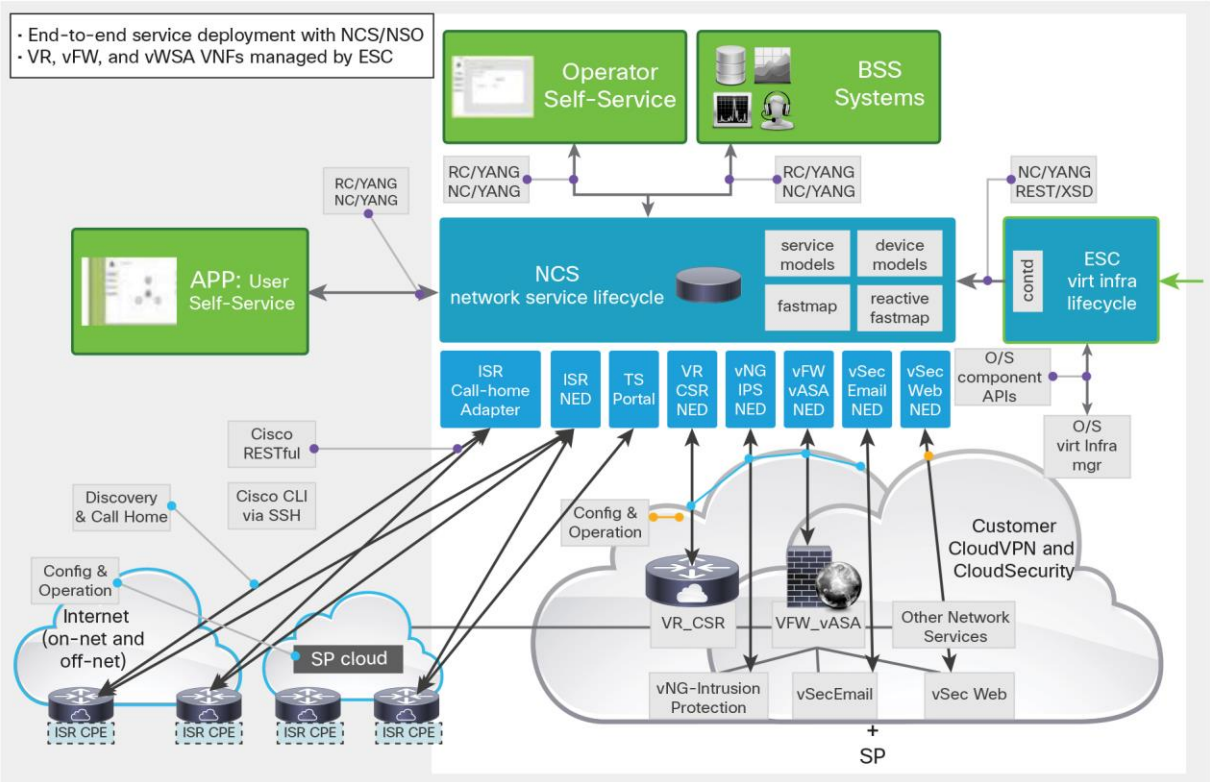
The Cisco Virtual Managed Services (vMS) solution is a platform for software-defined networking (SDN)/NFV service delivery and a set of service software packages such as Cloud VPN. Cisco vMS helps service providers offer cost-effective, secure, cloud-based business connectivity and application services to their end customers with a click of a mouse.

Using Cloud VPN, service providers’ enterprise customers can rapidly create and deploy highly secure business connectivity services over any network access. Cloud VPN software function packages include SSL VPN, IPsec VPN, and remote-access capabilities. They can be combined with firewall, intrusion protection, and web and email security applications. The solution enables you to create and activate them in minutes.

This use case illustrates the role Cisco ESC plays in a larger Cisco NFV solution, encompassing Cisco ESC and Cisco NSO to deliver virtual services in the cloud.

Cisco ESC integrates with the Cisco NSO orchestrator out of the box using the NETCONF-Yang interface, and provides all lifecycle management functions for VPN, firewall, and web security VNFs in the service, including dynamically creating these VNFs, monitoring them, and automated recovery/response to failure scenarios.

Figure 4. Cisco ESC in Cisco vMS Solution



The solution also provides affinity intelligence for VPN placement for each tenant (for example, each service provider customer).

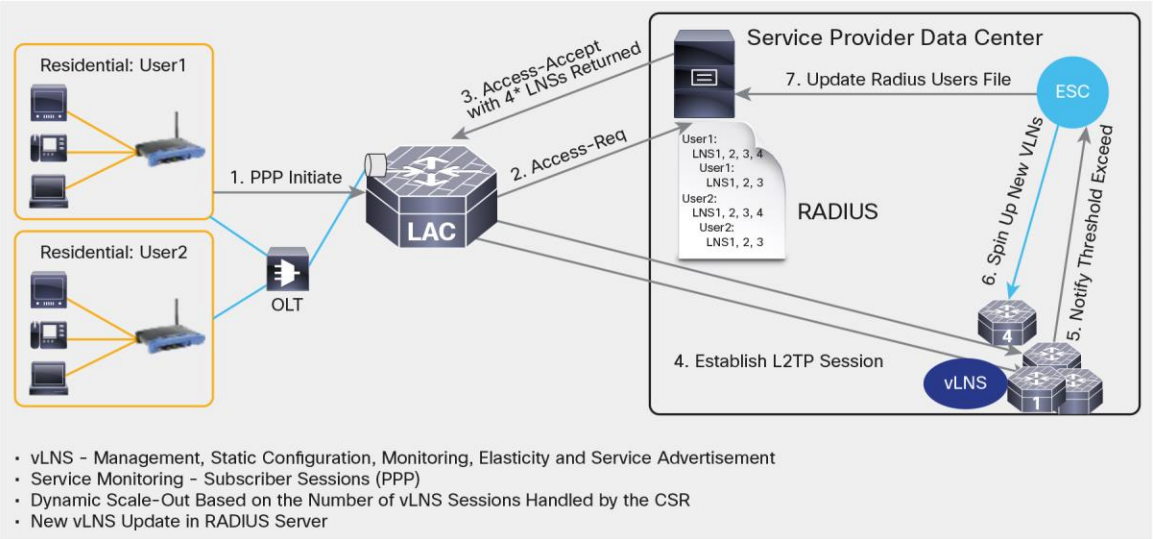
The vMS use case depicted here spans the entire data center. The entire service lifecycle, from onboarding a tenant to configuring physical and virtual devices to activating services, happens automatically, with a click on the GUI. The portal calls the Cisco NSO, which creates the topology files based on the services required for that customer, and passes them onto Cisco ESC to instantiate the service. And this entire process happens in real time. NSO communicates with Cisco ESC to download the configuration profile, brings up the VNFs, and activates Cisco Smart Licensing. Cisco ESC then hands over the VNFs to NSO to set up the dynamic service configurations such as VPN tunnel, firewall policies, and others.

Next-Generation Virtual Broadband

In a next-generation virtual broadband solution, virtualization typically happens in small steps. In certain scenarios, the virtual Intelligent Services Gateway (vISG) or virtual Layer-2 Tunneling Protocol Network Server (vLNS) service is virtualized in the initial stage. During this stage, Cisco ESC can manage and automate the virtualized services, and elastically provision and manage vLNS service modules. In this use case, you can see how Cisco ESC automates the deployment of vLNS virtual machines and provisions day-zero configurations, including static LNS configuration (Figure 6).

When the vLNS is alive, Cisco ESC triggers RADIUS server updates to make the new vLNS service module active to accept new subscriber requests in the solution.

Figure 5. Cisco ESC Enabling Elasticity in a Next-Generation Virtual Broadband Service



Why Cisco ESC?

The introduction of NFV can enable unprecedented speed and efficiency for service providers and enterprises. But too often, these advantages are limited by the complexity, manual operations, and domain-specific expertise that typical virtualization management systems require.

Cisco ESC helps you make the promise of NFV a reality in your environment. It automates the entire VNF lifecycle - including VNF advertisements, smart licensing, and elastic scaling - while providing comprehensive tools to monitor the health of your virtualized resources and services. With standards-based interfaces and well-defined APIs, it provides an open, interoperable, and virtual infrastructure- and VNF-agnostic platform that quickly adapts to your existing environment. By combining all of the capabilities, Cisco ESC can help you fully capitalize on the virtualization revolution to deliver services faster and more efficiently, and give you the agility to quickly respond to changing business needs.

To learn more, visit: http://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-734976-00 07/15