

# Мониторинг ключей реестра Windows

Для мониторинга ключей реестра в KUMA можно использовать стандартные механизмы аудита Windows. Для этого необходимо настроить расширенный аудит на доступ к реестру и определить разделы, операции с ключами которых необходимо мониторить. Данные настройки могут быть выполнены локально на сервере, а также заданы с помощью групповой политики. В статье ниже будет рассказано о локальных настройках.

---

## Настройка политики аудита

Запустите cmd.exe из-под учетной записи Администратора и выполните следующую команду:

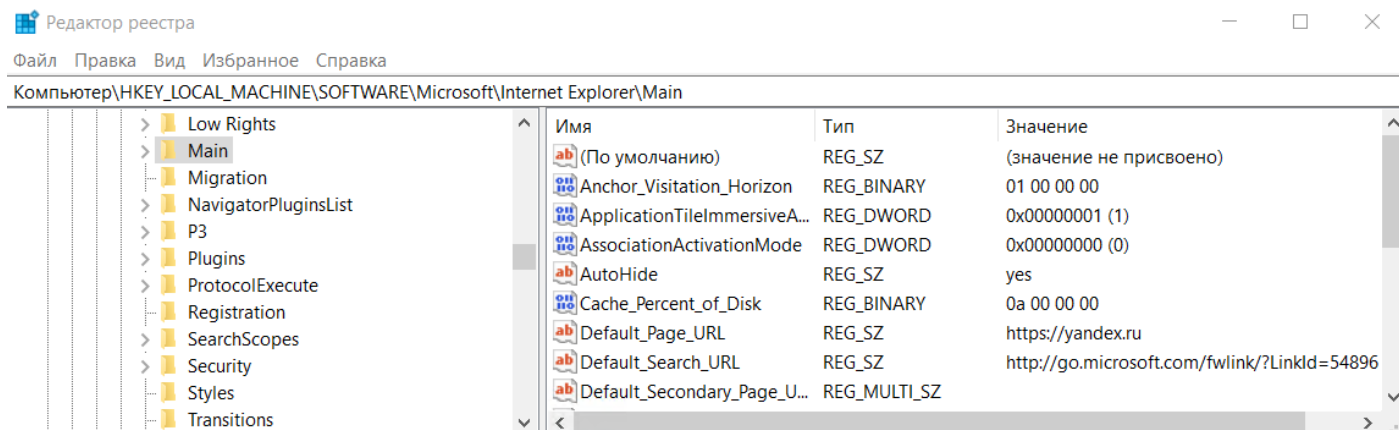
```
auditpol /set /subcategory:"Реестр" /success:enable /failure:enable
```

Другим вариантом является внесение изменений в локальную политику безопасности. Чтобы выполнить его, откройте редактор Локальной политики безопасности и перейдите в "Параметры безопасности" - "Конфигурация расширенной политики аудита" - "Политики аудита системы" - "Объект локальной групповой политики" - "Доступ к объектам".

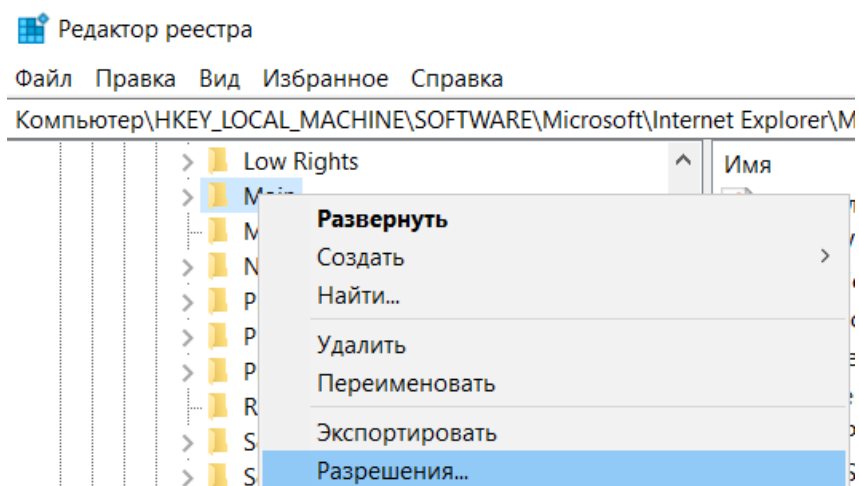


# Настройка аудита раздела реестра

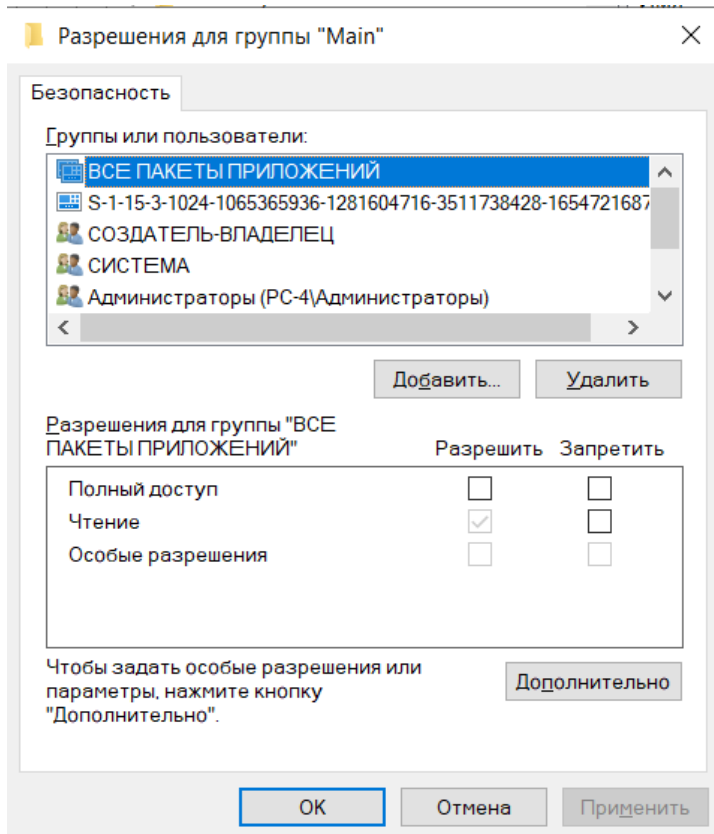
Откройте оснастку "Редактор реестра" и перейдите к разделу, аудит которого необходимо настроить



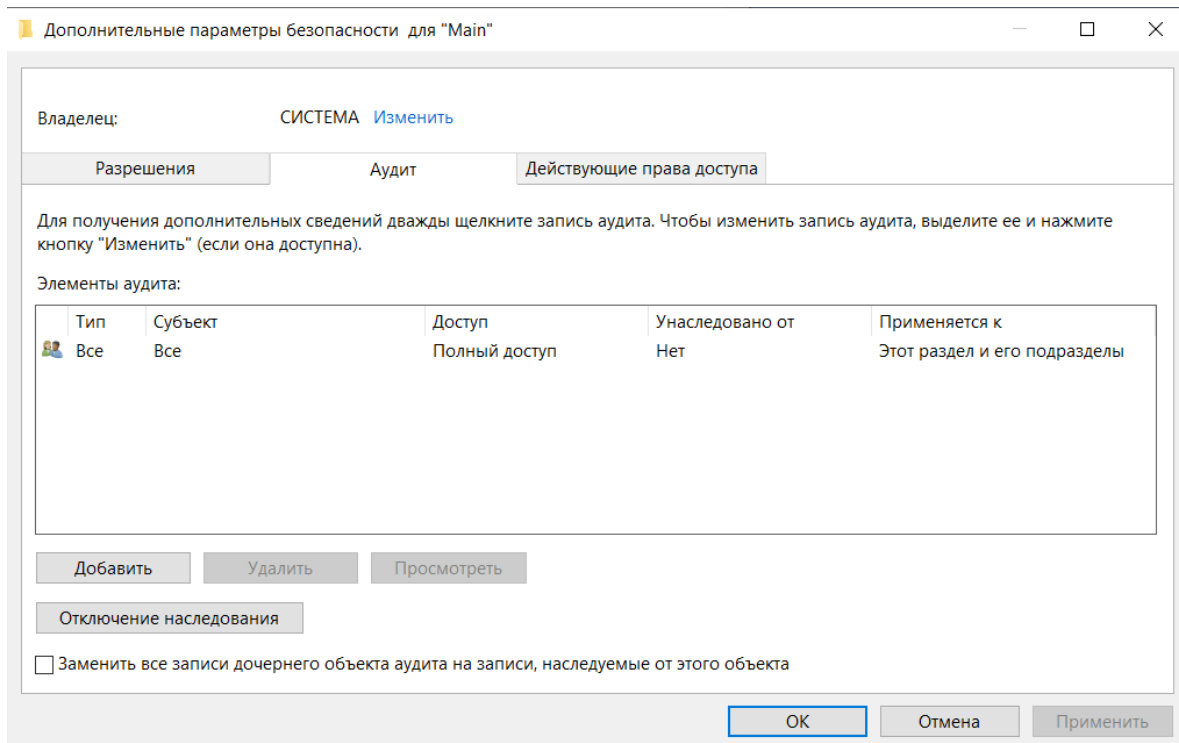
Нажмите ПКМ на нужном разделе и выберите пункт Разрешения



В открывшемся окне нажмите на кнопку "Дополнительно"



В новом окне перейдите на вкладку "Аудит" и добавьте необходимое правило аудита раздела. В данном примере настроен аудит полного доступа всех субъектов к текущему разделу и всем его подразделам.



Примените выполненные настройки.

# Результат

В результате выполненных настроек в журнале безопасности (security) Windows будут появляться события в зависимости от настроенного аудита.

События, которые могут появляться:

- 4663(S): An attempt was made to access an object.
- 4656(S, F): A handle to an object was requested.
- 4658(S): The handle to an object was closed.
- 4660(S): An object was deleted.
- 4657(S): A registry value was modified.
- 5039(-): A registry key was virtualized.
- 4670(S): Permissions on an object were changed.

Как это выглядит в KUMA (на примере события 4657):

События

Не обновлять 1d 24

SELECT \* FROM 'events' WHERE DeviceProduct = 'Windows' AND DeviceHostName='pc-4.demo.lab' AND DeviceEventClassID='4657' ORDER BY Timestamp DESC LIMIT 250

Timestamp↓	Name	SourceUserName	DeviceHostName	DestinationProces...	FileName	DeviceCustomStri...	DeviceCustomStri...
08.11.2023 11:37:09	A registry value was modified.	bob	pc-4.demo.lab	C:\Windows\regedit.exe	\REGISTRY\MACHINE\...	https://yandex.ru	https://google.com

TenantName	Main	DestinationUserName	s-1-5-21-2175569601-655194666-3432137315-1114
Timestamp	08.11.2023 11:37:09:133	DestinationUserPrivileges	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege
<u>Name</u>	<u>A registry value was modified</u>	DeviceCustomIPv6Address2Label	Source IPv6 Address
EndTime	08.11.2023 11:37:09:133	DeviceCustomNumber1	3
<u>DeviceAction</u>	<u>Existing Registry Value modified</u>	DeviceCustomNumber1Label	LogonType
DeviceAssetID	<a href="#">PC-4</a>	DeviceCustomString3	0x5300
DeviceEventCategory	Microsoft-Windows-Security-Auditing	DeviceCustomString3Label	Process ID
DeviceEventClassID	4657	DeviceCustomString4	<a href="https://yandex.ru">https://yandex.ru</a>
DeviceHostName	pc-4.demo.lab	DeviceCustomString4Label	New Value
DeviceNtDomain	DEMO.LAB	DeviceCustomString5	<a href="https://google.com">https://google.com</a>
DeviceProduct	Windows	DeviceCustomString5Label	OldValue
DeviceReceiptTime	08.11.2023 11:43:26:756	DeviceCustomString6	Default_Page_URL
DeviceTimeZone	+03:00	DeviceCustomString6Label	Object Value Name
DeviceVendor	Microsoft	Service	<a href="#">WMI-Collector (TCP/5550)</a>
SourceAccountID	<a href="#">bob dylan</a>	ExternalID	1469905
SourceAssetID	<a href="#">XDR-KSC</a>	FileID	0x358
SourceHostName	xdr-ksc.demo.lab	FileName	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main
SourceNtDomain	DEMO.LAB	FlexString1	0x493e0ca
SourceProcessName	Advapi	FlexString1Label	Destination Logon ID
SourceUserID	S-1-5-21-2175569601-655194666-3432137315-1105	Type	Base
<u>SourceUserName</u>	<u>bob</u>		
DestinationHostName	localhost.demo.lab		
DestinationNtDomain	DEMO.LAB		
<u>DestinationProcessName</u>	<u>C:\Windows\regedit.exe</u>		
DestinationUserID	0x493e0ca		

Revision #1  
Created 9 November 2023 09:57:46 by Koala  
Updated 18 December 2024 10:16:19 by Koala