Maximize your Remote Desktop Services

White paper

Parallels®

An Overview of Remote Desktop Services

Virtualization has added new issues to information technology. Today, businesses look not only at optimizing business resources, but also at management of when, where, and how data is accessed. Remote desktop services (RDS) allow businesses to deliver secure remote services to end users effectively.

An Overview of Remote Desktop Services

Virtualization has added new issues to information technology. Today, businesses look not only at optimizing business resources, but also at management of when, where, and how data is accessed. Remote desktop services (RDS) allow businesses to deliver secure remote services to end users effectively.

What are Remote Desktop Services?

RDS is a component of the Windows Server® operating system, and was formerly known as terminal services in Windows Server 2008 and earlier versions. It enables users to remotely access a computer or virtual machine on a network. With RDS, any computer that supports remote desktop protocol can remotely access the full desktop and Windows® software. Windows NT 4.0 first featured RDS in the form of terminal services, which improved with every new version of Windows Server OS. Microsoft added advanced remote desktop features to terminal services and changed the name to Remote Desktop Services in the Windows Server 2008 R2 edition and Windows Server 2012. Today, users can take advantage of RDS to access corporate networks from the comfort of their homes.

How do Remote Desktop Services Work?

In simple terms, RDS runs applications or user desktops on the server rather than on user workstations. The RDS server sends screen images of the user desktop to the end user workstation, and keystrokes and mouse clicks are returned to the server. Terminal servers either use a Virtual Desktop Infrastructure (VDI) environment or shared sessions to deliver user desktops remotely.

Virtual Desktops with Remote Desktop Services

RDS offers a low-cost virtualization solution to businesses of all sizes. RDS runs on Windows terminal servers in which the client connects to one or more servers. Unlike VDI environments where user applications run in a virtual environment, applications are run on the terminal server. The user desktop is remotely delivered, providing a native-like experience to the end user.

Remote Desktop Services for Business — SMBs and Larger Enterprises

Businesses can choose from two options to deliver virtual desktops: VDI and RDS. The latter provides low-cost virtualization solutions, and the complexity of handling virtual machines is comparatively low. Today, small businesses are considering the implementation of RDS as a cost-effective solution. According to Business News Daily, more and more small and medium businesses are looking at Desktop-as-a-Service (DaaS) as a good solution when it comes to reallocating resources or outsourcing IT processes. Windows 2008 R2 offers additional benefits in the form of the RD Web Interface feature. This new feature allows businesses to publish RDS applications over the Internet, and users can simply type the URL in the browser to access them. For enterprise networks, this results in more reliable and faster networks, streamlined IT services, and cost-effective remote solutions with enhanced security.

Remote Desktop Services with Thin Clients

A thin client is a program that depends on another computer to perform computing tasks. As they are not fully-featured computers, thin clients cost less than regular PCs. In an RDS environment, regular PCs can be replaced by thin clients to reduce costs. A user first connects to the terminal server using a thin client. The terminal server, in turn, connects to various other servers such as file servers, Microsoft exchange servers, application servers or SQL servers to deliver the required data to the end user with a native-like desktop experience.

Remote Desktop Services Data Security

While RDS provides innovative features like RD Virtualization Host, RemoteApp, and RD Gateway, security challenges arise as users access corporate information from outside the organization; the security issues depend on the type of RDS deployment. Windows 2008 R2 comes with powerful security features. A Network Level Authentication (NLA) for every connection offers the best security. Before every session is created, NLA requires every user to be authenticated with the RD Host Session server.

Additionally, every RDS session can be protected with three types of security layers:

a) RDP Security layer
b) Negotiate – TLS 1.0 (SSL)
c) SSL – TLS 1.0

SSL-TLS encryption offers the best security. In addition, you can choose the level of encryption for a connection in the Group Policy settings for RDS.

RD Web Access provides browser-based remote access to computers that do not have remote client software installed. The RD Web Access interface is configured with SSL to provide a high level of security.

Moreover, customized access to remote applications can be provided based on user privileges using an Access Control List (ACL). Computers that use RD Gateway to access remote networks on the Internet are monitored by a Network Policy Server (NPS) using two different policies that check which devices and users can connect to that network.

Today's Remote Desktop Services offer highly scalable remote network solutions that run in a secure environment. By properly deploying RDS, businesses can optimize resources and improve revenue.

Remote Desktop Services with Parallels RAS

RDS is an amazing tool to create a cost-effective virtualization environment, but it has some hidden costs in its configuration and maintenance. For instance, server load balancing and application virtualization require extra components, and the process to get them up and running is far from easy.
Parallels® RAS effectively meets these challenges with low complexity: It can be up and running in less than five minutes. Other advantages of Parallels RAS include the following:

- Reduced setup and configuration time
- Publishing any application is a matter of a few clicks.
- Easy, high availability: Additional gateways, servers, and backup servers can be added through a wizard.
- Backup and restore are centralized and manageable from the console.
- Mix different hypervisors from VMware®, Hyper-v®, and Citrix®.
- Rely on different technologies: VDI and RDS.
- Built-in resource-based load balancing
- Shadowing is preconfigured: Take control of the entire workstation, not just the remote desktop.
- Reinforced filter and control, in addition to Active Directory, by MAC and IP address and client
- Supports "one time code" authentication such as DeepNet and SafeNet
- Report log is centralized for easy reporting and monitoring
- Parallels RDP Client runs on Windows, Mac®, Linux®, iOS, Android™, and several other platforms.
- Parallels RAS converts Windows XP and Windows 7 and 8 workstations into secure pseudo thin clients.
- Complete control of Windows workstations from XP, 7, 8, and 8.1
- Printing redirection and scanning are embedded in the product.
- Printing redirection is also available on mobile devices.

Publish applications instantly: You just need a few clicks to deliver whatever you wish to your network. Using the console, you can easily manage the entire remote connection. Corporate data security is enhanced with user- and group-based filtering. Parallels RAS can reinforce the active directory policy with filters on the Gateway, MAC address, IP address, and the client.

Resource-based load balancing is embedded to guarantee the best possible performance. Parallels RAS controls and monitors user activity, license usage, and network load, allowing you to be in control of your infrastructure. Parallels RAS administers and controls Windows devices from XP up to Windows 8.1, and the Windows desktop can be converted into a pseudo thin client to maximize security. Parallels RAS adds functionality to RDS to guarantee outstanding performance in application and remote desktop delivery.