Мониторинг ключей реестра Windows

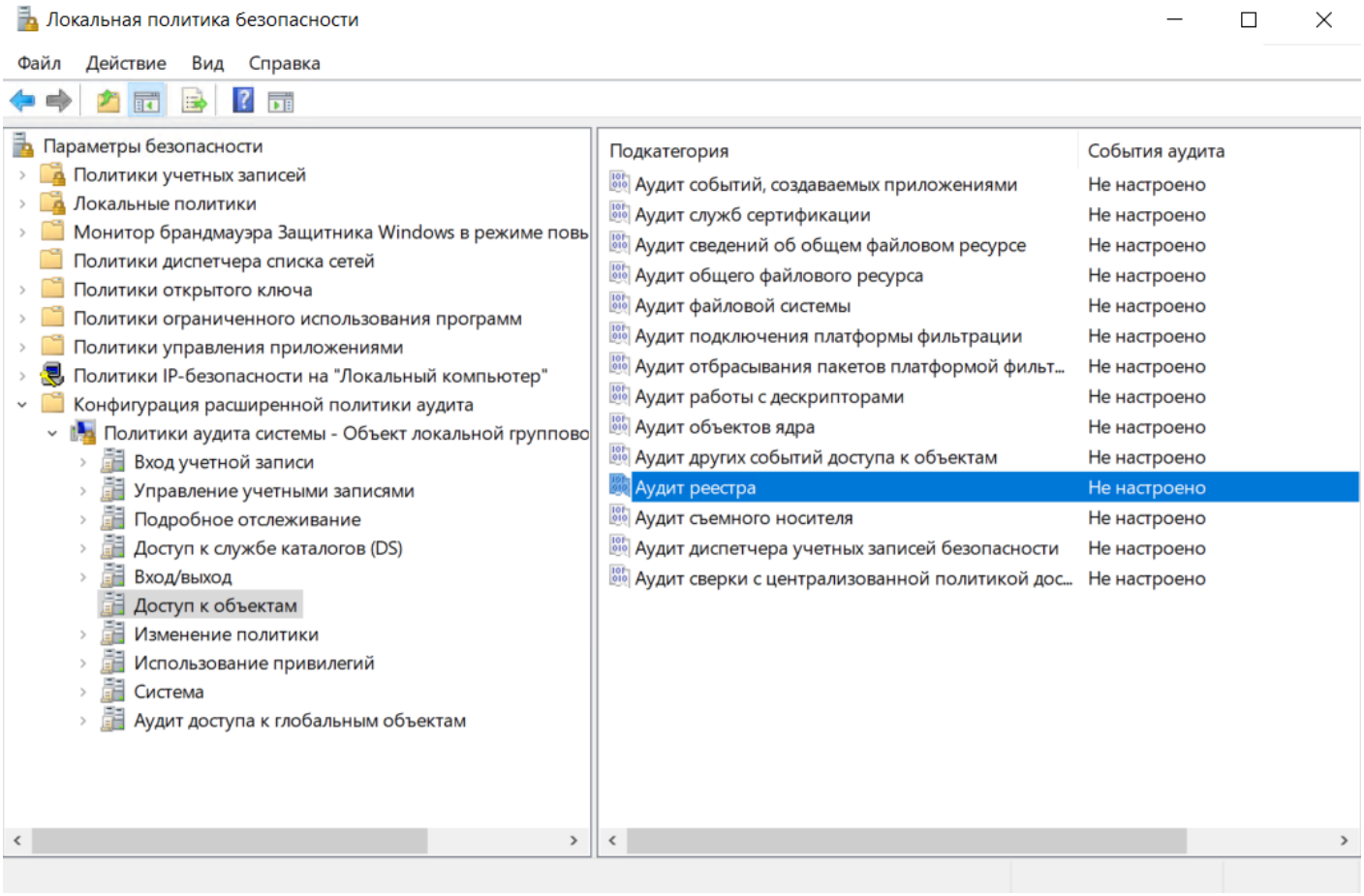
Для мониторинга ключей реестра в KUMA можно использовать стандартные механизмы аудита Windows. Для этого необходимо настроить расширенный аудит на доступ к реестру и определить разделы, операции с ключами которых необходимо мониторить. Данные настройки могут быть выполнены локально на сервере, а также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

Настройка политики аудита

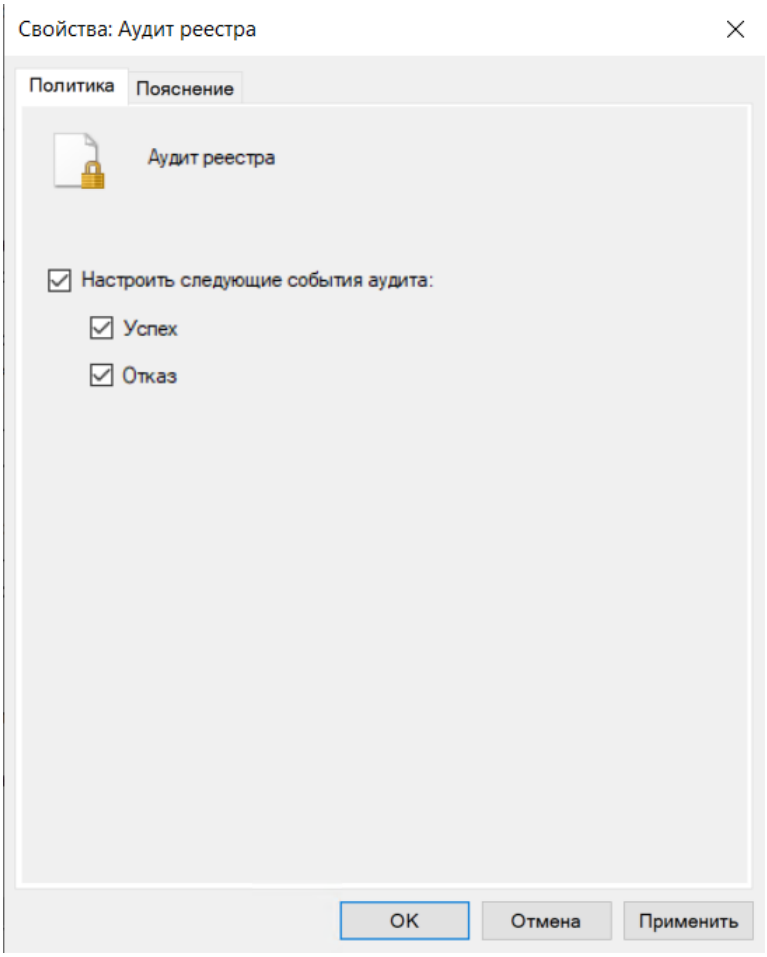
Запустите cmd.exe из-под учетной записи Администратора и выполните следующую команду:

```
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".

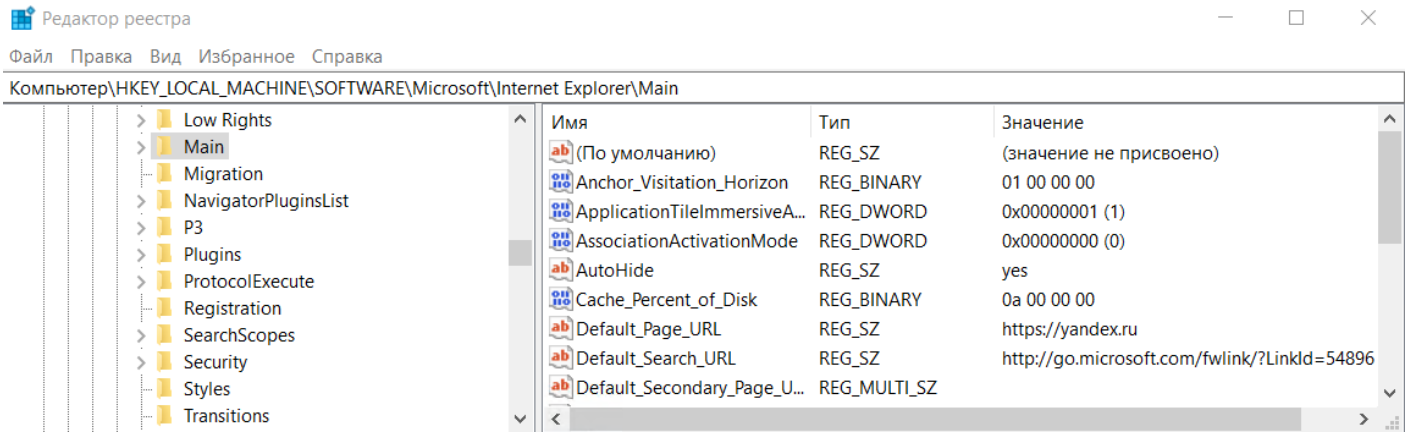


Откройте подкатегорию "Аудит реестра" и выставите необходимые значения

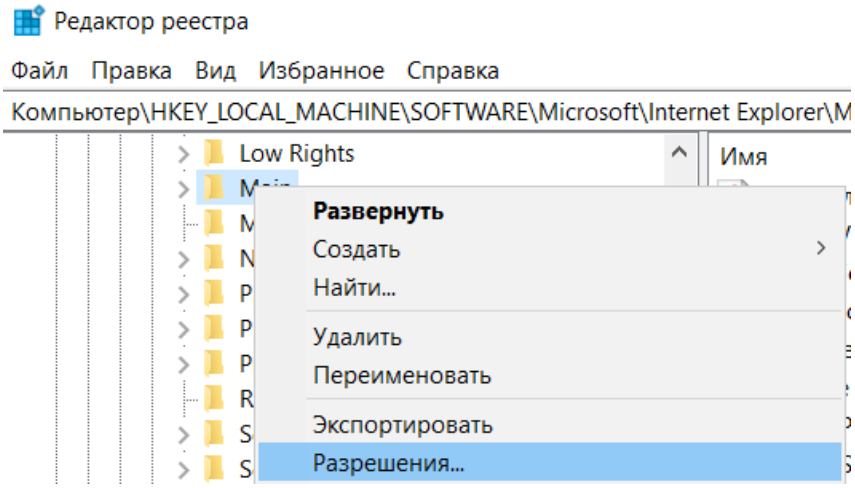


Настройка аудита раздела реестра

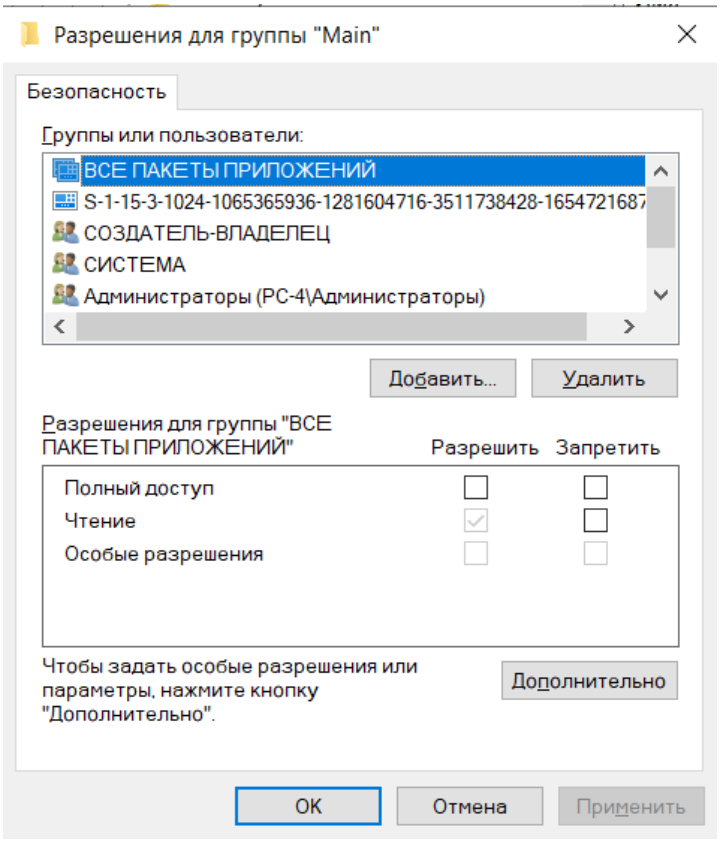
Откройте оснастку "Редактор реестра" и перейдите к разделу, аудит которого необходимо настроить



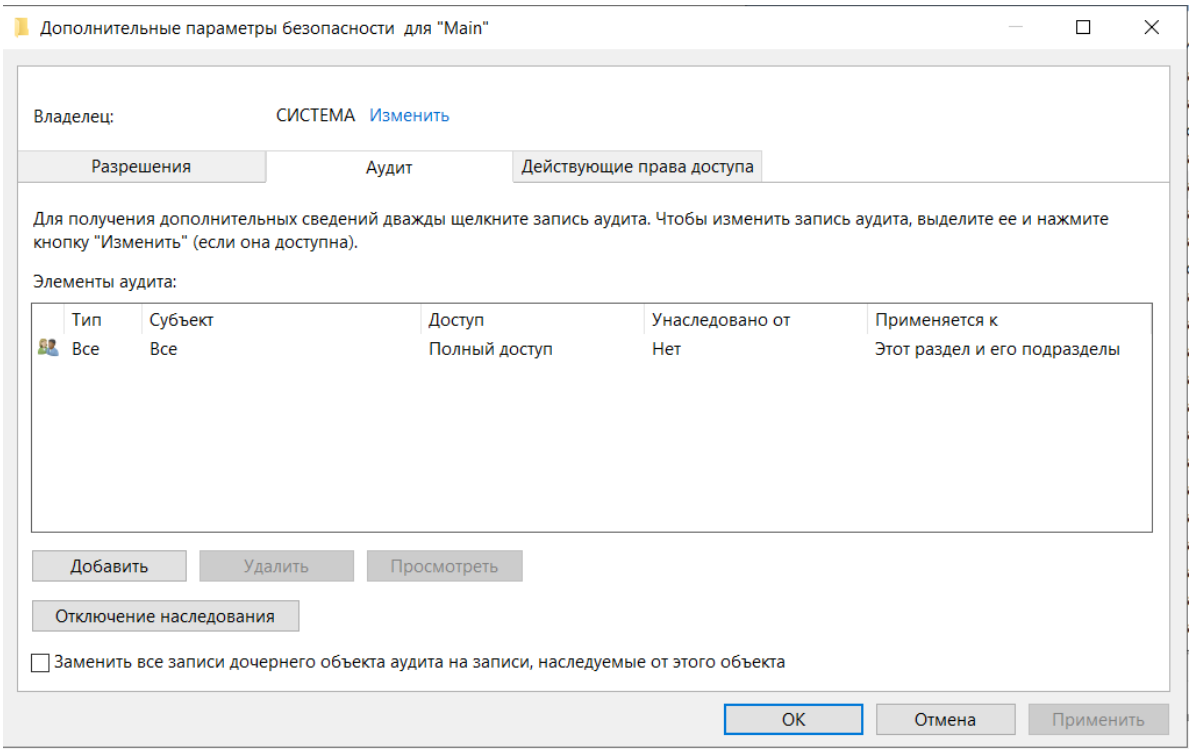
Нажмите ПКМ на нужном разделе и выберите пункт Разрешения



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):

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

Revision #1
Created 9 November 2023 09:57:46 by Koala
Updated 26 June 2024 14:59:17 by Koala