Remote Desktop Services

Wesley Faxlanger

School of Cybersecurity

CYSE:608 Cyber War

Dr. Malik A. Gladden

16 October 2026

Remote Desktop Services

Remote Desktop Services (RDS) is a Windows Server feature that allows users, primarily network administrators, to remotely access Windows desktops, applications, and other resources hosted on a server within a network. This technology lets an organization provide centralized virtual environments without requiring users to be physically present at a server. Remote Desktop Protocol (RDP) is used by RDS to establish remote connections, providing display and keyboard/mouse functionality between the user and the remote device. User Profile Disks (UPDs) are designed to make Remote Desktop Services (RDS) in Windows Server 2019 more consistent for employees who connect to different session hosts. This is important as UDPs allow users to retain their desktop settings, files, applications, and other configurations between uses and connections to different remote servers. This is achieved using a Virtual Hard Disk (VHD). A VHD is essentially a virtual drive stored on a network that is attached to a user's UPD, allowing for secure storage and instant access to their data and configurations upon logging onto the remote session. Microsoft explains that UPDs allow "user data, customizations, and application settings to follow a user across virtual instances" (Microsoft, 2024b). This is primarily useful in organizations where individuals share access to remote infrastructure. These Individuals expect their desktop preferences, documents, and application configurations to remain available to them without granting access to others using the same infrastructure.

According to Microsoft's article on Remote Desktop Services (Secure Data Storage), each UPD is a "per-user, per-collection VHD file," stored on a central network share (Microsoft, 2024b). This implies that once a user signs in, RDS mounts a designated virtual disk to the user's session that behaves like local storage. This is similar to when a user creates a virtual hard disk to use on a virtual machine. These virtual disks are ultimately allocated segments from a physical

hard disk stored within the host device. However, profiles move only among hosts in the same collection; a UPD is not a universal profile that follows the user into unrelated RDS collections (Microsoft, 2024b). This means that the profiles are not universal but rather specific to a provider. Ultimately, Administrators are responsible for designating how these virtual disks are distributed and maintained. According to Microsoft, PowerShell is ideal for managing individual UPDs (Microsoft, 2024b). Server Manager can be used to manage UPDs, although this option is primarily for managing groups rather than individual users. It is important to ensure that users have adequate storage to complete tasks required by their role within the organization without over-allocating resources.

Proper implementation of access controls requires the use of two layers. Those layers include permissions to access the RDS collection and permission for the session host to access UPD files. For the first layer, "You can use Active Directory Domain Services (AD DS) to grant access to the shared remote resources" (Microsoft, 2024a). This is effective as administrators can manage groups and user settings, limiting collection access to individuals with a legitimate need for the resources. As standard best practice, review group memberships regularly. It is also important that these groups are not too broad, as this can create confusion and ultimately result in managing access becoming needlessly complicated and time-consuming. Group membership alone does not replace file-share security because the profile disks contain potentially sensitive or personal information. While it is important to provide the access that RDS requires, it is equally important to ensure that unnecessary access is not provided. Considering the disks contain sensitive user information, protecting these storage devices is important. Regular backups, implementation of zero trust, encryption, and recovery testing are all necessary steps. These security measures are not automatically provided by UPDs; however, they are relatively

easy to implement. When properly implemented, RDS provides organizations with the convenience of personalized remote desktops without sacrificing much of the security offered by physical devices.

References

Microsoft. (2024, November 1). *Manage users in your RDS Collection*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-user-management

Microsoft. (2025, October 30). *Remote Desktop Services Overview in windows server*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/overview

Microsoft. (2024b, November 1). *Remote Desktop Services - Secure Data Storage*. Remote Desktop Services - Secure data storage | Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-secure-data-storage