

# Auditing Addition, Removal or Changes to Print Queues on a Windows Print Server

by Pete Zerger, MCSE (Messaging)

<http://www.it-jedi.net>  
[pete.zerger@gmail.com](mailto:pete.zerger@gmail.com)

updated April 2006

## Table of Contents

Auditing Addition, Removal or Changes to Print Queues on a Windows Print Server.....	1
Introduction .....	2
Creating the Event Rule.....	2
Verifying Rule Functionality .....	4
Feedback .....	4

## Tables and Figures

Table 1 - Printer Creation Event Rule Properties .....	2
Table 2 - Printer Deletion Event Rule Properties .....	3
Table 3 - Print Driver Update Event Rule Properties.....	3
Table 4 - Printer Port Change Event Rule Properties .....	4

## Introduction

While the Microsoft Windows Print Server Management Pack provides rules to validate print queue, printer and spooler health, it does not address other changes to print servers, such as the addition and removal of shared printers, or the change or update to printer ports or print drivers. These events can all lead to service interruptions, especially in the cases such as the update of a print driver on a Windows Terminal Server or Citrix Server, or deletion of a shared office printer.

The following rules, when created, will be triggered based on events written to the System Event Log during the following events targeted for audit: Printer creation and deletion, print driver updates, and changes printer port definition.

While the printer creation process will generate some duplicate alerts (because it triggers the driver and port update rules), this rule set does effectively augment the existing functionality of the Print Server Management Pack.

## Creating the Event Rule

To create the custom print server audit rules, perform the following steps:

1. In the MOM Administrator Console, create a custom rule group.
2. On the Computer Groups tab, add the Microsoft Windows Print Servers group.
3. Right click Event Rules, and in the **Select Event Rule Type** dialogue, select Alert On or Respond To Event.
4. Set the event parameters in the rule creation wizard as defined in the following tables:

*NOTE: Advanced Criteria substrings are case sensitive!*

**Table 1 - Printer Creation Event Rule Properties**

Tab	Property	Value
General	Name	Detect Printer Creation
Data Provider	System	Windows NT Event Log
Criteria	From Source	Print
Criteria	Type	Information
Criteria	Event ID	36
Advanced Criteria	Description matches substring	successfully created
Alert	Generate alert	Checked
Alert	Alert severity	Warning

**Table 2 - Printer Deletion Event Rule Properties**

<b>Tab</b>	<b>Property</b>	<b>Value</b>
General	Name	Detect Printer Deletion
Data Provider	System	Windows NT Event Log
Criteria	From Source	Print
Criteria	Type	Warning
Criteria	Event ID	3
Advanced Criteria	Description matches substring	was deleted
Alert	Generate alert	Checked
Alert	Alert severity	Warning

**Table 3 - Print Driver Update Event Rule Properties**

<b>Tab</b>	<b>Property</b>	<b>Value</b>
General	Name	Detect Print Driver Update
Data Provider	System	Windows NT Event Log
Criteria	From Source	Print
Criteria	Type	Warning
Criteria	Event ID	20
Advanced Criteria	Description matches substring	Printer Driver
Alert	Generate alert	Checked
Alert	Alert severity	Warning

**Table 4 - Printer Port Change Event Rule Properties**

Tab	Property	Value
General	Name	Detect Printer Port Update
Data Provider	System	Windows NT Event Log
Criteria	From Source	Print
Criteria	Type	Information
Criteria	Event ID	9
Advanced Criteria	Description matches substring	was set
Alert	Generate alert	Checked
Alert	Alert severity	Warning

5. Be sure to right click the Management Packs node in the console and select Commit Change when complete!

### ***Verifying Rule Functionality***

1. On the MOM Management Server, Printers applet, select Add Printer
2. Run the wizard, adding a Generic Text printer, accepting the defaults throughout the wizard.
3. In the MOM Operator Console, verify the Detect Printer Creation rule fired successfully.
4. Repeat step 2, selecting default. This will update the print driver causing the Detect Print Driver Update rule to fire. Verify a Warning Alert was generated in the Operator Console for this rule.
5. Right click either printer and select Properties
6. On the Ports tab, select a different printer port. Verify a Warning Alert was generated in the Operator Console
7. Finally, delete either printer, verifying after deletion that a Warning Alert was generated for the deletion event.

### ***Feedback***

I hope you find this guide helpful. Please direct question, comments and errata to [pete.zerger@gmail.com](mailto:pete.zerger@gmail.com)