Руководство по справочной информации в файле журнала

Программное обеспечение McAfee ePolicy Orchestrator 5.1.0

Файлы журнала ePolicy Orchestrator

Файлы журналов, описанные в этом руководстве, представляют собой лишь часть файлов журналов McAfee® ePolicy Orchestrator® — внимание здесь обращено, в первую очередь, на те файлы журналов, которые используются при управлении продуктами и устранении проблем с ними.

Файлы журналов и их категории

Программное обеспечение McAfee ePolicy Orchestrator создает файлы журналов, содержащие важную информацию, необходимую для поиска и устранения неполадок.

Указанные файлы журналов делятся на три категории:

- Журналы установщика — включают сведения о пути установки, учетных данных пользователя, использованной базе данных и настроенных портах связи.
- Журналы сервера — включают сведения о функциях сервера, истории событий клиента и службах администрирования.
- Журналы агента — включают сведения об установке агента, его вызовах, обновлении и применении политик.

Использование переменных пути

Расположение файлов журнала зависит от того, как и где ePolicy Orchestrator и агент установлены в вашей среде.

Эти переменные используются в данном документе для указания мест расположения файлов журнала.

Переменная	Описание
[ПУТЬ_К_ДАННЫМ_АГЕНТА]	Чтобы определить фактическое местоположение файлов данных агента, посмотрите раздел реестра `HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\TVD\SHARED COMPONENTS\FRAMEWORK\DATA PATH`. Дополнительную информацию см. в разделе *Каталог установки агента* в руководстве по продукту ePolicy Orchestrator или в справке.
%temp%	Это папка Temp пользователя, находящегося в системе в данный момент. Для перехода к этой папке выберите **Пуск** | **Выполнить**, затем введите `%temp%` в текстовом поле **Открыть** и щелкните **ОК**.
[КАТАЛОГ_УСТАНОВКИ]	Местоположение по умолчанию программного обеспечения сервера ePolicy Orchestrator: `C:\PROGRAM FILES\MCAFEE\EPOLICY ORCHESTRATOR`

Журналы установщика

Файлы журналов установщика содержат перечень сведений об установке ePolicy Orchestrator.

Указанные журналы содержат следующую информацию:

- действия, выполненные определенными компонентами;
- службы администрирования, использованные сервером;
- успех или неудачное завершение ключевых процессов.

Имя файла	Тип журнала	Местоположение	Описание
`AH500-Install-MSI.log`	Установка обработчиков агентов	`%temp%\McAfeeLogs`	В указанный файл записываются все сведения об установке обработчика агентов, включая следующие: • действия установщика; • сбои при установке.
`AH500-ahetupdll.log`	Временный	`%temp%` (на сервере обработчика агентов)	В указанный файл записываются выходные события обработчика агентов.
`core-install.log`	Временный	`%temp%\McAfeeLogs\ePO500-Troubleshoot\MFS`	Создается при вызове установщика MFS ANT из установщика ePolicy Orchestrator. Содержит следующую информацию: • создание таблиц базы данных сервера; • установка компонентов сервера. В случае успешного завершения установки данный файл удаляется.
`epo-install.log`	Установка	`%temp%\McAfeeLogs\ePO500-Troubleshoot\Mercury Framework`	Создается при вызове установщика ePO ANT из установщика ePolicy Orchestrator.

Имя файла	Тип журнала	Местоположение	Описание
EPO500-Checkin-Failure.log	Установка	%temp%\McAfeeLogs	Создается, если установщику ePolicy Orchestrator не удается проверить на входе один из указанных типов пакетов: • расширения; • подключаемые модули; • пакеты развертывания; • пакеты агента.
EPO500-CommonSetup.log	Установка	%temp%\McAfeeLogs	Содержит следующие сведения установщика ePolicy Orchestrator: • запись пользовательских действий; • SQL, DTS (службы трансформации данных Microsoft) и служебные вызовы; • регистрацию и отмену регистрации DLL-файлов; • Файлы и папки, отмеченные к удалению при перезагрузке.
EPO500-Install-MSI.log	Установка	%temp%\McAfeeLogs	Основной журнал установки ePolicy Orchestrator. Содержит сведения об установке, в том числе информацию о действиях установщика и сбоях установки.
<ИМЯ_ФАЙЛА_РАСШИРЕНИЯ>.cmd	Временный	%temp%\McAfeeLogs\ePO500-troubleshoot\OutputFiles	Создается установщиком ePolicy Orchestrator. Содержит команду регистрации расширений (направляемые удаленному клиенту). В случае успешного завершения установки данные файлы удаляются.
MFS500-CommonSetup.log	Установка	%temp%\McAfeeLogs	Содержит сведения об установщике MFS.

Журналы сервера

Файлы журналов сервера содержат сведения о функциональных возможностях сервера и различных службах администрирования, используемых ePolicy Orchestrator.

Имя файла	Тип журнала	Местоположение	Описание
EpoApSvr.log	Основной	[КАТАЛОГ_УСТАНОВКИ]\DB\Logs	Файл журнала сервера приложений с таким сведениями о действиях в репозитории как: • задачи извлечения; • проверка пакетов развертывания на входе в репозиторий; • удаление пакетов развертывания из репозитория. Данный файл создается после первого запуска служб.
Errorlog.<ТЕКУЩИЕ_ДАТА_И_ВРЕМЯ>	Apache	[КАТАЛОГ_УСТАНОВКИ]\Apache2\logs	Содержит сведения о службах Apache. Данный файл создается после первого запуска службы Apache.
Eventparser.log	Основной	[КАТАЛОГ_УСТАНОВКИ]\DB\Logs	Содержит сведения о службах анализатора событий ePolicy Orchestrator, такие как сведения об успехах и сбоях анализа событий продуктов.
Jakarta_service_<ДАТА>.log	Tomcat	[КАТАЛОГ_УСТАНОВКИ]\Server\logs *	Содержит сведения о службах сервера приложений ePolicy Orchestrator. Данный файл создается после первого запуска службы Tomcat.
Localhost_access_log.<ДАТА>.txt	Tomcat	[КАТАЛОГ_УСТАНОВКИ]\Server\logs *	Записывает все обращения к серверу McAfee ePO со стороны клиентских систем. Данный файл создается после первого запуска службы Tomcat.
Orion.log	Основной	[КАТАЛОГ_УСТАНОВКИ]\Server\logs *	Содержит сведения о платформе McAfee Foundation Services и всех загруженных по умолчанию расширениях. Данный файл создается при первом запуске службы сервера приложений ePolicy Orchestrator.
Replication.log	Сервер	[КАТАЛОГ_УСТАНОВКИ]\DB\Logs	Файл журнала репликации сервера McAfee ePO. Данный файл создается при соблюдении всех следующих условий: • существуют распределенные репозитории; • настроена задача репликации; • запускалась задача репликации.

Имя файла	Тип журнала	Местоположение	Описание
`Server.log`	Основной	`[КАТАЛОГ_УСТАНОВКИ]\DB\Logs`	Содержит сведения, связанные со службами сервера McAfee ePO: • Связь агента с сервером • Обработчик агентов сервера McAfee ePO Данный файл создается после первого запуска служб.
`Stderr.log`	Tomcat	`[КАТАЛОГ_УСТАНОВКИ]\Server\logs` *	Содержит все выдаваемые стандартные ошибки, фиксируемые службой Tomcat. Данный файл создается после первого запуска служб Tomcat.

* В кластерной среде файл журнала находится в папке `[Каталог_установки]\Bin\Server\logs`.

Журналы агента

В файлах журналов агентов содержатся действия, выполненные или инициированные McAfee® Agent.

Имя файла	Тип журнала	Местоположение	Описание
`<GUID_АГЕНТА>_<ОТМЕТКА_ВРЕМЕНИ>_Server.xml`	Политика	`[КАТАЛОГ_УСТАНОВКИ]\DB\DEBUG`	Содержит сведения о проблемах обновления политик. Для включения указанного файла выполните следующее. 1 Перейдите к указанному разделу реестра: `HKEY_LOCAL_MACHINE\Software\Network Associates\ePolicy Orchestrator\` 2 Создайте переменную типа DWORD со значением 1: `SaveAgentPolicy` 3 Перезапустите службу сервера McAfee ePolicy Orchestrator 5.1.0 (Apache). Рекомендуется включить этот файл на минимальный промежуток времени, необходимый для захвата необходимой информации, поскольку размер итоговых файлов быстро возрастает.
`Agent_<СИСТЕМА>.log`	Агент	`[ПУТЬ_К_ДАННЫМ_АГЕНТА]\DB`	Создается на клиентских системах при развертывании на них агента сервером. Данный файл содержит сведения, касающиеся следующего: • связь агента с сервером; • применения политик; • других задач агента.

Имя файла	Тип журнала	Местоположение	Описание
FrmInst_<СИСТЕМА>.log	Агент	%temp%\McAfeeLogs	Создается, если для установки McAfee Agent используется файл FrmInst.exe. Данный файл содержит следующие сведения: • информационные сообщения; • сообщения о ходе выполнения; • сообщения о неудаче в случае неудачной установки.
MCScript.log	Отладка агента	[ПУТЬ_К_ДАННЫМ_АГЕНТА]\DB	Содержит результаты выполнения команд сценария, используемых в ходе развертывания и обновления агента. Чтобы включить режим DEBUG для данного журнала, установите указанное значение типа DWORD в разделе реестра клиента: HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\TVD\SHARED COMPONENTS\FRAMEWORK\DWDEBUGSCRIPT=2 По завершении поиска и устранения неполадок удалите указанный раздел реестра.
MfeAgent.MSI.<ДАТА>.log	Агент	%temp%\McAfeeLogs	Содержит сведения об установке MSI агента.
PrdMgr_<СИСТЕМА>.log	Агент	[ПУТЬ_К_ДАННЫМ_АГЕНТА]\DB	Содержит сведения о сеансах связи агента с другими продуктами McAfee.
UpdaterUI_<СИСТЕМА>.log	Агент	%temp%\McAfeeLogs	Содержит сведения об обновлениях управляемых продуктов в клиентской системе.

Журналы ошибок McAfee Agent

Когда McAfee Agent регистрирует ошибки, такие ошибки записываются в журналах ошибок агента. Журналы ошибок агента именуются для их аналогов основных журналов. Например, если ошибка возникла при выполнении задачи клиента, создается файл MCScript_Error.log. Журналы ошибок содержат только информацию об ошибках.

Процесс ведения файла журнала

Когда файл журнала достигает максимального размера, перед расширением имени файла добавляется суффикс backup и создается новый файл журнала.

Например, если файл Agent_<СИСТЕМА>.log достигает максимального размера, он переименовывается в Agent_<СИСТЕМА>_backup.log. Если файл журнала с суффиксом backup уже существует, он будет заменен. В зависимости от того, насколько недавно создан файл с суффиксом backup, он может содержать текущие записи. Изучите оба файла журнала, чтобы не пропустить ни одной из текущих записей.

Чтобы изменить размер журнала, создайте значение LOGSIZE типа DWORD в разделе реестра HKEY_LOCAL_MACHINE\Software\Network Associates\ePolicy Orchestrator, затем задайте желаемый размер журнала в этом значении. Например, 20=20MB.

Включение ведения журнала доступа

Чтобы включить ведение журнала доступа Apache, внесите соответствующие изменения в файл `httpd.conf`.

Процедура

1 Откройте файл `httpd.conf` в папке `[КАТАЛОГ_УСТАНОВКИ_ePO]\Apache2\conf`.

2 Для внесения изменений в файл выполните следующую команду.

```
CustomLog "|C:/PROGRA~1/McAfee/EPOLIC~1/Apache2/bin/rotatelogs.exe -l
            C:/PROGRA~1/McAfee/EPOLIC~1/Apache2/logs/accesslog.%Y-%m-%d 86400" common
```

(Удалите из строки символ #.)

Указанный путь к файлу предполагает путь установки ePolicy Orchestrator по умолчанию. В случае выборочной установки используйте путь, указанный в файле `httpd.conf`.

3 Сохраните файл и перезапустите службы ePolicy Orchestrator.

Уровни ведения журналов для отладки

Охват и глубина информации в большинстве файлов журналов определяются уровнем журнала, значение которого составляет от 1 до 8.

В зависимости от уровня журнала в нем содержится следующая информация.

- Сообщения, записываемые на каждом уровне, включают все сообщения на текущем уровне и всех более низких уровнях ведения журнала.
- Для обычной отладки считается нормальным значение по умолчанию (7).
- В журнал уровня 8 включается каждый запрос SQL не зависимо от наличия ошибок. Журнал уровня 8 также предоставляет сведения о связи для устранения проблем, связанных с сетью и прокси-сервером.

Сообщения, регистрируемые в журнале на каждом уровне журнала

Тип сообщения	Описание	Уровень ведения журнала
e (ошибка)	Сообщение об ошибке пользователя, переведенное	1
w (предупреждение)	Сообщение о предупреждении пользователя, переведенное	2
i (информация)	Сообщение с информацией пользователя, переведенное	3
x (расширенные данные)	Сообщение с расширенной информацией о пользователе, переведенное	4
E (ошибка)	Сообщение об ошибке при отладке, только на английском	5
W (предупреждение)	Предупреждение при отладке, только на английском	6

Тип сообщения	Описание	Уровень ведения журнала
I (информация) или ничего	Сообщение с информацией об отладке, только на английском	7
X (расширенные данные)	Сообщение с расширенной информацией об отладке, только на английском	8

Местоположения значений, управляющих уровнями журнала и срок вступления их в силу

Изменять уровни ведения журнала для всех журналов нельзя.

Имя файла журнала	Местоположение значения уровня журнала	Продолжительность обновления
`Agent_<СИСТЕМА>.log`	Значение записи реестра DWORD в: `HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY ORCHESTRATOR\LOGLEVEL`	1 минута (приблизительно)
`Core-install.log`	Неприменимо	Неприменимо
`EpoApSvr.log`	Значение записи реестра DWORD в: `HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY ORCHESTRATOR\LOGLEVEL`	1 минута (приблизительно)
`Errorlog.<ТЕКУЩИЕ_ДАТА_И_ВРЕМЯ>.log`	Неприменимо (файл, созданный службой Apache)	Неприменимо
`Eventparser.log`	Значение записи реестра DWORD в: `HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY ORCHESTRATOR\LOGLEVEL`	1 минута (приблизительно)
`FrmInst_<СИСТЕМА>.log`	Значение записи реестра DWORD в: `HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY ORCHESTRATOR\LOGLEVEL`	Во время выполнения
`Jakarta_Service_<ДАТА>.log`	`[КАТАЛОГ_УСТАНОВКИ]\SERVER\CONF\ORION\LOG-CONFIG.XML`	После запуска службы сервера приложений ePolicy Orchestrator
`Localhost_access_log.<ДАТА>.txt`	`[КАТАЛОГ_УСТАНОВКИ]\SERVER\CONF\ORION\LOG-CONFIG.XML`	После запуска службы сервера ePolicy Orchestrator
`MCSCRIPT.log`	Платформы Windows: dwDebugScript в `HKEY_LOCAL_MACHINE\Software\Network Associates\TVD\Shared Components\Framework` Платформы UNIX: DebugScript в каталоге `/etc/cma.d/<ИДЕНТИФИКАТОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АГЕНТА ePO>/config.xml`	Немедленно
`Orion.log`	`[КАТАЛОГ_УСТАНОВКИ]\SERVER\CONF\ORION\LOG-CONFIG.XML`. См. значение параметра MaxFileSize в разделе **Rolling log file**. См. также значение Priority Value в разделе **Root**.	После запуска службы сервера приложений ePolicy Orchestrator

Имя файла журнала	Местоположение значения уровня журнала	Продолжительность обновления
PrdMgr_<СИСТЕМА>.log	Значение записи реестра DWORD в: HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY ORCHESTRATOR\LOGLEVEL	1 минута (приблизительно)
Replication.log	Неприменимо	Неприменимо
Server.log	Значение записи реестра DWORD в: HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY ORCHESTRATOR\LOGLEVEL	После запуска службы сервера ePolicy Orchestrator
Stderr.log	Неприменимо	Неприменимо
UpdaterUI_<СИСТЕМА>.log	Значение записи реестра DWORD в: HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY ORCHESTRATOR\LOGLEVEL	1 минута (приблизительно)

Журнал операций агента

Журнал операций агента (AGENT_<СИСТЕМА>.XML) содержит копии сообщений от AGENT_<СИСТЕМА>.LOG, включая переведенные сообщения, типов «e», «w» и «i» (соответствующие уровням ведения журнала 1–3).

Этот файл предназначен не для отладки, а для предоставления информации пользователем, которые, вероятно, не занимаются ею. В журнал действий могут быть включены сообщения типа «x» (уровень ведения журнала 4). Сведения об установке уровней см. в разделе *Уровни ведения журнала для отладки*.

Сведения в журнале действий также появляются в **Мониторе агента**.

Если включить удаленный доступ к файлу журнала операций агента, то файлы журнала отладки агента также можно будет просматривать удаленно, щелкнув кнопку **Просмотр журнала отладки** (**текущего** или **предыдущего**) в заголовке окна **Показать журнал агента**. Инструкции см. в разделах *Журналы операций агента* и *Просмотр журнала операций агента* в руководстве по продукту McAfee ePolicy Orchestrator или в справке.

Настройка уровня журнала Orion

Файл orion.log создается сервером приложений ePolicy Orchestrator.

Можно настроить уровень журнала для отображения в нем различных типов сведений Orion.

Процедура

1 Используя текстовый редактор, откройте файл Log-Config.xml, расположенный по адресу

```
C:\PROGRAM FILES\McAfee\ePolicyOrchestrator\Server\conf\orion
```

2 В следующей строке замените warn на info или debug:

```
<root><priority value ="warn"/><appender-ref
ref="ROLLING" /><appender-ref ref="STDOUT/></root>
```

Параметр debug следует использовать только при поиске неполадок в течение короткого периода времени. Задание значения параметра debug вызывает регулярное удаление старых файлов журнала.

3 Сохраните и закройте файл.

Tomcat автоматически установит уровень ведения журнала при перезапуске служб сервера приложений ePolicy Orchestrator.

Устранение неполадок с продуктами

Для устранения неполадок с продуктами используйте журналы.

Задания

- *Устранение проблем с обновлениями политик* на стр. 10
  Устранение неполадок в добавочных обновлениях политик со стороны сервера.
- *Интерпретация кодов ошибок Windows* на стр. 10
  Для понимания сообщений об ошибке Windows определите код ошибки и найдите его в библиотеке MSDN.

Устранение проблем с обновлениями политик

Устранение неполадок в добавочных обновлениях политик со стороны сервера.

Процедура

1 Создайте значение реестра типа DWORD `SAVEAGENTPOLICY = 1` в

`HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\EPOLICY ORCHESTRATOR`

2 Перезапустите все службы ePolicy Orchestrator.

Сервер ePolicy Orchestrator создает файл `<GUID АГЕНТА>_<ОТМЕТКА ВРЕМЕНИ>_SERVER.XML` в `<ПУТЬ УСТАНОВКИ>\DB\DEBUG`, в который входит копия содержимого, развернутого сервером.

Интерпретация кодов ошибок Windows

Для понимания сообщений об ошибке Windows определите код ошибки и найдите его в библиотеке MSDN.

Процедура

1 Найдите сообщение типа «e» или «E» в файле журнала.

2 Определите время возникновения проблемы, если оно известно.

3 Отметьте код ошибки Windows, связанный с событием проблемы.

4 Найдите код ошибки в библиотеке MSDN по адресу:

http://msdn2.microsoft.com/en-us/library/ms681381.aspx

Например, при обнаружении сообщения об ошибке, включающего код 1326, перейдите к этому коду в списке кодов ошибок системы и щелкните его. Отобразится объяснение кода:

```
1326 ERROR_LOGON_FAILURE Logon failure: unknown user name or bad password [Ошибка при
входе в систему: неизвестное имя пользователя или неверный пароль]
```

Для определения причин ошибок, скрывающихся за этими кодами, также можно использовать служебную программу `ERRLOOK.EXE`. Эта служебная программа распространяется с Microsoft Visual Studio.