LANDesk® System Manager 8.7

Руководство пользователя

Никакая часть данного документа не является предоставлением обязательств, гарантии или лицензии, явных или подразумеваемых. LANDesk отказывается от какой-либо ответственности по таким обязательствам, гарантиям или лицензиям, включая, но не ограничиваясь следующими положениями: пригодность для конкретных целей, годность для продажи, патентная чистота интеллектуальной собственности или другие права третьих сторон или LANDesk; погашение ответственности и все остальное. Продукты LANDesk не предназначены для использования в медицинских и спасательных средствах или средствах жизнеобеспечения. Читатель ставится в известность, что у третьих сторон могут быть права на интеллектуальную собственность, имеющую отношение к данному документу и упомянутым здесь технологиям. Рекомендуем проконсультироваться с компетентным юрисконсультом (без обязательства LANDesk).

Компания LANDesk оставляет за собой право в любое время и без предварительного уведомления вносить изменения в данный документ или соответствующие спецификации и описания продуктов. Компания LANDesk не предоставляет гарантии на использование данного документа и не несет ответственности за возможные ошибки в документе, а также не принимает на себя обязательств по обновлению содержащейся здесь информации.

LANDesk, Autobahn, NewRoad, Peer Download и Targeted Multicast являются зарегистрированными товарными знаками или товарными знаками LANDesk Software, Ltd. или ее дочерних компаний в США и/или других странах.

*Другие товарные знаки и наименования являются собственностью соответствующих владельцев.

Содержание

Обзор

О программе LANDesk® System Manager

Вас приветствует LANDesk® System Manager8.70, автономное приложение управления, которое позволяет обслуживать доступ к серверам, включая серверы Windows, Linux, HP-UX и AIX. Это приложение может быть установлено и использоваться в противоположность LANDeskManagement Suite с применением этой же базы данных главного сервера и в качестве Management Suite для упрощения IT-отчетности.

Разработанный с акцентом на минимальное влияние на ресурсы, данный продукт имеет несколько агентов, работающих "по требованию", и служб, которые запускаются только при необходимости, тем самым, освобождая память и ЦП для других задач. Компания LANDesk знает, что доступность устройств является критически важным фактором для бизнеса, поэтому продукт разработан с учетом стабильности и возможности функционирования 24 часа в сутки, 7 дней в неделю. Она обеспечивает вас возможностью управления программным обеспечением, работающим в ваших устройствах. Можно установить полного агента, выбрать конкретные компоненты или поместить устройства в специальный список без установки агентов.

Для правильного отображения диалоговых и других окон необходимо включить Web-сайт System Manager в список разрешенных от блокирования раскрывающихся окон браузера.

Что нового в версии 8.70

Следующие функции добавлены или обновлены с момента выпуска предыдущей версии System Manager:

Управление устройствами без агентов. Выполнение управления устройствами в списке **Мои устройства** без установки в них агента управления, но когда они поддерживают технологию внеполосного управления, такую как Intel* AMT, IPMI или DRAC.

Выборочные группы в списке"Запланированные задачи". Возможность группировки задач в выборочные группы для запуска.

Режим начинающего пользователя. Возможность отображения надписей для кнопок инструментальной панели, что упрощает для новых пользователей возможность идентификации кнопок. Подобные сведений также можно получить, подведя указатель мыши к выбранной кнопке (советы также отображаются после подведения указателя мыши).

Конфигурация оборудования. Новый инструмент, позволяющий конфигурацию параметров устройств с поддержкой функций Intel* AMT. Вы можете сконфигурировать идентификаторы аутентификации устройств Intel AMT, просмотреть созданные идентификаторы и изменить параметры конфигурации, связанные с аутентификацией устройств Intel AMT. Также можно определить политики прерывателя цепи, которые необходимы для блокировки несанкционированных действий в устройствах.

Расширенная поддержка технологии Intel Active Management Technology. Этот продукт теперь поддерживает технологию Intel* Active Management Technology 2 (в дополнение к версии 1). AMT версии 2 также поддерживает функции управления, не требующие установки агентов, и возможности автоматического обнаружения устройств Intel* AMT 2.

Функции продукта

System Manager позволяет из простой полученной информации выбрать уровень управления для анализа производительности, защиты и конфигурации. System Manager включает следующее:

Простая в использовании Web-консоль. Запуск продукта в любое время, из любого места с помощью Web-консоли, разработанной для отображения важной информации при использовании удобного интерфейса. Консоль можно запустить с сервера на основной рабочей станции (или на любой другой рабочей станции) без выполнения установки. Просто перейдите по адресу http://*главный сервер*/LDSM. Назначение "целевых" устройств для выполнения таких операций, как распространение программного обеспечения, выполняется путем выбора устройств и помещения их в список **Целевых устройства**, подобно модели "торговой корзины" для большинства Web-приложений.

Расширенная поддержка операционных систем. Управление разнообразным окружением сервера с помощью одной интегрированной консоли. В дополнение к управлению серверами Windows 2000 и 2003 System Manager обеспечивает поддержку нескольких вариантов Linux и Unix:

- 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 Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

Запланированные задачи. Список всех запланированных или выполненных развертываний агентов, результаты поиска, обновление программного обеспечения и настраиваемые сценарии. Можно перепланировать задачу, изменить ее или установить ее повторяющийся запуск.

Поддержка Intel* AMT. Поддержка технологии Intel* Active Management Technology версий 1 и 2. Технология Intel AMT позволяет осуществлять удаленное управление сетевыми устройствами, находящимися в любом системном состоянии, с использованием внеполосного взаимодействия (OOB), даже если операционная система не отвечает или устройство выключено. Одним единственным требованием к устройству является то, что оно должно быть подключено к корпоративной сети и находиться в состоянии ожидания.

Поддержка IPMI. Продукт обеспечивает поддержку IPMI-серверов (Intelligent Platform Management Interface) версий 1.5 или 2.0, позволяя выполнять удаленное внеполосное восстановление закрытых серверов и просматривать автономные данные управления, даже если ОС или процессор серверов не работает.

Инструментальное средство для создания сценариев. Выборочные задачи могут быть выполнены на устройствах путем создания локальных сценариев планировщика.

Мониторинг производительности. Можно выполнять мониторинг производительности управляемых корпоративных и blade-серверов в режиме реального времени с помощью различных атрибутов. Можно отслеживать эти атрибуты и просматривать данные о производительности, заносимые в отчеты в течение нескольких дней. Можно осуществлять мониторинг как устройств, на которых установлен агент, так и внеполосных IPMI-серверов, на которых агент не установлен.

Поддержка blade-серверов. Поддерживаются blade-корпуса и blade-серверы IBM, включая функции обнаружения, определение корпуса, инвентаризации и управления исправлениями. Для более эффективного сбора данных инструментальные средства продукта позволяют группировать blade-серверы по функциям, корпусам, стойкам или любым другим критериям.

Отчеты. Можно получить отчеты о любом устройстве в базе данных. В отчеты включается такая информация, как статистика использования, выделение ресурсов и множество других данных. В продукт включено несколько подготовленных (заранее сформированных) отчетов. Эти отчеты составляются быстро при прямом обращении к базе данных для запроса информации и представления данных в виде двух- или трехмерных круговых диаграмм и гистограмм. С помощью настраиваемых запросов можно создать дополнительные отчеты.

Мониторинг состояния/предупреждения. Упрощение мониторинга общего состояния устройства. Можно установить предельные значения для таких параметров, как дисковое пространство или использование ЦП, и настроить выдачу предупреждений о достижении этих значений. Просмотреть состояние выбранных устройств и инициировать определенные функции для устранения проблем можно заранее, до того, как пользователи обнаружат снижение производительности или возникнет простой из-за какой-либо проблемы.

Обновления программного обеспечения. Можно получать программные обновления для System Manager, а также для оборудования Intel*. Обновления можно загрузить вручную с помощью функций распространения программного обеспечения.

Ролевое администрирование. Добавление пользователей и настройка их доступа к инструментальным средствам и другим устройствам осуществляется в зависимости от административной роли пользователей. С помощью ролевого администрирования можно назначить область для определения устройств, которые пользователь может видеть и

которыми может управлять, а также права для определения задач, которые он может выполнять (например, получать отчет только о пользователях).

Инвентаризация. С помощью инструментального средства сканирования инвентаризации продукт собирает информацию о состоянии оборудования, а также информацию о программном обеспечении, и сохраняет ее в базе данных главного сервера. Затем эти данные можно просмотреть, распечатать и экспортировать.

Обнаружение устройств. Это средство для того, чтобы знать, какие устройства находятся в сети. Функция обнаружения устройств собирает основную информацию обо всех устройствах в доступном окружении, тем самым позволяя улучшить контроль и ускорить загрузку агентов на целевые устройства.

Поддержка ПО Active System Console. Поддержка программного обеспечения Active System Console, которое обеспечивает быстрый обзор состояния системы, когда в устройство установлен агент Active System Console. Вы можете отобразить сведения о нормальной работе выбранных элементов оборудования или о местах возникновения возможных проблем. Также можно отобразить подробные сведения показателей производительности и вывести список компонентов, включая журналы оборудования, программного обеспечения и информацию о компонентах Intel* AMT и IPMI (если устройство имеет их поддержку).

Справка. К данному продукту прилагается руководство по началу работы, а также контекстно-зависимая электронная справка.

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.

Приступая к работе

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. 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** или другой 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**.

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.

Предоставление лицензии

Процесс лицензирования помогает вашей организации работать в соответствии с соглашениями по лицензированию узлов, постоянно выполняя процесс авторизации. Данный подход также позволяет вам использовать различные главные серверы с определенной пользовательской учетной записью. В процессе лицензирования для создания и управления учетными записями пользователей используется резервная база данных. В процесс лицензирования происходит передача простого запроса и ответа с главного сервера серверу данных, позволяя главному серверу обновить свою деятельность на последующий период.

При запуске продукта (или любом добавлении) после установки вы можете активировать временную оценочную лицензию или ввести имя пользователя и пароль для активации лицензии, приобретенной при покупке LANDesk. Те же имя пользователя и пароль используются для активации всех главных серверов для существующей учетной записи.

Процесс активации, по сути, одинаков для пробных продуктов и для приобретенных продуктов. Если устройство подключено к Интернету, процесс представляет собой простой обмен информацией. Если устройство не подключено к Интернету, необходимо вручную отправить по электронной почте файл в LANDesk, а затем сохранить полученный файл на главном сервере. Процесс активации работает следующим образом.

1. Пользователь запускает процесс Активировать утилиту главного сервера
2. Создается файл, содержащий информацию о сервере и использовании. Он подписывается закрытым ключом главного сервера и шифруется посредством открытого ключа LANDesk.
3. Если есть связь с Интернетом, происходит взаимодействие главного сервера и сервера LANDesk, и главный сервер передает файл активации. Сервер обрабатывает информацию и посылает обратно информацию активации, которая записана непосредственно в базе данных.
4. Если устройство не подключено к Интернету, вы можете отправить по электронной почте файл, находящийся в папке \Программы\LANDesk\Authorization Files, по адресу licensing@landesk.com.

Добавление лицензий

Доступные с консоли функции зависят от ключа лицензии. Вы можете добавить новый ключ лицензии для получения дополнительных функций или для обновления количества пользователей. При установке генерируется временная 45-дневная лицензия. При добавлении действительной лицензии с консоли временная лицензия удаляется.

Добавление ключа лицензии

1. В левой навигационной панели выберите **Предпочтения**.
2. Выберите вкладку **Лицензия**.
3. Внизу экрана щелкните ссылку http:/www.landesk.com/contactus/.

Если вышеуказанная ссылка не работает, это значит, что уровень безопасности обозревателя не установлен на "Средний". В Internet Explorer поменяйте уровень

безопасности Интернета, установленный по умолчанию, на "Средний" (**Сервис > Свойства обозревателя > Безопасность > Интернета > По умолчанию**).

Консоль

Запуск консоли

Запуск консоли

1. На главном сервере выберите **Пуск | Все программы | LANDesk** | **LANDesk System Manager**.

   или

   На удаленной рабочей станции откройте браузер и введите адрес консоли. Необходим следующий формат: http://*corename*/ldsm.

2. Укажите необходимое имя пользователя и пароль.

   Если выполняется дистанционное подключение к главному серверу, выполните обычные процедуры Windows для удаленного входа (например, если пользователь имеет локальную учетную запись на главном сервере, нужно ввести имя, а если пользователь имеет запись в домене, нужно ввести доменное имя\имя пользователя).
3. Нажмите **OK**.

Если список устройств и кнопки не отображаются после запуска консоли, возможно, нужно активизировать главный сервер.

Диалог входа System Manager

Этот диалог используется для запуска консоли и подключения к главному серверу.

- **Имя пользователя.** Используется для идентификации пользователя. Пользователь может быть администратором или другим пользователем продукта с ограниченными правами (дополнительную информацию см. в разделе Ролевое администрирование). Пользователь должен быть членом группы LANDesk Management Suite главного сервера. Если выполняется дистанционное подключение к главному серверу, введите имя домена и имя пользователя.
- **Пароль.** Пароль пользователя.

Использование консоли

Следующие средства используются для просмотра, настройки, управления и защиты сетевых устройств при с одной консоли. Сюда включены такие функции, как изменение параметров программного обеспечения или конфигурации, выполнение диагностики проблем с программным и аппаратным обеспечением, а также администрирование пользователей (их выполняемой роли) для контроля за доступом к функциям и устройствам. Кроме того, используя продукты LANDesk, можно подключаться к ним напрямую с консоли.

В верхней панели на консоли отображается сервер, в который вы вошли, 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 управлять устройствами и пользователями, просматривать отчеты, запускать функции поиска, изменять запросы и т.д. Размер панелей и столбцов в списке **Мои устройства** можно изменять. Если в устройстве не установлены агенты, информация о таком устройстве отображается только в столбцах имени и адреса IP. В некоторых случаях может быть также отображена операционная система.

Для удобства и возможности отображения в Web-браузере приложение System Manager обеспечивает некоторую функциональность, совместимую с приложениями Windows.

- Для просмотра доступных функций устройства (например, функций эхо-теста и проверки цели) в списке **Мои устройства** щелкните правой кнопкой мыши нужное устройство.
- Для выбора нескольких последовательных элементов в списке щелкните первый элемент, а затем, удерживая нажатой клавишу **Shift**, щелкните последний элемент.
- Для выбора нескольких непоследовательных элементов в списке щелкните каждый нужный элемент, удерживая нажатой клавишу **Ctrl**.

Для правильного отображения диалоговых и других окон необходимо включить Web-сайт приложения System Manager в список разрешенных от блокирования раскрывающихся окон браузера.

Ролевое администрирование
Выполнение функций просмотра и управления устройствами в списке **Мои устройства** и возможность использования инструментальных средств управления зависят от прав доступа к устройствам, а также от области устройств, которые назначаются пользователям администратором. Для получения дополнительной информации см. "Ролевое администрирование".

В данном разделе приводится информация по следующим темам:

Список "Мои устройства"

Список **Мои устройства** содержит описанные ниже группы и подгруппы. Кроме того, в зависимости от прав доступа пользователя и области устройства для упрощения управления устройствами можно создать свои собственные группы.

Все устройства

В списке **Все устройства** отображаются устройства, в которые текущий пользователь в зависимости от его области выполнил вход. Список представлен в виде простого перечисления (без указания подгрупп). При подключении к основному серверу администратор сможет просмотреть каждое устройство, управление которым осуществляется данным сервером. С другой стороны, права пользователей продукта ограничены, и они могут просматривать только те устройства, которые размещены в назначенных им областях (область зависит от запроса базы данных или от расположения каталога).

Устройства, в которых работают агенты продукта (стандартный агент управления и служба инвентаризации), включаются в список **Все устройства** автоматически, если для них выполнено сканирование инвентаризации, и они включены в базу данных главного сервера. Обычно сканирование первый раз выполняется во время начальной настройки устройства. После сканирования и включения в базу данных главного сервера устройство рассматривается как управляемое главным сервером устройство. Для получения дополнительной информации о настройке устройств см. Конфигурация агентов клиентов.

Так как группа **Все устройства** пополняется автоматически с помощью сканирования инвентаризации, возможно, необходимость выполнять поиск устройств вручную никогда не возникнет. Однако для поиска устройств, которые еще не включены в базу данных главного сервера (или для переноса неуправляемых устройств в серверную группу), можно воспользоваться инструментальным средством поиска для сканирования сети. Для получения дополнительной информации см. раздел Обнаружение устройств.

Группа **Все устройства** предоставляет описанную ниже информацию о каждом устройстве. Для открытия списка дважды щелкните **Все устройства**.

- **Имя.** Хост-имя устройства, например, имя компьютера Windows*.
- **IP-адрес.** IP-адрес устройства.
- **Состояние.** Состояние и доступность устройства. Значениями могут быть: "Нормальное", "Предупредительное" или "Критическое".
- **Агент.** Текущий агент, работающий в устройстве.
- **Тип устройства** Отображает тип оборудования компьютера (Intel AMT, IPMI, ASIC или IPMI Advanced).
- **Операционная система.** Тип операционной системы, работающей в устройстве.
- **Работает с.** Дата и время, с которых компьютер работает без перерыва (в часовом поясе, где расположена база данных).

Когда вы выбираете устройство, его свойства отображаются в навигационной панели **Свойства** под списком устройств. На панели **Свойства** отображается большое количество важных атрибутов устройства.

- **Идентификатор.** Идентификационный номер устройства. Этот номер определяется последовательностью, в которой устройство было добавлено в список **Все устройства**.
- **IP-адрес.** IP-адрес устройства.
- **Производитель.** Изготовитель устройства.
- **Модель.** Модель устройства.
- **Скорость процессора.** Скорость ЦП устройства.

- **Тип процессора.** Тип ЦП устройства.

На консоли можно посмотреть подробную информацию инвентаризации, а также дать указание выполнить какое-либо действие, например, запустить составление отчета.

Если дважды щелкнуть устройство в списке **Все устройства**, откроется окно Информационная консоль сервера, в котором отобразится сводная информация об устройстве, параметры дистанционного управления и информация о наборе правил предупреждения.

Общие группы

В списке **Общие группы** отображаются группы устройств, которые были созданы пользователем с правами администратора. Другие пользователи также могут видеть эти группы.

Кроме того, в этом списке отображаются группы корпусов blade-серверов, которые создаются автоматически при добавлении в список управляемых устройств модуля управления корпусом (CMM). В группе отображаются модули CMM и каждый ассоциированный с ними управляемый blade-сервер. В некоторых случаях после создания группы корпуса вы не сможете редактировать ее параметры.

Группы могут быть статическими или динамическими. Динамические группы содержат устройства, которые соответствуют критериям предварительно настраиваемой фильтрации, например, таким критериям, как скорости процессора, ОС устройства или настраиваемые атрибуты (например, тип устройства). В статические группы могут быть включены списки устройств, другие статические или динамические группы.

Закрытые группы

В списке **Закрытые группы** отображаются списки устройств, созданные вошедшим в данный момент пользователем. Другие пользователи не могут видеть закрытые группы, поэтому такие пользователи не могут использовать эти группы.

Значки устройств

Значки устройств отображаются в списке **Все устройства** и определяют текущее состояние каждого устройства. В списке **Мои устройства** есть возможность одновременно выбрать несколько устройств и обновить их состояние нажатием кнопки **Обновить**, расположенной на панели инструментов.

В приведенной ниже таблице перечислены возможные устройства, их значки состояния, а также их значения.

Значок	Описание
	Устройство в нормальном состоянии

Значок	Описание
	Устройство в состоянии предупреждения
	Устройство в критическом состоянии
	Устройство в неизвестном состоянии

Использование контекстных меню

Для всех элементов консоли, включая группы, устройства, запросы, запланированные задачи, сценарии и т.д., доступно контекстное меню. Контекстное меню обеспечивает быстрый доступ к общим задачам и критической информации об элементе.

Для просмотра контекстного меню необходимо щелкнуть элемент правой кнопкой мыши. Например, если в списке **Мои устройства** щелкнуть правой кнопкой мыши какое-либо управляемое устройство, появится контекстное меню данного устройства со следующими типичными параметрами:

- **Удалить из группы.** Удаляет элемент из определенной пользователем группы.
- **Цель.** Осуществляет перенос выбранного устройства в список Целевые устройства. **Примечание.** Если устройства не отображаются в списке **Целевые устройства**, нажмите кнопку **Обновить** на вкладке **Целевые устройства**.
- **Ping-запрос устройства.** Проверяет активность устройства.
- **Трассировка устройства.** Осуществляет отправку команды трассировки маршрута для просмотра отправляемых и получаемых сетевых пакетов и количества узлов, через которые пакет проходит до цели.

В справке не описывается каждое контекстное меню элемента, отображаемого на консоли, однако рекомендуется щелкнуть правой кнопкой мыши каждый из элементов, чтобы просмотреть доступные параметры.

Использование инструментальных средств

Инструментальные средства можно выбрать в левой панели. Для просмотра всех инструментальных средств воспользуйтесь кнопками-стрелками вверху панели.

Администратор может видеть все инструментальные средства в левой навигационной панели. Другие пользователи будут видеть только те инструментальные средства (функции), для которых им назначены права. Например, если пользователю не предоставлено право "Отчеты", инструментальное средство "Отчеты" не появится в левой навигационной панели.

Далее предоставлен полный список инструментальных средств.

- **Обновления программного обеспечения.** Загрузка соответствующих пакетов обновления.
- **Сценарии.** Создание сценариев и управление ими.
- **Запланированные задачи.** Просмотр всех задач в планировщике (создаются с помощью утилит "Конфигурация агента", "Уязвимые места", "Обнаружение устройств" или "Сценарии").
- **Мониторинг.** Мониторинг производительности управляемых устройств в режиме реального времени с помощью различных атрибутов.
- **Предупреждения.** Настройка предупреждений, установка предельных значений и настройка ответа, который будет использоваться продуктом при превышении предельных значений.
- **Конфигурация агента.** Настройка конфигурации агента IPMI (контроллера BMC), Linux или Windows.
- **Обнаружение устройств.** Поиск устройств в сети, которые еще не добавлены в основную базу данных.
- **Журналы.** Отображение журнала предупреждений, в котором регистрируются предупреждения, отмеченные пользователем для управляемых устройств.
- **Отчеты.** Управление предварительно настраиваемыми отчетами служб.
- **Запросы.** Создание и изменение запросов, направляемых в базу данных для выделения конкретных устройств в соответствии с определенными критериями.
- **Пользователи.** Контроль за доступом пользователей к инструментальным средствам и устройствам в соответствии с назначенными им правами и областью.
- **Предпочтения.** Создание настраиваемых атрибутов инвентаризации и просмотр лицензионной информации.
- **Конфигурация оборудования.** Отдельное окно, отображающее параметры конфигурации для устройств Intel* AMT.

При выборе имени инструментального средства оно запускается в окне в правой панели.

Просмотр свойств устройства

В списке **Мои устройства** можно быстро получить информацию о каком-либо устройстве, выбрав его в списке и нажав **Свойства** в нижней панели.

Более подробная информация об устройстве доступна в его инвентаризационных данных. Инвентаризационные данные можно посмотреть в списке **Все устройства**, выбрав устройство и открыв вкладку **Просмотр инвентаризации** в нижней панели. При этом откроется окно **Инвентаризация**.

Целевые устройства

Список **Целевые устройства** помогает выполнять задачи на выбранных устройствах, такие как развертывание агентов или сканирование обновлений ПО для выбранной группы устройств.

Рекомендуемое число устройств для добавления к списку не должно превышать 250. Устройства остаются в списке до истечения тайм-аута сеанса консоли (отсутствие активности в течение 20 минут).

Добавьте устройства в список **Целевые устройства**, выбрав их из любого списка устройств. Если вы не видите желаемое устройство, воспользуйтесь кнопкой **Найти** на панели инструментов. Выполните поиск одного или нескольких устройств, используя универсальный шаблон % или *. На панели инструментов нажмите кнопку **Цель**, чтобы добавить устройство к списку **Целевые устройства**. Если эта кнопка не отображена, нажмите кнопку **<<**.

Если обнаружено несколько устройств, выберите необходимое устройство, а затем нажмите **Цель**. Если полученный список устройств занимает несколько страниц, следует нажимать **Цель** для каждой страницы. Вы не можете выбрать устройства на нескольких страницах и для всех нажать кнопку только один раз. Чтобы выбрать количество устройств, отображаемых на каждой странице, воспользуйтесь кнопкой со стрелкой "вниз" в правой части панели инструментов. На одной странице можно отображать до 500 устройств. Для изменения количества устройств в списке см. Параметры страницы в меню **Предпочтения**.

С одним или несколькими устройствами в списке **Целевые устройства** можно выполнить действие, такое как, развертывание конфигурации агента на каждом из целевых устройств или перемещение неуправляемых устройств в список **Мои устройства**.

Назначение цели для устройств

1. В списке **Мои устройства** или **Обнаруженные устройства** выберите устройство, для которого нужно выполнить действие. Вы можете выбрать несколько устройств, используя стандартный метод (сочетание клавишей: нажатая SHIFT + щелчок мыши или нажатая CTRL + щелчок мыши).
2. Нажмите кнопку **Цель**. Если она не отображается, нажмите значок **<<** на панели инструментов. Кнопка находится справа.

На нижней панели выбранные устройства будут отображены на вкладке **Целевые устройства**. Если они перечислены на этой вкладке, вы можете открыть инструментальное средство (например, Развертывания агента) и запланировать действие для применения на целевых устройствах. Если в качестве цели вы выбрали неуправляемые устройства, откройте вкладку **Управление** и переместите их в список **Мои устройства**.

Фильтрация отображаемого списка

В списке **Мои устройства** есть значок фильтра, который вы можете использовать, чтобы определить, какие устройства отобразятся в списке. Вы можете фильтровать по одному критерию (по имени устройства или по адресу IP), или можно объединить критерии для работы с подгруппой компьютеров.

Фильтрация отображаемого списка

1. В списке **Мои устройства** дважды щелкните **Все устройства** или перейдите к одной из групп.
2. На панели инструментов нажмите кнопку **Фильтр**  .
3. В раскрывающемся списке выберите **Имя устройства** или **IP-адрес**.

4. В текстовом окне укажите параметры выбранного критерия. В окне **Найти** не поддерживаются следующие специальные символы: < , > , " , ' , !.

   При фильтрации по имени устройства введите имя хоста или диапазон имен компьютеров. Для поиска определенных имен компьютеров можно использовать универсальный шаблон (например, *srv).

5. Нажмите кнопку **Найти**.

Использование групп

Для упрощения управления устройства могут быть организованы в группы. Группы могут быть созданы для организации устройств по функциям, географическому расположению, подразделению, атрибутам устройств и по любой другой нужной вам категории. Например, можно создать группу Web-серверов для всех серверов, сконфигурированных в качестве Web-серверов, или группу, включающую все устройства, работающие под управлением отдельной операционной системы. Можно щелкнуть правой кнопкой мыши название группы для ее открытия, удаления или выбора в виде целей всех ее устройств для выполнения действий, например, развертывания наборов правил предупреждений и агентов.

Главный вид программы **Мои устройства** содержит следующие группы:

- **Все устройства.** Перечисляет все устройства, которые может увидеть текущий пользователь, основываясь на назначенной для него области (без подгрупп). Для администратора в списке **Все устройства** отображаются все устройства, которые были просканированы или перемещены в базу данных главного сервера. Устройства, сконфигурированные со стандартными агентами управления, автоматически включаются в группу/папку **Все устройства**, когда сканером инвентаризации для них выполняется сканирование в базу данных главного сервера. Пользователи, в том числе администраторы, не могут создавать группы внутри папки **Все устройства**.
- **Общие группы.** Перечисляет группы/устройства, которые администратор добавил из группы **Все устройства**, а также группы корпусов блейд-серверов. Администратор (пользователь с административными правами) может видеть все устройства в этой группе, в то время как другие пользователи видят только устройства в разрешенной для них рабочей области. Только администраторы могут создавать группы внутри папки **Общие группы**.
- **Закрытые группы.** Перечисляет группы/устройства для текущего пользователя в системе на основании назначенной для него рабочей области. Пользователь может создавать подгруппы устройств только внутри папки **Закрытые группы**. Пользователи могут добавлять устройства в свои **Закрытые группы** или их подгруппы, перемещая или копируя их из групп **Общие группы** и **Все устройства**. Все пользователи могут создавать группы внутри групп **Закрытые группы**.

Для получения дополнительной информации о том, какие устройства вы можете просматривать, какими - управлять и какими средствами управления пользоваться см. раздел "Ролевое администрирование."

Типы группы

Вы можете создавать и управлять двумя типами групп:

- **Статические группы**. *Статическая группа* - это ряд устройств, вручную добавленных в группу. Изменения статических групп могут выполняться только вручную путем добавления или удаления из них устройств.
- **Динамические группы**. *Динамическая группа* - это группа компьютеров, удовлетворяющих критериям фильтрации или определению запроса. При каждом развертывании группы выполняется ее запрос, и отображаются его результаты. Например, динамическая группа может содержать все устройства, которые сейчас находятся в предупредительном состоянии. Машины перемещаются в группу и из нее при изменении их текущих состояний.

Создание статической группы

1. На экране консоли для устройства щелкните дважды родительскую группу (например, **Закрытые группы**) и выберите **Добавить группу**.
2. Введите имя новой группы.
3. Выберите **Статическая**, а затем **OK**.

После создания статической группы вы можете перемещать или копировать устройства в группу, выбирая их из списка и нажимая на инструментальной панели **Перенос/копирование**. Вы можете копировать устройства из списка **Все устройства** в группу или перемещать/копировать их из других групп.

Создание динамической группы

1. На экране консоли для устройства щелкните дважды родительскую группу (например, **Закрытые группы**), а затем выберите **Добавить группу**.
2. Введите имя новой группы.
3. Выберите **Динамическая**, а затем **OK**.

После создания динамической группы необходимо создать фильтр для определения компьютеров, включаемых в эту группу. Может быть создан новый фильтр или указан фильтр на основе существующего запроса.

Создание нового фильтра

1. Выберите свою созданную динамическую группу (в нижней панели отобразится **Свойства группы**).
2. В окне **Свойства группы** выберите **Создать новый фильтр**, а затем **Новый фильтр**.
3. Выберите нужные критерии фильтра и нажмите **OK**.

Создание фильтра на основе существующего запроса

1. Выберите созданную вами динамическую группу (в нижней панели отобразится **Свойства группы**).

2. В окне **Свойства группы** выберите **Создать фильтр на основе существующего запроса**.
3. Выберите существующий запрос, который нужно использовать для фильтрации группы и щелкните **Новый фильтр**.
4. Добавьте любые другие критерии фильтра, а затем нажмите **OK**.

Если вы создали фильтр на основании существующего запроса, который впоследствии был изменен вами или другим пользователем, данный фильтр не будет динамически меняться для соответствия изменениям запроса.

Использование вкладки "Действия"

Вкладку **Действия** можно использовать для выполнения операций с выбранными и целевыми устройствами. Вы можете удалять устройства из списка управляемых компьютеров, включать, выключать, перезагружать и отслеживать их подключения к управляемым устройствам.

- Удалить устройства
- Параметры питания
- Мониторинг устройств

Удаление устройств

Параметр **Удалить устройства** позволяет удалить выбранные или целевые устройства из списка управляемых компьютеров. Эта функция может удалять одно или несколько устройств из любой группы (группы по умолчанию или созданной пользователем) в System Manager. Как только устройство удаляется из группы, оно полностью удаляется из всех списков управляемых/инвентаризуемых устройств, включая группу по умолчанию **Все устройства**.

При удалении большого числа устройств это действие может занять много времени. Если действие не завершается в отведенное время, попробуйте разбить его на меньшие по размеру действия.

Параметры питания

Функция **Параметры питания** позволяет выключать, перезагружать, и в случае с управляемыми машинами, имеющими поддержку IPMI, включать питание удаленных устройств. Если серверы не имеют IPMI-поддержки, в них должен быть развернут агент LANDesk для выполнения дистанционной перезагрузки и выключения питания. В машинах с поддержкой IPMI необходимо иметь правильно сконфигурированную идентификационную информацию IPMI для включения/выключения питания и выполнения перезагрузки. Если в устройстве с поддержкой IPMI развернут агент LANDesk, можно использовать функции включения и выключения питания без использования идентификационной информации IPMI. Используйте утилиту конфигурации служб для установки пароля IPMI BMC для управляемых серверов с поддержкой IPMI.

Использование параметров управления питанием

1. В списке **Мои устройства** выберите устройство или цель в списке устройств.
2. На нижней панели выберите вкладку **Действия**.
3. Выберите **Параметры питания**.
4. Выберите для выполнения действий в устройствах, находящихся в списке Целевые устройства, или только в выбранных устройствах.
5. Выберите следующие параметры:
   - Перезагрузка
   - Выключение питания
   - Включение питания (работает в устройствах с поддержкой IPMI и устройствах с функцией Wake on LAN)

6. Выберите **Показать окно переназначения консоли** для запуска небольшой процедуры с помощью программы запуска (гораздо легче перекомпилировать программу запуска для систем EM64T, чем выполнять управление через службу TmTY).

   При включении или выключении питания управляемого сервера с поддержкой IPMI можно открыть окно переназначения консоли, в котором отображается информация о загрузке сервера. Это полезно, когда нужно проверить процесс загрузки сервера. Окно консоли может также использоваться для приостановки процесса загрузки и изменения настроек BIOS в управляемом сервере.

   Для отображения окна переназначения консоли в системной BIOS сервера должен быть активен порт переназначения консоли через последовательный интерфейс. Данные консоли отправляются в последовательный порт. Если сервер и административная консоль соединены с помощью кабеля последовательного интерфейса, переназначение консоли выполняется через это подключение. В противном случае System Manager инициирует переназначение последовательного интерфейса через ЛС (SOL) для отправки данных из последовательного порта в локальную сеть. Подключение SOL остается активным, пока открыто окно консоли. После завершения отображения данных на консоли нужно закрыть ее окно.

   Если окно консоли останется открытым, появится второе окно для отображения сообщений. Можно закрыть это окно сообщений. После появления окна переназначения консоли, в котором еще нет отображения загрузки, вы можете увидеть отображение случайных символов. Это происходит потому, что контроллер BMC начинает отправлять сообщения поддержки соединения, получаемые на административной консоли. Эти символы не отображаются во время показа экрана загрузки, но могут появиться вновь после завершения загрузки.

Мониторинг устройств

Используйте функцию "Мониторинг устройства" для проверки подключений выбранных устройств. Если устройство потеряет подключение к сети, оно не сможет отправить предупреждение в главный сервер. Функция мониторинга устройств проверяет способность устройств взаимодействовать в сети.

1. В списке **Все устройства** выберите устройство или цель в списке устройств.

2. В нижней панели выберите вкладку **Действия**, затем щелкните **Мониторинг устройства**.
3. Чтобы просмотреть список устройств, контролируемых на текущий момент, щелкните **Показать устройства для мониторинга**.
4. Введите время ожидания (в минутах) между сеансами эхо-теста и число раз, которое продукт будет пытаться связаться с устройством.
5. Укажите, следует ли выполнять данные действия для устройств в списке целевых устройств или для всех устройств в группе **Все устройства**.
6. Для остановки мониторинга всех устройств выберите **Полная отмена тестирования (эхо-теста) устройств**.
7. Нажмите **Применить**.

В процессе мониторинга контролируется только последняя выбранная группа целевых устройств. Например, если целевыми назначены устройства A и B и к ним применяется мониторинг устройств, базовый сервер будет отправлять запросы только устройствам A и B. Если назначить целевыми устройства C и D и применить к ним мониторинг устройств, контролироваться будут только устройства C и D; мониторинг устройств A и B будет отменен.

Выборочные столбцы

Используйте функцию **Выборочные столбцы** для редактирования имен и полей столбцов. "Имя" — название столбца, а "Поле" — атрибут(ы), которые могут отображаться в столбце (при наличии атрибута). Другие пользователи не будут видеть изменения столбцов. Изменения выборочных столбцов отображаются в окне **Мои устройства**.

В этот продукт включен набор столбцов по умолчанию, состоящий из семи столбцов. Вы не можете редактировать набор столбцов по умолчанию, но можно выбрать набор выборочных столбцов и использовать его в качестве вашего набора по умолчанию.

Не рекомендуется создавать выборочные столбцы, содержащие несколько имен полей. Например, если необходимо создать поле Computer.Software.Package.Name, а на устройстве установлено несколько пакетов, то в каждой строке списка System Manager будет отображаться только одно имя пакета, даже если в одном и том же устройстве присутствуют разные имена пакета, вследствие чего в списке **Все устройства** для одного и того же устройства будет выводиться несколько записей.

Создание набора выборочных столбцов

1. В левой навигационной панели нажмите **Предпочтения**.
2. Откройте вкладку **Выборочные столбцы**.
3. Щелкните **Новый**.
4. Введите имя выборочного столбца.

5. В верхнем окне выберите все заголовки столбцов, которые вы хотите включить в набор столбцов и нажмите **Добавить**.

   Откроется окно со списком всех данных инвентаризации, содержащихся в базе данных. Внимательно просмотрите этот список и выберите атрибут, который будет отображаться в списке результатов запроса. Не забудьте указать атрибуты, которые помогут определить клиентов, возвращаемых запросом. Если в списке нет необходимых атрибутов, то их можно добавить в диалоговом окне Выборочные атрибуты. При этом необходимо назначить атрибуты машинам, прежде чем они появятся в диалоговом окне запроса.

   Примечание. Если в базе данных выбран атрибут с отношением 1:*, то для отдельного устройства будут получены дублирующиеся записи. При выборе атрибута с отношением 1:1 (единственный возможный атрибут, как, например, Computer.System.Asset Tag) записи не будут дублироваться.

6. Чтобы изменить порядок следования столбцов, выделите заголовок и щелкните **Вверх** или **Вниз**.
7. Для удаления столбца выберите его в нижнем окне и нажмите **Удалить**.
8. Чтобы заменить существующий заголовок столбца, выберите его в нижнем окне, щелкните **Правка**, внесите свои изменения и нажмите **Enter**. Следующие специальные символы не поддерживаются: < , > , ' , " , !.
9. Для сохранения набора столбцов нажмите **OK**.
10. Для использования набора столбцов при просмотре списка **Все устройства**, выберите его и нажмите **Назначить в качестве текущего набора столбцов** на панели инструментов.

Правка набора выборочных столбцов

1. В левой навигационной панели выберите **Предпочтения**.
2. Откройте вкладку **Выборочные столбцы**.
3. Выберите набор выборочных столбцов и нажмите **Правка**.
4. В верхнем окне выберите заголовок столбца и нажмите **Добавить** для добавления столбца (см. выше примечания к действию 5).
5. Для удаления столбца выберите его в нижнем окне и нажмите **Удалить**.
6. Чтобы заменить существующий заголовок столбца, выберите его в нижнем окне, щелкните **Правка**, внесите свои изменения и нажмите **Enter**. Следующие специальные символы не поддерживаются: < , > , ' , " , !.
7. Чтобы изменить порядок следования столбцов, выделите заголовок и щелкните **Вверх** или **Вниз**.
8. Для сохранения своих изменений нажмите **OK**.

Выборочные атрибуты

Атрибуты - это характеристики или свойства устройства. Чем больше атрибутов имеет устройство в базе данных, тем легче его идентифицировать. Можно создать дополнительные атрибуты только, если вы используете для этого LANDesk® Server

Manager с правами администратора. Если выборочные атрибуты были созданы и добавлены в базу данных главного сервера, можно назначить их значения для управляемого устройства. Если выборочные атрибуты не были добавлены в главную базу данных, параметр **Назначить атрибуты** не будет отображаться на вкладке **Действия**.

Назначение выборочных атрибутов для устройств

1. В списке **Все устройства** выберите одно или несколько устройств.
2. На нижней панели выберите вкладку **Действия**.
3. В левой панели выберите **Назначить атрибуты**.
4. Каждое имя атрибута имеет раскрывающийся список значений. Выберите значение из раскрывающегося списка имени атрибута и повторите необходимые действия. Щелкните **Выбранные устройства**.
5. Нажмите **Назначить**, а затем **OK**.

Выборочные атрибуты могут быть назначены для нескольких выбранных целевых устройств. Если устройства находятся в списке целевых устройств, в приведенном ранее действии 4 выберите **Целевые устройства**.

Параметры страницы

Вкладка **Параметры страницы** используется для настройки параметров отображения страниц, содержащих списки устройств или графические данные.

1. В левой навигационной панели нажмите **Предпочтения**.
2. Откройте вкладку **Параметры страницы**.
3. В раскрывающемся списке **Тип диаграммы** выберите тип диаграммы, который хотите использовать в **отчетах**.
4. В окне **Элементов на странице** введите максимальное число элементов, которые могут отображаться на каждой странице, использующей разбиение текста на страницы. Число элементов не может быть более 500.

Режим начинающего пользователя

Можно настроить показ текста рядом с кнопками на панели инструментов, что помогает новым пользователям идентифицировать функции продукта. Если этот параметр не выбран, на панели инструментов отображаются только значки. Текст будет отображен только после помещения над значком указателя мыши.

1. Для отображения текста рядом с кнопками на панели инструментов выберите **Показать текст на панели инструментов**
2. Нажмите кнопку **Обновить**.

Просмотр информационной консоли сервера

Информационная консоль сервера используется для отображения главной информации об устройствах, системной информации, например, сведений о ЦП или вентиляторах, контроля состояния и предельных значений важных компонентов устройства, управления

уязвимыми местами, включением или выключение питания устройств или управления их перезагрузкой. Информационная консоль сервера имеет разделы, отображаемые на левой навигационной панели.

- Системная информация
- Обновления программного обеспечения
- Мониторинг
- Наборы правил
- Параметры питания
- Конфигурация оборудования

Для просмотра информационной консоли устройства сначала необходимо в этом устройстве установить стандартного агента управления (см. Конфигурация агентов). Кроме того, после установки агента устройство необходимо перезагрузить для правильного функционирования информационной консоли сервера. Перезагрузка также необходима после установки агента в главном сервере и в управляемых устройствах.

Просмотр информационной консоли сервера

1. В окне **Мои устройства** дважды щелкните имя устройства.

   Консоль откроется в новом окне браузера и по умолчанию отобразится страница **Сводка состояния**.

2. Для просмотра информации о сервере и использования доступных средств выберите кнопки в левой навигационной панели.

Системная информация

Системная информация содержит сводку данных о состоянии устройства, а также информацию о программном и аппаратном обеспечении, системные журналы и другие данные, например, информацию об инвентаризации и сети.

Сводка состояния

На странице **Сводка состояния** приводится краткое описание состояния данного устройства. Вы можете отобразить сведения о нормальной работе выбранных элементов оборудования или о местах возникновения возможных проблем.

Если какие-либо из элементов находятся в состоянии предупреждения или критической ошибки, соответствующая кнопка будет желтой (предупреждение) или красной (критическая ошибка), указывая на возникновение проблемы. Щелкните соответствующую кнопку, чтобы просмотреть описание предупреждения или критической ошибки.

Сводка системы

Используйте страницу **Сводка системы** для отображения важной информации о выбранном устройстве. На этой странице может отображаться следующая информация в зависимости от типа оборудования и программного обеспечения устройства:

- **Состояние.** Общее состояние устройства на основании определенных условий и параметров.
- **Тип.** Тип устройства, например, принтер, приложение или база данных.
- **Производитель.** Производитель устройства.
- **Модель.** Модель устройства.
- **Версия BIOS.** Версия BIOS устройства.
- **Операционная система.** Операционная система устройства.
- **Версия ОС.** Номер версии операционной системы.
- **ЦП.** Изготовитель, модель и скорость процессора устройства.
- **Сканер уязвимых мест.** Версия сканера уязвимых мест.
- **Дистанционное управление.** Версия агента дистанционного управления.
- **Распространение ПО.** Версия агента распространения программного обеспечения.
- **Сканер инвентаризации.** Версия сканера инвентаризации.
- **Тип IPMI, версия IPMI.** Тип и версия используемого устройством IPMI.
- **Версия SDR.** Версия датчика SDR контроллера BMC устройства.
- **Версия BMC.** Версия контроллера BMC устройства.
- **Ядро.** Для устройств Linux версия установленного ядра.
- **Мониторинг.** Версия агента мониторинга устройства.
- **Использование ЦП.** Процентное значение текущего использования процессора.
- **Использовано физической памяти*.** Процентное значение от общего количества физической памяти, используемой устройством.
- **Использовано виртуальной памяти*.** Процентное значение от общего количества виртуальной памяти, используемой устройством.
- **Последняя перезагрузка*.** Дата и время последней перезагрузки устройства (согласно часовому поясу базы данных).
- **Диск.** Диски устройства с общим количеством и процентным значением использования.

Данная информация берется из системного реестра Windows или из файлов конфигурации Linux.

*Данная информация отображается только в случае использования установленного в устройстве агента.

Оборудование

Используйте страницу **Оборудование** для просмотра сведений о конфигурации аппаратного обеспечения устройства. Элементы в списке **Оборудование** сгруппированы в описанные ниже категории. Обратите внимание, что не все категории относятся ко всем устройствам. Например, если устройство не оборудовано вентилятором и температурными датчиками, категория **Охлаждение** не появится в списке.

- **ЦП.** Процессоры и кэш.

- **Устройство хранения.** Логические диски, физические диски, съемные носители и соответствующие адаптеры.
- **Память.** Информация об использовании и модули памяти.
- **Корпус.** Корпус сервера; определение, закрыт корпус или открыт.
- **Устройства ввода.** Клавиатура, мышь и другие устройства.
- **Системная плата.** Системная плата, слоты расширения и BIOS.
- **Охлаждение.** Вентиляторы и температурные датчики.
- **Питание.** Блоки питания и напряжение.

Установка предельных значений для элементов оборудования

Некоторые элементы в списке **Оборудование** предоставляют данные, полученные от датчиков устройства, например, температурных датчиков. Если управляемое устройство содержит компоненты, поддерживающие датчики, можно изменить отображение показаний датчиков для выдачи предупреждений. Например, датчик температуры ЦП может быть настроен на выдачу предупреждения и критической ошибки при повышении температуры. Предельные значения обычно являются рекомендуемыми производителем параметрами, однако верхние и нижние значения можно изменить с помощью диалогового окна **Предельные значения**.

1. На информационной консоли сервера выберите **Системная информация**.
2. Откройте папку **Оборудование** и найдите необходимый элемент (например, **Охлаждение | Температуры**).
3. В списке датчиков дважды щелкните датчик, для которого необходимо установить предельные значения.
4. Введите параметры для верхнего и/или нижнего предельного значения в соответствующих полях или для изменения значений переместите ползунок влево или вправо.
5. Для сохранения изменений нажмите **Обновить**.
6. Для возврата к исходным предельным значениям нажмите **Восстановить параметры по умолчанию**.

Журналы

На странице журналов отображаются локальные системные журналы, журнал системных событий (SEL) для устройств IPMI, а также журнал предупреждений.

Локальные журналы, например, журналы приложений, безопасности и системы не имеют кнопок для очистки с консоли, однако их можно просмотреть и очистить с помощью службы управления компьютером Windows.

Если BIOS данного устройства имеет возможность выполнять очистку журнала SMBIOS, нажмите кнопку **Очистить журнал** для удаления всех записей журнала. Если кнопка недоступна, BIOS не поддерживает такую функцию.

Программное обеспечение

На странице **Программное обеспечение** отображается сводка о процессах, службах и пакетах, установленных в устройстве, а также список текущих переменных окружения.

- **Процессы.** Отображение работающих процессов; выберите процесс и для его завершения нажмите **Завершить процесс**.
- **Службы.** Отображение доступных в устройстве служб и их состояние; выберите службу и нажмите **Стоп**, **Пуск** или **Перезапуск** для выполнения изменений.
- **Пакеты.** Список установленных пакетов с номерами версий и названиями поставщиков.
- **Среда.** Список набора переменных окружения для данного устройства.

Другое

На странице **Другое** отображается информация об активах и сводка информации о сетевом оборудовании и соединениях.

- **Информация актива.** Просмотр и изменение информации об управлении активами, например, о расположении и номере тега актива; можно также просмотреть информацию о системе, например, о серийном номере, производителе и типе корпуса.
- **Сетевая информация.** Просмотр списка установленного оборудования, статистики сетевой активности, адреса шлюза по умолчанию, сводки конфигурации (включая адрес IP, адрес шлюза по умолчанию и информацию о серверах WINS, DHCP и DNS), а также списка текущих сетевых соединений (назначенные диски).

Обновления программного обеспечения

Используйте страницу **Обновления программного обеспечения** для запуска сканирования обнаруженных уязвимых мест на выбранном устройстве.

Проверка обнаруженных уязвимых мест

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать. В новом окне просмотра откроется информационная консоль сервера.

2. В левой навигационной панели выберите **Обновления программного обеспечения**.

Описания столбцов

- **Идентификатор.** Идентифицирует уязвимые места с помощью уникального кода изготовителя.
- **Важность.** Указывает важность уровня уязвимости. Возможные уровни важности: пакет обновления, критическое, высокого приоритета, среднего приоритета, низкого приоритета, не применимо и неизвестное.
- **Название.** Кратко описывает природу и назначение обновления уязвимых мест.
- **Язык.** Указывает язык операционной системы, подверженной появлению уязвимых мест.
- **Дата публикации.** Указывает дату публикации изготовителем определения уязвимых мест.

- **Автоматическая установка.** Определяет способ автоматической установки файла ассоциированного исправления уязвимых мест (без участия пользователя). Для некоторых уязвимых мест может потребоваться более одного исправления. Если любое из исправлений уязвимых мест не имеет автоматической установки, атрибут **Автоматическая установка** имеет значение **Нет**.
- **Исправимое.** Указывает, может ли уязвимое место быть исправлено с помощью развертывания или установки файла исправления. Возможные значения: "Да", "Нет" и "Некоторые" (для уязвимых мест, которые содержат несколько правил обнаружения и для тех, которые не все могут быть исправлены).

Мониторинг

Мониторинг используется для контроля датчиков производительности, отображения диаграмм и настройки предельных значений состояния компонентов устройства. Для получения дополнительной информации об этой функции см. раздел Мониторинг устройств.

Выбор датчика производительности для мониторинга

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать. В новом окне просмотра откроется информационная консоль сервера.
2. В левой навигационной панели выберите **Мониторинг**.
3. Откройте вкладку **Настройки датчиков производительности**.
4. Из столбца **Объекты** выберите объект, который хотите контролировать.
5. Из столбца **Экземпляры** выберите экземпляры (если имеются), которые вы хотите контролировать.
6. Из столбца **Датчики** выберите датчик, который вы хотите контролировать.
7. Укажите частоту опроса и количество дней, в течение которых необходимо хранить информацию о датчиках.
8. В текстовом окне **Предупреждать, когда датчик вне диапазона** укажите число раз, которое датчик может нарушать предельное значение перед созданием предупреждения.
9. Укажите верхнее и/или нижнее предельные значения.
10. Нажмите **Применить**.

Просмотр диаграммы производительности контролируемого датчика

1. Откройте вкладку **Активные датчики производительности**.
2. Выберите датчик из списка.
3. В списке **Датчики** выберите датчик, для которого необходимо отобразить диаграмму производительности.
4. Выберите **Просмотр данных в режиме реального времени**, чтобы отобразить диаграмму производительности реального времени, или выберите **Просмотр сведений**, чтобы отобразить диаграмму производительности за период времени, указанный при выборе датчика (Хранить сведения).

Горизонтальная ось диаграммы производительности соответствует прошедшему времени. Вертикальная ось отображает единицы измерения, например, байты в секунду (при

контроле над передачей файлов), проценты (при контроле над задействованными ресурсами процессора) или свободные байты (при контроле над дисковым пространством).

Наборы правил

Используйте страницу **Наборы правил** для просмотра списка правил предупреждений и мониторинга, закрепленных за выбранным устройством, а также для просмотра подробностей каждого предупреждения.

Просмотр наборов правил предупреждений

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать. Консоль открывается в новом окне браузера.
2. В левой навигационной панели выберите **Наборы правил**.
3. Откройте вкладку **Набор правил предупреждений**.

В следующем тексте даны подробности для каждого предупреждения. Дополнительную информацию об изменении данных сведений см. в разделе Использование предупреждений.

- **Достижение состояния.** Предупреждение генерируется при достижении указанного вами состояния.
- **Влияет на состояние.** Если состояние предупреждения достигает указанного предельного значения, его состояние начинает воздействовать на общее состояние устройства. Выбор состояния, влияющего на общее положение устройства, определяется в диалоге "Наборы правил предупреждений".
- **Имя набора правил.** Имя набора правил предупреждений, определенного в диалоговом окне Наборы правил предупреждений.
- **Тип предупреждения.** Тип генерируемого предупреждения: электронное письмо, предупреждение SNMP или выполнение программы.
- **Конфигурация действия.** Действие, определенное в диалоговом окне Наборы правил действий, которое происходит при генерировании предупреждения.
- **Описатель предупреждения.** Описатель, связанный с предупреждением, например, описатель e-mail.
- **Экземпляр.** Указывает конкретный источник предупреждения.

Просмотр наборов правил мониторинга

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать. В новом окне просмотра откроется информационная консоль сервера.
2. В левой навигационной панели выберите **Наборы правил**.
3. Откройте вкладку **Набор правил мониторинга**.

Далее даны сведения для каждого набора правил мониторинга. Дополнительную информацию об изменении данных подробностей см. в разделе О службе мониторинга.

- **Имя.** Имя конфигурации набора правил, определенной на странице Мониторинг.
- **Имя набора правил.** Определяет, является ли набор правил, набором по умолчанию или нет.

- **Включено.** Определяет, был ли набор правил включен для выполнения в устройстве или нет.
- **Предупредительный предел.** Предельное значение, при превышении которого устройство отправит предупредительное сообщение в главный сервер.
- **Критический предел.** Предельное значение, при превышении которого устройство отправит критическое сообщение в главный сервер.
- **Проверять каждые.** Частота контроля элемента.

Параметры питания

Функция **Параметры питания** позволяет выключать, перезагружать, и в случае управления устройствами, имеющими поддержку IPMI и Intel AMT, включать питание удаленных устройств. Если серверы не имеют IPMI-поддержки, в них должен быть развернут агент LANDesk для выполнения дистанционной перезагрузки и выключения питания.

В устройствах с поддержкой IPMI и Intel AMT необходимо иметь правильно сконфигурированную идентификационную информацию для включения/выключения питания и выполнения перезагрузки. Если устройства с поддержкой IPMI или Intel AMT имеют развернутых агентов LANDesk, тогда вы можете выполнять выключение и перезагрузку, используя идентификационные данные IPMI или Intel AMT. Для конфигурации идентификационной информации BMC для устройств с поддержкой IPMI или Intel AMT нужно использовать утилиту служб конфигурации (см. раздел Настройка служб и идентификационной информации).

Использование параметров питания в выбранном устройстве

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать. Консоль открывается в новом окне браузера.
2. В левой навигационной панели выберите **Параметры питания**.
3. Выберите следующие параметры:

   -  Перезагрузка
   -  Выключение питания
   -  Включение питания

Конфигурация оборудования

Средство **Конфигурация оборудования** позволяет настроить параметры устройств с поддержкой IPMI или Intel* AMT. Данное средство и все его параметры отображаются только на устройствах с соответствующим оборудованием (например, параметры IPMI отображаются только в том случае, если устройство имеет поддержку IPMI).

Вы можете сконфигурировать идентификаторы аутентификации устройств Intel AMT, просмотреть созданные идентификаторы и изменить параметры конфигурации, связанные с аутентификацией устройств Intel AMT. Можно также определять политики прерывателя цепи, с помощью которых определяется и блокируется несанкционированная сетевая

активность на устройствах. Для проверки работы агентов управления на устройствах можно включить мониторинг работы агентов. Для получения дополнительной информации см. Поддержка Intel AMT.

Для устройств IPMI можно настроить такие параметры конфигурации, как таймер контроля, параметры питания и параметры пользователя BMC. Кроме того, можно настроить использование канала ЛС или переназначение последовательного интерфейса через ЛС для поддержки внеполосного взаимодействия с устройством IPMI. Для получения дополнительной информации см. Конфигурация IPMI BMC.

Для устройств, имеющих контроллер Dell* DRAC (контроллер удаленного доступа), можно просмотреть журналы Dell DRAC и изменять имена пользователей для доступа к администратору сервера OpenManage. Для получения дополнительной информации см. Управление устройствами Dell DRAC.

Управление устройствами Intel* AMT

После того, как устройство Intel* AMT обнаружено и добавлено в базу данных главного сервера, им можно управлять несколькими способами, даже если на нем не установлен агент LANDesk. (См. раздел Обнаружение устройств Intel* AMT для получения информации об обнаружении устройств и их перемещении в базу данных главного сервера).

В следующей таблице перечислены параметры, доступные для устройств, имеющих только поддержку Intel AMT, в противоположность устройствам, имеющим поддержку Intel AMT и установленный агент приложения System Manager.

	Только Intel AMT	**Intel AMT и агент**	**Только агент**
Инвентаризация	сводка	X	X
Журнал событий	X	X	X
Менеджер удаленной загрузки	X	X	
Отключение сети ОС		X	
Включение сети ОС		X	
Принудительный запуск поиска уязвимых мест при перезагрузке		X	

	Только Intel AMT	Intel AMT и агент	Только агент
История инвентаризации		X	X
Дистанционное управление		X	X
Обмен информацией		X	X
Передача файлов		X	X
Удаленное выполнение		X	X
Активизация		X	X
Завершение работы		X	X
Перезагрузка		X	X
Сканирование инвентаризации		X	X
Запланированные задачи и политики	ограничено	X	X
Параметры группы		X	X
Запуск отчета об инвентаризации		X	X
Предупреждения Intel AMT		X	X

Просмотр сводки инвентаризации Intel AMT для устройства

1. Дважды щелкните устройство в списке **Все устройства**.
2. В информационной консоли сервера выберите **Параметры Intel AMT**.
3. Щелкните **Сводка инвентаризации**.

В сводке отображается GUID устройства, название продукта и производитель, серийный номер, краткая информация о BIOS, процессоре и памяти, а также номер версии Intel AMT. Если какая-либо информация отсутствует, можно выполнить обновление данных, выбрав **Обновить инвентаризацию**.

Доступ к устройствам, вошедшим в систему в корпоративном режиме (Enterprise)

При входе устройства Intel AMT в корпоративном режиме (Enterprise) главный сервер устанавливает в устройстве сертификат, необходимый для защиты связи. Если необходимо, чтобы устройством управлял другой главный сервер, то необходимо отменить идентификацию устройства, а затем снова идентифицировать его другим главным сервером. Если этого не сделать, функция Intel AMT устройства не будет отвечать, так как у нового главного сервера нет соответствующего сертификата. Если другой компьютер попытается использовать функцию Intel AMT устройства, это будет невозможно из-за отсутствия соответствующего сертификата. См. раздел Поддержка Intel* AMT для получения информации о режимах входа.

Журнал событий AMT

System Manager предоставляет доступ к журналу событий, который генерируется устройствами Intel AMT. В настройках параметров указывается, какие события отражаются в журнале. Можно просмотреть дату и время события, источник события (столбец, в котором указан объект), описание и степень важности, соответствующая настройкам Intel AMT (критическое или некритическое состояние). Можно экспортировать данные журнала в файл формата CSV (текст с разделителями-запятыми).

Просмотр журнала событий Intel AMT

1. Дважды щелкните устройство в списке **Все устройства**.
2. На информационной консоли сервера выберите **Информация о системе**.
3. Разверните окно **Журналы** и выберите **Журнал Intel AMT**.
4. Чтобы экспортировать журнал в файл в формате CSV, нажмите кнопку **Экспорт** на панели инструментов и укажите, куда необходимо сохранить файл.
5. Для удаления всех данных в журнале нажмите кнопку **Очистить журнал** на панели инструментов.
6. Для обновления записей журнала нажмите кнопку **Обновить журнал** на панели инструментов.

Команды управления питанием Intel AMT

В продукте System Manager содержатся команды включения и выключения устройств Intel AMT. Эти команды можно использовать даже в случае отсутствия реакции операционной системы устройства, если устройство подключено к сети и находится в режиме ожидания.

При использовании продуктом System Manager команд управления питанием не всегда удается проверить, поддерживаются ли эти команды принимающим оборудованием. Некоторые устройства с поддержкой Intel AMT могут не поддерживать все функции управления питанием (например, устройство может поддерживать перезагрузку IDE-R с

компакт-диска, но не поддерживать эту команду с гибкого диска). Если команда управления питанием не работает на каком-либо устройстве, см. документацию к этому устройству. Если команды управления питанием работают неправильно, попробуйте использовать обновления встроенного программного обеспечения и BIOS, предоставляемые компанией Intel.

Можно просто включать или выключать питание устройства, а можно перезагружать его, указав при этом параметры перезагрузки. Параметры описаны в приведенной ниже таблице.

Выключение питания	Выключение питания устройства
Включение питания	Включение питания устройства
Перезагрузка	Выключение питания устройства, а затем его включение
Нормальная загрузка	Запуск устройства с использованием любой последовательности загрузки, установленной по умолчанию для данного устройства
Загрузка с локального жесткого диска	Принудительная загрузка с жесткого диска устройства независимо от режима загрузки по умолчанию для данного устройства
Загрузка с локального устройства CD/DVD	Принудительная загрузка с компакт-диска или DVD-диска устройства независимо от режима загрузки по умолчанию для данного устройства
Загрузка PXE	При перезапуске устройство с поддержкой PXE выполняет поиск в сети сервера PXE; если он найден, на устройстве начинается сеанс загрузки PXE
Загрузка IDE-R	Перезагрузка устройства с помощью выбранного параметра переназначения IDE (см. ниже)
Вход в программу настройки BIOS	При загрузке устройства пользователю предоставляется возможность войти в программу настройки BIOS

Показать окно переназначения консоли	Перезагрузка устройства запускается последовательно в режиме локальной сети и отображает окно переназначения консоли
Переназначение IDE: перезагрузка с гибкого диска	Перезагрузка устройства запускается с дисковода для гибких дисков или указанного образа (файлы образа гибкого диска должны иметь формат .img; см. замечания ниже)
Переназначение IDE: перезагрузка с компакт-диска или DVD-диска	Перезагрузка устройства запускается с компакт-диска или указанного образа (файлы образа компакт-диска должны иметь формат .iso; см. замечания ниже)
Переназначение IDE: перезагрузка из указанного файла образа	Загрузка устройства выполняется из указанного файла образа (см. примечание ниже)

Использование команд управления питанием Intel AMT

1. Дважды щелкните устройство в списке **Все устройства**.
2. На информационной консоли сервера выберите **Параметры питания**.
3. Выберите команду управления питанием. Если выбрана команда **Перезагрузка**, то выберите параметр загрузки.
4. Выберите **Отправить** для запуска команды.

Замечания по использованию параметров переназначения IDE

Чтобы использовать параметры переназначения IDE, необходимо указать следующие параметры: загрузка с гибкого диска или файла образа гибкого диска и загрузка с компакт-диска/DVD-диска или файла образа компакт-диска/DVD-диска. Файлы образа гибкого диска должны иметь формат .img, а файлы образа компакт-диска должны иметь формат .iso. Для некоторых BIOS необходимо, чтобы образ компакт-диска находился на жестком диске.

В обычном режиме Intel AMT запоминает последние настройки IDE-R, но System Manager очищает настройки через 45 секунд, поэтому при последующих загрузках функция IDE-R не перезапускается. Сеанс IDE-R на устройстве Intel AMT продолжается в течение 6 часов или до тех пор, пока не будет отключена консоль System Manager. Все операции IDE-R, продолжающиеся более 6 часов, будут прерваны.

Принудительный запуск поиска уязвимых мест и отключение доступа к сети на машинах Intel AMT

Если в устройстве с поддержкой Intel AMT установлен агент LANDesk, он позволяет решить проблемы появления вредных программ и другие проблемы, связанные с ограничением доступа к устройству.

Вместе с агентом LANDesk устанавливается служба amtmon.exe. Если в устройстве запущена эта служба, то при следующей перезагрузке можно выполнить принудительный поиск уязвимых мест, что поможет определить наличие в устройстве вредных программ. Если связь с устройством прервана, можно отключить сетевое подключение устройства, даже если операционная система не функционирует, например, если вредное программное обеспечение блокировало операционную систему, полностью заняв процессор. Отключив сетевое соединение, можно предотвратить отправку устройством нежелательных пакетов через сеть.

Если в устройстве Intel AMT установлен агент LANDesk, то на странице **Параметры Intel AMT** доступны следующие параметры:

- **Сетевое подключение операционной системы.** Щелкните **Отключить**, чтобы отключить сетевой стек ОС для прекращения доступа к сети; щелкните **Включить**, чтобы включить сетевой доступ ОС, если он был отключен.
- **Сканировать уязвимые места после перезагрузки.** Принудительный запуск сканирования уязвимых мест при следующей перезагрузке устройства.

Если устройство не отвечает, или на нем может присутствовать вредное программное обеспечение, рекомендуется при следующей перезагрузке выполнить сканирование уязвимых мест с целью определения причины возникновения проблемы. Если проблема сохраняется, и машина продолжает заражать или атаковать сеть, или невозможно обратиться к устройству, то можно отключить сетевой адаптер ОС.

Запуск сканирования уязвимых мест после перезагрузки

1. Дважды щелкните устройство в списке **Все устройства**.
2. В окне консоли устройства выберите **Параметры Intel AMT**.
3. Выберите **Параметры конфигурации**, а затем **Сканировать**. На устройстве появится сообщение о том, что сканирование начнется после его следующей перезагрузки.
4. Чтобы завершить работу или перезагрузить устройство, используйте описанные выше функции менеджера удаленной загрузки Intel AMT.

Отключение или включение сетевого соединения на устройстве, от которого нет ответа

1. Дважды щелкните устройство в списке **Все устройства**.
2. В окне консоли устройства выберите **Параметры Intel AMT**.
3. Чтобы отключить сетевой адаптер устройства с целью прекращения связи с другими устройствами сети, выберите **Отключить**. При отключении сетевого соединения на устройстве появляется сообщение об отключении сетевого адаптера.

4. Если устройство безопасно и его можно снова подключить к сети, нажмите **Включить**. При восстановлении сетевого соединения на устройстве появляется сообщение о том, что сетевой адаптер вновь включен.

Открытие экрана настройки Intel AMT

System Manager имеет ссылку, позволяющую открыть экран настройки Intel AMT. Это интерфейс, предоставляемый компанией Intel и позволяющий просмотреть состояние устройства, информацию об оборудовании, журнал событий Intel AMT, настройки удаленной загрузки и настройки сети. Он позволяет также добавить и изменить учетные записи пользователей Intel AMT для устройства. Окно с этой информацией отображается отдельно от консоли System Manager. При возникновении вопросов по использованию этого интерфейса необходимо обратиться в службу технической поддержки производителя устройства.

Открытие экрана настройки Intel AMT

1. Дважды щелкните устройство в списке **Все устройства**.
2. В окне консоли устройства выберите **Параметры Intel AMT**.
3. Щелкните **Консоль Intel AMT**, затем выберите **Запустить web-консоль Intel AMT**.

Ролевое администрирование

О ролевом администрировании

Ролевое администрирование используется для настройки доступа пользователей к инструментальным средствам продукта и другим устройствам, основываясь на их административной роли в системе. Вместе с административной ролью назначается и область действия, определяющая устройства, которые пользователь может просматривать и которыми он может управлять.

Администраторы (пользователи с правами администратора) могут воспользоваться инструментом ролевого администрирования, выбрав параметр **Пользователи** в левой навигационной панели.

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.

Роли можно создавать на основании обязанностей пользователей, задач, которые они должны выполнять, а также устройств, которые они будут видеть, к которым будут иметь доступ и которыми будут управлять. Доступ к устройствам можно ограничить географическим положением, например, страна, регион, штат, город или даже отдельный офис или отдел. Также доступ можно ограничить выбранной платформой, типом процессора или другим аппаратным или программным атрибутом устройства. Вы можете назначать столько ролей, сколько потребуется, выбирать пользователей для этих ролей и регулировать область действия.

Примеры административных ролей

В следующей таблице перечислены некоторые из административных ролей, которые вы можете создать, общие задачи, выполняемые пользователем, и права, которые будут необходимы пользователю для эффективного выполнения назначенной роли.

Роль	Задачи	Необходимые права
Администратор	Конфигурация главных серверов, управление пользователями, конфигурация предупреждений, интеграция продукции других компаний и т.п. (Администратор с полными правами может выполнять любые задачи).	Администратор (все права)

Роль	Задачи	Необходимые права
Менеджер активов	Обнаружение устройств, их конфигурация, запуск сканера инвентаризации, включение записи истории инвентаризации и т.п.	Обнаружение устройств, распространение программного обеспечения и управление общими запросами
Менеджер отчетов	Запуск типовых отчетов, печать отчетов и т.п.	Отчеты (необходимо для всех отчетов)

Это всего лишь примеры ролей. Функция ролевого администрирования является достаточно гибкой для создания необходимого количества выборочных ролей. Вы можете присваивать одинаковые ограниченные права нескольким пользователям, но ограничивать их доступ к определенному диапазону устройств с помощью области действия. Даже область действия администратора можно ограничить отдельным географическим регионом или типом управляемых устройств. Оптимальная работа с функцией ролевого администрирования зависит от вашей сети и штатных ресурсов, а также от ваших потребностей.

Чтобы реализовать и принудительно применить ролевое администрирование, 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). Следуйте указанной ниже последовательности действий.

Понятие "права"

Права обеспечивают доступ к различным инструментальным средствам и функциям. Для выполнения определенных задач пользователь должен иметь соответствующее право (права). Например, для удаленного управления устройствами в своей области действия, пользователь должен иметь право на удаленное управление. Если вы установили несколько продуктов управления LANDesk, права можно назначить пользователям с любой консоли, и они эффективны на всех консолях.

Если пользователю не назначено право, то он не сможет увидеть инструментальные средства, связанные с этим правом. Например, если пользователю не назначено право на составление отчетов, то "Отчеты" не появляются в левой навигационной панели. В следующей таблице представлены права, которые требуются для использования разных инструментальных средств.

Инструментальное средство	Права, необходимые для его использования, в левой навигационной панели
Мои устройства	Основная web-консоль
Конфигурация агента	Администратор

Инструментальное средство	Права, необходимые для его использования, в левой навигационной панели
Предупреждения	Предупреждения и мониторинг
Обнаружение устройств	Обнаружение устройств
Мониторинг	Предупреждения и мониторинг
Запросы	Основная web-консоль, управление общими запросами, отчеты
Отчеты	Отчеты, управление исправлениями
Запланированные задачи	Обнаружение устройств
Сценарии	Управление исправлениями
Пользователи	Администратор
Обновления программного обеспечения	Управление исправлениями
Предпочтения	Основная web-консоль
Конфигурация оборудования	Администратор

В следующем описании представлена более подробная информация о правах для каждого продукта, а также об использовании и создании административных ролей.

Область действия контролирует доступ к устройствам
При использовании функций, разрешенных этими правами, пользователи всегда будут ограничены областью действия (устройствами, которые они могут видеть и которыми они могут управлять).

Администратор

Администратор имеет полный доступ ко всем инструментальным средствам продукта (однако, использование этих средств ограничено устройствами, входящими в область действия администратора).

Это право по умолчанию для всех вновь добавленных пользователей. Изменить его можно в шаблоне пользователя по умолчанию.

Право администратора предоставляет пользователю следующие возможности:

- Просмотр и доступ к профилям **Пользователей** в левой навигационной панели.
- Просмотр лицензии продуктов в меню **Предпочтения** в левой навигационной панели.
- Выполнение всех задач, разрешенных правами, перечисленными ниже.

Не рекомендуется удалять пользователя администратор. Если вы являетесь последним администратором, вошедшим на консоль LDSM, который открыл функцию Windows для управления компьютером и удалил пользователя администратор из группы Management Suite, у вас могут возникнуть проблемы при следующем открытии консоли. Вы все еще будете в системе в качестве администратора в течение следующих 20 минут (время тайм-аута сеанса по умолчанию), затем будет инициирован процесс обновления консоли или выполнено действие обновления браузера (клавиша F5), куда вы вошли как администратор, и любые права, принадлежащие администратору, будут утеряны. Рекомендуется ни в коем случае не удалять пользователя администратор.

Примечание по правами и инструментальным средствам
Право администратора жестко связано с утилитой **Пользователи**. Если у пользователя нет права администратора, это инструментальное средство не будет отображаться на консоли.

Все утилиты в продукте консоли ассоциированы с соответствующими правами (описывается далее).

Обнаружение устройств

Права на обнаружение устройств предоставляют пользователю следующие возможности:

- Поиск в сети устройств, которые не предоставили данные сканирования инвентаризации в базу данных главного сервера продукта, одним из следующих способов: сканирование сети, обнаружение стандартного агента управления, обнаружение IPMI.
- Планирование периодического поиска.
- Перемещение устройств из списка "Обнаруженные" в список "Управляемые".

Управление общими запросами

Права на управление общими запросами предоставляют пользователю следующие возможности:

- Создание запросов, доступных всем пользователям.
- Создание или удаление общих запросов.
- Изменение/правка существующих общих запросов.

Отчеты

Права на отчеты предоставляют пользователю следующие возможности:

- Просмотр и доступ к инструментальному средству **Отчеты** в левой навигационной панели.
- Запуск типовых отчетов.

Управление исправлениями

Права на управление исправлениями являются специфическими для сканирования уязвимых мест. Дополнительную информацию см. в разделе "Использование средства обновления программного обеспечения".

Основная web-консоль

Право на основную web-консоль дает пользователям возможность использовать функции, связанные с данным правом. Эти функции перечислены ниже вместе с исключениями для каждой из них.

- **Мои устройства** (право не позволяет обновлять открытые группы или удалять устройства на вкладке **Действия**).
- Изменение предпочтений (но не выборочных атрибутов).

Предупреждения и мониторинг

Право на предупреждения и мониторинг предоставляет пользователю следующие возможности:

- Контроль работы различных систем и компонентов ОС, таких как диски, процессоры, память, процессы, скорость передачи информации через системный web-сервер и т.п.
- Запись точного состояния всех управляемых устройств.
- Сортировка отправляемых предупреждений по степени важности (Критическое, Предупредительное, Информационное, ОК, Неизвестно) или по предельному значению (например, если жесткий диск занят более чем на 90%).
- Выбор действия, которое будет производиться, если значение предупреждения превысит предельное значение (путем добавления информации в журнал, отправления электронного сообщения, запуска программы на главном сервере или на отдельном устройстве или отправки предупреждения SNMP на консоль управления SNMP по сети).

Добавление пользователей продукта

Пользователи продукта - это пользователи, которые могут зарегистрироваться на консоли продукта и выполнить определенные задания для определенных устройств в сети.

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 на главном сервере. В группе **Пользователи** отображаются все пользователи, которые в данный момент включены в группу LANDesk Management Suite в главном сервере.

В группе **Пользователи** существует два пользователя по умолчанию:

- **Шаблон пользователя по умолчанию.** Данный пользователь обычно содержит шаблон свойств (права и область), который используется для настройки новых пользователей при их добавлении в группу LANDesk Management Suite. Другими словами, когда пользователь добавляется в эту группу в среде Windows, ему назначаются права и область, определенные в свойствах пользователя шаблона по умолчанию. Если в шаблоне пользователя по умолчанию выбраны все права и все области машин по умолчанию, любой 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 поменять свойства параметров для шаблона пользователя по умолчанию, щелкнув его правой кнопкой и выбрав **Редактировать права доступа**. 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 шаблона пользователя по умолчанию, а затем уже добавьте пользователей в группу LANDesk Management Suite (инструкции см. ниже).

  Пользователь шаблона по умолчанию не может быть удален.

- **Администратор по умолчанию.** Это административный пользователь, который зарегистрировался в сервере при установке этого продукта главного сервера.

При добавлении пользователя в группу LANDesk Management Suite в Windows данный пользователь автоматически помещается в группу **Все пользователи** в окне **Пользователи** с предоставлением тех же прав и области, которые установлены в шаблоне пользователя по умолчанию. Будут отображены имя пользователя, область и права.

Если вы удалите пользователя из группы LANDesk Management Suite в окружении пользователей Windows, пользователь более не будет активен и может быть удален из списка **Пользователи**. Учетная запись пользователя остается в вашем сервере и может быть снова добавлена в группу LANDesk Management Suite в любое время. Кроме того, подгруппы пользователей в списке **Устройства пользователя**, **Запросы пользователя**, **Отчеты пользователя** и **Сценарии пользователя** сохраняются таким образом, что вы можете восстановить пользователя без потери данных о нем, а также копировать данные для других пользователей.

Для обновления списка **Пользователи** с целью отображения вновь добавленных пользователей, выберите **Пользователи**, а затем щелкните кнопку **Обновить** в вашем браузере.

Добавление группы пользователей или доменов в группу LANDesk Management Suite

1. Найдите служебную программу сервера **Администрирование | Управление компьютером | Локальные пользователи и группы | Группы**.
2. Щелкните правой кнопкой мыши **Группа LANDesk Management Suite**, а затем выберите **Добавить в группу**.
3. Щелкните **Добавить**, затем введите или выберите пользователя (или пользователей) из списка.
4. Нажмите **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 в Windows, вы должны сначала создать их на сервере.

Создание новой учетной записи пользователя

1. Найдите служебную программу сервера **Администрирование | Управление компьютером | Локальные пользователи и группы | Пользователи**.
2. Щелкните правой кнопкой мыши **Пользователи**, а затем выберите **Новый пользователь**.
3. В диалоговом окне "Новый пользователь" введите имя и пароль.
4. Укажите параметры пароля.
5. Щелкните **Создать**. Диалоговое окно "Новый пользователь" остается открытым для того, чтобы вы могли создать дополнительных пользователей.
6. Щелкните **Закрыть**, чтобы выйти из диалогового окна.
7. Добавьте пользователя в группу LANDesk Management Suite, чтобы он появился в группе "Пользователи" на консоли.

Теперь вы можете назначить пользователям продукта права и область действия.

Создание областей

Область действия определяет устройства, которые пользователь может видеть и которыми он может управлять. Если вы установили несколько продуктов управления LANDesk, области действия можно присвоить пользователям с любой консоли, и они эффективны на всех консолях.

Область действия может быть большой или маленькой, по вашему усмотрению, при этом может выполняться сканирование всех управляемых устройств в базу данных, или только одного устройства, или не выполняться сканирование ни одного из устройств. Эта гибкость в комбинации с модульным доступом к инструментальным средствам делает администрирование на основе ролей такой универсальной функцией управления.

Области действия по умолчанию

Администрирование на основе ролей включает в себя две области действия по умолчанию. Эти две стандартные области могут быть полезны при конфигурации свойств пользователей с использованием шаблона пользователя по умолчанию.

- **(По умолчанию) Область "Нет компьютеров".** Исключает все устройства в базе данных.
- **(По умолчанию) Область "Все компьютеры".** Включает все устройства в базе данных.

Области действия "по умолчанию" нельзя исправить или удалить.

Выборочные области действия

Вы может создавать следующие типы выборочных областей действия и назначать их пользователям.

- **Область действия на основе запроса.** Эта область контролирует доступ только к устройствам, соответствующим параметрам поиска выборочного запроса. Вы можете выбрать существующий запрос или создать новые запросы для определения области действия в диалоговом окне **Запрос**. Для получения информации о создании запросов см. раздел "Создание запросов баз данных".
- **Область действия на основе группы.** Эта область контролирует доступ только к тем устройствам, которые расположены в выбранной группе. Для определения области действия можно выбрать группы в диалоговом окне **Свойства области действия группы**.

Любому пользователю можно назначить несколько областей действия. Если пользователю назначаются несколько областей действия, то общая эффективная область (т.е. полный набор устройств, к которым имеется доступ и которыми можно управлять в результате комбинации назначенных областей) является одним целым.

Изменять эффективную область действия можно, добавляя или удаляя области в любое время. Любые типы областей можно использовать одновременно.

Создание области действия

1. В левой навигационной панели выберите **Пользователи**.
2. На вкладке **Область действия** нажмите кнопку **Новая область действия запроса** или **Новая область действия группы** на панели инструментов.
3. Введите имя для новой области действия.
4. При выборе области действия на основе запроса выберите существующий запрос или нажмите **Определить** для создания нового запроса. Нажмите **OK**.
5. При выборе области действия на основе группы выберите группу, а затем нажмите **OK**.
6. Щелкните **OK** для сохранения области действия и закройте диалоговое окно.

Назначение прав и областей для пользователей

После того как вы добавили пользователей продукта, ознакомились с правами и с тем, как они контролируют доступ к свойствам и инструментальным средствам, и создали области действия устройств для разрешения или ограничения доступа к управляемым устройствам, следующим шагом в задании условий администрирования на основе ролей будет предоставление соответствующих прав и области действия для каждого пользователя.

Вы можете изменять права пользователей и область действия в любое время.

При изменении прав пользователей или области действия изменения вступают в силу при последующей регистрации пользователя на консоли.

Предоставление пользователям прав и области действия

1. В левой навигационной панели выберите **Пользователи**.
2. Раскройте список пользователей для просмотра всех пользователей, являющихся в настоящее время членами группы LANDesk Management Suite в среде Windows NT главного сервера.

   Данный список отображает имена пользователей и предоставленные им права (право разрешено или активно, если помечено флажком).

3. Щелкните правой кнопкой мыши имя пользователя, а затем выберите **Правка**.
4. В диалоговом окне **Права пользователя/область действия** отметьте или удалите права по желанию.
5. Нажмите вкладку **Область** и выберите область действия из списка **Назначенные области**.
6. Нажмите **Применить**.

Новые права отображаются рядом с именем пользователя в списке и вступят в силу при следующем подключении пользователя к главному серверу.

Удаление области действия

1. В левой навигационной панели выберите **Пользователи**.
2. На вкладке **Область** выберите область действия, которую вы хотите удалить, и нажмите **Удалить**. Нажмите **OK**.

Будьте осторожны при удалении областей действия. Пользователи, которым они были назначены, получат права, ранее запрещенные областью действия.

Диалоговое окно "Права пользователей / область действия"

Используйте данное диалоговое окно для просмотра и изменения прав и области действия, назначенных пользователю. Откройте диалоговое окно, выбрав пользователя и щелкнув **Правка**.

Вкладка "Права". Отображает права, назначенные пользователю.

- **Администратор**
- **Обнаружение устройств**
- **Управление общими запросами**
- **Отчеты**
- **Управление исправлениями**
- **Основная web-консоль**
- **Предупреждения и мониторинг**

Вкладка "Область". Отображает области действия, назначенные пользователю.

- **Назначенные области.** Идентифицирует области действия пользователя в настоящее время.
- **Добавить.** Открывает диалоговое окно **Добавить область действия** для выбора области действия и добавления ее пользователю.
- **Удалить.** Удаляет выбранные области действия.
- **Отмена.** Закрывает диалоговое окно без сохранения изменений.

Обнаружение устройств

Использование обнаружения устройств

При обнаружении устройств в вашей сети выявляются те устройства, в которых не установлены агенты и которые не предоставили информации о сканировании инвентаризации в базу данных главного сервера. Существуют различные способы обнаружения устройств в вашей сети.

- **Сканирование сети.** Поиск компьютеров с помощью эхо-теста ICMP. Данный поиск является самым основательным, но, в то же время не является достаточно быстрым (если используется определение IP-отпечатков). Вы можете ограничить поиск по определенному IP-адресу и по диапазонам подсети. По умолчанию данный параметр использует NetBIOS для сбора информации об устройстве. Вы также можете выбрать параметр "Отпечатки IP", который определяет тип ОС (в большинстве случаев). В настройках сканирования сети также есть параметр **Использовать SNMP**, который можно использовать для конфигурации сканирования с использованием SNMP для устройств, например, принтеров.
- **Обнаружение CBA.** Поиск стандартного агента управления в компьютерах (ранее известен как агент common base [CBA] в Management Suite). Эта функция выполняет поиск компьютеров, управляемых из Server Manager, System Manager и т.д. Можно выбрать параметр PDS2 для обнаружения устройств со старой версией агента LANDesk PDS2. 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 интерфейсом Intelligent Platform Management Interface, позволяющим доступ к к контроллеру BMC, независимо от того, включен ли сервер или выключен, а также независимо от состояния ОС.
- **Корпус сервера.** Поиск модулей управления корпуса blade-сервера (CMM). Blade-серверы в корпусе сервера обнаруживаются как обычные серверы.
- **Intel* AMT.** Поиск устройств с технологией Active Management Technology (версия 1), позволяющим доступ к ограниченному числу функциям управления, независимо от того, включен ли сервер или выключен, а также независимо от состояния ОС.

Во время обнаружения устройств производится попытка получения основной информации о каждом устройстве. Приведенная ниже информация действительна не для всех устройств.

- **Имя узла.** Имя обнаруженного устройства (если доступно).
- **IP-адрес.** Обнаруженный IP-адрес.
- **Маска подсети.** Обнаруженная маска подсети.
- **Категория.** Группа обнаружения, к которой принадлежит устройство.
- **Имя ОС.** Описание обнаруженной ОС (если доступно).

При первом обнаружении устройства система обнаружения обращается в базу данных главного сервера для проверки наличия в списке базы данных **Мои устройства** IP-адреса и имени этого устройства. Для устройства, находящегося в списке **Неуправляемые**, будет выполнено повторное обнаружение и также получена дополнительная информация. Если

данные совпадают, система обнаружения игнорирует данное устройство. Если данные не совпадают, система обнаружения добавляет данное устройство в таблицу **Неуправляемые**. Устройства в таблице **Неуправляемые** не используют лицензию System Manager. Устройство считается управляемым, если осуществляется сканирование его инвентаризации в базе данных главного сервера. После перемещения устройства в группу **Все устройства**, данное устройство перестает отображаться в списке **Обнаруженные устройства**.

Устройства IPMI должны иметь контроллер BMC (Baseboard management controller), который конфигурируется с целью обнаружения устройств IPMI и полного функционального использования IPMI. Если контроллер BMC не сконфигурирован, устройство обнаруживается как компьютер. Вы можете затем добавить это устройство в список управляемых устройств и запустить функцию конфигурации оборудования для конфигурирования пароля BMC. Данное приложение определит функциональность устройства IPMI. Помните, что IP-адрес контроллера BMC может отличаться от IP-адреса операционной системы, поэтому, будет невозможно выполнить непосредственную установку агента на IP-адрес BMC. Повторный поиск по стандартным IP-адресам может быть необходим для получения стандартного агента по IP-адресу контроллера BMC. IP-адрес BMC IP может использоваться для получения агента.

Устройства, имеющие поддержку Intel* AMT (версия 1), должны быть сконфигурированы с именем Intel AMT и паролем для реорганизации и повторного обнаружения в качестве устройств Intel AMT. После обнаружения можно использовать функцию конфигурации оборудования для настройки Intel AMT и идентификации устройства в режиме малого бизнеса или в защищенном корпоративном режиме.

Для автоматизации обнаружения устройств вы можете запланировать периодический запуск обнаружения. Например, можно разделить сеть на подсети и запланировать на каждую ночь эхо-тест для разных подсетей. Все виды обнаружения осуществляются главным сервером.

Для обнаружения устройств сети и управления ими выполните следующие действия:

- Создайте конфигурации обнаружения
- Запланируйте и выполните обнаружение
- Просмотрите обнаруженные устройства
- Переместите обнаруженные устройства в список **Мои устройства**

Использование обнаружения неуправляемых устройств с помощью устройств брандмауэра

Обратите внимание, что при обнаружении неуправляемых устройств не выявляются устройства, использующие брандмауэр, например, брандмауэр Windows, кроме случаев, когда производилась ручная настройка брандмауэра. Вы должны открыть следующие порты. Для изменения этих настроек перейдите к функции конфигурации брандмауэра Windows, используя для этого Панель управления Windows.

Управляемые серверы:

- Совместное использование файлов и принтеров. TCP 139, 445; UDP 137,138 (принудительная отправка программного обеспечения без этого не работает).

- Распространение ПО. TCP 9595 (принудительная отправка программного обеспечения без этого не работает).
- Дополнительно - ICMP. "Разрешить входящие эхо-запросы" (невозможно обнаружить, если этот параметр отключен).

Главный сервер:

- Инвентаризация. 5007
- Дистанционное управление: 9535

Создание конфигураций обнаружения

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 описательного 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 полным, и 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. Дополнительную информацию см. в разделе Конфигурация сканирования 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 разрешить 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. Обзор IPMI см. в разделе Поддержка IPMI.
- **Корпус сервера.** Поиск модулей управления корпуса blade-сервера (CMM). Blade-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 IP-адрес для диапазона адресов, которые необходимо просканировать.
- **Маска подсети.** Введите маску подсети для диапазона адресов IP, которые необходимо просканировать.
- **Добавить.** Добавляет диапазоны IP-адресов 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.

Правка или удаление конфигурации

- На вкладке **Конфигурации обнаружения** выберите необходимую вам конфигурацию, затем нажмите **Правка** или **Удалить**.

Конфигурация сканирования SNMP

Во время сканирования сети можно использовать протокол SNMP. В зависимости от конфигурации SNMP в вашей сети, может потребоваться ввести дополнительную информацию в конфигурации обнаружения. Выберите **Конфигурация** рядом с параметром **SNMP** после чего отобразится диалог **Конфигурация SNMP**, содержащий следующие настройки:

- **Попытки.** Число попыток, которое функция обнаружения устройств пытается установить SNMP-подключение.
- **Ожидание ответа (сек.).** Время ожидания функции обнаружения устройств для ответа SNMP.
- **Порт.** Порт обнаружения устройств для выполнения SNMP-запросов.
- **Имя сообщества.** Имя SNMP-сообщества, используемое во время обнаружения устройств.
- **Конфигурация SNMP V3.** Функция обнаружения устройств также поддерживает SNMP V3. Нажмите эту кнопку для настройки параметров SNMP V3 в диалоге **Конфигурация SNMP V3**.

В диалоге **Конфигурация SNMP V3** есть три параметра:

- **Имя пользователя.** Имя пользователя, которое обнаружение устройств использует для аутентификации в удаленной службе SNMP.
- **Пароль.** Пароль для удаленной службы SNMP.
- **Тип аутентификации.** Тип аутентификации SNMP. Возможные значения: **MD5**, **SHA** или **Нет**.
- Тип **защиты.** Метод шифрования, используемый службой SNMP. Возможные значения: **DES**, **AES128** или **Нет**.
- Пароль **защиты.** Пароль, используемый с указанным типом защиты. Недоступен, если выбран тип защиты **Нет**.

Планирование и выполнение обнаружения

Используйте кнопку **Расписание** на вкладке **Конфигурации обнаружения** для отображения диалогового окна **Запланированные задачи**. Используйте данное диалоговое окно для планирования времени выполнения конфигураций обнаружения. Вы можете осуществить запуск конфигурации обнаружения немедленно, в определенный момент времени в будущем, запустить в соответствии с определенным графиком или однократно.

Задачи обнаружения можно перепланировать или удалить с вкладки **Задачи обнаружения**. После того, как вы запланировали поиск, см. вкладку **Задачи обнаружения** для определения статуса обнаружения. Вы также можете получить доступ к статусу задачи обнаружения с помощью утилиты **Запланированные задачи**. По завершении задачи

поиска новые устройства, которые еще не находятся в базе данных главного сервера, будут добавлены в категории "Обнаруженные устройства".

Диалоговое окно **Задача обнаружения** имеет следующие параметры.

- **Показать в общих задачах.** Обеспечивает просмотр задач пользователями. Во время редактирования или запуска задачи пользователь становится владельцем экземпляра задачи.
- **Владелец.** Владелец задачи.
- **Не планировать.** (по умолчанию). Оставляет задание в списке задач для дальнейшего планирования.
- **Запустить сейчас.** Запускает задание в ближайшее время. Для запуска задания может потребоваться до одной минуты.
- **Запустить в запланированное время.** Задача запускается в указанное вами время. При выборе данного параметра необходимо ввести следующие данные:
    - **Дата.** Назначаемая вами дата начала выполнения задания. В зависимости от вашего местонахождения дата устанавливается в формате день-месяц-год или месяц-день-год.
    - **Время.** Назначаемое вами время начала выполнения задачи.
    - **Повторять каждые.** Если вы хотите, чтобы данное задание повторялось, выберите частоту повторения (ежедневно, еженедельно или ежемесячно). Если вы выбрали "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 обнаружения

1. В левой навигационной панели выберите **Обнаружение устройств**.
2. На вкладке **Конфигурации обнаружения** выберите необходимую вам конфигурацию, затем нажмите **Расписание**. Настройте расписание обнаружения. После завершения щелкните **Сохранить**.
3. Следите за ходом процесса обнаружения на вкладке **Задачи обнаружения**.
4. После завершения процесса обнаружения просмотрите все результаты поиска в верхней части панели **Обнаруженные устройства**. Если дважды щелкнуть задачу обнаружения, то количество и процентное значение числа устройств будет равно нулю, так как эти величины связаны с целевыми устройствами, а задачи обнаружения не имели целей.

На вкладке **Задачи обнаружения** отображается состояние процесса обнаружения. Данное состояние включает в себя:

- Имя конфигурации обнаружения.
- Состояние задания, которое может быть следующим: "Идет обработка", "Все выполнено", "Ничего не выполнено", "Ошибка".
- Время последнего запуска задания.
- Тип выполняемого задания.

Удаление или переназначение обнаружения

Если вы хотите удалить задание из списка, независимо от того, выполняется оно или нет, выберите задание, затем нажмите **Удалить**. Если данное задание еще не запущено или является повторяющимся, его удаление предотвратит дальнейшее выполнение.

Вы можете также переназначить задание обнаружения в списке для повторного выполнения или для запуска в другое время, выбрав данное задание, затем выбрав **Правка**, затем **Расписание**, и переустановить расписание. Для немедленного выполнения задачи выберите ее и щелкните **Запустить сейчас**.

Просмотр состояния задачи обнаружения

1. В левой навигационной панели выберите **Обнаруженные устройства**.
2. Выберите вкладку **Задачи обнаружения** или щелкните **Обновить** на панели инструментов.

Просмотр обнаруженных устройств

В верхней панели **Обнаружение устройств** можно просмотреть все обнаруженные устройства. Эта панель отображает результаты всех заданий обнаружения, которые вы выполнили. При выполнении нового задания обнаружения любые найденные устройства добавляются в список.

Когда программа обнаружения находит устройство, она пытается определить его тип, чтобы добавить к одной из следующих категорий:

- **Корпус.** Содержит модули управления корпусами blade-серверов (CMM).
- **Компьютеры.** Содержит компьютеры. Системы Linux могут быть помечены как системы Unix в колонке **Название ОС**.
- **Инфраструктура.** Содержит маршрутизаторы и другое сетевое оборудование.
- **Intel AMT.** Содержит устройства с поддержкой Intel* Active Management Technology.
- **IPMI.** Содержит устройства с поддержкой IPMI.
- **Другое.** Содержит неопределенные устройства.
- **Принтеры.** Содержит принтеры.

Эти семь категорий позволяют организовать список **Обнаружение устройств** так, чтобы было легко находить интересующие вас устройства. Можно сортировать список устройств по любому заголовку, щелкнув на нужный заголовок. Устройства могут не всегда корректно распределяться по категориям. Если какое-либо устройство было неправильно идентифицировано, его можно легко переместить в правильную группу, нажав правой кнопкой мыши, затем выбрать **Переместить**, потом выбрать правильную категорию и снова нажать **OK**.

Иногда главный сервер может быть указан дважды. Это случается потому, что обнаружение некоторых машины выполняется с использованием других механизмов (например, CBA, IPMI, CMM, PDS1 и PDS2), и информация машины добавляется в базу данных с использованием этого механизма.

Как только вы развернули агенты на обнаруженном устройстве и устройство посылает сканирование инвентаризации в главный сервер, обнаруженное устройство удаляется из списка обнаруженных устройств.

Фильтрация списка устройств

Используя окно панели инструментов **Фильтровать по**, вы сможете найти устройства, соответствующие заданным вами критериям поиска. Вы можете установить фильтр по имени узла, IP-адресу, маске подсети, категории или имени ОС. При использовании фильтра устройства сортируются в алфавитном порядке по атрибуту фильтра, указанному вами.

Фильтрация списка устройств

1. В левой навигационной панели выберите **Обнаружение устройств**.
2. В дереве **Неуправляемые** выберите группу, которую вы хотите отфильтровать.
3. Для параметра **Фильтровать по** выберите атрибут, по которому вы хотите фильтровать. (Если параметр **Фильтровать по** не отображается, щелкните **>>**, чтобы развернуть его).
4. В окне рядом с атрибутом введите текст, по которому должна проводиться фильтрация.
5. Нажмите кнопку **Найти**.

Добавление категорий

Можно создавать категории устройств для группирования неуправляемых устройств. При перемещении устройства в другую категорию оно появится в этой группе снова, если программа обнаружения устройств найдет его позже. Перемещая в другие группы устройства, которыми вы не будете управлять с консоли, вам легче будет увидеть новые устройства в группе **Компьютеры**.

При удалении группы, содержащей устройства, программа обнаружения устройств перемещает эти устройства в группу **Другие**.

Добавление категории устройства

1. В окне просмотра **Обнаружение устройств** выберите **Добавить категорию**.
2. Введите имя группы в окне **Имя категории**, затем щелкните **OK**.
3. Для удаления добавленной категории выберите ее и щелкните **Удалить категорию**, а затем **OK** для подтверждения удаления.

Перемещение обнаруженных устройств в список "Мои устройства"

После обнаружения устройства можно переместить в список **Мои устройства**. В процессе перемещения информация устройств добавляется в базу данных. После того, как информация будет помещена в базу данных, вы можете развернуть конфигурацию агента, создать запросы и отчеты по ним, а также выполнить другие задачи управления.

Устройства , управляемые с помощью внеполосного управления (например, имеющие поддержку функциональности IPMI, Intel AMT или DRAC), могут также управляться без развертывания агента. После выбора такого управления информация устройства заносится в базу данных, а контроллер устройства BMC настраивается для использования функций внеполосного управления.

Перемещение обнаруженных устройств в список "Мои устройства"

1. В окне **Обнаружение устройств** выберите устройство, которое вы хотите переместить в список **Мои устройства**. Вы можете выбрать несколько устройств, используя стандартный метод (нажатая SHIFT + щелчок мыши или нажатая CTRL + щелчок мыши).
2. Нажмите кнопку **Цель**. Выбранные устройства будут отображены на вкладке **Целевой список**.
3. Выберите вкладку **Управление**.
4. Выберите **Переместить целевые устройства**.
5. Если устройство поддерживает внеполосное управление, и вы не хотите устанавливать в него агента управления, выберите **Управление внеполосными устройствами без агента**.
6. Нажмите кнопку **Переместить**.

Устройства будут удалены из списка неуправляемых устройств и появятся в списке **Все устройства**.

Если был выбран параметр внеполосного управления, можно просмотреть состояние процесса перемещения, выбрав вкладку **Состояние перемещения** в нижней части панели. Здесь также отображаются любые ошибки конфигурации. Для перемещения устройства, имеющего поддержку IPMI, в список **Мои устройства**, необходимо ввести верную идентификационную информацию для контроллера BMC в диалоге утилиты конфигурации служб, чтобы главный сервер мог выполнить аутентификацию в устройстве.

При перемещении модуля управления корпусом (CMM) в список **Мои устройства** он также отображается в списке **Все устройства** и, в качестве группы, в списке **Открытые группы**. Информация группы содержит сведения о CMM и о списке доступных отсеков блока в корпусе с именами blade-серверов, находящихся в этих отсеках. Blade-серверы также обнаруживаются и управляются как отдельные серверы.

Поиск устройств Intel* AMT

System Manager включает параметр поиска устройств, сконфигурированных с технологией Intel* Active Management Technology (Intel* AMT) версии 1. Обнаружение устройств в качестве устройств с поддержкой Intel AMT возможно только после открытия на устройстве экрана настройки Intel AMT и изменения установленного производителем пароля по умолчанию на безопасный пароль. (Для получения информации о доступе к экрану настройки Intel AMT см. документацию к устройству.) Если этого не сделать, поиск устройств будет выполняться, но они не будут идентифицироваться в качестве устройств с поддержкой Intel AMT, и нельзя будет просмотреть сводку инвентаризации в полном объеме.

Устройства с поддержкой Intel AMT версии 2 не могут быть обнаружены во время этого процесса. После ввода идентификаторов и IP-адреса главного сервера, введенных на экране конфигурации Intel AMT, поиск устройств будет выполняться автоматически. См. раздел Конфигурация устройств Intel AMT для получения подробной информации о работе с версией 2.

Обнаружение устройств Intel ® AMT

1. В левой навигационной панели выберите **Обнаружение устройств**.
2. Выберите **Новая**, чтобы создать новую конфигурацию и введите ее имя. Или выберите существующую конфигурацию и нажмите **Правка**, чтобы изменить ее.
3. Проверьте параметр **Обнаружить устройства Intel AMT**.
4. Введите начальный и конечный IP-адреса диапазона сканирования и укажите маску подсети.
5. Нажмите **Добавить**, а затем **OK**.
6. Выберите конфигурацию и нажмите **Расписание**. Установите параметры расписания или нажмите **Запустить сейчас**, а затем **Сохранить**.
7. Для просмотра процесса сканирования выберите вкладку **Задачи обнаружения**.

AMT-сконфигурированные устройства отображаются в папке с именем **Intel AMT**. В этой папке можно выбрать устройство и переместить его в список управляемых устройств.

Чтобы добавить устройство в базу данных главного сервера для последующего управления им, необходимо, чтобы имя пользователя/пароль для устройства соответствовали имени пользователя/паролю, сохраненному утилитой конфигурации служб, что позволяет System Manager аутентифицироваться в устройстве. После сохранения конфигурации пароля в утилите конфигурации служб, последняя хранит эту информацию в базе данных главного сервера, чтобы System Manager продолжал аутентифицироваться в устройствах Intel AMT.

Если вы используете устройства Intel AMT с различной идентификационной информацией, перед их управлением нужно обеспечить соответствие их учетных данных, информации хранимой утилитой конфигурации служб.

Если система Intel AMT обнаружена и перенесена в список **Мои устройства**, она автоматически идентифицируется с использованием режима, который был выбран в утилите конфигурации служб. Режим малого бизнеса позволяет использовать основные функции управления без служб сети infrastructure и незащищенной сети, а корпоративный режим разработан для больших предприятий и обеспечивает безопасную работу на основе таких сетевых служб, как DHCP, DNS и служба центров сертификации TLS.

Если главный сервер использует прокси-сервер, для обнаружения устройств Intel AMT он должен поддерживать аутентификацию цифрового доступа.

Конфигурация пароля Intel AMT

1. Выберите **Пуск | Все программы |** LANDesk **| Конфигурация служб**. Выберите вкладку **Конфигурация Intel AMT**.

2. Введите имя текущего пользователя и пароль. Они должны соответствовать имени и паролю, сконфигурированным на экране конфигурации Intel AMT (доступен в настройках BIOS) для управления устройствами Intel AMT.
3. Для изменения имени и пароля заполните раздел **Новый пароль Intel AMT**.
4. Выберите режим (**малый бизнес** или **корпоративный**), который нужно использовать для идентификации устройств после добавления их в базу данных главного сервера для управления.
5. Нажмите **OK**. Данное изменение вступит в силу после запуска конфигурации клиента.

Перемещение обнаруженных устройств Intel AMT в список управляемых устройств

1. Выберите одно или несколько устройств из списка неуправляемых устройств.
2. На панели задач нажмите кнопку **Цель**.
3. Нажмите кнопку **Управление** в нижней части панели, затем **Переместить целевые устройства** и щелкните **Переместить**.

   Если все устройства, которые необходимо переместить, находятся в списке, выберите их, нажав в нижней панели кнопку **Управление**, затем выберите **Переместить целевые устройства**, а затем **Переместить**.

Устройство будет перемещено из списка неуправляемых устройств и появится в списке **Все устройства**. Помните, что когда вы перемещаете устройства из списка **Мои устройства**, процедура аутентификации Intel AMT запускает несколько фоновых процессов. В это время вы можете продолжать выполнять другие задачи обнаружения или управления.

Дополнительную информацию об управлении устройствами Intel AMT см. в разделах Управление устройствами Intel* AMT и Поддержка Intel* AMT.

Установка и конфигурация агента устройства

Обзор установки и конфигурации агента устройства

Чтобы управлять устройствами на консоли, необходимо установить на них агенты управления. Вы можете выбрать между установкой конфигурации агентов по умолчанию (которая устанавливает все агенты продукта) или настроить ваши собственные конфигурации агентов для установки на ваших устройствах. При установке System Manager агенты не устанавливаются автоматически на главное устройство; необходимо вручную установить агенты на главное устройство, а затем перезагрузить его. Конфигурация агентов должна включать агент мониторинга для получения предупреждений о состоянии устройства.

Вы можете установить агенты управления с помощью одного из описанных далее способов.

- Развертывание агентов. Выберите устройства в списке **Мои устройства**, а затем запланируйте задание конфигурации агентов для удаленной установки агентов на устройствах.
- Установка агентов с помощью пакета установки. Создайте самораспаковывающийся пакет установки устройства. Для установки агентов запустите этот пакет локально на устройстве. Это необходимо сделать, войдя в систему с правами администратора.
- Извлечение агента. Откройте общую папку главного сервера ldlogon (//*имя_сервера*/ldlogon) и запустите SERVERCONFIG.EXE.
- Вручную на устройствах с портативным устройством порта USB (см. раздел Установка агентов с пакетом установки).

Другой ресурс для установки и конфигурации агента - это глава Обнаружение устройств в *руководстве пользователя*.

Примечание. Вы можете установить конфигурацию устройства по умолчанию, выбрав конфигурацию на странице **Конфигурация агента** и щелкнув **Установить по умолчанию**. Конфигурация "IPMI только BMC" не может использоваться по умолчанию. Конфигурации по умолчанию не могут быть удалены.

В системах Windows для обеспечения полной функциональности продукта необходимо вручную сконфигурировать следующие параметры порта брандмауэра. Для изменения этих настроек перейдите к функции конфигурации брандмауэра Windows, используя для этого Панель управления Windows.

Управляемые серверы:

- Совместное использование файлов и принтеров. TCP 139, 445; UDP 137,138 (принудительная отправка программного обеспечения без этого не работает).

- Распространение ПО. TCP 9595 (принудительная отправка программного обеспечения без этого не работает).
- Дополнительно. ICMP - "Разрешить входящие эхо-запросы" (невозможно обнаружить, если этот параметр отключен).

Главный сервер.

- Инвентаризация. 5007
- Дистанционное управление: 9535

Для выполнения нажмите **Пуск** | **Панель управления** | **Безопасность**.

Обновление существующих агентов

Вы можете отправить конфигурации агентов в свои устройства, даже если стандартные агенты управления и агенты удаленного управления еще не существуют. См. раздел Настройка служб и идентификационной информации в *руководстве пользователя* для получения сведений о настройке идентификационной информации.

Как только вы установили пакет агентов, предыдущий пакет удаляется и устанавливается новый. Вы можете удалить агента, создав новый пакет агентов, не содержащий агента, который вы хотите удалить.

Удаление агентов

Если вам необходимо удалить агенты с сервера, выполните следующую процедуру.

Внимание! По умолчанию модуль Uninstallwinclient.exe перезагружает устройство после удаления агентов, если не будет использован параметр командной строки **/noreboot**. Перезагрузка необходима для завершения процесса удаления. Если выдана команда перезагрузки, сервер будет перезагружен без специального уведомления, а все приложения будут принудительно закрыты. Параметр /noreboot позволяет продолжить работу сервера без перезагрузки.

Удаление агентов с сервера

1. Выполните вход в сервер с правами администратора.
2. Назначьте диск в общий каталог главного сервера **ldmain**.
3. Откройте окно командной строки, измените букву устройства папки ldmain и введите следующую команду:

   ```
   uninstallwinclient.exe /noreboot
   ```

Удаление всех агентов будет выполнено без выдачи запроса на подтверждение.

Вы также можете выбрать **Пуск** > **Выполнить** > ***главный_сервер*\ldmain\uninstallwinclient.exe /noreboot**.

Удаление агентов с сервера Linux

1. Скопируйте файл linuxuninstall.tar.gz во временный каталог устройства Linux. Его можно найти в общей папке главного сервера ManagementSuite.

   В системе Linux может быть не установлена/настроена служба Samba, поэтому, вы не сможете выполнить прямое копирование; это может быть сделано с помощью команды pscp на главном сервере, копированием файла в папку ldlogon или копированием на съемный носитель.
2. Из командной строки оболочки (на машине Linux) распакуйте этот файл, используя параметры tar и x, z и f.

   ```
   tar -xzf linuxuninstall.tar.gz
   ```
3. После распаковки файла запустите из командной строки оболочки сценарий linuxuninstall (из текущего каталога):

   ```
   ./linuxuninstall.sh
   ```

Конфигурация агентов

Перед тем, как начать полное управление устройствами на консоли, необходимо установить на них агенты управления. Во время установки System Manager агенты ядра не устанавливаются автоматически; необходимо вручную установить агентов главного сервера, а затем перезагрузить его. Независимо от того, используете ли вы одну из конфигураций агента по умолчанию или создаете конфигурацию агента на консоли, вы можете установить ее на устройства с операционными системами Windows или Linux, используя один из трех способов:

- Выберите устройства в списке **Мои устройства**, а затем запланируйте задание конфигурации агентов для удаленной установки агентов на устройствах.
- Создайте самораспаковывающийся пакет установки. Для установки агентов запустите этот пакет локально на устройстве. Это необходимо сделать, войдя в систему с правами администратора. Для получения дополнительной информации см. раздел Установка агентов с помощью пакета установки.
- На устройстве Windows откройте общую папку главного сервера ldlogon (*myserver*\ldlogon) и запустите SERVERCONFIG.EXE.

Создание конфигурации агента

1. В левой навигационной панели выберите **Конфигурация агента**.
2. Щелкните **Новый**.
3. Введите имя новой конфигурации в диалоге **Имя конфигурации**.

   Введите имя, описывающее используемую конфигурацию. Это может быть уже существующее имя конфигурации или новое имя.

4. Выберите платформу для конфигурации.

5. Выберите тип установки для конфигурации (выбираемый пользователем или только IPMI BMC). Выберите **IPMI только BMC** в диалоге **Конфигурация** для конфигурации контроллера BMC на устройствах с поддержкой IPMI (см. примечание далее в действии 9).

   Конфигурация "IPMI только BMC" выполняет настройку контроллера BMC для внеполосного доступа, и осуществляет полное сканирование инвентаризации, а затем удаляет себя. Конфигурация "IPMI только BMC" не может устанавливаться по умолчанию. Во время создания конфигурации "IPMI только BMC" помните, что большинство редактируемых параметров, описываемых в следующих действиях, недоступны.

6. Выберите только что созданную конфигурацию и щелкните **Правка**.

   На вкладках некоторые параметры недоступны, потому что они не являются настраиваемыми для выбранной вами конфигурации.
7. На вкладке **Агент** выберите агентов, которые вы хотите развернуть.

   - **Все.** На выбранное устройство устанавливаются все агенты.
   - **Стандартный агент управления.** Создает основы коммуникаций между устройством и главным сервером. Этот агент обязателен (за исключением конфигураций "IPMI только BMC"). Большинство процессов в таких агентах выполняются по требованию.
   - **Обновления программного обеспечения.** Устанавливает сканер обновлений программного обеспечения. После установки этого агента можно сконфигурировать работу сканера. Данный агент не является агентом, работающим по требованию.
   - **Мониторинг.** Установка агента мониторинга на выбранный сервер. Агент мониторинга поддерживает множество типов мониторинга, включая мониторинг ASIC, внутриполосные и внеполосные IPMI и CIM. Данный агент не является агентом, работающим по требованию.
   - **Active System Console.** Устанавливает агент, который предоставляет доступ к консоли Active System Console с System Manager через интерфейс или меню. Этот агент поддерживается только на устройствах с системными платами Intel.

8. В окне типов **Конфигурации** системы выберите тип. Если данный параметр недоступен, значит, вы уже выбрали этот тип.

9. Выберите параметр **Перезагрузка**.

   Перезагрузка вручную означает, что после установки не произойдет перезагрузка устройств. Перезагрузка устройства не является обязательной после конфигурации агентов. Вы должны вручную перезагрузить устройство.

   Перезагрузка по необходимости вызывает перезагрузку обновлений агента, когда файлы обновлений блокированы.

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 устройству.
- **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. Сканер может быть запущен вручную на управляемом сервере; он может быть запущен из меню Пуск | Все программы | Управление LANDesk | Сканер инвентаризации. В системе Linux нужно зарегистрироваться с именем root и в командной строке выполнить следующую команду: `/usr/LANDesk/ldms/ldiscan -ntt`

    - **Всегда выполнять при запуске.** Запускает сканер инвентаризации при запуске устройства. Если вы создаете конфигурацию HP-UX, эта кнопка будет недоступна, так как сканер HP-UX настроен для запуска сценария службы cron, которая будет выполняться ежедневно, еженедельно или ежемесячно. Эта настройка недоступна для изменения.
    - **Время запуска.** Укажите диапазон часов, в течение которых будет работать сканер. 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 инвентарные сканирования устройств проходили поочередно, и они не посылали результаты сканирования одновременно.
    - **Повторять каждые.** Введите число, которое представляет приращение (например, 1, 2 или 3), и единицы измерения (минуты, часы или дни).
    - **Ограничения.** Ограничивает доступные дни и время работы сканера инвентаризации. Выберите **Время дня**, **День недели** или **День месяца**, а затем введите включающие параметры. Например, введите 10 для **дня месяца** и 1:00 AM и 3:00 AM для **времени дня** и включения сканера инвентаризации 10-го числа каждого месяца в период с 1:00 ночи до 3:00 утра.

11. На вкладке **Обновления программного обеспечения** установите дни и часы работы сканера инвентаризации. Сканер будет запускаться автоматически без необходимости планирования задачи.
    - **Всегда выполнять при запуске.** Запускает сканер инвентаризации при запуске устройства.

- **Время запуска.** Укажите диапазон часов, в течение которых будет работать сканер. Если устройство регистрируется на сервере в промежуток времени, который вы указали, сканирование обновлений программного обеспечения запускается автоматически. Если устройство уже зарегистрировано на сервере, то как только подходит время сканирования, сканер обновлений программного обеспечения запускается автоматически. Данный параметр полезен, если вы хотите, чтобы сканирования на устройствах проходили поочередно, и они не посылали результаты сканирования одновременно.
- **Повторять каждые.** Введите число, которое представляет приращение (например, 1, 2 или 3), и единицы измерения (минуты, часы или дни).
- **Ограничения.** Ограничивает доступные дни и время работы сканера обновлений программного обеспечения. Выберите **Время дня**, **День недели** или **День месяца**, а затем введите включающие параметры. Например, введите 10 для **дня месяца** и 1:00 AM и 3:00 AM для **времени дня** и включения сканера инвентаризации 10-го числа каждого месяца в период с 1:00 ночи до 3:00 утра.

12. 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. Новые наборы правил могут быть созданы в разделах **Мониторинг** или **Предупреждения**. Чтобы вновь созданные наборы правил отображались в ниспадающем списке, вы должны создать файл XML для выборочного набора правил.
13. Для сохранения информации в базе данных выберите **Сохранить изменения**. Щелкните **Сохранить файл как**, чтобы сохранить конфигурацию как пакет распределения.

Примечание. Вы можете установить конфигурацию агентов по умолчанию, выбрав конфигурацию на странице **Конфигурации агента** и щелкнув **Установить по умолчанию**. Конфигурации по умолчанию не могут быть удалены.

Планирование заданий конфигураций агентов

1. В левой навигационной области выберите **Конфигурация агента**.
2. Выберите конфигурацию агента и нажмите **Назначить задачу**.
3. Отредактируйте список целевые устройства и расписание заданий.
4. Нажмите **Сохранить**.

Когда вы выбираете параметр **Назначить задачу**, создается задача (она не имеет целевого устройства и не запланирована). Если задача конфигурации агента будет отменена без сохранения, помните, что она все еще будет находится в списке **Задачи** и иметь состояние "Не запланировано". Она может быть удалена из списка **Мои задачи**.

После завершения задачи конфигурации агента необходимо перезагрузить устройство для отображения сведений об устройстве на консоли (см. раздел Просмотр информационной консоли сервера). Перезагрузка также необходима после установки агента в главном сервере и в управляемых устройствах. Процесс конфигурации агента позволяет отложить перезагрузку, чтобы не прерывать текущее использование сервера.

Развертывание агентов на управляемых серверах

Как только вы обнаружили устройства, можно развернуть на них агентов. Можно развертывать агентов только на устройствах с ОС Windows, Linux и HP-UX. Вы должны иметь права администратора для развертывания агентов в устройствах Windows и привилегии пользователя root для конфигурации устройств Linux и HP-UX.

Вы можете развертывать агенты в неуправляемых устройствах одним из указанных способов.

- Развертывание методом получения использует процесс обнаружения и учетную запись администратора домена, сконфигурированную для службы планировщика, которая обрабатывает результаты обнаружения. Учетная запись администратора домена предоставляет службе планировщика права, которые ему необходимы для установки агентов сервера. Это подходит для серверов семейства Windows NT.
- При развертывании принудительным методом используется стандартный агент управления. Если в серверах установлен стандартный агент управления, используемый многими программными продуктами LANDesk, вы можете проводить на них развертывание, не требуя учетной записи администратора домена.

При развертывании на обнаруженных устройствах используйте утилиту **Фильтровать по** в дереве **Неуправляемые**. Вы можете фильтровать по IP-адресу, чтобы изолировать устройства.

В системах Windows для обеспечения полной функциональности продукта необходимо вручную сконфигурировать следующие параметры порта брандмауэра. Для изменения этих настроек перейдите к функции конфигурации брандмауэра Windows, используя для этого Панель управления Windows.

Управляемые серверы.

- Совместное использование файлов и принтеров. TCP 139, 445; UDP 137,138 (принудительная отправка программного обеспечения без этого не работает).
- Распространение ПО. TCP 9594, 9595 (принудительная отправка программного обеспечения без этого не работает).
- Дополнительно - ICMP. "Разрешить входящие эхо-запросы" (невозможно обнаружить, если этот параметр отключен).

Главный сервер.

- Инвентаризация. 5007
- Дистанционное управление: 9535

Конфигурация идентификационной информации устройства

Неуправляемые устройства с установленным стандартным агентом управления не требуют идентификационную информацию для развертывания агентов. Для установки агентов на серверы с ОС Windows, на которых нет стандартного агента управления, укажите

идентификационные данные, которые служба планировщика будет использовать в устройстве консоли для получения необходимых прав доступа.

Для установки агентов устройства на неуправляемых устройствах, служба планировщика должна иметь возможность подключаться к устройствам, используя учетную запись администратора. По умолчанию служба планировщика использует учетную запись LocalSystem. Идентификационная информация LocalSystem обычно работает с устройствами, которые не принадлежат домену.

Если устройства принадлежат домену, вы должны указать учетную запись администратора домена. Если вы конфигурируете неуправляемые устройства в нескольких доменах, нужно конфигурировать по одному домену за раз, так как служба планировщика аутентифицируется с одним набором идентификационной информации, и каждому домену необходима отличная от других учетная запись администратора.

На главном сервере есть утилита конфигурации служб, которую можно использовать для настройки параметров инвентаризации. Данная утилита работает только на главном сервере.

Конфигурация идентификационной информации при регистрации службы планировщика

1. Для запуска утилиты конфигурации служб на главном сервере щелкните **Пуск | Программы |** LANDesk **| Конфигурация служб**.
2. Выберите вкладку **Планировщик**.
3. Нажмите кнопку **Смена имени**.
4. Введите идентификационную информацию, которую данная служба должна использовать для клиентов; обычно это учетная запись администратора домена.

Установка агентов

Как только вы создали конфигурацию агентов на консоли, нужно установить их на устройства. Во время установки System Manager агенты не устанавливаются автоматически в главный сервер; необходимо вручную установить агентов главного сервера, а затем перезагрузить его.

Пакет агентов клиента - это один самораспаковывающийся исполняемый файл. По умолчанию пакеты хранятся в папке \Program Files\LANDesk\ManagementSuite\ldlogon на главном сервере. Запуск исполняемого файла устанавливает агенты клиента, не требуя никаких действий со стороны пользователя. Для успешной установки агента браузер на целевом устройстве не требуется.

Установка агентов

Вы можете обновить агенты, создав новую конфигурацию клиентов и распределив ее с консоли, или установить агенты непосредственно на неуправляемые устройства.

Как только вы установите пакет агентов клиента, установка других пакетов агентов клиента удаляет все агенты и устанавливает специально выбранные агенты. Вы можете удалить агент, создав новый пакет агентов, не содержащий агент, который вы хотите удалить.

Удаление агентов

Если нужно удалить агентов с устройств, см. раздел Установка агентов и обзор конфигураций.

Установка агентов с пакетом установки

Один из способов установки агентов - это использование самораспаковывающегося пакета агентов для работы с устройством. Это позволяет вам копировать файл на компакт-диск или устройство USB для установки агентов вручную. Такие пакеты можно создавать, выбирая параметр **Сохранить файл как** в нижней части диалогового окна **Конфигурация**.

1. Выберите параметр **Конфигурация агента**, а затем дважды щелкните имя конфигурации.
2. В диалоговом окне **Конфигурация агента** выберите **Сохранить файл как**, а затем щелкните **Закрыть**.

При выборе параметра **Сохранить файл как** создается самораспаковывающийся исполняемый пакет с именем файла, соответствующим заданному вами имени конфигурации. Создание пакета может занять несколько минут, после этого он будет доступен в папке \Program Files\LANDesk\ManagementSuite\ldlogon\ConfigPackages на главном сервере.

Запуск исполняемого файла устанавливает агенты, не требуя никаких действий со стороны пользователя. Вы должны войти в систему с правами администратора.

Если ваши пользователи не могут войти в систему с правами администратора для того, чтобы установить пакет, вы можете развернуть пакеты по электронной почте, используя загрузку из Интернета, с помощью сценариев входа или из папки общего доступа.

Запрос агентов

В данном разделе содержится информация о развертывании агентов из командной строки. Вы можете контролировать, какие компоненты установлены на устройствах, используя параметры командной строки SERVERCONFIG.EXE. Вы можете запустить SERVERCONFIG.EXE в самостоятельном режиме. Этот файл хранится в общей папке *http:**coreserver**LDLogon*, которая читается с сервера Windows.

SERVERCONFIG.EXE использует SERVERCONFIG.INI для конфигурации устройств.

Понятие SERVERCONFIG.EXE

SERVERCONFIG.EXE конфигурирует серверы семейства Windows NT для управления, используя следующие:

1. SERVERCONFIG определяет, был ли компьютер предварительно сконфигурирован с агентом управления. Если он был сконфигурирован, SERVERCONFIG удаляет все компоненты и переустанавливает выбранные компоненты.

2. SERVERCONFIG загружает необходимый файл инициализации (SERVERCONFIG.INI) и выполняет содержащиеся в нем инструкции.

Следующие параметры командной строки доступны для SERVERCONFIG.EXE:

Параметр	Описание
/I	Компоненты для включения (кавычки включены): "Агент Common Base" "Сканер инвентаризации" "Предупреждения" "Сканер уязвимых мест" "Контроль сервера" Вы можете комбинировать эти компоненты в одной командной строке. Например: `SERVERCONFIG.EXE /I="Alerting" /I="Vulnerability Scanner"`
/L или /Log=	Путь к файлам журнала CFG_YES и CFG_NO, в которых происходит регистрация сконфигурированных и несконфигурированных серверов.
/LOGON	Выполнение префиксных команд [LOGON]
/N или /NOUI	Не отображать интерфейс пользователя
/NOREBOOT	Не перезагружать сервер после окончания установки (по умолчанию)
/REBOOT	Принудительно перезагрузить сервер после выполнения установки
/X=	Компоненты для исключения. Например: `SERVERCONFIG.EXE /X=SD`
/CONFIG= /[CONFIG]=	Определение файла конфигурации сервера для использования вместо файлов по умолчанию SERVERCONFIG.INI. Например, если вы создали файлы конфигурации, называемые

Параметр	Описание
	NTTEST.INI, тогда используйте синтаксис: `SERVERCONFIG.EXE /CONFIG=TEST.INI` Файлы .INI должны быть в том же каталоге, что и SERVERCONFIG.EXE. Обратите внимание, что параметр /config использует имя файла без префикса NT.
/? или /H	Отображение окна справки

Создание конфигурации агента

Используйте **Конфигурацию агента** для создания и обновления конфигураций агентов (таких как, агенты установленные на управляемые устройства). Вы можете создать различные конфигурации для специальных нужд группы. Например, вы можете создать одну конфигурацию для web-серверов и другую - для серверов приложений.

Для установки конфигурации на сервере методом получения вам необходимо:

- **Создать конфигурацию агента**. Настроить определенные конфигурации для ваших серверов.
- **Запланировать конфигурацию агента**. Для получения конфигурации на серверах или из сервера нужно запустить SERVERCONFIG.EXE из общей папки LDLogon главного сервера.

Создание конфигурации агента

1. На консоли выберите **Конфигурация агента**.
2. Нажмите кнопку на панели инструментов **Новая**.
3. Введите **Имя конфигурации** и выберите операционную систему, затем нажмите **OK**.
4. Выберите новое имя конфигурации и затем нажмите **Правка**.
5. Выберите агента для развертывания.
6. Используйте вкладки в верхней части диалогового окна для поиска параметров, относящихся к выбранным компонентам. Настройте выбранные параметры, если необходимо.
7. Нажмите **Сохранить изменения** и закройте диалоговое окно.
8. Если вы хотите, чтобы конфигурация стала конфигурацией по умолчанию, выберите **Установить по умолчанию**.

Отправка конфигурации агента Linux

Получение конфигурации агента Linux

1. Создайте временный каталог в устройстве 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 "FILE*xx"*, 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 нужно переименовать в internal.ruleset.xml
    - файл monitorrules\<*любой текст*>.ruleset.monitor.xml нужно переименовать в masterconfig.ruleset.monitor.xml

2. Если устройство имеет поддержку IPMI/BMC (мониторинг включен в установку), в командной строке введите:

   ```
   export BMCPW="(пароль bmc)"
   ```

3. Войдя в систему с именем root, выполните 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 очистки, а затем снова используйте команды push или pull, и после выполнения операции в устройстве останется только файл с идентификатором GUID.

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

Создание автономных пакетов конфигураций агентов

Как правило, утилита конфигурации агента SERVERCONFIG.EXE производит конфигурацию агентов на управляемых устройствах. По желанию в окне **Конфигурация агента** можно создать один самораспаковывающийся исполняемый файл, который устанавливает конфигурацию агента на сервер, на котором он работает. Это полезно, если вы хотите установить агенты с компакт-диска или с переносного устройства USB.

Получение конфигурации агента в устройствах

Получение конфигурации агента

1. В консоли выберите устройства, в которых вы хотите развернуть агенты, затем нажмите **Цель**.
2. В левой навигационной области выберите **Конфигурация агента**.
3. Правым щелчком кнопки мыши выберите конфигурацию агента, которая будет доставляться методом получения, затем нажмите **Назначить задачу.**
4. Выберите **Целевые устройства** в диалоговом окне **Свойства назначенных задач**, а затем нажмите **Добавить список целей**.
5. Нажмите **Назначить задачу**.
6. Укажите время для развертывания агента и нажмите **Сохранить**.

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. Для установки агентов на сервере Linux вы должны иметь привилегии пользователя root.

Установка по умолчанию Linux (Red Hat 3, 4 и SUSE) включает модули RPM, которые требуются стандартному агенту управления Linux. Если вы выберите агента мониторинга в **Конфигурации агента** вам понадобится дополнительный модуль RPM — sysstat. Полный список RPM, необходимых для данного продукта, содержится в руководстве по развертыванию System Manager *Deployment Guide*.

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 выполняется конфигурация сервера 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 **Стоп**, а затем **Пуск** на вкладке **Планировщик**, чтобы перезапустить службу. При этом происходит активизация внесенных вами изменений.

Развертывание агентов Linux.

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 и 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 диалоге **Конфигурации агента** нажмите **Новая**.
2. Введите имя конфигурации, щелкните **HP-UX** или **Версия сервера Linux**, выберите тип установки (сервер или настольная система), 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. 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.
7. Нажмите **Сохранить**.

Для развертывания конфигурации агента выберите его в списке **Конфигурации агентов** и щелкните **Запланировать задачу**. Сконфигурируйте задачу и следите за процессом выполнения на вкладке **Задачи конфигурации**.

Примечание. Вы не получите информацию о состоянии на устройстве Linux, пока сканер инвентаризации не завершит первое сканирование после установки.

Получение конфигурации агента Linux

1. Создайте временный каталог в устройстве Linux (например, /tmp/ldcfg) и скопируйте туда следующее:
   - Все файлы из каталога LDLOGON\unix\linux.
   - Имя конфигурации присваивается имени сценария оболочки (<*имя конфигурации*>.sh).
   - После конфигурации файл получает имя *.0. Значок * звездочки можно заменить восемью символами (0-9, a-f).
   - Все файлы перечислены в файле <*имя конфигурации*>.ini. Для идентификации этих файлов выполните поиск файлов "FILE*xx*", 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 нужно переименовать в internal.ruleset.xml
     - файл monitorrules\<*любой текст*>.ruleset.monitor.xml нужно переименовать в masterconfig.ruleset.monitor.xml

2. Если устройство имеет поддержку IPMI/BMC (мониторинг включен в установку), в командной строке введите:

   ```
   export BMCPW="(пароль bmc)"
   ```

3. Войдя в систему под именем root и используя следующий путь, выполните сценарий оболочки для конфигурации:

   ```
   /tmp/ldcfg/lsminstall.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 очистки, а затем снова используйте команды push или pull, и после выполнения операции в устройстве останется только файл идентификатором GUID.

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

Параметры командной строки сканера инвентаризации

Сканер инвентаризации ldiscan имеет несколько параметров командной строки, которые определяют его работу. См. описания "ldiscan -h" или "man ldiscan" для получения подробного описания каждого из них. Каждому параметру должен предшествовать символ '-' или '/'.

Параметр	Описание
-d=Dir	Запускает процесс сканирования программного обеспечения в каталоге Dir вместо корневого каталога. По умолчанию сканирование начинается в корневом каталоге.
-f	Запускает принудительное сканирование. Если вы не укажите параметр -f, сканер будет проводить сканирование программного обеспечения с интервалом через определенное количество дней (по умолчанию ежедневно), которое указано на консоли в каталоге **Конфигурация	Службы	Инвентаризация	Настройки сканера**.
-f	Отключает сканирование программного обеспечения.
-i=ConfName	Определяет имя файла конфигурации. По умолчанию /etc/ldappl.conf.
-ntt=address:port	Имя хоста или IP-адрес главного сервера. Порт не обязателен.
-o=File	Записывает информацию инвентаризации в определенный выходной файл.
-s=Server	Указывает главный сервер. Это необязательная команда, которая необходима только для обратной совместимости.
-stdout	Записывает информацию инвентаризации в стандартный выходной файл.
-v	Включает подробные сообщения о состоянии во время сканирования.
-h или -?	Отображает окно справки.

Примеры

Чтобы вывести данные в виде текстового файла, введите:

```
ldiscan -o=data.out -v
```

Чтобы послать данные главному серверу, введите:

```
ldiscan -ntt=ServerIPName -v
```

Файлы сканера инвентаризации Linux

Файл	Описание
ldiscan	Исполняемый файл, управляемый с помощью параметров командной строки и служащий для указания действия, которое нужно выполнить. Все пользователи, которые будут запускать сканер, должны иметь достаточно прав для исполнения файла. Существуют различные версии данного файла для каждой из платформ, указанных выше.
/etc/ldiscan.conf	Файл всегда находится в папке /etc и содержит следующую информацию: • Уникальный идентификатор, назначенный сканером инвентаризации • Последнее сканирование оборудования • Последнее сканирование программного обеспечения Все пользователи, которые запускают сканер, должны иметь права на чтение и запись данного файла. Уникальный идентификатор, находящийся в файле /etc/ldiscan.conf — это уникальный номер, назначенный компьютеру при первом запуске сканера инвентаризации. Данный номер используется для идентификации компьютера. Если изменить данный номер, то главный сервер распознает его как другой компьютер, что приведет к появлению дубликата записи в базе данных. **Внимание!** Не изменяйте уникальный идентификатор или удалите файл ldiscan.conf после его создания.
/etc/ldappl.conf	Этот файл предназначен для выбора списка исполняемых файлов, о которых вам сообщит сканер инвентаризации после сканирования программного обеспечения. Файл содержит некоторые примеры, которые полезны для добавления записей для используемых пакетов программного обеспечения. Критерий поиска основан на имени и размере файла. Хотя обычно данный файл находится в папке /etc, сканер может использовать альтернативный файл, с помощью параметра командной строки -i=.
ldiscan.8	Оперативная страница руководства man для ldiscan.

Интеграция консоли

Как только компьютер с установленной ОС Linux найден и добавлен с базу данных главного сервера, вы можете:

- Запрашивать информацию о любом из атрибутов, данные о котором были добавлены в базу данных главного сервера.
- Использовать параметр создания отчетов, включающих информацию, которую получает сканер Linux. Например, в сводке об операционной системе в качестве типа ОС будет указана система Linux.
- Просматривать информацию инвентаризации для компьютеров Linux.

Запросы "Время работы системы" сортируются по алфавиту, возвращая неожиданные результаты.
Если вы хотите сделать запрос, чтобы узнать сколько компьютеров работало дольше определенного количества дней (например, 10 дней), пошлите запрос "Запуск системы", а не "Время работы системы". Запросы о времени работы системы также могут возвратить неожиданные результаты, так как время работы системы сформатировано в виде простой строки x дней, y часов, z минут и j секунд. Сортировка осуществляется по алфавиту, а не по временным интервалам.

Путь к файлам config, указанный в ldappl.conf, не отображается в консоли.
Записи ConfFile, указанные в файле ldappl.conf, должны содержать путь.

Мониторинг устройств

О службе мониторинга

System Manager предоставляет несколько методов для мониторинга состояния устройства. Средства мониторинга собирают информацию из различных источников, что позволяет вам наблюдать за разнообразными данными ваших устройств, например:

- Уровни использования
- События ОС
- Процессы и службы
- Архивные данные производительности
- Датчики оборудования (вентиляторы, напряжение, температуры и т.д.)

В этой главе содержится информация о различных функциях, которые осуществляют контроль за управляемыми устройствами:

- Установка агента мониторинга на устройства и создание наборов правил, которые могут быть развернуты в устройстве.
- Настройка датчиков производительности в устройствах и мониторинг данных производительности.
- Мониторинг изменений конфигурации с предупреждениями о возникновении изменений.
- Периодический эхо-тест устройств для мониторинга их подключения с использованием функции **Мониторинг устройства**.

Предупреждения - это сопутствующая функция, которая использует агент мониторинга для инициализации действий предупреждений, таких как отправка сообщений на электронный адрес или пейджер или внесение информации в журнал предупреждений. Предупреждения могут быть сгенерированы для любого события контролируемого устройства. Дополнительную информацию см. в разделе "Использование предупреждений".

Примечания

- Связь с агентом мониторинга происходит с использованием протокола HTTP, передаваемого через сети TCP/IP, в форме запросов GET, POST или XML. Ответы на запросы приходят в форме таблиц XML или HTML.
- Для выполнения и сохранения запроса о состоянии устройств (Computer.Health.State) необходимо убедиться, что состояние представлено числом в базе данных. Числа соответствуют следующим состояниям: 4=критическое, 3=предупредительное, 2=нормальное, 1=информационное, null или 0=неизвестно.
- Мониторинг устройств зависит от возможностей их аппаратного обеспечения, а также от правильности настройки. Например, если в устройстве с отключенной в системной BIOS функцией S.M.A.R.T. установлен жесткий диск с поддержкой S.M.A.R.T. или если BIOS устройства не поддерживает диски S.M.A.R.T., данные мониторинга будут недоступны.

- Если получение отчетов с конкретной машины прекратилось, воспользуйтесь файлом restartmon.exe в папке LDCLIENT для перезапуска коллектора данных и всех провайдеров мониторинга. Эта утилита предназначена для машин, на которых была установлена служба предоставления отчетов, но предоставление прекратилось. Используйте эту утилиту для перезапуска коллектора данных и провайдеров без перезагрузки устройства.

Развертывание агента мониторинга на устройствах

System Manager немедленно предоставляет общую информацию о состоянии устройства, как только в него устанавливается агент мониторинга. Агент мониторинга - это один из шести агентов, который может быть установлен в управляемых устройствах. Он регулярно проверяет аппаратное обеспечение устройства и отображает изменения в состоянии устройства. Это отображается значком состояния в списке **Мои устройства**, а подробная информация приводится в записях журнала (показано в сводке устройства **Информация о системе**) и диаграммах (показано на странице сводки устройства **Мониторинг**).

Например, контролируемое устройство, имеющее заполняемое дисковое устройство, может отображать на экране предупредительный значок, когда 90% диска будет заполнено, и менять его на критический значок, когда будет заполнено 95% диска. Вы также можете получить предупредительные сообщения для этого диска, если в устройстве настроен набор правил, в который входят правила предупреждений по объему свободного места на диске.

Вы можете развернуть стандартный набор правил мониторинга для устройств. Или, если нужно, можно создать свой собственный набор правил, в который будут входить лишь те параметры состояния, которые вас интересуют.

Создание набора правил мониторинга

Вы можете выбрать параметры устройства, которые будут отслеживаться, создав для этого набор правил мониторинга, в котором определяется, что агент мониторинга проверяет в устройстве. Вы можете развернуть набор правил на одном устройстве или на целевой группе устройств. Например, вы можете определить один набор правил для серверов, предназначенных для хранения, и использовать другой набор правил для Web-серверов.

Стандартный набор правил включает в себя 16 элементов. При создании набора правил вы можете активировать или деактивировать любой из этих параметров, указав, с какой частотой они будут проверяться, а для некоторых элементов установить предельное значение производительности. Вы также можете выбрать службы, работающие в устройствах, которые вы хотите контролировать.

Общий процесс создания и развертывания правил предупреждений:

1. Выберите устройства, на которых будет развернут набор правил, и выберите **Цель**, чтобы добавить их в список **Целевые устройства**.

2. Создайте или измените набор правил мониторинга. Помните, что нужно пометить флажком каждое из событий, для которых будет производиться мониторинг. Не все события по умолчанию включены в список мониторинга. Некоторые события, такие как службы, также требуют выбора каждой службы, мониторинг которой вы хотите осуществлять. (Далее см. подробное описание).
3. Примените эти правила на целевых устройствах. При необходимости перед развертыванием набора правил можно выбрать дополнительные устройства. (Далее см. подробное описание).

Создание набора правил мониторинга

1. В левой навигационной панели выберите **Мониторинг**.
2. Выберите **Новое**, введите имя и описание конфигурации, а затем щелкните **OK**.
3. Выберите конфигурацию в левом столбце.
4. В списке элементов выберите тот, который нужно изменить, и нажмите **Правка**.
5. Для отключения мониторинга элемента снимите флажок рядом с ним и нажмите **Обновить**.
6. Для изменения частоты проверки элемента выберите **Секунды** или **Минуты** и введите число в текстовом окне.
7. Если допускается, установите процентную величину предельного значения для предупредительных и критических состояний.
8. Для мониторинга **служб** выберите ОС из раскрывающегося списка. Выберите одну или несколько служб для мониторинга (для выбора нескольких служб удерживайте нажатой клавишу CTRL), а затем нажмите **>>** для добавления служб в список справа.
9. После внесения каждого изменения нажмите **Обновить** для применения изменений конфигурации. Если вы изменили элемент, а потом решили, что его не нужно изменять, нажмите **Возврат** (к предшествующему состоянию) для восстановления первоначальных настроек.

При редактировании служб в конфигурации мониторинга из главного сервера в списке **Доступные службы** отображаются известные службы из базы данных инвентаризации. В списке **Доступные службы** не будет ничего отображаться до тех пор, пока агент LANDesk не будет развернут в одном или в нескольких устройствах, а сканирование инвентаризации не предоставит данные на главный сервер. Например, для выбора из списка служб Linux следует развернуть агент в устройстве, в котором установлена система Linux.

Развертывание набора правил мониторинга

1. В левой навигационной панели выберите **Мои устройства**, затем щелкните группу **Все устройства**.
2. Выберите устройства, для которых нужно развернуть набор правил, затем выберите **Цель** для размещения устройств в списке **Целевые устройства**.
3. В левой навигационной панели выберите **Мониторинг**, затем откройте вкладку **Развернуть набор правил**.
4. В окне **Наборы правил мониторинга** выберите набор правил, который вы хотите развернуть.
5. Щелкните ссылку для просмотра списка **Целевые устройства**. Для удаления устройства из этого списка щелкните его правой кнопкой, а затем выберите **Удалить**. (Для добавления устройств нужно добавить их в список так, как описано в действии 2).

6. Щелкните **Развернуть** для развертывания выбранного набора правил на целевых устройствах.

Как часть процесса развертывания, создается страница XML, в которой указан набор правил и устройства, на которых этот набор правил был развернут. Этот отчет сохраняется в главном сервере в каталоге LDLOGON и получает имя по порядковому номеру, назначаемому базой данных. Если вы хотите просмотреть эту страницу XML отдельно от развертывания набора правил, нажмите кнопку **Создать XML**, а затем щелкните ссылку для просмотра этого файла. Создание набора правил в виде файла XML также позволяет отображать список доступных наборов правил в настройках **Конфигурации агента**.

Отключение службы ModemView

Служба ModemView - служба (драйвер), которая отслеживает звонки модема (входящие и исходящие) и генерирует предупреждение при их обнаружении. Эта служба занимает до 10 МБ памяти, поскольку использует MFC. Вы можете ее отключить (в особенности, если к устройству не подключен модем).

Отключение службы ModemView

1. На устройстве выберите (непосредственно или через дистанционное управление) **Пуск** > **Панель управления** > **Администрирование** > **Службы**.
2. Дважды щелкните **Служба описания сообщений LANDesk**.
3. На вкладке **Тип запуска** выберите **Вручную** и щелкните **OK**.

Вы также можете выбрать **Останов** в окне **Состояние службы**.

Настойка датчиков производительности

System Manager позволяет выбирать элементы производительности (датчики), которые вы хотите контролировать на управляемом устройстве. Можно контролировать множество различных элементов, включая компоненты оборудования (например, драйверы, процессоры и память), или компоненты операционной системы (например, процессы) или компоненты приложений (такие как скорость передачи данных (байты в сек) через web-сервер системы). При выборе датчика производительности необходимо указать частоту опроса элемента, а также предельное значение производительности и число нарушений, допустимых перед созданием предупреждения.

После выбора датчика производительности вы можете контролировать производительность на странице **Мониторинг** путем просмотра диаграммы в реальном времени или архивных данных. "Дополнительную информацию см. в разделе "Мониторинг производительности".

Выбор датчика производительности для мониторинга

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать. В новом окне просмотра откроется информационная консоль сервера.
2. В левой навигационной панели выберите **Мониторинг**.

3. Откройте вкладку **Настойка датчиков производительности**.
4. Из столбца **Объекты** выберите объект, который хотите контролировать.
5. Из столбца **Экземпляры** выберите экземпляры (если имеются), которые вы хотите контролировать.
6. Из столбца **Датчики** выберите датчик, который вы хотите контролировать.

   Если этот датчик не отображен в списке, нажмите **Перезагрузка датчиков** чтобы обновить список с любыми новыми объектами, экземплярами или датчиками.

7. Установите частоту опроса (**Проверять каждые** *n* **секунд**), а также число дней, в течение которых будет храниться запись датчика.
8. В текстовом окне **Предупреждать, когда датчик вне диапазона** укажите число раз, которое датчик может нарушать предельное значение перед созданием предупреждения.
9. Укажите верхнее и/или нижнее предельные значения.
10. Нажмите **Применить**.

Примечания

- Файлы журнала производительности могут быстро увеличиваться в размере. Опрос одного датчика с интервалом в две секунды увеличивает объем информации в журнале производительности на 2,5 МБ ежедневно.
- Предупреждение генерируется, когда датчик производительности нарушает нижнее предельное значение любого устройства с ОС Windows или Linux. Когда датчик производительности обнаруживает нарушение верхнего предельного значения устройства Linux, генерируется предупредительное сообщение. Когда датчик производительности обнаруживает нарушение верхнего предельного значения устройства Windows, генерируется критическое сообщение.
- Устанавливая предельное значение, помните, что предупреждения будут генерироваться независимо от того, нарушается ли верхнее или нижнее значение. Например, если речь идет об объеме свободного места на диске, вы можете пожелать, чтобы предупреждение генерировалось только в том случае, если объем устройства почти исчерпан. В данном случае вам необходимо установить верхнее предельное значение на достаточно высоком уровне, чтобы вы не получали сообщение, если на устройстве становится доступным много свободного дискового пространства.
- Изменение значения **Предупреждать, когда датчик вне диапазона** позволяет обращать внимание на событие, которое повторяется постоянно или является единичным. Например, если вы контролируете число байт, отправляемых с web-сервера, System Manager может предупредить вас, когда скорость передачи постоянно высока. Или вы можете указать небольшое число нарушений (1 или 2), для получения предупреждения, когда анонимное FTP-подключение превышает определенное количество пользователей.

Мониторинг производительности

Страница **Мониторинг** позволяет контролировать производительность различных системных объектов. Можно контролировать определенные компоненты оборудования, например, драйверы, процессоры и память, или компоненты операционной системы, например, процессы или скорость передачи данных (байты в сек) через web-сервер

системы. Страница **Мониторинг** содержит диаграмму, отображающую данные реального времени или архивные данные для датчиков.

Для осуществления контроля над датчиком производительности сначала необходимо выбрать датчик, добавив его в список контролируемых датчиков. При этом также необходимо указать частоту опроса элемента и установить предельные значения производительности и число нарушений, допустимых перед созданием предупреждения. Подробную информацию о выбираемых датчиках см. в разделе "Настройка датчиков производительности".

Просмотр диаграммы производительности контролируемого датчика

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать. В новом окне просмотра откроется информационная консоль сервера.
2. В левой навигационной панели выберите **Мониторинг**.
3. При необходимости откройте вкладку **Активные датчики производительности**.
4. В раскрывающемся списке **Датчики** выберите датчик, для которого необходимо отобразить диаграмму производительности.
5. Выберите **Просмотр данных в режиме реального времени**, чтобы отобразить диаграмму производительности реального времени.

   или

   Выберите **Просмотр сведений**, чтобы отобразить диаграмму производительности за период времени, указанный при выборе датчика (Хранить сведения).

Горизонтальная ось диаграммы производительности соответствует прошедшему времени. Вертикальная ось отображает единицы измерения, например, байты в секунду (при контроле над передачей файлов), проценты (при контроле над задействованными ресурсами процессора) или свободные байты (при контроле над дисковым пространством). Высота кривой не является фиксированной. Она изменяется в соответствии с пиковыми значениями данных; для одного датчика вертикальная ось может соответствовать диапазону от 1 до 100, а для другого – от 1 до 500 000. При большом разбросе значений минимальные изменения могут отображаться в виде горизонтальных участков.

Примечания

- При выборе другого датчика диаграмма обновляется, и устанавливаются другие единицы измерения.
- Чтобы очистить и перезапустить диаграмму, нажмите **Обновить**.
- При появлении предупреждения, сгенерированного датчиком в списке, щелкните правой кнопкой мыши датчик и нажмите **Подтвердить**, чтобы очистить предупреждение.

Отмена контроля над датчиком производительности

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать. В новом окне просмотра откроется информационная консоль сервера.

2. В левой навигационной панели выберите **Мониторинг**.
3. При необходимости откройте вкладку **Активные датчики производительности**.
4. В поле **Рабочие датчики производительности** щелкните правой кнопкой мыши датчик и нажмите **Удалить**.

Контроль над изменениями конфигурации

При установленном агенте мониторинга данный продукт может генерировать предупреждения при изменении конфигурации аппаратного или программного обеспечения устройства. Такие изменения могут влиять на производительность и стабильность устройства, а также вызывать проблемы со стандартной установкой. Контроль над жизненно важными компонентами устройства может способствовать снижению полной стоимости владения данным продуктом.

К изменениям конфигурации, при которых генерируются предупреждения, относятся:

- **Установка или удаление приложения.** Позволяет отследить пользователей, установивших или удаливших приложения. Данная возможность может оказаться полезной для отслеживания лицензий и определения производительности сотрудников. Учитываются только приложения, зарегистрированные в списке "Установка и удаление программ" панели управления Windows. Остальные приложения игнорируются. В журнале предупреждений или в окне предупреждения отображается имя приложения, используемое в списке "Установка и удаление программ" панели управления Windows.
- **Установка или удаление памяти.** Данный продукт обнаруживает и отслеживает количество и тип установленной памяти. При изменении конфигурации генерируется предупреждение.
- **Установка или удаление жестких дисков.** Данный продукт обнаруживает и отслеживает тип и размер установленных жестких дисков. При изменении конфигурации генерируется предупреждение.
- **Добавление, удаление или изменение процессора (или процессоров).** Данный продукт обнаруживает и отслеживает количество, тип и скорость процессора (процессоров). При изменении конфигурации генерируется предупреждение.
- **Установка или удаление сетевой карты.** Данный продукт обнаруживает и отслеживает количество и тип сетевых интерфейсных плат и генерирует предупреждение при изменении конфигурации.

Сведения о предупреждениях об изменении конфигурации содержатся в журнале предупреждений на информационной консоли сервера. Подробную информацию см. в разделе "Просмотр журнала предупреждений".

Контроль подключения

В большинстве случаев устройства могут оповещать пользователя о критических ситуациях, например, о переполнении жесткого диска или поломке вентилятора. Однако в некоторых ситуациях устройство может отключиться, прежде чем успеет отправить предупреждение. Например, неполадки коммутатора или маршрутизатора могут привести к нарушению сетевого трафика, либо может произойти сбой питания устройства.

В таких ситуациях данный продукт может производить периодическую проверку устройств с целью определения их наличия в сети. Если устройство не отвечает на запрос, его состояние изменяется на критическое при следующем обновлении списка **Мои устройства**.

Для этого необходимо настроить периодическую проверку целевых устройств или всех устройств в группе **Все устройства**.

Настройка мониторинга устройств

1. В списке **Мои устройства** выберите устройства, которые хотите контролировать. Для этого можно воспользоваться группой **Все устройства**, а также общей или закрытой группой.
2. Выберите **Цель**.
3. В нижней панели выберите вкладку **Действия**, затем щелкните **Мониторинг устройства**.
4. Чтобы просмотреть список устройств, контролируемых на текущий момент, щелкните **Показать устройства для мониторинга**.
5. Введите время ожидания (в минутах) между сеансами эхо-теста и число раз, которое продукт будет пытаться связаться с устройством.
6. Укажите, следует ли выполнять данные действия для устройств в списке целевых устройств или для всех устройств в группе **Все устройства**.
7. Для остановки мониторинга всех устройств выберите **Полная отмена тестирования (эхо-теста) устройств**.
8. Нажмите **Применить**.

Контролируется только последняя выбранная группа целевых устройств. Например, если целевыми назначены устройства A и B и к ним применяется мониторинг устройств, базовый сервер будет отправлять запросы только устройствам A и B. Если назначить целевыми устройства C и D и применить к ним мониторинг устройств, контролироваться будут только устройства C и D; мониторинг устройств A и B будет отменен.

Конфигурация предупреждений

Использование предупреждений

Когда возникает неисправность или другая проблема с устройством (например, отсутствует свободное дисковое пространство), System Manager может отправить предупреждение. Вы можете настроить эти предупреждения, выбрав степень важности или уровень, активизирующий предупреждение. Предупреждения отправляются на консоль и могут быть сконфигурированы для выполнения специальных действий. В этой главе описывается, как работают предупреждения.

Как я могу увидеть предупреждения?

Это приложение может известить вас о проблемах и других событиях в компьютере при помощи:

- Ввода дополнительной информации в журнал
- Отправки электронного сообщения или сообщения на пейджер
- Выполнения программы на главном сервере или отдельном устройстве
- Отправки через сеть SNMP-предупреждения на консоль управления SNMP
- Перезагрузки и завершения работы устройства

Имейте в виду, что некоторые предупреждения для определенных групп машин могут одновременно генерировать большое количество ответов. Например, можно настроить предупреждение "Изменение конфигурации компьютера" и связать его с действием электронной почты. При развертывании исправления ПО на машинах с такой настройкой предупреждения на главном сервере будет создано столько электронных сообщений, на скольких машинах было установлено это исправление, что, в конечном итоге, может "перегрузить" почтовый сервер. В этом случае необходимо предусмотреть такую обработку предупреждения, при которой оно будет протоколироваться в журнале главного сервера без отправки электронного сообщения.

Какие неисправности устройства могут генерировать предупреждения?

Данное приложение имеет большой список событий, которые могут создавать предупреждения. Некоторые из этих проблем требуют немедленного вмешательства; другие являются изменениями конфигурации, которые могут (или не могут) вызвать какую-либо проблему, но предоставляют полезную информацию системному администратору. (Для получения дополнительной информации см. раздел "Мониторинг изменений конфигурации"). Предупреждения могут быть созданы только при оснащении устройств

соответствующим оборудованием. Например, предупреждения, создаваемые при считывании показателей датчиков, применяются только для устройств, оснащенных соответствующими датчиками.

Типы событий, которые потенциально вы можете контролировать, включают перечисленные ниже.

- **Изменение оборудования.** Добавлен или удален компонент, такой как процессор, память, диск или плата.
- **Приложение установлено или удалено.** Приложение установлено или удалено из устройства.
- **Событие службы.** На устройстве запущена или остановлена служба.
- **Производительность.** Предельное значение производительности вышло за допустимые рамки, например, объем диска, доступный объем памяти и т.д.
- **Событие IPMI.** Произошло событие, обнаруженное устройствами IPMI, например, изменения контроллеров, датчиков, журналов событий и т.д.
- **Использование модема.** Обнаружено использование модема системы, или он был установлен или удален.
- **Физическая защита.** Обнаружен несанкционированный доступ в корпус, цикл питания или другое физическое изменение.
- **Установка пакета**. Пакет установлен на целевом компьютере.
- **Действие дистанционного управления.** Обнаружен сеанс дистанционного управления, например, запуск, останов или сбой.

Служба мониторинга оборудования, создающая предупреждения, зависит от возможностей оборудования, установленного на устройстве, а также от его правильной конфигурации. Например, если жесткий диск с поддержкой S.M.A.R.T. установлен в устройстве с отключенной в системной BIOS функцией S.M.A.R.T. или BIOS устройства не имеет поддержки дисков S.M.A.R.T., системой мониторинга дисков S.M.A.R.T. предупреждения генерироваться не будут.

Конфигурация уровней важности событий

Проблемы или события устройства могут быть частично или полностью связаны с представленными ниже уровнями важности.

- **Информационное.** Определяет изменения конфигурации или события, которые производители могут включить в свои системы. Этот уровень важности не влияет на состояние устройства.
- **OK.** Показывает, что состояние устройства находится на допустимом уровне.
- **Внимание!** Отображает дополнительные предупреждения перед тем, как проблема достигнет критической точки.
- **Критическое.** Указывает на то, что проблема требует немедленного рассмотрения.
- **Неизвестно.** Состояние предупреждения не может быть определено, или агент службы мониторинга контроля не был установлен в устройстве.

В зависимости от типа событий или от проблемы на сервере, некоторые уровни важности событий не применимы и поэтому не включены. Например, при возникновении события несанкционированного доступа к корпусу, когда корпус устройства открыт или закрыт. Если он открыт, это может включить действие предупреждения предупредительного уровня.

События другого рода, например, с дисковым пространством или виртуальной памятью, включают три уровня важности (OK, предупредительный и критический).

Вы можете выбрать уровень важности или предельное значение, которые активизируют создание предупреждений. Например, можно выбрать различные действия после появления предупредительного или критического предупреждений. Неизвестное состояние не может быть выбрано для создания предупреждения, но может послужить указателем того, что состояние не определено.

Процесс конфигурации выборочных наборов правил предупреждений

Вы можете сконфигурировать набор правил предупреждений для развертывания в отдельном устройстве или в группе целевых устройств. Каждое управляемое устройство должно содержать компонент мониторинга продукта, установленный перед тем, как он сможет отправлять предупреждения на главный сервер. (Дополнительную информацию см. в разделе "Конфигурация агентов").

Когда компонент мониторинга установлен на управляемом устройстве, активизируется набор правил предупреждений по умолчанию, предоставляющий информацию о состоянии устройства на консоль. Этот набор правил по умолчанию включает следующие предупреждения:

- Диск установлен или удален
- Дисковое пространство
- Использование памяти
- Температура, вентиляторы и напряжение
- Мониторинг производительности
- События IPMI (для поддерживаемого оборудования)

В дополнение к набору правил по умолчанию, можно сконфигурировать и развернуть выборочные наборы правил предупреждений. Их также можно использовать для ответов на определенные события. Например, если вентилятор не работает, можно послать предупреждение или электронное сообщение группе поддержки оборудования.

Общий процесс создания и развертывания правил предупреждений:

1. Выберите устройства, на которых будет развернут набор правил, и выберите **Цель**, чтобы добавить их в список **Целевые устройства**.
2. Создайте набор правил предупреждений, который вы будете использовать. Эти наборы правил определяют действия, которые будут выполняться при появлении предупреждений. (Дополнительную информацию см. в разделе "Конфигурация действий предупреждения").
3. Создайте выборочный набор правил предупреждений. После этого вы можете выбрать ряд действий, определенных ранее. (Дополнительную информацию см. в разделе "Конфигурация набора правил предупреждений").
4. Примените эти правила на целевых устройствах. Перед развертыванием набора правил можно выбрать дополнительные устройства. (Дополнительную информацию см. в разделе "Развертывание наборов правил").

Далее приведен пример этого процесса.

Например, конфигурация набора правил предупреждения при недостатке дискового пространства

1. В левой навигационной панели выберите **Мои устройства**, а затем дважды щелкните группу **Все устройства**.
2. Выберите устройства, для которых нужно установить предупреждения, затем выберите **Цель** для размещения устройств в списке **Целевые устройства**.
3. Щелкните **Предупреждения**, затем вкладку **Наборы правил действий**.
4. В раскрывающемся списке **Действия** выберите действия, которые необходимо сконфигурировать (например, **Отправить эл. письмо/сообщение на пейджер**). Нажмите **Новое**, введите имя в поле **Имя**, а затем щелкните **OK**.
5. Вернитесь на страницу **Набор правил действий**, выберите набор правил, имя которого вы только что задали, а затем щелкните **Действия правки**. В текстовом поле укажите необходимые данные. После завершения нажмите **Сохранить**.
6. Откройте вкладку **Наборы правил предупреждений**.
7. Выберите **Новое**, введите информацию, например, "Недостаток дискового пространства" в поле **Имя**, введите описание в поле **Описание**, а затем щелкните **OK**.
8. Выделите только что названный набор правил предупреждений и нажмите кнопку **Правка набора правил**.
9. Нажмите кнопку **Новое**.
10. В раскрывающемся списке **Тип предупреждения** выберите **Дисковое пространство**.
11. Отметьте состояние, при котором нужно отправить предупреждение: **OK**, **Предупредительное** или **Критическое**. (Если нужно определить одно действие для нескольких состояний, выберите более одного состояния. Если нужно определить несколько действий для каждого состояния, создайте отдельную конфигурацию для каждого состояния, чтобы выполнять разные действия для разных уровней состояния).
12. В раскрывающемся списке **Действие** выберите действие, которое будет выполняться при выполнении условий, указанных в пунктах 6 и 7. Если в списке нет необходимого действия, можно создать его, используя страницу **Наборы правил действий**. (Если вы не создали набор правил действий предупреждений, его не будет в списке).
13. В раскрывающемся списке **Действие предупреждения** выберите необходимую конфигурацию.
14. Проверьте параметр **Воздействует на состояние устройства**, если нужно, чтобы предупреждение отражало состояние сервера в списке **Все устройства**. Если для предупреждения выбран только один уровень важности - **Информационное**, предупреждение не будет затрагивать состояние устройства.
15. Нажмите кнопку **Добавить**.
16. Если хотите добавить дополнительные предупреждения, повторите действия 6-12.
17. После завершения щелкните **Закрыть**.
18. Если нужно изменить в правиле какие-либо типы предупреждений, выберите тип предупреждения и щелкните **Правка**, сделайте необходимые изменения, нажмите **Обновить**, затем **Закрыть**.
19. Когда набор правил предупреждений определен, примените его к целевым устройствам: выберите **Развертывание наборов правил**, выберите набор правил и щелкните **Развернуть**.

Конфигурация действий предупреждений

Используйте страницу **Набор правил действий** для того, чтобы внести дополнительную информацию о том, как нужно выполнять выбираемые действия. При достижении предельного значения создается предупреждение. Предупреждение можно ассоциировать с действием, таким как отправка электронного письма. Для каждого действия используется своя собственная конфигурация.

Создание набора правил действия

1. В левой навигационной панели выберите **Предупреждения**, затем откройте вкладку **Наборы правил действий**.
2. В раскрывающемся списке **Действия** выберите действие, которое нужно сконфигурировать. Для каждого действия существует список уникальных конфигураций.
3. Нажмите **Новое**, введите имя в поле **Имя**, а затем щелкните **OK**.
4. Вернитесь на страницу **Наборы правил действий**, выберите набор правил, имя которого вы только что задали, а затем щелкните **Действия правки**.
5. Если вы выбрали **Выполнять программу на главном компьютере** или **Выполнять программу на клиенте**, введите или скопируйте путь к программе, которую нужно выполнять при возникновении предупреждения, а затем щелкните **Сохранить**. Если вы выбираете любое из действий **Выполнять программу**, помните, что программы на рабочем столе могут отображаться не так, как вы предполагали. Когда программа выполняется, она запускается как служба Windows и не отображается как обычное приложение. Программы, работающие таким образом, не должны иметь пользовательского интерфейса, предполагающего действия человека. Чтобы определить, выполнилась ли программа, посмотрите процессы в Диспетчере задач Windows.

   Если вы выбрали **Отправить эл. письмо/сообщение на пейджер**, введите полный электронный адрес лица, которое будет получать предупреждения, в поле **Кому**; введите действующий электронный адрес в поле **От**; введите тему письма в поле **Тема**; введите сообщение в поле **Текст**; выберите день и время, в которые будет отправлено сообщение; введите местонахождения сервера SMTP в поле **SMTP-сервер**. Нажмите **Справка** для получения сведений об отправке сообщений нескольким получателям, а также об использовании в сообщениях переменных. После завершения нажмите **Сохранить**.

   При выборе **Отправить предупреждение SNMP** введите имя узла, выберите версию, введите строку сообщества в окне **Строка сообщества**, затем щелкните **Сохранить**.

Примечания

- Некоторые предупреждения для определенных групп машин могут одновременно генерировать большое количество ответов. Например, можно настроить предупреждение "Изменение конфигурации компьютера" и связать его с действием электронной почты. При развертывании исправления ПО на машинах с такой настройкой предупреждения на главном сервере будет создано столько электронных сообщений, на скольких машинах было установлено это исправление, что, в конечном итоге, может "перегрузить" почтовый сервер. В этом случае необходимо предусмотреть такую обработку предупреждения, при которой оно будет протоколироваться в журнале главного сервера без отправки электронного сообщения.
- Некоторые действия предупреждений не влияют на состояние устройства. Среди них: "Выполнить программу на клиенте", "Завершение работы/Перезапуск" и любые другие, которые предоставляются исключительно в информационных целях. Однако если какие-либо из этих действий объединяются с другими действиями предупреждений, которые влияют на состояние устройств, тогда любое созданное предупреждение будет затрагивать состояние устройства и появляться в журнале предупреждений.
- Поле **От** в электронном сообщении должно содержать действующий адрес электронной почты для правильной работы предупреждений SMTP.
- Предупреждения SNMP, имеющие версию 1, будут обрабатываться, в то время как предупреждения, имеющие версию 3, будут только перенаправляться.
- Для предупреждений SNMP уровни важности событий отображаются в поле "Тип специального предупреждения" данного предупреждения. Возможные значения 1 = неизвестно, 2 = инфо, 3 = OK, 4 = предупредительное, 5 = критическое.

Конфигурация набора правил предупреждений

Для создания нового набора правил предупреждений используйте страницу **Наборы правил предупреждений**. Прежде чем настраивать предупреждения, необходимо настроить действия. (Дополнительную информацию см. в разделе "Конфигурация действий предупреждения").

По умолчанию страница **Наборы правил предупреждений** содержит два набора:

- **Набор правил предупреждений главного сервера**. Данный набор правил обеспечивает отсылку предупреждений главному серверу при включенной функции **Мониторинг устройства** (см. Мониторинг подключения). Данный набор правил содержит стандартную группу типов предупреждений, в том числе Мониторинг устройства, Предупреждения прерывателя цепи AMT и Сеанс соединений через ЛС. Вы можете редактировать статус, действие, действие предупреждения и параметры состояния для основных типов предупреждений, но попытки произвести любые другие изменения будут проигнорированы.

- **Набор правил по умолчанию**. Данный набор правил развертывается на всех контролируемых устройствах и содержит несколько типов предупреждений, которые обычно используются большинством администраторов сети. Этот набор правил можно редактировать: добавлять другие типы предупреждений и менять параметры стандартных типов предупреждений. При редактировании набора правил изменения всегда распространяются на все контролируемые устройства, даже при неявном повторном развертывании набора.

Помимо этих наборов правил можно создавать выборочные наборы для применения их к целевым группам контролируемых устройств. Для отображения наборов правил в **Конфигурации агента** их следует создавать в формате XML.

При создании выборочного набора правил на устройстве имейте в виду, что, если набор правил по умолчанию уже был развернут на устройстве, могут возникнуть наложение или конфликт наборов правил предупреждений. Если вы развернете набор правил по умолчанию во время конфигурирования управляемого устройства, а затем развернете выборочный набор правил, оба набора правил будут выполняться на устройстве. Например, если оба набора правил генерируют предупреждения одного типа, но функционируют по-разному, как результат, могут быть предприняты дублирующиеся или непредсказуемые действия предупреждения. Хотя вы не можете удалить набор правил по умолчанию после того, как он был развернут, вы можете отредактировать набор правил по умолчанию, если хотите изменить какую-либо его часть.

Создание набора правил предупреждений

1. В левой навигационной панели выберите **Предупреждения**, затем откройте вкладку **Наборы правил предупреждений** (при необходимости).
2. Выберите **Новый**, заполните поле **Имя**, введите описание предупреждения в поле **Описание** и нажмите кнопку **OK**.
3. Выделите только что названный набор правил и нажмите кнопку **Правка набора правил**.
4. Щелкните **Новый**.
5. В раскрывающемся списке **Тип предупреждения** выберите компонент, действие или тип события, о которых будут поступать предупреждения.
6. Выберите состояния для предупреждений: **Информационное**, **OK**, **Предупредительное** или **Критическое**. Например, для получения предупреждения о превышении предельного значения типом, выбранным в пункте 5, установите флажок в поле **Критическое**.

7. В раскрывающемся списке **Действие** выберите действие, которое будет выполняться при выполнении условий, указанных в пунктах 5 и 6. Эти действия определяются заранее; если в списке нет необходимого действия, можно создать его, используя страницу **Наборы правил действий**.

   Примечание. Некоторые предупреждения для определенных групп машин могут одновременно генерировать большое количество ответов. Например, можно настроить предупреждение "Изменение конфигурации компьютера" и связать его с действием электронной почты. При развертывании исправления ПО на машинах с такой настройкой предупреждения в главном сервере будет создано столько электронных сообщений, на скольких машинах было установлено это исправление, что в конечном итоге может "перегрузить" почтовый сервер. В этом случае необходимо предусмотреть такую обработку предупреждения, при которой оно будет протоколироваться в журнале главного сервера без отправки электронного сообщения.

8. В раскрывающемся списке **Действие предупреждения** выберите конфигурацию. Список может содержать только одну конфигурацию (содержимое списка меняется в зависимости от вашего выбора в пункте 7).
9. Проверьте параметр **Воздействует на состояние устройства**, если нужно, чтобы предупреждение отражало состояние сервера в списке **Все устройства**. Если для предупреждения выбран только один уровень важности - **Информационное**, предупреждение не затрагивает состояние устройства.
10. Нажмите кнопку **Добавить**.
11. Если хотите добавить дополнительные предупреждения, повторите действия 5-10.
12. После завершения щелкните **Закрыть**.

Для правки набора правил предупреждений выберите набор (действие 3), щелкните **Правка набора правил** и выполните описанные выше действия.

Через несколько минут после создания или правки набора правил служба развертывания наборов правил автоматически попытается обновить все компьютеры, на которых был развернут этот набор. Для немедленного развертывания набора правил откройте вкладку **Набор правил развертывания** и нажмите **Развернуть**.

Развертывание наборов правил

Воспользуйтесь страницей **Развертывание наборов правил** для перемещения выбранного набора правил предупреждений в целевые устройства.

Для развертывания набора правил на управляемом устройстве на нем сначала нужно установить агент управления. При развертывании стандартного агента управления разворачивается набор правил по умолчанию. После завершения настройки агента можно обновить или развернуть новые наборы правил. Сначала назначьте устройства, на которых вы хотите развернуть набор правил предупреждений.

Развертывание набора правил предупреждений

1. В левой навигационной панели выберите **Мои устройства**, затем щелкните группу **Все устройства**.

2. Выберите устройства, для которых нужно развернуть набор правил предупреждений, затем выберите **Цель** для размещения устройств в списке **Целевые устройства**.
3. В левой навигационной панели выберите **Предупреждения**, затем откройте вкладку **Развернуть набор правил**.
4. В окне **Наборы правил предупреждений** выберите набор правил, который вы хотите развернуть.
5. Щелкните ссылку для просмотра списка целевых устройств. Для удаления устройства из этого списка щелкните его правой кнопкой, а затем выберите **Удалить**. Для удаления всех устройств щелкните правой кнопкой имя любого устройства, а затем **Сброс**. Для добавления устройств нужно добавить их в список целевых устройств (см. действия 1-2 выше).
6. Закройте окно **Список целей**, затем щелкните **Развернуть** для развертывания выбранной конфигурации на целевых устройствах.

Как часть процесса развертывания, создается страница XML, в которой указан набор правил и устройства, на которых этот набор правил был развернут. Этот отчет сохраняется на главном сервере в каталоге \ldlogon\alertrules и получает имя по порядковому номеру, назначаемому базой данных. Если вы хотите просмотреть эту страницу XML отдельно от развертывания набора правил, нажмите кнопку **Создать XML**, а затем щелкните ссылку для просмотра этого файла.

Обратите внимание, что на управляемом устройстве в заданный момент времени может действовать только один выборочный набор правил. Если вы развернули один выборочный набор правил, а затем на том же устройстве развернули второй, первый выборочный набор правил будет перезаписан вторым, который и будет работать.

Просмотр наборов правил предупреждений для устройства

Используйте страницу **Наборы правил предупреждений** для просмотра списка правил предупреждений, закрепленных за выбранным устройством, а также для просмотра подробностей каждого предупреждения.

Просмотр наборов правил предупреждений

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать. В новом окне просмотра откроется информационная консоль сервера.
2. В левой навигационной панели выберите **Наборы правил**.
3. Откройте вкладку **Набор правил предупреждений**.

В каждом наборе правил доступны следующие подробности. Дополнительную информацию об изменении данных подробностей см. в разделе Использование предупреждений.

- **Достижение состояния.** Предупреждение генерируется при достижении указанного вами состояния.

- **Воздействие на состояние системы.** Показывает, применим ли статус предупреждения к состоянию сервера при его отображении на инструментальной панели или в списке **Все устройства**.
- **Имя набора правил.** Имя набора правил предупреждений, определенного в диалоговом окне Наборы правил предупреждений
- **Тип предупреждения.** Описание источника предупреждения (оборудование, ПО, событие и т.д.).
- **Конфигурация действия.** Действие, определенное в диалоговом окне Конфигурация действий, которое происходит при генерировании предупреждения.
- **Описатель предупреждения.** Тип генерируемого предупреждения: электронное письмо, предупреждение SNMP или выполнение программы.
- **Экземпляр.** Указывает конкретный источник предупреждения.

Также можете нажать кнопку **Журнал предупреждений** для открытия журнала предупреждений устройства и просмотра подробностей предупреждений. (См. Просмотр журнала предупреждений для получения дополнительной информации.)

Просмотр журнала предупреждений

Для просмотра предупреждений, отправленных главному серверу (глобальный журнал предупреждений) или контролируемым устройствам, используется страница **Журнал предупреждений**. Журнал сортируется по времени (GMT); последние предупреждения добавляются в начало журнала.

Журнал предупреждений содержит следующие столбцы:

- **Имя предупреждения.** Имя, присвоенное предупреждению, которое указывается на странице **Настройки предупреждения**.
- **Время.** Дата и время генерирования предупреждения (GMT).
- **Состояние.** Состояние предупреждения может быть одним из перечисленных ниже.
  - **Неизвестно.** Невозможно определить состояние.
  - **Информационное.** Определяет изменения конфигурации или события, которые производители могут включить в свои системы.
  - **OK.** Показывает, что состояние устройства на допустимом уровне.
  - **Внимание!** Отображает предупреждения перед тем, как проблема достигнет критической точки.
  - **Критическое.** Указывает на то, что проблема требует немедленного рассмотрения.
- **Экземпляр.** Указывает конкретный источник предупреждения.
- **Имя устройства.** Имя устройства, на котором было сгенерировано предупреждение. Именем устройства должно быть полное доменное имя (только для глобального журнала предупреждений).
- **IP-адрес.** IP-адрес устройства, на котором было сгенерировано предупреждение (только для глобального журнала предупреждений).

Полное доменное имя может не отображаться в том случае, если программе не удалось определить полное доменное имя устройства.

Просмотр глобального журнала предупреждений

1. В левой навигационной панели выберите **Журналы**.
2. Чтобы отсортировать записи по времени, имени, состоянию или экземпляру, щелкните заголовок столбца.
3. Для просмотра более подробного описания предупреждения дважды щелкните его в столбце **Имя предупреждения**.
4. Для получения списка записей журнала по имени, состоянию или экземпляру выберите критерии фильтрации в раскрывающемся списке фильтра. Например, выберите **Имя предупреждения** и введите полное имя (например, "Производительность") или часть имени со знаком подстановки * (например, "Удаленный*"). Для поиска по дате выберите **Включение фильтрации по дате**, введите диапазон дат (начало и конец), затем нажмите **Найти**.
5. Чтобы очистить состояние предупреждения, выберите его нажатием порядкового номера в столбце **Имя предупреждения**, затем нажмите **Очистить предупреждение** и щелкните **OK**. Для удаления записи из журнала выберите предупреждение и нажмите **Удалить запись**.
6. Для удаления всех записей журнала нажмите **Очистить журнал**.

Просмотр журнала предупреждений для конкретного устройства

1. Дважды щелкните устройство в списке **Мои устройства**.
2. В левой навигационной панели выберите **Информация о системе**.
3. Выберите **Журналы**, а затем дважды щелкните **Журнал предупреждений**.
4. Чтобы отсортировать записи по времени, имени, состоянию или экземпляру, щелкните заголовок столбца.
5. Для просмотра более подробного описания предупреждения щелкните его в столбце **Имя предупреждения**.
6. Для получения списка записей по имени, состоянию или экземпляру нажмите кнопку **Фильтр** на панели инструментов и выберите критерии фильтрации. Например, выберите **Имя предупреждения** и введите полное имя (например, "Производительность") или часть имени со знаком подстановки * (например, "Удаленный*"). Затем щелкните "Найти" на панели инструментов для просмотра предупреждений, отвечающих указанным критериям фильтрации.
7. Чтобы просмотреть записи журнала за определенное время, снимите флажок **Показать события для всех дат** и укажите диапазон дат. Нажмите **Обновить** для отображения записей этого диапазона дат.

Обновления программного обеспечения

System Manager содержит инструмент обновлений программного обеспечения для поиска обновлений приложения управления, операционной системы и драйверов устройств. После выгрузки и установки этих обновлений (также называются исправлениями) можно исправить необходимые устройства.

В этой главе вы изучите следующее:

Обзор обновлений программного обеспечения

Средство обновления программного обеспечения предназначено для поддержания на современном уровне программного обеспечения управляемых устройств вашей сети. Можно автоматизировать периодичность процесса обслуживания текущего программного обеспечения, загрузки файлов соответствующих обновлений, развертывания и установки необходимых обновлений в нужные устройства.

В этом продукте используется стандартное ролевое администрирование для назначения доступа пользователей, имеющих утилиту обновлений программного обеспечения. Ролевое администрирование - это модель организации доступа продукта и модели защиты, которая позволяет администраторам ограничивать доступ к утилитам и устройствам. Каждый пользователь имеет назначенные права и область, определяющую функции, которые он может использовать, и устройства, которыми он может управлять. Администратор назначает эти права другим пользователям (см. раздел О ролевом администрировании для получения дополнительной информации). Для использования утилиты обновлений программного обеспечения пользователю нужно войти в систему с правами для управления исправлениями, основной Web-консолью и отчетами.

Поддерживаемые серверные платформы

Обновления программного обеспечения предназначены для большинства серверных платформ, позволяя сканировать обновления и развертывать их в управляемых серверах, работающих под управлением следующих операционных систем:

- Windows 2000 Server SP4

- Windows 2000 Advanced Server SP4
- Windows 2000 Professional SP4
- Windows 2003 Standard Edition SP1
- Windows 2003 Enterprise Edition SP1
- Windows XP Pro SP2
- RedHat Enterprise Linux ES/AS 3
- SUSE Linux Server 9 (Professional, Enterprise и Advanced)

Окно "Обновления программного обеспечения"

Пользователи, имеющие права на использование исправлений, смогут увидеть утилиту **Обновления программного обеспечения** в левой навигационной панели консоли. После того, как вы щелкните **Обновления программного обеспечения**, вы увидите инструментальную панель и две панели в правой части окна. В левой панели отображается структура дерева групп обновлений программного обеспечения. Выберите группу для отображения ее содержимого в правой панели. На правой панели в виде столбца отображаются сведения обновлений программного обеспечения. В верхней части находится кнопка **Найти** для быстрого поиска по заданным критериям. В окне **Найти** не поддерживаются следующие специальные символы: <, >, ', ", !.

Кнопки инструментальной панели

- **Обновить.** Открывает диалог **Обновить настройки обнаружения уязвимых мест**, в котором можно указать платформы и языки, для которых нужно обновить информацию о программном обеспечении. Также можно указать место размещения обновлений в группе **Сканировать** или можно выгрузить соответствующие исправления в место загрузки обновлений и настроек прокси-сервера.
- **Запланировать загрузку.** Используется для открытия диалога **Запланированная задача**, в котором можно настроить параметры задачи. После нажатия **Сохранить** загружаемая задача помещается в окно **Запланированные задачи** на вкладке **Задачи обнаружения уязвимых мест**.
- **Задачи планирования исправлений.** Открывает диалог **Задачи планирования исправлений**, в котором можно указать имя и параметры сканера.
- **Обновить.** Обновляет список информации о последних загруженных обновлениях на правой панели.
- **Удалить.** Открывает диалог **Удалить определения защиты и исправлений**, в котором можно указать платформы и языки, для которых нужно удалить из базы данных информацию об уязвимых местах.

Левая панель (вид дерева)

В левой панели окна отображаются следующие группы:

- **Сканировать.** Перечисляет все обновления, обнаруженные во время работы утилиты обновлений в управляемых устройствах. Другими словами, если обновление включено в эту группу, оно будет входить в операцию следующего сканирования; в противном случае, оно не будет просканировано.

  Сканирование может рассматриваться в виде одного из трех состояний уязвимых мест, наряду с функциями "Не сканировать" и "Не назначено". Поэтому, обновление программного обеспечения может находиться одновременно только в одной из этих групп. Каждое состояние идентифицируется уникальным значком (знак вопроса (?) - не назначено, красный крестик (X) - не сканировать и обычный значок сканирования уязвимых мест). Перемещение обновления из одной группы в другую автоматически меняет его состояние.

  Для перемещения обновления программного обеспечения из одной группы в другую щелкните правой кнопкой мыши обновление и выберите группу.

  Переместив обновления в группу "Сканировать", вы сможете управлять поведением и контролировать размер следующего сканирования обновлений программного обеспечения.

  Новые обновления могут быть также автоматически добавлены в группу "Сканировать" во время обновления с проверкой параметра **Поместить новые определения в группу "Сканировать"** из диалога **Обновить настройки обнаружения уязвимых мест**.

  Предосторожности при перемещении обновлений из группы "Сканировать"
  Когда вы перемещаете обновления программного обеспечения из группы "Сканировать" в группу "Не сканировать", текущая информация базы данных главного сервера о сканированных устройствах, обнаруживших эти обновления, удаляется из базы данных и более не будет доступна в диалоге свойств обновления программного обеспечения или в диалоге информации сканирований сервера. Для восстановления необходимой информации нужно переместить обновления программного обеспечения назад в группу сканирования и запустить процесс сканирования.

- **Не сканировать.** Перечисляет обновления программного обеспечения, поиск которых не будет выполняться при следующем запуске в устройствах процесса сканирования. Как уже говорилось ранее, если обновление находится в этой группе, оно не может также находиться в группах "Сканировать" или "Не назначено". Вы можете переместить обновления в эту группу для удаления их из процесса сканирования программного обеспечения.

- **Обнаружено.** Перечисляет обновления программного обеспечения, обнаруженные при предыдущем сканировании, для всех целевых устройств, включенных в эту операцию сканирования. Содержимое этой группы всегда определяется по последнему сканированию обновлений программного обеспечения на основании сведений о выполнении сканирования на одном или нескольких устройствах.

  Список обнаруженных уязвимых мест включает все обновления программного обеспечения, обнаруженные во время последнего сканирования. В столбцах сканированных и обнаруженных обновлений отображается, сколько устройств было просканировано, и сколько обновлений было обнаружено для этих устройств. Для того чтобы увидеть, какие серверы имеют обнаруженные обновления, щелкните правой кнопкой мыши определение в окне **Показать задействованные компьютеры**. Помните, что информацию об обновлениях для конкретного сервера можно просмотреть в диалоге Информационная консоль сервера.

  Вы можете только перемещать определения обновлений программного обеспечения мест из группы обнаруженных в группу не назначенных или группу, запрещающую сканирование.

- **Не назначено.** Перечисляет обновления программного обеспечения, которые не включены в группы сканирования и запрещения сканирования. Группа не назначенных определений - это группа определений обновлений программного обеспечения, хранимых до принятия решения о необходимости их сканирования.

  По умолчанию накопленные определения обновлений добавляются во время обновления в группу "Сканировать".

  Вы можете переместить определения обновлений программного обеспечения из группы не назначенных в группу сканирования или группу, запрещающую сканирование.

- **Проверить с помощью ОС.** Перечисляет все загруженные обновления программного обеспечения, организованные в специальные подгруппы по операционным системам устройств. Эти подгруппы помогают идентифицировать обновления по категории ОС. Вы можете использовать эти подгруппы ОС для помещения обновлений программного обеспечения в группу сканирования для сканирования только конкретных операционных систем.

  Определения обновлений программного обеспечения могут быть скопированы из группы ОС в группы сканирования, запрещения сканирования или не назначенных определений. Обновления могут находиться одновременно в нескольких группах платформ и/или продуктов.

- **Отобразить по продуктам.** Перечисляет все загруженные обновления программного обеспечения, организованные в специальные подгруппы по продуктам. Эти подгруппы помогают идентифицировать обновления по категории продуктов. Вы можете использовать эти подгруппы продуктов для помещения обновлений в группу сканирования для сканирования только определенных продуктов.

Правая панель (список)

На правой панели окна отображаются следующие сведения обновлений программного обеспечения в виде отсортированных столбцов:

- **Идентификатор.** Идентифицирует обновление с помощью уникального кода изготовителя.
- **Важность.** Показывает уровень важности обновления. Возможные уровни важности: пакет обновления, критическое, высокого приоритета, среднего приоритета, низкого приоритета, не применимо и неизвестное.
- **Название.** Кратко описывает природу и назначение обновления.
- **Язык.** Указывает язык операционной системы, для которого предназначено обновление.
- **Дата публикации.** Указывает дату публикации обновления изготовителем.
- **Автоматическая установка.** Указывает на возможную автоматическую установку файла исправления ассоциированного обновления (без участия пользователя). Некоторые обновления могут содержать несколько исправлений. Если исправления, входящие в обновление, не устанавливаются автоматически, атрибут автоматической установки установлен в значение "Нет".
- **Исправимое.** Указывает, может ли обновление программного обеспечения быть исправлено с помощью развертывания или установки файла исправления. Возможные значения: "Да", "Нет" и "Некоторые" (для обновлений, которые содержат несколько правил обнаружения и не для всех обнаруженных обновлений, которые могут быть исправлены).

Щелкните дважды идентификатор обновления для отображения дополнительной информации в диалоге свойств. В диалоге свойств обновления программного обеспечения можно найти правила обнаружения обновления, загрузить ассоциированные файлы исправлений и выбрать правило для отображения подробного диалога его свойств.

Конфигурация устройств для сканирования обновлений программного обеспечения

Перед тем, как управляемые устройства могут быть просканированы на наличие уязвимых мест и получат исправления, в них нужно установить агентов обновления программного обеспечения.

Самым простым способом развертывания агентов обновления программного обеспечения в несколько управляемых устройств является создание конфигурации нового агента с выбранными для него обновлениями программного обеспечения (установлено по умолчанию) и последующее назначение конфигураций для нужных целевых устройств с **запланированными задачами**.

Во время конфигурации устройств поддержки для обновлений программного обеспечения необходимые файлы для сканирования обновлений и исправлений (например, развертывание и установка исправлений) устанавливаются в целевые устройства.

Определения обновлений программного обеспечения

В вашей сети постоянно можно найти уязвимые места, в которых существуют проблемы, связанные с необходимостью установки обновлений программного обеспечения и исправлением проблем. Утилита обновлений программного обеспечения быстро выполняет сбор информации о самых свежих исправлениях, позволяя вам обновлять программное обеспечение, используя базу данных, хранимую LANDesk. Данная служба накапливает известные обновления, получаемые из авторитетных источников признанных производителей/поставщиков.

Поддерживая и обслуживая информацию о современных исправлениях, вы будете лучше понимать природу и потребность установки обновлений программного обеспечения для операционной системы каждого поддерживаемого вами сервера. Во-первых, необходимо поддерживать информацию об обновлениях на современном уровне.

Вы можете сконфигурировать и выполнить единовременное обновление программного обеспечения или создать запланированные задачи для периодического выполнения обновлений.

Обновление информации обновлений программного обеспечения

1. В левой навигационной панели выберите **Обновления программного обеспечения**. (Описание этого диалога см. в разделе Окно "Обновления программного обеспечения".)
2. Нажмите кнопку панели задач **Обновить**.
3. Выберите сайт-источник загрузки из списка доступных серверов.
4. Выберите платформы, информацию об обновлении программного обеспечения которых, нужно обновить. Вы можете выбрать из списка одну или несколько платформ. Чем больше платформ вы выберете, тем дольше будет выполняться обновление.
5. Выберите языки, информацию об обновлении программного обеспечения которых, нужно обновить для указанных платформ. Вы можете выбрать из списка один или несколько языков. Чем больше языков вы выберете, тем дольше будет выполняться обновление.
6. Если нужно, чтобы определения обновлений программного обеспечения (например, уже существующие в базе данных) автоматически помещались в группу не назначенных обновлений вместо местоположения по умолчанию (группа сканирования), отмените выбор параметра **Поместить новые определения в группу "Сканировать"**.
7. Если нужно автоматически загружать действительные файлы исполнимых исправлений, отметьте параметр **Загрузить исправления для указанных выше определений** и выберите один из параметров загрузки.

    - **Только для обнаруженных определений.** Выполняет загрузку только тех исправлений, которые ассоциированы с обнаруженными обновлениями программного обеспечения во время последнего сканирования обновлений (например, обновления, находящиеся сейчас в группе обнаруженных обновлений).
    - **Для всех указанных определений.** Загружает ВСЕ исправления, ассоциированные с обновлениями программного обеспечения, находящимися сейчас в группе сканирования. Это может занять достаточно долго времени.

Исправления загружаются в местоположение, указанное в диалоге раздела "Настройки исправления" (см. процедуру далее).

8. Если в вашей сети для передачи информации в Интернет используется прокси-сервер (необходимо обновить информацию определений для обновлений программного обеспечения и загрузить исправления), выберите вкладку **Настройки прокси** и отметьте параметр **Использовать прокси-сервер**. Укажите адрес сервера, номер порта и идентификационную информацию, если таковые нужны для входа в прокси-сервер.
9. В любое время можно нажать **Применить** для сохранения настроек.
10. Щелкните **Обновить сейчас** для запуска обновления программного обеспечения. В диалоге **Обновить определения защиты и исправлений** отобразится состояние текущей операции.
11. Когда обновление завершится, нажмите **Закрыть**. Если вы выберете **Отмена** до завершения обновления, будет обработана только информация об обновлении программного обеспечения, которая была загружена в базу данных главного сервера. Потребуется вновь запустить обновление для получения оставшейся информации.

Примечание. Не закрывайте консоль, пока выполняется процесс обновления, иначе он будет прекращен. Это не относится к задаче запланированной загрузки.

Если программное обеспечение System Manager и LANDesk® Management Suite установлены в один главный сервер, оба эти приложения используют одни настройки для определения типов обновляемых определений уязвимых мест. В некоторых случаях после запуска процесса обновления в System Manager отображаются обновления, которые конфигурируются в программном обеспечении Management Suite. Например, если для обновления в Management Suite был выбран параметр обновления определений обновлений программного обеспечения, а после этого в System Manager было выбрано обновление определений обновлений программного обеспечения, после запуска обновлений в System Manager будут отображаться элементы обновления определений обновлений программного обеспечения и для угроз защиты.

Конфигурация местоположения загрузки исправления

1. В диалоге **Обновить настройки обнаружения уязвимых мест** выберите вкладку **Настройки исправления**.
2. Введите путь UNC, в который нужно скопировать файлы исправления. Местоположение по умолчанию - каталог \LDLogon\Patch.
3. Если введенный путь UNC отличен от пути для главного сервера, введите допустимое имя пользователя и пароль для аутентификации в новом местоположении.

   Папка должна иметь разрешение для совместного использования и анонимного доступа.

4. Введите Web-адрес, откуда серверы могут загружать исправления для последующего развертывания. Web-адрес должен совпадать с указанным выше путем UNC.
5. Вы можете выбрать **Настройки тестирования** для проверки подключения к указанному выше Web-адресу.

6. Если нужно восстановить значения по умолчанию для пути UNC и Web-адреса, выберите **Сброс настроек исправления**. Местоположение по умолчанию - каталог \LDLogon\Patch.

Планирование загрузки обновлений программного обеспечения

Вы можете сконфигурировать задачу обновления программного обеспечения в виде запланированной задачи для периодического автоматического выполнения в будущем в указанное время. Для этого нажмите кнопку панели задач **Запланировать загрузку** для открытия диалога **Запланированная задача - свойства**, в котором можно назвать задачу и сконфигурировать ее параметры. После того, как вы нажмете **Сохранить**, задача появится в окне запланированных задач.

Все запланированные задачи обновления определений обновлений программного обеспечения будут использовать текущие настройки, находящиеся в диалоге **Обновить настройки обнаружения уязвимых мест**. Таким образом, если потребуется изменить сайт-источник, платформы, языки, сайт загрузки исправлений или настройки прокси-сервера для определенного задания обновления, нужно сначала изменить эти параметры в **настройках обновлений для уязвимых мест**, а потом запланировать запуск задачи.

Конфигурация задачи планирования загрузки

1. В левой навигационной панели выберите **Обновления программного обеспечения**.
2. Выберите **Запланировать загрузку**.
3. На странице **Назначить задачу** сконфигурируйте ее расписание.
4. Нажмите **Сохранить**.

После того, как вы выберете **Запланировать загрузку**, задача будет создана (в ней еще не указаны целевые устройства и не создано расписание). Если вы отмените процедуру **запланированной задачи**, убедитесь, что она была удалена и более не отображается в списке **Мои задачи**.

Просмотр обновления программного обеспечения и информации правила обнаружения

После обновления информации обновлений программного обеспечения из службы безопасности LANDesk, вы можете на консоли увидеть списки обновлений, сортировать их по платформам и продуктам, и перемещать обновления в различные группы по состояниям. Для получения дополнительной информации о различных группах, отображаемых в окне, и вариантах их использования, см. раздел Окно "Обновления программного обеспечения".

Дл отображения сведений программного обеспечения дважды щелкните ИД обновления программного обеспечения для открытия диалога свойств. Из этого диалога также можно получить доступ к информации **правил обнаружения**, дважды щелкнув имя файла исправления в списке правил обнаружения для открытия диалога свойств исправления (см. раздел Обновления программного обеспечения).

Эта информация может быть полезна при определении важных обновлений для ваших платформ поддерживаемых серверов, при определении действий правил обнаружения обновлений во время проверки уязвимых мест, для проверки доступности исправлений и получения сведений о конфигурации и выполнении исправлений задействованных устройств.

Также непосредственно с консоли можно отобразить определение обновления программного обеспечения и конкретную информацию правила обнаружения для сканируемых устройств, выбрав на консоли список **Мои устройства** и нажав **Обновления программного обеспечения** в левой навигационной панели.

Очистка информации обновлений программного обеспечения

В окне обновлений программного обеспечения можно очистить информацию об обновлениях (и впоследствии из базы данных главного сервера), если вы обнаружите, что она не соответствует действительной информации.

Во время очистки информации обновления программного обеспечения из базы данных также удаляется ассоциированная информация правил обнаружения. Однако во время этого процесса сами исполнимые файлы исправлений не удаляются. Файлы исправлений должны быть удалены вручную из локального хранилища, которое обычно располагается в главном сервере.

Очистка информации обновлений программного обеспечения

1. Нажмите кнопку **Удалить** на панели задач. (Описание диалога см. в разделе Диалог удаления неиспользуемой информации об уязвимых местах).
2. Выберите платформы, информацию об обновлениях программного обеспечения которых нужно удалить. Вы можете выбрать из списка одну или несколько платформ.

   Если определение обновления ассоциировано с одной или несколькими платформами, нужно выбрать все эти платформы в порядке удаления информации.

3. Выберите языки, информацию об обновлении программного обеспечения которых нужно удалить (ассоциированные с указанными выше платформами).

   Если была выбрана платформа Windows, для удаления нужно указать информацию определения обновления программного обеспечения для нужно языка. Если была выбрана платформа UNIX, нужно указать независимый от языка параметр (Language-neutral) для удаления сведений обновления сразу для нескольких языков.

4. Нажмите **Удалить**.

Сканирование устройств для обновлений программного обеспечения

Оценка обновления программного обеспечения означает проверку текущих установленных версий рабочих файлов для конкретных операционных систем и ключей реестра устройств

в отношении текущих известных обновлений программного обеспечения для идентификации необходимых обновлений для серверов. После проверки информации текущих известных обновлений программного обеспечения (получаемых их известных в отрасли источников) и принятия решения о необходимости сканирования нужных обновлений вы можете выполнить выборочную оценку обновлений в управляемых серверах, в которых установлен агент обновления программного обеспечения. (Для получения информации о конфигурации устройств для сканирования и развертывания исправлений см. раздел Конфигурация устройств для сканирования обновлений программного обеспечения, описанный ранее в этой главе).

Во время выполнения сканирования обновления программного обеспечения всегда происходит считывание содержимого группы сканирования и поиск указанных в ней обновлений. Перед сканированием серверов для обновлений нужно всегда проверять, что необходимые обновления включены в эту группу. Вы можете переместить обновления программного обеспечения в группу сканирования для настройки объема и выполнения сканирования.

Выполнение сканирования программного обеспечения

Сканирование обновлений программного обеспечения может быть принудительно запущено с консоли в виде запланированной задачи.

Создание задачи сканирования обновлений программного обеспечения

1. В левой навигационной панели выберите **Обновления программного обеспечения**.
2. Проверьте, что определения обновлений программного обеспечения были недавно обновлены.
3. Проверьте, что группа сканирования содержит только нужные обновления.
4. Нажмите кнопку **Задачи планирования исправлений** на панели задач. (Описание диалога см. в разделе "О диалоге описания сканирования уязвимых мест").
5. Введите уникальное имя задачи сканирования. Если сценарий задачи уже существует, вы можете перезаписать существующий сценарий.
6. Укажите, нужно ли в целевом устройстве отображать диалог процесса выполнения сканирования обновлений программного обеспечения. Также можно указать, нужно ли отображать кнопку "Отмена" в диалоге сканирования, чтобы пользователь имел возможность отменить этот процесс.
7. Выберите, нужно ли закрыть диалог сканера обновлений программного обеспечения после завершения работы на целевых устройствах. Можно указать, чтобы этот диалог был закрыт пользователем или автоматически через определенный промежуток времени.
8. Нажмите **OK**.
9. На нижней панели выберите задачу (в списке **Задачи обнаружения уязвимых мест**) и щелкните **Правка**. Выберите целевые устройства и параметры расписания, а затем выберите **Сохранить**.

Просмотр обнаруженных обновлений

Если сканер обнаружит новые версии обновлений программного обеспечения на любом их целевых устройств, информация обнаружения будет сообщена в главный сервер и добавлена в список **обнаруженных** обновлений.

Вы можете использовать любой из следующих способов для просмотра обнаруженных обновлений после выполнения их сканирования:

По группе "Обнаруженные"

В окне обновлений программного обеспечения выберите группу **Обнаруженные** для отображения полного списка всех обновлений, обнаруженных при последнем сканировании.

По отдельному устройству

Дважды щелкните имя устройства в списке **Мои устройства** и выберите **Обновления программного обеспечения** для отображения информации оценки обновлений программного обеспечения для этого устройства.

Загрузка исправлений

Для развертывания исправлений в устройствах с обнаруженными обновлениями программного обеспечения необходимо сначала загрузить исполнимый файл исправления в сетевое локальное хранилище исправлений. По умолчанию местоположение для загрузки файлов исправлений находится в каталоге главного сервера /LDLogon. Это местоположение можно изменить на вкладке **настроек исправления** диалога **Настройки обновлений уязвимых мест**.

Местоположение загрузки исправлений и настройки прокси-сервера
Во время загрузки исправлений всегда используются настройки загрузки, находящиеся на вкладке **настроек исправлений** диалога **настроек обновлений уязвимых мест**. Также помните, что если для доступа в Интернет используется прокси-сервер, для загрузки файлов исправлений нужно сначала сконфигурировать его параметры в разделе **настроек прокси-сервера** диалога **настроек обновления уязвимых мест**.

Продукт сначала попытается загрузить файл исправлений из указанного сетевого адреса (показано в диалоге "Свойства исправления"). Если не удалось выполнить подключение или исправление недоступно по какой-либо причине, продукт выполнит загрузку исправления с помощью службы защиты LANDesk, которая представляет собой базу данных компании, содержащую исправления, полученные из доверенных источников.

Вы можете загружать исправления по одному или выбрать набор исправлений для их одновременной загрузки.

Загрузка одного исправления

1. Дважды щелкните имя обновления программного обеспечения для открытия диалога **Свойства**.
2. В разделе **Правила обнаружения** выберите необходимые для загрузки файлы исправления для правила обнаружения и нажмите **Загрузить выбранные исправления**.
3. Процесс загрузки и его состояние отображаются в диалоге **Загрузка исправлений**. В любое время можно нажать кнопку **Отмена** для остановки всего процесса загрузки.
4. После завершения процесса загрузки нажмите кнопку **Закрыть**.

Загрузка нескольких исправлений

Все запланированные задачи обновления определений обновлений программного обеспечения будут использовать текущие настройки, находящиеся в диалоге **Обновить настройки обнаружения уязвимых мест**. Таким образом, если потребуется изменить сайт-источник, платформы, языки, сайт загрузки исправлений или настройки прокси-сервера для определенного задания обновления, нужно сначала изменить эти параметры в **настройках обновлений для уязвимых мест**, а потом запланировать запуск задачи.

1. В левой навигационной панели выберите **Обновления программного обеспечения**.
2. Выберите **Запланировать загрузку**.
3. На странице **Назначить задачу** выполните настройки расписания.
4. Нажмите **Сохранить**.

Удаление файлов исправлений

Для удаления файлов исправлений нужно вручную удалить файлы из хранилища исправлений, которое обычно находится в каталоге LDLogon главного сервера.

Исправление обновлений программного обеспечения

После обновления определений обновлений программного обеспечения нужно поместить необходимые обновления в группу сканирования, запустить сканирование на управляемых устройствах, определить обновления, для которых нужны исправления, и выгрузить необходимые исправления, а затем выполнить исправление путем их развертывания и установки в выбранных целевых устройствах.

Исправление обновлений выполняется путем модернизации отдельных обновлений программного обеспечения. Другими словами, нужно создать задачу исправления для конкретного обновления, которая развертывает и устанавливает необходимые файлы исправлений.

Помните, что исправление, подобно сканированию обновлений программного обеспечения, работает только на сконфигурированных с помощью агента обновлений программного обеспечения устройствах. Дополнительную информацию см. в описанной ранее главе Конфигурация устройств для сканирования обновлений программного обеспечения.

Исправление может быть выполнено в системе Linux. Вы можете использовать утилиту обновлений программного обеспечения для обнаружения уязвимых мест в устройствах Linux, а затем решить, нужно ли выполнять исправления обновлений. Если вы решите, что исправления необходимы, можно использовать подписку поставщика Linux для загрузки необходимых модулей RPM, а затем для развертывания в устройствах этих пакетов RPM.

Внимание! Многие исправления после установки автоматически перезагружают устройства.

Создание выборочной задачи исправления

1. В левой навигационной панели выберите **Обновления программного обеспечения**.
2. Выберите группу **Обнаруженные** для просмотра обновлений программного обеспечения, обнаруженных во время последнего сканирования. (Необязательно выбирать эту группу. Если нужно создать выборочный сценарий исправления для обновления, которое не было просканировано или еще не было обнаружено, щелкните другие группы уязвимых мест для отображения их содержимого и выбора нужного уязвимого места).
3. Щелкните правой кнопкой определение, затем выберите параметр **Показать задействованные устройства** для отображения устройств, задействованных при обновлении программного обеспечения.
4. Щелкните правой кнопкой определение, а затем выберите **Создать задачу исправления**.
5. (Необязательно). Измените имя задачи в текстовом поле **Имя задачи**.
6. Выберите нужные параметры и нажмите **OK**.
    - **Копировать задействованные компьютеры в целевую область.** Копирует компьютеры, задействованные в обновлении программного обеспечения в целевой список исправления.
    - **Показать процесс выполнения.** Позволяет сканеру отображать информацию о выполнении в устройствах конечного пользователя. Выберите этот параметр, если нужно отобразить активность процесса сканирования и если нужно сконфигурировать в этом диалоге другие параметры отображения и воздействия на процесс. Если вы не выберете этот параметр, параметры не будут доступны для конфигурации, а процесс сканирования устройств будет скрыт от пользователя.
    - **Требовать вмешательства пользователя при закрытии диалога сканирования уязвимых мест**. Выберите этот параметр, если нужно, чтобы сканер известил пользователя перед закрытием диалога в устройстве. Если вы выберете этот параметр, и конечный пользователь не ответит на запрос, а диалог останется открытым, это может привести к тайм-ауту других запланированных задач.
    - **Закрыть диалог автоматически после тайм-аута.** Выберите этот параметр для закрытия диалога сканера по истечении указанного времени.

Сценарии

Сценарии управления

Для выполнения выборочных задач на устройствах в данном продукте используются сценарии. После выполнения действий в диалоговом окне создания сценария будет создан файл ASCII в формате INI-файлов Windows с расширением .INI. Эти сценарии хранятся на главном сервере в папке \Program Files\LANDesk\ManagementSuite\Scripts. Имя файла сценария становится именем сценария на консоли. Вы можете создавать сценарии локального планировщика для устройств Windows в окне **Сценарии** (в левой навигационной панели нажмите **Сценарии**) или писать свои собственные файлы сценариев и сохранять их в папке "Сценарии".

В окне **Сценарии** сами сценарии разбиты на следующие категории:

- **Мои сценарии.** Сценарии, которые вы ассоциируете с данной группой.
- **Все другие сценарии.** Все сценарии на главном сервере.
- **Сценарии пользователя** (доступны только администраторам). Сценарии, созданные всеми пользователями продукта. Эти сценарии сортируются создателем.

В окне **Мои сценарии** можно создавать группы для дальнейшей классификации ваших сценариев. Для создания нового сценария локального планировщика нажмите кнопку **Локальный**.

После создания сценария в его контекстном меню можно выбрать **Расписание**. В окне **Мои устройства** можно назначить устройства для выполнения необходимых задач. Можно также запланировать запуск задачи в окне **Запланированные задачи**. Дополнительную информацию о планировании задач см. в разделе "Планирование задач".

Изменение информации о владельце сценариев и задач для пользователей предыдущих версий Management Suite

В предыдущих версиях Management Suite (версиях, предшествующих 8.70) все сценарии были доступны для просмотра всем пользователям. Теперь сценарии могут видеть только их создатель и администраторы.

В окне **Сценарии** имеется столбец "Состояние". Если все пользователи могут просматривать сценарий, в столбце "Состояние" отображается "Общий". В противном случае, если сценарий могут видеть только создавший его пользователь или администраторы, в этом столбце отображается "Закрытый". Для изменения состояния сценария пользователи могут щелкнуть правой кнопкой мыши созданные ими сценарии и выбрать "Закрытый" или "Общий". Администраторы могут изменять состояние любого сценария.

По умолчанию используется DOS PE (процессорный элемент DOS). При выборе любого другого ПЭ вы не сможете создавать командный сценарий. Для ПЭ Windows и Linux вы можете создавать только сценарий захвата или развертывания.

При выборе ПЭ Linux вы сможете пользоваться только параметрами LANDesk или средствами обработки изображений в разделе "Другие". При выборе ПЭ Windows вы сможете пользоваться опциями LANDesk, средствами обработки изображений в разделе "Другие" и Microsoft* XImage.

Создание сценария локального планировщика

Локальный планировщик является службой, запускаемой на устройствах. Он устанавливается при развертывании конфигурации агентов как часть стандартного агента управления. Обычно локальный планировщик выполняет обработку задач продукта, например, периодический запуск сканера инвентаризации. Другие планируемые вами задачи выполняются главным сервером, а не локальным планировщиком. Локальный планировщик можно использовать для планирования собственных задач для их периодического запуска на устройствах. После создания сценария локального планировщика его можно развернуть на других управляемых устройствах, как и любые другие сценарии.

Локальный планировщик назначает каждому заданию идентификационный номер. Сценарий локального планировщика использует диапазон идентификаторов, отличающийся от используемых продуктом сценариев локального планировщика по умолчанию. Активным на каждом устройстве может быть только один выборочный сценарий планировщика. При создании и развертывании на других устройствах нового сценария он заменит старый сценарий (любой сценарий в диапазоне идентификаторов выборочного локального планировщика) без влияния на сценарии локального планировщика по умолчанию, например, на расписание локального сканирования инвентаризации.

При выборе параметров расписания для сценария имейте в виде, что для ряда параметров существуют ограничительные характеристики. Например, если вы выбрали "Понедельник" в качестве дня недели и "17" в качестве дня месяца, задание будет выполняться только в тот понедельник, на который выпадет семнадцатое число месяца, что происходит очень редко.

Вы можете создать сценарий для запуска файла restartmon.exe на локальной машине немедленно или в любое удобное для вас время. Если получение отчетов с конкретной машины прекратилось, воспользуйтесь файлом restartmon.exe в папке LDClient для перезапуска коллектора данных и всех провайдеров мониторинга. Эта утилита предназначена для машин, на которых была установлена служба предоставления отчетов, но получение отчетов прекратилось. Используйте эту утилиту для перезапуска коллектора данных и провайдеров без перезагрузки устройства.

1. В левой навигационной панели нажмите **Сценарии**.
2. Нажмите кнопку **Локальный**.
3. Введите имя сценария.
4. Для определения параметров сценария нажмите **Добавить**.
5. Настройте параметры локального планировщика, как было описано ранее. После завершения нажмите **Сохранить**.

6. Для сохранения сценария нажмите **Сохранить**.
7. Выберите сценарий из группы **Мои сценарии**, затем нажмите **Расписание** для развертывания сценария, созданного вами для устройств.

О параметрах полосы пропускания

При конфигурации команд локального планировщика можно указать минимальную полосу пропускания управляемого устройства для выполнения задания. Если пришло время для запуска задания, каждое устройство с работающим локальным планировщиком отправляет небольшое количество сетевых пакетов ICMP на указанный вами компьютер для оценки производительности передачи. Если целевой компьютер недоступен, задача не будет запущена.

Можно выбрать следующие параметры полосы пропускания:

- **RAS.** Задача выполняется, если сетевое соединение устройства с целевым компьютером осуществляется, как минимум, со скоростью, обеспечивающей работу службы удалённого доступа RAS, или со скоростью коммутируемого соединения dialup. При выборе этого параметра обычно задача запускается всегда, если установлено сетевое соединение устройства любого типа.
- **WAN.** Задача выполняется, если соединение устройства с целевым компьютером осуществляется со скоростью глобальной сети WAN. Скорость глобальной сети WAN определяется как соединение, отличное от RAS, которое является более медленным, чем пороговая величина локальной сети LAN.
- **ЛС.** Задача выполняется, если соединение устройства с целевым компьютером превышает скорость ЛС. Скорость ЛС по умолчанию определяется как 262144 бит в секунду.

Планирование задач сценариев

В окне **Запланированные задачи** отображается состояние запланированных задач, их выполнение и завершение. Служба планировщика взаимодействует с устройствами двумя следующими способами:

- С помощью стандартного агента управления (должен быть установлен в устройствах).
- С помощью системной учетной записи на уровне домена. Выбранная учетная запись должна иметь для входа привилегии службы и имя и пароль должны быть указаны в утилите конфигурации служб. Дополнительную информацию о настройке учетной записи планировщика см. в разделе "Конфигурация службы планировщика".

LANDesk устанавливает несколько стандартных сценариев, которые можно использовать для выполнения служебных задач, например, запуск сканирования базы данных инвентаризации в выбранных устройствах. В левой навигационной панели выберите **Сценарии**, а затем для просмотра и планирования этих сценариев выберите **Все другие сценарии**.

Планирование задачи

1. В левой навигационной панели нажмите **Сценарии**.

2. Перейдите к группе сценариев.
3. Выберите сценарий и нажмите **Расписание**.
4. Введите имя задачи и нажмите **OK**.
5. На вкладке **Задачи выборочного сценария** выберите **Все задачи**, выберите задачу с назначенным в действии 3 именем и нажмите **Правка**.
6. Заполните страницы задач выборочного сценария. Для получения справки на любой странице нажмите кнопку "Справка" или см. справку Планировщик задач.

После того, как вы выберете **Расписание**, задача будет создана (в ней еще не указаны целевые устройства и не создано расписание). При отмене процедуры планирования задачи будьте внимательны, так как задача все равно будет создана и появится в списке "Задачи".

Использование сценариев по умолчанию

Данный продукт поставляется с двумя сценариями по умолчанию. Их можно использовать для выполнения некоторых обычных задач. Эти сценарии доступны при выборе дерева **Все другие сценарии** в окне **Сценарии** (левая навигационная панель **| Сценарии**).

- **Сканер инвентаризации.** Для выбранных устройств запускается сканер инвентаризации. Этот сценарий содержит документацию, в которой описывается, как записывать файл сценария; для получения дополнительной информации о правильном использовании команд и параметров прочитайте или напечатайте этот файл сценария.
- **Восстановление записей клиента.** Для выбранных устройств запускается сканер инвентаризации, но отчеты сканирования отправляются в базу данных главного сервера, с которой было сконфигурировано данное устройство. При восстановлении базы данных данная задача позволяет добавлять устройства в нужную базу данных главного сервера в среде с несколькими базами данных главных серверов.

Планирование задач

Утилита **Запланированные задачи** является общей для конфигурации агентов, обновлений ПО, сценариев и обнаружения устройств. Задания фильтруются на нижней панели страниц определенных функций и отображают только результаты, имеющие к ним непосредственное отношение. Например, если открыть средство **Обнаружение устройств**, задания обнаружения отобразятся на вкладке **Задачи обнаружения** на нижней панели. Все задания можно просмотреть с помощью утилиты **Запланированные задачи**. Здесь вы можете запланировать выполнение конфигураций немедленно, в определенный момент времени в будущем, запустить в соответствие с определенным графиком или однократно.

На левой панели страницы **Запланированные задачи** отображаются следующие группы заданий:

- **Мои задачи.** Запланированные вами задачи. Эти задачи можете видеть только вы и пользователи с правами администратора.
- **Все задачи.** Ваши задачи и задачи, помеченные как общедоступные.
- **Стандартные задачи.** Задачи, помеченные пользователями как стандартные. Каждый, кто редактирует или выбирает задание из этой группы, становится его владельцем. Задача остается в группе стандартных задач, а также отображается в группе "Задачи пользователя" для данного пользователя.
- **Задачи пользователя** (только для пользователей с правами администратора). Задачи, созданные пользователями.

При выборе параметров **Мои задачи**, **Стандартные задачи** или **Все задачи**, на правой панели отображается следующая информация:

- **Задача.** Имена задач.
- **Вкл.** Время выполнения запланированной задачи. Выберите имя задачи, затем **Правка** для редактирования времени начала работы или его изменения.
- **Состояние.** Общее состояние задачи. Подробную информацию см. на правой панели столбца "Состояние". На правой панели отображается состояние задания, которое может быть следующим: "Обработка", "Все выполнено", "Ничего не выполнено", "Ошибка".
- **Пакет для распространения.** Пакет определяет распространение задач. Это поле используется для распространения ПО.
- **Метод доставки.** Метод доставки, используемый задачей. Это поле используется для распространения ПО.
- **Владелец.** Имя лица, создавшего сценарий, который используется данным заданием.

Если дважды щелкнуть запланированную задачу, на правой панели отобразится сводная информация.

- **Имя.** Имя состояния задачи.
- **Количество.** Число устройств для каждого состояния задачи.
- **Проценты.** Процентное содержание устройств для каждого состояния задачи.

Перед планированием задач для какого-либо устройства ему должен быть назначен надлежащий агент, и он должен находиться в базе данных инвентаризации. Конфигурации сервера являются исключением. Они могут выполняться на устройстве, не имеющем стандартного агента управления. Задачи могут быть перепланированы (отредактированы) или удалены с вкладки заданий. После того, как вы запланировали задачу, см. вкладку заданий для определения ее состояния.

Для редактирования задачи выберите ее и нажмите **Правка**. Задание откроется с возможностями редактирования, применимыми к данной задаче.

Выборочные группы задач

Вы можете создать выборочные группы для таких типов задач, как **Мои задачи**, **Все задачи** и **Стандартные задачи**. Используя выборочные группы, вы можете группировать связанные друг с другом задачи, например, сканирование уязвимых мест и выполнение сценария. Группы и подгруппы могут уходить вглубь на 20 уровней.

Создание выборочной группы задач

1. В левой навигационной панели выберите **Запланированные задачи**.
2. В левой панели выберите тип задачи, в которой вы хотите создать группу.
3. На панели инструментов нажмите **Новая группа**.
4. Введите имя в текстовом окне **Имя группы** и нажмите **OK**.

После создания выборочной группы вы можете перемещать или копировать задачи или другие группы в группу, выбирая их из списка и нажимая на панели инструментов **Перенос**.

Страница целевых устройств

Используйте эту страницу, чтобы добавить целевые устройства для конфигурируемой задачи. На этой вкладке также отображаются целевые устройства, запросы и группы устройств для данной задачи. Если вы установили несколько продуктов управления LANDesk, группы устройств, созданные в одном продукте, могут быть отображены на всех консолях. Эта страница не нужна для задач обнаружения устройств.

- **Добавить список целей.** Добавление устройств, помещенных прежде в список целей из списка **Мои устройства**.
- **Добавить запрос.** Этот параметр направлен на результаты запроса, созданного вами раньше.
- **Удалить.** Удаление выбранных целей.

На данной странице отображаются группы целевых устройств, но обратите внимание на то, что группы будут отображаться только в том случае, если на главном сервере установлена LANDesk Management Suite. Если вы используете Server Manager, System Manager или Web-консоль в Management Suite, группы устройств не назначаются в качестве групп. Вместо этого, при выборе и назначении группы, индивидуальные устройства в данной группе добавляются к списку целевых устройств; они будут отображаться в списке **Целевые устройства**, а не в списке **Целевые группы**.

Страница планирования задачи

Планировщик содержит вкладку **Свойства запланированной задачи**, включающую в себя следующие параметры.

- **Не планировать** (по умолчанию). Оставляет задание в списке задач для дальнейшего планирования.
- **Запустить сейчас**. Запускает задание в ближайшее время. Для запуска задания может потребоваться до одной минуты, в зависимости от других настроек.
- **Запустить в запланированное время**. Задание запускается в указанное вами время. При выборе данного параметра необходимо ввести следующие данные:
  - **Дата**. Назначаемая вами дата начала выполнения задания. В зависимости от вашего местонахождения дата устанавливается в формате день-месяц-год или месяц-день-год.
  - **Время**. Назначаемое вами время начала выполнения задания.
  - **Повторять каждые**. Если нужно, чтобы данное задание повторялось, выберите, хотите ли вы, чтобы оно повторялось каждый **Час**, **День**, **Неделю** или **Месяц**. Если вы выбрали **Месяц**, а в этом месяце нет данного числа (например, отсутствует 31 число), задание будет выполняться лишь в те месяцы, в которых имеется данное число.
- **Запланировать данные устройства.** Когда задание выполняется в первый раз, необходимо оставить настройки по умолчанию "Ожидание" или "В процессе выполнения". Для последующего выполнения выберите из параметров "Все", "Устройства, не выполнившие задачу" или "Устройства, не пытавшиеся выполнить задачу". Данные параметры представлены ниже более детально.
  - **Устройства, не выполнившие задачу.** Этот параметр выбирается только в том случае, если вы хотите выполнить задачу на всех устройствах, не завершивших задание в первый раз. Устройства, на которых задание завершено успешно, исключаются. Задача будет выполняться на устройствах, имеющих все возможные другие состояния, включая состояния "Ожидание" или "Активное". Используйте этот параметр, если задание необходимо выполнить на максимальном количестве устройств, не выполнивших задачу, но вам нужно, чтобы задание было успешно завершено на каждом устройстве один раз.
  - **Состояния "Ожидание" или "В процессе выполнения".** Этот параметр выбирается в том случае, если вы хотите выполнить задачу на устройствах, находящихся в состоянии ожидания выполнения задания или в процессе его выполнения.
  - **Все.** Этот параметр выбирается, если вы хотите выполнить задачу на всех устройствах независимо от состояния. Используйте его, если у вас есть задание (особенно если оно повторяющееся), которое необходимо выполнить на максимальном количестве устройств.

- **Устройства, не пытавшиеся выполнить задачу.** Этот параметр выбирается только в том случае, если вы хотите выполнить задачу на устройствах, не завершивших задание, и на устройствах, на которых не произошел сбой при выполнении задания. Устройства, которые находились в состоянии " Выкл.", "Занято", "Ошибка" или "Отменено", исключаются. Используйте этот параметр, если имелось в наличии большое количество устройств, на которых произошел сбой задания, но которые не являются важными целевыми устройствами.

Страница выборочных сценариев

- **Текущий выборочный сценарий.** Выберите сценарий, который вы хотите запланировать.

Отчеты

Об отчетах

Программа System Manager включает в себя службу отчетов, которую вы можете использовать для генерирования разнообразных специализированных отчетов, предоставляющих критическую информацию об управляемых устройствах в вашей сети.

System 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 вместе. Служба отчетов пользуется дальнейшими преимуществами данных сканирования инвентаризации, получая и формируя их в удобном формате отчетов.

Вы можете использовать типовые отчеты службы и отчеты активов инвентаризации. После выполнения отчета вы можете просмотреть его на консоли.

Если у вас установлены и Server Manager, и Management Suite, то отчеты, выполняемые в Server Manager, будут включать только данные по серверам. Если вы выполните запрос, вы получите данные и по серверам, и по другим устройствам, если только запрос не был сконфигурирован для исключения других устройств.

Если получение отчетов с конкретной машины прекратилось, воспользуйтесь файлом restartmon.exe в папке LDCLIENT для перезапуска коллектора данных и всех провайдеров мониторинга. Эта утилита предназначена для машин, на которых была установлена служба предоставления отчетов, но предоставление прекратилось. Используйте эту утилиту для перезапуска коллектора данных и провайдеров без перезагрузки устройства.

Понятие групп отчетов и типовых отчетов

Отчеты организованы по группам в окне **Отчеты** (левая навигационная панель **| Отчеты**). Администраторы могут просматривать содержимое отчетов во всех группах. System Manager включает особую функцию, называемую "Отчеты", позволяющую другим пользователям просматривать отчеты без предоставления им доступа к другим возможностям управления. Для получения дополнительной информации см. "Ролевое администрирование". Пользователи с правом доступа к отчетам могут также просматривать и запускать отчеты, но только на устройствах, включенных в их область действия.

В окне **Отчеты** имеются следующие группы отчетов:

- Оборудование
- Программное обеспечение

Просмотр отчетов

Вы можете запустить любой отчет из окна **Отчеты**.

В окне **Отчеты** выберите группу отчетов, а затем отчет, который вы хотите запустить. Данные отчета отображаются в окне **Просмотр отчета**.

Окно просмотра отчетов

Отчеты предоставляют вам быстрый доступ к графическому представлению содержимого компьютеров ваших клиентов. Отчеты создаются из данных, хранящихся в базе данных сканера. Вы можете просматривать отчеты в вашем браузере или печатать их.

Просмотр отчета

1. В левой навигационной панели нажмите **Отчеты**. Категории отчетов отображаются в правой панели. Щелкните заголовок категории для просмотра списка отчетов. Значок, расположенный рядом с каждым отчетом, показывает тип отчета.

    Отчет со значком диаграммы отображается в виде круговой или простой диаграммы (двух- или трехмерной). На диаграмме можно нажать на любую цветную полосу или сектор для раскрытия сводки.

    Отчет со значком документа отображается в виде текста.

2. Для просмотра отчета выберите его название.
3. Для получения сводки о дате сканирования оборудования и ПО, выберите начальную и конечную даты для установки интервала времени, а затем нажмите **Выполнить**.

Сводка о дисковом пространстве содержит данные только для устройств Windows.

Чтобы напечатать отчет, щелкните правой кнопкой мыши страницу, а затем нажмите **Печать**. В диалоговом окне печати щелкните **Печать**. Если отчет занимает несколько страниц, для печати щелкайте правой кнопкой мыши каждую страницу.

Распространение отчета

- Для отправки отчета по электронной почте рекомендуем распечатать отчет в .PDF файл, а затем прикрепить его к вашему сообщению.

На консоли отображаются диаграммы отчетов в виде круговой или простой диаграммы. Нажмите на раскрывающийся список типов отчетов, чтобы выбрать один из двух типов, а затем поменяйте тип диаграммы.

Для просмотра интерактивных круговых и простых диаграмм, отображенных в большом количестве отчетов, нужно иметь установленный Macromedia Flash Player* 7.

Запросы

Использование запросов

Запросы - это специальные процедуры поиска в базах данных главного сервера. Этот продукт предоставляет инструментальные средства, позволяющие вам создавать запросы баз данных для устройств в базе данных вашего главного сервера. Создание запросов базы данных главного сервера осуществляется на экране консоли **Запрос**. Общие запросы System Manager доступны для просмотра в LANDesk® Management Suite, и наоборот, если используются оба продукта.

В этой главе вы изучите следующие разделы:

- Обзор запросов
- Группы запросов
- Создание запросов баз данных
- Выполнение запросов
- Импорт и экспорт запросов

Обзор запросов

Запросы помогают управлять сетью, позволяя осуществлять поиск и организацию устройств в базе данных главного сервера на основании указанных системных или пользовательских критериев.

Например, вы можете создать и выполнить запрос, который будет охватывать только устройства с тактовой частотой процессора менее 166 МГц или ОЗУ менее 64 МБ, или с жестким диском объемом менее 2 ГБ. Создайте один или несколько запросов с такими условиями и установите их взаимосвязь, используя стандартные логические операции. При выполнении запросов вы можете распечатать их результаты, получить доступ и управлять устройствами, которые соответствуют данным запросам.

Группы запросов

Запросы могут быть ассоциированы с группами на экране **Мои устройства**. Это так называемые динамические группы. Содержанием динамической группы являются результаты запроса, ассоциированного с данной динамической группой. Например, группа, содержащая все устройства определенного региона, может ассоциироваться с запросом по памяти, размеру жесткого диска и так далее.

Дополнительную информацию о том, как группы запросов и запросы отображаются на экране **Все устройства**, и какие операции вы можете выполнять с ними, см. в разделе "Группировка устройств для выполнения действий".

Создание запросов баз данных

Используйте диалог **Новый запрос** для создания запроса, выбирая атрибуты, их значения и сопутствующие операции. Сформируйте положение запроса, выбрав атрибут

инвентаризации и связав его с допустимым значением. Свяжите логически положения запроса друг с другом для того, чтобы они образовали группу, перед тем как соотнести их с другими положениями или группами.

Создание запроса базы данных

1. На экране консоли **Запросы** выберите **Новый**.
2. Выберите **компонент** из списка атрибутов инвентаризации.
3. В **действии 1 "Условия поиска"** выберите **Правка**.
    1. Прокрутите список для выбора атрибутов условий поиска. Например, для поиска всех клиентов, использующих определенный тип программного обеспечения, выберите Computer.Software.Package.Name.
    2. После выбора атрибутов вы увидите, что в правой стороне окна появится несколько полей. Чтобы закончить создание условий поиска, выберите в этих полях оператор и значение. Например, для поиска всех клиентов, использующих Internet Explorer 5.0, атрибутами будут "Computer.Software.Package.Name", оператор "=" и значение "Internet Explorer 5".
    3. Для заполнения пустого поля в условии поиска внизу окна нажмите **Добавить**.
    4. Вы можете в дальнейшем детализировать свой запрос, создавая другие условия поиска, и затем добавляя их к первому условию с логическим оператором (И или ИЛИ). Также используйте кнопки для добавления, удаления, замены, группирования и разгруппирования созданных вами условий.
    5. После завершения нажмите **OK**.
4. В **действии 2 "Отображаемые атрибуты"** выберите **Правка**.
    1. Внимательно просмотрите этот список и выберите атрибут, который будет отображаться в списке результатов запроса. Не забудьте указать атрибуты, которые помогут определить клиентов, возвращаемых запросом. Если в списке нет необходимых атрибутов, то их можно добавить в диалоговом окне Выборочные атрибуты. При этом необходимо назначить атрибуты машинам, прежде чем они появятся в диалоговом окне запроса.

    2. После выбора атрибута щелкните **Добавить**, чтобы переместить атрибут в пустое поле в нижней части окна. При необходимости пронумеровать список результатов запроса нажмите **Включить подсчет**.
    3. Чтобы добавить другие атрибуты, повторите вышеописанные действия. Для удаления атрибутов воспользуйтесь кнопкой **Удалить**, а для изменения порядка атрибутов – кнопками **Вверх/Вниз**.
    4. Чтобы с результатами запроса можно было выполнять какие-либо действия, щелкните **Сделать результаты назначаемыми**.
    5. После завершения нажмите **OK**.
5. (Необязательно). В **действии 3 "Сортировать результаты по атрибутам"** выберите **Правка** для указания порядка отображения результатов запроса.
6. Если нужно выполнить данный запрос еще несколько раз, выберите **Сохранить запрос** и введите для него уникальное имя. Если выполнить запрос, не сохранив его, то параметры запроса будут потеряны, и нужно будет восстанавливать содержимое запроса при повторном выполнении.
7. В **действии 4 "Выполнение запроса"** выберите **Выполнить запрос**.

Порядок выполнения положений запроса.
Если группы запросов не были созданы, перечисленные в данном диалоговом окне запросы выполняются снизу вверх. Проверьте, чтобы составляющие группы запросов были оценены в качестве группы; иначе результаты запроса могут отличаться от ожидаемых.

Выполнение запросов

Выполнение запроса

1. В левой навигационной панели выберите **Запросы**.
2. Выберите запрос и щелкните **Выполнить**.

   или

   Для внесения изменений в запрос перед его выполнением щелкните его дважды, затем **Правка**, измените действия 1-3, а потом **Выполнить запрос**.

   Примечание. Если вы изменили запрос и хотите сохранить изменения, выберите **Сохранить запрос** для сохранения изменений или **Сохранить запрос как**, чтобы присвоить измененному запросу новое имя. Это необходимо сделать перед выполнением запроса. Если вы не сохраните изменения перед выполнением запроса, они не будут сохранены в запросе.

3. Результаты запроса (соответствующие устройства) отображаются в правой части окна **Все устройства**.

Импорт и экспорт запросов

Вы можете использовать функцию импорта и экспорта для перемещения запросов из одной базы данных в другую. Экспортированные запросы сохраняются как файлы .XML.

Импорт запроса

1. Щелкните правой кнопкой мыши нужную группу запросов для размещения в ней импортируемого запроса.
2. Выберите **Импорт** в меню быстрого вызова команд.
3. Найдите и выберите запрос, который нужно импортировать.
4. Выберите **Открыть** для добавления запроса в выбранную группу запросов в окне **Все устройства**.

Экспорт запроса

1. Щелкните правой кнопкой мыши экспортируемый запрос.
2. Выберите **Экспорт** в меню быстрого вызова команд.
3. Укажите, куда нужно сохранить запрос (в виде файла .XML).
4. Введите имя запроса.
5. Нажмите **Сохранить** для экспорта запроса.

Понятие выборочных запросов

Выборочные запросы полезны, если вы хотите получить подробности инвентаризации об установленном на ваших устройствах оборудовании и программном обеспечении. Используйте выборочный запрос для формирования списка компьютеров с похожей инвентаризацией. Выборочные запросы также используются для определения групп и областей действия.

На странице **Выборочные запросы** (щелкните **Запросы** в левой навигационной панели) отображается список запросов, которые вы сохранили. Для запуска сохраненного запроса выберите его и нажмите **Выполнить**.

Если список запросов размещен на нескольких страницах, воспользуйтесь стрелками в верхней части страницы для перехода между страницами. Введите число элементов, которые будут отображаться на странице и нажмите **Установить**.

Создание выборочных запросов

Выборочные запросы полезны, если вы хотите получить подробности инвентаризации об установленном на ваших устройствах оборудовании и программном обеспечении. Используйте выборочный запрос для формирования списка устройств с похожей инвентаризацией. Например, если вы хотите обновить процессоры во всех устройствах до 750 МГц, можно запросить в вашей базе данных все устройства с тактовой частотой процессора меньше, чем 750 МГц. Выборочные запросы также используются для определения групп и областей действия.

Вы можете запросить любой из элементов инвентаризации (называемых атрибутами), которые сканер инвентаризации хранит в базе данных, а также любые другие выборочные атрибуты.

Управление запросами

Управляйте запросами в окне **Запросы**. Используйте данное окно для создания, правки или удаления запросов.

- Для запуска существующего запроса выберите его и нажмите **Выполнить**.
- Для создания нового запроса нажмите **Новый**. После создания и сохранения запроса его имя появится в списке на этой странице.
- Для правки запроса в списке щелкните его дважды. Появится страница **Правка запроса** с параметрами запроса, доступными для редактирования.
- Для редактирования последнего запроса нажмите **Правка текущего запроса**.
- Для удаления запроса выберите его и нажмите **Удалить**.

Создание запроса осуществляется в 4 этапа.

1. **Создание условий поиска.** Укажите набор атрибутов инвентаризации, которые будут являться основой вашего запроса.

2. **Выбор атрибутов для отображения.** Очистите или "отфильтруйте" запрос для отображения самых необходимых вам атрибутов, таких как IP-адреса или имена компьютерных устройств.
3. **Сортировка результатов по атрибутам (необязательно).** Укажите, как вы хотите отсортировать результаты запроса. (Применимо только, если в действии 2 вы выбрали отображение более одного типа атрибута в результатах запроса.)
4. **Выполнение запроса.** Запустите выполнение созданного запроса. Вы также можете сохранить его для дальнейшего использования или очистить всю информацию о запросе для создания нового.

Действие 1. Создание условия поиска (обязательно)

Условие поиска — набор атрибутов инвентаризации и связанных с ними запрашиваемых значений. Для формирования основы запроса можно использовать одно условие поиска или сгруппировать несколько условий.

На странице **Правка запроса** выполняются следующие действия. Откройте окно **Выполнить запрос**, щелкните **Новый** или выберите существующий запрос и нажмите **Правка**.

Создание условия поиска

1. В **действии 1** выберите **Правка**. Откроется окно со списком всех данных инвентаризации, содержащихся в настоящее время в базе данных.
2. Прокрутите список для выбора атрибутов условий поиска. Например, для поиска всех клиентов, использующих определенный тип программного обеспечения, выберите Computer.Software.Package.Name.
3. После выбора атрибутов вы увидите, что в правой стороне окна появится несколько полей. Чтобы закончить создание условий поиска, выберите в этих полях оператор и значение. Например, для поиска всех клиентов, использующих Internet Explorer 5.0, атрибутами будут "Computer.Software.Package.Name", оператор "=" и значение "Internet Explorer 5".
4. Для заполнения пустого поля в условии поиска внизу окна нажмите **Добавить**.
5. Вы можете в дальнейшем детализировать свой запрос, создавая другие условия поиска, и затем добавляя их к первому условию с логическим оператором (И или ИЛИ). Также используйте кнопки для добавления, удаления, замены, группирования и разгруппирования созданных вами условий.
6. После завершения нажмите **OK**.

Для выполнения и сохранения запроса о состоянии серверов (Computer.Health.State) необходимо убедиться, что состояние представлено числом в базе данных. Для создания условий поиска используйте следующую таблицу. Например, чтобы создать условие поиска для машин с состоянием "Неизвестно", используйте оператор "NOT EXIST".

Состояние	Оператор
Неизвестно	NOT EXIST
Нормальное	2

Состояние	Оператор
Предупредительное	3
Критическое	4

Действие 2. Выбор отображаемых атрибутов (обязательно)

Для действия 2 необходимо выбрать атрибуты, которые будут наиболее полезными для идентификации компьютеров, обнаруженных в результате запроса. Например, при необходимости физического обнаружения всех компьютеров, соответствующих критериям поиска, выбранным для первого действия, укажите в качестве атрибута отображаемое имя компьютера (Computer.DisplayName) или его IP-адрес (Computer.Network.TCPIP.Address).

На странице **Правка запроса** выполняются следующие действия.

Выбор отображаемых атрибутов

1. В **действии 2** выберите **Правка**. Откроется окно со списком всех данных инвентаризации, содержащихся в настоящее время в базе данных.
2. Внимательно просмотрите этот список и выберите атрибут, который будет отображаться в списке результатов запроса. Не забудьте указать атрибуты, которые помогут определить клиентов, возвращаемых запросом. Если в списке нет необходимых атрибутов, то их можно добавить в диалоговом окне Выборочные атрибуты. При этом необходимо назначить атрибуты машинам, прежде чем они появятся в диалоговом окне запроса.

   Примечание. При использовании базы данных Oracle обязательно выберите хотя бы один атрибут, который был определен сканером инвентаризации (например, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name и т.д.).

3. После выбора атрибута щелкните **>>**, чтобы переместить атрибут в пустое поле в правой части окна. При необходимости пронумеровать список результатов запроса нажмите **Включить подсчет**.
4. Чтобы добавить другие атрибуты, повторите вышеописанные действия. Для добавления или удаления атрибутов воспользуйтесь кнопками со стрелками, а для изменения порядка атрибутов – кнопками **Вверх/Вниз**.
5. Чтобы с результатами запроса можно было выполнять какие-либо действия, щелкните **Сделать результаты назначаемыми**.
6. После завершения нажмите **OK**.

К списку результатов запроса можно добавлять заголовки столбцов.

Изменение заголовков столбцов (необязательно)

1. В **действии 2** выберите **Правка**.

2. В нижнем окне выберите заголовок столбца и нажмите кнопку **Правка**. Измените заголовок и нажмите **Enter**. При необходимости повторите действия.
3. Нажмите **OK**.

На данном этапе возможно сохранение запроса; следующая процедура в процессе создания запроса является необязательной и применима только к результатам запроса, содержащим не менее двух столбцов. Для сохранения запроса выберите **Сохранить запрос** в верхней части страницы. Отобразится окно, предлагающее ввести имя запроса. Введите имя запроса и нажмите **Сохранить** в правом верхнем углу окна.

Действие 3. Сортировка результатов по атрибуту (необязательно)

Эта процедура необходима только в том случае, если вы указали более одного атрибута и заголовка столбца в действии 3, а теперь хотите отсортировать результаты в алфавитном или числовом порядке в одном из этих столбцов.

Например, вы указали два разных атрибута, которые будут отображаться в списке запросов: IP-адрес и тип процессора для каждого обнаруженного компьютера. В действии 3 вы можете отсортировать результаты в алфавитном порядке по типу процессора.

Если вы пропустите это действие, то запросы автоматически будут сортироваться по первому атрибуту, выбранному в действии 2.

Сортировка результатов по атрибуту

1. В **действии 3** выберите **Правка**. Появляется окно, в котором показаны атрибуты, выбранные в **действии 2**.
2. Выберите атрибут, по которому будет вестись сортировка, а затем щелкните **>>** для перемещения его в пустое текстовое окно.
3. Нажмите **OK**.

Действие 4. Выполнение запроса

После создания своего запроса вы можете его запустить, сохранить или очистить для повторного создания.

Чтобы сохранить запрос для дальнейшего использования, на панели инструментов нажмите кнопку **Сохранить**. Запрос появляется в списке на странице **Выборочные запросы**. Если ваш запрос - это измененная версия существующего запроса, на панели инструментов нажмите кнопку **Сохранить как** для задания нового имени.

По умолчанию сохраненные запросы видны только пользователю, который их сохранил. Если перед сохранением выбрать **Общий запрос**, сохраненный запрос будет виден всем пользователям. Общий запрос может создаваться только администраторами с соответствующими правами.

Если у вас установлено семейство, состоящее из множества продуктов, запросы совместно используются этими продуктами. Если вы сохранили запрос в консоли одного из продуктов, его также можно будет увидеть на консолях других продуктов.

Для просмотра результатов запроса на панели инструментов нажмите кнопку **Выполнить**.

Для удаления параметров запроса со страницы **Правка запроса** на панели инструментов нажмите кнопку **Очистить**. Если запрос уже был сохранен, он удаляется с этой страницы, однако остается в списке **Выборочные запросы**.

Просмотр результатов запроса

Результаты запроса соответствуют критериям поиска, указанным в процессе создания запроса. Если результаты не соответствуют ожидаемым, вернитесь на страницу **Правка запроса** и уточните информацию.

Для просмотра дополнительной информации об одном из устройств в списке результатов запроса дважды щелкните данные запроса или щелкните их правой кнопкой мыши и в появившемся меню выберите **Просмотр компьютера**.

На странице **Результаты запроса** щелкните **Сохранить как CSV** на панели инструментов для экспорта результатов в формат, совместимый с электронной таблицей или другим приложением.

Для распечатки результатов запроса щелкните **Печать** на странице результатов запроса.

Просмотр подробностей о результатах запроса

Результаты запроса соответствуют критериям поиска, указанным в процессе создания запроса. Если результаты не соответствуют ожидаемым, вернитесь на страницу **Правка запроса** и уточните информацию.

Для просмотра дополнительной информации об одном из устройств в списке результатов запроса дважды щелкните данные запроса или щелкните их правой кнопкой мыши и в появившемся меню выберите **Просмотр компьютера**.

Экспорт результатов запроса в файлы CSV

Для просмотра результатов запроса в приложении электронной таблицы экспортируйте данные в файл CSV (текст с разделителями-запятыми). На странице **Результаты запроса** на панели инструментов щелкните значок **Сохранить как CSV**, чтобы сохранить информацию как файл CSV. Затем для импорта и работы с файлом CSV можно использовать такое приложение, как Microsoft Excel*.

Изменение заголовков столбцов запросов

1. Откройте существующий запрос или создайте новый.
2. В нижнем окне выберите заголовок столбца и нажмите кнопку **Правка**. Измените заголовок и нажмите **Enter**. При необходимости повторите действия.

3. Нажмите **OK**.

Экспорт и импорт запросов

Любые созданные вами запросы можно экспортировать и импортировать. Все запросы экспортируются как файлы XML. При повторном экспорте запроса с одним и тем же именем файла существующий файл будет перезаписан. Во избежание этого, после экспорта можно скопировать файл в другое местоположение.

Функции экспорта и импорта можно использовать двумя способами.

- Если требуется переустановка базы данных, воспользуйтесь функциями экспорта/импорта, чтобы сохранить существующие запросы для использования в новой базе.

  Например, можно экспортировать запросы, а затем переместить их в каталог, который не будет изменен при переустановке базы данных. После переустановки базы данных можно переместить запросы обратно в каталог запросов вашего web-сервера, а затем импортировать их в новую базу данных.
- Вы также можете воспользоваться функциями экспорта/импорта для копирования запросов в другую базу данных.

  Например, можно экспортировать запрос в каталог запросов на вашем web-сервере, а затем отправить его кому-нибудь с помощью электронной почты или FTP. Потом этот человек может поместить запросы в каталог запросов на другом web-сервере, а затем импортировать их в другую базу данных. Вы также можете назначить диск и скопировать запросы непосредственно в каталог запросов другого web-сервера.

Экспорт запроса

Выполняйте эти действия, когда вы подключены к базе данных, содержащей запрос, который нужно экспортировать.

1. В левой навигационной панели выберите **Запросы**.
2. На странице **Выборочные запросы** выберите имя запроса, который вы хотите экспортировать. Нажмите **Правка**.
3. На странице **Правка запроса** нажмите кнопку панели инструментов **Экспорт** для экспорта запроса на диск.
4. На странице **Запрос экспортирован** щелкните правой кнопкой мыши запрос для его загрузки в формате XML в выбранный каталог. Запрос преобразуется в файл XML.

Обратите внимание, что при повторном экспорте запроса с одним и тем же именем файла существующий файл будет перезаписан. Во избежание этого, после экспорта можно скопировать файл в другое местоположение.

Если вы захотите импортировать запрос обратно в базу данных, вам понадобиться переместить его в каталог запросов, который распознается web-сервером. По умолчанию это каталог c:\inetpub\wwwroot\LANDesk\LDSM\queries.

Импорт запроса

Выполняйте эти действия, когда вы подключены к базе данных, в которую хотите импортировать запрос.

1. В левой навигационной панели выберите **Запросы**.
2. На странице **Выборочные запросы** выберите **Новый**.
3. На странице **Правка запроса** нажмите кнопку панели инструментов **Импорт**.
4. Выберите запрос, который вы хотите импортировать. Для проверки параметров данного запроса перед импортом нажмите **Просмотр**.
5. Выберите **Импорт** для загрузки запроса на страницу **Правка запроса**.
6. После загрузки запроса прокрутите его и выберите **Сохранить запрос** для его сохранения в данной базе данных.

Управление инвентаризацией

Вы можете использовать утилиту сканирования инвентаризации для добавления устройств в базу данных главного сервера и для сбора информации о программном обеспечении и оборудовании устройств. Вы можете просматривать, печатать и экспортировать данные инвентаризации. Вы также можете использовать их для определения запросов, группирования устройств и создания специальных отчетов.

В этой главе вы изучите следующие разделы:

Обзор сканирования инвентаризации

При настройке устройства с помощью параметра установки устройств сканер инвентаризации является одним из компонентов, которые устанавливаются в устройстве. При создании конфигурации клиента вы можете указать время запуска сканера инвентаризации в устройстве.

Сканер инвентаризации запускается автоматически при исходной конфигурации устройства. Исполняемым файлом сканера для Windows является LDISCAN32.EXE, а для Linux - LDISCAN . Сканер инвентаризации собирает сведения о программном обеспечении и оборудовании и вносит 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. Для конфигурации параметров сканирования программного обеспечения на главном сервере щелкните **Пуск | Программы |** LANDesk **|** LANDesk **Конфигурация служб**.

Для дополнительной информации о конфигурации службы инвентаризации см. Конфигурация службы инвентаризации в приложении B.

После первоначального сканирования сканер инвентаризации может быть запущен с консоли в качестве назначенной задачи. Стандартный агент управления должен быть установлен на удаленных устройствах, чтобы на них можно было запланировать проведение сканирования.

Примечание. Данные инвентаризации об устройстве, которое было добавлено в базу данных главного сервера с помощью обнаружения, еще не были сосканированы в базу данных главного сервера. Вы должны запустить сканирование инвентаризации на каждом устройстве, чтобы получить о нем полные данные инвентаризации.

Вы можете просматривать данные инвентаризации и использовать их для выполнения следующих действий:

- Задание выборочных параметров столбцов списка **Все устройства** для отображения определенных атрибутов инвентаризации.

- Отправка запросов в базу данных главного сервера для серверов с определенными атрибутами инвентаризации.
- Группирование устройств для ускорения выполнения задач управления.
- Создание специализированных отчетов на основании атрибутов инвентаризации.
- Наблюдение за изменениями оборудования и программного обеспечения в устройствах и генерирование предупреждений или записей в журнале, когда происходят подобные изменения.

Прочитайте следующие разделы, чтобы узнать, как работает сканер инвентаризации.

Дельта-сканирование

После того как первоначальное сканирование устройства уже проведено, при последующем проведении сканирования инвентаризации сканер фиксирует только различия в изменениях и посылает их в базу данных главного сервера. Используйте параметр сканера /RSS для сбора информации о программном обеспечении из реестра Windows.

Принудительный запуск полного сканирования

Если вы хотите принудительно запустить полное сканирование оборудования устройства и данных ПО, вы можете удалить существующий файл дельта-сканирования и изменить настройки в приложении **Конфигурация служб ПО LANDesk**.

1. Удалите из сервера файл **invdelta.dat**. Копия последнего сканирования инвентаризации хранится локально в виде скрытого файла invdelta.dat в корневом каталоге жесткого диска. (Переменная среды LDMS_LOCAL_DIR устанавливает местоположение для этого файла).
2. Добавьте параметр **/sync** в командную строку утилиты сканера инвентаризации. Для редактирования командной строки щелкните **Пуск | Все программы | LANDesk Management**, затем щелкните правой кнопкой мыши значок **Сканирование инвентаризации** и выберите **Свойства | Shortcut**, а затем измените путь **Цель**.
3. В главном сервере выберите **Пуск | Все программы | LANDesk | Конфигурация служб LANDesk**.
4. Откройте вкладку **Инвентаризация**, затем нажмите **Дополнительные параметры**.
5. Щелкните параметр **Do Delta**. В поле **Значение** введите **0**.
6. Дважды щелкните **OK**, затем **Да** в подсказке, чтобы перезапустить службу.

Сжатие данных сканирования

Сжатие данных сканирования инвентаризации, выполненного сканером инвентаризации Windows (LDISCAN32.EXE), происходит по умолчанию. Сканер сжимает данные полного сканирования и данные delta-сканирования с коэффициентом сжатия примерно 8:1. Данные сканирования сначала полностью находятся в памяти, потом они сжимаются и отправляются на главный сервер в пакете большого размера. Сжатие данных сканирования требует использования меньшего числа пакетов и сохраняет пропускную способность сети.

Шифрование данных сканирования

Данные сканирования инвентаризации шифруются (только данные сканирования TCP/IP). Можно отключить шифрование данных сканирования инвентаризации путем изменения параметра в приложении Конфигурация служб LANDesk.

1. В главном сервере выберите **Пуск | Все программы | LANDesk | Конфигурация служб LANDesk**.
2. Откройте вкладку **Инвентаризация**, затем нажмите **Дополнительные параметры**.
3. Щелкните параметр **Отключение шифрования**. В поле **Значение** введите **1**.
4. Нажмите **Установить**, а затем **OK**.
5. Щелкните **OK**, затем **Да** в подсказке, чтобы перезапустить службу.

Просмотр данных инвентаризации

После сканирования устройства сканером инвентаризации вы можете просмотреть его системную информацию на консоли.

Данные инвентаризации устройств хранятся в базе данных главного сервера и включают информацию об оборудовании, драйвере устройства, программном обеспечении, памяти и среде. Вы можете использовать данные инвентаризации для помощи в управлении и конфигурации устройств, а также для быстрого обнаружения проблем в системе.

Вы можете просматривать данные инвентаризации следующим образом:

- Сводка инвентаризации
- Полная инвентаризация
- Просмотр свойств атрибута
- Системная информация

Вы также можете просматривать данные инвентаризации в отчетах, которые вы генерируете. Для дополнительной информации см. "Обзор отчетов".

Просмотр сводки инвентаризации с информационной консоли сервера

Сводка инвентаризации расположена на странице **Сводка** в информационной консоли сервера. В ней предоставлен краткий обзор основной конфигурации ОС устройств и информация о системе.

Примечание. Данные об устройстве, которое было добавлено в базу данных главного сервера с помощью обнаружения, еще не были сосканированы в базу данных главного сервера. Вы должны запустить сканирование инвентаризации на сервере, чтобы успешно завершить получение сводки инвентаризации.

Просмотр сводки инвентаризации

1. В окне консоли **Все устройства** выберите устройство двойным щелчком.

2. В левой навигационной панели выберите **Информация о системе**, а затем **Сводка системы**.

Краткие данные сервера Windows 2000/2003

Данная информация появляется при просмотре сводки инвентаризации для сервера Windows 2000/2003.

- **Состояние.** Текущее состояние сервера.
- **Тип.** Тип сервера, а именно приложение, файл, e-mail и т.п.
- **Производитель.** Производитель сервера.
- **Модель.** Тип модели сервера.
- **Версия BIOS.** Версия BIOS ПЗУ.
- **Операционная система.** На сервере установлена ОС Windows или Linux: 2000, 2003 или Red Hat.
- **Версия ОС.** Номер версии ОС Windows 2000/2003 или Linux, установленной на сервере.
- **ЦП.** Тип процессора/ов, установленных на сервере.
- **Сканер уязвимых мест.** Версия установленного агента.
- **Сканер инвентаризации.** Версия установленного агента.
- **Мониторинг.** Версия установленного сканера мониторинга.
- **Последняя перезагрузка.** Время последней перезагрузки сервера.
- **Использование ЦП.** Процент текущей загрузки процессора.
- **Загрузка физической памяти.** Объем доступной ОЗУ на сервере.
- **Загрузка виртуальной памяти.** Объем памяти, которая доступна серверу, включая ОЗУ и память файла подкачки.
- **Использованное дисковое пространство.** Процентное значение текущего использования дискового пространства. Если имеется более одного жесткого диска, каждый из дисков будет указан.

В серверах с включенным IPMI отображаются дополнительные данные, характерные для IPMI. В серверах Linux также отображается похожая информация в окне **Сводка**.

Просмотр полной инвентаризации

Полная инвентаризация предоставляет полный список компонентов оборудования и программного обеспечения устройства. Список содержит объекты и атрибуты объектов.

Просмотр полной инвентаризации

1. В окне консоли **Все устройства** выберите устройство.
2. На вкладке **Свойства** выберите **Просмотр инвентаризации**.

Просмотр свойств атрибута

Вы можете просмотреть свойства атрибута для объектов инвентаризации устройства в списке инвентаризации. Свойства атрибутов предоставят вам характеристики и значения

объектов инвентаризации. Вы также можете создавать новые выборочные атрибуты и редактировать атрибуты, указанные пользователем.

Для просмотра свойств атрибута щелкните атрибут в левой панели.

Чтобы распечатать данную информацию в Internet Explorer, щелкните правой кнопкой мыши фрейм и затем выберите **Печать**. Для печати в браузере Mozilla щелкните правой кнопкой мыши фрейм и затем выберите **Этот фрейм | Сохранить фрейм как**, щелкните **Сохранить**, затем откройте файл в приложении и щелкните **Печать**.

Системная информация

Из информационной консоли сервера вы можете просматривать и изменять системную информацию устройства. Информация, указанная в категориях **Оборудование**, **Программное обеспечение**, **Журналы** и **Другие**, является сохраненными данными или данными реального времени. Если вы выберите информационную ссылку, вы можете просмотреть подробную информацию о выбранных компонентах и при необходимости установить пороговые значения и ввести информацию.

1. В окне консоли **Все устройства** выберите устройство двойным щелчком.
2. В левой навигационной панели информационной консоли сервера выберите **Информация о системе**.
3. Разверните группу и щелкните информационную ссылку, которую вы хотите просмотреть.

Настройка выборочных параметров инвентаризации

На консоли есть утилита конфигурации служб, которую можно использовать для настройки параметров инвентаризации. Установленных по умолчанию параметров должно быть достаточно. Однако, если вы хотите их изменить, можно запустить данную утилиту. Для запуска утилиты конфигурации служб на главном сервере щелкните **Пуск | Программы |** LANDesk **|** LANDesk **Конфигурация служб**. (Имя файла данной утилиты svccfg.exe).

Используйте утилиту конфигурации служб для конфигурации следующих параметров.

- Имя базы данных, имя пользователя и пароль
- Интервал сканирования программного обеспечения, обслуживания, дней для проведения сканирования инвентаризации и продолжительность истории регистрации клиента
- Обработка идентификатора дубликата устройства
- Конфигурации планировщика, включая запланированные задания и интервалы между оценками запросов
- Настройки специальных заданий, включая тайм-аут удаленного выполнения

Для дополнительной информации см. **Справка** на каждой вкладке в утилите конфигурации служб.

Правка файла LDAPPL3.TEMPLATE

Информация о параметрах сканера инвентаризации хранится в файле LDAPPL3.TEMPLATE. Этот файл шаблона работает совместно с файлом LDAPPL3.INI для идентификации инвентаризации ПО устройства. Данный файл сохраняется на управляемых устройствах Windows как часть конфигурации агента. Параметры файла устанавливаются на вкладке инвентаризации Конфигурация агента.

На устройствах Linux похожий файл конфигурации (/etc/ldappl.conf) содержит информацию о параметрах сканера. Для изменения работы сканера отредактируйте данный файл. В файле содержатся инструкции по изменению работы сканера Linux.

Вы можете исправлять раздел "Инвентаризация LANDesk" файла шаблона с целью конфигурации параметров, определяющих процесс идентификации сканером инвентаризации ПО. По умолчанию файл LDAPPL3.TEMPLATE расположен на главном сервере в общем каталоге LDLogon.

Следующая таблица поможет вам отредактировать раздел "Инвентаризация LANDesk" в текстовом редакторе.

Параметр	Описание
Режим	Определяет, как сканер сканирует ПО на устройствах. Параметром по умолчанию является "Перечислены". Ниже приведены все настройки. • **Перечислены.** Регистрируются файлы, перечисленные в LDAPPL3. • **Не перечислены.** Регистрируются имена и даты всех файлов с расширениями, перечисленными в строке ScanExtensions, но не определенными в LDAPPL3. Этот режим позволяет обнаружить неразрешенное ПО в сети. • **Все.** Обнаруживает как перечисленные, так и неперечисленные файлы.
Дубликат	Регистрирует несколько копий одного файла. Установите значение "Выкл." для регистрации только первой копии, или "Вкл." для регистрации всех обнаруженных копий. Параметром по умолчанию является "Вкл.".
ScanExtensions	Устанавливает расширения файлов (.EXE, .COM, .CFG и т.д.), которые будут сканироваться. Для разделения расширений файлов используйте пробел. По умолчанию сканируются только файлы с расширением .EXE.
Версия	Номер версии файла LDAPPL3.

Параметр	Описание
Редакция	Номер редакции файла LDAPPL3; позволяет обеспечить совместимость в будущем.
CfgFiles 1-4	Регистрируется дата, время, размер и содержание указанных файлов. Букву диска можно опустить (например, c:), если вы хотите вести поиск по всем локальным дискам. Вы можете указать более одного файла в каждой из четырех строк, но при этом длина строки не должна превышать 80 символов. Разделяйте имена путей к файлам в одной строке пробелами. Сканер сравнивает дату и размер текущего файла с данными прошлого сканирования. Если дата и размер не совпадают, сканер регистрирует содержание файла как новую редакцию.
ExcludeDir 1-3	Исключает указанные каталоги из сканирования. Букву диска можно опустить (например, c:), если вы хотите исключить все локальные диски. Нумерация должна начинаться с 1 и быть непрерывной. Каждую строчку следует заканчивать знаком "\".
MifPath	Указывает местоположения файлов MIF на локальном диске клиента. Местоположением файла по умолчанию является каталог c:\DMI\DOS\MIFS.
UseDefaultVersion	Если данный переключатель установлен на "TRUE", то сканер сообщает о совпадении, когда из двух параметров - имя и размер - файл соответствуют только точному имени, указанному в LDAPPL3 (версия будет фигурировать в отчете как СУЩЕСТВУЕТ). Это может привести к появлению ложных положительных результатов для приложений, которые используют файлы с одинаковым именем совместно с неизвестным приложением. В поставляемом файле LDAPPL3.TEMPLATE для этого параметра установлено значение "FALSE"; в этом случае запись добавляется только при полном совпадении. Если параметр отсутствует, то значением по умолчанию будет "TRUE".
SendExtraFileData	При выборе "TRUE" на главный сервер отправляется дополнительный файл с данными. Параметром по умолчанию является "FALSE". Это означает, что по умолчанию в базу данных главного сервера заносятся только путь к файлу, имя и версия.

Редактирование файла LDAPPL3.TEMPLATE

1. Из главного сервера войдите в каталог \Program Files\LANDesk\ManagementSuite\LDLogon и откройте файл LDAPPL3.TEMPLATE с помощью программы Notepad или другого текстового редактора.
2. Прокрутите содержимое файла до параметра, который вам нужно обновить, и внесите изменения.
3. Сохраните файл.

Обновление списка приложений

Данные из списка приложений DEFAULTS.XML сохраняются на главном сервере. Поскольку имена и номера версий общих программных приложений изменяются довольно часто, LANDesk публикует новый файл DEFAULTS.XML несколько раз в год (в предыдущих версиях ПО LANDesk этот файл назывался LDAPPL.INI).

Обновление списка приложений

1. Загрузите новый файл DEFAULTS.XML или LDAPPL3.TEMPLATE из http://www.landesk.com/support/downloads. Выберите продукт и щелкните **Обновление ПО** для загрузки файла.
2. Сохраните файл в каталог LDLOGON.
3. Опубликуйте новый файл LDAPPL3.INI согласно процедуре, описанной в разделе "Публикация списка приложений".

Обновление списка приложений

Публикация списка приложений требует импорта списка часто используемых приложений, содержащихся в файле DEFAULTS.XML, в базу данных, а потом комбинирования списка приложений с содержимым файла LDAPPL3.TEMPLATE с целью генерирования обновленного файла LDAPPL3.INI. В каталоге \Program Files\LANDesk\ManagementSuite есть самостоятельная утилита COREDBUTIL.EXE, которая используется для автоматического выполнения двух указанных действий.

Публикация списка приложений

1. Запустите CoreDBUtil.exe.
2. Щелкните кнопку **Опубликовать список приложений**.

Вы должны опубликовать список после внесения изменений или загрузки новой версии файлов LDAPPL3.TEMPLATE или DEFAULTS.XML.

Конфигурация оборудования

Поддержка Intel* AMT

System Manager поддерживает устройства, использующие Intel* Active Management Technology (Intel* AMT), программные и аппаратные средства, обеспечивающие удаленное управление устройствами. Технология Intel AMT использует внеполосное (out-of-band – OOB) взаимодействие для обеспечения доступа к устройствам независимо от состояния операционной системы устройства, а также режима подачи питания.

Поддержка Intel AMT в этом продукте распространяется на версии 1 и 2. Процесс аутентификации для устройств Intel AMT 2 включает некоторые новые возможности, отсутствующие в версии 1. См. раздел Конфигурация устройств Intel AMT для получения сведений о процессе аутентификации в версии 2. Информация, предлагаемая в этом разделе, применима к обеим версия, за некоторыми указанными исключениями.

Средство конфигурации оборудования включает следующие функции для управления устройствами Intel AMT:

- Автоматическая генерация идентификаторов аутентификации (PID и PPS) (версия 2)
- Изменение имени пользователя и пароля для управляемых устройств
- Конфигурация и включение политик System Defense (версия 2)
- Конфигурация и включение мониторинга агента Agent Presence (версия 2)

Управление устройствами с агентами управления и без них

Если устройство поддерживает технологию Intel AMT, то некоторые функции управления доступны даже в том случае, если в устройстве не установлен агент LANDesk. Если устройства подключены к сети и находятся в режиме ожидания, то их можно обнаружить и включить в инвентаризацию для того, чтобы ими можно было управлять из других устройств сети.

Если устройство поддерживает Intel AMT, но в нем не установлен агент управления, то его можно обнаружить с помощью функции обнаружения неуправляемых устройств, поместить в базу данных инвентаризации, а затем отобразить в списке **Мои устройства**. Однако при этом многие функции управления System Manager являются недоступными. Эти функции становятся доступными только при установке агента LANDesk. Ниже перечислены функции управления, доступные для устройств с поддержкой технологии Intel AMT:

- **Сводка инвентаризации.** Часть обычной базы данных инвентаризации, которую можно просматривать в реальном времени и в которой можно запрашивать данные об устройстве, даже если оно отключено.
- **Журнал событий.** Журнал событий Intel AMT, содержащий описание и степень важности событий. Может просматриваться в реальном времени.

- **Менеджер удаленной загрузки.** Операции включения и выключения устройства, а также некоторые команды загрузки можно запустить с консоли удаленного управления независимо от состояния операционной системы и питания устройства. Доступные команды зависят от того, поддерживает ли их конкретное устройство. Некоторые устройства поддерживают не все команды загрузки.
- **Запуск сканирования уязвимых мест и отключение сети ОС.** Если есть подозрение, что в устройстве работает вредное программное обеспечение, то при следующей перезагрузке можно запустить сканирование уязвимых мест. В случае необходимости можно отменить доступ к сети на уровне операционной системы, чтобы предотвратить распространение по сети нежелательных пакетов.

Дополнительную информацию о параметрах управления см. в разделе Управление устройствами Intel AMT.

Требования аутентификации Intel AMT версии 1

Обнаружение устройств в качестве устройств с поддержкой Intel AMT возможно только после открытия на устройстве экрана настройки Intel AMT и изменения установленного производителем пароля по умолчанию на безопасный пароль. (Для получения информации о доступе к экрану настройки Intel AMT см. документацию к устройству.) Если этого не сделать, то устройства будут обнаруживаться, но не будут идентифицироваться в качестве устройств с поддержкой Intel AMT, и нельзя будет просмотреть сводку инвентаризации в полном объеме.

Для успешной аутентификации обнаруженных устройств Intel AMT в главном сервере необходимо, чтобы параметры имени пользователя и пароля соответствовали идентификационной информации, настроенной с помощью утилиты служб конфигурации. Можно изменить идентификационную информацию на экране настройки Intel AMT.

При добавлении устройства Intel AMT, которым необходимо управлять, в базу данных главного сервера, System Manager выполняет его автоматическую идентификацию в режиме, который был выбран в утилите служб конфигурации, независимо от того, было ли это устройство уже идентифицировано или нет. Режим малого бизнеса позволяет использовать основные функции управления без служб сети infrastructure и незащищенной сети, а корпоративный режим разработан для больших предприятий и обеспечивает безопасную работу на основе таких сетевых служб, как DHCP, DNS и служб центров сертификации TLS для обеспечения безопасного взаимодействия между управляемым устройством и главным сервером.

При входе устройства Intel AMT в корпоративном режиме (Enterprise) главный сервер устанавливает в устройстве сертификат, необходимый для защиты коммуникаций. Если необходимо, чтобы устройством управлял другой главный сервер, то необходимо отменить идентификацию устройства, а затем снова идентифицировать его другим главным сервером. Если этого не сделать, функция Intel AMT устройства не будет отвечать, так как у нового главного сервера нет соответствующего сертификата. Если другой компьютер попытается использовать функцию Intel AMT устройства, это будет невозможно из-за отсутствия соответствующего сертификата.

Конфигурация устройств Intel* AMT

Устройства, оборудованные функцией Intel AMT, должны быть сконфигурированы во время их первой установки и включения питания. Процесс аутентификации включает несколько оценок защиты для гарантированного доступа к функциям оценки Intel AMT только авторизованных пользователей.

Устройства Intel AMT взаимодействуют в сети с сервером аутентификации. Этот сервер аутентификации принимает в сети сообщения от устройств Intel AMT и позволяет IT-персоналу управлять серверами через внеполосные коммуникации, независимо от состояния операционной системы устройства. System Manager работает в качестве сервера аутентификации для устройств Intel AMT и включает функции, которые помогают при идентификации устройств во время их установки. После этого можно начать управление устройствами с установленными дополнительными агентами управления System Manager или без них.

В этом разделе представлен процесс, рекомендуемый для конфигурации новых устройств Intel AMT (версия 2). Во время этого процесса будет использован System Manager для создания набора идентификаторов аутентификации (PID и PPS). После ввода на экране конфигурации устройства Intel AMT эти идентификаторы гарантируют безопасное подключение к серверу аутентификации, который использует их, чтобы устройство Intel AMT могло выполнить начальный процесс аутентификации.

Устройство с функцией Intel AMT версии 1 используют подобный процесс, но без идентификатора PID и ключа PPS. Подробную информацию см. в примечаниях в конце этого раздела.

Аутентификация для устройств Intel AMT 2

Когда получено устройство Intel AMT 2, IT-инженер собирает компьютер и включает его. После включения устройства инженер входит на экран конфигурации BIOS Intel ME (Management Engine) и меняет пароль по умолчанию (admin) на более надежный пароль. Это открывает доступ к экрану конфигурации Intel AMT Configuration Screen.

На экране конфигурации вводится следующая предварительная аутентификационная информация Intel AMT:

- Идентификатор аутентификации (PID)
- Предварительный ключ-пароль (PPS) также называемый предварительно опубликованным ключом (PSK)
- IP-адрес сервера аутентификации
- Порт 9982 в качестве порта для взаимодействия и сервером аутентификации
- Нужно выбрать корпоративный режим (Enterprise)
- Хост-имя устройства Intel AMT

Ключ PPS должен быть известен серверу аутентификации и управляемому устройству, но в целях безопасности не может быть передан по сети. Он должен быть введен вручную на устройстве (на экране конфигурации Intel AMT Configuration Screen) и сохранен в сервере аутентификации, который в этом случае также является главным сервером для

приложения System Manager. Пара PID/ключ PPS генерируется приложением System Manager и хранится в базе данных. Можно распечатать список используемых при аутентификации сгенерированных пар идентификаторов.

IT-инженер должен ввести IP-адрес главного сервера System Manager в качестве сервера аутентификации и указать порт 9982. Иначе, устройство Intel AMT по умолчанию будет отправлять общие широковещательные сообщения, которые могут быть получены севером конфигурации, через порт 9971.

Имя пользователя и пароль по умолчанию для доступа к экрану конфигурации Intel AMT - "admin" и "admin". Они могут быть изменены во время процесса аутентификации. Имя пользователя может оставаться неизменным, но пароль нужно изменить на более надежный. Новое имя пользователя и пароль вводятся так, как описано далее, в утилите конфигурации служб, которая входит в состав System Manager. После конфигурации каждого из устройств можно изменить имя пользователя и пароль отдельно для каждого устройства, но в целях безопасности аутентификации нужно использовать имя пользователя и пароль, находящиеся в службах конфигурации.

После того, как указанная ранее информация введена на экране конфигурации Intel AMT, устройство во время первого подключения к сети отправляет сообщения приветствия "hello", пытаясь взаимодействовать с сервером аутентификации. Если сервер аутентификации получит эти сообщения, после установления сервером подключения к устройству начинается процесс аутентификации.

Когда главный сервер получает сообщения приветствия и сверяет их с PID/ключом PPS, он выполняет аутентификацию устройства Intel AMT в режиме TLS. Режим TLS (Transport Layer Security) устанавливает защищенный коммуникационный канал между главным и управляемым сервером для процесса аутентификации. Этот процесс включает создание записи в базе данных с идентификатором устройства UUID и шифрованными идентификационными данными. После того, как данные устройства занесены в базу данных, устройство появляется в списке неуправляемых устройств.

Когда устройство Intel AMT будет аутентифицировано главным сервером, оно может управляться только с использованием функции Intel AMT. Оно может быть выбрано из списка неуправляемых и добавлено в число управляемых устройств . Можно также развернуть в устройстве агентов System Manager для использования большего числа функций управления.

Далее представлен рекомендуемый процесс использования System Manager для аутентификации устройств Intel AMT 2. Особые инструкции для элементов 1 и 2 приводятся в следующих процедурах.

1. Запустите утилиту служб конфигурации для указания нового, защищенного пароля для аутентификации устройств Intel AMT. (Далее см. подробное описание).
2. Используйте System Manager для генерации файла набора идентификаторов аутентификации Intel AMT (PID и PPS) и распечатки списка ключей. (Далее см. подробное описание).
3. Войдите в экран конфигурации Intel ME из программы BIOS и измените пароль по умолчанию на более надежный пароль.

4. Войдите в экран конфигурации Intel AMT. Введите пару идентификатор PID/ключ PPS из списка распечатанных идентификаторов аутентификации. Введите IP-адрес главного сервера (сервер аутентификации) и укажите порт 9982. Убедитесь, что для аутентификации выбран корпоративный режим (Enterprise). Введите хост-имя устройства Intel AMT.
5. После выхода из экрана BIOS устройство начнет отправку сообщений приветствия (hello).
6. Главный сервер получает сообщения приветствия и проверяет PID/ключ PPS на соответствие списку сгенерированных ключей. Если они совпадают, выполняется аутентификация устройства для режима TLS.
7. Устройство добавляется в список обнаруженных неуправляемых устройств.
8. Выберите его и добавьте к управляемым устройствам. По умолчанию оно будет управляться в качестве устройства без агентов, и далее на нем можно развернуть агенты управления.

Установка имени пользователя и пароля Intel AMT в службах конфигурации

1. На главном сервере выберите **Пуск| LANDesk | Службы конфигурации**.
2. Выберите вкладку **Конфигурация Intel AMT**.
3. Введите **admin** в качестве имя пользователя и пароль в окне **Текущая идентификационная информация Intel AMT**.
4. Введите имя пользователя (необязательно) и надежный пароль в диалоге **Аутентификация с новыми учетными данными Intel AMT**.
5. Нажмите **OK**.

Эти имя пользователя и пароль должны быть введены перед созданием набора идентификаторов аутентификации.

Генерация набора идентификаторов аутентификации Intel AMT

1. В левой навигационной панели главного сервера выберите **Конфигурация оборудования**.
2. Разверните список **AMT** и перейдите к полю **Идентификация** для **генерации идентификаторов AMT**.
3. Введите число генерируемых идентификаторов (обычно это число планируемых для аутентификации устройств).
4. Если для идентификаторов нужно использование другого префикса, введите его в поле **Префикс PID**. Этот префикс может содержать только символы алфавита, введенные на верхнем регистре, и цифры из кодовой таблицы ASCII. Длина префикса не может превышать 7 символов.
5. Введите имя набора для идентификации группы сгенерированных идентификаторов.
6. Отметьте параметр **Показать сгенерированные идентификаторы AMT** (Show generated AMT IDs) для отображения списка сгенерированных идентификаторов. Если этот параметр не будет отмечен, сгенерированные идентификаторы будут сохранены в базе данных, но не будут отображаться на экране.
7. Щелкните **Сгенерировать идентификаторы** (Generate IDs).
8. После создания идентификаторов выберите параметр **Печать идентификаторов** (Print ID list) для открытия нового окна со списком идентификаторов. (В этом новом окне отображаются только текущие, разрешенные для показа идентификаторы). Для распечатки списка можно использовать функцию печати браузера.

9. Для просмотра списка всех сгенерированных идентификаторов не заполняйте поле **Имя набора** (Batch name) и щелкните **Просмотр идентификаторов набора** (View batch IDs).
10. Для просмотра одного набора сгенерированных идентификаторов введите имя набора в текстовом поле **Имя набора** (Batch name) и выберите **Просмотр идентификаторов набора** (View batch IDs).

За один раз можно сгенерировать любое количество ключей аутентификации. Эти ключи хранятся в базе данных для дальнейшего использования во время аутентификации устройств Intel AMT. После того, как устройства аутентифицированы, а ключи использованы, отображается страница **Generate AMT IDs** (Generate AMT IDs), на которой использованные идентификаторы показаны с затенением, что обеспечивает простоту контроля их использования.

Префикс идентификатора PID добавляется для удобства определения идентификаторов, но его использование необязательно. Рекомендуется использовать 0-4 символа; максимальная длина префикса - 7 символов.

Необходимо указать имя для идентификации набора ключей аутентификации. Это должно быть описательное имя, которое указывает на принадлежность идентификаторов к устройствам. Например, можно сгенерировать наборы для каждого подразделения внутри компании и назвать их: "Производство", "Маркетинг", "Финансы" и т.д. Если позднее нужно будет просмотреть сгенерированные идентификаторы, можно ввести имя набора и выбрать **Просмотр идентификаторов набора** для отображения списка идентификаторов только этого набора.

Надежные пароли

Для повышения защиты сетевых коммуникаций Intel AMT требует использования надежного пароля. Пароли должны удовлетворять следующим требованиям:

- Длина пароля должна быть не менее 8 символов
- Пароль должен содержать не менее одной цифры (0-9)
- Пароль должен включать один не алфавитно-цифровой символ ASCII (например, !, &, %)
- Пароль должен содержать латинские символы, введенные на верхнем и нижнем регистре, или символы не ASCII (UTF+00800 и далее)

Ошибки процесса аутентификации

Если будет введен идентификатор PID, не соответствующий ключу PPS (например, ключ PPS соответствовал другому идентификатору), в журнале контроля входа появится сообщение об ошибке, а процесс аутентификации будет прекращен. Необходимо перезапустить устройство и ввести правильную пару идентификатора и ключа PPS на экране конфигурации Intel AMT.

Если ошибка отобразится во время ввода идентификатора на экране конфигурации Intel AMT, значит вы неверно ввели идентификатор. Для обеспечения правильности ввода проводится проверка его контрольной суммы.

Поиск устройств Intel AMT 1.0

После запуска программы поиска устройств выполняется обнаружение устройств Intel AMT версии 1 и добавление их в папку Intel AMT списка **неуправляемых** устройств. Устройства обнаруживаются в качестве устройств Intel AMT, если они были сконфигурированы с защищенными именем пользователя и паролем, на который были заменены установки, выполненные изготовителем устройства.

Когда на экране конфигурации Intel AMT вы добавляете защищенное имя пользователя и пароль, можно также ввести IP-адрес сервера аутентификации и указать номер порта 9982, как это выполняется при конфигурации устройств Intel AMT 2. Однако для аутентификации устройств Intel AMT 1 не используется пара - идентификатор и ключ PPS. Если был указан IP-адрес сервера аутентификации, главный сервер будет работать в качестве сервера аутентификации, и вы сможете управлять устройствами без установленных агентов управления.

Помните, что устройства Intel AMT версии 1 не могут использовать тот же уровень защиты, что и устройства версии 2. Компания Intel рекомендует, чтобы устройства версии 1 были сконфигурированы в изолированной и защищенной сети. После конфигурации их можно переместить для управления в менее защищенную сеть.

Изменение имени пользователя и пароля для устройств Intel* AMT

Имя пользователя и пароль необходимы для идентификации в новых устройствах Intel AMT (версия 1). Для устройств, которые будут управляться с помощью System Manager, имя пользователя и пароль, вводимые на экране конфигурации Intel AMT, должны быть аналогичны имени и паролю, вводимым в утилите конфигурации служб System Manager. Имя пользователя и пароль в утилите конфигурации служб сохраняются в базе данных и применяются для идентификации всех устройств Intel AMT.

Для повышения защиты сетевых коммуникаций Intel AMT требует использования надежного пароля. Пароли должны удовлетворять следующим требованиям:

- Длина пароля должна быть не менее 8 символов
- Пароль должен содержать не менее одной цифры (0-9)
- Пароль должен включать один не алфавитно-цифровой символ ASCII (например, !, &, %)
- Пароль должен содержать латинские символы, введенные на верхнем и нижнем регистре, или символы не ASCII (UTF+00800 и далее)

После аутентификации для обслуживания IT-безопасности необходимо регулярно менять имена пользователей и пароли. Можно использовать различные комбинации имени пользователя и пароля для каждого устройства с поддержкой Intel AMT или только одну комбинацию имени пользователя и пароля для нескольких устройств. Новые комбинации имени пользователя и пароля, вводимые на странице аппаратной конфигурации, хранятся в базе данных и используются приложением System Manager для защищенного взаимодействия с управляемыми устройствами Intel AMT.

Изменение имени пользователя и пароля для устройств Intel AMT

1. В левой навигационной панели главного сервера выберите **Конфигурация оборудования**.
2. Разверните список **AMT** и перейдите к полю **Конфигурация**.
3. В списке **Все устройства** выберите одно или несколько устройств, для которых нужно изменить имя пользователя и пароль. На панели инструментов нажмите кнопку **Цель**.
4. В нижней части панели введите новое имя пользователя, а затем введите и подтвердите новый пароль.
5. Выберите **Целевые устройства**, затем **Применить**.

   В этом же списке можно выбрать одно или несколько устройств, затем щелкнуть **Выбранные устройства**, а затем **Применить**.

Конфигурация политики System Defense

Intel AMT* 2.0 включает в себя функцию System Defense, поддерживающую политику безопасности сети на устройствах с функциональными возможностями Intel AMT 2.0. Можно выбрать и применить политику System Defense на управляемых устройствах, используя инструментальное средство **Конфигурация оборудования**.

При применении политики System Defense на устройстве Intel AMT, устройство фильтрует входящие и исходящие сетевые пакеты в соответствии с определенной политикой. При совпадении сетевого трафика с условиями предупреждения, определенными для фильтра, генерируется предупреждение, и сетевой доступ к устройству блокируется. Устройство будет изолировано от сети до тех пор, пока вы не завершите процесс исправления для соответствия данной политике.

System Manager содержит предварительно определенные политики System Defense, которые вы можете применить для устройств Intel AMT. Каждая политика содержит набор фильтров, определяющий, какой вид сетевого трафика недопустим и какие действия нужно выполнить в результате, когда трафик снова станет соответствовать критериям фильтра. Ниже приведен процесс выбора и применения политики.

1. Назначьте одно или более управляемых устройств.
2. Выберите политику System Defense, которую хотите применить; при необходимости, отредактируйте политику.
3. Примените политику на целевых устройствах.

Когда политика System Defense активна на управляемом устройстве, устройство контролирует весь входящий и исходящий сетевой трафик. При обнаружении условий фильтрации происходит следующее.

1. Управляемое устройство посылает предупреждение ASF на главный сервер и в журнале предупреждений производится запись.
2. Главный сервер определяет, какая политика была нарушена, и отключает сетевой доступ на управляемом устройстве.
3. Устройство записывается в очередь исправления System Defense (в инструментальном средстве **Конфигурация оборудования**).

4. Для восстановления сетевого доступа устройства администратор выполняет необходимые исправления и затем удаляет устройство из очереди исправления. Таким образом, восстанавливается первоначальная политика System Defense на устройстве.

В следующем разделе этот процесс описан более детально.

Выбор и применение политики System Defense

System Manager содержит следующие предварительно определенные политики System Defense, которые можно применить для устройств Intel AMT 2.0. Политики определяются с помощью следующих параметров: номер порта, тип пакета и количество пакетов за определенное время. При включении политики она регистрируется с Intel AMT на выбранных вами устройствах. Политики сохраняются в виде файлов XML на управляемом устройстве в папке CircuitBreakerConfig.

- **BlockFTPSrvr.** Эта политика предупреждает трафик через порт FTP. При посылке и получении пакетов через порт FTP 21 пакеты отбрасываются, и сетевой доступ приостанавливается.
- **LDCBKillNics.** Эта политика блокирует трафик через все сетевые порты, кроме следующих портов управления:

Описание портов	Диапазон номеров	Направление трафика	Протокол
Управление LANDesk	9593-9595	Послать/получить	TCP, UDP
Управление Intel AMT	16992-16993	Послать/получить	Только TCP
DNS	53	Послать/получить	Только UDP
DHCP	67-68	Послать/получить	Только UDP

Когда главный сервер прекращает сетевой доступ к управляемому устройству, он практически применяет данную политику к этому устройству. После удаления устройства из очереди исправления на устройстве восстанавливается первоначальная политика.

- **LDCBSYNFlood.** Эта политика обнаруживает атаку в виде синхронной лавины пакетов, происходит отказ от обслуживания: при включенном флажке SYN за одну минуту пропускаются не более 10000 пакетов TCP. При превышении этого количества пакетов сетевой доступ приостанавливается.
- **UDPFloodPolicy.** Эта политика обнаруживает атаку в виде потока UDP-пакетов, происходит отказ от обслуживания: пропускаются не более 20,000 UDP пакетов в минуту на портах, пронумерованных от 0 до 1023. При превышении этого количества пакетов сетевой доступ приостанавливается.

Выбор политики System Defense

1. В левой навигационной области выберите **Конфигурация оборудования**.
2. Выберите **AMT**, просмотрите дерево сверху вниз и найдите **Политики**.
3. В списке устройств выберите устройства, на которых вы хотите применить политику (для выбора нескольких устройств используйте сочетание клавишей: нажатая Ctrl+щелчок мыши или нажатая Shift+щелчок мыши).
4. На панели инструментов нажмите кнопку **Цель**, чтобы добавить устройства к списку **Целевые устройства**.
5. На нижней панели выберите политику из раскрывающегося списка.
6. Выберите **Целевые устройства** и щелкните **Применить**.

Восстановление сетевого доступа к устройствам в очереди исправлений

Если сетевой доступ к устройству был приостановлен в результате применения политики System Defense, устройство появляется в очереди исправлений. Оно остается там до тех пор, пока вы не удалите его из списка, после чего восстанавливается активная политика на данном устройстве. Перед тем, как это сделать, вы должны решить проблему, в результате которой устройство было помещено в очередь. Например, если был обнаружен трафик FTP, вы должны подтвердить, что были предприняты необходимые действия для предупреждения дальнейшего нежелательного трафика FTP на устройстве.

Удаление устройства из очереди исправлений

1. В левой навигационной области выберите **Конфигурация оборудования**.
2. Выберите **AMT**, просмотрите дерево сверху вниз и найдите **Исправление**.
3. Выберите устройства, на которых можно восстановить первоначальную политику System Defense и нажмите **Удалить**.

Конфигурация Intel* AMT Agent Presence

Версия Intel* AMT 2.0 включает в себя средство обеспечения безопасности Agent Presence, которое следит за наличием агентов ПО на управляемых устройствах. Можно подключить мониторинг Agent Presence, чтобы убедиться, что агенты управления на ваших устройствах постоянно работают, а также для получения предупреждения об остановке агента даже в том случае, если другие агенты, работающие на базе ПО, не могут обнаружить проблему.

Программа System Manager использует Intel AMT Agent Presence для наблюдения за двумя агентами: стандартным агентом управления и службой мониторинга. Это очень полезно в ситуациях, когда взаимодействие, необходимое для нормального мониторинга, отсутствует. Например, уровень взаимодействия устройства не функционирует или сам агент мониторинга перестал работать. По умолчанию Agent Presence также следит за своим собственным процессом мониторинга, в случае его остановки вы будете предупреждены.

Мониторинг Agent Presence осуществляется с помощью конфигурации таймера, который "слушает" сообщения о тактовых импульсах от агентов управления на устройстве для получения подтверждения о работе агентов. Если таймер прекращает работу вследствие

отсутствия сообщения о тактовых импульсах, Intel AMT посылает предупреждение на главный сервер.

Когда вы производите конфигурацию Agent Presence, агент устройства регистрируется на Intel AMT для отсылки тактовых импульсов прямо на Intel AMT; если получение тактовых импульсов прекращается, Intel AMT может послать предупреждение на главный сервер с помощью внеполосного взаимодействия о том, что агент устройства не отвечает. Intel AMT посылает предупреждение о событии прерывания на конкретной платформе (PET) на главный сервер с описанием изменившегося состояния. По умолчанию это предупреждение записывается в журнале с сообщением о состоянии устройства. Можно сконфигурировать инициализацию других действий предупреждений при получении данного предупреждения (информацию о конфигурации действий предупреждений см. в разделе Конфигурация действий предупреждений).

При конфигурации мониторинга Agent Presence можно включить или отключить мониторинг для двух агентов и установить следующие значения:

- **Тактовый импульс:** максимальный интервал времени (в секундах) между импульсами. Если новый импульс не был получен в течение заданного интервала времени, считается, что агент не отвечает. По умолчанию это значение равно 120 сек для стандартного агента управления и 180 сек для службы мониторинга; минимальное значение для обоих - 30 сек.
- **Время запуска:** максимальный интервал времени (в секундах), допустимый после начала работы операционной системы до момента, когда должен быть получен тактовый импульс от агента. Если заданный интервал времени превышен, считается, что агент не отвечает. Agent Presence конфигурируется на Intel AMT при установке агента, Этого времени должно быть достаточно, чтобы агент начал работать и мог послать свой первый тактовый импульс. Значение по умолчанию 360 сек; минимальное значение - 30 сек.

Редактирование конфигурации Intel* AMT Agent Presence

1. В левой навигационной области выберите **Конфигурация оборудования**.
2. Разверните **AMT**, просмотрите дерево сверху вниз и найдите **Конфигурация AP**.
3. Для отключения мониторинга службы Agent Presence на устройствах Intel AMT 2.0, снимите флажок **Включить мониторинг Agent Presence**.
4. Для отключения мониторинга отдельного агента, снимите флажок, находящийся рядом с именем агента. (Даже при снятии обоих флажков Agent Presence будет продолжать следить за своим собственным процессом мониторинга, пока он будет оставаться включенным).
5. В текстовом окне введите новое значение для параметра **Тактовый импульс** для изменения максимального интервала времени между импульсами (минимум 30 сек).
6. В текстовом окне введите новое значение для параметра **Время запуска** для изменения максимального интервала времени, допустимого после начала работы операционной системы устройства до момента, когда должен быть получен тактовый импульс от агента (минимум 30 сек; рекомендуется - 120 сек).

Поддержка IPMI

System Manager обеспечивает поддержку IPMI (Intelligent Platform Management Interface) версий 1.5 и 2.0. IPMI - спецификация, разработанная компаниями Intel,*, H-P*, NEC* и Dell* для определения интерфейса сообщений и систем управляемого оборудования. IPMI содержит функции мониторинга и восстановления, которые позволяют использовать большинство функций независимо от того, включен компьютер или нет, или от состояния операционной системы. Для получения более подробной информации о IPMI посетите Web-сайт Intel.

Мониторинг IPMI управляется контроллером BMC (Baseboard Management Controller). Контроллер BMC функционирует в режиме автономного питания и автономного опроса состояния систем. Если контроллер BMC определит, что какие-либо элементы находятся вне требуемого диапазона, можно настроить определенные действия IPMI, например, регистрацию события, выдачу предупреждений или выполнение таких автоматических действий, как выключение питания системы или сброс.

Для определения контроллера BMC в системе необходимо установить SMBIOS версии 2.3.1 или выше. Если контроллер BMC не определяется, некоторая информация IPMI не будет отображаться в отчетах, экспортироваться и т.д.

IPMI определяет общие интерфейсы для оборудования, которые используются для мониторинга физического состояния таких характеристик, как температуры, напряжения, вращение вентиляторов, работа источников питания и определение вскрытия корпуса. Кроме того, для мониторинга состояния IPMI обеспечивает другие системные функции управления, включая автоматическую выдачу предупреждений, автоматическую функцию закрытия и перезапуска системы, функцию удаленного перезапуска, функции контроля электропитания и отслеживания активов.

Команды меню System Manager изменяются в зависимости от устройства IPMI, а также от состояния операционной системы.

Функции управления для устройств IPMI

Функции мониторинга зависят от компонентов, установленных в наблюдаемом устройстве, а также от состояния устройства. После настройки любого устройства IPMI с установленным контроллером BMC с помощью консоли администратора с некоторыми ограничениями можно выполнять мониторинг этого устройства без установки дополнительных агентов управления. Сюда включено внеполосное управление при прекращении подачи питания на устройство или при нефункционирующей операционной системе. Полнофункциональное управление возможно при установленном агенте управления, при наличии контроллера BMC, при включенном питании устройства, а также при функционировании операционной системы. В приведенной ниже таблице сравниваются функциональные возможности различных конфигураций.

	Только BMC*	**BMC + агент**	**Агент (без IPMI)**
Внеполосное управление	X	X	

	Только BMC*	**BMC + агент**	**Агент (без IPMI)**
включено			
Внутриполосное управление включено		X	X
Обнаружение устройства разрешено**	X	X	X
Чтение датчиков окружения	X	X	В зависимости от оборудования
Удаленное включение/выключение питания	X	X	X
Чтение и очистка журнала событий	X	X	
Настройка предупреждений	X	X	X
Чтение информации ОС		X	X
Корректное закрытие		X	X
Чтение информации SMBIOS (процессор, слоты, память)		X	X
Синхронизация IP (ОС-BMC)		X	
Таймер контроля		X	
BMC взаимодействует с главным сервером	X	X	

	Только BMC*	BMC + агент	Агент (без IPMI)
Локальные компоненты System Manager взаимодействуют с главным сервером		X	X
Полный диапазон функций управления System Manager		X	

*Стандартный контроллер BMC. Мини-контроллер BMC является упрощенной версией контроллера BMC. Данный контроллер обладает перечисленными выше функциями со следующими ограничениями:

- Не поддерживает переназначение последовательных соединений через ЛС (SOL).
- Для управления BMC назначается только одно имя пользователя.
- Для взаимодействия с BMC используется только один канал.
- Сокращен объем памяти для хранения журнала (SEL).

**Если контроллер BMC не настроен, он не будет отвечать на эхо-тест ASF, который используется в продукте для функции обнаружения IPMI. Это означает, что вам нужно будет искать его как обычный компьютер. При развертывании агента управления исполнимая конфигурация сервера просканирует используемую систему, определит наличие IPMI и сконфигурирует BMC.

Конфликты с другими драйверами IPMI

Если установлено другое программное обеспечение управления, которое содержит драйверы IPMI в устройствах, которыми нужно управлять с помощью System Manager, нужно удалить эти продукты перед развертыванием агентов Management Suite с функциями управления IPMI.

Например, Microsoft* Windows* Server 2003 имеет IPMI-поддержку с использованием WinRM (Windows Remote Management), который включает поставщика услуг WMI (Windows Management Instrumentation) и драйвер IPMI. Однако программное обеспечение System Manager не поддерживает работу этого драйвера IPMI и устанавливает свой драйвер. Если WinRM установлен в устройство, которым нужно управлять с помощью System Manager, сначала нужно удалить WinRM, используя функцию Windows установки/удаления программ (**Пуск | Панель управления | Установка и удаление программ | Добавление и удаление компонентов Windows | Средства управления и наблюдения |**; отмените пометку параметра **Управление оборудованием** | щелкните **OK**).

Конфигурация IPMI BMC

Страница **Конфигурации IPMI BMC** используется для настройки параметров взаимодействия с устройствами с IPMI-поддержкой. Описанные ниже функции доступны

для внутриполосных устройств; если устройство является внеполосным, параметры доступны только для конфигурации энергопотребления и пользователей BMC.

ВНИМАНИЕ. Настоятельно рекомендуется не изменять параметры IPMI, если только пользователь не является специалистом в области спецификации IPMI и знаком с соответствующими технологиями, используемыми для реализации этих параметров. Неправильное использование этих параметров конфигурации может привести к ошибкам System Manager при взаимодействии с устройствами IPMI.

Доступны следующие параметры конфигурации:

- Таймер контроля
- Конфигурация энергопотребления
- Настройки пользователя
- Пароль BMC
- Конфигурация ЛС
- Конфигурация SOL
- Конфигурация IMM

Изменение настроек таймера контроля

IPMI обеспечивает интерфейс для таймера контроля BMC. Таймер может быть установлен для периодического истечения и настраивается для запуска определенных действий (например, для выключения и включения питания). System Manager настраивается на периодический сброс таймера, чтобы он не завершал работу; если устройство становится недоступным (например, прекратился доступ питания или устройство "зависло"), таймер не сбрасывается, а по его истечении выполняется действие.

Можно указать период времени до истечения таймера и выбрать какое-либо действие, которое будет запущено по истечении таймера. Можно не предпринимать никаких действий, выполнить полный сброс (завершение работы системы и перезагрузка) устройства, корректно выключить питание системы или выполнить цикл выключения и включения питания (корректное выключение и включение питания системы).

Также можно настроить контроллер BMC для прекращения отправки широковещательных сообщений ARP (Address Resolution Protocol) во время работы таймера контроля, что может снизить объем сетевого трафика. Если вы приостановите рассылку сообщений ARP, они будут возобновлены после истечения таймера контроля.

Изменение настроек таймера контроля

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать.
2. В левой навигационной панели информационной консоли сервера выберите **Конфигурация оборудования**.
3. Разверните список **Конфигурация IPMI BMC** и выберите **Таймер контроля**.
4. Отметьте параметр **Включить таймер контроля** для включения таймера.
5. Укажите частоту проверки таймера (количество минут или секунд).
6. Выберите действие для запуска по истечении таймера контроля.

7. Если не требуется, чтобы BMC выполнял широковещательную передачу сообщений протокола ARP при включенном таймере контроля, отметьте параметр **Приостановить BMC ARP**.
8. Нажмите **Применить**.
9. Если после изменения параметров таймера контроля необходимо установить их значения по умолчанию, выберите **Восстановить параметры по умолчанию**.

Изменение настроек конфигурации электропитания

При прекращении подачи питания в компьютер IPMI можно указать действие, которое должно будет выполнено при возобновлении подачи питания. Рекомендуется восстановить состояние компьютера во время прекращения подачи питания, однако можно выбрать вариант прекращения работы или всегда включать компьютер после восстановления питания.

Изменение параметров конфигурации электропитания

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать.
2. В левой навигационной панели информационной консоли сервера выберите **Конфигурация оборудования**.
3. Разверните список **Конфигурация IPMI BMC** и выберите **Конфигурация энергопотребления**.
4. Выберите действие при восстановлении питания.
5. Нажмите **Применить**.
6. Если после изменения параметров энергопотребления необходимо установить их значения по умолчанию, выберите **Восстановить параметры по умолчанию**.

Изменение настроек пользователя BMC

System Manager выполняет аутентификацию в BMC, используя уникальную для BMC комбинацию имени и пароля пользователя (отличную от других имен пользователей System Manager). System Manager резервирует первое имя пользователя для взаимодействия с BMC. Если BMC позволяет определение других имен пользователей, для аутентификации BMC можно определить дополнительные имена и пароли пользователей.

Можно указать уровень привилегий для каждого пользователя. Для усовершенствованных модулей IMM можно указать уровни привилегий протокола для каждого канала (telnet, http и https).

ВНИМАНИЕ! Будьте предельно осторожны во время изменения этих настроек. При неправильной настройке параметров взаимодействие контроллера BMC устройства взаимодействие с данным продуктом будет невозможно.

Изменение настроек пользователя BMC

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать.

2. В левой навигационной панели информационной консоли сервера выберите **Конфигурация оборудования**.
3. Разверните список **Конфигурация IPMI BMC** и выберите **Настройки пользователя**.
4. Для очистки поля имени пользователя щелкните номер указателя и выберите **Очистить**.
5. Для добавления или изменения имени пользователя, щелкните номер указателя и выберите **Правка**.
6. Введите имя пользователя.
7. Для установки пароля отметьте параметр **Задать пароль**, затем введите и подтвердите пароль.
8. Выберите уровни привилегий для локальной сети и последовательного интерфейса.
9. Нажмите **Сохранить**.

Конфигурация пароля BMC

Приложение System Manager выполняет аутентификацию в контроллере BMC устройства, используя имя пользователя по умолчанию (user 1) и пароль. Вы не можете изменить имя этого пользователя, но можете изменить его пароль. После изменения пароля, новые значения сохраняются в базе данных и в BMC.

Изменение пароля по умолчанию для BMC

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать.
2. В левой навигационной панели информационной консоли сервера выберите **Конфигурация оборудования**.
3. Разверните список **Конфигурация IPMI BMC** и выберите **Пароль**.
4. Введите и подтвердите новый пароль.
5. Нажмите **Применить**.

Изменение конфигураций ЛС

Сообщения IPMI могут выдаваться напрямую из BMC в интерфейс ЛС в дополнение к системному интерфейсу устройства. Включение взаимодействия по ЛС позволяет главному серверу получать предупреждения IPMI, даже если устройство выключено. Главный сервер обслуживает данное взаимодействие до тех пор, пока устройство физически подключено к сети и имеет сетевой адрес, а также до тех пор, пока на устройство подается основное питание.

ВНИМАНИЕ! При выборе настраиваемой конфигурации соединений с контроллером BMC через ЛС или последовательный интерфейс будьте предельно осторожны при изменении параметров. При неправильной настройке параметров взаимодействие контроллера BMC устройства с данным продуктом будет невозможно.

Если вы определили канал локальной сети, можно использовать настройки по умолчанию для BMC-контроллера устройства или можно изменить настройки IP-адреса и сетевого шлюза. Чтобы настроить цели для предупреждений SNMP, отправляемых контроллером BMC для каждого предупреждения о событиях конкретной платформы (PET), воспользуйтесь этими настройками.

Также можно изменить настройку строки SNMP-сообщества для отправки предупреждений по локальной сети. Во время конфигурации этих настроек необходимо указать строку SNMP-сообщества для SNMP-аутентификации. Для каждой конфигурации можно настроить информацию цели отправляемых предупреждений, где указывается, где и как предупреждения были отправлены, а также были ли они подтверждены.

Установка свойств конфигурации канала ЛС

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать.
2. В левой навигационной панели информационной консоли сервера выберите **Конфигурация оборудования**.
3. Разверните список **Конфигурация IPMI BMC** и выберите **Конфигурация ЛС**.
4. В раскрывающемся списке коммуникаций ЛС выберите **Всегда доступно** для поддержания открытого доступа к BMC-контроллеру. Если было выбрано **Выключено**, вы не сможете получить доступ к BMC через локальную сеть, когда устройство будет недоступно для внутриполосного управления.
5. Выберите уровень привилегий пользователя для канала: **Административный уровень** - доступ ко всем командам; **Уровень пользователя** - ограниченный доступ: только чтение (если выбран уровень пользователя, набор возможностей ограничен).
6. Отметьте параметр **Полностью выключить BMC ARP** (Permanently turn off BMC ARPs) для выключения отправки из BMC сообщений протокола ARP (Address Resolution Protocol). Это уменьшит сетевой трафик, но может не позволить взаимодействие с BMC-контроллером, когда устройство будет недоступно для внутриполосного управления.
7. Отметьте параметр **Выключить ответы ARP** (Turn off ARP responses) для запрещения BMC отправлять сообщения ответов ARP, когда недоступна операционная система. Если будет включен этот параметр, вероятно, будет нарушено взаимодействие с BMC, когда устройство будет недоступно для внутриполосного управления.
8. IP-настройки для канала локальной сети устанавливаются автоматически, если контроллер BMC синхронизирован с каналом ОС. В противном случае будет установлен флажок на вкладке **IP-настройки** (IP settings). Можно не менять эту установку для использования параметров протокола DHCP, которая установлена автоматически, или можно снять этот флажок и исправить текстовые поля, добавив статические адреса. Однако предпочтительнее использовать автоматические настройки.
9. Выберите вкладку **Отправлять предупреждения через ЛС** (Send alerts over LAN) для конфигурации строки SNMP-сообщества (см. далее).
10. Для сохранения своих изменений нажмите **Применить**.

Свойства отправки предупреждений по ЛС

1. Откройте страницу **Конфигурация ЛС** (LAN configuration) (см. выше действия 1-3).
2. Выберите вкладку **Отправлять предупреждения через ЛС** (Send alerts over LAN).
3. Отметьте параметр **Включено** для разрешения отправки SNMP-предупреждений.
4. Укажите строку в поле **Строка SNMP-сообщества** (SNMP community string) для использования аутентификации SNMP.
5. Для конфигурации целей предупреждений дважды щелкните номер указателя и откройте диалог **Свойства**.

6. Укажите IP-адрес, для которого BMC будет отправлять предупреждения (а также соответствующий MAC-адрес).
7. Укажите число попыток, частоту повторов и предпочитаемый сетевой шлюз.
8. Если нужно, чтобы предупреждения были подтверждены (увеличивает сетевой трафик), отметьте параметр **Подтвердить предупреждения** (Acknowledge alerts).
9. Нажмите **OK**.
10. После завершения настроек на странице конфигурации локальной сети щелкните **Применить**.

Изменение конфигурации переназначения последовательного интерфейса через ЛС (SOL)

Используйте конфигурацию SOL (Serial Over LAN) для настройки параметров модема последовательного интерфейса в случае его специального использования, например, при переназначении сообщений теста BIOS POST в порт модема последовательного интерфейса. Если для BMC-контроллера необходимо коммутируемое подключение через модем, укажите параметры модема, такие как, строки инициализации и строки набора.

Для работы модема последовательного интерфейса нужно сконфигурировать системную BIOS платы устройства и перемычки на ней. Для получения информации о конфигурации конкретного устройства, см. документацию к этому устройству.

ВНИМАНИЕ! При выборе настраиваемой конфигурации соединений с контроллером BMC через ЛС или последовательный интерфейс будьте предельно осторожны при изменении параметров. При неправильной настройке параметров взаимодействие контроллера BMC устройства с данным продуктом будет невозможно.

Изменение параметров конфигурации SOL

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать.
2. В левой навигационной панели информационной консоли сервера выберите **Конфигурация оборудования**.
3. Разверните список **Конфигурация IPMI BMC** и выберите **Конфигурация SOL**.
4. Отметьте параметр **Включить коммуникации последовательного интерфейса через ЛС** для включения SOL.
5. Выберите минимальный уровень: **Уровень пользователя, необходимый для активизации SOL**.
6. Выберите **Скорость SOL-сеансов**, которая соответствует конфигурации оборудования устройства.
7. Нажмите **Применить**.

Изменение конфигураций IMM

Страница **Конфигурация IMM** отображается только для устройств с поддержкой IPMI, оборудованных дополнительной расширительной платой IMM. Параметры этой страницы позволяют включать и выключать протоколы и функции, используемые с устройствами, имеющими поддержку IMM. Перед тем, как менять настройки IMM, обратитесь к документации изготовителя.

Изменение параметров конфигурации электропитания

1. В окне **Мои устройства** дважды щелкните устройство, которое хотите сконфигурировать.
2. В левой навигационной панели информационной консоли сервера выберите **Конфигурация оборудования**.
3. Разверните список **Конфигурация IPMI BMC** и выберите **Конфигурация IMM**.
4. Отметьте включаемые протоколы и функции, а затем добавьте любые нужные настройки. Доступны следующие параметры:
   - KVM
   - SNMP
   - telnet
   - Предупреждения SMTP
   - HTTP
   - HTTPS
5. Нажмите **Применить**.

Управление устройствами Dell* DRAC

Этот продукт включает интеграцию управления с устройствами, содержащими Dell* DRAC (Remote Access Controller контроллер удаленного доступа). DRAC - это аппаратный контроллер удаленного управления с интерфейсом для управления оборудованием серверов с IPMI-поддержкой на основе устройств Dell. Контроллер DRAC имеет назначенный IP-адрес, используемый для идентификации устройства DRAC во время поиска и управления устройствами.

Устройства, содержащие контроллер Dell DRAC, могут управляться также, как и другие устройства с IPMI-поддержкой. Когда устройство обнаружено и добавлено в список управляемых устройств, его управление будет выполняться так же, как и управление любых других устройств с IPMI-поддержкой. Кроме того, приложение System Manager также имеет уникальные функции Dell DRAC.

Функция администрирования сервера OpenManage - это консоль на основе Web-интерфейса, предоставляемая компанией Dell для управления устройствами Dell с контролерами DRAC. Обычно доступ к ней осуществляется в браузере по IP-адресу контроллера DRAC с вводом имени пользователя и пароля. Когда устройство с контроллером Dell DRAC управляется с помощью приложения System Manager, можно также открыть эту утилиту из интерфейса System Manager.

Приложение System Manager также позволяет управлять именами пользователей и паролями для доступа к функции администрирования сервера OpenManager и отображает на информационной консоли сервера три журнала этой утилиты.

Открытие функции администрирования OpenManage Server Administrator для устройства Dell DRAC

1. Дважды щелкните устройство в списке **Все устройства**.
2. В информационной консоли сервера разверните список **Hardware** (Оборудование) и щелкните **Dell DRAC**. Будет отображен IP-адрес и другая идентификационная информация.

3. Щелкните **Launch Dell DRAC utility** (Запуск утилиты Dell DRAC) для открытия в новом окне средства администрирования сервера OpenManage.

Журналы Dell DRAC доступны для просмотра в приложении System Manager

Три журнала утилиты администрирования сервера OpenManage отображаются на информационной консоли приложения System Manager.

- **Dell DRAC log** (Журнал Dell DRAC). Отслеживает все события, записанные программой Server Administrator, например, процедуры входа в систему, состояние сеанса, состояние обновления микропрограммы и взаимодействие контроллера DRAC с другими компонентами устройства. Информация, отображаемая в приложении System Manager включает важность произошедших событий, описание и предложение действий для исправления ошибок.
- **Dell DRAC command log** (Журнал команд Dell DRAC). Отслеживает все команды, выданные для приложения Server Administrator. В журнале отображаются команды: кем и когда выполнены, число попыток входа и выхода из системы, а также ошибки доступа.
- **Dell DRAC trace log** (Журнал трассировки Dell DRAC). Полезен для контроля сведений о событиях во время сетевого взаимодействия, например, предупреждения, отправка сообщений на пейджер или сетевое подключение, инициированное DRAC.

Просмотр журналов для устройства Dell DRAC

1. Дважды щелкните устройство в списке **Все устройства**.
2. На информационной консоли сервера разверните список **Журналы**.
3. Щелкните **Dell DRAC log** (Журнал Dell DRAC), **Dell DRAC Command log** (Журнал команд Dell DRAC) или **Dell DRAC trace log** (Журнал трассировки Dell DRAC).

Управление именами пользователей для устройств с поддержкой Dell DRAC

Для доступа к интерфейсу администрирования сервера OpenManage нужно войти в систему с именем пользователя и паролем, определенным для устройства. По умолчанию пользователь **root** является первым в списке и не может быть удален, но его пароль можно изменить. В список можно добавить до 15 других пользователей. В то время, как имена пользователей контроллера DRAC могут иметь различный уровень доступа, приложение System Manager определяет только имена пользователей на административном уровне.

Добавление или редактирование имен пользователей и паролей для устройства с поддержкой DRAC

1. Дважды щелкните устройство в списке **Все устройства**.
2. На информационной консоли сервера выберите **Информация об оборудовании**.

3. На консоли конфигурации оборудования разверните список **Dell DRAC configuration** (Конфигурация Dell DRAC) и щелкните **Dell DRAC users** (Пользователи Dell DRAC). В списке будут отображены уже определенные пользователи.
4. Для изменения пароля пользователя щелкните номер пользователя и выберите **Change password** (Изменить пароль). Введите и подтвердите новый пароль, а затем выберите **Apply** (Применить). (Для назначения одного пароля для нескольких пользователей выберите их с помощью нажатия комбинации Ctrl+щелчок мыши или нажмите клавишу Shift+щелчок мыши).
5. Для добавления пользователя выберите **Add user** (Добавить пользователя). Введите имя пользователя, пароль и подтвердите новый пароль, а затем выберите **Apply** (Применить). Пользователь будет добавлен в список.

   Примечание. Если будет введено имя пользователя, которое уже есть в списке, новый пароль , введенный для этого пользователя, перезапишет существующий пароль этого пользователя; второй пользователь с таким же именем не будет добавлен в список.

6. Для удаления пользователя щелкните его номер и выберите **Delete user** (Удалить пользователя), а затем щелкните **OK**. (Для удаления нескольких пользователей, выберите их с помощью нажатия комбинации Ctrl+щелчок мыши или нажмите клавишу Shift+щелчок мыши).

Все пользователи в этом списке имеют административный уровень доступа для открытия средства администрирования сервера OpenManage Server Administrator.

Установка и обслуживание базы данных главного сервера

Установка базы данных главного сервера

При установке по умолчанию данного продукта база данных Microsoft MSDE устанавливается на ваш главный сервер. Это единственный возможный параметр для базы данных, доступный в System Manager, и может быть установлена только одна база данных главного сервера. База данных должна быть установлена только в отдельном специализированном сервере.

Схема базы данных поддерживает Microsoft SQL Server 2000 с пакетом обновления версии 4 (SP4). На всех серверах баз данных необходимо установить MDAC 2.8.

Установленная в главном сервере база данных должна быть абсолютно новой. Если вы устанавливаете System Manager на сервер, где раньше были установлены LANDesk® Management Suite или Server Manager, вы не можете использовать существующую структуру базы данных для установки System Manager.

В утилите конфигурации служб LANDesk имеется интерфейс, который позволяет настраивать различные службы. На вкладке "Общие" данной утилиты отображается имя текущего сервера, имя базы данных и имя/пароль пользователя, необходимые для доступа к базе данных главного сервера. Эти имена и пароль используются всеми службами для доступа к базе данных главного сервера. Так как System Manager может использовать только одну базу данных главного сервера, имена сервера и базы данных изменять не нужно. Если необходимо, можно изменить имя пользователя и пароль. Дополнительную информацию см. в Приложении B. Конфигурация служб.

Приложение A. Системные требования и использование портов

Главный сервер должен иметь статический IP-адрес.

Главный административный сервер

Главный административный сервер поддерживает следующие операционные системы:

- Microsoft Windows 2000 Server (c SP4)
- Microsoft Windows 2000 Advanced Server (c SP4)
- Microsoft Windows 2003 Server Standard Edition (SP1)
- Microsoft Windows 2003 Server Enterprise Edition (SP1)

Поддержка сервера (агенты)

- Microsoft Windows 2000 Server (c SP4)
- Microsoft Windows 2000 Advanced Server (c SP4)
- Microsoft Windows 2000 Professional (c SP4)
- Microsoft Windows 2003 Server Standard Edition x86 (c SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (c SP1)
- Microsoft Windows 2003 Server Enterprise Edition x86 (c SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (c SP1)
- Microsoft Windows XP Professional (c SP2)
- Microsoft Windows XP Professional x64 (c SP2)
- Windows Small Business Server 2000 (c SP4)
- Windows Small Business Server 2003 (c 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

Браузеры

- Microsoft Internet Explorer 6.x (SP1)
- Mozilla 1.7 и выше
- Firefox 1.5 и выше

Базы данных

- MSDE (SP4)

Компоненты Microsoft Data Access

- MDAC 2.8 или более поздняя версия

Если нужно, чтобы два продукта управления LANDesk использовали одну базу данных, нужно установить их на один главный сервер. Соответственно, если нужно установить несколько продуктов на один главный сервер, необходимо использовать одну базу данных. Если оба продукта используют одну базу данных, они оба должны иметь версию 8.70.

Использование портов

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. Если вы не знакомы с этим предметом, здесь можно найти общую информацию по основным концепциям их работы.

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), являются целевыми портами.

Известные порты, например, порт 5007 (используемый службой инвентаризации) относятся 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
9595, 9594	с консоли на устройство	TCP	Конфигурация сервера
9595	с консоли на устройство	UDP	обнаружение
623	с консоли на устройство	UDP	ASF, обнаружение IPMI
5007	с консоли на устройство	TCP	инвентаризация
9535	с консоли на устройство	TCP	дистанционное управление
139, 145	с консоли на устройство	TCP	совместное использование файлов и принтеров
137, 138	с консоли на устройство	UDP	совместное использование файлов и принтеров

Перед тем, как данный продукт сможет осуществлять управление узлами, он должен их обнаружить с помощью установленного стандартного 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).

Приложение Б. Активизация главного сервера

Прежде чем использовать консоль, вы должны активировать главный сервер с помощью утилиты активизации главного сервера (Core Server Activation). Обычно это одноразовая процедура, которую нужно повторять только при приобретении дополнительных лицензий. Утилита активизации главного сервера используется для следующих целей:

- Активация нового сервера в первый раз.
- Обновление существующего главного сервера или модернизация Management Suite или Server Manager.
- Активизация нового сервера с использованием временной лицензии сроком на 45 дней.

Для запуска утилиты нажмите **Пуск | Все программы |** LANDesk **| Активизация главного сервер**. Если ваш главный сервер не подключен к Интернету, см. "Активизация главного сервера вручную или проверка данных количества узлов" ниже в данном разделе.

Для каждого главного сервера необходим авторизованный сертификат. Разные главные серверы не могут иметь общий сертификат авторизации, однако они могут проверять количество узлов одной и той же учетной записи LANDesk. Данная утилита запускается автоматически при первой перезагрузке после установки программы System Manager.

Периодически главный сервер генерирует информацию о проверке количества узлов в файле "\Программы\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 в данном файле, сделанные вручную, сделают недействительным содержимое сервера, и при следующем использовании будет послан отчет на 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, связь с сервером лицензий происходит автоматически и не требует выполнения каких-либо действий вручную. Если главный сервер не подключен к Интернету, при перезагрузке выберите **Закрыть** и отправьте файл авторизации по электронной почте по адресу: licensing@landesk.com.

Утилита активизации главного сервера не запускает автоматическое подключение к Интернету, но если вы соединитесь вручную и запустите утилиту активизации, то она сможет использовать удаленное соединение для отправки отчета с данными по использованию.

Если главный сервер не подключен к Интернету, можно проверить и отослать значение количества узлов вручную, как указано ниже в настоящем разделе.

Активизация сервера с использованием учетной записи ПО LANDesk

Перед тем как вы сможете активизировать новый сервер с полной лицензией, вы должны настроить учетную запись с помощью ПО LANDesk, предоставляющего вам лицензии на продукты ПО LANDesk и количество приобретенных вами узлов. Для активизации сервера вам необходима информация об учетной записи (контактное имя и пароль). Если у вас нет данной информации, свяжитесь с вашим торговым представителем по программному обеспечению LANDesk.

Не изменяйте дату или время главного сервера в промежутке между установкой продукта и активизацией главного сервера. Произойдет сбой активизации. Вам нужно будет удалить и переустановить продукт.

Активизация сервера

1. Выберите **Пуск | Все программы |** LANDesk **| Активизация главного сервера**.
2. Нажмите **Активировать**.

Активизация сервера с использованием временной лицензии

Временная лицензия сроком на 45 дней активизирует ваш сервер на сервере лицензирования ПО LANDesk. После истечения 45-дневного периода оценки вы не сможете зарегистрироваться на сервере, и он прекратит принимать сканирование инвентаризации, однако потери существующих данных в программном обеспечении или в базе данных не произойдет. Во время или после использования 45-дневной лицензии вы можете перезапустить утилиту для активизации базового сервера и перейти к полной активизации с использованием учетной записи ПО LANDesk. Если срок действия временной лицензии истек, то при переходе к использованию полной лицензии происходит повторная активизация главного сервера.

Активизация сервера для 45-дневной оценки

1. Выберите **Пуск | Все программы |** LANDesk **| Активизация главного сервера**.
2. Выберите **Активизировать главный сервер для 45-дневной оценки**.
3. Нажмите кнопку **Оценка**.

Обновление существующей учетной записи

Параметр обновления посылает информацию об использовании серверу лицензирования ПО LANDesk. Данные об использовании посылаются автоматически, если у вас есть подключение к Интернету, поэтому, как правило, нет необходимости использовать данный параметр для отправки данных о проверке количества узлов. Вы также можете использовать данный параметр для изменения главного сервера, ассоциированного с учетной записью ПО LANDesk. С помощью данного параметра можно также перейти от использования временной лицензии к полной лицензии.

Обновление существующей учетной записи

1. Выберите **Пуск | Все программы |** LANDesk **| Активизация главного сервера**.
2. Выберите **Обновить базовый сервер с контактным именем и паролем** LANDesk.
3. Введите **Контактное имя** и **Пароль**, которые будут использоваться на главном сервере. Если вы введете имя и пароль, отличные от использованных при первоначальной активизации главного сервера, произойдет переключение сервера на новую учетную запись.
4. Нажмите **Активировать**.

Активизация главного сервера вручную или проверка данных количества узлов

Если главный сервер не подключен к Интернету, утилита активизации главного сервера не сможет отправлять данные о количестве узлов. Вы увидите сообщение, предлагающее отправить данные активизации и проверки количества узлов вручную по электронной почте. Процесс активизации по электронной почте достаточно прост. 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 вручную или проверка данных количества узлов

1. Когда главный сервер предлагает вам вручную проверить данные количества узлов, он создает файл данных ACTIVATE.XML в папке \Программы\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. ПО LANDesk обработает прикрепление и отправит ответ по адресу, с которого прислано сообщение. ПО LANDesk содержит инструкции и новый файл авторизации.
3. Сохраните прикрепленный файл авторизации в папке \Программы\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.

Приложение B. Конфигурация служб

Вы можете использовать программу конфигурации служб для настройки следующих служб на вашем главном сервере и в базе данных:

Для запуска утилиты конфигурации служб в главном сервере щелкните **Пуск | Программы |** LANDesk **|** LANDesk **Конфигурация служб**.

Две кнопки отображаются за пределами вкладок:

- **Параметры.** Открывает диалог идентификационной информации сервера, в котором можно добавлять устройства, работающие в качестве предпочитаемых серверов. Для добавления устройства выберите **Добавить**. Это откроет диалог **Имя пользователя и пароль**.
- **Подтверждение OSD.** Для создания сред предварительной загрузки для Windows PE- или DOS необходимо обеспечить доступ к установочным компакт-дискам Windows PE 2005 и Windows NT 4. Выберите параметр **Проверить** для образов обеих сред, введите путь к соответствующему компакт-диску и щелкните **OK**.

Диалог "Имя пользователя и пароль"

Диалог **Имя пользователя и пароль** используется для предоставления информации о добавляемом предпочитаемом сервере.

Ввод информации о предпочитаемом сервере

1. В программе конфигурации служб выберите **Параметры**.
2. В диалоге идентификационной информации сервера выберите **Добавить**.
3. Введите описание, аутентификационную информацию и диапазон IP-адресов.
4. Выберите **Тест параметров** для проверки правильности указанной информации.
5. Щелкните **OK** для добавления предпочитаемого сервера в диалог идентификационной информации сервера.

- **Имя сервера.** Имя предпочитаемого сервера.
- **Имя пользователя.** Имя пользователя для аутентификации в сервере. Это должно быть полностью определенное доменное имя (например, домен\имя_пользователя).
- **Описание.** Это описание предпочитаемого сервера.
- **Пароль.** Пароль предпочитаемого сервера.

- **Начальный IP-адрес.** Введите начальный адрес IP для диапазона адресов, которыми нужно ограничить использование предпочитаемого сервера. Начальный адрес не должен быть больше конечного IP-адреса. Первые три октета начального и конечного адресов должны совпадать, например 10.100.10.1 и 10.100.10.255.
- **Конечный IP-адрес.** Введите конечный IP-адрес для диапазона адресов, которые необходимо просканировать.
- **Добавить.** Добавляет диапазоны IP-адресов к рабочей очереди внизу диалогового окна.
- **Удалить.** Обеспечивает удаление выбранного диапазона адресов IP из рабочей очереди.

Вкладки конфигурации служб

Прежде чем приступить к конфигурации служб, откройте вкладку **Общие** и укажите главный сервер и базу данных, для которых вы хотите сконфигурировать данную службу.

Примечание. Любые изменения в конфигурации служб, которые вы делаете для главного сервера или базы данных, не вступят в силу до тех пор, пока вы не перезапустите службу на этом главном сервере.

Выбор главного сервера и базы данных

Вкладка **Общие** позволяет выбрать главный сервер и базу данных и предоставляет идентификационную информацию, чтобы вы могли сконфигурировать службы для данного главного сервера.

Диалог конфигурации служб. Вкладка "Общие"

Используйте данный диалог для выбора главного сервера и базы данных, для которых вы хотите сконфигурировать определенную службу. Затем выберите вкладку службы и укажите настройки для данной службы.

- **Имя сервера.** Отображает имя главного сервера, к которому вы в настоящий момент подключены.
- **Сервер.** Позволяет вам вводить имя другого главного сервера и каталог его базы данных.
- **База данных.** Позволяет вводить имя базы данных главного сервера.
- **Имя пользователя.** Идентифицирует пользователя в базе данных главного сервера с помощью идентификационной информации (указывается при установке).
- **Пароль.** Идентифицирует пароль пользователя, необходимый для доступа к базе данных главного сервера (указывается при установке).
- **Это база данных Oracle.** Указывает на то, что база данных главного сервера, указанная выше, является базой данных Oracle. (Не применимо для System Manager.)
- **Обновить настройки.** Восстанавливает настройки, существовавшие во время открытия диалога конфигурации служб.

Конфигурация службы инвентаризации

Используйте вкладку **Инвентаризация** для конфигурации данной службы на главном сервере и в базе данных главного сервера, которые вы выбрали на вкладке "Общие".

Диалог "Конфигурация служб" Вкладка "Инвентаризация"

Используйте данную вкладку для указания следующих параметров инвентаризации:

- **Имя сервера**. Отображает имя главного сервера, к которому вы в настоящий момент подключены.
- **Журнал статистики**. Ведет журнал действий базы данных главного сервера и статистики.
- **Транспорт шифрованных данных.** Позволяет сканеру инвентаризации посылать данные инвентаризации об устройстве из сканируемого устройства обратно главному серверу в виде шифрованных данных через SSL.
- **Сканировать сервер в**. Определяет время для сканирования главного сервера.
- **Начать обслуживание в**. Определяет время для проведения стандартного обслуживания базы данных главного сервера.
- **Дни сканирования инвентаризации**. Устанавливает количество дней до того, как произойдет удаление записи сканирования инвентаризации.
- **Входы основного владельца**. Устанавливает число сканирований инвентаризации для отслеживания регистраций пользователя с целью определения основного владельца устройства. Основным владельцем является пользователь, который регистрировался на сервере чаще всего за установленное количество входов. Значением по умолчанию является 5; минимальным и максимальным значением - 1 и 16 соответственно. Если каждая регистрация выполняется разными пользователями, то основным владельцем считается, тот, кто зарегистрировался последним. В каждый момент времени устройство может иметь только одного основного владельца, связанного с ним. Данные о регистрации основного пользователя включают полное имя и в ADS, и в NDS, доменное имя или имя в местном формате (в том же порядке), а также дату последнего входа.
- **Дополнительно.** Открывает диалог **Дополнительно**, в котором можно установить различные параметры сканера инвентаризации. Для изменения настроек выберите параметр, измените его в поле **Значение**, после чего нажмите **Установить**. Для просмотра описаний настроек выберите параметр и просмотрите его сведения в поле **Описание**.
- **Программное обеспечение.** Открывает диалог **Настройки сканирования программного обеспечения**, в котором вы можете сконфигурировать время сканирования программного обеспечения сервера и параметры истории.
- **Атрибуты.** Открывает диалог выбора атрибутов, в котором можно выбрать хранимые в базе данных атрибуты сканирования инвентаризации.
- **Обработка дубликатов. Устройства**. Открывает диалог Конфигурация обработки дубликатов имен устройств, в котором можно выбрать параметры для удаленных устройств с дублированными именами, MAC-адресами или и тем и другим (см. далее раздел **Дублированные устройства**).

- **Обработка дубликатов. ИД устройства.** Открывает диалог **Идентификатор дубликата устройства**, где вы можете выбрать атрибуты, по которым идентифицируются устройства. Вы можете использовать данный параметр, чтобы избежать сканирования идентификаторов дублирующихся устройств в базу данных главного сервера (см. ниже Конфигурация обработки идентификатора дубликата устройства).
- **Состояние службы инвентаризации**. Показывает, запущена или остановлена служба на главном сервере.
- **Пуск**. Запускает службу на главном сервере.
- **Останов**. Останавливает службу на главном сервере.

Диалог "Настройки сканирования программного обеспечения"

Используйте данный диалог для настройки частоты сканирования программного обеспечения. Оборудование устройства сканируется каждый раз, когда в устройстве запускается сканер инвентаризации, однако программное обеспечение устройства сканируется только с интервалом, указанным вами в данном диалоге.

- **При каждом входе.** Сканирует все программное обеспечение, установленное в устройстве, при каждой регистрации пользователя.
- **Через (дни).** Сканирует программное обеспечение устройства только с определенным дневным интервалом, как автоматическое сканирование.
- **Сохранить историю за (дни).** Определяет, как долго должна сохраняться история инвентаризации устройства.

Конфигурация обработки дубликатов имен устройств

Используйте диалог "Дублированные устройства" для удаления дублированных устройств из базы данных.

1. На вкладке "Инвентаризация" выберите **Устройства**.
2. В диалоге "Дублированные устройства" выберите параметр, который вы хотите использовать при удалении дублированных устройств, а затем нажмите **ОК**.

   Удалить дубликаты при.
   - **Совпадение имен устройств.** Удаляет более старые записи, когда в базе данных совпадают имена двух или более устройств.
   - **Совпадение MAC-адресов.** Удаляет более старые записи, когда в базе данных совпадают MAC-адреса двух или более устройств.
   - **Совпадение имен устройств и MAC-адресов.** Удаляет более старую запись ТОЛЬКО в том случае, если совпадают имена и MAC-адреса (для одной и той же записи) двух или более устройств.

Конфигурация обработки идентификатора дубликата устройства

Так как для конфигурации устройств в сети часто используются образы, возможность существования дублирующихся идентификаторов устройств увеличивается. Вы можете избежать этого, указав другие атрибуты устройства, что в комбинации с идентификатором

устройств, создает уникальный идентификатор для ваших устройств. Примерами таких атрибутов являются: имя устройства, имя домена, BIOS, шина, сопроцессор и т. д.

Функция дублирующегося идентификатора позволяет вам выбирать атрибуты устройства, которые могут быть использованы для уникальной идентификации сервера. Вы указываете, чем являются данные атрибуты, и какое количество атрибутов должно быть пропущено, прежде чем устройство определяется как дубликат другого устройства. Если сканер инвентаризации выявляет дублированное устройство, он записывает событие в журнал событий приложений для указания идентификатора дублированного устройства. Диалог "Идентификатор дубликата устройства" содержит следующие параметры:

- **Список атрибутов.** Отображает список всех атрибутов, которые вы можете выбрать для уникальной идентификации устройства.
- **Идентификация атрибутов.** Отображает атрибуты, которые вы выбрали для уникальной идентификации устройства.
- **Переключатели идентификатора дубликата устройства.**
  - **Идентификация атрибутов.** Определяет количество атрибутов, которые должны не совпасть, прежде чем будет выявлено, что это дубликат другого устройства.
  - **Аппаратные атрибуты.** Определяет количество аппаратных атрибутов, которые должны не совпасть, прежде чем будет выявлено, что это дубликат другого устройства.
- **Отклонить идентичность дубликатов.** Заставляет сканер инвентаризации записывать идентификатор дублирующегося устройства и отклонять любые последующие попытки сканирования этого идентификатора устройства. Затем сканер инвентаризации генерирует новый идентификатор устройства.

Конфигурация обработки идентификатора дубликата устройства

1. В диалоге "Конфигурация служб" выберите вкладку **Инвентаризация**, а затем щелкните **Идентификатор устройства**.
2. Выберите из **Списка атрибутов** атрибуты, которые вы хотите использовать для уникальной идентификации устройства, а затем нажмите стрелку вправо для добавления атрибута в список **Атрибуты идентификации**. Вы можете добавить любое количество атрибутов.
3. Выберите количество атрибутов идентификации (и атрибутов оборудования), которые должны не совпасть, прежде чем будет выявлено, что это дубликат другого устройства.
4. Если вы хотите, чтобы сканер инвентаризации отклонял дублирующиеся идентификаторы устройств, выберите параметр **Отклонить идентичность дубликатов**.

Конфигурация службы планировщика

Используйте вкладку **Планировщик** для конфигурации данной службы на главном сервере и в базе данных сервера, которые вы выбрали на вкладке **Общие**. Вы должны иметь соответствующие права для выполнения данных задач, включая полные привилегии администратора на управляемых устройствах, позволяющие им получать пакеты, распространяемые System Manager. Вы можете указать несколько видов идентификационной информации для устройств, щелкнув **Смена имени**.

Диалог "Конфигурация служб" Вкладка "Планировщик"

Используйте данную вкладку для просмотра имени главного сервера и базы данных, которые вы выбрали ранее, и для указания следующих параметров назначенных заданий:

- **Имя пользователя**. Пользователь, под чьим именем будет работать служба назначения заданий. Имя пользователя может быть изменено. Для этого нажмите кнопку **Смена имени**.
- **Число секунд между попытками**. При настройке выполнения назначенных заданий со множеством попыток, данный параметр контролирует число секунд ожидания между попытками выполнения назначенных заданий.
- **Число секунд между попытками пробуждения**. Когда назначенное задание сконфигурировано для использования функции Wake on LAN, данная настройка контролирует число секунд, в течение которых служба назначения заданий будет ожидать пробуждения устройства.
- **Интервал между оценками запросов**. Число, указывающее количество времени между оценками запросов и единицу измерения данного числа (минуты, часы, дни, недели).
- **Настройки Wake on LAN**. **Порт IP**, который будет использоваться пакетом Wake On LAN, установленным назначенными заданиями для пробуждения устройства.
- **Состояние службы планирования**. Показывает запущена или остановлена служба на главном сервере.
- **Пуск**. Запускает службу на главном сервере.
- **Останов**. Останавливает службу на главном сервере.
- **Перезапуск.** Перезапускает службу на главном сервере.
- **Дополнительно.** Открывает диалог **Дополнительные настройки планировщика**, в котором можно изменить настройки управления работой планировщика заданий. Для изменения настроек выберите **Правка**, выполните изменение и щелкните **OK**.

Диалог конфигурации служб. Диалог "Смена имени"

Используйте диалог **Смена имени** (выберите **Смена имени** на вкладке **Планировщик**), чтобы изменить имя пользователя, установленное в планировщике по умолчанию. Вы также можете указать альтернативную идентификационную информацию для службы планировщика, когда ей необходимо выполнить задание на неуправляемом устройстве.

Для установки агентов System Manager на неуправляемых устройствах, служба планировщика должна иметь возможность подключаться к устройствам, используя учетную запись администратора. По умолчанию служба планировщика использует учетную запись LocalSystem. Идентификационная информация LocalSystem обычно работает с устройствами, которые не принадлежат домену. Если устройства принадлежат домену, вы должны указать учетную запись администратора домена.

Если вы хотите изменить данные учетной записи службы планировщика, вы можете указать другую учетную запись администратора домена для использования в устройстве. Если вы управляете устройствами в нескольких доменах, вы можете добавить дополнительную идентификационную информацию для службы планировщика. Если для службы планировщика нужно использовать учетную запись, отличную от LocalSystem или

если нужно предоставить альтернативную идентификационную информацию, необходимо указать имя основного пользователя службы планировщика, который имеет административные права на главном сервере. Альтернативная идентификационная информация не требует наличия административных прав для главного сервера, но в нее должны входить административные права для устройств.

Служба планировщика сначала использует идентификационную информацию, указанную по умолчанию, а потом использует информацию, которую вы указали в списке **Альтернативная идентификационная информация**, до тех пор пока не найдет подходящую или пока не останется информации. Идентификационная информация, которую вы указываете, надежно шифруется и сохраняется в реестре главного сервера.

Вы можете установить данные параметры для идентификационной информации планировщика, указанной по умолчанию.

- **Имя пользователя.** Введите домен\имя пользователя по умолчанию или имя пользователя, которые будет использовать планировщик.
- **Пароль.** Введите пароль для идентификационной информации, которую вы указали.
- **Подтвердите пароль.** Введите пароль для подтверждения еще раз.

Вы можете установить данные параметры для дополнительной идентификационной информации планировщика.

- **Добавить.** Нажмите для добавления имени пользователя и пароля, которые вы указали в списке альтернативной идентификационной информации.
- **Удалить.** Нажмите для удаления идентификационной информации из списка.
- **Изменить.** Нажмите для внесения изменений в выбранную идентификационную информацию.

При добавлении альтернативной идентификационной информации укажите следующее:

- **Имя пользователя.** Введите имя пользователя, которое будет использовать планировщик.
- **Домен.** Введите домен для имени пользователя, которое вы указали.
- **Пароль.** Введите пароль для идентификационной информации, которую вы указали.
- **Подтвердите пароль.** Введите пароль для подтверждения еще раз.

Конфигурация службы специальных заданий

Используйте вкладку **Особые задания** для конфигурации данной службы на сервере и в базе данных сервера, которые вы выбрали на вкладке "Общие". Примерами специальных заданий являются сканирование инвентаризации или распространение программного обеспечения.

Если вы отключаете удаленное выполнение TCP, как протокол удаленного выполнения, служба специальных заданий по умолчанию использует протокол стандартного агента управления, независимо от того отключен он или нет. Кроме того, если включены и удаленное выполнение TCP, и стандартный агент управления, служба специальных заданий старается использовать вначале удаленное выполнение TCP и, если оно отсутствует, использует удаленное выполнение стандартного агента управления.

Вкладка **Особые задания** также позволяет вам выбирать параметры для обнаружения сервера. Перед тем, как служба специальных заданий сможет обработать задание, ей необходим текущий IP-адрес каждого сервера. Данная вкладка позволяет вам сконфигурировать связь службы с сервером.

Диалог "Конфигурация служб". Вкладка "Особые задания"

Используйте данную вкладку для указания следующих особых заданий:

Параметры удаленного выполнения

- **Отключить выполнение TCP**. Отключает TCP, как протокол удаленного выполнения, и в связи с этим использует по умолчанию протокол CBA.
- **Отключить выполнение CBA / перенос файлов**. Отключает стандартный агент управления, как протокол удаленного выполнения. Если стандартный агент управления отключен, а протокол удаленного выполнения TCP не найден в устройстве, произойдет сбой удаленного выполнения.
- **Включить тайм-аут удаленного выполнения**. Включает тайм-аут удаленного выполнения и определяет число секунд, после которого наступает тайм-аут. Тайм-ауты удаленного выполнения инициируются, если устройство посылает импульсы, но работа в устройстве зависла или зациклилась. Данная настройка применима к обоим протоколам (TCP или стандартный агент управления). Данное число может быть между 300 сек (5 мин) или 86400 сек (1 день).
- **Включить тайм-аут клиента**. Включает тайм-аут устройства и определяет число секунд, после которого наступает тайм-аут. По умолчанию протокол удаленного выполнения TCP посылает импульсы от устройства к устройству с интервалом в 45 секунд до тех пор, пока удаленное выполнение не завершится или наступит тайм-аут. Тайм-ауты клиента инициируются, когда устройство не посылает импульсы другому устройству.
- **Порт удаленного выполнения (по умолчанию 12174)**. Порт, через который происходит удаленное выполнение TCP. Если данный порт меняется, изменения должны быть внесены в конфигурацию клиента.

Параметры распространения

- **Распространение в <nn> серверов одновременно**. Максимальное количество устройств, на которые одновременно будут распространены особые задания.

Параметры обнаружения

- **UDP.** При выборе UDP используется запрос стандартного агента управления по UDP. Большинство компонентов System Manager зависит от стандартного агента управления, поэтому на ваших управляемых устройствах должен быть установлен стандартный агент управления. Это наиболее быстрый метод обнаружения и он установлен по умолчанию. С помощью UDP вы также можете выбрать эхо-тест UDP: **Попытки** и **Тайм-аут**.

- **TCP.** При выборе TCP используется HTTP-соединение с сервером, порт 9595. Данный метод обнаружения имеет преимущество, поскольку может работать через брандмауэр, если вы откроете порт 9595, но он может приводить к тайм-аутам HTTP-связи в случае отсутствия устройств. Данные тайм-ауты длятся 20 секунд и более. Если многие целевые устройства не отвечают на подключение TCP, выполнение вашего задания задержится.
- **Оба.** При выборе параметра "Оба" служба пытается обнаружить устройства, сначала используя UDP, потом TCP, и в конце концов, DNS/WINS, если он выбран.
- **Отключить широковещание в подсети.** Если этот параметр отмечен, поиск через широковещание в подсети выключен.
- **Отключить поиск DNS / WINS.** Отключает службу поиска имени для каждого устройства, если выбранный метод обнаружения TCP/UDP не работает.

Конфигурация службы многоадресной рассылки

Используйте вкладку **Многоадресная рассылка** для конфигурации параметров обнаружения представителей домена многоадресной рассылки на главном сервере и в базе данных, которые вы выбрали на вкладке **Общие**.

Диалог "Конфигурация служб". Вкладка "Многоадресная рассылка"

Используйте данную вкладку для указания следующих параметров многоадресной рассылки:

- **Использовать представителя домена многоадресной рассылки.** Использует список представителей домена многоадресной рассылки, который хранится в группах представления сети **Конфигурация > Представители домена многоадресной рассылки**.
- **Использовать кэшированный файл.** Запрашивает каждый домен многоадресной рассылки, чтобы обнаружить место, где уже имеется кэшированный файл. В этом случае вместо загрузки файла представителю может быть использован кэшированный файл.
- **Использовать кэшированный файл до предпочитаемого представителя домена.** Изменяет порядок обнаружения для выполнения в первую очередь параметра **Использовать кэшированный файл**.
- **Использовать широковещание.** Посылает широковещательные сообщения в подсеть, чтобы обнаружить любое устройство данной подсети, которое может быть представителем домена многоадресной рассылки.
- **Период сброса журнала (дни). Определяет** количество дней, в течение которых будут сохраняться записи в журнале.

Конфигурация пароля BMC

Используйте вкладку **Пароль BMC** для создания пароля для контроллера IPMI BMC (Baseboard Management Controller).

- На вкладке **Пароль BMC** введите пароль в поле **Пароль** и введите его еще раз в поле **Подтвердите пароль**, а затем щелкните **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.

Конфигурация параметров Intel AMT

Используйте вкладку **Конфигурация Intel AMT** для создания или изменения пароля на устройствах, совместимых с технологией Intel Active Managament, и просмотра инструкций поиска устройств AMT.

Конфигурация пароля Intel AMT

1. Введите имя текущего 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

Обнаружение и аутентификация устройств Intel AMT

Для обнаружения устройств AMT в поле идентификации главного сервера системы AMT BIOS введите IP-адрес главного сервера и порт 9982. Нажмите **Справка** в диалоге **Конфигурация служб** для получения дополнительной информации. Если устройство Intel AMT обнаружено и перенесено в список **Мои устройства**, оно автоматически инициализируется с использованием режима TLS.

Приложение Г. Защита агентов и доверенные сертификаты

Каждый главный сервер имеет уникальный сертификат и закрытый ключ, который создает программа установки во время первой установки главного сервера на устройстве. Устройства взаимодействуют только с теми главными серверами, для которых имеется соответствующий файл доверенного сертификата.

Устанавливаемые закрытые ключи и файлы сертификатов:

- **<Имя ключа>.key.** Файл .KEY является закрытым ключом для главного сервера и находится только на главном сервере. Если ключ дискредитирован, главный сервер и связь между серверами не будут защищены. Храните этот ключ в безопасном месте. Например, не посылайте его по электронной почте.
- **<Имя ключа>.crt.** Файл .CRT содержит открытый ключ для главного сервера. Файл .CRT является удобной для просмотра версией открытого ключа (можно просматривать информацию о ключе).
- **<Хэш>.0.** Файл .0 является файлом доверенного сертификата и его содержание идентично файлу .CRT. Однако он назван таким образом, чтобы компьютер мог быстро найти файл сертификата в каталоге, содержащем большое количество различных сертификатов. Имя - это хэш (контрольная сумма) информации об объекте сертификата. Для определения имени хэш-файла для определенного сертификата смотрите файл <имя ключа>.CRT. В файле есть сегмент файла .INI [LDMS]. Пара хэш=значение показывает значение <хэш>.

Все ключи хранятся на главном сервере в каталоге \Program Files\LANDesk\Общие файлы\Ключи. Открытый ключ <хэш>.0 также хранится в каталоге LDLOGON и должен оставаться там по умолчанию. <Имя ключа> - это имя сертификата, указанное вами при установке главного сервера. При установке желательно указать подробное имя ключа, например, имя главного сервера (или даже его полное имя) как имя ключа (например: ldcore или ldcore.org.com). Это облегчит идентификацию файлов сертификата/закрытого ключа в среде с несколькими серверами.

Создание резервных копий и восстановление файлов сертификата / закрытого ключа на главных серверах

Когда вы устанавливаете новый главный сервер, программа установки создает новый сертификат. Если вы выполняете повторную установку поверх существующего главного сервера, программа установки также создает новый сертификат. Если вы устанавливаете устройства с сертификатом, который не соответствует новому сертификату главного сервера, главный сервер не сможет взаимодействовать с этими устройствами. Если вы хотите переустановить главный сервер, у вас есть две возможности.

1. Переустановить агенты вручную с помощью конфигурации, встроенной на вашем новом главном сервере. Вы не можете использовать распределение ПО для обновления агентов, так как для главного сервера и устройств отсутствуют соответствующие сертификат и ключ.

2. Перед повторной установкой главного сервера создайте резервные копии существующих файлов сертификатов и ключей в надежном месте. После завершения повторной установки скопируйте старые ключи в место установки нового главного сервера. Новые и старые ключи могут работать совместно. Главный сервер будет использовать необходимый ключ автоматически.

Главные серверы могут содержать несколько файлов сертификатов/закрытых ключей. До тех пор, пока клиент может быть аутентифицирован с помощью одного из ключей в главном сервере, он может взаимодействовать с данным главным сервером.

В данный продукт включена утилита, которая предоставляет вторую возможность, указанную ниже. Утилита перемещения данных главного сервера (CoreDataMigration.exe) устанавливается в папку \Program Files\LANDesk\ManagementSuite. Она управляет резервным копированием и копированием таких данных, как ключи и сертификаты, при установке нового главного сервера.

Сохранение и восстановление набора сертификат/закрытый ключ

1. На исходном главном сервере откройте папку \Program Files\LANDesk\Shared Files\Keys.
2. Скопируйте файлы <имя ключа>.key, <имя ключа>.crt и <хэш>.0 на дискету или в другое безопасное место.
3. На целевом главном сервере скопируйте файлы с исходного места в ту же папку (\Program Files\LANDesk\Shared Files\Keys). Ключи вступят в силу немедленно.

Внимание! Храните файл с закрытым ключом в надежном месте.
Убедитесь, что закрытый ключ <имя ключа>.key не дискредитирован. Не передавайте ключ ненадежным методом, например, по электронной почте или путем общего доступа к открытому файлу. Главный сервер использует этот файл для аутентификации устройств, а также любой главный сервер с соответствующим файлом <имя ключа>.key может производить удаленные действия и перемещение файлов в управляемое устройство.

Советы по поиску и устранению неисправностей

Следующие советы относятся к проблемам, которые наиболее часто происходят на консоли.

Я не могу активировать главный сервер.
Если вы установили главный сервер, после чего изменили время устройства, вам не удастся активизировать сервер. Для активизации главного сервера нужно переустановить продукт.

При активизации главного сервера я получаю сообщение об ошибке, что невозможно прочитать базу данных главного сервера.
Проверьте физическое подключение главного сервера к сети и к Интернету. Если кабель отсоединен или Интернет-соединение главного сервера не установлено, процесс активизации не может быть выполнен.

Я не знаю URL-адреса страниц консоли.
Обратитесь к лицу, установившему главный сервер. Обычно это системный администратор. Однако обычно адрес для Server Manager и System Manager - это http://*имя_машины_главного_сервера*/ldsm. URL-адрес для Management Suite - http://*имя_машины_главного_сервера*/remote.

Какое имя использовалось при моем входе?
Посмотрите над панелью под именем LANDeskSystem Manager в разделе **Подключен как**.

Какой компьютер используется для моего входа?
Посмотрите над панелью под именем LANDeskSystem Manager в разделе **Подключен к**.

Я запускаю System Manager и сразу же получаю сообщение "Session Timed Out" (Тайм-аут сеанса).
При открытии System Manager из избранного или из закладок с расширением "/frameset.aspx" в конце адреса продукт может работать неправильно. Для устранения проблемы исправьте избранное или закладки, удалив это расширение, или скопируйте адрес (без расширения) прямо в командную строку браузера.

Я не вижу некоторые ссылки на навигационной панели.
Это происходит из-за того, что ваш администратор сети использует ролевое администрирование LANDeskSystem Manager или параметр уровня защиты, который ограничивает для вас выполнение некоторых задач, на которые у вас имеются права.

Сканер не может подключиться к устройству.
Если сканер не может подключиться к устройству, проверьте, что каталог Web-приложения сконфигурирован правильно. Если вы используете протокол https, нужно иметь допустимый сертификат. Проверьте наличие такого сертификата.

Я получаю ошибку "доступ запрещен" (permission denied) во время доступа к консоли.
Для использования защиты на уровне служб в Windows 2000 и 2003 необходимо отключить

анонимную аутентификацию. Проверьте настройки аутентификации на Web-сайте и папку Web-сайта ..\LANDesk\ldsm.

1. На сервере, содержащем Web-консоль, выберите **Пуск | Администрирование | Диспетчер служб IIS**.
2. Из меню ярлыка **Веб-узел по умолчанию** выберите **Свойства**.
3. На вкладке **Безопасность каталога** в области **анонимного доступа и контроля аутентификации** выберите **Правка**. Отмените параметр **Анонимный доступ** и выберите параметр **Встроенная проверка подлинности Windows**.
4. Нажмите **OK** для выхода из диалога.
5. На Web-сайте в подпапке по умолчанию .\LANDesk\ldsm выберите **Свойства**. Повторите действия с 3 по 4.

При просмотре консоли я вижу неверный сеанс.
Возможно, произошел тайм-аут сеанса браузера. Используйте кнопку **обновления** браузера для начала нового сеанса.

При попытке запуска Web-консоли появляется ошибка ASP.NET.
Если при попытке войти в Web-консоль появилось сообщение об ошибке ASP.NET, возможно, неправильно настроены разрешения ASP и каталога ASP. Переустановите конфигурацию ASP.NET путем ввода следующей команды:

```
ASPNET_REGIIS.EXE -i
```

Число элементов на странице отличается от указанного.
Когда вы указываете число элементов отображения на странице, это значение хранится в каталоге cookies Web-браузера и устаревает с наступлением тайм-аута сеанса.

Слишком часто возникает тайм-аут консоли.
Измените значение тайм-аута сеанса по умолчанию для отображения Web-страниц консоли. Значение по умолчанию для IIS - 20 минут отсутствия активности, перед истечением срока бездействия в системе. Для изменения тайм-аута сеанса IIS:

1. На Web-сервере откройте диспетчер службы Интернета IIS (IIS Internet Service Manager).
2. Разверните отображение Web-сайта по умолчанию.
3. Щелкните правой кнопкой мыши папку **LDSM**, а затем **Свойства**.
4. На вкладке **Виртуальный каталог** выберите **Конфигурация**.
5. Выберите вкладку **Параметры приложения** и измените значение тайм-аута.

Примечание.LANDeskSystem Manager8.70 - это продукт, работающий в сеансовом режиме. Не отключайте состояние сеанса.

Отчет отображается неправильно.
Для отображения интерактивных диаграмм во многих отчетах необходимо использовать Macromedia Flash Player*. Установите его и запустите отчет еще раз.

Почему я вижу в базе данных две копии одного устройства?
Возможно, вы удалили устройство из базы данных главного сервера и переустановили его с помощью UninstallWinClient.exe.

UninstallWinClient.exe находится в общей папке LDMain, которая является главной папкой программы ManagementSuite. К ней имеют доступ только администраторы. Эта программа удаляет агентов LANDesk из любого устройства, на котором выполняется. Вы можете переместить ее в любую папку по желанию или включить в сценарий входа. Это приложение Windows, работающее в фоновом режиме без отображения на интерфейсе. Вы можете видеть в базе данных две копии только что удаленного устройства. Одна из этих копий содержит только архивные данные, в то время как другая - всю текущую информацию. См. *руководство по развертыванию* для получения дополнительной информации о программе UninstallWinClient.exe.

Когда я пытаюсь обнаружить устройство IPMI, оно не отображается в папке IPMI на странице устройств без управления.
Устройства IPMI должны иметь контроллер BMC (Baseboard management controller), который конфигурируется с целью обнаружения устройств IPMI и полного функционального использования IPMI. Если контроллер BMC не сконфигурирован, устройство обнаруживается как компьютер. Вы можете затем добавить это устройство в список управляемых устройств и запустить утилиту служб конфигурации для конфигурирования пароля BMC. Данное приложение определит функциональность устройства IPMI.

Я добавляю в сервер диск S.M.A.R.T., Однако я не вижу диск S.M.A.R.T. в списке инвентаризации данного сервера для мониторинга.
Мониторинг устройств зависит от возможностей аппаратного обеспечения, установленного в устройстве, а также от правильности его настройки. Например, если в устройстве с отключенной в системной BIOS функцией S.M.A.R.T. установлен жесткий диск с поддержкой S.M.A.R.T. или устройство не имеет поддержки дисков S.M.A.R.T., данные мониторинга будут недоступны, а генерация ошибок невозможна.

Дисковое устройство USB не отображается в списке инвентаризации, пока не будет выполнено сканирование инвентаризации.
Когда дисковое устройство подключено с помощью кабеля USB к управляемому устройству, оно не будет сразу же отображено в списке жестких дисков инвентаризации устройства. Сразу после подключения оно будет показано в списке логических дисков. Оно не появится в списке жестких дисков, пока не будет выполнена инвентаризация устройства.

В управляемых системах Linux диск USB может быть смонтирован для отображения в списке инвентаризации. Если он был смонтирован, но без сканирования инвентаризации, он появится в списке логических дисков; после сканирования инвентаризации он также отобразится в списке жестких дисков. При отключении устройства оно должно быть демонтировано в системе. В некоторых системах Linux, работающих со старой версией ядра, устройство может оставаться в списке инвентаризации даже после размонтирования и отсоединения. В этом случае нужно перезагрузить управляемое устройство для удаления диска из списка инвентаризации.

При просмотре указателя справки Web-консоли он оказывается пустым.
Интерактивная HTML-справка Web-консоли обладает полнотекстовой функцией поиска, которая использует службу индексирования Windows. Обычно она включена по умолчанию. Если необходимо включить индексирование на Web-сервере, выполните следующие действия:

1. Выберите **Пуск | Программы | Администрирование | Службы**.
2. Дважды щелкните элемент **Indexing Service** и нажмите **Пуск**.
3. Нажмите **OK** для выхода из диалога.

Возможно, необходимо будет подождать (до нескольких часов), пока служба выполнит индексирование сервера.