WIND™

Network Virtualization the Easy Way

Wind River Titanium Cloud Delivers a Simplified, Cost-Effective Approach to the Installation, Operations, and Maintenance of Virtualized Critical Infrastructure

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

Network virtualization is a critical part of the digital transformation journey for many businesses. The shift from proprietary hardware to software-based implementations, running on industry-standard servers in cloud environments, will reduce equipment and operating costs and increase flexibility and productivity. Virtualization will have profound business benefits for companies that manage critical infrastructure across many industrial sectors, such as communication services, transportation, healthcare, manufacturing, and energy production.

But the practical implementation of virtualized networks can be a daunting challenge. Even with the most skilled IT departments, virtualization projects can overrun schedules and budgets. The amount of work involved and the staff requirements in a new technology implementation can easily be underestimated. In the transition to software-based networking, companies are finding that their network transformation initiatives go beyond technology and impact their workforce with requirements for new skill sets, retraining, and cultural changes within their organizations.

This paper discusses virtualization challenges in a transformation in progress in the telecom arena. It then analyzes how the Wind River® Titanium Cloud™ virtualization software platform simplifies installation, operation, and maintenance to make network virtualization as easy as possible for network operators running critical infrastructure.

TABLE OF CONTENTS

WIND

ONE COMPANY'S VIRTUALIZATION JOURNEY

A prominent example of virtualization challenges in the telecom sector comes from AT&T. The network operator is on track to move 75% of its network onto software by 2020. To support the transition, AT&T launched a company-wide workforce retraining program to ensure that all employees have the skills they need. But not all operators have resources available to support this level of in-house development and mass retraining.

4G LTE technology is more efficient than previous generations in handling high-bandwidth traffic, but the conventional RAN architecture widely deployed today is challenged to deliver the additional capacity, cost savings, service agility, and scalability that CSPs need to meet future demand.

> "The transformation that we have to undertake is so large by scale and so ambitious by the amount of activity that we couldn't simply retrain and hope that over time our experience would morph itself into what was required to move into a brave new world of a new technology architecture. So we really had no choice except to think about entirely reskilling ourselves."
>
> — John Donovan, CEO,
> AT&T Communications

Given the skill set challenges that telecom and industrial network operators face, it is imperative that virtual networks be easy to install, operate, and maintain. The virtualization business case is largely built on cost savings. If deployment and operations are too complex, then the additional time and resources required could increase costs and undermine the business case.

NETWORK VIRTUALIZATION THE HARD WAY

Critical infrastructure operators have many choices when it comes to selecting a virtualization platform. After all, choice and flexibility are among the big advantages of network virtualization, thanks to the reliance on open standards and open source software, which allow operators to avoid costly proprietary platforms and vendor lock-in. Operators can build their own platforms by downloading the latest OpenStack distribution or by adopting solutions that were originally designed for data centers and enterprise applications. But neither option is simple or easy when it comes to installation, operations, and maintenance.

Operators of critical infrastructure need to focus on the benefits that virtualization will bring to their core business, and not be overwhelmed by the complexity of deploying and operating new software platforms. For example, GE views virtualization and digital transformation as ways to enable new services and boost productivity.

> "GE is really focused on what we call the digital-physical transformation. How do we bridge the traditional assets—whether it be a gas turbine or locomotive or jet engine—to enable a new set of digital services on top of that so that we can go create that next new capability in terms of not just allowing the system to run in a safe and secure manner, but also do so in a more efficient way?"
>
> — Wes Skeffington,
> Senior Principal Engineer,
> GE Global Research

The following encapsulates how network virtualization can be more difficult than it needs to be for operators, outlining the challenges that Wind River has solved with the Titanium Cloud portfolio of products.

Lengthy Installation

The build-your-own approach is very challenging and requires broad in-house expertise. With a plain, "vanilla" OpenStack distribution, the installation process is complex and time-consuming because individual servers—whether controller, compute, or storage node—need to be manually configured one at a time. The process involves acquiring all the images that will be needed for the deployment as well as all the separate installation instructions for the images. OpenStack distributions do not come with

automated provisioning, so any mistakes introduced during the configuration will result in more time spent on troubleshooting. The entire process of installing, configuring, and troubleshooting could take days to complete.

Few companies will want to spend the time, resources, and money necessary to install an OpenStack distribution. It is estimated that a build-your-own approach could add 12 to 24 months to the deployment process, delaying time-to-market for new services and applications.

Inefficient, Unsecure Operations

Operational efficiency is critical to the network virtualization business case. Indeed, much of the cost savings are derived from operational improvements in industrial control infrastructure and communications networks. But not all platforms are inherently designed to provide the security and visibility into the network that are needed to increase efficiency.

Enterprise-based solutions were originally designed to be deployed in large data centers, which have robust, physical security in place to prevent intrusions and protect the equipment. But many of the Industrial Internet of Things (IIoT) and telecom use cases are edge deployments, whereby edge servers will not be installed in a secured data center but at a cellular tower, or inside enterprise premises, or within manufacturing facilities. Since the locations themselves are less physically secure, the virtualization platform must have security built into the system.

Network managers need to know that their virtual network software cannot be tampered with or hacked into. But vanilla OpenStack distributions do not come with such security support, leaving users to bolt on inferior security fixes.

> "Cybersecurity is the most important issue facing the world of Industrial IoT. All it takes is one bad attack and the entire industry will pull back and say, 'We're not going to connect our systems to IoT.'"
>
> — Pirth Banerjee, Executive VP and CTO, Schneider Electric

> "Cybersecurity has to be built in from the ground up—i.e., right into the control system itself. And you have to embed it not just in hardware but in software."
>
> — Wes Skeffington, Senior Principal Engineer, GE Global Research

In addition to security shortcomings, vanilla OpenStack also does not provide full visibility into the state of the network or alarm systems to signal any failures or connectivity issues. These vital operations features must be sourced elsewhere.

Disruptive Maintenance

Scheduled maintenance is inevitable in the life of any network. But the procedures are costly and the longer they take, the higher the cost to the business. Critical infrastructure operators can plan for scheduled outages and manage downtimes, especially if they are short and infrequent. But it's extremely problematic and costly when basic maintenance causes unplanned downtime. For example, a routine patch can take far longer than expected to implement, or a simple upgrade can introduce an error that causes a system-wide outage.

With vanilla OpenStack, network operators can schedule maintenance for routine patches and upgrades. But no matter how short in duration, any outage can be disruptive to network services. Network operators can build redundancy into the network, but this would increase the cost of deployment. For routine maintenance, operators need a network virtualization platform that streamlines the process and won't incur any unexpected downtime.

NETWORK VIRTUALIZATION THE EASY WAY

There is an easier way to implement virtualized networks. The process does not have to be overly complex, time-consuming, or costly. The Titanium Cloud virtualization platform is designed and optimized to simplify installation, operations, and maintenance so that critical infrastructure operators can focus on their core businesses.

The Titanium Cloud portfolio comprises a range of platforms to suit different network operator needs: Wind River Titanium Control for highly reliable industrial control applications; Wind River Titanium Core for communications service provider data centers, central offices, and PoPs; and Wind River Titanium Edge and Wind River Titanium Edge SX for small-footprint telecom network edge applications.

Fast and Simple Installation

Titanium Cloud is delivered as a pre-integrated, single image package that is easy and quick to install and configure. It is truly a plug-and-play platform. Unlike the build-your-own approach or enterprise solutions, which can take days to install, Titanium Cloud can be up and running in just 20 minutes. With automated provisioning and a simple setup wizard, the single image installs and configures each node with no manual intervention, for deployments of any size—from a two-node system to large-scale implementation.

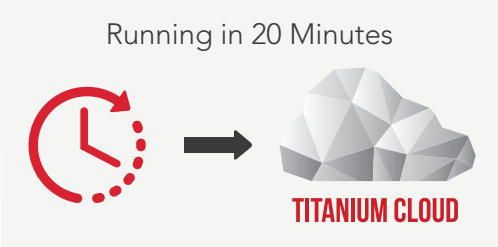

Figure 1. Titanium Cloud is a pre-integrated, single image package that is quick to install and configure

The configuration files do not need to be manually edited. Via the setup wizard, users simply select the personality profile and parameters for the servers. The system automatically discovers nodes and resources and then assigns the profiles and all the necessary functions to any control, compute, or storage node. The network interfaces are defined along with the necessary tenant networks.

The setup wizard stores all configuration parameters so that when the system needs to be expanded, the deployments are repeatable, efficient, and predictable. Users do not have to reinvent the wheel with each system upgrade. When ready, Titanium Cloud nodes perform a system self-check to validate the installation and configuration, and then put themselves into service. It's that simple.

Secure and Reliable Operations

Titanium Cloud ensures that virtual network systems are secure and ultrareliable, delivering six nines (99.9999%) availability, which amounts to less than 30 seconds of downtime per year.

Security is baked into Titanium Cloud from the ground up and is not an afterthought add-on. The platform is built using TL 9000 design methodology and was first to market with the virtual Trusted Platform Module (vTPM), which delivers the highest security in virtual machine environments. The vTPM secures the platform software just as a heavily guarded data center protects physical equipment from malicious attacks. At the hardware level, Titanium Cloud also provides Transport Layer Security (TLS) with certificate storage in TPM 2.0 hardware to protect management operations.

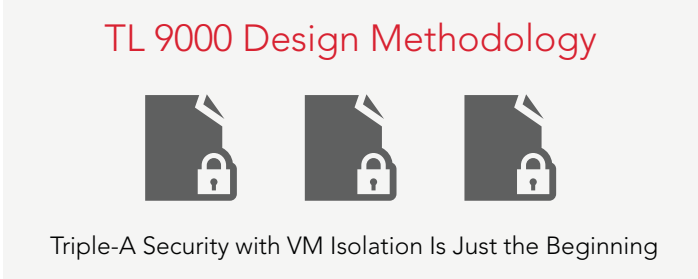

Figure 2. The Titanium Cloud platform uses TL 9000 design methodology and delivers the highest security in virtual machine environments

Other security features include Unified Extensible Firmware Interface (UEFI) secure boot, which ensures that only trusted software can be loaded onto VMs; and cryptographically signed images and support for network-level authentication, authorization, and accounting (AAA). Titanium Cloud also leverages Intel's Enhanced Platform Awareness.

The platform provides total visibility into the state of the network via a remote monitoring dashboard comprising system alarms, analytics, and performance and fault management tools to flag issues before they affect services. The platform monitors parameters including cluster connectivity, process failures, out-of-band activities, and SNMP trap reporting. Alarms alert network managers to problems or automatically trigger corrective actions. Extensive management interfaces with open APIs can be integrated with orchestration services.

Easy Maintenance with No Downtime

To ensure that patches and upgrades do not disrupt network services, Titanium Cloud features an integrated, system-aware upgrade wizard that automates the entire upgrade process. Whether it is a minor patch or a full system upgrade, there is no service downtime during the process.

> "Wind River Titanium Control provides us a platform where we can host a lot of the applications that today are distributed across a mess of boxes. . . . [It] allows us to consolidate that and do some of the best practices that cloud brings in terms of how to manage networks—it all becomes a software-defined function that can be centrally managed, upgraded, and controlled."
>
> — Wes Skeffington,
> Senior Principal Engineer,
> GE Global Research

This is achieved through support for in-service patching and hitless upgrades. First, virtual functions are live migrated from one server node to another. Then the operating system, OpenStack components, hypervisor, and virtualization infrastructure manager (VIM) are upgraded along with the rest of the Titanium Cloud package. In this way, the entire system and all the security features remain up and running. None of the platform's features are sacrificed during the upgrade.

Network managers have visibility into the process through messages, logs, and alarms. Also, rollback points are created for controlled fallback, if needed, and all system data will be reformatted and migrated.

Titanium Cloud performs system-wide updates that are completely transparent to users, who see no service downtime. Even during maintenance, the platform delivers service continuity that businesses can rely on.

Figure 3. Titanium Cloud's integrated, system-aware upgrade wizard automates the entire process, whether a minor patch or a full system upgrade

CONCLUSION

Wind River Titanium Cloud takes the pain out of installation, operations, and maintenance of virtualized networks. By reducing complexity and optimizing for security and reliability, the platform saves critical infrastructure operators time, money, and resources, while also removing barriers to deployment. The operational efficiency of Titanium Cloud enables digital transformation initiatives across a variety of sectors and allows operators to focus on their core business and accelerate the introduction of new services.

WIND

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.