



Telework, Workforce Mobility and Disaster Recovery in Federal Agencies

Technology Best Practices

Overview

The record snowstorms that paralyzed Washington, D.C. in the winter of 2009/2010 underscored the effectiveness of telework as a strategy for keeping the wheels of government turning when employees cannot get to their offices. Initial estimates of \$100 million per day in lost productivity were revised downward to \$71 million by the Office of Personnel Management, thanks to the contributions of teleworking federal employees. This positive outcome has given new urgency to pending legislation -- the Senate's Telework Enhancement Act of 2009 and the House's Telework Improvements Act of 2009 -- both calling for federal agencies to create expanded programs that allow employees to telework to the maximum extent possible.

Further, the Base Realignment and Closure (BRAC) process currently underway within the Department of Defense will present many employees with the prospect of a move to a new location. Telework is one of the alternatives being offered to ease the impact of BRAC on displaced workers.

Although there is renewed interest in telework -- and its sister scenarios, workforce mobility and disaster recovery -- agencies continue to express concerns about such issues as data security and worker productivity. Now, new advances in information technology offer agencies improved solutions for telework and mobile work, both during normal situations and in a disaster scenario. These technologies, including desktop and server virtualization and Web-based collaboration, provide a high level of data security, are easy and cost-effective to implement, use and support, and deliver excellent reliability and consistent performance across different usage scenarios. They also offer the freedom to use a wide variety of computing devices, network connections, and existing agency software and infrastructure.

This white paper will describe best-practice technologies for telework, workforce mobility and disaster recovery that have been proven in private industry. These technologies can enable federal agencies to expand their initiatives with the least amount of budget and staff resources, while giving employees simple, secure and reliable solutions for connecting to the information and resources they need to remain productive while working outside the office.

Implementing technology best practices

Desktop virtualization: delivering a full user desktop as an on-demand service

One of the best solutions for telework is desktop virtualization, a new technology that delivers a full, personalized desktop of applications and other resources to each worker over the network. At a high level, this means means that instead of installing and running software and the operating system locally on each PC or other computer, these components, plus the user's personalizations, run on servers in the datacenter. They are delivered "virtually" to users -- either a desktop image is transmitted to the user's computer, or the desktop is streamed down to the device.

Each time an employee logs on to the agency's network, his or her virtual desktop is dynamically assembled in the datacenter utilizing the latest applications and operating system version. IT teams can easily and efficiently manage many desktops because the virtual desktop solution is centralized on servers.

Desktop virtualization also offers the ability to tailor the desktop according to the needs of the individual. Different types of workers need different types of desktops. Some require simplicity and standardization, while others require high performance and personalization. Customizing the virtual desktop in the datacenter minimizes IT administration and helps to ensure a high level of user productivity and satisfaction.

It's obvious why desktop virtualization is an ideal scenario for remote, mobile and displaced workers. IT teams are relieved of the burden of tracking down and performing maintenance on devices scattered across multiple locations. Virtual desktops can be delivered to just about any type of device, giving users the freedom to choose a PC, Mac, thin client or smartphone – or to use any available device with a network connection during a disaster situation. For strong security, application data remains in the datacenter behind the firewall, and desktop images are encrypted over the network. Even when the virtual desktop is streamed to the device, no data is left behind once the user session ends.

Web conferencing: effective teamwork regardless of employee location

Teambuilding and interpersonal relationships can suffer when individuals lack regular contact with colleagues and managers. To make telework and workforce mobility more effective, and to maintain continuity during an interruption, agencies need a tool that enables employees to collaborate on projects and documents, and hold meetings without requiring travel.

Web conferencing solutions allow employees to schedule and conduct meetings or one-on-one collaborations with anyone who has a browser-enabled device. Meeting attendees do not need pre-loaded software or administrative privileges to participate – they can attend by simply clicking a Web link sent from the meeting host. Once all invited attendees are in the meeting, the presenter can instantly share any file or application on the desktop, change presenters, or give keyboard and mouse control to an attendee.

Not only does online collaboration boost productivity while reducing travel costs, but it also helps to build and maintain work relationships when individuals are away from the office for extended periods or permanently.

Server virtualization: fast recovery from an interruption

Server virtualization, which allows more than one “virtual machine” to run on the same physical server, is an important technology for disaster recovery. Provisioning capabilities of a server virtualization solution enable server workloads on a failed system to be restarted quickly on any other available server, dramatically reducing agency downtime. Essentially, by using virtualization technology, an IT team can transmit a virtual machine over the network and make it available on another server in an alternate location for employees to access. This capability alone can cut downtime in the event of system failure from days to hours, or less.

Server virtualization makes it possible to run multiple, non-compatible workloads on the same server in “isolation,” helping to minimize the number of physical machines that are needed in a disaster recovery facility – or the main datacenter.

Putting telework concerns to rest

Ensuring maximum productivity

Sustaining user productivity is one of the top concerns for agencies that are implementing or expanding telework initiatives. There are several aspects to optimal user productivity that can be resolved using technology solutions; these include a positive user experience with specific applications; resolving network latency; and fixing IT issues.

High-definition experience

Employees whose jobs require sophisticated, specialized software, such as audio, multimedia or 3D graphics, need the same high performance and responsiveness at home or on the road that they would enjoy in an agency office. New desktop virtualization technologies available today can deliver a high-definition user experience over any network connection. By cutting bandwidth requirements by up to 90 percent, these technologies ensure high availability and reliability.

WAN optimization

Especially when employees are traveling or are displaced due to a disaster or other interruption, slow performance of desktops over wide-area networks can pose a challenge to productivity and satisfaction. Latency over the WAN, especially when employees are connecting at long distances from the datacenter, can significantly impact response time and force them to wait for software to launch or actions to be implemented.

There is technology available to optimize desktop and application delivery over IP-based WANs, including private leased lines, public Internet VPNs, and satellite and wireless WANs. This technology, installed in the datacenter, automatically and dynamically applies to each data flow the best combination of performance-boosting techniques depending upon the application, the data and the network conditions. Teleworkers and mobile employees will experience LAN-line application performance over the WAN, which means less time waiting and more time using their desktop applications and other resources.

Online technical support

Nothing can discourage employees from teleworking faster than technical problems. Whether related to the network, the server, the device or even the application itself, the result can be frustration, lost productivity and repeated calls to the help desk. Instead of trying to diagnose a problem over the phone, federal agencies need tools to pinpoint the source for fast resolution.

Web-based support tools enable an IT staff member to view and, with permission, take over a user's computer session to troubleshoot and fix issues, and train the user to avoid future problems. This approach avoids the need for teleworkers and mobile users to bring their devices into the agency for support, and helps ensure fast resolution so the worker can stay productive. Further, during a disaster scenario or other interruption, IT staff can still assist employees even when both groups have been displaced.

Strengthening data security

Another major telework and mobile work concern expressed by many federal agencies is data security, especially when workers are using home computers that may not be equipped with the latest antivirus and other protections.

Policy-based IT control

Delivering applications over the network – particularly the Internet – demands a security solution that can safeguard data from hackers and other cyberspace threats. For telecommuting security, the National Institute of Standards and Technology (NIST) recommends installation of anti-virus and spyware-removal software on each computer; however, it is very difficult to ensure that remote devices – especially public terminals – have full and up-to-date protection. Therefore, it is critical to have a method for remotely controlling the degree of user access to applications based on how secure each device is.

For example, if a mobile user is connecting from a public Internet kiosk, it would be undesirable to allow data to be downloaded and possibly left on the machine. Or if a teleworker's antivirus protection is not current, it would be unwise to allow data to be saved on the computer until the antivirus has been updated. For practical reasons, IT staff must be able to enforce these controls from the datacenter.

Virtual private networks (VPNs) based on the Secure Sockets Layer (SSL) protocol can provide secure access to specific application resources. They use a downloadable Web software client that does not require on-site installation or updating by IT staff. In addition to stringent encryption of application data over the network – also called for by NIST – and support for two-factor authentication devices such as tokens, these SSL VPNs offer centralized, dynamic controls over user actions including viewing, downloading, saving, editing or printing based on the security level of each work scenario.

Protection against theft and loss

There have been a number of cases involving the potential exposure of highly confidential data, such as Social Security numbers, when a computer brought home by an agency employee was stolen or mislaid. To avoid this possibility, desktop virtualization keeps sensitive application data behind the agency firewall instead of stored locally on laptops, PCs or other devices. If a computer is lost or stolen, this data is not placed at risk because it remains securely in the datacenter.

Single sign-on access and password management

The use and management of application passwords can be a big security issue for federal agencies and a giant headache for users and IT staff alike. Many applications are password-protected, forcing users to remember multiple logins and take care of password changes on a regular basis. With so many different passwords to manage, employees may write them down or use weak passwords, increasing security risks – especially when working from an untrusted device. They also may overload the help desk with requests for password assistance and resets.

Implementing an enterprise single sign-on (ESSO) solution reduces the burden of application passwords for users and IT staff while strengthening security. With an ESSO solution, the logon process for individual applications is automated: users log on just once to the agency's system and the solution authenticates them to each application. This means a single password to remember instead of many, and consequently, fewer help desk calls.

An ESSO solution typically provides powerful, centralized management tools for IT staff, allowing them to specify strong passwords, automate application password changes and quickly terminate a user's access. These solutions also support the use of two-factor authentication tokens, biometrics and other technologies.

Conclusion

There are a number of different issues that must be resolved before a federal telework or workforce mobility initiative or a disaster recovery plan can succeed. One critical enabler is the IT system: if people have a fast, simple, secure and high-performance way to access their desktops and teammates and obtain technical support from any location, on any device or connection, they can focus on getting work done. Similarly, the right technology can ease the IT department's challenges of managing an increasingly distributed user environment.

Thousands of companies have successfully implemented technologies that provide the latest in virtual desktop delivery, data security, WAN optimization, and remote support and collaboration. These best-practice solutions are making it feasible and cost-effective for people to work productively from anywhere, and are delivering benefits of improved retention and satisfaction; reduced costs, congestion and environmental impact of commuting and other travel; and greater flexibility.

Learn more www.citrix.com/Federal

The Citrix Delivery Center™ product family is composed of virtualization and networking product lines for an end-to-end system that virtualizes servers, applications and desktops, centralizes them in the datacenter and broadcasts them to users over any network as an on-demand service:

Citrix® XenDesktop™ is a desktop virtualization system that centralizes and delivers desktops as a service to users anywhere, improving security and reducing desktop TCO.

Citrix® XenApp™ is a Windows application delivery system that virtualizes applications, manages them in the datacenter and delivers them as an on-demand service to users anywhere.

Citrix® XenServer™ is an open, enterprise-class, cloud-proven virtualization platform with advanced virtualization management and automation that transforms datacenters into dynamic delivery centers.

Citrix® NetScaler® is a Web application delivery controller that accelerates performance while reducing costs and improving Web application security.

Citrix® Access Gateway™ is an SSL VPN for secure application access, providing users with easy, anywhere access, and providing administrators with market-leading application-level control.

Citrix® Branch Repeater™ is a branch optimization solution that accelerates and amplifies applications for users working in remote locations.

Citrix Receiver™ is a lightweight software client that empowers users to choose their business applications and desktops, and receive them on any device on-demand from the Citrix Delivery Center.

©2010 Citrix Systems, Inc. All rights reserved. Citrix® is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.