Руководство по планированию **Cisco WebEx Meetings Server**

Первая публикация: 21 tsʕlsʷвtɕʷ 2012 ɕtsHƟ

Последнее изменение: 21 tsʕlsʷвtɕʷ 2012 ɕtsHƟ

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

СОДЕРЖАНИЕ

ГЛАВА 1

Введение и топология центра обработки данных для вашей системы

В этом разделе приводится введение, обзор центров обработки данных и требования VMware vCenter к системе.

Введение в **Cisco WebEx Meetings Server**

Cisco Webex Meetings Server представляет собой безопасное, полностью виртуализированное частное (локальное) облако для проведения конференций, в котором представлены аудио-, видео- и веб-компоненты для сокращения расходов на проведение конференций и расширения ваших инвестиций в Cisco Unified Communications.

Cisco WebEx Meetings Server учитывает потребности современных компаний, представляя комплексное решение для проведения конференций со всеми инструментами, необходимыми для эффективного и приятного сотрудничества. Таким образом обеспечивается интерактивная и эффективная работа пользователей.

Вы можете произвести развертывание этого продекта для проведения конференций и управлять им в рамках своего частного облака за брандмауэром центра обработки данных. Продукт разработан для серверов Cisco UCS и VMware 5.0. Кроме того, он отличается скоростным виртуальным развертыванием и содержит эффективные инструменты, позволяющие администраторам настраивать систему, управлять ею и контролировать ее ключевые параметры.

Как и другие решения Cisco WebEx, этот продукт предлагает инструменты для сотрудничества в режиме реального времени, включая функцию организации совместного доступа к документам, приложениям и рабочему столу, инструменты аннотирования, полный контроль со стороны организатора для эффективного управления совещанием, список участников интегрированной конференции с функцией активации абонента, а также функцию переключения, записи и воспроизведения видео. Продукт обеспечивает высокое качество видеосвязи, позволяющее организовывать общий доступ без задержек и помех.

Помимо этого, пользователи мобильных устройств могут принимать участие в конференциях с помощью iPhone и iPad.

Важные аспекты работы вашей системы

Необходимо учитывать приведенные ниже обстоятельства.

- Прокси-серверы переадресации не рекомендуется, однако их использование возможно при учете некоторых ограничений.

  Для получения полных сведений см. Руководство по устранению неисправностей *Cisco WebEx Meetings Server*.

- Обратные веб-прокси – поддерживаются только обратные веб-прокси, включенные в комплект этого продукта.

- NAT – поддерживается только при условии соответствия требованиям к системе.

  Для получения полных сведений см. Использование преобразования сетевых адресов в системе, на странице 58

- Несколько центров обработки данных – для этого выпуска поддерживается только развертывание в пределах одного центра обработки данных.

  Для получения полных сведений см. Развертывание системы в одном центре обработки данных, на странице 3

Предупреждение

При вашем несоблюдении этих рекомендаций и требований во время развертывания системы компания Cisco не несет ответственность за какие-либо проблемы, с которыми вы можете в результате этого столкнуться.

Информация для клиентов **Cisco Unified MeetingPlace**

Будучи бывшим или настоящим пользователем Cisco Unified MeetingPlace, для получения информации о переходе к новому продукту см. Примечания к выпуску *Cisco WebEx Meetings Server*.

Важное примечание

Вследствие архитектурных различий не существует пути миграции (для существующих учетных записей пользователя, настроек и совещаний) от Cisco Unified MeetingPlace в Cisco WebEx Meetings Server. Это два отдельных продукта.

Можно провести простой переход для пользователей, продолжив поддержку как Cisco Unified MeetingPlace, так и Cisco WebEx Meetings Server, на период времени, необходимый для перехода пользователей на новую систему. Для помощи в обучении пользователей во время перехода Cisco предлагает обучающие видео, доступ к которым можно получить на странице "Справка" конечного пользователя.

Развертывание системы в одном центре обработки данных

Настоящая структура системы с дополнительной системой высокой доступности разработана для развертывания в одном центре обработки данных.

Система высокой доступности включает в себя дублирующие виртуальные машины для каждого типа виртуальных машин в развертывании. Например.

- Основная система на 250 пользователей содержит виртуальную машину администратора, виртуальную машину медиа и обратный веб-прокси (для общего доступа). При добавлении системы высокой доступности составная система на 250 пользователей содержит две виртуальные машины администратора, две виртуальные машины медиа и две виртуальные машины обратного веб-прокси.
- Основная система на 2000 пользователей содержит виртуальную машину администратора, три виртуальные машины медиа, две виртуальные машины сети и обратный веб-прокси (для общего доступа). При добавлении системы высокой доступности составная система на 2000 пользователей содержит две виртуальные машины администратора, четыре (три плюс одна дублирующая) виртуальные машины медиа, три (две плюс одна дублирующая) виртуальные машины сети и две виртуальные машины обратного веб-прокси.

В системе высокой доступности к публичному виртуальному IP-адресу и частному виртуальному IP-адресу предоставляется совместный доступ. При выключении одной из виртуальных машин вторая виртуальная машина использует тот же виртуальный IP-адрес. В таком случае сбой в работе виртуальной машины практически незаметен для конечных пользователей (поскольку совещания продолжаются), что исключает подачу необычных требований в инфраструктуру DNS. Однако совместный виртуальный IP-адрес используется только в одном сетевом сегменте или виртуальной локальной сети. Согласно нашему опыту разделение виртуальной локальной сети на два центра обработки данных создает множество проблем.

Мы требуем наличие высокодоступного подключения между внутренними виртуальными машинами, что существенно сокращает проблему различения ошибки виртуальной машины и ошибки сети. Разделение сети может привести к разделению совещаний и конфликту обновлений баз данных. Значительно практичнее создать действительно высокодоступный сегмент сети в пределах одного центра обработки данных, а не двух.

Согласно убеждениям специалистов компании Cisco для создания действительно отказоустойчивой системы необходима работа всех компонентов в режиме "полной доступности". Однако некоторые ключевые компоненты, а именно базы данных, работают в режиме "активный/ждущий". Веб-серверы и медиасоставляющие в системе высокой доступности зависят от компонентов "основной системы". Задержка и нарушение работы этого соединения приводят к сбоям в работе конечных пользователей, особенно при планировании совещаний и присоединении к ним. Задержка между компонентами медиаслужб напрямую

увеличивает задержку аудио- и видеосигнала для некоторых пользователей во время совещаний.

Использование **VMware vSphere** с системой

VMware vSphere

Этот продукт устанавливается исключительно на платформу виртуализации VMware vSphere. Для получения более подробной информации о требованиях VMware см. Требования к системе *Cisco WebEx Meetings Server*.

Cisco осуществляет развертывание продукта только в одном центре обработки данных. За исключением незначительных конфигураций все установки предполагают развертывание нескольких виртуальных машин.

- Для экономии времени Cisco рекомендует стандартные серверы Cisco UCS со специальными настройками аппаратного обеспечения и продуктами VMware.
- Тем не менее, Cisco WebEx Meetings Server предназначен для работы с любым аналогичным сервером Cisco UCS с соответствующими или лучшими характеристиками.

  Для получения более подробной информации о требованиях к аппаратному обеспечению и VMware см. Требования к системе *Cisco WebEx Meetings Server*.
- Вам следует приобрести VMware vSphere 5.0 для использования в качестве управляющей платформы для Cisco WebEx Meetings Server одним из описанных ниже способов.
  - Купите vSphere 5.0 непосредственно у компании Cisco, используя GPL (Глобальный список цен). Cisco является официальным партнером и дистрибьютором VMware.

    Это чрезвычайно удобно для тех, кто желает "приобрести все у одного продавца".
  - Купите vSphere 5.0 непосредственно у компании VMware, заключив соответствующие прямые соглашения с VMware.

Преимущества развертывания системы с помощью **VMware vSphere**

В этом разделе приводится объяснение, почему VMware vSphere и vCenter являются неотъемлемыми составляющими при использовании продукта Cisco WebEx, а также некоторые принципы работы с ними.

Развертывание системы

- Этот продукт представляет собой виртуальную машину OVA, совместимую с VMware vSphere 5.0, а не собрание программных пакетов на DVD-диске. Для развертывания OVA необходимо иметь vCenter. В противном случае продукт ее не установит.
- Предоставляя продукт как виртуальную машину, мы обеспечиваем быстрое развертывание. В некоторых случаях менее часа.

- Для быстрой установки с помощью виртуального устройства OVA вы можете выбрать автоматическое развертывание для большинства размеров системы. Просто предоставьте учетные данные vCenter, и мы развернем все виртуальные машины в вашей системе без ручного вмешательства. Эта инновация максимально сократит время работы и затраты труда.
- Для Cisco WebEx Meetings Server от покупателей требуется запустить VMware ESXi 5.0, ESXi 5.0 (обновление 1) или установить образ Cisco ISO для VMware ESXi 5.0. Обе эти версии содержат драйверы, поддерживающие серверы Cisco UCS Server, необходимые для Cisco WebEx Meetings Server. Подробнее см. http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_26617.pdf.

Простое восстановление после системных ошибок

- При использовании VMware Data Recovery у вас есть возможность быстро отменить влияющие на систему изменения, если они не оправдали ваши ожидания. Это позволяет избежать выключения и возможного нежелательного повторного развертывания системы.

Рекомендации в отношении **vSphere**

Ниже приведены рекомендации по заданию параметров фильтрации.

- Вы можете переместить виртуальную машину в другой хост ESXi. Однако, необходимо сохранить структуру виртуальных машин в рамках хоста ESXi. Другими словами, если вы планируете переместить виртуальную машину, которая находится вместе с виртуальной машиной сети, следует либо переместить ее в отдельный хост ESXi (в котором она будет единственной виртуальной машиной), либо переместить ее в хост ESXi, уже содержащий виртуальную машину сети.

Примечание Ваш новый хост ESXi должен соответствовать таким же системным требованиям, как и существующий хост ESXi.

- Несмотря на то, что вы можете перемещать виртуальные машины, не следует этого делать с помощью VMotion и Storage VMotion, поскольку они не поддерживаются в этом выпуске.
- VMware Distributed Resource Schedule (DRS) не поддерживается.
- Система высокой доступности vSphere не поддерживается.
- Кластеризация и совместный доступ с помощью vSphere не поддерживаются.

Рекомендации в отношении **vSphere** для этого продукта

- Cisco не рекомендует делать снимки виртуальных машин. Если вы все же решили использовать снимки, то после подтверждения изменений в системе при необходимости следует либо обновить их, либо как можно скорее удалить. Хранение снимков в течение длительного времени приведет к ухудшению рабочих характеристик.
- Для сред SAN выполните развертывание образов диска в SAN с высокими показателями операций ввода-вывода в секунду.

- Убедитесь в том, что в SAN остался достаточный объем памяти. Снимки хранятся в той же сети SAN.
- Выполните развертывание сети 10 ГБ для обеспечения максимальной скорости развертывания и снижения загруженности канала при последующем расширении.
- Управление всеми виртуальными машинами должен осуществлять один vCenter. Благодаря этому облегчается процесс восстановления, если вам понадобится восстанавливать свою систему.

Требования к **vCenter Server**

В дополнение к vSphere 5.0 необходимо установить vCenter Server 5.0.

- Для развертывания этого виртуального устройства необходимо также использовать vCenter для развертывания виртуальных машин в вашей системе и управления ими. Этот продукт не будет работать без vCenter Server.
- Cisco рекомендует перед важными изменяющими систему действиями создавать резервные копии и снимки системы. Создание резервных копий позволяет отменить изменения, если обновление не оправдывает ваши ожидания. Автоматизировать резервные копии и снимки можно с помощью vCenter.
- Несмотря на то, что для систем на 50 или 250 пользователей требуется vSphere Standard Edition, вы можете рассмотреть возможность покупки комплекта vSphere 5.0 Essentials Plus. Обратите внимание, что комплект vSphere 5.0 Essentials Plus полезен, в первую очередь, для экономных пользователей, разворачивающих систему на 50 пользователей. Однако комплект Essentials Plus не предполагает несколько дополнительных возможностей, которые необходимы для обычных пользователей предприятия.

vSphere 5.0 Enterprise Plus Edition для систем на **800** и **2000** пользователей

- Системы на 800 и 2000 пользователей содержат виртуальные машины, требующие от 30 до 40 процессоров vCPU. Эти виртуальные машины используют процессоры vCPU для выполнения заданий, требующих очень большой вычислительной мощности, например шифрование и дешифрование SSL, смешение аудиопотоков и т. д.
- Как минимум, необходимо приобрести версию vSphere 5.0 Enterprise Plus, поскольку более ранние версии vSphere не поддерживают количество необходимых процессоров vCPU.

vSphere 5.1 не поддерживается для этого выпуска **Cisco WebEx Meetings Server**

- Cisco WebEx Meetings Server 1.0 поддерживает только выпуски vSphere 5.0 и 5.0 обновление 1. В данный момент поддержка vSphere 5.1 отсутствует.
- VMware больше не продает vSphere 5.0, вам следует приобрести vSphere 5.1 у компании VMware или непосредственно у компании Cisco. Затем для организации Cisco WebEx Meetings Server следует произвести "понижение версии" системы до vSphere 5.0. Лицензия vSphere 5.1 дает право на понижение до vSphere выпуска 5.0.

Общие принципы развертывания системы

Размеры систем

- Система на 50 одновременных пользователей
  - Как правило, поддерживает компанию со штатом от 500 до 1000 сотрудников.
  - Основная система (без системы высокой доступности) содержит виртуальную машину администратора и дополнительный обратный веб-прокси (для общего доступа).
- Система на 250 одновременных пользователей
  - Как правило, поддерживает компанию со штатом от 2500 до 5000 сотрудников.
  - Основная система (без системы высокой доступности) содержит виртуальную машину администратора, виртуальную машину медиа и дополнительный обратный веб-прокси (для общего доступа).
- Система на 800 одновременных пользователей
  - Как правило, поддерживает компанию со штатом от 8000 до 16 000 сотрудников.
  - Основная система (без системы высокой доступности) содержит виртуальную машину администратора, виртуальную машину медиа и дополнительный обратный веб-прокси (для общего доступа).
- Система на 2000 одновременных пользователей
  - Как правило, поддерживает компанию со штатом от 20 000 до 40 000 сотрудников.
  - Основная система (без системы высокой доступности) содержит виртуальную машину администратора, 3 виртуальные машины медиа, 2 машины сети и дополнительный обратный веб-прокси (для общего доступа).

Термины, используемые во время развертывания

Название поля	Описание
URL сайта WebEx	URL безопасного http для пользователей для организации и посещения совещаний.
URL администрирования WebEx	URL безопасного http для администраторов для настройки и контроля системы и управления ею.
Публичный виртуальный IP-адрес	IP-адрес для URL сайта WebEx

Название поля	Описание
Частный виртуальный IP-адрес	• IP-адрес для URL сайта Администрирования • IP-адрес для URL сайта WebEx (только для внутренних пользователей, если у вас DNS по схеме "расщепление горизонта").

Присоединение к совещаниям

Пользователи могут присоединяться к совещаниям с помощью браузера или клиента рабочего стола.

Для получения полных сведений о работе конечных пользователей см. онлайн-справку для конечных пользователей этого продукта. Войдите на веб-сайт WebEx и нажмите Справка.

Пользователи **Windows**

- Для Microsoft Internet Explorer 8 и 9 пользователи могут установить элемент управления ActiveX или подключаемый модуль Java, скачать программу установки WebEx Meetings или запустить приложение во временной системной папке (например, TFS). Клиент скачивается и автоматически устанавливается при первом присоединении пользователя к совещанию.
- Для Google Chrome и Mozilla Firefox пользователи могут установить подключаемый модуль Java, скачать приложение WebEx Meetings или запустить приложение во временной системной папке. Клиент скачивается и автоматически устанавливается при первом присоединении пользователя к совещанию.
- Предыдущие маркированные элементы предполагают наличие на ПК пользователей прав администратора Windows для присоединения к совещаниям WebEx. Если такие права отсутствуют, системные администраторы могут установить клиент приложения WebEx Meetings на рабочих столах пользователей с помощью стандартного ПО для управления настольными системами, например IBM Tivoli. См. Загрузка и массовое развертывание приложений, на странице 89.
- Для использования с этим продуктом не требуются специальные настройки администратора для ActiveX, подключаемого модуля Java, программы установки WebEx Meetings или TFS.

Пользователи **Mac**

- Если поддержка Java включена (поддержка Java выключена по умолчанию в Mac OS X Lion (версия 10.7) и OS X Mountain Lion (версия 10.8), пользователи могут установить подключаемый модуль Java. Программа клиента скачивается и автоматически устанавливается при первом присоединении пользователя к совещанию.
- После отключения Java пользователь может скачать и установить приложение WebEx Meetings.

ГЛАВА 2

Топология сети для вашей системы

Работа конечных пользователей с Cisco WebEx Meetings Server предполагает работу с веб-сайтом, который используется ими для планирования совещаний и доступа к ним. Особенностью этого веб-сайта являются компоненты организации конференций в реальном времени, которые позволяют организовывать онлайн-совещания.

В этом разделе приведены различные топологии сети, поддерживаемые для этого продукта, включая их преимущества и недостатки. Выберите компонент, который наиболее точно отвечает вашим требованиям и развертыванию вашей сети. Однако, если вы хотите, чтобы мобильные пользователи посещали совещания, выберите топологию сети, включающую виртуальную машину обратного веб-прокси, которая предполагает общий доступ.

Рекомендованная топология сети

Cisco WebEx Meetings Server содержит две группы виртуальных машин: внутренние виртуальные машины и виртуальные машины обратного веб-прокси. Все системы должны содержать одну или более внутренних виртуальных машин. Обратный веб-прокси необходим только для систем, в которых внешние пользователи могут организовывать или посещать совещания по Интернету и с помощью мобильных устройств. Без обратного веб-прокси только внутренние пользователи и пользователи VPN могут организовывать и посещать совещания.

Внутренние виртуальные машины

Внутренние виртуальные машины означают виртуальную машину администратора и при наличии виртуальные машины медиа и сети.

- Внутренние виртуальные машины должны находиться в одной общей сети VLAN или подсети. Во время развертывания системы отобразятся сообщения об ошибке, если ваши назначения IP-адреса нарушают это правило. Проектирование системы предполагает, что все внутренние виртуальные машины, включая все виртуальные машины высокой доступности, подключены друг к другу в локальной сети LAN, что обеспечивает между этими виртуальными машинами высокую пропускную способность, незначительный уровень потери пакетов и задержку менее 1 мс. Система Cisco WebEx Meetings Server не предназначена для разделения между несколькими центрами обработки данных.
- Cisco рекомендует размещать все внутренние виртуальные машины в одном коммутаторе Ethernet (как правило, в той же стойке, что и виртуальные машины) с минимальной пропускной способностью
  - 1 Гбит/с для систем на 50 и 250 пользователей
  - 10 Гбит/с для систем на 800 и 2000 пользователей

  для связей между граничным и центральным коммутаторами. Задержка сети должна быть менее 1 мс.

  Примечание В обратном веб-прокси сетевая плата "видит" двойной сетевой трафик других устройств, поскольку передача данных проходит через нее дважды: экспорт и импорт.

  Голос, данные, видео и сеть SAN зависят от пропускной способности сети. Чрезвычайно важно развернуть сеть, способную работать с необходимой нагрузкой.
- При необходимости разместить виртуальные машины в разных коммутаторах Ethernet в рамках одного центра обработки данных, ваша сеть должна соответствовать требованиям, приведенным в этом разделе. В таком случае межстанционная магистраль должна отвечать тем же характеристикам сети, что и задержка L3 и пропускная способность одного физического коммутатора.

Для получения дополнительной информации о системах с высокой доступностью см. Дублирующая сеть в развертываниях систем высокой доступности, на странице 11.

Виртуальные машины обратного веб-прокси

- Виртуальные машины обратного веб-прокси имеют те же общие сетевые требования, что и внутренние виртуальные машины. Для настройки DNS с "расщеплением горизонта" и без него виртуальные машины обратного веб-прокси разворачиваются в сети DMZ, а не внутренней сети.
- Поскольку стандартной практикой является размещение внутренних виртуальных машин и виртуальных машин обратного веб-прокси в разных стойках, серверах и хостах ESXi, компания Cisco рекомендует приведенное ниже.
  - Системы на 50 и 250 пользователей – соединения 1 Gigabit Ethernet с двойным дублированием между коммутаторами DMZ и коммутаторами, используемыми внутренними виртуальными машинами.

- Системы на 800 и 2000 пользователей – соединения 10 Gigabit Ethernet с двойным дублированием между коммутаторами DMZ и коммутаторами, используемыми внутренними виртуальными машинами.

Дублирующая сеть в развертываниях систем высокой доступности

- Дублирующие виртуальные машины (высокая доступность) должны находиться в одном центре обработки данных с основными виртуальными машинами. Все эти машины должны находиться в одной сети VLAN или подсети. Требования к скорости и задержке для соединения между основными компонентами и компонентами высокой доступности совпадают с определенными ранее, применимыми для основных виртуальных машин.

Важное примечание	Cisco не рекомендует разделять основные и дублирующие (высокая доступность) компоненты системы между центрами обработки данных.

- Соединение между всеми внутренними виртуальными машинами, как основными так и высокой доступности, должно быть полностью дублирующим, чтобы ошибка коммутатора или сетевого соединения не нарушила соединение между основными компонентами и компонентами высокой доступности. Для достижения такой дублирующей способности каждый хост-сервер должен иметь соединения с двойным дублированием для коммутаторов Ethernet (это соединение с коммутатором A и соединение с коммутатором B).
- Основные и дублирующие виртуальные машины обратного веб-прокси (высокая доступность) должны находиться в общей сети VLAN или подсети (как правило, отличной от подсети, в которой находятся внутренние виртуальные машины). Соединение между этими двумя виртуальными машинами обратного веб-прокси должно быть полностью дублирующим, как и для внутренних виртуальных машин.

Разные типы топологии сети для вашей системы

Этот продукт поддерживает приведенные ниже топологии сети.

- Топология сети внутреннего обратного веб-прокси, на странице 12
- Топология сети без "расщепления горизонта", на странице 13
- Топология единой внутренней сети, на странице 14
- Топология сети с "расщеплением горизонта", на странице 15

Примечание Если в топологии вашей сети используются прокси-серверы переадресации, для обеспечения надлежащей работы они должны отвечать особым требованиям, применимым к виртуальным машинам обратного веб-прокси. Для получения полных сведений см. Руководство по устранению неисправностей *Cisco WebEx Meetings Server*.

Топология сети внутреннего обратного веб-прокси

В этом разделе описана сетевая топология, когда все виртуальные машины в вашей системе, включая обратный веб-прокси, принадлежат одной внутренней сети.

Примечание Такая конфигурация позволяет пользователям безопасно входить и присоединяться к совещаниям из Интернета без соединения по VPN.

Примечание При автоматическом развертывании хосты ESXi для всех ваших виртуальных машин (включая обратный веб-прокси) должны управляться из одного приложения VMware vCenter. Эта информация vCenter требуется при автоматическом развертывании системы.

URL Администрирования, URL сайта WebEx, частный виртуальный IP-адрес и публичный виртуальный IP-адрес вы укажете во время развертывания системы. Чтобы получить более подробную информацию об этих терминах и этапе их указания, см. раздел "Установка" Руководства по администрированию *Cisco WebEx Meetings Server*.

Это схематическое представление топологии всей внутренней сети обратного веб-прокси.

Примечание Для полного списка параметров доступа к портам, необходимых для этого развертывания, см. Доступ к портам, когда все виртуальные машины находятся во внутренней сети, на странице 51.

Преимущества топологии единой внутренней сети обратного веб-прокси

- Обеспечивает более низкий уровень задержки вследствие наличия меньшего количества прыжков между виртуальными машинами.
- В сравнении с сетевой топологией без "расщепления горизонта" в DMZ нет виртуальных машин.
- В сравнении с сетевой топологией без "расщепления горизонта" сетевой трафик для внутренних пользователей не связывается через DMZ для организации или посещения совещаний.

Недостатки топологии единой внутренней сети обратного веб-прокси

- Общий доступ (внешние пользователи также имеют доступ к системе) требует открытия входящих портов (80 и 443) непосредственно из Интернета во внутреннюю сеть.

Топология сети без "расщепления горизонта"

В этом разделе описывается топология сети при наличии DNS без "расщепления горизонта". Внутренние виртуальные машины (администратора и при наличии медиа и сети) принадлежат внутренней сети, а обратный веб-прокси – сети DMZ.

Примечание Такая конфигурация позволяет пользователям безопасно входить и присоединяться к совещаниям из Интернета без соединения по VPN.

Для этого продукта основное различие между топологией сети с "расщеплением горизонта" и без него заключается в том, что в системе с "расщеплением горизонта" внутренние пользователи получают доступ к URL сайта WebEx с помощью частного виртуального IP-адреса. Внешние пользователи (за пределами брандмауэра) получают доступ к URL сайта WebEx с помощью публичного виртуального IP-адреса. В сети без "расщепления горизонта" все пользователи (внутренние и внешние) получают доступ к URL сайта WebEx с помощью публичного виртуального IP-адреса.

URL Администрирования, URL сайта WebEx, частный виртуальный IP-адрес и публичный виртуальный IP-адрес вы укажете во время развертывания системы. Чтобы получить более подробную информацию об этих терминах и этапе их указания, см. раздел "Установка" Руководства по администрированию *Cisco WebEx Meetings Server*.

Это схематическое представление топологии сети без "расщепления горизонта".

Примечание Для полного списка параметров доступа к портам, необходимых для этого развертывания, см. Доступ к портам с помощью обратного веб-прокси в сети DMZ, на странице 52.

Преимущества топологии сети без "расщепления горизонта"

- Точный контроль входящего и исходящего трафика сети.
- Применение более стандартных и простых требований к сети DNS.

Недостатки топологии сети без "расщепления горизонта"

- Комплексная настройка, но не насколько полная, как для топологии сети с "расщеплением горизонта".
- Внутренний трафик направляется в сеть DMZ. Весь сетевой трафик из Интернета, как и из внутренней (частной) сети, направляется на обратный веб-прокси в сети DMZ, а затем возвращается во внутренние виртуальные машины.
- Требует открытия большего количества портов в брандмауэре между DMZ и внутренней сетью, чем для топологии всей внутренней сети.
- Автоматическое развертывание системы (для систем на 50, 250 или 800 одновременных пользователей) требует более сложной настройки в vCenter.
- Среди трех топологий сети эта конфигурация в наибольшей степени влияет на производительность сети, поскольку вся нагрузка от совещаний приходится на обратный веб-прокси. Вследствие большого количества переходов влияние оказывается и на задержку в сети.

Топология единой внутренней сети

В этом разделе описана сетевая топология, когда все виртуальные машины в вашей системе принадлежат одной внутренней сети. Общий доступ отсутствует. Только внутренние пользователи и пользователи VPN могут организовывать совещания и присоединяться к ним.

Примечание При автоматическом развертывании хосты ESXi для всех ваших виртуальных машин должны управляться из одного приложения VMware vCenter. Эта информация vCenter требуется при автоматическом развертывании системы.

URL Администрирования, URL сайта WebEx и частный виртуальный IP-адрес вы укажете во время развертывания системы. Чтобы получить более подробную информацию об этих терминах и этапе их указания, см. раздел "Установка" Руководства по администрированию *Cisco WebEx Meetings Server*.

Это схематическое представление топологии всей внутренней сети.

Преимущества топологии единой внутренней сети

- Обеспечивает более низкий уровень задержки вследствие наличия меньшего количества прыжков между виртуальными машинами.

Недостатки топологии единой внутренней сети

- Отсутствие общего доступа (внешние пользователи имеют доступ к системе) и мобильного доступа.

Топология сети с "расщеплением горизонта"

В этом разделе описывается топология сети при наличии DNS с "расщеплением горизонта". Внутренние виртуальные машины (администратора и при наличии медиа и сети) принадлежат внутренней сети, а обратный веб-прокси – сети DMZ.

Примечание Такая конфигурация позволяет пользователям безопасно входить и присоединяться к совещаниям из Интернета без соединения по VPN.

Для этого продукта основное различие между топологией сети с "расщеплением горизонта" и без него заключается в том, что в системе с "расщеплением горизонта" внутренние пользователи получают доступ к URL сайта WebEx с помощью частного виртуального IP-адреса. Внешние пользователи (за пределами брандмауэра) получают доступ к URL сайта WebEx с

помощью публичного виртуального IP-адреса. В сети без "расщепления горизонта" все пользователи (внутренние и внешние) получают доступ к URL сайта WebEx с помощью публичного виртуального IP-адреса.

URL Администрирования, URL сайта WebEx, частный виртуальный IP-адрес и публичный виртуальный IP-адрес вы укажете во время развертывания системы. Чтобы получить более подробную информацию об этих терминах и этапе их указания, см. раздел "Установка" Руководства по администрированию *Cisco WebEx Meetings Server*.

Это схематическое представление топологии сети с "расщеплением горизонта".

Примечание

Для полного списка параметров доступа к портам, необходимых для этого развертывания, см. Доступ к портам с помощью обратного веб-прокси в сети DMZ, на странице 52.

Преимущества топологии сети с "расщеплением горизонта"

- Точный контроль входящего и исходящего трафика сети.
- Существует разделение сетевого трафика, поступающего в систему, что позволяет более эффективно распределить нагрузку.

  Трафик из Интернета поступает на обратный веб-прокси. Трафик из внутренней (частной) сети поступает непосредственно на внутренние виртуальные машины (администратора, и по возможности медиа и сети).
- Характеристики производительности и задержки в сети лучше, чем при использовании DNS без "расщепления горизонта", однако хуже, чем в топологии всей внутренней сети.

Недостатки топологии с "расщеплением горизонта"

- Из трех различных топологий сети это предполагает самую сложную настройку.
- Требует сложное сопоставление DNS.
- Требует открытия большего количества портов в брандмауэре между DMZ и внутренней сетью, чем для топологии всей внутренней сети.
- Автоматическое развертывание системы (для систем на 50, 250 или 800 одновременных пользователей) требует более сложной настройки в vCenter.

- Вследствие переадресации сети для внутренних пользователей URL сайта WebEx заменяется URL, предоставляющим имя хоста виртуальной машины, которая содержит веб-службы, а также виртуальных машин медиа.

Топология сети с "расщеплением горизонта"

ГЛАВА 3

Выбор размера системы

В этом разделе описаны различные размеры системы, а также руководство по определению необходимого размера для вашей компании.

Пользователи

- Удаление пользователей в системе невозможно. Однако пользователя в системе можно деактивировать.

  Программа позволяет администраторам повторно активировать ранее деактивированные учетные записи пользователей даже после длительных периодов неактивности. Совещания пользователя и другой контент (включая записи) восстанавливаются.

- Максимальное количество учетных записей пользователей для системы – 400 000. Это общее количество активных и деактивированных учетных записей пользователей. Это число достаточно для обеспечения поддержки ожидаемого роста базы данных пользователей.

Размеры развертывания для вашей системы

Определение размера системы

При выборе размера системы определите ожидаемое количество пользователей, которое будет использовать систему в определенные моменты времени. Для системы на 50 пользователей максимальное количество одновременных пользователей, посещающих совещание, составляет 50 человек. Если начать или посетить совещание пытаются более 50 человек, отобразится сообщение об ошибке, уведомляющее о том, что они не могут начать или посетить совещание в данный момент.

- Определите количество пользователей, которое будет посещать совещания одновременно в любое время. Необходимо выбрать размер системы, поддерживающий количество ваших пользователей в большинстве случаев, за исключением редких или необычных ситуаций.
- Выбрав размер системы, его можно всегда увеличить. Однако, для увеличения размера ваше аппаратное обеспечение должно соответствовать минимальным требованиям или превышать их, либо же вы можете приобрести дополнительное оборудование.
- При необходимости добавить систему высокой доступности требуется выполнить развертывание как основной системы, так и системы высокой доступности, затем "объединить" их в единую систему с высокой доступностью. Не забудьте включить дополнительные виртуальные машины для системы высокой доступности при покупке аппаратного обеспечения.

Примечание Добавление системы высокой доступности не увеличивает емкость "порта" или системы. Таким образом только повышается уровень защиты от сбоев виртуальных машин в системе.

Примечание Определив размер системы компании, купите соответствующее оборудование и достаточное количество лицензий VMware для поддержки минимальных требований для этого размера системы.

- Система на 50 пользователей, на странице 22
- Система на 250 пользователей, на странице 22
- Система на 800 пользователей, на странице 23
- Система на 2000 пользователей, на странице 23

Требования к совместному размещению **vCenter**

Совместное размещение VMware vCenter поддерживается только для конфигураций систем на 50 и 250 одновременных пользователей.

Примечание

При планировании разместить VMware vCenter на том же хосте, что и систему на 50 или 250 одновременных пользователей, закажите вместе с сервером UCS дополнительное ОЗУ. Для получения информации о точном необходимом объеме ОЗУ см. требования к размеру системы в разделе Требования к системе *Cisco WebEx Meetings Server*.

Виртуальные машины в вашей системе

Далее приведены виртуальные машины, созданные для вашей системы. Для небольших систем некоторые функции объединены в одной виртуальной машине.

- Виртуальная машина администратора – главный узел системы. Включает базу данных системы и обеспечивает административные функции.
- Виртуальная машина медиа – обеспечивает медиа-службы (функции аудио и видео, службы телефонии и совещаний).

  Включена в виртуальную машину администратора в системе на 50 одновременных пользователей.
- Виртуальная машина сети – предоставляет веб-службы (список и записи совещаний). Дает пользователю возможность планировать будущие совещания.

  Включена в виртуальную машину администратора в системе на 50, 250 и 800 одновременных пользователей.

  Конечные пользователи входят на веб-сайт WebEx. Администраторы входят на веб-сайт администрирования.
- Обратный веб-прокси (IRP) – обеспечивает общий доступ и позволяет пользователям организовывать и посещать совещания из Интернета и с помощью мобильных устройств. Несмотря на то, что этот элемент необязателен, Cisco рекомендует включить его для обеспечения более высокого качества работы пользователей в мобильной среде.

Примечание

С этой системе может использоваться только обратный веб-прокси, предоставленный с этим продуктом. Обратные веб-прокси или системы распределения нагрузки, предоставляемые другими поставщиками, не поддерживаются. Обратный веб-прокси, предоставляемый с этим продуктом, оптимизирован для работы с совместными данными, аудио- и видеотрафиком от внешних пользователей, присоединившихся из Интернета.

Примечание В рамках настоящей документации мы используем термин "внутренние виртуальные машины" в отношении машин системного администратора, а также медиа и сети (если таковые имеются).

Обратный веб-прокси находится в сети DMZ (для топологии сети как без "расщепления горизонта", так и с ним) или во внутренней сети (для любой топологии внутренней сети).

- Топология сети без "расщепления горизонта", на странице 13
- Топология сети с "расщеплением горизонта", на странице 15
- Топология сети внутреннего обратного веб-прокси, на странице 12

Система на **50** пользователей

Это схематическое представление системы на 50 пользователей. На схеме приведены две версии развертывания системы на 50 пользователей. Если вы планируете добавить систему высокой доступности, эти виртуальные машины будут отображены как "дублирующие". При отсутствии необходимости в высокой доступности разверните только основную систему.

Примечание Для краткости мы используем в представленной ниже диаграмме аббревиатуру IRP для обозначения обратного веб-прокси.

Система на **250** пользователей

Это схематическое представление системы на 250 пользователей. Если вы планируете добавить систему высокой доступности, эти виртуальные машины будут отображены как "дублирующие". При отсутствии необходимости в высокой доступности разверните только основную систему.

Примечание Для краткости мы используем в представленной ниже диаграмме аббревиатуру IRP для обозначения обратного веб-прокси.

Система на **800** пользователей

Это схематическое представление системы на 800 пользователей. Если вы планируете добавить систему высокой доступности, эти виртуальные машины будут отображены как "дублирующие". При отсутствии необходимости в высокой доступности разверните только основную систему.

Примечание Для краткости мы используем в представленной ниже диаграмме аббревиатуру IRP для обозначения обратного веб-прокси.

Система на **2000** пользователей

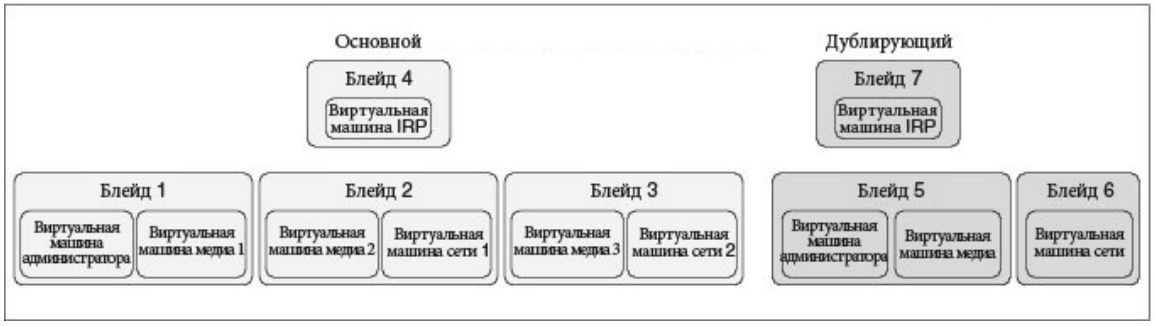
Это схематическое представление системы на 2000 пользователей. Если вы планируете добавить систему высокой доступности, эти виртуальные машины будут отображены как

"дублирующие". При отсутствии необходимости в высокой доступности разверните только основную систему.

Примечание Для краткости мы используем в представленной ниже диаграмме аббревиатуру IRP для обозначения обратного веб-прокси.

Важное примечание Убедитесь в том, что развертывание виртуальных машин выполнено согласно представленной ниже схеме. Благодаря установке на физическом сервере виртуальных машин различных типов вы можете снизить риск преждевременного закрытия системы в случае сбоя в работе аппаратного обеспечения. Например, размещение виртуальных машин медиа и сети на одном физическом сервере является более мобильным, чем размещение обеих виртуальных машин сети на одном физическом сервере.

Компоновка виртуальной машины
Развертывание системы на 2000 одновременных пользователей



ГЛАВА 4

Сетевые изменения, необходимые для развертывания

В этом разделе приведен список изменений, необходимых для развертывания системы.

- IP-адреса, необходимые для системы
- Изменения конфигурации DNS
- Конфигурация брандмауэра и доступ к портам
- Изменения маршрутизации сети

- Перечень действий в сети для установки или увеличения размера системы с помощью развертывания вручную без общего доступа, страница 48
- Доступ к портам, когда все виртуальные машины находятся во внутренней сети, страница 51
- Доступ к портам с помощью обратного веб-прокси в сети DMZ, страница 52
- Использование преобразования сетевых адресов в системе, страница 58
- Прокси-серверы переадресации, страница 61

Контрольный список сети для системы

Контрольный список сети содержит изменения сети, необходимые для системы в зависимости от конфигурации DNS компании и от того, включен ли в системе общий доступ (могут ли пользователи организовывать и посещать совещания из Интернета или мобильного устройства).

Выберите соответствующий контрольный список на основании того, используете ли вы автоматическое развертывание системы (рекомендуется для развертывания системы на 50, 250 и 800 пользователей) или развертывание системы вручную (необходимо для развертывания системы на 2000 пользователей).

- Все виртуальные машины, включая обратный веб-прокси, находятся в вашей внутренней сети (самая простая конфигурация для вашей системы).
  - Перечень действий в отношении сети для установки или увеличения размера системы с помощью автоматического развертывания с общим доступом и всеми внутренними виртуальными машинами, на странице 27
  - Перечень действий в отношении сети для установки или увеличения размера системы с помощью развертывания вручную с общим доступом и всеми внутренними виртуальными машинами, на странице 30
- DNS без "расщепления горизонта" (самая стандартная конфигурация DNS для компаний)
  - Перечень действий в отношении сети для установки или увеличения размера системы с помощью автоматического развертывания с общим доступом и DNS без "расщепления горизонта", на странице 33
  - Перечень действий в отношении сети для установки или увеличения размера системы с помощью развертывания вручную с общим доступом и DNS без "расщепления горизонта", на странице 36
- DNS с "расщеплением горизонта"
  - Перечень действий в отношении сети для установки или увеличения размера системы с помощью автоматического развертывания с общим доступом и DNS с "расщеплением горизонта", на странице 40
  - Перечень действий в отношении сети для установки или увеличения размера системы с помощью развертывания вручную с общим доступом и DNS с "расщеплением горизонта", на странице 43

- Система без общего доступа
  - Перечень действий в сети для установки или увеличения размера системы с помощью автоматического развертывания без общего доступа, на странице 46
  - Перечень действий в сети для установки или увеличения размера системы с помощью развертывания вручную без общего доступа, на странице 48

Перечень действий в отношении сети для установки или увеличения размера системы с помощью автоматического развертывания с общим доступом и всеми внутренними виртуальными машинами

Развертывание виртуальных машин

При автоматическом развертывании мы производим развертывание всех виртуальных машин (помимо виртуальной машины администратора) вместо вас. Автоматическое развертывание доступно при развертывании системы на 50, 250 или 800 пользователей.

- Убедитесь в том, что виртуальная машина сети (при наличии) находится в той же подсети, что и виртуальная машина администратора.
- Убедитесь в том, что виртуальные машины обратного веб-прокси находятся в вашей внутренней сети.
- Убедитесь в том, что хосты ESXi для всех ваших виртуальных машин (включая обратный веб-прокси) управляются из одного приложения VMware vCenter.

Обязательные **IP**-адреса

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины администратора	Внутр.	
Фактический IP-адрес виртуальной машины медиа (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес обратного веб-прокси	Внутр. (может быть в той же подсети, что и виртуальная машина администратора)	
URL Администрирования (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	

Описание	Сетевое местоположения	**IP**-адрес
URL сайта WebEx (используется исключительно системой; сопоставление с публичным виртуальным IP-адресом)	Внутр. (та же подсеть, что и у обратного веб-прокси) Примечание Этот IP-адрес должен быть общедоступным.	
Фактический IP-адрес виртуальной машины администратора системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины медиа системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес обратного веб-прокси системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для обратного веб-прокси основной системы, однако может использовать преобразование сетевых адресов с частным IP-адресом)	

Конфигурация **DNS**

Выполните приведенную ниже настройку DNS.

Действие	Пример
Обновите DNS-сервер с учетом имен хостов и IP-адресов для внутренних виртуальных машин: виртуальная машина администратора и по возможности виртуальная машина медиа.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Обновите DNS-сервер с учетом имени хоста и IP-адреса для виртуальной машины обратного веб-прокси.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Обновите DNS-сервер с учетом URL сайта Администрирования и частного виртуального IP-адреса.	• <Administration-site-URL> <Private-VIP-address>

Действие	Пример
Обновите DNS-сервер с учетом URL сайта WebEx и публичного виртуального IP-адреса.	• <WebEx-site-URL> <Public-VIP-address>

Конфигурация брандмауэра

В целях безопасности Cisco рекомендует разместить обратный веб-прокси в отдельной подсети, отличной от той, в которой находятся внутренние виртуальные машины (администратора и медиа, при наличии).

Несмотря на то, что это не рекомендуется, мы также поддерживаем размещение всех виртуальных машин (обратного веб-прокси и внутренних) в одной подсети. См. Доступ к портам, когда все виртуальные машины находятся во внутренней сети, на странице 51.

Настройка сетевой маршрутизации

Выполните приведенные ниже настройки сетевой маршрутизации.

Действие	Сравните эти **IP**-адреса
Включите маршрутизацию Уровня 3 (L3) между внутренней сетью и сетью DMZ	• Внутренняя подсеть <internal-subnet>/24 • Подсеть DMZ <DMZ-subnet>/24
Убедитесь в том, что публичный виртуальный IP-адрес и виртуальные машины обратного веб-прокси относятся к одной подсети. Примечание При внутреннем развертывании всех виртуальных машин системы (обратный веб-прокси не принадлежит сети DMZ) эта подсеть должна быть во внутренней сети.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Убедитесь в том, что частный виртуальный IP-адрес и внутренние виртуальные машины относятся к одной подсети.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Перечень действий в отношении сети для установки или увеличения размера системы с помощью развертывания вручную с общим доступом и всеми внутренними виртуальными машинами

Развертывание виртуальных машин

При развертывании вручную вы создаете все виртуальные машины для вашей системы с помощью мастера OVA из клиента vSphere. Затем вы устанавливаете систему с помощью развертывания вручную.

При необходимости развертывания системы на 2000 пользователей выберите развертывание вручную.

- Убедитесь в том, что все дополнительные внутренние виртуальные машины (по возможности медиа и сети) принадлежат той же подсети, что и виртуальная машина администратора.
- Убедитесь в том, что виртуальные машины обратного веб-прокси находятся в вашей внутренней сети.

Обязательные **IP**-адреса

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины администратора	Внутр.	
Фактический IP-адрес виртуальной машины медиа (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес второй виртуальной машины медиа (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес третьей виртуальной машины медиа (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес виртуальной машины сети (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес второй виртуальной машины сети (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес обратного веб-прокси	Внутр. (может быть в той же подсети, что и виртуальная машина администратора)	
URL Администрирования (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
URL сайта WebEx (используется исключительно системой; сопоставление с публичным виртуальным IP-адресом)	Внутр. (та же подсеть, что и у обратного веб-прокси) Примечание Этот IP-адрес должен быть общедоступным.	
Фактический IP-адрес виртуальной машины администратора системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины медиа системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины сети системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес обратного веб-прокси системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для обратного веб-прокси основной системы, однако может использовать преобразование сетевых адресов с частным IP-адресом)	

Конфигурация **DNS**

Выполните приведенную ниже настройку DNS.

Действие	Пример
Обновите DNS-сервер с учетом имен хостов и IP-адресов для внутренних виртуальных машин: виртуальная машина администратора и по возможности виртуальные машины сети.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Обновите DNS-сервер с учетом имени хоста и IP-адреса для виртуальной машины обратного веб-прокси.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Обновите DNS-сервер с учетом URL сайта Администрирования и частного виртуального IP-адреса.	• <Administration-site-URL> <Private-VIP-address>
Обновите DNS-сервер с учетом URL сайта WebEx и публичного виртуального IP-адреса.	• <WebEx-site-URL> <Public-VIP-address>

Конфигурация брандмауэра

В целях безопасности Cisco рекомендует разместить обратный веб-прокси в отдельной подсети, отличной от той, в которой находятся внутренние виртуальные машины (администратора, медиа и сети, при наличии).

Несмотря на то, что это не рекомендуется, мы также поддерживаем размещение всех виртуальных машин (обратного веб-прокси и внутренних) в одной подсети. См. Доступ к портам, когда все виртуальные машины находятся во внутренней сети, на странице 51.

Настройка сетевой маршрутизации

Выполните приведенные ниже настройки сетевой маршрутизации.

Действие	Сравните эти **IP**-адреса
Включите маршрутизацию Уровня 3 (L3) между внутренней сетью и сетью DMZ для приведенных ниже виртуальных машин: виртуальная машина администратора и по возможности виртуальные машины сети.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Убедитесь в том, что публичный виртуальный IP-адрес и виртуальные машины обратного веб-прокси относятся к одной подсети. Примечание При внутреннем развертывании всех виртуальных машин системы (обратный веб-прокси не принадлежит сети DMZ) эта подсеть должна быть во внутренней сети.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Убедитесь в том, что частный виртуальный IP-адрес и внутренние виртуальные машины (виртуальная машина администратора и по возможности виртуальная машина медиа и сети) относятся к одной подсети.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Перечень действий в отношении сети для установки или увеличения размера системы с помощью

автоматического развертывания с общим доступом и **DNS** без "расщепления горизонта"

Развертывание виртуальных машин

При автоматическом развертывании мы производим развертывание всех виртуальных машин (помимо виртуальной машины администратора) вместо вас. Автоматическое развертывание доступно при развертывании системы на 50, 250 или 800 пользователей.

- Убедитесь в том, что виртуальная машина сети (при наличии) находится в той же подсети, что и виртуальная машина администратора.
- Убедитесь в том, что виртуальные машины обратного веб-прокси находятся в вашей сети DMZ.

Обязательные **IP**-адреса

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины администратора	Внутр.	
Фактический IP-адрес виртуальной машины медиа (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес обратного веб-прокси	DMZ (однако может использовать преобразование сетевых адресов с частным IP-адресом)	
URL Администрирования (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
URL сайта WebEx (используется исключительно системой; сопоставление с публичным виртуальным IP-адресом)	DMZ (та же подсеть, что и для обратного веб-прокси)	
Фактический IP-адрес виртуальной машины администратора системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины медиа системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес обратного веб-прокси системы высокой доступности (при наличии)	DMZ – та же подсеть, что и для обратного веб-прокси основной системы (однако может использовать преобразование сетевых адресов с частным IP-адресом)	

Конфигурация **DNS**

Выполните приведенную ниже настройку DNS.

Действие	Пример
Обновите DNS-сервер с учетом имен хостов и IP-адресов для внутренних виртуальных машин: виртуальная машина администратора и по возможности виртуальная машина медиа.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Обновите DNS-сервер с учетом имени хоста и IP-адреса для виртуальной машины обратного веб-прокси.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Обновите DNS-сервер с учетом URL сайта Администрирования и частного виртуального IP-адреса.	• <Administration-site-URL> <Private-VIP-address>
Обновите DNS-сервер с учетом URL сайта WebEx и публичного виртуального IP-адреса.	• <WebEx-site-URL> <Public-VIP-address>

Конфигурация брандмауэра

В целях безопасности Cisco рекомендует разместить обратный веб-прокси в отдельной подсети, отличной от той, в которой находятся внутренние виртуальные машины (администратора и медиа, при наличии). См. Доступ к портам с помощью обратного веб-прокси в сети DMZ, на странице 52.

Настройка сетевой маршрутизации

Выполните приведенные ниже настройки сетевой маршрутизации.

Действие	Сравните эти **IP**-адреса
Включите маршрутизацию Уровня 3 (L3) между внутренней сетью и сетью DMZ	• Внутренняя подсеть <internal-subnet>/24 • Подсеть DMZ <DMZ-subnet>/24
Убедитесь в том, что публичный виртуальный IP-адрес и виртуальные машины обратного веб-прокси относятся к одной подсети.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Убедитесь в том, что частный виртуальный IP-адрес и внутренние виртуальные машины относятся к одной подсети.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Перечень действий в отношении сети для установки или увеличения размера системы с помощью развертывания вручную с общим доступом и **DNS** без **"**расщепления горизонта**"**

Развертывание виртуальных машин

При развертывании вручную вы создаете все виртуальные машины для вашей системы с помощью мастера OVA из клиента vSphere. Затем вы устанавливаете систему с помощью развертывания вручную.

При необходимости развертывания системы на 2000 пользователей выберите развертывание вручную.

- Убедитесь в том, что все дополнительные внутренние виртуальные машины (по возможности медиа и сети) принадлежат той же подсети, что и виртуальная машина администратора.

- Убедитесь в том, что виртуальные машины обратного веб-прокси находятся в вашей сети DMZ.

Обязательные **IP**-адреса

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины администратора	Внутр.	
Фактический IP-адрес виртуальной машины медиа (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес второй виртуальной машины медиа (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес третьей виртуальной машины медиа (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес виртуальной машины сети (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес второй виртуальной машины сети (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес обратного веб-прокси	DMZ (однако может использовать преобразование сетевых адресов с частным IP-адресом)	
URL Администрирования (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
URL сайта WebEx (используется исключительно системой; сопоставление с публичным виртуальным IP-адресом)	DMZ (та же подсеть, что и для обратного веб-прокси)	
Фактический IP-адрес виртуальной машины администратора системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины медиа системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины сети системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес обратного веб-прокси системы высокой доступности (при наличии)	DMZ – та же подсеть, что и для обратного веб-прокси основной системы (однако может использовать преобразование сетевых адресов с частным IP-адресом)	

Конфигурация **DNS**

Выполните приведенную ниже настройку DNS.

Действие	Пример
Обновите DNS-сервер с учетом имен хостов и IP-адресов для внутренних виртуальных машин: виртуальная машина администратора и по возможности виртуальные машины сети.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Обновите DNS-сервер с учетом имени хоста и IP-адреса для виртуальной машины обратного веб-прокси.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Обновите DNS-сервер с учетом URL сайта Администрирования и частного виртуального IP-адреса.	• <Administration-site-URL> <Private-VIP-address>
Обновите DNS-сервер с учетом URL сайта WebEx и публичного виртуального IP-адреса.	• <WebEx-site-URL> <Public-VIP-address>

Конфигурация брандмауэра

В целях безопасности Cisco рекомендует разместить обратный веб-прокси в отдельной подсети, отличной от той, в которой находятся внутренние виртуальные машины (администратора, медиа и сети, при наличии). См. Доступ к портам с помощью обратного веб-прокси в сети DMZ, на странице 52.

Настройка сетевой маршрутизации

Выполните приведенные ниже настройки сетевой маршрутизации.

Действие	Сравните эти **IP**-адреса
Включите маршрутизацию Уровня 3 (L3) между внутренней сетью и сетью DMZ для приведенных ниже виртуальных машин: виртуальная машина администратора и по возможности виртуальные машины сети.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Убедитесь в том, что публичный виртуальный IP-адрес и виртуальные машины обратного веб-прокси относятся к одной подсети.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Убедитесь в том, что частный виртуальный IP-адрес и внутренние виртуальные машины (виртуальная машина администратора и по возможности виртуальная машина медиа и сети) относятся к одной подсети.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Перечень действий в отношении сети для установки или увеличения размера системы с помощью автоматического развертывания с общим доступом и **DNS** с "расщеплением горизонта"

Развертывание виртуальных машин

При автоматическом развертывании мы производим развертывание всех виртуальных машин (помимо виртуальной машины администратора) вместо вас. Автоматическое развертывание доступно при развертывании системы на 50, 250 или 800 пользователей.

- Убедитесь в том, что виртуальная машина сети (при наличии) находится в той же подсети, что и виртуальная машина администратора.
- Убедитесь в том, что виртуальные машины обратного веб-прокси находятся в вашей сети DMZ.

Обязательные **IP**-адреса

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины администратора	Внутр.	
Фактический IP-адрес виртуальной машины медиа (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес обратного веб-прокси	DMZ (однако может использовать преобразование сетевых адресов с частным IP-адресом)	
URL Администрирования (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	

Описание	Сетевое местоположения	**IP**-адрес
URL сайта WebEx (используется исключительно системой; сопоставление с двумя виртуальными IP-адресами) • Внутренние пользователи – частный виртуальный IP-адрес • Внутренние пользователи – публичный виртуальный IP-адрес	• Внутренние пользователи – внутр. (та же подсеть, что и для виртуальной машины администратора) • Внешние пользователи – DMZ (та же подсеть, что и для обратного веб-прокси)	
Фактический IP-адрес виртуальной машины администратора системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины медиа системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес обратного веб-прокси системы высокой доступности (при наличии)	DMZ – та же подсеть, что и для обратного веб-прокси основной системы (однако может использовать преобразование сетевых адресов с частным IP-адресом)	

Конфигурация **DNS**

Выполните приведенную ниже настройку DNS.

Действие	Пример
Обновите DNS-сервер (который включает внутренний поиск) с учетом имен хостов и IP-адресов для внутренних виртуальных машин: виртуальная машина администратора и по возможности виртуальная машина медиа.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Обновите DNS-сервер (который включает внутренний поиск) с учетом имени хоста и IP-адреса для виртуальной машины DMZ.	• <IRP-vm-FQDN> <IRP-vm-IP-address>

Действие	Пример
Обновите DNS-сервер (который включает внутренний поиск) с учетом URL сайта WebEx, URL сайта Администрирования и частного виртуального IP-адреса.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
Обновите DNS-сервер (который включает внутренний поиск) с учетом URL сайта WebEx и публичного виртуального IP-адреса.	• <WebEx-site-URL> <Public-VIP-address>

Конфигурация брандмауэра

В целях безопасности Cisco рекомендует разместить обратный веб-прокси в отдельной подсети, отличной от той, в которой находятся внутренние виртуальные машины (администратора и медиа, при наличии). См. Доступ к портам с помощью обратного веб-прокси в сети DMZ, на странице 52.

Настройка сетевой маршрутизации

Выполните приведенные ниже настройки сетевой маршрутизации.

Действие	Сравните эти **IP**-адреса
Включите маршрутизацию Уровня 3 (L3) между внутренней сетью и сетью DMZ	• Внутренняя подсеть <internal-subnet>/24 • Подсеть DMZ <DMZ-subnet>/24
Убедитесь в том, что публичный виртуальный IP-адрес и виртуальные машины обратного веб-прокси относятся к одной подсети.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Убедитесь в том, что частный виртуальный IP-адрес и внутренние виртуальные машины относятся к одной подсети.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Перечень действий в отношении сети для установки или увеличения размера системы с помощью развертывания вручную с общим доступом и **DNS** с "расщеплением горизонта"

Развертывание виртуальных машин

При развертывании вручную вы создаете все виртуальные машины для вашей системы с помощью мастера OVA из клиента vSphere. Затем вы устанавливаете систему с помощью развертывания вручную.

При необходимости развертывания системы на 2000 пользователей выберите развертывание вручную.

- Убедитесь в том, что все дополнительные внутренние виртуальные машины (по возможности медиа и сети) принадлежат той же подсети, что и виртуальная машина администратора.
- Убедитесь в том, что виртуальные машины обратного веб-прокси находятся в вашей сети DMZ.

Обязательные **IP**-адреса

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины администратора	Внутр.	
Фактический IP-адрес виртуальной машины медиа (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес второй виртуальной машины медиа (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес третьей виртуальной машины медиа (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес виртуальной машины сети (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес второй виртуальной машины сети (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес обратного веб-прокси	DMZ (однако может использовать преобразование сетевых адресов с частным IP-адресом)	
URL Администрирования (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
URL сайта WebEx (используется исключительно системой; сопоставление с двумя виртуальными IP-адресами) • Внутренние пользователи – частный виртуальный IP-адрес • Внутренние пользователи – публичный виртуальный IP-адрес	• Внутренние пользователи – внутр. (та же подсеть, что и для виртуальной машины администратора) • Внешние пользователи – DMZ (та же подсеть, что и для обратного веб-прокси)	
Фактический IP-адрес виртуальной машины администратора системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины медиа системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины сети системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес обратного веб-прокси системы высокой доступности (при наличии)	DMZ – та же подсеть, что и для обратного веб-прокси основной системы (однако может использовать преобразование сетевых адресов с частным IP-адресом)	

Конфигурация **DNS**

Выполните приведенную ниже настройку DNS.

Действие	Пример
Обновите DNS-сервер (который включает внутренний поиск) с учетом имен хостов и IP-адресов для внутренних виртуальных машин: виртуальная машина администратора и по возможности виртуальные машины сети.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Обновите DNS-сервер (который включает внутренний поиск) с учетом имени хоста и IP-адреса для виртуальной машины DMZ.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Обновите DNS-сервер (который включает внутренний поиск) с учетом URL сайта WebEx, URL сайта Администрирования и частного виртуального IP-адреса.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
Обновите DNS-сервер (который включает внутренний поиск) с учетом URL сайта WebEx и публичного виртуального IP-адреса.	• <WebEx-site-URL> <Public-VIP-address>

Конфигурация брандмауэра

В целях безопасности Cisco рекомендует разместить обратный веб-прокси в отдельной подсети, отличной от той, в которой находятся внутренние виртуальные машины (администратора, медиа и сети, при наличии). См. Доступ к портам с помощью обратного веб-прокси в сети DMZ, на странице 52.

Настройка сетевой маршрутизации

Выполните приведенные ниже настройки сетевой маршрутизации.

Действие	Сравните эти **IP**-адреса
Включите маршрутизацию Уровня 3 (L3) между внутренней сетью и сетью DMZ для приведенных ниже виртуальных машин: виртуальная машина администратора и по возможности виртуальные машины сети.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Убедитесь в том, что публичный виртуальный IP-адрес и виртуальные машины обратного веб-прокси относятся к одной подсети.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Убедитесь в том, что частный виртуальный IP-адрес и внутренние виртуальные машины (виртуальная машина администратора и по возможности виртуальные машины медиа и сети) относятся к одной подсети.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Перечень действий в сети для установки или увеличения размера системы с помощью автоматического развертывания без общего доступа

Развертывание виртуальных машин

При автоматическом развертывании мы производим развертывание всех виртуальных машин (помимо виртуальной машины администратора) вместо вас. Автоматическое развертывание доступно при развертывании системы на 50, 250 или 800 пользователей.

- Убедитесь в том, что виртуальная машина сети (при наличии) находится в той же подсети, что и виртуальная машина администратора.

Обязательные **IP**-адреса

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины администратора	Внутр.	
Фактический IP-адрес виртуальной машины медиа (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
URL Администрирования (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
URL сайта WebEx (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес виртуальной машины администратора системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины медиа системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	

Конфигурация **DNS**

Выполните приведенную ниже настройку DNS.

Действие	Пример
Обновите DNS-сервер (который включает внутренний поиск) с учетом имен хостов и IP-адресов для внутренних виртуальных машин: виртуальная машина администратора и по возможности виртуальная машина медиа.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Обновите DNS-сервер с учетом URL сайта Администрирования, URL сайта WebEx и частного виртуального IP-адреса.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

Конфигурация брандмауэра

Выполните приведенные ниже настройки брандмауэра.

Действие	Пример
Настройте все брандмауэры внутренней сети, чтобы разрешить веб-браузерам осуществлять доступ к частному виртуальному IP-адресу.	HTTP <Private-VIP-address>:80 HTTPS <Private-VIP-address>:443

Настройка сетевой маршрутизации

Выполните приведенные ниже настройки сетевой маршрутизации.

Действие	Сравните эти **IP**-адреса
Убедитесь в том, что частный виртуальный IP-адрес и внутренние виртуальные машины (виртуальная машина администратора и по возможности виртуальная машина медиа) относятся к одной подсети.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Перечень действий в сети для установки или увеличения размера системы с помощью развертывания вручную без общего доступа

Развертывание виртуальных машин

При развертывании вручную вы создаете все виртуальные машины для вашей системы с помощью мастера OVA из клиента vSphere. Затем вы устанавливаете систему с помощью развертывания вручную.

При необходимости развертывания системы на 2000 пользователей выберите развертывание вручную.

- Убедитесь в том, что все дополнительные внутренние виртуальные машины (по возможности медиа и сети) принадлежат той же подсети, что и виртуальная машина администратора.

Обязательные **IP**-адреса

Описание	Сетевое местоположения	**IP**-адрес
Фактический IP-адрес виртуальной машины администратора	Внутр.	
Фактический IP-адрес виртуальной машины медиа (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес второй виртуальной машины медиа (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес третьей виртуальной машины медиа (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес виртуальной машины сети (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес второй виртуальной машины сети (только для системы на 2000 пользователей)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
URL Администрирования (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
URL сайта WebEx (используется исключительно системой; сопоставление с частным виртуальным IP-адресом)	Внутр. (та же подсеть, что и для виртуальной машины администратора)	
Фактический IP-адрес виртуальной машины администратора системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины медиа системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	
Фактический IP-адрес виртуальной машины сети системы высокой доступности (при наличии)	Внутр. (та же подсеть, что и для виртуальной машины администратора основной системы)	

Конфигурация **DNS**

Выполните приведенную ниже настройку DNS.

Действие	Пример
Обновите DNS-сервер (который включает внутренний поиск) с учетом имен хостов и IP-адресов для внутренних виртуальных машин: виртуальная машина администратора и по возможности виртуальные машины сети.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Обновите DNS-сервер с учетом URL сайта Администрирования, URL сайта WebEx и частного виртуального IP-адреса.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

Конфигурация брандмауэра

Выполните приведенные ниже настройки брандмауэра.

Действие	Пример
Настройте все брандмауэры внутренней сети, чтобы разрешить веб-браузерам осуществлять доступ к частному виртуальному IP-адресу.	• HTTP <Private-VIP-address>:80 • HTTPS <Private-VIP-address>:443

Настройка сетевой маршрутизации

Выполните приведенные ниже настройки сетевой маршрутизации.

Действие	Сравните эти **IP**-адреса
Убедитесь в том, что частный виртуальный IP-адрес и внутренние виртуальные машины (виртуальная машина администратора и по возможности виртуальная машина медиа и сети) относятся к одной подсети.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Доступ к портам, когда все виртуальные машины находятся во внутренней сети

В этом разделе приводится описание доступа к портам, необходимых во внутреннем брандмауэре при наличии всех виртуальных машин системы (администратора и при необходимости медиа, сети и обратного веб-прокси) во внутренней сети. Это топология сети внутреннего обратного веб-прокси.

Доступ к портам во внешнем брандмауэре

При включении общего доступа приведенные ниже порты открыты в качестве входящих непосредственно в Интернете для виртуальных машин обратного веб-прокси во внутренней сети.

Важное примечание — Убедитесь в том, что брандмауэр или решение по распределению нагрузки перенаправляет запросы на перечисленные ниже порты, а конечные пользователи могут организовывать совещания и присоединяться к ним.

- TCP-порт 80 для публичного виртуального IP-адреса
- TCP-порт 443 для публичного виртуального IP-адреса

Доступ к портам с помощью обратного веб-прокси в сети **DMZ**

В этом разделе приводится описание доступа к порту, необходимого во внешнем и внутреннем брандмауэрах при наличии внутренних виртуальных машин (администратора и при необходимости медиа и сети) во внутренней сети и обратного веб-прокси в сети DMZ.

Настройте списки управления доступом (ACL) на коммутатор, позволяющий передачу трафика на хосты ESXi для виртуальных машин системы.

Доступ к портам во внешнем брандмауэре

Если вы открыли общий доступ, то нижеприведенные порты открыты для входящего трафика из Интернета на виртуальные машины обратного веб-прокси в DMZ.

Важное примечание

Убедитесь в том, что брандмауэр или решение по распределению нагрузки перенаправляет запросы на перечисленные ниже порты, а конечные пользователи могут организовывать совещания и присоединяться к ним.

Примечание

Cisco настоятельно рекомендует открыть порт 80 (http) в дополнение к порту 443 (https) для упрощения работы конечных пользователей (в браузере пользователи вводят URL сайта WebEx без необходимости запоминать, относится ли он к http или https; однако для этого продукта фактический сетевой трафик всегда проходит через порт 443 (https с шифрованием SSL).

Протокол	Порт	Источник	Адресат	Зачем это нужно
TCP	443	Любые внешние клиенты	Публичный виртуальный IP-адрес (Eth1) обратного веб-прокси	Внешние клиенты, осуществляющие доступ к URL сайта WebEx с помощью https. Соединения TCP инициируются из машин внешних клиентов на виртуальные машины обратного веб-прокси.

Протокол	Порт	Источник	Адресат	Зачем это нужно
TCP	80	Любые внешние клиенты	Публичный виртуальный IP-адрес (Eth1) обратного веб-прокси	Внешние клиенты, осуществляющие доступ к URL сайта WebEx с помощью http. Соединения TCP инициируются из машин внешних клиентов на виртуальные машины обратного веб-прокси.
UDP	53	Фактический IP-адрес (Eth0) обратного веб-прокси	DNS-сервер	Это необходимо при наличии брандмауэра между виртуальными машинами и сервером DNS для надлежащего развертывания и работы системы.

Доступ к портам во внутреннем брандмауэре

Следующие порты должны быть открыты, когда обратный веб-прокси принадлежит сети DMZ. При наличии ограничений на соединения из внутренней сети в сеть DMZ применяется приведенная ниже таблица. Дайте разрешение на соединения TCP, исходящие от внутренней сети в сегмент сети DMZ в приведенных ниже портах.

Примечание Для соответствующей работы этого продукта соединения TCP из сегмента DMZ во внутреннюю сеть разрешены не должны быть.

Примечание Порт UDP 10162 является единственным открытым входящим портом из DMZ во внутренние виртуальные машины. Этот порт обязателен для мониторинга обратного веб-прокси системой.

Протокол	Порт	Источник	Адресат	Зачем это нужно
TCP	64001	Все внутренние виртуальные машины (Eth0 IP)	Фактический IP-адрес (Eth0) виртуальных машин обратного веб-прокси	Это требуется внутренними виртуальными машинами для установки обратных соединений с обратным веб-прокси. Соединения TCP устанавливаются из внутренних виртуальных машин на виртуальные машины обратного веб-прокси.
TCP	7001	Все внутренние виртуальные машины (Eth0 IP)	Фактический IP-адрес (Eth0) виртуальных машин обратного веб-прокси	Это требуется внутренними виртуальными машинами для установки обратных соединений с обратным веб-прокси. Соединения TCP инициируются из внутренних виртуальных машин на виртуальные машины обратного веб-прокси.

Протокол	Порт	Источник	Адресат	Зачем это нужно
TCP	64616	Виртуальные машины администратора (Eth0 IP)	Фактический IP-адрес (Eth0) виртуальных машин обратного веб-прокси	Требуется для начальной загрузки обратного веб-прокси. Соединения TCP инициируются из виртуальных машин администратора на виртуальные машины обратного веб-прокси.
TCP	873	Виртуальные машины администратора (Eth0 IP)	Фактический IP-адрес (Eth0) виртуальных машин обратного веб-прокси	Требуется для сохранения журналов из обратного веб-прокси. Соединения TCP инициируются из виртуальных машин администратора на виртуальные машины обратного веб-прокси.
TCP	22	Любые машины внутреннего клиента	Фактический IP-адрес (Eth0) виртуальных машин обратного веб-прокси	Требуется для устранения неполадок с виртуальными машинами обратного веб-прокси с помощью учетной записи Remote Support.

Протокол	Порт	Источник	Адресат	Зачем это нужно
TCP	443	Любые машины внутреннего клиента	Частный виртуальный IP-адрес (Eth1) виртуальных машин администратора	Внутренние пользователи, осуществляющие доступ к URL сайта WebEx с помощью https. Соединения TCP устанавливаются из машины внутреннего клиента на виртуальную машину администратора.
TCP	80	Любые машины внутреннего клиента	Частный виртуальный IP-адрес (Eth1) виртуальных машин администратора	Внутренние пользователи, осуществляющие доступ к URL сайта WebEx с помощью http. Соединения TCP устанавливаются из машины внутреннего клиента на виртуальную машину администратора.
TCP	10200	Любые машины внутреннего клиента	Фактический IP-адрес (Eth0) виртуальных машин администратора	Требуется для развертывания начальной системы. Соединения TCP устанавливаются из машин внутреннего клиента на виртуальные машины администратора.

Протокол	Порт	Источник	Адресат	Зачем это нужно
UDP	161	Фактический IP-адрес (Eth0) виртуальных машин администратора	Фактический IP-адрес (Eth0) обратного веб-прокси	Требуется для разрешения отправки запросов GET SNMP из виртуальных машин администратора на виртуальные машины обратного веб-прокси. Соединение TCP инициируется из виртуальных машин администратора на виртуальные машины обратного веб-прокси.
UDP	10162	Фактический IP-адрес (Eth0) обратного веб-прокси	Фактический IP-адрес (Eth0) виртуальных машин администратора	Требуется для разрешения отправки информации и ловушек SNMP из виртуальных машин обратного веб-прокси на виртуальные машины администратора. Соединение TCP инициируется в качестве входящего из обратного веб-прокси на виртуальные машины администратора.

Протокол	Порт	Источник	Адресат	Зачем это нужно
UDP	53	Все внутренние виртуальные машины (Eth0 IP)	DNS-сервер	Это необходимо при наличии брандмауэра между виртуальными машинами и сервером DNS для надлежащего развертывания и работы системы.

Порты **VMware vCenter**

Эти порты используются только для передачи данных между хостом ESXi и vCenter. Если хост ESXi и vCenter подключены к отдельной сети управления, вам может не потребоваться открывать эти порты через брандмауэр.

- Порт 902 UDP/TCP в обоих направлениях между vCenter и хостами ESXi для управления vCenter
- (Дополнительно) Порт 22 TCP от клиента vSphere к хостам ESXi для управления SSH
- Порт 443 TCP от vCenter к хостам ESXi для безопасного управления https
- Порт 514 UDP от хостов ESXi для вашей системы к внутреннему системному журналу
- Порт 5989 TCP в обоих направлениях между vCenter и хостами ESXi для управления XML

Использование преобразования сетевых адресов в системе

Cisco в этом продукте поддерживает обход преобразования сетевых адресов (NAT) для IP-адресов виртуальных машин и виртуальных IP-адресов (частных и публичных виртуальных IP-адресов), используемых в вашей системе.

Примечание Для получения более подробной информации о NAT см. http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml.

В схеме ниже приведен стандартный обход NAT для системы на 50 пользователей без системы высокой доступности. С помощью NAT вы можете сократить количество публичных *IP*-адресов, необходимых для продукта, до всего одного IP-адреса вместо двух (или трех в случае развертывания системы высокой доступности). Вы также можете произвести похожие развертывания NAT при условии соблюдения общих требований к системе.

Примечание

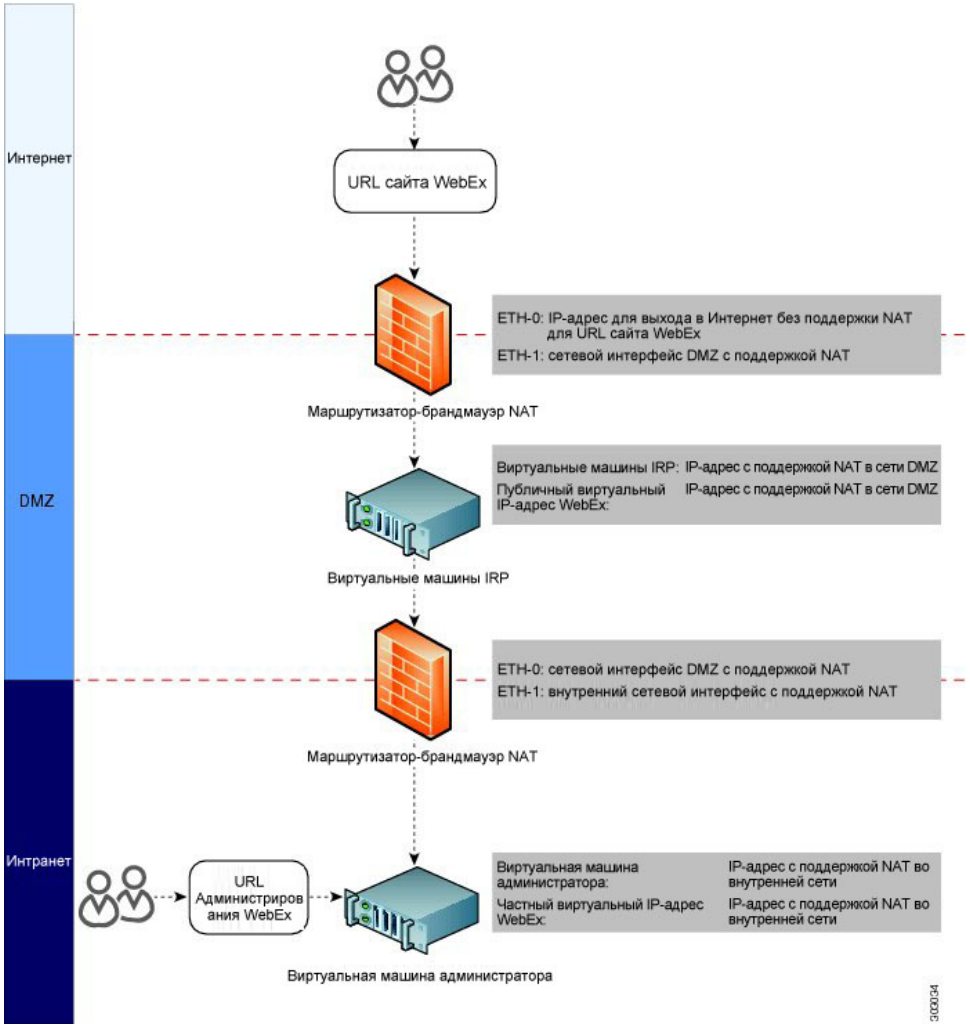
Использование нескольких NAT и брандмауэров приводит к увеличению задержки, что снижает качество трафика в реальном времени для пользователей.

Важное примечание

При использовании нескольких доменов NAT маршрутизация между этими доменами NAT может предполагать некоторые сложности. Однако использовать IP-адреса с поддержкой NAT можно, пока соблюдаются приведенные ниже требования.

- Все виртуальные машины в системе могут использовать IP-адреса с поддержкой NAT.
- IP-адрес виртуальной машины обратного веб-прокси должен быть доступным для виртуальной машины администратора в пределах внутренней сети.
- Публичный виртуальный IP-адрес не должен быть видимым для всех пользователей, однако он должен быть реализуемым из Интернета.
- При развертывании публичного доступа URL сайта WebEx должен быть связан с IP-адресом, видимым в Интернете. Этот видимый в Интернете IP-адрес должен быть доступным для внешних пользователей, а также связанным с публичным виртуальным IP-адресом, настраиваемым во время развертывания системы.

  Вы можете выбрать отображение публичного виртуального IP-адреса из Интернета. Если вы не настроите его публичное отображение, он должен быть реализуемым из Интернета.



На схеме внешний пользователь предоставляет доступ к сайту WebEx для организации совещания или присоединения к нему. После поиска DNS IP-адрес для сайта WebEx является публичным IP-адресом с поддержкой NAT (Eth0). Этот публичный IP-адрес с поддержкой NAT используется для внешнего маршрутизатора брандмауэра NAT (брандмауэр и маршрутизатор NAT 1) между внешней сетью и сетью DMZ.

Маршрутизатор брандмауэра получает запрос от внешнего пользователя и в рамках сети направляет запрос на частный IP-адрес с поддержкой NAT для маршрутизатора (Eth1, открытым для сети DMZ). Затем Eth1 отправляет запрос на публичный виртуальный IP-адрес (также IP-адрес с поддержкой NAT в частном сетевом сегменте для сайта WebEx).

Вы можете использовать IP-адреса с поддержкой NAT для публичного виртуального IP-адреса и IP-адресов обратного веб-прокси. Единственным публичным IP-адресом с поддержкой NAT является IP-адрес Eth0 для маршрутизатора брандмауэра NAT.

Примечание Для обеспечения надлежащей маршрутизации входящих пакетов этим маршрутизатором брандмауэра NAT (между Интернетом и сетью DMZ) настройте конфигурацию сопоставления портов на устройстве NAT или примените другие схожие механизмы для организации правильной отправки пакета на публичный виртуальный IP-адрес и обратный веб-прокси.

Как правило, существует второй внутренний маршрутизатор брандмауэра NAT между сетью DMZ и внутренней сетью. Как и внешний маршрутизатор брандмауэра NAT, Eth0 является частным IP-адресом NAT сети DMZ и интерфейсом сети DMZ. Eth1 является частным IP-адресом с поддержкой NAT, представляющим собой интерфейс для внутренней сети.

Вы можете использовать IP-адреса с поддержкой NAT для частного виртуального IP-адреса и IP-адресов виртуальной машины администратора.

Прокси-серверы переадресации

Если в топологии вашей сети используются прокси-серверы переадресации, для обеспечения надлежащей работы они должны отвечать особым требованиям, применимым к виртуальным машинам обратного веб-прокси. Для получения полных сведений см. раздел "Использование прокси-серверов переадресации в вашей системе" Руководства по устранению неисправностей *Cisco WebEx Meetings Server*.

ГЛАВА 5

Таблицы для быстрой справки о емкости системы

В этом модуле содержатся таблицы емкости системы.

Максимальная емкость и масштабируемость сети для каждого размера системы

В таблице ниже приведены данные по максимальной емкости сети для каждого размера системы.

Максимальное количество	**50** одновременных пользователей	**250** одновременных пользователей	**800** одновременных пользователей	**2000** одновременных пользователей
Пользователи аудио и сети (совмещ.)	50	250	800	2000
Одновременные пользователи с видео высокого качества и совместный доступ к видеофайлам (объединен.)	25	125	400	1000
Участники в совещании	50	100	100	100
Записи воспроизведений совещаний, которые уже закончились	13	63	200	500

Максимальное количество	**50** одновременных пользователей	**250** одновременных пользователей	**800** одновременных пользователей	**2000** одновременных пользователей
Записи совещаний, которые идет в данный момент	5	25	80	200
Звонки в секунду	1	3	8	20
Конференции (предположительно 2 участника в одном совещании)	25	125	400	1000

Требования к максимальному суммарному использованию пропускной способности приведены ниже.

- 50 одновременных пользователей – 125 Мбит/с
- 250 одновременных пользователей – 625 Мбит/с
- 800 одновременных пользователей – 2 Гбит/с
- 2000 одновременных пользователей – 5 Гбит/с

Этот список составлен при условии, что наименьшая пропускная способность составляет 1,8 Мбит/с для одного соединения на основании общего показателя. Это значение включает ограничение, что только половина максимального количества пользователей может в любое время использовать видео, и что пользователи не будут работать в режиме театра при смене слайдов и воспроизведении видео в совместном доступе. Среднее использование составляет менее половины этого значения, однако необходимо принимать во внимание это предупреждение при предоставлении меньшей пропускной способности, поскольку качество работы пользователей резко снижается при насыщении сетевых соединений. Этот трафик наблюдается на сетевых соединениях, входящих и исходящих от центров обработки данных.

Примечание Требования к пропускной способности для этого продукта в основном такие же, как и для облачных служб Cisco WebEx. При необходимости оптимизировать обеспечение сети см. http://www.webex.com/pdf/wp_bandwidth.pdf.

Для получения более подробной информации о емкости системы см. Требования к системе *Cisco WebEx Meetings Server*.

ГЛАВА 6

Настройка **Cisco Unified Communications Manager (CUCM)**

Настройка **Cisco Unified Communications Manager (CUCM)**

Настройка параметров управления вызовами с помощью CUCM. Для управления вызовами следует настроить одну систему CUCM, однако для получения высокой доступности аудио можно дополнительно настроить вторую систему CUCM.

Cisco WebEx Meetings Server поддерживает CUCM версий 7.1, 8.6 и 9.0.

Для настройки одной системы CUCM (без обеспечения высокой доступности аудио) выполните приведенное ниже.

- Для выполнения звонка на номер системы Cisco WebEx Meetings Server с помощью CUCM необходимо настроить шаблон маршрутов звонков на номер системы на задействованных в конференции серверах распределения нагрузки, а также шаблон маршрутов SIP на задействованных в конференции серверах приложения. Шаблон маршрутов звонков на номер системы позволяет системе CUCM осуществлять маршрутизацию звонков исходя из настроенного номера внутреннего вызова. Шаблон маршрутов SIP представляет собой шаблон для телефонной связи, с помощью которого система CUCM может маршрутизировать звонки исходя из URL-адреса SIP, содержащегося в сообщениях SIP исходящих вызовов.

  Примечание Номер шаблона маршрутов звонков на номер системы одновременно является номером доступа, необходимым для выполнения звонков на номер системы, с помощью которого вы сможете настраивать свои аудиопараметры на сайте Администрирования. Убедитесь в надлежащей настройке номеров портов, как описано в приведенных ниже разделах.

  - Настройте указание нескольких магистралей SIP на задействованные в конференции средства распределения нагрузки сервера Cisco WebEx Meetings Server и настройте группу, список и шаблон маршрутов.
  - Настройте указание нескольких магистралей SIP на задействованные в конференции серверы приложения Cisco WebEx Meetings Server и настройте несколько шаблонов маршрутов SIP.

- Для осуществления внешнего вызова в CUCM с помощью Cisco WebEx Meetings Server выполните указанные ниже действия.
  - Войдите на сайт Администрирования и настройте CUCM. Чтобы получить более подробные сведения, см. раздел "Первая настройка аудиопараметров" в Руководстве по администрированию.

    Примечание Для CUCM необходимо, чтобы задействованный в конференции сервер приложения был настроен в системе CUCM как магистраль SIP. В противном случае сообщения сервера приложения будут отклоняться.

Совместимость функций **CUCM** и поддержка

В таблицах ниже представлена информация о совместимости функций поддерживаемых версий CUCM.

Совместимость функций **CUCM**

В таблице ниже представлена информация о совместимости функций поддерживаемых версий CUCM. Емкость системы Cisco WebEx Meetings Server не зависит от выбора конфигурации.

Примечание Cisco WebEx Meetings Server не поддерживает версии CUCM, отсутствующие в списке, а также любые приложения прокси SIP третьих сторон.

Функция	**CUCM 7.1**	**CUCM 8.6**	**CUCM 9.0**	Предварительные условия/замечания
Внешний вызов (IPv6)	Да	Да	Да	В процессе установки настройте систему Cisco WebEx Meetings Server с IPv6-адресами.
Звонок на номер системы (IPv6)	Да	Да	Да	В процессе установки настройте систему Cisco WebEx Meetings Server с IPv6-адресами.
TLS/SRTP	Да	Да	Да	В процессе установки настройте систему Cisco WebEx Meetings Server с адресами безопасности.
RFC2833	Да	Да	Да	Выберите этот параметр во время настройки магистрали CUCM SIP.
KPML	Да	Да	Да	Выберите этот параметр во время настройки магистрали CUCM SIP.
Keepalive – отправка Cisco WebEx Meetings Server	Да	Да	Да	Выполнено с помощью сообщения ПАРАМЕТРЫ SIP.

Функция	**CUCM 7.1**	**CUCM 8.6**	**CUCM 9.0**	Предварительные условия/замечания
Keepalive – получение Cisco WebEx Meetings Server	Нет	Да	Да	Выполнено с помощью сообщения ПАРАМЕТРЫ SIP.
Качество обслуживания	Да	Да	Да	Для пакетов управления.
TCP	Да	Да	Да	Убедитесь в том, что ваши порты по умолчанию настроены таким образом: 5060 для задействованных в конференции серверов распределения нагрузки; 5062 для задействованных в конференции серверов приложений.
TLS	Да	Да	Да	Убедитесь в том, что ваши порты по умолчанию настроены таким образом: 5061 для задействованных в конференции серверов распределения нагрузки; 5063 для задействованных в конференции серверов приложений.

Функция	**CUCM 7.1**	**CUCM 8.6**	**CUCM 9.0**	Предварительные условия/замечания
UDP	Да	Да	Да	Убедитесь в том, что ваши порты по умолчанию настроены таким образом: 5060 для задействованных в конференции серверов распределения нагрузки; 5062 для задействованных в конференции серверов приложений.
Самоподписанные сертификаты	Да	Да	Да	Н/Д
Сертификаты третьих сторон	Да	Да	Да	Н/Д

Функции вызовов телефонии

Cisco WebEx Meetings Server поддерживает представленные функции вызовов CUCM.

Примечание Программа CUCM 9.0, которая является частью продукта BE6K (Business Edition 6000), также поддерживается службой Cisco WebEx Meetings Server.

Функция	**CUCM 7.1**	**CUCM 8.6**	**CUCM 9.0**
Удержание вызова	Да	Да	Да
Неудержание вызова	Да	Да	Да
Отображение идентификатора звонящего на EP	Да	Да	Да
Отображение имени звонящего на EP	Да	Да	Да
Перевод звонка (с IPv4 на IPv4)	Да	Да	Да
Перевод звонка (с IPv6 на IPv4)	Да	Да	Да

Функция	**CUCM 7.1**	**CUCM 8.6**	**CUCM 9.0**
Перевод звонка (с IPv4 на IPv6)	Нет	Нет	Да
Перевод звонка (с IPv6 на IPv6)	Нет	Нет	Да

Функции медиасвязи телефонии

Cisco WebEx Meetings Server может одновременно поддерживать участников с кодеками G.711/G.722/G.729. Изменение конфигурации кодека не влияет на работу системы.

Функция	**G.711**	**G.722**	**G.729**
Подавление шумов	Да	Да	Да
Комфортный шум	Да	Нет	Нет
Подавление эха	Нет	Нет	Нет
Маскирование потери пакетов	Да	Да	Нет
Автоматическое получение управления	Да	Да	Да
Качество обслуживания	Да	Да	Да

Базовая конфигурация **CUCM**

Для управления вызовами для системы Cisco WebEx Meetings Server необходимо создать некоторые базовые конфигурации CUCM. Несколько систем могут иметь одинаковую базовую конфигурацию. Базовая конфигурация состоит из приведенного ниже.

- Профиль защиты магистрали SIP
- Профиль SIP

Контрольный список конфигурации

Контрольный список конфигурации отображает количество типов конфигурации CUCM, которые следует настроить для вашей системы.

Размер системы	Проф. безопасн. (баз. конф.)	Проф. **SIP** (баз. конф.)	Магистр. **SIP** (спец. конф.)	Груп. маршр. (спец. конф.)	Спис. маршр. (спец. конф.)	Шабл. маршр. (спец. конф.)	Шабл. маршр. **SIP** (спец. конф.)
50 польз.	2	1	2	1	1	Нет[1]	1
50 польз. с выс. дост.	2	1	4	1	1	Нет	2
250 польз.	2	1	2	1	1	Нет	1
250 польз. с выс. дост.	2	1	4	1	1	Нет	2
800 польз.	2	1	2	1	1	Нет	1
800 польз. с выс. дост.	2	1	4	1	1	Нет	2
2000 польз.	2	1	5	1	1	Нет	3
2000 польз. с выс. дост.	2	1	6	1	1	Нет	4

[1] Это количество номеров доступа к системе, настраиваемое вами в Cisco WebEx Meetings Server.

Настройка профиля безопасности магистрали **SIP**

Настройка профиля безопасности магистрали **SIP** для сервера распределения нагрузки

Перед началом работы

Если система Cisco WebEx Meetings Server настроена на TLS, необходимо импортировать сертификат безопасного проведения телеконференций. Для получения дополнительной информации см. раздел "Импорт сертификатов безопасного проведения телеконференций" Руководства по администрированию.

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Выберите Система > Безопасность > Профиль безопасности магистрали **SIP**.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** Настройте приведенные ниже поля.

- Имя – введите имя для определения профиля безопасности магистрали SIP.
- Режим безопасности устройства – выберите Небезопасный для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью UDP/TCP. Нажмите Зашифрованный для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS.
- Имя объекта X.509 – введите имя сертификата для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS.

  Примечание Для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS другая система Cisco WebEx Meetings Server не может иметь тот же профиль безопасности магистрали SIP, поскольку все системы должны иметь разные сертификаты. Получить имя сертификата Cisco WebEx Meetings Server можно на веб-сайте Администрирования. Чтобы получить более подробные сведения, см. раздел "Управление сертификатами" в Руководстве по администрированию.
- Входящий порт – введите 5060 для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью UDP/TCP. Введите 5061 для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS.

Примечание Не изменяйте поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Сохранить.

Настройка профиля безопасности магистрали **SIP** для сервера приложений

Перед началом работы

Если система Cisco WebEx Meetings Server настроена на TLS, необходимо импортировать сертификат безопасного проведения телеконференций. Для получения дополнительной информации см. раздел "Импорт сертификатов безопасного проведения телеконференций" Руководства по администрированию.

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Выберите Система > Безопасность > Профиль безопасности магистрали **SIP**.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** Настройте приведенные ниже поля.

- Имя – введите имя для определения профиля безопасности магистрали SIP.
- Режим безопасности устройства – выберите Небезопасный для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью UDP/TCP. Нажмите Зашифрованный для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS.
- Имя объекта X.509 – введите имя сертификата для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS.

  Примечание Для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS другая система Cisco WebEx Meetings Server не может иметь тот же профиль безопасности магистрали SIP, поскольку все системы должны иметь разные сертификаты. Получить имя сертификата Cisco WebEx Meetings Server можно на веб-сайте Администрирования. Чтобы получить более подробные сведения, см. раздел "Управление сертификатами" в Руководстве по администрированию.
- Входящий порт – выберите 5062 для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью UDP/TCP. Введите 5063 для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS.

Примечание Не изменяйте поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Сохранить.

Настройка профиля **SIP**

Настройка стандартного профиля **SIP**

Стандартный профиль SIP использует параметры по умолчанию и не требует дополнительных действий по настройке.

Настройка профиля **TLS SIP**

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Нажмите Устройство > Параметры устройства > Профиль **SIP**.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** Настройте приведенные ниже поля.

- Имя – введите имя профиля SIP.
- Перенаправление по приложению – установите флажок.

Примечание Не изменяйте поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Сохранить.

Настройка профиля **IPv6 SIP**

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Нажмите Устройство > Параметры устройства > Профиль **SIP**.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** Настройте приведенные ниже поля.

- Имя – введите имя профиля SIP.
- Включить ENAT – установите флажок.

Примечание Не изменяйте поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Сохранить.

Конфигурация для **CUCM**

Для отдельных систем Cisco WebEx Meetings Server следует произвести настройку приведенных ниже конфигураций CUCM. Эти конфигурации не могут принадлежать нескольким системам.

- Управление сертификатами
- SIP-магистраль
- Группа маршрутов
- Список маршрутов
- Шаблон маршрутов
- Шаблон маршрутов SIP

Управление сертификатами

Для связи CUCM с сервером Cisco WebEx Meetings Server с помощью TLS необходимо выполнить приведенное ниже.

- Получите сертификат Cisco WebEx Meetings Server на сайте Администрирования и затем загрузите его в CUCM.
- Скачайте сертификат CUCM и затем загрузите его на сайт Администрирования Cisco WebEx Meeting Server.

Для получения более подробной информации см. раздел "Управление сертификатами" в онлайн-справке и Руководство по администрированию.

Загрузка сертификатов **Cisco WebEx Meetings Server**

Процедура

Шаг **1** Скачайте и отправьте сертификат Cisco WebEx Meetings Server.

a) Войдите на сайт Администрирования Cisco WebEx Meetings Server.
b) Выберите Параметры > Безопасность > Сертификаты.
c) Скопируйте имя сертификата в разделе "Сертификат SSL".
d) Выберите Больше параметров > Экспорт сертификата **SSL**.

e) Сохраните сертификат на локальный жесткий диск.

Шаг **2** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **3** Выберите **Cisco Unified OS Administration**.

Шаг **4** Выберите Безопасность > Управление сертификатами.

Шаг **5** Нажмите Загрузить сертификат/цепочку сертификатов.

Шаг **6** Выберите **CallManager-trust** в раскрывающемся меню "Сертификат".

Шаг **7** Нажмите кнопку Обзор и выберите сертификат, сохраненный на локальный жесткий диск.

Шаг **8** Нажмите Отправить файл.
Подождите, пока отобразится сообщение "Успешно выполнено: сертификат загружен.".

Шаг **9** Нажмите Закрыть.

Скачивание сертификатов **CUCM**

Обратитесь к документации CUCM, чтобы получить дополнительную информацию о создании сертификатов CUCM.

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified OS Administration**.

Шаг **3** Выберите Безопасность > Управление сертификатами.

Шаг **4** Найдите сертификат с именем "CallManager" в поле "Имя сертификата". Выберите поле "Файл .PEM".

Шаг **5** Нажмите Скачать, чтобы сохранить сертификат CUCM (CallManager.pem) на локальный жесткий диск.

Что дальше

Чтобы получить более подробные сведения о загрузке сертификатов CUCM в Cisco WebEx Meetings Server, см. раздел "Управление сертификатами" в онлайн-справке и Руководство по администрированию.

Настройка магистрали **SIP**

Настройка магистрали **SIP** на сервере распределения нагрузки

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Нажмите Устройство > Магистраль.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** В раскрывающемся меню Тип магистрали выберите Магистраль **SIP**.

Примечание Не изменяйте другие поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Далее.

Шаг **7** Настройте приведенные ниже поля.

- Имя устройства – введите имя для магистрали SIP.
- Резерв устройства – выберите По умолчанию из раскрывающегося меню.
- Адрес назначения – введите адрес IPv4 сервера распределения нагрузки.
- Адрес IPv6 назначения – введите адрес IPv6 сервера распределения нагрузки при необходимости включения IPv6 между CUCM и Cisco WebEx Meetings Server.
- Порт назначения – выберите 5060 для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью UDP/TCP. Введите 5061 для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS.
- Профиль безопасности магистрали SIP – выберите профиль безопасности сервера распределения нагрузки из раскрывающегося меню.
- Профиль SIP – выберите Стандартный профиль **SIP** для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью UDP/TCP. Выберите Профиль **TLS SIP** для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS. Выберите Профиль **IPv6 SIP**, чтобы включить IPv6 между CUCM и Cisco WebEx Meetings Server.

Примечание Не изменяйте другие поля на этой странице. Оставьте значения по умолчанию.

Шаг **8** Нажмите Сохранить.

Шаг **9** Выберите Сброс и затем Сброс и перезагрузка во всплывающем окне.
Для завершения настройки необходимо сбросить настройки магистрали SIP.

Настройка магистрали **SIP** для сервера приложений

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Нажмите Устройство > Магистраль.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** В раскрывающемся меню Тип магистрали выберите Магистраль **SIP**.

Примечание Не изменяйте другие поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Далее.

Шаг **7** Настройте приведенные ниже поля.

- Имя устройства – введите имя для магистрали SIP.
- Резерв устройства – выберите По умолчанию из раскрывающегося меню.
- Адрес назначения – введите адрес IPv4 сервера распределения нагрузки.
- Адрес IPv6 назначения – введите адрес IPv6 сервера распределения нагрузки при необходимости включения IPv6 между CUCM и Cisco WebEx Meetings Server.
- Порт назначения – выберите 5062 для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью UDP/TCP. Введите 5063 для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS.
- Профиль безопасности магистрали SIP – выберите профиль безопасности сервера распределения нагрузки из раскрывающегося меню.
- Профиль SIP – выберите Стандартный профиль **SIP** для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью UDP/TCP. Выберите Профиль **TLS SIP** для передачи данных между CUCM и Cisco WebEx Meetings Server с помощью TLS. Выберите Профиль **IPv6 SIP**, чтобы включить IPv6 между CUCM и Cisco WebEx Meetings Server.

Примечание Не изменяйте другие поля на этой странице. Оставьте значения по умолчанию.

Шаг **8** Нажмите Сохранить.

Шаг **9** Выберите Сброс и затемСброс и перезагрузка во всплывающем окне.
Для завершения настройки необходимо сбросить настройки магистрали SIP.

Настройка группы маршрутов

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Нажмите Маршрутизация вызова > Маршрут/Поиск > Группа маршрутов.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** Настройте приведенные ниже поля.

- Имя группы маршрутов – введите имя группы маршрутов.
- Алгоритм распределения. Выберите Циклический в раскрывающемся меню.

  Примечание Выбрав вариант Циклический, вы разрешаете CUCM распределение звонков для неактивных и доступных пользователей, начиная от пользователя (N+1) группы маршрутов, где N-й участник является участником, которому система CUCM позднее всего произвела вызов. Если N-й пользователь является последним участником группы маршрутов, CUCM отправляет вызов первому участнику группы маршрутов.
- Поиск устройств для добавления группы маршрутов – выберите Магистраль **SIP** сервера распределения нагрузки в списке доступных устройств. Затем выберите Добавить в группу маршрутов.

Примечание Не изменяйте другие поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Сохранить.

Что дальше

Создайте список маршрутов в группу маршрутов. Перейдите к Настройка списка маршрутов, на странице 80.

Настройка списка маршрутов

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Нажмите Маршрутизация вызова > Маршрут/поиск > Список маршрутов.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** Настройте приведенные ниже поля.

- Имя – введите имя списка маршрутов.
- Группа Cisco Unified Communications Manager – выберите По умолчанию из раскрывающегося списка.

Примечание Не изменяйте другие поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Сохранить.

Шаг **7** Выберите Добавить группу маршрутов.
Отобразится страница Конфигурация данных списка маршрутов.

Шаг **8** Выберите ранее настроенную группу маршрутов в раскрывающемся меню Группа маршрутов и выберите Сохранить.
Отобразится страница Конфигурация списка маршрутов.

Шаг **9** Нажмите Сохранить.

Что дальше

Настройка шаблона маршрутов для списка маршрутов. Перейдите к Настройка шаблона маршрутов, на странице 80.

Настройка шаблона маршрутов

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Нажмите Маршрутизация вызова > Маршрут/поиск > Шаблон маршрутов.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** Настройте приведенные ниже поля.

- Шаблон маршрутов – введите имя шаблона маршрутов.
- Список маршрутов/шлюзов – выберите ранее настроенный список маршрутов из раскрывающегося меню.

Примечание Не изменяйте другие поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Сохранить.

Настройка шаблона маршрутов **SIP**

Процедура

Шаг **1** Войдите на сайт http://ccm-server/, где *ccm-server* – это полное доменное имя или IP-адрес сервера Cisco Unified Communications Manager.

Шаг **2** Выберите **Cisco Unified CM Administration**.

Шаг **3** Нажмите Маршрутизация вызова > Шаблон маршрутов **SIP**.

Шаг **4** Нажмите кнопку Добавить.

Шаг **5** Настройте приведенные ниже поля.

- Использование шаблона – выберите Маршрутизация **IP**-адреса.
- Шаблон IPv4 – введите IP-адрес сервера приложений.
- Маршрутизация SIP – выберите ранее настроенную магистраль SIP для сервера приложений из раскрывающегося меню.

Примечание Не изменяйте другие поля на этой странице. Оставьте значения по умолчанию.

Шаг **6** Нажмите Сохранить.

Настройка **CUCM** для систем с высокой доступностью и без нее

В разделах ниже приведено описание заданий, требуемых для настройки систем разных размеров с высокой доступностью и без нее.

Настройка **CUCM** в системах на **50, 250** и **800** пользователей без высокой доступности

В этом разделе приводится информация и подробные инструкции о настройке CUCM для систем на 50, 250 и 800 пользователей без высокой доступности.

Необходимая информация

- IP-адрес одного сервера распределения нагрузки
- IP-адрес одного сервера приложений
- Количество номеров доступа к системе, настраиваемое в системе

Процедура настройки

Выполните приведенные ниже действия в указанном порядке.

Действие	Описание	Подробная информация
1	Просмотрите существующий профиль безопасности магистрали SIP и определите, удовлетворяет ли он требованиям для запуска Cisco WebEx Meetings Server. Если нет, настройте два профиля безопасности магистрали SIP.	Добавьте профиль безопасности магистрали SIP для сервера распределения нагрузки и профиль безопасности магистрали SIP для сервера приложений. См. разделы Настройка профиля безопасности магистрали SIP для сервера распределения нагрузки, на странице 71 и Настройка профиля безопасности магистрали SIP для сервера приложений, на странице 72.
2	Просмотрите существующий профиль SIP и определите, удовлетворяет ли он требованиям для запуска Cisco WebEx Meetings Server. Если нет, настройте профиль SIP соответствующим образом.	Настройте профиль SIP согласно требованиям в разделе Настройка профиля TLS SIP или Настройка профиля IPv6 SIP, на странице 74.
3	Настройте одну магистраль SIP для сервера распределения нагрузки.	См. Настройка профиля безопасности магистрали SIP для сервера распределения нагрузки, на странице 71.
4	Настройте одну магистраль SIP для сервера приложений.	См. Настройка профиля безопасности магистрали SIP для сервера приложений, на странице 72.

Действие	Описание	Подробная информация
5	Настройте одну группу маршрутов с помощью магистрали SIP, настроенной для сервера распределения нагрузки в действии 3 выше.	См. Настройка группы маршрутов, на странице 79.
6	Настройте один список маршрутов с помощью группы маршрутов, настроенного в действии 5 выше.	См. Настройка списка маршрутов, на странице 80.
7	Настройте шаблоны маршрутов(*N*) с помощью списка маршрутов выше. *N* является количеством номеров доступа к системе, установленным в параметрах аудиосвязи на сайте Администрирования.	См. Настройка шаблона маршрутов, на странице 80.
8	Настройте один шаблон маршрутов SIP для сервера приложений.	См. Настройка шаблона маршрутов SIP, на странице 81.

Настройка **CUCM** в системах на **50, 250** и **800** пользователей с высокой доступностью

В этом разделе приводится информация и подробные инструкции о настройке CUCM для систем на 50, 250 и 800 пользователей с высокой доступностью.

Необходимая информация

- IP-адреса двух серверов распределения нагрузки
- IP-адреса двух серверов приложений
- Количество номеров доступа к системе, настраиваемое в системе

Процедура настройки

Выполните приведенные ниже действия в указанном порядке.

Действие	Описание	Подробная информация
1	Просмотрите существующий профиль безопасности магистрали SIP и определите, удовлетворяет ли он требованиям для запуска Cisco WebEx Meetings Server. Если нет, настройте два профиля безопасности магистрали SIP.	Добавьте профиль безопасности магистрали SIP для сервера распределения нагрузки и профиль безопасности магистрали SIP для сервера приложений. См. разделы Настройка профиля безопасности магистрали SIP для сервера распределения нагрузки, на странице 71 и Настройка профиля безопасности магистрали SIP для сервера приложений, на странице 72.
2	Просмотрите существующий профиль SIP и определите, удовлетворяет ли он требованиям для запуска Cisco WebEx Meetings Server. Если нет, настройте профиль SIP соответствующим образом.	Настройте профиль SIP согласно требованиям в разделе Настройка профиля TLS SIP или Настройка профиля IPv6 SIP, на странице 74.
3	Настройте две магистрали SIP для серверов распределения нагрузки.	См. Настройка профиля безопасности магистрали SIP для сервера распределения нагрузки, на странице 71.
4	Настройте две магистрали SIP для серверов приложений.	См. Настройка профиля безопасности магистрали SIP для сервера приложений, на странице 72.
5	Настройте одну группу маршрутов с помощью магистрали SIP, настроенной для сервера распределения нагрузки в действии 3 выше.	См. Настройка группы маршрутов, на странице 79.
6	Настройте один список маршрутов с помощью группы маршрутов, настроенного в действии 5 выше.	См. Настройка списка маршрутов, на странице 80.
7	Настройте шаблоны маршрутов(*N*) с помощью списка маршрутов выше. *N* является количеством номеров доступа к системе, установленным в параметрах аудиосвязи на сайте Администрирования.	См. Настройка шаблона маршрутов, на странице 80.
8	Настройте два шаблона маршрутов SIP для серверов приложений.	См. Настройка шаблона маршрутов SIP, на странице 81.

Настройка **CUCM** в системах на **2000** пользователей без высокой доступности

В этом разделе приводится информация и подробные инструкции о настройке CUCM для систем на 2000 пользователей без высокой доступности.

Необходимая информация

- IP-адреса двух серверов распределения нагрузки
- IP-адреса трех серверов приложений
- Количество номеров доступа к системе, настраиваемое в системе

Процедура настройки

Выполните приведенные ниже действия в указанном порядке.

Действие	Описание	Подробная информация
1	Просмотрите существующий профиль безопасности магистрали SIP и определите, удовлетворяет ли он требованиям для запуска Cisco WebEx Meetings Server. Если нет, настройте два профиля безопасности магистрали SIP.	Добавьте профиль безопасности магистрали SIP для сервера распределения нагрузки и профиль безопасности магистрали SIP для сервера приложений. См. разделы Настройка профиля безопасности магистрали SIP для сервера распределения нагрузки, на странице 71 и Настройка профиля безопасности магистрали SIP для сервера приложений, на странице 72.
2	Просмотрите существующий профиль SIP и определите, удовлетворяет ли он требованиям для запуска Cisco WebEx Meetings Server. Если нет, настройте профиль SIP соответствующим образом.	Настройте профиль SIP согласно требованиям в разделе Настройка профиля TLS SIP или Настройка профиля IPv6 SIP, на странице 74.
3	Настройте две магистрали SIP для серверов распределения нагрузки.	См. Настройка профиля безопасности магистрали SIP для сервера распределения нагрузки, на странице 71.
4	Настройте три магистрали SIP для серверов приложений.	См. Настройка профиля безопасности магистрали SIP для сервера приложений, на странице 72.

Действие	Описание	Подробная информация
5	Настройте одну группу маршрутов с помощью магистрали SIP, настроенной для сервера распределения нагрузки в действии 3 выше.	См. Настройка группы маршрутов, на странице 79.
6	Настройте один список маршрутов с помощью группы маршрутов, настроенного в действии 5 выше.	См. Настройка списка маршрутов, на странице 80.
7	Настройте шаблоны маршрутов(*N*) с помощью списка маршрутов выше. *N* является количеством номеров доступа к системе, установленным в параметрах аудиосвязи на сайте Администрирования.	См. Настройка шаблона маршрутов, на странице 80.
8	Настройте три шаблона маршрутов SIP для серверов приложений.	См. Настройка шаблона маршрутов SIP, на странице 81.

Настройка **CUCM** в системах на **2000** пользователей с высокой доступностью

В этом разделе приводится информация и подробные инструкции о настройке CUCM для систем на 2000 пользователей с высокой доступностью.

Необходимая информация

- IP-адреса двух серверов распределения нагрузки
- IP-адреса четырех серверов приложений
- Количество номеров доступа к системе, настраиваемое в системе

Процедура настройки

Выполните приведенные ниже действия в указанном порядке.

Действие	Описание	Подробная информация
1	Просмотрите существующий профиль безопасности магистрали SIP и определите, удовлетворяет ли он требованиям для запуска Cisco WebEx Meetings Server. Если нет, настройте два профиля безопасности магистрали SIP.	Добавьте профиль безопасности магистрали SIP для сервера распределения нагрузки и профиль безопасности магистрали SIP для сервера приложений. См. разделы Настройка профиля безопасности магистрали SIP для сервера распределения нагрузки, на странице 71 и Настройка профиля безопасности магистрали SIP для сервера приложений, на странице 72.
2	Просмотрите существующий профиль SIP и определите, удовлетворяет ли он требованиям для запуска Cisco WebEx Meetings Server. Если нет, настройте профиль SIP соответствующим образом.	Настройте профиль SIP согласно требованиям в разделе Настройка профиля TLS SIP или Настройка профиля IPv6 SIP, на странице 74.
3	Настройте две магистрали SIP для серверов распределения нагрузки.	См. Настройка профиля безопасности магистрали SIP для сервера распределения нагрузки, на странице 71.
4	Настройте четыре магистрали SIP для серверов приложений.	См. Настройка профиля безопасности магистрали SIP для сервера приложений, на странице 72.
5	Настройте одну группу маршрутов с помощью магистрали SIP, настроенной для сервера распределения нагрузки в действии 3 выше.	См. Настройка группы маршрутов, на странице 79.
6	Настройте один список маршрутов с помощью группы маршрутов, настроенного в действии 5 выше.	См. Настройка списка маршрутов, на странице 80.
7	Настройте шаблоны маршрутов(*N*) с помощью списка маршрутов выше. *N* является количеством номеров доступа к системе, установленным в параметрах аудиосвязи на сайте Администрирования.	См. Настройка шаблона маршрутов, на странице 80.
8	Настройте четыре шаблона маршрутов SIP для серверов приложений.	См. Настройка шаблона маршрутов SIP, на странице 81.

ГЛАВА 7

Загрузка и массовое развертывание приложений

Для использования этого продукта необходимы дополнительные приложения, которые необходимо скачать на компьютеры ваших пользователей. Вы можете скачать и выполнить массовое развертывание этих приложений с помощью инструментов, доступных на вашем сайте Администрирования. Эти приложения включают приведенное ниже.

- Cisco WebEx Meetings (для Windows и Mac)
- Инструменты повышения производительности Cisco WebEx (Windows)
- Проигрыватель сетевых записей Cisco WebEx (для Windows и Mac)

Чтобы установить эти приложения на компьютеры ваших пользователей, вы можете настроить автоматическое скачивание с помощью сайта Администрирования, разрешить пользователям самостоятельно скачивать приложения, установить приложения на компьютеры ваших пользователей или скачать установочные файлы и установить их вручную на компьютерах своих пользователей.

Этот продукт может использоваться на компьютерах, имеющих права администратора и не имеющих их. Автоматическое скачивание, скачивание и установка пользователем и установка приложений на компьютеры ваших пользователей применимы только если ваши пользователи обладают правами администратора. Если ваша компания не предоставляет пользователям права администратора, вам необходимо будет использовать альтернативный подход для установки приложений на их компьютеры.

На ПК с правами администратора.

- Пользователи могут скачать и установить приложение Cisco WebEx Meetings, Инструменты повышения производительности и проигрыватель сетевых записей на страницах для скачивай конечных пользователей. Дополнительные действия администратора не требуются.
- Во время первого входа пользователям будет предложено установить Инструменты повышения производительности.
- Приложение Cisco WebEx Meetings скачивается по запросу, когда пользователь впервые присоединяется к совещанию, и устанавливается без предупреждения на ПК пользователя.

На ПК без прав администратора.

- Рекомендуется запустить приложение Cisco WebEx Meetings и Инструменты повышения производительности в автономном режиме на рабочих столах конечных пользователей перед тем, как сообщить им о созданных учетных записях. Благодаря этому ваши пользователи смогут начинать совещания и присоединяться к ним с помощью своих веб-браузеров и рабочих столов Windows при первом входе.
- Программы установки MSI можно получить на странице: Администратор > Параметры > Скачивания. Для получения дополнительной информации см. Настройка параметров скачивания.
- Если вы решите не запускать приложения для своих пользователей, они смогут получить доступ к этим приложениям на страницах скачиваний конечных пользователей. Если на ПК пользователей запрещена установка скачанных приложений, они не смогут завершить процесс установки.
- Пользователи могут успешно присоединяться к совещаниям, если они используют для этой цели веб-браузеры (приложение Cisco WebEx Meetings можно скачать по запросу). Кроме того, приложение Cisco WebEx Meetings попытается выполнить установку, чтобы ускорить начало следующих совещаний или присоединение к ним. Ошибка возникает вследствие того, что на этом ПК нет прав администратора.

- Скачивание приложений на сайте Администрирования, страница 90
- Содержание файлов ZIP приложения, страница 92
- Групповое развертывание Инструментов повышения производительности Cisco WebEx, страница 94
- Групповое развертывание приложения Meetings, страница 102
- Групповое развертывание проигрывателя сетевых записей, страница 105

Скачивание приложений на сайте Администрирования

Вы можете настроить систему таким образом, чтобы администраторы могли вручную скачивать приложения рабочего стола Cisco WebEx для пользователей, кроме того, вы можете разрешить пользователям скачивать материалы самостоятельно.

Процедура

Шаг **1** Войдите на сайт Администрирования.

Шаг **2** Выберите Параметры > Скачивания.

Шаг **3** Установите флажок Автоматическое обновление Инструментов повышения производительности **WebEx**, чтобы настроить периодические автоматические обновления. (По умолчанию**.** Флажок установлен.)

Шаг **4** Выберите метод скачивания.

- Разрешить пользователям скачивать приложения рабочего стола WebEx

- Вручную устанавливать настольные приложения WebEx на рабочий стол пользователя

Выбрав Разрешить пользователям скачивать приложения рабочего стола **WebEx**, можно нажать Сохранить, чтобы завершить настройку параметров скачивания. Дальнейшие действия не требуются. Выбрав Вручную устанавливать настольные приложения **WebEx** на рабочий стол пользователя, перейдите к следующему шагу.

Чтобы включить параметр проведения конференций для пользователей, у которых нет прав администратора, включите функцию Вручную устанавливать настольные приложения **WebEx** на рабочий стол пользователя.

При выборе Вручную устанавливать настольные приложения **WebEx** на рабочий стол пользователя на странице появляются разделы "Cisco WebEx Meetings", "Инструменты повышения производительности" и "Проигрыватель сетевых записей".

Шаг **5** В разделе "WebEx Meetings" выберите Скачать и Сохранить, чтобы сохранить файл ZIP в системе.
Файл ZIP содержит установщики для платформ Windows и Mac на всех доступных языках. По открытии файла ZIP выберите установщик для вашей платформы и языка. Установщик для системы Windows – это файл MSI. Установщик для системы Mac – это файл DMG.

Шаг **6** В разделе "Инструменты повышения производительности" выберите Скачать и Сохранить, чтобы сохранить файл ZIP в системе.
Файл ZIP содержит установщики для всех доступных языков. По открытии файла ZIP выберите установщик для вашего языка. Установщик представляет собой файл MSI.

Шаг **7** В разделе "Проигрыватель сетевых записей WebEx" выберите Скачать и Сохранить, чтобы сохранить файл ZIP в системе.
Файл ZIP содержит установщики для платформ Windows и Mac на всех доступных языках. По открытии файла ZIP выберите установщик для вашей платформы и языка. Установщик для системы Windows – это файл MSI. Установщик для системы Mac – это файл DMG.

Шаг **8** Нажмите Сохранить, чтобы сохранить параметры скачивания.

Что дальше

Распакуйте файл MSI или DMG и разверните эти клиенты на рабочих столах конечных пользователей с помощью корпоративной программы для группового развертывания. Это гарантирует мгновенную доступность клиентов, когда пользователь начинает планирование совещания, присоединяется к нему или просматривает записи. Для получения дополнительной информации о развертывании клиентов в среде Windows см. приведенные ниже разделы.

- Групповое развертывание Инструментов повышения производительности Cisco WebEx, на странице 94
- Групповое развертывание приложения Meetings, на странице 102
- Групповое развертывание проигрывателя сетевых записей, на странице 105

Каждый файл ZIP содержит установщик приложения для всех 13 поддерживаемых языков. Для получения информации об определении установщика, необходимого для каждого файла ZIP, см. раздел Содержание файлов ZIP приложения, на странице 92.

Содержание файлов **ZIP** приложения

В этом разделе приводится описание приложений установки, содержащихся в каждом файле ZIP, загружаемом на сайте Администрирования. Файлы ZIP содержат одно приложение установки для одного языка. В этом разделе также приводится справка в отношении определения языка каждого установщика. Приложения установки для Windows существуют на 13 языках. Приложения установки для Mac предлагаются только на английском.

Ключ языка приложения

Файл установки приложения на английском в каждом файле ZIP не содержит в названии суффикс языка. Например, клиент WebEx Meetings имеет название onpremmc.msi (Windows) и webexmc_onprem.dmg (Mac). Файл установки приложения для других 12 языков имеет в названии сокращение, указывающее на язык содержащегося приложения. В таблице ниже приведены сокращения, используемые для каждого из языков.

Сокращ.	Язык
B5	Китайский (традиционное письмо)
DE	Немецкий
ES	Испанский (страны Латинской Америки)
FR	Французский
GB	Китайский (упрощенное письмо)
IT	Итальянский
JP	Японский
KO	Корейский
NL	Голландский
PT	Португальский
RU	Русский
SP	Испанский

Примечание Файлы для шведского языка (SV) и поставщика телефонных услуг (TSP) также включены в файлы ZIP. Эти файлы не поддерживаются и не должны использоваться в целях установки приложений для использования с Cisco WebEx Meetings Server.

Содержание файла **ZIP** Инструментов повышения производительности

Файл ZIP Инструментов повышения производительности содержит приведенные ниже файлы. Используйте ключ в таблице выше, чтобы определить язык каждого из файлов. Обратите внимание на отсутствие Инструментов повышения производительности для Mac.

- ptools.msi
- ptools_B5.msi
- ptools_DE.msi
- ptools_ES.msi
- ptools_FR.msi
- ptools_GB.msi
- ptools_IT.msi
- ptools_JP.msi
- ptools_KO.msi
- ptools_NL.msi
- ptools_PT.msi
- ptools_RU.msi
- ptools_SP.msi
- ptools_SV.msi
- ptools_TSP.msi

Содержание файла **ZIP** клиента **WebEx Meetings**

Файл ZIP клиента WebEx Meetings содержит приведенные ниже файлы. Используйте ключ в таблице выше, чтобы определить язык каждого из файлов.

- onpremmc.msi
- onpremmc_B5.msi
- onpremmc_DE.msi
- onpremmc_ES.msi
- onpremmc_FR.msi
- onpremmc_GB.msi
- onpremmc_IT.msi
- onpremmc_JP.msi
- onpremmc_KO.msi
- onpremmc_NL.msi
- onpremmc_PT.msi
- onpremmc_RU.msi

- onpremmc_SP.msi
- onpremmc_SV.msi
- onpremmc_TSP.msi
- webexmc_onprem.dmg

Содержимое файла **ZIP** проигрывателя сетевых записей

Файл ZIP проигрывателя сетевых записей содержит приведенные ниже файлы. Используйте ключ в таблице выше, чтобы определить язык каждого из файлов.

- nbr2player_onprem.msi
- nbr2player_onprem_B5.msi
- nbr2player_onprem_DE.msi
- nbr2player_onprem_ES.msi
- nbr2player_onprem_FR.msi
- nbr2player_onprem_GB.msi
- nbr2player_onprem_IT.msi
- nbr2player_onprem_JP.msi
- nbr2player_onprem_KO.msi
- nbr2player_onprem_NL.msi
- nbr2player_onprem_PT.msi
- nbr2player_onprem_RU.msi
- nbr2player_onprem_SP.msi
- nbr2player_onprem_SV.msi
- nbr2player_onprem_TSP.msi
- webexnbrplayer_onprem.dmg

Групповое развертывание Инструментов повышения производительности **Cisco WebEx**

В этом разделе приведены описания заданий в рамках установки Инструментов повышения производительности Cisco WebEx. Раздел представляет собой полное руководство по различным типам установки, включая установку программы на одном компьютере и большом количестве машин с помощью сервера Microsoft Systems Management Server 2003 (SMS) Cisco WebEx Meetings Server поддерживает интеграцию для Outlook, содержащуюся в пакете ptools.msi.

Автоматическая установка администратором с помощью командной строки

Администраторы могут войти на компьютер пользователя и установить Инструменты повышения производительности WebEx с помощью автоматического режима.

Процедура

Шаг **1** Войдите на компьютер пользователя.

Шаг **2** Скачайте пакет MSI на жесткий диск компьютера и затем откройте Windows Command Prompt.

Примечание В Windows 7 и Windows Vista для его открытия следует использовать "Запуск от имени администратора".

Шаг **3** Запустите команду MSI для установки Инструментов повышения производительности WebEx в автоматическом режиме.

Пример:
msiexec.exe /q /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1

Имя параметра	Значение	Описание
OI	1	Включить Outlook Integration
	0 (по умолчанию)	Выключить Outlook Integration

Шаг **4** Перезапустите компьютер.

Автоматическое удаление администратором с помощью командной строки

Администраторы могут войти на компьютер пользователя и удалить Инструменты повышения производительности WebEx с помощью автоматического режима.

Процедура

Шаг **1** Войдите на компьютер пользователя.

Шаг **2** Скачайте пакет MSI в выбранное вами местоположение и затем откройте Windows Command Prompt.

Пример:

Примечание В Windows 7 и Windows Vista для его открытия следует использовать "Запуск от имени администратора".

Шаг **3** Удалить все компоненты пакета MSI ptools.msi, введя такую команду:

Пример:
msiexec.exe /q /x "ptools.msi"

Автоматическая установка с помощью **SMS**

Приведенные ниже ограничения касаются автоматической установки с помощью SMS.

- Индивидуальный режим SMS не поддерживается.
- Если администратор SMS хочет добавить функцию для Инструментов повышения производительности WebEx, ему следует сначала запустить команду **REMOVE** и затем команду **ADDSOURCE**, даже если функция не была прежде установлена.
- Если пользователь входит на компьютер с помощью удаленного рабочего стола, пока администратор размещает пакет, он должен перезапустить компьютер, чтобы обеспечить нормальную работу Инструментов повышения производительности WebEx.

Объявление Инструментов повышения производительности **Cisco WebEx** с помощью системной автономной программы **SMS**

Будучи администратором SMS, выполните приведенную ниже процедуру для объявления Инструментов повышения производительности Cisco WebEx с помощью системной автономной программы SMS.

Перед началом работы

Войдите на сайт Администрирования и вручную установите Инструменты повышения производительности на рабочем столе пользователя. Для получения дополнительных сведений см. раздел "Настройка параметров скачивания" Руководства по администрированию *Cisco WebEx Meetings Server*.

Процедура

Шаг **1** Создайте пакет из определения. Для получения дополнительной информации см. Создание пакета из определения, на странице 101.

Шаг **2** Измените параметры программы на "Автономная, системная" до объявления.

a) Откройте консоль администратора SMS и выберите База данных сайта > Пакеты > Инструменты повышения производительности **Cisco WebEx 2.80, Cisco WebEx LLC,** англ. > Программы.

b) Щелкните правой кнопкой мыши по параметру Автономная**,** системная и затем выберите Свойства, чтобы открыть диалоговое окно Свойства системной автономной программы.

c) Откройте вкладку Среда.

- Для параметра Программа может запускаться выберите Только когда пользователь выполнил вход.
- В разделе Режим работы выберите Работать с правами администратора. (Не включайте Разрешать пользователям взаимодействовать с этой программой.)

d) Откройте вкладку Общая информация.
e) Добавьте дополнительный параметр в командную строку, чтобы определить некоторые параметры для Инструментов повышения производительности Cisco WebEx.

- Добавьте SITEURL="http://sample.webex.com", чтобы указывать URL сайта WebEx, используемый вашей компанией.
- Добавьте флажки Инструментов повышения производительности, чтобы указать компонент, включенный для Инструментов повышения производительности WebEx. Параметр указывается в верхнем регистре, и значением по умолчанию является 0 (выключено).

  В приведенном ниже примере начальная командная строка соответствует msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi".
- Добавьте флажки и параметры Инструментов повышения производительности в командную строку: msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1.

  Примечание Чтобы получить информацию об определениях параметров, см. таблицу параметров в разделе Автоматическая установка администратором с помощью командной строки, на странице 95.

Шаг **3** Теперь вы можете объявить программу.

a) Откройте консоль администратора SMS и выберите База данных сайта > Пакеты > Инструменты повышения производительности **Cisco WebEx 2.80, Cisco WebEx LLC,** англ. > Программы.
b) Правой кнопкой мыши щелкните по Системная, автономная.
c) Нажмите Все действия > Распределить программное обеспечение.
d) Нажмите Далее в Мастере распределения программного обеспечения.
e) Выберите сервер SMS и нажмите Далее.
f) Выберите собрание и нажмите Далее.
g) Введите имя объявления в поле Имя и выберите Далее.
h) Укажите, должно ли объявление касаться вложенных коллекций, и нажмите Далее.
i) Укажите, когда программа будет объявлена, и нажмите Далее.
j) Укажите, присваивать ли программу, и нажмите Далее.
k) Нажмите Завершить на странице Завершение работы с мастером распределения программного обеспечения.
l) Перейдите в каталог \Site Database\System Status\Advertisement Status и проверьте состояние объявления.
   При включении уведомлений пользователь увидит сообщение с указанием того, что присвоенная программа запустится после ее объявления. Присвоенная программа запустится автоматически.

Удаление компонентов Инструментов повышения производительности с помощью системной автономной программы SMS

Для удаления Инструментов повышения производительности выполните приведенное ниже.

Процедура

Шаг **1** Создайте новую программу и скопируйте все параметры из области "системная автономная программа", как описано в разделе Объявление Инструментов повышения производительности Cisco WebEx с помощью системной автономной программы SMS, на странице 96, и затем обновите командную строку.

a) Откройте консоль администратора SMS и выберите База данных сайта > Пакеты > Инструменты повышения производительности **Cisco WebEx 2.80, Cisco WebEx LLC,** англ. > Программы.
b) Правой кнопкой мыши щелкните по пустой области и затем выберите Создать > Программа.
c) Введите имя программы и командную строку по умолчанию.
d) В диалоговом окне Свойства выберите вкладку Среда.
   - Для параметра Программа может запускаться выберите Только когда пользователь выполнил вход.
   - В разделе Режим работы выберите Работать с правами администратора. Не включайте Разрешать пользователям взаимодействовать с этой программой.
e) Обновите командную строку на вкладке Общие.
f) Добавьте REMOVE в командную строку и укажите функции, которые следует удалить.

   Пример:
   При необходимости удалить OI введите такую команду: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI"

Шаг **2** Объявите программу для выбранных коллекций рабочих машин в домене. Для получения дополнительной информации см. Автоматическая установка с помощью SMS, на странице 96.
Инструменты повышения производительности Cisco WebEx будут обновлены на этих машинах автоматически.

Добавление компонентов Инструментов повышения производительности с помощью системной автономной программы **SMS**

Чтобы администратор мог добавить компонент в Инструменты повышения производительности, он должен сначала запустить команду REMOVE и затем ADDSOURCE, даже если компонент не был ранее установлен.

Процедура

Шаг **1** Создайте новую программу под именем "Add-phase1" и скопируйте все параметры из области "системная автономная программа" и затем обновите командную строку.

a) Откройте консоль администратора SMS и перейдите к База данных сайта > Пакеты > Инструменты повышения производительности **Cisco WebEx 2.80, Cisco WebEx LLC,** англ. > Программы.
b) Правой кнопкой мыши щелкните по пустой области и затем выберите Создать > Программа.
c) Введите имя программы и командную строку по умолчанию.
d) В диалоговом окне "Свойства" откройте вкладку Среда.

- Для параметра Программа может запускаться выберите Только когда пользователь выполнил вход.
- В разделе Режим работы выберите Работать с правами администратора. Не включайте Разрешать пользователям взаимодействовать с этой программой.

e) Обновите командную строку на вкладке Общие.
f) Добавьте REMOVE в командную строку и укажите функции, которые следует добавить.

Пример:
При необходимости добавить службы OI их необходимо сначала удалить (REMOVE), даже если они не были ранее установлены: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI"

Шаг **2** Объявите программу для выбранных коллекций рабочих машин в домене. Для получения дополнительной информации см. Автоматическая установка с помощью SMS, на странице 96.

Шаг **3** Создайте вторую программу под именем "Add-phase2" и скопируйте все параметры из области "системная автономная программа" и затем обновите командную строку.

a) Откройте консоль администратора SMS и перейдите к База данных сайта > Пакеты > Инструменты повышения производительности **Cisco WebEx 2.80, Cisco WebEx LLC,** англ. > Программы.
b) Правой кнопкой мыши щелкните по пустой области и затем выберите Создать > Программа.
c) Введите имя программы и командную строку по умолчанию.
d) В диалоговом окне "Свойства" откройте вкладку Среда.

- Для параметра Программа может запускаться выберите Только когда пользователь выполнил вход.

- В разделе Режим работы выберите Работать с правами администратора. Не включайте Разрешать пользователям взаимодействовать с этой программой.

e) В диалоговом окне "Свойства" откройте вкладку Расширенные.
f) Включите Сначала запускать другую программу и выберите программу **Add-phase1**.
g) Обновите командную строку на вкладке Общие.
h) Добавьте ADDSOURCE в командную строку и укажите функции, которые следует добавить.

Пример:
При необходимости добавить службы OI их необходимо сначала удалить (REMOVE), даже если они не были ранее установлены: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" ADDSOURCE="OI" OI=1

Шаг **4** Объявите программу для выбранных коллекций рабочих машин в домене. Для получения дополнительной информации см. Автоматическая установка с помощью SMS, на странице 96.
Инструменты повышения производительности Cisco WebEx будут обновлены на этих машинах автоматически.

Установка Инструментов повышения производительности с помощью системной программы удаления **SMS**

Администратор SMS может удалить Инструменты повышения производительности Cisco WebEx с помощью системной программы удаления SMS, выполнив приведенные ниже действия.

Процедура

Шаг **1** Используйте пакет установки SMS, созданный в Создание пакета из определения, на странице 101.

Шаг **2** Объявите системную программу удаления, чтобы удалить Инструменты повышения производительности Cisco WebEx.
Инструменты повышения производительности Cisco WebEx будут удалены на этих машинах автоматически.

Объявление программы дляо бновления новой версии Инструментов повышения производительности **WebEx**

Для объявления программы для обновления новой версии Инструментов повышения производительности Cisco WebEx выполните приведенное ниже.

Перед началом работы

Войдите на сайт Администрирования, выберите Параметры > Скачивания и выключите приведенные ниже параметры.

- Автоматическое обновление Инструментов повышения производительности **Cisco WebEx**
- Разрешить пользователям скачивать приложения рабочего стола **WebEx**

Процедура

Шаг **1** Создайте новый пакет установки SMS с помощью пакета MSI Инструментов повышения производительности WebEx. Для получения дополнительной информации см. Создание пакета из определения, на странице 101.

Шаг **2** До объявления измените параметры программы на Автономная**,** системная. Для получения дополнительной информации см. Добавление компонентов Инструментов повышения производительности с помощью системной автономной программы SMS, на странице 99.

Шаг **3** Объявите программу. Для получения дополнительной информации см. Добавление компонентов Инструментов повышения производительности с помощью системной автономной программы SMS, на странице 99.
Старая версия Инструментов повышения производительности WebEx удалена, и новая версия Инструментов повышения производительности WebEx установлена автоматически.

Создание пакета из определения

Выполните приведенные ниже действия, чтобы создать пакет из определения.

Процедура

Шаг **1** Откройте консоль администратора SMS и выберите База данных сайта > Пакет.

Шаг **2** Правой кнопкой мыши щелкните по Пакет.

Шаг **3** Выберите Создать > Пакет из определения.

Шаг **4** В мастере Создание пакета из определения выберите Далее.

Шаг **5** Нажмите Обзор, чтобы найти и выбрать пакет MSI Инструментов повышения производительности WebEx, и затем нажмите Далее.

Шаг **6** Выберите Всегда получать файлы из каталога источника и нажмите Далее.

Шаг **7** Выберите местоположение каталога источника. Путь каталога представляет собой папку, содержащую пакет установки. Затем нажмите "Далее".

Шаг **8** Нажмите Завершить.

Шаг **9** Выберите База данных сайта > Пакеты > Инструменты повышения производительности **Cisco WebEx 2.80, Cisco WebEx LLC,** англ**.** > Программы. Доступно шесть программ по умолчанию.

Групповое развертывание приложения **Meetings**

В этом разделе приведены описания заданий в рамках установки приложения Cisco WebEx Meetings. Раздел представляет собой полное руководство по различным типам установки, включая установку программы на одном компьютере и большом количестве машин с помощью сервера Microsoft Systems Management Server 2003 (SMS)

Установка **Cisco WebEx Meetings**

Перед началом работы

Приведенные ниже необходимые условия применяются к установщику Cisco WebEx Meetings.

- Установка пакета MSI Cisco WebEx требует наличия прав администратора. Пакет MSI устанавливается в папку по умолчанию "Программы" операционной системы, для доступа к которой необходимы права администратора.
- Пакет MSI Cisco WebEx разработан для Windows Installer Service 2.0 и более новых версий. Если локальная машина настроена с помощью более ранней версии, отобразится сообщение об ошибке, информирующее о том, что для установки этого пакета MSI необходима более новая версия программы Windows Installer Service. По выполнении пакета MSI пользователю будут приведены инструкции в отношении базового интерфейса MSI.

Процедура

Шаг **1** Запустите установщик на компьютере пользователя.
Откроется мастер установки с приветственным сообщением.

Шаг **2** Нажмите Далее в нескольких следующих диалоговых окнах, пока не отобразится диалоговое окно установки.

Шаг **3** Нажмите Установить.

Шаг **4** Нажмите Завершить по окончании установки.

Автоматическая установка администратором с помощью командной строки

Вы можете войти на компьютер пользователя и установить приложение Cisco WebEx с помощью автоматического режима.

Процедура

Шаг **1** Войдите на компьютер пользователя.

Шаг **2** Скачайте пакет MSI на жесткий диск компьютера и затем откройте Windows Command Prompt.

Примечание В Windows 7 и Windows Vista для его открытия следует использовать "Запуск от имени администратора".

Шаг **3** Введите команду MSI для установки приложений совещаний Cisco WebEx в автоматическом режиме.

Пример:
Введите msiexec /i onpremmc.msi /qn.

Шаг **4** Перезапустите компьютер.

Автоматическое удаление администратором с помощью командной строки

Вы можете войти на компьютер пользователя и удалить приложение Cisco WebEx с помощью автоматического режима.

Процедура

Шаг **1** Войдите на компьютер пользователя.

Шаг **2** Скачайте пакет MSI в выбранное вами местоположение и затем откройте Windows Command Prompt.

Примечание В Windows 7 и Windows Vista для его открытия следует использовать "Запуск от имени администратора".

Шаг **3** Удалите все компоненты пакета MSI onpremmc.msi, введя такую команду: msiexec/x onpremmc.msi/qn.

Автоматическая установка с помощью **SMS**

Перед началом работы

Приведенные ниже ограничения касаются автоматической установки с помощью SMS.

- Индивидуальный режим SMS не поддерживается.
- Если пользователь входит на компьютер с помощью удаленного рабочего стола, пока администратор размещает пакет, он должен перезапустить компьютер, чтобы обеспечить нормальную работу приложения WebEx Meetings.

Объявление приложения **Cisco WebEx Meetings** с помощью системной автономной программы **SMS**

Будучи администратором SMS, выполните приведенную ниже процедуру для объявления приложения Cisco WebEx Meetings с помощью системной автономной программы SMS.

Перед началом работы

Войдите на сайт Администрирования и настройте параметры скачивания на установку приложений рабочего стола WebEx на рабочий стол пользователя вручную. Для получения дополнительных сведений см. раздел "Настройка параметров скачивания" Руководства по администрированию Cisco WebEx Meetings Server.

Процедура

Шаг **1** Создайте пакет из определения. Для получения дополнительной информации см. Создание пакета из определения, на странице 101.

Шаг **2** Измените параметры программы на "Автономная, системная" до объявления.

a) Откройте консоль администратора SMS и выберите База данных сайта > Пакеты > **Cisco WebEx Meeting Application, Cisco WebEx LLC,** англ. > Программы.
b) Щелкните правой кнопкой мыши по параметру Автономная**,** системная и затем выберите Свойства, чтобы открыть диалоговое окно Свойства системной автономной программы.
c) Откройте вкладку Среда.
   - Для параметра Программа может запускаться выберите Только когда пользователь выполнил вход.
   - В разделе Режим работы выберите Работать с правами администратора. Не включайте Разрешать пользователям взаимодействовать с этой программой.
d) Откройте вкладку Общая информация.
e) Добавьте дополнительный параметр в командную строку, чтобы определить некоторые параметры для приложения WebEx Meetings.

   Пример**.**
   Например, начальная командная строка представляет собой: msiexec /i "onpremmc.msi" /qn

Шаг **3** Теперь вы можете объявить программу.

a) Откройте консоль администратора SMS и выберите База данных сайта > Пакеты > **Cisco WebEx Meeting Application, Cisco WebEx LLC,** англ**.** > Программы.
b) Правой кнопкой мыши щелкните по Системная**,** автономная.
c) Нажмите Все действия > Распределить программное обеспечение.
d) Нажмите Далее в Мастере распределения программного обеспечения.
e) Выберите сервер SMS и нажмите Далее.
f) Выберите собрание и нажмите Далее.
g) Введите имя объявления в поле Имя и выберите Далее.
h) Укажите, должно ли объявление касаться вложенных коллекций, и нажмите Далее.

i) Укажите, когда программа будет объявлена, и нажмите Далее.
j) Укажите, присваивать ли программу, и нажмите Далее.
k) Нажмите Завершить на странице Завершение работы с мастером распределения программного обеспечения.
l) Перейдите в каталог \Site Database\System Status\Advertisement Status и проверьте состояние объявления.
   При включении уведомлений пользователь увидит сообщение с указанием того, что присвоенная программа запустится после ее объявления. Присвоенная программа запустится автоматически.

Удаление приложения **Cisco WebEx Meetings** с помощью системной программы удаления **SMS**

Администратор SMS может удалить приложение Cisco WebEx Meetings с помощью системной программы удаления SMS, выполнив приведенные ниже действия.

Процедура

Шаг **1** Используйте пакет установки SMS, созданный в Создание пакета из определения, на странице 101.

Шаг **2** Объявите системную программу удаления, чтобы удалить приложение Cisco WebEx Meetings. Приложение Cisco WebEx Meetings будет автоматически удалено на выбранных машинах.

Групповое развертывание проигрывателя сетевых записей

В этом разделе приведены описания заданий в рамках установки проигрывателя сетевых записей Cisco WebEx. Раздел представляет собой полное руководство по различным типам установки, включая установку программы на одном компьютере и большом количестве машин с помощью сервера Microsoft Systems Management Server 2003 (SMS)

Установка проигрывателя сетевых записей

Перед началом работы

Приведенные ниже необходимые условия применяются к установщику проигрывателя сетевых записей Cisco WebEx.

- Установка пакета MSI Cisco WebEx требует наличия прав администратора. Пакет MSI устанавливается в папку по умолчанию "Программы" операционной системы, для доступа к которой необходимы права администратора.
- Пакет MSI Cisco WebEx разработан для Windows Installer Service 2.0 и более новых версий. Если локальная машина настроена с помощью более ранней версии, отобразится сообщение об ошибке, информирующее о том, что для установки этого пакета MSI необходима более новая версия программы Windows Installer Service. По выполнении пакета MSI пользователю будут приведены инструкции в отношении базового интерфейса MSI.

Процедура

Шаг **1** Запустите установщик на компьютере пользователя.
Откроется мастер установки с приветственным сообщением.

Шаг **2** Нажмите Далее в нескольких следующих диалоговых окнах, пока не отобразится диалоговое окно установки.

Шаг **3** Нажмите Установить.

Шаг **4** Нажмите Завершить по окончании установки.

Автоматическая установка администратором с помощью командной строки

Вы можете войти на компьютер пользователя и установить проигрыватель сетевых записей Cisco WebEx с помощью автоматического режима.

Процедура

Шаг **1** Войдите на компьютер пользователя.

Шаг **2** Скачайте пакет MSI на жесткий диск компьютера и затем откройте Windows Command Prompt.

Примечание В Windows 7 и Windows Vista для его открытия следует использовать "Запуск от имени администратора".

Шаг **3** Введите команду MSI для установки проигрывателя сетевых записей Cisco WebEx в автоматическом режиме.

Пример:
Введите msiexec/i nbr2player_onprem.msi/qn.

Шаг **4** Перезапустите компьютер.

Автоматическое удаление администратором с помощью командной строки

Вы можете войти на компьютер пользователя и удалить проигрыватель сетевых записей Cisco WebEx с помощью автоматического режима.

Процедура

Шаг **1** Войдите на компьютер пользователя.

Шаг **2** Скачайте пакет MSI в выбранное вами местоположение и затем откройте Windows Command Prompt.

Примечание В Windows 7 и Windows Vista для его открытия следует использовать "Запуск от имени администратора".

Шаг **3** Удалите все компоненты пакета MSI onpremmc.msi, введя такую команду: msiexec/i nbr2player_onprem.msi/qn.

Автоматическая установка с помощью **SMS**

Перед началом работы

Приведенные ниже ограничения касаются автоматической установки с помощью SMS.

- Индивидуальный режим SMS не поддерживается.
- Если пользователь входит на компьютер с помощью удаленного рабочего стола, пока администратор размещает пакет, он должен перезапустить компьютер, чтобы обеспечить нормальную работу приложения WebEx Meetings.

Объявление проигрывателя сетевых записей **Cisco WebEx** с помощью системной автономной программы **SMS**

Будучи администратором SMS, выполните приведенную ниже процедуру для объявления проигрывателя сетевых записей Cisco WebEx с помощью системной автономной программы SMS.

Перед началом работы

Войдите на сайт Администрирования и настройте параметры скачивания на установку приложений рабочего стола WebEx на рабочий стол пользователя вручную. Для получения дополнительных сведений см. раздел "Настройка параметров скачивания" Руководства по администрированию Cisco WebEx Meetings Server.

Процедура

Шаг **1** Создайте пакет из определения. Для получения дополнительной информации см. Создание пакета из определения, на странице 101.

Шаг **2** Измените параметры программы на "Автономная, системная" до объявления.

a) Откройте консоль администратора SMS и выберите База данных сайта > Пакеты > Проигрыватель сетевых записей **Cisco WebEx, Cisco WebEx LLC,** англ. > Программы.

b) Щелкните правой кнопкой мыши по параметру Автономная, системная и затем выберите Свойства, чтобы открыть диалоговое окно Свойства системной автономной программы.

c) Откройте вкладку Среда.

- Для параметра Программа может запускаться выберите Только когда пользователь выполнил вход.
- В разделе Режим работы выберите Работать с правами администратора. Не включайте Разрешать пользователям взаимодействовать с этой программой.

d) Откройте вкладку Общая информация.

e) Добавьте дополнительный параметр в командную строку, чтобы определить некоторые параметры для приложения WebEx Meetings.

Пример:
Например, начальная командная строка представляет собой: msiexec /i "nbr2player_onprem.msi" /qn

Шаг **3** Теперь вы можете объявить программу.

a) Откройте консоль администратора SMS и выберите База данных сайта > Пакеты > Проигрыватель сетевых записей **Cisco WebEx, Cisco WebEx LLC,** англ. > Программы.

b) Правой кнопкой мыши щелкните по Системная, автономная.

c) Нажмите Все действия > Распределить программное обеспечение.

d) Нажмите Далее в Мастере распределения программного обеспечения.

e) Выберите сервер SMS и нажмите Далее.

f) Выберите собрание и нажмите Далее.

g) Введите имя объявления в поле Имя и выберите Далее.

h) Укажите, должно ли объявление касаться вложенных коллекций, и нажмите Далее.

i) Укажите, когда программа будет объявлена, и нажмите Далее.

j) Укажите, присваивать ли программу, и нажмите Далее.

k) Нажмите Завершить на странице Завершение работы с мастером распределения программного обеспечения.

l) Перейдите в каталог \Site Database\System Status\Advertisement Status и проверьте состояние объявления.
При включении уведомлений пользователь увидит сообщение с указанием того, что присвоенная программа запустится после ее объявления. Присвоенная программа запустится автоматически.

Удаление проигрывателя сетевых записей **Cisco WebEx** с помощью системной программы удаления **SMS**

Администратор SMS может удалить проигрыватель сетевых записей Cisco WebEx с помощью системной программы удаления SMS, выполнив приведенные ниже действия.

Процедура

Шаг **1** Используйте пакет установки SMS, созданный в Создание пакета из определения, на странице 101.

Шаг **2** Объявите системную программу удаления, чтобы удалить проигрыватель сетевых записей Cisco WebEx.
Проигрыватель сетевых записей Cisco WebEx будет автоматически удален на выбранных машинах.

Удаление проигрывателя сетевых записей **Cisco WebEx** с помощью системной программы удаления **SMS**

ГЛАВА 8

Управление лицензиями

О лицензиях

В этом разделе описывается метод лицензирования для указанной продукции.

Этот продукт предполагает лицензирование на основе пользователя, в соответствие с которым необходима покупка лицензии для каждого пользователя, желающего проводить совещания. Лицензии рассчитываются приведенным ниже образом.

- Если пользователь организовывает по крайней мере одно совещание в течение 30-дневного периода, он использует одну лицензию. При организации дополнительных совещаний в тот же 30-дневный период пользователь по-прежнему будет использовать одну лицензию, если только этот пользователь не будет проводить одновременные совещания.
- При проведении пользователем одновременных совещаний (в один день и в одно и то же время) система будет засчитывать дополнительную лицензию для каждого одновременного совещания, организованного пользователем в течение 30-дневного периода.
- Если пользователь не организовывает в течение 30-дневного периода ни одного совещания, лицензия не используется.

Примечание Известна проблема, вследствие которой плата за лицензию не взимается, если пользователь запрашивает исключительно телеконференцию совещания (но не веб-составляющую). В будущих версиях продукта организация как телеконференции, так и веб-составляющей совещания (а также обеих составляющих) приведет к использованию лицензии.

Примечание Система засчитывает использование лицензии для каждого пользователя каждые 30 дней, как указано в таблице ниже.

Сценарий	Дата совещания	Время начала совещания	Одноврем. совещания	Колич. исп. лицензий за **30**-дневн. Период
Пользователь А планирует совещание, однако не организовывает его.	1 января	9:00	Нет	0
Пользователь Б организовывает одно совещание.	2 января	9:00	Нет	1
Пользователь В организовывает два совещания в разное время.	3 января 4 января	9:00 10:00	Нет	1
Пользователь Г организовывает два совещания в одно время.	6 января 6 января	9:00 9:00	Да (2)	2
Пользователь Д организовывает два совещания в один день и в одно время и еще два одновременных совещания в другой день и в другое время в течение месяца.	6 января 6 января 10 января 10 января	9:00 9:00 16:00 16:00	Да (2)	2
Пользователь Е организовывает два совещания в один день и в одно время, но не посещает ни одно из них. Совещания состоялись.	7 января 7 января	9:00 9:00	Да (2)	2

Сценарий	Дата совещания	Время начала совещания	Одноврем. совещания	Колич. исп. лицензий за **30**-дневн. Период
Пользователь Ё организовывает совещание и передает право на его проведение другому участнику во время совещания. После чего пользователь организовывает второе совещание, которое проводится одновременно с первым.	8 января 8 января	9:00 9:00	Да (2)	2
Пользователь Ж организовывает совещание, однако все участники совещания присоединяются только к его телеконференции (не веб-составляющей) с выбранным параметром Подключиться раньше организатора.	9 января	9:00	Нет	0
Пользователь З организовывает два совещания в одно время, однако все участники совещания присоединяются только к их телеконференции (не веб-составляющей) с выбранным параметром Подключиться раньше организатора.	10 января 10 января	9:00 9:00	Нет	0

Сценарий	Дата совещания	Время начала совещания	Одноврем. совещания	Колич. исп. лицензий за **30**-дневн. Период
Пользователь И организовывает совещание и передает право на его проведение другому участнику во время совещания. После чего пользователь организовывает второе совещание, проводимое одновременно с первым, но все его участники присоединяются только к аудиоконференции (не веб-составляющей) с выбранным параметром Подключиться раньше организатора.	11 января 11 января	10:00 10:00	Нет	1

180-дневный бесплатный пробный период

После первого входа в программу и завершения следования подсказкам мастера первого использования начинается 180-дневный бесплатный пробный период. В течение пробного периода администраторы могут настраивать систему, а пользователи – планировать и организовывать совещания, а также принимать в них участие. Вверху страницы сайта Администрирования отображается баннер, указывающий на то, через сколько дней истечет бесплатный пробный период. За тридцать дней до окончания бесплатного пробного периода вы получите электронное письмо с предложением купить и установить лицензии на свою систему, прежде чем она будет отключена.

По истечении бесплатного пробного периода ваша система будет отключена. Вы сможете войти в систему, но не сможете использовать ее функции до тех пор, пока не приобретете необходимые лицензии. Дополнительную информацию об управлении лицензиями вы найдете в Руководстве по администрированию *Cisco WebEx Meetings Server*.

Получение лицензий

Обратитесь к торговому представителю Cisco для заказа лицензий для вашей системы. Когда вы свяжитесь со своим торговым представителем, вам необходимо будет уточнить требуемое количество лицензий. Вам понадобится приобрести по одной лицензии на каждого сотрудника вашей компании, который будет организовывать совещания.

Есть несколько способов определения нужного количества лицензий. Вы можете использовать панель отчетов для просмотра сведений об использовании, истории ресурсов и динамики совещаний, чтобы определить количество пользователей, организовывающих совещания и принимающих в них участие с помощью вашей системы. После использования продукта в течение нескольких месяцев вы можете использовать общие ежемесячные отчеты и специальные подробные отчеты – они помогут вам при определении необходимого количества лицензий. В ваших общих ежемесячных отчетах отображается статистика касательно пользования услугой и использования лицензий пользователей. В статистике, касающейся пользования услугой, отображаются показатели использования услуги вашими пользователями за предыдущие три месяца и ожидаемая динамика использования в течение следующих трех месяцев. В статистике, касающейся использования лицензий, отображается информация об их использовании за предыдущие три месяца и ожидаемая динамика использования в течение следующих трех месяцев.

После покупки лицензий у торгового представителя Cisco последний отправит вам электронное письмо с ключом авторизации продукта (PAK). Используйте инструмент управления лицензиями на сайте Администрирования, чтобы ввести ключ авторизации продукта и зарегистрировать свои лицензии. Дополнительную информацию об управлении лицензиями вы найдете в Руководстве по администрированию *Cisco WebEx Meetings Server*.

Превышение количества используемых лицензий

После приобретения и настройки лицензий в системе вам следует убедиться, что вы приобрели достаточное количество лицензий для всех организаторов в вашей системе. Каждые 30 дней система проверяет, достаточно ли лицензий у каждого организатора. Если количество организаторов в системе превышает количество лицензий, администратор получает электронное письмо с извещением о превышении количества используемых лицензий. Вам предоставляется шестимесячный кредитный период для приобретения дополнительных лицензий, чтобы их количество соответствовало количеству организаторов или превышало его. Если вы не приобретете достаточное количество лицензий в течение шести месяцев, ваша система будет отключена. О том, когда это произойдет, администратор узнает из соответствующего электронного письма.

Система проверяет и обновляет данные о количестве лицензий, отображенные на сайте Администрирования. Администратор аудита запускается раз в день (в 2:00), чтобы при необходимости обновить данные о превышении количества используемых лицензий. В конце каждого 30-дневного периода система проверяет частоту использования лицензий. Если количество организаторов становится ниже количества приобретенных лицензий, предупреждение о превышении количества используемых лицензий отменяется. Если количество организаторов по-прежнему превышает количество лицензий, каждый месяц вашему администратору будет отправляться новое электронное письмо с извещением о превышении количества используемых лицензий и датой потенциального отключения системы.

Если по истечении шести месяцев превышение количества используемых лицензий не прекратится, ваша система будет отключена, и администратор получит соответствующее электронное письмо с извещением. После отключения системы пользователи больше не

смогут планировать, организовывать совещания или просто принимать в них участие с ее помощью. Сайт Администрирования при этом будет работать в обычном режиме, и администратор сможет войти и добавить лицензии. После того как администратор добавит необходимые лицензии, пользователи снова смогут планировать, организовывать совещания или просто принимать в них участие.

Временные лицензии

Если в вашей системе настроены временные лицензии, их статус будет отображаться на баннере каждой страницы сайта Администрирования. На этом баннере содержится информация о настроенных лицензиях и сроке действия временных лицензий. По истечении срока действия временных лицензий система вернется к прежнему статусу.

Устаревшие лицензии

При обновлении системы вам также необходимо будет обновить лицензии. После обновления системы ваш администратор получит электронное письмо с извещением о том, что ему предоставлен шестимесячный кредитный период для обновления лицензий. Если вы не обновите лицензии в течение этого периода, система будет отключена. О том, когда это произойдет, администратор узнает из соответствующего электронного письма.

Система проверяет и обновляет данные о количестве лицензий, отображенные на сайте Администрирования. Администратор аудита запускается раз в день (в 2:00 д. п.) чтобы при необходимости обновить количество устаревших лицензий. В конце каждого 30-дневного периода система проверяет наличие обновленных лицензий с предыдущего периода. Если лицензии были обновлены, предупреждение о том, что они устарели, отменяется. Если лицензии еще не были обновлены, ваш администратор будет каждый месяц получать новое электронное письмо с извещением о том, что лицензии устарели и датой потенциального отключения системы.

Если по истечении шести месяцев вы все еще не обновили лицензии, ваша система будет отключена, и администратор получит соответствующее извещение в электронном письме. После отключения системы пользователи больше не смогут планировать, организовывать совещания или просто принимать в них участие с ее помощью. Сайт Администрирования при этом будет работать в обычном режиме, так что администратор сможет войти и обновить лицензии. После того как администратор обновит лицензии, пользователи снова смогут планировать, организовывать совещания или просто принимать в них участие.

Потеря соединения с Диспетчером соединений **Enterprise License Manager (ELM)**

При покупке лицензий вы используете встроенный инструмент ELM для ввода ключа авторизации продукта и регистрации лицензий. ELM выполняет синхронизацию каждые 12 часов для обновления статуса лицензии и последнего согласованного времени. Если проходит два дня без подключения к ELM, администратору отправляется электронное письмо с извещением о том, что синхронизация ELM с вашей системой невозможна. Вам предоставляется шестимесячный кредитный период для повторного подключения к ELM. Если вы не подключитесь к ELM в течение шестимесячного периода, система будет отключена. О том, когда это произойдет, администратор узнает из соответствующего электронного письма.

Каждый месяц вашему администратору будет отправляться новое электронное письмо с извещением о невозможности соединения с ELM и датой потенциального отключения системы. Если система подключается к ELM до истечения шестимесячного кредитного периода, соответствующее предупреждение отменяется.

Если по истечении шести месяцев подключение к ELM не будет выполнено, ваша система будет отключена, и администратор получит соответствующее электронное письмо с извещением. После отключения системы пользователи больше не смогут планировать, организовывать совещания или просто принимать в них участие с ее помощью. Сайт Администрирования при этом будет работать в обычном режиме, так что администратор сможет войти в систему, однако, система при этом должна будет подключиться к ELM для отмены текущего статуса и восстановления возможности планировать и организовывать совещания, а также принимать в них участие.

ГЛАВА 9

Конфигурация системы единого входа **SAML**

Обзор системы единого входа

Стандарты системы единого входа веб-федерации, например SAML 2.0, предполагают безопасные механизмы для передачи учетных данных и соответствующей информации между различными веб-сайтами, имеющими собственные системы авторизации и аутентификации. SAML 2.0 является открытым стандартом, разработанным техническим комитетом компании OASIS Security Services.

Протокол SAML 2.0 стал чрезвычайно успешным и становится все более популярным в сфере финансовых услуг, высшего образования, систем правления и других отраслевых сегментов. Поддержка протокола SAML 2.0 обеспечивается всеми крупными поставщиками сетевых систем управления. Управление служб общего назначения правительства США требует, чтобы все поставщики, участвующие в программе Федерации удостоверений электронной аутентификации США, осуществляли поддержку протокола SAML 2.0.

Веб-сайты, совместимые с SAML 2.0, обмениваются учетными данными пользователей посредством утверждений SAML. Утверждение SAML является документом XML, содержащим достоверные данные о предмете, включая, например, имя пользователя и права. Утверждения SAML, как правило, снабжаются цифровой подписью, удостоверяющей их подлинность.

Множество больших предприятий развернули в своих корпоративных интрасетях объединенную систему управления идентификацией и доступом (IAM), а также систему поставщика удостоверений (IdP), например Ping Identity, Ping Federate, CA SiteMinder, Open AM и Windows ADFS 2.0. Эти системы IAM и IdP управляют аутентификацией пользователя и требованиями системы единого входа для сотрудников и партнеров. Системы IAM и IdP используют протоколы SAML для взаимодействия с веб-сайтами партнеров вне их брандмауэров. Пользователи

могут использовать системы IAM и IdP для автоматической аутентификации своих пользователей в службах организации совещаний Cisco WebEx. Это повышает общую эффективность системы вследствие того, что пользователям не нужно запоминать имена пользователей и пароли, чтобы начинать совещания и присоединяться к ним на веб-сайтах Cisco WebEx.

Примечание WebEx Meetings Server поддерживает только системы SAML 2.0 IdP. Служба не поддерживает системы IdP более старых стандартов SAML 1.1 и WS-Federate в отличие от облачных служб организации совещаний Cisco WebEx, которые продолжают поддерживать протоколы SAML 1.1 и WS-Federate. Далее приведен список систем SAML 2.0 IdP, утвержденных для работы с Cisco WebEx Meetings Server.

- Microsoft ADFS 2.0 (бесплатная надстройка для Microsoft Active Directory 2010)
- Ping Identity Ping Federate 6.6.0.17
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP6

Поскольку SAML 2.0 является открытым стандартом, другие системы SAML 2.0 IdP также могут работать с Cisco WebEx Meetings Server. Однако другие системы SAML 2.0 IdP не были испытаны компанией Cisco. Поэтому приведение таких интеграций в действие входит в обязанности пользователя.

Преимущества системы единого входа

Система единого входа имеет приведенные ниже преимущества.

- Упрощенная аутентификация пользователей. Будучи программой, не требующей предварительной настройки, Cisco WebEx Meetings Server предполагает вход пользователей с помощью адресов электронной почты и их собственных паролей, созданных специально для системы Meetings Server. Пользователи самостоятельно выбирают пароли при активации учетных записей Meetings Server. Такой подход идеален для небольших и средних организаций, однако организации большего размера предпочитают использовать аутентификацию с помощью корпоративных учетных данных, то есть Active Directory, для обеспечения более высокого уровня безопасности. Этого можно достичь с помощью системы единого входа SAML 2.0.

  Примечание Одним из преимуществ системы единого входа в отношении безопасности является то, что корпоративный пароль после успешной аутентификации пользователя фактически никогда не отправляется и не хранится в Cisco WebEx Meetings Server.

- Упрощенное управление пользователями. Большие организации с непостоянными трудовыми ресурсами вследствие естественной убыли персонала предпочитают

автоматизировать процесс управления пользователями с помощью интеграции с WebEx Meetings Server. Это предполагает автоматизацию приведенного ниже.

- Создание учетных записей пользователей при приеме сотрудников в организацию.
- Обновления учетных записей при изменении ролей пользователей внутри организации.
- Деактивация учетных записей пользователей при увольнении сотрудников.

Эти действия могут выполняться автоматически путем настройки функций Автоматическое создание учетной записи и Автоматическое обновление учетной записи в разделе системы единого входа сайта Администрирования Cisco WebEx Meetings Server. Мы рекомендуем включить эти функции, если они также поддерживаются SAML IdP. Учетные записи пользователей автоматически создаются и обновляются "по запросу" при успешной аутентификации пользователей, исключая при этом необходимость создавать пользователей вручную с помощью сайта Администрирования Cisco WebEx. Таким же образом, пользователи больше не смогут входить в их учетные записи после выхода из организации, поскольку SAML 2.0 IdP блокирует их после удаления из базы данных пользователей SAML 2.0 IdP, которая, как правило, является прокси-сервером для основного корпоративного каталога.

Обзор настройки системы единого входа **SAML 2.0**

Важное примечание

Если вы или кто-либо в вашей организации не имеете опыта в использовании системы единого входа SAML 2.0, мы рекомендуем обратиться к квалифицированному партнеру Cisco AUC или представителю служб Cisco Advanced Services. Мы даем такие рекомендации, поскольку настройка системы единого входа SAML может быть достаточно сложной.

Просмотрите приведенные ниже общие инструкции для настройки системы единого входа SAML 2.0.

1. Убедитесь в том, что инфраструктура системы единого входа SAML 2.0 находится в соответствующем месте и интегрирована в корпоративный каталог. Это означает настройку SAML 2.0 IdP и веб-сайта аутентификации системы единого входа. Веб-сайт аутентификации является порталом, на котором пользователи вводят свои корпоративные учетные данные.
2. Убедитесь в том, что пользователи имеют доступ к веб-сайту аутентификации системы единого входа. Этот шаг важен, поскольку в составе процедуры входа Cisco WebEx Meetings Server перенаправляет пользователей на указанный веб-сайт аутенификации.

Примечание Если ваша система Cisco WebEx Meetings Server настроена на общий доступ, что позволяет пользователям входить и присоединяться к совещаниям из Интернета, чрезвычайно важно также обеспечить доступ к веб-сайту аутентификации системы единого входа из Интернета. Как правило, это означает развертывание SAML 2.0 IdP в DMZ. Без этого дополнительного шага пользователи при входе в Cisco WebEx Meetings Server из Интернета столкнуться с ошибкой "404: сайт не найден".

3 Подключите WebEx Meetings Server к SAML 2.0 IdP с помощью двух приведенных ниже способов.

- Нажмите Параметры > Безопасность > Система единого входа веб-федерации на сайте Администрирования Cisco WebEx Meetings Server.
- Следуйте инструкциям, приведенным в документации к SAML 2.0 IdP. Обратите внимание, что эти инструкции могут отличаться в зависимости от продавца или версии SAML 2.0 IdP. Это еще одна причина обратиться к квалифицированному партнеру Cisco AUC или представителю служб Cisco Advanced Services за помощью во внедрении этого продукта.

Примечание Не используйте инструкции в отношении настройки SAML 2.0 IdP, приведенные в сети разработчиков Cisco, поскольку эти инструкции предназначены для облачных служб проведения совещаний Cisco WebEx и потому не работают с Cisco WebEx Meetings Server надлежащим образом.

Отличия системы единого входа **SAML 2.0** для облачных служб **WebEx Meeting** и службы **WebEx Meetings Server**

В то время как облачные службы организации совещаний Cisco WebEx при создании учетных записей пользователей используют уникальные идентификаторы пользователей, Cisco WebEx Meetings Server использует для этого электронные адреса. Это приводит к указанным ниже последствиям для системы единого входа SAML 2.0.

- Для утверждения SAML обязательно иметь адрес электронной почты в поле "NameID". Без этого происходит ошибка аутентификации пользователя и создания учетной записи вследствие того, что Cisco WebEx Meetings Server не разрешает создание учетных записей пользователей без соответствующих электронных адресов.
- Облачные службы организации совещаний Cisco WebEx разрешают удаление домена электронной почты, например "@cisco.com", из UPN (имя участника-пользователя), когда функция автоматического создания учетных записей включена. Это приводит к созданию учетной записи пользователя, похожей на идентификатор пользователя. Поскольку WebEx Meetings Server для создания учетных записей пользователей использует полный электронный адрес, вы не можете удалить домен электронной почты из UPN.

Практически, вы можете сначала развернуть Cisco WebEx Meetings Server без системы единого входа SAML 2.0 и включить ее позднее. Это приводит к определенным последствиям в отношении аутентификации пользователей, автоматического создания учетных записей и их автоматического обновления.

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
Вы не включили систему единого входа. В системе были созданы учетные записи пользователя.	Пользователи выполняют вход с помощью их электронных адресов и паролей.	Н/Д	Н/Д	Н/Д	Н/Д

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
Затем вы включаете систему единого входа. Пользователи с существ. учетными записями входят на свой сайт WebEx, в Инструменты повышения произв. WebEx или приложение Cisco WebEx Meetings с их мобильных устройств.	Пользователи перенапр. на веб-сайт аутентиф. SAML 2.0 IdP, на котором им необходимо выполнить вход с помощью их корпоративных учетных данных, а не собственных электронных адресов и паролей. Пользователи успешно входят на сайт, поскольку распознаются системой SAML 2.0 IdP как действ. пользователи. Не будучи действ. польз., они получат сообщение от системы SAML 2.0 IdP о том, что они не могут использовать WebEx Meetings Server или что они являются недействительными.	Н/Д	Н/Д	Н/Д	Н/Д

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
Система единого входа включена. Пользователи не имеют существующих учетных записей в системе.	Совпадает с предыдущим сценарием.	Учетные записи пользователей в Cisco WebEx Meetings Server создаются "по запросу" после их входа. Необходимое условие: утверждение SAML в поле "NameID" содержит действ. электронный адрес.	Пользователи не имеют существующих учетных записей в системе. Они смогут войти, но не смогут использовать Cisco WebEx Meetings Server. Самым простым способом решить эту ситуацию является приведенное ниже. • Оставить функцию AAC вкл. • Перед входом польз. вручную создать учетные записи польз. с помощью функций "Импорт файла CSV" или "Создать польз." на сайте Админ. Cisco WebEx.	Н/Д	Н/Д

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
Система единого входа включена. Пользователи, которые уже выполняли вход в систему единого входа, входят повторно.	Совпадает со вторым сценарием.	Н/Д	Н/Д	Существующие учетные записи пользователей автоматически обновляются согласно всем изменениям учетных данных пользователя (как правило, имя или фамилия), пока данные в поле "NameID" неизменны.	Н/Д

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
Следующим шагом выключите систему единого входа. Это необычный сценарий, поскольку заказчики, как правило, оставляют систему единого входа включенной. Пользователи, которые уже выполняли вход в систему единого входа, входят повторно.		Н/Д	Н/Д	Н/Д	Н/Д

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
	Когда пользователи вводят свои корпор. учетные данные, они не могут войти, поскольку WebEx Meetings Server ожидает от них указание электронных адресов и собственных паролей. В таком случае сообщите пользователям о переустановке собственных паролей в учетных записях WebEx и дайте им достаточно времени до выключения системы единого входа. После переустановки паролей пользователи смогут входить в систему с помощью				

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
	своих электронных адресов и собственных паролей.				

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
Особый случай. Пользователь также является системным админ. Сценарий А. Пользователь входит на сайт WebEx. Сценарий Б. Пользователь входит на сайт Админ. Cisco WebEx.		Сценарий А. Результат соответствует представленному в предыдущем сценарии. Сценарий Б. Н/Д	Сценарий А. Результат соответствует представленному в предыдущем сценарии. Сценарий Б. Н/Д	Сценарий А. Результат соответствует представленному в предыдущем сценарии. Сценарий Б. Н/Д	Сценарий А. Результат соответствует представленному в предыдущем сценарии. Сценарий Б. Н/Д

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
	Сценарий А. Результат соответствует представл. в предыдущем сценарии. Сценарий Б. В отличие от входа на сайт WebEx при входе на сайт Админ. Cisco WebEx пользователю всегда необходимо вводить электронный адрес и собственный пароль. Другими словами, система единого входа не действует при входе на сайт Админ. Cisco WebEx. Это мера безопасности, предпол. продуктом, для гарантир. входа системных админ. на сайт Админ. Cisco WebEx. Если же сайт Админ. Cisco WebEx также поддерживает				

Сценарий	Процесс аутентиф. пользователя	Автоматич. создание учетной записи **(AAC)** включено	**AAC** выключено	Автоматич. обновление учетной записи **(AAC)** включено	**AAU** выключено
	систему единого входа, сбои в работе SAML 2.0 IdP и разрыв сетевого соединения между Cisco WebEx Meetings Server и SAML 2.0 IdP могут привести к тому, что системные админ. больше не смогут входить в продукт и управлять им. Поэтому система единого входа не поддерживается сайтом Админ. Cisco WebEx.				

ГЛАВА 10

Управление сетью

Требования к управлению сетью

В дополнение к функциям мониторинга, доступным на инструментальной панели, Cisco WebEx Meetings Server поддерживает Cisco Unified Operations Manager (CUOM) для отслеживания работы системы, включая отслеживание нагрузки, проверку работоспособности и отчетность об ошибках.

Примечание Cisco WebEx Meetings Server не поддерживает конфигурацию CUOM и функции управления.

На каждой виртуальной машине в вашей системе работает агент SNMP. Каждая виртуальная машина, таким образом, отображается в CUOM. Агент SNMP поддерживает протокол SNMPv3, включая механизмы аутентификации и шифрования в SNMPv3.

Каждый агент SNMP на данный момент поддерживает приведенные ниже стандартные форматы MIB.

- MIB-II (RFC-1213)
- SYSAPPL MIB (RFC-2287)
- SNMPv2-SMI
- SNMPv2-CONF
- SNMPv2-TC
- INET-ADDRESS-MIB
- Размещение ресурсов, MIB (RFC-2780)
- SNMP-FRAMEWORK-MIB
- Cisco Discovery Protocol (CDP) MIB
- CISCO-SMI

Примечание Назначение CUOM можно настроить на сайте Администрирования. Для получения дополнительной информации см. раздел "Настройка вашей системы" в Руководстве по администрированию.

Кроме того, каждая виртуальная машина поддерживает один или несколько форматов MIB для приложений.

Далее приведен список поддерживаемых частных форматов MIB.

- CISCO-WBX-COMMON-MIB
  - CANA (Cisco Assigned Numbers Authority) OID 796 – стандартный MIB, используемый для всех зарегистрированных компонентов сервера, запущенных на каждой виртуальной машине.
- CISCO-WBX-DATA-MIB
  - CANA (Cisco Assigned Numbers Authority) OID 795 – MIB для серверов с общим доступом в сети.
- CISCO-WBX-MEDIA-MIB
  - CANA (Cisco Assigned Numbers Authority) OID 797 – MIB для видео и серверов приложения для голосового соединения с помощью компьютера.
- CISCO-WBX-SSLGW-MIB
  - CANA (Cisco Assigned Numbers Authority) OID 794 – MIB для шлюза SSL.
- CISCO-WBX-TELEPHONY-MIB
  - CANA (Cisco Assigned Numbers Authority) OID 799 – MIB для сервера телефонии, соединяющий службы внешней голосовой телефонии и приложение Cisco WebEx.
- CISCO-WBX-TELSVR-MIB
  - CANA (Cisco Assigned Numbers Authority) OID 788 – MIB для сервера сетевых записей.

Среди приведенных выше частных форматов MIB CISCO-WBX-COMMON-MIB также предоставляет всю необходимую информацию, поддерживаемую для каждой виртуальной машины в отношении элементов ниже.

- Использование системных ресурсов
- Общая информация о сервере
- Информация о менеджере процессов
- Атрибуты процессов Daemon
- Ресурсы уведомлений

Далее приведены примеры некоторых объектов MIB из CISCO-WBX-COMMON-MIB.

- Общая информация о сервере
  - cwCommServIndex
  - cwCommServType
  - cwCommServID
  - cwCommServIPAddrType
  - cwCommServIPAddr
  - cwCommServCmdLine
  - cwCommServStatus
  - cwCommServStartTime
  - cwCommServErrorMsg
  - cwCommServVersion
  - cwCommServAction
  - cwCommServMEMUsed
  - cwCommServCPUUsage
- Поддерживаемые события для уведомлений
  - cwCommSystemResourceUsageNormalEvent
  - cwCommSystemResourceUsageMinorEvent
  - cwCommSystemResourceUsageMajorEvent
  - cwCommCPUUsageNormalEvent
  - cwCommCPUUsageMinorEvent
  - cwCommCPUUsageMajorEvent
  - cwCommNodeMgrUpEvent
  - cwCommNodeMgrDownEvent
  - cwCommWBXDScriptStartErrorEvent
  - cwCommDaemonUpStatusEvent
  - cwCommDaemonDownStatusEvent
  - cwCommServMEMUsageNormalEvent
  - cwCommServMEMUsageExceededEvent
  - cwCommServCPUUsageNormalEvent
  - cwCommServCPUUsageExceededEvent

ГЛАВА 11

Записи совещаний

Записи совещаний занимают память на вашем сервере хранения. В этом разделе описываются пороговые значения, сигналы тревоги сервера хранения, а также объем памяти, занимаемый записями совещаний на сервере хранения, и порядок удаления старых записей.

О записях совещаний

Вы можете настроить сервер хранилища любой емкости. Количество записей, которые можно хранить, зависит от настроенного объема доступного места для хранения. Если для вашей организации необходимо хранить записи более чем за шесть месяцев, вы можете периодически архивировать их с помощью других виртуальных средств.

Для поддержания достаточного количества памяти ваша система выполняет две описанные ниже задачи.

- После шести месяцев она удаляет записи, отмеченные для удаления вашими пользователями.
- Если за трехмесячный период объем памяти, занимаемый вашими записями, превышает определенный порог, отмеченные для удаления записи удаляются ранее, чем через шесть месяцев.

Если пользователь удаляет запись, она становится недоступной для интерфейса пользователя, однако, сохраняется в памяти в течение шести месяцев. Таким образом, у вас остается доступ к серверу хранения, благодаря которому вы можете копировать, делать резервные копии или использовать файлы записей в течение шести месяцев после того, как они были отмечены пользователем для удаления.

Каждое совещание занимает приблизительно 50–100 МБ памяти, поэтому, учитывая то, что объем памяти системы составляет 1 ТБ, она рассчитана на хранение записей за шесть месяцев при стандартном использовании. В любом случае, если сохраненные в вашей системе записи занимают более 75 процентов памяти за период в три месяца, система автоматически удаляет первые 10 файлов, отмеченных пользователем для удаления.

Например, если пользователь удалил два файла, пять файлов на следующий день и девять файлов через день, и объем памяти при этом превысил предел 75 % после 3 месяцев использования, система в соответствующем порядке удалит сначала первые два файла, затем пять файлов, удаленных на следующий день, а потом – первые три файла, удаленные через день.