Guest Blog: Remote Desktop Team Considerations

Devolutions

THIS ARTICLE IS PART OF A BLOG SERIES CREATED BY THE PETRI IT KNOWLEDGEBASE TEAM AND TECHNICAL WRITER MICHEAL OTEY, IN PARTNERSHIP WITH DEVOLUTIONS.

In today's corporate environment, IT administrators typically need to manage many different remote systems. These systems can be physical systems that are on-premises or they can be virtual machines (VMs) that are local or in the cloud. Although scripted management is a growing trend for remote management, almost every administrator uses Remote Desktop Connections for various management tasks many times a day. Almost all medium businesses up through the enterprise have many people using Remote Desktop Connections, and these users are often separated into different systems or application management teams. Let's have a closer look at some of the most important team considerations for using Remote Desktop Connections.

Standardize Your RDP Connection Names

One of the first steps toward better team support for your Remote Desktop Connections is to standardize your RDP file connection names. Using standardized system names and RDP files names enables all of your administrators and other Remote Desktop Connection users to quickly identify and connect to the desired remote systems. Standardized system and RDP names eliminate guesswork and prompt better team efficiency.

Organizing Your RDP Connections with Shared Folders

One of the best ways you can make your team usage of Remote Desktop Connections more efficient is by organizing your different RDP files into shared folders. Shared folders enable all your administrators and other authorized users to manage like groups of remote systems without having to create their own set of unique and different desktop icons. Instead, they can just create shortcuts to the existing shared folders of RDP connections on their desktops. You can lock down the access to the folders using Windows share permissions. Using shared folders for Remote Desktop Connections fosters administrative standardization and productivity.

Locking Down Your Remote Desktop Connections

For auditing purposes, it's important not to use shared administrator accounts on your remote systems. Using shared administrative accounts makes it impossible to later audit the administrative changes on those remote systems. If you adopt shared folders, be sure to apply specific permissions to those folders and do not include the Everyone role in those permissions. In addition, shared RDP filesshouldrequireremoteloginsbyselectingtheAlwaysaskfor credentials prompt in the RDP file.

Document the Remote Desktop Connections and Management Actions

When you're working with teams it's also important to document both your connections as well as the common management actions for those remote systems and to store that documentation in commonly accessible locationssuchasOneDrive,SharePoint,orafileshare.Although experts typically know their way around Remote Desktop Connections, new administrators and other application managers may not. For instance, document the use of keyboard shortcuts such as using CTL+ALT+END on the remote desktop in place of CTL+ALT+DEL or using CTRL+ALT+PLUS SIGN (+) in place of the PrtScn. PetriBlogSeries-RemoteDesktop-Team-Considerations

Taking Advantage of Third-Party Remote Desktop Management Tools

You can also use third-party remote desktop managementtoolstomakeyourorganization'sremotesystem management both more efficient and more secure. Tools such as Devolutions Remote Desktop Manager have built-in team support that includes centralized remote password management; support for multiple remote tools such as VNC, Putty, LogMeIn, and Citrix; as well as integration with other management tools such as VMware and Hyper-V.