DoIt4Me Manual

Name

DoIt4Me - a tool for automating administrative tasks on Windows NT networks.

Synopsis

DoIt4Me.pl <option>
Option: <1> Auditing
<2> Configure the Registry
<3> Check the status of ALL NT services
<4> Check the status of a subset NT services
<5> Change NT services status (Start/Stop)
<6> Reboot a subset of workstations
<7> Help

Examples

C:\>doit4me\DoIt4Me.pl 1
Scan a subset of computers for a Registry Auditing

C:\>doit4me\DoIt4Me.pl 6
Reboot a subset of workstations

Files

Pclist.cfg	Subset of computers
Regaudit.cfg	Subset of Registry values to Audit
Regconfig.cfg	Subset of Registry values to Configure
Serviceconfig.cfg	Subset of Services with the new status
Serviceaudit.cfg	Subset of Services to Audit
Reboot.cfg	Subset of computers to Reboot

Author

Alessandro Augusto, Célio Guimarães, Paulo Lício de Geus
University of Campinas - UNICAMP
Computing Institute IC
{alessandro.augusto, celio, paulo}@ic.unicamp.br

1. Overview

The process to secure a Windows NT computer is simple when the system administrator knows the required configuration settings. However, even with this knowledge, to apply the same configuration to hundreds of NT-based computers can be frustrating and laborious. Remote administration of a large Windows NT network is a complex task. The tools provided by standard NT installations are, at best, inadequate. The explosive growth in network sizes over the last years has resulted in large and complex sites but no significant new tools were created.

DoIt4Me is an automated and remote administrative tool for Microsoft Windows NT operating systems. It can manage small or large NT network from a single console. Infrequent trips to distant machines will only be necessary in case of hardware failures.

It is specifically aimed at administrating and securing Windows NT 4.0 machines, although some of the functionality could also be used on Windows 2000.

DoIt4Me can perform all the following options to a subset of computers:

- ? Perform remote Registry Auditing;
- ? Configure remote Registry;
- ? Perform services status auditing;
- ? Start or stop remote NT services;
- ? Reboot Workstations;
- ? Apply ACLs; (not disposable in this version yet)

2. Installation

By installing DoIt4Me on the domain controller (DC), the administrator can remotely control any subset of workstations served by the DC.

To install DoIt4Me, just copy "doit4me.exe" to a folder of the domain controller, for example "C:\DOIT4ME\".

3. Usage

DoIt4Me needs to be execute by the command shell/prompt (cmd.exe) of the Windows NT. The interface should looks like as:

```
C:\> DoIt4Me.pl
------------------------------------------------------------------------
DoIt4Me - Automate NT Administrative Tasks Remotely

Usage : DoIt4Me.pl <option>
Option:   <1> Auditing
          <2> Configure the Registry
          <3> Check the status of ALL NT services
          <4> Check the status of a subset NT services
          <5> Change NT services status (Start/Stop)
          <6> Reboot a subset of workstations
          <7> Help
------------------------------------------------------------------------
```

3.1 Option < 1 >: Auditing

The first feature of DoIt4Me, is the ability to scan any subset of network and to report the results for auditing.

In this phase, also called Data Collection, the administrator specifies which configuration settings he or she wants to audit. It is only necessary to specify the subset of machines that will be scanned and the subset of Registry keys that will be collected.

Configure the file *pclist.cfg* with the computer's name that will be scanned, and the file *regaudit.cfg* with the subset of Registry keys that will be analyzed. The format of this file should be one computer per line followed by ";" . Each Registry key has to be in in line. Table 1 shows an example of this files. In *Regaudit.cfg,* each Registry key should be followed by ";" and by the full path. Table 2 shows who to audit the keys *HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/ComputerName/ActiveComputerName/ComputerName* and *HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/Winlogon/DontDisplayLastUserName*

File: Pclist.cfg
Mustang; Porche; Ferrari

Table1: Example of pclist.cfg file configuration

File: regaudit.cfg
ComputerName;HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/ComputerName/ActiveComputerName DontDisplayLastUserName;HKEY_LOCAL_MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon

Table2: Example of regaudit.cfg file configuration

3.2 Option < 2 >: Registry Configuring

After the auditing, sometimes the system administrator needs to make some adjustments or configure some Registry values to make some computers compliance with the security policy.

The process is very similar to the Registry Auditing, the difference here is: in this option, besides the administrator specify the subset of computers and the subset of Registry keys, it is necessary to specify the new value that will receive this Registry key. The file that should be configured in this option is *regconf.cfg*.

Table 3 show an example of how to configure the value 0 to the DontDisplayLastUserName Registry key.

File: regconfig.cfg
DontDisplayLastUserName;HKEY_LOCAL_MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon; 0

Table3: Example of *regconfig.cfg* file configuration

3.3 Option < 3 >: Services Status Auditing

DoIt4Me facilitates the process to get the status of NT services of remote computers. In this option, the administrator will audit the status of ALL services from a subset of computers. The administrator needs just to configure the *pclist.cfg* file, specifying which computers he wants to collect the services status.

3.4 Option < 4 >: Some Services Status Auditing

This options differs from the last one by the subset of services that will be collect. In this option, the administrator is able to specify a subset of services that can be collect from a subset of computers.

To perform this option, the administrator needs to specify the subset of computers and the services. The *serviceaudit.cfg* file should be configured with the "name" of the services that will be collect.

File: serviceaudit.cfg
Alerter;
NetDDE;

Table4: Example of serviceaudit.cfg file configuration

3.5 Option < 5 >: Chance Service Status

It is also possible to change the status of any service. DoIt4Me permits the system administrator to start or stop any service in any subset of computers. Like the above configurations, it is only necessary to define the subset of computers (*pclist.cfg*), the subset of services and its news status, for example 1 to start or 0 to stop it.

The services and the values is configured on the file *serviceconfig.cfg*. Table 5 shows how to start the "alerter" service and how to stop the "NetDDE" service.

File: servicconfig.cfg
Alerter; 1
NetDDE; 0

Table5: Example of serviceconfig.cfg file configuration

3.6 Option < 6 >: Reboot

This option permits the system administrator to reboot any subset of computer. To reboot a subset of computers, it is only necessary to configure the file *reboot.cfg* with the name of each computer (to be reboot) per line, similar as the configuration of the file *pclist.cfg* in table 1.