

6. Подготовка Windows-хоста

Агент **ничего не меняет в политике аудита хоста**. Он читает журналы и проверяет настройки. По умолчанию Windows не регистрирует большую часть нужных событий (создание процессов, изменение групп, проверку учётных данных), а размер журнала Security — 20 МБ. Такой журнал на сервере перезаписывается за часы.

В домене параметры задаются **групповой политикой** (§2–§5). На отдельных хостах и для проверки можно использовать скрипт `prepare-host.ps1` (§1). Доменная политика имеет приоритет: при следующем `groupdate` она перезапишет локальные значения.

Что читает агент

Канал	Нагрузка	Что нужно
Security	до 2 000 событий/с	расширенная политика аудита (§2), размер журнала (§4)
System	до 500 событий/с	установка служб (7045), изменение режима запуска (7040), остановки, перезагрузки (1074, 6005, 6006, 6008), очистка журнала (104)

Классифицируемые события Security: 4624, 4625, 4634, 4647, 4648, 4672, 4673, 4688, 4697, 4698, 4719, 4720, 4722–4726, 4728, 4732, 4733, 4740, 4756, 4767, 4776, 1100, 1102, 1104, 4946–4948, 6416.

1. Быстрая подготовка: `prepare-host.ps1`

Скрипт находится в `deploy/host-prep/windows/` внутри `gits-deploy_<ver>.zip`. Запуск от имени администратора:

```
powershell -ExecutionPolicy Bypass -File prepare-host.ps1 -Check      # только отчёт; код возврата 1 – нес
оответствия
powershell -ExecutionPolicy Bypass -File prepare-host.ps1            # применить
powershell -ExecutionPolicy Bypass -File prepare-host.ps1 -NtpServer ntp1.bank.local,ntp2.bank.local -Ena
bleWinRM
```

Параметр	Действие
<code>-Check</code>	ничего не менять
<code>-SecurityLogMB</code>	размер журнала Security, МБ (по умолчанию 1024; для серверов рекомендуется 4096)
<code>-OtherLogMB</code>	размер журналов System и Application, МБ (по умолчанию 256)
<code>-NtpServer</code>	источники NTP для хостов вне домена
<code>-EnableWinRM</code>	включить WinRM для push-установки агента (§6)

Скрипт настраивает подкатегории аудита по GUID, поэтому работает при любом языке ОС. Он задаёт параметры реестра из §3, размеры журналов, режим запуска W32Time и проверяет источник времени. Текущие значения подкатегорий читаются так же, как их читает агент: через `auditpol /backup`. Повторный запуск ничего не меняет.

2. Расширенная политика аудита

GPO: «Конфигурация компьютера» → «Политики» → «Конфигурация Windows» → «Параметры безопасности» → «Конфигурация расширенной политики аудита» → «Политики аудита».

Подкатегория	GUID	Требуется	События
Вход в систему (Logon)	{0CCE9215-...}	Успех и сбой	4624, 4625, 4648
Выход из системы (Logoff)	{0CCE9216-...}	Успех	4634, 4647
Блокировка учётной записи (Account Lockout)	{0CCE9217-...}	Сбой	4625 (заблокированная УЗ)
Специальный вход (Special Logon)	{0CCE921B-...}	Успех	4672
Проверка учётных данных (Credential Validation)	{0CCE923F-...}	Успех и сбой	4776
Управление учётными записями пользователей	{0CCE9235-...}	Успех и сбой	4720, 4722–4726, 4740, 4767
Управление группами безопасности	{0CCE9237-...}	Успех и сбой	4728, 4732, 4733, 4756
Создание процесса (Process Creation)	{0CCE922B-...}	Успех	4688
Изменение политики аудита	{0CCE922F-...}	Успех и сбой	4719
Изменение политики проверки подлинности	{0CCE9230-...}	Успех	—
Использование прав, затрагивающее конфиденциальные данные	{0CCE9228-...}	Успех и сбой	4673
Изменение состояния безопасности	{0CCE9210-...}	Успех	—
Расширение системы безопасности	{0CCE9211-...}	Успех (рекоменд.)	4697
Другие события доступа к объектам	{0CCE9227-...}	Успех (рекоменд.)	4698 (задания планировщика)
Изменение политики на уровне правил MPSSVC	{0CCE9232-...}	Успех (рекоменд.)	4946–4948 (правила брандмауэра)
События Plug and Play	{0CCE9248-...}	Успех (рекоменд.)	6416 (внешние устройства)

Суффикс всех GUID: -69AE-11D9-BED3-505054503030. Первые 12 строк проверяет CHK-MAS-010a. Остальные нужны, чтобы соответствующие события вообще появлялись в журнале.

Вручную (имена подкатегорий локализованы, поэтому указывайте GUID):

```
auditpol /set /subcategory:{0CCE922B-69AE-11D9-BED3-505054503030} /success:enable
auditpol /get /category:*
```

3. Параметры реестра аудита

Параметр	GPO	Реестр (DWORD = 1)
Принудительное использование подкатегорий	«Параметры безопасности» → «Локальные политики» → «Параметры безопасности» → «Аудит: принудительно переопределяет параметры категорий политики аудита...»	HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy
Командная строка в 4688	«Административные шаблоны» → «Система» → «Аудит создания процессов» → «Включать командную строку в события создания процессов»	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit\ProcessCreationIncludeCmdLine_Enabled
Журналирование блоков сценариев PowerShell	«Административные шаблоны» → «Компоненты Windows» → «Windows PowerShell» → «Включить ведение журнала блоков сценариев PowerShell»	HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\EnableScriptBlockLogging

Командная строка процессов и блоки сценариев PowerShell могут содержать пароли, переданные в параметрах. Доступ к журналам Security и Microsoft-Windows-PowerShell/Operational ограничьте администраторами. Канал PowerShell/Operational агент сейчас не собирает: CHK-MAS-010a проверяет только сам параметр.

4. Размеры журналов

GPO: «Административные шаблоны» → «Компоненты Windows» → «Служба журнала событий» → Security / System / Application → «Максимальный размер журнала (КБ)».

Журнал	Минимум (CHK-MAS-013a)
Security	1 048 576 КБ (1 ГБ) на APM; для серверов рекомендуется 4 194 304 КБ
System, Application	262 144 КБ (256 МБ)

Без GPO: `wevtutil sl Security /ms:1073741824`. Если размер задан и групповой политикой, и параметром службы, действует значение из политики.

5. Время

Члены домена синхронизируются с контроллером домена (`W32Time\Parameters\Type = NT5DS`). Хосты вне домена синхронизируются с внутренними серверами NTP:

```
w32tm /config /manualpeerlist:"ntp1.bank.local,0x8 ntp2.bank.local,0x8" /syncfromflags:manual /update
w32tm /resync
w32tm /query /source          :: не «Local CMOS Clock» и не «Free-running System Clock»
```

Служба W32Time должна работать и запускаться автоматически. CHK-MAS-009a проверяет тип синхронизации, источник и расхождение с часами сервера (не более 5 секунд).

6. WinRM для push-установки

Нужен только для push-установки агента из консоли (04 §7).

```
Enable-PSRemoting -Force -SkipNetworkProfileCheck # слушатель HTTP 5985, правило брандмауэра
```

- Исполнитель (ядро или ретранслятор) подключается к порту 5985 по NTLM с шифрованием сообщений или к порту 5986 по HTTPS с Basic-аутентификацией. Разрешите ему доступ на межсетевом экране хоста.
- Для входа **локальной** учётной записью администратора по сети нужен `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy = 1`. Скрипт с `-EnableWinRM` задаёт этот параметр. Для доменных администраторов он не требуется.
- После установки агентов WinRM можно отключить, если он не нужен для других задач.

7. Прочее

- **Службы.** Должны работать «Журнал событий Windows» (EventLog) и WMI (Winmgmt). Нужен Windows PowerShell 5.x в `%SystemRoot%\System32\WindowsPowerShell\v1.0`: часть проверок выполняется через него.
- **Антивирус.** Добавьте в исключения `%ProgramFiles%\GITS Agent\` и `%ProgramData%\GITS\agent\`.

8. Проверки агента и настройки хоста

Проверка	Что должно быть	Где настроить
CHK-MAS-010a	подкатегории аудита (§2), параметры реестра (§3)	GPO: расширенная политика аудита
CHK-MAS-013a	размеры журналов (§4)	GPO: служба журнала событий
CHK-MAS-009a	NT5DS или NTP, источник не локальные часы, расхождение не более 5 с	W32Time
CHK-UZP-010a	состав локальной группы «Администраторы» соответствует утверждённому эталону	GPO «Группы с ограниченным доступом», эталон в консоли
CHK-UZP-010b	UAC: <code>EnableLUA=1</code> , <code>ConsentPromptBehaviorAdmin</code> 1 или 2, <code>ConsentPromptBehaviorUser</code> 0 или 1, <code>PromptOnSecureDesktop=1</code>	GPO: «Параметры безопасности» → «Контроль учётных записей»
CHK-RD-011a	блокировка после 1–10 неудачных попыток; длительность блокировки и сброс счётчика — не меньше 30 мин	GPO: «Политика блокировки учётной записи»
CHK-RD-019, 021, 023, 025	срок действия пароля не больше 365 дней и не 0; длина не меньше 8; сложность включена; минимальный срок не меньше 1 дня	GPO: «Политика паролей»
CHK-RD-013a, 014a, 015	блокировка сеанса разрешена; неактивность не больше 900 с; хранитель экрана с паролем	GPO компьютера и пользователя
CHK-RD-018a	<code>LmCompatibilityLevel=5</code> , <code>NoLMHash=1</code> , подпись SMB всегда, <code>LDAPClientIntegrity ≥ 1</code>	GPO: «Параметры безопасности»
CHK-RD-030a	<code>RestrictAnonymous=1</code> , <code>RestrictAnonymousSAM=1</code> , <code>EveryoneIncludesAnonymous=0</code>	GPO: «Сетевой доступ»
CHK-RD-034	заполнены «Отказать в доступе к компьютеру из сети» и «Запретить вход через службы удалённых рабочих столов»	GPO: «Назначение прав пользователя»
CHK-RD-036, 037a	показ сведений о предыдущих входах; не показывать последнего пользователя; Ctrl+Alt+Del не отключён; текст уведомления задан	GPO: «Интерактивный вход»
CHK-RD-031	на общих папках нет прав «Изменение» и «Полный доступ» для Everyone, Users, Authenticated Users	права общих папок

Проверка	Что должно быть	Где настроить
CHK-RD-005a	службы не работают под персональными доменными учётными записями	службы
CHK-CZI-019b	AlwaysInstallElevated=0; SmartScreen включён	GPO
CHK-CZI-017, CHK-CZI-024, CHK-CZI-026b	утверждённые эталоны ПО и целостности; нет Java Runtime без обоснования	консоль, карточка хоста
CHK-ZVK-001b, 008, 009, 010, 006, 012	Microsoft Defender: защита включена, сигнатуры не старше суток, защита в реальном времени, Tamper Protection, проверка съёмных дисков, расписание полной проверки	GPO: Microsoft Defender
CHK-ZUD-010	ноутбуки: BitLocker на системном томе, TPM+PIN	GPO: шифрование диска BitLocker
CHK-MAS-021	буфер агента заполнен меньше чем на 80 %, доставка работает	связь с сервером

9. Самопроверка

```
powershell -ExecutionPolicy Bypass -File prepare-host.ps1 -Check
auditpol /get /category:*
Get-WinEvent -LogName Security -MaxEvents 5 | Format-Table Id, TimeCreated
sc.exe query gits-agent
```

На стенде (Windows 10 LTSC 2021, русская локаль, член домена) скрипт исправил 18 параметров. После этого все требования аудита и журналов выполнены. Осталось одно несоответствие: источник времени Local CMOS Clock, так как хост не синхронизировался с контроллером домена.