

Перевод выполнен компанией ООО Системы 21

<https://systems21.ru>

<https://orf-filter.ru>

Адрес оригинального документа <https://vamssoft.com/support/docs/how-tos/multi-server-6.1>

Руководство по применению в мультисерверной среде

Введение

Данное руководство поможет при настройке и использовании ORF на нескольких серверах вашей сети. Целевая аудитория этого документа – системные администраторы.

Содержание

- [Введение](#)
 - [О настройке синхронизации](#)
 - [О внешних базах данных](#)
- [Планирование](#)
 - [Определение области синхронизации](#)
 - [Планирование различий файловой системы](#)
 - [Планирование более сложных различий](#)
 - [Настройка внешних БД](#)
 - [Выбор распознавателя DNS](#)
 - [Настройка безопасности сети](#)
- [Настройка](#)
 - [Настройка издателя](#)
 - [Настройка подписчика](#)
- [Примечания](#)
 - [Объединение журналов](#)
 - [Переадресация элементов удаленного управления](#)
 - [Отказоустойчивость и синхронизация конфигурации](#)

Введение

Организации, использующие несколько серверов электронной почты, сталкиваются с проблемой унификации управления и эксплуатации серверов. ORF поддерживает данный сценарий использования, позволяя легко обмениваться настройками и данными ORF между серверами.

Примеры сценариев, когда будет полезно данное руководство:

- Почтовые серверы с несколькими периметрами (например, первичные и вторичные MX)
- Установка на нескольких площадках (например, вспомогательные почтовые серверы с централизованным управлением)
- Серверы с балансировкой нагрузки
- Отдельные установки роли Microsoft® Exchange (например, отдельные серверы Exchange 2013 Client Access Server и Mailbox)

О настройке синхронизации

Совместное использование конфигурации в ORF обеспечивается функцией синхронизации конфигурации. Для этого используется модель подписчик-издатель (*Subscriber-Publisher*).

Издатель - это сервер ORF, назначенный в качестве центрального репозитория

(хранилища) конфигурации. Серверы-подписчики получают свои настройки от издателя. Один издатель может обслуживать одного или нескольких подписчиков.

Подписчики периодически (ежеминутно) проверяют издателя на наличие изменений конфигурации, автоматически загружая и применяя любые изменения.

У издателей и подписчиков редко полностью совпадают настройки и роли в сети, поэтому подписчики могут переопределять настройки издателя для учета таких различий.

Применительно к ORF такое переопределение называется «локализацией» и она доступна в двух областях применения:

- *Локализация функций*: Позволяет переопределить настройки для всей функции целиком, например, список промежуточных хостов или черный список отправителей. Граница локализации соответствует странице настроек в инструменте администрирования.
- *Локализация путей файловой системы*: Позволяет переопределить пути файловой системы, настроенные в ORF. Это менее жесткий вариант, чем локализация функций, но он редко охватывает все различия.

О внешних базах данных

В нескольких функциях ORF используются данные, которые должны быть доступны во всей организации. Вот эти функции:

- Auto Sender Whitelist Test (проверка по белому списку отправителей)
- Greylisting Test (проверка по Greylisting)
- Directory Harvest Attack (DHA) Protection Test (проверка для защиты от атак сбора действующих адресов)
- Honeypot Tests (проверки Honeypot)

Все вышеперечисленные функции могут совместно использовать свои данные при помощи внешнего хранилища данных, которое в ORF называется *External Database* (внешняя БД). Это БД SQL, чаще всего какая-то версия Microsoft® SQL Server® (включая её бесплатные версии Express).

Планирование

Определение области синхронизации

Издатели и подписчики конфигурации часто отличаются в разных деталях, таких как пути файловой системы и расположение сервера в сети. На этом этапе планирования необходимо точно выяснить, каковы данные отличия и как они влияют на настройки ORF. При настройке синхронизации вы сможете настроить подписчика на «локализацию» отличающихся настроек.

Планирование для отличий файловой системы

Вы можете легко переопределить любые настройки путей, полученных от издателя, используя *Path Localizations* (локализацию путей) ORF. Например, если вы держите журналы на издателе в C:\Logs\ORF, но на подписчике предпочитаете хранить их в D:\Email\Logs\ORF, локализация путей позволит вам это сделать, не переопределяя остальную часть настройки функции ведения журналов.

Ниже приведен список путей, которые можно локализовать.

Настраиваемый путь	Расположение в инструменте администрирования
Путь к ORF Text Logs	<i>System / Log > Configure: ORF Text Log > Settings tab</i>
Путь к ORF PowerLogs	<i>System / Log > Configure: ORF PowerLogs</i>
Путь к Statistics Storage	<i>System / Statistics Settings</i>
Путь к DNS Cache	<i>System / DNS > DNS Settings > Caching</i>

Настраиваемый путь	Расположение в инструменте администрирования
Путь к Exchange 2019/2016/2013/2010/2007 Replay Directory	<i>System / Microsoft® Exchange</i>
Путь к Auto Sender Whitelist Private Local Database	<i>Whitelists / Auto Sender Whitelist > Database > Configure</i>
Путь к Greylisting Private Local Database	<i>Blacklists / Greylisting > Database > Configure</i>
Путь к DHA Protection Test Private Local Database	<i>Blacklists / DHA Protection Test > Database > Configure</i>
Путь к Honeypot Test Private Local Database	<i>Blacklists / Honeypot test > Database > Configure</i>
Путь к папке Attachment Quarantine	<i>Blacklists / Attachment Filtering > Settings</i>

На этом этапе **составьте список тех путей файловой системы, которые отличаются у издателя и подписчика**. Если вы конвертируете существующий сервер ORF в подписчика, то ORF может импортировать ваши текущие настройки пути и этот шаг можно будет пропустить.

Планирование более сложных различий

Если у издателя и подписчика не одинаковая роль в сети, то вам, вероятно, придется переопределить определенные части настроек издателя. На подписчиках это можно сделать при помощи локализации функций.

«Функция» здесь определяется как приблизительно одна страница в инструменте администрирования ORF.

На этом этапе **составьте список тех функций, которые отличаются у издателя и подписчика**. Ознакомьтесь с приведенным ниже списком доступных функций.

Список локализуемых функций

- System / DNS
- System / Log
- System / Microsoft® Exchange
- System / Statistics Settings
- Filtering / Actions
- Filtering / Intermediate Hosts
- Filtering / Tests
- Whitelists / Authentication Whitelist
- Whitelists / Auto Sender Whitelist
- Whitelists / DNS Whitelist
- Whitelists / IP Whitelist
- Whitelists / Keyword Whitelist
- Whitelists / Recipient Whitelist
- Whitelists / Sender Whitelist
- Blacklists / Attachment Filtering
- Blacklists / Charset Blacklist
- Blacklists / DHA Protection Test
- Blacklists / DKIM Test
- Blacklists / DMARC Test
- Blacklists / DNS Blacklists
- Blacklists / External Agents
- Blacklists / Greylisting
- Blacklists / HELO Blacklist

- Blacklists / Honeypot Test
- Blacklists / IP Blacklist
- Blacklists / Keyword Blacklist
- Blacklists / Recipient Blacklist
- Blacklists / Recipient Validation
- Blacklists / Reverse DNS Test
- Blacklists / Sender Blacklist
- Blacklists / SPF Test
- Blacklists / SURBL Test
-

Советы по локализации

- **Обратите внимание на отличия в расположении в сети.** Например, если издатель является сервером периметра сети, а подписчик находится не на периметре, то, вероятно, потребуется другой набор назначенных проверок (*Filtering / Tests*), другой список промежуточных хостов (*Filtering / Intermediate Host List*) и, возможно, отличающиеся действия (*Filtering / Actions*). Обычно эти настройки зависят от места, занимаемого ORF в сети.
- Настройки внешнего агента синхронизированы, *а сами агенты – нет.* Удостоверьтесь, что одни и те же агенты установлены в одном и том же месте, как на издателе, так и на подписчике (или локализируйте эту функцию).
- На серверах Exchange 2019, Exchange 2016, Exchange 2013 Edge и Mailbox, серверах Exchange 2010 и 2007, для ORF необходимо указать путь к каталогу преобразования Exchange. Это зависит от ваших настроек вашего экземпляра Exchange, поэтому *обычно* требуется локализовать либо путь, либо функцию (*System / Microsoft® Exchange*). Мы рекомендуем локализовывать функцию, поскольку это позволит в любой момент обновлять путь из текущих настроек Exchange при помощи нажатия кнопки *Detect* («Определить»). Обратите внимание, что серверы клиентского доступа Exchange 2013 не имеют каталогов Replay, поэтому необходимо настроить резервный сервер SMTP. Дополнительную информацию см. в [соответствующем разделе справки](#).
- Привязки сервера (*System / Server Bindings*) для службы SMTP IIS не включаются в синхронизацию. Обязательно настройте подписчику правильные привязки сервера.
- *Локализации путей* имеют приоритет над *локализациями функций*. Например, если вы локализуете функцию *System / Log* и одновременно локализуете *путь к текстовому журналу ORF*, то ORF сначала применит вашу локализацию к функции, а затем локализует путь к текстовому журналу ORF.
- Параметры в разделе *System / Configuration Subscription* and *System / Remote Access* не включаются в синхронизацию.

После составления списка различий в функциях, переходите к следующему пункту.

Установка внешних баз данных

Обмен данными между издателем конфигурации и подписчиком очень важен, если вы используете любую из следующих функций:

- Auto Sender Whitelist
- Greylisting
- DHA Protection Test
- Honeypot Test

Совместное использование данных может быть реализовано в ORF при помощи внешних БД. Если вы используете какие-либо из перечисленных выше функций ORF, учитывайте эти БД как часть планирования. ORF поддерживает широкий спектр решений для БД.

Подробнее см. страницу [Руководства по БД](#) с полным списком и инструкциями по настройке базы данных.

Выбор распознавателя DNS

ORF широко использует DNS и предлагает два метода получения данных DNS: использование *встроенного распознавателя DNS* (по умолчанию) и использование *внешних DNS-серверов*.

Если ORF *одновременно* работает на нескольких серверах в вашей сети, то вы можете получить выигрыш за счет использования общего кэша DNS, предоставляемого используемым внешним DNS-сервером. Такой общий кэш DNS может обеспечить более быстрое распознавание имен и снизить трафик DNS, направляемый на DNSBL, SURBL и другие ресурсы DNS.

При таких конфигурациях системы мы рекомендуем использовать в качестве распознавателя один и тот же внешний DNS-сервер вместо встроенного распознавателя по умолчанию. Обязательно ознакомьтесь с требованиями [Руководства по развертыванию](#) к внешним DNS-серверам.

Настройка безопасности сети

Связь между подписчиком и издателем осуществляется через назначаемый порт удаленного доступа ORF. Попытки установить подключение делает только подписчик, издатель никогда не обращается к подписчику. Убедитесь, что на вашем оборудовании, обеспечивающем безопасность сети, открыт нужный порт.

При установке ORF может потребоваться доступ к дополнительным сетевым службам. Описание приведено ниже.

Порт	Описание
TCP/6242	Порт по умолчанию для синхронизации конфигурации и удаленного управления ORF.
UDP/53 и TCP/53	Трафик DNS. При использовании встроенного распознавателя по умолчанию, эти порты должны быть открыты для всех интернет-хостов. При использовании внешних DNS-серверов, порты DNS могут быть открыты только для определенных серверов.
TCP/80	Связь по HTTP между инструментами управления и серверами ORF (поддерживаются HTTP-прокси).
TCP/389 or TCP/3268	Порты по умолчанию для связи Active Directory LDAP или GC, если в ORF с <i>источником Active Directory</i> включен <i>тест проверки получателей (Recipient Validation Test)</i> . Опция (если вышеуказанный тест отключен).
(разные)	Связь с внешними БД (например, Microsoft® SQL Server), если ORF настроен для их использования. Информацию о номерах используемых портов см. в руководстве для используемой вами БД.

Настройка

Чтобы настроить синхронизацию конфигурации между издателем и подписчиком, выполните нижеописанные действия. Последующие шаги предполагают, что вы уже завершили [настройку внешних БД](#)

Настройка издателя

На издателе откройте страницу инструмента администрирования ORF *System / Remote Access*.

Установите флажок «Enable Remote Access».

Нажмите «Local Bindings» и выберите сетевые интерфейсы и порты, которые будут принимать подключения от сервера-подписчика.

Нажмите «Allowed IPs» и добавьте IP-адрес(а) подписчика, чтобы разрешить им подключение к серверу издателя. Убедитесь, что *Configuration Synchronization* (синхронизация конфигурации) входит в число услуг, разрешенных для подписчика. Вы также можете предоставить право *удаленного администрирования* ([и вот почему](#)).

Нажмите «Set Password» и задайте пароль для удаленного доступа к издателю.

Сохраните конфигурацию, воспользовавшись *File | Save Configuration* или нажав CTRL-S.

Настройка подписчика

- 1 На подписчике откройте страницу инструмента администрирования *ORF System / Configuration Subscription*.
- 2 Нажмите кнопку «Subscribe».
- 3 Нажмите кнопку *Publisher Access* и задайте имя/порт сервера издателя. Нажмите кнопку *Test Connection*, чтобы убедиться, что подписчик получает доступ к издателю. При необходимости настройте параметры прокси-сервера в этом же диалоговом окне или при помощи кнопки *Proxy Settings* на предыдущей странице.
- 4 Если во время планирования вы определили какие-либо пути, нажмите «Local Paths» и задайте эти пути.
При преобразовании имеющегося экземпляра ORF в подписчика, можно также нажать в этом диалоговом окне кнопку *Import*, чтобы получить пути из текущих настроек ORF.
- 5 Нажмите *Feature Localizations* и выберите те функции, которые необходимо переопределить на подписчике (обратите внимание, что некоторые функции переопределяются по умолчанию).
- 6 Сохраните конфигурацию, воспользовавшись *File | Save Configuration* или нажав CTRL-S.
- 7 Запустите *ORF Log Viewer* и удостоверьтесь, что синхронизация выполнена успешно.

Поздравляем, вы успешно настроили ORF для использования в мультисерверной среде.

Примечания

Объединение журналов

Хотя ведение журналов на сетевых дисках не поддерживается (учетная запись пользователя службы ORF не имеет прав доступа к сети), вы можете обеспечить единое представление журналов ORF, вручную копируя файлы журналов в сетевое расположение и настроив программу просмотра журнала ORF для загрузки журналов из этого места.

Во избежание конфликтов имен файлов, мы рекомендуем сменить формат имени файла журнала со стандартного *orf- {yyyy} - {mm} - {dd} .log* на *orf-server1- {yyyy} - {mm} - {dd}* (*System / Log > Configure: ORF Text Log > Settings tab*). Включите в программе просмотра журнала столбец *Server*, чтобы вместе с событиями отображалось имя сервера (меню *View | Choose Columns*).

Переадресация элементов удаленного управления

Удаленное управление - это функция ORF, позволяющая отправлять IP-адреса и адреса электронной почты непосредственно из программы просмотра журналов ORF в такие списки ORF, как черный список IP-адресов или белый список отправителей. При работе с

серверами-подписчиками, список-получатель может управляться настройками издателя, поэтому ваши попытки отправки будут игнорироваться. Чтобы это предотвратить, программа просмотра журналов может запросить у подписчика пересылку такой отправки издателю. Эта пересылка имеет следующие ограничения:

- Поскольку удаленное управление является административной функцией, подписчик должен иметь право удаленного администрирования на издателе.
- Отправка может занять до одной минуты, чтобы данные вернулись обратно к подписчику.
-

Отказоустойчивость и синхронизация конфигурации

- В случае, если издатель окажется недоступен, подписчики продолжают свою работу с последней известной конфигурацией и будут продолжать пробовать подключиться к издателю с обычной периодичностью (1 раз в минуту).
- Если критически важные настройки будет невозможно применить к подписчику после локализации, служба ORF может отключиться, чтобы предотвратить потерю электронной почты. Это не приведет к прерыванию потока электронной почты, но фильтрация электронной почты ORF окажется недоступна, пока не будет устранена возникшая проблема.