An Executive's Guide To
Remote Desktop Monitoring Strategies
In the Teleworking Era

Visit www.rdpsoft.com for more information
and a free 30-day evaluation.

Executive Summary

The percentage of organizations that permit some form of teleworking has exploded over the past decade. From 2005 to 2011, regular telecommuting expanded by 73%. In fact, federal and state governments had the greatest growth in teleworking during that time period, with growth rates of 424% and 114% respectively.[i] Undoubtedly, the Telework Enhancement Act of 2010 will only continue to fuel this upward trend, as federal agencies are now required to establish telework policies for eligible employees, and designate a Telework Managing Officer to oversee these efforts.[ii]

As a result, executives and managers continue to make major capital expenditures in new and emerging technologies to facilitate seamless transitions from in office to at home work environments. Examples of these technologies include VDI (Virtual Desktop Infrastructure, with offerings by Vmware, Citrix, and Microsoft), as well as RDS (Remote Desktop Services - a built in feature of all Microsoft operating systems, whether running on physical hardware or within a virtual environment).

Given the cost differential between full VDI solutions and RDS, many organizations elect to use RDS on its own to facilitate telework. While a wonderful technology in its own right, RDS has many inherent limitations in the area of user, security, and performance monitoring that must be overcome by organizations to make it a fully auditable solution in the enterprise. The rest of this whitepaper will break down each of these challenges, as well as demonstrate how RDPSoft's Remote Desktop Reporter can solve each one.

Introduction to RDS

RDS - Remote Desktop Services - are everywhere. Put most simply, RDS is the technology built into every Microsoft operating system that effectively "remotes" a user's desktop (e.g. their screen) to a different computer. In order to connect to a remote workstation or server, a user first starts a piece of client software – in most cases, the Remote Desktop Connection utility. If you are an IT veteran well versed in the history of Microsoft operating systems, you may remember that this tool used to be called the "Terminal Services Client."

Within the Remote Desktop Connection tool, a user can specify a.) the remote system the user wants to connect to, b.) display characteristics of the remoted desktop, such as screen size and color depth, c.) whether or not to connect local resources to the remote computer, such as printers and disk drives, and d.) performance characteristics of the display window, given the amount of available bandwidth between the user's local computer and the remote system to which they are connecting.

Once connected, information begins to flow back and forth between the user's local system and the remote system via RDP - the Remote Desktop Protocol. RDP's capabilities have expanded markedly over time - while initially only providing a mechanism for a user to control a computer remotely within a full, graphical environment, RDP now offers extensions called Virtual Channels that provide for file transfer between the local and remote system, printer redirection, and most recently, a new display technology called RemoteFX that provides a richer visual experience for Remote Desktop users, providing optimized methods for streaming video and exchanging other types of data with the client.

Also, in the recent era of "BYOD" – Bring Your Own Device – RDS can bridge the gap between different mobile device OS platforms for Microsoft shops. For instance, Microsoft already publishes a Remote Desktop Connection client for Mac devices. There are numerous commercial RDS clients currently available for Android devices, and rdesktop is an example of a popular open source RDS client for various Linux distributions.

Anonymized Case Studies

Being such a versatile technology, organizations elect to utilize Remote Desktop Services in a variety of ways. For the purposes of example, we've created several anonymized case studies that offer actual examples of how RDS is used in the field.

Case Study 1 – Large Accounting Firm Depends on RDS for Teleworking During Tax Season

111CPA, LLP, provides their accounting professionals with a flextime arrangement by enabling Remote Desktop Services on their key application servers. Many company accountants now elect to telework extensively during the Spring tax season, so they don't lose valuable billing hours to lengthy commute times.

As a matter of due diligence, the managing partners at 111CPA have decided to audit how their employees are utilizing RDS. Specifically, they want to make sure that a.) their employees are honoring the terms of their flextime agreement – for example, that they do put in time on weekends in March and April, and b.) that the time they bill to clients is in line with the time they are connected to corporate servers and workstations via RDS.

Currently, this level of auditing is being done manually in a painstaking fashion by 111CPA's network administrators; each network admin checks the Microsoft Terminal Services Manager daily and logs who is connected into a spreadsheet. However, this situation is untenable, and management has agreed to look for an automated solution to report on employee RDS activity.

Case Study 2 - RDS in Private Cloud Supports Acme Co's Sales Team

To assist its mobile network of sales reps, Acme Co recently established a private cloud at a local datacenter to host its CRM software. Acme's sales professionals utilize Remote Desktop Services from their mobile devices to enter orders, research customer history, and log customer interactions while on the road. Each of the servers in the private cloud runs an instance of Microsoft Windows Server 2008, with each server capable of supporting many simultaneous RDS sessions.

Acme's management is pleased with this arrangement, as it allows them to track in near real time incoming orders for fulfillment, as well as the current sales pipeline. However, they are keen to audit the amount of bandwidth being used across their RDS sessions, as they pay both their datacenter and mobile data provider based on data consumed monthly. They also want to monitor the number of RDS sessions on each server, so they can plan additional capacity before a resource bottleneck is realized. Finally, they want to benchmark the hours of the day when RDS use is at its peak.

Case Study 3 - Software Company Allows Employees to Telework Via RDS On Individual Workstations

Emca Software, Inc is growing rapidly. They've recently acquired multiple smaller software companies in related fields across the US and Canada. As such, their IT infrastructure is decentralized, and they depend heavily on RDS in order to facilitate testing, support, and development.

For example, Emca's QA team is located at their headquarters in Toronto, but is now tasked with testing the software currently in development in Phoenix, where one of their recently acquired subsidiaries is located. To accomplish this, the Toronto QA team uses RDS to connect to a farm of Hyper-V Virtual Machines in the Phoenix office. Each of these VMs run the most up-to-date software builds so the Toronto QA team can perform feature and regression testing on a regular basis.

On top of that, Emca recently established a dedicated technical support office in Raleigh, NC to support all of their product lines. To reduce turnover, the general manager of the Raleigh office instituted a "work from home" policy. Each technical support engineer is now allowed to telework from home up to two days per week. When teleworking, Emca's support engineers first connect to their corporate VPN, and then establish Remote Desktop Sessions to their Windows 7 workstations physically located in the Raleigh office. Once the RDS sessions are established, they connect to the company's CRM software via a shortcut on their desktop. Often, during support calls, technicians will start new RDS sessions to connect to VMWare Virtual Machines that reside in Toronto, which host the latest shipping build of the software. By making this second remote desktop connection, they can attempt to reproduce the problem a client is experiencing immediately.

Given this flurry of M&A activity at Emca, Emca's HR department is having a difficult time evaluating employee productivity, with all of their new branch offices now spread across North America. While Emca's HR professionals do not want to stifle corporate growth with ill-conceived and inflexible top-down mandates, they are in need of a way to obtain productivity metrics for both individuals and company departments who leverage RDS to bridge the gap between geographically distant offices.

RDS Monitoring Challenges

In the previous section, we presented case studies about companies that depend on Remote Desktop Services to serve both their customers and employees. Now it's time to talk about some challenges inherent in proper RDS monitoring.

Monitoring Challenge 1 - *Much of Remote Desktop Session Activity cannot be tracked through the event log.*

Yes, unfortunately this is true, even though many log management vendors would want you to believe otherwise. While it *is* true that you can isolate remote desktop service logons from the Security Log (you must look for Logon Type 10), it's very hard to correlate them with the corresponding logoff events, which do not post a specific logon type. Rather, you must correlate the Logon ID from the originating logon event with the logoff event, which is even more tedious and is not something easily accomplished by many third-party log management packages.

Consequently, it's very hard to establish the duration of a remote desktop session by using event log records alone, much less to discern what actually happened in the remote desktop session. Furthermore, there is no way to determine the overall *productivity* of a user session based solely on these logon/logoff events.

Similarly, while Windows auditing can determine when applications are started and ended by particular users, there is no logging data that indicates *what remote desktop session* the process was started within. Therefore, attempting to determine the programs used on a Terminal Server in a given user session with the event log alone is a fruitless endeavor.

Monitoring Challenge 2 - *Built in Microsoft tools, like the Microsoft Terminal Services Manager, only provide snapshots of current Remote Desktop activity*

Veteran network administrators are well familiar with the Microsoft Terminal Services Manager utility, which is the built-in Remote Desktop Management tool found on Microsoft Windows Server Operating Systems. When loaded, you can view a current snapshot of many items on your Remote Desktop servers, such as session status, connected users, programs running, etc. However, that's all it is - a snapshot. There is no way to calculate the changes in this information over time, which requires routinely aggregating this information at regular intervals. The built in tools for Remote Desktop Management provided by Microsoft have no facility by which to do this, and this is where RDPSoft's Remote Desktop Reporter utility can prove most useful.

The RDPSoft Remote Desktop Reporter is a solution specifically designed to remove the key challenges surrounding remote desktop monitoring and reporting. First, let's examine the product's architecture, and then discuss the sort of RDS activity it tracks and reports upon.

Remote Desktop Reporter Architecture

RDPSoft's Remote Desktop Reporter solution has three main components: 1.) The primary application user interface, 2.) the Remote Desktop Reporter service, and 3.) the Remote Desktop Reporter database.

The **primary user interface** is a standard Windows application where administrators can:

- Select the servers and workstations that are polled for Remote Desktop activity
- Configure the database used to store the collected RDS information
- Change the frequency at which servers and workstations are polled for changes in RDS activity
- Build reports on an ad-hoc basis, or schedule recurring reports to track certain RDS activity
- Build filters to limit the information in reports based on criteria like server, user, client address, etc.
- Configure other operating behaviors of the Remote Desktop Reporter Service.

The **Remote Desktop Reporter Service** is an **agentless** process that routinely polls all specified servers and workstations for RDS information, and aggregates that information into a central database. In addition to collecting the RDS information, this service is responsible for creating scheduled reports, as well as doing periodic database grooming to remove older information over time.

Being agentless, the service does not need to be loaded on each of the servers or workstations that you want to monitor. Rather, you can install it remotely and assign a user account to the service that has permission to poll

RDS information from networked computers. This confers an advantage to a manager or IT professional that wants to do monitoring or auditing of user activity without alerting the user that such monitoring is taking place.

Lastly, the **Remote Desktop Reporter database** is a Microsoft SQL Server database where polled RDS information is held for reporting. By default, a special instance of Microsoft SQL Server Express is installed by the Remote Desktop Reporter installation package. However, for larger implementations, administrators can specify that the Remote Desktop Reporter use a full version of Microsoft SQL Server already deployed on the network.

Available Reporting Categories

User Session Tracking / Time and Productivity Tracking

Internally, Microsoft's Remote Desktop Services keep track of how long a remote desktop session has been connected, disconnected, and idle. By collecting this sort of information over time, Remote Desktop Reporter can subsequently produce reports that provide an estimate of how long users remain connected in their sessions, as well as show a ratio of how "active" they are in any particular session or group of sessions over time.

These reports become highly useful in determining whether or not a teleworking arrangement is being honored as intended by the employee. For instance, an employer or Telework Managing Officer can look at productivity levels over time (where productivity is defined as active versus idle time in remote desktop sessions) to see how productivity is trending for one or more employees. In another scenario, a manager may wish to look for outliers in terms of when employees are working - for instance, is a certain employee working late at night for instance?

Also, with properly crafted filters, organizations can create “roll call” or “virtual attendance” reports to see what users are logged on to different terminal servers at different times of the day.

Application Tracking

Application Tracking is another category of reports offered by Remote Desktop Reporter. Often, it is useful to correlate the programs that users are running in their sessions. Are they running approved business applications? Are they running applications such as Internet Explorer, Firefox, etc that may be consuming a lot of RDP bandwidth? Using the RDPSoft solution, it is easy to see what applications individual users, as well as the user base at large, run most frequently.

Client Network Information

In most cases, IT departments go to great lengths to secure client notebooks and other computing devices that will be for telework. However, for organizations that do not require certificate-based authentication, is there any way to know whether remote desktop sessions are being established using authorized versus non-authorized telework devices? Moreover, some mobile device Remote Desktop clients do not offer certificate-based authentication at all, so organizations are often forced to lower security levels in order to support a wider variety of telework devices owned personally by their user base.

Remote Desktop Reporter can quickly produce a report showing, for a given user or users, all of the client network addresses and client device names that were used to establish a remote session. As a result, it becomes rather easy to spot unauthorized devices and the users who used them.

Remote Desktop Protocol Bandwidth Consumption

Given that Remote Desktop is graphically intensive by design, its demands on an organization's bandwidth are non-trivial. In addition, since RDP connections often come in over company VPNs, remote desktop sessions quickly start competing with other corporate Internet-bound traffic, such as VOIP calls, offsite backup operations, etc. In most cases, it is the types of programs that users run in their sessions that directly determine bandwidth consumed – for instance, if they stream a YouTube video from within a web browser in their session, their bandwidth consumption will increase markedly. Therefore, it becomes vital to monitor RDP bandwidth on both a per user and per computer basis to spot anomalies and unauthorized program use.

Remote Desktop Reporter provides the ability to produce reports detailing bandwidth consumption from individual users, as well as the aggregate bandwidth used by servers on a daily basis.

Terminal Server Performance Metrics

Lastly, since RDS infrastructure is critical to telework initiatives at government agencies and corporations, it is absolutely necessary to routinely monitor and report on performance metrics over time. For instance, a high average number of disconnected sessions on a terminal server equates to wasted resources, as each abandoned session is still utilizing memory and processor cycles. Likewise, tracking the number of sessions in use on a particular server by hour of day can quickly pinpoint when a server may start becoming less responsive. Fortunately, RDPSoft's Remote Desktop Reporter can track these performance trends and others, producing daily or weekly reports so that administrators can adjust remote desktop policies and/or provision new equipment to keep up with user demand.

Conclusion

As more and more organizations commit to technologies to facilitate employee teleworking, there will be commensurate demands placed on management to monitor and audit that telework activity. Given the inherent licensing cost differential between Remote Desktop Services and Virtual Desktop Infrastructure for a similar number of users, more organizations will elect to use RDS rather than VDI as the preferred technology for remote work arrangements.

Since neither built-in Remote Desktop management tools nor the native Windows event log is sufficient to track RDS activity in a fully automated fashion, third party tools must be leveraged by IT staff to reliably monitor telework activity and Terminal Server performance. RDPSoft's Remote Desktop Reporter is a prototypical example of a best-of-breed tool focused on automating RDS monitoring and reporting for the benefit of Windows network administrators and their managers.

---

[i] Telework Research Network - http://www.teleworkresearchnetwork.com/telecommuting-statistics
[ii] Telework.gov - http://www.telework.gov/Telework_Enhancement_Act/Highlights/index.aspx