Sigma**Uptime**

volume 15 number 2

The Digital Workspace

VMware's new Workspace ONE is designed to simplify and unify disjointed digital working styles.

Technology services to help you streamline operations, reduce costs and improve business processes.

Companies today must align IT strategy with their corporate objectives, strategy and business model. Pivot has created a portfolio of operating companies and partners with a focus on helping you enhance and extend the capabilities of your technology assets.

Pivot provides technology services ranging from initial needs assessment and design, through procurement and implementation, to on-going support. As an adjunct to your IT team, we provide the resources that allow your team to offload some of the day-to-day operational challenges and focus on innovations that will drive business value and competitive advantage.

Contact us to learn more.

PIVOT
TECHNOLOGY SERVICES

www.pivotts.com   888-895-0495

Contents

4

Sigma Uptime

the Digital Wor

VMware's new Workspace ONE is designed to simplify and unify disjointed digital working styles.

Mobile, cloud and collaborative technologies have dramatically changed both the way we work and the workplace itself. In fact, even the idea of being "at work" has become a rather squishy concept — that smartphone in your pocket means you can be "in the office" even if you're physically at the grocery store, the bank or an A$AP Rocky concert.

Untethered from traditional company-owned desktop workstations, today's workers can get things done from just about any location at any time. It would not be unusual to begin the day checking email from a laptop at home, updating Dropbox files from a tablet at the coffee shop, working within key line-of-business applications on a PC at the office and finally using a smartphone on the way home to communicate with colleagues via social apps such as Yammer or Chatter.

"We don't go to work, we work on the go," said Chris Reed, Mobility and EUC Practice Manager, Sigma Solutions. "Unfortunately, this new work style isn't always as fluid and effective as it is meant to be. Instead of becoming more agile and responsive, organizations often become just the opposite — fragmented and inefficient.

"When new technologies are implemented in a piecemeal fashion without a cohesive end-user strategy, organizations wind up struggling to manage and secure the proliferation of devices, apps and services. Users can become frustrated when they find themselves constantly switching between multiple devices and applications in order to complete work."

Key Components

An evolving set of solutions comprising the "digital workspace" are emerging to address the challenge. The workspace is designed to unify these transformative technologies in a more consumer-like, employee-friendly environment that improves ease of use, security and end-to-end support. It orchestrates desktop virtualization, device management, application delivery, identity management

and more into a single platform that allows users to simply and securely access applications, content and services with any device.

Desktop virtualization in particular plays an important role in the digital workspace. Virtual desktop infrastructure (VDI) allows IT to centrally manage the entire desktop environment and deliver it to users as a service. When integrated into the workspace concept, VDI reduces endpoint and platform dependence and facilitates user access to other applications and data that may be relevant.

Enterprise mobility management (EMM) improves the security footing in the digital workspace by helping IT enforce security policies across a range of employee devices. EMM tools streamline device onboarding, push out updates and applications, and segregate personal and business data.

Identity management is another critical element. Growing numbers of end-users require access to resources on either side of the network firewall, and many organizations devote significant time and effort to the task of adding, changing and deleting user information and permissions. Identity management solutions streamline these processes, ensuring that users have secure and seamless access to the applications and resources that correspond to their profiles. Identity management can also enable automation and self-service, potentially saving millions of dollars per year in support costs.

'Consumer Simple, Enterprise Secure'

With the recent release of its Workspace ONE platform, VMware has made it easier than ever for organizations to deploy all the elements required for the digital workspace. The result of more than two years of planning and well over $1 billion in investments, Workspace ONE integrates device management, application delivery, identity management, data security and more in a platform the company describes as "consumer simple, enterprise secure."

"From a user's perspective, Workspace ONE is very straightforward. It delivers a consumer-like experience with self-service access to applications across all devices," said Reed. "At the same time, it delivers improved security from an IT perspective with better management over devices and apps and stricter control over who has access to company data."

Self-service device provisioning allows users to self-configure their laptops, tablets and smartphones — both company-owned and personal devices — in ways that seem familiar and comfortable. Once authenticated through the Workspace ONE app, users can instantly access a personalized enterprise app catalog where they can subscribe to almost any mobile, cloud or Windows app. One-touch mobile single sign-on en-

AirWatch Complements Workspace ONE

With the latest release of its AirWatch enterprise mobility management (EMM) platform, VMware is extending its digital workspace strategy by improving security and workflows for business mobility.

Workspace ONE allows users to access any application — native, web or remote — through a single application catalog across every device. With mobile single sign-on (SSO), AirWatch 8.3 allows users to access these apps without passwords or complex PINs. AirWatch 8.3 also introduces template-driven workflows that identify and recommend the best iOS apps, configurations and policies for their business initiatives.

"Employees will be able to access virtually any app with one click in a new mobile experience that's focused on protecting privacy," said Noah Wasmer, senior vice president of mobile products, End-User Computing, VMware. "For administrators, AirWatch 8.3 will facilitate new workflows for line of business built on the VMware foundation of world-class security and management."

ables simple access to all apps without having to enter passwords or PIN numbers for each one.

Identity and device management combined with VMware's ComplianceCheck Conditional Access enforces security policies across any application or device. This approach combines traditional identity- and role-based policies with device compliance policies such as location and device security.

Workspace ONE was designed with a strong emphasis on giving employees the ability to access and use the resources they need in ways that make the most sense for them. Gartner Research Vice President Matt Cain said that approach is important with a technology-savvy workforce. Empowering users to decide when, where and how work is done will encourage greater collaboration and innovation and help create a more productive and satisfied workforce.

"Today's employees possess a greater degree of digital dexterity," said Cain. "They operate their own wireless networks at home, attach and manage various devices, and use apps and Web services in almost every facet of their personal lives. They participate in sharing economies for transport, lodging and more. . . . Organizations that formally embrace and extend the digital competencies of their employees will experience improved business outcomes and gain competitive advantage."

Unlocking the Value of VDI

Converged and hyper-converged infrastructure solutions enable the rapid rollout of VDI along with predictable performance and seamless scalability.

Desktop virtualization is becoming more and more relevant in the "post-PC era" — a term introduced by Steve Jobs when the Apple iPad was released in 2010. Today's mobile workers no longer sit in front of a PC, but they still need ready access to applications and the desktop environment. By storing a user's desktop in the data center and delivering it to virtually any device, virtual desktop infrastructure (VDI) provides a desktop experience while freeing employees from the confines of the physical workspace.

"While mobility is increasingly prevalent, there remains a gap between the mobile experience and the desktop experience," said Chris Reed, Mobility and EUC Practice Manager, Sigma Solutions. "Mobile devices are great for accessing email and web content, but they aren't really productivity tools. Desktop virtualization helps to bridge the gap between the desktop and mobile worlds."

Although users still need a desktop environment, it makes little sense for organizations to buy, deploy, manage and support PCs — particularly for users who are frequently away from the office. However, desktop virtualization comes with its own set of headaches that has limited its value in the enterprise environment.

"Desktop virtualization enables IT to centrally manage desktop images, increasing flexibility and security while reducing total cost of ownership," Reed said. "On the other hand, VDI is notoriously difficult to implement. Organizations often need server and network upgrades to meet performance demands and ensure a high-quality user experience. Significant storage capacity is required to store and back up virtual desktop

images and data. Hardware complexity frequently stalls VDI projects.

"That's why converged and hyper-converged infrastructure solutions are viewed as a game-changer for VDI. Convergence removes that complexity so that organizations can deploy VDI faster and with more confidence than ever before."

'Preferred Platform'

A new report by Research and Markets predicts that the global market for VDI will grow at a compound annual rate of 54.9 percent through 2020. This projection represents a significant increase over the firm's earlier forecast of 32.47 percent growth through 2019. According to the report, desktop virtualization has become a top priority for organizations seeking to reduce operational costs while giving employees anywhere, anytime access to data.

Of course, industry experts have been saying "this is the year for VDI" for some time now. Clear challenges with VDI implementation have kept that prediction from becoming a reality. Desktop virtualization requires significant expertise and a scalable architecture that can respond to changing demands. Poorly executed VDI deployments lead to poor user experiences, preventing organizations from maximizing the cost and operational advantages that VDI has to offer.

Converged and hyper-converged infrastructure solutions promise to change that dynamic by simplifying VDI implementation. With converged infrastructure, compute, networking, storage access, virtualization and management resources are delivered in one preconfigured, pretested, highly automated solution. Hyper-convergence builds upon this model by more tightly integrating these components and adding data optimization and protection capabilities.

Converged and hyper-converged solutions accelerate the roll-out of IT services by eliminating the need to design, build and configure infrastructure using best-of-breed components. Be-

cause resources are pooled in a modular system, performance and capacity can be increased by simply adding modules as needed.

"Convergence has gained a lot of attention because it gets IT shops out of the systems integration business," said Reed. "But convergence really shines when it comes to VDI, providing predictable performance that enables the delivery of virtual desktop services to thousands of users. According to a recent IDC Analyst Connection, converged infrastructure solutions are becoming the preferred platform for desk-

> # "Convergence enables you to scale quickly and cost-effectively with minimal disruption."

top virtualization because they directly address the pain points of VDI deployments."

Ready to Grow

Growth is a primary concern with VDI. Organizations need the ability to expand capacity to ensure a high-quality user experience. Traditionally that meant overprovisioning compute and networking resources due to the time required for implementation.

"Overprovisioning is one way to solve the problem but it ties up IT budget in underused resources," Reed said. "Convergence enables you to scale quickly and cost-effectively with minimal disruption. Depending upon the solution, you can scale out the var-

ious resources incrementally without increasing complexity or operational overhead."

Today, there are a number of converged infrastructure options, including blocks built using traditional data center architectures, racks built with industry-standard servers and appliances built using industry-standard servers but with simplified operation. In addition, there are systems that have been designed and validated for VDI and template-based solutions for repeatable deployments.

"Tested and benchmarked solutions further minimize risk by enabling more predictable, reliable results. However, organizations will need to evaluate the various 'flavors' of converged infrastructure to determine the best fit for their performance and scalability needs," said Reed.

Long term, convergence reduces total cost of ownership by simplifying management and improving resource allocation. Unified management also improves security by enabling centralized, policy-based control over workloads and data.

There's no question that mobile devices have dramatically changed how we work. Nevertheless, the continued demand for PCs and laptops indicates that tablets and smartphones have not yet replaced the desktop. Desktop virtualization enables organizations to give mobile workers access to applications and data while maximizing flexibility, security and efficiency.

Converged and hyper-converged infrastructure solutions provide an integrated, centrally managed platform for VDI that further reduces costs and operational headaches. It enables IT organizations to implement VDI confidently and cost-effectively, and to seamlessly scale to thousands of virtual desktops while meeting user requirements for a high-quality experience.

Virtualizing the Network

VMware's NSX enables new levels of network agility and creates a path to the software-defined data center.

Traditional network architectures are increasingly ill-suited for modern data center workloads. The need to support countless objects, devices, people and applications has substantially increased network traffic and connectivity demands, placing immense strain on the hardware-centric network designs that have been used for nearly 30 years.

VMware's NSX network virtualization platform can relieve much of the burden. NSX treats the entire physical network as a common pool of transport capacity that can be consumed and re-purposed on demand. That makes it easy for organizations to roll out, scale and adjust workloads and resources to meet changing needs.

"Traditional networks weren't designed to meet the constant demand for new services that organizations face today," said Chris Reed, Mobility and EUC Practice Manager, Sigma Solutions. "Everybody wants to be agile, but provisioning network services is really complicated. You have to reconfigure switches, routers and firewalls, and you have to take your time to get it right — configuration errors are the No. 1 cause of network downtime.

"VMware NSX lets you bypass all of that and reduce provisioning time from days to just a few seconds. That's a game-changer for IT. With the ability to deploy, change and move network resources at will, you can scale the network to meet changing demands and lay the foundation for a software-defined data center."

Removing Complexity

In traditional network design, tiers of switches and routers implement diverse protocols to connect devices using proprietary interfaces. A typical network will employ a multitude of protocols, each designed to regulate a specific function such as data interchange, access method, data transfer speed and more. Any change to the network requires multiple updates to protocol-based mechanisms using device-level management tools. That level of complexity is a huge problem in a virtualized environment where IT may have to configure thousands of virtual machines. Significant changes can take days or weeks, and make it difficult for IT to apply a consistent set of access, security, QoS and other policies.

VMware NSX resolves these issues by extending the principles of virtualization across the entire data center. In server virtualization, an abstraction layer (hypervisor) reproduces key attributes of a physical server such as CPU, RAM and network connectivity in software, and these components can be programmatically assembled to produce a unique virtual machine in a matter of seconds. Similarly, network virtualization uses software to reproduce layer 2 to layer 7 networking services such as switching, routing and load balancing. These services can then be programmatically assembled to quickly produce unique virtual networks.

Virtual networks can be provisioned, changed, stored, deleted and restored without making any configuration changes to the physical network infrastructure. This allows organizations to run entire virtual networks in parallel on top of existing network hardware, which is merely responsible for transporting data according to pre-programmed policies. These virtual overlay networks are customized for specific workloads and run independent of all physical and virtual network devices.

NSX causes no disruption of physical networking resources. It can be deployed on any IP network from any vendor — including both traditional networking models and next-generation fabric architectures. The physical network infrastructure already in place is all that is required to deploy network virtualization with NSX.

Network automation, faster provisioning and improved resource utilization are the obvious benefits of NSX, but there are many others. It gives organizations the ability to run multiple isolated virtualized networks simultaneously to support the needs of different customers, lines of business or departments. It makes it easy to spin up a network segment for application testing or other intermittent workloads. NSX also includes an API that integrates with

Boosting Security

NSX also provides several security advantages over traditional hardware-defined network security approaches, including in-kernel, scale-out firewalling distributed to every hypervisor. This firewall distribution allows a fine-grained approach to security known as "micro-segmentation." Instead of having just one firewall at the network perimeter, a micro-segmented network has firewall protection at the perimeter, between application tiers and between devices. This allows the creation of more compact "zero-trust" security zones and boosts both east-west and north-south firewalling.

East-west firewalling is potentially a breakthrough defense against modern advanced persistent threats (APTs). Once an APT has breached the network perimeter, it often moves laterally through the network to harvest credentials and collect confidential data. Micro-segmentation can limit this east-west access, but that hasn't been possible with traditional firewalls — the sheer number required would make configuration and change management functionally impossible.

NSX makes micro-segmentation operationally feasible with the creation of a distributed firewall embedded as a service in the hypervisor kernel of every virtual network. The firewall service enforces security policies at the interface level, ensuring that every data packet is inspected as it is sent from one virtual machine to another. This allows strict isolation of network segments with very little management overhead. Policy and configuration changes applied at the kernel level are instantly propagated throughout the network.

This type of policy-driven automation is key to the development of a software-defined data center (SDDC) in which legacy infrastructures, cloud platforms and emerging workload services are integrated in an overarching architecture that drives business agility. The SDDC vision is one reason 88 percent of organizations in a recent SDxCentral survey said it was "important" or "mission-critical" to find a network virtualization solution in the next two to five years.

"Virtualization technologies have transformed the way IT handles servers and storage, and now network virtualization with VMware NSX is delivering the same kind of transformative effect for network and security operations," said Reed. "NSX eliminates a lot of existing barriers in physical networks, enabling unprecedented levels of agility and efficiency without any disruption to the existing infrastructure. NSX creates a clear path to a software-defined approach to IT delivery that will drive both economic and operational efficiencies."