



MULTI-PLATFORM ADMINISTRATION AND MANAGEMENT LAB

Published: April 2010

Abstract

This IVA Lab demonstrates how to use Weston Software Inc.'s Power Tool Administrator to securely manage and control non-Windows systems from a Microsoft desktop. In this Lab, you will see how you can use this non-intrusive solution that does not require system modification or the installation of software agents. As this Lab demonstrates, Power Tool Administrator does not require any specific skills to manage a heterogeneous environment.

Table of Contents

MULTI-PLATFORM ADMINISTRATION AND MANAGEMENT LAB	1
Abstract	1
Introduction.....	3
Lab Scenarios	5
Scenario 1: Configuring Power Tool Administrator.....	5
Adding Power Tool Administrator in the Microsoft Management Console.....	5
Adding a User	9
Adding a Host	12
Scenario 2: Creating a New User in a Linux System by Using Power Tool Administrator on a Windows System.....	14
Scenario 3: Creating a New Group in a Linux System by Using Power Tool Administrator on a Windows System.....	16
Scenario 4: Viewing Linux Group Information from a Windows Desktop by Using Power Tool Administrator	19
Scenario 5: Exporting Power Tool Administrator Reports.....	21
Scenario 6: Viewing Power Tool Administrator Process Information	23
Scenario 7: Automating Tasks by Using Existing Information in Your Environment.....	24
Scenario 8: Viewing Event Logs for Windows and Non-Windows Systems	26
Appendix: The Interop Vendor Alliance	28

Introduction

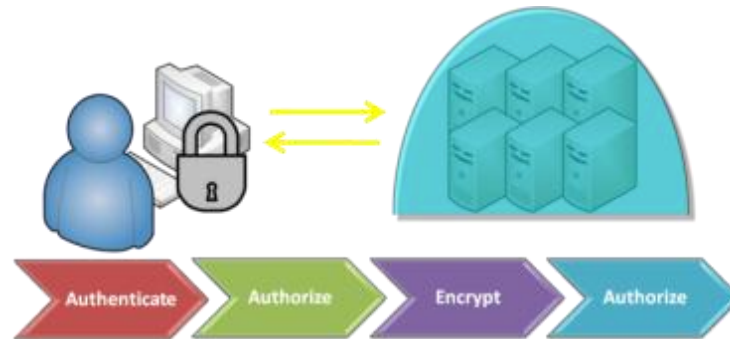
With the increasing complexity of heterogeneous and mixed IT systems, the necessities of securely managing and controlling heterogeneous environments represents a significant challenge to the IT field. This Lab explores various scenarios on how to use Weston Software Inc.'s Power Tool Administrator to securely manage and control non-Windows systems from a Microsoft desktop.

Power Tool Administrator is a non-intrusive, agent-less, and interoperable solution for managing accounts in heterogeneous IT environments where identity management, security, compliance auditing, and efficient control of IT administration costs are critical requirements for an enterprise. Power Tool Administrator enables you to control and manage heterogeneous environments regardless of their location ensuring that your systems can reside in emerging Computing Clouds, Virtualized environments (VMWare, Xen Source, and Hyper-V), or in Data Centers.

The Power Tool Framework™ merges the SSH protocol, the Microsoft Management Console API, the Windows Audit and Event log API, and the Microsoft Windows Security APIs to form a new platform for the secure management of non-Microsoft systems. Power Tool Administrator eliminates the need for a server-based management infrastructure by leveraging the value of advanced multi-processor architecture on a Windows-based desktop. Power Tool Administrator also serves as a trusted application that enables organizations to securely delegate user and group maintenance tasks to Windows-based help desk and support staff instead of highly-skilled UNIX administrators. The following list provides the key benefits of using Power Tool Administrator:

- Reduce costs: delegate tasks to authorities that do not need in-depth knowledge of other operating system commands, eliminate updates, installations, or configurations in the existing IT environment, leverage built-in SSO integration, automate maintenance tasks
- Achieve compliance: real-time reporting, consolidated reporting (orphan, access), real-time audit and event correlation, path-level reporting
- Improve efficiency: use one console to natively manage all environments (cloud, virtual, data center)
- Ensure security and reduce attacks: fine-grain, role-based administrative control of accounts and groups, administrative efficiency, and cross-platform auditing

The following illustration outlines how Power Tool Administrator accesses a UNIX or Linux host from a security-enabled Microsoft host.



1. User is authenticated by Windows.
2. User executes an authorized task within a Secure Store Enabled Management Console.
3. Credentials for connecting to the remote UNIX or Linux host are looked up within the Windows Credential Manager.
4. SSH connection started and communication to the remote host is performed over an encrypted communication channel.
5. Task execution is performed based on the authenticated token. Task execution is based on token allowed tasks as defined by the UNIX or Linux authorization sub-system.
6. Results of the command are displayed in the Secure Store Enabled Console.

For more information of Weston Software's solutions, visit:

- <http://www.westonsoftwareinc.com/products/Products.aspx>

Lab Scenarios

This IVA Lab consists of various scenarios that demonstrate how to use Power Tool Administrator to securely manage and control non-Windows systems from a Microsoft desktop. In this Lab, you will see that Power Tool Administrator does not require system modification or the installation of software agents on non-Windows systems. As this Lab demonstrates, Power Tool Administrator does not require any specific skills to manage a heterogeneous environment.

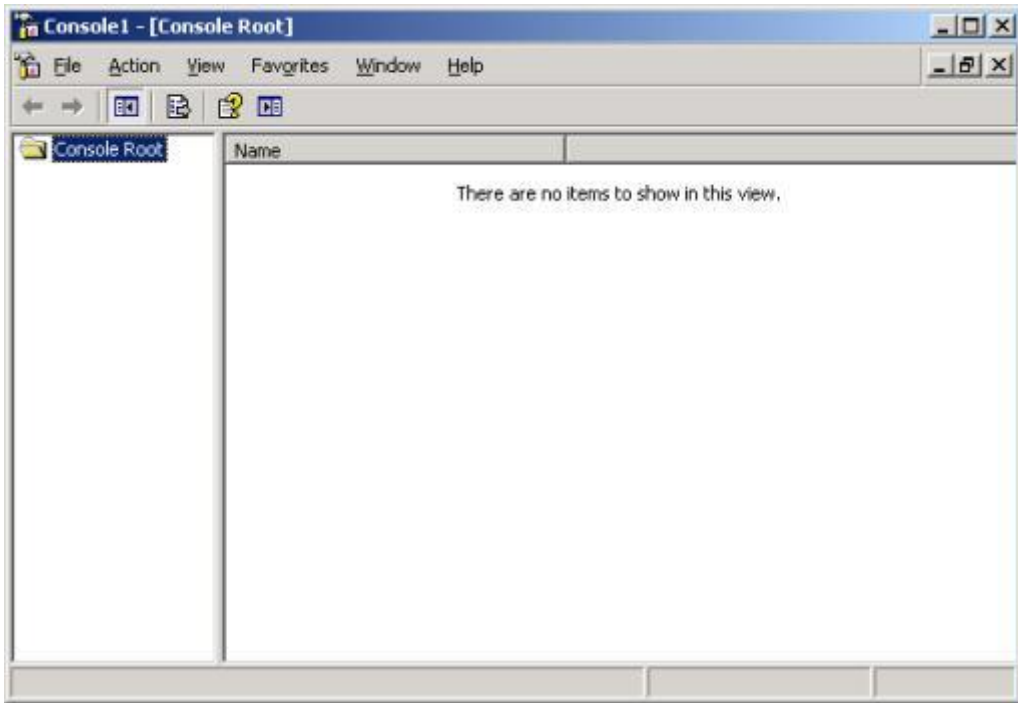
Scenario 1: Configuring Power Tool Administrator

Before you can start managing and controlling heterogeneous environments, you must first configure the Power Tool Administrator software that is installed on a Windows host. Power Tool Administrator does not require any additional deployment or configuration on the rest of the systems or the IT environments that you want to manage.

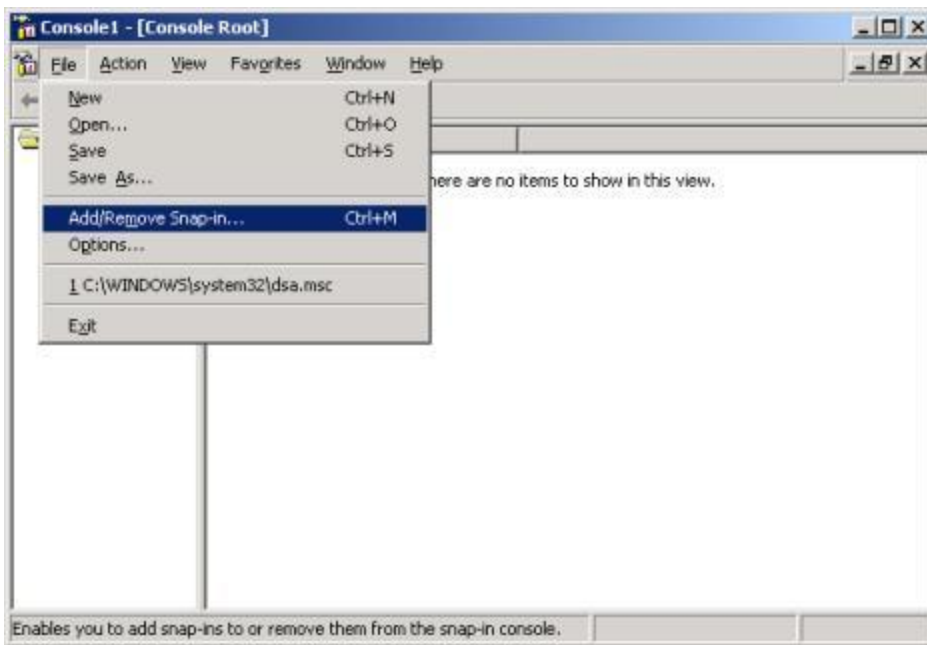
Adding Power Tool Administrator in the Microsoft Management Console

Before you can start using Power Tool Administrator, you must first add Power Tool Administrator in the Microsoft Management Console of the Windows host. To add Power Tool Administrator in the Microsoft Management Console, perform the following steps:

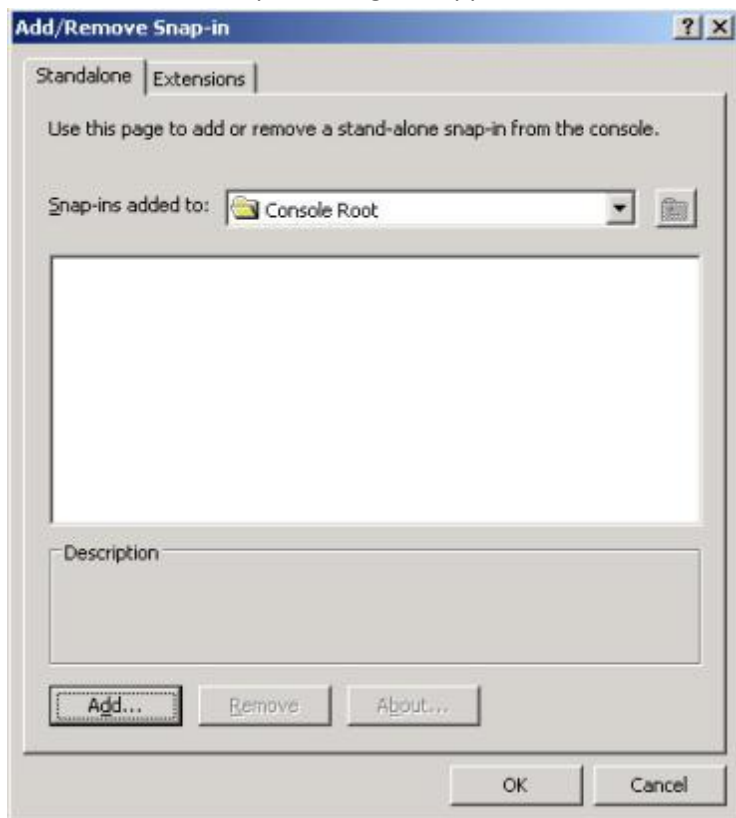
1. Click the **Start** button, and then click **Run**.
The **Run** dialog box appears.
2. In the Open box, type **mmc**, and then click **OK**.
The **Microsoft Management Console** appears.



3. On the **File** menu, click **Add/Remove Snap-in**.



The *Add/Remove Snap-in* dialog box appears.



4. Click **Add**.

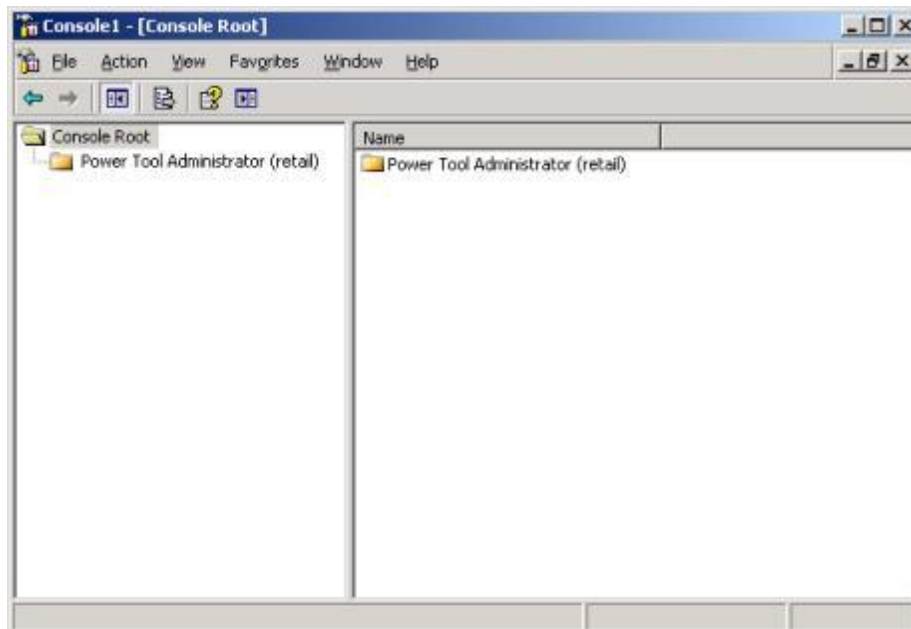
The *Add Standalone Snap-in* dialog box appears.



5. Click **Power Tool – Administrator**, click **Add**, and then click **Close**.

6. In the *Add/Remove Snap-in* dialog box, click **OK**.

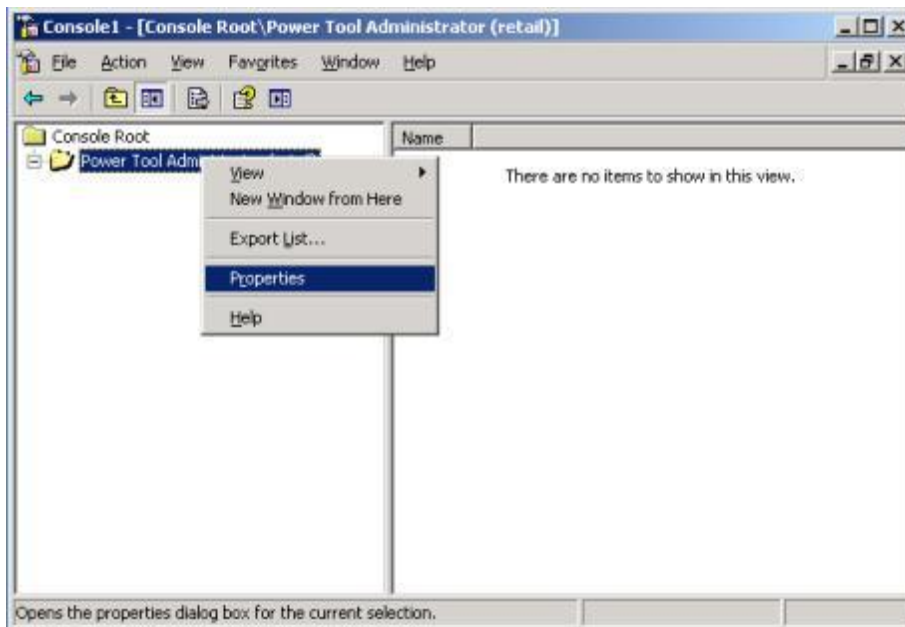
The Console Root now displays *Power Tool Administrator*.



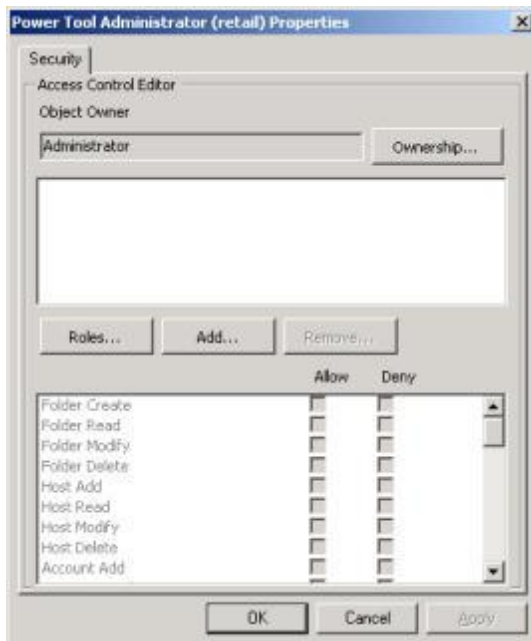
Adding a User

To ensure that only authorized users operate Power Tool Administrator, users and their roles are configured in the Power Tool Administrator. To add a user to Power Tool Administrator, perform the following steps:

1. On the *Microsoft Management Control* window, right-click on the *Power Tool Administrator* the folder, and then select **Properties**.



The *Power Tool Administrator Access Control Editor* dialog box appears.



2. Click **Add**.

The *Select Users, Groups and Computers* dialog box appears.

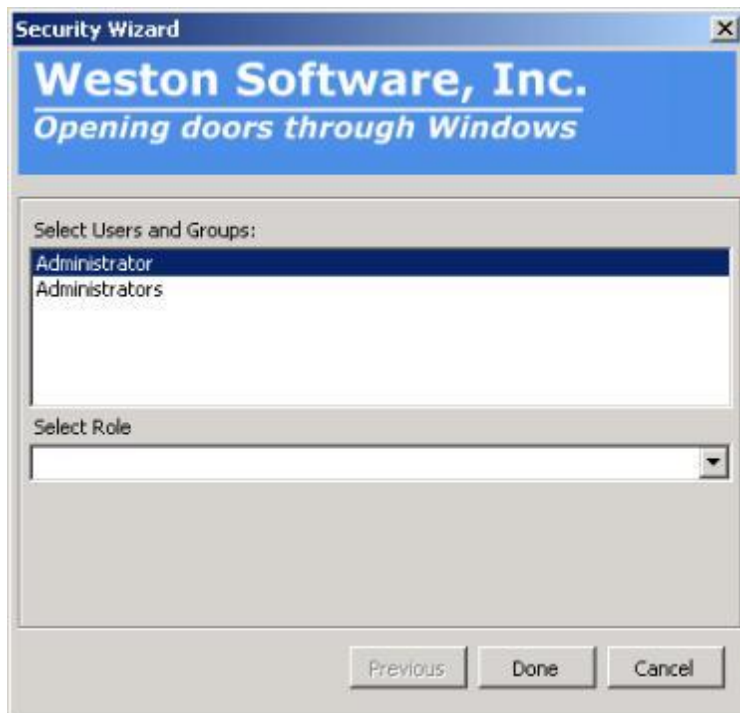


3. Select the users that you want to add and then click **OK**. To add a user from a locale or domain other than the local machine, click **Add**, click **Location**, select the appropriate folder, and then click **OK**.

The users that you added appear in the *Power Tool Administrator Access Control Editor*.

4. To define and set the security rights for the user, click **Roles**.

The *Security Wizard* dialog box appears.



5. In the *Select Role* list, click the role that you want to set for this user, and then click **Done**.



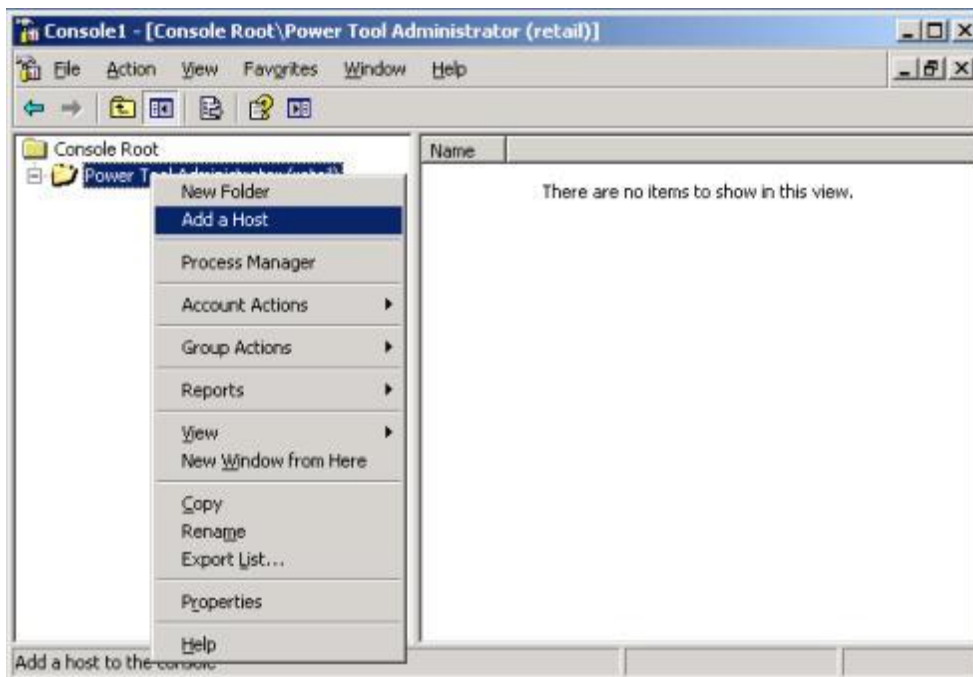
The user that you added can now use Power Tool Administrator.

Adding a Host

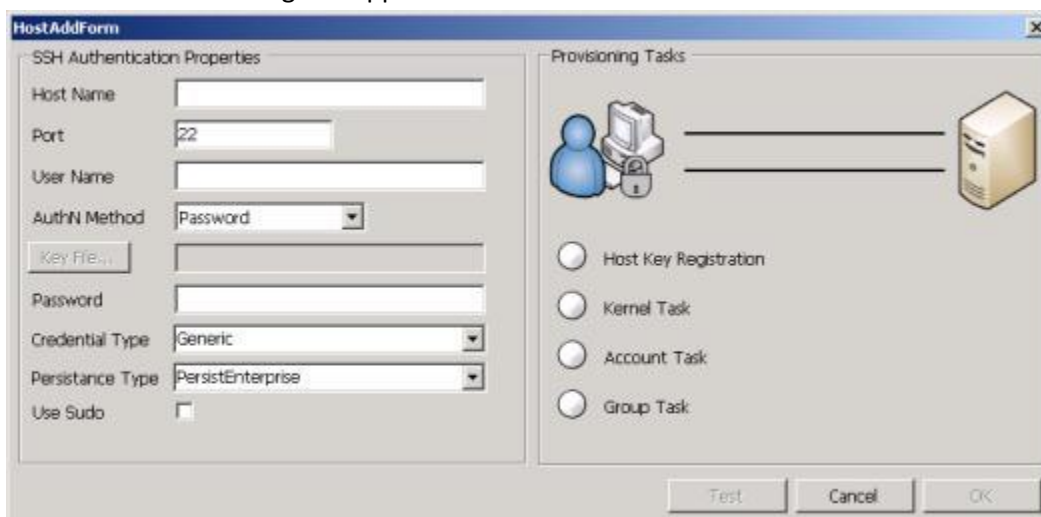
Adding non-Windows hosts to Power Tool Administrator allows you to securely manage and control various hosts from a Microsoft desktop. Power Tool Administrator eliminates the need for additional deployment or configuration on the rest of the systems or the IT environments that you want to manage.

To add a host to Power Tool Administrator, perform the following steps:

1. On the *Microsoft Management Control* window, right-click on the *Power Tool Administrator* the folder, and then click **Add a Host**.



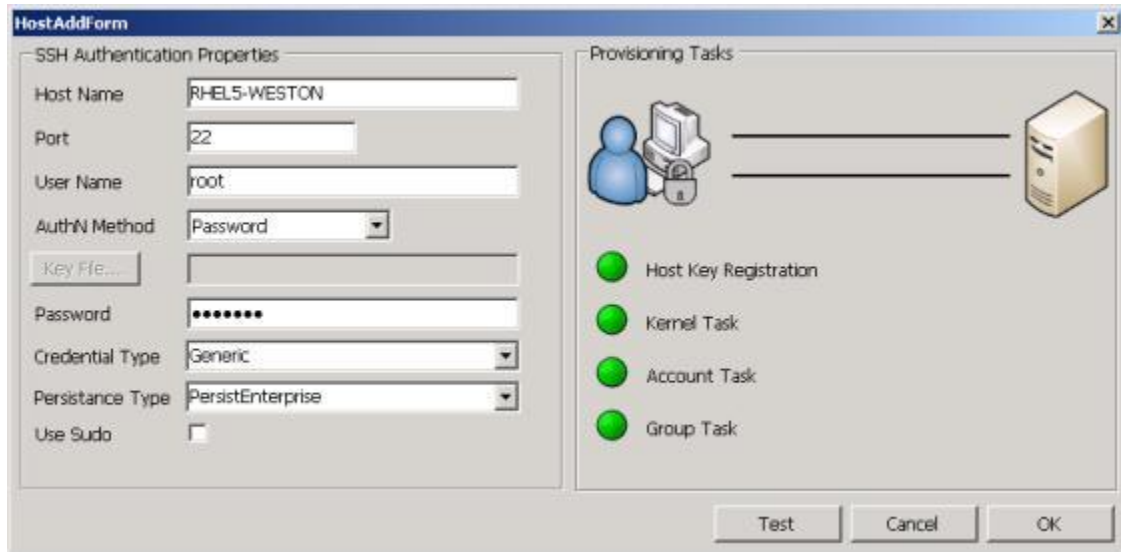
The *HostAddForm* dialog box appears.



2. Add the appropriate information in each field, and then click **Test**.
Power Tool Administrator starts an interactive terminal that enables the verification of SSH Host

Keys/password. It also provides queries of the remote host for kernel information, users, and groups.

3. Once all *Provisioning Tasks* are green, which confirms that each task is complete and the connection to the host is successfully established, click **OK**.



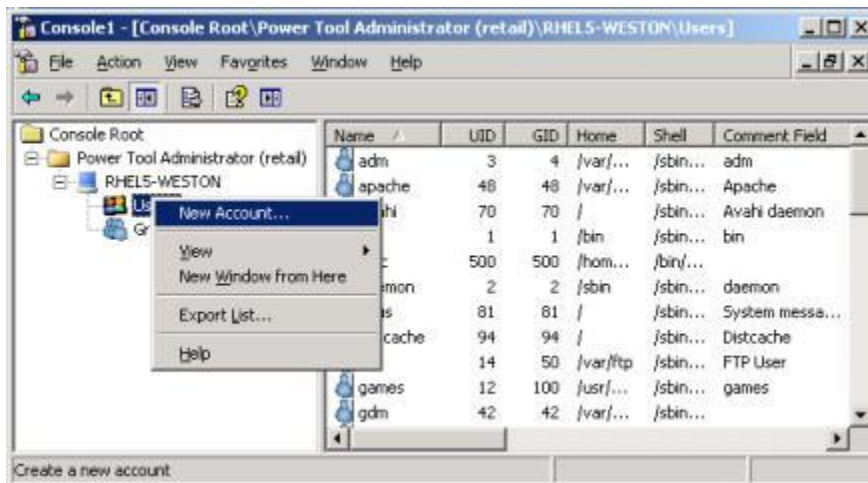
Power Tool Administrator now allows you to manage and control this non-Windows host from a Windows desktop.

Scenario 2: Creating a New User in a Linux System by Using Power Tool Administrator on a Windows System

This Lab demonstrates how to use Power Tool Administrator to add a user to a Linux host, from a Microsoft desktop.

Using Power Tool Administrator, you can add a new user to the Linux host, from the Windows desktop, by performing the following steps:

1. On the *Microsoft Management Control* window, under the *Power Tool Administrator* the folder, click the **Expand** icon for the Linux host to which you want to add a new user.
2. Right-click **Users**, and then click **New Account**.



The *Create Account* dialog box appears.

The screenshot shows the 'Create Account' dialog box. It contains the following fields and buttons:

- Account ID:
- UID:
- Comment Field:
- Home Directory:
- Default Shell:
- Primary Group:
- Password:
- Confirm Password:
- Buttons: Next, Look up..., Cancel, OK

3. Enter the appropriate information in each field, and then click **OK**.

The screenshot shows a 'Create Account' dialog box with the following fields and values:

Field	Value
Account ID:	Operator2
UID:	65537
Comment Field:	Operator
Home Directory:	/root
Default Shell:	/sbin/nologin
Primary Group:	0
Password:	*****
Confirm Password:	*****

Buttons: Next, Lookup..., Cancel, OK

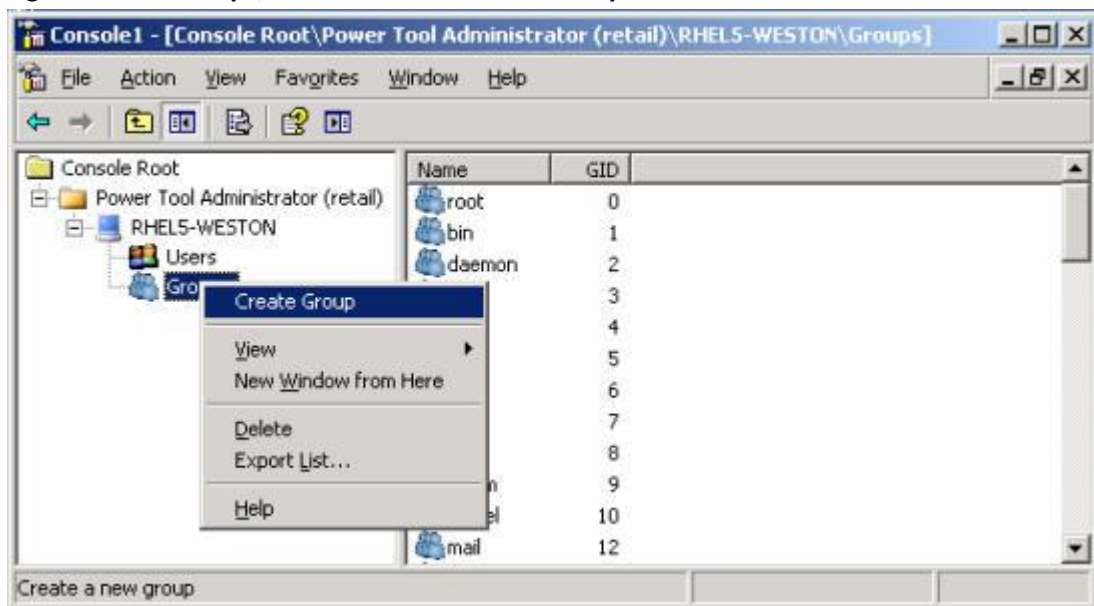
The user account is created in the Linux system.

Scenario 3: Creating a New Group in a Linux System by Using Power Tool Administrator on a Windows System

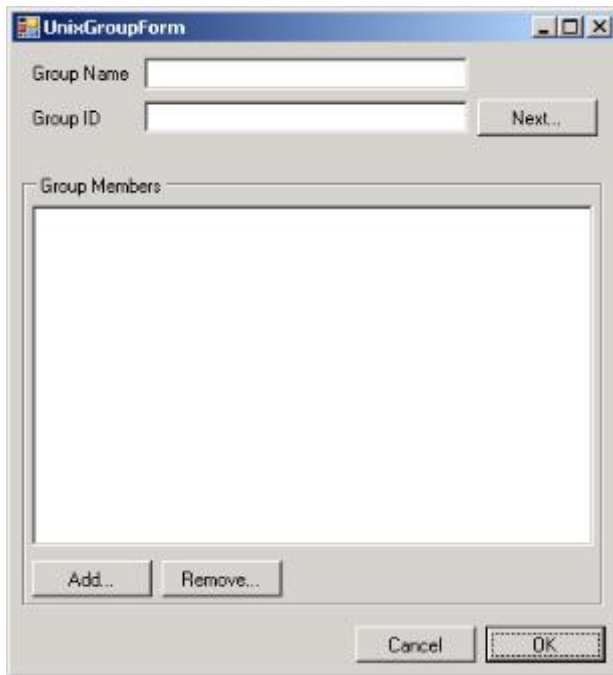
This Lab demonstrates how to use Power Tool Administrator to create a group in a Linux host from a Microsoft desktop.

Using Power Tool Administrator, you can create a new group in the Linux host, from the Windows desktop, by performing the following steps:

1. On the *Microsoft Management Control* window, under the *Power Tool Administrator* folder, click the **Expand** icon for the Linux host where you want to create a new group.
2. Right-click on **Groups**, and then select **Create Group**.



The *UnixGroupForm* dialog box appears.

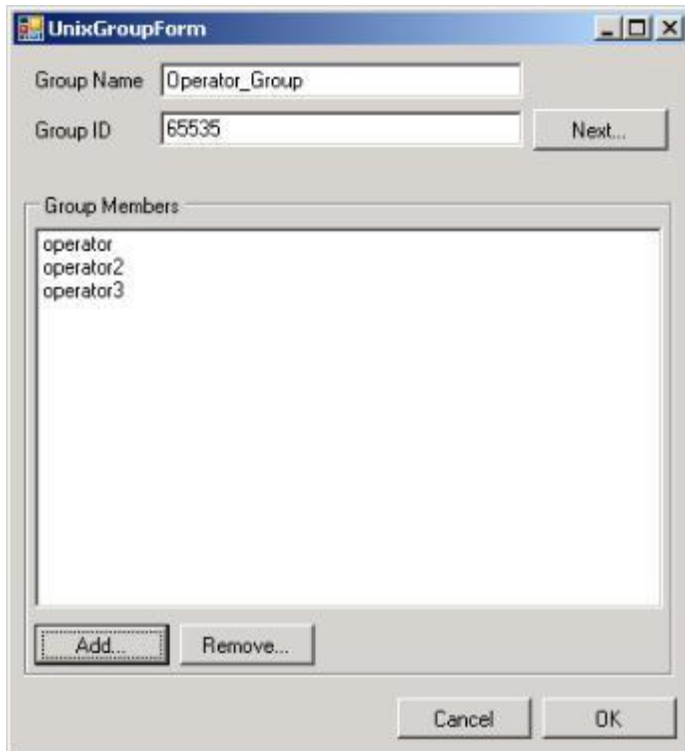


3. Enter the appropriate information in the **Group Name** and **Group ID** field.
4. To add members to this group, click **Add**.

The *Select Users* dialog box appears.



5. Select the users that you want to add to this group, and then click **OK**.
The users that you selected appear in the **Group Members** list.



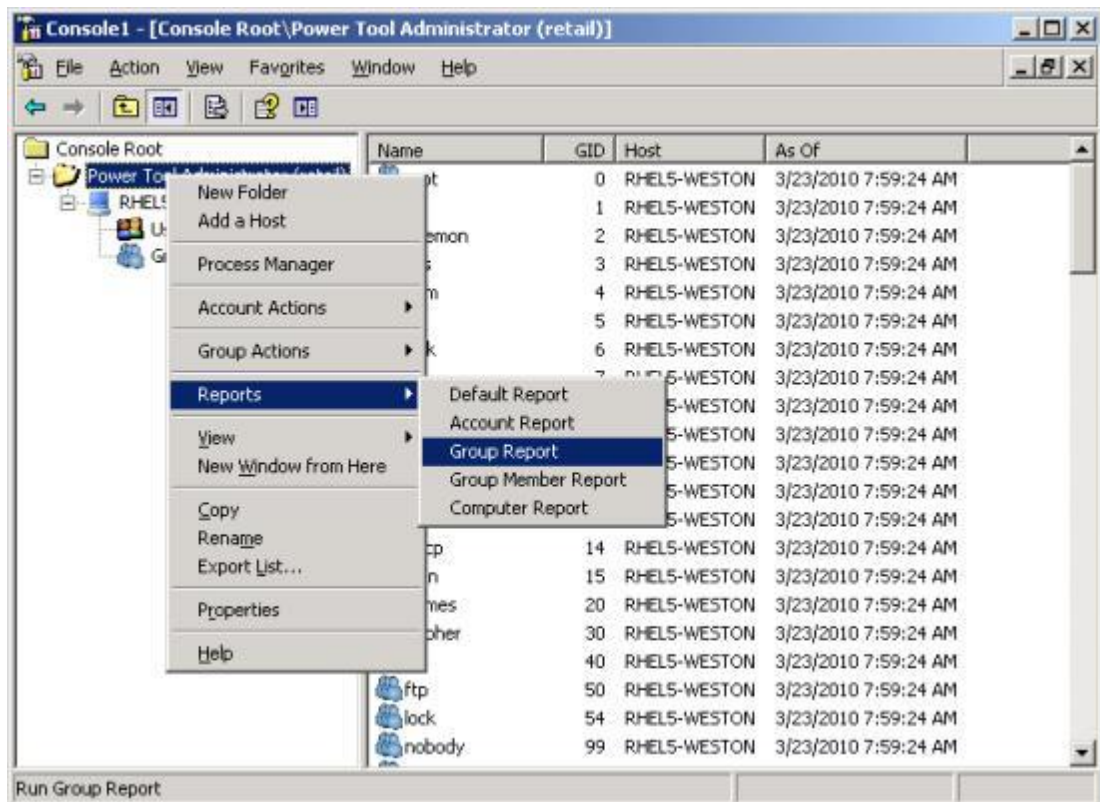
6. Click **OK**.
The group, with its appropriate group members, is created in the Linux system.

Scenario 4: Viewing Linux Group Information from a Windows Desktop by Using Power Tool Administrator

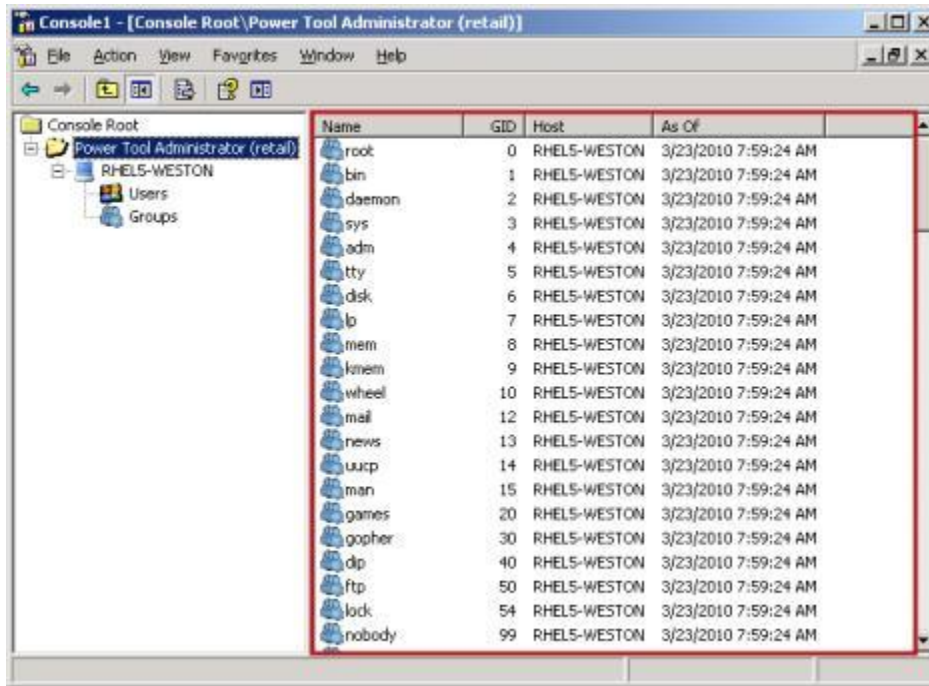
Power Tool Administrator provides reports that display significant information about various systems. This Lab scenario demonstrates how to use Power Tool Administrator to view significant information about various groups within a Linux host.

Using Power Tool Administrator, you can view group information within a Linux host, from the Windows desktop, by performing the following steps:

1. On the *Microsoft Management Control* window, right-click on the *Power Tool Administrator* folder, select **Reports**, and then **Group Report**.



2. The *Group Report* appears on the right pane.

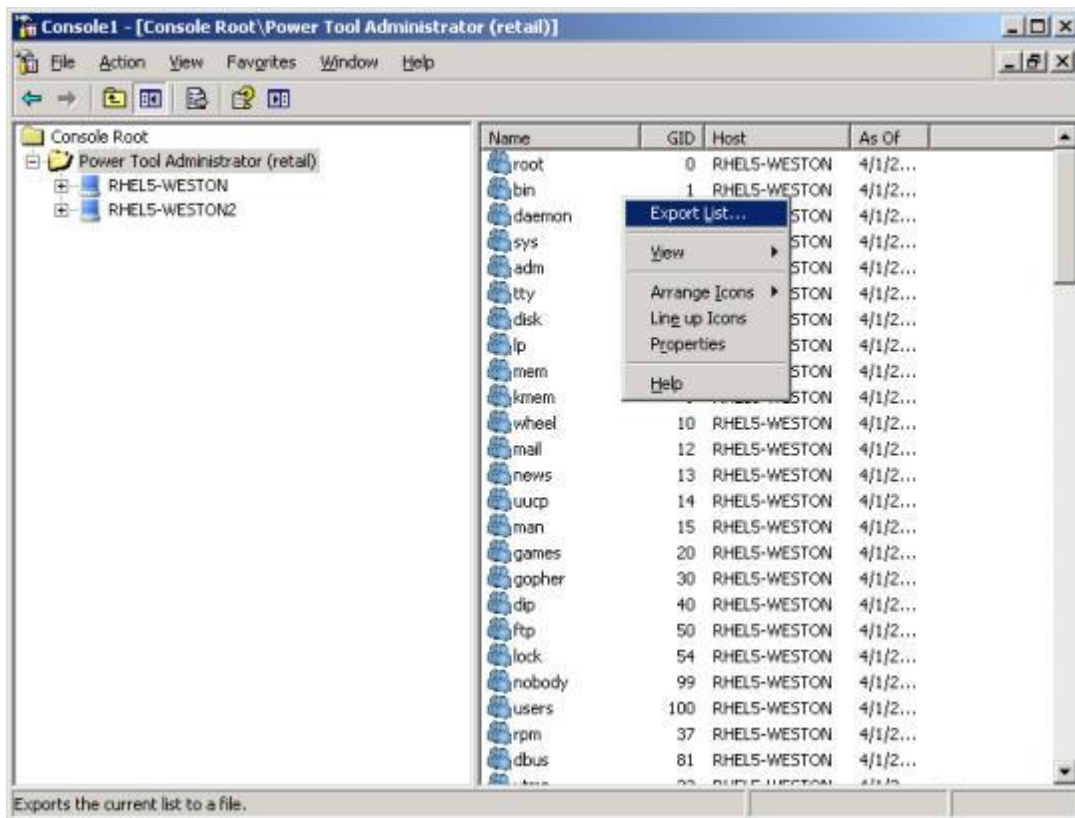


Scenario 5: Exporting Power Tool Administrator Reports

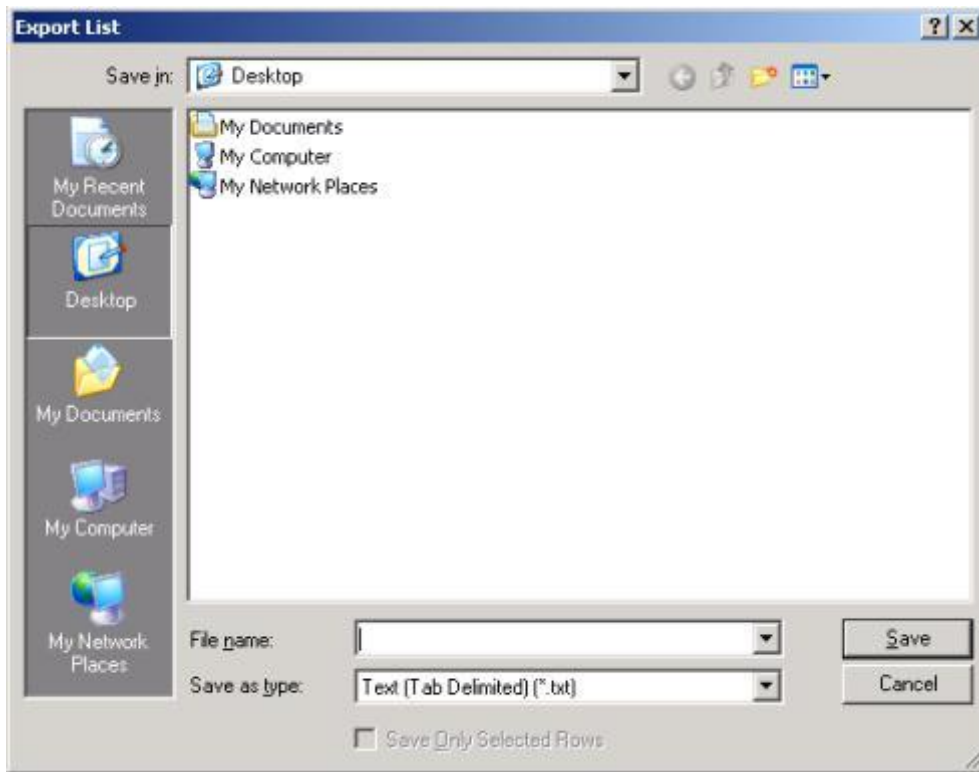
This Lab demonstrates how to use Power Tool Administrator to export a report. Power Tool Administrator allows you to export reports to many different formats, such as comma-delimited files (CSV) or tab-delimited files (TXT). This allows you to save, analyze, share, open, or convert data to a Microsoft Excel spreadsheet. The comma-separated format also allows you to easily import data into databases, such as Microsoft SQL Server, and leverage reporting services for custom report generation.

To export a report, perform the following steps:

1. Right-click on the desired report, and then select **Export List**.



The *Export List* dialog box appears.



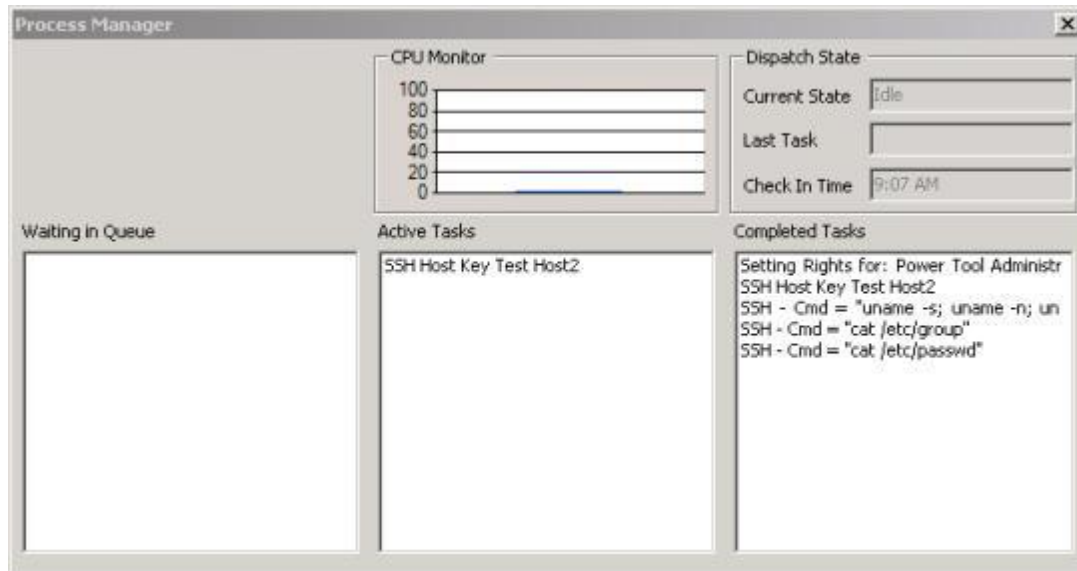
2. Save the report in the required file type.

Scenario 6: Viewing Power Tool Administrator Process Information

The Power Tool Administrator Process Manager provides various process-related information, such as the CPU usage, dispatch state, active tasks, completed tasks, and tasks waiting in queue.

To view process-related information, on the *Microsoft Management Control* window, right-click the *Power Tool Administrator* folder, and then click **Process Manager**.

The *Process Manager* dialog box appears and displays the CPU usage, dispatch state, active tasks, completed tasks, and tasks waiting in queue.



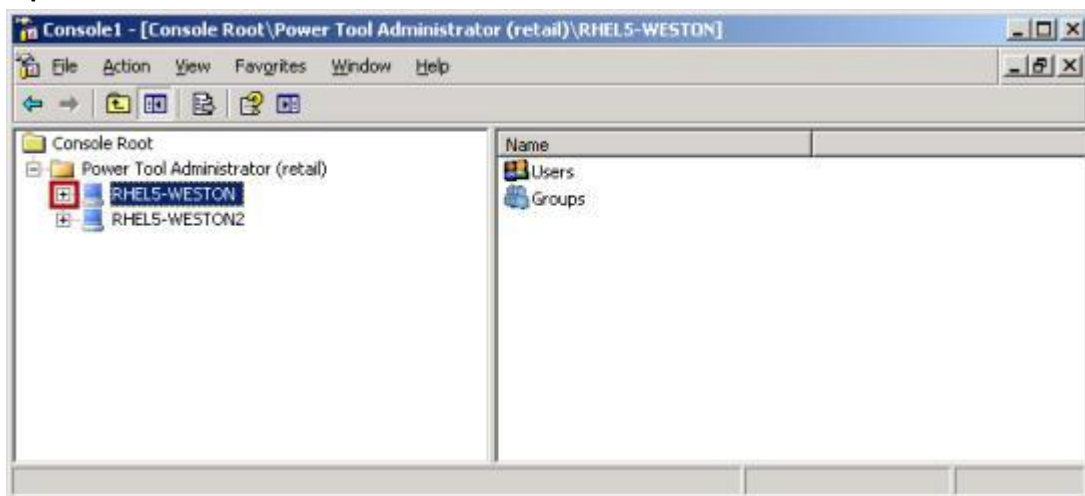
Scenario 7: Automating Tasks by Using Existing Information in Your Environment

This Lab demonstrates how to use Power Tool Administrator to automate tasks by using existing information in any of the systems that are added to Power Tool Administrator. With this feature in Power Tool Administrator, you can now perform and complete tasks in a matter of minutes.

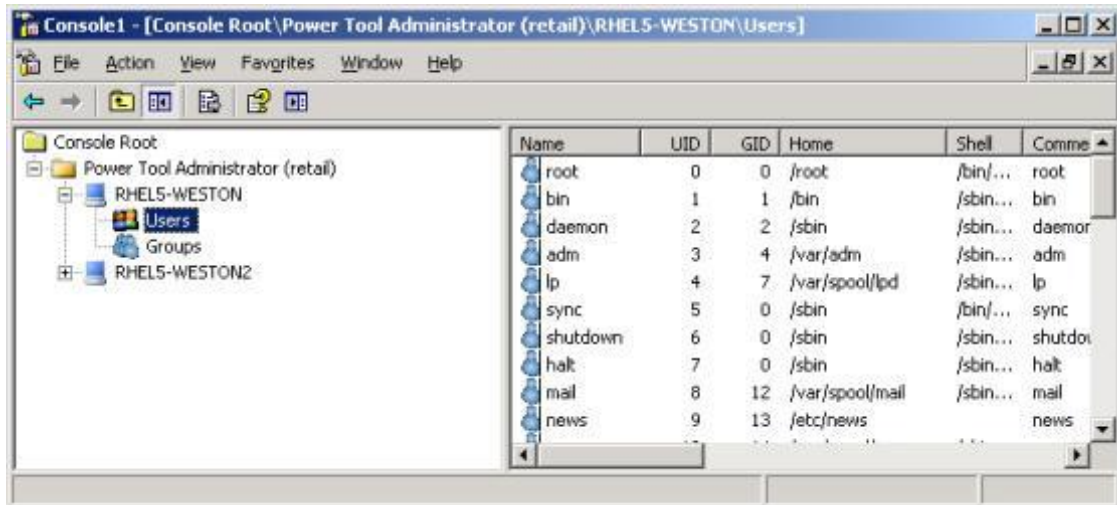
In this Lab, a Linux system named **RHEL5-WESTON** has a user named **operator2**. This Lab demonstrates how you can create the same user, **operator2**, in other systems by simply using the drag and drop feature in Power Tool Administrator.

You can create the same user in all other systems that are added to Power Tool Administrator by performing the following steps:

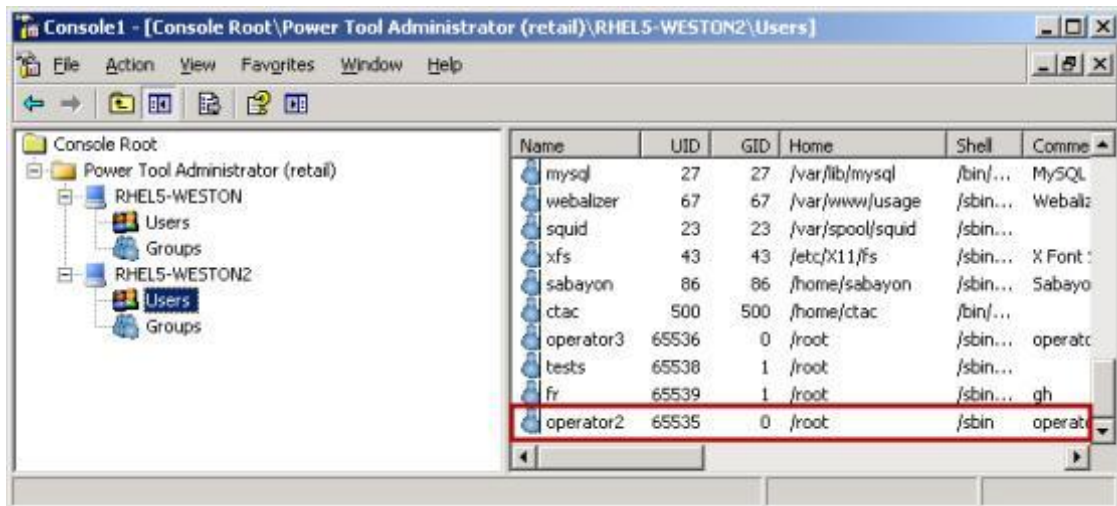
1. On the *Microsoft Management Control* window, under the *Power Tool Administrator* folder, click the **Expand** icon for the system where the user currently exists. For example, in this Lab, the user **Operator 2** exists on a Linux system named **RHEL5-WESTON** so you must click the **Expand** icon for **RHEL5-WESTON**.



2. Click **Users**.
The list of users that exist in this system appear.



3. Drag and drop the user that exists in the system to the Power Tool Administrator folder. For example, in this Lab, drag and drop **operator2** to the Power Tool Administrator folder. Power Tool Administrator creates the user in all the systems that are added to Power Tool Administrator.

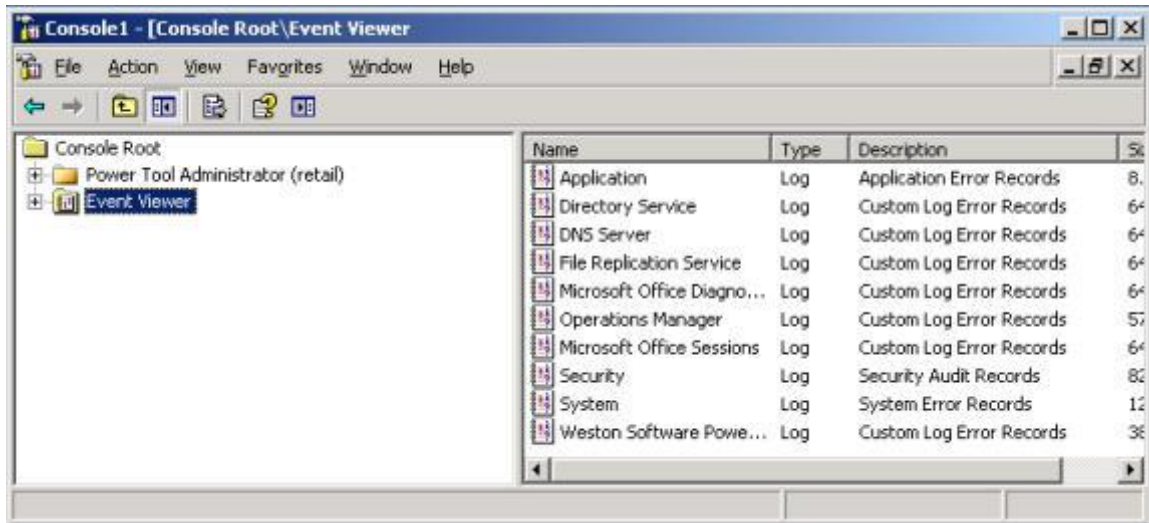


Scenario 8: Viewing Event Logs for Windows and Non-Windows Systems

This Lab demonstrates how to use Power Tool Administrator to view event logs for Windows and Non-Windows systems. With this feature in Power Tool Administrator, you can now view events that occur in various heterogeneous systems from one central location.

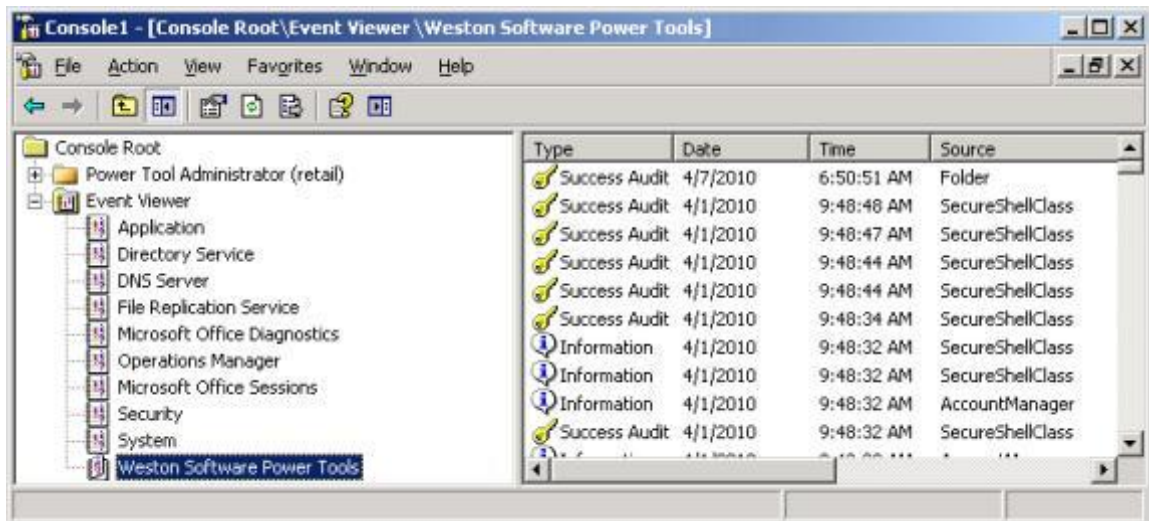
To view event information for a system, perform the following steps:

1. On the *Microsoft Management Control* window, click the **Expand** icon for the *Event Viewer*.

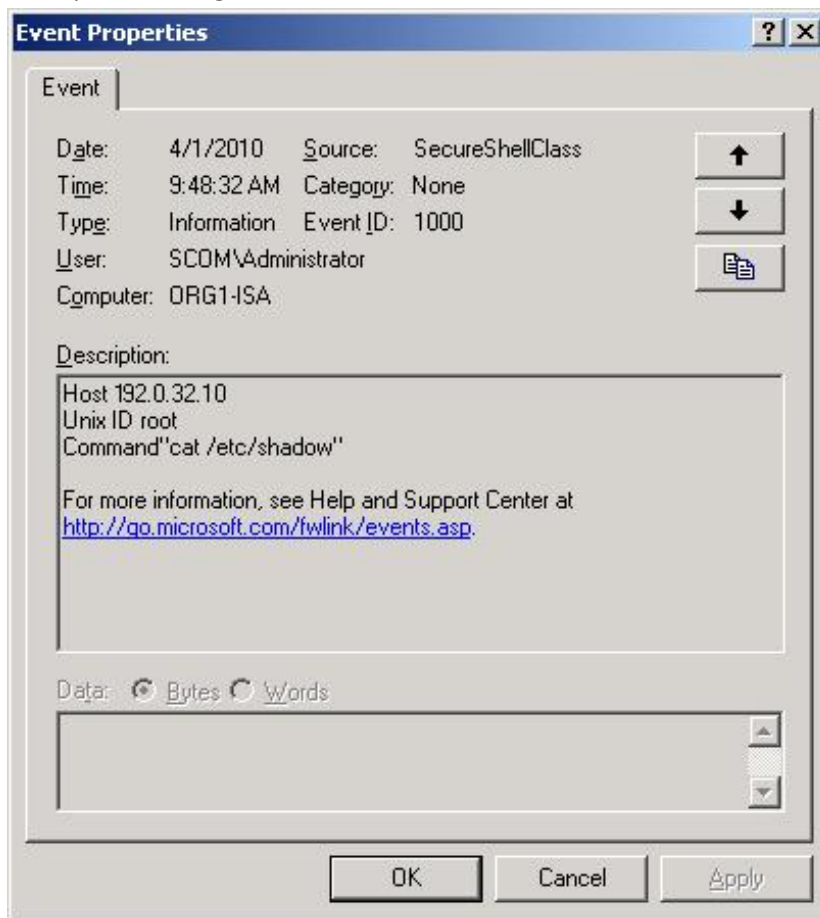


2. Click **Weston Software Power Tools**.

The right panel displays the events for Windows and non-Windows systems.



3. Double-click the event type for which you want to view more information.
The *Event Properties* dialog box appears with the event information. The image below illustrates a sample event log.



Appendix: The Interop Vendor Alliance

The Interop Vendor Alliance is an industry group working to identify and share opportunities to better connect people, data, and diverse systems through better interoperability with Microsoft systems and to jointly market the interoperability solutions of its members.

The organization serves as a collaborative forum for developing and sharing common technology models, facilitating scenario-based testing of multivendor solutions, and communicating additional best practices to customers and partners.

Since its formation in 2006, alliance membership has more than doubled as the IVA has developed multiple interoperability labs, including System Management, Centralized Directory, Federated Identity, Content Management, and Open XML.

You can learn more by visiting <http://interopvendoralliance.com/>.

The screenshot shows the homepage of the Interop Vendor Alliance website. At the top left is the logo for Interop Vendor Alliance, consisting of three colored circles (blue, green, orange) and the text "interop VENDOR ALLIANCE". To the right of the logo is a search bar with a "SEARCH" button and a "RSS 2.0" icon. Below the logo is a navigation menu with links for "HOME", "ABOUT", "EVENTS", "INTEROP LABS", and "MEMBER DIRECTORY". The main content area features a large banner with a photograph of three people (two men and one woman) in a professional setting. The banner text reads "Working Together Toward Interoperable Solutions" and "The Interop Vendor Alliance is a community of software and hardware vendors working together to enhance interoperability with Microsoft Systems. [More...](#)". To the right of the banner is a "News" section with a green grid icon, a title "News", and a news item: "Weston Software, Inc. announces support for Microsoft Windows 7_30/07/2009" with a "More News" link below it. At the bottom of the page are three dark grey boxes with icons and text: "Interop Labs" with a date "10/01/2007" and a link to "Federated Identity Lab"; "Member Solutions" with a date "31/03/2009" and a link to "Centrify Joins Microsoft..."; and "Upcoming Events" with the text "New events are coming, covering various topics. Stay tuned. [More Events](#)".

This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

Distributed under Creative Commons Attribution-Noncommercial-No Derivative Works 3.0

