

Active Directory Printer logs

The presentation shows a successful print to an Active Directory Printer. The presentation retrieves the successful print log event from the Print Server Event Viewer. The presentation shows an unsuccessful print to an Active Directory Printer. The presentation retrieves the unsuccessful print log event from the local computer.

Preuss

10/22/2014



preuss@dragon.example.org

Password



The presentation logs on to the dragon.example.org domain. The Windows 7 computer is a member computer of the domain.





Recycle Bin

Mozilla
Firefox

Dragon Web

Hardware and Sound > Devices and Printers

Search Devices and Printers

Add a device Add a printer

Devices (4)

- Generic Non-PnP Monitor
- VMware Virtual USB Mouse
- VMware, VMware Virtual S SCSI Disk Device
- WIN7-AL

Printers and Faxes (3)

- Fax
- Microsoft XPS Document Writer
- Black Magic on PERU

7 items

The printer is successfully added for this account on Windows 7. The printer is available to installed printing application programs in Windows 7.

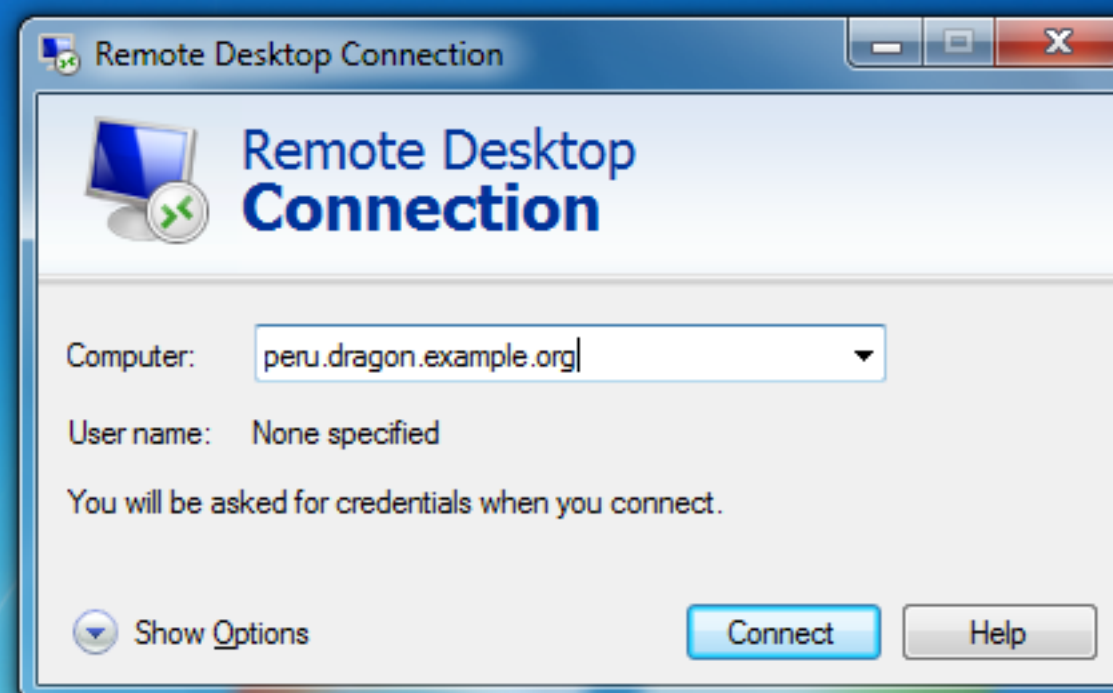
The presentation opens a program and sends a print job to the Active Directory printer.



Recycle Bin

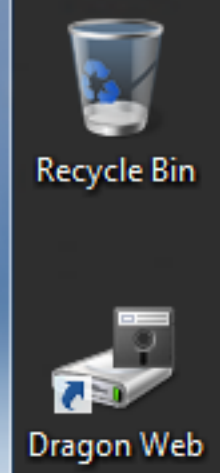
Mozilla
Firefox

Dragon Web



The presentation uses Remote Desktop Connection to log on to the server. The server must be the server hosting the printer.

The presentation uses an administration account. The account must be a member of the OU administration group.



Server Manager

Local Server

- Dashboard
- Local Server**
- All Servers
- File and Storage Services
- IIS
- Print Services
- Remote Desktop Services
- WSUS

PROPERTIES

Operating system version: Microsoft Windows Server 2012 R2 Datacenter
Hardware information: VMware, Inc. VMware Virtual Platform

IPv6 enabled

TASKS

The presentation opens the Server Manager. The presentation selects the Local Server option.

Windows Server 2012 R2

Print Management

File Action View Help

- Print Management
 - Custom Filters
 - Print Servers
 - peru (local)
 - Drivers
 - Form Servers
 - Ports
 - Printers
 - Deployed P...

Printer Name	Queue Status	Jobs In ...	Server Name	Driver Name	Actions
Microsoft XPS Document Write...	Ready	0	peru (local)	Remote Des	Printers
Microsoft XPS Document Writer	Ready	0	peru (local)	Microsoft XI	More Actions

Advanced Security Settings for Black Magic

Owner: SYSTEM [Change](#)

Permissions Effective Access

Effective Access allows you to view the effective permissions for a user, group, or device account. In addition to viewing the effective permissions for a user, group, or device account, you can also evaluate the impact of potential additions to the security token for the account. For example, if you are adding a group, any group that the intended group is a member of must be added separately.

User/ Group: preuss (preuss@dragon.example.org) [Select a user](#)

View effective access

Effective access	Permission	Access limited by
	Print	
	Manage this printer	
	Read permissions	
	Change permissions	
	Take ownership	

The presentation opens the Print Management section from the Server Manager. The presentation opens the printer properties. The presentation opens the security tab of the printer. The presentation checks the effective settings for a logon.

This logon may use the printer.



Recycle Bin

Server Manager

Server Manager ▸ Local Server

Manage Tools View Help

- Dashboard
- Local Server**
- All Servers
- File and Storage Services ▸
- Remote Desktop Services ▸

PROPERTIES For Chile

Computer name	Chile
Domain	mait.example.org
Windows Firewall	Domain: On, Public: On
Remote management	Enabled
Remote Desktop	
NIC Teaming	
Ethernet 3	
Ethernet 4	
Operating System	Windows Server 2012 R2
Hardware	Standard

- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Module for Windows PowerShell
- Active Directory Sites and Services
- Active Directory Users and Computers
- ADSI Edit
- Component Services
- Computer Management
- Defragment and Optimize Drives
- DNS
- Event Viewer
- Group Policy Management
- iSCSI Initiator
- Local Security Policy
- Microsoft Azure Services
- ODBC Data Sources (32-bit)
- ODBC Data Sources (64-bit)
- Performance Monitor
- Resource Monitor
- Security Configuration Wizard
- Services
- System Configuration
- System Information
- Task Scheduler
- Terminal Services

The presentation opens the Event Viewer on the server.



Recycle Bin

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
- Applications and Services Logs
- Subscriptions

Event Viewer (Local)

Overview and Summary Last refreshed: 10/23/2014 4:40:49 PM

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours
Critical	-	-	-	0	0

Created

Enabled Retention

Enabled Overwrite

Enabled Overwrite

Actions

- Event Viewer (Local)
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Connect to Another C...
- View
- Refresh
- Help

The presentation opens the Event Viewer.

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
- Applications and Services Logs
 - Hardware Events
 - Internet Explorer
 - Key Management Services
 - Microsoft
 - Windows
 - All-User-Installed Applications
 - AppHost
 - AppID
 - ApplicabilityErrors
 - Application Security
 - Application Execution Events
 - Application Repackaging
 - AppLocker
 - AppModel Runtime
 - AppReadiness
 - Apps
 - Apps-API
 - AppXDeployment
 - AppXDeployment
 - AppXPackaging
 - ASN1
 - ATAPort
 - Audio

Overview and Summary Last refreshed: 10/22/2014 8:53:59 PM

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events log contains events, regardless of source. An

Last hour 24 hour

0

Log Name	Size (Current)	Modified	Enabled	Retention
Application	3.07 MB/2...	10/16/2014 8:48:16 AM	Enabled	Overv

Actions

Event Viewer (Local)

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Connect to Another Computer...
- View
- Refresh
- Help

The presentation opens the Applications and Services | Microsoft | Windows log section.

The screenshot shows the Windows Event Viewer application. The left-hand tree view is expanded to 'PrintService | Operational'. A yellow callout box with a white arrow points to this selection, containing the text: 'The presentation opens the PrintService | Operational log.' The main pane displays a list of events for the 'Operational' log, with the following data:

Level	Date and Time	Source	Event ID	Task Cat...
Error	10/22/2014 8:53:22 PM	PrintSer...	603	Client-si...
Error	10/22/2014 8:53:22 PM	PrintSer...	603	Client-si...
Information	10/22/2014 8:53:00 PM	PrintSer...	300	Adding ...
Information	10/22/2014 8:52:57 PM	PrintSer...	300	Adding ...
Information	10/22/2014 8:52:57 PM	PrintSer...	300	Adding ...

The 'Event 603, PrintService' details pane is open, showing the 'General' tab. The description reads: '...tion because it could not read the ... 13400074-3126433249-2230376872- ... n the registry key. This can occur if t ... became unavailable.' The 'Details' tab shows the following information:

- Time: 10/22/2014 8:53:22 PM
- Category: Client-side rendering
- Source: Client Side Rendering (CSR),C
- Source GUID: peru.dragon.example.org

The 'Actions' pane on the right shows various options for the selected event, including 'Open Saved Log...', 'Create Custom View...', 'Filter Current Log...', 'Properties', 'Disable Log', 'Find...', 'Save All Events As...', 'Attach a Task To this Lo...', 'View', 'Refresh', 'Help', 'Event Properties', 'Attach Task To This Eve...', 'Copy', and 'Save Selected Events...'.

Event Viewer

File Action View Help

Operational Number of events: 567

Event Properties - Event 801, PrintService

General Details

Printing job 3.

Log Name: Microsoft-Windows-PrintService/Operational
Source: PrintService
Event ID: 801
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 10/8/2014 7:18:59 PM
Task Category: Print job diagnostics
Keywords: WDI Diag
Computer: peru.dragon.example.org

Copy Close

This is a general view of printing success.

Windows Server 2012 R2

Event Viewer

File Action View Help

Operational Number of events: 567

Event Properties - Event 801, PrintService

General Details

Friendly View XML View

```
- <Event
  xmlns="http://schemas.microsoft.com/win/2004/08/events/event"
  - <System>
    <Provider Name="Microsoft-Windows-PrintService"
      Guid="{747EF6FD-E535-4D16-B510-42C90F6873A1}" />
    <EventID>801</EventID>
    <Version>0</Version>
    <Level>4</Level>
    <Task>43</Task>
    <Opcode>0</Opcode>
    <Keywords>0x4004000000000000</Keywords>
    <TimeCreated SystemTime="2014-10-22T18:50:07.4000000-07:00" />
```

Copy Close

Windows Server 2012 R2

8:55 PM 10/22/2014

This is the XML of printing success.

Print Management

File Action View Help

Print Management

- Custom Filters
- Print Servers
 - peru (local)
 - Drivers
 - Forms
 - Ports
 - Printers
- Deployed Printers

Printer Name	Queue Status	Jobs In ...	Server Name	Driver Name	Actions
Microsoft XPS Document Write...	Ready	0	peru (local)	Remote De	Printers
Microsoft XPS Document Writer	Ready	0	peru (local)	Microsoft	More Actions
Fax (redirected 2)	Ready	0	peru (local)	Remote De	Black Magic
Black Magic on PERU (redirecte...	Ready	0	peru (local)	Remote De	More Actions
Black M	Off	?	peru (local)	HP M	

Black Magic Properties

General | Sharing | Ports | Advanced | Color Management

Security | Device Settings | About

Group or user names:

- People (DRAGON\peopleZenon)
- Melvin Lee Campbell (Melvin_Lee_Campbell@dc=dragon.example.org)
- T Preuss (tpreuss@dragon.example.org)
- print (DRAGON\printzenon)
- Katherine A Carlisle (Katherine_A_Carlisle@dragon.example.org)
- James Carlson (James_Carlson@dragon.example.org)
- no-print (DRAGON\no-print)**

Add... Remove

Permissions for no-print	Allow	Deny
Print	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Manage this printer	<input type="checkbox"/>	<input type="checkbox"/>
Manage documents	<input type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Advanced

OK Cancel Apply

The presentation creates a group named no-print. The members of the group may not print to the Active Directory printer.

The screenshot shows the Windows Print Management console. A table lists two printers: 'Microsoft XPS Document Writer' and 'Microsoft XPS Document Write...'. An 'Advanced Security Settings for Black Magic' dialog box is open, showing the 'Effective Access' tab. A yellow callout box with an arrow points to the 'Effective Access' tab, containing the text: 'The presentation checks the effective access to the printer for a member of no-print.' Below the callout, a table shows the effective access for the user 'Alphonse Albatross (aalbatross@dragon.example.org)'. All permissions are marked with a red 'X', indicating they are denied.

Printer Name	Queue Status	Jobs In ...	Server Name	Driver Name
Microsoft XPS Document Write...	Ready	0	peru (local)	Remote De
Microsoft XPS Document Writer	Ready	0	peru (local)	Microsoft

Effective access	Permission	Access limited by
×	Print	Object permissions
×	Manage this printer	Object permissions
×	Read permissions	Object permissions
×	Change permissions	Object permissions
×	Take ownership	Object permissions

The presentation checks the effective access to the printer for a member of no-print.



aalbatross@dragon.example.org

Password



Log on to dragon.example.org
or to another domain?

ch User

The presentation logs on the domain. The account is an account without printing permission on the Active Directory printer.





Control Panel > Hardware and Sound > Devices and Printers

Search Devices and Printers

Add a device Add a printer

Devices (4)

- Virtual se
- VMware, VMware Virtual S SCSI Disk Device
- WIN7-AL
- Fax
- Microsoft XPS Document Writer

6 items

The presentation selects Add a printer in the Devices and Printers section.



Control Panel > Hardware and Sound > Devices and Printers

Search Devices and Printers

Add a device

Device

Printers

Generic Monitor

Add Printer

What type of printer do you want to install?

- ➔ Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)
- ➔ Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

Next Cancel

The presentation selects Add a network, wireless or Bluetooth printer. The presentation selects Next.



Control Panel > Hardware and Sound > Devices and Printers

Search Devices and Printers

Add a device

Devices

Printers

Generic Monitor

Add Printer

Select a printer

Printer Name	Address
Black Magic on PERU	Bridges 165/166

Search again

Printer that I want isn't listed

Next Cancel

The presentation selects the appropriate printer. The presentation selects Next.



Control Panel > Hardware and Sound > Devices and Printers

Search Devices and Printers

Add a device

Devices

Printers

Generic Monitor

Black Magic V

Next Cancel

Connect to PERU

Connecting to PERU

User name: aalbatross@dragon.examj

Password:

Remember my password

OK Cancel

The presentation enters the same logon name and password from initial domain logon.



Control Panel > Hardware and Sound > Devices and Printers

Search Devices and Printers

Add a device

Devices

Printers

Generic Monitor

Black Mag

Search again

Next Cancel

Connect to Printer

The credentials supplied are not sufficient to access this printer. Do you want to specify new credentials?

Yes No

The credentials entered by the presentation do not have permission to logon or print.

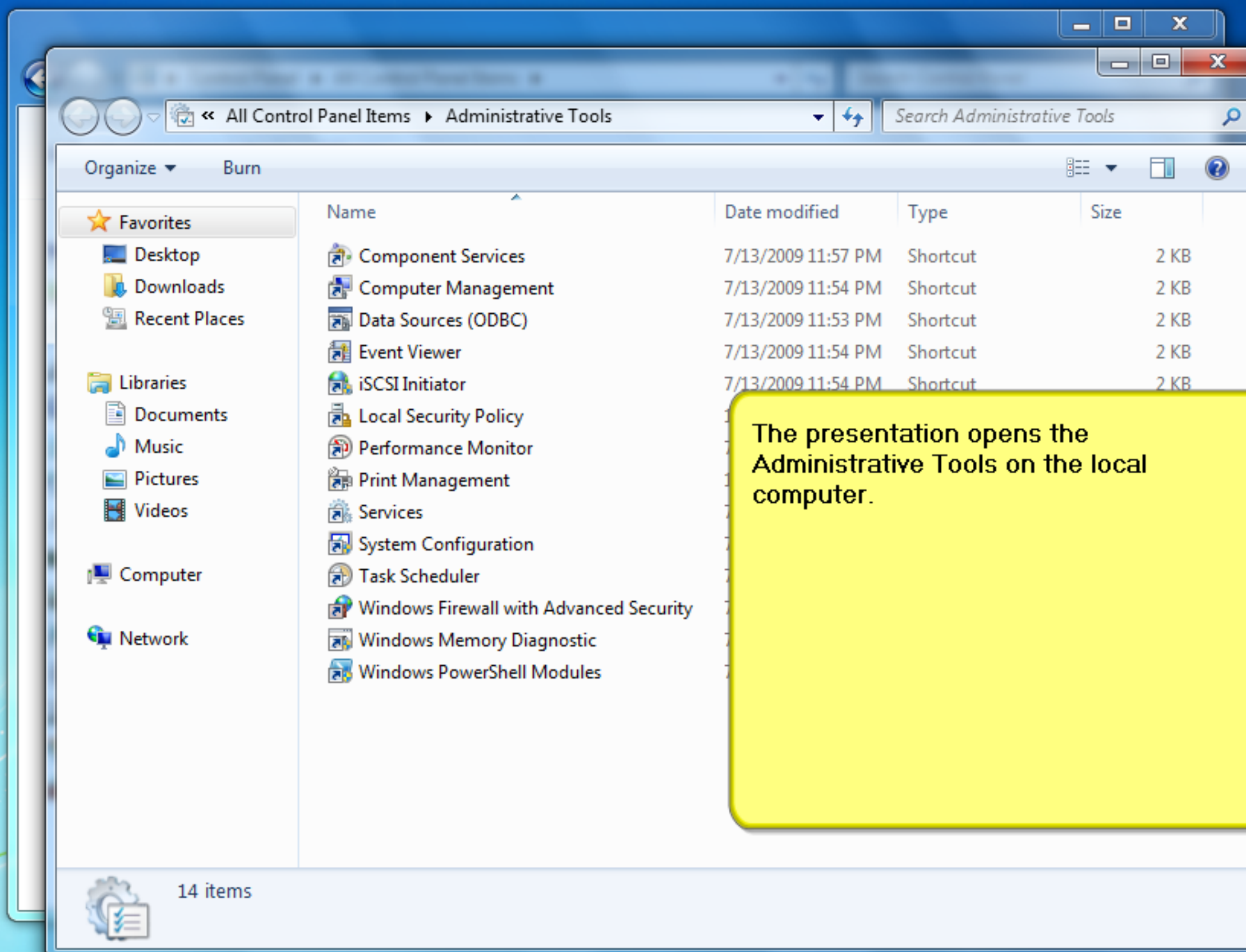
The local computer Event Viewer will have a record of this event. The event is a security event showing logon not allowed.



Recycle Bin

Mozilla
Firefox

Dragon Web



The screenshot shows a Windows 7 desktop with a blue background. On the desktop are icons for Recycle Bin, Mozilla Firefox, and Dragon Web. A window titled "Administrative Tools" is open, displaying a list of system utilities. The window's address bar shows "All Control Panel Items > Administrative Tools" and a search box labeled "Search Administrative Tools". The left sidebar shows "Favorites" (Desktop, Downloads, Recent Places), "Libraries" (Documents, Music, Pictures, Videos), "Computer", and "Network". The main pane shows a list of 14 items, each with a name, date modified, type, and size. A yellow callout box is overlaid on the right side of the window, containing text.

Name	Date modified	Type	Size
Component Services	7/13/2009 11:57 PM	Shortcut	2 KB
Computer Management	7/13/2009 11:54 PM	Shortcut	2 KB
Data Sources (ODBC)	7/13/2009 11:53 PM	Shortcut	2 KB
Event Viewer	7/13/2009 11:54 PM	Shortcut	2 KB
iSCSI Initiator	7/13/2009 11:54 PM	Shortcut	2 KB
Local Security Policy			
Performance Monitor			
Print Management			
Services			
System Configuration			
Task Scheduler			
Windows Firewall with Advanced Security			
Windows Memory Diagnostic			
Windows PowerShell Modules			

14 items

The presentation opens the Administrative Tools on the local computer.





Administrative Tools window

Search Administrative Tools

Name	Date modified	Type	Size
Component Services	7/13/2009 11:57 PM	Shortcut	2 KB
Computer Management	7/13/2009 11:54 PM	Shortcut	2 KB
Data Sources (ODBC)	7/13/2009 11:53 PM	Shortcut	2 KB
Event Viewer	7/13/2009 11:54 PM	Shortcut	2 KB
...

Context menu for Event Viewer:

- Open
- Open file location
- Author
- Run as administrator
- Scan with Microsoft Security Ess...
- Open with...
- Pin to Taskbar
- Pin to Start Menu
- Restore previous versions
- Send to
- Cut
- Copy
- Create shortcut
- Delete
- Rename
- Properties

Event Viewer Shortcut

The presentation opens the Event Viewer by using the Run as administrator option.



Administrative Tools window showing a list of items. A User Account Control dialog is overlaid on top.

User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Microsoft Management Console
Verified publisher: **Microsoft Windows**
File origin: Hard drive on this computer

To continue, type an administrator password, and then click Yes.

tpreuss@dragon.example.org
Password
Domain: dragon.example.org

Show details Yes No

The presentation enters the logon credentials for a member of the administration group on the local computer.

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security**
 - Setup
 - System
 - Forwarded Events
- Applications and Services Logs
- Subscriptions

Security Number of events: 10,833

Keywords	Date and Time	Source	Event ID	Task Category
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4634	Logoff
		Microsoft Windo...	4672	Special Logon
		Microsoft Windo...	4624	Logon
		Microsoft Windo...	4624	Logon
		Microsoft Windo...	4648	Logon
		Microsoft Windo...	4625	Logon
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4648	Logon
		Microsoft Windo...	4673	Sensitive Privileg...
		Microsoft Windo...	4673	Sensitive Privileg...

Audit Failure 10/22/2014 9:01:02 PM

Audit Success 10/22/2014 9:00:26 PM

Audit Failure 10/22/2014 8:59:28 PM

Audit Failure 10/22/2014 8:59:28 PM

Event 4673, Microsoft Windows security auditing.

General Details

A privileged service was called.

Subject:

Log Name: Security

Source: Microsoft Windows security

Event ID: 4673

Level: Information

User: N/A

Logged: 10/22/2014 9:02:41 PM

Task Category: Sensitive Privilege Use

Keywords: Audit Success

Computer: win7-al.dragon.example.org

Actions

Security

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 4673, Microsoft Windows ...

- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

The presentation opens the Security log listing.

Event Viewer

File Action View Help

Event Viewer (Local) Security Number of events: 10,833

Keywords	Date and Time	Source	Event ID	Task Category
				ensitive Privileg...
				ensitive Privileg...
				ensitive Privileg...
				ensitive Privileg...
				goff
				pecial Logon
				gon
				gon
				gon
				gon
				ensitive Privileg...
				ensitive Privileg...
				ensitive Privileg...

Event Properties - Event 4648, Microsoft Windows security auditing.

General Details

A logon was attempted using explicit credentials.

Subject:

Security ID:	DRAGON\aalbatrosszenon
Account Name:	aalbatrosszenon
Account Domain:	DRAGON
Logon ID:	0xa53f2

Log Name: Security

Source: Microsoft Windows security

Event ID: 4648

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 10/22/2014 9:00:26 PM

Task Category: Logon

Keywords: Audit Success

Computer: win7-al.dragon.example.org

Copy Close

The presentation find the log entry showing the client beginning the logon process. The next entry is the interesting entry.

The presentation found this entry by correlating the time of printer installation.

Event Viewer

File Action View Help

Event Viewer (Local) Security Number of events: 10,833

Keywords	Date and Time	Source	Event ID	Task Category
				Sensitive Privileg...
				Sensitive Privileg...
				Sensitive Privileg...
				Sensitive Privileg...
				goff
				Special Logon
				gon
				gon
				gon
				gon
				Sensitive Privileg...
				Sensitive Privileg...
				Sensitive Privileg...

Event Properties - Event 4673, Microsoft Windows security auditing.

General Details

A privileged service was called.

Subject:

Security ID:	DRAGON\aalbatrosszenon
Account Name:	aalbatrosszenon
Account Domain:	DRAGON
Logon ID:	0xa53f2

Log Name: Security

Source: Microsoft Windows security

Event ID: 4673

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 10/22/2014 9:01:02 PM

Task Category: Sensitive Privilege Use

Keywords: Audit Failure

Computer: win7-al.dragon.example.org

Copy Close

This is the log entry showing logon failure during the printer installation.

A privileged service was called.

Subject:

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4673
Level:	Information
User:	N/A

Logged: 10/22/2014 9:01:02 PM

Task Category: Sensitive Privilege Use

Keywords: Audit Failure

Computer: win7-al.dragon.example.org

Event Viewer

File Action View Help

Event Viewer (Local) Security Number of events: 10,833

Keywords Date and Time Source Event ID Task Category

Event Properties - Event 4673, Microsoft Windows security auditing.

General Details

Friendly View XML View

```

- <Event
  xmlns="http://schemas.microsoft.com/win/2004/08/events/event"
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing"
    Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
  <EventID>4673</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>13056</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8010000000000000</Keywords>
  <TimeCreated SystemTime="2014-10-22T21:02:13.1660000Z" />

```

Copy Close

Actions

Security

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh

A privileged service was called.

Subject:

Log Name:	Security	Logged:	10/22/2014 9:01:02 PM
Source:	Microsoft Windows security	Task Category:	Sensitive Privilege Use
Event ID:	4673	Keywords:	Audit Failure
Level:	Information	Computer:	win7-al.dragon.example.org
User:	N/A		

This is the XML view of the log entry showing logon failure. Since the account could not logon, the account could not print.