Категории расширенной политики аудита (AAP)

В таблице описаны категории и подкатегории событий расширенной политики аудита (AAP). Для каждой подкатегории даны рекомендации по настройке аудита на контроллерах домена (**«Д»**), серверах (**«С»**) и рабочих станциях (**«К»**).

Используются следующие обозначения:

- **прочерк** — включение аудита не требуется;
- **«Успех», «Отказ»** — рекомендуется включить аудит успехов и отказов;
- **«(Успех)», «(Отказ)»** — условие, при котором рекомендуется включить аудит успехов и отказов, указано в примечании.

Категории расширенной политики аудита

№	Подкатегория	Описание	Д	С	К
Вход учетной записи (Account Logon) — содержит события, регистрируемые при проверке учетных данных. Доменные учетные записи проверяются контроллером домена (по протоколу NTLM), локальные учетные записи — серверами и рабочими станциями					
1	Аудит проверки учетных данных (Audit Credential Validation)	Содержит события 4774, 4775, 4776, 4777. На рабочих станциях регистрируется большое количество событий	Успех, Отказ	Успех, Отказ	Успех, Отказ
2	Аудит службы проверки подлинности Kerberos (Audit Kerberos Authentication Service)	Содержит события 4768, 4771, 4772. События регистрируются только на контроллерах домена. Регистрируется большое количество событий. При включении аудита успехов регистрируются события успешных запросов Ticket Granting Ticket (TGT). При включении аудита отказов регистрируются события неуспешных запросов TGT (неправильно указано имя, пароль и т. п.) и их причины	Успех, Отказ	—	—
3	Аудит операций с билетами службы Kerberos (Audit Kerberos Service Ticket Operations)	Содержит события 4769, 4770, 4773. События регистрируются только на контроллерах домена. Регистрируется большое количество событий. При включении аудита успехов регистрируются события успешных запросов Ticket Granting Service (TGS). При включении аудита отказов регистрируются события неуспешных запросов TGS (не пройдена проверка подлинности, неправильный сетевой адрес и т. п.) и их причины	Успех, Отказ	—	—
Управление учетными записями (Account Management) — содержит события, связанные с новыми пользователями и группами: изменение имени, включение и отключение учетной записи, изменение пароля, включение аудита событий управления учетными записями					
4	Аудит управления группами приложений (Audit Application Group Management)	Содержит события 4783, 4784, 4785, 4786, 4787, 4788, 4789, 4790, 4791, 4792. События относятся к группам пользователей приложений (Application Group): создание, изменение, удаление группы и ее членов. Нет событий аудита отказов. При использовании Application Group рекомендуется включить аудит успехов	—	—	—
5	Аудит управления учетными записями компьютеров (Audit Computer Account Management)	Содержит события 4741, 4742, 4743. События регистрируются только на контроллерах домена. Число событий небольшое. События регистрируются при создании, изменении и удалении учетной записи компьютера. Нет событий аудита отказов. Рекомендуется отслеживать состояние критически важных учетных записей	Успех	—	—

№	Подкатегория	Описание	Д	С	К
6	Аудит управления группами распространения (Audit Distribution Group Management)	Содержит события 4744, 4745, 4746, 4747, 4748, 4749, 4750, 4751, 4752, 4753, 4759, 4760, 4761, 4762, 4763. События регистрируются на контроллерах домена при создании, изменении и удалении группы распространения, при добавлении и удалении членов группы. Число событий небольшое. Нет событий аудита отказов. Рекомендуется отслеживать состояние критически важных групп распространения	Успех	—	—
7	Аудит других событий управления учетными записями (Audit Other Account Management Events)	Содержит события 4782, 4793. Событие регистрируется на контроллерах домена и серверах. Нет событий аудита отказов	Успех	Успех	—
8	Аудит управления группами безопасности (Audit Security Group Management)	Содержит события 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4754, 4755, 4756, 4757, 4758, 4764, 4799. Включение аудита успехов позволяет отслеживать события создания, изменения и удаления групп, добавления и удаления членов групп. Нет событий аудита отказов	Успех	Успех	Успех
9	Аудит управления учетными записями пользователей (Audit User Account Management)	Содержит события 4720, 4722, 4723, 4724, 4725, 4726, 4738, 4740, 4765, 4766, 4767, 4780, 4781, 4794, 4798, 5376, 5377. Позволяет отслеживать создание, изменение, удаление, переименование, включение, отключение, блокировку и разблокировку учетных записей, попытки сброса и изменения пароля, попытки изменения пароля администратора Directory Services Restore Mode, резервное копирование и восстановление учетных записей в Credential Manager	Успех, Отказ	Успех, Отказ	Успех, Отказ

Подробное отслеживание (Detailed Tracking) — содержит события мониторинга активности приложений и пользователей компьютера

10	Аудит активности DPAPI (Audit DPAPI Activity)	Содержит события 4692, 4693, 4694, 4695. Содержит информационные события (попытки резервного копирования и восстановления главного ключа защиты данных, попытки защиты или снятия защиты отслеживаемых защищенных данных), использующиеся для поиска ошибок в работе Data Protection Application Interface (DPAPI)	—	—	—
11	Аудит активности PNP (Audit PNP Activity)	Содержит события 6416, 6419, 6420, 6421, 6422, 6423, 6424. Позволяет отслеживать изменения в конфигурации аппаратного обеспечения. Нет событий аудита отказов	Успех	Успех	Успех
12	Аудит создания процессов (Audit Process Creation)	Содержит события 4688, 4696. События подкатегории позволяют узнать, кто, где и с какими параметрами запускал процесс. Объем событий большой. Нет событий аудита отказов	Успех	Успех	Успех
13	Аудит завершения процессов (Audit Process Termination)	Содержит событие 4689. Регистрируются события успехов при завершении процесса. Нет событий аудита отказов	Успех	Успех	Успех
14	Аудит событий RPC (Audit RPC Events)	Содержит событие 5712. Событие регистрируется при попытке удаленного вызова процедуры (RPC)	—	—	—

№	Подкатегория	Описание	Д	С	К
15	Проверка изменений прав маркера (Audit Token Right Adjustment)	Содержит событие 4703. Событие регистрируется при изменении прав пользователя	—	—	—

Доступ к службе каталогов (DS Access) — категория аудита применяется только к контроллерам домена. Данный аудит генерирует события, содержащие информацию о попытках доступа и модификации объектов Active Directory Domain Services (AD DS)

№	Подкатегория	Описание	Д	С	К
16	Аудит подробной репликации службы каталогов (Audit Detailed Directory Service Replication)	Содержит события 4928, 4929, 4930, 4931, 4934, 4935, 4936, 4937. События генерируются при установке, модификации, удалении контекста именования источника репликации. В событии необходимо отслеживать поле SourceAddr, так как источник новой репликации (новый Directory Replication Agent) должен быть авторизован	Успех, Отказ	—	—
17	Аудит доступа к службе каталогов (Audit Directory Service Access)	Содержит события 4661, 4662. Содержит события запроса дескриптора объекта и выполнения операции с объектом. Событие 4661 генерируется, если включен аудит успехов подкатегории Audit Handle Manipulation. Событие 4662 генерируется только для объектов Active Directory с настроенным System Access Control List	Успех, Отказ	—	—
18	Аудит изменения службы каталогов (Audit Directory Service Changes)	Содержит события 5136, 5137, 5138, 5139, 5141. Содержит события создания, удаления, восстановления, перемещения, модификации объектов Active Directory. Нет событий аудита отказов	Успех	—	—
19	Аудит репликации службы каталогов (Audit Directory Service Replication)	Содержит события 4932, 4933. События начала и окончания репликации между двумя контроллерами домена. События используются для поиска ошибок репликации	Успех	—	—

Вход/Выход (Logon/Logoff) — содержит события, позволяющие отследить интерактивный и сетевой вход на компьютер. Эти события генерируются на компьютере, на котором выполнена попытка входа. Они позволяют отследить пользовательскую активность или выявить потенциальные атаки на сетевые ресурсы

№	Подкатегория	Описание	Д	С	К
20	Аудит блокировки учетных записей (Audit Account Lockout)	Содержит событие аудита отказов 4625, при этом поле status=0xC0000234, task category=12546	Отказ	Отказ	Отказ
21	Аудит заявок пользователей или устройства на доступ (Audit User / Device Claims)	Содержит событие 4626. Событие генерируется для новых учетных записей. Подкатегория доступна начиная с Windows 8, Windows Server 2012	—	—	—
22	Членство в группе аудита (Audit Group Membership)	Содержит событие 4627. Подкатегория доступна начиная с Windows 10, Windows Server 2016	—	—	—
23	Аудит расширенного режима IPsec (Audit IPsec Extended Mode)	Содержит события 4978, 4979, 4980, 4981, 4982, 4983, 4984	—	—	—

№	Подкатегория	Описание	Д	С	К
24	Аудит основного режима IPsec (Audit IPsec Main Mode)	Содержит события 4646, 4650, 4651, 4652, 4653, 4655, 4976, 5049, 5453	—	—	—
25	Аудит быстрого режима IPsec (Audit IPsec Quick Mode)	Содержит события 4977, 5451, 5452	—	—	—
26	Аудит выхода из системы (Audit Logoff)	Содержит события 4634, 4647. События аудита успехов информируют о длительности сессии (корреляция событий 4624 (подкатегория Audit Logon) и 4634)	Успех	Успех	Успех
27	Аудит входа в систему (Audit Logon)	Содержит события 4624, 4625, 4648, 4675. События аудита успехов информируют, с использованием какой учетной записи, когда и с какого компьютера произведен вход на тот или иной компьютер. События аудита отказов показывают попытки входа и причины отказа	Успех, Отказ	Успех, Отказ	Успех, Отказ
28	Аудит сервера политики сети (Audit Network Policy Server)	Содержит события 6272, 6273, 6274, 6275, 6276, 6277, 6278, 6279, 6280. Аудит успехов и отказов позволяет отслеживать запросы предоставления и отказа при помещении пользователя в карантин. Для получения событий необходимо настроить сбор событий с серверов с ролью Microsoft Network Policy Server	Успех, Отказ	Успех, Отказ	—
29	Аудит других событий входа и выхода (Audit Other Logon/Logoff Events)	Содержит события 4649, 4778, 4779, 4800, 4801, 4802, 4803, 5378, 5632, 5633. Включение аудита успехов позволит отслеживать подключение и отключение от существующей терминальной сессии, блокировку и разблокировку компьютера, включение и отключение экранной заставки. Включение аудита отказов позволит отслеживать запросы делегирования учетных записей (Credential Security Support Provider), запрещенных политикой	Успех, Отказ	Успех, Отказ	Успех, Отказ
30	Аудит специального входа (Audit Special Logon)	Содержит события 4672, 4964. Включение аудита успехов позволяет отслеживать события входа в систему пользователя, входящего в Special Groups, а также присвоение новой пользовательской сессии слишком высоких привилегий. Нет событий аудита отказов	Успех	Успех	Успех

Доступ к объектам (Object Access) — аудит доступа пользователей к объектам (например, файлам, папкам, разделам реестра), для которых указан System Access Control List (SACL). SACL состоит из Access Control Entry (ACE). Каждая запись состоит из трех элементов: отслеживаемый участник безопасности (пользователь, компьютер или группа); отслеживаемые типы доступа, образующие маску доступа; параметр, указывающий, отслеживать ли только неуспешные попытки обращений, только успешные или обе категории. При создании SACL следует вносить в них только те действия, которые реально требуется отслеживать. Например, для исполняемых файлов можно включить параметр Write and Append Data Auditing

31	Аудит событий, создаваемых приложениями (Audit Application Generated)	Содержит события 4665, 4666, 4667, 4668. В подкатегории генерируются события приложений, использующих Authorization Manager (начиная с Windows Server 2012, Authorization Manager считается устаревшим). Рекомендуется включить аудит успехов и отказов, если используются приложения, использующие Authorization Manager	—	—	—

№	Подкатегория	Описание	Д	С	К
32	Аудит служб сертификации (Audit Certification Services)	Содержит события 4868, 4869, 4870, 4871, 4872, 4873, 4874, 4875, 4876, 4877, 4878, 4879, 4880, 4881, 4882, 4883, 4884, 4885, 4886, 4887, 4888, 4889, 4890, 4891, 4892, 4893, 4894, 4895, 4896, 4897, 4898. Подкатегория позволяет отслеживать события служб сертификации (если установлена роль AD CS): запуск, остановку, резервное копирование и восстановление параметров Active Directory Certificate Services (AD CS), запрос, выдачу, отзыв сертификата и другие события. Необходимо настроить сбор событий с серверов с ролью Microsoft Certification Authority	Успех, Отказ	Успех, Отказ	—
33	Аудит сведений об общем файловом ресурсе (Audit Detailed File Share)	Содержит событие 5145. Подкатегория доступна начиная с Windows 7, Windows Server 2008 R2. Подкатегория позволяет отслеживать попытки доступа к файлам и папкам, находящимся в общей папке. События генерируются каждый раз при обращении к файлу или папке. События включают в себя информацию о полномочиях, используемых для разрешения или запрета доступа. Если подкатегория включена, то события будут генерироваться для всех общих папок. Поток событий аудита успехов высокий на файловых серверах и контроллерах домена. События аудита отказов будут генерироваться, если доступ ограничен на уровне общей папки. Если доступ ограничен на уровне файловой системы, события генерироваться не будут	Успех, Отказ	Успех, Отказ	Успех, Отказ
34	Аудит общего файлового ресурса (Audit File Share)	Содержит события 5140, 5142, 5143, 5144, 5168. Подкатегория позволяет отслеживать события создания, удаления, модификации и попыток доступа к общей папке. Если подкатегория включена, события будут генерироваться для всех общих папок	Успех, Отказ	Успех, Отказ	Успех, Отказ
35	Аудит файловой системы (Audit File System)	Содержит события 4656, 4658, 4660, 4663, 4664, 4670, 4985, 5051. Подкатегория позволяет отслеживать попытки доступа пользователя к объектам файловой системы. События генерируются для объектов с настроенным SACL, если тип доступа и запрос пользователя совпадает с SACL. Необходимо определить критически важные объекты файловой системы и настроить для них SACL	Успех, Отказ	Успех, Отказ	Успех, Отказ
36	Аудит подключения платформы фильтрации (Audit Filtering Platform Connection)	Содержит события 5031, 5150, 5151, 5154, 5155, 5156, 5157, 5158, 5159. Подкатегория позволяет отслеживать события блокировки или разрешения соединения Windows Filtering Platform	Успех	Успех	Успех
37	Аудит отбрасывания пакетов платформой фильтрации (Audit Filtering Platform Packet Drop)	Содержит события 5152, 5153. Подкатегория позволяет отслеживать события блокировки сетевого пакета Windows Filtering Platform. События генерируются на каждое событие блокировки сетевого пакета. Аудит используется для поиска ошибок	—	—	—
38	Аудит работы с дескрипторами (Audit Handle Manipulation)	Содержит события 4658, 4690. Подкатегория позволяет отслеживать события 4658 для подкатегорий Audit File System, Audit Kernel Object, Audit Registry, Audit Removable Storage и Audit SAM. При корреляции с событием 4656 можно понять, как долго объект был открыт. Нет событий аудита отказов	Успех	Успех	Успех

№	Подкатегория	Описание	Д	С	К
39	Аудит объектов ядра (Audit Kernel Object)	Содержит события 4656, 4658, 4660, 4663. Подкатегория позволяет отслеживать попытки пользователя получить доступ к объектам ядра: мьютексам (mutex), событиям (events), семафорам (semaphore). Для генерации события необходимо включить Audit: Audit the access of global system objects и перезагрузить компьютер. Объем событий большой. События используются разработчиками для поиска ошибок	Успех	Успех	Успех
40	Аудит других событий доступа к объектам (Audit Other Object Access Events)	Содержит события 4671, 4691, 4698, 4699, 4700, 4701, 4702, 5148, 5149, 5888, 5889, 5890. Подкатегория доступна начиная с версии Windows 2008 R2 и с Windows 7. Аудит успехов позволяет отслеживать события планировщика задач (создание, удаление, включение, выключение, обновление) и объектов COM+ (добавление, обновление, удаление). При включении аудита отказов Windows Filtering Platform генерирует события о начале и прекращении DoS-атаки	Успех, Отказ	Успех, Отказ	Успех, Отказ
41	Аудит реестра (Audit Registry)	Содержит события 4663, 4656, 4658, 4660, 4657, 5039, 4670. Подкатегория позволяет отслеживать попытки доступа пользователя к объектам реестра. События генерируются для объектов с настроенным SACL, если тип доступа и запрос пользователя совпадает с SACL. Необходимо определить критически важные объекты реестра и настроить для них SACL	Успех, Отказ	Успех, Отказ	Успех, Отказ
42	Аудит съемного носителя (Audit Removable Storage)	Содержит события 4656, 4658, 4663. Подкатегория доступна начиная с Windows 8, Windows Server 2012. Подкатегория позволяет отслеживать события (запрос дескриптора, закрытие дескриптора, доступ к объекту) доступа к объектам файловой системы на внешнем носителе. События генерируются для всех объектов для всех видов доступа независимо от параметров SACL	Успех, Отказ	Успех, Отказ	Успех, Отказ
43	Аудит диспетчера учетных записей безопасности (Audit SAM)	Содержит событие 4661. Подкатегория позволяет отслеживать попытки запроса дескриптора безопасности объектов Security Account Manager (SAM): SAM_ALIAS: A local group, SAM_GROUP: A group that is not a local group, SAM_USER: A user account, SAM_SERVER: A computer account	Успех, Отказ	Успех, Отказ	Успех, Отказ
44	Аудит сверки с централизованной политикой доступа (Audit Central Access Policy Staging)	Содержит событие 4818. Подкатегория доступна начиная с Windows Server 2012 R2 и Windows 8.1. Событие используется для тестирования и поиска ошибок в работе Dynamic Access Control	—	—	—

Изменение политики (Policy Change) — категория содержит события, связанные с изменением различных политик

45	Аудит изменения политики аудита (Audit Policy Change)	Содержит события 4902, 4904, 4905, 4907, 4715, 4719, 4817, 4906, 4908, 4912. Подкатегория позволяет отслеживать события, связанные с изменением политики аудита: изменение дескриптора безопасности политики аудита; изменение Audit Policy; изменение Global Object Access; изменение параметров аудита для пользователя; изменение состава Special Groups; добавление и удаление источника событий из журнала Security; изменение параметров аудита для объекта (файл, ключ реестра); изменение значения параметра CrashOnAuditFail. Нет событий аудита отказов	Успех	Успех	Успех

№	Подкатегория	Описание	Д	С	К
46	Аудит изменения политики проверки подлинности (Audit Authentication Policy Change)	Содержит события 4670, 4706, 4707, 4713, 4716, 4717, 4718, 4739, 4864, 4865, 4866, 4867. Подкатегория позволяет отслеживать: изменения политик Kerberos Policy, Account Lockout Policy, Password Policy, Network security: Force logoff when logon hours expire; предоставление пользователю или группе полномочий: Access this computer from the network, Deny access to this computer from the network, Allow logon locally, Deny log on locally, Allow logon through Remote Desktop, Deny log on through Remote Desktop Services, Logon as a batch job, Deny log on as a batch job, Logon as a service, Deny log on as a service; создание, удаление и модификацию доверия между доменами. Нет событий аудита отказов	Успех	Успех	Успех
47	Аудит изменения политики авторизации (Audit Authorization Policy Change)	Содержит события 4703, 4704, 4705, 4670, 4911, 4913. Подкатегория позволяет отслеживать: добавление и удаление привилегий пользователю или группе (Shut down the system и другие, не вошедшие в подкатегорию Audit Authentication Policy Change); изменение политики Encrypting File System (EFS); изменение атрибутов ресурса объекта; изменение Central Access Policy для объекта. Нет событий аудита отказов	Успех	Успех	Успех
48	Аудит изменения политики платформы фильтрации (Audit Filtering Platform Policy)	Содержит события 4709, 4710, 4711, 4712, 5040, 5041, 5042, 5043, 5044, 5045, 5046, 5047, 5048, 5440, 5441, 5442, 5443, 5444, 5446, 5448, 5449, 5450, 5456, 5457, 5458, 5459, 5460, 5461, 5462, 5463, 5464, 5465, 5466, 5467, 5468, 5471, 5472, 5473, 5474, 5477. Подкатегория позволяет отслеживать события, генерируемые Windows Filtering Platform (WFP): состояние служб IPsec; изменение параметров IPsec; состояние и изменение модуля и поставщиков WFP; действия службы агента политики IPsec	—	—	—
49	Аудит изменения политики на уровне правил MPSSVC (Audit MPSSVC Rule Level Policy Change)	Содержит события 4944, 4945, 4946, 4947, 4948, 4949, 4950, 4951, 4952, 4953, 4954, 4956, 4957, 4958. Подкатегория позволяет отслеживать: активности политики при запуске службы Windows Firewall; изменения правил Windows Firewall; изменение списка исключений Windows Firewall; изменение параметров Windows Firewall; игнорирование или неприменение правил службы Windows Firewall; изменение параметров групповой политики Windows Firewall	Успех	Успех	Успех
50	Аудит других событий изменения политики (Audit Other Policy Change Events)	Содержит события 4714, 4819, 4826, 4909, 4910, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5447, 6144, 6145. Подкатегория позволяет отслеживать события Central Access Policies; Boot Configuration Data, политики агента восстановления данных EFS, ошибки применения групповых политик, операции криптографического провайдера	—	—	—

Использование привилегий (Privilege Use) — категория позволяет отслеживать использование предоставленных пользователям привилегий. Количество регистрируемых событий может быть очень большим

51	Аудит использования привилегий, не затрагивающих конфиденциальные данные (Audit Non-Sensitive Privilege Use)	Содержит события 4673, 4674, 4985. Подкатегория позволяет отслеживать использование полномочий: Access Credential Manager as a trusted caller; Add workstations to domain; Adjust memory quotas for a process; Bypass traverse checking; Change the system time; Change the time zone; Create a page file; Create global objects; Create permanent shared objects; Create symbolic links; Force shutdown from a remote system; Increase a process working set; Increase scheduling priority; Lock pages in memory; Modify an object label; Perform volume maintenance tasks; Profile single process; Profile system performance; Remove computer from docking station; Shut down the system; Synchronize directory service data	—	—	—
52	Аудит других событий использования привилегий (Audit Other Privilege Use Events)	Содержит событие 4985	—	—	—

№	Подкатегория	Описание	Д	С	К
53	Аудит использования привилегий, затрагивающих конфиденциальные данные (Audit Sensitive Privilege Use)	Содержит события 4673, 4674, 4985. Подкатегория позволяет отслеживать использование слишком высоких привилегий: Act as part of the operating system; Back up files and directories; Restore files and directories; Create a token object; Debug programs; Enable computer and user accounts to be trusted for delegation; Generate security audits; Impersonate a client after authentication; Load and unload device drivers; Manage auditing and security log; Modify firmware environment values; Replace a process level token; Take ownership of files or other objects	—	—	—

Система (System) — категория позволяет отслеживать изменения компьютера на уровне системы, которые не включены в другие категории аудита

54	Аудит драйвера IPsec (Audit IPsec Driver)	Содержит события 4960, 4961, 4962, 4963, 4965, 5478, 5479, 5480, 5483, 5484, 5485. Подкатегория позволяет отслеживать действия драйвера IPsec: запуск и завершение работы служб IPsec; отклонение пакетов из-за сбоя проверки целостности; отклонение пакетов из-за сбоя проверки повторения; отклонение пакетов из-за передачи в виде открытого текста; получены пакеты с неправильным Security Parameter Index; сбой обработки фильтров IPsec	—	—	—
55	Аудит других системных событий (Audit Other System Events)	Содержит события 5024, 5025, 5027, 5028, 5029, 5030, 5032, 5033, 5034, 5035, 5037, 5058, 5059, 6400, 6401, 6402, 6403, 6404, 6405, 6406, 6407, 6408, 6409, 5379. Подкатегория позволяет отслеживать события запуска и завершения работы службы и драйвера Windows Firewall, обработки политики безопасности службой Windows Firewall, операций с файлом ключа шифрования и операций переноса ключа шифрования	Успех, Отказ	Успех, Отказ	Успех, Отказ
56	Аудит изменения состояния безопасности (Audit Security State Change)	Содержит события 4608, 4616, 4621. Подкатегория позволяет отслеживать события изменения системного времени, запуска системы, восстановления системы из CrashOnAuditFail. Нет событий аудита отказов	Успех	Успех	Успех
57	Аудит расширения системы безопасности (Audit Security System Extension)	Содержит события 4610, 4611, 4614, 4622, 4697. Подкатегория позволяет отслеживать события загрузки кода расширения безопасности (пакета проверки подлинности, уведомлений или безопасности) в Local Security Authority, установки службы. Нет событий аудита отказов	Успех	Успех	Успех
58	Аудит целостности системы (Audit System Integrity)	Содержит события 4612, 4615, 4618, 4816, 5038, 5056, 5057, 5060, 5061, 5062, 6281, 6410. Подкатегория позволяет отслеживать события ошибок записи событий в журнал, возникающих при проверке целостности кода, целостности при расшифровке входящего сообщения Remote Procedure Calling	Успех, Отказ	Успех, Отказ	Успех, Отказ

Аудит доступа к глобальным объектам (Global Object Access Auditing).

Для регистрации событий категории необходимо включить аудит подкатегории File System

59	Файловая система (File System)	Подкатегория позволяет настраивать глобальный SACL в файловой системе компьютера. Если на компьютере настроены SACL и глобальный SACL, то будет применяться список SACL, полученный путем их объединения	—	—	—
60	Реестр (Registry)	Подкатегория позволяет настраивать глобальный SACL в реестре компьютера	—	—	—

ID статьи: 1618
Последнее обновление: 14 апр., 2026
Обновлено от: Михалева А.
Ревизия: 1

Руководство разработчика -> Подключение источников событий в Логикор -> Настройка источников -> Настройка аудита
https://docs.axel.pro/entry/1618/