LANDesk® System Manager 8.7

Руководство по установке и развертыванию

LANDesk®

Содержание

Введение **1**
Содержание **3**
Обзор **4**
Что нового в данной версии 4
Основные сведения о продукте 5
Стратегии установки и развертывания 7
Обзор установки и развертывания 8
Приступая к работе 9
Этап 1. Дизайн домена управления **23**
Сбор информации о сети 23
Системные требования 25
Этап 2. Установка главного сервера **33**
Установка главного сервера 33
Активизация главного сервера 34
Развертывание на устройствах Windows 36
Развертывание на устройствах Linux 38
Этап 3. Поэтапное развертывание **41**
Стратегия поэтапного развертывания 41
Контрольный список для конфигурирования устройств 41
Развертывание на устройствах Windows 44
Развертывание устройств из командной строки 46
Понятие архитектуры конфигурации агентов 46
Удаление главного сервера **50**
Удаление агентов продуктов с устройств 50
Удаление главного сервера 51
Поддержка **53**

Обзор

Это руководство также проведет вас через процесс установки и развертывания продукта LANDesk® System Manager, который поможет снизить полную стоимость владения, упрощая управление компьютером, и предлагает решение распространенных проблем при работе с компьютером.

В данном обзоре рассматриваются следующие темы:

- Что нового в данной версии
- Основные сведения о продукте (включая терминологию)
- Стратегии установки и развертывания
- Обзор установки и развертывания

Что нового в данной версии

По мере роста компьютерной промышленности компьютерные системы становятся все более сложными и трудными для управления. Время, которое тратится на обслуживание и исправление компьютера на протяжении срока его эксплуатации, может значительно увеличить полную стоимость владения по сравнению с его ценой при приобретении. LANDesk® System Manager поможет снизить полную стоимость владения, упрощая управление компьютером и устранение распространенных проблем в работе компьютера.

- **Обзор инвентаризации системы.**System Manager предоставляет полную информацию о конфигурации оборудования и программного обеспечения компьютера.
- **Наблюдение за состоянием компьютера.**System Manager выдает соответствующий отчет, когда компьютер находится в предупредительном или критическом состоянии, сообщая информацию о таких элементах, как температура, напряжение, свободная память и дисковое пространство.
- **Получение предупреждений о событиях системы.**System Manager может использовать различные методы предупреждения для уведомления о проблемах.
- **Наблюдение производительности в режиме реального времени или за прошедшие периоды времени.**System Manager позволяет вести наблюдение за производительностью различных объектов системы, таких как дисководы, процессоры, память и службы. Можно задать действия предупреждений, активизирующие уведомление в том случае, если указанный датчик превышает верхнее или нижнее предельные значения предварительно определенного количества событий.
- **Наблюдение за текущими процессами и службами.**System Manager позволяет просматривать текущие службы и их состояние или задавать действия предупреждений для уведомления об изменениях в состоянии служб.
- **Удаленное выключение, включение и перезагрузка компьютера.**System Manager позволяет осуществлять удаленное управление питанием с консоли администратора для поддерживающих его систем.
- **Запланированные задачи.** Просмотр или перепланирование из единой точки всех операций развертывания агентов, ,

- **Расширенная поддержка ОС.** Управление всеми устройствами в гетерогенной среде с единой консоли. Поддерживаются следующие операционные системы: Windows 2000, 2003 и XP Professional, Red Hat Linux, SUSE Linux, HP-UX, AIX. См. Этап 1. Требования к системе для получения дополнительной информации.
- **Поддержка Intel* AMT и интерфейса Intelligent Platform Management Interface (IPMI).**System Manager поддерживает компоненты аппаратного управления, обеспечивающие возможность удаленного управления сетевыми устройствами в любом состоянии системы через внеполосное (OOB) взаимодействие. Если устройство подключено к корпоративной сети и находится в состоянии ожидания, можно получить доступ к инвентаризации, просмотреть информацию об удаленной диагностике и выполнить удаленную перезагрузку системы.
- **Поддержка blade-серверов.** Поддержка blade-серверов и модулей управления корпусами blade-серверов, включая функции как управления, так и инвентаризации.
- **Инструментальное средство для создания сценариев.** Можно планировать и выполнять специальные задачи на устройствах
- **Планировщик задач.** Единая схема базы данных с улучшенной целостностью данных и масштабируемостью позволяет получить доступ к обширной информации об управляемых устройствах (включая полную интеграцию с Management Suite). Частью этой единой схемы является планировщик задач. Теперь в общем окне можно просмотреть все задачи (поиск , конфигурация агентов, . Из этого окна можно осуществлять перепланирование, изменение или повторение расписания.
- **Ролевое администрирование.** Настройка доступа пользователей к утилитам и сетевым устройствам на основании административной роли пользователя в организации. Вместе с административной ролью назначается и область действия, определяющая устройства, которые пользователь может просматривать и которыми он может управлять.
- **Обнаружение неуправляемых устройств.** Обнаружение устройств в сети выполняется различными способами. Продукт идентифицирует серверы, работающие под управлением Windows или Linux, blade-серверы и корпусы blade-серверов, серверы с поддержкой IPMI, серверы с поддержкой Intel AMT, а также прочие сетевые устройства. Планируйте обнаружение устройств таким образом, чтобы регулярно получать сведения о новых устройствах. Можно также создавать отчеты по неуправляемым устройствам в сети.
- **Улучшенная защита.** Модель системы защиты с поддержкой сертификатов позволяет устройствам взаимодействовать только с разрешенными главными серверами и консолями.
- **Распространение ПО.** Автоматизация процесса установки приложений программного обеспечения или распространения файлов в устройства.
- **Отчеты.** Для планирования и стратегического анализа доступны предварительно определенные служебные отчеты.
- **Поддержка запланированных задач.** Обеспечивает множественные входы в систему для аутентификации со службой планировщика при выполнении задач в устройствах, не имеющих агентов. Это особенно полезно для управления устройствами в нескольких доменах Windows.

Основные сведения о продукте

System Manager осуществляет управление устройствами, в которых работают несколько различных операционных системам, включая Windows 2000 Pro SP4, Windows XP Pro SP1, серверы Windows* 2000/2003, серверы Red Hat Enterprise Linux v3, серверы SUSE Linux 9,

серверы HP-UX и AIX, и обеспечивает общий интерфейс для управления устройствами этих сетевых операционных систем. Также может работать с другими продуктами LANDesk, например, LANDesk® Management Suite и LANDesk® Server Manager.

Терминология продукта

- **Главный сервер.** Центр домена управления. Все ключевые файлы и службы продукта находятся в главном сервере. В домене управления может быть только один главный сервер. Главный сервер может быть новым сервером или сервером с измененной специализацией.
- **Консоль.** Консоль в виде браузера представляет собой основной интерфейс продукта.
- База данных главного сервера.Продукт создает на главном сервере базу данных MSDE для хранения данных управления.
- **Управляемые устройства.** Устройства в сети, в которых установлены агенты продукта. Понятие "устройства" включает настольные компьютеры, серверы, портативные или переносные компьютеры, корпусы blade-серверов и т.д. Главный сервер может осуществлять управление тысячами устройств
- **Общие.** Элементы (например, группы, пакеты распределения или задачи), видимые для всех пользователей. Когда пользователь меняет элемент списка "Общие", изменение остается в этом списке. Общие группы создаются пользователями с административными правами.
- **Закрытые или пользовательские.** Элементы, созданные текущим, находящимся в системе пользователем. Они невидимы для других пользователей. Закрытые или пользовательские элементы отображаются в списках **Мои методы доставки**, **Мои пакеты** и **Мои задачи**. Пользователи, имеющие права администратора, могут видеть закрытые и пользовательские пакеты и задачи.
- **Общие.** Элементы, видимые для всех пользователей. Если пользователь имеет права на общий элемент (после его изменения), элемент разделяется на две части: общую часть и пользовательскую, сохраненную в папке пользователя. Пользовательская часть более недоступна для других пользователей. Пользователь может пометить любую свою задачу в качестве общей, после чего она станет доступна для других пользователей. Как только пользователь отменит пометку параметра свойств "Общие", задача станет доступна только в группе пользовательских задач.

Как продукт подходит к моей сети?

Этот продукт использует инфраструктуру существующей сети для установления соединений с управляемыми устройствами. Управление существующими устройствами значительно упрощается как для небольшой сети, так и для среды крупного предприятия.

Использование System Manager с Management Suite или Server Manager

Если при наличии системы System Manager требуется использовать Management Suite или Server Manager, необходимо воспользоваться утилитой активизации главного сервера, чтобы предоставить действующее имя пользователя и пароль для продукта, вместе с которым предполагается использовать System Manager. Установка System Manager /

Management Suite предоставляет возможность использования трех консолей: консоль Windows 32 и Web-консоль Management Suite, а также Web-консоль System Manager. Консоль Server Manager включает три навигационных элемента (предупреждения, мониторинг и журналы), содержащие функциональные возможности, отсутствующие в двух консолях Management Suite.

При развертывании Management Suite в процессе установки Management Suite в управляемых устройствах удаляется агент System Manager, и наоборот. Во время запуска Management Suite с System Manager функция конфигурации Management Suite включает параметры мониторинга.

Установка System Manager с уже установленным программным обеспечением Management Suite или Server Manager

Если в главном сервере уже установлен Management Suite или Server Manager и требуется добавить System Manager, используется та же процедура установки, которая выполнялась при первоначальной установке Management Suite или Server Manager.

1. Откройте autorun.exe.
2. Нажмите **Установить сейчас**.
3. Выберите язык и нажмите **OK**.
4. Отобразится экран приветствия. Нажмите **Далее**.
5. Выберите **Изменить** (если необходимо) и нажмите **Далее.**
6. Нажмите LANDesk® Server Manager, а затем **Далее**.
7. Выполните инструкции на экране мастера.

Требования к системе главного сервера

При выборе сервера, который будет использоваться в качестве главного, просмотрите требования к системе и убедитесь, что выбранный сервер соответствует или превосходит требования, перечисленные в разделе "Этап 1. Требования к системе". Средство проверки необходимых требований осуществляет это автоматически.

Настоятельно рекомендуется использовать выделенный главный сервер
Из-за трафика, проходящего через главный сервер при управлении доменом, настоятельно рекомендуется, чтобы каждый главный сервер были специально выделены для продукта.

В случае установки в тот же сервер других продуктов могут возникать краткосрочные или долгосрочные проблемы с ресурсами.

Не устанавливайте компоненты главного сервера в главный контроллер домена, резервный контроллер домена или контроллер Active Directory.

Стратегии установки и развертывания

Когда установка выполняется с использованием автозагрузки с носителя продукта, программа установки автоматически проверяет соответствие главного сервера указанным

требованиям. Для установки и развертывания системы в гетерогенной сети необходима хорошо продуманная методика и осмотрительное планирование *перед* выполнением программы установки. В данном руководстве содержатся стратегии установки продукта. Перед развертыванием продукта необходимо кратко сформулировать требования к управлению.

Анализ стратегии развертывания

Развертывание – это процесс распределения возможностей управления в серверы, которые следует включить в домен. В данном руководстве развертывание рассматривается по "этапам".

Стратегия поэтапного развертывания предлагает структурированный подход к активизации управления в устройствах. Такой подход основан на двух простых принципах:

- Во-первых, развертывание следует осуществлять постепенно, начиная с компонентов продукта, оказывающих минимальное влияние на существующую сеть, до компонентов, оказывающих наибольшее влияние.
- Во-вторых, развертывание продукта следует выполнять в несколько хорошо продуманных этапов вместо того, чтобы разворачивать все службы одновременно, что может усложнить поиск и устранение возможных проблем.

Данное руководство имеет логическую структуру, призванную оказать помощь в развертывании продукта. Начните с первой главы: "Этап 1. Проектирование домена управления", приведенной позднее в данном руководстве. Затем необходимо последовательно пройти каждый этап.

Обзор установки и развертывания

В данном руководстве задачи установки и развертывания сгруппированы в перечисленные ниже этапы. Каждому этапу соответствует определенный раздел руководства, описывающий эту часть процесса установки. Глава "" помогает быстро начать использование продукта, выполнив настройку служб, запуск консоли, обнаружение устройств, перемещение устройств в список "Мои устройства" и конфигурирование управляемых устройств для действий. Информация в этой главе изложена кратко, но более подробную информацию по тем или иным вопросам можно найти в остальных главах книги. Некоторые процедуры, описанные в данном руководстве, повторяются в главе "Приступая к работе".

Этап 1

Во время первого этапа процесса установки вы создаете проект домена управления, выполняя следующие задачи:

- Сбор информации о сети
- Проверка соответствия сети требованиям к системе

Более подробную информацию см. в главе "Этап 1. Проектирование домена управления", приведенной позднее в данном руководстве.

Этап 2

Во время второго этапа вы осуществляете установку продукта, выполняя следующие задачи:

- Установка главного сервера

Более подробную информацию см. в главе "Этап 2. Установка главного сервера и консоли", приведенной позднее в данном руководстве.

Этап 3

Во время третьего этапа процесса установки осуществляется обнаружение устройств в сети и развертывание агентов продукта. Вы можете отправлять агенты с консоли или извлекать из совместно используемого ресурса сервера.

Более подробную информацию см. в главе "Этап 3. Развертывание агентов на устройствах", приведенной позднее в данном руководстве.

Приступая к работе

- Обзор
- Запуск программы установки
- Активизация главного сервера
- Добавление пользователей
- Настройка служб и идентификационной информации
- Запуск консоли
- Обнаружение устройств
- Планирование и запуск обнаружения
- Просмотр обнаруженных устройств
- Перемещение устройств в список "Мои устройства"
- Группирование устройств для определенных действий
- Настройка устройств для управления
- Что дальше?

Обзор

Добро пожаловать в LANDesk® System Manager, отдельное приложение управления устройствами, с помощью которого можно использовать время с максимальной эффективностью, быстро и легко управляя устройствами, и, таким образом, экономить время и деньги вашей организации и ваши собственные. System Manager позволяет управлять вашими устройствами в определенном местоположении, группировать их для различных действий (например, для выключения/включения питания, поиска уязвимых мест или настройки предупреждений), дистанционно выявлять и устранять проблемы, поддерживать безопасность сети, а также устанавливать последние обновления на устройствах.

Целью данного руководства является помощь пользователю в быстром запуске System Manager путем настройки служб, запуска консоли, обнаружения устройств, переноса устройств в список "Мои устройства" и настройки управляемых устройств для выполнения действий.

System Manager является Web-приложением, доступ к которому осуществляется посредством браузера, позволяющим управлять серверами с удаленной рабочей станции. Продукт работает как большинство привычных Web-приложений, однако для удобства использования он содержит несколько дополнительных элементов управления Windows. Например, при помещении курсора мыши на элемент управления можно его щелкнуть дважды или щелкнуть правой кнопкой мыши (как в любых других приложениях Windows). Например, в списке Мои устройства можно дважды щелкнуть имя устройства, чтобы получить доступ к информации о нем, или щелкнуть устройство правой кнопкой мыши для просмотра доступных действий.

Приведенные ниже инструкции помогут запустить System Manager, обнаружить устройства в сети, выбрать серверы для переноса в список **Мои устройства**, развернуть агенты и назначить устройства для выполнения различных задач.

Запуск программы установки

Во время установки на странице автозапуска выберите LANDesk® System Manager. Конкретные инструкции по установке можно найти в главе "Этап 2" "Руководства по установке и развертыванию".

После установки System Manager все готово для запуска этого продукта. В приведенных ниже разделах описывается выполнение нескольких обязательных задач: это запуск утилиты активации главного сервера, настройка служб, обнаружение компьютеров, определение управляемых устройств путем их переноса в список "Мои устройства", группирование устройств, добавление пользователей и развертывание агентов. После завершения данных заданий можно начать изучение того, как набор надежных средств System Manager поможет вам в управлении устройствами.

Активизация главного сервера

Продукт невозможно запустить без активизации главного сервера.

Утилита активизации главного сервера используется для следующих целей:

- Первоначальная активизация нового главного сервера System Manager.
- Обновление существующего главного сервера System Manager.

Каждый главный сервер должен иметь уникальный сертификат авторизации.

Данная утилита запускается автоматически при первой перезагрузке.

Убедитесь, что главный сервер подключен к Интернету, и выполните следующие действия.

1. Нажмите **Пуск | Все программы | Активизация главного сервера**.
2. Имя пользователя и пароль заполнены.
3. Нажмите **Активировать**.

Главный сервер связывается с сервером лицензирования ПО посредством HTTP. При использовании прокси-сервера выберите вкладку Прокси и введите соответствующую информацию. Если главный сервер подключен к Интернету, взаимодействие с сервером лицензирования устанавливается автоматически и в дальнейшем не требует от вас какого-либо вмешательства. Если главный сервер не подключен к Интернету, при перезагрузке выберите "Закрыть" и отправьте файл авторизации по электронной почте по адресу: licensing@landesk.com.

Периодически в главном сервере запускается проверка количества узлов, информация о которой записывается в файл "\Program Files\LANDesk\Authorization Files\LANDesk.usage". Этот файл периодически посылается серверу лицензирования ПО LANDesk. Этот файл генерируется в формате XML и отправляется в зашифрованном виде с электронной подписью. Любые изменения, сделанные в этом файле вручную, сделают его содержимое недействительным, и о последующем использовании будет послан отчет на сервер лицензирования ПО.

- Утилита активизации главного сервера не запускает автоматически коммутируемое соединение с Интернетом, однако, если вручную запустить коммутируемое соединение и утилиту активизации, утилита сможет использовать данное соединение для отчета об использовании данных.
- Главный сервер можно также активировать по электронной почте. Отправьте файл с расширением .TXT, расположенный в каталоге Program Files\LANDesk\Authorization, по адресу licensing@landesk.com. Специалисты службы поддержки LANDesk ответят по электронной почте и пришлют файл и инструкции по его копированию на главный сервер для завершения процесса активизации.

Добавление пользователей

Пользователями System Manager являются пользователи, которые могут входить на консоль и выполнять определенные задачи для определенных устройств в сети. Вы можете управлять пользователями с помощью средства ролевого администрирования. Ролевое администрирование позволяет присваивать пользователям продукта определенные административные роли, основанные на их правах и области действия. Права определяют инструментальные средства и функции продукта для просмотра и использования пользователем. Область действия определяет набор устройств для просмотра и управления пользователем. Вы можете создавать различных пользователей и устанавливать их права и область действия в соответствии с вашими требованиями по управлению. Например, вы можете создать пользователя, выполняющего роль справочного стола, путем присвоения данному пользователю прав, необходимых для этой роли. Дополнительную информацию см. в главе "Ролевое администрирование" Руководства пользователя System Manager.

После установки продукта автоматически создаются учетные записи для двух пользователей (см. ниже). Если необходимо добавить дополнительных пользователей, это можно сделать вручную. В действительности пользователи не создаются на консоли. Вместо этого, они появляются в группе "Пользователи" (в левой навигационной панели нажмите Пользователи) после их добавления в группу LANDesk Management Suite в пользовательской среде Windows NT на главном сервере. В группе "Пользователи" отображаются все пользователи, которые в данный момент включены в группу LANDesk Management Suite на главном сервере.

В группе "Пользователи" находятся два следующих пользователя по умолчанию. Первый пользователь - Администратор по умолчанию. Это административный пользователь, который зарегистрировался на сервере при установке продукта.

Другой пользователь по умолчанию - Пользователь шаблона по умолчанию. Данный пользователь имеет шаблон свойств пользователя (права и область), который используется для конфигурации новых пользователей при их добавлении в группу Management Suite. Другими словами, когда пользователь добавляется в эту группу в среде Windows NT, ему назначаются права и область, определенные в свойствах пользователя шаблона по умолчанию. Если у пользователя шаблона по умолчанию выбраны все права и области всех машин по умолчанию, любой новый пользователь, помещенный в группу LANDesk Management Suite, будет добавлен в группу "Пользователи" с правами на все инструментальные средства продукта и доступом ко всем устройствам.

Вы можете изменить параметры свойств для пользователя шаблона по умолчанию, выбрав его и нажав **Правка**. Например, если необходимо одновременно добавить большое количество пользователей, но не нужно наделять их правами для доступа ко всем инструментальным средствам и устройствам, сначала измените параметры пользователя шаблона по умолчанию, а затем уже добавьте пользователей в группу LANDesk Management Suite (инструкции см. ниже). Пользователь шаблона по умолчанию не может быть удален.

При добавлении пользователя в группу LANDesk Management Suite в Windows NT данный пользователь автоматически помещается в группу "Пользователи" в окне **Пользователи** с предоставлением тех же прав и области, которые установлены для пользователя шаблона по умолчанию. Будут отображены имя пользователя, область и права. Кроме того, в группах "Устройства пользователя", "Запросы пользователя", "Отчеты пользователя" и "Сценарии пользователя" создаются подгруппы нового пользователя, названные по уникальному идентификатору входа данного пользователя (обратите внимание, что группы пользователей сможет видеть ТОЛЬКО администратор).

И наоборот, при удалении пользователя из группы LANDesk Management Suite пользователь также удаляется из списка **Пользователи**. Учетная запись пользователя остается на главном сервере и может быть снова добавлена в группу LANDesk Management Suite в любое время. Кроме того, подгруппы пользователя сохраняются в группах "Устройства пользователя", "Запросы пользователя", "Отчеты пользователя" и "Сценарии пользователя", и вы можете восстановить пользователя без потери данных, а также скопировать эти данные другим пользователям.

Для обновления окна **Пользователи** на консоли System Manager нажмите **F5**. Для добавления группы пользователей или доменов в группу LANDesk Management Suite или создания учетной записи нового пользователя см. "Добавление пользователей продукта" в главе "Ролевое администрирование" *Руководства пользователя*System Manager.

Добавление группы пользователей или доменов в группу LANDesk Management Suite

1. Перейдите к утилите сервера **Администрирование | Управление компьютерами | Локальные пользователи и группы | Группы**.
2. Щелкните правой кнопкой мыши **Группа LANDesk Management Suite**, а затем выберите **Добавить в группу**.
3. Щелкните **Добавить**, а затем введите или выберите из списка пользователя (или пользователей).

4. Щелкните **Добавить**, а затем **OK**.

Примечание. Пользователей в группу LANDesk Management Suite можно также добавить, щелкнув правой кнопкой мыши учетную запись пользователя в списке **Пользователи**, выбрав **Свойства | Член группы**, а затем **Добавить** для выбора группы и добавления пользователя.

Если учетные записи пользователей еще не созданы на сервере, сначала необходимо их создать.

Создание новой учетной записи пользователя

1. Перейдите к утилите сервера **Администрирование | Управление компьютерами | Локальные пользователи и группы | Пользователи**.
2. Щелкните правой кнопкой мыши **Пользователи**, а затем **Новый пользователь**.
3. В диалоговом окне **Новый пользователь** введите имя и пароль.
4. Укажите параметры пароля.
5. Нажмите кнопку **Создать**. Диалоговое окно **Новый пользователь** остается открытым, так что можно создавать дополнительных пользователей.
6. Для выхода из диалогового окна нажмите **Закрыть**.

Добавьте пользователя в группу LANDesk Management Suite, чтобы он появился в группе Пользователи на консоли.

Настройка служб и идентификационной информации

Перед началом управления устройствами в сети необходимо предоставить System Manager необходимую идентификационную информацию об устройствах. Воспользуйтесь утилитой конфигурации служб на главном сервере (SVCCFG.EXE) для предоставления необходимой идентификационной информации для операционной системы, Intel* AMT и IPMI BMC. Кроме того, можно указать дополнительные параметры, например, параметры инвентаризации по умолчанию, параметры обслуживания очередей PXE и параметры базы данных LANDesk.

Утилита конфигурации служб используется для настройки следующих параметров.

- Имя базы данных, имя пользователя и пароль. (Настраиваются во время установки).
- Идентификационная информация для планирования заданий на управляемых устройствах. (Можно указать более одного набора идентификационной информации администратора).
- Идентификационная информация для настройки IPMI BMC. (Можно указать только один набор идентификационной информации BMC).
- Идентификационная информация для настройки устройств с поддержкой Intel AMT. (Можно указать только один набор идентификационной информации Intel AMT).
- Интервал сканирования программного обеспечения сервера, информация об обслуживании, дни сканирования инвентаризации и объем журнала регистрации.
- Обработка идентификатора дубликата устройства.
- Конфигурация планировщика, включая запланированные задания и интервалы между оценками запросов.
- Конфигурация специальных заданий, включая тайм-аут удаленного выполнения.

1. На главном сервере выберите Пуск | Все программы | LANDesk | Конфигурация служб LANDesk.
2. Выберите вкладку Планировщик.
3. Нажмите кнопку Смена имени.
4. Введите идентификационную информацию службы для использования на управляемых устройствах. Обычно это учетная запись администратора домена.
5. Нажмите кнопку Добавить. При необходимости добавьте дополнительную идентификационную информацию, если не все управляемые устройства поддерживают одинаковые учетные записи администраторов.
6. Нажмите Применить.
7. Если в вашей среде есть серверы с поддержкой IPMI, выберите вкладку **Пароль BMC**. В текстовом поле Пароль введите пароль, в поле Подтверждение пароля введите пароль еще раз и нажмите OK. (На всех управляемых серверах IPMI необходимо установить одинаковые имя пользователя и пароль BMC).
8. При наличии устройств с поддержкой Intel AMT выберите вкладку **Конфигурация Intel AMT**. В текстовом окне Имя пользователя введите текущее имя пользователя Intel AMT, а текущий пароль в текстовом окне Пароль. В текстовом окне Подтверждение пароля введите пароль еще раз и нажмите OK.
9. По желанию установите любые другие параметры, например, интервалы сканирования ПО.
10. Для сохранения изменений нажмите **OK**.

Дополнительную информацию см. в окне **Справка** на каждой вкладке служб конфигурации.

Запуск консоли

В System Manager включен полный спектр инструментальных средств, которые позволяют просматривать, настраивать, управлять и защищать устройства вашей сети. Консоль является точкой входа, с которой вы можете использовать эти инструментальные средства.

В верхней панели на консоли отображается сервер, в котором вы зарегистрированы, а также имя пользователя, использованное при входе. Список Мои устройства является главным окном консоли, а также отправной точкой для выполнения большинства функций. В левой панели отображаются доступные инструментальные средства. В правой панели консоли отображаются диалоговые окна и экраны, которые позволяют вам выполнять задания управления.

Удобство консоли заключается в том, что можно выполнять все ее функции в удаленном режиме (например, с вашей рабочей станции), тем самым, исключая необходимость посещений серверной комнаты или каждого управляемого устройства индивидуально для планового техобслуживания или устранения неполадок.

Консоль запускается одним из трех способов.

- На главном сервере выберите **Пуск | Все программы | LANDesk |** System Manager**.**
- В браузере на удаленной рабочей станции введите адрес URL http://coreserver/LDSM.

Обнаружение устройств

Используйте вкладку **Конфигурации обнаружения** для создания новых конфигураций обнаружения, правки и удаления существующих конфигураций, а также планирования конфигурации для обнаружения. Каждая конфигурация обнаружения состоит из подробного имени, диапазонов IP для сканирования и типа обнаружения.

Создав конфигурацию, используйте диалог **Планировать обнаружение** для настройки ее запуска.

1. В левой навигационной панели выберите **Обнаружение устройств**.
2. На вкладке **Конфигурации обнаружения** нажмите кнопку **Новая**.
3. Заполните поля, описанные ниже. После завершения нажмите кнопку **Добавить**, а затем **OK**.

Далее описываются компоненты диалогового окна **Конфигурация обнаружения**.

- **Имя конфигурации.** Введите имя данной конфигурации. Присвойте конфигурации имя, имеющее такой смысл, что вам было бы легко запомнить данную конфигурацию. Имя конфигурации может содержать до 255 символов, и не должно содержать следующие символы: **"**, **+**, **#**, **&** или **%**. При использовании данных символов имя конфигурации не отобразится.
- **Стандартное сканирование сети.** Поиск устройств путем отправки пакетов ICMP в диапазоне назначенных вами адресов IP. Данный поиск является самым основательным, но, в то же время, самым медленным. По умолчанию данный параметр использует NetBIOS для сбора информации об устройстве.

  Параметр сканирования сети также включает в себя параметр **Отпечатки IP**, с помощью которого при обнаружении устройств осуществляется попытка обнаружения типа ОС по полученным пакетам TCP. Параметр "Отпечатки IP" в некоторой степени замедляет обнаружение.

  В настройках сканирования сети также есть параметр **Использовать SNMP**, который можно использовать для конфигурации сканирования с использованием SNMP. Выберите **Конфигурация** для ввода информации конфигурации SNMP.

- **Обнаружение CBA LANDesk.** Поиск стандартного агента управления на устройствах (ранее известен как агент Common base [CBA] в Management Suite). Стандартный агент управления позволяет главному серверу обнаруживать клиентов сети и взаимодействовать с ними. Данный параметр обнаруживает устройства с установленными на них агентами продукта. Маршрутизаторы блокируют стандартный агент управления и трафик PDS2. Для выполнения стандартного обнаружения CBA по нескольким подсетям маршрутизатор должен быть сконфигурирован так, чтобы позволять управляемое широковещание по нескольким подсетям.

  В параметр "Обнаружение CBA" также включен параметр **Обнаружение PDS2 LANDesk**, который осуществляет поиск службы обнаружения LANDesk Ping Discovery Service (PDS2) на устройствах. Продукты ПО LANDesk, такие как LANDesk® System Manager, Server Manager и LANDesk Client Manager используют агент PDS2. Выберите этот параметр, если в вашей сети имеются устройства с данными установленными продуктами. Обнаружение CBA не поддерживается в машинах Linux, однако, если вы выберите PDS2, машины Linux с установленным в них агентом могут быть обнаружены.
- **IPMI.** Поиск серверов с поддержкой IPMI. IPMI - спецификация, разработанная компаниями Intel,*, H-P*, NEC* и Dell* для определения интерфейса сообщений и систем управляемого оборудования. IPMI включает в себя функции мониторинга и восстановления. Доступ к данным функциям обеспечивается вне зависимости от того, включено ли устройство или нет, а также в каком состоянии находится операционная система. Обратите внимание, что, если контроллер BMC не сконфигурирован, он не будет отвечать на эхо-запросы ASF, использующиеся продуктом для обнаружения IPMI. Это означает, что вам нужно будет искать его как обычный компьютер. При запуске клиента ServerConfig просканирует используемую систему, определит наличие IPMI и сконфигурирует BMC.
- **Корпус сервера.** Поиск модулей управления корпуса блейд-сервера (CMM). Блейд-серверы в корпусе сервера обнаруживаются как обычные серверы.
- **Intel* AMT.** Поиск устройств с поддержкой Intel Active Management Technology.
- **Начальный IP.** Введите начальный адрес IP для диапазона адресов, которые необходимо просканировать.
- **Конечный IP.** Введите конечный адрес IP для диапазона адресов, которые необходимо просканировать.
- **Маска подсети.** Введите маску подсети для диапазона адресов IP, которые необходимо просканировать.
- **Добавить.** Добавление диапазонов адресов IP к рабочей очереди внизу диалогового окна.
- **Очистить.** Очистка полей с диапазонами адресов IP.
- **Правка.** Выберите диапазон адресов IP из рабочей очереди и нажмите **Правка**. Диапазон отображается в текстовом окне над рабочей очередью, где его можно отредактировать и добавить новый диапазон в рабочую очередь.
- **Удалить.** Удаление выбранного диапазона адресов IP из рабочей очереди.
- **Удалить все.** Удаление всех диапазонов адресов IP из рабочей очереди.

Теперь, когда задача обнаружения сконфигурирована, ее можно использовать для обнаружения устройств, подключенных к вашей сети, путем планирования времени выполнения задачи обнаружения.

Планирование и запуск обнаружения

"Используйте кнопку "Расписание" на вкладке "Поиск устройств" для отображения диалогового окна "Планировать обнаружение". Используйте данное диалоговое окно для планирования времени выполнения обнаружения. Вы можете осуществить запуск задачи обнаружения немедленно, в определенный момент времени в будущем, запустить в соответствии с определенным графиком или однократно.

После того, как вы запланировали поиск, см. вкладку Задачи обнаружения для определения статуса обнаружения. Планирование запуска задачи обнаружения в соответствии с графиком помогает автоматически выполнять поиск новых устройств, появляющихся в сети.

Диалоговое окно **Планировать обнаружение** имеет следующие параметры.

- Не планировать. Задача не включается в расписание, но остается в списке Конфигурации обнаружения для использования в будущем.
- Запустить сейчас. Запускает задание в ближайшее время. Для запуска задания может потребоваться до одной минуты.
- Запустить в запланированное время. Задание запускается в указанное вами время. При выборе данного параметра необходимо ввести следующие данные:
    - Время. Назначаемое вами время начала выполнения задания.
    - Дата. Назначаемая вами дата начала выполнения задания. В зависимости от вашего местонахождения дата устанавливается в формате день-месяц-год или месяц-день-год.
    - Повторять каждые. Если необходимо регулярно запускать задание, выберите соответствующее значение: Ежедневно, Еженедельно или Ежемесячно. Если вы выбрали значение "Ежемесячно", а в этом месяце нет данного числа (например, отсутствует 31 число), задание будет выполняться лишь в те месяцы, в которых имеется данное число.

Планирование задачи обнаружения

1. В левой навигационной панели выберите Обнаруженные устройства.
2. На вкладке "Конфигурации обнаружения" выберите необходимую вам конфигурацию, затем нажмите "Расписание". Сконфигурируйте расписание обнаружения и нажмите "Сохранить".
3. Следите за ходом процесса обнаружения на вкладке **Задачи обнаружения**. Для обновления состояния нажмите "Обновить".
4. После завершения обнаружения нажмите **Неуправляемые** для просмотра всех обнаруженных устройств в верхней панели **Обнаруженные устройства** (эта панель не обновляется автоматически).

Просмотр обнаруженных устройств

Обнаруженные устройства разбиваются на категории по типу устройств на панели **Обнаруженные устройства**. По умолчанию также отображается папка Компьютеры. Для просмотра устройств в различных категориях выберите папки в левой панели. Для просмотра всех устройств, найденных с помощью функции обнаружения, нажмите Неуправляемые.

- Корпуса блейд-серверов отображаются в папке **Корпуса**.
- Стандартные корпоративные устройства отображаются в папке **Компьютеры**.
- Маршрутизаторы и другие устройства отображаются в папке **Инфраструктура**.
- Устройства с поддержкой Intel AMT отображаются в папке **Intel AMT**.
- Серверы с поддержкой IPMI отображаются в папке **IPMI**.
- Не попадающие ни в одну категорию устройства отображаются в папке **Другие**.
- Принтеры отображаются в папке **Принтеры**.

Примечание. Для некоторых серверов Linux в качестве названия операционной системы отображается "Unix" (иногда такие серверы попадают в категорию "Другие"). При развертывании стандартного агента управления название ОС в списке Мои устройства для таких серверов обновляется и отображается полная информация инвентаризации.
Просмотр обнаруженных серверов

1. На странице **Обнаружение устройств** в левой панели выберите **Компьютеры** илидругой тип устройства для просмотра. Результаты отображаются на правой панели.
2. Чтобы отфильтровать результаты, щелкните значок фильтра , введите хотя бы часть имени искомого элемента и выберите **Найти**.

Назначение имен

При выполнении сканирования сети некоторые серверы возвращают незаполненное поле имени узла (или имени хоста). Наиболее часто это происходит с серверами Linux. В этом случае перед использованием функции "Управление" для перемещения устройства в список "Мои устройства" необходимо назначить ему имя.

1. На странице **Обнаружение устройств** выберите устройство с незаполненным полем имени. (В столбце имени узла нужно щелкнуть в пустой области).
2. На панели инструментов выберите "Назначить имя".
3. Введите имя и нажмите OK.

При установке агента продукта на устройстве автоматически выполняется сканирование имени хоста и обновление базы данных главного сервера.

Перемещение устройств в список "Мои устройства"

После обнаружения необходимо вручную назначить устройства, которыми вы хотите управлять, и переместить их в список **Мои устройства**. При перемещении на устройстве не устанавливается никакого программного обеспечения. Это только делает их доступными для запросов, группирования и сортировки в списке Мои устройства. Вы "назначаете" конкретные устройства для выполнения определенных действий, это похоже на использование "тележки" во многих Web-приложениях.

1. В окне **Обнаруженные устройства** выберите устройство, которое нужно переместить в список **Мои устройства**. Вы можете выбрать несколько устройств, используя стандартный метод (сочетание клавишей: нажатая SHIFT + щелчок мыши или нажатая CTRL + щелчок мыши).
2. Нажмите кнопку Цель. Если устройство не отображается, нажмите значок << на панели инструментов. Кнопка находится на краю справа. Или щелкните правой кнопкой мыши выбранные серверы и нажмите Цель.

3. На нижней панели выберите вкладку **Управление**.
4. Переместите выбранные устройства в базу данных управления или выберите целевые устройства для переноса.
5. Нажмите кнопку **Переместить**.
6.

Выберите **Переместить**, чтобы добавить устройства в список **Мои устройства** и разместить информацию об устройствах в базе данных. После сохранения информации в базе данных она доступна для выполнения ограниченных запросов и отчетов (например, по имени устройства, IP-адресу или ОС).

Группирование устройств для определенных действий

Устройства можно организовать в группы, например, по географическому местоположению или функциям, для более быстрого выполнения действий с ними. Например, вы можете захотеть просмотреть скорость процессоров для устройств, находящихся в определенном местоположении.

1. В списке **Мои устройства**выберите **Закрытые группы** или **Общие группы**, а затем нажмите **Добавить группу**.
2. Введите имя группы в окне Имя группы.
3. Выберите тип создаваемой группы.
    - Статическая. Устройства, добавленные в данную группу. Они остаются в группе до их удаления или до окончания управления ими пользователем.
    - Динамическая. Устройства, соответствующие одному или нескольким критериям, определенным в запросе. Например, в группу могут быть включены все серверы, которые в данный момент находятся в состоянии "Предупредительное". Они остаются в группе до тех пор, пока они соответствуют критериям, определенным для данной группы. В динамические группы устройства добавляются автоматически, если они соответствуют критериям запроса группы.
4. После завершения нажмите OK.
5. Для добавления устройств в статическую группу выберите устройства в правой панели списка **Мои устройства**, нажмите **Перенос/копирование**, выберите группу и нажмите **OK**.

Настройка устройств для управления

Собственно обнаружение устройств еще не обеспечивает их управление. Перед началом полного управления устройствами с помощью консоли и получением предупреждений о состоянии необходимо установить в устройствах агенты управления. Вы можете выбрать между установкой конфигурации агентов по умолчанию (которая устанавливает все агенты управления) или настроить ваши собственные конфигурации агентов для установки на ваших устройствах. (Конфигурация агентов должна включать агент мониторинга для получения предупреждений о состоянии устройства).

Вы можете установить агенты управления любым образом, описанным ниже.

- Выберите устройства в списке Мои устройства, а затем запланируйте задание конфигурации агентов для удаленной установки агентов на устройствах (см. действия ниже).

- Назначьте общий доступ к каталогу главного сервера LDlogon (//coreserver/ldlogon) и запустите SERVERCONFIG.EXE (см. действия в разделе "Извлечение агентов" в главе "Установка и конфигурация агента устройства" Руководства пользователя System Manager).
- Создайте самораспаковывающийся пакет установки для устройства. Для установки агентов запустите этот пакет локально на устройстве. Это необходимо сделать, войдя в систему с правами администратора (см. действия в разделе "Установка агентов с помощью пакета установки" в главе "Установка и конфигурация агента устройства" Руководства пользователя System Manager).

Перенос агента

1. Назначьте устройства в списке **Мои устройства** в качестве целевых (как описано выше в разделе "Перемещение устройств в список "Мои устройства"").
2. В левой навигационной панели выберите **Конфигурация агента**, щелкните правой кнопкой мыши конфигурацию, которую необходимо перенести, и выберите **Запланировать задачу**.
3. На левой панели выберите **Целевые устройства**, а затем нажмите кнопку **Добавить список целей**.
4. Выберите "Назначить задачу", нажмите "Запустить сейчас" для немедленного запуска задания или "Запустить позже" и установите дату и время запуска, а затем нажмите "Сохранить".

Состояние задания можно посмотреть на вкладке Задачи конфигурации.

Установка агентов серверов Linux

Вы можете дистанционно развернуть и установить агенты Linux и RPM на серверы Linux. Для выполнения этой операции сервер Linux должен быть правильно сконфигурирован. Инструкции по правильной установке сервера Linux см. в разделе "Установка агентов сервера" в главе "Установка и конфигурация агента устройства" *Руководства пользователя* System Manager.

Настройка предупреждений

Когда возникает неисправность или другая проблема на устройстве (например, отсутствует свободное дисковое пространство), System Manager может отправить предупреждение. Вы можете настроить эти предупреждения, выбрав степень важности или уровень, активизирующий отправку предупреждения. Предупреждения отправляются на консоль и могут быть сконфигурированы для выполнения специальных действий. Можно задавать предупреждения для разнообразных событий и потенциальных проблем. Продукт поставляется с набором правил предупреждений по умолчанию, этот набор правил устанавливается на управляемом устройстве при установке компонента мониторинга. Этот набор правил предупреждений обеспечивает обратную связь, предоставляющую информацию о состоянии устройств на консоль. Этот набор правил по умолчанию включает в себя следующие предупреждения:

- Диск установлен или удален
- Дисковое пространство
- Использование памяти

- Температура, вентиляторы и напряжение
- Мониторинг производительности
- События IPMI (для поддерживаемого оборудования)

Дополнительную информацию о предупреждениях см. в главе "Конфигурация предупреждений" "Руководства пользователя System Manager".

Настройка предупреждений

Когда возникает неисправность или другая проблема на устройстве (например, отсутствует свободное дисковое пространство), System Manager может отправить предупреждение. Вы можете настроить эти предупреждения, выбрав степень важности или уровень, активизирующий отправку предупреждения. Предупреждения отправляются на консоль и могут быть сконфигурированы для выполнения специальных действий. Можно задавать предупреждения для разнообразных событий и потенциальных проблем. Продукт поставляется с набором правил предупреждений по умолчанию, этот набор правил устанавливается на управляемом устройстве при установке компонента мониторинга. Этот набор правил предупреждений обеспечивает обратную связь, предоставляющую информацию о состоянии устройств на консоль. Этот набор правил по умолчанию включает в себя следующие предупреждения:

- Диск установлен или удален
- Дисковое пространство
- Использование памяти
- Температура, вентиляторы и напряжение
- Мониторинг производительности

Дополнительную информацию о предупреждениях см. в главе "Конфигурация предупреждений" *Руководства пользователяSystem Manager*.

Что дальше?

Теперь ваш Server Manager готов к работе и запущен. На данный момент вы использовали только небольшую часть возможностей, доступных в Server Manager (например, обнаружение устройств и конфигурацию агентов). В комплекте руководств (*Руководство по установке и развертыванию* и *Руководство пользователя*) представлена детальная информация обо всех функциональных возможностях продукта. Примеры функциональных возможностей продукта.

Обновления программного обеспечения. Устанавливает постоянный уровень безопасности с внесением исправлений на управляемых устройствах по всей вашей сети. Можно автоматизировать повторяющиеся процессы для поддержания текущей информации об уязвимых местах, для доступа к уязвимым местам на ваших управляемых устройствах, работающих на различных ОС, для загрузки необходимых исполняемых файлов исправлений, для исправления уязвимых мест с помощью развертывания и установки необходимых исправлений на затронутых устройствах и для контроля за успешной установкой исправлений.

Предупреждения. Убедитесь, что вы будете получать предупреждения, в случае достижения вашими устройствами определенного порога предельного значения. С

помощью предупреждений вы можете быть извещены различными способами с помощью функции мониторинга. Например, если вам нужно знать, когда ваши устройства хранения будут заняты более чем на 95%, можно выбрать желательный способ предупреждения (агент может отправить сообщение электронной почты или на пейджер, завершить работу или перезагрузить устройство или сделать запись в журнале предупреждений).

Запросы. Управляйте своей сетью с помощью поиска и организации устройств в базе данных главного сервера на основании заданных системных или пользовательских критериев. Вы можете посылать запросы на управляемые устройства, которые удовлетворяют указанным вами критериям (например, на все устройства, расположенные в корпоративном офисе, или на все устройства с ОЗУ 256 Кб) и группировать их для соответствующих действий. Эти группы могут быть статическими (членство в группе можно менять только вручную) или динамическими (члены в группе меняются, когда устройства приходят в соответствие или несоответствие с определенными критериями).

Мониторинг. Контролирует состояние устройства при помощи одного из поддерживаемых типов мониторинга (прямой мониторинг ASIC, внутриполосные и внеполосные IPMI, CIM и т.п.). Мониторинг позволяет контролировать разнообразные данные на ваших устройствах (например, уровни использования, события ОС, процессы и службы, архивные данные производительности и датчики оборудования (вентиляторы, напряжение, температуры и т.д.)). Предупреждения - это сопутствующая функция, которая использует агент мониторинга для инициализации действий предупреждений.

Отчеты. Генерирует разнообразные специализированные отчеты, предоставляющие критическую информацию об управляемых устройствах в вашей сети. Server Manager использует утилиту сканирования инвентаризации для добавления устройств (и полученных данных об оборудовании и программном обеспечении этих устройств) в базу данных главного сервера. Вы можете просмотреть и распечатать данные инвентаризации из окна инвентаризации устройств, а также использовать его для определения запросов и группирования устройств. Служба отчетов пользуется дальнейшими преимуществами данных сканирования инвентаризации, получая и формируя их в удобном формате отчетов; это может быть полезно при сборе и форматировании данных для регулятивных отчетов.

Обнаружение неуправляемых устройств. Обнаруживает устройства, неуправляемые с консоли. Обнаружение является первым этапом, позволяющим быстро установить управление новыми машинами. Вы можете настроить задачу обнаружения для ежемесячного поиска новых машин.

Этап 1. Дизайн домена управления

На этапе 1 производится сбор информации об инфраструктуре сети, и принимаются решения, помогающие в настройке домена управления.

На этом этапе вы изучите следующие разделы:

- Сбор информации о сети
- Выбор главного сервера
- База данных главного сервера
- Планирование системы защиты и организационная модель
- Системные требования

Сбор информации о сети

Определение и сбор всей наиболее важной информации о сети и ее отношения к System Manager. В частности, необходимо выполнить следующие действия:

- Определить конфигурации устройств.
- Выбрать главный сервер.

Выбор главного сервера

Главный сервер является центром домена управления. Все основные файлы и службы находятся в главном сервере. Физически это может быть новый или переназначенный сервер.

С помощью браузера можно запустить консоль администратора с удаленной рабочей станции, на которой выполняются такие функции управления, как управление предупреждениями, выполнение запросов к базе данных главного сервера или создание специальных сценариев.

Убедитесь, что сервер, выбранный в качестве главного сервера, соответствует системным требованиям. Далее см. раздел "Системные требования".

Планирование размещения файлов программ

В процессе установки можно определить, куда будут устанавливаться файлы программ. Используйте целевые каталоги по умолчанию, если нет веских причин для их изменения. Если необходимо изменить целевой каталог, имейте в виду, что при указании пути к целевому каталогу нельзя использовать двухбайтовые символы.

Целевой каталог по умолчанию для файлов главного сервера:

```
C:\Program Files\LANDesk\ManagementSuite
```

База данных главного сервера

System Manager устанавливает базу данных MSDE на главном сервере. Размер базы данных MSDE не должен превышать 2 ГБ. Число серверов, поддерживаемых этой базой данных, зависит от размера файла сканирования при выполнении инвентаризации сети.

Проблемы производительности при работе с MSDE наиболее ощутимы при выполнении более пяти одновременных действий с использованием этой базы данных. Например, если пять администраторов System Managerодновременно обращаются к базе данных. одновременно обращаются к базе данных.

Система защиты главного сервера и клиента

Данный продукт использует систему аутентификации на основе сертификатов. Во время установки главного сервера программа установки создает сертификат для этого сервера. При установке соединения с главным сервером клиенты выполняют поиск этого сертификата. Если у клиентов нет сертификата для данного главного сервера, они не могут с ним взаимодействовать.

Устройства могут взаимодействовать только с теми с главными серверами, для которых у них есть файл соответствующего доверенного сертификата. Каждый главный сервер имеет свой сертификат и секретные ключи. По умолчанию агенты клиента, развернутые из каждого главного сервера, будут взаимодействовать только с тем главным сервером, с которого было развернуто программное обеспечение.

Планирование области

Ролевое администрирование – это мощное средство управления защитой. Чтобы получить доступ к средствам ролевого администрирования, нажмите "Пользователи" в левой панели консоли. Необходимо выполнить вход с правами администратора.

Ролевое администрирование расширяет возможности по управлению устройствами, позволяя добавлять пользователей в систему и назначать этим пользователям права и области действия. Права определяют инструментальные средства и функции, которые пользователь может видеть и использовать (см. раздел "Понятие "права"" в Руководстве пользователя Server Manager). Область определяет диапазон устройств, которые пользователь может видеть и которыми он может управлять (см. раздел "Создание областей" в Руководстве пользователя Server Manager).

Можно создавать роли на основе обязанностей пользователя, административных функций, которые он должен исполнять, а также устройств для отображения, доступа и управления. Доступ к устройствам может быть ограничен географическим расположением, например, определенной страной, регионом, штатом, городом или определенной группой или типом серверов.

Чтобы реализовать данный тип ролевого администрирования по всей сети, просто настройте параметры текущих пользователей или создайте и добавьте новых пользователей в качестве пользователей продукта, а затем назначьте им необходимые права (для доступа к функциям продукта) и области (для управляемых устройств).

Главный сервер использует области для ограничения устройств, которые могут видеть пользователи консоли. Пользователю можно назначить несколько областей, а также одна область может использоваться несколькими пользователями. Области могут быть основаны на одном из перечисленных ниже методов:

- (По умолчанию) **Область "Все компьютеры"**. Пользователи могут видеть все устройства.
- **На основе запроса.** Пользователи могут видеть устройства, которые соответствуют выбранному критерию определенного запроса, назначенного им администратором.
- **На основе группы.** Пользователи могут видеть устройства, соответствующие критерию группы.

Для получения дополнительной информации об областях см. Server Manager*Руководство пользователя*.

Системные требования

Перед установкой проверьте, соответствует ли система приведенным ниже требованиям. В этом вам поможет проверка необходимых условий.

Главные серверы и серверы баз данных

Убедитесь в том, что все главные серверы и серверы баз данных соответствуют приведенным требованиям.

- Windows 2000 Server или Advanced Server с пакетом обновления 4, Windows Server 2003 Standard или Enterprise edition x86 с пакетом обновления SP1, или Windows 2003 R2.
- Microsoft Data Access Components (MDAC) 2.8 или выше.
- Microsoft .NET Framework 1.1.
- Информационные службы Интернета (Internet Information Services – IIS).
- Поддержка IIS для сценариев ASP.NET v1.1.
- Internet Explorer 6.0 SP1 или выше.
- Microsoft NT File System (NTFS).
- Необходимо установить сервер Windows, используемый для главного сервера, в качестве автономного сервера, а не главного контроллера домена (primary domain controller - PDC), резервного контроллера домена (backup domain controller – BDC) или контроллера Active Directory.
- Необходимо установить SNMP. Необходимо запустить SNMP и службу предупреждений SNMP.
- 200 МБ свободного дискового пространства на системном диске и 900 МБ свободного дискового пространства, как минимум, на одном диске.
- Привилегии администратора.
- Клиент LANDesk должен иметь правильную версию или не быть установленным вовсе.

Требования к главному серверу.
Файл подкачки Windows должен быть не менее 12 + *N* (где *N* – это число мегабайт ОЗУ на главном сервере). В противном случае приложения продукта могут выдавать сообщения об ошибках памяти.

Если планируется установить оба продукта Management Suite и Management Suite на одном главном сервере, то рекомендуется иметь на главной машине 1 гигабайт памяти.

Все службы продукта располагаются в одном сервере

Для небольших доменов управления можно установить главный сервер и главную базу данных на одном сервере. Для таких сетей можно использовать базу данных Microsoft MSDE по умолчанию, которую обычно поддерживать легче. Этот единственный вариант базы данных для продукта System Manager.

Ограничения

Для установки главного сервера и главной базы данных сервер должен соответствовать приведенным ниже минимальным системным требованиям:

- Процессор Pentium 4
- 4 ГБ свободного дискового пространства на дисках со скоростью 10000 об/мин или выше
- Не менее 768 МБ ОЗУ

Компьютеры для управляемого сервера

Данные продукты поддерживают перечисленные ниже серверные операционные системы (не все операционные системы поддерживаются одинаково):

- Microsoft Windows 2000 Server (с SP4)
- Microsoft Windows 2000 Advanced Server (с SP4)
- Microsoft Windows 2000 Professional (с SP4)
- Microsoft Windows 2003 Server R2
- Microsoft Windows 2003 Server Standard Edition x86 (с SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (с SP1)
- Microsoft Windows 2003 Server Enterprise Edition x86 (с SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (с SP1)
- Microsoft Windows XP Professional (с SP2)
- Microsoft Windows XP Professional x64 (с SP2)
- Windows Small Business Server 2000 (с SP4)
- Windows Small Business Server 2003 (с SP1)
- Red Hat Enterprise Linux v3 (ES) 32-bit - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32-bit - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (AS) 32-bit - U6
- Red Hat Enterprise Linux v3 (AS) EM64t - U6

- Red Hat Enterprise Linux v4 (ES) 32-bit - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (AS) 32-bit - U2
- Red Hat Enterprise Linux v4 (AS) EM64t - U2
- Red Hat Enterprise Linux v4 WS 32-bit - U2
- Red Hat Enterprise Linux v4 WS EM64t - U2
- SUSE* Linux Server 9 ES 32-bit SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Server 10 ES 32-bit
- SUSE Linux Server 10 EM64t
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

Компьютеры для управляемого сервера Linux

Ниже приведен список требований к брандмауэру и пакетам RPM для обеспечения возможности управления устройствами Linux.

Брандмауэр

Для первоначальной установки агента управления и настройки сервера Linux для взаимодействия с главным сервером (с использованием метода "Push") необходимо разрешить подключение SSH через локальный брандмауэр сервера Linux:

22 – только TCP

Чтобы обеспечить возможность взаимодействия агентов с главными серверами (операции сканирования при выполнении инвентаризации, распространении программного обеспечения, обновления уязвимых мест защиты и т.д.), локальный брандмауэр сервера Linux должен быть сконфигурирован таким образом, чтобы разрешать взаимодействие через следующие порты:

9593 – только TCP

9594 – только TCP

9595 – TCP и UDP

Для обеспечения взаимодействия с агентом локальный брандмауэр сервера Linux должен быть сконфигурирован таким образом, чтобы разрешать взаимодействие через следующие порты:

6780 – только TCP

Требуемые пакеты RPM (версия № или более поздняя)

Рекомендуется хранить все пакеты RPM продукта в каталоге ...\ManagementSuite\ldlogon\RPMS. Просмотреть этот каталог можно с помощью http://имя главного сервера/RPMS.

REDHAT_ENTERPRISE

python

Версия RPM:2.2.3-5 (RH3)

2.3.4-14 (RH4)

Двоичная версия:2.2.3

pygtk2 Версия RPM:1.99.16-8 (RH3)

2.4.0-1 (RH4)

Двоичная версия:

sudo

Версия RPM:1.6.7p5-1

Двоичная версия:1.6.7.p5

bash Версия RPM:2.05b-29 (RH3)

3.0-19.2 (RH4)

Двоичная версия:2.05b.0(1)-release

xinetd Версия RPM:2.3.12-2.3E (RH3)

2.3.13-4 (RH4)

Двоичная версия:2.3.12

mozilla Версия RPM: 1.7.3-18.EL4 (RH4)

Двоичная версия:1.5

openssl Версия RPM:0.9.7a-22.1 (RH3)

0.9.7a-43.1 (RH4)

Двоичная версия:0.9.7a

sysstat Версия RPM:4.0.7-4

Двоичная версия:4.0.7

lm_sensors

Версия RPM: 2.6 (эта версия может быть недостаточна для отображения датчиков на более новых машинах ASIC. Для получения более подробной информации см. документацию по lm_sensors на web-сайте по адресу: http://www2.lm-sensors.nu/~lm78).

SUSE LINUX

(SUSE 64)

bash

Версия RPM: 2.05b-305.6

mozilla

Версия RPM: 1.6-74.14

net-snmp

Версия RPM: 5.1-80.9

openssl

Версия RPM: 0.9.7d-15.13

python-gtk

Версия RPM: 2.0.0-215.1 [примечание: имя пакета изменено]

python

Версия RPM: 2.3.3-88.1

sudo

Версия RPM: 1.6.7p5-117.1

sysstat

Версия RPM: 5.0.1-35.1

xinetd

Версия RPM: 2.3.13-39.3

lm_sensors

Версия RPM: н/п (примечание: включена в ядро для версии 2.6)

Использование порта продукта

Введение

При использовании продукта в средах, имеющих брандмауэры (или маршрутизаторы, которые фильтруют трафик), необходимо сконфигурировать брандмауэр или маршрутизатор таким образом, чтобы обеспечить возможность работы продукта. В данном разделе описаны порты, используемые различными компонентами продукта. Основной упор сделан на информации, необходимой для конфигурирования маршрутизаторов и брандмауэров, не акцентируя внимания на сведениях о локально используемых портах (внутри индивидуальных подсетей).

Вводная информация о правилах брандмауэра

Ниже приводятся сведения о настройке правил брандмауэра. Этот раздел включает в себя вводную информацию об основных концепциях, которая будет полезна пользователям, не знакомым с данным вопросом.

Правила брандмауэра

"Открытие порта" – это не точный термин. Нельзя просто подойти к брандмауэру и "открыть порт x." Для открытия порта необходимо настроить правило брандмауэра. Правила брандмауэра описывают, какой трафик разрешен или не разрешен через брандмауэр. Правила брандмауэра не фильтруют трафик только по номеру порта. Правила могут основываться на протоколах, исходных и целевых номерах портов, направлении (входящий / исходящий), исходном и целевом IP-адресе и других параметрах.

Пример типичного правила брандмауэра: "allow inbound traffic on TCP port 9535" (разрешить входящий трафик через порт TCP 9535). Это правило необходимо для поддержки дистанционного управления при использовании данного продукта. Правило основано на трех элементах:

1. Протокол (TCP или UDP)
2. Номер порта
3. Направление (входящий или исходящий)

Эти три элемента обязательны для настройки правил брандмауэра.

Исходный и целевой порты, динамические порты

Во взаимодействии по протоколу TCP или UDP всегда участвуют два порта. Любой пакет TCP или UDP направляется из исходного в целевой порт. Правила брандмауэра могут основываться на информации исходного порта, целевого порта или обоих портов. Порты, перечисленные в данном документе (например, приведенный ниже порт), всегда являются целевыми портами.

Известные порты, например, порт 5007 (используемый службой инвентаризации) относится только к одной из взаимодействующих сторон. Вторая из взаимодействующих сторон использует динамический порт. Динамические порты назначаются операционной системой автоматически в диапазоне 1024-5000.

Брандмауэры и трафик UDP

Чтобы разрешить прохождение трафика TCP через брандмауэр, достаточно одного правила. Необходимо просто разрешить входящие соединения TCP с портом 5007. После установления соединения TCP данные могут передаваться по этому соединению в обоих направлениях.

Трафик UDP организован по-другому, так как для него не требуется установление соединения. Например, по умолчанию главный сервер будет "опрашивать" устройства UDP-порта 38293 перед запуском задачи. Правило брандмауэра, которое разрешает прохождение исходящих пакетов UDP в порт 38293, разрешает прохождение пакетов с главного сервера на устройство, расположенное за брандмауэром, но не разрешает прохождение ответных пакетов от устройства.

Правило, которое разрешает прохождение как исходящих, так и входящих пакетов в порт 38293 не подходит, так как только одна из взаимодействующих сторон прослушивает порт. Вторая сторона использует динамический порт. Так как исходящие пакеты главного сервера направляются из динамического порта в порт 38293, ответные пакеты устройства отправляются из порта 38293 в динамический порт, который не является портом 38293. Для использования двустороннего взаимодействия нужно правило, допускающее UDP-пакеты с исходным или целевым портом, равным 38293. Такое правило обычно приемлемо для среды внутренней сети, но не для связи с внешними сетями (так как, оно пропускает все входящие пакеты для всех портов UDP).

По этой причине трафик UDP обычно не считается "удобным для брандмауэра". Возвращаясь к предыдущему примеру, можно сказать, что существует альтернатива для порта UDP 38293: TCP-порт 9595. При управлении устройствами через брандмауэр можно настроить продукт на использование TCP-порта.

Используемые порты

Порт	Направление	Протокол	Служба
31770	с консоли на устройство, с устройства на главный сервер	TCP	взаимодействие между консолью и устройством
6787	с консоли на устройство	TCP	взаимодействие между консолью и устройством

Порт	Направление	Протокол	Служба
9595	с консоли на устройство	UDP	обнаружение
9595	с консоли на устройство	TCP	конфигурация агента
623	с консоли на устройство	UDP	ASF, обнаружение IPMI
9535	с консоли на устройство	TCP	дистанционное управление

Перед тем, как данный продукт сможет осуществлять управление узлами, он должен их обнаружить с помощью установленного агента управления. Для обнаружения используется UDP-порт 9595. Можно вручную добавить отдельные устройства к консоли, но для этого необходимо, чтобы устройство ответило на "опрос" UDP-порта 9595. Для взаимодействия между консолью и устройством используются TCP-порты 31770 и 6787. Трафик через последний порт выполняется с использованием HTTP. UDP-порт 623 используется для обнаружения ASF (alert standard forum). Кроме того, этот продукт использует TCP-порт 9535 для дистанционного управления. Обнаружение IPMI связано с обнаружением ASF и использует тот же порт (udp/623).

Этап 2. Установка главного сервера

Этот этап посвящен установке главного сервера.

На этом этапе рассматриваются следующие темы:

- Установка главного сервера
- Активизация главного сервера
- Развертывание на устройствах Windows
- Развертывание на устройствах Linux

Для установки компонентов, описанных для этого этапа, требуется около 30-40 минут.

Установка главного сервера

Установка главного сервера

Перед началом установки рекомендуется закрыть все приложения и сохранить все открытые файлы. На сервере Windows 2000/2003, выбранном в качестве главного сервера, сделайте следующее:

1. Вставьте носитель продукта в устройство чтения компакт-дисков или запустите AUTORUN.EXE из образа установки. Отображается экран автозапуска.
2. Щелкните **Проверить требования и установить**.
3. Запускается функция проверки требований к системе, проверяющая соответствие сервера минимальным требованиям. Убедитесь в соответствии всем требованиям. Если что-либо не соответствует, нажмите **Ошибка** на ссылке ошибочных требований для получения ссылок или информации относительно установки не соответствующего требования.
4. Нажмите **Установить сейчас** для запуска программы установки.
5. Выберите язык для установки. Нажмите **OK**.
6. Появляется экран приветствия. Нажмите **Далее** для продолжения.
7. На экране лицензионного соглашения, если вы согласны с условиями, выберите **Я принимаю условия лицензионного соглашения** для продолжения. Нажмите **Далее**.
8. Подтвердите целевую папку по умолчанию или укажите специальную целевую папку и нажмите **Далее**. Путь к целевой папке не может содержать двухбайтовых символов. В случае изменения папки не забывайте подставлять свой путь во все пути, указанные в документации по продукту.
9. Введите пароль базы данных MSDE. Запомните этот пароль или запишите его. Нажмите **Далее** для продолжения.
10. Укажите организацию и имя сертификата защиты главного сервера. Эта информация идентифицирует и описывает сертификат. Нажмите **Далее**.
11. На странице "Готово к установке" (Ready to Install) выберите **Установка**. Начнется установка продукта.
12. По завершении установки появляется диалоговое окно **Мастер установки завершен**.
13. Нажмите **Готово**.

14. Программа установки предложит перезапустить сервер. Для завершения установки необходимо выбрать **Да**. При перезапуске сервера после входа в систему вы получите уведомление о том, что программа установки запустится еще на несколько минут для завершения установки. Программа установки больше не запрашивает никакой информации во время первой перезагрузки.

Во время установки главной базы данных MSDE на сервер Windows 2003 Server операционная система Windows может прервать установку и запросить подтверждение для открытия SETUP.EXE. Если такой запрос появился, нажмите "Открыть", иначе продукт не будет правильно установлен.
Если нужно установить Intel Platform Extensions для программного обеспечения LANDesk, следуйте инструкциям мастера, который открывается после установки Server Manager.

Активизация главного сервера

Перед использованием продукта System Manager в главном сервере необходимо активизировать сервер. Сервер можно активизировать либо автоматически через Интернет, либо вручную через электронную почту. В случае существенного изменения конфигурации оборудования главного сервера, возможно, потребуется его повторная активизация.

Компонент активизации в главном сервере периодически формирует данные, относящиеся к следующим областям:

- Точное число используемых устройств.
- Неперсонифицированная шифрованная конфигурация оборудования.
- Использующиеся особые программы приложения LANDesk (все вместе "накопленные данные сервера").

Во время активизации не осуществляется сбор или формирование каких-либо других данных. Ключевой код оборудования формируется в главном сервере с помощью таких показателей неперсонифицированной конфигурации оборудования, как размер жесткого диска, быстродействие компьютера и т.п. Ключевой код оборудования передается в LANDesk в зашифрованном формате, и закрытый ключ шифрования размещается только на главном сервере. Код аппаратного ключа используется программным обеспечением LANDesk для создания части авторизованного сертификата.

После установки главного сервера утилита активизации главного сервера (**Пуск | Все программы | LANDesk | Активизация главного сервера**) во время первого запуска активизирует ядро с помощью имени пользователя и пароля, предоставленных OEM-изготовителем.

Можно выполнить обновление System Manager на Server Manager или Management Suite, используя для этого утилиту обновления главного сервера. См. раздел "Использование System Manager с Management Suite или Server Manager".

После активизации главного сервера можно использовать диалоговое окно консоли **Предпочтения | Лицензия** для просмотра информации о лицензировании продукта. Лицензия Intel OEM дает разрешение на запуск агента продукта в каждом сервере или основной плате Intel.

Об утилите активизации главного сервера

Утилита активизации главного сервера (Core Server Activation) используется для первой активизации нового сервера. Для запуска утилиты нажмите **Пуск | Все программы | LANDesk | Активизация главного сервера**. Если главный сервер не имеет подключения к Интернету, см. "Активизация главного сервера или проверка данных сервера вручную" далее в этом разделе.

Для каждого главного сервера необходим уникальный авторизованный сертификат.

Время от времени главный сервер выполняет проверку лицензирования, создавая файл "\Program Files\LANDesk\Authorization Files\LANDesk.usage". Этот файл периодически посылается серверу лицензирования ПО LANDesk. Этот файл генерируется в формате XML и отправляется в зашифрованном виде с электронной подписью. Любые изменения, сделанные в этом файле вручную, сделают его содержимое недействительным, и о последующем использовании будет послан отчет в сервер лицензирования ПО LANDesk.

Главный сервер связывается с сервером лицензирования ПО LANDesk посредством HTTP. При использовании прокси-сервера выберите вкладку **Прокси** и введите соответствующую информацию. Если главный сервер подключен к Интернету, взаимодействие с сервером лицензирования устанавливается автоматически и в дальнейшем не требует какого-либо вмешательства пользователя.

Помните, что утилита активизации главного сервера не запускает автоматически коммутируемое соединение с Интернетом, но если установить коммутируемое соединение вручную и запустить утилиту активизации, она может использовать это соединение для передачи отчета с данными об использовании.

Если в главном сервере отсутствует соединение с Интернетом, вы можете проверить и передать данные сервера вручную в соответствии с описанием, приведенным позднее в этом разделе.

Активизация главного сервера

Активизация сервера

1. Нажмите **Пуск | Все программы | LANDesk | Активизация главного сервера**.
2. Выберите **Активизировать данный главный** сервер с использованием вашего контактного имени и пароля LANDesk.

Контактное имя и пароль заполняются автоматически.

Активизация главного сервера или проверка данных сервера вручную

Если в главном сервере нет подключения к Интернету, утилита активизации главного сервера не сможет передать накопленные данные сервера. Затем появится сообщение, предлагающее передать данные активизации и проверки данных сервера вручную по электронной почте. Активизация по электронной почте – простой и быстрый процесс. Когда

в главном сервере появляется сообщение об активизации вручную, или если такое сообщение появляется при использовании утилиты активизации главного сервера, выполните следующие действия.

Активизация главного сервера или проверка данных сервера вручную

1. Когда главный сервер предлагает вручную выполнить проверку данных сервера, он создает файл данных с названием activate.txt в папке "\Program Files\LANDesk\Authorization Files". Прикрепите данный файл к сообщению электронной почты и отправьте по адресу: licensing@landesk.com. Тема и текст сообщения не имеют существенного значения.
2. Программное обеспечение LANDesk обработает прикрепление и отправит ответ по адресу, с которого прислано сообщение. Программное обеспечение LANDesk содержит инструкции и новый файл авторизации.
3. Сохраните прикрепленный файл авторизации в папке "\Program Files\LANDesk\Authorization Files". Главный сервер сразу обработает файл и обновит состояние активизации.

Если активизация вручную не удалась или главный сервер не может обработать прикрепленный файл авторизации, расширение скопированного файла авторизации меняется на .rejected, и утилита регистрирует событие вместе с дополнительной информацией в журнале приложения программы просмотра событий Windows.

Вход на консоль

После завершения установки, перезагрузки главного сервера и активизации запустите консоль, для чего откройте браузер и введите адрес сервера в следующем формате: http://servername/ldsm. (В главном сервере выберите "Пуск | Все программы | LANDesk | System Manager"). Сразу после запуска консоли появляется окно входа в консоль. Возможно, для входа вам будет предложено ввести идентификационную информацию учетной записи, использовавшейся при установке LDSM. Вход возможен только для пользователей из группы LANDesk Management Suite в главном сервере. По умолчанию программа установки добавляет пользователя, с помощью которого был выполнен вход при установке главного сервера, в группу LANDesk Management Suite. Чтобы предоставить доступ к консоли другим пользователям, добавьте их в эту группу.

При первом запуске консоли в браузере процесс ее отображения может занять до 90 секунд. Возможная задержка связана с тем, что серверу приходится выполнять единовременную компиляцию некоторых кодов. Последующие запуски консоли осуществляются быстрее.

Развертывание на устройствах Windows

Данный продукт поддерживает плановый метод принудительной конфигурации, позволяющий удаленное развертывание агентов.

Чтобы включить использование конфигурации с поддержкой автоматического развертывания для серверов Windows 2000/2003, в которых еще не функционирует стандартный агент управления, необходимо предоставить надлежащую идентификационную информацию для входа:

1. На главном сервере выберите **Пуск | Все программы | LANDesk | LANDeskСлужбы конфигурации LANDesk**, затем щелкните вкладку **Планировщик**.
2. Выберите **Смена имени**.
3. В полях **Имя пользователя и Пароль** укажите учетную запись администратора домена (в формате домен\имя пользователя).
4. Остановите и перезапустите службу планировщика.
5. С Web-консоли выберите целевые устройства, затем нажмите **Конфигурация агента > Запланированная задача** для развертывания конфигураций.

Вы можете указать администратора домена при конфигурировании серверов-участников домена Windows 2000/2003 в качестве главного сервера. Для конфигурирования серверов Windows 2000/2003 в других доменах необходимо установить доверительные отношения. Помните, что указанная в приведенном выше действии 3 учетная запись, будет использоваться также для запуска службы планировщика в главном сервере. Убедитесь, что учетная запись имеет право **Вход в качестве службы**.

Если конфигурация с автоматическим развертыванием завершилась ошибкой и отображается сообщение "Невозможно найти агента", попробуйте обнаружить проблему, выполнив приведенные ниже действия. Эти действия имитируют действия планировщика во время конфигурации с автоматическим развертыванием.

1. Найдите имя пользователя, с помощью которого запущена служба планировщика.
2. В главном сервере выполните вход с именем пользователя, использованном в действии 1.
3. Назначьте диск для \\имя сервера\C$. (Это действие является одним из наиболее вероятных источников ошибки. Существуют две возможных причины ошибки. Вероятно, что у вас нет административных прав в сервере. Если имя пользователя не имеет административных прав, возможно, общий доступ (C$) к административным функциям запрещен.)
4. Создайте каталог \\server name\C$\$ldtemp$ и скопируйте в него файл.
5. С помощью диспетчера служб Windows попробуйте запускать и останавливать службы в сервере.

Если устройство поддерживает IPMI, необходимо указать пароль BMC. Используйте вкладку **Пароль BMC** функции **Конфигурация служб** для создания пароля для контроллера IPMI Baseboard Management Controller (BMC).

1. На вкладке **Пароль BMC** введите пароль в текстовом окне **Пароль**, введите пароль еще раз в текстовом окне **Подтвердите пароль**, а затем нажмите **OK**.

Пароль не может содержать более 15 символов, каждый из которых должен быть цифрой от 0 до 9 или большой/маленькой буквой от a до z.

Если устройство поддерживает Intel* AMT, необходимо указать пароль Intel AMT. С помощью вкладки **Конфигурация Intel AMT утилиты** служб конфигурации можно создать или изменить пароль в устройствах, поддерживающих технологию Intel AMT (Active Management Technology).

Конфигурация пароля Intel AMT

1. На вкладке **Конфигурация Intel AMT** введите текущее имя пользователя и пароль. Они должны соответствовать имени и паролю, сконфигурированным на экране конфигурации Intel AMT (доступен в настройках BIOS).

2. Для изменения имени пользователя и пароля заполните раздел **Новый пароль Intel AMT**.
3. Нажмите **OK**. Данное изменение вступит в силу после запуска конфигурации клиента.

Примечание.Новый пароль должен быть очень надежным, т .е.:

- состоять как минимум из семи символов
- содержать буквы, цифры и символы
- иметь как минимум один буквенный символ со второй по шестую позиции
- значительно отличаться от предыдущих паролей
- не содержать имена или имена пользователей
- не быть распространенным словом или именем

Развертывание на устройствах Linux

Вы можете дистанционно развернуть и установить агенты Linux и RPM на серверы Linux. Для выполнения этой операции сервер Linux должен быть правильно сконфигурирован. Для установки агентов на сервере Linux вы должны иметь привилегии пользователя root.

Установка по умолчанию Linux (Red Hat 3, 4 и SUSE) включает RPM, которые требуются стандартному агенту управления Linux. Если вы выберите агента мониторинга в "Конфигурации агента" вам понадобятся дополнительный модуль RPM — sysstat.

Для исходных конфигураций агента Linux главный сервер использует SSH-соединение с целевыми серверами Linux. Вы должны иметь работающее SSH-соединение с аутентификацией с помощью имени пользователя/пароля. Продукт не поддерживает аутентификацию с использованием открытого/закрытого ключа. Любые брандмауэры между главным серверами и серверами Linux должны обеспечивать доступ к порту SSH. Обратите внимание, что необходимо протестировать соединения SSH главного сервера с использованием приложения SSH независимого производителя.

Пакет установки агентов Linux состоит из сценария оболочки, агентов tarball, .INI-конфигурации агента и сертификатов аутентификации агента. Данные файлы хранятся в общей папке главного сервера LDLogon. При выполнении сценария оболочки файлы извлекаются из пакетов tarball, устанавливаются RPM и конфигурируется сервер для загрузки агентов и периодического запуска сканера инвентаризации с учетом интервалов времени, указанных в конфигурации агента. Файлы помещаются в папку /usr/landesk.

Вы также должны сконфигурировать службу планировщика в главном сервере для использования на вашем сервере Linux информации аутентификации SSH (имя пользователя/пароль). Служба планировщика использует данную идентификационную информацию для установки агентов на ваших серверах. Используйте утилиту конфигурации служб для внесения идентификационной информации SSH, которую будет использовать служба планировщика в качестве альтернативной идентификационной информации. Должно появиться напоминание о перезагрузке службы планировщика. Если оно не появилось, нажмите Stop, а затем Start во вкладке **Планировщик**, чтобы перезапустить службу. При этом происходит активация внесенных вами изменений.

После конфигурации ваших серверов Linux и добавления идентификационной информации Linux в главный сервер вы должны добавить серверы в список **Мои устройства**, чтобы развернуть агенты Linux. Перед началом развертывания в сервере вы должны добавить его в список **Мои устройства**. Сделайте это с помощью обнаружения сервера Linux, используя параметр "Обнаружить устройства".

Обнаружение серверов Linux

1. Во время обнаружения устройств создается задание обнаружения устройства для каждого сервера Linux. Используйте стандартное сканирование сети и введите IP-адрес сервера Linux для начального и конечного IP-диапазонов. Если у вас большое количество серверов Linux, введите диапазон IP-адресов. Нажмите OK после того, как добавите IP-диапазоны для обнаружения.
2. Назначьте задачу обнаружения, которую вы только что создали, выбрав ее и щелкнув **Расписание**. После завершения задачи проверьте, были ли обнаружены серверы Linux, которыми вы хотите управлять.
3. В списке обнаружения устройств выберите серверы для управления, щелкните **Цель** для добавления выбранных устройств в список целевых устройств. Выберите вкладку **Управление** в нижней части окна. Выберите **Переместить выбранные устройства** и щелкните **Переместить**. Так серверы добавляются в список **Мои устройства** для назначения будущего развертывания.

Создание конфигурации агента Linux

1. В конфигурации агента нажмите **Новая**.
2. Введите имя конфигурации, щелкните "HP-UX" или "Версия сервера Linux", а затем нажмите **OK**.
3. Выберите конфигурацию, которую вы только что создали, и нажмите **Правка**.
4. Выберите агента.
5. На вкладке "Инвентаризация" выберите параметры и интервал частоты сканирования. Сценарий установки добавит задание cron, которое запускает сканер в указанные интервалы времени.
6. Нажмите **Сохранить**.

Для развертывания вашей конфигурации агента выберите ее в окне "Конфигурации агента" и щелкните **Назначить задачу**. Сконфигурируйте задачу и следите за процессом выполнения на вкладке "Задачи конфигурации".

Примечание. Вы не получите информацию о состоянии на машине Linux, пока сканер инвентаризации не завершит первое сканирование после установки. **Получение конфигурации агента Linux**

1. Создайте временный каталог в машине Linux (например, /tmp/ldcfg) и скопируйте туда следующее:
    1. Все файлы из каталога LDLOGON\unix\linux.
    2. Скопируйте во временный каталог сценарий оболочки после конфигурации (<имя конфигурации>.sh).
    3. Скопируйте после конфигурации во временный каталог файл с именем *.0. Значок * звездочки можно заменить восемью символами (0-9, a-f).

4. Скопируйте во временный каталог все файлы, перечисленные в файле <имя конфигурации>.ini. Для идентификации этих файлов выполните поиск файлов "FILExx" с расширением .INI, где xx - число. Большинство найденных файлов уже были скопированы в клиентский компьютер во время первого действия, однако также нужно скопировать файлы с расширением .XML. Имена файлов не должны быть изменены за исключением:
    - файл alertrules\<любой текст>.ruleset.xml должен быть переименован в internal.ruleset.xml
    - файл monitorrules\<любой текст>.ruleset.monitor.xml должен быть переименован в masterconfig.ruleset.monitor.xml

2. Если данная машина является машиной IPMI/BMC (мониторинг включен в установку), в командной строке введите:

export BMCPW="(пароль bmc)"

3. При запуске из корневого каталога выполняется сценарий оболочки для конфигурации. Например, если сценарий имеет имя "pull", используйте полный путь указанный далее:

/tmp/ldcfg/pull.sh

4. Удалите временный каталог и все его содержимое.

Примечание. Имейте в виду, что если вы будете использовать технологию оперативной рассылки или извлечения информации агента на машине Linux, затем выполните команду

./linuxuninstall.sh -f ALL

для его очистки, затем снова запустите команду push или pull, после чего на машине останется только файл с идентификатором GUID.

Параметр -f удаляет все каталоги, принадлежащие продукту. Для получения дополнительной информации см. документацию об удалении с сервера Linux.

Этап 3. Поэтапное развертывание

В третьем этапе описывается поэтапное развертывание. *Развертывание* – это процесс установки возможностей управления на устройства, которые следует включить в домен управления.

Развертывание данного продукта включает загрузку агентов продукта и служб на устройства. Благодаря этому становится возможным централизованное управление устройствами.

На этапе 3 рассматриваются следующие темы:

- Стратегия поэтапного развертывания
- Контрольный список для конфигурирования устройств
- Развертывание на устройствах Windows
- Понятие архитектуры конфигурации устройств

Стратегия поэтапного развертывания

В основе поэтапного развертывания лежат три принципа:

1. Сначала осуществите развертывание на устройства, которые меньше используются или оказывают минимальное влияние на существующую сеть, а затем постепенно переходите к устройствам, которые больше используются или оказывают наибольшее влияние.
2. Перед развертыванием остальных агентов убедитесь, что каждое управляемое устройство функционирует стабильно.
3. Выполняйте развертывание продукта в несколько хорошо продуманных этапов вместо того, чтобы разворачивать агенты во все типы устройств одновременно, что может усложнить поиск и устранение возможных проблем.

Если выполнены два первых этапа, то вы готовы начать эту завершающую фазу развертывания продукта на устройствах.

Контрольный список для конфигурирования устройств

Конфигурирование устройств можно осуществлять посредством удаленного развертывания агентов с Web-консоли или установки из управляемого устройства. Для конфигурации с поддержкой автоматического развертывания необходимо сконфигурировать службы всех компьютеров с IPMI или AMT Intel*. Можно использовать утилиту служб конфигурации для конфигурирования приведенных ниже служб для любых главных серверов и баз данных. Для запуска утилиты конфигурации служб на главном сервере щелкните **Пуск | Программы | LANDesk | LANDesk Конфигурация служб**. Используйте вкладку "Пароль BMC" или "Конфигурация Intel AMT".

- **Конфигурация с поддержкой автоматического развертывания.** С помощью конфигурации агента определите конфигурацию устройства. Предоставьте необходимую идентификационную информацию для машин AMT Intel или IPMI с помощью служб конфигурации (см. раздел "Службы конфигурации" в документе *Руководство пользователя*). Выберите целевые устройства, затем запланируйте задачу для отправки конфигурации на устройства. См. раздел "Конфигурация агентов" в документе *Руководство пользователя*.
- **Конфигурация вручную.** Из управляемого устройства назначьте логический диск в каталог общего доступа LDLogon на главном сервере и запустите программу конфигурации сервера SERVERCONFIG.EXE. В диалоговом режиме необходимо выбрать компоненты для развертывания на устройство.

Очевидно, что конфигурация вручную не применяется при установке и конфигурировании устройств в масштабных средах. В большинстве случаев осуществляется автоматическое развертывание агентов на управляемые устройства. Помните, что во время установки продукта агенты ядра не устанавливаются автоматически; необходимо вручную установить агенты ядра, а затем перезагрузить его.

Независимо от способа конфигурирования устройств убедитесь, что на консоли используется Конфигурация агента для создания конфигурации устройства, которую вы хотите развернуть.

Для обеспечения полной функциональности продукта в системах Windows XP Professional SP2 или 2003 SP1 требуется конфигурация брандмауэра вручную. Укажите для этих устройств следующие настройки: **Управляемые серверы.**

Совместное использование файлов и принтера - TCP 139, 445; UDP 137,138 (автоматическое развертывание агента без этого не работает).

Распространение программного обеспечения – TCP 9594, 9595 (автоматическое развертывание агента без этого не работает).

Дополнительно – ICMP – "Разрешить входящие эхо-запросы" (невозможно обнаружить устройство, если этот параметр не включен).

Главный сервер.

Инвентаризация - 5007

Для указания этих настроек на управляемом устройстве нажмите **Пуск | Панель управления | Безопасность**. Данный продукт поставляется с конфигурацией агента по умолчанию, которая включает: стандартный агент управления, обновление ПО и агенты мониторинга.

Можно создавать новые конфигурации, включающие только компоненты, которые требуется установить, или (только для версий OEM) добавить компонент Intel Active System Console к конфигурации агента по умолчанию. Помните, что процесс развертывания агентов не является кумулятивным; при любом развертывании удаляются все существующие агенты. Для добавления нового агента в конфигурацию необходимо включить его вместе со всеми предыдущими агентами, которые должны быть представлены в конфигурации. **Создание конфигурации устройства**

1. В левой навигационной области выберите **Конфигурация агента**.

2. Щелкните **Новый**.
3. Введите имя новой конфигурации в окне "Имя конфигурации".

Введите имя, описывающее используемую конфигурацию, например, DBServer или Executive Office Server. Это может быть уже существующее имя конфигурации или новое имя.

4. Выберите **Linux server edition**, **Microsoft Windows server edition** или HP-UX.
5. Для управления серверами с поддержкой IPMI без установки агентов программного обеспечения продукта выберите конфигурацию **Только для BMC IPMI**, если конфигурация предназначена для IPMI-совместимых серверов, затем нажмите **OK**.
6. Выберите конфигурацию, которую вы только что создали, и нажмите **Правка**.

На вкладках некоторые параметры могут быть заблокированы, поскольку они не применяются для выбранной конфигурации. Например, если выбрана конфигурация только для BMC IPMI, настраиваемые параметры отсутствуют.

7. На вкладке **Агент** выберите агенты, которые вы хотите развернуть.
    - **Все.** На выбранное устройство устанавливаются все агенты.
    - **Обновление программного обеспечения.** Установка агента обновления программного обеспечения. Если установлен этот агент, можно настроить запуск сканера для обнаружения доступных обновлений.
    - **Мониторинг.** Устанавливает агент мониторинга на выбранное устройство. Агент мониторинга позволяет выполнять множество типов мониторинга, включая прямой мониторинг ASIC, внутриполосной IPMI, внеполосной IPMI, компонент Intel Active System Console, Intel AMT и CIM.
8. **Конфигурация** отображается только для сведения.
9. Выберите параметр перезагрузки.

Перезагрузка вручную означает, что устройства не перезагружаются даже тогда, когда выбранные агенты требуют перезагрузки. Вы должны вручную перезагрузить устройство. Если требуется перезагрузить устройство, установленные агенты не будут работать правильно, пока устройство не перезагружено. Параметр "Перезагружать серверы при необходимости" позволяет перезагружать устройства только тогда, когда агент требует перезагрузки.

Примечание. Только устройства, обновляющие существующие версии агентов 8.5 требуют перезагрузки.

10. На вкладке **Инвентаризация** выберите параметры конфигурации сканера инвентаризации. Их описание приводится ниже.

- **Автоматическое обновление.** Во время сканирования программного обеспечения удаленные устройства считывают список ПО с главного сервера. Если данный параметр установлен, каждое устройство должно иметь диск, назначенный в каталог LDLOGON на главном сервере, чтобы устройства имели доступ к списку ПО. Изменения, внесенные в список ПО, становятся немедленно доступными для устройств.
- **Обновление вручную.** Список программного обеспечения, используемый для исключения заголовков во время сканирования ПО, загружается для каждого удаленного устройства. Каждый раз, когда список ПО изменяется на консоли, вы должны вручную пересылать его удаленным устройствам.

- **Настройки сканера инвентаризации.** Время выполнения инвентаризации. Можно указать частоту выполнения инвентаризации, а также задать выполнение инвентаризации при запуске.

Если выбран параметр сканера инвентаризации **В течение (часы)**, можно указать интервал времени (в часах), в течение которого выполняется запуск сканера. Если устройство регистрируется на сервере в промежуток времени, который вы указали, сканирование инвентаризации запускается автоматически. Если устройство уже зарегистрировано на сервере, то, как только подходит время сканирования, сканер запускается автоматически. Данный параметр полезен, если вы хотите, чтобы сканирование инвентаризации устройств проходило поочередно, и они не посылали результаты сканирования одновременно.

- **Всегда выполнять при запуске.** Сканер инвентаризации запускается при каждом запуске устройства.

11. На вкладке **Наборы правил** выберите любые наборы правил мониторинга или предупреждений, которые вы хотите включить в конфигурацию. Эти наборы правил сохраняются в папке ldlogon/alertrules. Можно создать новые правила в разделах "Мониторинг" или "Предупреждения". Чтобы вновь созданные наборы правил отображались в ниспадающем списке, вы должны создать файл XML для выборочного набора правил.
12. Нажмите **Сохранить изменения** для сохранения конфигурации агента.

Дополнительную информацию о развертывании на устройства см. в разделе "Понятие архитектуры конфигурации агента" в конце данной главы.

Развертывание на устройствах Windows

Данный продукт поддерживает плановый метод конфигурации с поддержкой автоматического развертывания, позволяющий удаленное развертывание агентов.

Чтобы включить использование конфигурации с поддержкой автоматического развертывания для серверов Windows 2000/2003, в которых еще не функционирует стандартный агент управления, необходимо предоставить надлежащую идентификационную информацию для входа:

1. На главном сервере выберите **Пуск | Все программы |** LANDesk | LANDesk**Службы конфигурации**, а затем вкладку **Планировщик**.
2. Выберите **Смена имени**.
3. В полях Имя пользователя и пароль укажите учетную запись администратора домена (в формате домен\имя пользователя).
4. Остановите и перезапустите службу планировщика.
5. С Web-консоли назначьте целевые устройства, затем нажмите **Конфигурация агента > Запланированная задача** для развертывания конфигураций.

Вы можете указать администратора домена при конфигурировании серверов-участников домена Windows 2000/2003, принадлежащих к тому же домену, в качестве главного сервера. Для конфигурирования серверов Windows 2000/2003 в других доменах необходимо установить доверительные отношения. Помните, что указанная в приведенном выше действии 3 учетная запись будет использоваться также для запуска службы

планировщика на главном сервере. Убедитесь, что учетная запись имеет право **Вход в качестве службы**.

Если конфигурация с автоматическим развертыванием завершилась ошибкой и отображается сообщение "Невозможно найти агент", попробуйте обнаружить проблему, выполнив приведенные ниже действия. Эти действия имитируют действия планировщика во время конфигурации с автоматическим развертыванием.

1. Найдите имя пользователя, с помощью которого запущена служба планировщика.
2. На главном сервере выполните вход с именем пользователя, использованном в действии 1.
3. Назначьте диск на \\имя сервера\C$. (Это действие является одним из наиболее вероятных источников ошибки. Существуют две возможных причины ошибки. Вероятнее всего, что у вас нет прав администратора на сервере. Если имя пользователя не имеет прав администратора, возможно, общий доступ (C$) к административным функциям запрещен).
4. Создайте каталог \\имя сервера\C$\$ldtemp$ и скопируйте в него файл.
5. С помощью диспетчера служб Windows попробуйте запускать и останавливать службы на сервере.

Если устройство поддерживает IPMI, необходимо указать пароль BMC. Используйте вкладку **Пароль BMC** служб конфигурации для создания пароля для контроллера управления системной платой IPMI (BMC).

1. На вкладке **Пароль BMC** введите пароль в текстовом окне **Пароль**, введите пароль еще раз в текстовом окне **Подтвердить пароль**, а затем нажмите **OK**.

Пароль не может содержать более 15 символов, каждый из которых должен быть цифрой от 0 до 9 или большой/маленькой буквой от a до z.

Если устройство поддерживает Intel* AMT, необходимо указать пароль AMT Intel. С помощью вкладки **Конфигурация Intel AMT** утилиты служб конфигурации можно создать или изменить пароль на устройствах, поддерживающих технологию Intel AMT (Active Management Technology).

Конфигурация пароля Intel AMT

1. На вкладке **Конфигурация Intel AMT** введите текущее имя пользователя и пароль. Они должны соответствовать имени и паролю, сконфигурированным на экране **Конфигурация Intel AMT** (доступен в настройках BIOS).
2. Для изменения имени пользователя и пароля заполните раздел **Новый пароль Intel AMT**.
3. Нажмите **OK**. Данное изменение вступит в силу после запуска конфигурации клиента.

Примечание. Новый пароль должен быть очень надежным, т.е.:

- состоять как минимум из семи символов
- содержать буквы, цифры и символы
- иметь как минимум один буквенный символ со второй по шестую позиции
- значительно отличаться от предыдущих паролей
- не содержать имена или имена пользователей
- не быть распространенным словом или именем

Проверка успешного завершения развертывания агента

Чтобы убедиться в успешном развертывании агента управления на устройствах, подтвердите, что вы можете выполнять приведенные ниже задачи с консоли. Если для выполнения этих задач необходима дополнительная информация, см. главы в документе *System Manager Руководство пользователя*, касающиеся соответствующих функций.

Инвентаризация

- В списке **Мои устройства** дважды щелкните устройство, затем просмотрите список установленных агентов.
- Выполните запрос инвентаризации.
- Выберите устройство, затем нажмите **Инвентаризация**, чтобы просмотреть данные для этого устройства.
- Измените файл WIN.INI устройства Windows, выполните повторное сканирование устройства, затем убедитесь, что изменения были записаны в журнал CHANGES.LOG.

Развертывание устройств из командной строки

С помощью параметров командной строки в SERVERCONFIG.EXE можно регулировать состав компонентов, устанавливаемых на устройства.

Вы можете запустить SERVERCONFIG.EXE в самостоятельном режиме. Эта программа находится на главном сервере в каталоге (системный диск)\Программы\LANDesk\ManagementSuite\LDLogon. SERVERCONFIG.EXE можно также найти в каталоге общего доступа \\coreservername\LDLogon, который читается из любого сервера Windows 2000/2003.

Понятие архитектуры конфигурации агентов

Понятие SERVERCONFIG.EXE

SERVERCONFIG.EXE является утилитой конфигурации устройства продукта. Она выполняет конфигурирование серверов Windows для управления в три действия:

1. SERVERCONFIG определяет, был ли компьютер ранее сконфигурирован с помощью другого продукта LANDesk. Если да, то SERVERCONFIG удаляет старые файлы и отменяет все остальные изменения.
2. SERVERCONFIG ищет скрытый файл с названием CCDRIVER.TXT, чтобы определить, нуждается ли сервер в повторном конфигурировании. (Процесс принятия решения утилитой SERVERCONFIG описан ниже). Если повторное конфигурирование устройства не требуется, SERVERCONFIG завершает работу.
3. Если устройство требуется переконфигурировать, SERVERCONFIG загружает соответствующий файл инициализации (SERVERCONFIG.INI) и выполняет содержащиеся в нем инструкции.

Если SERVERCONFIG.EXE запускается второй раз и при этом выбраны другие агенты по сравнению с первым выполнением, агенты из первого выполнения утилиты удаляются. При каждом новом запуске SERVERCONFIG.EXE необходимо выбирать каждый требуемый агент, даже если агенты ранее были установлены.

Следующие параметры командной строки доступны для SERVERCONFIG.EXE:

Параметр	**Описание**
/I=	Компоненты для включения (включая кавычки): "Common Base Agent" "Inventory Scanner" "Alerting" "Vulnerability scanner" "Server Monitor" "Active System Console" Их можно объединять в одной командной строке. Пример. SERVERCONFIG.EXE /I="Mirror Driver" /I="Vulnerability scanner"
/IP	Конфигурация с использованием IP
/L или /Log=	Путь к файлам журналов CFG_YES и CFG_NO, в которых регистрируется информация о сконфигурированных и несконфигурированных устройствах
/LOGON	Выполнение префиксных команд [LOGON]
/N или /NOUI	Не отображать интерфейс пользователя
/NOREBOOT	Не перезагружать устройство по завершении
/P	Запрашивать разрешение пользователя на выполнение
/REBOOT	Принудительно перезагрузить сервер после выполнения установки
/TCPIP	То же, что и IP (см. выше)
/X=	Исключить компоненты Пример. SERVERCONFIG.EXE /X=SD
/CONFIG=	/CONFIG]= Использовать указанный файл конфигурации устройства вместо

используемого по умолчанию файла SERVERCONFIG.INI.

Например, если вы создали файлы конфигурации, называемые NTTEST.INI, используйте синтаксис:

SERVERCONFIG.EXE /CONFIG=TEST.INI

Специальные файлы .INI должны находиться в одном каталоге с утилитой SERVERCONFIG.EXE, и примите во внимание, что вместе с параметром /config используются имена файлов без приставки 95.

/? или /C Отображение окна справки

Развертывание стандартного агента управления

Стандартный агент управления является обязательным и представляет собой основополагающий протокол продукта.

Развертывание сканера уязвимых мест

Агент сканера уязвимых мест выполняет операции сканирования и исправления. Кнопка **Запланировать задачу защиты** позволяет создать задачу, запускающую программу vulscan.exe без параметров. При запуске без параметров программа vulscan определяет главный сервер, присваивая ключу реестра "hklm\software\intel\landesk\LDWM" значение "CoreServer". Затем программа запрашивает последний список уязвимых мест для сканирования, выполняет сканирование и передает результаты на главный сервер. Результаты помещаются в список обнаруженных обновлений. Обнаруженные обновления необходимо загрузить на главный сервер. Обновления могут быть модифицированы в процессе исправления. Если в процессе исправления успешно устанавливаются одно исправление или несколько, выполняется повторное сканирование, и новые результаты передаются на главный сервер. Этот процесс касается обновлений LANDesk и обновлений OEM.

Развертывание сканера инвентаризации

С помощью сканера инвентаризации можно добавлять устройства в базу данных главного сервера и собирать данные об аппаратном и программном обеспечении устройств. Сканер инвентаризации запускается автоматически при исходной конфигурации устройства. Сканер собирает данные об оборудовании и программном обеспечении и вводит их в базу данных главного сервера. После этого сканирование оборудования происходит каждый раз при загрузке устройства, а сканирование программного обеспечения происходит только через определенные интервалы времени, которые вы установите.

Развертывание агента мониторинга

Агент мониторинга позволяет выполнять множество типов мониторинга, включая прямой мониторинг ASIC, внутриполосной IPMI, внеполосной IPMI, Intel AMT и CIM.

Развертывание Intel(R) Active System Console

Устанавливает агент, который предоставляет доступ к консоли Intel Active System Console из System Manager посредством интерфейса или меню. Этот агент устанавливается только на устройствах с платами Intel; при включении данного агента в развертывание на платах, отличных от Intel, он не будет установлен.

Удаление главного сервера

Существует определенная стратегия, которой необходимо следовать при развертывании различных компонентов. Имеется также соответствующая стратегия удаления компонентов.

В приведенных ниже разделах описано, как правильно удалять каждый компонент. Необходимо удалять компоненты в следующем порядке:

1. Удалите с устройств агенты продуктов.
2. Удалите главный сервер.

Удаление агентов продуктов с устройств

Первым действием удаления программного обеспечения продукта из сети является удаление его агентов с ваших устройств.

Удаление агентов из серверов

1. Выполните вход в сервер с правами администратора.
2. Назначьте устройство в общую папку главного сервера ManagementSuite.
3. Откройте окно командной строки, измените букву устройства папки ManagementSuite и введите следующую команду:

uninstallwinclient.exe

4. Удаление всех агентов будет выполнено без выдачи запроса на подтверждение.

Можно выбрать Пуск, Выполнить, затем ввести *core name*\LANDesk\ManagementSuite\uninstallwinclient.exe.**Полное удаление агента Linux с сервера Linux**

1. В папке общего доступа ManagementSuite найдите файл linuxuninstall.tar.gz и скопируйте его в окно Linux.
2. Запустите этот файл, используя параметры x, z и f. Командная строка:

tar xzf linuxuninstall.tar.gz

3. После запуска файла выполните команду ./linuxuninstall.sh из командной строки.

Для получения справки запустите команду с параметром -h. Примечание. Имейте в виду, что если вы будете использовать технологию оперативной рассылки или извлечения информации агента на машине Linux, а затем выполните команду

./linuxuninstall.sh -f ALL

для ее очистки и повторно используете технологию оперативной рассылки или извлечения информации агента, то данный процесс создаст дублирующиеся записи в базе данных для одной и той же машины с тем же именем и адресом IP, так как GUID машины был удален.

Параметр -f удаляет все каталоги, принадлежащие продукту. Для дополнительной информации см. документацию об удалении с сервера Linux.

После удаления остается только файл /etc/ldiscnux.conf. Этот файл помогает избежать засорения базы данных дублированными устройствами. Если вы не собираетесь снова помещать данное устройство в базу данных, то этот файл можно спокойно удалить. UninstallWinClient.exe является общей папкой в ManagementSuite. К ней имеют доступ только администраторы. Эта программа удаляет агентов продукта из любого устройства, на котором выполняется. Это приложение Windows, работающее в фоновом режиме без отображения на интерфейсе. После удаления в базе данных могут присутствовать две копии сервера. Одна из этих копий содержит только архивные данные, в то время как другая - всю текущую информацию.

Примечание. По умолчанию программа Uninstallwinclient.exe выполняет перезагрузку после удаления агентов. Чтобы избежать перезагрузки, используйте в командной строке параметр /noreboot.

Удаление главного сервера

Заключительным действием удаления продукта из сети является удаление программного обеспечения из главного сервера. Перед этим необходимо убедиться, что агенты ПО продукта удалены с ваших серверов.

Удаление главного сервера

1. Перейдите на главный сервер.
2. Нажмите **Пуск** | **Настройки** | **Панель управления,** затем дважды щелкните **Установка и удаление программ**.
3. Выберите ПО Intel Platform Extensions for LANDesk software (если оно установлено) и нажмите Добавить/Удалить.
4. Для удаления ПО продукта выберите LANDesk software.
5. Нажмите кнопку **Добавить/Удалить**.

Удаление базы данных главного сервера
Необходимо вручную удалить базу данных главного сервера.

Удаление базы данных главного сервера

По умолчанию база данных главного сервера не удаляется при удалении LANDesk® System Manager. Важно.Не удаляйте базу данных главного сервера, если вы будете позднее переустанавливать на вашем компьютере LANDesk® System Manager.

Удаление базы данных главного сервера

1. Перейдите на главный сервер.
2. Нажмите **Пуск** | **Настройки** | **Панель управления,** затем дважды щелкните **Установка и удаление программ**.

3. Для удаления базы данных главного сервера выберите Microsoft SQL Server Desktop Engine (LDMSDATA).
4. Нажмите **Добавить/Удалить**.

Файлы базы данных

При удалении компонента Microsoft SQL Server Desktop Engine не выполняется удаление файлов базы данных, использующих LANDesk® System Manager. Можно оставить эти файлы в компьютере, если только нет необходимости освободить дисковое пространство. Для удаления файлов базы данных вручную удалите содержимое папки \ProgramFiles\Microsoft SQL Server\MSSQL$LDMSDATA\Data.

Поддержка

Вы можете связаться со службой поддержки в интерактивном режиме ПО LANDesk через Web-сервер (только на английском языке). Службы поддержки предоставляют самую последнюю информацию о программных продуктах LANDesk. Можно также найти информацию об установке, советы по поиску и устранению неисправностей, обновления ПО и информацию о технической поддержке. Перейдите на Web-сайт по указанному ниже адресу и выберите страницу соответствующего продукта.

http://www.landesk.com/support/index.php

Можно также загрузить последние версии документации и примечаний к выпуску, содержащие информацию, которая не была доступна на момент поставки продукта. Если вы приобрели System Manager у OEM-производителя, обратитесь в его службу поддержки.

Если вы не можете решить проблему с помощью данного руководства или Web-сайта службы технической поддержки ПО LANDesk, служба технической поддержки ПО LANDesk предоставляет разнообразные платные услуги по оказанию поддержки, консультаций и по партнёрству. Для получения дополнительной информации см. страницу технической поддержки по адресу:

http://www.landesk.com/wheretobuy/

Перед тем, как обратиться в службу технической поддержки, подготовьте следующую информацию:

- Ваше имя, название компании и версию используемого продукта.
- Используемая сетевая операционная система (название и версия).
- Какие исправления или пакеты обновления установлены.
- Подробное описание действий для воспроизведения проблемы.
- Действия, которые были предприняты для устранения проблемы.
- Любая информация, которая может помочь инженеру службы технической поддержки понять проблему, например, вид используемого приложения для работы с базами данных, модель установленного видеоадаптера, изготовитель и модель используемого компьютера.