Lenovo

Lenovo XClarity Administrator Руководство по планированию и установке для сред Docker

Версия 4.0.0

Примечание

Перед тем как воспользоваться этой информацией и самим продуктом, обязательно прочтите замечания по общим и юридическим вопросам в документации по XClarity Administrator в Интернете.

Первое издание (Февраль 2023 г.)

Содержание

Содержание i

Рисунки iii

Табл. v

Сводная информация по изменениям vii

Глава 1. Обзор Lenovo XClarity Administrator 1

Глава 2. Планирование для XClarity Administrator 7

Лицензии и бесплатная 90-дневная пробная версия 7
Обязательные требования к оборудованию и программному обеспечению 8
Брандмауэры и прокси-серверы 10
Доступность портов 12
Замечания по управлению 18
Замечания по сети 19
Ограничения конфигурации IP 19
Типы сетей 20
Конфигурации сети 20
Замечания по безопасности 32
Управление инкапсуляцией 32
Криптографическое управление 33
Сертификаты безопасности 35
Аутентификация 36
Учетные записи пользователей и группы ролей 39
Безопасность учетной записи пользователя 40
Замечания по высокому уровню доступности . . 40
Features on Demand 41

Глава 3. Установка Lenovo XClarity Administrator 43

Единая сеть данных и управления 43
Шаг 1. Подключение рамы, стоечных серверов и хоста Lenovo XClarity Administrator к стоечным коммутаторам верхнего уровня 46
Шаг 2. Настройка стоечных коммутаторов верхнего уровня 46
Шаг 3. Настройка модулей CMM 47
Шаг 4. Настройка Коммутаторы Flex 49
Шаг 5. Установка и настройка хоста 49
Шаг 6. Установка и настройка XClarity Administrator 50
Физически раздельные сети данных и управления 53
Шаг 1. Подключение рамы, стоечных серверов и хоста Lenovo XClarity Administrator к стоечным коммутаторам верхнего уровня 56
Шаг 2. Настройка стоечных коммутаторов верхнего уровня 57
Шаг 3. Настройка модулей CMM 57
Шаг 4. Настройка Коммутаторы Flex 59
Шаг 5. Установка и настройка хоста 60
Шаг 6. Установка и настройка XClarity Administrator 61
Топология виртуально разделенных сетей данных и управления 64
Шаг 1. Подключение рамы и стоечных серверов к стоечным коммутаторам верхнего уровня 67
Шаг 2. Настройка стоечных коммутаторов верхнего уровня 68
Шаг 3. Настройка модулей CMM 69
Шаг 4. Настройка Коммутаторы Flex 71
Шаг 5. Установка и настройка хоста 72
Шаг 6. Установка и настройка XClarity Administrator 73
Топология сети только для управления. 77
Шаг 1. Подключение рамы, стоечных серверов и хоста Lenovo XClarity Administrator к стоечным коммутаторам верхнего уровня 79
Шаг 2. Настройка стоечных коммутаторов верхнего уровня 79
Шаг 3. Настройка модулей CMM 80
Шаг 4. Настройка Коммутаторы Flex 82
Шаг 5. Установка и настройка хоста 83
Шаг 6. Установка и настройка XClarity Administrator 83
Реализация высокой доступности 87

Глава 4. Настройка Lenovo XClarity Administrator 89

Доступ к веб-интерфейсу Lenovo XClarity Administrator в первый раз 89
Создание учетных записей пользователей . . . 92
Настройка доступа к сети 93
Настройка даты и времени 100
Настройка обслуживания и поддержки 102
Настройка безопасности 105

Управление устройствами 106

Глава 5. Регистрация XClarity Administrator 119

Глава 6. Установка лицензии на полнофункциональную активацию 121

Установка лицензий на полнофункциональную активацию с помощью веб-интерфейса XClarity Administrator 123

Установка лицензий на использование всех функций с помощью веб-портала Features on Demand . . 127

Глава 7. Обновление XClarity Administrator как 131

Глава 8. Удаление XClarity Administrator 135

Рисунки

1. Пример реализации единой сети для управления, данных и развертывания операционной системы 24
2. Пример реализации физически разделенных сетей данных и управления, где сеть операционной системы является частью сети данных. 26
3. Пример реализации физически разделенных сетей данных и управления, где сеть операционной системы является частью сети управления 27
4. Пример реализации виртуально разделенных сетей данных и управления, где сеть операционной системы является частью сети данных. 29
5. Пример реализации виртуально разделенных сетей данных и управления, где сеть операционной системы является частью сети управления 30
6. Пример реализации сети управления, не поддерживающей развертывание операционной системы 31
7. Пример реализации сети только для управления с поддержкой развертывания операционной системы 32
8. Пример единой топологии сети данных и управления для виртуального устройства 44
9. Пример топологии единой сети данных и управления для контейнеров 45
10. Пример кабельных соединений для единой сети данных и управления 46
11. Места установки Коммутатор Flexв раме 49
12. Пример физически раздельных данных и топологии сети управления для виртуального устройства 55
13. Пример физически раздельных данных и топологии сети управления для контейнеров 55
14. Пример кабельных соединений для физически раздельных сетей данных и управления 56
15. Места установки Коммутатор Flexв раме 60
16. Пример виртуально раздельных данных и топологии сети управления для виртуального устройства 65
17. Пример виртуально раздельных данных и топологии сети управления для контейнеров 66
18. Пример кабельных соединений для виртуально раздельных сетей данных и управления 68
19. Пример конфигурации для Коммутаторы Flex в виртуально разделенных сетях данных и управления (VMware ESXi), в которой добавление меток VLAN включено в сети управления 69
20. Пример конфигурации для Коммутаторы Flex в виртуально разделенных сетях данных и управления (VMware ESXi), в которой добавление меток VLAN включено в сети управления 72
21. Пример топологии сети только для управления для виртуального устройства 78
22. Пример топологии сети только для управления для контейнеров. 78
23. Пример кабельных соединений для сети только для управления 79
24. Места установки Коммутатор Flexв раме 82

Табл.

1. Требуемые подключения к Интернету . . . 11
2. Назначение каждого сетевого интерфейса зависит от топологии сети 22
3. Назначение каждого сетевого интерфейса зависит от топологии сети 95

Сводная информация по изменениям

Последующие выпуски программного обеспечения управления Lenovo XClarity Administrator обеспечивают поддержку нового оборудования, усовершенствования программного обеспечения и исправления.

Обратитесь к файлу истории изменений (*.chg), который содержится в пакете обновлений для получения сведений об исправлениях.

Сведения обо всех поддерживаемых аппаратных средствах (включая серверы, раму и коммутаторы Flex) см. в Обязательные требования к оборудованию и программному обеспечению.

Сведения об изменениях в более ранних выпусках см. в разделе Что нового в документации по XClarity Administrator в Интернете.

В этом выпуске поддерживается указанное ниже оборудование.

- **Серверы и устройства**
  - ThinkAgile HX630 V3 (7D6M)
  - ThinkAgile HX645 V3 (7D9M)
  - ThinkAgile HX650 V3 (7D6N)
  - ThinkAgile HX665 V3 (7D9N)
  - ThinkAgile MX630 V3 (7D6U)
  - ThinkAgile MX650 V3 (7D6S)
  - ThinkAgile VX630 V3 (7D6X, 7Z63)
  - ThinkAgile VX635 V3 (7D9V)
  - ThinkAgile VX645 V3 (7D9K)
  - ThinkAgile VX650 V2-DPU (7Z63)
  - ThinkAgile VX650 V3 (7D6W)
  - ThinkAgile VX650 V3-DPU (7D6W)
  - ThinkAgile VX655 V3 (7D9W)
  - ThinkAgile VX665 V3 (7D9L)
  - ThinkAgile VX850 V3 (7DDK)
  - ThinkEdge SE350 V2 (7DA9)
  - ThinkEdge SE455 V3 (7DBY)
  - ThinkEdge SE360 V2 (7DAM)
  - ThinkSystem SD555 V3 (7DDP, 7DDQ)
  - ThinkSystem SD650 V3 (7D7M)
  - ThinkSystem SD650-I V3 (7D7L)
  - ThinkSystem SD650-N V3(7D7L)
  - ThinkSystem SD665 V3 (7D9P)
  - ThinkSystem SD665-N V3 (7DAZ)
  - ThinkSystem SR630 V3 (7D72, 7D73, 7D74)
  - ThinkSystem SR635 V3 (7D9G, 7D9H)
  - ThinkSystem SR645 V3 (7D9C, 7D9D)
  - ThinkSystem SR650 V3 (7D75, 7D76, 7D77)
  - ThinkSystem SR655 V3 (7D9E, 7D9F)
  - ThinkSystem SR665 V3 (7D9B, 7D9A)
  - ThinkSystem SR675 V3 (7D9Q, 7D9R)
  - ThinkSystem SR850 V3 (7D96, 7D97, 7D98)
  - ThinkSystem SR860 V3 (7D93, 7D94, 7D95)
  - ThinkSystem SR950 V3 (7DC4, 7DC5, 7DC6)
  - ThinkSystem ST650 V3 (7D7A, 7D7B)

- **Устройства хранения данных**
  - Массив ThinkSystem DE6400F All Flash (7DB6)
  - Массив ThinkSystem DE6400H Hybrid Flash (7DB6)
  - Массив ThinkSystem DE6600F All Flash (7DB7)
  - Массив ThinkSystem DE6600H Hybrid Flash (7DB7)
- **Коммутаторы**
  - Коммутатор ThinkSystem DB730S FC SAN (7D9J)
  - Директор ThinkSystem DB400D FC SAN (6684)
  - Директор ThinkSystem DB800D FC SAN (6682)

Эта версия поддерживает следующие усовершенствования в области планирования или установки программного обеспечения управления.

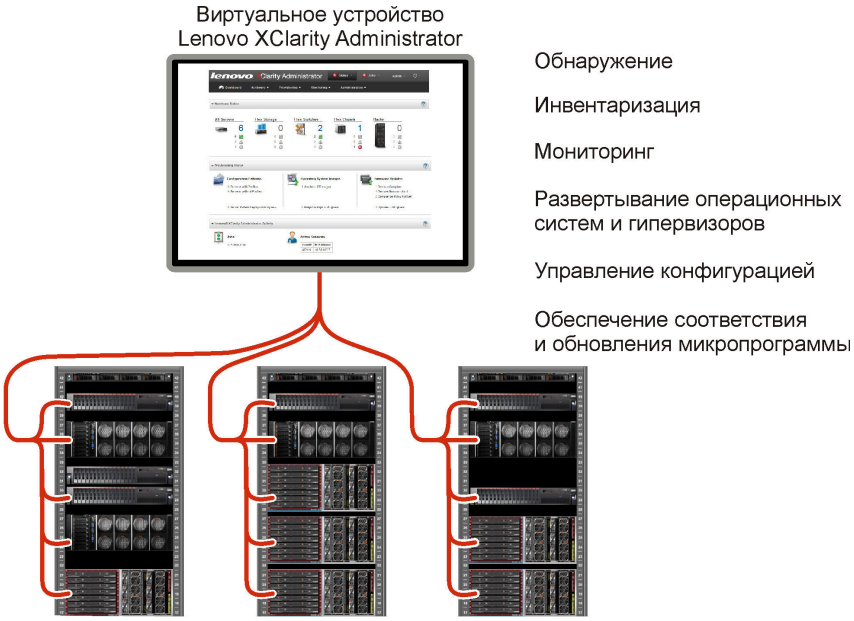
Функция	**Описание**
Планирование и установка	Из списка поддерживаемых алгоритмов ключа хоста удален ssh-rsa и добавлены ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 и ecdsa-sha2-nistp521 (см. раздел Криптографическое управление).

Глава 1. Обзор Lenovo XClarity Administrator

Lenovo XClarity Administrator — это централизованное решение для управления ресурсами, которое упрощает управление инфраструктурой, сокращает время ответов и повышает доступность серверных систем и решений Lenovo®. Оно работает как виртуальное устройство, автоматизирующее обнаружение, инвентаризацию, отслеживание, мониторинг и подготовку оборудования серверов, сети и хранилища в защищенной среде.

Подробнее:

- XClarity Administrator: управление оборудованием как программным обеспечением
- XClarity Administrator: обзор



XClarity Administratorпредоставляет централизованный интерфейс для выполнения следующих функций для всех управляемых устройств.

Управление оборудованием

XClarity Administrator обеспечивает управление оборудованием без агентов. Система может автоматически обнаруживать управляемые устройства, включая сервер, сеть и оборудование систем хранения. Данные инвентаризации управляемых устройств собираются и используются для составления обзорного представления инвентаря и состояния управляемого оборудования.

Существуют различные задачи управления для каждого поддерживаемого устройства, включая просмотр состояния и свойств, настройку параметров системы и сети, запуск интерфейсов управления, включение и выключение и удаленное управление. Дополнительные сведения об управлении устройствами см. в разделах Управление рамой, Управление серверами и Управление коммутаторами в документации по XClarity Administrator в Интернете.

Рекомендация. Сервер, сеть и оборудование систем хранения, которые могут управляться XClarity Administrator, называются *устройства*. Оборудование, которое находится под управлением XClarity Administrator, называется *управляемые устройства*.

Можно использовать представление стойки в XClarity Administrator для группировки управляемых устройств, чтобы отразить физические настройки стойки в вашем центре обработки данных. Дополнительные сведения о стойках см. в разделе Управление стойками в документации по XClarity Administrator в Интернете.

Подробнее:

- XClarity Administrator: обнаружение
- XClarity Administrator: инвентарь
- XClarity Administrator: удаленное управление

Мониторинг оборудования

XClarity Administrator обеспечивает централизованное представление всех событий и оповещений, которые создаются из управляемых устройств. Событие или оповещение передается XClarity Administrator и отображается в журнале событий или оповещений. Сводка всех событий и оповещений доступна на информационной панели и в строке состояния. События и оповещения для конкретного устройства доступны на странице сведений «Оповещения и события» для данного устройства.

Дополнительные сведения о мониторинге оборудования см. в разделах Работа с событиями и Работа с оповещениями в документации по XClarity Administrator в Интернете.

Подробнее: XClarity Administrator: мониторинг

Управление конфигурацией

С помощью единообразной конфигурации можно быстро подготовить к работе (включая предварительную подготовку) все ваши серверы. Параметры конфигурации (такие как локальное хранилище, адаптеры ввода-вывода, параметры загрузки, микропрограммы, порты, а также контроллер управления и UEFI) сохраняются в качестве серверного шаблона, который можно применить к одному или нескольким управляемым серверам. При обновлении серверных шаблонов изменения автоматически развертываются на соответствующих серверах.

Шаблоны серверов также включают поддержку виртуализации адресов ввода-вывода, что позволяет виртуализировать межкомпонентные соединения Flex System или изменять назначение серверов, не нарушая работу межкомпонентной сети.

Дополнительные сведения о настройке серверов см. в разделе Настройка серверов с помощью XClarity Administrator в документации по XClarity Administrator в Интернете.

Подробнее:

- XClarity Administrator: от исходного состояния к кластеру
- XClarity Administrator: шаблоны конфигурации

Обеспечение соответствия и обновления микропрограммы

Управление микропрограммами упрощается благодаря назначению управляемым устройствам политик соответствия микропрограмм. При создании и назначении политики соответствия управляемым устройствам XClarity Administrator отслеживает изменения во всех этих устройствам и помечает любые несоответствующие устройства.

Если какое-либо устройство не соответствует требованиям, с помощью программы XClarity Administrator можно применить и активировать обновления микропрограммы для всех устройств соответствующего устройства из управляемого вами репозитория обновлений микропрограмм.

Примечание: Обновление репозитория и загрузка обновлений микропрограмм требует подключения к Интернету. Если у XClarity Administrator нет подключения к Интернету, вы можете вручную импортировать обновления микропрограммы в репозиторий.

Дополнительные сведения об обновлении микропрограммы см. в разделе Обновление микропрограммы на управляемых устройствах в документации по XClarity Administrator в Интернете.

Подробнее:

- XClarity Administrator: от исходного состояния к кластеру
- XClarity Administrator: обновления микропрограммы
- XClarity Administrator: подготовка обновлений безопасности микропрограммы

Развертывание операционной системы

XClarity Administrator можно использовать для управления репозиторием образов операционной системы и параллельного развертывания образов операционной системы на нескольких (до 28) управляемых серверах.

Дополнительные сведения о развертывании операционных систем см. в разделе Развертывание образа операционной системы в документации по XClarity Administrator в Интернете.

Подробнее:

- XClarity Administrator: от исходного состояния к кластеру
- XClarity Administrator: развертывание операционной системы

Управление пользователями

XClarity Administrator предоставляет централизованный сервер аутентификации для создания учетных записей пользователей и для управления учетными данными пользователей и их аутентификации. Сервер аутентификации создается автоматически во время первого запуска сервера управления. Учетные записи пользователей, созданные для XClarity Administrator, можно использовать также для входа в систему управляемой рамы и серверов в режиме управляемой аутентификации. Дополнительные сведения о пользователях см. в разделе Управление учетными записями пользователей в документации по XClarity Administrator в Интернете.

XClarity Administrator поддерживает три типа серверов аутентификации:

- **Локальный сервер аутентификации**. По умолчанию XClarity Administrator настроен для использования локального сервера аутентификации, который находится в узле управления.
- **Внешний сервер LDAP**. В настоящее время поддерживается только Microsoft Active Directory. Этот сервер должен находиться на внешнем сервере Microsoft Windows, подключенном к сети управления.При использовании внешнего сервера LDAP локальный сервер аутентификации отключается.
- **Внешний SAML 2.0поставщик удостоверений**. В настоящее время поддерживается только Microsoft Active Directory Federation Services (AD FS). В дополнение ко вводу имени пользователя и пароля можно настроить многофакторную проверку подлинности, обеспечивающую дополнительную безопасность, так как требуется ввести ПИН-код, считать смарт-карту и предоставить сертификат клиента.

Дополнительные сведения о типах аутентификации см. в разделе Управление сервером аутентификации в документации по XClarity Administrator в Интернете.

При создании учетной записи пользователя ей задается заранее определенная или настраиваемая группа ролей, чтобы управлять уровнем доступа для этого пользователя. Дополнительные сведения о группах ролей см. в разделе Создание группы ролей в документации по XClarity Administrator в Интернете.

XClarity Administrator включает журнал аудита, который содержит записи о действиях пользователей за прошлые периоды, например о входе в систему, создании новых пользователей

и изменении паролей пользователей. Дополнительные сведения о журнале аудита см. в разделе Работа с событиями в документации по XClarity Administrator в Интернете.

Аутентификация устройств

XClarity Administrator использует следующие методы аутентификации управляемых рам и серверов.

- **Управляемая аутентификация**. Когда управляемая аутентификация включена, учетные записи пользователей, созданные в XClarity Administrator, используются для аутентификации управляемых рам и серверов.

  Дополнительные сведения о пользователях см. в разделе Управление учетными записями пользователей в документации по XClarity Administrator в Интернете.

- **Локальная аутентификация**. Когда управляемая аутентификация отключена, сохраненные учетные данные, определенные в XClarity Administrator, используются для аутентификации управляемых серверов. Сохраненные учетные данные должны соответствовать активной учетной записи пользователя на устройстве или в Active Directory.

  Дополнительные сведения о сохраненных учетных данных см. в разделе Управление сохраненными учетными данными в документации по XClarity Administrator в Интернете.

Безопасность

Если рабочая среда должна соответствовать стандарту NIST SP 800-131A, XClarity Administrator поможет создать среду, полностью соответствующую требованиям.

XClarity Administrator поддерживает самозаверяющие сертификаты SSL (которые выпускаются внутренним центром сертификации) и внешние сертификаты SSL (которые выпускаются частным или коммерческим ЦС).

Брандмауэры на рамах и серверах можно настроить так, чтобы они принимали входящие запросы только от XClarity Administrator.

Дополнительные сведения о безопасности см. в разделе Реализация безопасной среды в документации по XClarity Administrator в Интернете.

Обслуживание и поддержка

XClarity Administrator можно настроить для автоматического сбора и отправки диагностических файлов выбранному вами поставщику услуг, когда определенные обслуживаемые события происходят в XClarity Administrator и на управляемых устройствах. Можно отправлять диагностические файлы в Lenovo Поддержка с помощью функции Call Home или другому поставщику услуг с помощью SFTP. Кроме того, можно вручную собрать диагностические файлы, открыть запись неполадки и отправить диагностические файлы в Lenovo Центр поддержки.

Подробнее:  XClarity Administrator: обслуживание и поддержка

Автоматизация задач с помощью сценариев

XClarity Administrator можно интегрировать во внешние платформы управления и автоматизации более высокого уровня, используя открытые интерфейсы API REST. С помощью интерфейсов API REST легко интегрировать XClarity Administrator с существующей инфраструктурой управления.

Набор инструментов PowerShell предоставляет библиотеку командлетов для автоматизации подготовки и управления ресурсами из сеанса Microsoft PowerShell. Набор инструментов Python предоставляет библиотеку команд и API для автоматизации подготовки и управления ресурсами из среды OpenStack, например Ansible или Puppet. Оба эти набора инструментов предоставляют интерфейсам API REST XClarity Administrator интерфейс для автоматизации следующих функций:

- Вход в XClarity Administrator

- Управление и отмена управления рамами, серверами, устройствами хранения и стоечными коммутаторами верхнего уровня (устройства)
- Сбор и просмотр данных инвентаризации для устройств и компонентов
- Развертывание образа операционной системы на один или несколько серверов
- Настройка серверов с помощью шаблонов конфигурации
- Применение обновлений микропрограмм к устройствам

Интеграция с другим управляемым программным обеспечением

Модули XClarity Administrator интегрируют XClarity Administrator с программным обеспечением управления стороннего производителя для поддержки функций обнаружения, мониторинга, настройки и управления, чтобы снизить стоимость и сложность ежедневного администрирования систем на поддерживаемых устройствах.

Дополнительные сведения о XClarity Administrator см. в следующих документах:
- Lenovo XClarity Integrator для Microsoft System Center
- Lenovo XClarity Integrator для VMware vCenter

Дополнительные соображения см. в разделе Замечания по управлению.

Подробнее:
-  Обзор Lenovo XClarity Integrator для Microsoft System Center
-  Lenovo XClarity Integrator для VMware vCenter

Документация

Документация по XClarity Administrator на английском языке регулярно обновляется. Актуальную информацию и описание процедур можно найти на странице: Документация по XClarity Administrator в Интернете.

Ниже перечислены языки, на которых можно найти документацию в Интернете.
- Немецкий (de)
- Английский (en)
- Испанский (es)
- Французский (fr)
- Итальянский (it)
- Японский (ja)
- Корейский (ko)
- Португальский (Бразилия) (pt_BR)
- Русский (ru)
- Тайский (th)
- Упрощенный китайский (zh_CN)
- Традиционный китайский (zh_TW)

Язык документации в Интернете можно изменить одним из следующих способов.

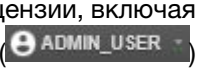
- Измените настройку языка в веб-браузере
- Добавьте `?lang=`*<language_code>* в конце URL-адреса. Например, для отображения документации на упрощенном китайском языке:
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html`**?lang=zh_CN**

Глава 2. Планирование для XClarity Administrator

Перед установкой Lenovo XClarity Administrator ознакомьтесь со следующими рекомендациями, которые помогут спланировать установку и повседневное управление.

Лицензии и бесплатная 90-дневная пробная версия

Lenovo XClarity Administrator предлагает бесплатную пробную лицензию на 90 дней, которая позволяет в полной мере использовать все доступные функции в течение ограниченного времени.

Можно определить статус лицензии, включая сколько дней осталось в пробной лицензии, щелкнув в меню действий пользователя (

) в строке заголовка XClarity Administrator и выбрав **Информация**.

XClarity Administrator поддерживает следующую лицензию.

- **Lenovo XClarity Pro**. Каждая лицензия предоставляет следующие права на одно устройство.
  - Обслуживание и поддержка Lenovo XClarity Integrator
  - Обслуживание и поддержка XClarity Administrator
  - Дополнительные функции в составе XClarity Administrator:
    - Настройка серверов с использованием шаблонов конфигурации
    - Развертывание операционных систем
    - Сообщение о проблемах XClarity Administrator с помощью Call Home (это не повлияет на Call Home для оповещений оборудования)

Необходимо приобрести лицензию для каждого управляемого устройства, которое поддерживает расширенные функции. Лицензия не привязана к определенному устройству.

Соответствие требованиям лицензии определяется с учетом числа управляемых устройств, поддерживающих расширенные функции. Число управляемых устройств не должно превышать общее число лицензий во всех активных лицензионных ключах. Если XClarity Administrator не соответствует установленным лицензиям (например, если срок действия лицензий истек или если из-за управления дополнительными устройствами общее число активных лицензий превышено), у вас есть льготный период 90 дней, чтобы установить соответствующие лицензии. Каждый раз когда XClarity Administrator перестает отвечать требованиям, льготный период сбрасывается до 90 дней. Если льготный период (включая бесплатную пробную версию) завершается до получения соответствующих требованиям лицензий, расширенные функции отключаются для всех устройств.

Примечания:

- По истечении льготного периода функции настройки сервера и развертывания операционной системы будут отключены.
- Если лицензии не соответствуют требованиям, функция Call Home для разрешения проблем XClarity Administrator (функция Call Home для программного обеспечения) отключается. Льготный период для этой функции не предусмотрен. В то же время функция Call Home для оповещений оборудования не затрагивается.

Если лицензии уже установлены, при обновлении до нового выпуска XClarity Administrator новые лицензии *не* требуются.

Для получения сведений о приобретении лицензий Lenovo XClarity Pro обратитесь к представителю Lenovo или авторизованному бизнес-партнеру.

Сведения об установке лицензии см. в Установка лицензии на полнофункциональную активацию в документации по XClarity Administrator в Интернете.

Обязательные требования к оборудованию и программному обеспечению

Управляющее устройство Lenovo XClarity Administrator запускается в виртуальной машине в хост-системе.

Требования к гипервизору

Среды контейнеров

Для запуска XClarity Administrator в качестве контейнера поддерживаются следующие среды.

- Docker 20.10.9
- Docker-compose 1.29.2

Гипервизоры

Для запуска XClarity Administrator в качестве виртуального устройства поддерживаются указанные ниже гипервизоры.

- Гипервизор Citrix 8.2
- Citrix XenServer v7.6
- CentOS 7 и 8[1]
- Microsoft Windows Server 2022 с установленным Hyper-V
- Microsoft Windows Server 2019 с установленным Hyper-V
- Microsoft Windows Server 2016 с установленным Hyper-V
- Microsoft Windows Server 2012 R2 с установленным Hyper-V
- Microsoft Windows Server 2012 с установленным Hyper-V
- Nutanix Acropolis Hypervisor (AHV)
- Red Hat v8.x с установленной виртуальной машиной на основе ядра (KVM) 2.12.0
- Red Hat v7.x с установленной KVM v1.2.17
- Ubuntu 20.04.2 LTS с установленной KVM версии 4.2.3
- VMware ESXi 7.0, U1, U2 и U3
- VMware ESXi 6.7, U1, U2[2] и U3

Примечания:

1. CentOS Linux больше не обновляется компанией Red Hat. Рассмотрите возможность перехода на Red Hat Enterprise Linux (см. раздел Red Hat: как преобразовать разработку в CentOS или Oracle Linux в веб-страницу RHEL).
2. Для VMware ESXi 6.7 U2 необходимо использовать образ ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso или более поздней версии.

Для VMware и Citrix виртуальная машина доступна как шаблон OVF. Для Hyper-V и Nutanix AHV виртуальная машина является образом виртуального диска (VHD). Для CentOS и KVM виртуальная машина доступна в формате qcow2.

Важно: В средах Hyper-V, работающих на Linux-серверах с базой ядра 2.6 и использующих большие объемы памяти для виртуального устройства, необходимо отключить использование неравномерного доступа к памяти (NUMA) на панели параметров Hyper-V из диспетчера Hyper-V. Для изменения этого параметра необходимо перезапустить службу Hyper-V, которая также перезапускает все запущенные виртуальные машины. Если этот параметр не отключен, в процессе первоначальной загрузки виртуального устройства XClarity Administrator может возникнуть неполадка.

Требования к оборудованию

Для XClarity Administrator должны быть выполнены следующие *минимальные требования*. В зависимости от размера вашей среды и использования Шаблоны конфигурации, для обеспечения оптимальной производительности могут потребоваться дополнительные ресурсы.

- Два виртуальных микропроцессора
- 8 ГБ памяти
- 192 ГБ хранилища для использования виртуальным устройством XClarity Administrator.
- Дисплей с минимальным разрешением 1024 пикселей по ширине (XGA)

В следующей таблице перечислены минимальные рекомендуемые конфигурации для указанного количества устройств. Помните, что при запуске минимальной конфигурации выполнение задач управления может занять больше времени, чем ожидалось. Для задач подготовки, таких как развертывание операционной системы, обновления микропрограммы и конфигурация сервера, может потребоваться временно увеличить ресурсы.

Количество управляемых устройств	Конфигурация виртуального ЦП/памяти
От 0 до 100 устройств	2 vCPU, 8 ГБ ОЗУ
От 100 до 200 устройств	4 vCPU, 10 ГБ ОЗУ
От 200 до 400 устройств	6 vCPU, 12 ГБ ОЗУ
От 400 до 600 устройств	8 vCPU, 16 ГБ ОЗУ
От 600 до 800 устройств	10 vCPU, 20 ГБ ОЗУ
От 800 до 1000 устройств	12 vCPU, 24 ГБ ОЗУ

Примечания:

- Один экземпляр XClarity Administrator поддерживает до 1 000 устройств.
- Последние рекомендации и дополнительные замечания по производительности см. в документе XClarity Administrator: руководство по производительности (информационный документ).
- В зависимости от размера управляемой среды и шаблона, используемого в установке, может потребоваться добавить ресурсы для поддержания надлежащей производительности. Если использование процессора на панели мониторинга ресурсов системы часто имеет высокое или очень высокое значение, рассмотрите возможность добавления 1 или 2 ядер виртуального процессора. Если значение использования памяти не опускается ниже 80 % в режиме ожидания, рассмотрите возможность добавления 1 или 2 ГБ ОЗУ. Если система отвечает при конфигурации, представленной в таблице, рассмотрите возможность более длительного выполнения виртуальной машины для оценки производительности системы.
- Сведения о том, как освободить дисковое пространство, удалив ненужные ресурсы XClarity Administrator, см в Управление дисковым пространством в документации по XClarity Administrator в Интернете.

Требования к программному обеспечению

- **Сервер Orchestrator**

  При управлении большим количеством устройств с использованием нескольких экземпляров XClarity Administrator можно централизировать мониторинг, управление, подготовку и аналитику с помощью Lenovo XClarity Orchestrator. XClarity Orchestrator поддерживает неограниченное количество экземпляров XClarity Administrator, которые совместно управляют максимум **10°000** устройствами, не являющимися устройствами ThinkEdge-Client.

  Для управления экземплярами XClarity Administrator версии 4.0 или более поздней версии с использованием Lenovo XClarity Orchestrator требуется XClarity Orchestrator версии не ниже 2.0.

- **Сервер аутентификации**

  Если вы решите использовать внешний сервер аутентификации, поддерживается только Microsoft Active Directory, работающий на Windows Server 2008 или более поздней версии.

  Если вы решите использовать поставщика идентификации SAML, поддерживается Microsoft Active Directory Federation Services (AD FS) только версии 2.0 или более поздней версии, запущенная в Windows Server 2012.

- **Сервер NTP**

  Сервер Network Time Protocol (NTP) необходим для обеспечения того, чтобы отметки времени для всех событий и оповещений, полученных от управляемых устройств, были синхронизированы с XClarity Administrator. Убедитесь, что сервер NTP доступен через сеть управления (обычно это интерфейс Eth0).

  Рекомендация: Рассмотрите возможность использования хост-системы, в которой в качестве сервера NTP устанавливается XClarity Administrator. В этом случае убедитесь, что хост-система доступна через сеть управления.

Управляемые ресурсы

Один экземпляр XClarity Administrator может управлять максимум **1000** физическими устройствами, а также осуществлять их мониторинг и подготовку.

Полный список поддерживаемых устройств и дополнительных компонентов (например, средств ввода-вывода, модулей DIMM и адаптеров хранилища), минимально необходимые уровни микропрограмм и замечания по ограничениям можно найти в Веб-страница поддержки XClarity Administrator — совместимость, открыв вкладку **Совместимость** и щелкнув ссылку для соответствующих типов устройств.

Общие сведения о конфигурации оборудования и аппаратных компонентах для определенного устройства см. в разделе Веб-страница Lenovo Server Proven.

Ограничение. Если хост-система, в которой установлен XClarity Administrator, является управляемым стоечным сервером или вычислительным узлом, XClarity Administrator нельзя использовать для применения обновлений микропрограммы к этой хост-системе или ко всей раме одновременно. Когда к хост-системе применяются обновления микропрограммы, необходимо перезапустить хост-систему. Перезапуск хост-системы также перезапускает XClarity Administrator, что делает XClarity Administrator недоступным для завершения обновлений в хост-системе.

Поддерживаемые веб-браузеры

Веб-интерфейс XClarity Administrator работает в следующих веб-браузерах.
- Chrome™ 48.0 или выше (55.0 или выше для удаленной консоли)
- Firefox® ESR 38.6.0 или выше
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 или выше (IOS 7 или выше и OS X)

Брандмауэры и прокси-серверы

Для некоторых функций Lenovo XClarity Administrator, включая обновления сервера управления, обновления микропрограммы, обслуживание и поддержку, требуется доступ к Интернету. При наличии брандмауэров в сети настройте их таким образом, чтобы разрешить серверу управления XClarity Administrator выполнять эти операции. Если у сервера управления нет прямого доступа к Интернету, настройте XClarity Administrator для использования прокси-сервера.

Брандмауэры

Убедитесь, что в брандмауэре открыты следующие имена DNS и порты.

Примечание: IP-адреса могут быть изменены. По возможности используйте имена DNS.

Табл. 1. Требуемые подключения к Интернету

Имя DNS	Адрес IPv4	Адрес IPv6	Порты	Протоколы
Загрузка ключей активации лицензии				
fod.lenovo.com	Неприменимо	Неприменимо	443	HTTPS
Загрузка бюллетеней технического обслуживания				
download.lenovo.com/servers/LXCA_Bulletin_Service.json	Неприменимо	Неприменимо	443 и 80	HTTPS
Загрузка обновлений (обновлений сервера управления, микропрограмм, пакетов UpdateXpress System Pack (драйверов устройств ОС) и пакетов репозитория)				
datacentersupport.lenovo.com	Неприменимо	Неприменимо	443 и 80	HTTPS
download.lenovo.com	Неприменимо	Неприменимо	443 и 80	HTTPS
filedownload.lenovo.com	Неприменимо	Неприменимо	443 и 80	HTTPS
support.lenovo.com	Неприменимо	Неприменимо	443 и 80	HTTPS и HTTP
supportapi.lenovo.com	Неприменимо	Неприменимо	443 и 80	HTTPS
Загрузка микропрограммы (только Flex System x220, x222, x240, x280 X6, x440, x480 X6, x880 X6, некоторые коммутаторы Flex и CMM первого поколения)				
www.ibm.com	129.42.56.216, 129.42.58.216, 129.42.60.216, 129.42.160.51, 207.25.252.19-7	Неприменимо	443 и 80	HTTPS и HTTP
www-03.ibm.com	204.146.30.17	Неприменимо	443 и 80	HTTPS и HTTP
download3.boulder.ibm.com	170.225.126.2-4	Неприменимо	443	HTTPS
download4.boulder.ibm.com	170.225.126.4-3	Неприменимо	443 и 80	HTTPS и HTTP
delivery04-bld.dhe.ibm.com	170.225.126.4-5	Неприменимо	443 и 80	HTTPS и HTTP
delivery04-mul.dhe.ibm.com	170.225.126.4-6	Неприменимо	443 и 80	HTTPS и HTTP
delivery04.dhe.ibm.com	170.225.126.4-4	Неприменимо	443 и 80	HTTPS и HTTP
Отправка данных по обслуживанию в службу поддержки Lenovo Support (Call Home)				
soaus.lenovo.com	3.222.8.29, 52.6.14.20	Неприменимо	443	HTTPS

Табл. 1. Требуемые подключения к Интернету (продолж.)

Имя DNS	Адрес IPv4	Адрес IPv6	Порты	Протоколы
logupload.lenovo.com/BLL/Logupload.ashx	Неприменимо	Неприменимо	443 и 80	HTTPS
Отправка данных по обслуживанию в средство обновления Lenovo				
logupload.lenovo.com/BLL/Logupload.ashx	Неприменимо	Неприменимо	443 и 80	HTTPS
Загрузка информации о гарантии				
ibase.lenovo.com (во всем мире)	Неприменимо	Неприменимо	443 и 80	HTTPS и HTTP
service.lenovo.com.cn (только для Китая)	114.247.140.2-12 (только для Китая)	Неприменимо	83	HTTP
supportapi.lenovo.com	Неприменимо	Неприменимо	443 и 80	HTTPS и HTTP

Внимание: Для пользователей в Китае необходимо выполнить обновление до XClarity Administrator v1.3.1 или более поздней версии, чтобы получить информацию о гарантии для управляемых устройств с помощью XClarity Administrator.

Прокси-сервер

Если у сервера управления нет прямого доступа к Интернету, проверьте, что сервер управления настроен для использования прокси-сервера HTTP (см. раздел Настройка доступа к сети).
- Убедитесь, что на прокси-сервере настроено использование базовой аутентификации.
- Убедитесь, что прокси-сервер настроен в качестве непрерывающего прокси.
- Убедитесь, что прокси-сервер настроен в качестве прокси переадресации.
- Убедитесь, что балансировщики нагрузки настроены таким образом, чтобы поддерживать сеансы с одним прокси-сервером и не переключаться между ними.

Доступность портов

Должно быть доступно несколько портов в зависимости от реализации брандмауэров в вашей среде. Если требуемые порты заблокированы или используются другим процессом, некоторые функции Lenovo XClarity Administrator могут не работать.

Чтобы выяснить, какие порты должны быть открыты в вашей среде, ознакомьтесь с информацией в следующих разделах. В таблицах этих разделов содержатся сведения об использовании каждого порта в XClarity Administrator, затронутом управляемом устройстве, протоколе (TCP или UDP) и направлении трафика. *Входящий* трафик соответствует потокам от управляемого устройства или внешних систем к XClarity Administrator, поэтому порты необходимо открыть на устройстве XClarity Administrator. Направление *исходящего* трафика — от XClarity Administrator к управляемому устройству.

- Доступ к серверу XClarity Administrator
- Доступ между XClarity Administrator и управляемыми устройствами
- Доступ между XClarity Administrator и сетью передачи данных для развертывания ОС и обновления драйверов устройств ОС

Доступ к серверу XClarity Administrator

Если сервер XClarity Administrator и все управляемые устройства находятся за брандмауэром и вы намерены получить доступ к этим устройствам из браузера, который находится за пределами брандмауэра, вы должны убедиться, что порты XClarity Administrator открыты. Если вы используете SNMP и SMTP для управления событиями, может также быть нужно убедиться, что порты, которые используются сервером XClarity Administrator для перенаправления событий, открыты.

Сервер XClarity Administrator ожидает передачи данных на портах, перечисленных в следующей таблице, и отвечает через них.

Примечания:

- XClarity Administrator — это соответствующее требованиям REST приложение, которое безопасно взаимодействует по протоколу TCP в порту 443.
- XClarity Administrator можно также настроить для создания исходящих подключений к нескольким внешним службам, например LDAP, SMTP и syslog. Для этих подключений могут потребоваться дополнительные порты, которые обычно определяются пользователями и не включены в данный список. Для них также может потребоваться доступ к серверу службы доменных имен (DNS) через TCP- или UDP-порт 53 для разрешения имен внешних серверов.

Связь	Программно-аппаратный комплекс XClarity Administrator	Внешние серверы аутентификации	Службы перенаправления событий	Службы Lenovo (включая Call Home)
Исходящие (порты, открытые во внешних системах)	• DNS — TCP/UDP на порте **53**	• LDAP — TCP на порте **389**[1] • LDAPS — TCP на порте **636** • Аутентификация SAML — TCP на портах **3268, 3269**	• Сервер FTP — TCP на порте **21**[1] • Сервер электронной почты (SMTP) — UDP на порте **25**[1] • Веб-служба REST (HTTP) — UDP на порте **80**[1] • Диспетчер SNMP — UDP на порте **161**[2], **162**[1] • MS Azure — UDP на порте **443**[1] • Syslog — UDP на порте **514**[1] • Push-уведомления Apple[3] — TCP на портах **443, 2195, 5223** • Push-уведомления Google[4] — TCP на портах **443, 5288, 5299, 5230**	• Гарантия (только в Китае) — TCP на порте **83**[5] • HTTPS (Call Home) — TCP на порте **443**
Входящие (порты, открытые на устройстве XClarity Administrator)	• HTTPS — TCP на порте **443**	Неприменимо	• SNMP — UDP на порте **161**	Неприменимо

1. Это порт по умолчанию. Его можно настроить в пользовательском интерфейсе.
2. Этот порт используется при настройке перенаправления событий SNMP с аутентификацией пользователей.
3. Откройте этот порт, если сеть Wi-Fi находится за брандмауэром или частной точкой доступа (APN) для передачи данных по сотовой сети. На этом порте требуется прямое соединение с серверами APN без прокси. Этот порт используется для обратного переключения только на Wi-Fi, когда устройства не могут связаться со службой push-уведомлений Apple через порт 5223. Диапазон IP-адресов — 17.0.0.0/8.
4. Сведения о диапазоне IP-адресов см. в разделе Google ASN 15169. Домен — android.googleapis.com.
5. Хотя это не требуется за пределами Китая, XClarity Administrator может попытаться подключиться к этой службе в других странах.

Доступ между XClarity Administrator и управляемыми устройствами

Если управляемые устройства (такие как вычислительные узлы или стоечные серверы) находятся за брандмауэром, и если вы намерены управлять этими устройствами с сервера XClarity Administrator, который находится вне брандмауэра, необходимо убедиться, что все порты, занимающиеся обеспечением связи между XClarity Administrator и контроллером управления материнской платой в каждом управляемом устройстве открыты.

Если предполагается устанавливать операционные системы на управляемых устройствах с помощью XClarity Administrator, обязательно проверьте список портов в разделе Доступ между XClarity Administrator и сетью передачи данных для развертывания ОС и обновления драйверов устройств ОС.

- **CMM рамы Flex**

Связь	Модули CMM рамы Flex
Исходящая (порты, открытые во внешних системах)	– SLP — UDP/TCP на порте **427** – CIM HTTP — TCP на порте **5988**[2] – CIM HTTPS — TCP на порте **5989** – Команда TCP — TCP на порте **6090**[2] – Защищенная команда TCP — TCP на порте **6091**
Входящие (порты, открытые на устройстве XClarity Administrator)	– SFTP — TCP на порте **22**[1] – HTTPS для индикации CIM — TCP **9090** – LDAPS — TCP на порте **50637**

1. Этот порт служит для передачи обновлений микропрограмм с помощью SFTP.
2. По умолчанию управление осуществляется с использованием защищенных портов. Использовать незащищенные порты необязательно.

- **Серверы и вычислительные узлы**

Связь	ThinkSystem и ThinkAgile	System x	Flex System	ThinkServer
Исходящая (порты, открытые во внешних системах)	– SFTP — TCP на порте **115** – SLP — UDP/TCP на порте **427** – HTTPS — TCP на порте **443** – Обнаружение SSDP — UDP на порте **1900** – Удаленное управление — TCP на порте **3888**[4] – Удаленная консоль KVM — TCP на порте **3889**[4] – CIM HTTPS — TCP на порте **5989** – Обновления микропрограмм — TCP на порте **6990**[5]	– SLP — UDP/TCP на порте **427** – HTTPS — TCP на порте **443** – IPMI — TCP на порте **623** – Удаленное управление — TCP на порте **3888**[4] – Удаленная консоль KVM — TCP на порте **3889**[4] – CIM HTTP — TCP на порте **5988**[3] – CIM HTTPS — TCP на порте **5989**[3] – Обновления микропрограмм — TCP на порте **6990**[5]	– SLP — UDP/TCP на порте **427** – Удаленное управление — TCP на порте **3888**[4] – Удаленная консоль KVM — TCP на порте **3889**[1, 4] – CIM HTTP — TCP на порте **5988**[3] – CIM HTTPS — TCP на порте **5989**[3] – Обновления микропрограмм — TCP на порте **6990**[5]	– Ловушки SNMP — UDP на порте **162** – IPMI — UDP на порте **623**
Входящие (порты, открытые на устройстве XClarity Administrator)	– SFTP — TCP на порте **22**[2] – HTTPS — TCP на порте **443** – Обнаружение SSDP — UDP на порте **1900** – Обновления микропрограмм — TCP на порте **6990**[5] – HTTPS для индикации CIM — TCP **9090** – LDAPS — TCP на портах **50636**[6] **и 50637**	– SFTP — TCP на порте **22**[2] – HTTPS — TCP на порте **443** – Обновления микропрограмм — TCP на порте **6990**[5] – HTTPS для индикации CIM — TCP **9090** – LDAPS — TCP на портах **50636**[6] **и 50637**	– SFTP — TCP на порте **22**[2] – HTTPS — TCP на порте **443** – Обновления микропрограмм — TCP на порте **6990**[5] – HTTPS для индикации CIM — TCP **9090** – LDAPS — TCP на портах **50636**[6] **и 50637**	– Ловушки SNMP — UDP на порте **162**

1. Этот порт должен быть открыт только для серверов с IMM2.
2. Этот порт служит для передачи обновлений микропрограмм с помощью SFTP.
3. По умолчанию управление осуществляется с использованием защищенных портов. Использовать незащищенные порты необязательно.
4. Удаленное управление и удаленная консоль KVM запускаются из веб-браузера, а не с сервера XClarity Administrator.
5. Этот порт служит для подключения к ОС BMU для передачи файлов и выполнения команд обновления.
6. Этот порт необходим для настройки серверов с использованием шаблонов конфигурации.

- **Стоечные коммутаторы и коммутаторы Flex**

Связь	Стоечные коммутаторы	Коммутаторы Flex
Исходящая (порты, открытые во внешних системах)	– SSH — TCP на порте **22**[1,3] – SNMP — UDP на порте **161**[2] – SLP — UDP/TCP на порте **427**[6] – HTTPS — TCP на порте **443**[7]	– SSH — TCP на порте **22**[3] – SNMP — UDP на порте **161**[5]
Входящие (порты, открытые на устройстве XClarity Administrator)	– SFTP — TCP на порте **22**[4] – Ловушки SNMP — TCP на портах **162**[2]	– SFTP — TCP на порте **22**[4] – Ловушки SNMP — TCP на порте **162**[2]

1. В стоечных коммутаторах ENOS этот порт используется для настройки учетных данных HoS, используемых в коммуникации между CMM и коммутаторами Flex, активации гнезда микропрограммы и очистки ключей хостов SSH перед операциями передачи файлов по протоколу SFTP.
2. Этот порт должен быть открыт на устройстве XClarity Administrator (для входящего трафика), если коммутаторы расположены в сети, отличной от сети, где находится XClarity Administrator, чтобы продукт XClarity Administrator мог получать события для этих устройств.
3. Этот порт используется для управления (SSH).
4. Этот порт служит для передачи обновлений микропрограмм с помощью SFTP.
5. В стоечных коммутаторах ENOS этот порт используется для передачи данных инвентаризации.
6. Этот порт используется для обнаружения.
7. Этот порт служит для применения обновлений микропрограмм.

- **Устройства хранения данных**

Связь	Устройства хранения данных
Исходящая (порты, открытые во внешних системах)	– FTP — TCP на порте **21** – SFTP — TCP на порте **22**[2] – SLP — UDP/TCP на порте **427** – HTTPS — TCP на порте **443**[1]
Входящие (порты, открытые на устройстве XClarity Administrator)	– HTTPS — TCP на порте **443**[2] – Ловушки SNMP — UDP на порте **115**

1. Этот порт служит для передачи обновлений микропрограмм.
2. Этот порт служит для передачи и применения обновлений микропрограмм.

Доступ между XClarity Administrator и сетью передачи данных для развертывания ОС и обновления драйверов устройств ОС

Связь	Развертывание ОС[1, 2, 3]	Обновления драйверов устройств ОС[2]
Исходящая (порты, открытые во внешних системах)		• WinRM через HTTP — TCP на порте **5985**[5] • WinRM через HTTPS — TCP на порте **5986**[6]
Входящие (порты, открытые на устройстве XClarity Administrator)	• Связь по протоколу SMB — TCP на портах **445**[4] • HTTPS (кроме ThinkServer) — TCP на порте **8443**[6]	• Связь по протоколу SMB — TCP на портах **445**[4]

1. Если вы настроили XClarity Administrator для использования сети развертывания операционных систем, в этой сети должны быть открыты порты.
2. Список портов, которые должны быть доступны для развертывания операционных систем, см. в разделе Наличие портов для развернутых операционных систем в документации по XClarity Administrator в Интернете. Например, если развертывание операционной системы настроено для использования сети данных (eth1), в этой сети должны быть открыты эти порты.
3. Каждый экземпляр XClarity Administrator имеет уникальный центр сертификации (ЦС), который используется только для развертывания ОС. Этот ЦС подписывает сертификат, используемый для целевого сервера на порте 8443. При запуске процесса развертывания ОС сертификат ЦС включается в образ ОС, который отправляется на целевой сервер. В ходе процесса развертывания этот сервер снова подключается к порту 8443 и проверяет сертификат, который порт 8443 предоставляет во время установления соединения, поскольку он имеет сертификат ЦС.
4. Этот порт служит для передачи файлов драйверов Windows.
5. Этот порт служит для подключения к целевому серверу WinRM.
6. Этот порт используется для обмена данными между целевой ОС и XClarity Administrator, включая образы ОС и статус.

Замечания по управлению

Существует несколько вариантов для выбора при управлении устройствами. В зависимости от управляемых устройств вам может потребоваться одновременно использовать нескольких решений управления.

Устройство может управляться только одним экземпляром Lenovo XClarity Administrator. Однако можно использовать другое программное обеспечение управления (например, VMware vRealize Operations Manager) в сочетании с Lenovo XClarity Administrator для *мониторинга* устройств, которыми управляет XClarity Administrator.

Внимание: Необходимо проявлять особую осторожность при использовании нескольких инструментов управления для управления вашими устройствами в целях предотвращения непредвиденных конфликтов. Например, передача изменений состояния питания с использованием другого инструмента может конфликтовать с заданиями конфигурации или обновления, запущенными в XClarity Administrator.

Устройства ThinkSystem, ThinkServer и System x

Если для мониторинга управляемых устройств предполагается использовать другое программное обеспечение управления, создайте через интерфейс IMM нового локального пользователя с соответствующими параметрами SNMP и IPMI. Убедитесь, что вы предоставляете полномочия SNMP и IPMI, в зависимости от ваших потребностей.

Устройства Flex System

Если предполагается использовать другое программное обеспечение управления для мониторинга ваших управляемых устройств, и если это программное обеспечение управления использует SNMPv3 или связь IPMI, необходимо подготовить вашу среду, выполнив следующие действия для каждого управляемого CMM:

1. Войдите в веб-интерфейс контроллера управления для рамы, используя имя пользователя и пароль `RECOVERY_ID`.
2. Если политика безопасности имеет значение **Secure**, измените метод аутентификации пользователя.
   a. Нажмите **Mgt Module Management → Учетные записи пользователей**.
   b. Перейдите на вкладку **Учетные записи**.
   c. Нажмите **Параметры глобального входа**.
   d. Перейдите на вкладку **Общие**.
   e. Сначала выберите **внешняя, затем локальная аутентификация** для метода аутентификации пользователя.
   f. Нажмите **OK**.
3. Создайте нового локального пользователя с правильными параметрами SNMP и IPMI через веб-интерфейс контроллера управления.
4. Если политика безопасности имеет значение **Secure**, выйдите из системы, а затем войдите в веб-интерфейс контроллера управления, используя новое имя пользователя и пароль. При появлении запроса измените пароль для нового пользователя.

Теперь можно использовать нового пользователя в качестве активного пользователя SNMP или IPMI.

Примечание: Если вы отменяете управление, а затем вновь управляете рамой, эта новая учетная запись пользователя блокируется и отключается. В этом случае повторите эти шаги для создания новой учетной записи пользователя.

Замечания по сети

При планировании установки Lenovo XClarity Administrator примите во внимание топологию сети, которая реализована в вашей среде, и каким образом XClarity Administrator вписывается в эту топологию.

Важно: Настройте устройства и компоненты таким образом, чтобы свести к минимуму изменения IP-адресов. Рассмотрите возможность использования статических IP-адресов вместо протокола динамической настройки хостов (DHCP). Если используется протокол DHCP, убедитесь, что изменения IP-адреса сведены к минимуму.

Ограничения конфигурации IP

Для указанных ниже функций и управляемых устройств необходимо настроить для сетевых интерфейсов адреса IPv4. Адреса IPv6 не поддерживаются.

- Обновления микропрограммы для устройств Lenovo Storage
- Серверы ThinkServer
- Устройства Lenovo Storage

Управление устройствами RackSwitch с использованием локального адреса канала IPv6 через порт передачи данных или порт управления не поддерживается.

Трансляция сетевых адресов (NAT), которая перераспределяет одно пространство IP-адресов в другое, не поддерживается.

Типы сетей

В целом большинство сред реализует следующие типы сетей. В зависимости от ваших требований, можно реализовать только одну из этих сетей или все три.

- **Сеть управления**

  Сеть управления обычно используется только для связи между Lenovo XClarity Administratorи процессорами управления для управляемых устройств. Например, сеть управления может быть настроена так, чтобы включать XClarity Administrator, CMM для каждой управляемой рамы и контроллер управления материнской платой каждого сервера, которым управляет XClarity Administrator.

- **Сеть данных**

  Сеть данных обычно используется для связи между операционными системами, которые установлены на серверах и в корпоративной интрасети, Интернете или и там, и там.

- **Сеть развертывания операционной системы**

  В некоторых случаях сеть развертывания операционной системы настраивается для разделения сообщений, которые требуются для развертывания операционных систем на серверах. Если она реализована, эта сеть обычно включает XClarity Administrator и все хосты серверов.

  Вместо реализации отдельной сети развертывания операционной системы можно включить эту функциональность в сеть управления или сеть данных.

Конфигурации сети

Lenovo XClarity Administrator можно настроить для использования одного или двух сетевых интерфейсов.

Внимание:

- При изменении IP-адреса XClarity Administrator после управления устройствами устройства могут перейти в XClarity Administrator в состояние «не в сети». Перед изменением IP-адреса убедитесь, что все устройства являются неуправляемыми.
- Можно включить или отключить проверку дублированных IP-адресов в одной подсети, нажав переключатель **Проверка дублированных IP-адресов**. По умолчанию эта проверка отключена. Если такая проверка включена, при попытке изменить IP-адрес XClarity Administrator или управлять устройством, IP-адрес которого совпадает с IP-адресом другого устройства, находящегося под управлением, или при обнаружении другого устройства в той же подсети программное обеспечение XClarity Administrator создает оповещение.

  Примечание: Если она включена, XClarity Administrator выполняется сканирование ARP, чтобы найти активные устройства IPv4 в той же подсети. Чтобы не допустить сканирования ARP, отключите параметр **Проверка дублированных IP-адресов**.
- При запуске XClarity Administrator в качестве виртуального устройства IP-адрес интерфейса управления может измениться при истечении срока аренды DHCP, если сетевой интерфейс для сети управления настроен на использование протокола DHCP. Если IP-адрес меняется, необходимо отключить управление рамой, стоечными и башенными серверами, а затем снова включить управление ими. Чтобы избежать этой неполадки, измените интерфейс управления на статический IP-адрес или убедитесь, что конфигурация DHCP-сервера установлена так, что адрес DHCP основан на MAC-адресе или что срок аренды DHCP не истекает.

- Если применять XClarity Administrator для развертывания операционной системы и обновления драйверов устройств ОС *не* планируется, можно отключить серверы Samba и Apache, изменив сетевой интерфейс, чтобы использовать параметр **Только обнаружение и управление оборудованием**. Следует иметь в виду, что после изменения сетевого интерфейса сервер управления перезапускается.
- При запуске XClarity Administrator в качестве контейнера.
  - Можно только включить или выключить проверку дублирующихся IP-адресов, изменить роли сетевых интерфейсов и изменить параметры прокси-сервера. Все остальные параметры сети (включая IP-адрес, шлюз и DNS) переопределяются при настройке контейнера.
  - Убедитесь, что сеть macvlan настроена в хост-системе.

XClarity Administrator имеет два отдельных сетевых интерфейса, которые могут быть определены для вашей среды, в зависимости от используемой топологии сети. Для виртуальных устройств эти сети называются eth0 и eth1. Для контейнеров можно выбирать пользовательские имена.

- Присутствует только один сетевой интерфейс (eth0):
  - Этот интерфейс должен быть настроен для поддержки обнаружения устройства и управления им (например, конфигурация сервера и обновления микропрограммы). Он должен иметь возможность связываться с CMM и коммутаторами Flex в каждой управляемой раме, контроллером управления материнской платой в каждом управляемом сервере, и с каждым коммутатором RackSwitch.
  - Если предполагается получать обновления микропрограммы и драйверов устройств ОС с помощью XClarity Administrator, по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр. В противном случае обновления необходимо импортировать в репозиторий.
  - Если предполагается осуществлять сбор данных по обслуживанию или использовать автоматическое уведомление о неполадках (включая Call Home и средство загрузки Lenovo), по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр.
  - Если вы собираетесь развертывать образы операционной системы и обновлять драйверы устройств ОС, интерфейс должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к основной операционной системе.

    Примечание: Если для развертывания операционных систем и обновлений драйверов устройств ОС создана отдельная сеть, можно настроить второй сетевой интерфейс для подключения к этой сети, а не к сети данных. Однако, если операционная система на каждом сервере не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между операционной системой хоста и сетью данных.
- Присутствуют два сетевых интерфейса (eth0 и eth1):
  - Первый сетевой интерфейс (обычно интерфейс Eth0) необходимо подключить к сети управления и настроить для поддержки обнаружения устройств и управления ими (включая конфигурацию сервера и обновления микропрограммы). Он должен иметь возможность связываться с CMM и коммутаторами Flex в каждой управляемой раме, контроллером управления в каждом управляемом сервере, и с каждым коммутатором RackSwitch.
  - Второй сетевой интерфейс (обычно eth1) можно настроить для связи с внутренней сетью данных, сетью данных общего пользования или с обеими сетями.
  - Если предполагается получать обновления микропрограммы и драйверов устройств ОС с помощью XClarity Administrator, по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр. В противном случае обновления необходимо импортировать в репозиторий.

– Если предполагается осуществлять сбор данных по обслуживанию или использовать автоматическое уведомление о неполадках (включая Call Home и средство загрузки Lenovo), по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр.
– Если вы планируете развертывать образы операционной системы и обновлять драйверы устройств, можно использовать интерфейс eth1 или eth0. Однако используемый интерфейс должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к операционной системе хоста.

  Примечание: Если для развертывания операционных систем и обновлений драйверов устройств ОС создана отдельная сеть, можно настроить второй сетевой интерфейс для подключения к этой сети, а не к сети данных. Однако, если операционная система на каждом сервере не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между операционной системой хоста и сетью данных.

В следующей таблице показаны возможные конфигурации для сетевых интерфейсов XClarity Administrator в зависимости от типа топологии сети, реализованной в вашей среде. Используйте эту таблицу для выяснения способа определения каждого сетевого интерфейса.

Табл. 2. Назначение каждого сетевого интерфейса зависит от топологии сети

Топология сети	**Назначение интерфейса 1 (eth0)**	**Назначение интерфейса 2 (eth1)**
Конвергентная сеть (сеть данных и управления с поддержкой развертывания ОС и обновлений драйверов устройств ОС)	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии • Развертывание ОС • Обновления драйверов устройств ОС	Нет
Отдельные сеть управления с поддержкой развертывания ОС и обновлений драйверов устройств ОС и сеть данных	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии • Развертывание ОС • Обновления драйверов устройств ОС	Сеть данных • Нет

Табл. 2. Назначение каждого сетевого интерфейса зависит от топологии сети (продолж.)

Топология сети	**Назначение интерфейса 1 (eth0)**	**Назначение интерфейса 2 (eth1)**
Отдельные сеть управления и сеть данных с поддержкой развертывания ОС и обновлений драйверов устройств ОС	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии	Сеть данных • Развертывание ОС • Обновления драйверов устройств ОС
Отдельные сеть управления и сеть данных без поддержки развертывания ОС и обновлений драйверов устройств ОС	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии	Сеть данных • Нет
Только сеть управления (развертывание ОС и обновления драйверов устройств ОС не поддерживаются)	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии	Нет

Единая сеть данных и управления

В этой топологии сети управление связью, обмен данными и развертывание операционной системы происходит в одной сети. Эта топология называется *конвергированной* сетью.

Важно: Реализация общей сети данных и управления может привести к сбоям трафика, например выпадению пакетов или неполадкам подключения сети управления, в зависимости от конфигурации вашей сети (например, если трафик от серверов имеет высокий приоритет, а трафик от контроллеров управления имеет низкий приоритет). Сеть управления использует UDP-трафик в дополнение к TCP. UDP-трафик может иметь более низкий приоритет при высоком сетевом трафике.

При установке Lenovo XClarity Administrator определите сетевой интерфейс eth0 с учетом следующих соображений.

- Этот интерфейс должен быть настроен для поддержки обнаружения устройства и управления им (например, конфигурация сервера и обновления микропрограммы). Он должен иметь возможность связываться с CMM и коммутаторами Flex в каждой управляемой раме, контроллером управления материнской платой в каждом управляемом сервере, и с каждым коммутатором RackSwitch.
- Если предполагается получать обновления микропрограммы и драйверов устройств ОС с помощью XClarity Administrator, по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр. В противном случае обновления необходимо импортировать в репозиторий.

- Если предполагается осуществлять сбор данных по обслуживанию или использовать автоматическое уведомление о неполадках (включая Call Home и средство загрузки Lenovo), по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр.
- Если вы собираетесь развертывать образы операционной системы и обновлять драйверы устройств ОС, интерфейс должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к основной операционной системе.

  Примечание: Если для развертывания операционных систем и обновлений драйверов устройств ОС создана отдельная сеть, можно настроить второй сетевой интерфейс для подключения к этой сети, а не к сети данных. Однако, если операционная система на каждом сервере не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между операционной системой хоста и сетью данных.
- Можно настроить XClarity Administrator в любой системе, которая отвечает требованиям для XClarity Administrator, включая управляемый сервер, только при реализации топологии с единой сетью данных и управления или виртуально разделенной сети данных и управления; однако нельзя использовать XClarity Administrator для применения обновлений микропрограммы на управляемом сервере. Даже в этом случае только часть микропрограммы применяется с немедленной активацией, и XClarity Administrator принудительно перезапускает целевой сервер, что приводит к перезапуску и XClarity Administrator. Если используется отложенная активация, при перезапуске XClarity Administrator применяются только некоторые части микропрограммы.

Также можно настроить второй сетевой интерфейс для подключения к той же сети из XClarity Administrator для резервирования.

На следующем рисунке показан пример реализации конвергентной топологии сети.

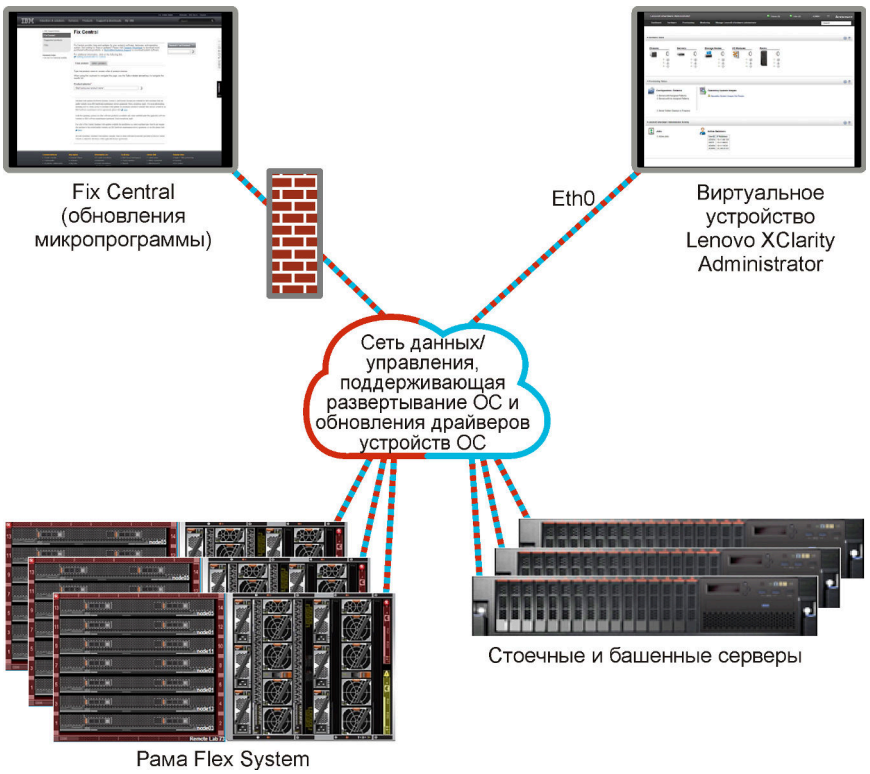


Рис. 1. Пример реализации единой сети для управления, данных и развертывания операционной системы

Физическое разделение сети данных и управления

В этой топологии сети сеть управления и сеть данных являются физически раздельными сетями, а сеть развертывания операционной системы настраивается либо как часть сети управления, либо как часть сети данных.

При установке Lenovo XClarity Administrator определите параметры сети с учетом следующих соображений:

- Первый сетевой интерфейс (обычно интерфейс Eth0) необходимо подключить к сети управления и настроить для поддержки обнаружения устройств и управления ими (включая конфигурацию сервера и обновления микропрограммы). Он должен иметь возможность связываться с CMM и коммутаторами Flex в каждой управляемой раме, контроллером управления в каждом управляемом сервере, и с каждым коммутатором RackSwitch.
- Второй сетевой интерфейс (обычно eth1) можно настроить для связи с внутренней сетью данных, сетью данных общего пользования или с обеими сетями.
- Если предполагается получать обновления микропрограммы и драйверов устройств ОС с помощью XClarity Administrator, по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр. В противном случае обновления необходимо импортировать в репозиторий.
- Если предполагается осуществлять сбор данных по обслуживанию или использовать автоматическое уведомление о неполадках (включая Call Home и средство загрузки Lenovo), по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр.
- Если вы планируете развертывать образы операционной системы и обновлять драйверы устройств, можно использовать интерфейс eth1 или eth0. Однако используемый интерфейс должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к операционной системе хоста.

  Примечание: Если для развертывания операционных систем и обновлений драйверов устройств ОС создана отдельная сеть, можно настроить второй сетевой интерфейс для подключения к этой сети, а не к сети данных. Однако, если операционная система на каждом сервере не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между операционной системой хоста и сетью данных.

Рис. 2 «Пример реализации физически разделенных сетей данных и управления, где сеть операционной системы является частью сети данных» на странице 26 отображает пример реализации раздельных сетей управления и данных, в которых сеть развертывания операционной системы настроена как часть сети передачи данных.

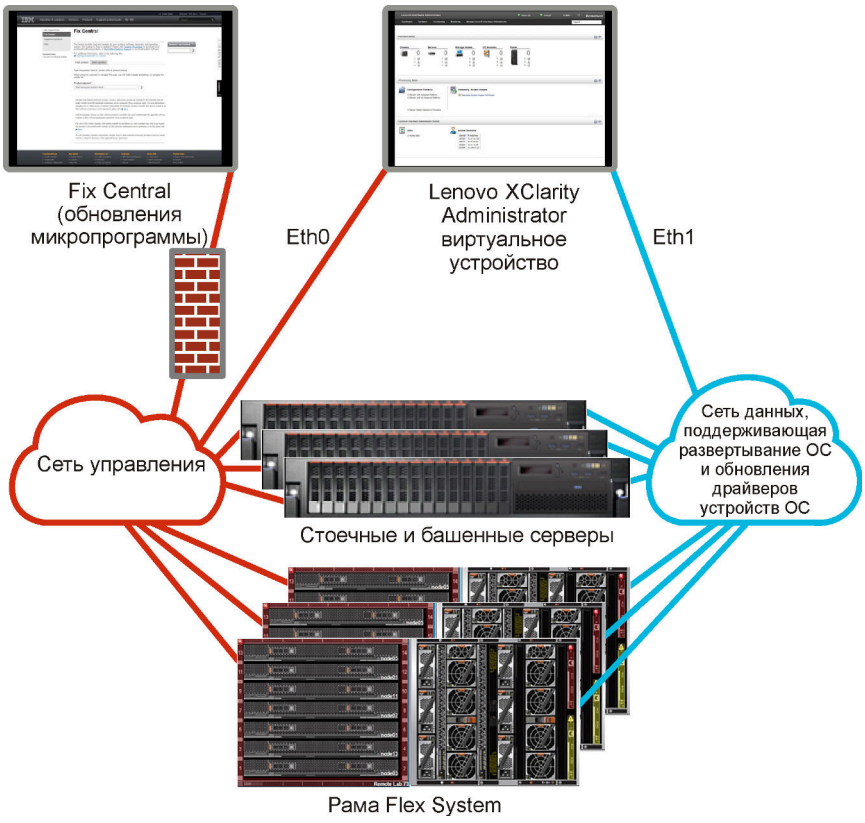


Рис. 2. Пример реализации физически разделенных сетей данных и управления, где сеть операционной системы является частью сети данных

Рис. 3 «Пример реализации физически разделенных сетей данных и управления, где сеть операционной системы является частью сети управления» на странице 27 отображает другой пример реализации раздельных сетей управления и данных, в которых сеть развертывания операционной системы настроена как часть сети управления. В этой реализации XClarity Administrator не требуется подключение к сети данных.

Примечание: Если сеть развертывания операционной системы не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между основной системой сервера и сетью данных.

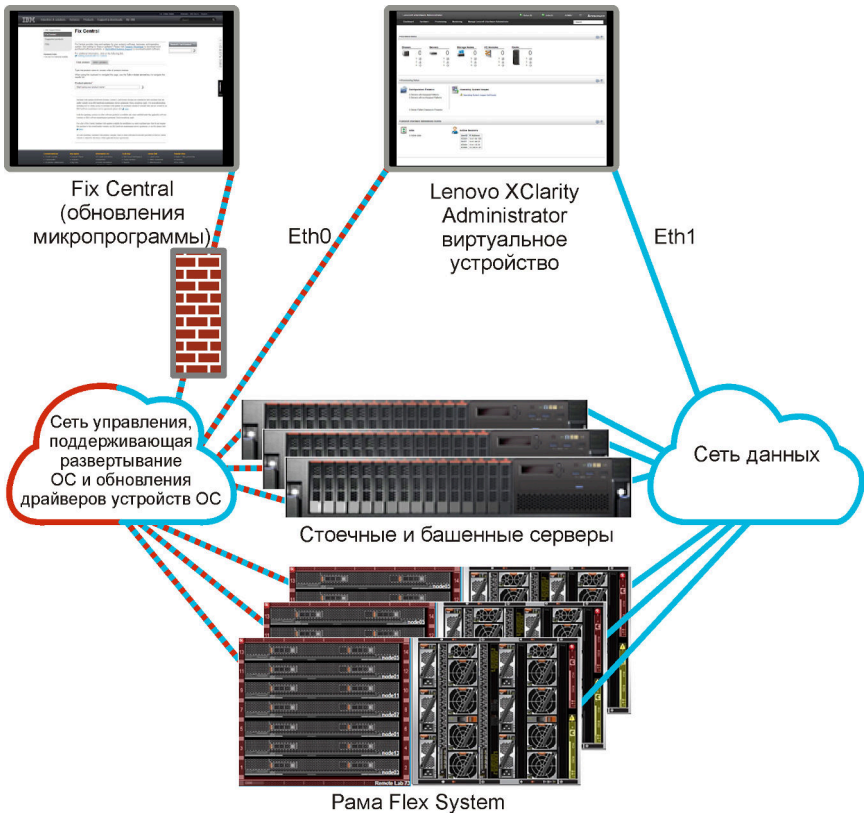


Рис. 3. Пример реализации физически разделенных сетей данных и управления, где сеть операционной системы является частью сети управления

Виртуальное разделение сети данных и управления

В этой топологии сеть передачи данных и сеть управления виртуально разделены. Пакеты из сети передачи данных и пакеты из сети управления отправляются через одно физическое подключение. Для разделения трафика двух сетей во всех пакетах данных сети управления используется добавление меток виртуальной локальной сети.

Примечание: Если Lenovo XClarity Administrator установлен на хост, работающий на управляемом сервере в раме, нельзя использовать XClarity Administrator для применения обновления микропрограммы во всей раме одновременно. При применении обновления микропрограммы необходимо перезапустить хост-систему.

При установке XClarity Administrator определите параметры сети с учетом следующих соображений:

- Первый сетевой интерфейс (обычно интерфейс Eth0) необходимо подключить к сети управления и настроить для поддержки обнаружения устройств и управления ими (включая конфигурацию сервера и обновления микропрограммы). Он должен иметь возможность связываться с CMM и коммутаторами Flex в каждой управляемой раме, контроллером управления в каждом управляемом сервере, и с каждым коммутатором RackSwitch.
- Второй сетевой интерфейс (обычно eth1) можно настроить для связи с внутренней сетью данных, сетью данных общего пользования или с обеими сетями.
- Если предполагается получать обновления микропрограммы и драйверов устройств ОС с помощью XClarity Administrator, по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр. В противном случае обновления необходимо импортировать в репозиторий.

- Если предполагается осуществлять сбор данных по обслуживанию или использовать автоматическое уведомление о неполадках (включая Call Home и средство загрузки Lenovo), по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр.
- Если вы планируете развертывать образы операционной системы и обновлять драйверы устройств, можно использовать интерфейс eth1 или eth0. Однако используемый интерфейс должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к операционной системе хоста.

  Примечание: Если для развертывания операционных систем и обновлений драйверов устройств ОС создана отдельная сеть, можно настроить второй сетевой интерфейс для подключения к этой сети, а не к сети данных. Однако, если операционная система на каждом сервере не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между операционной системой хоста и сетью данных.
- Можно настроить XClarity Administrator в любой системе, которая отвечает требованиям для XClarity Administrator, включая управляемый сервер, только при реализации топологии с единой сетью данных и управления или виртуально разделенной сети данных и управления; однако нельзя использовать XClarity Administrator для применения обновлений микропрограммы на управляемом сервере. Даже в этом случае только часть микропрограммы применяется с немедленной активацией, и XClarity Administrator принудительно перезапускает целевой сервер, что приводит к перезапуску и XClarity Administrator. Если используется отложенная активация, при перезапуске XClarity Administrator применяются только некоторые части микропрограммы.

Рис. 4 «Пример реализации виртуально разделенных сетей данных и управления, где сеть операционной системы является частью сети данных» на странице 29 отображает пример реализации виртуально раздельных сетей управления и данных, в которых сеть развертывания операционной системы настроена как часть сети данных. В этом примере XClarity Administrator установлен на управляемом сервере в раме.

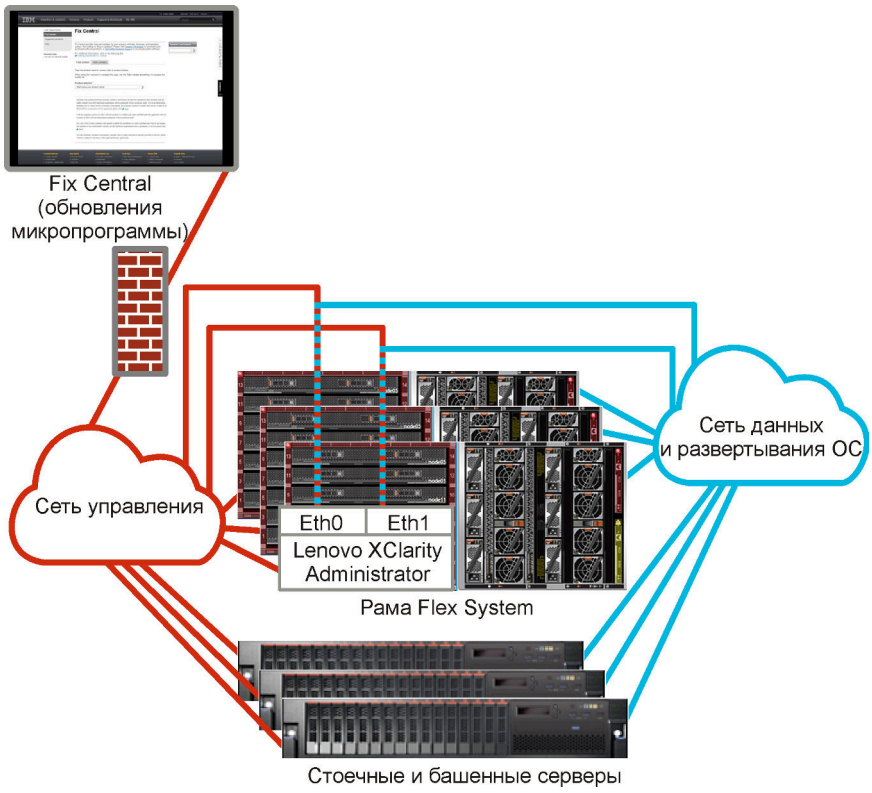


Рис. 4. Пример реализации виртуально разделенных сетей данных и управления, где сеть операционной системы является частью сети данных

Рис. 5 «Пример реализации виртуально разделенных сетей данных и управления, где сеть операционной системы является частью сети управления» на странице 30 отображает другой пример реализации виртуально раздельных сетей управления и данных, в которых сеть развертывания операционной системы настроена как часть сети управления, а XClarity Administrator установлен на управляемом сервере в раме. В этой реализации XClarity Administrator не требуется подключение к сети данных.

Примечание: Если сеть развертывания операционной системы не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между основной системой сервера и сетью данных.

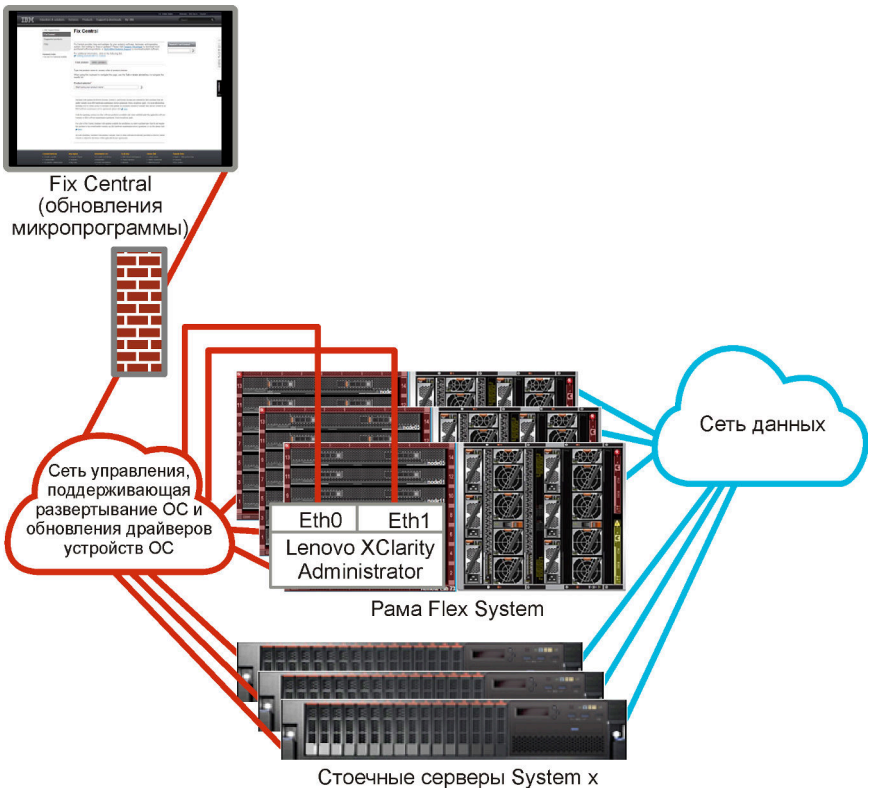


Рис. 5. Пример реализации виртуально разделенных сетей данных и управления, где сеть операционной системы является частью сети управления

Сеть только для управления

В этой топологии у Lenovo XClarity Administrator имеется доступ только к сети управления. Он не имеет доступа к сети данных. Однако XClarity Administrator должен иметь доступ к сети развертывания операционной системы, если планируется развертывание образов операционной системы с XClarity Administrator на управляемые серверы.

При установке XClarity Administrator и определении сетевых параметров сетевой интерфейс eth0 необходимо настроить для выполнения следующих функций.

- Этот интерфейс должен быть настроен для поддержки обнаружения устройства и управления им (например, конфигурация сервера и обновления микропрограммы). Он должен иметь возможность связываться с CMM и коммутаторами Flex в каждой управляемой раме, контроллером управления материнской платой в каждом управляемом сервере, и с каждым коммутатором RackSwitch.
- Если предполагается получать обновления микропрограммы и драйверов устройств ОС с помощью XClarity Administrator, по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр. В противном случае обновления необходимо импортировать в репозиторий.
- Если предполагается осуществлять сбор данных по обслуживанию или использовать автоматическое уведомление о неполадках (включая Call Home и средство загрузки Lenovo), по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр.
- Если вы собираетесь развертывать образы операционной системы и обновлять драйверы устройств ОС, интерфейс должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к основной операционной системе.

Примечание: Если для развертывания операционных систем и обновлений драйверов устройств ОС создана отдельная сеть, можно настроить второй сетевой интерфейс для подключения к этой сети, а не к сети данных. Однако, если операционная система на каждом сервере не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между операционной системой хоста и сетью данных.

Также можно настроить второй сетевой интерфейс для подключения к той же сети из XClarity Administrator для резервирования.

Рис. 6 «Пример реализации сети управления, не поддерживающей развертывание операционной системы» на странице 31 отображает пример реализации сети только для управления, в которой не поддерживается развертывание операционной системы из XClarity Administrator.

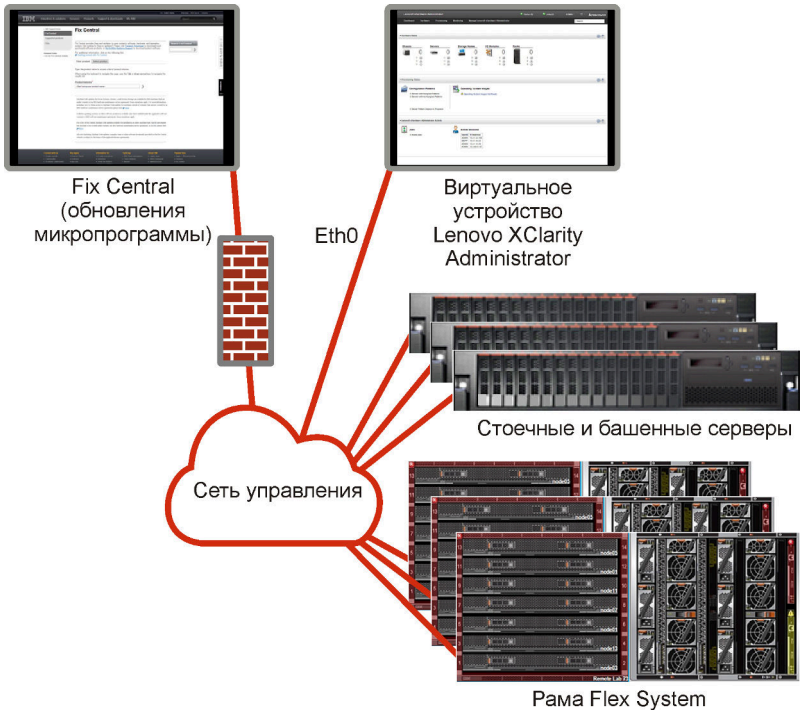


Рис. 6. Пример реализации сети управления, не поддерживающей развертывание операционной системы

Рис. 6 «Пример реализации сети управления, не поддерживающей развертывание операционной системы» на странице 31 отображает пример реализации сети только для управления, в которой поддерживается развертывание операционной системы из XClarity Administrator.

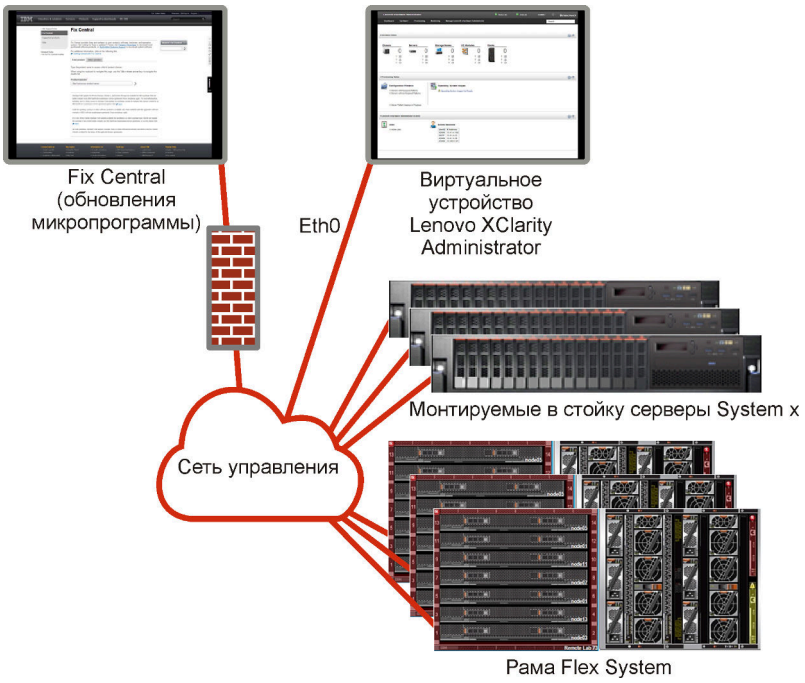


Рис. 7. Пример реализации сети только для управления с поддержкой развертывания операционной системы

Замечания по безопасности

Планируйте обеспечение безопасности Lenovo XClarity Administrator и всех управляемых устройств.

Управление инкапсуляцией

При управлении рамой Lenovo и серверами в Lenovo XClarity Administrator можно настроить Lenovo XClarity Administrator на изменение правил брандмауэра для устройств, чтобы входящие запросы принимались только от Lenovo XClarity Administrator. Это называется *инкапсуляцией*. Можно также включить или отключить инкапсуляцию на раме и серверах, которыми уже управляет Lenovo XClarity Administrator.

Если инкапсуляция включена на поддерживающих ее устройствах, Lenovo XClarity Administrator изменяет режим инкапсуляции устройства на «encapsulationLite» и изменяет правила брандмауэра для этого устройства, чтобы разрешить получение входящих запросов только от этого Lenovo XClarity Administrator.

Если инкапсуляция отключена, включается режим «нормальная». Если инкапсуляция была ранее включена на устройствах, правила брандмауэра для инкапсуляции удаляются.

Внимание: Если инкапсуляция включена и XClarity Administrator становится недоступным до отмены управления устройством, необходимо выполнить ряд действий, чтобы отключить инкапсуляцию для установки связи с устройством. Процедуры восстановления см. в разделах Восстановление управления рамы с CMM после сбоя узла управления и Восстановление управления стоечным или башенным сервером после сбоя сервера управления в документации по XClarity Administrator в Интернете.

Примечания:

- Инкапсуляция не поддерживается для коммутаторов, устройств хранения, рам и серверов других производителей (не Lenovo).

- Когда интерфейс сети управления настроен для использования протокола DHCP и инкапсуляция включена, управление стоечным сервером может занимать много времени.

Дополнительные сведения о инкапсуляции см. в разделе Включение инкапсуляции в документации по XClarity Administrator в Интернете.

Криптографическое управление

Криптографическое управление состоит из режимов обмена данным и протоколов, которые управляют безопасным обменом данными между Lenovo XClarity Administrator и управляемыми устройствами (такими как рамы, серверы и коммутаторы Flex).

Алгоритмы криптографии

XClarity Administrator поддерживает TLS 1.2 и более надежные криптографические алгоритмы для защищенных сетевых подключений.

Для повышения безопасности поддерживаются только шифры высокой стойкости. Клиентские операционные системы и веб-браузеры должны поддерживать один из указанных ниже наборов шифров.
- SSH-ED25519
- SSH-ED25519-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP521
- ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM
- RSA-SHA2-512
- RSA-SHA2-256
- RSA-SHA2-384

Криптографические режимы для сервера управления

Этот параметр определяет режим, который должен использоваться для защищенного обмена данными с сервером управления.

- **Совместимость**. Это режим по умолчанию. Он совместим со старыми версиями микропрограмм, браузерами и другими сетевыми клиентами, в которых не реализованы строгие стандарты безопасности, необходимые для обеспечения соответствия NIST SP 800-131A.
- **NIST SP 800-131A**. Этот режим соответствует стандарту NIST SP 800-131A. XClarity Administrator разработан так, чтобы всегда использовать стойкую криптографию внутри системы и, если это возможно, защищенные стойкой криптографией сетевые подключения. Однако в этом режиме не допускаются сетевые подключения, использующие криптографию, не одобренную NIST SP 800-131A, включая отклонение сертификатов TLS, подписанных SHA-1 или более слабым хэшем.

  Если выбран этот режим:

  – Для всех портов, кроме порта 8443, все шифры TLS CBC и все шифры, не поддерживающие полную безопасность пересылки (Perfect Forward Secrecy), отключены.

  – Push-уведомления о событиях могут не проходить успешно на некоторые подписки мобильных устройств (см. Перенаправление событий для мобильных устройств в документации по XClarity Administrator в Интернете). Внешние сервисы, такие как Android и iOS, предоставляют сертификаты, подписанные SHA-1: алгоритмом, не соответствующим более строгим требованиям режима NIST SP 800-131A. В результате любые подключения к этим службам могут завершиться ошибкой, связанной с исключением сертификата или сбоем квитирования.

Дополнительные сведения о соответствии NIST SP 800-131A см. в разделе Обеспечение соответствия NIST 800-131A в документации по XClarity Administrator в Интернете.

Дополнительные сведения о настройке режимов безопасности на сервере управления см. в разделе Настройка криптографического режима и протоколов связи в онлайн-документации по XClarity Administrator.

Режимы безопасности для управляемых серверов

Этот параметр определяет режим, который должен использоваться для защищенного обмена данными с управляемыми серверами.

- **Безопасность с совместимостью**. Выберите этот режим, если необходимая для служб и клиентов криптография не должна соответствовать требованиям стандартов CNSA/FIPS. В этом режиме поддерживается широкий спектр алгоритмов криптографии и могут быть включены все службы.
- **NIST SP 800-131A**. Выберите этот режим для обеспечения соответствия стандарту NIST SP 800-131A. Это подразумевает использование ключей RSA с разрядностью не менее 2048 бит, использование для цифровых подписей хэшей SHA-256 или большей длины и гарантированное использование только алгоритмов симметричного шифрования, одобренных NIST. В этом режиме в качестве режима SSL/TLS должен быть выбран режим **Сервер-клиент TLS 1.2**.

  Этот режим *не* поддерживается для серверов с XCC2.
- **Стандартная безопасность** (только для серверов с XCC2). Это режим безопасности по умолчанию для серверы с XCC2. Выберите этот режим, если нужно обеспечить соответствие стандарту FIPS 140-3. Для работы XCC в режиме подтвержденного соответствия FIPS 140-3 можно включить только службы, которые поддерживают криптографию уровня FIPS 140–3. Службы, не поддерживающее криптографию на уровне FIPS 140-2/140-3, по умолчанию отключены, но при необходимости могут быть включены. В случае включения какой-либо службы, использующей криптографию, которая не соответствует уровню FIPS 140-3, XCC не может работать в режиме подтвержденного соответствия FIPS 140-3. Этот режим требует наличия сертификатов уровня FIPs.
- **Режим безопасности «Корпоративный строгий»** (только для серверы с XCC2). Это наиболее безопасный режим. Выберите этот режим, если требуется обеспечить соответствие стандарту CNSA. В этом режиме разрешены только службы, которые поддерживают криптографию уровня CNSA. Небезопасные службы по умолчанию отключены и не могут быть включены. Этот режим требует наличия сертификатов уровня CNSA.

  В режиме **Режим безопасности «Корпоративный строгий»** XClarity Administrator использует сертификат RSA-3072/SHA-384.

  Важно:

  – Для использования этого режима на каждом выбранном серверы с XCC2 должен быть установлен ключ Feature On Demand XCC2.

  – Если в этом режиме XClarity Administrator использует самозаверяющий сертификат, XClarity Administrator должен использовать корневой сертификат и сертификат сервера на основе RSA3072/SHA384. Если XClarity Administrator использует внешний подписанный сертификат, XClarity Administrator должен создать запрос на подпись сертификата на основе RSA3072/SHA384 и связаться с внешним ЦС для подписания нового сертификата сервера на основе RSA3072/SHA384.

  – Если XClarity Administrator использует сертификат на основе RSA3072/SHA384, XClarity Administrator может отключать устройства, если это не следующие устройства: рамы (CMMS) и серверы Flex System, серверы ThinkSystem, серверы ThinkServer, серверы System x M4 и M5, коммутаторы серии Lenovo ThinkSystem DB, Lenovo RackSwitch, коммутаторы Flex System, коммутаторы Mellanox, устройства хранения данных ThinkSystem DE/DM, хранилище на основе ленточной библиотеки IBM и серверы ThinkSystem SR635/SR655 с микропрограммой более

ранней версии, чем 22C. Чтобы продолжить управление отключенными устройствами, установите еще один экземпляр XClarity Administrator с сертификатом на основе RSA2048/SHA384.

Необходимо иметь в виду следующие последствия изменения криптографического режима.

- Переход из режима **Безопасность с совместимостью** или **Стандартная безопасность** в режим **Режим безопасности «Корпоративный строгий»** не поддерживается.
- Если при переходе из режима **Безопасность с совместимостью** в режим **Стандартная безопасность** (повышение режима безопасности) выясняется, что импортированные сертификаты или открытые ключи SSH не соответствуют требованиям, отображается соответствующее предупреждение, однако переход в режим **Стандартная безопасность** все равно возможен.
- При переходе из режима **Режим безопасности «Корпоративный строгий»** в режим **Безопасность с совместимостью** или **Стандартная безопасность** (понижение режима безопасности):
  - Сервер автоматически перезапускается, чтобы режим безопасности вступил в силу.
  - Если в XCC2 истек срок действия ключа FoD строгого режима или этот ключ отсутствует и если XCC2 использует самозаверяющий сертификат TLS, XCC2 повторно создает самозаверяющий сертификат TLS на основе алгоритма, соответствующего режиму «Стандартный-строгий». XClarity Administrator сообщает о сбое подключения из-за ошибки сертификата. Сведения об устранении ошибки недоверенного сертификата см. в разделе Разрешение ненадежного сертификата сервера в онлайн-документации по XClarity Administrator. Если в XCC2 используется пользовательский сертификат TLS, XCC2 допускает понижение режима и предупреждает о необходимости импортировать сертификат сервера, основанный на криптографии режима **Стандартная безопасность**.
- Режим **NIST SP 800-131A** не поддерживается для серверов с XCC2.
- Если для XClarity Administrator установлен криптографический режим TLS версии 1.2 и если на управляемых серверах, использующих управляемую аутентификацию, установлен режим безопасности TLS версии 1.2, изменение режима безопасности сервера на TLS версии 1.3 с помощью XClarity Administrator или XCC приведет к тому, что сервер будет постоянно находиться в автономном режиме.
- Если для XClarity Administrator установлен криптографический режим TLS версии 1.2, а вы пытаетесь управлять сервером с XCC, для которого установлен режим безопасности TLS версии 1.3, сервером невозможно управлять с использованием управляемой аутентификации.

Параметры безопасности можно изменить для указанных ниже устройств.
- Серверы Lenovo ThinkSystem с процессорами Intel или AMD (кроме SR635/SR655)
- Серверы Lenovo ThinkSystem версии 2
- Серверы Lenovo ThinkSystem версии 3 с процессорами Intel или AMD
- Серверы Lenovo ThinkEdge SE350/SE450
- Серверы Lenovo System x

Дополнительные сведения о настройке режимов безопасности на управляемом сервере см. в разделе Настройка параметров безопасности для сервера в онлайн-документации по XClarity Administrator.

Сертификаты безопасности

Lenovo XClarity Administrator использует сертификаты SSL, чтобы устанавливать безопасные, надежные соединения между XClarity Administrator и его управляемыми устройствами (например, рамами и процессорами служб на серверах System x), а также соединения пользователей с XClarity Administrator или с разными службами. По умолчанию XClarity Administrator, CMM и контроллеры

управления материнскими платами используют сертификаты, созданные в XClarity Administrator, которые являются самозаверяющими и подписаны во внутреннем центре сертификации.

Самозаверяющий сертификат сервера по умолчанию, который создается уникально в каждом экземпляре XClarity Administrator, обеспечивает достаточный уровень безопасности для многих сред. Можно разрешить XClarity Administrator управлять сертификатами за вас или взять на себя более активную роль и настроить или заменить сертификаты серверов. XClarity Administrator предоставляет параметры для настройки сертификатов для вашей среды. Доступные варианты:

- Создать новую пару ключей, воссоздав внутренний центр сертификации и (или) сертификат конечного сервера, использующий определенные для вашей организации значения.
- Создать запрос подписи сертификата (CSR), который может быть отправлен в центр сертификации на ваш выбор для подписи пользовательского сертификата и который затем можно отравить в XClarity Administrator для использования в качестве сертификата конечного сервера для всех размещенных сервисов
- Скачать сертификат сервера в свою локальную систему, чтобы иметь возможность импортировать этот сертификат в список доверенных сертификатов веб-браузера.

Дополнительные сведения о сертификатах см. в разделе Работа с сертификатами безопасности в документации по XClarity Administrator в Интернете.

Аутентификация

Поддерживаемые серверы аутентификации

Сервер аутентификации — это реестр пользователей, который используется для аутентификации их учетных данных. Lenovo XClarity Administrator поддерживает серверы аутентификации следующих типов.

- **Локальный сервер аутентификации**. По умолчанию решение XClarity Administrator настроено на использование встроенного сервера LDAP, находящегося на сервере управления.
- **Внешний сервер LDAP**. В настоящее время поддерживаются только Microsoft Active Directory и OpenLDAP. Этот сервер должен находиться на внешнем сервере Microsoft Windows, подключенном к сети управления. При использовании внешнего сервера LDAP локальный сервер аутентификации отключается.

  Внимание: Чтобы настроить метод привязки Active Directory для использования учетных данных для входа, на контроллерах управления материнскими платами для всех управляемых серверов должна быть микропрограмма от сентября 2016 г. или новее.
- **Внешняя система управления идентификацией**. В настоящее время поддерживается только CyberArk.

  Если учетные записи пользователей для сервера ThinkSystem или ThinkAgile регистрируются в CyberArk, можно настроить XClarity Administrator для извлечения учетных данных из CyberArk для входа на сервер при первоначальной настройке серверов для управления (с управляемой или локальной аутентификацией). Извлечь учетные данные из CyberArk можно только после определения путей CyberArk в XClarity Administrator и установки взаимного доверия между CyberArk и XClarity Administrator с использованием взаимной аутентификации в TLS и клиентских сертификатов.
- **Внешний SAML поставщик удостоверений**. В настоящее время поддерживается только Microsoft Active Directory Federation Services (AD FS). В дополнение ко вводу имени пользователя и пароля можно настроить многофакторную проверку подлинности, обеспечивающую дополнительную безопасность, так как требуется ввести ПИН-код, считать смарт-карту и предоставить сертификат клиента. При использовании SAML поставщик удостоверений сервер локальной аутентификации не отключается. Для прямого входа в систему управляемой рамы или сервера (если на этом

устройстве не включена Encapsulation) и для аутентификации на основе PowerShell и REST API, а также для восстановления, если внешняя аутентификация недоступна, требуются локальные учетные записи пользователей.

Можно использовать и внешний сервер LDAP, и внешний поставщик удостоверений. Если включены оба сервера, внешний сервер LDAP используется для прямого входа в систему управляемых устройств, а поставщик удостоверений — для входа на сервер управления.

Дополнительные сведения о серверах аутентификации см. в разделе Управление сервером аутентификации в документации по XClarity Administrator в Интернете.

Аутентификация устройств

По умолчанию устройства управляются с помощью управляемой аутентификации XClarity Administrator для входа в систему устройства. При управлении стоечными серверами и рамой Lenovo для входа в устройства можно выбрать локальную или управляемую аутентификацию.

- Если для стоечных серверов, рамы Lenovo и стоечных коммутаторов Lenovo применяется *локальная аутентификация*, XClarity Administrator использует сохраненные учетные данные для аутентификации на устройстве. *Сохраненные учетные данные* могут быть активной учетной записью пользователя на устройстве или учетной записью пользователя на сервере Active Directory.

  В XClarity Administrator необходимо создать сохраненные учетные данные, которые соответствуют активной учетной записи пользователя на устройстве или учетной записи пользователя на сервере Active Directory, прежде чем приступать к управлению устройством с помощью локальной аутентификации (см. раздел Управление сохраненными учетными данными в документации по XClarity Administrator в Интернете).

  Примечания:

  – Устройства RackSwitch поддерживают для аутентификации только сохраненные учетные данные. Учетные данные пользователей XClarity Administrator не поддерживаются.

- *Управляемая аутентификация* позволяет управлять несколькими устройствами и отслеживать их с помощью учетных данных на сервере аутентификации XClarity Administrator, а не локальных учетных данных. Если для устройства используется управляемая аутентификация (не коммутаторы и не серверы ThinkServer и System x M4), XClarity Administrator настраивает устройство и его установленные компоненты на использование сервера аутентификации XClarity Administrator для централизованного управления.

  – Если управляемая аутентификация включена, для управления устройствами можно использовать учетные данные, вводимые вручную, или сохраненные учетные данные (см. разделы Управление учетными записями пользователей и в документации по XClarity Administrator в Интернете).

    Сохраненные учетные данные используются только до тех пор, пока XClarity Administrator не настроит параметры LDAP на устройстве. После этого все изменения в сохраненных учетных данных не оказывают влияния на управление или мониторинг устройства.

    Примечание: Если для устройства включена управляемая аутентификация, изменить для него сохраненные учетные данные с помощью XClarity Administrator невозможно.

  – Если используется локальный или внешний сервер LDAP в качестве сервера аутентификации XClarity Administrator, учетные записи пользователей, которые определены на сервере аутентификации, используются для входа в XClarity Administrator, CMM и контроллеры управления материнской платой в домене XClarity Administrator. Локальные учетные записи пользователей CMM и контроллера управления отключены.

  – Если используется поставщик удостоверений SAML 2.0 в качестве сервера аутентификации XClarity Administrator, учетные записи SAML недоступны для управляемых устройств. Однако

если поставщик удостоверений SAML и сервер LDAP используются вместе, и если поставщик удостоверений использует учетные записи, существующие на сервере LDAP, учетные записи пользователей LDAP можно использовать для входа на управляемые устройства, а более сложные способы аутентификации, предоставляемые SAML 2.0 (например, многофакторная аутентификация и единый вход), могут использоваться для входа в XClarity Administrator.

- Единый вход позволяет пользователю, который уже выполнил вход в XClarity Administrator, автоматически входить в контроллер управления материнской платой. Единый вход включается по умолчанию, если управление сервером ThinkSystem или ThinkAgile осуществляется с помощью XClarity Administrator (кроме случаев, когда управление серверами осуществляется с помощью паролей CyberArk). Можно задать глобальную настройку для включения или выключения единого входа на всех управляемых серверах ThinkSystem и ThinkAgile. При включении единого входа для определенных серверов ThinkSystem и ThinkAgile переопределяется глобальная настройка для всех серверов ThinkSystem и ThinkAgile (см. раздел Управление серверами в документации по XClarity Administrator в Интернете).

  Примечание: При использовании для аутентификации системы управления идентификацией CyberArk функция единого входа отключается автоматически.

- При включенной управляемой аутентификации для серверов ThinkSystem SR635 и SR655:
  - Микропрограмма контроллера управления материнской платой поддерживает до пяти ролей пользователей LDAP. XClarity Administrator добавляет эти роли пользователей LDAP к серверам во время управления: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** и **lxc-os-admin**.

    Пользователи должны быть назначены по крайней мере одной из указанных ролей пользователей LDAP для связи с серверами ThinkSystem SR635 и SR655.
  - Микропрограмма контроллера управления не поддерживает пользователей LDAP с тем же именем пользователя, что и у локального пользователя сервера.
- Для серверов ThinkServer и System x M4 сервер аутентификации XClarity Administrator не используется. Вместо этого на устройстве создается учетная запись IPMI с префиксом «LXCA_», за которым следует случайная строка. (Существующие локальные учетные записи пользователей IPMI не отключаются.) При прекращении управления сервером ThinkServer учетная запись пользователя «LXCA_» отключается, и префикс «LXCA_» заменяется префиксом «DISABLED_». Чтобы определить, управляется ли сервер ThinkServer другим экземпляром, XClarity Administrator проверяет наличие учетных записей IPMI с префиксом «LXCA_». Если вы решили перевести управляемый сервер ThinkServer на принудительное управление, все учетные записи IPMI на устройстве с префиксом «LXCA_» отключаются и переименовываются. Возможно, стоит вручную удалить учетные записи IPMI, которые больше не используются.

  Если вы используете учетные данные, вводимые вручную, XClarity Administrator автоматически создает сохраненные учетные данные и использует их для управления устройством.

  Примечания: Если для устройства включена управляемая аутентификация, изменить для него сохраненные учетные данные с помощью XClarity Administrator невозможно.
  - При каждом управлении устройством с использованием учетных данных, введенных вручную, для этого устройства создаются новые сохраненные учетные данные, даже если в ходе предыдущего процесса управления для этого устройства были созданы другие сохраненные учетные данные.
  - При прекращении управления устройством решение XClarity Administrator не удаляет сохраненные учетные данные, которые были автоматически созданы для этого устройства в ходе процесса управления.

Учетная запись пользователя для восстановления

Если задан пароль восстановления, XClarity Administrator отключает локальную учетную запись пользователя CMM или контроллера управления и создает на устройстве новую учетную запись пользователя для восстановления (RECOVERY_ID), предназначенную для аутентификации в будущем. Если происходит сбой сервера управления, можно использовать учетную запись RECOVERY_ID для входа в систему устройства, чтобы предпринять действия по восстановлению функций управления учетными записями на устройстве, пока узел управления не будет восстановлен или заменен.

Если вы прекращаете управление устройством, у которого есть учетная запись пользователя RECOVERY_ID, все локальные учетные записи пользователей включаются, а учетная запись RECOVERY_ID удаляется.

- Если вы изменяете отключенные локальные учетные записи пользователей (например, изменяете пароль), эти изменения не влияют на учетную запись RECOVERY_ID. В режиме управляемой аутентификации учетная запись RECOVERY_ID — единственная, которая активируется и работает.
- Учетная запись RECOVERY_ID используется только в чрезвычайных ситуациях, например при сбое на сервере управления или если проблема с сетью не позволяет устройству обмениваться данными с XClarity Administrator для аутентификации пользователей.
- Пароль RECOVERY_ID задается при обнаружении устройства. Обязательно запишите пароль для последующего использования.

Сведения о восстановлении управления устройством см. в разделах Восстановление управления рамы с CMM после сбоя узла управления и Восстановление управления стоечным или башенным сервером после сбоя сервера управления в документации по XClarity Administrator в Интернете.

Учетные записи пользователей и группы ролей

Учетные записи пользователей используются для входа в Lenovo XClarity Administrator, а также все управляемые рамы и серверы, и управления ими. Учетные записи пользователей XClarity Administrator участвуют в двух взаимозависимых процессах: аутентификация и авторизация.

Аутентификация — это механизм безопасности, с помощью которого проверяются учетные данные пользователя. Процесс аутентификации использует учетные данные пользователя, которые хранятся на настроенном сервере аутентификации. Он также предотвращает доступ к ресурсам со стороны несанкционированных серверов управления или системных приложений, управляемых злоумышленниками. После проверки подлинности пользователя можно получить доступ к XClarity Administrator. Однако для доступа к конкретному ресурсу или выполнению конкретной задачи пользователю также необходимы соответствующие разрешения.

Разрешение проверяет полномочия аутентифицированного пользователя и управляет доступом к ресурсам на основе членства пользователя в группах ролей. *Группы ролей* используются для назначения определенных ролей набору учетных записей пользователей, которые определяются и управляются на сервере аутентификации. Например, если пользователь является членом группы ролей, которая имеет разрешения администратора, этот пользователь может создавать, редактировать и удалять учетные записи пользователей из XClarity Administrator. Если пользователь имеет разрешения оператора, этот пользователь может только просматривать сведения учетной записи пользователя.

Дополнительные сведения об учетных записях пользователей и группах ролей см. в разделе Управление учетными записями пользователей в документации по XClarity Administrator в Интернете.

Безопасность учетной записи пользователя

Параметры учетной записи пользователя управляют сложностью пароля, блокировкой учетной записи и тайм-аутом веб-сеанса после неактивности. Значения параметров безопасности учетной записи можно изменить.

Дополнительные сведения о параметрах безопасности учетной записи см. в разделе Изменение параметров безопасности учетной записи пользователя в документации по Lenovo XClarity Administrator в Интернете.

Замечания по высокому уровню доступности

Для настройки высокой доступности для Lenovo XClarity Administrator используйте функции высокой доступности, которые являются частью операционной системы хоста или среды контейнеров.

Docker

Docker Datacenter можно использовать для настройки среды высокой доступности для контейнеров XClarity Administrator, работающих под управлением Docker Engine. Дополнительные сведения о высокой доступности на базе Docker Datacenter см. в разделе Веб-страница архитектуры высокой доступности и приложений с Docker Datacenter.

Citrix

Используйте функцию высокой доступности, предоставленную для среды Citrix. Дополнительные сведения см. в разделе Реализация высокой доступности (Citrix) в документации по XClarity Administrator в Интернете.

KVM (CentOS, RedHat и Ubuntu)

Можно использовать OpenStack, или если среда высокой доступности уже реализована, вы можете продолжать использовать уже существующие внутренние процессы. Дополнительные сведения о высоком уровне доступности OpenStack см. в разделе Реализация высокой доступности (KVM) в документации по XClarity Administrator в Интернете.

Microsoft Hyper-V

Используйте функцию высокой доступности, предоставленную для среды ESXi. Сведения см. в разделе Реализация высокой доступности (Microsoft Hyper-V) в документации по XClarity Administrator в Интернете.

Nutanix AHV

Используйте функцию высокой доступности виртуальной машины, предоставленную для среды Nutanix AHV. Дополнительные сведения см. в разделе Реализация высокой доступности (Nutanix) в документации по XClarity Administrator в Интернете.

VMware ESXi

В среде высокой доступности VMware несколько хостов настроены как кластер. Общее хранилище используется для создания образа диска виртуальной машины (ВМ) для хостов в кластере. ВМ работает одновременно только на одном хосте. При возникновении проблемы с виртуальной машиной на резервном хосте запускается другой экземпляр этой виртуальной машины.

VMware High Availability требует следующие компоненты:

- Как минимум два хоста, на которых установлено ESXi. Эти хосты становятся частью кластера VMware.
- Третий хост, на котором установлен VMware vCenter.

Рекомендация: убедитесь, что вы устанавливаете версию VMware vCenter, которая совместима с версиями ESXi, установленными на хостах, которые будут использоваться в кластере.

VMware vCenter может быть установлен на одном из хостов, которые используются в кластере. Однако, если этот хост отключен или недоступен, вы также теряете доступ к интерфейсу VMware vCenter.

- Общее хранилище (хранилища данных), доступ к которому могут получить все хосты в кластере. Можно использовать любой тип общего хранилища, поддерживаемый VMware. Хранилище данных используется VMware для определения того, должна ли виртуальная машина переключаться на другой хост (частота обмена).

Сведения о настройке кластера VMware High Availability см. в разделе Реализация высокой доступности (VMware ESXi) в документации по XClarity Administrator в Интернете.

Features on Demand

Features on Demand активирует компоненты, не требуя установки оборудования или приобретения нового оборудования. Эта активация выполняется путем приобретения и установки соответствующего ключа Features on Demand.

Чтобы использовать операции удаленного управления и развертывания операционной системы в Lenovo XClarity Administrator, необходимо включить уровень XClarity Controller, уровень Enterprise или расширенное обновление MM для серверов, у которых по умолчанию эти функции не активированы. Эти операции также требуют, чтобы на серверах ThinkSystem, Converged и System x был установлен ключ Features on Demand для удаленного присутствия. Можно определить, следует ли включить, отключить или не устанавливать удаленное присутствие на сервере, на странице «Серверы» (см. раздел Просмотр состояния управляемого сервера в документации по XClarity Administrator в Интернете).

Некоторые расширенные функции сервера активируются с помощью ключей Features on Demand. Если функции имеют настраиваемые параметры, которые отображаются во время установки UEFI, можно настроить этот параметр, используя Шаблоны конфигурации; однако полученная конфигурация не активируется до тех пор, пока не будет установлен соответствующий ключ Features on Demand.

Примечание: Вы не можете установить или управлять ключами Features on Demand через XClarity Administrator; однако можно просмотреть список ключей Features on Demand, которые в настоящее время установлены на управляемых серверах. Дополнительные сведения о просмотре установленных ключей Features on Demand см. в Просмотр клавиш Feature on Demand в документации поXClarity Administrator в Интернете.

Приобретение и установка ключей Features on Demand:

1. Приобретите обновление Features on Demand, используя соответствующий номер компонента.

   Можно приобрести ключи через Веб-портал Features on Demand. Когда ваша покупка будет завершена, вы получите код авторизации по электронной почте.
2. В Веб-портал Features on Demand, введите код авторизации, который вы получили, а также уникальный системный идентификатор сервера, который вы собираетесь обновить.
3. Загрузите ключ активации в виде .KEY-файла.
4. Загрузите ключ активации в контроллер управления для сервера.
5. Перезагрузите сервер. После завершения перезапуска функция будет активирована.

Дополнительные сведения о ключах Features on Demand см. в разделе Использование Lenovo Features on Demand.

Глава 3. Установка Lenovo XClarity Administrator

Существует несколько способов подключения управляемых устройств к сети и настройки виртуального устройства Lenovo XClarity Administrator для управления ими. Используйте информацию в этом разделе в качестве руководства по настройке управляемых устройств и установке XClarity Administrator

В этом разделе описывается порядок настройки нескольких распространенных топологий. Этот раздел не охватывает все возможные топологии сетей.

Внимание: Для управления устройствами XClarity Administrator необходимо иметь доступ к сети управления.

Подробнее:

- Установка Lenovo XClarity Administrator в VMware vCenter
- Установка Lenovo XClarity Administrator в VMware vSphere
- Установка Lenovo XClarity Administrator в Windows Hyper-V
- Установка Lenovo XClarity Administrator в Red Hat KVM

Единая сеть данных и управления

В этой сетевой топологии сеть передачи данных и сеть управления — это одна и та же сеть.

Перед началом работы

Убедитесь, что включены все соответствующие порты, включая порты, которые требуются XClarity Administrator (см. раздел Доступность портов).

Убедитесь, что на каждом устройстве, которым предполагается управлять с помощью XClarity Administrator, установлена микропрограмма, удовлетворяющая минимальным требованиям. Минимально необходимые уровни микропрограммы можно найти в Веб-страница поддержки XClarity Administrator — совместимость, открыв вкладку **Совместимость** и щелкнув ссылку для соответствующих типов устройств.

Важно: Настройте устройства и компоненты таким образом, чтобы свести к минимуму изменения IP-адресов. Рассмотрите возможность использования статических IP-адресов вместо протокола динамической настройки хостов (DHCP). Если используется протокол DHCP, убедитесь, что изменения IP-адреса сведены к минимуму.

Об этой задаче

Для виртуальных устройств вся связь между XClarity Administrator и сетью осуществляется через сетевой интерфейс eth0 на хосте. Для контейнеров можно использовать пользовательское имя; однако в этом сценарии используется eth0.

Важно: Реализация общей сети данных и управления может привести к сбоям трафика, например выпадению пакетов или неполадкам подключения сети управления, в зависимости от конфигурации вашей сети (например, если трафик от серверов имеет высокий приоритет, а трафик от контроллеров управления имеет низкий приоритет). Сеть управления использует UDP-трафик в дополнение к TCP. UDP-трафик может иметь более низкий приоритет при высоком сетевом трафике.

На рисунке ниже показан один из способов настройки среды для случая единой сети данных и управления. Цифры на рисунке соответствуют пронумерованным шагам, описанным в следующих разделах.

Примечание: На этом рисунке не показаны все возможные варианты подключения, которые могут потребоваться для вашей среды. На этом рисунке демонстрируются только требования к подключению стоечных серверов, стоечных коммутаторов, коммутаторов Flex и модулей CMM, связанные с настройкой единой сети данных и управления.

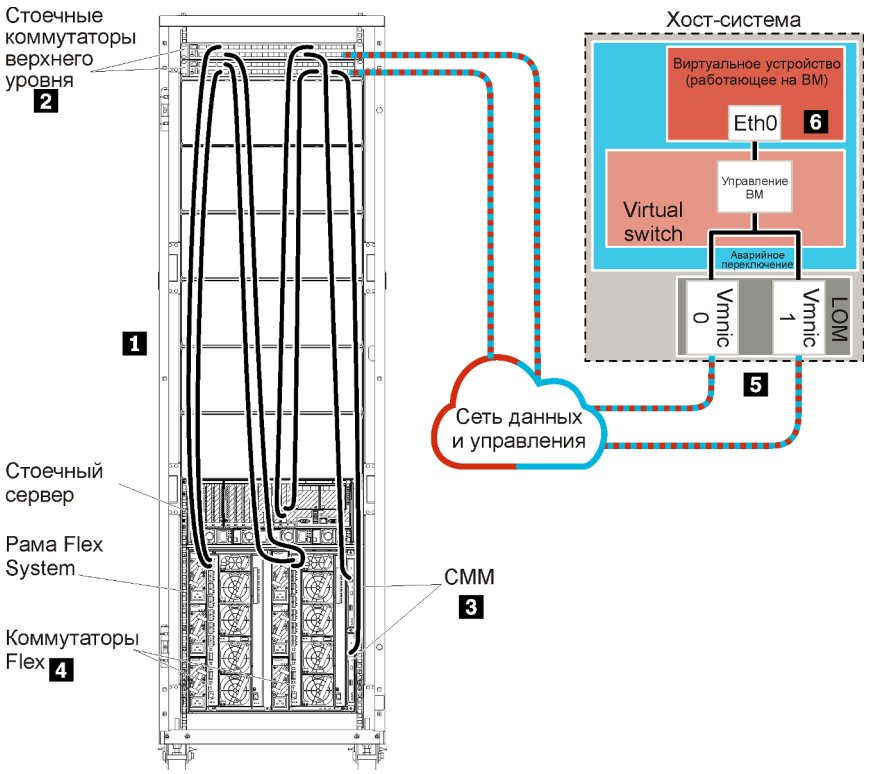


Рис. 8. Пример единой топологии сети данных и управления для виртуального устройства

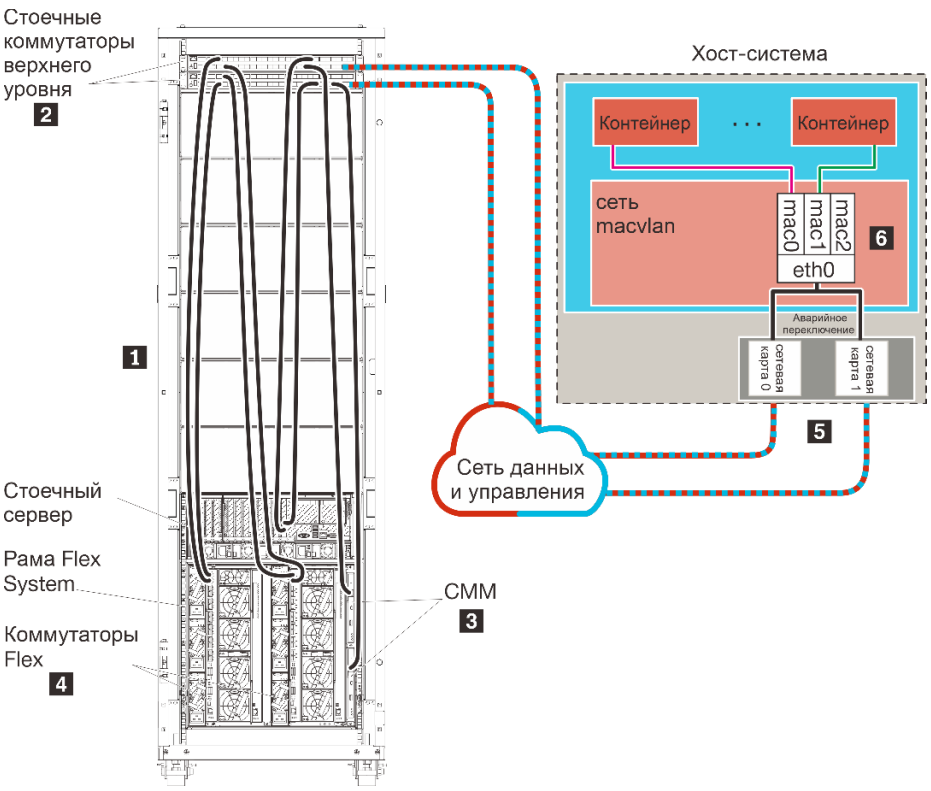


Рис. 9. Пример топологии единой сети данных и управления для контейнеров

Важно: XClarity Administrator можно установить на любой системе, отвечающей требованиям для XClarity Administrator, в том числе на управляемом сервере. Если для хоста XClarity Administrator используется управляемый сервер:

- Необходимо реализовать либо топологию с виртуальным разделением сети данных и сети управления, либо топологию с единой сетью данных и управления.
- Для применения обновлений микропрограммы к этому управляемому серверу невозможно использовать XClarity Administrator. Даже если только часть микропрограммного обеспечения применяется с немедленной активацией, XClarity Administrator принудительно перезапускает целевой сервер, что приводит к перезапуску XClarity Administrator. Если используется отложенная активация, при перезапуске XClarity Administrator применяются только некоторые части микропрограммы.
- Если вы используете сервер в раме Flex System, убедитесь, что на сервере настроено автоматическое включение. Этот параметр можно установить из веб-интерфейса CMM, нажав **Управление рамой → Вычислительные узлы**, выбрав сервер и выбрав **Автоматическое включение/выключение питания** для параметра **Режим автоматического включения**.

Если вы планируете установить XClarity Administrator для управления уже имеющимися и настроенными рамами и стоечными серверами, перейдите к разделу Шаг 5. Установка и настройка хоста.

Дополнительные сведения о планировании этой топологии, включая информацию о параметрах сети и конфигурации Eth1 и Eth0, см. в разделе Единая сеть данных и управления.

Шаг 1. Подключение рамы, стоечных серверов и хоста Lenovo XClarity Administrator к стоечным коммутаторам верхнего уровня

Подключите с помощью кабелей раму, стоечные серверы и хост XClarity Administrator к стоечным коммутаторам верхнего уровня, чтобы обеспечить связь между устройствами и вашей сетью.

Процедура

Подключите с помощью кабелей каждый коммутатор Flex и модуль CMM в каждой раме, каждый стоечный сервер и хост XClarity Administrator к обоим стоечным коммутаторам верхнего уровня. Для подключения можно использовать любые порты стоечных коммутаторов верхнего уровня.

На следующем рисунке приведен пример, иллюстрирующий подключение рамы (Коммутаторы Flex и модулей CMM), стоечных серверов и хоста XClarity Administrator с помощью кабелей к стоечным коммутаторам верхнего уровня.

Примечание: На этом рисунке не показаны все возможные варианты подключения, которые могут потребоваться для вашей среды. На этом рисунке демонстрируются только требования к подключению стоечных серверов, стоечных коммутаторов, коммутаторов Flex и модулей CMM, связанные с настройкой единой сети данных и управления.

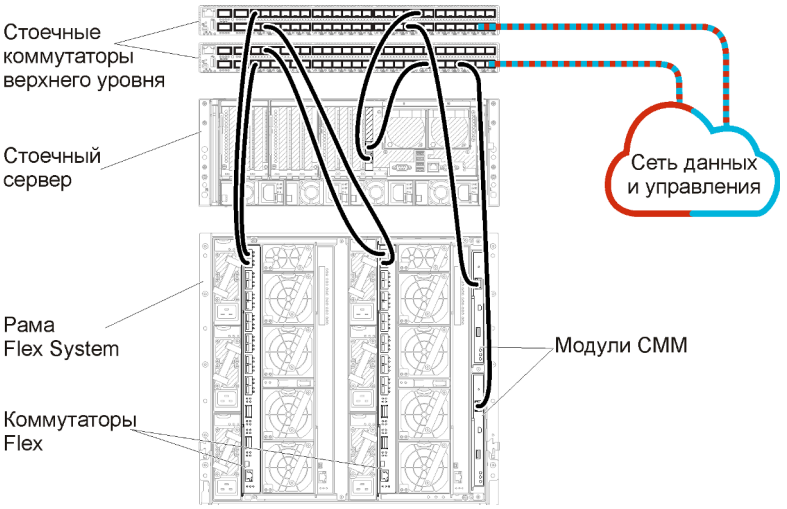


Рис. 10. Пример кабельных соединений для единой сети данных и управления

Шаг 2. Настройка стоечных коммутаторов верхнего уровня

Настройте стоечные коммутаторы верхнего уровня.

Перед началом работы

В дополнение к обычным требованиям к конфигурации для стоечных коммутаторов верхнего уровня, убедитесь, что включены все необходимые порты, в том числе внешние порты для связи с Коммутаторы Flex, стоечными серверами и сетью, а также внутренние порты для связи с модулями CMM, стоечными серверами и сетью.

Процедура

Действия по настройке могут отличаться в зависимости от типа установленных стоечных коммутаторов.

Сведения о настройке стоечных коммутаторов верхнего уровня Lenovo см. в Стоечные коммутаторы в документации по System x в Интернете. Если установлен другой стоечный коммутатор верхнего уровня, см. документацию, сопровождающую этот коммутатор.

Шаг 3. Настройка модулей CMM

Настройте основной модуль управления рамой (Chassis Management Module, CMM) в раме для управления всеми устройствами в раме.

Об этой задаче

Подробные сведения о настройке модуля CMM см. в разделе Настройка компонентов рамы в документации по устройствам Flex System в Интернете.

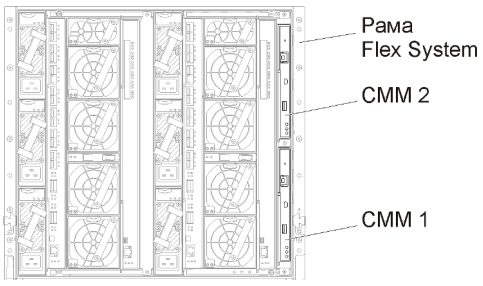
Также см. действия 4.1–4.5 на листе с инструкциями из комплекта поставки вашей рамы.

Процедура

Чтобы настроить модуль CMM, выполните указанные ниже действия.

Если установлены два модуля CMM, настройте только *основной* модуль CMM. Он автоматически синхронизирует конфигурацию с резервным модулем CMM.

Шаг 1. Подключите кабель Ethernet от модуля CMM в отсеке 1 к клиентской рабочей станции, чтобы создать прямое подключение.



При первом подключении к модулю CMM, возможно, потребуется изменить свойства протокола IP на клиентской рабочей станции.

Важно: Убедитесь, что подсеть клиентской рабочей станции совпадает с подсетью модуля CMM. (По умолчанию для CMM используется подсеть 255.255.255.0). IP-адрес, выбранный для клиентской рабочей станции, должен находиться в той же сети, что и IP-адрес модуля CMM (например, 192.168.70.0–192.168.70.24).

Шаг 2. Чтобы запустить интерфейс управления CMM, откройте веб-браузер на клиентской рабочей станции и направьте его на IP-адрес модуля CMM.

Примечания:

- Убедитесь, что используется безопасное подключение, и включите **https** в URL-адрес (пример: https://192.168.70.100). Если не включить «https», отобразится ошибка «Страница не найдена».
- Если вы используете IP-адрес по умолчанию 192.168.70.100, интерфейс управления CMM может стать доступен спустя несколько минут. Эта задержка возникает из-за того, что модуль CMM пытается получить адрес DHCP в течение двух минут, прежде чем вернуться к статическому адресу по умолчанию.

Шаг 3. Войдите в интерфейс управления модуля CMM, используя принимаемые по умолчанию идентификатор пользователя `USERID` и пароль `PASSWORD`. После входа пароль по умолчанию необходимо изменить.

Шаг 4. Выполните шаги мастера первоначальной настройки CMM, чтобы указать сведения для своей среды. Мастер первоначальной настройки включает в себя следующие параметры:

- Просмотр ресурсов и состояния работоспособности рамы.
- Импорт конфигурации из существующего файла конфигурации.
- Настройка общих параметров CMM.
- Установка даты и времени CMM.

  Совет. При установке XClarity Administrator настройте использование сервера NTP для XClarity Administrator и всех рам, которыми управляет XClarity Administrator.
- Настройте IP-информацию модуля CMM.
- Настройте политику безопасности модуля CMM.
- Настройте систему доменных имен (DNS).
- Настройте средства перенаправления событий.

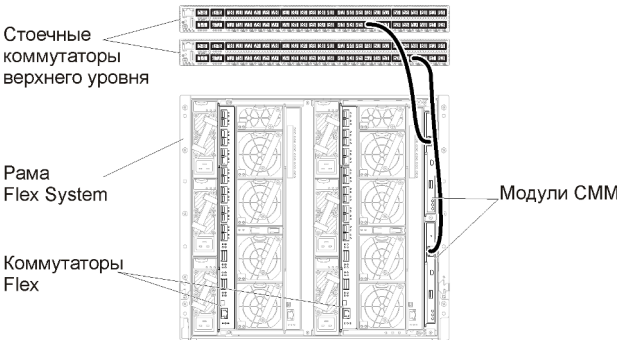
Шаг 5. Сохранив заданные значения параметров мастера настройки и применив изменения, настройте IP-адреса для всех компонентов в раме.

См. действие 4.6 на листе с инструкциями из комплекта поставки вашей рамы.

Примечание: Чтобы отобразились новые IP-адреса, необходимо сбросить процессор управления системой для каждого вычислительного узла и перезапустить коммутаторы Flex.

Шаг 6. Перезапустите модуль CMM с помощью интерфейса управления CMM.

Шаг 7. Пока модуль CMM перезапускается, подключите кабель от порта Ethernet модуля CMM к своей сети.



Шаг 8. Войдите в интерфейс управления модуля CMM, используя новый IP-адрес.

После завершения

В модуле CMM также можно настроить поддержку избыточности. Используйте справочную систему CMM, чтобы узнать больше о полях, доступных на каждой из следующих страниц.

- Настройте для модуля CMM аварийное переключение в случае аппаратного сбоя в основном модуле CMM. В интерфейсе управления CMM нажмите **Mgt Module Management → Свойства → Расширенное аварийное переключение**.
- Настройте аварийное переключение в случае неполадки с сетью (восходящий канал). В интерфейсе управления CMM нажмите **Mgt Module Management → Сеть**, откройте вкладку

Ethernet, а затем нажмите **Дополнительные параметры Ethernet**. Как минимум, убедитесь, что выбран параметр **Переключение при утрате физического сетевого подключения**.

Шаг 4. Настройка Коммутаторы Flex

Настройте Коммутаторы Flex (модули ввода-вывода) в каждой раме.

Перед началом работы

Убедитесь, что включены все необходимые порты, в том числе внешние порты для связи между коммутатором Flex и стоечным коммутатором верхнего уровня, а также внутренние порты для связи с модулем CMM.

Если в коммутаторах Flex настроено получение параметров динамической сети (IP-адреса, маски сети, шлюза и адреса DNS) посредством DHCP, убедитесь, что коммутаторы Flex имеют согласованные параметры (например, убедитесь, что IP-адреса находятся в одной подсети с IP-адресами модуля CMM).

Важно: Для каждой рамы Flex System убедитесь, что тип межкомпонентной сети карты расширения в каждом сервере в раме совместим с типом межкомпонентной сети всех коммутаторов Flex в этой же раме. Например, если в раме установлены коммутаторы Ethernet, все серверы в этой раме должны иметь возможность подключения к Ethernet с помощью разъема локальной сети на материнской плате или карты расширения Ethernet. Дополнительные сведения о настройке коммутаторов Flex см. в разделе Настройка модулей ввода-вывода в документации по устройствам Flex System в Интернете.

Процедура

Действия по настройке могут отличаться в зависимости от типа установленных Коммутаторы Flex. Дополнительную информацию о каждом из поддерживаемых Коммутаторы Flex см. в Сетевые коммутаторы Flex System в документации по устройствам Flex System в Интернете.

Как правило, требуется настроить коммутаторы Flex в отсеках 1 и 2 для коммутаторов Flex.

Совет. Отсек 2 для коммутатора Flex — это третий по счету модульный отсек, если смотреть на раму с тыльной стороны.

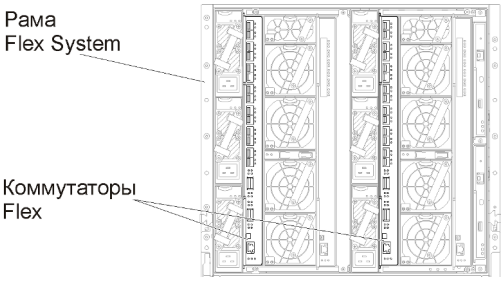


Рис. 11. Места установки Коммутатор Flexв раме

Шаг 5. Установка и настройка хоста

Docker можно установить на любом сервере, который отвечает требованиям для Lenovo XClarity Administrator.

Перед началом работы

Docker Datacenter можно использовать для настройки среды высокой доступности для контейнеров XClarity Administrator, работающих под управлением Docker Engine. Дополнительные сведения о высокой доступности на базе Docker Datacenter см. в разделе Веб-страница архитектуры высокой доступности и приложений с Docker Datacenter.

Убедитесь, что хост отвечает предварительным требованиям, которые определены в разделе Обязательные требования к оборудованию и программному обеспечению.

Убедитесь, что система хоста находится в той же сети, что и устройства, которыми вы хотите управлять.

Важно: XClarity Administrator можно установить на любой системе, отвечающей требованиям для XClarity Administrator, в том числе на управляемом сервере. Если для хоста XClarity Administrator используется управляемый сервер:

- Необходимо реализовать либо топологию с виртуальным разделением сети данных и сети управления, либо топологию с единой сетью данных и управления.
- Для применения обновлений микропрограммы к этому управляемому серверу невозможно использовать XClarity Administrator. Даже если только часть микропрограммного обеспечения применяется с немедленной активацией, XClarity Administrator принудительно перезапускает целевой сервер, что приводит к перезапуску XClarity Administrator. Если используется отложенная активация, при перезапуске XClarity Administrator применяются только некоторые части микропрограммы.
- Если вы используете сервер в раме Flex System, убедитесь, что на сервере настроено автоматическое включение. Этот параметр можно установить из веб-интерфейса CMM, нажав **Управление рамой → Вычислительные узлы**, выбрав сервер и выбрав **Автоматическое включение/выключение питания** для параметра **Режим автоматического включения**.

Процедура

Установите и настройте Docker на хосте согласно инструкциям, предоставляемым с дистрибутивом Docker.

Шаг 6. Установка и настройка XClarity Administrator

Установите и настройте контейнер Lenovo XClarity Administrator на только что установленном хосте Docker.

Перед началом работы

Убедитесь, что хост-система отвечает минимальным требованиям к оборудованию и программному обеспечению (см. раздел Обязательные требования к оборудованию и программному обеспечению).

Убедитесь, что включены все соответствующие порты, включая порты, которые требуются XClarity Administrator (см. раздел Доступность портов).

Убедитесь, что система хоста находится в той же сети, что и устройства, которыми вы хотите управлять.

Убедитесь, что ОС хоста и XClarity Administrator используют один и тот же сервер NTP.

XClarity Administrator позволяет использовать пользовательское имя сети для управления данными и оборудованием, а также развертывания ОС (см. раздел Конфигурации сети). В этом примере в следующей процедуре используется eth0.

Убедитесь, что сеть macvlan загружена в ядро хост-системы. Чтобы проверить, загружена ли она, воспользуйтесь командой **lsmod | grep macvlan**. Чтобы загрузить macvlan в ядро, выполните команду **modprobe macvlan**.

При запуске нескольких контейнеров XClarity Administrator в одном хосте следует использовать уникальное имя и IP-адрес для каждого контейнера.

Если вы предполагаете управлять ThinkServer и другими устаревшими устройствами, убедитесь, что в Docker включена поддержка IPv6.

1. Внесите следующие изменения в файл /etc/docker/daemon.json: установите значение «true» для ключа **ipv6** и укажите вашу подсеть IPv6 в качестве значения ключа **fixed-cidr-v6**. Пример файла daemon представлен ниже.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Перезагрузите файл конфигурации Docker, выполнив указанную ниже команду.
```
systemctl reload docker
```

Примечание: XClarity Administrator *не* работает в качестве привилегированного контейнера.

Процедура

Чтобы установить контейнер XClarity Administrator с помощью Docker compose, выполните следующие шаги.

Шаг 1. Скачайте образ виртуального устройства XClarity Administrator, файла среды и YAML-файла с Веб-страница загрузки XClarity Administrator на клиентскую рабочую станцию. Войдите на веб-сайт и используйте предоставленный вам ключ доступа для скачивания образа.

Шаг 2. Импортируйте образ контейнера XClarity Administrator в хост docker, выполнив следующую команду.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Шаг 3. Отредактируйте файл `docker_compose.env` и измените следующие переменные среды.

- **CONTAINER_NAME**. Уникальное имя контейнера, используемое для создания томов Docker для каждого экземпляра XClarity Administrator (например, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Статический адрес IPv4 для контейнера (например, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Необязательно) Путь удаленного общего ресурса, который можно использовать для хранения резервных копий XClarity Administrator. Он должен иметь вид `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Необязательно) Путь к удаленному общему ресурсу, который можно использовать в качестве удаленного репозитория для обновлений микропрограмм. Он должен иметь вид `/mnt/fw_share`.

Ниже приведен пример файла среды.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Шаг 4. Измените файл `docker_compose.yml` и измените следующие свойства.

- Задайте значение свойства **image** равным имени файла установочного образа, используемому в шаге 2.

Примечание: Имя файла образа можно изменить (например, на latest) с помощью команды `docker tag`.

- Если необходимо использовать удаленные общие ресурсы в качестве удаленного репозитория микропрограмм и для хранения резервных копий XClarity Administrator, задайте точку подключения хоста для каждого удаленного общего ресурса в свойстве **volumes**.
- Установите в качестве значения свойства **dns** IP-адрес серверов DNS.
- Этот контейнер использует тот же пул ресурсов процессора, памяти и хранения, которые доступны хосту. При необходимости определите ограничения использования ресурсов, настроив свойства **cpus** и **memory**.
- Задайте значение свойства **parent** равным имени сетевого интерфейса в хост-системе, который следует использовать в качестве родительского для интерфейса macvlan в контейнере. Этот интерфейс должен иметь прямой доступ к подсети, назначенной контейнеру.
- Задайте свойства **subnet (подсеть)** и **gateway (шлюз)** в соответствии с топологией вашей сети. Как правило, подсеть и шлюз предназначены для сети управления, к которой относится ${ADDRESS}.
- Если требуется поддержка IPv6, задайте для свойства **enable_ipv6** значение «true», укажите адрес IPv6 в качестве значения свойства **ipv6_address** и добавьте еще один набор свойств **subnet** и **gateway** в соответствии с топологией вашей сети (обычно для сети управления, к которой принадлежит адрес IPv6).

Примечание: XClarity Administrator использует macvlan для настройки контейнерной сети. Дополнительную информацию см. в разделе Веб-страница «Использование сетей macvlan».

Ниже представлен пример файла YML с включенной поддержкой IPv6.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
```

```
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
```

Шаг 5. Разверните образ в Docker, выполнив следующую команду, где <*ENV_FILENAME*> — имя файла переменных среды, созданного в шаге 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

После завершения

Войдите в систему и настройте XClarity Administrator (см. разделы Доступ к веб-интерфейсу Lenovo XClarity Administrator в первый раз и Настройка Lenovo XClarity Administrator).

Физически раздельные сети данных и управления

В этой топологии сеть передачи данных и сеть управления физически отделены друг от друга. Связь в целях управления между Lenovo XClarity Administrator и сетью осуществляется через сетевой интерфейс Eth0 на хосте. Передача данных производится через сетевой интерфейс Eth1.

Перед началом работы

Убедитесь, что включены все соответствующие порты, включая порты, которые требуются XClarity Administrator (см. раздел Доступность портов).

Убедитесь, что на каждом устройстве, которым предполагается управлять с помощью XClarity Administrator, установлена микропрограмма, удовлетворяющая минимальным требованиям. Минимально необходимые уровни микропрограммы можно найти в Веб-страница поддержки XClarity Administrator — совместимость, открыв вкладку **Совместимость** и щелкнув ссылку для соответствующих типов устройств.

Важно: Настройте устройства и компоненты таким образом, чтобы свести к минимуму изменения IP-адресов. Рассмотрите возможность использования статических IP-адресов вместо протокола динамической настройки хостов (DHCP). Если используется протокол DHCP, убедитесь, что изменения IP-адреса сведены к минимуму.

Об этой задаче

На рисунке ниже показан один из способов настройки среды в том случае, когда сеть передачи данных и сеть управления являются физически разными сетями. Цифры на рисунке соответствуют пронумерованным шагам, описанным в следующих разделах.

Примечание: На этом рисунке не показаны все возможные варианты подключения, которые могут потребоваться для вашей среды. На этом рисунке демонстрируются только требования к подключению для коммутаторов Flex, модулей CMM и стоечных серверов, связанные с настройкой физически раздельных сетей данных и управления.

Совет. Вместо настройки двух физических коммутаторов, подключенных к каждой сети для обеспечения избыточности (четырех коммутаторов в общей сложности), можно настроить по одному физическому коммутатору, подключенному к каждой из сетей (в сумме два коммутатора). В этом случае каждый коммутатор будет подключен к обеим сетям, и потребуется задействовать две виртуальные локальные сети (VLAN) для разделения трафика данных: одну для сети передачи данных и одну для сети управления.

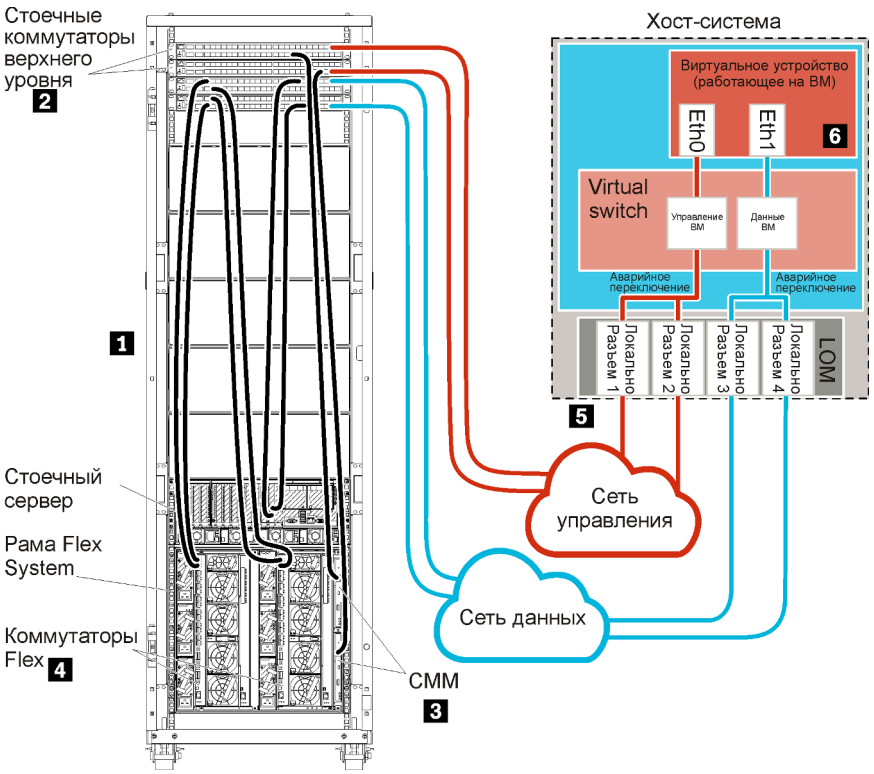


Рис. 12. Пример физически раздельных данных и топологии сети управления для виртуального устройства

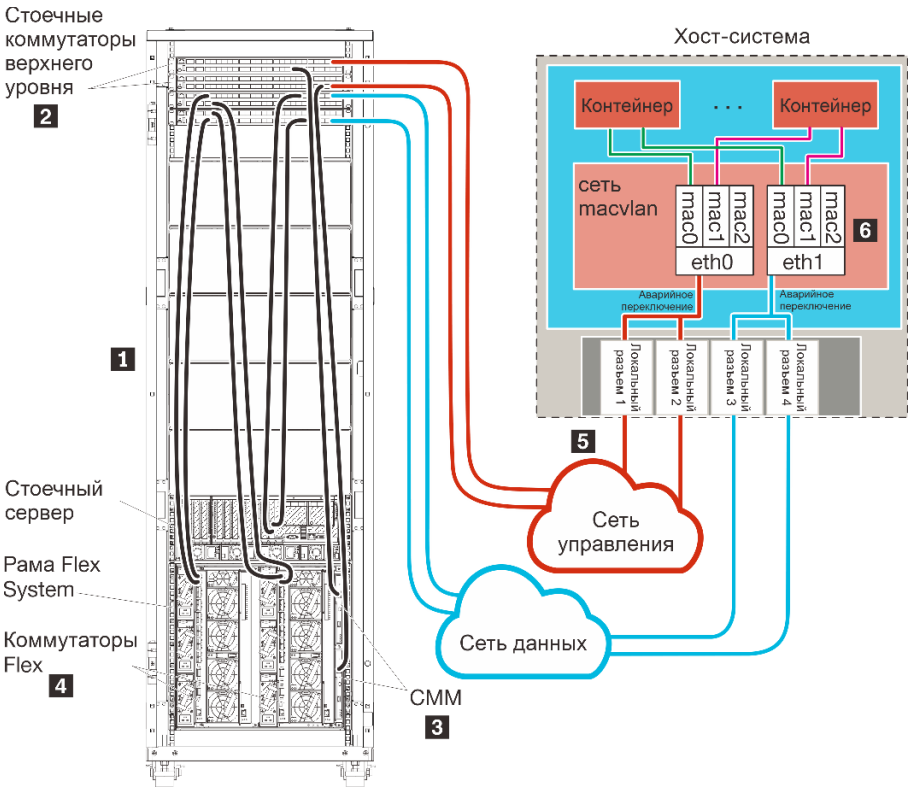


Рис. 13. Пример физически раздельных данных и топологии сети управления для контейнеров

Если вы планируете установить XClarity Administrator для управления уже имеющимися и настроенными рамами и стоечными серверами, перейдите к разделу Шаг 5. Установка и настройка хоста.

Дополнительные сведения о планировании этой топологии, включая информацию о параметрах сети и конфигурации Eth1 и Eth0, см. в разделе Физическое разделение сети данных и управления.

Шаг 1. Подключение рамы, стоечных серверов и хоста Lenovo XClarity Administrator к стоечным коммутаторам верхнего уровня

Подключите с помощью кабелей раму, стоечные серверы и хост XClarity Administrator к стоечным коммутаторам верхнего уровня, чтобы обеспечить связь между устройствами и вашими сетями.

Процедура

Подключите с помощью кабелей каждый коммутатор Flex и модуль CMM в каждой раме, каждый стоечный сервер и хост XClarity Administrator к обоим стоечным коммутаторам верхнего уровня. Для подключения можно использовать любые порты стоечных коммутаторов верхнего уровня.

На следующем рисунке приведен пример, иллюстрирующий подключение рамы (Коммутаторы Flex и модулей CMM), стоечных серверов и хоста XClarity Administrator с помощью кабелей к стоечным коммутаторам верхнего уровня.

Примечание: На этом рисунке не показаны все возможные варианты подключения, которые могут потребоваться для вашей среды. На этом рисунке демонстрируются только требования к подключению для коммутаторов Flex, модулей CMM и стоечных серверов, связанные с настройкой физически раздельных сетей данных и управления.

Совет. Вместо настройки двух физических коммутаторов, подключенных к каждой сети для обеспечения избыточности (четырех коммутаторов в общей сложности), можно настроить по одному физическому коммутатору, подключенному к каждой из сетей (в сумме два коммутатора). В этом случае каждый коммутатор будет подключен к обеим сетям, и потребуется задействовать две виртуальные локальные сети (VLAN) для разделения трафика данных: одну для сети передачи данных и одну для сети управления.

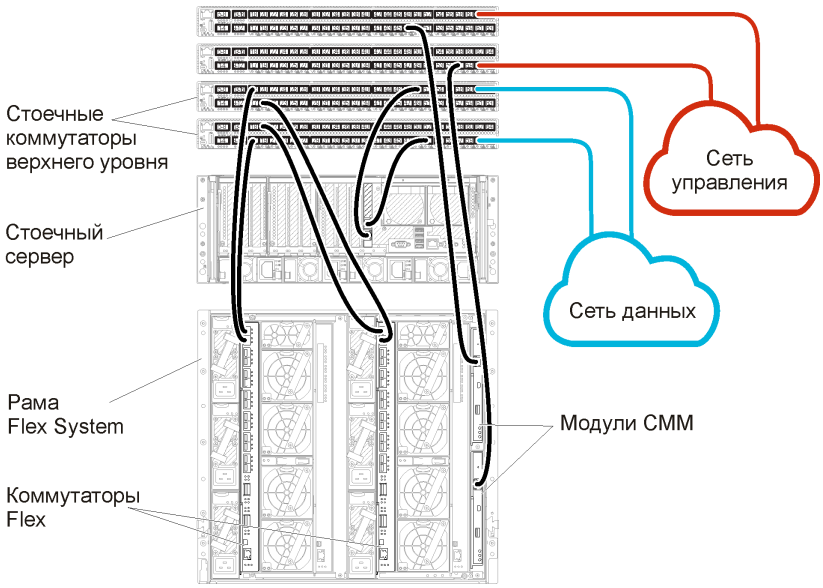


Рис. 14. Пример кабельных соединений для физически раздельных сетей данных и управления

Шаг 2. Настройка стоечных коммутаторов верхнего уровня

Настройте стоечные коммутаторы верхнего уровня.

Перед началом работы

В дополнение к обычным требованиям к конфигурации для стоечных коммутаторов верхнего уровня, убедитесь, что включены все необходимые порты, в том числе внешние порты для связи с Коммутаторы Flex, стоечными серверами и сетью, а также внутренние порты для связи с модулями CMM, стоечными серверами и сетью.

Процедура

Действия по настройке могут отличаться в зависимости от типа установленных стоечных коммутаторов.

Сведения о настройке стоечных коммутаторов верхнего уровня Lenovo см. в Стоечные коммутаторы в документации по System x в Интернете. Если установлен другой стоечный коммутатор верхнего уровня, см. документацию, сопровождающую этот коммутатор.

Шаг 3. Настройка модулей CMM

Настройте основной модуль управления рамой (Chassis Management Module, CMM) в раме для управления всеми устройствами в раме.

Об этой задаче

Подробные сведения о настройке модуля CMM см. в разделе Настройка компонентов рамы в документации по устройствам Flex System в Интернете.

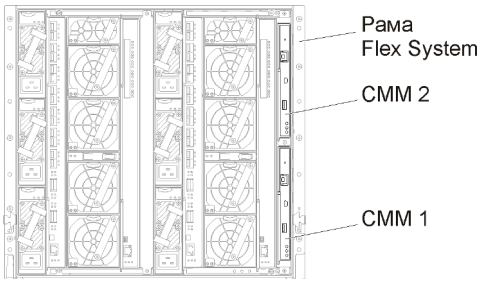
Также см. действия 4.1–4.5 на листе с инструкциями из комплекта поставки вашей рамы.

Процедура

Чтобы настроить модуль CMM, выполните указанные ниже действия.

Если установлены два модуля CMM, настройте только *основной* модуль CMM. Он автоматически синхронизирует конфигурацию с резервным модулем CMM.

Шаг 1. Подключите кабель Ethernet от модуля CMM в отсеке 1 к клиентской рабочей станции, чтобы создать прямое подключение.



При первом подключении к модулю CMM, возможно, потребуется изменить свойства протокола IP на клиентской рабочей станции.

Важно: Убедитесь, что подсеть клиентской рабочей станции совпадает с подсетью модуля CMM. (По умолчанию для CMM используется подсеть 255.255.255.0). IP-адрес, выбранный

для клиентской рабочей станции, должен находиться в той же сети, что и IP-адрес модуля CMM (например, 192.168.70.0–192.168.70.24).

Шаг 2. Чтобы запустить интерфейс управления CMM, откройте веб-браузер на клиентской рабочей станции и направьте его на IP-адрес модуля CMM.

Примечания:

- Убедитесь, что используется безопасное подключение, и включите **https** в URL-адрес (пример: https://192.168.70.100). Если не включить «https», отобразится ошибка «Страница не найдена».
- Если вы используете IP-адрес по умолчанию 192.168.70.100, интерфейс управления CMM может стать доступен спустя несколько минут. Эта задержка возникает из-за того, что модуль CMM пытается получить адрес DHCP в течение двух минут, прежде чем вернуться к статическому адресу по умолчанию.

Шаг 3. Войдите в интерфейс управления модуля CMM, используя принимаемые по умолчанию идентификатор пользователя `USERID` и пароль `PASSWORD`. После входа пароль по умолчанию необходимо изменить.

Шаг 4. Выполните шаги мастера первоначальной настройки CMM, чтобы указать сведения для своей среды. Мастер первоначальной настройки включает в себя следующие параметры:

- Просмотр ресурсов и состояния работоспособности рамы.
- Импорт конфигурации из существующего файла конфигурации.
- Настройка общих параметров CMM.
- Установка даты и времени CMM.

  Совет. При установке XClarity Administrator настройте использование сервера NTP для XClarity Administrator и всех рам, которыми управляет XClarity Administrator.
- Настройте IP-информацию модуля CMM.
- Настройте политику безопасности модуля CMM.
- Настройте систему доменных имен (DNS).
- Настройте средства перенаправления событий.

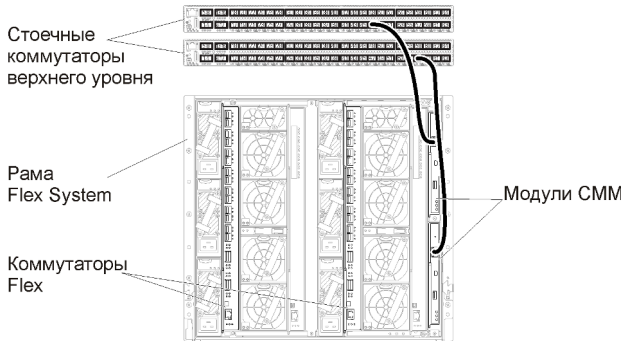
Шаг 5. Сохранив заданные значения параметров мастера настройки и применив изменения, настройте IP-адреса для всех компонентов в раме.

См. действие 4.6 на листе с инструкциями из комплекта поставки вашей рамы.

Примечание: Чтобы отобразились новые IP-адреса, необходимо сбросить процессор управления системой для каждого вычислительного узла и перезапустить коммутаторы Flex.

Шаг 6. Перезапустите модуль CMM с помощью интерфейса управления CMM.

Шаг 7. Пока модуль CMM перезапускается, подключите кабель от порта Ethernet модуля CMM к своей сети.



Шаг 8. Войдите в интерфейс управления модуля CMM, используя новый IP-адрес.

После завершения

В модуле CMM также можно настроить поддержку избыточности. Используйте справочную систему CMM, чтобы узнать больше о полях, доступных на каждой из следующих страниц.

- Настройте для модуля CMM аварийное переключение в случае аппаратного сбоя в основном модуле CMM. В интерфейсе управления CMM нажмите **Mgt Module Management → Свойства → Расширенное аварийное переключение**.
- Настройте аварийное переключение в случае неполадки с сетью (восходящий канал). В интерфейсе управления CMM нажмите **Mgt Module Management → Сеть**, откройте вкладку **Ethernet**, а затем нажмите **Дополнительные параметры Ethernet**. Как минимум, убедитесь, что выбран параметр **Переключение при утрате физического сетевого подключения**.

Шаг 4. Настройка Коммутаторы Flex

Настройте Коммутаторы Flex в каждой раме.

Перед началом работы

Убедитесь, что включены все необходимые порты, в том числе внешние порты для связи между коммутатором Flex и стоечным коммутатором верхнего уровня, а также внутренние порты для связи с модулем CMM.

Если в коммутаторах Flex настроено получение параметров динамической сети (IP-адреса, маски сети, шлюза и адреса DNS) посредством DHCP, убедитесь, что коммутаторы Flex имеют согласованные параметры (например, убедитесь, что IP-адреса находятся в одной подсети с IP-адресами модуля CMM).

Важно: Для каждой рамы Flex System убедитесь, что тип межкомпонентной сети карты расширения в каждом сервере в раме совместим с типом межкомпонентной сети всех коммутаторов Flex в этой же раме. Например, если в раме установлены коммутаторы Ethernet, все серверы в этой раме должны иметь возможность подключения к Ethernet с помощью разъема локальной сети на материнской плате или карты расширения Ethernet. Дополнительные сведения о настройке коммутаторов Flex см. в разделе Настройка модулей ввода-вывода в документации по устройствам Flex System в Интернете.

Процедура

Действия по настройке могут отличаться в зависимости от типа установленных Коммутаторы Flex. Дополнительную информацию о каждом из поддерживаемых Коммутаторы Flex см. в Сетевые коммутаторы Flex System в документации по устройствам Flex System в Интернете.

Как правило, требуется настроить коммутаторы Flex в отсеках 1 и 2 для коммутаторов Flex.

Совет. Отсек 2 для коммутатора Flex — это третий по счету модульный отсек, если смотреть на раму с тыльной стороны.

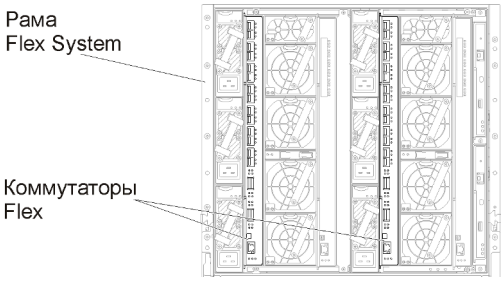


Рис. 15. Места установки Коммутатор Flexв раме

Шаг 5. Установка и настройка хоста

Docker можно установить на любом сервере, который отвечает требованиям для Lenovo XClarity Administrator

Перед началом работы

Docker Datacenter можно использовать для настройки среды высокой доступности для контейнеров XClarity Administrator, работающих под управлением Docker Engine. Дополнительные сведения о высокой доступности на базе Docker Datacenter см. в разделе Веб-страница архитектуры высокой доступности и приложений с Docker Datacenter.

Убедитесь, что хост отвечает предварительным требованиям, которые определены в разделе Обязательные требования к оборудованию и программному обеспечению.

Убедитесь, что система хоста находится в той же сети, что и устройства, которыми вы хотите управлять.

Важно: XClarity Administrator можно установить на любой системе, отвечающей требованиям для XClarity Administrator, в том числе на управляемом сервере. Если для хоста XClarity Administrator используется управляемый сервер:

- Необходимо реализовать либо топологию с виртуальным разделением сети данных и сети управления, либо топологию с единой сетью данных и управления.
- Для применения обновлений микропрограммы к этому управляемому серверу невозможно использовать XClarity Administrator. Даже если только часть микропрограммного обеспечения применяется с немедленной активацией, XClarity Administrator принудительно перезапускает целевой сервер, что приводит к перезапуску XClarity Administrator. Если используется отложенная активация, при перезапуске XClarity Administrator применяются только некоторые части микропрограммы.
- Если вы используете сервер в раме Flex System, убедитесь, что на сервере настроено автоматическое включение. Этот параметр можно установить из веб-интерфейса CMM, нажав **Управление рамой → Вычислительные узлы**, выбрав сервер и выбрав **Автоматическое включение/выключение питания** для параметра **Режим автоматического включения**.

Процедура

Установите и настройте Docker на хосте согласно инструкциям, предоставляемым с дистрибутивом Docker.

Шаг 6. Установка и настройка XClarity Administrator

Установите и настройте контейнер Lenovo XClarity Administrator на только что установленном хосте Docker.

Перед началом работы

Убедитесь, что хост-система отвечает минимальным требованиям к оборудованию и программному обеспечению (см. раздел Обязательные требования к оборудованию и программному обеспечению).

Убедитесь, что включены все соответствующие порты, включая порты, которые требуются XClarity Administrator (см. раздел Доступность портов).

Убедитесь, что система хоста находится в той же сети, что и устройства, которыми вы хотите управлять.

Убедитесь, что ОС хоста и XClarity Administrator используют один и тот же сервер NTP.

XClarity Administrator позволяет использовать пользовательское имя сети для управления данными и оборудованием, а также развертывания ОС (см. раздел Конфигурации сети). В этом примере в следующей процедуре используется eth0.

XClarity Administrator позволяет использовать пользовательское имя сети для управления данными и оборудованием, а также сети, используемой для развертывания ОС (см. раздел Конфигурации сети). В этом примере в следующей процедуре используются eth0 и eth1 соответственно

Убедитесь, что сеть macvlan загружена в ядро хост-системы. Чтобы проверить, загружена ли она, воспользуйтесь командой **lsmod | grep macvlan**. Чтобы загрузить macvlan в ядро, выполните команду **modprobe macvlan**.

При запуске нескольких контейнеров XClarity Administrator в одном хосте следует использовать уникальное имя и IP-адрес для каждого контейнера.

Если вы предполагаете управлять ThinkServer и другими устаревшими устройствами, убедитесь, что в Docker включена поддержка IPv6.

1. Внесите следующие изменения в файл /etc/docker/daemon.json: установите значение «true» для ключа **ipv6** и укажите вашу подсеть IPv6 в качестве значения ключа **fixed-cidr-v6**. Пример файла daemon представлен ниже.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Перезагрузите файл конфигурации Docker, выполнив указанную ниже команду.
```
systemctl reload docker
```

Примечание: XClarity Administrator *не* работает в качестве привилегированного контейнера.

Процедура

Чтобы установить контейнер XClarity Administrator с помощью Docker compose, выполните следующие шаги.

Шаг 1. Скачайте образ виртуального устройства XClarity Administrator, файла среды и YAML-файла с Веб-страница загрузки XClarity Administrator на клиентскую рабочую станцию. Войдите на веб-сайт и используйте предоставленный вам ключ доступа для скачивания образа.

Шаг 2. Импортируйте образ контейнера XClarity Administrator в хост docker, выполнив следующую команду.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Шаг 3. Отредактируйте файл `docker_compose.env` и измените следующие переменные среды.

- **CONTAINER_NAME**. Уникальное имя контейнера, используемое для создания томов Docker для каждого экземпляра XClarity Administrator (например, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Статический адрес IPv4 для контейнера (например, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Необязательно) Путь удаленного общего ресурса, который можно использовать для хранения резервных копий XClarity Administrator. Он должен иметь вид `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Необязательно) Путь к удаленному общему ресурсу, который можно использовать в качестве удаленного репозитория для обновлений микропрограмм. Он должен иметь вид `/mnt/fw_share`.

Ниже приведен пример файла среды.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Шаг 4. Измените файл `docker_compose.yml` и измените следующие свойства.

- Задайте значение свойства **image** равным имени файла установочного образа, используемому в шаге 2.

  Примечание: Имя файла образа можно изменить (например, на latest) с помощью команды `docker tag`.
- Если необходимо использовать удаленные общие ресурсы в качестве удаленного репозитория микропрограмм и для хранения резервных копий XClarity Administrator, задайте точку подключения хоста для каждого удаленного общего ресурса в свойстве **volumes**.
- Установите в качестве значения свойства **dns** IP-адрес серверов DNS.
- Этот контейнер использует тот же пул ресурсов процессора, памяти и хранения, которые доступны хосту. При необходимости определите ограничения использования ресурсов, настроив свойства **cpus** и **memory**.
- Задайте значение свойства **parent** равным имени сетевого интерфейса в хост-системе, который следует использовать в качестве родительского для интерфейса macvlan в контейнере. Этот интерфейс должен иметь прямой доступ к подсети, назначенной контейнеру.
- Задайте свойства **subnet (подсеть)** и **gateway (шлюз)** в соответствии с топологией вашей сети. Как правило, подсеть и шлюз предназначены для сети управления, к которой относится ${ADDRESS}.
- Если требуется поддержка IPv6, задайте для свойства **enable_ipv6** значение «true», укажите адрес IPv6 в качестве значения свойства **ipv6_address** и добавьте еще один набор свойств **subnet** и **gateway** в соответствии с топологией вашей сети (обычно для сети управления, к которой принадлежит адрес IPv6).

Ниже представлен пример файла YML с включенной поддержкой IPv6.

```
version: '3.8'
```

```
services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
```

```
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
        - subnet: "2001:8003:7d51:2005::/80"
```

Шаг 5. Разверните образ в Docker, выполнив следующую команду, где <*ENV_FILENAME*> — имя файла переменных среды, созданного в шаге 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

После завершения

Войдите в систему и настройте XClarity Administrator (см. разделы Доступ к веб-интерфейсу Lenovo XClarity Administrator в первый раз и Настройка Lenovo XClarity Administrator).

Топология виртуально разделенных сетей данных и управления

В этой топологии сеть передачи данных и сеть управления виртуально разделены. Пакеты из сети передачи данных и пакеты из сети управления отправляются через одно физическое подключение. Для разделения трафика двух сетей во всех пакетах данных сети управления используется добавление меток виртуальной локальной сети (меток VLAN).

Перед началом работы

Убедитесь, что включены все соответствующие порты, включая порты, которые требуются XClarity Administrator (см. раздел Доступность портов).

Убедитесь, что на каждом устройстве, которым предполагается управлять с помощью XClarity Administrator, установлена микропрограмма, удовлетворяющая минимальным требованиям. Минимально необходимые уровни микропрограммы можно найти в Веб-страница поддержки XClarity Administrator — совместимость, открыв вкладку **Совместимость** и щелкнув ссылку для соответствующих типов устройств.

Убедитесь, что для сети данных и сети управления настроены идентификаторы VLAN. При необходимости включите добавление меток VLAN из Коммутаторы Flex (если вы реализуете добавление меток из Коммутаторы Flex) или из стоечных коммутаторов верхнего уровня (если вы реализуете добавление меток из стоечных коммутаторов верхнего уровня).

Обязательно определите порты, к которым подключены модули CMM, как принадлежащие к сети VLAN управления.

Важно: Настройте устройства и компоненты таким образом, чтобы свести к минимуму изменения IP-адресов. Рассмотрите возможность использования статических IP-адресов вместо протокола динамической настройки хостов (DHCP). Если используется протокол DHCP, убедитесь, что изменения IP-адреса сведены к минимуму.

Об этой задаче

На рисунке ниже показан один из способов настройки среды, при котором сеть управления отделена от виртуальной сети. Цифры на рисунке соответствуют пронумерованным шагам, описанным в следующих разделах.

Примечание: На этом рисунке не показаны все возможные варианты подключения, которые могут потребоваться для вашей среды. На этом рисунке демонстрируются только требования к подключению для коммутаторов Flex, модулей CMM и стоечных серверов, связанные с настройкой виртуально раздельных сетей данных и управления.

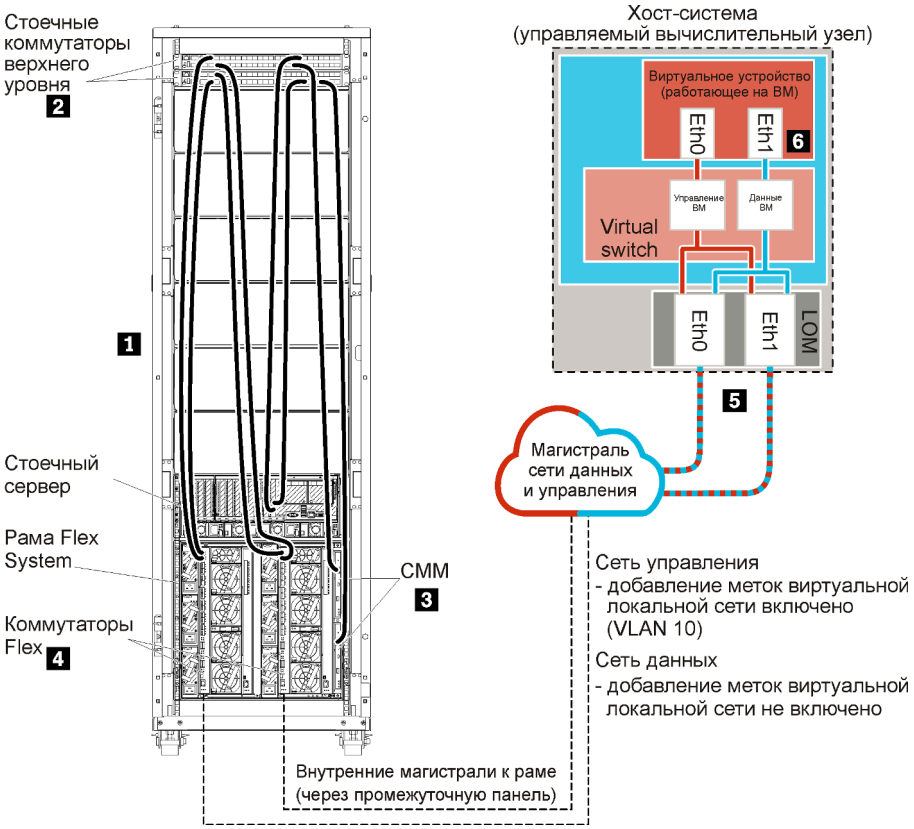


Рис. 16. Пример виртуально раздельных данных и топологии сети управления для виртуального устройства

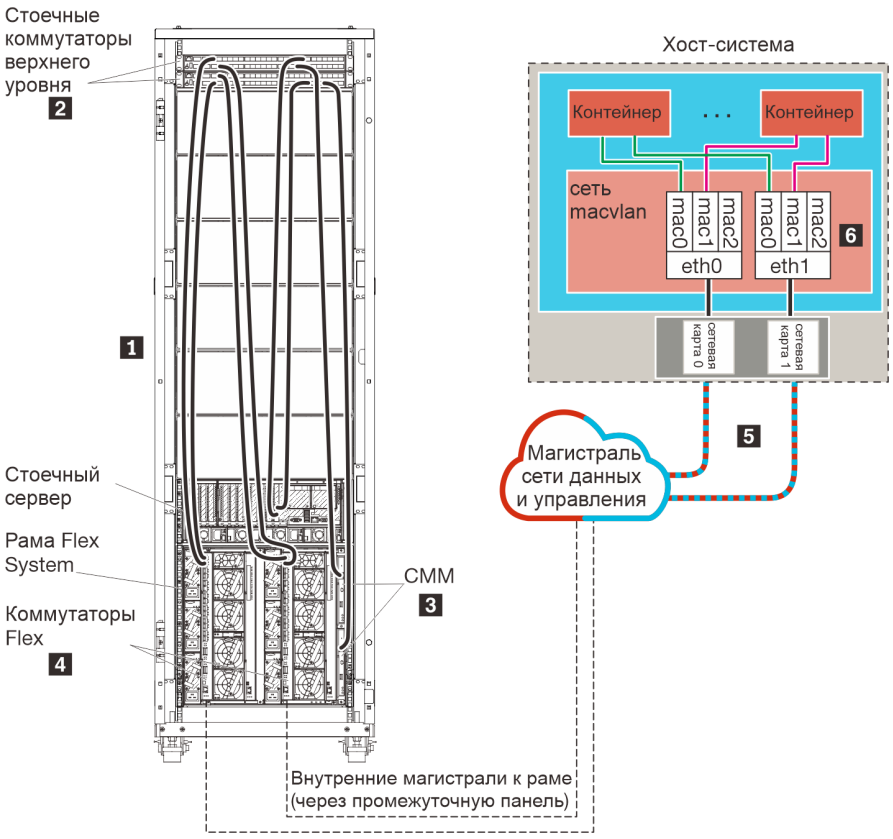


Рис. 17. Пример виртуально раздельных данных и топологии сети управления для контейнеров

В этом сценарии XClarity Administrator установлен на сервере в раме Flex System, которой управляет XClarity Administrator.

Важно: XClarity Administrator можно установить на любой системе, отвечающей требованиям для XClarity Administrator, в том числе на управляемом сервере. Если для хоста XClarity Administrator используется управляемый сервер:

- Необходимо реализовать либо топологию с виртуальным разделением сети данных и сети управления, либо топологию с единой сетью данных и управления.
- Для применения обновлений микропрограммы к этому управляемому серверу невозможно использовать XClarity Administrator. Даже если только часть микропрограммного обеспечения применяется с немедленной активацией, XClarity Administrator принудительно перезапускает целевой сервер, что приводит к перезапуску XClarity Administrator. Если используется отложенная активация, при перезапуске XClarity Administrator применяются только некоторые части микропрограммы.
- Если вы используете сервер в раме Flex System, убедитесь, что на сервере настроено автоматическое включение. Этот параметр можно установить из веб-интерфейса CMM, нажав **Управление рамой → Вычислительные узлы**, выбрав сервер и выбрав **Автоматическое включение/выключение питания** для параметра **Режим автоматического включения**.

Кроме того, в этом сценарии для передачи всех данных используются одни и те же физические подключения. Сеть управления отделяется от сети данных за счет добавления меток виртуальной локальной сети: определенные метки, которые соответствуют сети управления, добавляются ко входящим пакетам данных, и те направляются на соответствующие интерфейсы. Из исходящих пакетов данных метки удаляются.

Добавление меток виртуальной локальной сети (меток VLAN) можно включить на одном из следующих устройств:

- **Стоечные коммутаторы верхнего уровня**. Метки VLAN, соответствующие сети управления, добавляются к пакетам, когда те поступают на стоечный коммутатор верхнего уровня, после чего они проходят через Коммутаторы Flex и отправляются на серверы в раме Flex System. На обратном маршруте метки VLAN удаляются при отправке со стоечного коммутатора верхнего уровня на контроллеры управления.
- **Коммутаторы Flex**. Метки VLAN, соответствующие сети управления, добавляются к пакетам, когда те поступают на Коммутаторы Flex, после чего они отправляются на серверы в раме Flex System. На обратном маршруте метки VLAN добавляются серверами и отправляются на Коммутаторы Flex, где метки удаляются из пакетов при их пересылке на контроллеры управления.

Решение о том, следует ли применять добавление меток виртуальной локальной сети, зависит от потребностей и сложности вашей среды.

Если вы планируете установить XClarity Administrator для управления уже имеющимися и настроенными рамами и стоечными серверами, перейдите к разделу Шаг 5. Установка и настройка хоста.

Дополнительные сведения о планировании этой топологии, включая информацию о параметрах сети и конфигурации Eth1 и Eth0, см. в разделе Виртуальное разделение сети данных и управления.

Шаг 1. Подключение рамы и стоечных серверов к стоечным коммутаторам верхнего уровня

Подключите с помощью кабелей раму и стоечные серверы к одному стоечному коммутатору верхнего уровня, чтобы обеспечить связь между устройствами.

Процедура

Подключите с помощью кабелей каждый коммутатор Flex и модуль CMM в каждой раме и каждый стоечный сервер к обоим стоечным коммутаторам верхнего уровня. Для подключения можно использовать любые порты этого стоечного коммутатора верхнего уровня.

На следующем рисунке приведен пример, иллюстрирующий подключение рамы (коммутаторов Flex и модулей CMM) и стоечных серверов с помощью кабелей к стоечным коммутаторам верхнего уровня для случая, когда Lenovo XClarity Administrator установлен на сервере в раме, которой будет управлять XClarity Administrator.

Примечание: На этом рисунке не показаны все возможные варианты подключения, которые могут потребоваться для вашей среды. На этом рисунке демонстрируются только требования к подключению для коммутаторов Flex, модулей CMM и стоечных серверов, связанные с настройкой виртуально раздельных сетей данных и управления.

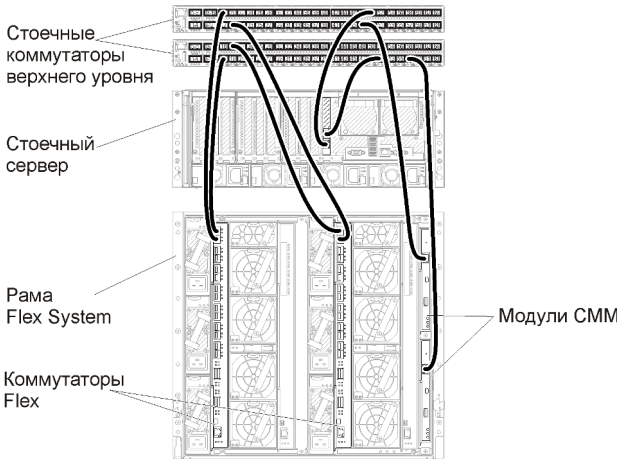


Рис. 18. Пример кабельных соединений для виртуально раздельных сетей данных и управления

Шаг 2. Настройка стоечных коммутаторов верхнего уровня

Настройте стоечные коммутаторы верхнего уровня.

Перед началом работы

В дополнение к обычным требованиям к конфигурации для стоечных коммутаторов верхнего уровня, убедитесь, что включены все необходимые порты, в том числе внешние порты для связи с Коммутаторы Flex, стоечными серверами и сетью, а также внутренние порты для связи с модулями CMM, стоечными серверами и сетью.

Добавление меток виртуальной локальной сети можно реализовать в коммутаторах Flex или стоечных коммутаторах верхнего уровня, что зависит от потребностей и сложности среды. Если добавление меток реализуется в стоечных коммутаторах верхнего уровня, включите добавление меток VLAN в стоечных коммутаторах верхнего уровня.

Убедитесь, что для сети управления и сети данных настроены идентификаторы VLAN.

Процедура

Действия по настройке могут отличаться в зависимости от типа установленных стоечных коммутаторов.

На следующем рисунке показан пример сценария, в котором добавление меток VLAN реализовано в стоечных коммутаторах верхнего уровня и включено только в сети управления. Сеть VLAN управления настроена как сеть VLAN 10.

В этом сценарии порты, к которым подключены модули CMM, необходимо определить как принадлежащие к сети VLAN управления.

Примечание: Добавление меток VLAN также можно включить в сети данных для настройки сети VLAN для данных.

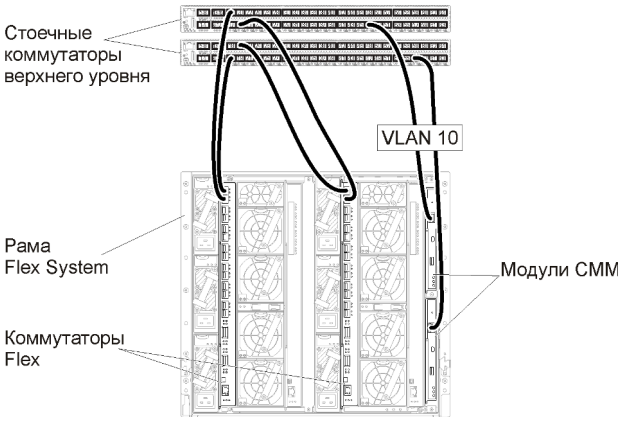


Рис. 19. Пример конфигурации для Коммутаторы Flex в виртуально разделенных сетях данных и управления (VMware ESXi), в которой добавление меток VLAN включено в сети управления

Сведения о настройке стоечных коммутаторов верхнего уровня Lenovo см. в Стоечные коммутаторы в документации по System x в Интернете. Если установлен другой стоечный коммутатор верхнего уровня, см. документацию, сопровождающую этот коммутатор.

Шаг 3. Настройка модулей CMM

Настройте основной модуль управления рамой (Chassis Management Module, CMM) в раме для управления всеми устройствами в раме.

Об этой задаче

Подробные сведения о настройке модуля CMM см. в разделе Настройка компонентов рамы в документации по устройствам Flex System в Интернете.

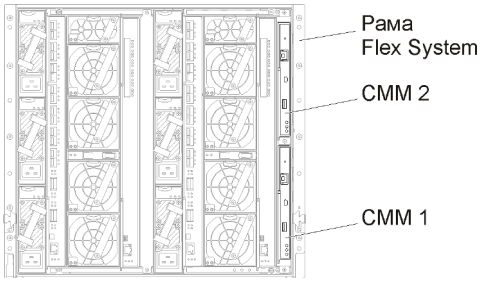
Также см. действия 4.1–4.5 на листе с инструкциями из комплекта поставки вашей рамы.

Процедура

Чтобы настроить модуль CMM, выполните указанные ниже действия.

Если установлены два модуля CMM, настройте только *основной* модуль CMM. Он автоматически синхронизирует конфигурацию с резервным модулем CMM.

Шаг 1. Подключите кабель Ethernet от модуля CMM в отсеке 1 к клиентской рабочей станции, чтобы создать прямое подключение.



При первом подключении к модулю CMM, возможно, потребуется изменить свойства протокола IP на клиентской рабочей станции.

Важно: Убедитесь, что подсеть клиентской рабочей станции совпадает с подсетью модуля CMM. (По умолчанию для CMM используется подсеть 255.255.255.0). IP-адрес, выбранный для клиентской рабочей станции, должен находиться в той же сети, что и IP-адрес модуля CMM (например, 192.168.70.0–192.168.70.24).

Шаг 2. Чтобы запустить интерфейс управления CMM, откройте веб-браузер на клиентской рабочей станции и направьте его на IP-адрес модуля CMM.

Примечания:

- Убедитесь, что используется безопасное подключение, и включите **https** в URL-адрес (пример: https://192.168.70.100). Если не включить «https», отобразится ошибка «Страница не найдена».
- Если вы используете IP-адрес по умолчанию 192.168.70.100, интерфейс управления CMM может стать доступен спустя несколько минут. Эта задержка возникает из-за того, что модуль CMM пытается получить адрес DHCP в течение двух минут, прежде чем вернуться к статическому адресу по умолчанию.

Шаг 3. Войдите в интерфейс управления модуля CMM, используя принимаемые по умолчанию идентификатор пользователя `USERID` и пароль `PASSWORD`. После входа пароль по умолчанию необходимо изменить.

Шаг 4. Выполните шаги мастера первоначальной настройки CMM, чтобы указать сведения для своей среды. Мастер первоначальной настройки включает в себя следующие параметры:

- Просмотр ресурсов и состояния работоспособности рамы.
- Импорт конфигурации из существующего файла конфигурации.
- Настройка общих параметров CMM.
- Установка даты и времени CMM.

  Совет. При установке XClarity Administrator настройте использование сервера NTP для XClarity Administrator и всех рам, которыми управляет XClarity Administrator.
- Настройте IP-информацию модуля CMM.
- Настройте политику безопасности модуля CMM.
- Настройте систему доменных имен (DNS).
- Настройте средства перенаправления событий.

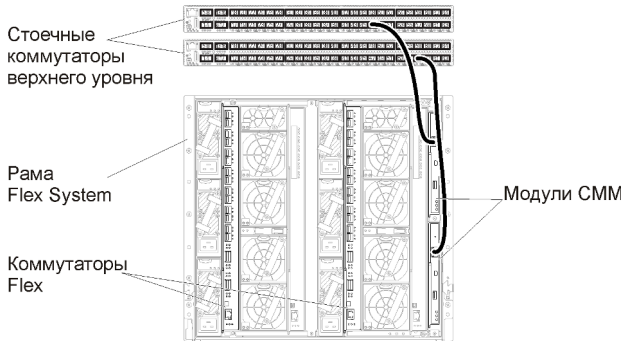
Шаг 5. Сохранив заданные значения параметров мастера настройки и применив изменения, настройте IP-адреса для всех компонентов в раме.

См. действие 4.6 на листе с инструкциями из комплекта поставки вашей рамы.

Примечание: Чтобы отобразились новые IP-адреса, необходимо сбросить процессор управления системой для каждого вычислительного узла и перезапустить коммутаторы Flex.

Шаг 6. Перезапустите модуль CMM с помощью интерфейса управления CMM.

Шаг 7. Пока модуль CMM перезапускается, подключите кабель от порта Ethernet модуля CMM к своей сети.



Шаг 8. Войдите в интерфейс управления модуля CMM, используя новый IP-адрес.

После завершения

В модуле CMM также можно настроить поддержку избыточности. Используйте справочную систему CMM, чтобы узнать больше о полях, доступных на каждой из следующих страниц.

- Настройте для модуля CMM аварийное переключение в случае аппаратного сбоя в основном модуле CMM. В интерфейсе управления CMM нажмите **Mgt Module Management → Свойства → Расширенное аварийное переключение**.
- Настройте аварийное переключение в случае неполадки с сетью (восходящий канал). В интерфейсе управления CMM нажмите **Mgt Module Management → Сеть**, откройте вкладку **Ethernet**, а затем нажмите **Дополнительные параметры Ethernet**. Как минимум, убедитесь, что выбран параметр **Переключение при утрате физического сетевого подключения**.

Шаг 4. Настройка Коммутаторы Flex

Настройте Коммутаторы Flex в каждой раме.

Перед началом работы

Убедитесь, что включены все необходимые порты, в том числе внешние порты для связи между коммутатором Flex и стоечным коммутатором верхнего уровня, а также внутренние порты для связи с модулем CMM.

Добавление меток виртуальной локальной сети можно реализовать в коммутаторах Flex или стоечных коммутаторах верхнего уровня, что зависит от потребностей и сложности среды. Если добавление меток реализуется в коммутаторах Flex, включите добавление меток VLAN в коммутаторах Flex.

Убедитесь, что для сети управления и сети данных настроены идентификаторы VLAN.

Важно: Для каждой рамы Flex System убедитесь, что тип межкомпонентной сети карты расширения в каждом сервере в раме совместим с типом межкомпонентной сети всех коммутаторов Flex в этой же раме. Например, если в раме установлены коммутаторы Ethernet, все серверы в этой раме должны иметь возможность подключения к Ethernet с помощью разъема локальной сети на материнской плате или карты расширения Ethernet. Дополнительные сведения о настройке коммутаторов Flex см. в разделе Настройка модулей ввода-вывода в документации по устройствам Flex System в Интернете.

Процедура

Действия по настройке могут отличаться в зависимости от типа установленных Коммутаторы Flex. Дополнительную информацию о каждом из поддерживаемых Коммутаторы Flex см. в Сетевые коммутаторы Flex System в документации по устройствам Flex System в Интернете.

На следующем рисунке показан пример сценария, в котором добавление меток VLAN реализовано в коммутаторах Flex и включено только в сети управления. Сеть VLAN управления настроена как сеть VLAN 10.

Примечание: Включив добавление меток VLAN в сети данных, можно настроить сеть VLAN для данных.

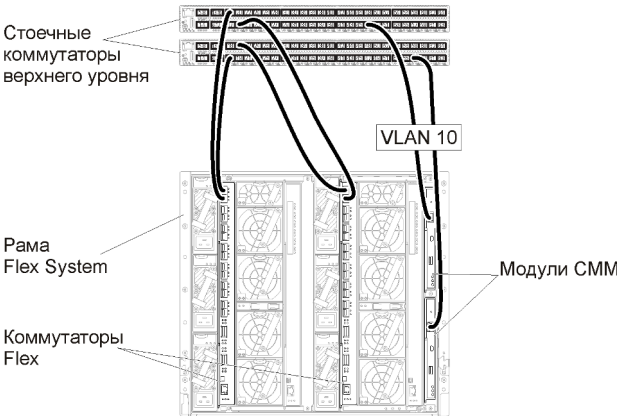


Рис. 20. Пример конфигурации для Коммутаторы Flex в виртуально разделенных сетях данных и управления (VMware ESXi), в которой добавление меток VLAN включено в сети управления

Чтобы настроить коммутаторы Flex для этого сценария, выполните указанные ниже действия.

Шаг 1. Настройте коммутатор Flex в отсеке 1 для коммутатора Flex:

a. Определите сеть VLAN управления (в этом примере выбрана сеть VLAN 10) таким образом, чтобы она содержала внешний порт, подключенный с помощью кабеля к стоечному коммутатору верхнего уровня (Ext1).

b. Определите внутренний порт как часть сети VLAN 10 (сеть VLAN управления). Убедитесь, что на этом порту включен транкинг VLAN.

Шаг 2. Настройте коммутатор Flex в отсеке 2 для коммутатора Flex:

Совет. Отсек 2 для коммутатора Flex — это третий по счету модульный отсек, если смотреть на раму с обратной стороны.

a. Определите сеть VLAN управления (в этом примере выбрана сеть VLAN 10) таким образом, чтобы она содержала внешний порт, подключенный с помощью кабеля к стоечному коммутатору верхнего уровня.

b. Определите внутренний порт как часть сети VLAN 10 (сеть VLAN управления). Убедитесь, что на этом порту включен транкинг VLAN.

Шаг 5. Установка и настройка хоста

Docker можно установить в любой системе, которая отвечает требованиям для Lenovo XClarity Administrator.

Перед началом работы

Docker Datacenter можно использовать для настройки среды высокой доступности для контейнеров XClarity Administrator, работающих под управлением Docker Engine. Дополнительные сведения о высокой доступности на базе Docker Datacenter см. в разделе Веб-страница архитектуры высокой доступности и приложений с Docker Datacenter.

Убедитесь, что хост отвечает предварительным требованиям, которые определены в разделе Обязательные требования к оборудованию и программному обеспечению.

Убедитесь, что система хоста находится в той же сети, что и устройства, которыми вы хотите управлять.

Важно: XClarity Administrator можно установить на любой системе, отвечающей требованиям для XClarity Administrator, в том числе на управляемом сервере. Если для хоста XClarity Administrator используется управляемый сервер:

- Необходимо реализовать либо топологию с виртуальным разделением сети данных и сети управления, либо топологию с единой сетью данных и управления.
- Для применения обновлений микропрограммы к этому управляемому серверу невозможно использовать XClarity Administrator. Даже если только часть микропрограммного обеспечения применяется с немедленной активацией, XClarity Administrator принудительно перезапускает целевой сервер, что приводит к перезапуску XClarity Administrator. Если используется отложенная активация, при перезапуске XClarity Administrator применяются только некоторые части микропрограммы.
- Если вы используете сервер в раме Flex System, убедитесь, что на сервере настроено автоматическое включение. Этот параметр можно установить из веб-интерфейса CMM, нажав **Управление рамой → Вычислительные узлы**, выбрав сервер и выбрав **Автоматическое включение/выключение питания** для параметра **Режим автоматического включения**.

Процедура

Установите и настройте Docker на хосте согласно инструкциям, предоставляемым с дистрибутивом Docker.

Шаг 6. Установка и настройка XClarity Administrator

Установите и настройте контейнер Lenovo XClarity Administrator на только что установленном хосте Docker.

Перед началом работы

Убедитесь, что хост-система отвечает минимальным требованиям к оборудованию и программному обеспечению (см. раздел Обязательные требования к оборудованию и программному обеспечению).

Убедитесь, что включены все соответствующие порты, включая порты, которые требуются XClarity Administrator (см. раздел Доступность портов).

Убедитесь, что система хоста находится в той же сети, что и устройства, которыми вы хотите управлять.

Убедитесь, что ОС хоста и XClarity Administrator используют один и тот же сервер NTP.

XClarity Administrator позволяет использовать пользовательское имя сети для управления данными и оборудованием, а также развертывания ОС (см. раздел Конфигурации сети). В этом примере в следующей процедуре используется eth0.

XClarity Administrator позволяет использовать пользовательское имя сети для управления данными и оборудованием, а также сети, используемой для развертывания ОС (см. раздел Конфигурации сети). В этом примере в следующей процедуре используются eth0 и eth1 соответственно.

Убедитесь, что сеть macvlan загружена в ядро хост-системы. Чтобы проверить, загружена ли она, воспользуйтесь командой **lsmod | grep macvlan**. Чтобы загрузить macvlan в ядро, выполните команду **modprobe macvlan**.

При запуске нескольких контейнеров XClarity Administrator в одном хосте следует использовать уникальное имя и IP-адрес для каждого контейнера.

Если вы предполагаете управлять ThinkServer и другими устаревшими устройствами, убедитесь, что в Docker включена поддержка IPv6.

1. Внесите следующие изменения в файл /etc/docker/daemon.json: установите значение «true» для ключа **ipv6** и укажите вашу подсеть IPv6 в качестве значения ключа **fixed-cidr-v6**. Пример файла daemon представлен ниже.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Перезагрузите файл конфигурации Docker, выполнив указанную ниже команду.
```
systemctl reload docker
```

Примечание: XClarity Administrator *не* работает в качестве привилегированного контейнера.

Процедура

Чтобы установить контейнер XClarity Administrator с помощью Docker compose, выполните следующие шаги.

Шаг 1. Скачайте образ виртуального устройства XClarity Administrator, файла среды и YAML-файла с Веб-страница загрузки XClarity Administrator на клиентскую рабочую станцию. Войдите на веб-сайт и используйте предоставленный вам ключ доступа для скачивания образа.

Шаг 2. Импортируйте образ контейнера XClarity Administrator в хост docker, выполнив следующую команду.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Шаг 3. Отредактируйте файл `docker_compose.env` и измените следующие переменные среды.

- **CONTAINER_NAME**. Уникальное имя контейнера, используемое для создания томов Docker для каждого экземпляра XClarity Administrator (например, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Статический адрес IPv4 для контейнера (например, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Необязательно) Путь удаленного общего ресурса, который можно использовать для хранения резервных копий XClarity Administrator. Он должен иметь вид `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Необязательно) Путь к удаленному общему ресурсу, который можно использовать в качестве удаленного репозитория для обновлений микропрограмм. Он должен иметь вид `/mnt/fw_share`.

Ниже приведен пример файла среды.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Шаг 4. Измените файл `docker_compose.yml` и измените следующие свойства.

- Задайте значение свойства **image** равным имени файла установочного образа, используемому в шаге 2.

Примечание: Имя файла образа можно изменить (например, на latest) с помощью команды `docker tag`.

- Если необходимо использовать удаленные общие ресурсы в качестве удаленного репозитория микропрограмм и для хранения резервных копий XClarity Administrator, задайте точку подключения хоста для каждого удаленного общего ресурса в свойстве **volumes**.
- Установите в качестве значения свойства **dns** IP-адрес серверов DNS.
- Этот контейнер использует тот же пул ресурсов процессора, памяти и хранения, которые доступны хосту. При необходимости определите ограничения использования ресурсов, настроив свойства **cpus** и **memory**.
- Задайте значение свойства **parent** равным имени сетевого интерфейса в хост-системе, который следует использовать в качестве родительского для интерфейса macvlan в контейнере. Этот интерфейс должен иметь прямой доступ к подсети, назначенной контейнеру.
- Задайте свойства **subnet (подсеть)** и **gateway (шлюз)** в соответствии с топологией вашей сети. Как правило, подсеть и шлюз предназначены для сети управления, к которой относится ${ADDRESS}.
- Если требуется поддержка IPv6, задайте для свойства **enable_ipv6** значение «true», укажите адрес IPv6 в качестве значения свойства **ipv6_address** и добавьте еще один набор свойств **subnet** и **gateway** в соответствии с топологией вашей сети (обычно для сети управления, к которой принадлежит адрес IPv6).

Ниже представлен пример файла YML с включенной поддержкой IPv6.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
```

```
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
          gateway: 192.0.122.1
        - subnet: "2001:8003:7d51:2003::/80"
          gateway: "2001:8003:7d51:2003::1"
```

Шаг 5. Разверните образ в Docker, выполнив следующую команду, где <*ENV_FILENAME*> — имя файла переменных среды, созданного в шаге 2.
COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file` <*ENV_FILENAME*> `up -d`

После завершения

Войдите в систему и настройте XClarity Administrator (см. разделы Доступ к веб-интерфейсу Lenovo XClarity Administrator в первый раз и Настройка Lenovo XClarity Administrator).

Топология сети только для управления

В этой топологии у Lenovo XClarity Administrator есть только сеть управления. Сеть данных отсутствует.

Перед началом работы

Убедитесь, что включены все необходимые порты, в том числе:
- Порты, которые требуются для XClarity Administrator (см. раздел Доступность портов)
- Внешние порты для связи по сети
- Внутренние порты для связи с модулем CMM

Убедитесь, что на каждом устройстве, которым предполагается управлять с помощью XClarity Administrator, установлена микропрограмма, удовлетворяющая минимальным требованиям. Минимально необходимые уровни микропрограммы можно найти в Веб-страница поддержки XClarity Administrator — совместимость, открыв вкладку **Совместимость** и щелкнув ссылку для соответствующих типов устройств.

Важно: Настройте устройства и компоненты таким образом, чтобы свести к минимуму изменения IP-адресов. Рассмотрите возможность использования статических IP-адресов вместо протокола динамической настройки хостов (DHCP). Если используется протокол DHCP, убедитесь, что изменения IP-адреса сведены к минимуму.

Об этой задаче

На рисунке ниже показан один из способов настройки среды в том случае, когда у Lenovo XClarity Administrator есть только сеть управления (сети данных нет). Цифры на рисунке соответствуют пронумерованным шагам, описанным в следующих разделах.

Примечание: На этом рисунке не показаны все возможные варианты подключения, которые могут потребоваться для вашей среды. На этом рисунке демонстрируются только требования к подключению для коммутаторов Flex, модулей CMM и стоечных серверов, связанные с настройкой сети только для управления.

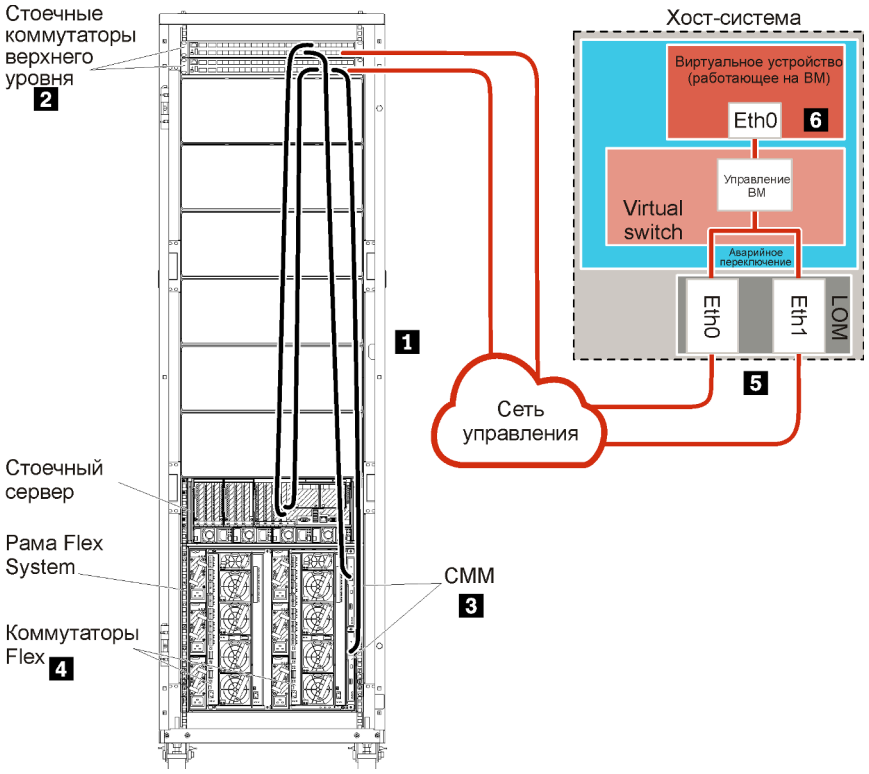


Рис. 21. Пример топологии сети только для управления для виртуального устройства

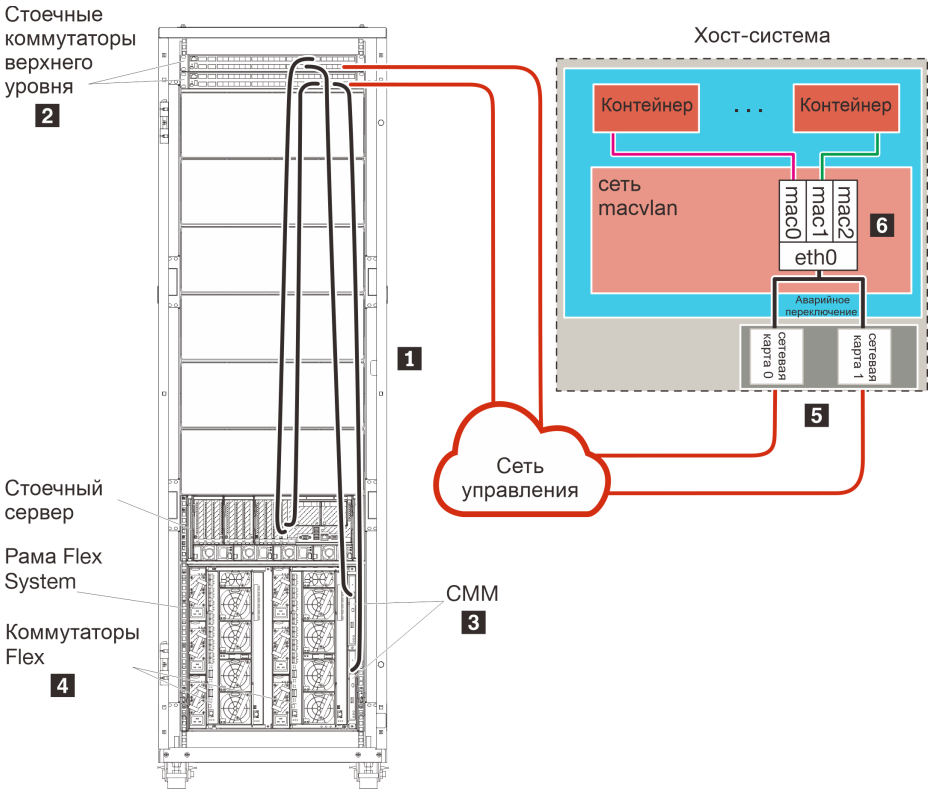


Рис. 22. Пример топологии сети только для управления для контейнеров

Если вы планируете установить XClarity Administrator для управления уже имеющимися и настроенными рамами и стоечными серверами, перейдите к разделу Шаг 5. Установка и настройка хоста.

Дополнительные сведения о планировании этой топологии, включая информацию о параметрах сети и конфигурации Eth1 и Eth0, см. в разделе Сеть только для управления.

Шаг 1. Подключение рамы, стоечных серверов и хоста Lenovo XClarity Administrator к стоечным коммутаторам верхнего уровня

Подключите с помощью кабелей раму, стоечные серверы и хост XClarity Administrator к стоечным коммутаторам верхнего уровня, чтобы обеспечить связь между устройствами и вашей сетью.

Процедура

Подключите с помощью кабелей каждый коммутатор Flex и модуль CMM в каждой раме, каждый стоечный сервер и хост XClarity Administrator к обоим стоечным коммутаторам верхнего уровня. Для подключения можно использовать любые порты стоечных коммутаторов верхнего уровня.

На следующем рисунке приведен пример, иллюстрирующий подключение рамы (коммутаторов Flex и модулей CMM), стоечных серверов и хоста XClarity Administrator с помощью кабелей к стоечным коммутаторам верхнего уровня.

Примечание: На этом рисунке не показаны все возможные варианты подключения, которые могут потребоваться для вашей среды. На этом рисунке демонстрируются только требования к подключению для коммутаторов Flex, модулей CMM и стоечных серверов, связанные с настройкой сети только для управления.

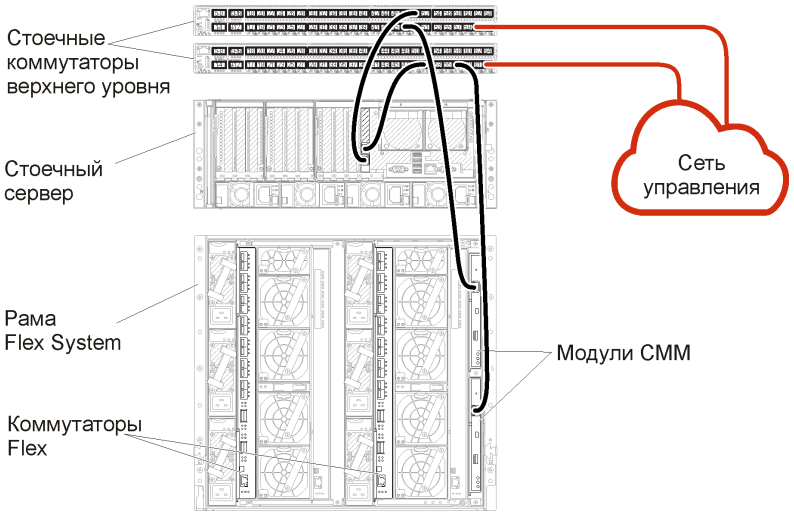


Рис. 23. Пример кабельных соединений для сети только для управления

Шаг 2. Настройка стоечных коммутаторов верхнего уровня

Настройте стоечные коммутаторы верхнего уровня.

Перед началом работы

В дополнение к обычным требованиям к конфигурации для стоечных коммутаторов верхнего уровня, убедитесь, что включены все необходимые порты, в том числе внешние порты для связи с

Коммутаторы Flex, стоечными серверами и сетью, а также внутренние порты для связи с модулями CMM, стоечными серверами и сетью.

Процедура

Действия по настройке могут отличаться в зависимости от типа установленных стоечных коммутаторов.

Сведения о настройке стоечных коммутаторов верхнего уровня Lenovo см. в Стоечные коммутаторы в документации по System x в Интернете. Если установлен другой стоечный коммутатор верхнего уровня, см. документацию, сопровождающую этот коммутатор.

Шаг 3. Настройка модулей CMM

Настройте основной модуль управления рамой (Chassis Management Module, CMM) в раме для управления всеми устройствами в раме.

Об этой задаче

Подробные сведения о настройке модуля CMM см. в разделе Настройка компонентов рамы в документации по устройствам Flex System в Интернете.

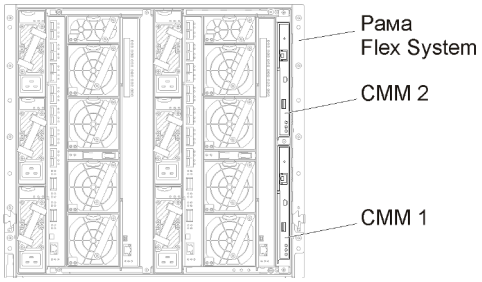
Также см. действия 4.1–4.5 на листе с инструкциями из комплекта поставки вашей рамы.

Процедура

Чтобы настроить модуль CMM, выполните указанные ниже действия.

Если установлены два модуля CMM, настройте только *основной* модуль CMM. Он автоматически синхронизирует конфигурацию с резервным модулем CMM.

Шаг 1. Подключите кабель Ethernet от модуля CMM в отсеке 1 к клиентской рабочей станции, чтобы создать прямое подключение.



При первом подключении к модулю CMM, возможно, потребуется изменить свойства протокола IP на клиентской рабочей станции.

Важно: Убедитесь, что подсеть клиентской рабочей станции совпадает с подсетью модуля CMM. (По умолчанию для CMM используется подсеть 255.255.255.0). IP-адрес, выбранный для клиентской рабочей станции, должен находиться в той же сети, что и IP-адрес модуля CMM (например, 192.168.70.0–192.168.70.24).

Шаг 2. Чтобы запустить интерфейс управления CMM, откройте веб-браузер на клиентской рабочей станции и направьте его на IP-адрес модуля CMM.

Примечания:

- Убедитесь, что используется безопасное подключение, и включите **https** в URL-адрес (пример: https://192.168.70.100). Если не включить «https», отобразится ошибка «Страница не найдена».
- Если вы используете IP-адрес по умолчанию 192.168.70.100, интерфейс управления CMM может стать доступен спустя несколько минут. Эта задержка возникает из-за того, что модуль CMM пытается получить адрес DHCP в течение двух минут, прежде чем вернуться к статическому адресу по умолчанию.

Шаг 3. Войдите в интерфейс управления модуля CMM, используя принимаемые по умолчанию идентификатор пользователя `USERID` и пароль `PASSWORD`. После входа пароль по умолчанию необходимо изменить.

Шаг 4. Выполните шаги мастера первоначальной настройки CMM, чтобы указать сведения для своей среды. Мастер первоначальной настройки включает в себя следующие параметры:

- Просмотр ресурсов и состояния работоспособности рамы.
- Импорт конфигурации из существующего файла конфигурации.
- Настройка общих параметров CMM.
- Установка даты и времени CMM.

  Совет. При установке XClarity Administrator настройте использование сервера NTP для XClarity Administrator и всех рам, которыми управляет XClarity Administrator.
- Настройте IP-информацию модуля CMM.
- Настройте политику безопасности модуля CMM.
- Настройте систему доменных имен (DNS).
- Настройте средства перенаправления событий.

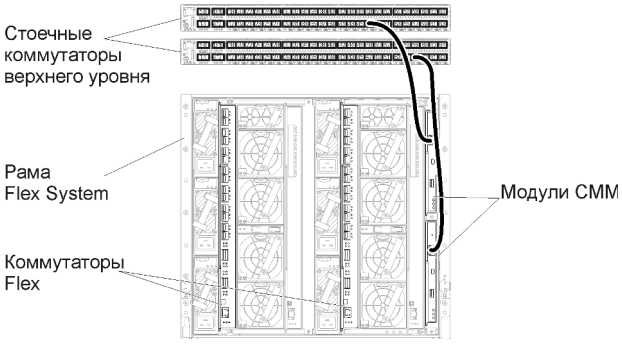
Шаг 5. Сохранив заданные значения параметров мастера настройки и применив изменения, настройте IP-адреса для всех компонентов в раме.

См. действие 4.6 на листе с инструкциями из комплекта поставки вашей рамы.

Примечание: Чтобы отобразились новые IP-адреса, необходимо сбросить процессор управления системой для каждого вычислительного узла и перезапустить коммутаторы Flex.

Шаг 6. Перезапустите модуль CMM с помощью интерфейса управления CMM.

Шаг 7. Пока модуль CMM перезапускается, подключите кабель от порта Ethernet модуля CMM к своей сети.



Шаг 8. Войдите в интерфейс управления модуля CMM, используя новый IP-адрес.

После завершения

В модуле CMM также можно настроить поддержку избыточности. Используйте справочную систему CMM, чтобы узнать больше о полях, доступных на каждой из следующих страниц.

- Настройте для модуля CMM аварийное переключение в случае аппаратного сбоя в основном модуле CMM. В интерфейсе управления CMM нажмите **Mgt Module Management → Свойства → Расширенное аварийное переключение**.
- Настройте аварийное переключение в случае неполадки с сетью (восходящий канал). В интерфейсе управления CMM нажмите **Mgt Module Management → Сеть**, откройте вкладку **Ethernet**, а затем нажмите **Дополнительные параметры Ethernet**. Как минимум, убедитесь, что выбран параметр **Переключение при утрате физического сетевого подключения**.

Шаг 4. Настройка Коммутаторы Flex

Настройте Коммутаторы Flex в каждой раме.

Перед началом работы

Убедитесь, что включены все необходимые порты, в том числе внешние порты для связи между коммутатором Flex и стоечным коммутатором верхнего уровня, а также внутренние порты для связи с модулем CMM.

Если в коммутаторах Flex настроено получение параметров динамической сети (IP-адреса, маски сети, шлюза и адреса DNS) посредством DHCP, убедитесь, что коммутаторы Flex имеют согласованные параметры (например, убедитесь, что IP-адреса находятся в одной подсети с IP-адресами модуля CMM).

Важно: Для каждой рамы Flex System убедитесь, что тип межкомпонентной сети карты расширения в каждом сервере в раме совместим с типом межкомпонентной сети всех коммутаторов Flex в этой же раме. Например, если в раме установлены коммутаторы Ethernet, все серверы в этой раме должны иметь возможность подключения к Ethernet с помощью разъема локальной сети на материнской плате или карты расширения Ethernet. Дополнительные сведения о настройке коммутаторов Flex см. в разделе Настройка модулей ввода-вывода в документации по устройствам Flex System в Интернете.

Процедура

Действия по настройке могут отличаться в зависимости от типа установленных Коммутаторы Flex. Дополнительную информацию о каждом из поддерживаемых Коммутаторы Flex см. в Сетевые коммутаторы Flex System в документации по устройствам Flex System в Интернете.

Как правило, требуется настроить коммутаторы Flex в отсеках 1 и 2 для коммутаторов Flex.

Совет. Отсек 2 для коммутатора Flex — это третий по счету модульный отсек, если смотреть на раму с тыльной стороны.

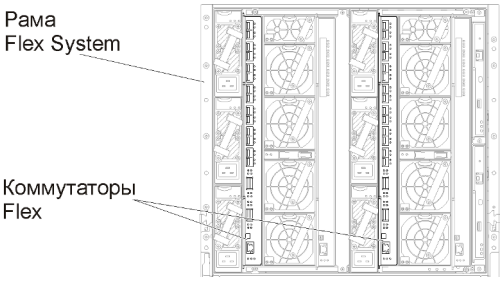


Рис. 24. Места установки Коммутатор Flexв раме

Шаг 5. Установка и настройка хоста

Docker можно установить в любой системе, которая отвечает требованиям для Lenovo XClarity Administrator.

Перед началом работы

Docker Datacenter можно использовать для настройки среды высокой доступности для контейнеров XClarity Administrator, работающих под управлением Docker Engine. Дополнительные сведения о высокой доступности на базе Docker Datacenter см. в разделе Веб-страница архитектуры высокой доступности и приложений с Docker Datacenter.

Убедитесь, что хост отвечает предварительным требованиям, которые определены в разделе Обязательные требования к оборудованию и программному обеспечению.

Убедитесь, что система хоста находится в той же сети, что и устройства, которыми вы хотите управлять.

Важно: XClarity Administrator можно установить на любой системе, отвечающей требованиям для XClarity Administrator, в том числе на управляемом сервере. Если для хоста XClarity Administrator используется управляемый сервер:

- Необходимо реализовать либо топологию с виртуальным разделением сети данных и сети управления, либо топологию с единой сетью данных и управления.
- Для применения обновлений микропрограммы к этому управляемому серверу невозможно использовать XClarity Administrator. Даже если только часть микропрограммного обеспечения применяется с немедленной активацией, XClarity Administrator принудительно перезапускает целевой сервер, что приводит к перезапуску XClarity Administrator. Если используется отложенная активация, при перезапуске XClarity Administrator применяются только некоторые части микропрограммы.
- Если вы используете сервер в раме Flex System, убедитесь, что на сервере настроено автоматическое включение. Этот параметр можно установить из веб-интерфейса CMM, нажав **Управление рамой → Вычислительные узлы**, выбрав сервер и выбрав **Автоматическое включение/выключение питания** для параметра **Режим автоматического включения**.

Процедура

Установите и настройте Docker на хосте согласно инструкциям, предоставляемым с дистрибутивом Docker.

Шаг 6. Установка и настройка XClarity Administrator

Установите и настройте контейнер Lenovo XClarity Administrator на только что установленном хосте Docker.

Перед началом работы

Убедитесь, что хост-система отвечает минимальным требованиям к оборудованию и программному обеспечению (см. раздел Обязательные требования к оборудованию и программному обеспечению).

Убедитесь, что включены все соответствующие порты, включая порты, которые требуются XClarity Administrator (см. раздел Доступность портов).

Убедитесь, что система хоста находится в той же сети, что и устройства, которыми вы хотите управлять.

Убедитесь, что ОС хоста и XClarity Administrator используют один и тот же сервер NTP.

XClarity Administrator позволяет использовать пользовательское имя сети для управления данными и оборудованием, а также развертывания ОС (см. раздел Конфигурации сети). В этом примере в следующей процедуре используется eth0.

XClarity Administrator позволяет использовать пользовательское имя сети для управления данными и оборудованием (см. раздел Конфигурации сети). В этом примере в следующей процедуре используется eth0

Убедитесь, что сеть macvlan загружена в ядро хост-системы. Чтобы проверить, загружена ли она, воспользуйтесь командой **lsmod | grep macvlan**. Чтобы загрузить macvlan в ядро, выполните команду **modprobe macvlan**.

При запуске нескольких контейнеров XClarity Administrator в одном хосте следует использовать уникальное имя и IP-адрес для каждого контейнера.

Если вы предполагаете управлять ThinkServer и другими устаревшими устройствами, убедитесь, что в Docker включена поддержка IPv6.

1. Внесите следующие изменения в файл /etc/docker/daemon.json: установите значение «true» для ключа **ipv6** и укажите вашу подсеть IPv6 в качестве значения ключа **fixed-cidr-v6**. Пример файла daemon представлен ниже.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Перезагрузите файл конфигурации Docker, выполнив указанную ниже команду.
```
systemctl reload docker
```

Примечание: XClarity Administrator *не* работает в качестве привилегированного контейнера.

Процедура

Чтобы установить контейнер XClarity Administrator с помощью Docker compose, выполните следующие шаги.

Шаг 1. Скачайте образ виртуального устройства XClarity Administrator, файла среды и YAML-файла с Веб-страница загрузки XClarity Administrator на клиентскую рабочую станцию. Войдите на веб-сайт и используйте предоставленный вам ключ доступа для скачивания образа.

Шаг 2. Импортируйте образ контейнера XClarity Administrator в хост docker, выполнив следующую команду.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Шаг 3. Отредактируйте файл `docker_compose.env` и измените следующие переменные среды.

- **CONTAINER_NAME**. Уникальное имя контейнера, используемое для создания томов Docker для каждого экземпляра XClarity Administrator (например, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Статический адрес IPv4 для контейнера (например, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Необязательно) Путь удаленного общего ресурса, который можно использовать для хранения резервных копий XClarity Administrator. Он должен иметь вид `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Необязательно) Путь к удаленному общему ресурсу, который можно использовать в качестве удаленного репозитория для обновлений микропрограмм. Он должен иметь вид `/mnt/fw_share`.

Ниже приведен пример файла среды.

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Шаг 4. Измените файл `docker_compose.yml` и измените следующие свойства.

- Задайте значение свойства **image** равным имени файла установочного образа, используемому в шаге 2.

  Примечание: Имя файла образа можно изменить (например, на latest) с помощью команды `docker tag`.

- Если необходимо использовать удаленные общие ресурсы в качестве удаленного репозитория микропрограмм и для хранения резервных копий XClarity Administrator, задайте точку подключения хоста для каждого удаленного общего ресурса в свойстве **volumes**.
- Установите в качестве значения свойства **dns** IP-адрес серверов DNS.
- Этот контейнер использует тот же пул ресурсов процессора, памяти и хранения, которые доступны хосту. При необходимости определите ограничения использования ресурсов, настроив свойства **cpus** и **memory**.
- Задайте значение свойства **parent** равным имени сетевого интерфейса в хост-системе, который следует использовать в качестве родительского для интерфейса macvlan в контейнере. Этот интерфейс должен иметь прямой доступ к подсети, назначенной контейнеру.
- Задайте свойства **subnet (подсеть)** и **gateway (шлюз)** в соответствии с топологией вашей сети. Как правило, подсеть и шлюз предназначены для сети управления, к которой относится ${ADDRESS}.
- Если требуется поддержка IPv6, задайте для свойства **enable_ipv6** значение «true», укажите адрес IPv6 в качестве значения свойства **ipv6_address** и добавьте еще один набор свойств **subnet** и **gateway** в соответствии с топологией вашей сети (обычно для сети управления, к которой принадлежит адрес IPv6).

Ниже представлен пример файла YML с включенной поддержкой IPv6.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
```

```
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
```

Шаг 5. Разверните образ в Docker, выполнив следующую команду, где <*ENV_FILENAME*> — имя файла переменных среды, созданного в шаге 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

После завершения

Войдите в систему и настройте XClarity Administrator (см. разделы Доступ к веб-интерфейсу Lenovo XClarity Administrator в первый раз и Настройка Lenovo XClarity Administrator).

Реализация высокой доступности

Docker Datacenter можно использовать для настройки среды высокой доступности для контейнеров Lenovo XClarity Administrator, работающих под управлением Docker Engine.

Дополнительные сведения о высокой доступности на базе Docker Datacenter см. в разделе Веб-страница архитектуры высокой доступности и приложений с Docker Datacenter.

Глава 4. Настройка Lenovo XClarity Administrator

Когда вы впервые осуществляете доступ к Lenovo XClarity Administrator, необходимо выполнить несколько действий для начальной настройки XClarity Administrator.

Подробнее: XClarity Administrator: настройка в первый раз

Процедура

Чтобы впервые выполнить настройку XClarity Administrator, выполните указанные ниже действия.

Шаг 1. Получите доступ к веб-интерфейсу XClarity Administrator.

Шаг 2. Прочитайте и примите лицензионное соглашение.

Шаг 3. Создайте учетные записи пользователей, обладающие полномочиями администратора.

Совет. Рекомендуется создать по крайней мере две учетные записи пользователей с правами администратора, чтобы иметь резервную копию на всякий случай.

Шаг 4. Настройте сетевой доступ, включая IP-адреса для сетей данных и управления.

Шаг 5. Настройте дату и время.

Шаг 6. Настройте параметры обслуживания и поддержки, включая заявление о конфиденциальности, данные об использовании и данные оборудования, службу поддержки Lenovo (Call Home), средство загрузки Lenovo и гарантию на продукт.

Шаг 7. Настройте параметры безопасности, в том числе сервер аутентификации, группы пользователей, сертификаты серверов и криптографический режим.

Шаг 8. Управляйте своей рамой, серверами, коммутаторами и устройствами хранения.

Доступ к веб-интерфейсу Lenovo XClarity Administrator в первый раз

Вы можете запустить веб-интерфейс XClarity Administrator с любого компьютера, который имеет сетевое подключение к виртуальной машине XClarity Administrator.

Перед началом работы

Убедитесь, что используется один из следующих поддерживаемых веб-браузеров:
- Chrome™ 48.0 или выше (55.0 или выше для удаленной консоли)
- Firefox® ESR 38.6.0 или выше
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 или выше (IOS 7 или выше и OS X)

Примечание: Запуск интерфейсов контроллера управления из XClarity Administrator с помощью веб-браузера Safari не поддерживается.

Убедитесь, что вход в веб-интерфейс XClarity Administrator выполняется из системы, у которой есть сетевое подключение к узлу управления XClarity Administrator.

Процедура

Для доступа к веб-интерфейсу XClarity Administrator в первый раз выполните указанные ниже действия.

Шаг 1. Введите в адресной строке браузера IP-адрес XClarity Administrator.

Рекомендация. Доступ к веб-интерфейсу осуществляется через защищенное соединение. Убедитесь, что используется протокол **https**.

- **Для контейнеров**: используйте адрес IPv4, указанный для переменной ${ADDRESS}, чтобы получить доступ к XClarity Administrator по следующему URL:
  `https://<IPv4_address>/ui/login.html`

  Например:
  `https://192.0.2.10/ui/login.html`

- **Для виртуальных устройств**. Используемый IP-адрес зависит от настроек вашей среды.

  Если интерфейсы Eth0 и Eth1 относятся к разным подсетям и в обеих подсетях используется протокол DHCP, для получения доступа к веб-интерфейсу при первоначальной настройке укажите IP-адрес интерфейса *Eth1*. При первом запуске XClarity Administrator для Eth0 и Eth1 протокол DHCP назначает IP-адрес, а в качестве шлюза XClarity Administrator по умолчанию протокол DHCP задает шлюз для *Eth1*.

  Использование статического адреса IPv4

  Если в eth0_config указывается адрес IPv4, используйте адрес IPv4 для доступа к XClarity Administrator по следующему URL-адресу:
  `https://<IPv4_address>/ui/login.html`

  Например:
  `https://192.0.2.10/ui/login.html`

  Использование DHCP-сервера в том же широковещательном домене, что и XClarity Administrator

  Если DHCP-сервер настроен в том же широковещательном домене, что и XClarity Administrator, используйте адрес IPv4, который отображается в консоли виртуальной машины XClarity Administrator, для получения доступа к XClarity Administrator по следующему URL-адресу:
  `https://<IPv4_address>/ui/login.html`

  Например:
  `https://192.0.2.10/ui/login.html`

  Использование DHCP-сервера в широковещательном домене, отличном от XClarity Administrator

  Если DHCP-сервер *не* настроен в том же широковещательном домене, используйте локальный адрес канала IPv6 (LLA), который отображается для eEth0 (сеть управления) в консоли виртуальной машины XClarity Administrator, для получения доступа к XClarity Administrator. Например:

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0
```

```
eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

Рекомендация. Локальный адрес канала IPv6 (LLA) можно получить из MAC-адреса интерфейса.

Внимание: При удаленной настройке XClarity Administrator должна быть возможность подключения к той же сети второго уровня. До завершения начальной настройки доступ должен осуществляться из адреса без маршрутизации. Поэтому рекомендуется получить доступ к XClarity Administrator из другой виртуальной машины, у которой есть подключение к XClarity Administrator. Например, можно получить доступ к XClarity Administrator из другой виртуальной машины хоста, где установлен XClarity Administrator.

– **Firefox:**

  Для доступа к веб-интерфейсу XClarity Administrator с помощью браузера Firefox войдите в систему, используя следующий URL-адрес. Обратите внимание, что при вводе адресов IPv6 необходимо добавить скобки.

  `https://[<IPv6_LLA>/ui/login.html]`

  Взяв в качестве основы предыдущий пример для Eth0, введите в адресной строке своего браузера следующий URL-адрес:

  `https://[fe80:21a:64ff:fe12:3456]/ui/login.html`

– **Internet Explorer:**

  Для доступа к веб-интерфейсу XClarity Administrator с помощью браузера Internet Explorer войдите в систему, используя следующий URL-адрес. Обратите внимание, что при вводе адресов IPv6 необходимо добавить скобки.

  `https://[<IPv6_LLA>%25<zone_index>]/ui/login.html`

  где *<zone_index>* — это идентификатор адаптера Ethernet, подключенного к сети управления с компьютера, на котором запущен веб-браузер. При использовании браузера в Windows выполните команду `ipconfig`, чтобы найти указатель зоны, который отображается после знака процента (%) в поле **Локальный адрес канала IPv6** для адаптера. В следующем примере указатель зоны имеет значение «30.»

  ```
  PS C:> ipconfig
  Windows IP Configuration

  Ethernet adapter vEthernet (teamVirtualSwitch):

     Connection-specific DNS Suffix  . :
     Link-local IPv6 Address . . . . . : 2001:db8:56ff:fe80:bea3%30
     Autoconfiguration IPv4 Address. . : 192.0.2.30
     Default Gateway . . . . . . . . . :
  ```

  При использовании браузера в Linux выполните команду `ifconfig`, чтобы найти указатель зоны. В качестве указателя зоны можно также использовать имя адаптера (обычно Eth0).

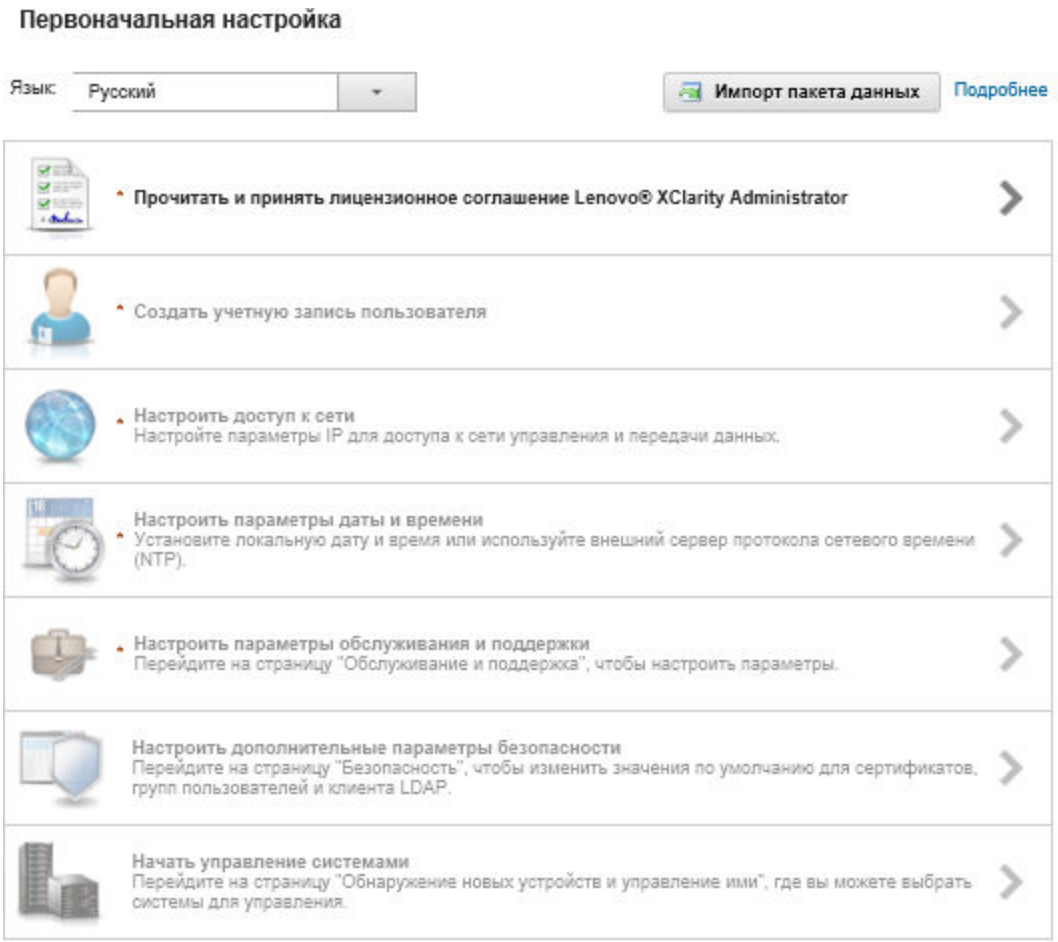
Взяв в качестве основы предыдущие примеры для Eth0 и указателя зоны, введите в адресной строке своего браузера следующий URL-адрес:

```
https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html
```

Шаг 2. При первом доступе к Lenovo XClarity Administrator могут отображаться предупреждения о безопасности или сертификатах. Эти предупреждения можно игнорировать.

Результаты

Появится страница Первоначальная настройка.



После завершения

Выполните действия по первоначальной настройке, чтобы настроить XClarity Administrator (см. раздел Настройка Lenovo XClarity Administrator).

Создание учетных записей пользователей

Учетные записи пользователей используются для управления авторизацией и доступом к Lenovo XClarity Administrator и устройствам, для которых требуется управляемая аутентификация.

Об этой задаче

Первая создаваемая учетная запись пользователя должна иметь роль «Администратор» и должна быть активирована (включена).

В качестве дополнительной меры безопасности создайте по крайней мере две учетные записи пользователей с ролью **Администратор**. Убедитесь, что пароли для этих учетных записей пользователей записаны, и сохраните их в безопасном месте, если потребуется восстановить Lenovo XClarity Administrator.

Процедура

Для создания учетных записей пользователей выполните указанные ниже действия.

Шаг 1. Заполните следующую информацию в диалоговом окне «Создание пользователя с правами администратора».

- Введите имя пользователя и описание.
- Введите новый пароль и подтверждение пароля. Правила для паролей основаны на текущих параметрах безопасности учетных записей.
- Выберите одну или несколько групп ролей, чтобы предоставить пользователю полномочия на выполнение соответствующих задач.

  Сведения о группах ролей и способах создания настраиваемых групп ролей см. в разделе Создание группы ролей в документации по XClarity Administrator в Интернете.
- (Необязательно) Установите параметр **Изменить пароль при первом входе** равным `Yes`, чтобы пользователь должен был менять свой пароль при первом входе в XClarity Administrator.

Шаг 2. Нажмите **Создать**.

Шаг 3. Нажмите значок **Создать** ( ) и повторите предыдущие шаги для создания дополнительных пользователей.

Шаг 4. Нажмите **Вернуться к первоначальной настройке**.

Настройка доступа к сети

Для настройки доступа к сети можно настроить до двух сетевых интерфейсов, имя хоста для Lenovo XClarity Administrator и серверы DNS, которые следует использовать.

Об этой задаче

XClarity Administrator имеет два отдельных сетевых интерфейса, которые могут быть определены для вашей среды, в зависимости от используемой топологии сети. Для виртуальных устройств эти сети называются eth0 и eth1. Для контейнеров можно выбирать пользовательские имена.

- Присутствует только один сетевой интерфейс (eth0):
  - Этот интерфейс должен быть настроен для поддержки обнаружения устройства и управления им (например, конфигурация сервера и обновления микропрограммы). Он должен иметь возможность связываться с CMM и коммутаторами Flex в каждой управляемой раме, контроллером управления материнской платой в каждом управляемом сервере, и с каждым коммутатором RackSwitch.
  - Если предполагается получать обновления микропрограммы и драйверов устройств ОС с помощью XClarity Administrator, по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр. В противном случае обновления необходимо импортировать в репозиторий.
  - Если предполагается осуществлять сбор данных по обслуживанию или использовать автоматическое уведомление о неполадках (включая Call Home и средство загрузки Lenovo), по

крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр.

- Если вы собираетесь развертывать образы операционной системы и обновлять драйверы устройств ОС, интерфейс должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к основной операционной системе.

  Примечание: Если для развертывания операционных систем и обновлений драйверов устройств ОС создана отдельная сеть, можно настроить второй сетевой интерфейс для подключения к этой сети, а не к сети данных. Однако, если операционная система на каждом сервере не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между операционной системой хоста и сетью данных.

- Присутствуют два сетевых интерфейса (eth0 и eth1):
  - Первый сетевой интерфейс (обычно интерфейс Eth0) необходимо подключить к сети управления и настроить для поддержки обнаружения устройств и управления ими (включая конфигурацию сервера и обновления микропрограммы). Он должен иметь возможность связываться с CMM и коммутаторами Flex в каждой управляемой раме, контроллером управления в каждом управляемом сервере, и с каждым коммутатором RackSwitch.
  - Второй сетевой интерфейс (обычно eth1) можно настроить для связи с внутренней сетью данных, сетью данных общего пользования или с обеими сетями.
  - Если предполагается получать обновления микропрограммы и драйверов устройств ОС с помощью XClarity Administrator, по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр. В противном случае обновления необходимо импортировать в репозиторий.
  - Если предполагается осуществлять сбор данных по обслуживанию или использовать автоматическое уведомление о неполадках (включая Call Home и средство загрузки Lenovo), по крайней мере один из сетевых интерфейсов должен быть подключен к Интернету, желательно через брандмауэр.
  - Если вы планируете развертывать образы операционной системы и обновлять драйверы устройств, можно использовать интерфейс eth1 или eth0. Однако используемый интерфейс должен иметь возможность подключения через IP-сеть к сетевому интерфейсу сервера, который используется для доступа к операционной системе хоста.

    Примечание: Если для развертывания операционных систем и обновлений драйверов устройств ОС создана отдельная сеть, можно настроить второй сетевой интерфейс для подключения к этой сети, а не к сети данных. Однако, если операционная система на каждом сервере не имеет доступа к сети данных, при необходимости следует настроить дополнительный интерфейс на серверах, обеспечивающий связь между операционной системой хоста и сетью данных.

В следующей таблице показаны возможные конфигурации для сетевых интерфейсов XClarity Administrator в зависимости от типа топологии сети, реализованной в вашей среде. Используйте эту таблицу для выяснения способа определения каждого сетевого интерфейса.

Табл. 3. Назначение каждого сетевого интерфейса зависит от топологии сети

Топология сети	**Назначение интерфейса 1 (eth0)**	**Назначение интерфейса 2 (eth1)**
Конвергентная сеть (сеть данных и управления с поддержкой развертывания ОС и обновлений драйверов устройств ОС)	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии • Развертывание ОС • Обновления драйверов устройств ОС	Нет
Отдельные сеть управления с поддержкой развертывания ОС и обновлений драйверов устройств ОС и сеть данных	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии • Развертывание ОС • Обновления драйверов устройств ОС	Сеть данных • Нет
Отдельные сеть управления и сеть данных с поддержкой развертывания ОС и обновлений драйверов устройств ОС	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии	Сеть данных • Развертывание ОС • Обновления драйверов устройств ОС

Табл. 3. Назначение каждого сетевого интерфейса зависит от топологии сети (продолж.)

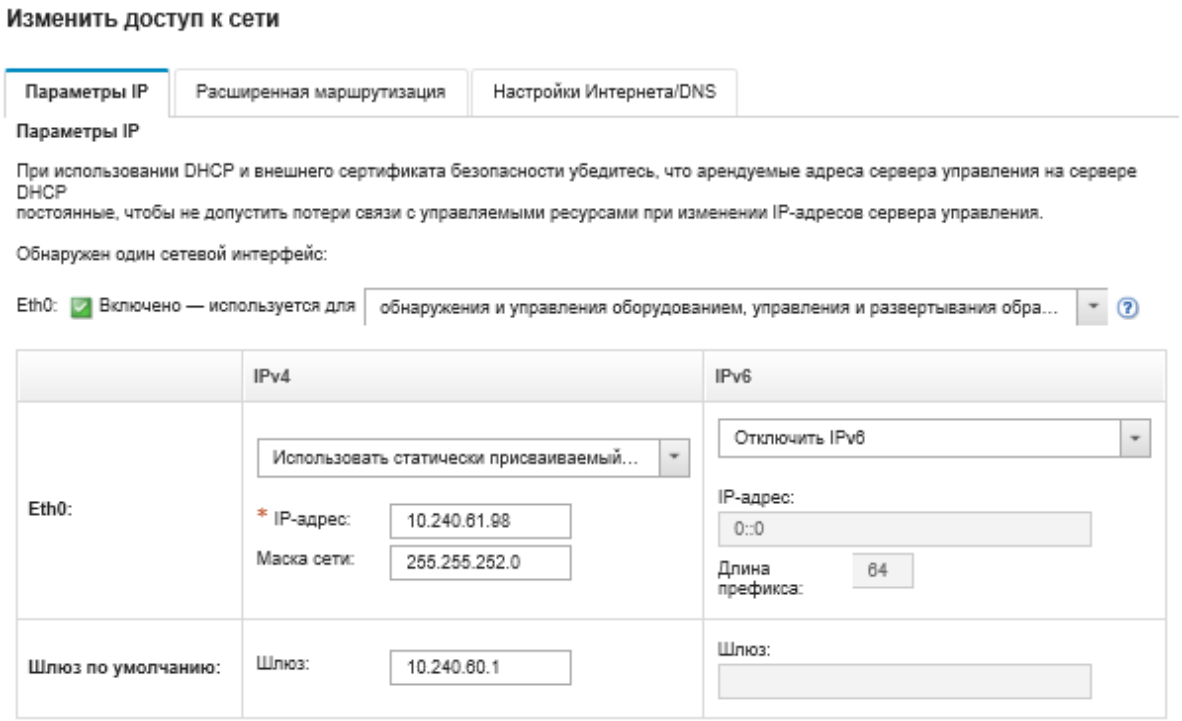
Топология сети	Назначение интерфейса 1 (eth0)	Назначение интерфейса 2 (eth1)
Отдельные сеть управления и сеть данных без поддержки развертывания ОС и обновлений драйверов устройств ОС	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии	Сеть данных • Нет
Только сеть управления (развертывание ОС и обновления драйверов устройств ОС не поддерживаются)	Сеть управления • Обнаружение и управление • Конфигурация сервера • Обновления микропрограммы • Сбор данных по обслуживанию • Автоматическое уведомление о неполадках (например, Call Home и средство загрузки Lenovo) • Получение данных гарантии	Нет

Дополнительные сведения о сетевых интерфейсах XClarity Administrator см. в разделе Замечания по сети.

Процедура

Чтобы настроить доступ к сети, выполните указанные ниже действия.

Шаг 1. На странице Первоначальная настройка нажмите **Настроить доступ к сети**. Откроется страница Изменить доступ к сети.



Шаг 2. Укажите сетевой интерфейс, который будет использоваться для управления операционными системами, если вы планируете развертывать операционные системы и обновлять драйверы устройств ОС с помощью XClarity Administrator.

- Если для XClarity Administrator определен только один интерфейс, выберите, следует ли использовать этот интерфейс только для обнаружения оборудования и управления им или же он также должен использоваться для управления операционными системами.
- Если для XClarity Administrator определены два интерфейса (Eth0 и Eth1), укажите, какой из них должен использоваться для управления операционными системами. В случае выбора варианта «Нет» развертывать образы операционных систем и обновлять драйверы устройств ОС на управляемых серверах с помощью XClarity Administrator будет *невозможно*.

Шаг 3. Задайте параметры IP-адресов.

a. Для первого интерфейса укажите адрес IPv4, адрес IPv6 или оба адреса.

- **IPv4**. Для интерфейса должен быть назначен адрес IPv4. Можно выбрать использование статически назначенного IP-адреса или получение IP-адреса от сервера DHCP.
- **IPv6**. Если требуется, интерфейсу можно назначить адрес IPv6, используя один из следующих методов назначения:
  - Использовать статически присваиваемый IP-адрес
  - Использовать конфигурацию адресов с запоминанием состояния (DHCPv6)
  - Использовать автоматическую настройку адреса без учета состояния

  Примечание: Сведения об ограничениях на адреса IPv6 см. в разделе Ограничения конфигурации IP.

b. Если доступен второй интерфейс, укажите адрес IPv4, адрес IPv6 или оба адреса.

Примечание: IP-адреса, назначаемые этому интерфейсу, и IP-адреса, назначаемые первому интерфейсу, должны принадлежать разным подсетям. Если для обоих интерфейсов (Eth0 и Eth1) выбрано назначение IP-адресов посредством DHCP, сервер DHCP не должен назначать одну и ту же подсеть для IP-адресов двух этих интерфейсов.

- **IPv4**. Можно выбрать использование статически назначенного IP-адреса или получение IP-адреса от сервера DHCP.
- **IPv6**. Если требуется, интерфейсу можно назначить адрес IPv6, используя один из следующих методов назначения:
  - Использовать статически присваиваемый IP-адрес
  - Использовать конфигурацию адресов с запоминанием состояния (DHCPv6)
  - Использовать автоматическую настройку адреса без учета состояния

c. Укажите шлюз по умолчанию.

Если указывается шлюз по умолчанию, это должен быть действительный IP-адрес и для него должна использоваться та же маска сети (та же подсеть), что и для IP-адреса одного из сетевых интерфейсов (Eth0 или Eth1). Если используется один интерфейс, шлюз по умолчанию должен находиться в той же подсети, что и сетевой интерфейс.

Если какой-либо из интерфейсов использует DHCP для получения IP-адресов, шлюз по умолчанию также использует DHCP. Чтобы вручную ввести адрес шлюза по умолчанию, который переопределяет адрес, полученный от сервера DHCP, установите флажок **Переопределить шлюз**.

Рекомендации.

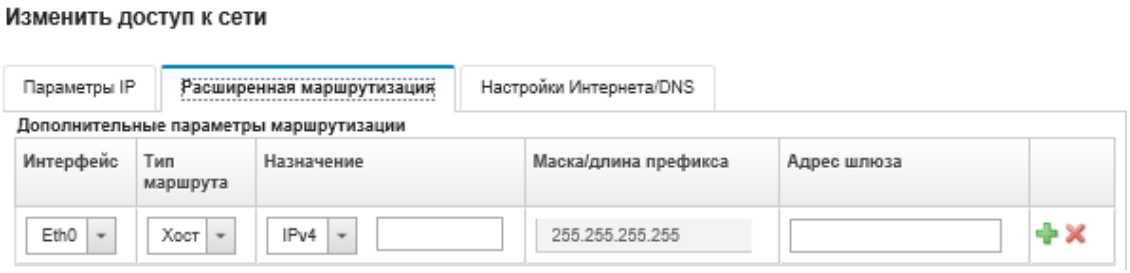
- Убедитесь, что шлюз соответствует одной из подсетей сетевых интерфейсов. Шлюз по умолчанию автоматически настраивается через такой сетевой интерфейс.
- Чтобы вернуться к шлюзу, предоставленному DHCP, снимите флажок **Переопределить шлюз**.

ОСТОРОЖНО:
Если вы решили переопределить шлюз, введите правильный адрес шлюза; в противном адресе этот сервер управления будет недоступен, а войти дистанционно и внести исправления будет невозможно.

d. Нажмите **Сохранить IP-настройки**.

Шаг 4. **Необязательно.** Настройте дополнительные параметры.

a. Перейдите на вкладку **Расширенная маршрутизация**.



b. Укажите в таблице **Дополнительные параметры маршрутизации** одну или несколько записей маршрута, которые будут использоваться этим интерфейсом.

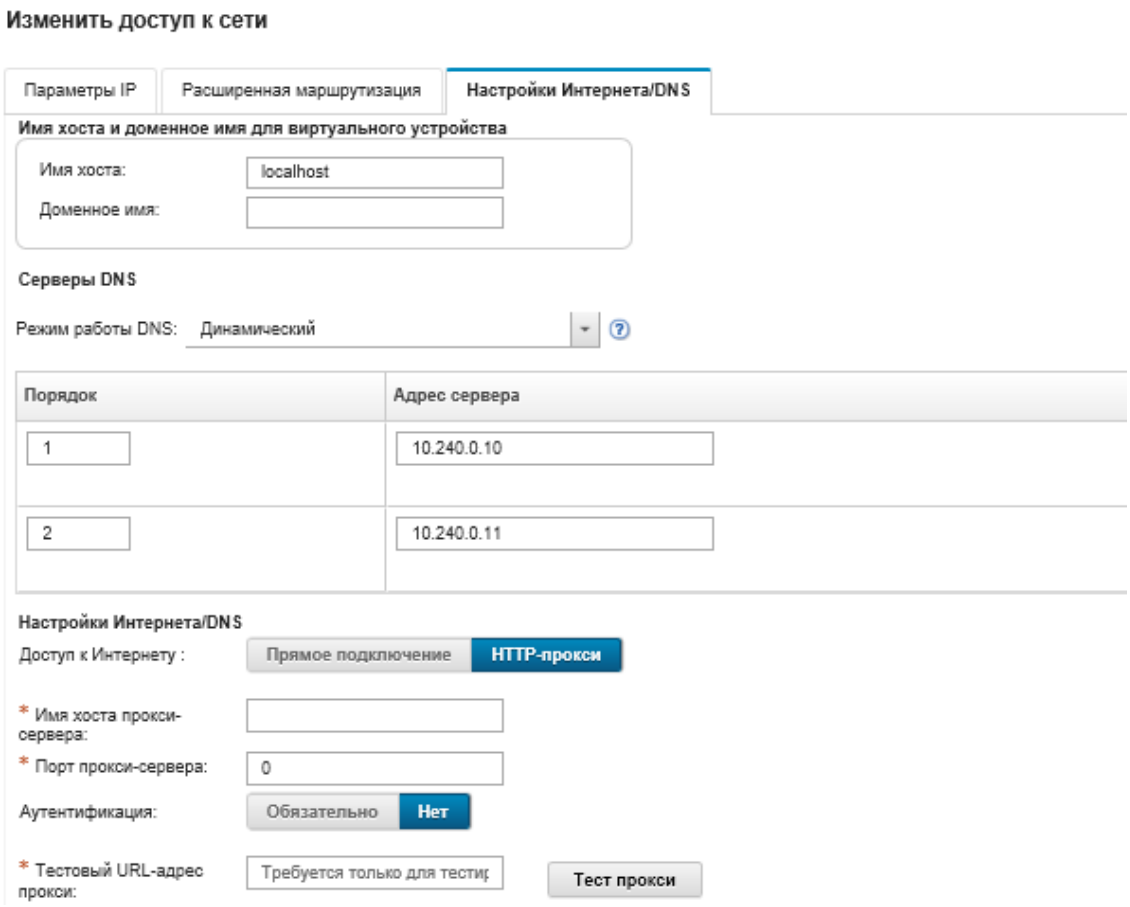
Чтобы определить одну или несколько записей маршрута, выполните указанные ниже действия.

1. Выберите интерфейс.
2. Укажите тип маршрута: это может быть маршрут к другому хосту или сети.
3. Укажите целевой хост или сетевой адрес, к которому ведет маршрут.
4. Укажите маску подсети для адреса назначения.
5. Укажите адрес шлюза, по которому должны отправляться пакеты.

c. Нажмите **Сохранить расширенную маршрутизацию**.

Шаг 5. При необходимости измените параметры DNS и прокси.

a. Перейдите на вкладку **DNS и прокси**.



b. Укажите имя хоста и доменное имя, которые будут использоваться для XClarity Administrator.

c. Выберите режим работы DNS. Может иметь значение **Статический** или **DHCP**.

   Внимание: При изменении режима работы DNS необходимо перезапустить сервер управления.

   Примечание: Если вы выбрали получение IP-адресов с использованием сервера DHCP, любые изменения, которые вы внесли в поля **Сервер DNS**, будет перезаписаны, когда XClarity Administrator в следующий раз обновит аренду DHCP.

d. Укажите IP-адрес одного или нескольких серверов службы доменных имен (DNS), которые будут использоваться, и порядок приоритета для каждого из них.

e. Укажите, как осуществляется доступ к Интернету: через прямое подключение или через прокси-сервер HTTP (если XClarity Administrator имеет доступ к Интернету).

   Примечания: При использовании прокси-сервера HTTP убедитесь, что выполняются следующие требования.
   - Убедитесь, что на прокси-сервере настроено использование базовой аутентификации.
   - Убедитесь, что прокси-сервер настроен в качестве непрерывающего прокси.
   - Убедитесь, что прокси-сервер настроен в качестве прокси переадресации.
   - Убедитесь, что балансировщики нагрузки настроены таким образом, чтобы поддерживать сеансы с одним прокси-сервером и не переключаться между ними.

   Если вы решили использовать прокси-сервер HTTP, заполните обязательные поля:
   1. Укажите имя хоста и порт прокси-сервера.

2. Выберите, следует ли использовать аутентификацию, и если да, укажите имя пользователя и пароль.
3. Укажите URL-адрес проверки прокси-сервера.
4. Нажмите **Проверить прокси**, чтобы убедиться, что параметры прокси-сервера настроены правильно и прокси-сервер работает корректно.

f. Нажмите **Сохранить DNS и прокси**.

g. Передайте полное доменное имя (FQDN) и информацию DNS сервера управления XClarity Administrator на управляемые серверы с IMM2, XCC и XCC2, чтобы управляемые серверы могли найти сервер управления с помощью этой информации.

1. Нажмите **Передать FQDN/DNS в BMC**.
2. Выберите, как нужно поступить с существующими записями DNS в контроллере управления материнской платой.
   - Сохранить существующие записи DNS и добавить записи DNS сервера управления в следующую доступную позицию.
   - Заменить все существующие записи DNS записями DNS сервера управления.
3. Введите **ДА** в поле редактирования.
4. Нажмите **Применить**.

Для выполнения этой операции создается задание. Ход выполнения задания можно отслеживать на карточке **Мониторинг → Задания**. Если задание не выполнено, нажмите ссылку на него, чтобы отобразить сведения о нем (см. раздел Работа с заданиями в документации по XClarity Administrator в Интернете).

Также можно удалить полное доменное имя и информацию DNS сервера управления с управляемых серверов с IMM2, XCC и XCC2, нажав **Удалить FQDN/DNS из BMC**. При этом можно выбрать один из следующих вариантов: не удалять другие существующие записи DNS, удалить все записи DNS или удалить только те записи, которые соответствуют информации сервера управления.

Шаг 6. Нажмите **Назад**.

Шаг 7. Нажмите **Проверить соединение** для проверки параметров сети.

Настройка даты и времени

Хотя дату и время для Lenovo XClarity Administrator можно устанавливать вручную, рекомендуется настроить сервер протокола сетевого времени (NTP), который можно использовать для синхронизации временных меток между XClarity Administrator и всеми управляемыми устройствами.

Перед началом работы

Необходимо использовать по крайней мере один (и до четырех) сервер протокола сетевого времени (NTP) для синхронизации меток времени для всех событий, которые были получены от управляемых устройств через XClarity Administrator.

Рекомендация. Сервер NTP должен быть доступен по сети управления (обычно это интерфейс Eth0). Желательно настроить сервер NTP на одном хосте с XClarity Administrator.

После изменения времени на сервере NTP синхронизация XClarity Administrator с новым временем может занять некоторое время.

Внимание: Виртуальное устройство XClarity Administrator и его хост необходимо настроить для синхронизации с одним и тем же источником времени, чтобы предотвратить случайную неправильную синхронизацию времени между программным обеспечением XClarity Administrator и его

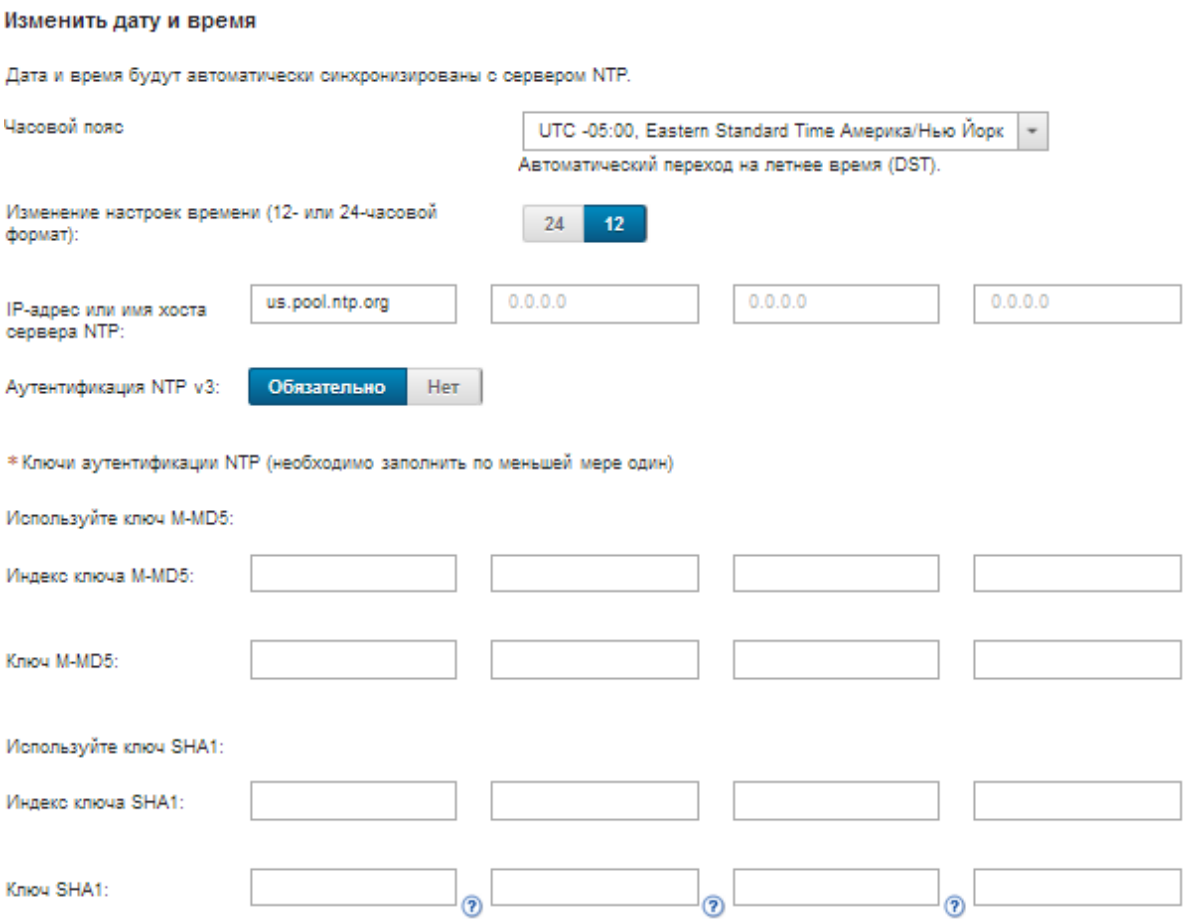
хостом. Обычно хост настраивается так, чтобы его виртуальные устройства синхронизировали время с ним. Если программное обеспечение XClarity Administrator настроено для синхронизации с источником, отличным от его хоста, синхронизацию времени между виртуальным устройством XClarity Administrator и его хостом необходимо отключить.

- Для ESXi следуйте инструкциям в разделе Веб-страница «VMware — отключение синхронизации времени».
- Для Hyper-V щелкните в диспетчере Hyper-V правой кнопкой мыши виртуальную машину XClarity Administrator и выберите пункт **Параметры**. В диалоговом окне выберите на панели навигации**Управление > Службы интеграции** и снимите флажок **Синхронизация времени**.

Процедура

Чтобы настроить сервер NTP для XClarity Administrator, выполните указанные ниже действия.

Шаг 1. На странице «Первоначальная настройка» нажмите **Настроить параметры даты и времени**. Откроется страница Изменить дату и время.



Шаг 2. Введите данные в диалоговом окне настройки даты и времени.

1. Выберите часовой пояс, в котором находится хост для XClarity Administrator.

   Если в выбранном часовом поясе действует переход на летнее время (DST), время автоматически корректируется с учетом летнего времени.

2. Выберите использование 12- или 24-часового формата времени.
3. Укажите имя хоста или IP-адрес для каждого сервера NTP в вашей сети. Можно определить до четырех серверов NTP.

4. Выберите **Обязательно**, чтобы включить аутентификацию NTP v3, или выберите **Нет**, чтобы использовать аутентификацию NTP v1 между XClarity Administrator и серверами NTP в сети.

   Аутентификацию v3 можно использовать, если в управляемых модулях CMM Flex System и контроллерах управления материнской платой установлены микропрограммы, для которых требуется аутентификация v3, и если между XClarity Administrator и одним или несколькими серверами NTP в сети требуется аутентификация NTP v3.

5. При включении аутентификации NTP v3 необходимо задать ключ аутентификации и индекс для каждого применимого сервера NTP. Можно указать ключ M-MD5, ключ SHA1 или оба ключа. Если заданы ключи M-MD5 и SHA1, XClarity Administrator передает ключ M-MD5 или SHA1 в управляемые модули CMM Flex System и контроллеры управления, поддерживающие его. XClarity Administrator использует ключ для аутентификации на сервере NTP.

   - Для ключа M-MD5 укажите строку ASCII, которая содержит только строчные и заглавные буквы (a–z, A–Z), цифры (0–9) и следующие специальные символы: @#.
   - Для ключа SHA1 укажите 40-символьную строку ASCII, используя только символы 0–9 и a–f.
   - Указанный индекс ключа и ключ аутентификации должны соответствовать значениям идентификатора ключа и пароля, заданным на сервере NTP. Например, если индекс введенного ключа SHA1 на сервере NTP имеет значение 5, указанный индекс ключа SHA1 XClarity Administrator также имеет значение 5. Сведения о настройке идентификатора ключа и пароля см. в документации по серверу NTP.
   - Необходимо указать ключ для каждого сервера NTP, на котором используется аутентификация v3, даже если два или более серверов NTP используют одинаковый ключ.
   - Если вы включили аутентификацию v3, но не предоставили ключ аутентификации и индекс для сервера NTP, по умолчанию будет использоваться аутентификация v1.
   - При указании нескольких серверов NTP все серверы NTP должны использовать либо аутентификацию v3, либо аутентификацию v1. Сочетание серверов NTP с аутентификацией v3 и v1 не поддерживается.
   - При указании нескольких серверов NTP с аутентификацией v3 индексы ключей должны быть уникальными, если ключи не совпадают. Например, серверы NTP 1 и 2 не могут иметь индекс ключа SHA1 1, если ключи SHA1 различаются в серверах NTP 1 и 2. Необходимо перенастроить один из серверов NTP, чтобы принять ключ с индексом, отличным от индекса другого сервера NTP. В противном случае последний определенный ключ, связанный с индексом ключа, будет настроен для всех серверов NTP с одинаковым индексом ключа.

Шаг 3. Нажмите **Сохранить**.

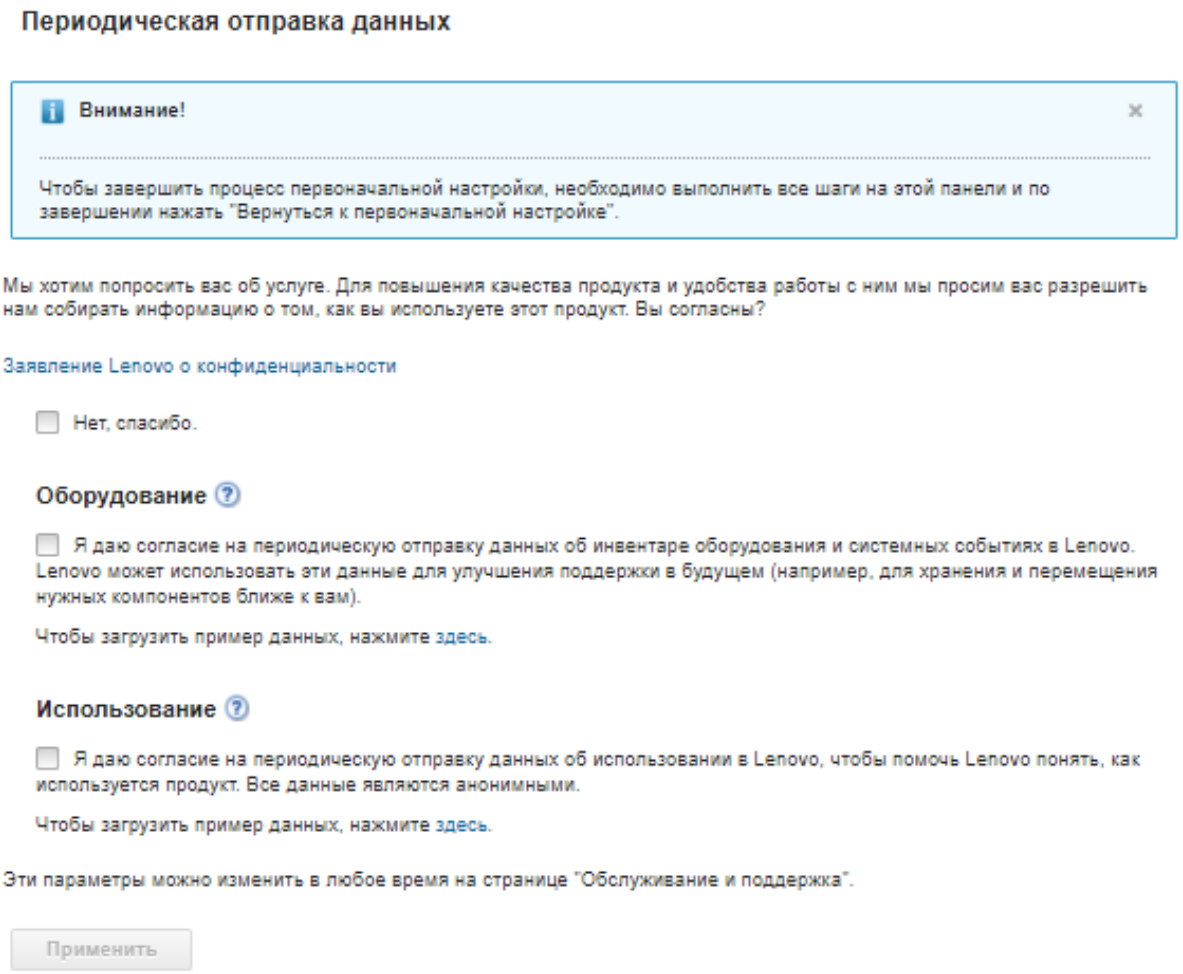
Настройка обслуживания и поддержки

Вы можете настроить параметры обслуживания и поддержки, включая данные об использовании, службу поддержки Lenovo (Call Home), средство загрузки Lenovo и гарантию на продукт.

Процедура

Для настройки безопасности выполните указанные ниже действия.

Шаг 1. На странице «Первоначальная настройка» нажмите **Настроить параметры обслуживания и поддержки**. Откроется страница Обслуживание и поддержка.



Шаг 2. Прочитайте и примите Заявление Lenovo о конфиденциальности.

Примечание: Вы не можете собирать и отправлять данные в Lenovo, не приняв Заявление Lenovo о конфиденциальности. Если вы решили отклонить заявление о конфиденциальности, вы можете просмотреть и принять его позже на странице **Обслуживание и поддержка → Конфигурация Call Home**.

Шаг 3. При необходимости разрешите Lenovo XClarity Administrator собирать информацию об использовании и оборудовании, затем нажмите **Применить**.

Можно собирать и отправлять в Lenovo следующие типы данных.

- **Данные об использовании**

  При согласии отправлять данные об использовании в Lenovo еженедельно собираются и отправляются следующие данные. Эти данные являются *анонимными*. Личные данные (включая серийные номера, коды UUID, имена хостов, IP-адреса и имена пользователей) не собираются и не отправляются в Lenovo.
  - Журнал выполненных действий.
  - Список событий, которые были созданы, и метки времени их создания.
  - Список событий аудита, которые были созданы, и метки времени их создания.
  - Список выполненных заданий, сведения об успехе или сбое для каждого задания.
  - Показатели XClarity Administrator, включая использование памяти, использование процессора и пространство на диске.
  - Ограниченные данные инвентаризации по всем управляемым устройствам.

- **Данные оборудования**

При согласии отправлять данные оборудования в Lenovo периодически собираются и отправляются следующие данные. Эти данные *не являются анонимными*. Данные оборудования включают атрибуты, такие как коды UUID и серийные номера. Они не включают IP-адреса или имена хостов.

- **Ежедневные данные оборудования**. При каждом изменении инвентаря собираются следующие данные.
  - Событие изменения инвентаря (FQXHMDM0001I).
  - Изменения данных инвентаризации для устройства, связанного с этим событием.
- **Еженедельные данные оборудования**. Включаются данные инвентаризации по всем управляемым устройствам.

Когда данные об использовании и данные оборудования отправляются в Lenovo, в журнале аудита регистрируется событие.

Можно изменить этот параметр в любое время и загрузить последний архив, собранный и отправленный в Lenovo, щелкнув **Администрирование → Обслуживание и поддержка** и открыв вкладку **Периодическая отправка данных**.

Шаг 4. При необходимости нажмите **Конфигурация Call Home**, чтобы настроить автоматическое уведомление о неполадках для службы поддержки Lenovo (Call Home). Затем нажмите **Применить и включить**, чтобы создать средство перенаправления обслуживания Call Home по умолчанию, или нажмите **Только применить**, чтобы сохранить контактную информацию.

Дополнительные сведения о настройке автоматического уведомления о неполадках для службы поддержки Lenovo см. в разделе Настройка функции Call Home в документации по XClarity Administrator в Интернете.

Шаг 5. При необходимости нажмите **Средство загрузки Lenovo**, чтобы настроить автоматическое уведомление о неполадках для средства загрузки Lenovo. Затем нажмите **Применить и включить**, чтобы создать средство перенаправления обслуживания для средства загрузки Lenovo по умолчанию, или нажмите **Только применить**, чтобы сохранить сведения о параметрах.

Дополнительные сведения о настройке автоматического уведомления о неполадках для средства загрузки Lenovo см. в разделе Настройка автоматической отправки уведомлений о неполадках в средство загрузки Lenovo в документации по XClarity Administrator в Интернете.

Шаг 6. При необходимости нажмите **Гарантия**, чтобы включить внешние подключения, необходимые для сбора информации о гарантии для своих управляемых устройств.

Дополнительные сведения о просмотре состояния гарантии (включая расширенные гарантии) управляемых устройств см. в разделе Просмотр информации о гарантии в документации по XClarity Administrator в Интернете.

Шаг 7. При необходимости нажмите **Услуга предоставления бюллетеней Lenovo**, чтобы разрешить Lenovo отправлять бюллетени технического обслуживания в XClarity Administrator и нажмите **Применить**

Дополнительные сведения о типах бюллетеней технического обслуживания, отправляемых компанией Lenovo, см. в разделе Получение бюллетеней от Lenovo в документации по XClarity Administrator в Интернете.

Шаг 8. Укажите пароль восстановления обслуживания, который можно использовать для сбора и загрузки данных по обслуживанию и журналов обслуживания, если решение XClarity Administrator перестает отвечать на запросы и восстановить его невозможно.

Дополнительные сведения о пароле восстановления обслуживания см. в разделе Изменение пароля восстановления обслуживания в документации по XClarity Administrator в Интернете.

Шаг 9. Нажмите **Вернуться к первоначальной настройке**.

Настройка безопасности

Можно настроить параметры безопасности, в том числе группы ролей, сервер аутентификации, параметры безопасности учетных записей пользователей, шифрование и сертификаты.

Процедура

Для настройки безопасности выполните указанные ниже действия.

Шаг 1. На странице «Первоначальная настройка» нажмите **Настроить дополнительные параметры безопасности**. Откроется страница Безопасность.

Шаг 2. Создайте настраиваемые группы ролей для управления авторизацией и доступом к ресурсам (см. раздел Создание группы ролей в документации по XClarity Administrator в Интернете).

Группа ролей представляет собой набор из одной или нескольких ролей и предназначена для назначения ролей сразу нескольким пользователям. Роли, настроенные для группы ролей, определяют уровень доступа, который предоставляется каждому из пользователей, входящих в эту группу ролей. Каждый пользователь XClarity Administrator должен быть участником по крайней мере одной группы ролей.

Шаг 3. Настройте сервер аутентификации (см. раздел Управление сервером аутентификации в документации по XClarity Administrator в Интернете).

Сервер аутентификации — это сервер Microsoft Active Directory (LDAP), который используется для аутентификации учетных данных пользователей. XClarity Administrator использует отдельный сервер аутентификации для централизованного управления пользователями всех управляемых устройств (кроме коммутаторов Flex). Когда устройством управляет XClarity Administrator, управляемое устройство и устанавливаемые в него компоненты (кроме коммутаторов Flex) настраиваются на использование сервера аутентификации XClarity Administrator. Учетные записи пользователей, определенные на сервере аутентификации, используются для входа в XClarity Administrator, модули CMM и контроллер управления материнской платой.

Можно выбрать использование внешнего сервера аутентификации вместо локального сервера аутентификации на узле управления.

Шаг 4. Настройте параметры безопасности учетных записей пользователя, которые контролируют сложность пароля, блокировку учетной записи и тайм-аут бездействия веб-сеанса (см. раздел Изменение параметров безопасности учетной записи пользователя в документации по XClarity Administrator в Интернете).

Шаг 5. Настройте параметр криптографии, определяющий режимы и протоколы связи, которые контролируют способ осуществления защищенной связи между XClarity Administrator и управляемыми устройствами (см. раздел Настройка криптографического режима и протоколов связи в документации по XClarity Administrator в Интернете).

Шаг 6. Если предполагается управлять стоечными серверами с использованием локальной аутентификации вместо аутентификации под управлением XClarity Administrator, создайте одни или несколько сохраненных учетных данных, соответствующих активным учетным записям пользователей на устройстве или в Active Directory, которые могут использоваться для входа в устройства в процессе управления. Дополнительные сведения о сохраненных учетных данных см. в разделе Управление сохраненными учетными данными в документации по XClarity Administrator в Интернете.

Шаг 7. Если вы планируете использовать настроенный сертификат сервера, включающий вашу собственную информацию, или использовать сертификат, подписанный сторонним центром, создайте и разверните новый сертификат, прежде чем приступать к управлению системами. Информацию о создании собственного сертификата безопасности см. в разделе Работа с сертификатами безопасности в документации по XClarity Administrator в Интернете.

Шаг 8. В вертикальном меню на странице «Безопасность» нажмите **Вернуться к первоначальной настройке**.

Управление устройствами

Lenovo XClarity Administrator может управлять несколькими типами систем, включая раму Flex System, стоечные и башенные серверы, коммутаторы RackSwitch и устройства хранения данных. Вы можете легко обнаруживать большое количество устройств в среде и управлять ими, импортируя информацию об устройствах с помощью файла массового импорта.

Перед началом работы

Важно:

- Одновременно можно управлять не более чем 300 устройствами. Не включайте в файл массового импорта более 300 устройств.
- Запустив операцию управления устройством, дождитесь завершения всего задания управления, прежде чем запускать следующую операцию управления устройством.

Компоненты рамы (например, модули CMM, вычислительные узлы, коммутаторы и устройства хранения) обнаруживаются и управляются автоматически при управлении рамой, которая их содержит. Невозможно обнаружить и управлять компонентами рамы отдельно от самой рамы.

Для связи с модулями CMM в раме и контроллерами управления материнской платой на серверах должны быть доступны некоторые порты. Прежде чем приступать к управлению системами, убедитесь, что эти порты доступны. Дополнительные сведения о портах см. в разделе Доступность портов.

Убедитесь, что на каждой системе, которой вы хотите управлять с помощью XClarity Administrator, установлена микропрограмма, удовлетворяющая минимальным требованиям. Минимально необходимые уровни микропрограммы можно найти в Веб-страница поддержки XClarity Administrator — совместимость, открыв вкладку **Совместимость** и щелкнув ссылку для соответствующих типов устройств.

Убедитесь, что для внеполосного обмена данными с CMM заданы по меньшей мере три сеанса режима команд TCP. Сведения о настройке количества сеансов см. в разделе Команда tcpcmdmode в документации по CMM в Интернете.

Рассмотрите возможность реализации адресов IPv4 *или* IPv6 для всех CMM и коммутаторов Flex, управляемых XClarity Administrator. Если для некоторых CMM и коммутаторов Flex используется IPv4, а IPv6 для других, некоторые события могут отсутствовать в журнале аудита (или как ловушки аудита).

Убедитесь, что включено многоадресное перенаправление SLP на стоечные коммутаторы верхнего уровня, а также маршрутизаторы в используемой среде. Чтобы проверить, включено ли многоадресное перенаправление SLP, и найти инструкции по его включению, см. документацию из комплекта конкретного коммутатора или маршрутизатора.

Важно:

- В зависимости от версии микропрограммы коммутатора RackSwitch, может потребоваться вручную включить многоадресное перенаправление SLP и SSH на каждом коммутаторе RackSwitch с помощью приведенных ниже команд, чтобы XClarity Administrator мог обнаружить коммутатор и управлять им. Дополнительные сведения: Стоечные коммутаторы в документации по System x в Интернете.
- Чтобы решение XClarity Administrator могло обнаружить устройство хранения, на каждом устройстве хранения должно быть включено многоадресное перенаправление SLP.
- Если вы планируете использовать настроенный сертификат сервера, включающий вашу собственную информацию, или использовать сертификат, подписанный сторонним центром, создайте и разверните новый сертификат, прежде чем приступать к управлению системами. Информацию о создании собственного сертификата безопасности см. в разделе Работа с сертификатами безопасности в документации по XClarity Administrator в Интернете.
- Если планируется использовать другое программное обеспечение управления помимо Lenovo XClarity Administrator для мониторинга рамы и если такое программное обеспечение управления использует обмен данными SNMPv3, сначала следует создать идентификатор локального пользователя CMM с соответствующими настройками SNMPv3, затем войти в CMM, используя этот идентификатор пользователя, и изменить пароль. Дополнительные сведения см. в разделе Замечания по управлению в документации по XClarity Administrator в Интернете.
- Протоколы обнаружения сервисов, например SLP и SSDP, позволяют XClarity Administrator автоматически обнаруживать тип устройства, которым необходимо управлять, а затем использовать соответствующий механизм для управления им. Устройства некоторых типов не поддерживают протоколы обнаружения сервисов, а в некоторых средах протоколы обнаружения сервисов намеренно отключены. В любом случае для управления необходимо выбрать соответствующий тип устройства. Устройства следующих типов должны идентифицироваться явно.
  - Коммутатор Lenovo ThinkSystem серии DB
  - Коммутатор NVIDIA Mellanox

Об этой задаче

XClarity Administrator может обнаруживать системы в вашей среде путем опроса управляемых устройств, расположенных в той же IP-подсети, что и XClarity Administrator, используя указанный IP-адрес или диапазон IP-адресов либо сведения, импортированные из электронной таблицы.

По умолчанию устройства управляются с помощью управляемой аутентификации XClarity Administrator для входа в систему устройства. При управлении стоечными серверами и рамой Lenovo для входа в устройства можно выбрать локальную или управляемую аутентификацию.

- Если для стоечных серверов, рамы Lenovo и стоечных коммутаторов Lenovo применяется *локальная аутентификация*, XClarity Administrator использует сохраненные учетные данные для аутентификации на устройстве. *Сохраненные учетные данные* могут быть активной учетной записью пользователя на устройстве или учетной записью пользователя на сервере Active Directory.

  В XClarity Administrator необходимо создать сохраненные учетные данные, которые соответствуют активной учетной записи пользователя на устройстве или учетной записи пользователя на сервере Active Directory, прежде чем приступать к управлению устройством с помощью локальной аутентификации (см. раздел Управление сохраненными учетными данными в документации по XClarity Administrator в Интернете).

  Примечания:

  - Устройства RackSwitch поддерживают для аутентификации только сохраненные учетные данные. Учетные данные пользователей XClarity Administrator не поддерживаются.

- *Управляемая аутентификация* позволяет управлять несколькими устройствами и отслеживать их с помощью учетных данных на сервере аутентификации XClarity Administrator, а не локальных учетных данных. Если для устройства используется управляемая аутентификация (не коммутаторы и не серверы ThinkServer и System x M4), XClarity Administrator настраивает устройство и его установленные компоненты на использование сервера аутентификации XClarity Administrator для централизованного управления.
  - Если управляемая аутентификация включена, для управления устройствами можно использовать учетные данные, вводимые вручную, или сохраненные учетные данные (см. разделы Управление учетными записями пользователей и в документации по XClarity Administrator в Интернете).

    Сохраненные учетные данные используются только до тех пор, пока XClarity Administrator не настроит параметры LDAP на устройстве. После этого все изменения в сохраненных учетных данных не оказывают влияния на управление или мониторинг устройства.

    Примечание: Если для устройства включена управляемая аутентификация, изменить для него сохраненные учетные данные с помощью XClarity Administrator невозможно.
  - Если используется локальный или внешний сервер LDAP в качестве сервера аутентификации XClarity Administrator, учетные записи пользователей, которые определены на сервере аутентификации, используются для входа в XClarity Administrator, CMM и контроллеры управления материнской платой в домене XClarity Administrator. Локальные учетные записи пользователей CMM и контроллера управления отключены.
  - Если используется поставщик удостоверений SAML 2.0 в качестве сервера аутентификации XClarity Administrator, учетные записи SAML недоступны для управляемых устройств. Однако если поставщик удостоверений SAML и сервер LDAP используются вместе, и если поставщик удостоверений использует учетные записи, существующие на сервере LDAP, учетные записи пользователей LDAP можно использовать для входа на управляемые устройства, а более сложные способы аутентификации, предоставляемые SAML 2.0 (например, многофакторная аутентификация и единый вход), могут использоваться для входа в XClarity Administrator.
  - Единый вход позволяет пользователю, который уже выполнил вход в XClarity Administrator, автоматически входить в контроллер управления материнской платой. Единый вход включается по умолчанию, если управление сервером ThinkSystem или ThinkAgile осуществляется с помощью XClarity Administrator (кроме случаев, когда управление серверами осуществляется с помощью паролей CyberArk). Можно задать глобальную настройку для включения или выключения единого входа на всех управляемых серверах ThinkSystem и ThinkAgile. При включении единого входа для определенных серверов ThinkSystem и ThinkAgile переопределяется глобальная настройка для всех серверов ThinkSystem и ThinkAgile (см. раздел Управление серверами в документации по XClarity Administrator в Интернете).

    Примечание: При использовании для аутентификации системы управления идентификацией CyberArk функция единого входа отключается автоматически.
  - При включенной управляемой аутентификации для серверов ThinkSystem SR635 и SR655:
    - Микропрограмма контроллера управления материнской платой поддерживает до пяти ролей пользователей LDAP. XClarity Administrator добавляет эти роли пользователей LDAP к серверам во время управления: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** и **lxc-os-admin**.

      Пользователи должны быть назначены по крайней мере одной из указанных ролей пользователей LDAP для связи с серверами ThinkSystem SR635 и SR655.
    - Микропрограмма контроллера управления не поддерживает пользователей LDAP с тем же именем пользователя, что и у локального пользователя сервера.
  - Для серверов ThinkServer и System x M4 сервер аутентификации XClarity Administrator не используется. Вместо этого на устройстве создается учетная запись IPMI с префиксом «LXCA_»,

за которым следует случайная строка. (Существующие локальные учетные записи пользователей IPMI не отключаются.) При прекращении управления сервером ThinkServer учетная запись пользователя «LXCA_» отключается, и префикс «LXCA_» заменяется префиксом «DISABLED_». Чтобы определить, управляется ли сервер ThinkServer другим экземпляром, XClarity Administrator проверяет наличие учетных записей IPMI с префиксом «LXCA_». Если вы решили перевести управляемый сервер ThinkServer на принудительное управление, все учетные записи IPMI на устройстве с префиксом «LXCA_» отключаются и переименовываются. Возможно, стоит вручную удалить учетные записи IPMI, которые больше не используются.

Если вы используете учетные данные, вводимые вручную, XClarity Administrator автоматически создает сохраненные учетные данные и использует их для управления устройством.

Примечания: Если для устройства включена управляемая аутентификация, изменить для него сохраненные учетные данные с помощью XClarity Administrator невозможно.

- При каждом управлении устройством с использованием учетных данных, введенных вручную, для этого устройства создаются новые сохраненные учетные данные, даже если в ходе предыдущего процесса управления для этого устройства были созданы другие сохраненные учетные данные.
- При прекращении управления устройством решение XClarity Administrator не удаляет сохраненные учетные данные, которые были автоматически созданы для этого устройства в ходе процесса управления.

После того как XClarity Administrator начинает управлять системами, XClarity Administrator периодически опрашивает каждую управляемую систему для сбора сведений об инвентаре, важных данных продукта, сведений о состоянии и т. п. Можно просматривать и контролировать каждую управляемую систему и выполнять действия по управлению (например, настраивать параметры системы, развертывать образы операционной системы, включать и выключать питание).

Одновременно только один экземпляр XClarity Administrator может управлять системой. Управление несколькими диспетчерами не поддерживается. Если системой управляет один экземпляр XClarity Administrator, а вы хотите, чтобы ей управлял другой экземпляр XClarity Administrator, сначала необходимо прекратить управление системой текущим экземпляром XClarity Administrator. После этого системой сможет управлять другой экземпляр XClarity Administrator. Сведения об отмене управления системой см. в разделах Неуправляемая рама, Отмена управления серверами, Отмена управления коммутатором RackSwitch и Отмена управления системой хранения данных Lenovo Storage в документации по XClarity Administrator в Интернете.

Примечание: XClarity Administrator не изменяет параметры безопасности или криптографические параметры (криптографический режим и режим, используемый для безопасного обмена данными) во время процесса управления. Криптографические параметры можно изменить после начала управления системой (см. раздел Настройка криптографического режима и протоколов связи в документации по XClarity Administrator в Интернете).

Примечание: XClarity Administrator можно предварительно заполнить инвентарем для демонстрационной рамы (включая модули CMM, вычислительные узлы и коммутаторы), а также демонстрационного стоечного или башенного сервера, имитирующих реальное оборудование. Демонстрационные устройства заполняются на страницах веб-интерфейса и могут использоваться для демонстрации операций управления. Однако эти операции управления будут завершаться сбоем. Например, можно создать шаблон конфигурации и развернуть его на демонстрационном сервере, но развертывание завершится сбоем. Демонстрационные устройства можно удалить, прекратив управление ими (см. разделы Неуправляемая рама и Отмена управления серверами в документации по XClarity Administrator в Интернете). После удаления демонстрационных устройств управлять ими снова будет невозможно.

Процедура

Для обнаружения и управления системами в XClarity Administrator с помощью файла массового импорта выполните следующие действия.

Примечание: При управлении коммутаторами с помощью массового импорта протокол HTTPS на коммутаторе включается и клиенты NTP на нем настраиваются для использования параметров NTP с сервера управления. Для изменения этих параметров необходимо управлять коммутаторами вручную.

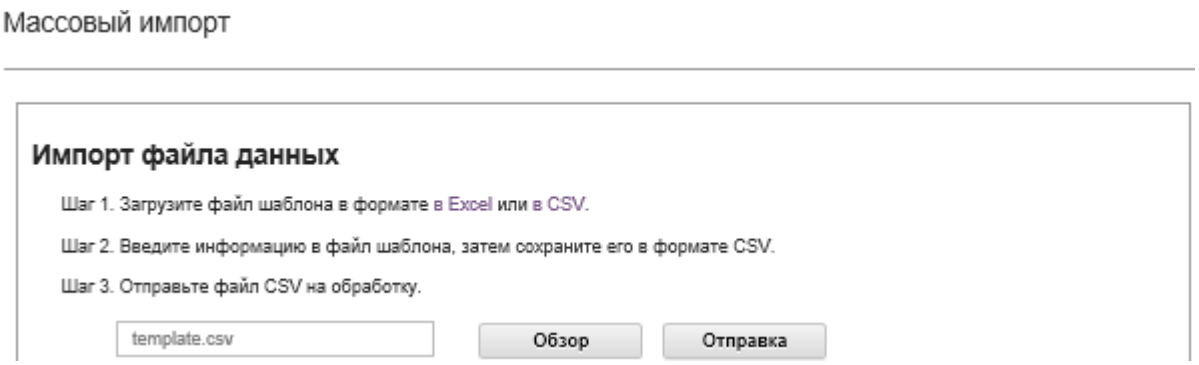
1. В строке меню XClarity Administrator нажмите **Оборудование → Обнаружение новых устройств и управление ими**. Откроется страница Обнаружение и управление.
2. Установите флажок **Включить инкапсуляцию на всех будущих управляемых устройствах**, чтобы изменить правила брандмауэра для всех устройств в процессе управления, чтобы входящие запросы принимались только от XClarity Administrator.

   Примечания:

   - Инкапсуляция не поддерживается для коммутаторов, устройств хранения, рам и серверов других производителей (не Lenovo).
   - Когда интерфейс сети управления настроен для использования протокола DHCP и инкапсуляция включена, управление стоечным сервером может занимать много времени.

   Инкапсуляция может быть включена или отключена на конкретных устройствах после начала управления.

   Внимание: Если инкапсуляция включена и XClarity Administrator становится недоступным до отмены управления устройством, необходимо выполнить ряд действий, чтобы отключить инкапсуляцию для установки связи с устройством. Процедуры восстановления см. в разделах Восстановление управления рамы с CMM после сбоя узла управления и Восстановление управления стоечным или башенным сервером после сбоя сервера управления в документации по XClarity Administrator в Интернете.
3. Нажмите **Массовый импорт**. Откроется мастер «Массовый импорт».



4. Нажмите **в Excel** или **в CSV** на странице «Импорт файла данных», чтобы загрузить шаблонный файл массового импорта в формате Excel или CSV.

   Важно: В зависимости от версии программного обеспечения файл шаблона может быть другим. Убедитесь, что всегда используется шаблон последней версии.
5. Заполните лист данных в файле шаблона и сохраните файл в формате CSV *с разделением запятыми*.

   Рекомендация. Шаблон Excel включает лист **Данные** и лист **Readme**. В листе **Данные** заполните данные устройства. Лист **Readme** содержит информацию о порядке заполнения всех полей на листе **Данные** (включая обязательные для заполнения поля) и примеры данных.

   Важно:

- Управление устройствами осуществляется в порядке, указанном в файле массового импорта.
- XClarity Administrator использует информацию о назначении стойки, определенную в конфигурации устройства, при управлении устройством. Если изменить назначение стойки в XClarity Administrator, XClarity Administrator обновит конфигурацию устройства. При обновлении конфигурации устройства после управления устройством изменения отобразятся в XClarity Administrator.
- Рекомендуется явным образом создать стойку в электронной таблице перед назначением стойки устройству, но это необязательно. Если стойка не определена явным образом и еще не существует в XClarity Administrator, информация о назначении стойки, указанная для устройства, используется для создания стойки с высотой по умолчанию 52U.

  Если требуется использовать другую высоту стойки, необходимо явно определить стойку в электронной таблице перед назначением ее устройству.

Для определения устройств в файле массового импорта заполните следующие столбцы.

- (Столбцы A–C) Для базового обнаружения необходимо указать тип устройства и текущий IP-адрес или серийный номер устройства. Поддерживаются следующие типы.
  - **filler**. Заполнители для неуправляемых устройств. В представлении стойки это устройство отображается в виде универсального заполнителя. Шаблон Excel для дополнительных типов заполнителей см. в листе **Readme**.
  - **flexchassis**. Рама 10U Flex System
  - **server**. Рама и башенные сервера, поддерживаемые XClarity Administrator
  - **rack**. Стойки 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U и 52U. Стойки с другой высотой не поддерживаются. По умолчанию используется 52U.
  - **storage**. Устройства хранения данных
  - **switch**. Коммутаторы RackSwitch

  Примечание: Вычислительные узлы Flex System, коммутаторы и устройства хранения считаются частью процесса обнаружения и управления рамы.
- (Столбцы D–H) Если вы решите использовать вводимые вручную учетные данные вместо сохраненных (столбец Z) или идентификаторов (столбцы AF–AJ), укажите текущее имя пользователя и пароль. Вводить учетные данные вручную полезно, если учетные данные для некоторых устройств различаются. Если не указывать учетные данные для одного или нескольких устройств в файле массового импорта, используются глобальные учетные данные, заданные в диалоговом окне Массовый импорт. Дополнительные сведения о вводимых вручную пользователях и управляемой аутентификации см. в разделе Управление учетными записями пользователей в документации по XClarity Administrator в Интернете.

  Примечания:
  - Для использования вводимых вручную учетных данных необходимо выбрать управляемую аутентификацию XClarity Administrator.
  - Некоторые поля не применяются к ряду устройств.
  - (Для рам) Если выбрана управляемая аутентификация (в столбце AA или в диалоговом окне «Массовый импорт»), необходимо указать пароль `RECOVERY_ID` в столбце G файла массового импорта или в диалоговом окне «Массовый импорт». Если выбрана локальная аутентификация, пароль восстановления не используется; не указывайте пароль восстановления в столбце G файла массового импорта или в диалоговом окне «Массовый импорт».
  - (Для стоечных серверов) Если выбрана управляемая аутентификация (в столбце AA или в диалоговом окне «Массовый импорт»), можно дополнительно указать пароль восстановления в столбце G файла массового импорта или в диалоговом окне «Массовый

импорт». Если выбрана локальная аутентификация, пароль восстановления не используется; не указывайте пароль восстановления в столбце G файла массового импорта или в диалоговом окне «Массовый импорт».

  – (Для стоечных коммутаторов) Устройства RackSwitch поддерживают только сохраненные учетные данные (в столбце Z) для аутентификации на коммутаторах. Учетные данные пользователя, вводимые вручную, не поддерживаются.

- (Столбцы I–U) При необходимости можно предоставить дополнительную информацию, если необходимо применить изменения для устройства после успешного управления.

  Примечание: Некоторые поля не применяются к ряду устройств. Эти поля не применяются к коммутаторам RackSwitch.

- (Столбцы V–Z) При необходимости можно указать сведения для создания и назначения стойки, включая имя стойки, расположение, помещение, самый нижний блок в стойке и высоту.

  Примечания:

  – При создании стойки необходимо указать имя и высоту стойки. Поддерживается следующая высота стойки: 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U и 52U. Стойки с другой высотой не поддерживаются.

  – При создании универсального заполнителя необходимо указать имя стойки и высоту заполнителя. Поддерживается следующая высота заполнителя: 1U, 2U и 4U.

  – При создании определенного заполнителя высота заполнителя игнорируется. XClarity Administrator знает высоту каждого определенного заполнителя. Типы и значения высоты заполнителей см. в шаблоне листа.

  – При назначении устройства стойке высота устройства игнорируется. Высота устройства извлекается из инвентаризации устройства.

- (Столбец AA) Если управление завершилось с одной из следующих ошибок, повторите эту процедуру, используя параметр принудительного управления.

  – Если управляющий экземпляр XClarity Administrator не работает и не может быть восстановлен.

    Примечание: Если предназначенный для замены экземпляр XClarity Administrator использует тот же IP-адрес, что и неисправный экземпляр XClarity Administrator, снова начните управлять устройством, используя учетную запись RECOVERY_ID, пароль (если применимо) и параметр «Принудительное управление».

  – Если управляющий экземпляр XClarity Administrator был отключен до того, как было прекращено управление устройствами.

  – Если управление устройствами было завершено с ошибкой.

  Одновременно только один экземпляр XClarity Administrator может управлять устройствами. Управление несколькими экземплярами XClarity Administrator не поддерживается. Если устройством управляет один экземпляр XClarity Administrator, а вы хотите, чтобы им управлял другой экземпляр XClarity Administrator, сначала прекратите управление устройством для исходного экземпляра XClarity Administrator и начните управление им с использованием другого экземпляра XClarity Administrator.

  Важно: Если вы измените IP-адрес сервера после того, как решение XClarity Administrator начало управлять сервером, XClarity Administrator распознает новый IP-адрес и продолжит управлять сервером. Однако XClarity Administrator не распознает изменение IP-адреса для некоторых серверов. Если после изменения IP-адреса XClarity Administrator показывает, что сервер недоступен, возобновите управление сервером, применив параметр Принудительное управление.

- (Столбец AB) Если вы решили использовать сохраненные учетные данные вместо вводимых вручную (столбец D–H) или идентификаторов (столбцы AF–AJ), укажите идентификатор сохраненных учетных данных. Идентификатор сохраненных учетных данных указан на странице «Сохраненные учетные данные»: выберите **Администрирование → Безопасность** в меню XClarity Administrator и нажмите **Сохраненные учетные данные** на левой панели навигации. Дополнительные сведения о сохраненных учетных данных и локальной аутентификации см. в разделе Управление сохраненными учетными данными в документации по XClarity Administrator в Интернете.

  Примечания:

  – Устройства RackSwtich поддерживают только сохраненные учетные данные для аутентификации. Учетные данные пользователя, вводимые вручную (в столбце D), не поддерживаются.

  – Если управление устройством осуществляется с помощью сохраненных учетных данных и включена управляемая аутентификация, невозможно изменить эти сохраненные учетные данные.

- (Столбец AC) Если вы решаете использовать управляемую аутентификацию для рам и стоечных серверов, можно указать пароль RECOVERY_ID в столбце G файла массового импорта или в диалоговом окне «Массовый импорт». Если выбрана локальная аутентификация, пароль восстановления не используется; не указывайте пароль восстановления в столбце G файла массового импорта или в диалоговом окне «Массовый импорт».
- (Столбец AD) Для стоечных серверов можно дополнительно выбрать использование локальной аутентификации вместо управляемой аутентификации XClarity Administrator, указав в этом столбце значение FALSE. Дополнительные сведения об управляемой и локальной аутентификации см. в разделе Управление сервером аутентификации в документации по XClarity Administrator в Интернете.
- (Столбец AE) При необходимости можно указать список групп ролей, которым разрешено просматривать это устройство и управлять им. Можно указать только группы ролей, к которым принадлежит текущий пользователь.

  Примечание: При добавлении устройств в управляемую раму новые устройства будут принадлежать к той же группе ролей, что и рама.

- (Столбец AF–AJ) Если вы решите использовать систему управления удостоверениями вместо вводимых вручную учетных данных (столбцы D–H) или сохраненных учетных данных (столбцы AB), укажите IP-адрес или имя хоста управляемого сервера, имя пользователя и при необходимости идентификатор приложения, сейф и папку.

  Если вы указываете ИД приложения, необходимо также указать сейф и папку, если применимо.

  Если идентификатор приложения не указывается, XClarity Administrator использует пути, которые были определены при настройке CyberArk для идентификации зарегистрированных в CyberArk учетных записей.

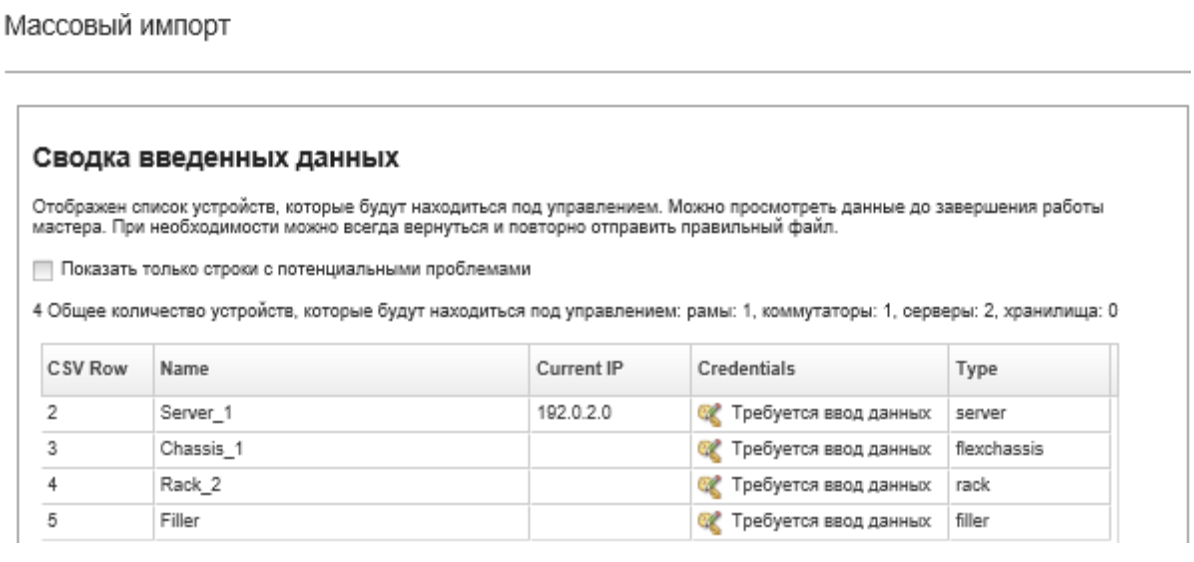
  Примечание: Поддерживаются только серверы ThinkSystem или ThinkAgile. Систему управления идентификацией необходимо настроить в XClarity Administrator, а Lenovo XClarity Controller для управляемых серверов ThinkSystem или ThinkAgile необходимо интегрировать с CyberArk.

На следующем рисунке показан пример файла массового импорта:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Required fields (Type + SN or IP)			Optional fields															
Type	Serial Number	Current IP	Current username	Current password	New password	Recovery password	Switch enable password	New IPv4	IPv4 subnet mask	IPv4 default gateway	IPv4 DNS1	IPv4 DNS2	New IPv6	IPv6 prefix	IPv6 gateway	IPv6 DNS1	IPv6 DNS2	Domain
server		10.1.0.198																
server	P67X30EL																	
flexchassis		10.1.0.213	USERID	passw0rdx	Pa55word@	abcd1234												
flexchassis	Z3499DD				Pa55word@	abcd1234		9.27.20.51	255.255.255.0	9.27.20.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
server	35T88XP												2002:939	2002:9:	2002:939:	2002:9:	2002:9	ebg.lenovo.com
server		10.1.0.214						10.1.2.213	255.255.255.0	10.1.2.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
rack																		
rack																		
filler																		
filler																		
filler																		

R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ
IPv6 DNS2	Domain	Host name	User-defined name	Rack name	Location	Room	Lowest rack unit	Height	Force	Stored credentials ID	Stored credentials ID for RECOVERY_ID	Managed authentication	Role Groups	IdentityManagementSystemEnabled	IMS type	IMS AppID	Folder	Safe
														TRUE	CyberArk	LXCA		Test
			chassis03	SH3G05A34			25		TRUE									
	ebg.lenovo.com	chassis01	chassis01	SH3G05A34			5											
2002:9	ebg.lenovo.com	host4	c02node01	SH3G05B12			38			2	3	FALSE						
	ebg.lenovo.com	host5	web02	SH3G05B12			10											
			SG2R01A01					37										
			SH3G05A34					46										
			APC UPS	SH3G05A34			1	4										
			FC switch	SH3G05A34			40	2										
			KVM switch	SH3G05B12			22	1										

6. В мастере Массовый импорт введите имя CSV-файла, чтобы отправить файл для обработки. Для указания местоположения файла можно нажать **Обзор**.
7. Нажмите **Отправить** для отправки и проверки файла.
8. Нажмите **Далее** для отображения страницы «Сводка ввода» со списком устройств для управления.



9. Просмотрите сводку устройств, которыми вы хотите управлять.

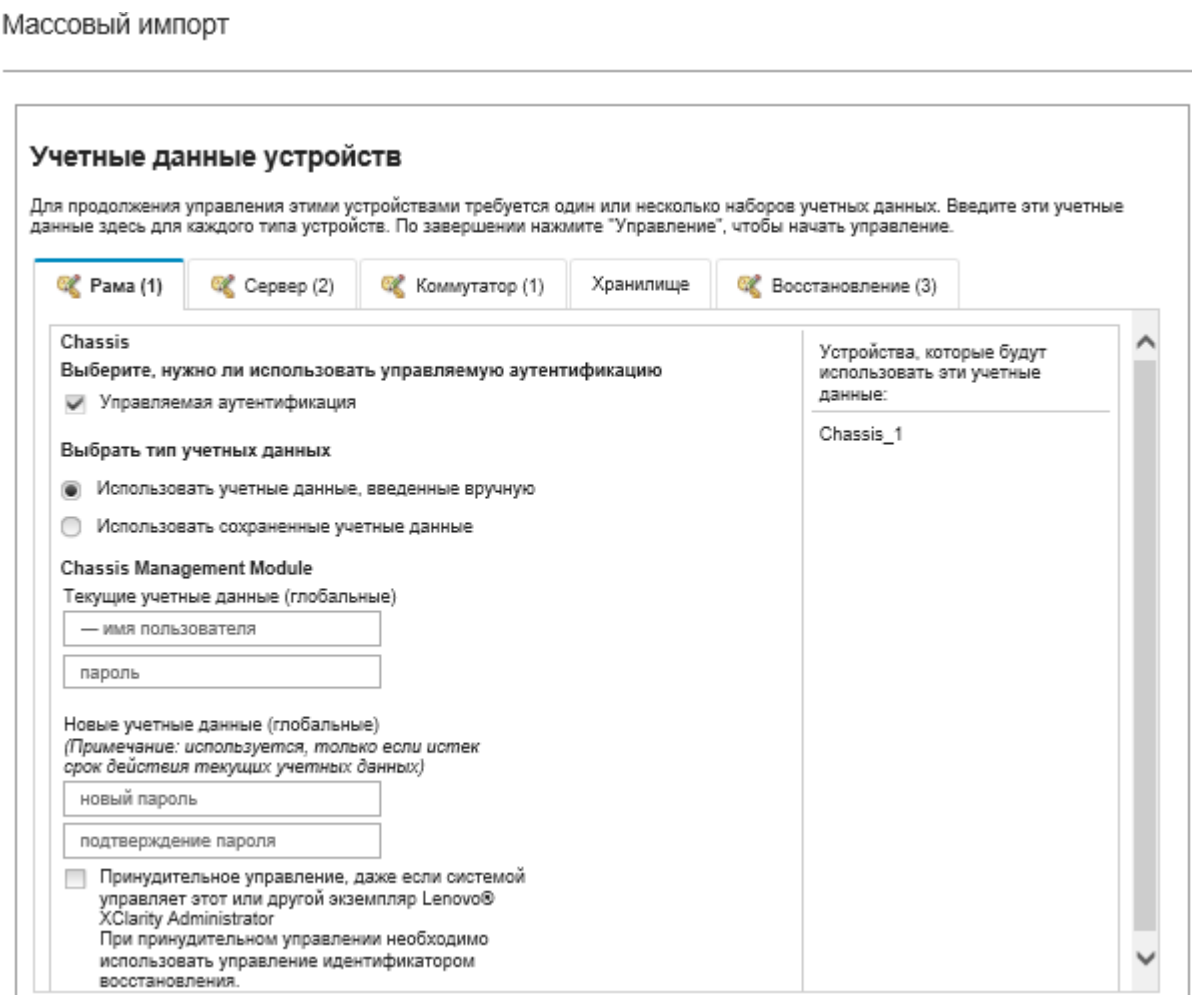
   Выберите **Показывать только строки с потенциальными проблемами**, чтобы отобразить строки с неполными данными. Исправьте все проблемы в файле массового импорта, затем нажмите **Назад** для отправки исправленного CSV-файла.

   Примечания:

   - Если требуемые данных не предоставлены в файле массового импорта, управление связанными устройствами осуществляться не будет.

- На странице Сводка ввода помечены строки, в которых не указаны учетные данные. Если не указать учетные данные в файле массового импорта, будут использоваться глобальные учетные данные, заданные в мастере Массовый импорт.

10. Нажмите **Далее**, чтобы отобразить страницу «Учетные данные устройства».



11. **Необязательно:** Нажмите каждую вкладку и при необходимости задайте глобальные параметры и учетные данные для всех устройств определенного типа. Устройства, которые будут использовать глобальные параметры и учетные данные, перечислены с правой стороны каждой вкладки.

    Если необходимо использовать глобальные учетные данные, учетные данные для определенного типа устройства должны быть одинаковыми для всех устройств одного типа, для которых не введены учетные данные в файле массового импорта. К примеру, учетные данные CMM должны быть одинаковыми для всех рам, а учетные данные управления хранилищем должны быть одинаковыми для всех устройств хранения. Если учетные данные не совпадают, необходимо указать учетные данные в файле массового импорта.

    - **Рама**. Укажите режим аутентификации и тип учетных данных. Укажите текущие учетные данные для входа для всех рам, которые заданы в файле массового импорта. Задайте новый пароль, если срок действия текущих учетных данных CMM истек.

      При принудительном управлении рамой укажите учетную запись RECOVERY_ID и пароль для учетных данных устройства.

- **Серверы**. Укажите режим аутентификации и тип учетных данных. Укажите текущие учетные данные для входа для всех стоечных и башенных серверов, которые заданы в файле массового импорта. Задайте новый пароль, если срок действия текущих учетных данных контроллера управления материнской платой истек.

  При принудительном управлении сервером укажите учетную запись RECOVERY_ID и пароль для учетных данных устройства.
- **Коммутаторы**. Укажите сохраненные учетные данные для входа на все коммутаторы RackSwitch, которые заданы в файле массового импорта. При этом также укажите пароль «включения», который используется для входа в режим привилегированного выполнения (Privileged Exec Mode) в коммутаторе.
- **Хранилище**. Укажите текущие учетные данные для входа во все устройства хранения, которые заданы в файле массового импорта.
- **Восстановление**. Укажите пароль восстановления для входа для всех серверов и рам, которые заданы в файле массового импорта.

  Можно использовать локальную учетную запись пользователя или сохраненные учетные данные восстановления. В любом случае именем пользователя всегда будет `RECOVERY_ID`.

  При задании пароля на устройстве создается учетная запись `RECOVERY_ID` и все учетные записи локальных пользователей отключаются.

  – Для рамы необходимо задать пароль восстановления.

  – Для серверов пароль восстановления является необязательным, если требуется управляемая аутентификация, однако такой пароль не используется, если требуется локальная аутентификация.

  – Убедитесь, что пароль соответствует политиками безопасности и пароля для устройства. Политики безопасности и пароля могут быть разными.

  – Обязательно запишите пароль восстановления для последующего использования.

  – Учетная запись восстановления не поддерживается для серверов ThinkServer и System x M4.

Сведения, указанные в файле массового импорта, заменяют аналогичные сведения, указанные на странице «Учетные данные устройства».

При необходимости можно включить принудительное управление каждым типом устройств, если:

- Устройства в настоящее время управляются другой системой управления, например другим экземпляром XClarity Administrator или IBM Flex System Manager.
- Решение XClarity Administrator было отключено, но перед отключением управление устройствами не было прекращено.
- Управление устройствами не было правильно прекращено, и подписка CIM не была очищена.

Примечание: Если устройство управляется другим экземпляром XClarity Administrator, устройство считается находящимся под управлением исходного экземпляра в течение определенного периода времени после начала принудительного управления. Можно прекратить управление устройством, чтобы удалить его из исходного экземпляра XClarity Administrator.

12. Нажмите **Управление**. На странице «Результаты мониторинга» отображаются сведения о состоянии управления каждого устройства в файле массового импорта.

    Для процесса управления создается задание. Если закрыть мастер «Массовый импорт», выполнение процесса управления продолжится в фоновом режиме. В журнале заданий можно отслеживать состояние процесса управления. Дополнительные сведения о журнале заданий см. в разделе Мониторинг заданий в документации по XClarity Administrator в Интернете.

    Если XClarity Administrator не может войти в систему устройства с учетными данными, которые указаны в файле массового импорта или с глобальными учетными данными, указанными в

диалоговом окне, управление этим устройством невозможно и XClarity Administrator переходит к следующему устройству в файле массового импорта.

Примечания: Если управление завершилось с одной из следующих ошибок, повторите эту процедуру с помощью параметра **Принудительное управление**.

- Если управляющий экземпляр XClarity Administrator не работает и не может быть восстановлен.

  Примечание: Если предназначенный для замены экземпляр XClarity Administrator использует тот же IP-адрес, что и неисправный экземпляр XClarity Administrator, снова начните управлять устройством, используя учетную запись RECOVERY_ID, пароль (если применимо) и параметр **Принудительное управление**.
- Если управляющий экземпляр XClarity Administrator был отключен до того, как было прекращено управление устройствами.
- Если управление устройствами было завершено с ошибкой.

Внимание: Одновременно только один экземпляр XClarity Administrator может управлять устройствами. Управление несколькими экземплярами XClarity Administrator не поддерживается. Если устройством управляет один экземпляр XClarity Administrator, а вы хотите, чтобы им управлял другой экземпляр XClarity Administrator, сначала прекратите управление устройством для исходного экземпляра XClarity Administrator и начните управление им с использованием другого экземпляра XClarity Administrator.

13. Если в файле массового импорта указана новая рама, проверьте и измените параметры сети управления для всей рамы (включая вычислительные узлы и коммутаторы Flex) и настройте информацию вычислительных узлов, локальные хранилища, адаптеры ввода-вывода, целевые объекты загрузки и параметры микропрограммы путем создания и развертывания шаблонов сервера. Дополнительные сведения см. в разделах Изменение параметров IP-адресов управления для рамы и Настройка серверов с помощью XClarity Administrator в документации по XClarity Administrator в Интернете.

После завершения

После управления системами можно выполнять следующие действия:

- Обнаруживать дополнительные системы и управлять ими (см. разделы Управление рамой, Управление стойками, Управление серверами, Управление устройствами хранения и Управление коммутаторами в документации по Lenovo XClarity Administrator в Интернете).
- Настраивать сведения о системе, локальное хранилище, адаптеры ввода-вывода, параметры загрузки и параметры микропрограммы путем создания и развертывания шаблонов серверов (см. раздел Настройка серверов с помощью XClarity Administrator в документации по Lenovo XClarity Administrator в Интернете).
- Развертывать образы операционной системы на серверах без операционной системы (см. раздел Развертывание образа операционной системы в документации по XClarity Administrator в Интернете).
- Обновлять микропрограмму на устройствах, которые не соответствуют текущим политикам (см. раздел Обновление микропрограммы на управляемых устройствах в документации по XClarity Administrator в Интернете).
- Добавлять новые управляемые системы в соответствующую стойку, чтобы отразить фактическую физическую среду (см. раздел Управление стойками в документации по XClarity Administrator в Интернете).
- Контролировать состояние оборудования и просматривать сведения о нем (см. раздел Просмотр состояния управляемого сервера в документации по XClarity Administrator в Интернете).
- Контролировать события и оповещения (см. разделы Работа с событиями и Работа с оповещениями в документации по XClarity Administrator в Интернете).

- Выключите или включите единый вход для управляемых серверов ThinkSystem и ThinkAgile.
  - Для всех управляемых серверов ThinkSystem и ThinkAgile (глобально) нажмите **Администрирование → Безопасность** в строке меню XClarity Administrator, нажмите **Активные сеансы** и включите или выключите **Единый вход**
  - Для определенного сервера ThinkSystem или ThinkAgile нажмите **Оборудование → Сервер** в строке меню XClarity Administrator, а затем нажмите **Все действия → Безопасность → Включение единого входа** или **Все действия → Безопасность → Отключить единый вход**.

  Примечание: Единый вход позволяет пользователю, который уже выполнил вход в XClarity Administrator, автоматически входить в контроллер управления материнской платой. Единый вход включается по умолчанию, если управление сервером ThinkSystem или ThinkAgile осуществляется с помощью XClarity Administrator (кроме случаев, когда управление серверами осуществляется с помощью паролей CyberArk). Можно задать глобальную настройку для включения или выключения единого входа на всех управляемых серверах ThinkSystem и ThinkAgile. При включении единого входа для определенных серверов ThinkSystem и ThinkAgile переопределяется глобальная настройка для всех серверов ThinkSystem и ThinkAgile.

Глава 5. Регистрация XClarity Administrator

Зарегистрировав экземпляр Lenovo XClarity Administrator, можно использовать основные функции, не получая повторяющихся предупреждений об истечении срока действия пробной версии и несоответствующих лицензиях. После регистрации предупреждения о несоответствующих лицензиях больше не отображаются. Однако все функции, для использования которых требуются лицензии, остаются отключенными до приобретения и установки лицензий в зависимости от количества управляемых устройств.

Об этой задаче

Для регистрации экземпляра XClarity Administrator предоставление контактной информации не требуется. Lenovo не передает полученную информацию сторонним организациям.

Если вы установили лицензии для расширенных функций, регистрировать экземпляр XClarity Administrator не требуется. Дополнительные сведения о лицензиях и расширенных функциях см. в разделе Установка лицензии на полнофункциональную активацию

Процедура

Чтобы зарегистрировать XClarity Administrator, выполните следующие действия.

- Если решение XClarity Administrator подключено к Интернету
  1. В строке меню Lenovo XClarity Administrator выберите **Администрирование → Регистрация**, чтобы открыть страницу «Регистрация».
  2. Нажмите **Регистрация**, чтобы зарегистрировать новый экземпляр XClarity Administrator.
  3. Укажите название компании, количество устройств, которыми требуется управлять с помощью XClarity Administrator, и страну, где находится XClarity Administrator.
  4. Нажмите **Отправить**.
- Если решение XClarity Administrator не подключено к Интернету
  1. Зарегистрируйте XClarity Administrator.
     a. В веб-браузере откройте Веб-портал регистрации Lenovo XClarity.
     b. Укажите название компании, количество устройств, которыми требуется управлять с помощью XClarity Administrator, и страну, где находится XClarity Administrator.
     c. Нажмите **Отправить**, чтобы получить маркер регистрации.
  2. В строке меню Lenovo XClarity Administrator выберите **Администрирование → Регистрация**, чтобы открыть страницу «Регистрация».
  3. Нажмите **Импорт**, чтобы импортировать маркер регистрации.
  4. Укажите маркер регистрации, полученный на шаге 1.
  5. Нажмите **Отправить**.

Глава 6. Установка лицензии на полнофункциональную активацию

По истечении срока действия бесплатной 90-дневной пробной версии необходимо приобрести и установить лицензии Lenovo XClarity Pro для всех управляемых устройств, которые поддерживают расширенные функции, чтобы продолжить использование функций развертывания операционных систем и настройки устройств в Lenovo XClarity Administrator. Для получения обслуживания и поддержки XClarity Administrator необходимо иметь лицензии Lenovo XClarity Pro для *всех* управляемых устройств.

Подробнее: XClarity Administrator: установка лицензии

Перед началом работы

Ознакомьтесь со следующими вопросами лицензирования.

- Лицензия *не* привязана к определенному устройству.
- Лицензия на раму предоставляет лицензии для 14 устройств.
- При использовании масштабируемых сложных серверов System x3850 X6 (6241) каждому серверу требуется отдельная лицензия независимо от разделов.
- Если при использовании масштабируемых сложных серверов System x3950 X6 (6241) в них нет деления на разделы, каждому серверу требуется отдельная лицензия. При наличии деления на разделы для каждого раздела требуется отдельная лицензия.
- Следующие устройства *не поддерживают* расширенные функции и, следовательно, *не требуют* лицензий для этих функций. Однако для получения обслуживания и поддержки XClarity Administrator необходимо приобрести лицензию для каждого из этих устройств.
  - Серверы ThinkServer
  - Серверы System x M4
  - Серверы System x X5
  - Серверы System x3850 X6 и x3950 X6 (3837)
  - Устройства хранения данных
  - Коммутаторы

Для установки лицензий необходимо обладать привилегиями **lxc-supervisor** или **lxc-security-admin**.

Об этой задаче

XClarity Administrator поддерживает следующую лицензию.

- **Lenovo XClarity Pro**. Каждая лицензия предоставляет следующие права на одно устройство.
  - Обслуживание и поддержка Lenovo XClarity Integrator
  - Обслуживание и поддержка XClarity Administrator
  - Дополнительные функции в составе XClarity Administrator:
    - Настройка серверов с использованием шаблонов конфигурации
    - Развертывание операционных систем
    - Сообщение о проблемах XClarity Administrator с помощью Call Home (это не повлияет на Call Home для оповещений оборудования)

Период активации лицензии начинается в момент приобретения лицензии и создания кода авторизации.

Соответствие требованиям лицензии определяется с учетом числа управляемых устройств, поддерживающих расширенные функции. Число управляемых устройств не должно превышать общее число лицензий во всех активных лицензионных ключах. Если XClarity Administrator не соответствует установленным лицензиям (например, если срок действия лицензий истек или если из-за управления дополнительными устройствами общее число активных лицензий превышено), у вас есть льготный период 90 дней, чтобы установить соответствующие лицензии. Каждый раз когда XClarity Administrator перестает отвечать требованиям, льготный период сбрасывается до 90 дней. Если льготный период (включая бесплатную пробную версию) завершается до получения соответствующих требованиям лицензий, расширенные функции отключаются для всех устройств.

Например, при управлении 100 дополнительными серверами ThinkSystem и 20 стоечными коммутаторами в существующем экземпляре XClarity Administrator у вас есть 90 дней, чтобы приобрести и установить 100 дополнительных лицензий, прежде чем расширенные функции будут отключены в пользовательском интерфейсе (для всех устройств). Для использования расширенных функций лицензии для 20 стоечных коммутаторов не нужны. Однако они необходимы, если требуется обслуживание и поддержка. Если расширенные функции отключены, они включаются снова после установки достаточного количества лицензий для восстановления соответствия требованиям.

Если вы используете бесплатную пробную лицензию или у вас есть льготный период для соответствия требованиям и вы выполняете обновление до более поздней версии XClarity Administrator, пробная лицензия или льготный период сбрасывается до 90 дней.

Примечания:

- По истечении льготного периода функции настройки сервера и развертывания операционной системы будут отключены.
- Если лицензии не соответствуют требованиям, функция Call Home для разрешения проблем XClarity Administrator (функция Call Home для программного обеспечения) отключается. Льготный период для этой функции не предусмотрен. В то же время функция Call Home для оповещений оборудования не затрагивается.

Если лицензии уже установлены, при обновлении до нового выпуска XClarity Administrator новые лицензии *не* требуются.

Можно определить статус лицензии, включая сколько дней осталось в пробной лицензии, щелкнув в меню действий пользователя (

) в строке заголовка XClarity Administrator и выбрав **Информация**.

Получение помощи

- Если у вас возникли проблемы и вы делали заказ через бизнес-партнера, обратитесь к бизнес-партнеру для проверки транзакции и активации.
- Если вы не получили электронное подтверждение активации, коды авторизации или ключи активации либо они были отправлены неверному лицу, обратитесь к своему региональному представителю.
  - ESDNA@lenovo.com (страны Северной Америки)
  - ESDAP@lenovo.com (страны Азиатско-Тихоокеанского региона)
  - ESDEMEA@lenovo.com (страны Европы, Среднего Востока и Азии)
  - ESDLA@lenovo.com (страны Латинской Америки)
  - ESDChina@Lenovo.com (Китай)
- Если сведения об активации неверны, обратитесь в службу поддержки Lenovo по адресу SW_override@lenovo.com и укажите следующую информацию:
  - Номер заказа
  - Контактную информацию, включая адрес электронной почты
  - Физический адрес

  - Изменения, которые необходимо внести
- При наличии проблем или вопросов о скачивании лицензии обратитесь в службу поддержки Lenovo по адресу -eSupport_-_Ops@lenovo.com.

Установка лицензий на полнофункциональную активацию с помощью веб-интерфейса XClarity Administrator

Если у XClarity Administrator есть доступ в Интернет, веб-интерфейс XClarity Administrator можно использовать для получения и активации лицензий для существующей авторизации, а затем для импорта и установки активированных лицензий.

Перед началом работы

Свяжитесь со своим представителем Lenovo или авторизованным бизнес-партнером, чтобы приобрести лицензии Lenovo XClarity Pro с учетом необходимых функций и числа устройств, которыми требуется управлять. После покупки лицензий вам отправляется код авторизации в *электронном письме с подтверждением ваших прав*. Код авторизации — это 22-значная буквенно-цифровая строка, которая необходима для получения и установки лицензий. Если вы не получили сообщение электронной почты и приобрели лицензии у бизнес-партнера, свяжитесь с бизнес-партнером для запроса кода авторизации.

Кроме того, можно получить коды авторизации из Веб-портал Features on Demand, нажав **Получить код авторизации**.

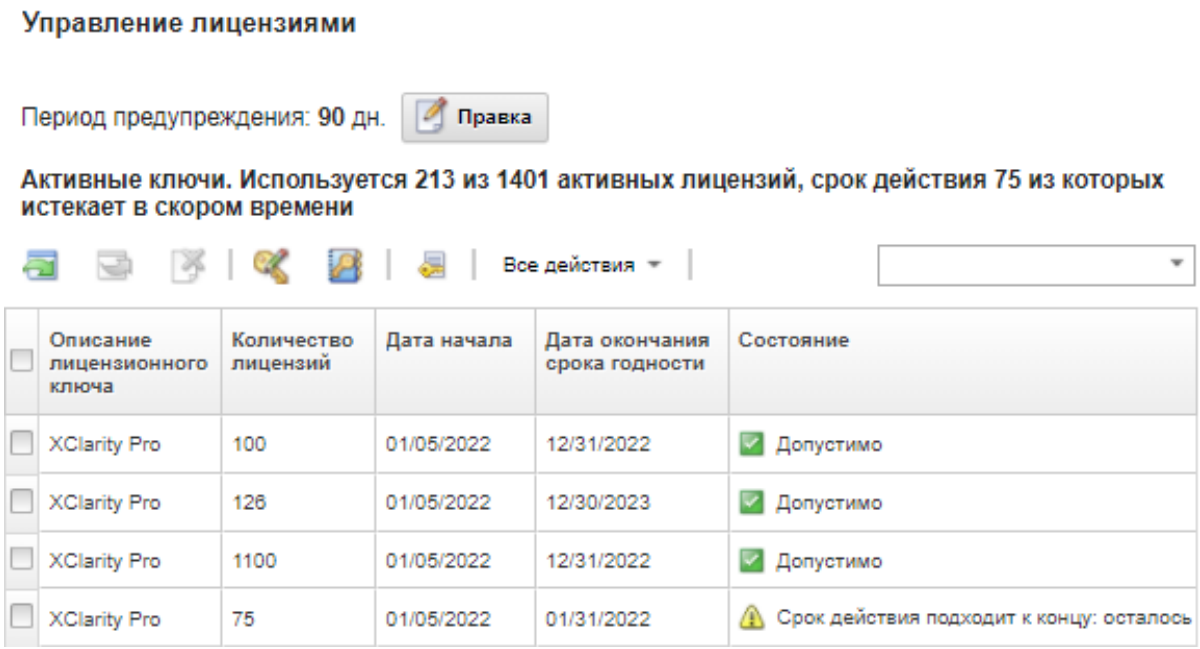
Процедура

Чтобы установить лицензии Lenovo XClarity Pro на сервере управления, выполните одну из следующих процедур.

- **Получение и установка всех или подмножества оставшихся лицензий с использованием одного кода авторизации**

  Можно активировать все доступные лицензии или их подмножество для одного кода авторизации, чтобы создать ключ активации лицензий, представляющий собой файл со всей информации об активированной лицензии. Затем можно установить активированные лицензии, используя файл ключа активации лицензии.

  1. В строке меню XClarity Administrator выберите **Администрирование → Лицензии**, чтобы открыть страницу Управление лицензиями.



2. Щелкните значок **Запросить ключ активации** (), чтобы отобразить диалоговое окно Запрос ключа активации.
3. Нажмите **Единый код авторизации**.
4. Введите 22-значный код авторизации и нажмите **Поиск**, чтобы найти информацию о приобретенных лицензиях для указанного кода авторизации на веб-сайте Features on Demand.

   Если полученный код авторизации не принимается, обратитесь в службу поддержки Lenovo.
5. Введите 10-значный номер клиента Lenovo в поле **Номер клиента Lenovo**.
6. Введите количество лицензий, которые требуется активировать, в поле **Количество для активации** и нажмите кнопку **Продолжить**.

   Чтобы активировать все доступные лицензии в этом коде авторизации, выберите соответствующее значение в поле **Доступные лицензии**.

   При активации подмножества доступных лицензий можно активировать оставшиеся лицензии позже, используя тот же код авторизации.

   Рекомендация. Каждый экземпляр XClarity Administrator поддерживает до 1000 управляемых устройств. Следовательно, один ключ активации лицензии, который можно установить в экземпляре XClarity Administrator, не должен иметь более 1000 лицензий.
7. Проверьте точность контактной информации и при необходимости внесите изменения.
8. Нажмите **Отправить запрос**, чтобы активировать лицензии и создать ключ активации лицензии.
9. Выберите ключ активации лицензии, содержащий лицензии для установки.
10. Нажмите **Установить**, чтобы установить лицензии на сервере управления.
11. Нажмите **Закрыть**.

- **Активируйте и установите все оставшиеся лицензии из нескольких кодов авторизации**

  Можно активировать все оставшиеся лицензии для нескольких кодов авторизации. Для каждого кода авторизации создается ключ активации лицензии. Затем можно установить активированные лицензии, используя ключи активации лицензий. Коды авторизации должны предоставляться в файле в формате CSV с использованием предоставленного шаблона.

1. В строке меню XClarity Administrator выберите **Администрирование → Лицензии**, чтобы открыть страницу Управление лицензиями.
2. Щелкните значок **Запросить ключ активации** (), чтобы отобразить диалоговое окно Запрос ключа активации.
3. Нажмите **Несколько кодов авторизации**.
4. Щелкните ссылку **Скачать шаблон**, чтобы открыть файл Excel. Добавьте каждый код авторизации в файл и сохраните его в формате CSV в локальной системе.
5. Нажмите **Обзор**, чтобы найти и выбрать CSV-файл с кодами авторизации, а затем нажмите **Поиск**, чтобы найти сведения о коде авторизации на веб-сайте поддержки Lenovo.
6. Просмотрите информацию о приобретенной лицензии и доступных ключах активации, связанных с каждым кодом авторизации.
7. Введите 10-значный номер клиента Lenovo в поле **Номер клиента Lenovo**.
8. Проверьте точность контактной информации и при необходимости внесите изменения. Затем нажмите **Продолжить**.
9. Выберите **Да, я хочу использовать все действительные коды авторизации**, а затем нажмите **Отправить запрос**, чтобы генерировать ключи активации лицензии.
10. Выберите ключи активации лицензий, которые требуется установить.
11. Нажмите **Установить**, чтобы установить ключи активации лицензий на сервере управления.
12. Нажмите **Закрыть**.

- **Получение и установка активированных лицензий**

  Можно скачать ключи активации лицензий в локальную систему из экземпляра XClarity Administrator с доступом к Веб-портал Features on Demand, а затем импортировать и установить эти ключи активации лицензий в другом экземпляре XClarity Administrator. Это полезно, если требуется установить лицензии в экземпляре XClarity Administrator, не имеющем доступа к Интернету, или при повторной установке XClarity Administrator, когда требуется восстановить установленные лицензии.

  1. В строке меню XClarity Administrator выберите **Администрирование → Лицензии**, чтобы открыть страницу Управление лицензиями.
  2. Щелкните значок **История извлечения** (), чтобы отобразить диалоговое окно «История извлечения».
  3. Введите номер клиента Lenovo или 22-значный код авторизации.
  4. Нажмите **Поиск**, чтобы извлечь информацию о доступных и активированных лицензиях.

     Если полученный код авторизации не принимается, обратитесь в службу поддержки Lenovo.
  5. Выберите файлы ключей лицензий, которые требуется установить.
  6. Нажмите **Установить**, чтобы установить ключи активации лицензий в XClarity Administrator.
  7. Нажмите **Закрыть**.

- **Импорт и установка активированных лицензий в другом экземпляре XClarity Administrator**

  Если вы активировали лицензии с помощью одного экземпляра XClarity Administrator и хотите установить эти лицензии на другом экземпляре XClarity Administrator или возникает ошибка, требующая восстановления установленных лицензий, файл ключа лицензии можно импортировать из локальной системы в другой экземпляр XClarity Administrator.

  1. В экземпляре XClarity Administrator с доступом к Веб-портал Features on Demand извлеките ключи активации лицензий из Веб-портал Features on Demand, а затем сохраните ключи активации лицензий в качестве файла в локальной системе.
     a. В строке меню XClarity Administrator выберите **Администрирование → Лицензии**, чтобы открыть страницу Управление лицензиями.

b. Щелкните значок **История извлечения** (), чтобы отобразить диалоговое окно «История извлечения».

c. Введите 22-значный код авторизации.

d. Щелкните **Поиск**, чтобы получить информацию о доступных и активированных лицензиях для этого кода авторизации.

   Если полученный код авторизации не принимается, обратитесь в службу поддержки Lenovo.

e. Выберите файлы ключей активации лицензий, которые требуется установить.

f. Щелкните **Скачать**, чтобы сохранить файлы ключей лицензий в локальную систему.

2. В экземпляре XClarity Administrator, где требуется установить ключи активации лицензий:

   a. В строке меню XClarity Administrator выберите **Администрирование → Лицензии**, чтобы открыть страницу Управление лицензиями.

   b. Щелкните значок **Импортировать и применить** (), чтобы импортировать и установить лицензии.

   c. Нажмите **Обзор**, чтобы выбрать ключи активации лицензий, которые требуется установить.

      Чтобы импортировать несколько ключей активации лицензий, упакуйте файлы .KEY в ZIP-архив и выберите ZIP-файл для импорта.

   d. Нажмите **Принять лицензию**, чтобы импортировать и применить лицензии.

      По завершении установки ключи активации лицензий отобразятся в таблице с количеством установленных лицензий и периодом активации (даты начала и окончания срока действия).

После завершения

На странице Лицензии можно выполнять следующие действия.

- Скачайте один или несколько ключей активации лицензий в локальную систему, щелкнув значок **Экспорт** ().

  Примечание: При экспорте нескольких ключей активации лицензий файлы скачиваются в виде одного ZIP-файла.

- Для удаления определенных ключей активации лицензий щелкните значок **Удалить** ().
- Настройте период предупреждения для лицензии, нажав кнопку **Изменить** в верхней части страницы. Период предупреждения лицензии — это количество дней до истечения срока действия лицензий, когда XClarity Administrator отправляет предупреждение.

Получение помощи

- Если у вас возникли проблемы и вы делали заказ через бизнес-партнера, обратитесь к бизнес-партнеру для проверки транзакции и активации.
- Если вы не получили электронное подтверждение активации, коды авторизации или ключи активации либо они были отправлены неверному лицу, обратитесь к своему региональному представителю.
  - ESDNA@lenovo.com (страны Северной Америки)
  - ESDAP@lenovo.com (страны Азиатско-Тихоокеанского региона)
  - ESDEMEA@lenovo.com (страны Европы, Среднего Востока и Азии)
  - ESDLA@lenovo.com (страны Латинской Америки)
  - ESDChina@Lenovo.com (Китай)

- Если сведения об активации неверны, обратитесь в службу поддержки Lenovo по адресу SW_override@lenovo.com и укажите следующую информацию:
  - Номер заказа
  - Контактную информацию, включая адрес электронной почты
  - Физический адрес
  - Изменения, которые необходимо внести
- При наличии проблем или вопросов о скачивании лицензии обратитесь в службу поддержки Lenovo по адресу -eSupport_-_Ops@lenovo.com.

Установка лицензий на использование всех функций с помощью веб-портала Features on Demand

Если у XClarity Administrator *нет* доступа в Интернет, вы можете с помощью Веб-портал Features on Demand получить и активировать лицензии для существующих кодов авторизации из другой системы с сетевым доступом к XClarity Administrator. Затем можно импортировать и установить активированные лицензии с помощью веб-интерфейса XClarity Administrator.

Процедура

Чтобы установить лицензии Lenovo XClarity Pro на сервере управления, выполните следующие действия.

Шаг 1. Приобретите лицензию Lenovo XClarity Pro для каждого управляемого устройства.

Свяжитесь со своим представителем Lenovo или авторизованным бизнес-партнером, чтобы приобрести лицензии Lenovo XClarity Pro с учетом необходимых функций и числа устройств, которыми требуется управлять. После покупки лицензий вам отправляется код авторизации в *электронном письме с подтверждением ваших прав*. Код авторизации — это 22-значная буквенно-цифровая строка, которая необходима для получения и установки лицензий. Если вы не получили сообщение электронной почты и приобрели лицензии у бизнес-партнера, свяжитесь с бизнес-партнером для запроса кода авторизации.

Кроме того, можно получить коды авторизации из Веб-портал Features on Demand, нажав **Получить код авторизации**.

Шаг 2. Активируйте все лицензии или подмножество лицензий с помощью кода авторизации. Сразу после активации лицензий будет создан файл ключа активации лицензии.

1. Откройте Веб-портал Features on Demand в веб-браузере и выполните вход на портал с помощью вашего адреса электронной почты (используется как ваш идентификатор пользователя).
2. Щелкните **Запросить ключ активации**.
3. Выберите **Ввести код авторизации**.
4. Введите 22-символьный код авторизации и нажмите кнопку **Продолжить**.
5. Введите номер клиента Lenovo в поле **Номер клиента Lenovo**.
6. Введите количество лицензий, которые требуется активировать, в поле **Количество для активации** и нажмите кнопку **Продолжить**.

   Чтобы активировать все доступные лицензии в этом коде авторизации, выберите соответствующее значение в поле **Доступные лицензии**.

   При активации подмножества доступных лицензий можно активировать оставшиеся лицензии в другом ключе активации, используя тот же код авторизации.

   Рекомендация. Каждый экземпляр XClarity Administrator поддерживает до 1000 управляемых устройств. Следовательно, один ключ активации лицензии,

устанавливаемый в экземпляре XClarity Administrator, не должен иметь более 1000 лицензий.

7. Следуйте инструкциям, введите сведения о продукте и контактную информацию, а затем нажмите кнопку **Продолжить**, чтобы создать ключ активации лицензии.
8. Дополнительно можно указать и других получателей ключей активации лицензий.
9. Нажмите **Отправить**, чтобы отправить ключи активации лицензий.

   Лицо, указанное в заказе на покупку, и другие получатели получат электронное письмо с ключом активации лицензии. Этот ключ представляет собой файл в формате .KEY.

   Примечание: Также можно скачать ключи активации лицензий (по одному или пакетом) из Веб-портал Features on Demand, нажав **История извлечения** и используя свой номер клиента Lenovo, чтобы найти свои ключи активации лицензий, а затем скачать все ключи или подмножество ключей. Затем нажмите **Эл. почта**, чтобы отправить себе ключи по электронной почте, или **Загрузка**, чтобы загрузить ключи в локальную систему.

Шаг 3. Импортируйте и установите лицензии в XClarity Administrator.

1. В строке меню XClarity Administrator выберите **Администрирование → Лицензии**, чтобы открыть страницу Управление лицензиями.
2. Щелкните значок **Импортировать и применить** (), чтобы установить лицензии.
3. Нажмите **Обзор**, чтобы выбрать файл ключа активации для лицензий, которые требуется установить.

   Рекомендация. Чтобы импортировать несколько ключей активации лицензий, упакуйте файлы .KEY в ZIP-архив и выберите ZIP-файл для импорта.
4. Нажмите **Принять лицензию**, чтобы импортировать и применить лицензии.

   По завершении установки ключ активации лицензии отобразится в таблице с количеством установленных лицензий и периодом активации (даты начала и окончания срока действия).

После завершения

На странице Лицензии можно выполнять следующие действия.

- Скачайте один или несколько ключей активации лицензий в локальную систему, щелкнув значок **Экспорт** ().

  Примечание: При экспорте нескольких ключей активации лицензий файлы скачиваются в виде одного ZIP-файла.
- Для удаления определенных ключей активации лицензий щелкните значок **Удалить** ().
- Настройте период предупреждения для лицензии, нажав кнопку **Изменить** в верхней части страницы. Период предупреждения лицензии — это количество дней до истечения срока действия лицензий, когда XClarity Administrator отправляет предупреждение.

Получение помощи

- Если у вас возникли проблемы и вы делали заказ через бизнес-партнера, обратитесь к бизнес-партнеру для проверки транзакции и активации.
- Если вы не получили электронное подтверждение активации, коды авторизации или ключи активации либо они были отправлены неверному лицу, обратитесь к своему региональному представителю.
  - ESDNA@lenovo.com (страны Северной Америки)
  - ESDAP@lenovo.com (страны Азиатско-Тихоокеанского региона)

  - ESDEMEA@lenovo.com (страны Европы, Среднего Востока и Азии)
  - ESDLA@lenovo.com (страны Латинской Америки)
  - ESDChina@Lenovo.com (Китай)
- Если сведения об активации неверны, обратитесь в службу поддержки Lenovo по адресу SW_override@lenovo.com и укажите следующую информацию:
  - Номер заказа
  - Контактную информацию, включая адрес электронной почты
  - Физический адрес
  - Изменения, которые необходимо внести
- При наличии проблем или вопросов о скачивании лицензии обратитесь в службу поддержки Lenovo по адресу -eSupport_-_Ops@lenovo.com.

Глава 7. Обновление XClarity Administrator как

При запуске Lenovo XClarity Administrator в качестве контейнера используйте эту процедуру обновления, чтобы установить новейшее ПО в качестве нового контейнера и привязать тома исходного контейнера к новому.

Перед началом работы

Обновление XClarity Administrator до версии 4.0 или более поздней версии можно выполнить только из экземпляра XClarity Administrator версии не ниже 3.0. Если вы используете XClarity Administrator более ранней версии, чем 3.0, нужно сначала выполнить обновление до версии 3.0 и только после этого выполнять обновление до версии 4.0.

Для управления экземплярами XClarity Administrator версии 4.0 или более поздней версии с использованием Lenovo XClarity Orchestrator требуется XClarity Orchestrator версии не ниже 2.0. Если вы обновляете XClarity Administrator до версии 4.0 или более поздней версии, убедитесь, что текущая версия XClarity Orchestrator не ниже 2.0.

Об этой задаче

Файл `docker-compose.yml` использует следующие переменные среды, которые вы задаете во время установки *исходного* контейнера. Эти переменные среды также используются новым контейнером.

- **CONTAINER_NAME**. Уникальное имя контейнера, используемое для создания томов Docker для каждого экземпляра XClarity Administrator (например, `CONTAINER_NAME=LXCA-203`)

  XClarity Administrator использует имя контейнера для создания томов для этого контейнера. Если вы используете то же имя для нового контейнера, новый экземпляр XClarity Administrator будет использовать те же тома и, следовательно, иметь доступ к тем же системным данным и параметрам, что и первоначальный экземпляр XClarity Administrator (контейнер).

  Если вы меняете имя контейнера, для контейнера создаются новые тома и новый экземпляр XClarity Administrator не будет иметь доступа к тем же системным данным и параметрам, что и первоначальный экземпляр XClarity Administrator (контейнер). Если нужно изменить имя или IP-адрес контейнера, создайте резервную копию системных данных и параметров исходного экземпляра XClarity Administrator, прежде чем устанавливать новый контейнер, а затем используйте эту резервную копию для восстановления системных данных и параметров в новом контейнере.
- **ADDRESS**. Статический адрес IPv4 или IPv6 для контейнера (например, `ADDRESS=192.0.2.0`)

  При изменении IP-адреса XClarity Administrator после управления устройствами устройства могут перейти в XClarity Administrator в состояние «не в сети». Перед изменением IP-адреса убедитесь, что все устройства являются неуправляемыми.
- **BACKUP_MOUNT** и **FIRMWARE_MOUNT**. (Необязательно) Пути удаленных общих ресурсов, которые можно использовать для хранения резервных копий XClarity Administrator или в качестве удаленного репозитория для обновлений микропрограмм. Пути должны иметь вид `/mnt/backup_share` и `/mnt/fw_share` соответственно.

Примечание: XClarity Administrator *не* работает в качестве привилегированного контейнера.

Процедура

Для обновления контейнера XClarity Administrator выполните следующие действия.

Шаг 1. Скачайте образ контейнера XClarity Administrator с Веб-страница загрузки XClarity Administrator на клиентскую рабочую станцию. Войдите на веб-сайт и используйте предоставленный вам ключ доступа для скачивания образа.

Шаг 2. Импортируйте образ контейнера XClarity Administrator в хост docker, выполнив следующую команду.

```
docker load -i lnvgy_sw_lxca_1l0-3.5.0_anyos_noarch
```

Шаг 3. Отредактируйте файл `docker-compose.yml`, который использовался для исходного контейнера. Обновите свойство образа в верхней части файла, чтобы указать на новый образ Docker из шага 2. Изменить метку образа можно с помощью команды `docker tag`.

Ниже представлен пример файла yml с включенной поддержкой IPv6.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
```

```
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
```

Шаг 4. Завершите работу *исходного* контейнера, выполнив следующую команду.
`docker-compose -p ${CONTAINER_NAME} down`

Шаг 5. Разверните *новый* образ в Docker, выполнив следующую команду, где <*ENV_FILENAME*> — имя файла переменных среды.
COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file` <*ENV_FILENAME*> `up -d`

Глава 8. Удаление XClarity Administrator

Выполните эти действия, чтобы удалить виртуальное устройство Lenovo XClarity Administrator или контейнер.

Процедура

Чтобы удалить виртуальное устройство XClarity Administrator, выполните указанные ниже действия.

Шаг 1. Прекратите управление всеми устройствами, которыми в настоящее время управляет XClarity Administrator (см. разделы Управление рамой, Управление серверами и Управление коммутаторами в документации по XClarity Administrator в Интернете).

Шаг 2. Для удаления XClarity Administrator выполните указанные ниже действия в зависимости от операционной системы.

- **Docker-compose**Выполните следующую команду, чтобы остановить контейнер и удалить сети и тома.
  ```
  docker-compose down -v
  ```
- **CentOS, Red Hat, Rocky и Ubuntu**
  1. Подключитесь к хосту с помощью диспетчера виртуальных машин.
  2. Щелкните правой кнопкой мыши виртуальную машину и выберите **Завершить работу → Принудительно выключить**.
  3. Снова нажмите правой кнопкой мыши виртуальную машину и выберите **Удалить**. Откроется диалоговое окно Подтверждение удаления.
  4. Установите все флажки и нажмите **Удалить**.
- **ESXi**
  1. Подключитесь к хосту с помощью VMware vSphere Client.
  2. Нажмите правой кнопкой мыши виртуальную машину и выберите **Питание → Выключить питание**.
  3. Снова нажмите правой кнопкой мыши виртуальную машину и выберите **Удалить с диска**.
- **Hyper-V**
  1. На информационной панели «Диспетчер серверов» нажмите **Hyper-V**.
  2. Нажмите правой кнопкой мыши сервер и выберите **Диспетчер Hyper-V**.
  3. Нажмите правой кнопкой мыши виртуальную машину и выберите **Завершить работу**.
  4. Снова нажмите правой кнопкой мыши виртуальную машину и выберите **Удалить**.