Перевод выполнен компанией ООО Системы 21
https://systems21.ru
https://orf-filter.ru
Адрес оригинального документа https://vamsoft.com/support/docs/how-tos/deployment-6.1

Руководство по развертыванию

Введение

Данное руководство поможет без проблем провести развертывание ORF в вашей сети. Целевая аудитория этого документа – системные администраторы.

Содержание

- Краткое введение в ORF
  - Основы фильтрации электронной почты
  - Интеграция с Exchange
  - Точки фильтрации в ORF
- Выбор места развертывания
  - Развертывание на периметре сети
  - Развертывание за периметром сети
  - Развертывание с вторичными MX
  - Исходящий почтовый трафик
  - Развертывание на нескольких серверах
  - Системные требования
  - Производительность, результативность и объемы
- Подготовка к развертыванию
  - Составление списка промежуточных хостов
  - Проверка соответствия DNS
  - Настройка безопасности сети
  - Настройка внешних БД
  - Подготовка к перерывам в обслуживании
- Следующий шаг: установка ORF

Краткое введение в ORF

Предполагается, что для вас это первое развертывание ORF и вы еще не знакомы с некоторыми основными концепциями нашего продукта. Если вы уже знакомы с ORF, преходите к следующему разделу.

В оставшейся части данного раздела кратко объясняется ряд основных технических концепций ORF. Это важно для понимания данного руководства.

Основы фильтрации электронной почты

ORF фильтрует почтовый трафик в режиме реального времени, в процессе передачи сообщений электронной почты по протоколу SMTP. Такой низкоуровневый контроль потока сообщений дает ORF возможность полностью блокировать спам благодаря ряду таких преимуществ, как отклонение электронной почты на уровне SMTP.

Интеграция с Exchange

Подключившись к Microsoft® Exchange или IIS SMTP при помощи интерфейсов интеграции Microsoft, ORF отслеживает трафик вашей электронной почты, не добавляя еще одного скачка в цепочку доставки электронной почты.

Точки фильтрации в ORF

Интеграция с Exchange/IIS основана на событиях: ORF получает уведомления о некоторых событиях, происходящих при передаче электронной почты по SMTP, а также получает возможность вмешаться в процесс доставки. **В ORF эти события называются «точками фильтрации»**, и таких точек две.

Точка фильтрации «до прибытия» возникает в момент указания отправляющим сервером адреса электронной почты получателя (команда RCPT TO) и ожидания им подтверждения от вашего сервера. **На данный момент содержимое электронной почты еще не передано**, но ORF уже в состоянии принимать решения по электронной почте: например, если известно, что отправляющий сервер распространяет спам, то ORF может отклонить такую почту.

Чуть позже в процессе доставки появляется **точка фильтрации «по прибытии»**, когда сервер отправителя передает сообщение электронной почты и ожидает подтверждения. **Поскольку теперь стало доступно содержимое электронной почты**, ORF может выполнить более глубокий анализ почты, а также произвести больше действий, чем в точке «до прибытия», например, перенаправить электронную почту или переместить ее в папку нежелательной почты конечных пользователей.

Из вышеприведенного описания может показаться, что точка «по прибытии» будет «*лучше*», но на практике свои преимущества имеются у обеих точек фильтрации.

Выбор места развертывания

Развертывание на периметре сети

ORF лучше всего развертывать на периметре сети, на основных серверах почтового обмена (основной MX) и, опционально, на всех дополнительных MX.

- **Развертывание с Microsoft® Exchange 2019 или 2016**
  Установите ORF на сервер с *ролью Edge Transport*, а если такого сервера нет в вашей организации, то с *ролью Mailbox Server.*
- **Развертывание с Microsoft® Exchange 2013**
  Установите ORF на сервере с *ролью Edge Transport*, имеющейся в Exchange 2013 с пакетом обновления 1 (SP1). Обратите внимание, что SP1 был опубликован с дефектом, который следует устранить в первую очередь путем установки исправления. Если у вас не используются пограничные серверы, то установите ORF на сервер с ролями серверов *Client Access* и *Mailbox*. Если эти роли установлены на разных серверах, установите ORF на обоих серверах, чтобы задействовать все функции ORF.
  Установка ORF только на сервере *Client Access* или *Mailbox* также будет работать, но некоторые функции окажутся недоступны.
  Дополнительную информацию см. в соответствующей статье базы знаний и нашем Руководстве по применению в мультисерверной среде.
- **Развертывание с Microsoft® Exchange 2010 или 2007**
  Установите ORF на сервере с *ролью Edge Transport*. Если у вас не используются пограничные серверы, установите на сервере с *ролью Hub Transport*.
  Установка ORF на сервере с ролью *Hub Transport* в *варианте установки Edge Transport-Hub Transport* также будет работать.

Развертывание за периметром сети

ORF также будет работать и за периметром сети, например, за внешними интерфейсами SMTP, непрозрачными брандмауэрами, антивирусными прокси-серверами или облачными службами фильтрации электронной почты. Тем не менее, **чтобы установить и**

поддерживать ORF в таком варианте установки может потребоваться больше времени. Ниже приведен список ограничений.

- **Возрастают затраты на обслуживание списка промежуточных хостов (IHL)**
  В этом списке содержатся IP-адреса серверов, находящихся между периметром сети и сервером ORF. IHL крайне важен для надежной работы ORF.
  Составление и ведение данного списка может оказаться непростой задачей в случае сложной сети или при обеспечении периметра сети третьей стороной (например, интернет-провайдером или облачной службой фильтрации электронной почты).
- **Растет вероятность ложных срабатываний DKIM/DMARC**
  Агенты передачи сообщений электронной почты, в том числе Microsoft® Exchange, часто вносят изменения в заголовок и тело сообщений при пересылке электронной почты на следующий скачок доставки. Это может нарушать цифровые подписи, используемые в тестах DKIM и DMARC для проверки происхождения и целостности сообщений. Если ORF будет установлен за периметром сети, то, возможно, вы не сможете применять эти проверки для надежной фильтрации фишинговых и мошеннических писем.
- **Не будет работать фильтрация «до прибытия»**
  Точка фильтрации «по прибытии» будет работать без каких-либо ограничений. Отсутствие фильтрации «до прибытия» приведет к следующим ограничениям:
  - Будет недоступна функция Greylisting: Greylisting – редко используемая и довольно агрессивная техника фильтрации спама, так что это несущественная потеря, если только вы специально не захотите использовать эту функцию.
  - **Backscattering**: Спам обычно рассылается от имени непричастных посторонних лиц. В этом варианте настройки *отклонение* спама *по прибытии* приведет к тому, что ваши пограничные серверы будут генерировать отчеты об отказах (также известные как отчеты о недоставке (NDR) или уведомления о доставке (DSN)) и бомбардировать ими непричастную сторону. Это явление называется *backscattering*. Чтобы избежать этого, мы рекомендуем использовать в этом варианте настройки маркировку электронной почты вместо ее отклонения.
  - **Не отклоняются сообщения для несуществующих получателей**: При использовании проверки достоверности получателей в ORF для отклонения сообщений электронной почты, направленных несуществующим локальным получателям, в некоторых случаях ORF не сможет инициировать отчет об отказе, то есть отправитель может не получить уведомления о невозможности доставки. Это связано с техническими ограничениями протокола SMTP.

Прежде чем выбирать развертывание ORF за периметром сети, удостоверьтесь, что вышеперечисленные ограничения будут для вас приемлемы.

Развертывание с вторичными MX

По иронии судьбы, основными целями спамеров являются вторичные почтовые обменники (MX) – часто они пропускают основной MX и обращаются непосредственно к вторичному MX. Удостоверьтесь, что электронные письма от ваших вторичных MX передаются через сервер ORF, чтобы он мог их фильтровать.

В идеальном случае **ORF должен быть развернут на всех вторичных MX**, а также на основном MX. Если это невозможно, то вы столкнетесь с теми же проблемами, что были описаны в предыдущем разделе, но ограничения будут касаться только электронных писем, поступающих через вторичные MX.

Исходящий почтовый трафик

Auto Sender Whitelist в ORF – это самообучающаяся функция, автоматически создающая список ваших доверенных почтовых партнеров путем отслеживания исходящего почтового трафика. Это существенно снижает затраты на администрирование и значительно уменьшает вероятность того, что легальные электронные письма окажутся приняты за спам.

Если возможно, **маршрутизируйте исходящую электронную почту через свой сервер ORF**. Это позволит ORF автоматически пополнять белый списка отправителей.

Развертывание на нескольких серверах

ORF поддерживает *синхронизацию конфигурации*, что позволяет тиражировать её изменения по модели «издатель-подписчик». Администратор назначает центральный сервер репозитория (издатель) и вносит на этом сервере все изменения, которые затем автоматически распространяются на серверы-подписчики.

Для обмена данными между экземплярами ORF, данная функция должна использоваться вместе с внешними БД.

Информацию по настройке и использованию ORF на нескольких серверах см. в Руководству по применению в мультисерверной среде.

Системные требования

Минимальные системные требования для серверов ORF следующие:

	Требования
Операционная система	Microsoft® Windows® Server 2019 Microsoft® Windows® Server 2016 Microsoft® Windows® Server 2012 R2 Microsoft® Windows® Server 2012 Microsoft® Windows® Server 2008 R2 Microsoft® Windows® Server 2008 Windows® Server Essentials 2016 Windows® Server Essentials 2012 R2 Windows® Server Essentials 2012 Windows® Small Business Server 2011 (Standard) Windows® Small Business Server 2008 (требуется последний пакет обновления)
Сервер электронной почты	Microsoft® Exchange 2019 Microsoft® Exchange 2016 Microsoft® Exchange 2013 (сведения о совместимости с пакетом обновления 1 см. в [2]) Microsoft® Exchange 2010 Microsoft® Exchange 2007 (только в 64-разрядной версии [1]) Microsoft® IIS SMTP Service 10.0 Microsoft® IIS SMTP Service 8.5 Microsoft® IIS SMTP Service 8.0 Microsoft® IIS SMTP Service 7.5 Microsoft® IIS SMTP Service 7.0
Платформа	Поддерживаются как 32-, так и 64-разрядные ОС [1].
Internet Explorer®	Microsoft® Internet Explorer® 6 или новее
Процессор	В соответствии с требованиями операционной системы
Дисковое пространство	Не менее 100 МБ
ОЗУ	Не менее 50Mb

[1] Microsoft выпустила 32-разрядную версию Exchange 2007 только для лабораторных тестов. ORF не совместим с данной версией.

[2] Для совместимости с Exchange 2013 с пакетом обновления 1 (SP1) требуется установка исправления от Microsoft.

Рекомендуемая конфигурация системы это Microsoft® Exchange. В целом, добавление ORF в систему, которая уже в состоянии беспрепятственно выполнять задачи Exchange или IIS SMTP, не добавляет для системы значительной дополнительной нагрузки. Тем не менее, оценить создаваемую ORF нагрузку очень сложно, поскольку она во многом зависит от набора используемых функций и конфигурации.

ORF требует значительного дискового пространства для хранения журналов, в среднем 500 байт на 1 запись журнала. Это дает следующие усредненные требования к дисковому пространству:

Почтовый трафик	Журналы за 1 сутки	Журналы за 30 суток
1000/сутки	488 кБ	14 МБ
10 000/сутки	4.5 МБ	143 МБ
50 000/сутки	24 МБ	715 МБ
100 000/сутки	48 МБ	1.4 ГБ
500 000/сутки	238 МБ	7 ГБ

Срок хранения журнала настраивается в ORF (по умолчанию 30 дней).

Производительность, результативность и объемы

ORF является не особенно ресурсоемким ПО: даже при интенсивном стрессовом тестировании, средний экземпляр ПО будет занимать незначительные или даже малые ресурсу памяти и ЦП, что связано с дизайном и оптимизацией ПО.

Однако высокая степень использования ORF информации, получаемой от DNS, ограничивает его пропускную способность. Основными факторами, влияющими на пропускную способность, являются ваши настройки и время ответа DNS. К сожалению, оба фактора очень изменчивы, что затрудняет получение универсальных оценок, подходящих для всех размеров и экземпляров ПО.

По нашему опыту, средняя конфигурация ORF, соответствующая нашим рекомендациям по лучшим методам работы, может без каких-либо проблем обрабатывать 250 000 электронных писем в сутки на сервер и сообщалось об экземплярах ORF с 750 000 –1 000 000 электронных писем в сутки на сервер.

Как правило, если сеть обрабатывает менее 100 000 электронных писем в сутки на сервер, то производительность и результативность вряд ли потребуют дополнительного внимания. Для трафика 100 000 электронных писем и более мы рекомендуем следующее:

- При использовании внешних DNS-серверов используйте только один, локальный сервер.
- Не завышайте время ожидания DNS (не более 5 секунд)
- Постепенно включайте DNS-проверки ORF и следите за количеством одновременных SMTP-подключений в Exchange (оно должно оставаться менее 10)
- Ознакомьтесь с ограничениями на использование DNSBL/SURBL: если ваш трафик превышает определенный уровень, может потребоваться передача зон DNS или использование платных услуг

Подготовка к развертыванию

Составление списка промежуточных хостов

Intermediate Host List содержит IP-адреса серверов, находящихся между периметром сети и сервером ORF. ORF использует этот список для отслеживания любых промежуточных скачков в истории доставки электронной почты, чтобы найти исходный IP-адрес, подключенный к вашей сети. Этот список крайне важен для надежной работы ORF.

Список будет пустым в том случае, если вы развернете ORF на периметре сети и дополнительных MX не будет. Но если у вас есть вторичные MX или ORF был развернут за другими серверами, вам необходимо составить данный список.

См. примеры

Проверка соответствия DNS

ORF во многих отношениях зависит от DNS. Он имеет встроенный рекурсивный распознаватель DNS, а также поддерживает использование в качестве распознавателей внешних DNS-серверов. **Хотя почти во всех случаях рекомендуется встроенный распознаватель**, может потребоваться использование внешнего DNS-сервера, если:

- ORF работает на нескольких серверах и предпочтительным является общий кэш DNS (предоставляемый общим DNS-сервером).
- сетевая политика ограничивает трафик DNS только специально назначенным DNS-сервером

В случае использования внешних DNS-серверов следуйте требованиям и рекомендациям для всех DNS-серверов:

- Сервер **должен** поддерживать рекурсию (по умолчанию включена в Microsoft® DNS)
- Сервер **должен** находиться в локальной сети или на компьютере ORF. Не рекомендуется использование DNS-серверов ISP и сторонних служб DNS (таких как OpenDNS или Google Public DNS).
- Сервер **не должен** использовать серверы пересылки (например, DNS-серверы ISP), а использовать вместо этого корневые ссылки.
- Сервер **не должен** быть тем же DNS-сервером, что поддерживает вашу Active Directory

Самый простой способ выполнить вышеуказанные требования – это установить Microsoft® DNS Server на тот же компьютер, что и ORF. Это ПО является частью Windows® Server и может быть добавлено в качестве роли сервера. См. данную статью базы знаний о настройке Microsoft® DNS Server совместно с ORF.

Настройка безопасности сети

Для ORF должны быть открыты нижеперечисленные порты.

Порт	Описание
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/6242	Порт по умолчанию для удаленного управления ORF и синхронизации конфигурации между серверами ORF. Опция (если в ORF отключен *Remote Access*).
TCP/80	Связь по HTTP между инструментами управления и серверами ORF (поддерживаются HTTP-прокси).
TCP/389 или TCP/3268	Порты по умолчанию для связи Active Directory LDAP или GC, если в ORF с *источником Active Directory* включен *тест проверки получателей* (*Recipient Validation Test*). Опция (если вышеуказанный тест отключен).
(разные)	Связь с внешними БД (например, Microsoft® SQL Server), если ORF настроен для их использования. Информацию о номерах используемых

Порт	Описание
	портов см. в руководстве для используемой вами БД.

Функция удаленного доступа ORF может быть дополнительно защищена при помощи VPN или подобный решений.

Установка внешних баз данных

Некоторые функции, такие как *автоматический белый список отправителей* и *тест защиты от атак сбора действующих адресов*, хранят свои данные в БД. Такими БД могут быть либо *личные локальные БД* (решение, встроенное в ORF и не требующее настройки), либо *внешние БД* (например, Microsoft® SQL Server). **Установка внешних БД необходима, если:**

- ...почтовый трафик достиг или превышает 50000 писем в сутки
- ... при установке нескольких серверов ORF (позволит обмениваться данными между серверами)

ORF поддерживает широкий спектр решений для БД. Подробнее см. страницу с полным списком и инструкциями по настройке БД.

Подготовка к перерывам в обслуживании

При планировании развертывания учитывайте, что в Microsoft® Exchange 2019, 2016, 2013, 2010 и 2007 установщик ORF перезапускает транспортные службы Exchange для завершения установки ПО. В зависимости от версии и настроек Exchange, это может быть служба *MSExchangeTransport* (служба пограничных транспортных серверов Exchange 2019 Edge Transport, Exchange 2016 Edge Transport, Exchange 2013 Edge или почтовых ящиков, все роли Exchange 2010 and 2007), *MSExchangeFrontEndTransport* (роль сервера клиентского доступа Exchange 2013) или оба (роль почтового ящика Exchange 2019 или роль почтового ящика Exchange 2016 или сервера клиентского доступа Exchange 2013 и роли почтовых ящиков на том же сервере). На время перезапуска этих служб будет прервана работа транспорта электронной почты по протоколу SMTP. Обычно это занимает менее минуты (реально требуемое время может отличаться). Рекомендуется планировать установку ПО на такое время, когда перерыв в обслуживании вызовет меньше всего проблем.

В случае IIS SMTP перерыва в обслуживании не будет.