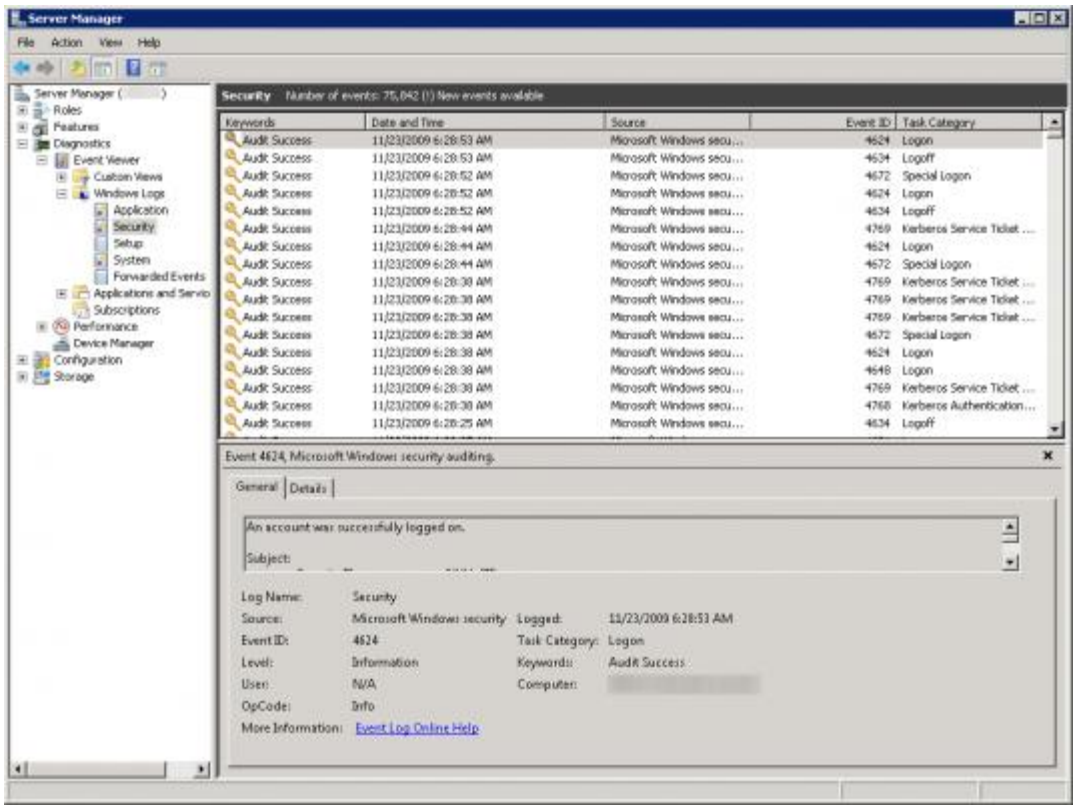
Generate Reports About User Actions on Windows Servers

Whenever there is need to generate reports about what users have been doing on your servers, most administrators are left empty handed. This need may arise due to some misconfiguration that someone did, a deleted configuration file, a registry key that someone edited, Active Directory objects such as users, groups or OUs that were changed or even deleted and many more. These configuration changes and other actions can potentially render a server or even the entire system inoperable, but the sad thing is that there are very few ways in which an administrator can truly see or tell what exactly happened and who did it.

The lack of reporting capability in Windows-based operating systems is not new. Administrators have been left "in the dark" ever since the old days, and although Windows Server 2008 and Windows Vista/7 have changed the way administrators work with the Event Viewer, it's still up to us to perform the tedious task of decrypting long and poorly written events, decipher event IDs (many of which share the same number, but for a wide variety of error codes and sources).

Even with the new and re-designed Windows Server 2008/Vista/7 Event Viewer, many human actions are still not recorded. For example, unless you specifically enable Object Access auditing in the local policy of the system (or through a GPO), there is no way on earth to tell what files have been modified or deleted, by whom, and in what context. For example, getting a security event saying that someone tried to delete the Web.Config file of a web server repeatedly means nothing on it's own, unless you can see who did it, what else did they do (or attempt to do), and under what context.

Now, lets say that your job requires you to perform a daily audit of all the privileged users' actions on a bunch of servers. How would you approach that kind of task? Is this something that Windows logs, Event Viewer, or any other type of built-in tool can give you? Can this help?



The answer to this is no. No matter how hard you try, no existing built-in Windows tool can even come close to getting you near the type of information you're after.

Enter ObserveIT.

ObserveIT is a company that has an amazing solution for one of the toughest questions that IT professionals face in today's dynamic IT world: Who touched my servers, what did they do, what did my privileged users do, what did my external vendors change on my servers. ObserveIT's product allows enterprise-wide recording and indexing of any human interaction with the servers, and what makes it so awesome is the fact that it indexes this data alongside with detailed metadata of what is seen on the screen, allowing full searches within the database. I've written more about ObserveIT's recording capabilities in my "Record and Audit Terminal, Citrix and RDP Sessions – ObserveIT Product Overview" article.

ObserveIT Express is a freeware version of ObserveIT's flag ship product - the Pro edition. Read more about it on my "Free Remote Desktop, Terminal & Citrix Session Recorder: ObserveIT Express" article.

By implementing the freeware version of ObserveIT in your environment, you can get full visual recordings of up to 5 monitored servers. Another limitation of the Express edition is the fact that you can only reply the past 24 hours, however, detailed textual information is still available even past this time . The Pro edition is licensed, and there is no limit to the number of servers that can be monitored by it, and no limit on the recorded data replay capabilities. Furthermore, the Pro edition has many interesting configuration capabilities, as described in the above article.

One of the coolest features of version 5.0.0 is its ability to create and generate very complex and detailed reports that are extracted from the recorded data. The Reports View allows the administrator or security auditor to get aggregated or summary information about server and user activity. In this version, ObserveIT offers a newly designed and feature-rich reports generator that can be used either by novice administrators to generate reports based on the pre-configured and built-in reports, or by advanced administrators and security auditors that require flexible application usage reports and trend analysis reviews alike.

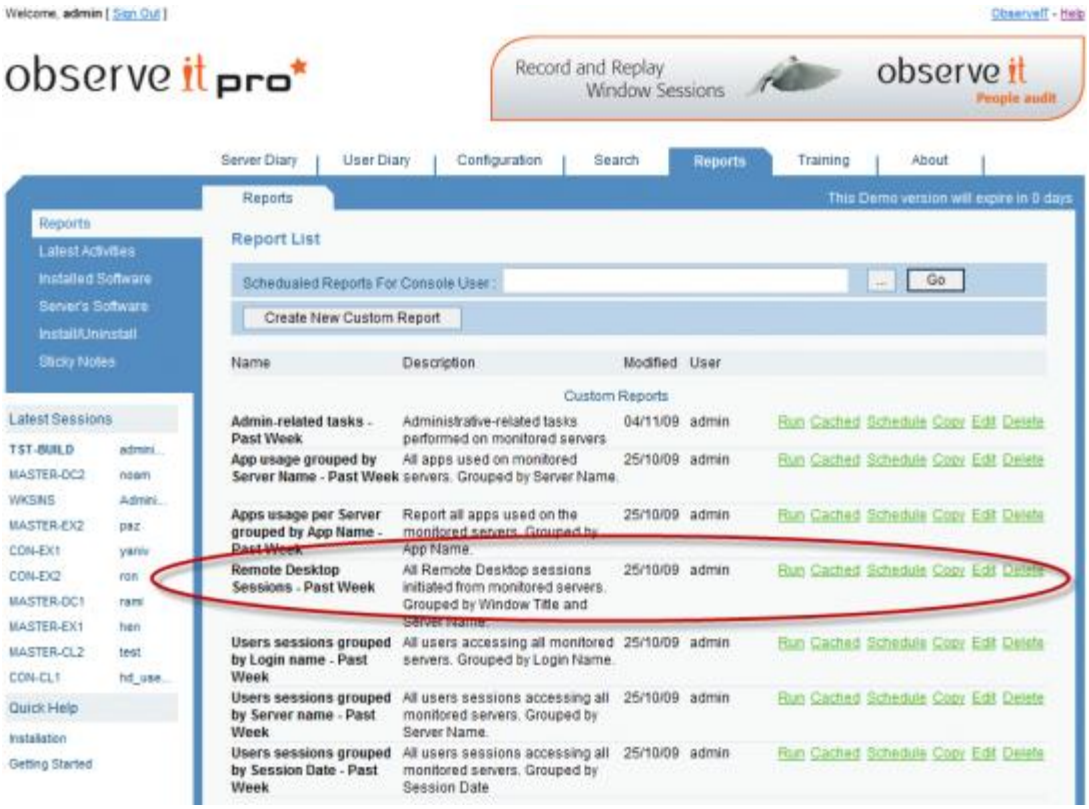
Experienced administrators or security auditors can create comprehensive reports based on their requirements. Reports can be created to identify trends and usage, identify applications and users, and specify enhanced filters and sort-by columns.

The built-in reports can be run by pressing one button, and within moments (based on the type and range of report), the administrator will be able to review the results in a separate window, print them or export the information to an Excel spreadsheet.

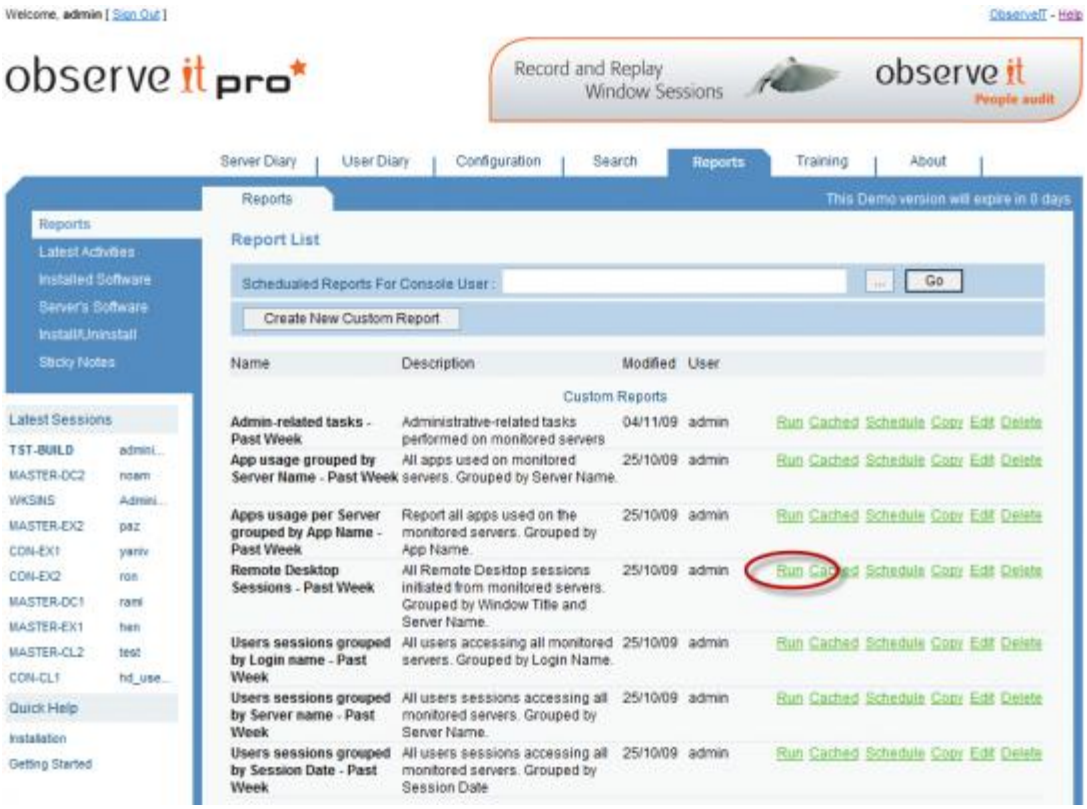
Reports can also be scheduled to run at pre-defined intervals, and the results can then be e-mailed to SMTP aliases that need to review the results. This allows the administrators or security auditors to get daily, weekly or monthly reports of any type of user activity that was performed on the monitored servers, without having to manually dig through tons of log files and event IDs, most of which cannot even come close to giving them the entire picture of what happened on the monitored machines.

The reports generator is controlled by the same granular permissions model that is used for Console Users, and this means that a report will not reveal information that the administrator does not have permissions to view.

In this example, lets say that a company's security auditor has deployed ObserveIT, and now wants to generate a report of all the instances of Remote Desktop access that were performed on any of the organization's servers. After logging on to the ObserveIT web console, the administrator reviews the existing sample reports that were built-in into ObserveIT. One of these reports does exactly that. It generates a report of all the instances of Remote Desktop Connection (mstsc.exe) usage on the monitored servers.



The administrator runs the built-in sample report. Within a few seconds, a detailed report of all the RDP sessions in the past week is displayed.



This sample report includes 3 results, representing 3 different sessions to 3 different servers.

Information can be expanded, as needed.

observe it pro

Report Name: **Remote Desktop Sessions - Past Week**

Convert To: Excel

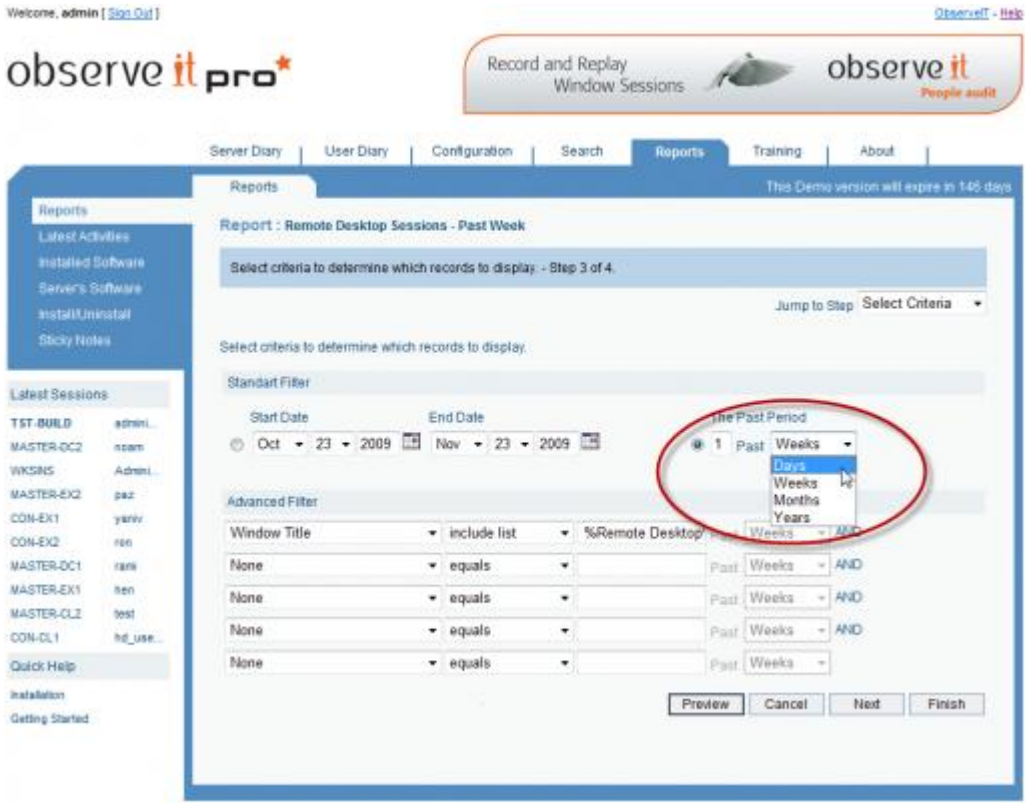
Filtered By:
Session Start DateTime Last 1 Week AND
Window Title include list **%Remote Desktop%**

Show All Details | Show Selected Details | Hide Details

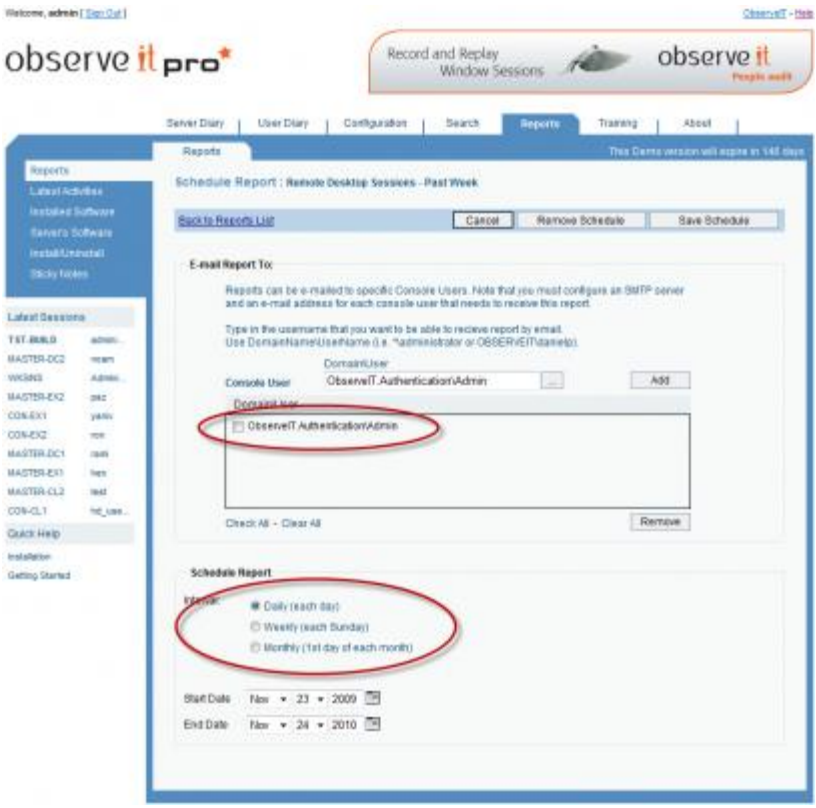
Server Name	Process Name	Login Name	User Name	Domain Name	Session Start Date	Session Start Time	Window Title Video
Window Title: 192.168.200.102 - Remote Desktop (1 record)							
TST-BUILD	mstsc.exe	administrator	n/a	TST-BUILD	11/23/2009	04:52PM	
Window Title: 192.168.200.150 - Remote Desktop (1 record)							
TST-BUILD	mstsc.exe	administrator	n/a	TST-BUILD	11/23/2009	04:52PM	
Window Title: 192.168.200.172 - Remote Desktop (1 record)							
TST-BUILD	mstsc.exe	administrator	n/a	TST-BUILD	11/23/2009	04:52PM	
Window Title: Remote Desktop Connection (1 record)							
TST-BUILD	mstsc.exe	administrator	n/a	TST-BUILD	11/23/2009	04:52PM	

Total: 4 records.

Reports can be edited to fit your needs. In this example, the built-in report looks at a one week period, but the administrator needs to get just the past day's results. So, they edit the report and save it. Note that editing reports is only available in the Pro edition.



As noted above, reports can be e-mailed to specific administrators or security auditors, making their job a lot easier. All the needed information is sent to their inbox, daily.



You can obtain the freeware version of ObserveIT Express edition from this link: