Microsoft RemoteApp for IT Tools

Jim Shakespear - Southern Utah University

Agenda

- Southern Utah University info
- Our IT Department
- Overview Remote Desktop Services
- SUU's deployment decisions
- RemoteApps list, publishing apps
- What security measures we've used
  - Separate IT Accounts
  - Deploying Software updates
- Gathering Statistics
- Contact info

Audience - Who are you and what do you want to know?

- How many are currently using RemoteApps?
- How many have deployed RemoteApps for:
  - End-user/customer type apps?
  - IT apps?
- How many have separate user accounts for privileges?
  - (separate Administrator account or other privileged account for faculty/staff computers, separate for Server Administrators, etc.)

Southern Utah University

- University of the Parks
- Shakespeare Festival - no I don't get free tickets :)
- Growing to almost 10,000 Students
- Full-Time Faculty/Staff around 900

SUU IT Department

- Centralized
- 23 Full-Time Technical Staff
- About 7 students in technical positions
- 13 technical help desk students
- Divisions: Academic Computing, Operations, Web Services, Security, Administrative Systems
- Implemented SCCM and Remote Desktop Services (RemoteApps) within the past couple years, currently using VMware for virtualization, and trying to improve security on a limited budget, currently implementing PKI

Previous way of getting IT work done

- All IT only have 1 user account that was used for everything
  - Email, computer login, Local Administrator for all computers/servers (as needed), Servers at least had Duo (two-factor) if they were important, and everything else
  - IT Workstations lived in a Privileged Subnet - could connect to any network devices/servers/computers (not quite ip any:any to all of campus, but close)
    - It's hard to leave such an environment, but I guess security is important
  - VPN Access
    - Again, with just the 1 user account
    - Pretty much same access as our Privileged Subnet

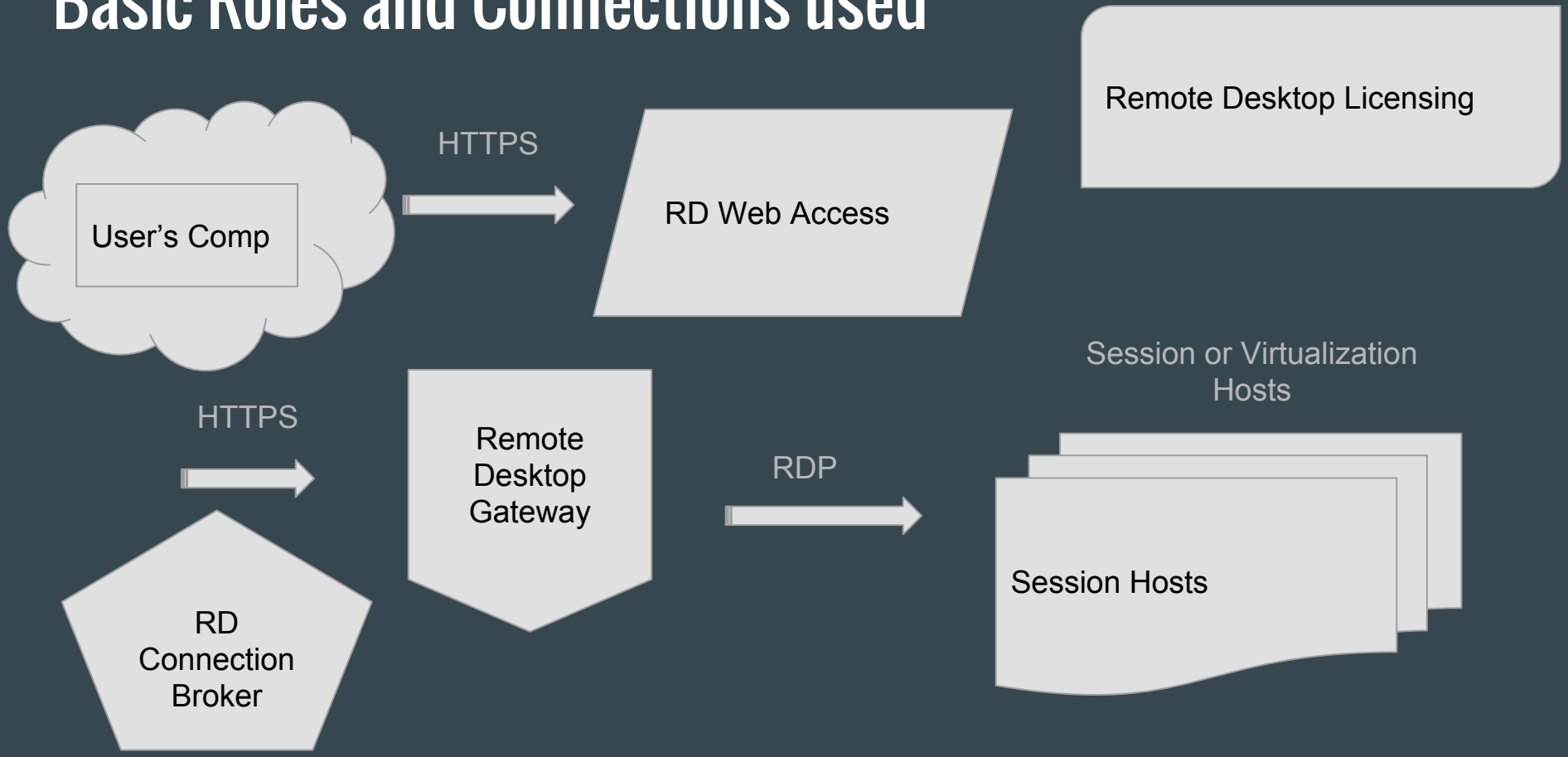
Remote Desktop Services

- RDS installation enables 6 role services
- Provides Remote Desktops and/or Applications
- Uses Remote Desktop protocol (RDP)
- RDP Gateway secures connections over the Internet, so users don’t need to use a VPN
- Faster access to remote data
- Less maintenance, quicker upgrades/deployments to apps, improved security

Remote Desktop Services - Roles

- RD Connection Broker
  - Manages connections to RemoteApps or virtual desktops
  - Session load balancing and reconnection
- RD Gateway
  - Authorizes secure connections over Internet (HTTPS encapsulation of RDP)
  - Authorization policies for who can connect and to what resources they can connect
- RD Web Access
  - Web-based interface to connect to RemoteApps
  - Publishes information to a feed for Start menu integration
- RD Licensing
  - Provides access to RDS CALs
  - Issues/tracks RDS CAL availability
- RD Virtualization Host
  - Integrates with Hyper-V role to provide VMs to be used as virtual desktops
  - Can have pooled and personal desktops
- RD Session Host
  - Provide session-based desktops and applications (RemoteApps)

Basic Roles and Connections used



Remote Desktop Services - SUU's Deployment decisions

- Why and how we'd use it?
  - IT apps only (improvement/replacement for IT workstations with privileged access to resources)
    - Use low privileged creds for workstation and higher privileged creds with RemoteApps
  - Separate enterprise software and flavor of the week programs
    - Limited Administrator rights (only few can approve and install RemoteApps needed)
  - Access to apps from any campus computer and from home
    - Improve security, but allow for more flexibility
- Servers Needed
  - Front-end Server (we'll call it Connect)
    - DMZ type subnet
  - Session Hosts: AcaComp, Ops, AdmSys, Sec, ITNet, Others as needed
    - Highly Protected Subnet with no direct Internet Access

Connect Server

- Roles
  - RD Connection Broker
  - RD Gateway
  - RD Web Access

Control Panel for RemoteApp points to this server for IT devices

Website connection made to this server on campus computers when IT needs a tool

Remote Desktop Gateway Managers (CAP and RAP policies)

RemoteApp Users Allowed (created local group)

Session Hosts and Apps

- AcaComp
  - Access Remote Administration Tools
  - Access All End-user subnets
  - Access limited servers for maintenance
- Ops
  - Access Remote Administration Tools
  - Access All Servers
- AdmSys
  - Access Remote Administration Tools
  - Access limited servers
- Sec
  - Access Remote Administration Tools
  - Access Security servers/devices/tools
- ITNet
  - Access Remote Administration Tools
  - Access All network devices

List of Apps

- Remote Administration Tools
  - Active Directory Users/Groups
  - Group Policy
  - DFS Management
  - Etc. . .
- Putty
- Chrome
- Firefox
- Terminals
- VMware vSphere
-

Publish RemoteApps

- Collection - Contains groups of session hosts that have the same apps and access
- Using the GUI
  - Finds apps automatically from the list of installed applications
  - Can’t customize all details, but does pretty good with defaults
  - Slow when you’re publishing lots of applications
- Using Powershell
  - Can get automatic list of installed applications
  - High customization - can be customized after using GUI
  - Quickly publish the same application to other collections

Powershell snippets

New-RDRemoteApp -CollectionName AcaComp -DisplayName "Active Directory Users and Groups" -FilePath "C:\Windows\System32\dsa.msc" -Alias ADUsers -IconPath "C:\Windows\system32\dsadmin.dll"

get-rdremoteapp -alias gpmc -CollectionName AcaComp | foreach-object {new-rdremoteapp -CollectionName Ops -alias $_.alias -FilePath $_.FilePath -IconPath $_.IconPath -IconIndex $_.IconIndex -DisplayName "Group Policy Management - Ops"}

Security

- Session hosts network restrictions
  - Limited to connect server going in
  - Hosts can only go out to subnets/servers they manage
  - Internet cannot be directly accessed
- Privileged IT accounts are not Administrators on Session Hosts
  - Limited number of admins for approval and installation of new apps
- Two-Factor logins using Duo Security
- CAP and RAP policies
- Each IT division has separate collections to use

Account Separation and VPN

- IT personnel should have multiple accounts
- Least Privileged
  - Used for Email, AD login without Administrative rights, treated like a regular campus user
  - Has VPN rights to connect to campus as well as hit the Remote Desktop Gateway/Website
- Campus Privileged
  - Used for Administrative rights on end-user computers
  - Can help limit pass-the-hash attacks, used only if needed on client workstations
- Server Privileged
  - Used for connecting to RemoteApps, performing server maintenance
  - Has VPN rights to get to Servers/Subnets depending on IT division
    - Provides a backup plan in case the RemoteApp Servers are down
- Domain Privileged/Specialized privileges
  - Should be very limited

Software updates

- Ninite for common programs
  - Chrome, Firefox, PuTTY, Notepad++, Java, etc.
  - “Frozen” installers created on different server with Internet access
  - Update script runs daily with Task Scheduler
  - Updates distributed using DFS
- Windows updated using local WSUS
- Other enterprise software updated manually as needed

Highlighted Programs

- PortableApps
  - Firefox with Java
    - Java can be installed as portable so it doesn't affect the whole server
    - Can have an older version of Firefox and Java to support older Java applets
  - Java
    - Launch JNLP files with new or old versions
- Terminals
  - Tabbed Remote Desktop
  - Can store credentials
  - Can provide an unlock password for further security

Gathering Statistics

- What kind of stats do you get for using RemoteApps?
  - Time an app runs (many probably run idle for a long time)
  - Number of app launches (easy to implement with a script)
  - Who uses what apps (can also be scripted)
  - Any other types of metrics?
- Basic script:
  - Echo %username% ProgramName %date% %time% > %date:~4,2%-%date:~7,2%-%computername%.txt
  - Start “Program Name” “Path/to/program.exe”
  - Publish that bat/cmd file as a RemoteApp

Our statistics program (written in C++)

- RemoteAppStats.exe
  - Has parameters for Program Name, Executable location, Executable Parameters, and launching a cmd file
  - Launched cmd file can export data into preferred format (with whatever commands you want)
  - Can be the published executable (with command-line parameters published also) or can be a parameter or ran in a script without specifying an executable location
- Caveats
  - Command-Prompt flashes with each app launch
  - One CSV file per server per day (but could be changed using launched script)
  - Data must be manipulated manually for reporting (currently using Excel Pivot charts)

Questions???

- Does it sound like something you'd implement?
- Did we cover everything for security?
- Would you do anything different?

Any questions for me?

Contact Info

Jim Shakespear

shakespear@suu.edu

www.jshakespear.com - Career website (needs an update)