6.1. Remote Desktop Services

Remote Desktop Services allows remote clients to run applications remotely on the Remote Desktop server or to access the desktop of the server. Remote Desktop Services minimizes processing on client computers through the Remote Desktop Protocol (RDP).

- The client computer runs the Remote Desktop Client (RDC) software. The client connects to the Remote Desktop server to establish a session.
- With a normal configuration, the Remote Desktop server creates a desktop session for each client. The desktop and all applications run on the Remote Desktop server, using the server's CPU, RAM, and disk resources.
- RDP sends the screen information from the desktop on the server to the RDP client.
- Mouse and keyboard actions performed on the client are forwarded to the server. These actions are executed on the server.
- The resulting changes to the desktop are returned to the client.

Use Remote Desktop Services to:

- Provide a desktop for thin clients or for clients running earlier versions of Windows or with lower-end hardware. The desktop running on the Remote Desktop server has access to the latest operating system updates and greater hardware resources.
- A run application on a client where the application is not compatible with the client or the client does not have sufficient resources to run the application.
- Remotely manage a server. As an administrator, you can connect to the server desktop to run management utilities and perform other tasks that can only be performed from the server console.
- Centralize the management of user desktops. Desktop settings are saved on the Remote Desktop server, and are available to the user regardless of the computer used for logon.
- Centralize data storage and application installations. All data generated from a Remote Desktop server session can be saved on the Remote Desktop server instead of individual workstations. In addition, you can

install and upgrade applications once on the Remote Desktop server instead of managing application installations on each workstation.

Remote Desktop server technology is used for the following:

- With Remote Desktop, each computer supports up to two connections. Use Remote Desktop to remotely connect to perform administration tasks. With previous Windows versions, you could have one console connection and two remote connections; with Windows Server 2008 and above, you are allowed a total of two connections (either remote or console). Remote Desktop does not require additional licensing.
- With Remote Desktop Services, the server can support additional remote connections. Use Remote Desktop Services to support desktop consolidation and running remote applications. Remote Desktop Services requires additional licensing for each connection.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

6.2. Remote Desktop Client

Client computers make a Remote Desktop or a Remote Desktop Services connection to another computer through the Remote Desktop Client software. Be aware of the following regarding the Remote Desktop client:

- The client software is already installed on Windows XP and later (including Server 2003/2008/2012/2016). You can add the client software to previous Windows versions if desired.
- Run **Mstsc.exe** to open the Remote Desktop client software.
- On Windows Server, you can also create connections to remote computers using the Remote Desktops console. Use this tool to manage multiple remote connections.
- The Remote Desktop client includes many settings that you can customize to configure the remote session.
    - Configure resource redirection to enable applications on the remote desktop to use your local clipboard, local printers, or local drives.
    - Configure experience settings to enable or disable visual elements. For example, you can disable the remote desktop background, disable themes and font smoothing, or enable bitmap caching to reduce the amount of data that needs to be transmitted to represent the remote desktop.
    - Configure advanced settings to enable server verification and RDS Gateway settings.
- You can save a remote connection as a Remote Desktop Protocol (.rdp) file. You can then open the remote session by opening the RDP file.
- The client version determines the features that are available. Features that are only available with the Remote Desktop client version 6.1 include:
    - The Easy Print driver allows users to print from a remote session to a local printer without installing the print driver on the Remote Desktop server.
    - RDS Web Access allows users to connect to a Remote Desktop server through a Web browser. RDS Web Access uses the client software instead of an Active X control.
    - RDP file signing lets you sign an RDP file.
    - RDS RemoteApp lets you run applications on the Remote Desktop server in a window without having to see the remote desktop.

    - Server authentication lets the client computer verify the identity of the Remote Desktop server.
    - Monitor spanning lets you stretch a Remote Desktop server desktop across multiple monitors.
    - RDS Gateway lets you connect to a Remote Desktop server through the Internet.

Before a remote connection is allowed, remote connections must be enabled on the target computer or Remote Desktop server.

- For Remote Desktop, allow remote connections in the system properties. You can select to:
    - Block RDP connections.
    - Allow all RDP connections from any remote client version.
    - Allow only RDP connections that use Network Level Authentication (NLA). Using NLA requires RDP client v6.0 or higher.
- By default, only local administrators can remotely access a Remote Desktop server. To allow other users to connect, add users to the Remote Desktop Users group. User accounts must be configured with a password.
- RDP uses port 3389. When you enable Remote Desktop or install the Remote Desktop Services role service, this port is opened automatically.

After a connection is opened, be aware of the following:

- Closing the Remote Desktop window does not end the session. The session remains active, with all applications still running. When you re-establish the Remote Desktop connection, the session is resumed.
- To end the remote session, choose Shutdown from the Start Menu within the Remote Desktop window. This closes all open applications and terminates the session. If you reconnect, a new session is created.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

6.3. Remote Desktop Server Installation

You do not need to install Remote Desktop Services on a computer to use the two free connections that allow for remote administration. Add the Remote Desktop Server role service to allow the server to support more than two remote client sessions or running remote applications. Be aware of the following when installing a Remote Desktop server:

- Add the Remote Desktop Services role with the Remote Desktop Server role service in Server Manager.
- During the installation you can choose to require Network Level Authentication (NLA). With NLA, authentication to the Remote Desktop server is performed before a desktop connection is made. A desktop session is only created if authentication is successful. Using NLA is more secure and uses fewer system resources during the initial connection. Using NLA has the following requirements:
    - The client computer must be running version 6.0 or later of the Remote Desktop Client.
    - The client computer must be using an operating system that supports the Credential Security Support Provider (CredSSP) protocol.
    - The Remote Desktop server must be running Windows Server 2008.
- The Remote Desktop server must be configured to identify the Remote Desktop Services Licensing mode. You can complete the installation without configuring licensing, but the server must be configured for licensing before the expiration of the grace period.
- Users must be allowed access to the Remote Desktop server.
    - By default, members of the Administrators group are allowed access and cannot be removed.
    - For Remote Desktop servers that are domain members, add authorized users to the Remote Desktop Users group in Local Users and Groups.
    - For Remote Desktop servers that are domain controllers, add authorized users to the Remote Desktop Users group in Active Directory.
- In addition to adding the Remote Desktop Server role service, you might add the following features to improve the user experience or to provide tools for administration.

User Feature	Description
Desktop Experience	Allows users to view the remote session as a Vista desktop. Desktop Experience provides support for: o Windows Media Player o Desktop Themes o Aero Experience o Photo Gallery
Quality Windows Audio Video Experience	Allows streaming of media across the network with high quality performance.
Administrator Feature	Description
Network Load Balancing	Allows you to distribute remote processing across multiple Remote Desktop servers in a Remote Desktop server farm.
Server Backup	Provides backup and restore tools for administrators to maintain the server remotely.
Windows PowerShell	Provides a command line environment and administrative scripting language for remote administration.
Group Policy Manager Console	Provides Group Policy management tools for admins who access the server remotely.
Windows System Resource Management	Enables you to use resource policies to manage processor and memory resources.

- Applications that will be used on the Remote Desktop server by remote users should be installed after the Remote Desktop Server role service is added.

6.4. Remote Desktop Server

A Remote Desktop server uses the following objects to identify and control client connections to the Remote Desktop server:

Component	Description
Session	A *session* is a current connection to a Remote Desktop server. The following types of sessions might exist: • The Services session is used by system processes on the Remote Desktop server. • The Console session is created when you establish an interactive logon to the server console. • The Listener session listens for and accepts new client connections. • Remote desktop sessions are created for each remote client connection. Use Remote Desktop Services Manager to view and manage current sessions.
User	A *user* is an authenticated user to the Remote Desktop server. When you install Remote Desktop Services, user account properties in Active Directory are modified to include settings that control the use of Remote Desktop Services by that user. • Configure the Sessions settings to control what happens when a connection is idle or when to automatically disconnect or end a session. • Configure the Remote Desktop Services Profile settings to identify an alternate user profile that is used for a Remote Desktop server connection. • Configure the Remote Control settings to identify whether administrators can interact with the user session. • Configure the Environment settings to run a program at logon or to connect drives and printers at logon.

	Use the following tools to manage Remote Desktop server users: • Use Active Directory Users and Computers to edit the settings for a specific user account. • Use Remote Desktop Services Manager to view and manage users connected to a Remote Desktop server. ***Note**: A user can establish multiple sessions with the same Remote Desktop server.*
Connection	A *connection* identifies a network connection to the Remote Desktop server. • A default connection named RDP-Tcp is automatically created on all servers, even if Remote Desktop Services is not installed. • Without Remote Desktop Services, the default connection allows a maximum of 2 connections. After you install Remote Desktop Services, you can modify the maximum number of simultaneous connections. • By default, the connection uses all installed network adapters. You can configure the connection to use only a specific network adapter. • You can create additional connections to control settings on a network adapter basis. However, each network adapter can be associated with only one connection. Use Remote Desktop Services Configuration to manage the connection settings for a Remote Desktop server.
Process	A *process* is an instance of software running on the Remote Desktop server. • An application might run multiple processes. • Each process has a unique process ID number. • Processes are identified by the user and the session. You can sort processes by user or by session. Use Remote Desktop Services Manager or Task Manager to view and manage processes running on a Remote Desktop server.

	***Note**: In Task Manager, be sure to select **Show processes from all users** to view processes from all connected users and not just the current user.*
Group Policy	You can use Group Policy to configure many different settings for both Remote Desktop servers and users. For example, with Group Policy you can enforce session settings for users without having to configure each user account individually. • Settings configured in the Computer Configuration apply to the Remote Desktop servers and connection objects. • Settings configured in the User Configuration apply to users connected to Remote Desktop servers. • Some Group Policy settings can be set for both computers and users. If both are configured, the computer settings will be used (this is because Remote Desktop server and connection settings override user account settings). Run the Group Policy Management console to open the Group Policy Management Editor to modify Group Policy settings.

6.5. Remote Desktop Server Management

Be aware of the following as you manage users and sessions:

- The following table lists the various session states:

State	Description
Active	An *active* session is currently connected with the user logged on.
Idle	An *idle* session is connected and the user is logged on, but there has not been any activity within the session. An idle session still shows as Active, but a timer keeps track of the amount of time the session has been idle.
Disconnected	A *disconnected* session is still connected, but the user is not logged on. The desktop state is maintained with all active applications still running. A user can reconnect to a disconnected session and resume working with the same desktop state. Sessions become disconnected when they have been idle for a specific period of time or when users take certain actions that do not terminate the session.
Ended	A session that has been ended has been disconnected, the user logged off, and the desktop has been shut down. Open windows or running programs are closed. Users can create a new session, but cannot resume the session.

- *Disconnect* a user or a session or have the user close the Remote Desktop window to disconnect the user from the active sessions while preserving the session state. *End* the session, log off the user, or choose Shut Down in the Remote Desktop session to gracefully close down applications and end the session. *Reset* a connection to terminate the session and forcefully end all running applications.
- Use the following command-line utilities to manage user connections and sessions:
    - Use ***Tscon.exe*** to connect to a Remote Desktop server session.
    - Use ***Tsdiscon.exe*** to disconnect a user or session.

- Use ***Msg.exe*** to send a message to a user.
- Use ***Logoff.exe*** to terminate a session.
- Use ***Query user*** to see information about current users, and ***Query session*** to see information about current sessions.
- Use ***Tskill.exe*** to end a process. Use the ***/ID:*** switch with the session ID to end all processes running within the specified session.
- Use ***Chglogon.exe*** to configure how logons are allowed on the server.

Switch	Description
/Query	Shows the current logon mode for the Remote Desktop server.
/Enable	Enables remote logons to the Remote Desktop server.
/Disable	Disables remote logons to the Remote Desktop server. Users cannot reconnect to existing sessions.
/Drain	Disables new logons, but allows users with existing sessions to reconnect, for example to end the session or log off.
/DrainUntilRestart	Temporarily disables new logons while allowing reconnections to existing sessions. The server will leave drain mode when the server restarts.

- Configure session settings to set timers for when sessions are disconnected or ended automatically. You can:
  - Set a time limit on the amount of time allowed within a session.
  - Set a time limit for how long a session can be idle.
  - Configure an action to take when the active or idle session time limit is reached. You can choose to disconnect or end sessions when the timer expires.
  - Set a time limit for how long a disconnected session is maintained. After the time limit is reached, the disconnected session is ended.

Session settings configured in the user account apply to the user, while session settings configured for the connection apply to all sessions that use that connection. Connection settings override user settings.

- You can configure users with a different profile for Remote Desktop Services than is used for other desktops.
    - To specify a custom profile for a user, edit the user account properties and add the profile path on the Remote Desktop Services Profile tab. This profile will be used when connecting to any Remote Desktop server. *(**Note**: The profile specified in the user account on the Profile tab is used when connecting to all computers, or to all Remote Desktop servers if a custom Remote Desktop server profile path is not configured.)*
    - To configure all users with a profile that is used for all Remote Desktop servers, configure a GPO that applies to the Remote Desktop servers and specify the path to the profile in the **Set path for RDS Roaming User Profile** policy.
        - When using this setting, a subdirectory is created in the path you specify for each user, and the user's profile is stored in that directory.
        - This profile is used for all Remote Desktop servers affected by the GPO.
    - To enforce a profile that applies to all users on a Remote Desktop server, edit the local security policy or configure a GPO with the following settings:
        - Enable the **Use mandatory profiles on the Remote Desktop server** policy.
        - Specify the path to the profile in the **Set path for RDS Roaming User Profile** policy.
- To connect to or remote control a session, you must be logged on to the Remote Desktop server remotely. If you are logged on through the console, you will be unable to view or remote control a current session.
    - You can enable or disable remote control for a specific user account. For example, you can disable remote control for an administrator to prevent remote control under any circumstances.
    - You can enable or disable remote control for a connection object on the server. For example, if you enable remote control on the server,

remote control of a session is possible regardless of the user account settings.
    - By default, remote control requires the user's permission to make the connection. You can configure the user account or the connection to allow remote control without permission, or to restrict remote control to viewing (but not interacting with) the session.
    - You can configure remote control settings using Group Policy and the **Set rules for remote control of Remote Desktop Services user sessions** policy.
- It is possible for a single user to have multiple sessions to the Remote Desktop server. To restrict users to a single session, edit the server properties in Remote Desktop Services Configuration.

Edit the connection settings in Remote Desktop Services Configuration to:

- Configure security settings, such as whether to use TLS, encryption, or Network Level Authentication.
- Specify a user account that is used for all connections.
- Configure the redirection of devices that are disabled (such as drives, printers, audio, clipboard, or Plug and Play devices).
- Identify the adapter used by the connection.
- Override settings in the user account properties (Sessions, Remote Control, and Environment settings). Settings configured for the connection apply to all users and all sessions, overriding settings in the individual user accounts.
- Configure connection permissions. Permissions set on the connection govern the actions users can perform on other Remote Desktop Services sessions. They do not have any impact on a users' ability to run programs or administer a server. Permissions can be granted individually through Special Permissions, or they are granted by allowing the following user access levels.

Access	Associated Permissions
Full Control	Grants all Remote Desktop Services permissions.
User Access	Grants the following permissions: o Logon o Query Information

	o Message o Connect By default, the Remote Desktop Users group has User Access permissions
Guest Access	Grants the Logon permission.

Remote Desktop Services with Windows Server 2008 and later includes the following new features:

Feature	Description
Single sign-on	Single sign-on allows credentials of the user's current session to be used as remote credentials on a Remote Desktop server. Users log on once to their local computer, and those credentials are used to automatically log on to the Remote Desktop servers. • Single sign-on requires domain user accounts and domain computer accounts. • Single sign-on requires Vista/7/8/10 or Server 2008/2012/2016 clients and servers. • You can use single sign-on with RDS Gateways. To configure single sign-on: • In a Group Policy object (GPO) that applies to the client computers, enable the **Allow Delegating Default Credentials** policy. Add the Remote Desktop servers to the list on which single sign-on is allowed. ***Tip****: You can use the wildcard symbol to identify multiple servers. For example, use* ***TERMSRV/**** *to allow single sign-on to all servers, or* ***TERMSRV/*.sales.westsim.com*** *to allow single sign-on to all servers in a specific OU or domain.* • On the Remote Desktop server, edit the properties of the connection and use **Negotiate** or **SSL (TLS 1.0)** for the **Security Layer** setting.

Easy Print driver	The Easy Print printer driver provides a driverless solution for printing from a remote connection. Historically a printer driver had to be installed on both the printer and the Remote Desktop server. With the Easy Print driver, print jobs from the Remote Desktop server are redirected to a printer defined on the client computer, without the need for the Remote Desktop server to have the printer driver installed. • The Easy Print printer driver is a proxy that redirects print requests back to the local client. • The printer appears to be on the remote system, but it is actually on the local system. • You can enforce use of this feature in both Computer Configuration and User Configuration Group Policy Management. • On a Windows Server 2008 or later system, the Easy Print Printer Driver is enabled when you install the Remote Desktop Server role. • A Remote Desktop for Administration connection cannot use the Easy Print feature. • The client must have the RDP client v6.1 plus the .NET Framework 3.0 SP1.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

6.6. RDS Licensing

A Remote Desktop Services client access license (RDS CAL) is required for each device or user connecting to a Remote Desktop server.

- Each server includes two free licenses that allow Remote Desktop access. These licenses are typically used by administrators for remote administration, not by clients for running applications.
- Remote Desktop Services provides a grace period of 120 days for the license server requirement. Clients can use the Remote Desktop server without licensing during this period. After the grace period, clients will not be able to connect without a valid license.

To manage licenses for Remote Desktop Services, add the RDS Licensing role service. Use the following process to configure Remote Desktop Services licensing:

1. Run Server Manager and add the RDS Licensing role service.
    - You can manage licenses for multiple Remote Desktop servers and clients with a single licensing server.
    - You can install the licensing server on a server running the Remote Desktop Server role service, or on a server that is not running any other Remote Desktop Services role service. For large environments, it is recommended that it be installed on a separate machine.
    - A licensing server running Windows 2000 or 2003 cannot issue licenses to a Remote Desktop server running Windows Server 2008. A licensing server running Windows Server 2008 can issue licenses to Remote Desktop servers running Windows 2000 or 2003. If you are deploying Windows Server 2008 or later Remote Desktop servers, the RDS Licensing role service must run on a Windows Server 2008 server or later.
    - During installation, you configure the discovery scope. The license *discovery scope* controls how Remote Desktop servers locate the licensing server. The licensing server can be configured to provide licensing services for a workgroup, a domain, or an entire forest.
2. Activate the RDS Licensing server. During activation, a digital certificate issued by Microsoft is installed on the RDS license server. The certificate

verifies server ownership and identity and is used to obtain and install additional licenses.

3. Install licenses on the licensing server.
4. Use the Remote Desktop Services Configuration (RDSC) console to configure each Remote Desktop server to use the RDS Licensing server. You can choose automatic discovery of the licensing server, or point to a specific licensing server. In addition, you configure the licensing mode used by the server.

Mode	Description
RDS CAL Per-User	A per-user license grants licenses to users to connect to a Remote Desktop server, regardless of the computer used for logon. o RDS Per user licensing is based on simultaneous connections. o Because per-user licenses are not enforced by RDS Licensing, it is possible to have more active client connections in an organization than installed licenses. This is a violation of the license agreement. o The license server must be a member of the Remote Desktop Server License Servers group in Active Directory Domain Services to issue RDS Per User CALs to users in the domain and track or report usage of the RDS Per User CALs on the license server.
RDS CAL Per-Device	A per-device license grants licenses to computers to connect to a Remote Desktop server, regardless of the user who is logged on. o Once a device has attached to a Remote Desktop server twice, a license is assigned to that device permanently and is considered used. o The license server automatically reclaims inactive licenses after a random period of between 52 and 89 days. o If a device connects and there are no more permanent licenses left, it will be assigned a temporary license that is

	good for 90 days. The device will be assigned a permanent license when one becomes available. o For devices whose CAL has been reclaimed, the license server will reissue a CAL the next time the device reconnects. o You can use the RDS Licensing Manager console on the license server to revoke 20 percent of issued CALs for an operating system.

Be aware of the following when managing Remote Desktop server licensing:

- If you are going to support a mixed environment, upgrade the license servers to Windows Server 2008 or later before installing other Remote Desktop Services components.
- You can confirm that each Remote Desktop server is able to contact the licensing server. Methods for verification are:
    - Use RDSC to perform a Licensing Diagnosis to verify that a Remote Desktop server is contacting the license server correctly.
    - Review the License tab of the RDS Configuration Server Settings to confirm the appropriate settings.
    - Review the configuration of the license server using Review Configuration in the RDS Licensing Manager.
- Discoverability of the licensing server by Remote Desktop servers depends on the discovery mode:
    - A licensing server in a workgroup will only be discovered if the licensing server is on the same subnet as the Remote Desktop server.
    - A licensing server using domain discovery will only be discovered if the licensing server is installed on a domain controller and if the Remote Desktop server is in the same domain as the licensing server.
    - A licensing server using forest discovery can be discovered by any server in the forest.
    - A Remote Desktop server with the licensing server role will always discover the licensing server running locally.

***Note**: You can always configure a Remote Desktop server to use a specific licensing server, even if that licensing server cannot be discovered automatically due to the restrictions listed here.*

- To allow a licensing server to issue licenses to both domain members and to non-domain members, configure the licensing server on a workgroup computer. Manually configure each Remote Desktop server to use the licensing server (domain members will not be able to auto-discover the licensing server, and non-domain members will only be able to auto-discover the licensing server if it is on the same subnet). ***Note****: You can only choose the workgroup discovery mode if the server is not a domain member.*
- By default, a licensing server issues licenses to any Remote Desktop server that requests a license. To control which Remote Desktop servers can get a license from the license server:
    - Enable the **License server security group** policy in a Group Policy object (GPO) that applies to the licensing server.
    - Add Remote Desktop servers that are authorized to get a license from the server to the Remote Desktop Server Computers group on the licensing server.

  With this configuration, only Remote Desktop servers that are members of the Remote Desktop Server Computers group can obtain licenses from the licensing server.

- You can generate a report to view the per-user or per-device licenses used.
    - For per-user reports, use the RDS Licensing Manager console or WMI scripts. You can generate a report that includes all licenses assigned to users in all trusted domains, a single domain, or an organizational unit (OU).
    - For per-device reports, use WMI scripts.
- To back up a license server, you back up the system state data and the folder in which the licensing database is installed (by default C:\Windows\System32\Lserver).

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

6.7. RDS Web Access

Install the RDS Web Access role service to allow clients to access a Remote Desktop server through a Web browser.

- Clients connect to a Remote Desktop server using a Web page rather than direct access through the RDC software. The RDC software runs inside the Web browser as an ActiveX control.
- RDS Web Access uses port 80 or 443 for connections. By contrast, the Remote Desktop Client uses port 3389. You can use RDS Web Access to provide access to Remote Desktop servers in situations where port 3389 cannot be opened in the firewall.
- Through the Web browser, clients can connect to any Remote Desktop server they have access to.
- The RDS Web Access server does not have to have the Remote Desktop Server role service installed.
- When you add the RDS Web Access role service, the IIS role and the Windows Process Activation features are required and added if necessary.
- Client computers must be running RDC 6.1. Clients must be running one of the following:
    - Windows XP with SP2
    - Windows Vista and later
    - Windows Server 2003 SP1
    - Windows Server 2008 and later
- On the client, use the following URL to connect to the server running RDS Web Access: **http://servername/RDSWeb**
- The list of applications shown in the Web page comes from a single Remote Desktop server.
    - You configure the RDS Web Access server to point to a single Remote Desktop server to populate the list of available applications.
    - To use a single Web access server with applications running on multiple Remote Desktop servers or multiple server farms, deploy Windows Sharepoint Services along with the RDS Web Access server role.
- Add users to the RDS Web Access Administrators group to allow them to modify the default RDS Web Access site.

6.8. RDS RemoteApp

TS RemoteApp allows a user to launch a program on a Remote Desktop server and run that program directly within a window on the client desktop. Users run the applications as if they were installed locally, instead of establishing a remote session and running the application through the desktop in the session window. Even though the application appears to be running on the client, the application is running on the Remote Desktop server using the server's hardware resources.

Using RDS RemoteApp has the following benefits:

- Users can launch the application directly from a shortcut on their desktop or through the Web Access interface. The Remote Desktop Services session window showing the desktop of the Remote Desktop server is never shown, thereby reducing confusion for inexperienced users.
- Applications run using the processing power of the Remote Desktop server, allowing applications to run on clients that have an incompatible operating system version or insufficient system resources.
- Users can run different versions of an application at the same time. Without RDS RemoteApp, installing a different version of an application might cause the previous version to stop working. With RDS RemoteApp, these different versions can run independently because they are not installed at the same time on the client.
- Administrators can deploy software by installing the software once on the Remote Desktop server, instead of on each client computer.
- Administrators can make an application available to a user without making the entire Remote Desktop server desktop available. This restricts the user to running only the authorized application and not any other applications available on the Remote Desktop server desktop.

***Note**: Most of these benefits can be realized by using Remote Desktop Services without RDS RemoteApp. However, without RDS RemoteApp, users might need to have multiple remote desktop sessions opened, and would have to launch applications from the remote desktop.*

Be aware of the following when using RDS RemoteApp:

- RDS RemoteApp is included when you install the Remote Desktop Server role service.
- The Remote Desktop server runs in two operating modes:
    - Execute mode is the normal operating mode for the Remote Desktop server. Users connect to the server and run applications while the server is in execute mode.
    - Install mode is a special mode that is used for installing applications on the Remote Desktop server that are available to remote clients. If you install applications while the server is in execute mode, the application might not be configured correctly to support multiple users.
- To install applications on the Remote Desktop server so they can be used by remote clients, use one of the following methods:
    - Install the application using the .msi file.
    - Run the Install Application on a Remote Desktop Server applet in the Control Panel.
    - Run the ***change user /install*** command from the command line to put the server into install mode. Install the application, then use the ***change user /execute*** command to put the server back into execute mode.
- On the Remote Desktop server, you deploy (identify) the specific applications that are available through RDS RemoteApp.
- After making an application available in RDS RemoteApp, you make that application available using one or more of the following methods:

Method	Description
.rdp Shortcut File	A .rdp shortcut file contains all of the information necessary to launch the application using RDS RemoteApp. After creating the .rdp file, copy the file to client computers. Users double-click the .rdp shortcut file to start the application.
.msi Installer Package	A .msi installer package is an installation file that creates the desktop and Start Menu shortcuts for launching RDS RemoteApp applications. After creating the .msi file, distribute the installer file and execute the file on client computers. The file adds the necessary components and shortcuts to the client computer.

	Use the .msi package to customize the location where the application icons are installed, or to enable extension invocation for starting the remote application. Configure extension invocation only if the client computer does not have the application installed locally.
RDS Web Access application list	With the RDS Web Access application list, an icon for the application is placed on the available applications list within the Web Access software. Users launch the Web Access software, then double-click the application icon to run the application. ***Note**: If the RDS Web Access service is running on a different server, add the Remote Desktop server with the installed applications to the RDS Web Access Computers group to allow the Web Access server to discover the applications available on the Remote Desktop server.*

- When deploying RDS RemoteApp programs using .rdp or .msi files, the client computer must be running RDC 6.0 or later. When deploying RDS RemoteApp programs using RDS Web Access, the client computer must be running RDC 6.1 or later.
- RemoteApp users must be members of the Remote Desktop Users group on the Remote Desktop server.
- If a user is running more than one RemoteApp program on the same Remote Desktop server, the RemoteApp programs will share the same Remote Desktop Services session.

6.9. RDS Session Broker

RDS Session Broker is a role service that creates a Remote Desktop server farm, where multiple Remote Desktop servers are grouped together to provide load balancing and fault tolerance.

- Clients establish an initial connection to a Remote Desktop server. To evenly distribute these initial connection requests, use DNS round robin or a network load balancing solution.
- The Remote Desktop server that accepts the client connection contacts the RDS Session Broker server to identify the Remote Desktop server that should be used for the client connection.
- The RDS Session Broker uses the user name and a session ID (if it exists) to direct the client connection to the appropriate Remote Desktop server in the farm.
    - If the user has an existing session, the connection is redirected to the server where the session resides.
    - If the user does not have an existing session, the connection is redirected to a server in the farm based on the load balancing configuration.
- If the load balancing feature is enabled, you configure a relative weight value for each server. The broker allocates connections to the server based on the server weight value. The weight value is a relative value, with higher values being allocated more connections than lower values. To identify how many connections are allocated to each server, add the weight values from all servers. Divide the total weight values with the weight value from a single server. For example, if you have one server with a value of 100 and a second with a value of 50, the first server will fulfill 2/3 of the overall requests to the farm.

Use the following process to configure Remote Desktop Services to use a session broker:

1. Install the RDS Session Broker role service on a Windows Server 2008 or later server.
    - Because the load on the RDS Session Broker is small, you only need a single broker for the Remote Desktop server farm.

    - The role service does not need to be installed on a Remote Desktop server.
2. On the RDS Session Broker server, add each Remote Desktop server to the Session Directory Computers local group (add servers to the domain group if the broker is a domain controller).
3. On each Remote Desktop server, configure the server to be a member of the server farm. Only servers running Windows Server 2008 can be configured as server farm members. Use the Remote Desktop Services Configuration tool to identify the following configuration information:
    - The name or IP address of the RDS Session Broker server.
    - The farm name. The farm name identifies a group of Remote Desktop servers. It is recommended that this name match the name used in DNS that identifies the farm cluster.
    - Whether load balancing is performed, and the relative weight for the server when using load balancing.
    - The IP address to use for redirection.

    ***Note**: You can also use Group Policy to configure broker settings on each Remote Desktop server.*

4. Configure either DNS round robin or Network Load Balancing (NLB) to point to the server farm. Client computers use DNS or NLB to locate the server farm for the initial connection. Following the initial connection, the RDS Session Broker redirects the connection to a specific Remote Desktop server. When configuring DNS round robin, configure multiple host (A) records using the server farm name as the host name and the IP address of the Remote Desktop servers for the IP addresses.
5. For Remote Desktop Services clients, ensure that they are running the Remote Desktop Client 5.2 or later when using load balancing.
    - When using DNS round robin, use the DNS name of the server farm to connect to Remote Desktop Services.
    - When using NLB, use the DNS name or IP address of the server farm to connect.

6.10. RDS Gateway

Remote Desktop Services Gateway (RDS Gateway) is a role service that allows users with the Remote Desktop client and an Internet connection to connect to computers on an internal network.

- RDS Gateway enables connections to Remote Desktop servers and connections to other computers running Remote Desktop.
- RDS Gateway encrypts the Remote Desktop Protocol (RDP) data using SSL over HTTP. This means that Remote Desktop communications use port 443, a port that is already allowed through most firewalls. This enables the remote connection without having to configure a separate VPN connection.
- RDS Gateway restricts access to computers on the private network that are running RDP. Additionally, you can further restrict access to specific servers.
- RDS Gateway is compatible with the Windows Server 2008 and later implementation of Network Access Protection (NAP). You can configure RDS Gateway to enforce health policies defined by NAP.

To configure access using RDS Gateway:

- Obtain an SSL certificate for the RDS Gateway server. The subject name in the certificate must match the name of the server that has the RDS Gateway role service installed.
- Add the RDS Gateway role service to a Windows Server 2008 or later server.
    - In a production deployment, the RDS Gateway server will have a connection to both the Internet and the private network.
    - The RDS Gateway server typically does *not* run the Remote Desktop Server role service.
    - The RDS Gateway server must be a domain member if it will use Active Directory accounts in RDS CAPs or RDS RAPs, or if you are using a load-balanced RDS Gateway server farm.
- The following services are also required and will be added automatically if required:
    - Remote Procedure Call (RPC) over HTTP Proxy
    - IIS 7.0/8.0/9.0

    - Network Policy and Access Services with the Network Policy Server role service
- The RDS Gateway server controls access to resources on the private network using the following policies:

Policy Type	Description
Connection Authorization Policy (RDS CAP)	A Connection Authorization Policy identifies the users who are allowed to establish a connection through the RDS Gateway server. The policy can restrict access based on: o User group membership o Computer group membership o Supported authentication method (either password or smart card)
Remote Authorization Policy (RDS RAP)	A Remote Authorization Policy identifies the internal resources that users are allowed to access. The policy restricts access: o Based on user group membership o For specific groups of computers (identifies to which computers access is allowed) o On specific ports, either 3389 or a custom port or port range

- Open port 443 in the external firewall, and port 3389 (or the custom port you specified in the RDS RAP) in the internal firewall.

Be aware of the following when using RDS Gateway:

- The RDS Gateway role service can only be installed on a server running Windows Server 2008 or higher
- Client computers require RDC version 6.0 or later. Supported clients are:
    - Windows XP SP2 or higher
    - Windows Vista or higher
    - Windows Server 2003 SP1 or higher

    - Windows Server 2008 or higher
- Internal computers that are running Remote Desktop can be accessed through the RDS Gateway. Supported Remote Desktop clients are:
    - Windows XP SP2 or higher
    - Windows Vista or higher
    - Windows Server 2003 with SP1 or higher
- Remote Desktop servers accessible through a RDS Gateway server must be running either Windows Server 2003 SP1 or higher, or Windows Server 2008 or higher.
- If you have multiple RDS Gateway Servers in a load balanced solution, you can set up a RDS Gateway server farm.
- Use the RDS Gateway Manager to configure RDS CAPs, RDS RAPs, to join the server to a RDS Gateway server farm, or to monitor client connections. You can view information about active connections including:
    - The connection ID, including the tunnel ID and the channel ID.
    - The domain and user ID of the user logged on to the client.
    - The date and time when the connection was initiated.
    - The length of time the connection was active.
    - The name of the internal network computer to which the client is connected.
    - The IP address of the client.
    - The port number used for the connection.
- To centralize RDS CAPs and RDS RAPs, you can configure the RDS Gateway server to use an NPS server that is configured as a RADIUS server.
- On the client computer, use the name or IP address of the Remote Desktop server you want to connect to. You can configure the Remote Desktop software to automatically detect the RDS Gateway server, or to use a specific RDS Gateway server when connecting to the Remote Desktop server.
- You can use a RDS Gateway server in conjunction with Microsoft Internet Security and Acceleration (ISA) Server to enhance security.
    - Place the ISA server in the perimeter network, and the RDS Gateway server in the private network. (Depending on the configuration, you can also place the RDS Gateway server inside the perimeter network.)
    - Copy the SSL certificate of the RDS Gateway server to the ISA server.
    - Create a Web publishing rule on the ISA server that uses SSL bridging.

        - To enable HTTPS-HTTP bridging, choose **Secure connections to clients**.
        - To enable HTTPS-HTTPS bridging, choose **Secure connection to clients and Web server**.
    - On the RDS Gateway server, enable HTTPS-HTTP bridging. This configures authentication to be performed by the ISA server.
    - In DNS, configure the A record for the RDS Gateway server to point to the ISA server.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

6.11. WSRM

Windows System Resource Manager (WSRM) is a tool that you can use to control the use of system resources by applications, processes, or services. By controlling resource allocation, you can ensure that critical processes will always have the necessary resources. Additionally, you limit the use of resources by other processes, ensuring that they cannot consume too many resources and negatively affect the running of other processes.

With WSRM you can:

- Control CPU utilization by process, allowing a specific process to use up to a target CPU utilization percentage.
- Allocate memory resources for an application, configuring the amount of RAM that can be used by an application.
- Control resource use by Remote Desktop Services users or groups. For example, you can limit the resources used by each user, or allow one user to consume additional resources.
- Allocate resources to specific IIS application pools.

Resources are allocated in WSRM by creating resource allocation policies. The policy identifies the user or application and the resource limits that apply. WSRM includes four built-in policies:

Policy	Description
Equal_Per_Process	The **Equal_Per_Process** policy allocates processor resources equally between all processes. For example, if five processes are running, each can use up to 20% of the available processor resources.
Equal_Per_User	The **Equal_Per_User** policy allocates processor resources equally between users. All processes are grouped according to the user who is running the process. Each user is allowed the same percentage of resource use, regardless of the number of processes they are running. For example, a user who is running one application

	would be allocated as many resources as another user who is running three applications. This policy is typically used for application servers and Remote Desktop Services.
Equal_Per_Session	The **Equal_Per_Session** policy allocates processor resources evenly between Remote Desktop Services sessions. Each session has equal resource access, regardless of the number of processes running within the session.
Equal_Per_IISAppPool	The **Equal_Per_IISAppPool** policy divides processor resources equally between each IIS application pool, up to 99% utilization. Applications not running in a pool only get resources not being used by the application pools.

Be aware of the following when using WSRM:

- Install WSRM by adding it as a feature in Server Manager.
- Without WSRM, a service or process will use all available resources (all resources allowed by the operating system) when necessary. With WSRM, you can control the amount of resources used by a process or service.
- You cannot edit the four default resource allocation policies. Create your own policies to create custom policies.
- Set a policy as the Managing Policy to enforce the limits. Only one policy can be the managing policy at a time.
- You can use WSRM to collect resource use data. Set the policy as the Profiling Policy to collect data without actually applying resource limits. Information can be stored in the internal Windows database or to a SQL Server database.
- Use calendar rules to apply policies based on date or time. For example, you can configure the policy to be enforced only between specific hours or on specific days.
- The default policies only control CPU utilization. To control memory use, create your own resource allocation policies.
- You can use resource manager to configure CPU use based on processor affinity or percentage.

- CPU utilization is only managed by WSRM when the processor utilization is above 70%. When it is below 70%, users or applications can exceed the utilization specified in the corresponding policy.
- Resources used by the operating system are excluded and not managed. Policies allocate the remaining resources not used by operating system or excluded applications. For example, if the operating system is using 20% of the CPU, and if you were using the **Equal_Per_Process** policy with four running processes, each process could use up to 20% of the CPU (the remaining 80% CPU would be divided equally between all four processes).
- When configuring resource allocation policies, the recommended practice is to allocate only CPU use. In most cases, avoid controlling memory use, except for applications that have consistently high memory use.
- Do not use WSRM to allocate resources for processes that include their own resource allocation managers.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

6.12. Display Data Prioritization

Display data prioritization customizes the priority that a Remote Desktop server places on virtual channel traffic that is used for display, keyboard, and mouse data. You can improve the performance for Remote Desktop server clients by increasing the priority given to this type of traffic compared to other traffic types such as for clipboard, printing, and file transfers. For example, if you have a large print job, traffic generated by the print job could adversely affect Remote Desktop server data traffic. To improve performance, you can increase the priority given to display data.

Prioritization is configured by setting the following registry keys. All keys are found in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TermDD.

Registry Key	Description
FlowControlDisable	This registry key configures whether data prioritization is performed. • Set the value to 1 to disable prioritization. Additional settings are ignored and will not be applied. • Set the value to 0 to enable prioritization and to enforce any additional settings.
FlowControlDisplayBandwidth	This registry key identifies the amount of bandwidth dedicated to display data. The amount of bandwidth allocated to display data is calculated as a ratio of display and non-display data.
FlowControlChannelBandwidth	This registry key identifies the amount of bandwidth dedicated to non-display data. The amount of bandwidth allocated to display data is calculated as a ratio of display and non-display data.

FlowControlChargePostCompression	This value controls whether display data bandwidth is calculated using compressed or non-compressed data. • A value of 0 uses uncompressed (pre-compression) values when calculating the bandwidth. • A value of 1 uses compressed (post-compression) values.

When controlling bandwidth for display data and non-display data, a ratio of the FlowControlDisplayBandwidth and FlowControlChannelBandwidth settings are used.

- For example, a setting of 15 for FlowControlDisplayBandwidth and a setting of 5 for FlowControlChannelBandwidth dedicates 75% of the bandwidth to display data and 25% to non-display data.
- The default ratio without custom settings is 70:30 (70% for display data and 30% for other data).

***Note**: After changing the registry values, restart the server for the settings to take effect.*

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757