



LOGbinder for SharePoint —Impact of Restrict Lookups

Introduction

LOGbinder for SharePoint by default makes every effort to fully translate and enrich SharePoint audit events through so called "lookups" where-in LOGbinder makes extra queries to SharePoint to obtain this information. But there is a cost/benefit relationship to be considered. Some events in the native SharePoint audit log include fields that are of low or no value to end users at many organizations. Each field in the native log, including these low or no value fields, requires a lookup by LOGbinder to resolve the native SharePoint data in to user friendly data.

For example, below is a sample of LOGbinder for SharePoint event ID 13:

Document checked in
Occurred: 6/25/2016 1:13:04 PM
Site: http://sp2010-sp
User: Administrator
Object
URL: Shared Documents/FinancialData.xlsx
Title: n/a
Version: 1.0

As you can see in the above event, the "Title" field returned from SharePoint is "n/a". This is obviously of no value to the end user. Since SharePoint includes these low/no value fields, LOGbinder for SharePoint includes an option to intelligently restrict the number of lookups it processes resulting in increased performance of LOGbinder. You can manage the amount of SharePoint lookups by opening the LOGbinder Control Panel selecting File and then Options. The amount of lookups performed by LOGbinder can be customized by choosing a value under "Amount of SharePoint lookups." See figure 1 below.

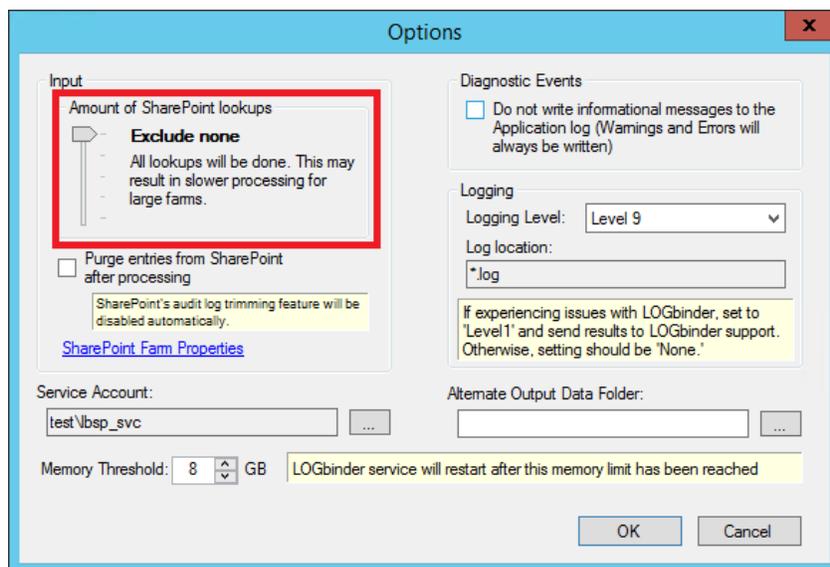


Figure 1: Managing the amount of SharePoint lookups

The fields that are affected (with the exception of the "Restrict all lookups option") are all child fields of the targeted object. "URL" is the most important field included in the events and that field is always reported except on some permission change events and only if the "Exclude high/medium-cost" option is selected.

Most organizations who need to speed up LOGbinder can safely use the "Exclude high-cost lookups" option without losing significant audit information. Please note that the "Exclude high/medium-cost" option does adversely impact permission change events.



LOGbinder for SharePoint —Impact of Restrict Lookups

The following chart outlines which fields are affected depending on which option is selected when managing the amount of SharePoint lookups.

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
10 Noise entry					
This entry was generated, but contains only data that is misleading or irrelevant.					
Occurred: %1					
Details: %2					
11 Site collection audit policy changed					
Occurred: %1					
Site: %2					
User: %3					x
New audit policy: %4					
12 Audit policy changed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
Subtype: %5		x ¹	x	x	x
URL: %6					
Title: %7		x ¹	x	x	x
Description: %8		x ¹	x	x	x
New audit policy: %9					
13 Document checked in					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Title: %5			x	x	x
Version: %6					
14 Document checked out					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Title: %5			x	x	x
Version: %6					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
15 Child object deleted					
Occurred: %1					
Site: %2					
User: %3					x
Parent Object					
Type: %4					
Subtype: %5		x ¹	x	x	x
URL: %6					
Title: %7		x ¹	x	x	x
Child Object					
Type: %8					
URL: %9					
16 Child object moved					
Occurred: %1					
Site: %2					
User: %3					x
Parent Object					
Type: %4					
Subtype: %5		x ¹	x	x	x
URL: %6					
Title: %7		x ¹	x	x	x
Description: %8		x ¹	x	x	x
Child Object					
Type: %9				x	x
Title: %10				x	x
Original location: %11					
New location: %12					
17 Object copied					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
Title: %5		x ¹	x	x	x
Description: %6		x ¹	x	x	x
Original location: %7					
New location: %8					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
18 Custom event					
Occurred: %1					
Site: %2					
User: %3					x
Details: %4					
Examine the details accompanying the event for more information.					
19 Object deleted					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Versions deleted: %6					
Recycled: %7					
20 SharePoint audit logs deleted					
Occurred: %1					
Site: %2					
User: %3					x
Logs deleted: %4					
Last date: %5					
Audit logs created before this date have been removed from SharePoint.					
Purge performed by LOGbinder: %6					
21 Object moved					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
Title: %5		x ¹	x	x	x
Original location: %6					
New location: %7					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
22 Object profile changed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
Subtype: %5		x ¹	x	x	x
URL: %6					
Title: %7		x ¹	x	x	x
Description: %8		x ¹	x	x	x
Profile details: %9					
23 SharePoint object structure changed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
Subtype: %5		x ¹	x	x	x
URL: %6					
Title: %7		x ¹	x	x	x
Description: %8		x ¹	x	x	x
Details: %9					
24 Search performed					
Occurred: %1					
Site: %2					
User: %3					x
Search: %4					
25 SharePoint group created					
Occurred: %1					
Site: %2					
User: %3					x
Group					
ID: %4					
Name: %5					
Initial members: %6					x

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
26 SharePoint group deleted					
Occurred: %1					
Site: %2					
User: %3					x
Group					
ID: %4					
The group name is not available because Microsoft does not report this. Refer to events 25, 27, 28, as these may contain the group name.					
27 SharePoint group member added					
Occurred: %1					
Site: %2					
User: %3					x
Group					
ID: %4					
Name: %5					x
Member					
ID: %6					
Name: %7					x ²
28 SharePoint group member removed					
Occurred: %1					
Site: %2					
User: %3					x
Group					
ID: %4					
Name: %5					x
Member					
ID: %6					
Name: %7					x ²
29 Unique permissions created					
Occurred: %1					
Site: %2					
User: %3					x
Parent Object					
Type: %4				x	x
Subtype: %5				x	x
URL: %6				x	x
Title: %7				x	x
Description: %8				x	x
Object					
URL: %9					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
This object no longer inherits permissions from the parent.					
30 Unique permissions removed					
Occurred: %1					
Site: %2					
User: %3					x
Parent Object					
Type: %4				x	x
Subtype: %5				x	x
URL: %6				x	x
Title: %7				x	x
Description: %8				x	x
Object					
URL: %9					
This object, which formerly had unique permissions, now inherits permissions from the parent.					
31 Permissions updated					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4				x	x
Subtype: %5				x	x
URL: %6				x	x
Title: %7				x	x
Description: %8				x	x
Target					
Name: %9					x
Type: %10					x
Permissions					
Role name: %11					x
Role description: %12					x
One instance of this event is logged for each role assigned this user. Look at adjacent events to determine all roles assigned to the user or group.					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
32 Permissions removed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4				x	x
Subtype: %5				x	x
URL: %6				x	x
Title: %7				x	x
Description: %8				x	x
Target					
Name: %9					x
Type: %10					x
Permissions					
Role name: %11					x
Role description: %12					x
33 Unique permission levels created					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Title: %6		x ¹	x	x	x
Description: %7		x ¹	x	x	x
This object has unique permission levels (role definitions) that are not inherited from its parent.					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
34 Permission level created					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Title: %6		x ¹	x	x	x
Description: %7		x ¹	x	x	x
Permission Level Details					
ID: %8					
Name: %9					
Type: %10					x
Description: %11					x
Permissions					
List permissions: %12					
Site permissions: %13					
Personal permissions: %14					
35 Permission level deleted					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Title: %6		x ¹	x	x	x
Description: %7		x ¹	x	x	x
Permission Level Details					
ID: %8					
The permission level name is not available because Microsoft does not report this. Refer to events 34 or 36, as these may contain the name.					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
36 Permission level modified					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Title: %6		x ¹	x	x	x
Description: %7		x ¹	x	x	x
Permission Level Details					
ID: %8					
Name: %9					
Type: %10					x
Description: %11					x
Permissions					
List permissions: %12					
Site permissions: %13					
Personal permissions: %14					
37 SharePoint site collection administrator added					
Occurred: %1					
Site: %2					
User: %3					x
Administrator					
ID: %4					
Name: %5					x ²
38 SharePoint site collection administrator removed					
Occurred: %1					
Site: %2					
User: %3					x
Administrator					
ID: %4					
Name: %5					x ²

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
39 Object restored					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Title: %6		x ¹	x	x	x
Description: %7		x ¹	x	x	x
This object was restored from the Recycle Bin.					
40 Site collection updated					
Occurred: %1					
Site: %2					
User: %3					x
41 Web updated					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Title: %5			x	x	x
Description: %6			x	x	x
42 Document library updated					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Title: %5			x	x	x
Description: %6			x	x	x
Library item updated: %7					
43 Document updated					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Title: %5			x	x	x
Version: %6					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
44 List updated					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Title: %6			x	x	x
Description: %7			x	x	x
45 List item updated					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Title: %5		x ¹	x	x	x
46 Folder updated					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Version: %5					
47 Document viewed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Title: %5			x	x	x
Version: %6					
48 Document library viewed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Title: %5			x	x	x
Description: %6			x	x	x

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
49 List viewed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4			x	x	x
URL: %5					
Title: %6			x	x	x
Description: %7			x	x	x
50 Object viewed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Title: %6		x ¹	x	x	x
Description: %7		x ¹	x	x	x
51 Workflow accessed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Title: %6		x ¹	x	x	x
Description: %7		x ¹	x	x	x
The object was accessed as part of a workflow.					
52 Information management policy created					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
Subtype: %5		x ¹	x	x	x
URL: %6					
Title: %7		x ¹	x	x	x
Description: %8		x ¹	x	x	x
Policy details: %9					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
53 Information management policy changed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
Subtype: %5		x ¹	x	x	x
URL: %6					
Title: %7		x ¹	x	x	x
Description: %8		x ¹	x	x	x
Policy details: %9					
54 Site collection information management policy created					
Occurred: %1					
Site: %2					
User: %3					x
Policy details: %4					
55 Site collection information management policy changed					
Occurred: %1					
Site: %2					
User: %3					x
Policy details: %4					
56 Export of objects started					
Occurred: %1					
Site: %2					
Requested by: %3					
Look at adjacent events to determine the number of items exported.					
57 Export of objects completed					
Occurred: %1					
Site: %2					
Requested by: %3					
Total number of items: %4					
Size: %5					
Look at adjacent events to determine when the export was started.					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
58 Import of objects started					
Occurred: %1					
Site: %2					
Requested by: %3					
Size: %4					
Look at adjacent events to determine the number of items imported.					
59 Import of objects completed					
Occurred: %1					
Site: %2					
Requested by: %3					
Total number of items: %4					
Look at adjacent events to determine when the import was started.					
60 Possible tampering warning					
There may have been potential tampering of: %1					
Details: %2					
It could indicate tampering, which could affect the integrity of the audit.					
61 Retention policy processed					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
URL: %5					
Title: %6		x ¹	x	x	x
Description: %7		x ¹	x	x	x
Action: %8					
62 Document fragment updated					
Occurred: %1					
Site: %2					
User: %3					x
Object					
URL: %4					
Title: %5		x ¹	x	x	x

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.



LOGbinder for SharePoint —Impact of Restrict Lookups

<i>Field will be blank if this setting is chosen ...</i>	Exclude none	Exclude highest-cost lookups	Exclude high-cost lookups	Exclude high/medium-cost lookups	Restrict all lookups
63 Content type imported					
Occurred: %1					
Site: %2					
User: %3					x
Source: %4					
Proxy: %5					
Package ID: %6					
64 Information management policy deleted					
Occurred: %1					
Site: %2					
User: %3					x
Object					
Type: %4					
Subtype: %5		x ¹	x	x	x
URL: %6					
Title: %7		x ¹	x	x	x
65 Item declared as a record					
Occurred: %1					
Site: %2					
User: %3					x
URL: %4					
66 Item undeclared as a record					
Occurred: %1					
Site: %2					
User: %3					x
URL: %4					

¹ This lookup is not done only when the target object is a list item. If the target item is a document, folder, list, or library, the lookup is performed.

² Applies to SharePoint 2007 only. In later versions this data is included in the event data without requiring a lookup.