ALTEX SOFT

ОТЧЁТ

№ отчёта	*f9a4d973-d302-48ad-87d3-38688b5e8ef7*
Профиль	*Конфигурации*
Задание	*Job_7335*
Формирование отчёта	*19.05.2015 15:35:02*
Имя	*Quick_localhost_189*
Описание	*Автогенерируемый отчет вкладки "История" для "localhost" из "Job_7335" задания.*
Хосты [1]	*localhost*

Хост: localhost

CPE	*cpe:/o:microsoft:windows_7:::enterprise*
Начало/завершение сканирования	*19.05.2015 09:42:11 / 19.05.2015 09:42:12*
Профиль	*Нет*
Агент	*Нет*

Конфигурация "Безопасная среда Windows 7"

Конфигурация не соответствует эталонной. Всего - 176, соответствие - 92 (52 %)

- **Соответствие (92)**
- **Несоответствие (84)**
- **Ошибка (0)**
- **Не проверено (0)**
- **Не выбрано (0)**
- **Неизвестно (0)**
- **Информация (0)**
- **Исправлено (0)**
- **Неприменимо (0)**

2 Параметры политики компьютеров

2.1 Назначение прав пользователя

- Архивация файлов и каталогов
- Блокировка страниц в памяти
- Восстановление файлов и каталогов
- Вход в качестве пакетного задания
- Вход в качестве службы
- Выполнение задач по обслуживанию томов
- Добавление рабочих станций к домену
- Доступ к диспетчеру учетных данных от имени доверенного вызывающего
- Доступ к компьютеру из сети
- Завершение работы системы
- Загрузка и выгрузка драйверов устройств
- Замена маркера уровня процесса
- Запретить вход в систему через службу удаленных рабочих столов
- Запретить локальный вход
- Изменение метки объекта
- Изменение параметров среды изготовителя
- Изменение системного времени

- ✓ Изменение часового пояса
- ✓ Имитация клиента после проверки подлинности
- ✗ Локальный вход в систему
- ✓ Настройка квот памяти для процесса
- ✗ Обход перекрестной проверки
- ✗ Отказать в доступе к этому компьютеру из сети
- ✗ Отказать во входе в качестве пакетного задания
- ✓ Отключение компьютера от стыковочного узла
- ✗ Отладка программ
- ✓ Принудительное удаленное завершение работы
- ✓ Профилирование одного процесса
- ✓ Профилирование производительности системы
- ✓ Работа в режиме операционной системы
- ✓ Разрешение доверия к учетным записям компьютеров и пользователей при делегировании
- ✗ Разрешить вход в систему через службу удаленных рабочих столов
- ✓ Синхронизация данных службы каталогов
- ✓ Смена владельцев файлов и других объектов
- ✓ Создание аудитов безопасности
- ✓ Создание глобальных объектов
- ✓ Создание маркерного объекта
- ✓ Создание постоянных общих объектов
- ✓ Создание символических ссылок
- ✓ Создание файла подкачки
- ✗ Увеличение приоритета выполнения
- ✗ Увеличение рабочего набора процесса
- ✗ Управление аудитом и журналом безопасности

✗ **2.2 Параметры безопасности**

- ✓ Аудит: Аудит доступа глобальных системных объектов
- ✓ Аудит: Аудит прав на архивацию и восстановление
- ✓ Аудит: Немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности
- ✗ Аудит: Принудительно переопределяет параметры категории политики аудита параметрами подкатегории политики аудита (Windows Vista или следующей версии)
- ✓ Доступ к сети: Разрешить трансляцию анонимного SID в имя
- ✓ Завершение работы: Очистка файла подкачки виртуальной памяти
- ✗ Завершение работы: Разрешить завершение работы системы без выполнения входа в систему
- ✗ Интерактивный вход в систему: Поведение при извлечении смарт-карты
- ✗ Интерактивный вход в систему: Количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)
- ✗ Интерактивный вход в систему: Напоминать пользователям об истечении срока действия пароля заранее
- ✗ Интерактивный вход в систему: Не отображать последнее имя пользователя
- ✗ Интерактивный вход в систему: Не требовать нажатия CTRL+ALT+DEL
- ✗ Интерактивный вход в систему: Требовать проверки на контроллере домена для отмены блокировки компьютера
- ✗ Клиент сети Microsoft: Использовать цифровую подпись (всегда)
- ✓ Клиент сети Microsoft: Использовать цифровую подпись (с согласия сервера)
- ✓ Клиент сети Microsoft: Посылать незашифрованный пароль сторонним SMB-серверам
- ✓ Консоль восстановления: Разрешить автоматический вход администратора
- ✓ Консоль восстановления: Разрешить копирование дискет и доступ ко всем дискам и папкам

- ✗ Контроллер домена: Запретить изменение пароля учетных записей компьютера
- ✗ Контроль учетных записей: Все администраторы работают в режиме одобрения администратором
- ✓ Контроль учетных записей: Обнаружение установки приложений и запрос на повышение прав
- ✗ Контроль учетных записей: Переключение к безопасному рабочему столу при выполнении запроса на повышение прав
- ✗ Контроль учетных записей: Поведение запроса на повышение прав для администраторов в режиме одобрения администратором
- ✗ Контроль учетных записей: Поведение запроса на повышение прав для обычных пользователей
- ✓ Контроль учетных записей: Повышать права для UIAccess-приложений только при установке в безопасных местах
- ✓ Контроль учетных записей: Повышение прав только для подписанных и проверенных исполняемых файлов
- ✓ Контроль учетных записей: При сбоях записи в файл или реестр виртуализация в размещение пользователя
- ✓ Контроль учетных записей: Разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол
- ✗ Контроль учетных записей: Режим одобрения администратором для встроенной учетной записи администратора
- ✗ Сервер сети Microsoft: Использовать цифровую подпись (всегда)
- ✗ Сервер сети Microsoft: Использовать цифровую подпись (с согласия клиента)
- ✓ Сервер сети Microsoft: Время бездействия до приостановки сеанса
- ✓ Сервер сети Microsoft: Отключать клиентов по истечении разрешенных часов входа
- ✓ Сетевая безопасность: Не хранить хеш-значение LAN Manager при следующей смене пароля
- ✗ Сетевая безопасность: Разрешить LocalSystem использовать нулевые сеансы
- ✗ Сетевая безопасность: Разрешить использование сетевых удостоверений в запросах проверки подлинности PKU2U к этому компьютеру
- ✗ Сетевая безопасность: Разрешить учетной записи локальной системы использовать удостоверение компьютера для NTLM
- ✓ Сетевая безопасность: Требование цифровой подписи для LDAP-клиента
- ✗ Сетевая безопасность: Минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)
- ✗ Сетевая безопасность: Минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)
- ✗ Сетевая безопасность: Уровень проверки подлинности LAN Manager
- ✓ Сетевой доступ: Запретить анонимный доступ к именованным каналам и общим ресурсам
- ✓ Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей
- ✓ Сетевой доступ: Не разрешать перечисление учетных записей SAM анонимными пользователями
- ✗ Сетевой доступ: Не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями
- ✓ Сетевой доступ: Не разрешать хранение паролей или учетных данных для сетевой проверки подлинности
- ✓ Сетевой доступ: Разрешать анонимный доступ к именованным каналам
- ✗ Сетевой доступ: разрешать анонимный доступ к общим ресурсам
- ✓ Сетевой доступ: Разрешать применение разрешений "Для всех" к анонимным пользователям
- ✓ Сетевой доступ: Удаленно доступные пути и вложенные пути реестра
- ✓ Сетевой доступ: Удаленно доступные пути реестра
- ✗ Сетевой сервер (Майкрософт): уровень проверки сервером имени участника-службы конечного объекта
- ✗ Системная криптография: обязательное применение сильной защиты ключей пользователей, хранящихся на компьютере
- ✓ Системные объекты: Усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок)
- ✓ Системные объекты: Учитывать регистр для подсистем, отличных от Windows
- ✗ Устройства: Запретить пользователям установку драйверов принтера
- ✗ Устройства: Разрешить доступ к дисководам гибких дисков только локальным пользователям
- ✗ Устройства: Разрешить доступ к дисководам компакт-дисков только локальным пользователям
- ✗ Устройства: Разрешить форматирование и извлечение съемных носителей
- ✗ Учетные записи: Переименование учетной записи администратора
- ✗ Учетные записи: Переименование учетной записи гостя
- ✓ Учетные записи: Разрешить использование пустых паролей только при консольном входе

- Учетные записи: Состояние учетной записи 'Администратор'
- Учетные записи: Состояние учетной записи 'Гость'
- Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания
- Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала
- Член домена: Максимальный срок действия пароля учетных записей компьютера
- Член домена: Отключить изменение пароля учетных записей компьютера
- Член домена: Требовать стойкий ключ сеанса (Windows 2000 или выше)
- Член домена: Цифровая подпись данных безопасного канала, когда это возможно
- Член домена: Шифрование данных безопасного канала, когда это возможно

2.3 Политики аудита

2.3.1 Вход учетной записи

- Аудит проверки учетных данных
- Аудит службы проверки подлинности Kerberos
- Аудит операции с билетами службы Kerberos
- Аудит других событий входа учетных записей

2.3.2 Управление учетными записями

- Аудит управления группами приложений
- Аудит управления учетными записями компьютеров
- Аудит управления группами распространения
- Аудит других событий управления учетными записями
- Аудит управления группами безопасности
- Аудит управления учетными записями пользователей

2.3.3 Подробное отслеживание

- Аудит активности DPAPI
- Аудит создания процессов
- Аудит завершения процессов
- Аудит событий RPC

3.2.4. Доступ к службе каталогов (DS)

- Аудит подробной репликации службы каталогов
- Аудит доступа к службе каталогов
- Аудит изменения службы каталогов
- Аудит репликации службы каталогов

2.3.5 События входа и выхода из системы

- Аудит блокировки учетных записей
- Аудит расширенного режима IPsec
- Аудит основного режима IPsec
- Аудит быстрого режима IPsec
- Аудит выхода из системы
- Аудит входа в систему
- Аудит сервера политики сети
- Аудит других событий входа и выхода
- Аудит специального входа

2.3.6 Доступ к объектам

- Аудит событий, создаваемых приложениями
- Аудит службы сертификации
- Аудит сведений об общем файловом ресурсе

- ✗ Аудит общих папок
- ✓ Аудит файловой системы
- ✓ Аудит подключения платформы фильтрации
- ✓ Аудит отбрасывания пакетов платформой фильтрации
- ✓ Аудит работы с дескрипторами
- ✓ Аудит объектов ядра
- ✗ Аудит других событий доступа к объектам
- ✓ Аудит реестра
- ✓ Аудит диспетчера учетных записей безопасности

✗ **2.3.7 Изменение политики**

- ✗ Аудит изменения политики аудита
- ✗ Аудит изменения политики проверки подлинности
- ✓ Аудит изменения политики авторизации
- ✓ Аудит изменения политики платформы фильтрации
- ✓ Аудит изменения политики на уровне правил MPSSVC
- ✓ Аудит других событий изменения политики

✗ **2.3.8 Использование прав**

- ✓ Аудит использования прав, не затрагивающих конфиденциальные данные
- ✗ Аудит других событий использования прав
- ✓ Аудит использования прав, затрагивающих конфиденциальные данные

✗ **2.3.9 Система**

- ✗ Аудит драйвера IPsec
- ✓ Аудит других системных событий
- ✗ Аудит изменения состояния безопасности
- ✗ Аудит расширения системы безопасности
- ✗ Аудит целостности системы

✗ **2.4 Политики домена**

✗ **2.4.1 Политика паролей**

- ✗ Вести журнал паролей
- ✓ Максимальный срок действия пароля
- ✗ Минимальная длина пароля
- ✓ Минимальный срок действия пароля
- ✗ Пароль должен отвечать требованиям сложности
- ✓ Хранить пароли, используя обратимое шифрование

✗ **2.4.2 Политика блокировки учетной записи**

- ✓ Время до сброса счетчика блокировки
- ✗ Пороговое значение блокировки
- ✓ Продолжительность блокировки учетной записи

Описание параметров

Группа

Название **2 Параметры политики компьютеров**

Описание

Все параметры.

Группа

Название **2.1 Назначение прав пользователя**

Описание

Параметры безопасности, описанные в этом разделе, применяются к компьютерам домена. Они принадлежат узлу Конфигурация компьютера редактора объектов групповой политики и сгруппированы в дочерние узлы Конфигурация Windows и Административные шаблоны.

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Архивация файлов и каталогов**

Описание

Эталонное значение: **Администраторы**

Это право пользователя определяет, какие пользователи могут игнорировать разрешения для файлов, каталогов, реестра и других постоянных объектов с целью архивации системы. В частности, это право пользователя подобно предоставлению следующих разрешений пользователю или группе для всех папок и файлов в системе: Обзор папок/Выполнение файлов Содержимое папки/Чтение данных Чтение атрибутов Чтение расширенных атрибутов Чтение разрешений Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Поскольку невозможно точно знать, что именно пользователь делает с данными - создает архив, крадет или копирует с целью распространения - назначайте это право только доверенным пользователям. По умолчанию на рабочих станциях и серверах: Администраторы Операторы архивации. По умолчанию на контроллерах домена: Администраторы Операторы архивации Операторы сервера

Источники

CCE-9389-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9389-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Блокировка страниц в памяти**

Описание

Эталонное значение: **Никто**

Этот параметр безопасности определяет, какие учетные записи могут использовать процессы для сохранения данных в физической памяти для предотвращения сброса этих данных в виртуальную память на диске. Применение этой привилегии может существенно повлиять на производительность системы, снижая объем доступной оперативной памяти (RAM). По умолчанию: нет.

Источники

CCE-9289-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9289-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Восстановление файлов и каталогов**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет пользователей, которые могут обойти разрешения на файлы, каталоги, реестр и другие постоянные объекты при восстановлении архивных копий файлов и каталогов, а также пользователей, которые могут назначить любого действительного субъекта безопасности владельцем объекта. В частности, это право пользователя подобно предоставлению следующих разрешений пользователю или группе для всех папок и файлов в системе: Обзор папок/Выполнение файлов Запись Внимание! Назначение этого права пользователя может представлять угрозу безопасности. Так как оно дает возможность перезаписывать параметры реестра, скрывать данные и получать во владение системные объекты, назначать его следует только доверенным пользователям. По умолчанию: Рабочие станции и серверы: Администраторы, Операторы архивации. Контроллеры домена: Администраторы, Операторы архивации, Операторы сервера.

Источники

CCE-9124-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9289-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Вход в качестве пакетного задания**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности позволяет пользователю входить в систему при помощи средства, использующего очередь пакетных заданий, и предоставляется только для совместимости с предыдущими версиями Windows. Например, если пользователь передает задание при помощи планировщика заданий, последний регистрирует этого пользователя в системе как пользователя с пакетным входом, а не как интерактивного пользователя. По умолчанию: Администраторы Операторы архивации.

Источники

CCE-9320-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9320-3&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Вход в качестве службы**

Описание

Эталонное значение: **Никто**

Этот параметр безопасности разрешает субъекту безопасности входить в систему в качестве службы. Службы можно настроить для запуска под учетными записями "Локальная система", "Локальная служба" или "Сетевая служба", встроенными в право для входа в систему в качестве службы. Это право требуется назначить любой службе, которая выполняется под отдельной учетной записью пользователя. По умолчанию: нет.

Источники

CCE-9461-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9461-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Выполнение задач по обслуживанию томов**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет пользователей и группы, которые могут выполнять задачи по обслуживанию томов, например, удаленную дефрагментацию. При назначении этого права пользователя следует соблюдать осторожность. Пользователи, имеющие данное право, могут просматривать диски и добавлять файлы в память, занятую другими данными. После открытия дополнительных файлов пользователь может читать изменять запрошенные данные. По умолчанию: Администраторы.

Источники

CCE-8475-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8475-6&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Добавление рабочих станций к домену**

Описание

Эталонное значение: **Никто**

Этот параметр безопасности определяет, какие группы или пользователи могут добавлять рабочие станции в домен. Этот параметр безопасности действителен только на контроллерах домена. По умолчанию любой пользователь, прошедший проверку подлинности, имеет такие права и может создать до 10 учетных записей компьютеров в домене. Добавление учетной записи компьютера к домену позволяет компьютеру работать в сетях на основе Active Directory. Например, добавление рабочей станции к домену позволяет этой рабочей станции распознавать учетные записи и группы, существующие в Active Directory. По умолчанию: пользователи, прошедшие проверку подлинности, на контроллерах домена. Примечание. Пользователи, имеющие разрешение на создание объектов-компьютеров в контейнере компьютеров Active Directory, также могут создавать учетные записи компьютеров в домене. Различие состоит в том, что возможность создания для пользователей с разрешениями для контейнера не ограничена всего 10 учетными записями компьютеров. При этом собственниками учетных записей компьютеров, созданных посредством добавления рабочих станций к домену, являются администраторы домена, в то время как собственниками учетных записей компьютеров, созданных с помощью разрешений для контейнера компьютеров, являются создатели этих учетных записей. Если у пользователя есть разрешения для контейнера, а также права на добавление рабочих станций в домен, то компьютер добавляется на основе разрешений для контейнера компьютеров, а не прав пользователя.

Источники

CCE-10636-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10636-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Доступ к диспетчеру учетных данных от имени доверенного вызывающего**

Описание

Эталонное значение: **Никто**

Этот параметр используется диспетчером учетных данных в ходе архивации и восстановления. Эта привилегия не должна предоставляться учетным записям, поскольку она предоставляется только Winlogon. Сохраненные пользователями учетные данные могут быть скомпрометированы, если эта привилегия предоставляется другим субъектам.

Источники

CCE-9380-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9380-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Доступ к компьютеру из сети**

Описание

Эталонное значение: **Пользователи, Администраторы**

Это право пользователя определяет пользователей и группы, которым разрешено подключаться к компьютеру по сети. Это право пользователя не влияет на службы удаленных рабочих столов. Примечание. Старое название служб удаленных рабочих столов в предыдущих версиях Windows Server - "службы терминалов". Значения по умолчанию на

рабочих станциях и серверах: Администраторы Операторы архивации Пользователи Все Значения по умолчанию на контроллерах домена: Администраторы Проверенные пользователи Контроллеры домена предприятия Все Доступ, совместимый с версиями, предшествующими Windows 2000.

Источники

CCE-9124-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9124-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Завершение работы системы**

Описание

Эталонное значение: **Администраторы, Пользователи**

Этот параметр безопасности определяет пользователей, которые после локального входа в систему могут завершить работу операционной системы при помощи команды "Завершить работу". Неправильное применение этого права пользователя может стать причиной отказа в обслуживании. По умолчанию на рабочих станциях: Администраторы, Операторы архивации, Пользователи. По умолчанию на серверах: Администраторы, Операторы архивации. По умолчанию на контроллерах домена: Администраторы, Операторы архивации, Операторы сервера, Операторы печати.

Источники

CCE-9014-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9014-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Загрузка и выгрузка драйверов устройств**

Описание

Эталонное значение: **Администраторы**

Это право пользователя определяет, какие пользователи могут динамически загружать и выгружать драйверы устройств или другой код в режиме ядра. Это право пользователя не применяется к драйверам устройств Plug and Play. Не рекомендуется назначать эту привилегию другим пользователям. Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Не назначайте это право пользователю, группе или процессу, которым нежелательно позволять управлять системой. По умолчанию на рабочих станциях и серверах: Администраторы. По умолчанию на контроллерах домена: Администраторы Операторы печати

Источники

CCE-9135-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9135-5&platform=win7

Ссылки

Ресурс

Тип	GPO

Источник Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Замена маркера уровня процесса**

Описание

Эталонное значение: **Local Service, Network Service**

Этот параметр безопасности определяет учетные записи пользователей, которые могут вызывать процедуру API-интерфейса CreateProcessAsUser() для того, чтобы одна служба могла запускать другую. Планировщик заданий - это пример процесса, использующего данное право пользователя. По умолчанию: Сетевая служба, Локальная служба.

Источники

CCE-8732-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8732-0&platform=win7

Ссылки

Ресурс
Тип GPO
Источник Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Низкий

Название **Запретить вход в систему через службу удаленных рабочих столов**

Описание

Эталонное значение: **Все**

Запретить вход в систему через службы удаленных рабочих столов Этот параметр безопасности определяет, каким пользователям и группам будет запрещено входить в систему как клиенту служб удаленных рабочих столов. Значение по умолчанию: нет. Внимание! Этот параметр не действует на компьютерах, работающих под управлением Windows 2000 без пакета обновлений 2 (SP2).

Источники

CCE-9274-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9274-2&platform=win7

Ссылки

Ресурс
Тип GPO
Источник Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Запретить локальный вход**

Описание

Эталонное значение: **Гости**

Этот параметр безопасности определяет, каким пользователям будет отказано во входе в систему. Этот параметр политики заменяет параметр "Разрешить локальный вход в систему", если к учетной записи применяются обе политики. Внимание! Если этот параметр безопасности применяется к группе "Все", никто не сможет войти в систему локально. По умолчанию: нет.

Источники

CCE-9239-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9239-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Изменение метки объекта**

Описание

Эталонное значение: **Никто**

Эта привилегия определяет, каким учетным записям пользователей разрешается изменять метки целостности объектов, таких как файлы, разделы реестра или процессы, владельцами которых являются другие пользователи. Процессы, выполняющиеся под учетной записью пользователя, без этой привилегии могут понижать уровень метки объекта, владельцем которого является данный пользователь. По умолчанию: Нет.

Источники

CCE-9149-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9149-6&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Изменение параметров среды изготовителя**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет, кто может изменять значения параметров аппаратной среды. Переменные аппаратной среды - это параметры, сохраняемые в энергонезависимой памяти компьютеров, архитектура которых отлична от x86. Действие параметра зависит от процессора. На компьютерах архитектуры x86 единственное значение аппаратной среды, которое можно изменить назначением данного права пользователя, - это параметр "Последняя удачная конфигурация", который должен изменяться только системой. В компьютерах на базе процессоров Itanium загрузочные данные хранятся в энергонезависимой памяти. Данное право пользователя должно назначаться пользователям для выполнения программы bootcfg.exe и изменения параметра "Операционная система по умолчанию" компонента "Загрузка и восстановление" диалогового окна свойств системы. На всех компьютерах это право пользователя требуется для установки и обновления Windows. Примечание. Этот параметр безопасности не влияет на пользователей, которые могут изменять системные и пользовательские переменные среды, отображаемые на вкладке "Дополнительно" диалогового окна свойств системы. По умолчанию: Администраторы.

Источники

CCE-9417-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9417-7&platform=win7

Ссылки

Ресурс

Тип	GPO

Источник Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Изменение системного времени**

Описание

Эталонное значение: **Local Service, Администраторы**

Это право пользователя определяет, какие пользователи и группы могут изменять время и дату внутренних часов компьютера. Пользователи с данным правом могут влиять на вид журналов событий. Если системное время было изменено, записи отслеженных событий отразят новое время, а не действительное время совершения событий. Это право пользователя определено в объекте групповой политики контроллеров домена по умолчанию и в локальной политике безопасности рабочих станций и серверов. По умолчанию на рабочих станциях и серверах: Администраторы Локальная служба По умолчанию на контроллерах домена: Администраторы Операторы сервера Локальная служба.

Источники

CCE-8612-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8612-4&platform=win7

Ссылки

Ресурс
Тип GPO
Источник Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Изменение часового пояса**

Описание

Эталонное значение: **Local Service, Администраторы, Пользователи**

Это пользовательское право определяет, какие пользователи и группы могут изменять часовой пояс, используемый компьютером для отображения местного времени, которое представляет собой сумму системного времени компьютера и смещения часового пояса. Само по себе системное время является абсолютным и не изменяется при изменении часового пояса. Это право пользователя определено в объекте групповой политики контроллера домена по умолчанию и в локальной политике безопасности рабочих станций и серверов. По умолчанию: Администраторы, Пользователи Имитация клиента после проверки подлинности Выдача пользователю этой привилегии позволяет программам, выполняемым от имени этого пользователя, олицетворять клиента. Требование этого права для подобного олицетворения не позволяет неавторизованному пользователю убедить клиента подключиться (например, через вызов удаленной процедуры (RPC) или именованные каналы) к созданной им службе, а затем олицетворить клиента, что даст возможность повысить его полномочия до административного или системного уровня. Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Назначайте такие права только доверенным пользователям. По умолчанию: Администраторы Локальная служба Сетевая служба Служба Примечание. По умолчанию к токенам доступа служб, запущенных диспетчером управления службами, добавляется встроенная группа "Служба". Встроенная группа "Служба" также добавляется к токенам доступа COM-серверов, запущенных COM-инфраструктурой и настроенных на выполнение под определенной учетной записью. Поэтому данные службы получают это пользовательское право при запуске. Кроме того, пользователь может олицетворять токен доступа и при выполнении любого из следующих условий. Олицетворяемый токен доступа назначен данному пользователю. В данном сеансе входа пользователь создал токен доступа, явно указав учетные данные при входе. Запрошенный уровень ниже, чем "Олицетворять", например: "Анонимный" или "Идентифицировать". Поэтому пользователям обычно не требуется это пользовательское право. Внимание! Включение этого параметра может привести к потере привилегии "Олицетворять" программами, имеющим эту привилегию, и заблокировать их выполнение.

Источники

CCE-8423-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8423-6&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Имитация клиента после проверки подлинности**

Описание

Эталонное значение: **Администраторы, SERVICE, Local Service, Network Service**

Выдача пользователю этой привилегии позволяет программам, выполняемым от имени этого пользователя, олицетворять клиента. Требование этого права для подобного олицетворения не позволяет неавторизованному пользователю убедить клиента подключиться (например, через вызов удаленной процедуры (RPC) или именованные каналы) к созданной им службе, а затем олицетворить клиента, что даст возможность повысить его полномочия до административного или системного уровня. Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Назначайте такие права только доверенным пользователям. По умолчанию: Администраторы Локальная служба Сетевая служба Служба Примечание. По умолчанию к токенам доступа служб, запущенных диспетчером управления службами, добавляется встроенная группа "Служба". Встроенная группа "Служба" также добавляется к токенам доступа COM-серверов, запущенных COM-инфраструктурой и настроенных на выполнение под определенной учетной записью. Поэтому данные службы получают это пользовательское право при запуске. Кроме того, пользователь может олицетворять токен доступа и при выполнении любого из следующих условий. Олицетворяемый токен доступа назначен данному пользователю. В данном сеансе входа пользователь создал токен доступа, явно указав учетные данные при входе. Запрошенный уровень ниже, чем "Олицетворять", например: "Анонимный" или "Идентифицировать". Поэтому пользователям обычно не требуется это пользовательское право. Внимание! Включение этого параметра может привести к потере привилегии "Олицетворять" программами, имеющим эту привилегию, и заблокировать их выполнение.

Источники

CCE-8467-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8467-3&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Локальный вход в систему**

Описание

Эталонное значение: **Администраторы, Пользователи**

Определяет пользователей, которые могут входить на данный компьютер. Внимание! Изменение этого параметра может повлиять на совместимость с клиентами, службами и приложениями. По умолчанию: •На рабочих станциях и серверах: Администраторы, Операторы архивации, Пользователи и Гости. •На контроллерах домена: Операторы учетных записей, Администраторы, Операторы архивации и Операторы печати.

Источники

CCE-9345-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9345-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Настройка квот памяти для процесса**

Описание

Эталонное значение: **Администраторы, Local Service, Network Service**

Это право определяет, кто может изменять максимальный объем памяти, используемый процессом. Это право пользователя определено в объекте групповой политики контроллера домена по умолчанию и в локальной политике безопасности рабочих станций и серверов. Примечание. Это право полезно при настройке системы, но его использование может нанести вред в случае, например, атак типа "отказ в обслуживании". По умолчанию: Администраторы Локальная служба Сетевая служба.

Источники

CCE-9068-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9068-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Обход перекрестной проверки**

Описание

Эталонное значение: **Пользователи, Network Service, Local Service, Администраторы**

Это право пользователя определяет, какие пользователи могут производить обзор деревьев каталога, даже если у этих пользователей отсутствуют разрешения на каталог. Это право не позволяет пользователям просматривать содержимое каталога, а позволяет только выполнять обзор. Это право пользователя определено в объекте групповой политики контроллеров домена по умолчанию и в локальной политике безопасности рабочих станций и серверов. По умолчанию на рабочих станциях и серверах: Администраторы Операторы архивации Пользователи Все Локальная служба Сетевая служба По умолчанию на контроллерах домена: Администраторы Проверенные пользователи Все Локальная служба Сетевая служба Доступ, совместимый с пред-Windows 2000

Источники

CCE-8414-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8414-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Отказать в доступе к этому компьютеру из сети**

Описание

Эталонное значение: **Гости**

Этот параметр безопасности определяет, каким пользователям будет отказано в доступе к компьютеру из сети. Этот параметр заменяет параметр политики "Разрешить доступ к компьютеру из сети", если к учетной записи пользователя применяются об политики. По умолчанию: Гость.

Источники

CCE-9244-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9244-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Отказать во входе в качестве пакетного задания**

Описание

Эталонное значение: **Гости**

Этот параметр безопасности определяет, каким учетным записям будет отказано во входе в систему в виде пакетного задания. Данный параметр замещает параметр "Разрешить вход в систему как пакетному заданию", если к учетной записи пользователя применяются оба параметра. По умолчанию: Отсутствует.

Источники

CCE-9212-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9212-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Низкий

Название **Отключение компьютера от стыковочного узла**

Описание

Эталонное значение: **Администраторы, Пользователи**

Этот параметр безопасности определяет, может ли пользователь отстыковать портативный компьютер от стыковочного узла без входа в систему. Если данный параметр включен, пользователь перед отключением портативного компьютера от стыковочного узла должен войти в систему. Если данный параметр отключен, пользователь может отключить портативный компьютер от стыковочного узла без входа в систему. По умолчанию: Администраторы, Опытные пользователи, Пользователи.

Источники

CCE-9326-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9326-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Отладка программ**

Описание

Эталонное значение: **Никто**

Это право пользователя определяет, какие пользователи могут подключать отладчик к любому процессу или ядру. то право не нужно назначать разработчикам, выполняющим отладку собственных приложений. Оно потребуется разработчикам для отладки новых системных компонентов. Это право пользователя обеспечивает полный доступ к важным компонентам операционной системы. Внимание! Назначение этого права пользователя может представлять угрозу безопасности. Назначайте его только доверенным пользователям. По умолчанию: Администраторы.

Источники

CCE-8583-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8583-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Принудительное удаленное завершение работы**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет, каким пользователям разрешено удаленное завершение работы компьютера. Неправильное применение этого права пользователя может стать причиной отказа в обслуживании. Это право пользователя определено в объекте групповой политики контроллеров домена по умолчанию и в локальной политике безопасности рабочих станций и серверов. По умолчанию: На рабочих станциях и серверах: Администраторы. На контроллерах домена: Администраторы, Операторы сервера.

Источники

CCE-9336-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9336-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Профилирование одного процесса**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет пользователей, которые могут использовать средства мониторинга производительности для отслеживания производительности несистемных процессов. По умолчанию: Администраторы, Опытные пользователи.

Источники

CCE-9388-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9388-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Профилирование производительности системы**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет пользователей, которые могут использовать средства мониторинга производительности для отслеживания производительности системных процессов. По умолчанию: администраторы.

Источники

CCE-9419-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9419-3&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Работа в режиме операционной системы**

Описание

Эталонное значение: **Никто**

Это право пользователя позволяет процессу олицетворять любого пользователя без проверки подлинности. Процесс, таким образом, может получать доступ к тем же локальным ресурсам, что и пользователь. Процессы, для которых требуется такое право, должны использовать уже содержащую это право учетную запись LocalSystem, а не отдельную учетную запись пользователя с этим правом. Если в организации используются только серверы с операционными системами семейства Windows Server 2003, нет необходимости назначать эти права пользователям. Однако если в организации используются серверы под управлением операционных систем Windows 2000 или Windows NT 4.0, назначение этих прав может потребоваться для использования приложений, обменивающихся паролями в обычном текстовом формате. Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Назначайте такие права только доверенным пользователям. По умолчанию: Нет.

Источники

CCE-9407-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9407-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Разрешение доверия к учетным записям компьютеров и пользователей при делегировании**

Описание

Эталонное значение: **Никто**

Этот параметр безопасности определяет, какие пользователи могут устанавливать параметр "Делегирование разрешено" для пользователя или объекта компьютера. Пользователь или объект, получившие это право, должны иметь доступ на запись к управляющим флагам учетной записи пользователя или объекта компьютера. Серверный процесс, выполняемый на компьютере (или в пользовательском контексте), которому разрешено делегирование, может получить доступ к ресурсам другого компьютера, используя делегированные учетные данные клиента, пока в учетной записи клиента не будет установлен управляющий флаг "Учетная запись не может быть делегирована". Это право пользователя определено в объекте групповой политики контроллера домена по умолчанию и в локальной политике безопасности рабочих станций и серверов. Внимание! Неправильное применение этого права пользователя или параметра "Делегирование разрешено" может сделать сеть уязвимой к изощренным атакам с помощью троянских программ, которые имитируют входящих клиентов и используют их учетные данные для получения доступа к сетевым ресурсам. По умолчанию: администраторы на контроллерах домена.

Источники

CCE-8930-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8930-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Разрешить вход в систему через службу удаленных рабочих столов**

Описание

Эталонное значение: **Никто**

Этот параметр безопасности определяет, какие пользователи или группы имеют право входа в систему в качестве клиента служб удаленных рабочих столов. Значения по умолчанию: На рабочих станциях и серверах: Администраторы; Пользователи удаленного рабочего стола. На контроллерах домена: Администраторы. Внимание! Этот параметр не действует на компьютерах с Windows 2000 без установленного пакета обновления 2 (SP2).

Источники

CCE-9107-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9107-4&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Синхронизация данных службы каталогов**

Описание

Эталонное значение: **Никто**

Этот параметр безопасности определяет пользователей и группы, которые имеют право синхронизировать все данные службы каталогов. Это также называется синхронизацией Active Directory. По умолчанию: нет.

Источники

CCE-10251-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10251-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Смена владельцев файлов и других объектов**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет пользователей, которые могут стать владельцем любого защищаемого объекта системы, в том числе: объектов Active Directory, файлов и папок, принтеров, разделов реестра, процессов и потоков. Внимание! Назначение этого права пользователя может представлять угрозу безопасности. Так как объекты полностью контролируются их владельцами, назначать данное право следует только доверенным пользователям. По умолчанию: Администраторы.

Источники

CCE-9309-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9309-6&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Создание аудитов безопасности**

Описание

Эталонное значение: **Local Service, Network Service**

Этот параметр безопасности определяет, какие учетные записи могут быть использованы процессом для добавления записей в журнал безопасности. Журнал безопасности используется для отслеживания несанкционированного доступа в систему. Неправильное применение этого права пользователя может стать причиной формирования множества событий аудита, которые могут скрыть свидетельства атаки или вызвать отказ в обслуживании, если включен параметр безопасности "Аудит: немедленно завершить работу системы при невозможности протоколирования аудита безопасности". По умолчанию: Локальная служба Сетевая служба.

Источники

CCE-9226-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9226-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Создание глобальных объектов**

Описание

Эталонное значение: **Администраторы, SERVICE, Local Service, Network Service**

Этот параметр безопасности определяет, могут ли пользователи создавать глобальные объекты, доступные для всех сеансов. Пользователи по-прежнему могут создавать отдельные объекты для их сеансов, не имея данного права. Создание глобальных объектов может влиять на процессы, выполняемые в сеансах других пользователей, ведя к ошибкам приложений и повреждению данных. Внимание! Назначение этого права пользователя может представлять угрозу безопасности. Назначайте его только доверенным пользователям. По умолчанию: Администраторы Локальная служба Сетевая служба Служба.

Источники

CCE-8431-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8431-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Создание маркерного объекта**

Описание

Эталонное значение: **Никто**

Этот параметр безопасности определяет, какие учетные записи могут быть использованы процессами для создания маркеров, которые затем могут быть использованы для получения доступа к любым локальным ресурсам, если для создания маркера доступа процесс использует внутренний интерфейс (API). Данное право используется операционной системой для внутренних целей. Если нет необходимости, не предоставляйте это право никаким пользователям, группам или процессам кроме пользователя "Локальная система". Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Не назначайте это право пользователю, группе или процессу, которым нежелательно позволять управлять системой. По умолчанию: нет.

Источники

CCE-9215-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9215-5 &platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Создание постоянных общих объектов**

Описание

Эталонное значение: **Никто**

Это право пользователя определяет, какие учетные записи могут использоваться процессами для создания объекта каталога при помощи диспетчера объектов. Это право пользователя используется внутри операционной системы и полезно для компонентов в режиме ядра, расширяющих пространство имен объекта. Поскольку это право уже назначено компонентам, выполняющимся в режиме ядра, его не нужно специально назначать. По умолчанию: нет.

Источники

CCE-9254-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9254-4&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Создание символических ссылок**

Описание

Эталонное значение: **Администраторы**

Создание символических ссылок Эта привилегия определяет для пользователя возможность создавать символические ссылки с компьютера, на который он вошел. По умолчанию: Администратор ВНИМАНИЕ! Эту привилегию следует предоставлять только доверенным пользователям. Символические ссылки могут обнажить уязвимые места в приложениях, которые не рассчитаны на их обработку. Примечание Этот параметр можно использовать вместе с параметром символических ссылок файловой системы, задаваемой в программе командной строки для контроля типа символических ссылок, разрешенных на компьютере. Для получения дополнительных сведений о программе fsutil и символических ссылках введите в командной строке "fsutil behavior set symlinkevaluation /?".

Источники

CCE-8460-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8460-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Создание файла подкачки**

Описание

Эталонное значение: **Администраторы**

Это право определяет пользователей и группы, которые могут вызывать встроенный интерфейс API для создания и изменения размера файла подкачки. Это право используется операционной системой для внутренних целей и обычно не нуждается в назначении каким-либо пользователям. По умолчанию: Администраторы.

Источники

CCE-9185-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9185-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Увеличение приоритета выполнения**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет, какие учетные записи могут использовать процесс, имеющий право доступа "Запись свойства" для другого процесса, для повышения приоритета выполнения, назначенного другому процессу. Пользователь, имеющий данную привилегию, может изменять приоритет выполнения процесса через пользовательский интерфейс диспетчера задач. По умолчанию: Администраторы.

Источники

CCE-8999-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8999-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Средний

Название **Увеличение рабочего набора процесса**

Описание

Эталонное значение: **Администраторы, Local Service**

Эта привилегия определяет, какие учетные записи пользователей могут увеличивать и уменьшать размер рабочего набора процесса. По умолчанию: пользователи Рабочий набор процесса - это набор страниц памяти, видимых процессу в физической оперативной памяти. Эти страницы являются резидентными; приложение может обращаться к ним, не вызывая ошибки страниц. Минимальный и максимальный размер рабочего набора влияет на поведение страниц виртуальной памяти процесса. Внимание: увеличение размера рабочего набора процесса приводит к уменьшению объема физической памяти, доступной в остальной части системы.

Источники

CCE-9048-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9048-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Параметр Критичность: Высокий

Название **Управление аудитом и журналом безопасности**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет, какие пользователи могут указывать параметры аудита доступа к объектам для отдельных ресурсов, таких как файлы, объекты Active Directory и разделы реестра. Данный параметр безопасности не разрешает пользователю включить аудит доступа к файлам и объектам в целом. Для включения такого аудита нужно настроить параметр доступа к объекту "Аудит" в пути "Конфигурация компьютера\Параметры Windows\Параметры безопасности\Локальные политики\Политики аудита". События аудита можно просмотреть в журнале безопасности средства просмотра событий. Пользователь с данной привилегией может также просматривать и очищать журнал безопасности. По умолчанию: Администраторы.

Источники

CCE-9223-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9223-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя

Группа

Название **2.2 Параметры безопасности**

Описание

Параметры этого раздела, распространяемые на компьютеры под управлением Windows 7 с помощью групповой политики, позволяют включать или отключать возможности и компоненты операционной системы, например, доступ к гибким дискам, доступ к приводам компакт-дисков или запрос на вход в систему. Они также контролируют массу других вещей, например, цифровое подписание данных, имена учетных записей администратора и гостя и способ установки драйверов.

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Аудит: Аудит доступа глобальных системных объектов**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, будет ли выполняться аудит доступа к глобальным системным объектам. Если данный параметр включен, то системные объекты, такие как мьютексы (флаги взаимного исключения), события, семафоры (механизмы блокировки, используемые диспетчерами или распределителями ресурсов) и DOS-устройства, будут создаваться с системным списком управления доступом (SACL) по умолчанию. Список SACL присваивается только именованным объектам; списки SACL не поддерживают объекты, не имеющие имен. Если также включена политика доступа к объектам аудита, будет выполняться аудит доступа к этим системным объектам. Примечание. Изменения в настройке этого параметра безопасности вступят в силу только после перезагрузки Windows. По умолчанию: Отключено.

Источники

CCE-9150-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9150-4&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Аудит: Аудит прав на архивацию и восстановление**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, будет ли выполняться аудит использования всех прав пользователя, включая "Архивация и восстановление", если включен параметр "Выполнять аудит использования привилегий". Включение этого параметра, когда также включен параметр "Выполнять аудит использования привилегий", создает событие аудита для каждого файла, с которым выполнялись операции архивации или восстановления. Если эта политика отключена, аудит использования права "Архивация и восстановление" не выполняется даже при включенном параметре "Выполнять аудит использования привилегий". Примечание. Изменения в настройке этого параметра безопасности вступят в силу только после перезагрузки Windows. По умолчанию: Отключено.

Источники

CCE-8789-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8789-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Аудит: Немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, будет ли завершена работа системы при невозможности протоколирования событий безопасности. Если этот параметр безопасности включен, система будет остановлена при невозможности протоколирования аудита безопасности по любой причине. Обычно протоколирование событий становится невозможным при переполнении журнала аудита безопасности, а его метод сохранения определен либо как "Не затирать события", либо как "Затирать старые события по дням". Если журнал аудита безопасности переполнен, и существующая запись не может быть затерта, а данный параметр безопасности включен, возникнет следующая Stop-ошибка: STOP: C0000244 {Неудачная попытка аудита} Неудачная попытка выполнения аудита безопасности. Для восстановления администратор должен войти в систему, заархивировать (необязательно) и очистить журнал и, при желании, сбросить данный параметр. Пока данный параметр безопасности не будет сброшен, никто из пользователей, за исключением членов группы администраторов, не может войти в систему, даже если журнал безопасности не будет заполнен. Примечание. Изменения в настройке этого параметра безопасности вступят в силу только после перезагрузки Windows. По умолчанию: Отключено.

Источники

CCE-9463-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9463-1&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Аудит: Принудительно переопределяет параметры категории политики аудита параметрами подкатегории политики аудита (Windows Vista или следующей версии)**

Описание

Эталонное значение: **Включен**

Windows 7 и более поздние версии Windows позволяют точнее управлять политикой аудита при помощи подкатегорий политики аудита. Установка политики аудита на уровне категории переопределит новую функцию политики аудита подкатегории. Чтобы обеспечить управление политикой аудита при помощи подкатегорий без необходимости изменения

групповой политики, в Windows 7 и более поздних версиях предусмотрено новое значение реестра (SCENoApplyLegacyAuditPolicy), запрещающее применение политики аудита уровня категории из групповой политики и из средства администрирования "Локальная политика безопасности". Если установленная здесь политика аудита уровня категории не согласуется с формируемыми событиями, то причина может быть в том, что установлен этот раздел реестра. Значение по умолчанию: включен.

Источники

CCE-9432-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9432-6&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Доступ к сети: Разрешить трансляцию анонимного SID в имя**

Описание

Эталонное значение: **Отключен**

Этот параметр политики определяет, может ли анонимный пользователь запрашивать атрибуты идентификатора безопасности (SID) другого пользователя. Если эта политика включена, то анонимный пользователь может запросить идентификатор безопасности любого другого пользователя. Например, анонимный пользователь, знающий идентификатор безопасности администратора, может подключиться к компьютеру, на котором включена эта политика, и получить имя администратора. Данный параметр влияет как на преобразование идентификатора безопасности в имя, так и на обратное преобразование (имя в идентификатор безопасности). Если этот параметр политики отключен, анонимный пользователь не может запрашивать идентификатор безопасности другого пользователя. Значение по умолчанию на рабочих станциях и рядовых серверах: отключен. Значение по умолчанию на контроллерах домена, работающих под управлением Windows Server 2008 или более поздней версии: отключено. Значение по умолчанию на контроллерах домена, работающих под управлением Windows Server 2003 R2 или более ранней версии: включено.

Источники

CCE-9531-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9531-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Завершение работы: Очистка файла подкачки виртуальной памяти**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, будет ли выполняться очистка файла подкачки виртуальной памяти при завершении работы системы. Поддержка виртуальной памяти использует файл подкачки системы для выгрузки страниц памяти на диск, когда они не используются. Во время работы системы файл подкачки открыт операционной системой в монопольном режиме и хорошо защищен. Однако если система настроена так, что допускает загрузку других операционных систем, необходимо убедиться, что при завершении работы системы выполняется очистка ее файла подкачки. Это гарантирует, что уязвимые сведения из памяти процессов, которые могли попасть в файл подкачки, не станут доступны пользователям, получившим прямой несанкционированный доступ к этому файлу. Если эта политика включена, при корректном завершении работы системы выполняется очистка файла подкачки системы. Если этот параметр безопасности включен, также выполняется обнуление файла режима гибернации (hiberfil.sys), когда этот режим

отключен. По умолчанию: Отключено.

Источники

CCE-9222-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9222-1&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Завершение работы: Разрешить завершение работы системы без выполнения входа в систему**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, можно ли завершить работу компьютера, не выполняя вход в систему Windows. Если эта политика включена, команду "Завершение работы" можно выбрать на экране входа в Windows. Если эта политика отключена, команда "Завершение работы" не отображается на экране входа в Windows. В этом случае, чтобы завершить работу системы, пользователю необходимо успешно выполнить вход в систему, и он должен иметь право на завершение работы системы. По умолчанию на рабочих станциях: включен. По умолчанию на серверах: отключен.

Источники

CCE-9707-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9707-1&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Интерактивный вход в систему: Поведение при извлечении смарт-карты**

Описание

Эталонное значение: **Блокировка рабочей станции**

Этот параметр безопасности определяет, что происходит при извлечении смарт-карты вошедшего пользователя из устройства чтения смарт-карт. Возможные варианты: \x00F2 Нет действия \x00F2 Заблокировать рабочую станцию \x00F2 Принудительный выход из системы \x00F2 Отключение в случае удаленного сеанса служб удаленных рабочих столов При выборе пункта "Заблокировать рабочую станцию" в диалоговом окне свойств этого параметра при извлечении смарт-карты рабочая станция блокируется, что позволяет пользователям покидать рабочее место, забрав смарт-карту с собой, но оставляя открытым защищенный сеанс. При выборе пункта "Принудительный выход из системы" в диалоговом окне свойств этого параметра при извлечении смарт-карты выполняется автоматический выход из системы. При выборе пункта "Отключение в случае удаленного сеанса служб удаленных рабочих столов" при извлечении смарт-карты сеанс завершается без выхода пользователя из системы. Это позволяет пользователю вставить смарт-карту и возобновить сеанс позднее на том же компьютере либо на другом компьютере с устройством чтения смарт-карт без необходимости снова входить в систему. Если сеанс выполняется на локальном компьютере, тогда эта политика действует так же, как при блокировании рабочей станции. Примечание. Старое название служб удаленных рабочих столов в предыдущих версиях Windows Server - "службы терминалов". По умолчанию: данная политика не определена; это означает, что система рассматривает параметр как имеющий значение "Нет действия". В Windows Vista и более поздних версиях: чтобы этот параметр работал, должна быть запущена служба политики извлечения смарт-карт.

Источники

CCE-9067-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9067-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Интерактивный вход в систему: Количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)**

Описание

Эталонное значение: **0 входов**

Сведения о предыдущих входах пользователей в систему кэшируются локально, чтобы обеспечить последующий вход в систему в случае отсутствия доступа к контроллеру домена. При отсутствии доступа к контроллеру домена и кэшировании сведений о входах пользователей в систему пользователь получает следующее сообщение: Windows не смогла связаться с сервером для подтверждения данных входа в систему. Вход в систему произведен на основе сохраненных ранее данных входа. Если эти данные были изменены со времени последнего входа в систему на этом компьютере, эти изменения не будут отражены во время этого сеанса. При отсутствии доступа к контроллеру домена и отсутствии кэширования данных о входах пользователей в систему пользователь получает следующее сообщение: Не удалось выполнить вход в систему, поскольку домен (DOMAIN_NAME) недоступен. Значение этого параметра "0" отключает кэширование данных входа. При любом значении выше 50 кэшируется только 50 попыток входа в систему. Значение по умолчанию: 25

Источники

CCE-8487-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8487-1&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Интерактивный вход в систему: Напоминать пользователям об истечении срока действия пароля заранее**

Описание

Эталонное значение: **14 дней**

Определяет, за сколько дней пользователи предупреждаются об истечении срока действия пароля. Это предварительное предупреждение дает пользователю время на создание пароля достаточной стойкости. По умолчанию: 14 дней.

Источники

CCE-9307-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9307-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Интерактивный вход в систему: Не отображать последнее имя пользователя**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, будет ли в экране входа в Windows отображено имя последнего пользователя, выполнившего вход. Если эта политика включена, в диалоговом окне входа не будет отображаться имя последнего пользователя, выполнившего вход. Если эта политика отключена, отображается имя последнего пользователя, выполнившего вход. По умолчанию: Отключено.

Источники

CCE-9449-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9449-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Интерактивный вход в систему: Не требовать нажатия CTRL+ALT+DEL**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, требуется ли нажатие клавиш CTRL+ALT+DEL перед входом в систему. Если этот параметр включен, нажатие клавиш CTRL+ALT+DEL перед входом в систему не обязательно. Если нажатие клавиш CTRL+ALT+DEL перед входом в систему не обязательно, пользователи будут уязвимы для атак, в ходе которых производится попытка перехвата паролей. Обязательное нажатие клавиш CTRL+ALT+DEL перед входом в систему гарантирует, что пользователи пользуются доверенным каналом при вводе паролей. Если этот параметр отключен, нажатие клавиш CTRL+ALT+DEL перед входом в систему обязательно для любого пользователя (кроме случаев, когда для входа в систему Windows используется смарт-карта). По умолчанию на компьютерах домена: отключен. По умолчанию на изолированных рабочих станциях: включен.

Источники

CCE-9317-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9317-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Интерактивный вход в систему: Требовать проверки на контроллере домена для отмены блокировки компьютера**

Описание

Эталонное значение: **Включен**

Для разблокировки блокированного компьютера необходимо предоставить данные входа. Для учетных записей доменов этот параметр безопасности определяет, необходимо ли установить связь с контроллером домена для разблокировки компьютера. Если этот параметр отключен, пользователь может разблокировать компьютер с помощью кэшированных

учетных данных. Если этот параметр включен, используемая для разблокировки компьютера учетная запись домена должна быть проверена контроллером домена на подлинность. По умолчанию: Отключен. Внимание! Этот параметр применяется к компьютерам под управлением Windows 2000, но не доступен на них через диспетчер конфигурации безопасности.

Источники

CCE-8818-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8818-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Клиент сети Microsoft: Использовать цифровую подпись (всегда)**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, требуется ли компонентом клиента SMB цифровая подпись для пакетов. Протокол блоков сообщений сервера (SMB) предоставляет основу для совместного доступа Windows к файлам и принтерам, а также для других сетевых операций (например, для удаленного администрирования Windows). Для предотвращения атак с перехватом, когда SMB-пакеты изменяются при передаче, протокол SMB поддерживает установку цифровой подписи для SMB-пакетов. Этот параметр определяет, необходимо ли соглашение о подписи SMB-пакетов до разрешения дальнейшей связи с SMB-сервером. Если этот параметр включен, сетевой клиент Microsoft не будет соединяться с сетевым сервером Microsoft, если сервер не выдаст согласие на установку цифровой подписи для SMB-пакетов. Если этот параметр отключен, между клиентом и сервером устанавливается соглашение о подписи SMB-пакетов. По умолчанию: Отключен. Внимание! Чтобы этот параметр действовал для компьютеров под управлением Windows 2000, необходимо включить подписывание пакетов клиентской стороной. Чтобы включить подписывание SMB-пакетов клиентской стороной, установите параметр "Сетевой клиент Microsoft: использовать цифровую подпись (при согласии сервера)". Компьютеры с этим параметром не смогут соединяться с компьютерами, на которых не установлено подписывание пакетов со стороны сервера. По умолчанию установка цифровой подписи для пакетов разрешена только на контроллерах доменов под управлением Windows 2000 или более поздней версии. Подписывание пакетов со стороны сервера может быть разрешено на компьютерах под управлением Windows 2000 или более поздней версии установкой параметра "Сетевой сервер Microsoft: использовать цифровую подпись (при согласии сервера)" Подписывание пакетов сервером может быть разрешено на компьютерах под управлением Windows NT с пакетом обновления 3 или более поздней версии присвоением значения "1" следующему ключу реестра: HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature Подписывание пакетов сервером невозможно включить на компьютерах под управлением Windows 95 или Windows 98. Примечания Все операционные системы Windows поддерживают как клиентский, так и серверный компоненты SMB. Чтобы воспользоваться цифровой подписью SMB-пакетов, на участвующих в соединении клиентском и серверном SMB-компонентах должно быть включено подписывание SMB-пакетов или оно должно требоваться. В операционной системе Windows 2000 и более поздних версиях требование или включение подписи пакетов для клиентского и серверного SMB-компонентов управляется следующими четырьмя параметрами: Сетевой клиент Microsoft: использовать цифровую подпись (всегда) - Определяет, требуется ли на клиентском SMB-компоненте подписывание пакетов. Сетевой клиент Microsoft: использовать цифровую подпись (при согласии сервера) - Определяет, включено ли на клиентском SMB-компоненте подписывание пакетов. Сетевой сервер Microsoft: использовать цифровую подпись (всегда) - Определяет, требуется ли на серверном SMB-компоненте подписывание пакетов. Сетевой сервер Microsoft: использовать цифровую подпись (при согласии клиента) - Определяет, включено ли на серверном SMB-компоненте подписывание пакетов. Если на стороне сервера требуется подписывание пакетов, клиент не сможет установить сеанс связи с этим сервером, если не включено подписывание пакетов на стороне клиента. По умолчанию подписывание SMB-пакетов на стороне клиента включено на рабочих станциях, серверах и контроллерах домена. Аналогичным образом, если требуется подписывание SMB-пакетов на стороне клиента, клиент не сможет установить сеанс связи с сервером, на котором не включено подписывание пакетов. По умолчанию подписывание SMB-пакетов на стороне сервера включено только на контроллерах домена. Если включено подписывание SMB-пакетов на стороне сервера, подписывание будет согласовываться с клиентами, с включенным подписыванием SMB-пакетов на стороне клиента. Подписывание SMB-пакетов может привести к снижению производительности до 15 процентов при транзакциях службы файлов.

Источники

CCE-9327-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9327-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Клиент сети Microsoft: Использовать цифровую подпись (с согласия сервера)**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, пытается ли SMB-клиент согласовывать подписывание SMB-пакетов. Протокол блоков сообщений сервера (SMB) предоставляет основу для совместного доступа Windows к файлам и принтерам, а также для других сетевых операций (например, для удаленного администрирования Windows). Для предотвращения атак с перехватом, когда SMB-пакеты изменяются при передаче, протокол SMB поддерживает установку цифровой подписи для SMB-пакетов. Этот параметр безопасности определяет, пытается ли SMB-клиент производить согласование подписывания SMB-пакетов при подключении к SMB-серверу. Если этот параметр включен, сетевой клиент Microsoft будет требовать от сервера подписывания SMB-пакетов при установке сеанса связи. Если подписывание пакетов на этом сервере включено, будет проведено согласование подписывания пакетов. Если этот параметр отключен, SMB-клиент никогда не будет производить согласование подписывания SMB-пакетов. По умолчанию: Включен. Примечания Все операционные системы Windows поддерживают как клиентский, так и серверный компоненты SMB. Чтобы воспользоваться цифровой подписью SMB-пакетов, на участвующих в соединении клиентском и серверном SMB-компонентах должно быть включено подписывание SMB-пакетов или оно должно требоваться. В операционной системе Windows 2000 и более поздних версиях требование или включение подписи пакетов для клиентского и серверного SMB-компонентов управляется следующими параметрами: Сетевой клиент Microsoft: использовать цифровую подпись (всегда) - Определяет, требуется ли на клиентском SMB-компоненте подписывание пакетов. Сетевой клиент Microsoft: использовать цифровую подпись (при согласии сервера) - Определяет, включено ли на клиентском SMB-компоненте подписывание пакетов. Сетевой сервер Microsoft: использовать цифровую подпись (всегда) - Определяет, требуется ли на серверном SMB-компоненте подписывание пакетов. Сетевой сервер Microsoft: использовать цифровую подпись (при согласии клиента) - Определяет, включено ли на серверном SMB-компоненте подписывание пакетов. Если требуется подписывание SMB-пакетов на стороне сервера, клиент не сможет установить сеанс связи с этим сервером, если не включено подписывание SMB-пакетов на стороне клиента. По умолчанию подписывание SMB-пакетов на стороне клиента включено на рабочих станциях, серверах и контроллерах домена. Аналогичным образом, если требуется подписывание SMB-пакетов на стороне клиента, клиент не сможет установить сеанс связи с сервером, на котором не включено подписывание пакетов. По умолчанию подписывание SMB-пакетов на стороне сервера включено только на контроллерах домена. Если включено подписывание SMB-пакетов на стороне сервера, подписывание будет согласовываться с клиентами, с включенным подписыванием SMB-пакетов на стороне клиента. Подписывание SMB-пакетов может привести к снижению производительности до 15 процентов при транзакциях службы файлов.

Источники

CCE-9344-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9344-3&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Клиент сети Microsoft: Посылать незашифрованный пароль сторонним SMB-серверам**

Описание

Эталонное значение: **Отключен**

Если этот параметр безопасности включен, перенаправителю блока сообщений сервера (SMB) разрешено отправлять пароли открытым текстом на серверы SMB, не принадлежащие Майкрософт, которые не поддерживают шифрование паролей во время проверки подлинности. Отправка незашифрованных паролей представляет риск для безопасности. По умолчанию: Отключено.

Источники

CCE-9265-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9265-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Консоль восстановления: Разрешить автоматический вход администратора**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, нужно ли вводить пароль учетной записи администратора для получения доступа к системе. Если эта политика включена, консоль восстановления не будет требовать пароль от администратора — он автоматически войдет в систему.

Источники

CCE-8807-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8807-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Консоль восстановления: Разрешить копирование дискет и доступ ко всем дискам и папкам**

Описание

Эталонное значение: **Отключен**

При включении этого параметра безопасности становится доступной команда SET консоли восстановления, которая позволяет задать следующие переменные среды консоли восстановления. AllowWildCards: позволяет использовать подстановочные знаки для некоторых команд (например, для команды DEL). AllowAllPaths: разрешает доступ к любым файлам и папкам компьютера. AllowRemovableMedia: позволяет копировать файлы на съемные носители, например, на дискеты. NoCopyPrompt: отменяет выдачу предупреждения при перезаписи существующих файлов. По умолчанию: эта политика не определена и команда SET консоли восстановления недоступна.

Источники

CCE-8945-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8945-8&platform=win7

Ссылки

Ресурс

Тип	GPO

Источник Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроллер домена: Запретить изменение пароля учетных записей компьютера**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, будут ли контроллеры домена отвергать запросы компьютеров, входящих в домен, на изменение паролей их учетных записей. По умолчанию компьютеры, входящие в домен, меняют пароли своих учетных записей каждые 30 дней. Если параметр включен, контроллер домена будет отвергать запросы на изменение паролей учетных записей. Включенный параметр не позволит контроллеру домена принять любые изменения паролей учетных записей компьютеров. По умолчанию: данный параметр не определен; это означает, что система рассматривает его как отключенный.

Источники

CCE-9295-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9295-7&platform=win7

Ссылки

Ресурс
Тип GPO
Источник Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: Все администраторы работают в режиме одобрения администратором**

Описание

Эталонное значение: **Включен**

Этот параметр политики определяет характеристики всех политик контроля учетных записей для компьютера. При изменении этого параметра политики необходимо перезагрузить компьютер. Возможные значения • Включено (по умолчанию). Режим одобрения администратором включен. Чтобы разрешить встроенной учетной записи администратора и всем остальным пользователям, являющимся участниками группы "Администраторы", работать в режиме одобрения администратором, эта политика должна быть включена, а все связанные политики управления учетными записями также должны быть установлены соответствующим образом. • Отключено. Режим одобрения администратором и все соответствующие параметры политики контроля учетных записей будут отключены. Примечание. Если этот параметр политики отключен, центр обеспечения безопасности выдаст уведомление, что общая безопасность операционной системы снизилась.

Источники

CCE-9189-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9189-2&platform=win7

Ссылки

Ресурс
Тип GPO
Источник Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: Обнаружение установки приложений и запрос на повышение прав**

Описание

Эталонное значение: **Включен**

Этот параметр политики определяет характеристики обнаружения установки приложений для компьютера. Возможные значения. • Включено (по умолчанию для дома). Когда установочный пакет приложения обнаруживает необходимость повышения прав, пользователю предлагается ввести имя пользователя и пароль учетной записи администратора. Если пользователь вводит правильные учетные данные, операция продолжается с соответствующими правами. • Отключено (по умолчанию для организации). Установочный пакет приложения не обнаруживает необходимость повышения прав и не выдает запрос пользователю. В организациях, использующих стандартные пользовательские настольные компьютеры и технологии делегированной установки, такие как GPSI (Group Policy Software Install) или SMS, этот параметр политики следует отключить. В этом случае обнаружение установщика является ненужным.

Источники

CCE-9616-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9326-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: Переключение к безопасному рабочему столу при выполнении запроса на повышение прав**

Описание

Эталонное значение: **Включен**

Этот параметр политики определяет, будут ли запросы на повышение прав выводиться на интерактивный рабочий стол пользователя или на безопасный рабочий стол. Возможные значения. • Включено (по умолчанию). Все запросы на повышение прав выводятся на безопасный рабочий стол независимо от параметров политики поведения приглашения для администраторов и обычных пользователей. • Отключено: все запросы на повышение прав выводятся на интерактивный рабочий стол пользователя. Используются параметры политики поведения приглашения для администраторов и обычных пользователей.

Источники

CCE-9395-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9395-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: Поведение запроса на повышение прав для администраторов в режиме одобрения администратором**

Описание

Эталонное значение: **Запрос учетных данных**

Этот параметр политики определяет поведение запроса на повышение прав для администраторов. Возможные значения. • Повышение без запроса. Позволяет привилегированным учетным записям выполнить операцию, требующую повышения прав, без подтверждения согласия или ввода учетных данных. Примечание. Этот вариант должен использоваться только в средах с максимальными ограничениями. • Запрос учетных данных на безопасном рабочем столе. Для любой операции,

требующей повышения прав, на безопасном рабочем столе выводится приглашение ввести имя и пароль привилегированного пользователя. Если вводятся правильные учетные данные, операция будет продолжена с максимальными доступными привилегиями пользователя. • Запрос согласия на безопасном рабочем столе. Для любой операции, требующей повышения прав, на безопасном рабочем столе выводится приглашение выбрать: "Разрешить" или "Запретить". Если пользователь выбирает "Разрешить", операция будет продолжена с максимальными доступными привилегиями пользователя. • Запрос учетных данных. Для любой операции, требующей повышения прав, выводится приглашение ввести имя пользователя и пароль учетной записи администратора. Если вводятся правильные учетные данные, операция будет продолжена с соответствующими привилегиями. • Запрос согласия. Для любой операции, требующей повышения прав, пользователю предлагается выбрать: "Разрешить" или "Запретить". Если пользователь выбирает "Разрешить", операция будет продолжена с максимальными доступными привилегиями пользователя. • Запрос согласия для сторонних двоичных файлов (не Windows) (по умолчанию). Когда операция для приложения стороннего (не Майкрософт) производителя требует повышения прав, на безопасном рабочем столе выводится приглашение выбрать: "Разрешить" или "Запретить". Если пользователь выбирает "Разрешить", операция будет продолжена с максимальными доступными привилегиями пользователя.

Источники

CCE-8958-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8958-1&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: Поведение запроса на повышение прав для обычных пользователей**

Описание

Эталонное значение: **Автоматически отклонять запросы на повышение прав**

Этот параметр политики определяет поведение запроса на повышение прав для обычных пользователей. Возможные значения. • Запрос учетных данных. Для любой операции, требующей повышения прав, выводится приглашение ввести имя пользователя и пароль учетной записи администратора. Если вводятся правильные учетные данные, операция будет продолжена с соответствующими привилегиями. • Автоматически запретить запросы на повышение прав. Для любой операции, требующей повышения прав, отображается настроенное сообщение об ошибке запрета доступа. Организации, настольные компьютеры которых используются обычными пользователями, могут выбрать этот параметр политики для уменьшения числа обращений в службу поддержки. • Запрос учетных данных на безопасном рабочем столе (по умолчанию). Для любой операции, требующей повышения прав, на безопасном рабочем столе выводится приглашение ввести имя и пароль другого пользователя. Если вводятся правильные учетные данные, операция будет продолжена с соответствующими привилегиями.

Источники

CCE-8813-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8813-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: Повышать права для UIAccess-приложений только при установке в безопасных местах**

Описание

Эталонное значение: **Включен**

Этот параметр политики управляет тем, должны ли приложения, запрашивающие выполнение на уровне целостности UIAccess, находиться в безопасной папке файловой системы. Безопасными считаются только следующие папки: - …\Program Files\, включая вложенные папки - …\Windows\system32\ - …\Program Files (x86)\, включая вложенные папки для 64-разрядных версий Windows Примечание. Windows принудительно проводит обязательную проверку подписей PKI для любого интерактивного приложения, запрашивающего выполнение на уровне целостности UIAccess, вне зависимости от состояния данного параметра безопасности. Возможные значения. • Включено (по умолчанию). Приложение будет запускаться с уровнем целостности UIAccess только в том случае, если оно находится в безопасной папке файловой системы. • Отключено. Приложение будет запускаться с уровнем целостности UIAccess, даже если оно не находится в безопасной папке файловой системы.

Источники

CCE-9801-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9801-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: Повышение прав только для подписанных и проверенных исполняемых файлов**

Описание

Эталонное значение: **Отключен**

Этот параметр политики задает проверку подписей PKI для любых интерактивных приложений, требующих повышения прав. Администраторы организации могут управлять списком разрешенных приложений, размещая сертификаты в хранилище доверенных издателей локальных компьютеров. Возможные значения • Включено. Принудительно инициирует проверку пути сертификации PKI, прежде чем разрешить выполнение данного исполняемого файла. • Отключено (по умолчанию). Не инициирует проверку пути сертификации PKI, прежде чем разрешить выполнение данного исполняемого файла.

Источники

CCE-9021-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9021-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: При сбоях записи в файл или реестр виртуализация в размещение пользователя**

Описание

Эталонное значение: **Включен**

Этот параметр политики управляет перенаправлением сбоев записи приложений в определенные расположения в реестре и файловой системе. Этот параметр политики позволяет уменьшить опасность приложений, которые выполняются от имени администратора и во время выполнения записывают данные в папку %ProgramFiles%, %Windir%; %Windir%\system32 или HKLM\Software\.... Возможные значения. • Включено (по умолчанию). Сбои записи приложений перенаправляются во время выполнения в определенные пользователем расположения в файловой системе и реестре. •

Отключено. Выполнение приложений, записывающих данные в безопасные расположения, заканчивается ошибкой.

Источники

CCE-8817-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8817-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: Разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол**

Описание

Эталонное значение: **Отключен**

Этот параметр политики определяет, могут ли UIAccess-приложения (UIA-программы) автоматически отключать безопасный рабочий стол для запросов на повышение, используемых обычным пользователем. • Включено. UIA-программы, в том числе удаленный помощник Windows, автоматически отключают безопасный рабочий стол для запросов на повышение прав. Если не отключен параметр политики "Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав", приглашение появится на интерактивном рабочем столе пользователя, а не на безопасном рабочем столе. • Отключено (по умолчанию). Безопасный рабочий стол может быть отключен только пользователем интерактивного рабочего стола или путем отключения параметра политики "Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав".

Источники

CCE-9301-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9301-3&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Контроль учетных записей: Режим одобрения администратором для встроенной учетной записи администратора**

Описание

Эталонное значение: **Включен**

Этот параметр политики определяет характеристики режима одобрения администратором для встроенной учетной записи администратора. Возможные значения • Включено. Для встроенной учетной записи администратора используется режим одобрения администратором. По умолчанию любая операция, требующая повышения прав, предлагает пользователю подтвердить операцию. • Отключено (по умолчанию). Встроенная учетная запись администратора выполняет все приложения с полными правами администратора.

Источники

CCE-8811-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8811-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Сервер сети Microsoft: Использовать цифровую подпись (всегда)**

Описание

Эталонное значение: **Включено**

Этот параметр безопасности определяет, требуется ли компонентом SMB-сервера цифровая подпись для пакетов. Протокол блоков сообщений сервера (SMB) предоставляет основу для совместного доступа Windows к файлам и принтерам, а также для других сетевых операций (например, для удаленного администрирования Windows). Для предотвращения атак с перехватом, когда SMB-пакеты изменяются при передаче, протокол SMB поддерживает установку цифровой подписи для SMB-пакетов. Этот параметр определяет, необходимо ли согласование подписывания SMB-пакетов до выдачи разрешения на дальнейшее соединение с SMB-клиентом. Если этот параметр включен, сетевой сервер Microsoft не будет соединяться с сетевым клиентом Microsoft, если клиент не выдаст согласие на установку цифровой подписи для SMB-пакетов. Если этот параметр отключен, подписывание SMB-пакетов согласуется между клиентом и сервером. По умолчанию: Отключено для рядового сервера. Включено для контроллеров домена.

Источники

CCE-9040-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9040-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Сервер сети Microsoft: Использовать цифровую подпись (с согласия клиента)**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, будет ли выполняться согласование подписывания SMB-пакетов с требующими этого клиентами. Протокол блоков сообщений сервера (SMB) предоставляет основу для совместного доступа Windows к файлам и принтерам, а также для других сетевых операций (например, для удаленного администрирования Windows). Для предотвращения атак с перехватом, которые изменяют SMB-пакеты при передаче, протокол SMB поддерживает установку цифровой подписи для SMB-пакетов. Этот параметр политики определяет, будет ли выполняться согласование подписывания SMB-пакетов с клиентами, которые это запрашивают. Если этот параметр включен, сервер для сетей Майкрософт будет согласовывать подписывание SMB-пакетов по требованию клиента. Таким образом, если для клиента включено подписывание пакетов, будет выполнено согласование подписывания пакетов. Если эта политика отключена, SMB-клиент не будет выполнять согласование подписывания SMB-пакетов. По умолчанию: Включено только на контроллерах домена.

Источники

CCE-8825-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8825-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Сервер сети Microsoft: Время бездействия до приостановки сеанса**

Описание

Эталонное значение: **15 минут**

Этот параметр безопасности определяет продолжительность отрезка времени SMB-сеанса до его приостановки по причине неактивности. Администраторы могут использовать этот параметр для управления временем приостановки неактивного SMB-сеанса компьютером. Если клиентская активность возобновляется, сеанс автоматически устанавливается заново. Для этого параметра значение "0" означает отсоединение сеанса сразу, как только это представится возможным. Максимальное значение - 99999, что составляет 208 дней; в действительности такое значение отключает этот параметр. По умолчанию: параметр не определен; это означает, что система рассматривает параметр как имеющий значение "15" для серверов и неопределенное значение для рабочих станций.

Источники

CCE-9406-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9406-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Сервер сети Microsoft: Отключать клиентов по истечении разрешенных часов входа**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, будут ли отключаться пользователи, подключенные к локальному компьютеру, по истечении разрешенного времени входа, заданного для их учетной записи. Этот параметр влияет на компонент протокола SMB. Если этот параметр включен, по истечении разрешенного времени входа клиента сеансы клиента со службой SMB принудительно разрываются. Если этот параметр отключен, по истечении разрешенного времени входа клиента его сеанс сохраняется. Значение по умолчанию в Windows Vista и более поздних версиях: включен. Значение по умолчанию в Windows XP: отключен

Источники

CCE-9358-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9358-3&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Сетевая безопасность: Не хранить хеш-значение LAN Manager при следующей смене пароля**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, нужно ли при следующей смене пароля сохранять хеш-значение диспетчера

LAN (LM) для нового пароля. Хэш LM является относительно слабым и уязвимым для атак по сравнению с более криптостойким хешем Windows NT. Поскольку хеш LM хранится в базе данных безопасности на локальном компьютере, в случае атаки на базу данных безопасности пароли могут быть расшифрованы. По умолчанию в Windows Vista и более поздних версиях: включен. По умолчанию в Windows XP: отключен. Внимание! Windows 2000 с пакетом обновления 2 (SP2) и выше поддерживает проверку подлинности предыдущих версий Windows, таких как Microsoft Windows NT 4.0. Этот параметр может повлиять на способность компьютеров под управлением Windows 2000 Server, Windows 2000 Professional, Windows XP и семейства Windows Server 2003 взаимодействовать с компьютерами под управлением Windows 95 и Windows 98.

Источники

CCE-8937-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8937-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Сетевая безопасность: Разрешить LocalSystem использовать нулевые сеансы**

Описание

Эталонное значение: **Отключен**

Разрешить NTLM возвращаться к нулевому сеансу при использовании с LocalSystem. Значение по умолчанию - TRUE вплоть до Windows Vista включительно и FALSE в Windows 7.

Источники

CCE-8804-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8804-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Сетевая безопасность: Разрешить использование сетевых удостоверений в запросах проверки подлинности PKU2U к этому компьютеру**

Описание

Эталонное значение: **Отключен**

По умолчанию эта политика отключена на компьютерах, включенных в домен. В Windows 7 это не позволяет сетевым удостоверениям проходить проверку подлинности на компьютерах, включенных в домен.

Источники

CCE-9770-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9770-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Сетевая безопасность: Разрешить учетной записи локальной системы использовать удостоверение компьютера для NTLM**

Описание

Эталонное значение: **Включен**

Этот параметр политики позволяет службам локальной системы, применяющим согласование, использовать удостоверение компьютера при откате к проверке подлинности NTLM. Если включить этот параметр политики, службы, работающие под учетной записью локальной системы и применяющие согласование, будут использовать удостоверение компьютера. Это может вызвать сбой и регистрацию ошибки для некоторых запросов проверки подлинности между операционными системами Windows. Если этот параметр политики не задан, службы, работающие под учетной записью локальной системы и применяющие согласование, при откате к проверке подлинности NTLM будут проходить проверку подлинности анонимно. Эта политика поддерживается по крайней мере в Windows 7 и Windows Server 2008 R2.

Источники

CCE-9096-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9096-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Сетевая безопасность: Требование цифровой подписи для LDAP-клиента**

Описание

Эталонное значение: **Согласование цифровой подписи**

Этот параметр безопасности определяет уровень подписи данных, который запрашивается от имени клиентов, отправляющих запросы LDAP BIND, следующим образом. Нет: запрос LDAP BIND отправляется с параметрами, указанными вызывающей стороной. Согласование цифровой подписи: если службы TLS и SSL не запущены, запрос LDAP BIND создается с набором параметров подписи данных LDAP в добавление к параметрам, указанным вызывающей стороной. Если службы TLS и SSL запущены, запрос LDAP BIND создается с параметрами, указанными вызывающей стороной. "Требовать подпись": то же, что и "Согласование цифровой подписи". Однако если промежуточный ответ saslBindInProgress LDAP-сервера не показывает, что требуется подпись трафика LDAP, вызывающая сторона получает сообщение о том, что запрос команды LDAP BIND завершился с ошибкой. Внимание Если на сервере задано значение "Требовать подпись", на клиенте значение должно быть таким же. Если на клиенте не задано такое же значение, это приведет к потере подключения к серверу. Примечание. Этот параметр не оказывает влияния на ldap_simple_bind или ldap_simple_bind_s. Клиенты Microsoft LDAP в составе Windows XP Professional не используют ldap_simple_bind или ldap_simple_bind_s для взаимодействия с контроллером домена. Значение по умолчанию: "Согласование цифровой подписи".

Источники

CCE-9768-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9768-3&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название	**Сетевая безопасность: Минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)**

Описание

Эталонное значение: **Требовать сеансовую безопасность NTLMv2**
Требовать 128-битное шифрование
Этот параметр безопасности позволяет клиенту требовать согласование конфиденциальности (шифрования) сообщений, целостность сообщений, использование 128-разрядного шифрования или сеансовую безопасность на базе NTLMv2. Эти значения зависят от значения параметра безопасности уровня проверки подлинности LAN Manager.

"Требовать целостность данных" - соединение не будет установлено, если не удалось согласовать требование целостности сообщений. Целостность сообщения может оцениваться анализом цифровой подписи сообщения. Подпись сообщения, удостоверяющая, что сообщение не подделано, реализуется путем включения криптографической подписи, идентифицирующей отправителя и являющейся числовым представлением содержимого сообщения. Эта подпись гарантирует неизменность исходного сообщения.

"Требовать конфиденциальность сообщения" - соединение будет разорвано, если не удастся согласовать требование шифрования. Путем шифрования данные преобразуются в форму, которая не позволяет прочесть их до тех пор, пока не выполнено дешифрование.

"Требовать сеансовую NTLMv2-безопасность" - соединение будет разорвано, если не удастся согласовать использование требование об использовании протокола NTLMv2.

"Требовать 128-разрядное шифрование" - соединение будет разорвано, если не удастся согласовать требование об использовании надежного (128-разрядного) шифрования.

По умолчанию: требования отсутствуют.

Источники

CCE-3156-7
http://cce.mitre.org

Ссылки

Ресурс

Тип	GPO
Источник	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Параметр Критичность: Высокий

Название	**Сетевая безопасность: Минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)**

Описание

Эталонное значение: **Требовать сеансовую безопасность NTLMv2**
Требовать 128-битное шифрование
Этот параметр безопасности позволяет серверу требовать согласование конфиденциальности (шифрования) сообщений, целостность сообщений, использование 128-битового шифрования или сеансовую безопасность на базе NTLMv2. Эти значения зависят от значения параметра безопасности уровня проверки подлинности LAN Manager.

"Требовать целостность данных" - соединение не будет установлено, если не удалось согласовать требование целостности сообщений. Целостность сообщения может оцениваться анализом цифровой подписи сообщения. Подпись сообщения, удостоверяющая, что сообщение не подделано, реализуется путем включения криптографической подписи, идентифицирующей отправителя и являющейся числовым представлением содержимого сообщения. Эта подпись гарантирует неизменность исходного сообщения.

"Требовать конфиденциальность сообщения" - соединение будет разорвано, если не удалось согласовать требование шифрования. Путем шифрования данные преобразуются в форму, которая не позволяет прочесть их до тех пор, пока не выполнено дешифрование.

"Требовать сеансовую NTLMv2-безопасность" - соединение будет разорвано, если не удалось согласовать использование требование об использовании протокола NTLMv2.

"Требовать 128-битовое шифрование" - соединение будет разорвано, если не удалось согласовать использование требование об использовании надежного (128-разрядного) шифрования.

По умолчанию: требования отсутствуют.

Источники

CCE-2799-5
http://cce.mitre.org

Ссылки

Ресурс

Тип	GPO
Источник	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Параметр Критичность: Высокий

Название **Сетевая безопасность: Уровень проверки подлинности LAN Manager**

Описание

Эталонное значение: **Отправлять только NTLMv2 - ответ. Отказывать LM и NTLM**

Этот параметр безопасности определяет, какие протоколы проверки подлинности с запросом и ответом используются для сетевого входа в систему. Значение этого параметра влияет на уровень протокола проверки подлинности, который используют клиенты, на уровень согласованной безопасности сеанса, а также на уровень проверки подлинности, принимаемой серверами, следующим образом. Отправлять ответы LM и NTLM: клиенты используют проверку подлинности LM и NTLM и никогда не используют сеансовую безопасность NTLMv2; контроллеры домена принимают проверку подлинности LM, NTLM и NTLMv2. Отправлять LM и NTLM - использовать сеансовую безопасность NTLMv2 при согласовании: клиенты используют проверку подлинности LM и NTLM, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена принимают проверку подлинности LM, NTLM и NTLMv2. Отправлять только NTLM-ответ: клиенты используют только проверку подлинности NTLM, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена принимают проверку подлинности LM, NTLM и NTLMv2. Отправлять только NTLMv2-ответ: клиенты используют только проверку подлинности NTLMv2, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена принимают проверку подлинности LM, NTLM и NTLMv2. Отправлять только NTLMv2-ответ и отказывать LM: клиенты используют только проверку подлинности NTLMv2, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена отклоняют LM (принимая только проверку подлинности NTLM и NTLMv2). Отправлять только NTLMv2-ответ и отказывать LM и NTLM: клиенты используют только проверку подлинности NTLMv2, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена отклоняют LM и NTLM (принимая только проверку подлинности NTLMv2). Внимание Этот параметр может повлиять на способность компьютеров под управлением Windows 2000 Server, Windows 2000 Professional, Windows XP Professional и семейства Windows Server 2003 к взаимодействию по сети с компьютерами под управлением Windows 4.0 и более ранних версий. Например, на момент создания данного документа компьютеры под управлением Windows NT 4.0 с пакетом обновления 4 (SP4) не поддерживали NTLMv2. Компьютеры под управлением Windows 95 и Windows 98 не поддерживали NTLM. Значение по умолчанию. Windows 2000 и Windows XP: отправлять ответы LM и NTLM на сервер Windows Server 2003: отправлять только ответ NTLM Windows Vista, Windows Server 2008, Windows 7 и Windows Server 2008 R2: отправлять только ответ NTLMv2

Источники

CCE-8806-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8806-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Сетевой доступ: Запретить анонимный доступ к именованным каналам и общим ресурсам**

Описание

Эталонное значение: **Включен**

Если этот параметр безопасности включен, он ограничивает анонимный доступ к общим ресурсам и именованным каналам в соответствии со значениями следующих параметров: Сетевой доступ: разрешать анонимный доступ к именованным каналам Сетевой доступ: разрешать анонимный доступ к общим ресурсам Значение по умолчанию: включен.

Источники

CCE-9540-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9540-6&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей**

Описание

Эталонное значение: **Обычная - локальные пользователи удостоверяются как они сами**

Этот параметр безопасности определяет, каким образом выполняется проверка подлинности при входе в сеть с использованием локальных учетных записей. Если данный параметр имеет значение "Обычная", при проверке подлинности для входа в сеть с учетными данными локальной учетной записи используются эти учетные данные. Обычная модель позволяет более гибко управлять доступом к ресурсам. С помощью обычной модели можно предоставить разным пользователям разные типы доступа к одному и тому же ресурсу. Если этот параметр имеет значение "Гостевая", операции входа в сеть с учетными данными локальных учетных записей автоматически сопоставляются с учетной записью гостя. При использовании гостевой модели между пользователями нет различий. Все пользователи проходят проверку подлинности с учетной записью гостя и получают одинаковый уровень доступа к данному ресурсу "Только чтение" или "Изменение". По умолчанию на компьютерах домена: Обычная. По умолчанию на автономных компьютерах: Гостевая. Внимание! Если используется гостевая модель, любой пользователь, имеющий доступ к компьютеру по сети (включая анонимных пользователей Интернета), может получить доступ к общим ресурсам. Для защиты компьютера от несанкционированного доступа необходимо использовать брандмауэр Windows или другую аналогичную программу. Кроме того, при использовании обычной модели локальные учетные записи должны быть защищены паролем, чтобы их нельзя было использовать для доступа к общим ресурсам системы. Примечание Этот параметр не влияет на операции интерактивного входа в систему, которые выполняются удаленно с помощью таких служб, как Telnet или служб удаленных рабочих столов. Старое название служб удаленных рабочих столов в предыдущих версиях Windows Server - "службы терминалов". Эта политика не распространяется на компьютеры, работающие под управлением Windows 2000. Если компьютер не входит в домен, параметры на вкладках "Доступ" и "Безопасность" в проводнике Windows также изменяются в соответствии с выбранной моделью совместного доступа и безопасности.

Источники

CCE-9503-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9503-4&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название	**Сетевой доступ: Не разрешать перечисление учетных записей SAM анонимными пользователями**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, какие дополнительные разрешения будут даны анонимным подключениям к этому компьютеру. Windows разрешает анонимным пользователям совершать определенные действия, такие как перечисление имен учетных записей домена и общих сетевых ресурсов. Это удобно, например, когда администратору требуется предоставить доступ пользователям в доверенном домене, не поддерживающем взаимное доверие. Этот параметр безопасности позволяет накладывать дополнительные ограничения на анонимные подключения. Включен: не разрешать перечисление учетных записей SAM. Этот параметр заменяет параметр "Все" на параметр "Прошедшие проверку" в разрешениях безопасности для ресурсов. Отключен: нет дополнительных ограничений. Используются разрешения по умолчанию. По умолчанию на рабочих станциях: включен. По умолчанию на сервере: отключен. Внимание! Эта политика не влияет на контроллеры доменов.

Источники

CCE-9249-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9249-4&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название	**Сетевой доступ: Не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, разрешено ли перечисление учетных записей SAM и общих ресурсов анонимными пользователями. Windows разрешает анонимным пользователям совершать некоторые действия (например, перечисление имен учетных записей домена и общих папок). Это удобно в случае, если администратор хочет предоставить доступ пользователям в доверенном домене, не поддерживающем взаимное доверие. Чтобы запретить перечисление учетных записей SAM и общих ресурсов анонимными пользователями, включите этот параметр. По умолчанию: Отключен.

Источники

CCE-9156-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9156-1&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название	**Сетевой доступ: Не разрешать хранение паролей или учетных данных для сетевой проверки подлинности**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, сохраняются ли диспетчером учетных данных пароли и учетные данные при

проверке подлинности доменом (для последующего использования). Если данный параметр включен, то сохранение паролей и учетных данных диспетчером учетных данных на данном компьютере не производится. Если данный параметр политики выключен или значение для него не задано, то диспетчер учетных данных будет сохранять пароли и учетные данные на этом компьютере (для использования в будущем при проверке подлинности доменом). Примечание. Изменения в конфигурации этого параметра безопасности вступят в силу только после перезагрузки Windows. По умолчанию: отключен.

Источники

CCE-8654-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8654-6&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Сетевой доступ: Разрешать анонимный доступ к именованным каналам**

Описание

Эталонное значение: **Отсутствует**

Этот параметр безопасности определяет, какие сеансы связи (каналы) будут иметь атрибуты и разрешения, дающие право анонимного доступа. По умолчанию: Отсутствует.

Источники

CCE-9218-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9218-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Сетевой доступ: разрешать анонимный доступ к общим ресурсам**

Описание

Эталонное значение: **Отсутствует**

Этот параметр безопасности определяет, к каким общим ресурсам могут получать доступ анонимные пользователи. Значение по умолчанию: нет.

Источники

CCE-9196-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9196-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Сетевой доступ: Разрешать применение разрешений "Для всех" к анонимным пользователям**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, какие дополнительные разрешения будут даны анонимным подключениям к компьютеру. Windows разрешает анонимным пользователям совершать некоторые действия (например, перечисление имен учетных записей домена и общих папок). Это удобно в случае, если администратор хочет предоставить доступ пользователям в доверенном домене, не поддерживающем взаимное доверие. По умолчанию идентификатор безопасности "Для всех" удаляется из токена, созданного для анонимных соединений. Таким образом, разрешения группы "Для всех" не затрагивают анонимных пользователей. Если этот параметр установлен, анонимные пользователи имеют доступ только к тем ресурсам, доступ к которым им разрешен явным образом. Если этот параметр включен, идентификатор безопасности "Для всех" добавляется к токену, созданному для анонимных соединений. В этом случае анонимные пользователи имеют доступ к любому ресурсу, разрешенному для группы "Для всех". По умолчанию: Отключен.

Источники

CCE-8936-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8936-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Сетевой доступ: Удаленно доступные пути и вложенные пути реестра**

Описание

Эталонное значение: **System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog**

Этот параметр безопасности определяет, какие пути и вложенные пути реестра могут быть доступны через сеть вне зависимости от пользователей или групп пользователей, указанных в таблице управления доступом (ACL) раздела реестра winreg. По умолчанию System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog System\CurrentControlSet\Services\CertSvc System\CurrentControlSet\Services\Wins Внимание! Неправильное редактирование реестра может нанести серьезный вред системе. Перед изменением реестра создайте резервную копию всех важных данных. Примечание. В Windows XP этот параметр безопасности назывался "Сетевой доступ: пути в реестре доступны через удаленное подключение". При настройке этого параметра на присоединенном к домену компьютере с операционной системой семейства Windows Server 2003 этот параметр наследуется компьютерами под управлением Windows XP, но отображается как параметр безопасности "Сетевой доступ: пути в реестре доступны через удаленное подключение".

Источники

CCE-9386-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9386-4&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Сетевой доступ: Удаленно доступные пути реестра**

Описание

Эталонное значение: **System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion**

Этот параметр безопасности определяет, какие пути реестра могут быть доступны через сеть вне зависимости от пользователей или групп пользователей, указанных в списке управления доступом (ACL) раздела реестра winreg. По умолчанию: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion Внимание! Неправильное редактирование реестра может нанести серьезный вред системе. Перед изменением реестра создайте резервную копию всех важных данных. Примечание. Этот параметр безопасности недоступен в более ранних версиях Windows. Параметр безопасности, отображаемый в Windows XP как "Сетевой доступ: пути в реестре доступны через удаленное подключение", соответствует параметру безопасности "Сетевой доступ: удаленно доступные пути и вложенные пути реестра" в семействе Windows Server 2003. По умолчанию System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion.

Источники

CCE-9121-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9121-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Сетевой сервер (Майкрософт): уровень проверки сервером имени участника-службы конечного объекта**

Описание

Эталонное значение: **Принимать, если предоставлено клиентом**

Этот параметр политики управляет уровнем проверки, выполняемой компьютером с общими папками или принтерами (сервером) над именем участника-службы, предоставляемым клиентским компьютером при установлении последним сеанса с помощью протокола SMB. Протокол SMB предоставляет основу для совместного доступа к файлам и принтерам, а также для других сетевых операций, например, для удаленного администрирования Windows. Протокол SMB поддерживает проверку имени участника-службы SMB-сервера в большом двоичном объекте, предоставляемом SMB-клиентом, для предотвращения класса атак против SMB-серверов, называемых атаками с перехватами. Этот параметр влияет на SMB1 и SMB2. Этот параметр безопасности определяет уровень проверки, выполняемой SMB-сервером над именем участника-службы, предоставляемым SMB-клиентом при установлении последним сеанса с SMB-сервером. Параметры: Откл. - имя участника-службы SMB-клиента не требуется (не проверяется) SMB-сервером. Принимать, если предоставлено клиентом - SMB-сервер принимает и проверяет имя участника-службы, предоставляемое SMB-клиентом, и разрешает сеанс, если оно совпадает со списком имен участников-служб SMB-сервера. Если имя НЕ совпадает, то сеанс для SMB-клиента отклоняется. Требовать от клиента - SMB-клиент ДОЛЖЕН отправить имя участника-службы при настройке сеанса, а указанное имя ДОЛЖНО совпадать с SMB-сервером, на который отправлен запрос на подключение. Если имя участника-службы не указано клиентом или оно не совпадает, сеанс отклоняется. Значение по умолчанию: "Откл.". Все операционные системы Windows поддерживают компонент SMB на стороне клиента и сервера. Этот параметр влияет на поведение SMB-сервера, и его реализацию следует тщательно анализировать и проверять, чтобы предотвратить отказы в доступе к функциям обслуживания, связанным с файлами и печатью.

Источники

CCE-8503-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8503-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Системная криптография: обязательное применение сильной защиты ключей пользователей, хранящихся на компьютере**

Описание

Эталонное значение: **Не требуется ввод данных пользователем при сохранении и использовании новых ключей**

Этот параметр безопасности определяет, требуется ли пароль для использования закрытых ключей пользователей. Доступны следующие варианты. Не требуется ввод данных пользователем при сохранении и использовании новых ключей. Пользователь получает запрос при первом использовании ключа. Пользователь должен вводить пароль при каждом использовании ключа. По умолчанию: эта политика не определена.

Источники

CCE-9381-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9381-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Системные объекты: Усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок)**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, насколько ограничивающим является список управления доступом на уровне пользователей (DACL) по умолчанию для объектов. Служба каталогов Active Directory содержит глобальный список общих ресурсов системы, таких как имена устройств DOS, мьютексы и семафоры. Это позволяет находить объекты и управлять совместным доступом процессов к ним. Каждый тип объекта создается со списком DACL по умолчанию, в котором указаны пользователи, имеющие доступ к объектам, и перечислены предоставленные разрешения. Если данная политика включена, список DACL по умолчанию является более ограничивающим. Пользователи без прав администратора имеют к общим объектам доступ на чтение, но не могут изменить объекты, которые созданы другими пользователями. Значение по умолчанию: включен.

Источники

CCE-9191-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9191-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Системные объекты: Учитывать регистр для подсистем, отличных от Windows**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, необходимо ли учитывать регистр для всех подсистем. Подсистема Win32 не учитывает регистр. Тем не менее, ядро поддерживает учет регистра для других подсистем, таких как POSIX. Если этот параметр включен, регистр не учитывается для всех объектов каталогов, символических ссылок, а также объектов ввода-вывода, включая файловые объекты. Отключение этого параметра не позволяет подсистеме Win32 учитывать регистр. Значение по умолчанию: включен.

Источники

CCE-9319-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9319-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Устройства: Запретить пользователям установку драйверов принтера**

Описание

Эталонное значение: **Включен**

Чтобы локальный компьютер мог использовать общий принтер, на нем должен быть установлен драйвер этого общего принтера. Этот параметр безопасности определяет, кому разрешено устанавливать драйвер принтера при добавлении общего принтера. Если этот параметр включен, при добавлении общего принтера драйвер принтера могут устанавливать только администраторы. Если параметр отключен, устанавливать драйвер принтера при добавлении общего принтера может любой пользователь. По умолчанию на серверах: Включено. По умолчанию на рабочих станциях: Отключено Примечания Этот параметр не влияет на возможность добавления локального принтера. Параметр не затрагивает администраторов.

Источники

CCE-9026-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9026-6&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Низкий

Название **Устройства: Разрешить доступ к дисководам гибких дисков только локальным пользователям**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, будет ли съемный дисковод гибких дисков доступен одновременно и локальным, и удаленным пользователям. Если данный параметр включен, доступ к съемным дисководам гибких дисков разрешен только пользователям, вошедшим в систему интерактивно. Если данный параметр включен, но никто не вошел

в систему интерактивно, дисковод гибких дисков будет доступен через сеть. По умолчанию: данная политика не определена, и доступ к дисководу гибких дисков не ограничивается только пользователями, вошедшими в систему интерактивно.

Источники

CCE-9440-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9440-9&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Низкий

Название **Устройства: Разрешить доступ к дисководам компакт-дисков только локальным пользователям**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, будет ли дисковод компакт-дисков доступен одновременно и локальным, и удаленным пользователям. Если данный параметр включен, доступ к компакт-дискам разрешен только пользователям, вошедшим в систему интерактивно. Если данный параметр включен, но никто не вошел в систему интерактивно, дисковод компакт-дисков будет доступен через сеть. По умолчанию: данная политика не определена, и доступ к компакт-дискам не ограничивается только пользователями, вошедшими в систему интерактивно.

Источники

CCE-9304-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9304-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Устройства: Разрешить форматирование и извлечение съемных носителей**

Описание

Эталонное значение: **Администраторы**

Этот параметр безопасности определяет, кому разрешено форматирование и извлечение съемных NTFS-носителей. Эта возможность может быть предоставлена: администраторам администраторам и интерактивным пользователям По умолчанию: данная политика не определена и такая возможность есть только у администраторов.

Источники

CCE-8868-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8868-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Учетные записи: Переименование учетной записи администратора**

Описание

Эталонное значение: **Рекомендовано переименовать учетную запись**

Этот параметр безопасности определяет, будет ли связано другое имя учетной записи с идентификатором безопасности (SID) учетной записи "Администратор". Переименование учетной записи "Администратор" несколько затрудняет угадывание посторонними лицами комбинации имени и пароля этого привилегированного пользователя. По умолчанию: Администратор.

Источники

CCE-8484-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8484-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Средний

Название **Учетные записи: Переименование учетной записи гостя**

Описание

Эталонное значение: **Рекомендовано переименовать учетную запись**

Этот параметр безопасности определяет, будет ли с идентификатором безопасности (SID) учетной записи "Гость" связано другое имя учетной записи. Переименование учетной записи "Гость" несколько затрудняет угадывание посторонними лицами комбинации имени и пароля этого пользователя. По умолчанию: гость.

Источники

CCE-9229-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9229-6&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Учетные записи: Разрешить использование пустых паролей только при консольном входе**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, могут ли локальные учетные записи, не защищенные паролем, использоваться для входа в систему из местоположений, отличных от физической консоли компьютера. Если параметр включен, то для локальных учетных записей, не защищенных паролем, вход в систему возможен только с клавиатуры компьютера. Значение по умолчанию: включено. Внимание! К компьютерам, находящимся в физически незащищенных местах, всегда должны принудительно применяться параметры надежных паролей для всех локальных учетных записей пользователей. В противном случае любой пользователь, имеющий физический доступ к компьютеру, может войти в систему при помощи пользовательской учетной записи, не имеющей пароля. Это особенно важно для портативных компьютеров. Если этот параметр безопасности применяется к группе "Все", никто не сможет войти в систему через службы удаленных рабочих

столов. Примечания. Данный параметр не оказывает влияния, если при входе в систему используются учетные записи домена. Приложения, использующие удаленный интерактивный вход в систему, могут обойти этот параметр. Старое название служб удаленных рабочих столов в предыдущих версиях Windows Server - "службы терминалов".

Источники

CCE-9418-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9418-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Учетные записи: Состояние учетной записи 'Администратор'**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, включена или отключена учетная запись локального администратора. Примечания При несоответствии пароля текущего администратора требованиям к паролю повторно включить учетную запись администратора, если ранее она была отключена, будет нельзя. В этом случае, пароль учетной записи администратора должен быть сброшен другим членом группы администраторов. Отключение учетной записи администратора при некоторых обстоятельствах может затруднить обслуживание. При перезагрузке в безопасном режиме отключенную учетную запись администратора можно включить только в том случае, если компьютер не присоединен к домену и отсутствуют другие активные учетные записи локального администратора. Если компьютер присоединен к домену, отключенная учетная запись администратора не может быть включена. По умолчанию: Отключено.

Источники

CCE-9199-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9199-1&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Учетные записи: Состояние учетной записи 'Гость'**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, включена или отключена учетная запись гостя. По умолчанию: Отключено. Примечание. Если учетная запись гостя отключена, а параметр безопасности "Сетевой доступ: модель совместного доступа и безопасности" для локальных учетных записей установлен в значение "Только гости", попытки входа в сеть, выполняемые, например, сервером сетей Майкрософт (служба SMB), завершатся неудачно.

Источники

CCE-8714-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8714-8&platform=win7

Ссылки

Ресурс

Тип	GPO

Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название	**Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, поддерживает ли поставщик безопасности TL/SS (Transport Layer Security/Secure Sockets Layer) только набор шифров TLS_RSA_WITH_3DES_EDE_CBC_SHA. Это по сути означает, что поставщик поддерживает только протокол TLS в качестве клиента и в качестве сервера (если такая конфигурация применима). При этом для шифрования TLS-трафика используется только алгоритм Triple DES, для обмена TLS-ключами и проверки их подлинности - только алгоритм открытых ключей RSA, а для TLS-хеширования - только алгоритм хеширования SHA1.

В службе EFS (Encrypting File System - шифрованная файловая система) для шифрования содержимого NTFS-файлов применяется только алгоритм шифрования DES (Triple Data Encryption Standard). По умолчанию служба EFS использует для шифрования данных файлов в семействе операционных систем Windows Server 2003 алгоритм шифрования AES (Advanced Encryption Standard) с 256-разрядным ключом и алгоритм DESX в операционной системе Windows XP. Дополнительные сведения о службе EFS см. в разделе "Шифрованная файловая система".

В службах терминалов для шифрования сетевых соединений поддерживается только алгоритм шифрования Triple DES. Сведения о службах терминалов см. в разделе "Службы терминалов".

По умолчанию: "Отключен".

Источники

CCE-3441-3
http://www.ccedbru.altx-soft.ru/CCE.aspx?id=CCE-3441-3&platform=win2k3

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название	**Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет необходимость подписывания или шифрования всего трафика безопасного канала, инициированного членом домена. При присоединении компьютера к домену создается учетная запись компьютера. После этого при запуске системы для создания безопасного канала с контроллером домена используется пароль учетной записи компьютера. Этот безопасный канал используется для таких операций, как выполнение проверки подлинности NTLM, поиск имени или кода LSA и т. д. Этот параметр безопасности определяет, соответствует ли минимальным требованиям безопасности весь трафик безопасного канала, инициированного членом домена. В частности, он определяет необходимость подписывания или шифрования всего трафика безопасного канала, инициированного членом домена. Если параметр включен, то безопасный канал не будет установлен до тех пор, пока не будет согласовано либо подписывание, либо шифрование всего его трафика. Если параметр отключен, то подписывание и шифрование всего трафика безопасного канала согласуется с контроллером домена; в этом случае уровень подписывания и шифрования зависит от версии контроллера домена и значений следующих двух параметров: Член домена: шифровать данные безопасного канала, когда это возможно Член домена: подписывать данные безопасного канала, когда это возможно По умолчанию: включен. Примечания: Если данный параметр включен, параметр "Член домена: подписывать данные безопасного канала, когда это возможно" считается включенным, независимо от его текущего состояния. Благодаря этому члены домена будут пытаться согласовать по крайней мере подписывание трафика

безопасного канала. Если данный параметр включен, параметр "Член домена: подписывать данные безопасного канала, когда это возможно" считается включенным, независимо от его текущего состояния. Благодаря этому члены домена будут пытаться согласовать по крайней мере подписывание трафика безопасного канала. Учетные данные, передаваемые по безопасному каналу, всегда шифруются, независимо от согласования шифрования остального трафика.

Источники

CCE-8974-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8974-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Член домена: Максимальный срок действия пароля учетных записей компьютера**

Описание

Эталонное значение: **30 дней**

Этот параметр безопасности определяет, как часто член домена будет пытаться изменить пароль учетной записи компьютера. По умолчанию: 30 дней. Внимание! Этот параметр применяется к компьютерам под управлением Windows 2000, но не доступен на них через диспетчер конфигурации безопасности.

Источники

CCE-9123-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9123-1&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Член домена: Отключить изменение пароля учетных записей компьютера**

Описание

Эталонное значение: **Отключен**

Определяет, производится ли периодическое изменение пароля учетной записи компьютера члена домена. При включении этого параметра член домена не пытается изменить пароль учетной записи компьютера. Если этот параметр отключен, член домена пытается изменить пароль учетной записи компьютера согласно значению параметра "Член домена: максимальный срок действия пароля учетной записи компьютера", имеющего по умолчанию значение "каждые 30 дней". По умолчанию: Отключено. Примечания Не следует включать этот параметр безопасности. Пароли учетных записей используются для установления безопасных каналов связи между членами домена и контроллерами домена, а также между самими контроллерами внутри домена. После установления связи безопасный канал используется для передачи конфиденциальных данных, необходимых для выполнения проверки подлинности и авторизации. Этот параметр не следует использовать для поддержки сценариев двойной загрузки, использующих одну и ту же учетную запись компьютера. Для двойной загрузки двух установок, объединенных в одном домене, присвойте этим установкам разные имена компьютеров.

Источники

CCE-9295-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9295-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Член домена: Требовать стойкий ключ сеанса (Windows 2000 или выше)**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, требуется ли для зашифрованных данных безопасного канала 128-разрядный ключ. При присоединении компьютера к домену создается учетная запись компьютера. После этого при запуске системы для создания безопасного канала с контроллером домена используется пароль учетной записи компьютера. Этот безопасный канал используется для совершения таких операций, как сквозная проверка подлинности NTLM, поиск имени или ИД безопасности LSA и т. д. В зависимости от версии Windows, используемой на контроллере домена, с которым осуществляется соединение, а также от значений параметров: Член домена: всегда требуется цифровая подпись или шифрование данных безопасного канала Член домена: шифровать данные безопасного канала, когда это возможно Будут зашифрованы все или некоторые данные, передаваемые по безопасному каналу. Этот параметр политики определяет, требуется ли для зашифрованных данных безопасного канала 128-разрядный ключ. Если этот параметр включен, безопасное соединение будет установлено только в том случае, если возможно 128-разрядное шифрование. Если этот параметр отключен, стойкость ключа согласуется с контроллером домена. По умолчанию: включен. Внимание! Чтобы использовать этот параметр на рабочих станциях и серверах, входящих в домен, все контроллеры, формирующие домен, должны работать под управлением операционной системы Windows 2000 или более поздней версии. Чтобы использовать этот параметр на контроллерах домена, все контроллеры в этом домене, а также в доверенных доменах должны работать под управлением операционной системы Windows 2000 или более поздней версии.

Источники

CCE-9387-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9387-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Член домена: Цифровая подпись данных безопасного канала, когда это возможно**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, пытается ли член домена согласовать подписывание всего инициированного им трафика безопасного канала. При присоединении компьютера к домену создается учетная запись компьютера. После этого при запуске системы для создания безопасного канала с контроллером домена используется пароль учетной записи компьютера. Этот безопасный канал используется для таких операций, как выполнение проверки подлинности NTLM, поиск имени или кода LSA и т. д. Этот параметр безопасности определяет, пытается ли член домена согласовать подписывание всего инициированного им трафика безопасного канала. Если этот параметр включен, член домена будет требовать подписывания всего трафика безопасного канала. Если контроллер домена поддерживает подписывание всего трафика безопасного канала, то будет подписываться весь трафик безопасного канала, что обеспечит невозможность его изменения при передаче. По умолчанию: включен. Примечания Если включен параметр "Член домена: всегда требуется цифровая подпись или шифрование данных безопасного канала", то данный параметр считается включенным вне зависимости от его текущего значения. Контроллеры домена также являются членами домена и устанавливают безопасные каналы с другими контроллерами домена как в том же домене, так и в доверенных доменах.

Источники

CCE-9375-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9375-7&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Параметр Критичность: Высокий

Название **Член домена: Шифрование данных безопасного канала, когда это возможно**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, будет ли член домена пытаться согласовать шифрование всего трафика безопасного канала, который он инициирует. При присоединении компьютера к домену создается учетная запись компьютера. После этого при запуске системы для создания безопасного канала с контроллером домена используется пароль учетной записи компьютера. Этот безопасный канал используется для таких операций, как выполнение проверки подлинности NTLM, поиск имени или кода LSA и т. д. Этот параметр определяет, будет ли член домена пытаться согласовать шифрование всего трафика безопасного канала, который он инициирует. Если параметр включен, член домена будет запрашивать шифрование всего трафика безопасного канала. Если контроллер домена поддерживает шифрование всего трафика безопасного канала, то весь трафик безопасного канала будет шифроваться. В противном случае шифроваться будут только учетные данные, передаваемые по безопасному каналу. Если параметр отключен, член домена не будет пытаться согласовывать шифрование безопасного канала. По умолчанию: включен. Внимание! Нет никаких оснований для отключения этого параметра. Помимо возможного снижения уровня потенциальной конфиденциальности безопасного канала, отключение данного параметра может привести к неоправданному снижению пропускной способности безопасного канала, так как параллельные вызовы API-процедур, использующих безопасный канал, возможны только при подписанном или шифрованном безопасном канале. Примечание. Контроллеры домена также являются членами домена и устанавливают безопасные каналы с другими контроллерами домена как в том же домене, так и в доверенных доменах.

Источники

CCE-9251-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9251-0&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Группа

Название **2.3 Политики аудита**

Описание

Политика аудита определяет те события, имеющие отношение к безопасности, учет которых нужно вести - так, чтобы ряд действий пользователя или системы оставлял записи в определенных категориях. Можно отследить, кто обращался к объекту, когда пользователи входили в систему и завершали работу, или какие изменения были внесены в параметры политики аудита. По этим причинам схему ведения аудита рекомендуется разработать и внедрить в рабочей среде. Приступая ко внедрению политики аудита, нужно прежде всего установить, какие категории событий надо отслеживать. Параметры аудита, которые будут выбраны в рамках категорий событий, и определяют политику аудита. Определившись с параметрами аудита для категории, можно создать политики, отвечающие им. Если параметры аудита не заданы, будет трудно или даже невозможно установить, что именно произошло при некоем инциденте. Если же, напротив, настроить аудит на регистрацию очень большого числа событий, то журнал безопасности будет слишком забит данными. Следующие разделы помогут определиться с событиями, которые в конкретной рабочей среде стоит отслеживать. В Windows 7 представлены те же девять категорий политики аудита, что и в предыдущих версиях Windows, плюс одна новая

категория Аудит доступа к глобальным объектам.

Группа

Название **2.3.1 Вход учетной записи**

Описание

Событие генерируется по факту проверки учетных данных. Оно происходит на том компьютере, которому принадлежат эти учетные данные. Например, в случае учетной записи домена событие генерируется на контроллере домена, а в случае локальной учетной записи - на локальном компьютере. В рамках домена большинство событий этой категории будет помещаться в журнал безопасности контроллера домена, на котором созданы учетные записи. Однако, если используются локальные учетные записи, эти события будут происходить и на других компьютерах .

Параметр Критичность: Высокий

Название **Аудит проверки учетных данных**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит событий, возникающих при проверке учетных данных для входа учетной записи пользователя. События этой подкатегории возникают только на компьютерах, заслуживающих доверия для этих учетных данных. Для учетных данных домена соответствующими полномочиями обладает контроллер домена. Для локальных учетных записей соответствующими полномочиями обладает локальный компьютер. Частота появления: высокая на контроллерах домена. По умолчанию в клиентских выпусках: нет аудита. По умолчанию в серверных выпусках: успех.

Источники

CCE-9725-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9725-3&platform=win7

CCE-9718-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9718-8&platform=win7

Параметр Критичность: Высокий

Название **Аудит службы проверки подлинности Kerberos**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при отправке запросов на получение билета предоставления билета проверки подлинности Kerberos (TGT). Если этот параметр политики настроен, событие аудита возникает после отправки запроса на получение билета TGT проверки подлинности Kerberos. Успешные и неудачные запросы регистрируются в соответствующих записях. Если этот параметр политики не настроен, после запроса билета TGT проверки подлинности Kerberos никакие события аудита не возникают. Частота появления: высокая для серверов центра распространения ключей Kerberos. По умолчанию в клиентских выпусках: нет аудита. По умолчанию в серверных выпусках: успех.

Источники

CCE-9258-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9258-5&platform=win7

CCE-9502-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9502-6&platform=win7

Параметр Критичность: Высокий

Название **Аудит операции с билетами службы Kerberos**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при подаче запросов на получение билета предоставления билета проверки подлинности Kerberos (TGT) для пользовательских учетных записей. Если этот параметр политики настроен, события аудита возникают после запроса билета TGT проверки подлинности Kerberos для учетной записи пользователя. Успешные и неудачные запросы регистрируются в соответствующих записях. Если этот параметр политики не настроен, после запроса билета TGT проверки подлинности Kerberos для учетной записи пользователя никакие события аудита не возникают. Частота появления: низкая. По умолчанию в клиентских выпусках: нет аудита. По умолчанию в серверных выпусках: успех.

Источники

CCE-9148-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9148-8&platform=win7

CCE-9269-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9269-2&platform=win7

Параметр Критичность: Высокий

Название **Аудит других событий входа учетных записей**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при получении ответов на запросы о входе учетной записи пользователя в систему, не относящиеся к проверке учетных данных и не являющиеся билетами Kerberos. В настоящий момент события этой подкатегории отсутствуют. По умолчанию: нет аудита.

Источники

CCE-9445-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9445-8&platform=win7

CCE-9808-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9808-7&platform=win7

Группа

Название **2.3.2 Управление учетными записями**

Описание

Эта категория помогает отслеживать попытки создания новых пользователей и групп, их переименования, включения или выключения, а также смены паролей. Анализ записей этого аудита позволяет выявить злонамеренные, случайные или санкционированные создания учетных записей пользователей и групп.

Параметр Критичность: Высокий

Название **Аудит управления группами приложений**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении следующих изменений групп приложений: - Создание, изменение или удаление группы приложений. - Добавление или удаление члена в группе приложений. Если этот параметр политики настроен, при попытке изменения группы приложений возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при изменении группы приложений никакие события аудита не возникают. Частота появления: низкая. По умолчанию: нет аудита.

Источники

CCE-8822-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8822-9&platform=win7

CCE-9591-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9591-9&platform=win7

Параметр Критичность: Высокий

Название **Аудит управления учетными записями компьютеров**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит событий, возникающих при изменении учетных записей компьютеров, например, при их создании, изменении или удалении. Если этот параметр политики настроен, при попытке изменения учетной записи компьютера возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при изменении учетной записи компьютера никакие события аудита не возникают. Частота появления: низкая. По умолчанию в клиентских выпусках: нет аудита. По умолчанию в серверных выпусках: успех.

Источники

CCE-9498-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9498-7&platform=win7

CCE-9608-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9608-1&platform=win7

Параметр Критичность: Высокий

Название **Аудит управления группами распространения**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении следующих изменений групп распространения: - Создание, изменение или удаление группы распространения. - Добавление участника в группу распространения или удаление из нее. - Изменение типа группы распространения. Если этот параметр политики настроен, при попытке изменения группы распространения возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при изменении группы распространения никакие события аудита не возникают. Примечание. События этой подкатегории регистрируются только на контроллерах домена. Частота появления: низкая. По умолчанию: нет аудита.

Источники

CCE-9644-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9644-6&platform=win7

CCE-8829-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8829-4&platform=win7

Параметр Критичность: Высокий

Название **Аудит других событий управления учетными записями**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении других изменений учетных записей пользователя, не указанных в этой категории: - Обращение к хешу пароля для учетной записи пользователя. Эта операция обычно выполняется при миграции паролей с использованием средства управления Active Directory. - Вызов API проверки политики паролей. Вызов этой функции может выполняться при атаках в тех случаях, когда вредоносное приложение проверяет политику, чтобы уменьшить число попыток во время словарной атаки. - Изменения групповой политики домена по умолчанию по следующим путям групповой политики: Конфигурация компьютера\Параметры Windows\Параметры безопасности\Политики учетных записей\Политики паролей Конфигурация компьютера\Параметры

Windows\Параметры безопасности\Параметры учетных записей\Политика блокировки учетных записей Примечание. Событие аудита безопасности регистрируется в случае применения параметра политики. Во время изменения параметров события не регистрируются. Частота появления: низкая. По умолчанию: нет аудита.

Источники

CCE-9657-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9657-8&platform=win7

CCE-9668-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9668-5&platform=win7

Параметр Критичность: Высокий

Название **Аудит управления группами безопасности**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении следующих изменений групп безопасности: - Создание, изменение или удаление группы безопасности. - Добавление участника в группу безопасности или удаление из нее. - Изменение типа группы. Если этот параметр политики настроен, при попытке изменения группы безопасности возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при изменении группы безопасности никакие события аудита не возникают. Частота появления: низкая. По умолчанию: успех.

Источники

CCE-9692-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9692-5&platform=win7

CCE-9056-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9056-3&platform=win7

Параметр Критичность: Высокий

Название **Аудит управления учетными записями пользователей**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит изменений, вносимых в учетные записи пользователей. Отслеживаются следующие события: - Создание, изменение, удаление, переименование, отключение, включение, блокировка и снятие блокировки учетных записей. - Установка или изменение пароля учетной записи пользователя. - Добавление идентификатора безопасности (SID) к журналу SID учетной записи пользователя. - Установка пароля для режима восстановления служб каталогов. - Изменение разрешений для учетных записей администраторов. - Архивация или восстановление учетных данных диспетчера учетных данных. Если этот параметр политики настроен, при попытке изменения учетной записи пользователя возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при изменении учетной записи пользователя никакие события аудита не возникают. Частота появления: низкая. По умолчанию: успех.

Источники

CCE-9542-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9542-2&platform=win7

CCE-9800-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9800-4&platform=win7

Группа

Название **2.3.3 Подробное отслеживание**

Описание

Эта категория позволят вести детальное отслеживание таких событий, как активация программы, завершение работы

процесса, создание копии дескриптора и косвенный доступ к объектам. Включение параметра Аудит отслеживания процессов приведет к записи большого числа событий, так что обычное значение этой политики - Не настроено. Однако, подробные сведения о том, какие процессы и когда были запущены, могут оказать неоценимую помощь в расследовании инцидента .

Параметр Критичность: Высокий

Название **Аудит активности DPAPI**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит событий, возникающих при выполнении запросов на шифрование или расшифровку к интерфейсу приложений защиты данных (DPAPI). Интерфейс DPAPI используется для защиты конфиденциальных данных, например, паролей и ключей. Если этот параметр политики настроен, события аудита возникают при выполнении запросов на шифрование или расшифровку к интерфейсу DPAPI. Успешные и неудачные запросы регистрируются в соответствующих записях. Если этот параметр политики не настроен, при выполнении запросов на шифрование и расшифровку к интерфейсу DPAPI никакие события аудита не возникают. Частота появления: низкая.

Источники

CCE-9412-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9412-8&platform=win7

CCE-9735-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9735-2&platform=win7

Параметр Критичность: Высокий

Название **Аудит создания процессов**

Описание

Эталонное значение: **Успех**

Этот параметр политики обеспечивает аудит событий, возникающих при создании или запуске процесса. Также осуществляется аудит имени пользователя или приложения, создавшего процесс. Если этот параметр политики настроен, событие аудита возникает при создании процесса. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при создании процесса никакие события аудита не возникают. Частота появления: в зависимости от типа используемого компьютера.

Источники

CCE-9562-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9562-0&platform=win7

CCE-9805-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9805-3&platform=win7

Параметр Критичность: Высокий

Название **Аудит завершения процессов**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит событий, возникающих при создании или запуске процесса. Также осуществляется аудит имени пользователя или приложения, создавшего процесс. Если этот параметр политики настроен, событие аудита возникает при создании процесса. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при создании процесса никакие события аудита не возникают. Частота появления: в зависимости от типа используемого компьютера.

Источники

CCE-9818-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9818-6&platform=win7

CCE-9227-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9227-0&platform=win7

Параметр Критичность: Высокий

Название **Аудит событий RPC**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит входящих подключений удаленного вызова процедур (RPC). Если этот параметр политики настроен, событие аудита возникает при попытке установления удаленного подключения RPC. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при попытке установления удаленного подключения RPC никакие события аудита не возникают. Частота появления: высокая на серверах RPC.

Источники

CCE-9364-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9364-1&platform=win7

CCE-9492-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9492-0&platform=win7

Группа

Название **3.2.4. Доступ к службе каталогов (DS)**

Описание

Эта категория применима только к контроллерам домена. Поэтому она и все ее подкатегории для целей настоящего руководства установлены в Не настроено .

Параметр Критичность: Высокий

Название **Аудит подробной репликации службы каталогов**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет аудит событий, возникающих при выполнении подробной репликации между контроллерами доменов в доменных службах Active Directory (AD DS). Частота появления: высокая. По умолчанию: нет аудита.

Источники

CCE-9526-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9526-5&platform=win7

CCE-9628-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9628-9&platform=win7

Параметр Критичность: Высокий

Название **Аудит доступа к службе каталогов**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при обращении к объектам доменных служб Active Directory (AD DS). Регистрируются только события для объектов AD DS с соответствующим системным списком

управления доступом (SACL). События этой подкатегории аналогичны событиям доступа к службе каталогов, представленным в предыдущих версиях Windows. Частота появления: высокая на контроллерах домена. Отсутствует на клиентских компьютерах. По умолчанию в клиентских выпусках: нет аудита. По умолчанию в серверных выпусках: успех.

Источники

CCE-9765-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9765-9&platform=win7

CCE-9791-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9791-5&platform=win7

Параметр Критичность: Высокий

Название **Аудит изменения службы каталогов**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при изменении объектов доменных служб Active Directory (AD DS). События регистрируются при создании, удалении, изменении, перемещении или отмене удаления объектов. Если это возможно, при возникновении событий этой подкатегории также регистрируются старые и новые значения свойств объекта. События этой подкатегории регистрируются только на контроллерах домена и только для объектов в AD DS с соответствующим системным списком управления доступом (SACL). Примечание. В соответствии с параметрами класса объекта в схеме при выполнении действий с некоторыми объектами и свойствами события аудита не возникают. Если этот параметр настроен, при попытке изменения объекта в AD DS возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр не настроен, при попытке изменения объекта AD DS никакие события аудита не возникают. Частота появления: высокая только для контроллеров домена. По умолчанию: нет аудита.

Источники

CCE-8850-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8850-0&platform=win7

CCE-9734-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9734-5&platform=win7

Параметр Критичность: Недоступно

Название **Аудит репликации службы каталогов**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит репликации между двумя контроллерами домена в доменных службах Active Directory (AD DS). Если этот параметр политики настроен, событие аудита возникает в процессе репликации AD DS. Успешные и неудачные операции репликации регистрируются в соответствующих записях аудита. Если этот параметр политики не настроен, в процессе репликации AD DS никакие события аудита не возникают. Примечание. События этой подкатегории регистрируются только на контроллерах домена. Частота появления: средняя для контроллеров домена. Отсутствует на клиентских компьютерах. По умолчанию: нет аудита.

Источники

CCE-9755-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9755-0&platform=win7

CCE-9526-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9526-5&platform=win7

Группа

Название **2.3.5 События входа и выхода из системы**

Описание

Эта категория позволяет отслеживать события создания и прекращения сеансов входа. События происходят на компьютере, к которому производится доступ. Так, при интерактивном входе событие произойдет на компьютере, где осуществлен вход, а при сетевом - на компьютере, где расположены ресурсы, к которым производится обращение. Если параметру Аудит событий входа в систему задать значение Не настроено, будет трудно, а то и невозможно, установить, кто именно обращался к каким-либо компьютерам или пытался это сделать.

Параметр Критичность: Высокий

Название **Аудит блокировки учетных записей**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет выполнять аудит событий, созданных при неудачной попытке входа в блокированную учетную запись. Если этот параметр политики настроен, то в случае, когда вход в компьютер с учетной записью невозможен из-за блокировки этой учетной записи, создается событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. События входа в систему важны для понимания действий пользователя и обнаружения возможных атак. Частота появления: низкая. По умолчанию: успех.

Источники

CCE-9725-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9725-3&platform=win7

CCE-9023-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9023-3&platform=win7

Параметр Критичность: Высокий

Название **Аудит расширенного режима IPsec**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, вызываемых протоколом IKE и протоколом IP с проверкой подлинности в процессе согласования расширенного режима. Если этот параметр политики настроен, в процессе согласования расширенного режима IPsec возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, в процессе согласования расширенного режима IPsec никакие события аудита не возникают. Частота появления: высокая. По умолчанию: нет аудита.

Источники

CCE-9725-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9725-3&platform=win7

CCE-9023-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9023-3&platform=win7

Параметр Критичность: Высокий

Название **Аудит основного режима IPsec**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, вызываемых протоколом IKE и протоколом IP с проверкой подлинности в процессе согласования основного режима. Если этот параметр политики настроен, в процессе согласования основного режима IPsec возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, в процессе согласования основного режима IPsec никакие события аудита не возникают. Частота появления: высокая. По умолчанию: нет аудита.

Источники

CCE-8956-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8956-5&platform=win7

CCE-9715-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9715-4&platform=win7

Параметр Критичность: Высокий

Название **Аудит быстрого режима IPsec**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, вызываемых протоколом IKE и протоколом IP с проверкой подлинности в процессе согласования быстрого режима. Если этот параметр политики настроен, в процессе согласования быстрого режима IPsec возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, в процессе согласования быстрого режима IPsec никакие события аудита не возникают. Частота появления: высокая. По умолчанию: нет аудита.

Источники

CCE-9632-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9632-1&platform=win7

CCE-9671-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9671-9&platform=win7

Параметр Критичность: Высокий

Название **Аудит выхода из системы**

Описание

Эталонное значение: **Успех**

Этот параметр политики позволяет вести аудит событий, возникающих при закрытии сеанса входа в систему. Эти события возникают на компьютере, к которому осуществлялся доступ. При интерактивном выходе из системы событие аудита безопасности возникает на компьютере, на который выполнен вход с использованием учетной записи пользователя. Если этот параметр политики настроен, событие аудита возникает при закрытии сеанса входа в систему. Успешные и неудачные попытки закрытия сеансов регистрируются в соответствующих записях. Если этот параметр политики не настроен, при закрытии сеанса входа в систему никакие события аудита не возникают. Частота появления: низкая. По умолчанию: успех.

Источники

CCE-8856-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8856-7&platform=win7

CCE-9058-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9058-9&platform=win7

Параметр Критичность: Высокий

Название **Аудит входа в систему**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит событий, возникающих при попытке входа в систему с использованием учетной записи пользователя. События этой подкатегории связаны с созданием сеансов входа в систему и возникают на компьютере, к которому осуществляется доступ. При интерактивном входе в систему событие аудита безопасности возникает на компьютере, на котором выполняется вход с использованием учетной записи. При входе в сеть, например, при обращении к общей папке в сети, событие аудита безопасности возникает на компьютере, на котором размещается ресурс. Отслеживаются следующие события: - Успешные попытки входа в систему. - Неудачные попытки входа в систему. - Попытки входа в систему с использованием явно указанных учетных данных. Это событие возникает при попытке входа процесса в учетную запись с явным указанием соответствующих учетных данных. Обычно это событие возникает в

конфигурациях пакетного входа в систему, например, при выполнении запланированных задач или команд RUNAS. - Запрет на вход в систему в результате фильтрации идентификаторов безопасности (SID). Частота появления: низкая на клиентских компьютерах, средняя на контроллере домена или на сетевом сервере. По умолчанию в клиентских выпусках: успех. По умолчанию в серверных выпусках: успех, отказ.

Источники

CCE-9683-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9683-4&platform=win7

CCE-9213-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9213-0&platform=win7

Параметр Критичность: Высокий

Название **Аудит сервера политики сети**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении запросов на доступ пользователей по протоколам RADIUS (IAS) и защиты доступа к сети (NAP). Отслеживаются запросы на предоставление, отказ, отзыв, помещение в карантин, блокировку и отмену блокировки. Если этот параметр политики настроен, событие аудита возникает для каждого запроса на доступ пользователей по протоколу IAS или NAP. Успешные и неудачные запросы на доступ пользователей регистрируются в соответствующих записях. Если этот параметр политики не настроен, аудит запросов на доступ пользователей по протоколам IAS и NAP не осуществляется. Частота появления: средняя или высокая для серверов политики сети и IAS-серверов. На других компьютерах отсутствуют. По умолчанию: успех, отказ.

Источники

CCE-9741-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9741-0&platform=win7

CCE-9076-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9076-1&platform=win7

Параметр Критичность: Высокий

Название **Аудит других событий входа и выхода**

Описание

Эталонное значение: **Успех**

Этот параметр политики позволяет вести аудит других событий входа и выхода, которые не регулируются параметром политики "Вход/выход", например: - Завершение сеансов служб терминалов. - Создание новых сеансов служб терминалов. - Блокировка и отмена блокировки рабочей станции. - Вызов заставки. - Отключение заставки. - Обнаружение атаки Kerberos с повторением пакетов, при которой дважды отправляется запрос Kerberos с одинаковыми данными. Это состояние может быть связано с неправильными настройками сети. - Предоставление доступа к беспроводной сети учетной записи пользователя или компьютера. - Предоставление доступа к проводной сети 802.1x учетной записи пользователя или компьютера. Частота появления: низкая. По умолчанию: нет аудита.

Источники

CCE-9622-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9622-2&platform=win7

CCE-9631-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9631-3&platform=win7

Параметр Критичность: Высокий

Название **Аудит специального входа**

Описание

Эталонное значение: **Не определено**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении таких операций специального входа, как следующие: - Использование специального входа, то есть входа в систему с правами, аналогичными правам администратора, который может использоваться для повышения уровня процесса. - Вход в систему участника специальной группы. При использовании специальных групп обеспечивается возникновение событий аудита при входе в сеть участника конкретной группы. В реестре можно настроить список идентификаторов безопасности (SID) группы. Событие регистрируется в том случае, если к токену добавлен один из заданных идентификаторов SID и включена эта подкатегория. Частота появления: низкая. По умолчанию: успех.

Источники

CCE-9763-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9763-4&platform=win7

CCE-9521-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9521-6&platform=win7

Группа

Название **2.3.6 Доступ к объектам**

Описание

Сам по себе этот параметр политики не приведет к появлению каких-либо событий. Он лишь определяет, следует ли вести аудит обращений пользователей к тем объектам, например, файлам, папкам, разделам реестра или принтерам, для которых указана системная таблица управления доступом (SACL). Таблица SACL состоит из записей управления доступом (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 неудачные попытки обращений, только успешные или обе категории. Если задать параметру Аудит доступа к объектам значение Успех, запись аудита будет создаваться каждый раз, когда пользователю разрешается доступ к объекту, которому присвоена таблица SACL. Если же задать значение Отказ, запись будет создаваться каждый раз, когда пользователю отказывается в доступе к объекту с присвоенной таблицей SACL. При создании таблиц SACL следует вносить в них только те действия, которые реально требуется отслеживать. Например, для исполняемых файлов можно включить параметр Аудит записи и дозаписи данных, потому что это позволит отслеживать изменение или замену таких файлов, а компьютерные вирусы, черви и троянские программы обычно внедряются в исполняемые файлы. Тем же способом можно отслеживать доступ или изменения в особо важных документах.

Параметр Критичность: Высокий

Название **Аудит событий, создаваемых приложениями**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит приложений, которые вызывают события с использованием программных интерфейсов аудита Windows. Эта подкатегория используется для регистрации событий аудита, которые связаны с работой приложений, использующих программные интерфейсы аудита Windows. Отслеживаются следующие события этой подкатегории: - Создание контекста клиента приложения. - Удаление контекста клиента приложения. - Инициализация контекста клиента приложения. - Другие операции приложений с использованием программных интерфейсов аудита Windows. Частота появления: зависит от приложения, вызывающего события.

Источники

CCE-9816-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9816-0&platform=win7

CCE-8860-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8860-9&platform=win7

Параметр Критичность: Высокий

Название **Аудит службы сертификации**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит операций служб сертификации Active Directory (AD CS). К операциям AD CS относятся следующие: - Запуск, завершение работы, резервное копирование и восстановление служб AD CS. - Изменение списка отзыва сертификатов (CRL). - Запросы новых сертификатов. - Выдача сертификата. - Отзыв сертификата. - Изменение параметров диспетчера сертификатов для служб AD CS. - Изменение конфигурации служб AD CS. - Изменение шаблона служб сертификации. - Импорт сертификата. - Публикация сертификата центра сертификации в доменных службах Active Directory. - Изменение разрешений безопасности для служб AD CS. - Архивация ключа. - Импорт ключа. - Извлечение ключа. - Запуск службы ответов OCSP. - Остановка службы ответов OCSP. Частота появления: средняя или низкая на компьютерах, на которых работают службы сертификации Active Directory.

Источники

CCE-9460-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9460-7&platform=win7

CCE-9488-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9488-8&platform=win7

Параметр Критичность: Высокий

Название **Аудит сведений об общем файловом ресурсе**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит попыток доступа к файлам и папкам в общих папках. Параметр позволяет протоколировать события при любой попытке обращения к файлу или папке, в то время как параметр "Общие папки" записывает только одно событие для любого подключения, установленного между клиентом и общей папкой. В события аудита этого параметра включаются подробные сведения о разрешениях или других критериях предоставления или запрета доступа. Если этот параметр настроен, при попытке обращения к файлу или папке в общей папке возникает событие аудита. Администратор может включить выполнение аудита для успешного выполнения, отказа или того и другого. Примечание: Для общих папок не предусмотрены системные списки управления доступом (SACL). Если этот параметр политики включен, выполняется аудит доступа ко всем общим файлам и папкам системы. Частота появления: высокая для файловых серверов или контроллеров домена, поскольку в соответствии с групповой политикой требуется доступ к сети SYSVOL.

Источники

CCE-8861-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8861-7&platform=win7

CCE-9720-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9720-4&platform=win7

Параметр Критичность: Высокий

Название **Аудит общих папок**

Описание

Эталонное значение: **Отказ**

Этот параметр политики позволяет вести аудит попыток доступа к общим папкам. Если этот параметр настроен, при попытке доступа к общей папке возникает событие аудита. Если этот параметр задан, администратор может указывать выполнение аудита только успешных выполнений, отказов или того и другого. Примечание. Для общих папок не предусмотрены системные списки управления доступом (SACL). Если этот параметр политики включен, осуществляется аудит доступа ко всем общим папкам в системе. Частота появления: высокая для файловых серверов или контроллеров домена, поскольку в соответствии с групповой политикой требуется доступ к сети SYSVOL.

Источники

CCE-9376-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9376-5&platform=win7

CCE-9405-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9405-2&platform=win7

Параметр Критичность: Высокий

Название **Аудит файловой системы**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит попыток доступа к объектам файловой системы со стороны пользователей. События аудита безопасности возникают только для тех объектов, для которых заданы системные списки управления доступом (SACL), и только в том случае, если запрашивается тип доступа на запись, чтение или изменение и запрашивающая учетная запись соответствует параметрам, установленным в списке SACL. Если этот параметр политики настроен, события аудита возникают при каждой операции доступа к объекту файловой системы с соответствующим списком SACL со стороны учетной записи. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при доступе к объекту файловой системы с соответствующим списком SACL со стороны учетной записи никаких событий аудита не возникает. Примечание. Чтобы задать список SACL для объекта файловой системы, воспользуйтесь вкладкой "Безопасность" диалогового окна "Свойства" объекта. Частота появления: зависит от параметров списков SACL файловой системы.

Источники

CCE-9217-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9217-1&platform=win7

CCE-9811-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9811-1&platform=win7

Параметр Критичность: Недоступно

Название **Аудит подключения платформы фильтрации**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит подключений, которые разрешаются или блокируются платформой фильтрации Windows (WFP). Отслеживаются следующие события: - Блокировка приема входящих сетевых подключений службой брандмауэра Windows. - Разрешение подключения платформой WFP. - Блокировка подключения платформой WFP. - Разрешение на привязку к локальному порту платформой WFP. - Блокировка привязки к локальному порту платформой WFP. - Разрешение подключения платформой WFP. - Блокировка подключения платформой WFP. - Разрешение платформы WFP на прослушивание порта входящих подключений приложением или службой. - Блокировка платформы WFP на прослушивание порта входящих подключений приложением или службой. Если этот параметр политики настроен, события аудита возникают при разрешении или блокировке подключений платформой WFP. При разрешении подключений возникают успешные события аудита, при блокировке - неудачные. Если этот параметр политики не настроен, при разрешении или блокировке подключений платформой WFP никакие события аудита не возникают. Частота появления: высокая.

Источники

CCE-9569-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9569-5&platform=win7

CCE-9728-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9728-7&platform=win7

Параметр Критичность: Высокий

Название **Аудит отбрасывания пакетов платформой фильтрации**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит пакетов, отбрасываемых платформой фильтрации Windows (WFP). Частота появления: высокая.

Источники

CCE-9133-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9133-0&platform=win7

Параметр Критичность: Высокий

Название **Аудит работы с дескрипторами**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит событий, возникающих при открытии или закрытии дескриптора объекта. События аудита безопасности возникают только для объектов с соответствующим системным списком управления доступом (SACL). Если этот параметр политики настроен, событие аудита возникает при выполнении операции с дескриптором. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при работе с дескриптором никакие события аудита не возникают. Примечание. События этой подкатегории возникают только для тех типов объектов, для которых включена подкатегория доступа к объектам. Например, события аудита безопасности работы с дескриптором возникают в том случае, если включен доступ к объектам файловой системы. Если доступ к объектам реестра не включен, события аудита безопасности работы с дескриптором не возникают. Частота появления: зависит от параметров списков SACL.

Источники

CCE-9789-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9789-9&platform=win7

CCE-10098-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10098-2&platform=win7

Параметр Критичность: Высокий

Название **Аудит объектов ядра**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит попыток доступа к ядру с использованием мьютексов и семафоров. События аудита безопасности возникают только для объектов ядра с соответствующим системным списком управления доступом (SACL). Примечание. Аудит: установленные по умолчанию списки SACL для объектов ядра управляются параметром аудита доступа глобальных системных объектов. Частота появления: высокая, если включен аудит доступа глобальных системных объектов.

Источники

CCE-9137-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9137-1&platform=win7

CCE-9803-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9803-8&platform=win7

Параметр Критичность: Высокий

Название **Аудит других событий доступа к объектам**

Описание

Эталонное значение: **Отказ**

Этот параметр политики обеспечивает аудит событий, возникающих при управлении заданиями планировщика задач или объектами COM+. Для заданий планировщика отслеживаются следующие события: - Создание задания. - Удаление задания. - Включение задания. - Отключение задания. - Обновление задания. Для объектов COM+ отслеживаются следующие события: - Добавление объекта каталога. - Обновление объекта каталога. - Удаление объекта каталога. Частота появления: низкая.

Источники

CCE-9455-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9455-7&platform=win7

CCE-9545-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9545-5&platform=win7

Параметр Критичность: Высокий

Название **Аудит реестра**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит попыток доступа к объектам реестра. События аудита безопасности возникают только для тех объектов, для которых заданы системные списки управления доступом (SACL), и только в том случае, если запрашивается тип доступа на чтение, запись или изменение и запрашивающая учетная запись соответствует параметрам, установленным в списке SACL. Если этот параметр политики настроен, события аудита возникают при каждой операции доступа к объекту реестра с соответствующим списком SACL со стороны учетной записи. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при доступе к объекту реестра с соответствующим списком SACL со стороны учетной записи никаких событий аудита не возникает. Примечание. Чтобы задать список SACL для объекта реестра, воспользуйтесь диалоговым окном "Разрешения". Частота появления: зависит от параметров списков SACL реестра.

Источники

CCE-9737-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9737-8&platform=win7

CCE-10078-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10078-4&platform=win7

Параметр Критичность: Высокий

Название **Аудит диспетчера учетных записей безопасности**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит событий, возникающих при попытке доступа к объектам диспетчера учетных записей безопасности (SAM). К объектам SAM относятся следующие: - SAM_ALIAS - локальная группа. - SAM_GROUP - группа, не являющаяся локальной. - SAM_USER - учетная запись пользователя. - SAM_DOMAIN - домен. - SAM_SERVER - учетная запись компьютера. Если этот параметр политики настроен, события аудита возникают при попытке доступа к объекту ядра. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр не настроен, при попытке доступа к объекту ядра никакие события аудита не возникают. Примечание. Изменять можно только системный список управления доступом (SACL) для объекта SAM_SERVER. Частота появления: высокая для контроллеров домена.

Источники

CCE-9845-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9845-9&platform=win7

CCE-9856-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9856-6&platform=win7

Группа

Название **2.3.7 Изменение политики**

Описание

Здесь можно назначить аудит каждого случая внесения изменений в политики назначения прав пользователей, политики брандмауэра Windows, политики доверия или сами политики аудита. Рекомендуемые параметры позволят отслеживать ситуации, в которых производится попытка повысить уровень своих привилегий.

Параметр Критичность: Высокий

Название **Аудит изменения политики аудита**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит изменений параметров политики аудита безопасности, таких как следующие: - Установка разрешений и параметров аудита для объекта политики аудита. - Изменения в политике аудита системы. - Регистрация источников событий безопасности. - Отмена регистрации источников событий безопасности. - Изменения параметров аудита для отдельных пользователей. - Изменения значения параметра CrashOnAuditFail. - Изменения системного списка управления доступом для объекта файловой системы или реестра. - Изменения списка специальных групп. Примечание. Аудит изменений в системном списке управления доступом (SACL) выполняется при изменении списка SACL для объекта, если при этом включена категория изменений политики. Аудит изменений в списке управления доступом на уровне пользователей (DACL) и изменений владения осуществляется в том случае, если включен аудит доступа к объектам и для списка SACL объекта настроен аудит изменений списка DACL или владения. Если этот параметр политики настроен, событие аудита возникает при попытке установления удаленного подключения RPC. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при попытке установления удаленного подключения RPC никакие события аудита не возникают. Частота появления: низкая. По умолчанию: успех.

Источники

CCE-10021-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10021-4&platform=win7

CCE-9235-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9235-3&platform=win7

Параметр Критичность: Высокий

Название **Аудит изменения политики проверки подлинности**

Описание

Эталонное значение: **Успех**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении изменений групп безопасности, таких как следующие: - Создание отношений доверия для леса или домена. - Изменение отношений доверия для леса или домена. - Удаление отношений доверия для леса или домена. - Изменения политики Kerberos по следующему пути: Конфигурация компьютера\Параметры Windows\Параметры безопасности\Политики учетных записей\Политика Kerberos. - Предоставление пользователю или группе следующих прав: - Доступ к компьютеру из сети. - Локальный вход. - Вход с использованием служб терминалов. - Вход с использованием пакетного задания. - Вход в службу. - Конфликт пространств имен (например, если имя нового отношения доверия совпадает с именем существующего пространства имен). Если этот параметр настроен, при попытке изменения политики проверки подлинности возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при изменении политики проверки подлинности никакие события аудита не возникают. Примечание. Событие аудита безопасности регистрируется в случае применения параметра политики. Во время изменения параметров события не регистрируются. Частота появления: низкая. По умолчанию: успех.

Источники

CCE-9976-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9976-2&platform=win7

CCE-10014-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10014-9&platform=win7

Параметр Критичность: Высокий

Название **Аудит изменения политики авторизации**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении изменений политики авторизации, таких как следующие: - Назначение прав (привилегий) пользователей, например, SeCreateTokenPrivilege, которые не проходят аудит в подкатегории "Изменение политики проверки подлинности". - Удаление прав (привилегий) пользователей, например, SeCreateTokenPrivilege, которые не проходят аудит в подкатегории "Изменение политики проверки подлинности". - Изменения политики шифрованной файловой системы (EFS). Если этот параметр политики настроен, событие аудита возникает при попытке изменения политики авторизации. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при изменении политики авторизации никакие события аудита не возникают. Частота появления: низкая. По умолчанию: нет аудита.

Источники

CCE-9633-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9633-9&platform=win7

CCE-10050-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10050-3&platform=win7

Параметр Критичность: Высокий

Название **Аудит изменения политики платформы фильтрации**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении изменений платформы фильтрации Windows (WFP), таких как следующие: - Состояние служб IPsec. - Изменения параметров политики IPsec. - Изменения параметров политики брандмауэра Windows. - Изменения поставщиков и модуля WFP. Если этот параметр политики настроен, событие аудита возникает при попытке изменений платформы WFP. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при изменении платформы WFP никакие события аудита не возникают. Частота появления: низкая. По умолчанию: нет аудита.

Источники

CCE-10081-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10081-8&platform=win7

CCE-9902-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9902-8&platform=win7

Параметр Критичность: Высокий

Название **Аудит изменения политики на уровне правил MPSSVC**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при изменении правил политики, используемых службой защиты Майкрософт (MPSSVC). Эта служба используется брандмауэром Windows. Отслеживаются следующие события: - Сообщения от активных политик при запуске службы брандмауэра Windows. - Изменения правил брандмауэра Windows. - Изменения в списке исключений брандмауэра Windows. - Изменения параметров брандмауэра Windows. - Пропуск или неприменение правил службой брандмауэра Windows. - Изменения параметров групповой политики брандмауэра Windows. Если этот параметр политики настроен, при попытке изменения правил, используемых службой MPSSVC, возникает событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при изменении правил политики, используемых службой MPSSVC, никакие события аудита не возникают. Частота появления: низкая. По умолчанию: нет аудита.

Источники

CCE-9913-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9913-5&platform=win7

CCE-9153-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9153-8&platform=win7

Параметр Критичность: Высокий

Название **Аудит других событий изменения политики**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении других изменений политики безопасности, не проходящих аудит в этой категории, таких как следующие: - Изменения конфигурации доверенного платформенного модуля (TPM). - Самотестирование шифрования в режиме ядра. - Операции поставщиков служб шифрования. - Контекстные операции или изменения шифрования. Частота появления: низкая. По умолчанию: нет аудита.

Источники

CCE-9596-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9596-8&platform=win7

CCE-10049-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10049-5&platform=win7

Группа

Название **2.3.8 Использование прав**

Описание

Эта категория контролирует аудит случаев использования предоставленных привилегий. Если задать этому параметру значение Успех, будет создаваться запись аудита каждый раз, когда пользователь успешно пользуется своим правом. Если задать значение Отказ, запись будет создаваться каждый раз, когда пользователю не удается воспользоваться привилегией. Количество записей, генерируемых этой политикой, может быть очень большим.

Параметр Критичность: Высокий

Название **Аудит использования прав, не затрагивающих конфиденциальные данные**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит событий, возникающих при использовании прав, не затрагивающем конфиденциальные данные (пользовательские права). Использование следующих прав не затрагивает конфиденциальные данные: - Доступ к диспетчеру учетных данных от имени доверенного вызывающего. - Доступ к компьютеру из сети. - Добавление рабочих станций к домену. - Настройка квот памяти для процесса. - Локальный вход в систему. - Вход в систему через службу терминалов. - Обход перекрестной проверки. - Изменение системного времени. - Создание файла подкачки. - Создание глобальных объектов. - Создание постоянных общих объектов. - Создание символических ссылок. - Запрет на доступ к компьютеру из сети. - Отказ во входе в качестве пакетного задания. - Отказ во входе в качестве службы. - Запрет на локальный вход. - Запрет на вход в систему через службу терминалов. - Принудительное удаленное завершение работы. - Увеличение рабочего набора процесса. - Увеличение приоритета выполнения. - Блокировка страниц в памяти. - Вход в качестве пакетного задания. - Вход в качестве службы. - Изменение метки объекта. - Выполнение задач по обслуживанию томов. - Профилирование одного процесса. - Профилирование производительности системы. - Отключение компьютера от стыковочного узла. - Завершение работы системы. - Синхронизация данных службы каталогов. Если этот параметр политики настроен, событие аудита возникает при вызове прав, не затрагивающем конфиденциальные данные. Успешные и неудачные вызовы регистрируются в соответствующих записях аудита. Если этот параметр политики не настроен, при вызове прав, не затрагивающем конфиденциальные данные, никакие события аудита не возникают. Частота появления: очень высокая.

Источники

CCE-9159-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9159-5&platform=win7

CCE-9190-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9190-0&platform=win7

Параметр Критичность: Высокий

Название **Аудит других событий использования прав**

Описание

Эталонное значение: **Успех и Отказ**

Другие события использования прав.

Источники

CCE-9314-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9314-6&platform=win7

CCE-9988-7
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9988-7&platform=win7

Параметр Критичность: Высокий

Название **Аудит использования прав, затрагивающих конфиденциальные данные**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики обеспечивает аудит событий, возникающих при использовании прав, затрагивающем конфиденциальные данные (пользовательских прав), следующим образом: - Вызов привилегированной службы. - Вызов одной из следующих привилегий: - Действие от имени компонента операционной системы. - Архивация файлов и каталогов. - Создание объекта-токена. - Отладка программ. - Включение учетных записей компьютеров и пользователей, которым разрешено делегирование. - Создание аудита безопасности. - Олицетворение клиента после проверки подлинности. - Загрузка и выгрузка драйверов устройств. - Управление журналом аудита и безопасности. - Изменение значения параметров аппаратной среды. - Замена токена на уровне процесса. - Восстановление файлов и каталогов. - Смена владельца файла или другого объекта. Если этот параметр политики настроен, события аудита возникают при выполнении запросов с использованием прав, затрагивающим конфиденциальные данные. Успешные и неудачные запросы регистрируются в соответствующих записях. Если этот параметр политики не настроен, при выполнении запросов с использованием прав, затрагивающим конфиденциальные данные, никакие события аудита не возникают. Частота появления: высокая.

Источники

CCE-9878-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9878-0&platform=win7

CCE-9172-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9172-8&platform=win7

Группа

Название **2.3.9 Система**

Описание

Эта категория определяет способ аудита системных событий, которые завершились успехом или неудачей. Анализ ее записей может помочь в обнаружении попыток несанкционированного доступа к системе. Под системными событиями понимаются запуск и завершение работы компьютеров, переполнение журналов событий и иные события из области безопасности, которые оказывают влияние на систему целиком

Параметр Критичность: Высокий

Название **Аудит драйвера IPsec**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит событий, возникающих в драйвере фильтров IPsec, таких как следующие: - Запуск и завершение работы служб IPsec. - Отбрасывание сетевых пакетов из-за сбоя проверки целостности. - Отбрасывание сетевых пакетов из-за сбоя проверки получения повторного пакета. - Отбрасывание сетевых пакетов из-за наличия в них открытого текста. - Получение сетевых пакетов с неверным значением индекса параметра безопасности (SPI). Это может свидетельствовать о неправильной работе сетевой карты или необходимости обновления драйвера. - Ошибки при обработке фильтров IPsec. Если этот параметр политики настроен, события аудита возникают при выполнении операций драйвера фильтров IPsec. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при выполнении операций драйвера фильтров IPsec никакие события аудита не возникают. Частота появления: низкая. По умолчанию: нет аудита.

Источники

CCE-9925-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9925-9&platform=win7

CCE-9802-0
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9802-0&platform=win7

Параметр Критичность: Высокий

Название **Аудит других системных событий**

Описание

Эталонное значение: **Нет аудита**

Этот параметр политики позволяет вести аудит следующих событий: - Запуск и завершение работы службы и драйвера брандмауэра Windows. - Обработка политики безопасности службой брандмауэра Windows. - Операции с файлами ключей шифрования и операции миграции. Частота появления: низкая. По умолчанию: успех, отказ.

Источники

CCE-10088-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-10088-3&platform=win7

CCE-9586-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9586-9&platform=win7

Параметр Критичность: Высокий

Название **Аудит изменения состояния безопасности**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит событий, возникающих при выполнении изменений состояния безопасности компьютера, таких как следующие: - Запуск и завершение работы компьютера. - Изменение системного времени. - Восстановление системы при событии CrashOnAuditFail, которое регистрируется после перезапуска системы в том случае, если журнал событий заполнен и настроена запись реестра CrashOnAuditFail. Частота появления: низкая. По умолчанию: успех

Источники

CCE-9850-9
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9850-9&platform=win7

CCE-9179-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9179-3&platform=win7

Параметр Критичность: Высокий

Название **Аудит расширения системы безопасности**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит событий, связанных с расширением системы безопасности, таких как следующие: - Загрузка расширения системы безопасности, например, пакета проверки подлинности, уведомления или безопасности, и его регистрация в системе администратора локальной безопасности (LSA). Оно используется для проверки подлинности при попытке входа, отправки запросов на вход в систему, а также при любых изменениях учетных записей или паролей. Примерами расширений системы безопасности являются Kerberos и NTLM. - Установка и регистрация службы в диспетчере управления службами. В журнале аудита регистрируются сведения об имени, двоичных файлах, типе, типе запуска и учетной записи службы. Если этот параметр политики настроен, события аудита возникают при попытке загрузки расширения системы безопасности. Успешные и неудачные события аудита регистрируются в соответствующих записях. Если этот параметр политики не настроен, при загрузке расширения системы безопасности никакие события аудита не возникают. Частота появления: низкая. События расширения системы безопасности чаще возникают на контроллере домена, а не на клиентских компьютерах или рядовых серверах. По умолчанию: нет аудита.

Источники

CCE-9863-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9863-2&platform=win7

CCE-9998-6
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9998-6&platform=win7

Параметр Критичность: Высокий

Название **Аудит целостности системы**

Описание

Эталонное значение: **Успех и Отказ**

Этот параметр политики позволяет вести аудит событий, связанных с нарушениями целостности подсистемы безопасности, такими как следующие: - События, которые не удается записать в журнал событий из-за ошибок системы аудита. - Процессы, использующие недопустимый порт локального вызова процедур (LPC) для олицетворения клиента посредством ответа, чтения или записи в адресном пространстве клиента. - Обнаружение удаленного вызова процедур (RPC), нарушающего целостность системы. - Обнаружение недопустимого значения хеша исполняемого файла средством проверки целостности кода. - Операции шифрования, нарушающие целостность системы. Частота появления: низкая. По умолчанию: успех, отказ.

Источники

CCE-9520-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9520-8&platform=win7

CCE-9194-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9194-2&platform=win7

Группа

Название **2.4 Политики домена**

Описание

Группа включает в себя политику блокировки учетных записей и политику паролей.

Ссылки

Ресурс

Тип	GPO
Источник	Computer Configuration\Windows Settings\Security Settings\Account Policies

Группа

Название **2.4.1 Политика паролей**

Описание

Сложные, регулярно сменяемые пароли снижают вероятность успешного подбора пароля. Политика паролей контролирует сложность и срок использования каждого пароля. Ее параметры задаются групповой политикой на уровне

домена. Помимо перечисленных ниже политик пароля, в некоторых организациях требуется централизованный контроль всех пользователей. В этом разделе рассказывается, как предотвратить изменение паролей пользователями, за исключением случаев, когда это изменение санкционировано. Централизованный контроль паролей пользователей - краеугольный камень хорошо спроектированной системы обеспечения безопасности Windows. С помощью групповой политики можно задать минимальный и максимальный срок действия пароля. Однако, если пароль требуется менять слишком часто, пользователям удастся обойти требования параметра Вести журнал паролей, если он установлен в вашей среде. Или, если минимально разрешенная длина пароля слишком велика, может увеличиться число обращений в службу поддержки по поводу забытого пароля. Пользователи могут изменить свой пароль в промежутке между минимальным и максимальным сроком его действия. Однако, конфигурация SSLF предусматривает, что менять пароль разрешается только по запросу самой операционной системы, который выдается по истечении его максимального срока действия в 90 дней. Для достижения такой степени контроля можно отключить кнопку Смена пароля диалогового окна Безопасность Windows, которое появляется при нажатии клавиш CTRL+ALT+DEL. Данное изменение можно ввести в силу для всего домена, используя групповую политику, а можно для отдельных пользователей, используя редактор реестра. Параметры политики паролей в редакторе объектов групповой политики расположены по следующему пути: Конфигурация компьютера\Конфигурация Windows\Параметры безопасности \Политики учетных записей\Политика паролей.

Ссылки

Ресурс

Тип	GPO
Источник	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

Параметр Критичность: Высокий

Название **Вести журнал паролей**

Описание

Эталонное значение: **24 пароля**

Этот параметр безопасности определяет число новых уникальных паролей, которые должны быть назначены учетной записи пользователя до повторного использования старого пароля. Число паролей должно составлять от 0 до 24. Эта политика позволяет администраторам улучшать безопасность, гарантируя, что старые пароли не будут повторно использоваться постоянно. По умолчанию: 24 на контроллерах домена. 0 на автономных серверах. Примечание. По умолчанию компьютеры-члены домена используют конфигурацию своих контроллеров домена. Чтобы сохранить эффективность журнала паролей, не позволяйте изменять пароль снова сразу после того, как он был изменен. Включите также параметр политики безопасности "Минимальный срок действия пароля".

Источники

CCE-8912-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-8912-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей

Параметр Критичность: Высокий

Название **Максимальный срок действия пароля**

Описание

Эталонное значение: **90 дней**

Этот параметр безопасности определяет период времени (в днях), в течение которого можно использовать пароль, пока система не потребует от пользователя сменить его. Срок действия пароля может составлять от 1 до 999 дней; значение 0 соответствует неограниченному сроку действия пароля. Если значение максимального срока действия пароля составляет от 1 до 999 дней, то значение минимального срока действия пароля должно быть меньше максимального. Если значение максимального срока действия пароля равно 0, то минимальный срок действия пароля может принимать любые значения в диапазоне от 0 до 998 дней. Примечание. Рекомендуется устанавливать для срока действия паролей значение от 30 до

90 дней, в зависимости от рабочей среды. В этом случае у злоумышленника ограничено время, в течение которого он может взломать пароль пользователя и получить доступ к сетевым ресурсам. По умолчанию: 42.

Источники

CCE-9193-4
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9193-4&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей

Параметр Критичность: Высокий

Название **Минимальная длина пароля**

Описание

Эталонное значение: **12 знаков**

Этот параметр безопасности определяет минимальное количество знаков, которое должно содержаться в пароле пользователя. Можно установить значение от 1 до 14 знаков, либо 0 знаков, если пароль не требуется. По умолчанию: 7 - на контроллерах домена. 0 - на автономных серверах. Примечание. По умолчанию компьютеры-члены домена используют конфигурацию своих контроллеров домена.

Источники

CCE-9357-5
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9357-5&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей

Параметр Критичность: Высокий

Название **Минимальный срок действия пароля**

Описание

Эталонное значение: **1 день**

Этот параметр безопасности определяет период времени (в днях), в течение которого пользователь должен использовать пароль, прежде чем его можно будет изменить. Можно установить значение от 1 до 998 дней либо разрешить изменять пароль сразу, установив значение 0 дней. Значение минимального срока действия пароля должно быть меньше значения максимального срока действия пароля, за исключением значения максимального срока, равного 0 дней, означающего, что срок действия пароля никогда не истечет. Если значение максимального срока действия пароля равно 0, то минимальный срок действия пароля может принимать любые значения в диапазоне от 0 до 998 дней. Установите значение минимального срока действия пароля больше 0, чтобы включить ведение журнала паролей. Без установки минимального срока действия пароля пользователь может изменять пароли повторно, пока не получит свой старый предпочитаемый пароль. Значение по умолчанию установлено вопреки этой рекомендации, поэтому администратор может назначить пользователю пароль, а затем потребовать сменить его при входе пользователя в систему. Если для журнала паролей установлено значение 0, пользователю не нужно выбирать новый пароль. По этой причине значение для журнала паролей по умолчанию равно 1. По умолчанию: 1 - на контроллерах домена. 0 - на автономных серверах. Примечание. По умолчанию компьютеры-члены домена используют конфигурацию своих контроллеров домена.

Источники

CCE-9330-2
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9330-2&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей

Параметр Критичность: Высокий

Название **Пароль должен отвечать требованиям сложности**

Описание

Эталонное значение: **Включен**

Этот параметр безопасности определяет, должен ли пароль отвечать требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям. Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков Иметь длину не менее 6 знаков Содержать знаки трех из четырех перечисленных ниже категорий: Латинские заглавные буквы (от A до Z) Латинские строчные буквы (от a до z) Цифры (от 0 до 9) Отличающиеся от букв и цифр знаки (например, !, $, #, %) Требования сложности применяются при создании или изменении пароля. По умолчанию: Включены на контроллерах домена. Отключены на автономных серверах. Примечание. По умолчанию компьютеры-члены домена используют конфигурацию своих контроллеров домена.

Источники

CCE-9370-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9370-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей

Параметр Критичность: Высокий

Название **Хранить пароли, используя обратимое шифрование**

Описание

Эталонное значение: **Отключен**

Этот параметр безопасности определяет, используется ли операционной системой для хранения паролей обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности. Хранение паролей с помощью обратимого шифрования - по существу то же самое, что и хранение паролей открытым текстом. По этой причине данная политика не должна применяться, пока требования приложения не станут более весомыми, чем требования по защите паролей. Эта политика необходима при использовании проверки подлинности протокола CHAP через удаленный доступ или службу проверки подлинности в Интернете (IAS). Она также необходима при использовании краткой проверки подлинности в IIS. По умолчанию: Отключена.

Источники

CCE-9260-1
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9260-1&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей

Группа

Название **2.4.2 Политика блокировки учетной записи**

Описание

Эта политика в AD DS отвечает за блокировку учетной записи пользователя. Пользователь будет заблокирован и не сможет войти в систему, если в течение определенного времени произведет определенное количество неудачных попыток входа. Попытки входа отслеживаются контроллерами домена, и их число сравнивается с числом разрешенных. Период, на который блокируется учетная запись, зависит от параметров политики. Эти параметры позволяют защититься от подбора пароля и снижают вероятность успешной атаки на сетевую среду. Однако, их включение может вылиться в повышение количества обращений в службу поддержки. Есть и другой побочный эффект политики блокировки учетных записей после определенного числа неудачных попыток входа - возможность для проведения DoS-атаки. Например, некоторое вредоносное ПО может пытаться подключаться к другим компьютерам, используя заранее собранный список имен учетных записей и словарь часто используемых паролей. В результате учетные записи многих пользователей могут оказаться заблокированными при превышении числа неудачных попыток входа. Минимизировать риск такой DoS-атаки можно, задав относительно небольшой срок блокировки. Перед включением указанных ниже параметров убедитесь, что эти дополнительные усилия по управлению паролями одобряются руководством компании. Для многих предприятий более выгодным и экономичным решением станет автоматический анализ журналов событий безопасности на контроллерах домена с генерированием административных оповещений в случае, если есть подозрение на подбор пароля к учетной записи. Параметры политики блокировки учетной записи в редакторе объектов групповой политики расположены по следующему пути: Конфигурация компьютера\Конфигурация Windows\Параметры безопасности \Политики учетных записей\Политика блокировки учетной записи.

Ссылки

Ресурс

Тип	GPO
Источник	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

Параметр Критичность: Высокий

Название **Время до сброса счетчика блокировки**

Описание

Эталонное значение: **15 минут**

Этот параметр безопасности определяет количество минут, которые должны пройти после неудачной попытки входа в систему до того, как счетчик неудачных попыток входа будет сброшен до 0. Допустимые значения: от 1 до 99999 минут. Если определено пороговое значение блокировки учетной записи, то время сброса должно быть меньше или равно длительности блокировки учетной записи. По умолчанию: Не задано, т.к. этот параметр политики принимает значения, только если задано пороговое значение блокировки учетной записи.

Источники

CCE-9400-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9400-3&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика блокировки учетных записей

Параметр Критичность: Высокий

Название **Пороговое значение блокировки**

Описание

Эталонное значение: **10 ошибок входа в систему**

Этот параметр безопасности определяет количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя. Заблокированная учетная запись не может использоваться до тех пор, пока не будет сброшена администратором, либо пока не истечет период блокировки этой учетной записи. Количество неудачных попыток входа в систему может составлять от 0 до 999. Если установить это значение равным 0, то учетная запись никогда не будет разблокирована. Неудачные попытки ввода паролей на рабочих станциях или серверах-членах домена, заблокированных с помощью клавиш CTRL+ALT+DELETE или с помощью защищенных паролем заставок, считаются неудачными попытками входа в систему. По умолчанию: 0.

Источники

CCE-9136-3
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9136-3&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика блокировки учетных записей

Параметр Критичность: Высокий

Название **Продолжительность блокировки учетной записи**

Описание

Эталонное значение: **15 минут**

Этот параметр безопасности определяет количество минут, в течение которых учетная запись остается заблокированной до ее автоматической разблокировки. Допустимые значения: от 0 до 99999 минут. Если продолжительность блокировки учетной записи равна 0, то учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее. Если определено пороговое значение блокировки учетной записи, то длительность блокировки учетной записи должна быть больше или равна времени сброса. По умолчанию: Не задано, т.к. этот параметр политики принимает значения, только если определено пороговое значение блокировки учетной записи.

Источники

CCE-9308-8
http://ovaldb.altx-soft.ru/CCE.aspx?id=CCE-9308-8&platform=win7

Ссылки

Ресурс

Тип	GPO
Источник	Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика блокировки учетных записей