Lenovo

Руководство пользователя XClarity Controller с Intel Xeon SP (1-го и 2-го поколений)

Примечание: Перед тем как воспользоваться этой информацией, обязательно прочтите общую информацию в разделе Приложение B «Замечания» на странице 223.

Пятнадцатое издание (Май 2021 г.)

Содержание

Глава 1. Введение

Lenovo XClarity Controller (XCC) — это контроллер управления нового поколения, который заменяет контроллер управления материнской платой (BMC) для серверов Lenovo ThinkSystem.

Это следующее поколение служебного процессора Integrated Management Module II (IMM2), объединяющее функциональность служебных процессоров, отличные показатели ввода-вывода, видеоконтроллер и функции удаленного присутствия в одном чипе на серверной материнской плате. Контроллер обеспечивает следующие функции:

- Возможность выбора выделенного или совместно используемого подключения Ethernet для управления системами
- Поддержка HTML5
- Поддержка доступа через XClarity Mobile
- Диспетчер XClarity Provisioning Manager
- Удаленная настройка конфигурации с помощью интерфейса командной строки XClarity Essentials или XClarity Controller.
- Возможность локального или удаленного доступа к XClarity Controller для приложений и инструментов
- Расширенные функции удаленного присутствия.
- Поддержка API REST (схема Redfish) для дополнительных услуг в Интернете и программных приложений.

  Примечание: В настоящее время XClarity Controller поддерживает API управления масштабируемыми платформами Redfish в спецификации 1.0.2 и схему 2016.2

Примечания:

- В веб-интерфейсе XClarity Controller контроллер BMC используется в применении к XCC.
- Выделенный сетевой порт управления системами может быть недоступен на некоторых серверах ThinkSystem; на таких серверах доступ к XClarity Controller возможен только через используемый совместно с серверной операционной системой сетевой порт.
- Для серверов Flex модуль Chassis Management Module (CMM) является основным модулем управления для выполнения функций системного управления. Доступ к контроллеру XClarity Controller возможен только через сетевой порт в модуле CMM.

В этом документе рассказывается об использовании функций контроллера XClarity Controller на сервере ThinkSystem. Контроллер XClarity Controller взаимодействует с XClarity Provisioning Manager и UEFI, обеспечивая функции системного управления для серверов ThinkSystem.

Для проверки обновлений микропрограммы выполните следующие действия.

Примечание: Осуществляя доступ на портал поддержки Support Portal в первый раз, необходимо выбрать категорию продукта, семейство продукта и номера моделей для своего сервера. При следующем входе на портал Support Portal выбранные вами изначально продукты будут предзагружены веб-сайтом, на странице отобразятся только ссылки на эти продукты. Чтобы изменить список продуктов или добавить в него записи, щелкните ссылку **Управление моими списками продуктов**. На веб-сайте периодически вносятся изменения. Процедуры поиска микропрограмм и документации могут несколько отличаться от описанных в данном документе.

1. Перейдите к шагу http://datacentersupport.lenovo.com.
2. В разделе **Support (Поддержка)** выберите **Data Center (Центр обработки данных)**.

3. При загрузке содержимого выберите **Servers (Серверы)**.
4. В разделе **Select Series (Выбор серий)** сначала выберите определенные серии серверного оборудования, затем в разделе **Select SubSeries (Выбор подсерий)** — определенные подсерии серверных продуктов, а в разделе **Select Machine Type (Выбор типа компьютера)** — определенный тип компьютера.

Функции XClarity Controller уровней Standard, Advanced и Enterprise

Пользователям XClarity Controller предлагается функциональность XClarity Controller уровней Standard, Advanced и Enterprise. См. дополнительные сведения об уровне контроллера XClarity Controller, установленного на вашем сервере, в документации к вашему серверу. На всех уровнях обеспечивается следующее:

- Круглосуточный удаленный доступ и управление сервером
- Удаленное управление независимо от состояния управляемого сервера
- Удаленный контроль оборудования и операционных систем

Примечание: Некоторые функции могут быть не применимы к серверам Flex System.

Ниже приводится список функций XClarity Controller уровня Standard:

Функции XClarity Controller уровня Standard

Ниже приводится список функций XClarity Controller уровня Standard:

Соответствующие отраслевым стандартам интерфейсы управления

- Интерфейс IPMI 2.0
- Redfish
- CIM-XML
- DCMI 1.5
- SNMPv3
- SNMPv1 (только ловушки) требует обновлений микропрограммы XCC до версии не ниже 2.10 или 2.12 в зависимости от типа сервера. См. подробные сведения в файле изменений в обновлениях микропрограммы XCC.

Другие интерфейсы управления

- Интернет
- Устаревший интерфейс командной строки
- USB-разъем на лицевой панели — виртуальная панель оператора на мобильном устройстве

Управление питанием/сбросом

- Питание включено
- Жесткое и мягкое завершение работы
- Управление питанием по расписанию
- Сброс системы
- Управление порядком загрузки

Журналы событий

- SEL IPMI

- Понятный для пользователя журнал
- Журнал аудита

Мониторинг окружающей среды

- Безагентский мониторинг
- Мониторинг датчиков
- Управление вентилятором
- Управление светодиодными индикаторами
- Ошибки набора микросхем (Caterr, IERR и т. д....)
- Индикация работоспособности системы
- Мониторинг производительности OOB для адаптеров ввода/вывода
- Отображение и экспорт инвентаризационных данных

RAS

- Виртуальное прерывание NMI
- Автоматическое восстановление микросхемы
- Автоматическое продвижение резервной микропрограммы
- Watchdog POST
- Watchdog загрузчика ОС
- Захват синего экрана (сбой ОС)
- Встроенные средства диагностики

Конфигурация сети

- IPv4
- IPv6
- IP-адрес, маска подсети, шлюз
- Режимы назначения IP-адресов
- Имя хоста
- Программируемый MAC-адрес
- Выбор двойного MAC-адреса (если поддерживается серверным оборудованием)
- Переназначения сетевых портов
- Добавление меток виртуальной локальной сети

Сетевые протоколы

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SNMPv1 (только ловушки)
- SSL
- SSH

- SMTP
- Клиент LDAP
- NTP
- SLP
- SSDP

Оповещения

- Ловушки PET
- Индикация CIM
- Ловушки SNMP
- Электронная почта
- События Redfish

Последовательное перенаправление

- SOL IPMI
- Конфигурация последовательного порта

Безопасность

- Базовый доверенный источник оценки (CRTM) XClarity Controller
- Обновления микропрограмм с цифровой подписью
- Управление доступом на основе ролей (RBAC)
- Локальные учетные записи пользователей
- Учетные записи пользователей LDAP/AD
- Безопасный откат микропрограмм
- Обнаружение нарушения целостности рамы (только в некоторых моделях серверов)
- Удаленное подтверждение XCC физического присутствия TPM UEFI
- Ведение журнала аудита изменений конфигурации и действий сервера
- Аутентификация с открытым ключом
- Вывод из эксплуатации/изменение назначения системы

Удаленное присутствие

- RDOC (Remote Disk on Card): подключение удаленных файлов ISO/IMG в качестве виртуальных носителей с использованием протоколов CIFS, NFS, HTTP, HTTPS, FTP, SFTP и LOCAL

Управление электропитанием

- Индикатор питания в режиме реального времени

Управление лицензиями

- Проверка и репозиторий ключей активации

Развертывание и настройка конфигурации

- Удаленная настройка конфигурации
- Инструменты развертывания и настройки конфигурации, а также пакеты драйверов, использующие встроенный диспетчер XClarity Provisioning Manager

- Резервное копирование и восстановление конфигурации

Обновления микропрограммы

- Безагентское обновление
- Удаленное обновление

Функции XClarity Controller уровня Advanced

Ниже приводится список функций XClarity Controller уровня Advanced:

Все функции XClarity Controller уровня Standard плюс:

Оповещения

- Syslog

Удаленное присутствие

- Удаленное управление KVM

Последовательное перенаправление

- Последовательное перенаправление через SSH

Безопасность

- Диспетчер Security Key Lifecycle Manager (SKLM)
- Блокировка IP-адресов

Управление электропитанием

- Графическое представление питания в режиме реального времени
- Счетчики питания за прошлые периоды
- Графическое представление температуры

Развертывание и настройка конфигурации

- Удаленное развертывание ОС с помощью встроенного диспетчера XClarity Provisioning Manager с функцией удаленного управления KVM XClarity Controller

Функции XClarity Controller уровня Enterprise

Ниже приводится список функций XClarity Controller уровня Enterprise:

Все функции XClarity Controller уровней Standard и Advanced плюс:

RAS

- Фиксация загрузки

Удаленное присутствие

- Управление качеством/полосой пропускания
- Совместная работа на виртуальной консоли (шесть пользователей)
- Чат виртуальной консоли
- Виртуальные носители

  - Подключение удаленных ISO/IMG-файлов через удаленную консоль
  - Подключение файла из сети: - подключение файла изображений ISO или IMG с файлового сервера (HTTPS, CIFS, NFS) к хосту в качестве накопителя DVD или USB

Управление электропитанием

- Ограничение энергопотребления
- Мониторинг производительности OOB — показатели производительности системы

Развертывание и настройка конфигурации

- Удаленное развертывание с помощью Lenovo XClarity Administrator. При использовании Lenovo XClarity Administrator для развертывания операционных систем дополнительные сведения о поддерживаемых операционных системах см. в разделе http://sysmgt.lenovofiles.com/help/index.jsp?topic=%2Fcom.lenovo.lxca.doc%2Fsupported_operating_system_images.html.

Обновление XClarity Controller

Если сервер поставлялся с микропрограммой XClarity Controller уровня Standard или Advanced, вы, возможно, сможете обновить функциональность XClarity Controller на вашем сервере. Дополнительные сведения о доступных уровнях обновления и способах оформления заказа см. в разделе Глава 8 «Управление лицензиями» на странице 95.

Требования к веб-браузеру и операционной системе

Воспользуйтесь информацией из этого раздела для просмотра списка поддерживаемых браузеров, комплектов шифров и операционных систем для вашего сервера.

Веб-интерфейс XClarity Controller требует использования одного из следующих веб-браузеров:

- Chrome 48.0 или выше (55.0 или выше для удаленной консоли)
- Firefox ESR 38.6.0 или выше
- Microsoft Edge
- Safari 9.0.2 или выше (iOS 7 или выше и OS X)

Примечание: Поддержка функции удаленной консоли недоступна в браузере на ОС для мобильных устройств.

Вышеперечисленные браузеры соответствуют микропрограммам XClarity Controller, которые поддерживаются в настоящее время. Микропрограмма XClarity Controller может периодически совершенствоваться путем добавления поддержки других браузеров.

В зависимости от версии микропрограммы XClarity Controller поддержка веб-браузеров может отличаться от перечисленных в этом разделе. Список поддерживаемых браузеров для текущих микропрограмм XClarity Controller доступен в пункте меню **Поддерживаемые браузеры** на странице входа XClarity Controller.

В целях безопасности при использовании HTTPS теперь поддерживаются только шифры высокой стойкости. При использовании HTTPS комбинация клиентской ОС и браузера должна поддерживать один из следующих комплектов шифров:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

В кэше интернет-браузера хранятся сведения о посещенных вами веб-страницах, поэтому в будущем они будут загружаться быстрее. После обновления микропрограммы XClarity Controller с удалением предыдущей версии ваш браузер, возможно, продолжит использовать информацию из кэша, вместо того чтобы извлекать ее из XClarity Controller. После обновления микропрограммы XClarity Controller рекомендуется очистить кэш браузера, чтобы обслуживаемые XClarity Controller веб-страницы отображались правильно.

Поддержка нескольких языков

Воспользуйтесь информацией из этого раздела для просмотра списка языков, поддерживаемых XClarity Controller.

По умолчанию выбранный язык веб-интерфейса XClarity Controller — английский. В интерфейсе может отображаться несколько языков. Сюда относятся следующие:

- Французский
- Немецкий
- Итальянский
- Японский
- Корейский
- Португальский (Бразилия)
- Русский
- Упрощенный китайский
- Испанский (международный)
- Традиционный китайский

Чтобы выбрать нужный язык, щелкните стрелку рядом с выбранным в настоящее время языком. Откроется раскрывающееся меню, где можно выбрать нужный язык.

Текстовые строки, создаваемые микропрограммой XClarity Controller, отображаются на языке, указанном браузером. Если браузер указывает язык, отличный от одного из вышеуказанных языков перевода, текст отображается на английском языке. Кроме того, любая текстовая строка, отображаемая микропрограммой XClarity Controller, но не созданная XClarity Controller (например, сообщения, созданные UEFI, адаптерами PCIe и т. д....) отображаются на английском языке.

Ввод текста на каком-либо языке, отличном от английского, например в *сообщении при нарушении*, в настоящее время не поддерживается. Поддерживается только текст, введенный на английском языке.

Базы MIB: введение

Воспользуйтесь информацией из этого раздела для получения доступа к базе информации управления.

Базы информации управления SNMP можно загрузить через https://support.lenovo.com/ (выполните поиск на портале по типу компьютера). Он содержит следующие четыре базы MIB:

- База **MIB SMI** содержит описание структуры информации управления для Lenovo Data Center Group.
- База **MIB продуктов** содержит описание идентификатора объектов для продуктов Lenovo.
- База **MIB XCC** содержит информацию о ресурсах и мониторинге для Lenovo XClarity Controller.
- База **MIB оповещений XCC** определяет ловушки для условий оповещений, обнаруженные Lenovo XClarity Controller.

Примечание: Эти четыре базы MIV импортируются в следующем порядке: **MIB SMI** → **MIB продуктов** → **MIB XCC** → **MIB оповещений XCC**.

Замечания в этом документе

Эти сведения помогут понять, какие замечания используются в этом документе.

В документации используются следующие замечания.

- **Примечание.** Эти замечания содержат важные советы, рекомендации или подсказки.
- **Важно!** Эти замечания содержат информацию или советы, которые могут помочь избежать неудобных или неприятных ситуаций.
- **Внимание!** Эти замечания указывают на опасность повреждения программ, устройств и данных. Замечание «Внимание!» размещается непосредственно перед инструкцией или ситуацией, в которой может произойти такое повреждение.

Глава 2. Открытие и использование веб-интерфейса XClarity Controller

В этом разделе описаны процедуры входа и действия, которые можно выполнить из веб-интерфейса XClarity Controller.

XClarity Controller сочетает на одной микросхеме функции обработки процессора служб, контроллера видео и удаленного присутствия. Для получения удаленного доступа к XClarity Controller с использованием веб-интерфейса XClarity Controller сначала необходимо выполнить вход в систему. В этой главе описаны процедуры входа и действия, которые можно выполнить из веб-интерфейса XClarity Controller.

Доступ к веб-интерфейсу XClarity Controller

В этом разделе содержится информация о доступе к веб-интерфейсу XClarity Controller.

XClarity Controller поддерживает статическую и динамическую адресацию DHCP IPv4. Статический адрес IPv4 по умолчанию, присваиваемый XClarity Controller, — 192.168.70.125. XClarity Controller изначально настраивается так, чтобы пытаться получить адрес от сервера DHCP; если сделать это не удается, используется статический адрес IPv4.

Контроллер XClarity Controller также поддерживает адрес IPv6, однако у него отсутствует фиксированный статический адрес IPv6 IP по умолчанию. Для первоначального доступа к XClarity Controller в среде IPv6 можно воспользоваться IP-адресом IPv4 или локальным адресом канала IPv6. XClarity Controller создает уникальный локальный адрес канала IPv6 на основе MAC-адреса IEEE 802, вставляя два октета с шестнадцатеричными значениями 0xFF и 0xFE в середине 48-битного MAC-адреса, как описано в RFC4291, и преобразуя второй бит справа в первом октете этого MAC-адреса. Например, если MAC-адрес имеет вид 08-94-ef-2f-28-af, локальный адрес канала будет выглядеть так: `fe80::0a94:efff:fe2f:28af`

При осуществлении доступа к XClarity Controller по умолчанию заданы следующие условия IPv6:

- Включена автоматическая конфигурация адреса IPv6.
- Статическая конфигурация IP-адреса IPv6 выключена.
- DHCPv6 включен.
- Автоматическая конфигурация без запоминания состояния включена.

XClarity Controller позволяет использовать *выделенное* сетевое подключение управления системами (если применимо) или *используемое совместно* с сервером. По умолчанию для установленных в стойку серверов и серверов башенного типа используется *выделенный* сетевой разъем управления системами.

Выделенное сетевое подключение управления системами на большинстве серверов предоставляется с помощью отдельного контроллера сетевого интерфейса 1Gbit. Однако в некоторых системах выделенное сетевое подключение управления системами может предоставлять с помощью интерфейса NCSI на одном из сетевых портов контроллера сетевых интерфейсов с несколькими портами. В этом случае выделенное сетевое подключение управления системами ограничено скоростью 10/100 интерфейса NCSI. Сведения о реализации порта управления в системе и любых применимых ограничениях см. в документации по системе.

Примечание: Возможно, *выделенный* сетевой порт управления системами недоступен на вашем сервере. Если на вашем оборудовании отсутствует *выделенный* сетевой порт, *используемый совместно* — единственный доступный параметр XClarity Controller.

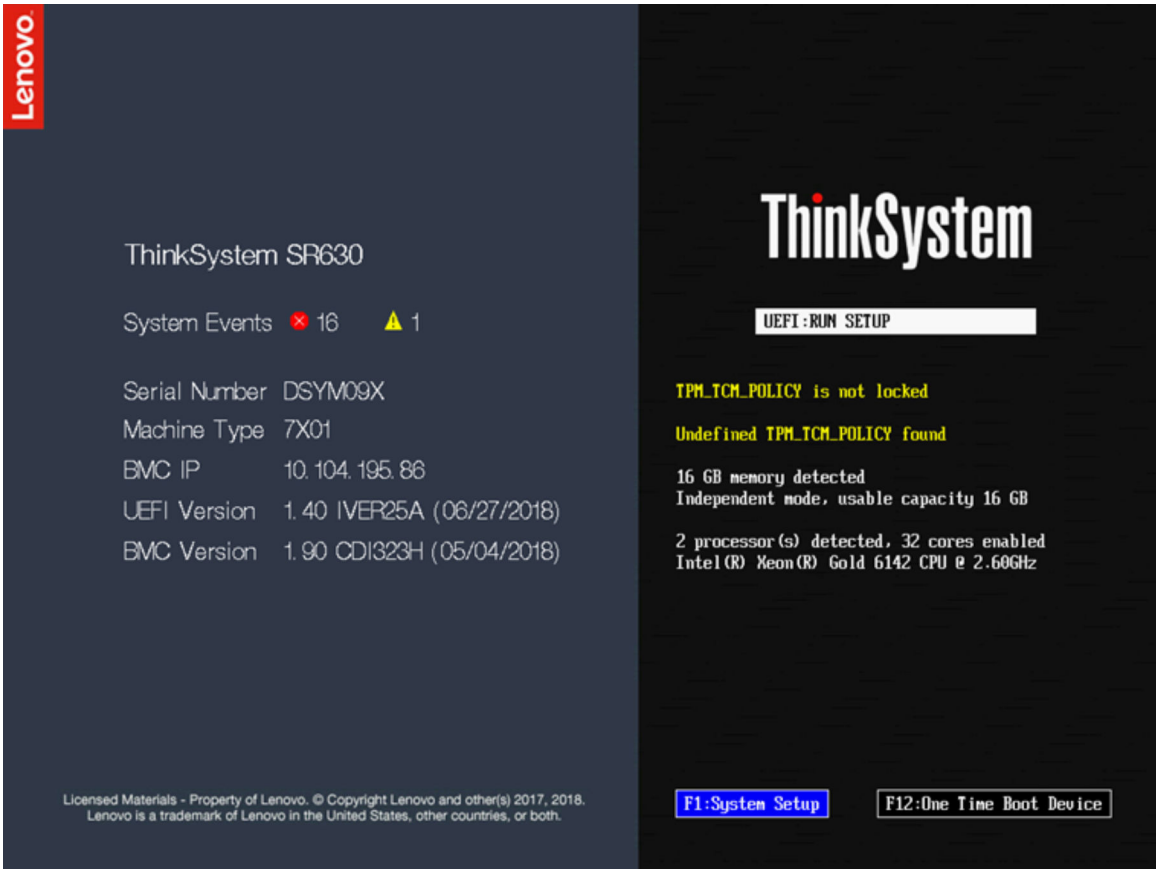
Настройка сетевого подключения XClarity Controller с помощью диспетчера XClarity Provisioning Manager

Воспользуйтесь информацией из этого раздела для настройки сетевого подключения XClarity Controller с помощью диспетчера XClarity Provisioning Manager.

Запустив сервер, можно воспользоваться диспетчером XClarity Provisioning Manager для настройки сетевого подключения XClarity Controller. Сервер с контроллером XClarity Controller должен быть подключен к серверу DHCP, либо сеть сервера должна быть настроена для использования статического IP-адреса XClarity Controller. Чтобы настроить сетевое подключение к XClarity Controller с помощью программы Setup Utility, выполните следующие действия:

Шаг 1. Включите сервер. Отобразится приветственный экран ThinkSystem.

Примечание: Кнопка питания становится активной примерно через 40 секунд после подключения сервера к сети переменного тока.



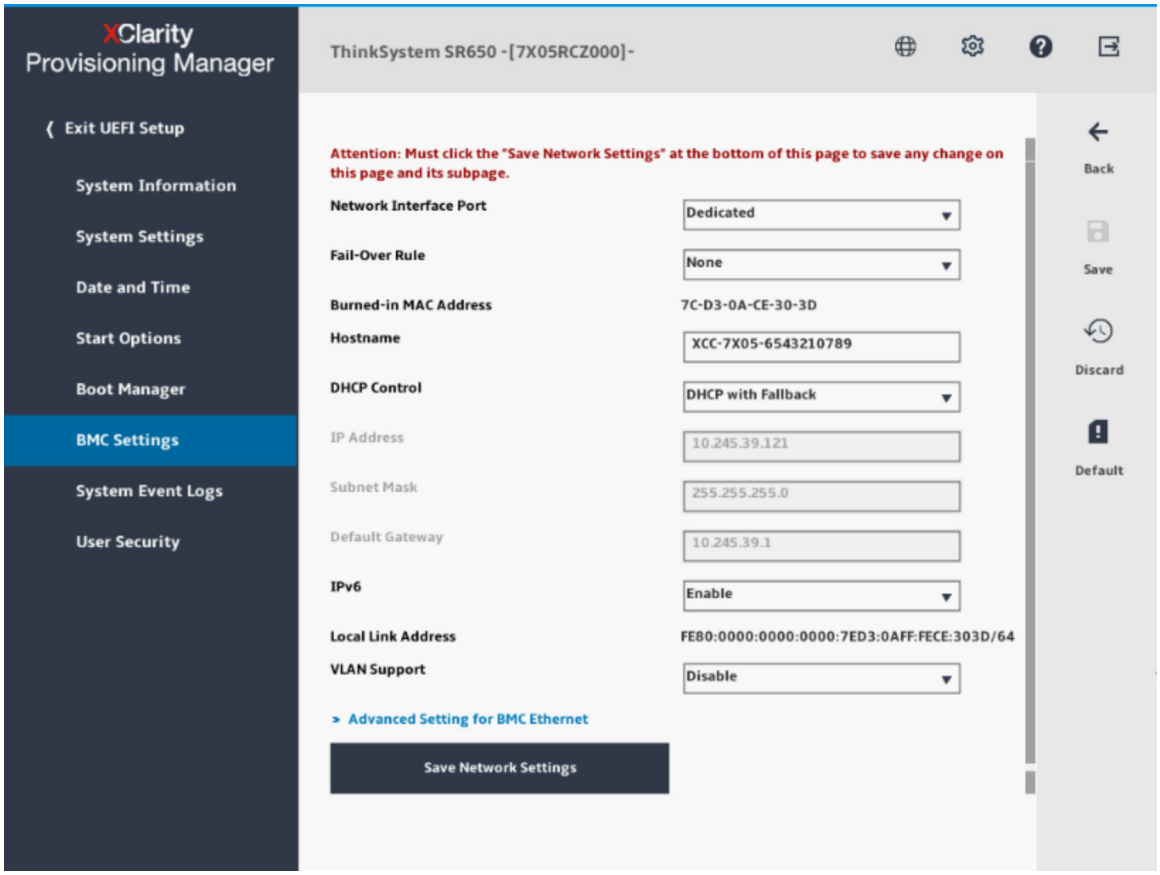
Шаг 2. При появлении запроса `<F1> System Setup` нажмите клавишу F1. Если задан пароль после включения питания и пароль администратора, для получения доступа к диспетчеру XClarity Provisioning Manager необходимо ввести пароль администратора.

Шаг 3. В главном меню XClarity Provisioning Manager выберите **UEFI Setup**.

Шаг 4. На следующем экране выберите **BMC Settings**; затем нажмите **Network Settings**.

Шаг 5. Существует три варианта сетевого подключения XClarity Controller в поле **DHCP Control**:

- Статический IP-адрес
- DHCP включен
- DHCP с отработкой отказа



Шаг 6. Выберите один из вариантов сетевого подключения.

Шаг 7. Если выбран статический IP-адрес, необходимо указать IP-адрес, маску подсети и шлюз по умолчанию.

Шаг 8. Можно также использовать Lenovo XClarity Controller Manager для выбора выделенного сетевого подключения (если на сервере имеется выделенный сетевой порт) или совместно используемого сетевого подключения XClarity Controller.

Примечания:

- Возможно, выделенный сетевой порт управления системами недоступен на вашем сервере. Если на вашем оборудовании отсутствует выделенный сетевой порт, *используемый совместно* — единственный доступный параметр XClarity Controller. На экране **Network Configuration** выберите **Dedicated** (если применимо) или **Shared** в поле **Network Interface Port**.
- Чтобы найти расположения разъемов Ethernet на сервере, используемых XClarity Controller, обратитесь к документации по серверу.

Шаг 9. Нажмите **Сохранить**.

Шаг 10. Выйдите из диспетчера XClarity Provisioning Manager.

Примечания:

- Необходимо подождать около 1 минуты, чтобы изменения вступили в силу, прежде чем микропрограмма сервера снова начнет работать.
- Кроме того, можно настроить сетевое подключение XClarity Controller в веб-интерфейсе или интерфейсе командной строки XClarity Controller. В веб-интерфейсе XClarity Controller сетевые подключения можно настроить, щелкнув **Конфигурация BMC** в левой панели навигации и выбрав **Network**. В интерфейсе командной строки XClarity Controller сетевые подключения настраиваются с помощью нескольких команд, которые зависят от конфигурации установки.

Вход в XClarity Controller

Воспользуйтесь информацией из этого раздела для доступа к XClarity Controller через веб-интерфейс XClarity Controller.

Важно: Изначально для XClarity Controller настроено имя пользователя `USERID` и пароль `PASSWORD` (с нулем, а не буквой O). Этот пользователь по умолчанию имеет уровень доступа «Администратор». В целях безопасности измените это имя пользователя и пароль во время первоначальной настройки. После внесения изменения будет невозможно повторно задать `PASSWORD` в качестве пароля для входа.

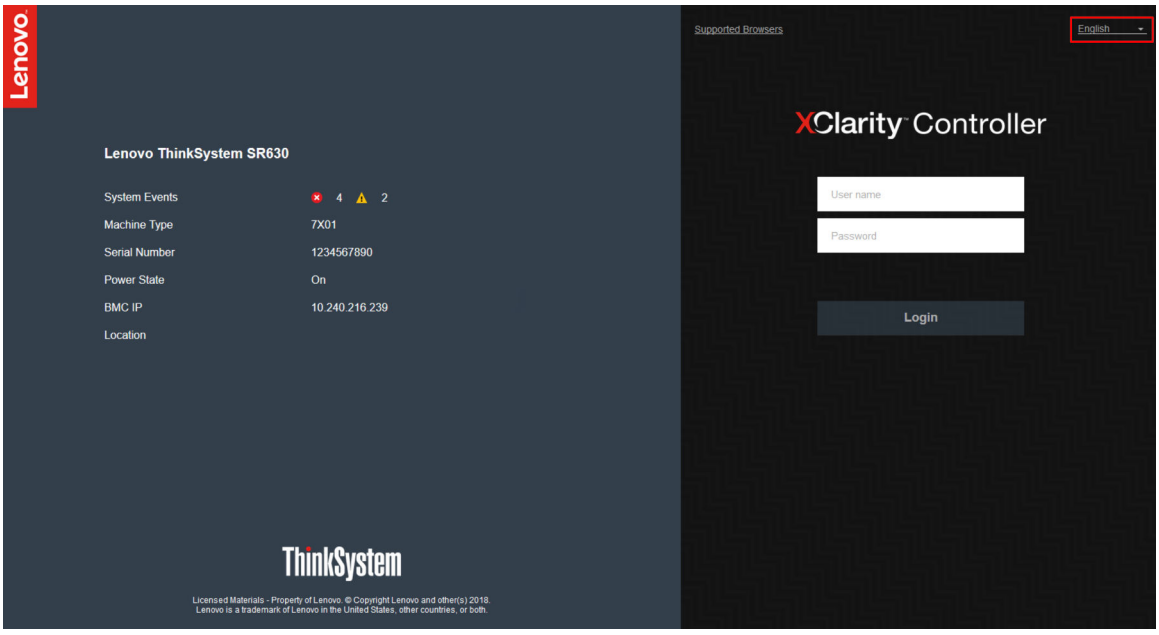
Примечание: В системе Flex System учетными записями пользователей XClarity Controller можно управлять с помощью модуля Flex System Chassis Management Module (CMM); для этого могут использоваться комбинации учетных данных, отличные от USERID/PASSW0RD.

Чтобы получить доступ к XClarity Controller из веб-интерфейса XClarity Controller, выполните следующие действия:

Шаг 1. Откройте веб-браузер. В поле адреса или URL-адреса введите IP-адрес или имя хоста XClarity Controller, к которому требуется подключиться.

Шаг 2. Выберите нужный язык из раскрывающегося списка.

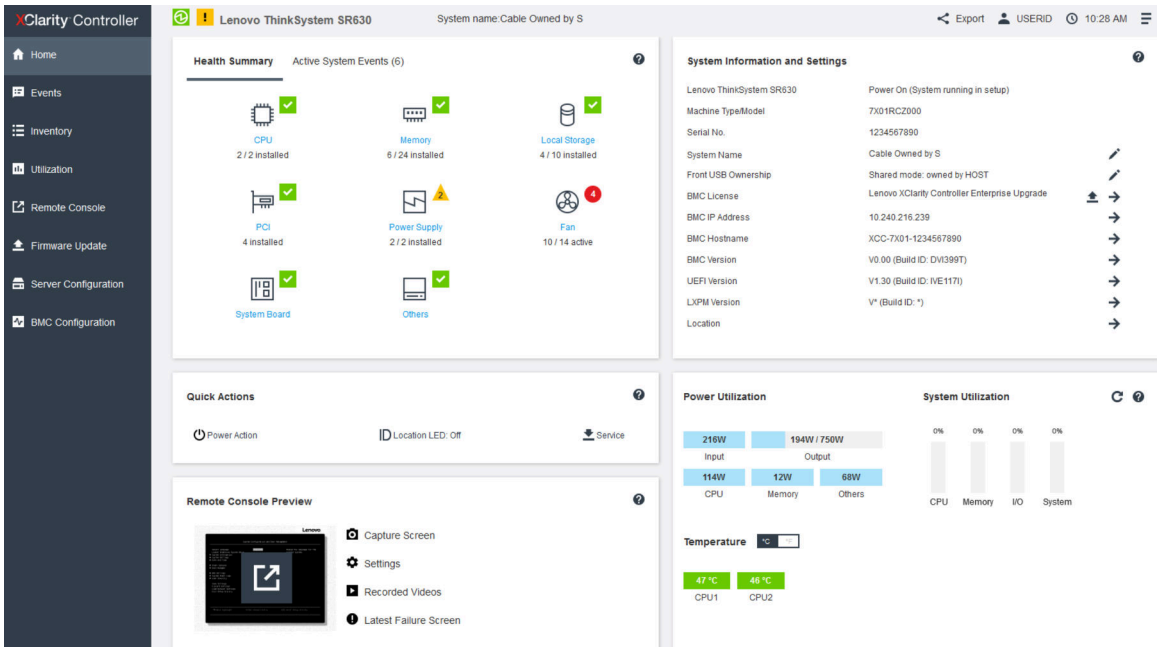
Окно входа в систему показано на следующем рисунке.



Шаг 3. Введите имя пользователя и пароль в окне входа в XClarity Controller. При первом использовании XClarity Controller имя пользователя и пароль можно получить у системного администратора. Все попытки входа регистрируются в журнале событий. В зависимости от

того, как ваш системный администратор настроил идентификатор пользователя, после входа, возможно, потребуется ввести новый пароль.

Шаг 4. Нажмите **Войти**, чтобы начать сеанс. В браузере откроется домашняя страница XClarity Controller, как показано на следующем рисунке. На домашней странице отобразится информация об управляемой контроллером XClarity Controller системе и значки, указывающие, сколько критических ошибок 1 и предупреждений 1 в настоящее время имеется в системе.



Домашняя страница разделена на два раздела. Первый — это панель навигации слева, представляющая собой набор тем для выполнения следующих действий:

- Мониторинг состояния сервера
- Настройка сервера
- Настройка XClarity Controller или BMC
- Обновление микропрограммы

Второй раздел — это графическая информация справа от панели навигации. Модульный формат позволяет быстро получить представление о состоянии сервера и некоторых доступных быстрых действиях.

Описание функций XClarity Controller в веб-интерфейсе

Ниже представлена таблица, описывающая функции XClarity Controller в левой панели навигации.

Примечание: Осуществляя навигацию по веб-интерфейсу, можно щелкнуть значок с изображением вопроса, чтобы открыть справку в Интернете.

Табл. 1. Функции XClarity Controller

В таблице из трех столбцов описаны действия, которые можно выполнить в веб-интерфейсе XClarity Controller.

Табл. 1. Функции XClarity Controller (продолж.)

Вкладка	Выбранные значения	Описание
Домашняя страница	Сводка состояния/активные системные события	Показывает текущее состояние основных аппаратных компонентов системы.
	Сведения о системе и параметры системы	Содержит сводку общих сведений о системе.
	Быстрые действия	Содержит быстрые ссылки для управления питанием сервера и светодиодным индикатором местоположения, а также кнопку для загрузки данных по обслуживанию.
	Использование питания/ Использование системы/ Температура	Содержит краткий обзор текущего использования питания и системы, а также общей температуры сервера.
	Предварительный просмотр удаленной консоли	Контроль сервера на уровне операционной системы. Можно просматривать консоль сервера и выполнять на ней действия с вашего компьютера. Раздел «Удаленная консоль» на домашней странице XClarity Controller содержит изображение экрана с кнопкой «Запустить». На панели инструментов справа доступны следующие быстрые действия: • Захват экрана • Параметры • Записанные видео • Экран последнего сбоя
События	Журнал событий	Предоставляет список всех аппаратных событий и событий управления за прошлые периоды.
	Журнал аудита	Содержит записи о действиях пользователей за прошлые периоды, например о входе в систему на контроллере Lenovo XClarity Controller, создании нового пользователя и изменении пароля пользователя. Журнал аудита можно использовать для отслеживания и документирования аутентификации и элементов управления в ИТ-системах.
	История обслуживания	Отображаются все сведения об истории обновлений микропрограмм, конфигурации и замены оборудования.
	Получатели оповещений	Управление получателями уведомлений о системных событиях. Позволяет настроить каждого получателя и управлять параметрами, которые действуют в отношении всех получателей событий. Кроме того, можно создать тестовое событие, чтобы подтвердить параметры конфигурации обновлений.
Инвентаризация		Отображает все компоненты в системе, их состояние и ключевые сведения. Можно щелкнуть устройство для отображения дополнительной информации. **Примечание:** Дополнительные сведения о состоянии питания решения см. в веб-интерфейсе SMM2.
Использование		Отображается температура окружающей среды/ компонентов, энергопотребление, уровни напряжения, сведения об использовании подсистем системы, а также информация о скорости работы вентиляторов сервера и его компонентов в графическом или табличном представлении.

Табл. 1. Функции XClarity Controller (продолж.)

Вкладка	Выбранные значения	Описание
Хранение	Подробно	Отображает физическую структуру и конфигурацию хранилища устройств хранения.
	Настройка RAID	Просмотр или изменение текущей конфигурации RAID, включая информацию о виртуальных дисках и физических устройствах хранения.
Удаленная консоль		Предоставляет доступ к функции удаленной консоли. Функцию виртуальных носителей можно использовать для подключения файлов ISO или IMG, находящихся в локальной системе или сетевом расположении, доступ к которому BMC может получать с помощью CIFS, NFS, HTTPS или SFTP. Подключенный диск отображается в качестве USB-диска, подключенного к серверу.
Обновление микропрограм-мы		• Отображает уровни микропрограммы. • Обновление микропрограмм XClarity Controller и сервера.
Конфигурация сервера	Адаптеры	Отображает сведения об установленных сетевых адаптерах и параметры, которые можно настроить с помощью XClarity Controller.
	Параметры загрузки	• Выбор загрузочного устройства для однократной загрузки при следующем перезапуске сервера • Изменение параметров режима и порядка загрузки.
	Политика питания	• Настройка резерва питания на случай сбоя блока питания. • Настройка политики ограничения мощности. • Настройка политики восстановления питания. **Примечание:** Дополнительные сведения о состоянии питания решения см. в веб-интерфейсе SMM2.
	Свойства сервера	• Мониторинг различных свойств, условий состояния и параметров для сервера. • Управление тайм-аутами запуска сервера с целью обнаружения зависаний сервера и восстановления из этого состояния. • Создание сообщения при нарушении. Сообщение при нарушении — это сообщение, которое можно создать для пользователей, чтобы отслеживать их вход в XClarity Controller.
Конфигурация BMC	Резервное копирование и восстановление	Сброс конфигурации XClarity Controller до заводских настроек, резервное копирование текущей конфигурации или восстановление конфигурации из файла.
	Лицензия	Управление ключами активации для дополнительных компонентов XClarity Controller.
	Сети	Настройка сетевых свойств, состояния и параметров для XClarity Controller.
	Безопасность	Настройка свойств безопасности, состояния и параметров для XClarity Controller.

Табл. 1. Функции XClarity Controller (продолж.)

Вкладка	Выбранные значения	Описание
	Пользователь/LDAP	• Настройка профилей входа в XClarity Controller и параметров глобального входа. • Просмотр учетных записей пользователей, которые в настоящее время выполнили вход в XClarity Controller. • На вкладке LDAP настраивается аутентификация пользователей для использования с одним или несколькими серверами LDAP. Кроме того, здесь можно включить или отключить безопасность LDAP и управлять соответствующими сертификатами.

Глава 3. Конфигурация XClarity Controller

Воспользуйтесь информацией из этой главы, чтобы понять доступные параметры конфигурации XClarity Controller.

При настройке XClarity Controller доступны следующие ключевые параметры:

- Резервное копирование и восстановление
- Лицензия
- Сети
- Безопасность
- Пользователь/LDAP

Настройка учетных записей пользователей/LDAP

Воспользуйтесь информацией из этого раздела, чтобы понять принципы управления учетными записями пользователей.

Щелкните **Пользователь/LDAP** в разделе **BMC Configuration** для создания, изменения и просмотра учетных записей пользователей, а также для настройки параметров LDAP.

На вкладке **Локальный пользователь** отображаются учетные записи пользователей, настроенные в XClarity Controller, от имени которых в настоящее время выполнен вход в XClarity Controller.

На вкладке **LDAP** представлена конфигурация LDAP для доступа к учетным записям пользователей, которые хранятся на сервере LDAP.

Метод аутентификации пользователей

Используйте информацию в этом разделе, чтобы понять, в каких режимах XClarity Controller может выполнять аутентификацию попыток входа.

Щелкните **Разрешить вход из**, чтобы указать способ аутентификации попыток входа пользователя. Можно выбрать один из следующих методов аутентификации:

- **Только локальная:** аутентификация пользователей выполняется путем поиска локальной учетной записи пользователя, настроенной в XClarity Controller. Если ИД пользователя и пароль не совпадают, в доступе отказано.
- **Только LDAP:** XClarity Controller пытается аутентифицировать пользователя, используя хранимые на сервере LDAP учетные данные. При использовании этого метода аутентификации поиск локальных учетных записей пользователя в XClarity Controller *не* выполняется.
- **Сначала локальная, затем LDAP:** сначала предпринимается попытка локальной аутентификации. Если локальная аутентификация завершается сбоем, система предпринимает попытку выполнить аутентификацию LDAP.
- **Сначала LDAP, затем локальный пользователь:** сначала предпринимается попытка аутентификации LDAP. Если аутентификация LDAP завершается сбоем, система предпринимает попытку выполнить локальную аутентификацию.

Примечания:

- Только учетные записи с локальным администрированием предоставляются в интерфейсы IPMI и SNMP. Эти интерфейсы не поддерживают аутентификацию LDAP.

- Пользователи IPMI и SNMP могут выполнить вход с помощью учетных записей с локальным администрированием, если в поле **Разрешить вход из** задано значение **Только LDAP**.

Создание новой учетной записи пользователя

Используйте информацию в этом разделе для создания нового локального пользователя.

Создание пользователя

Щелкните **Создать**, чтобы создать новую учетную запись пользователя.

Заполните следующие поля: **Имя пользователя**, **Пароль**, **Подтвердить пароль** и **Уровень разрешений**. Дополнительные сведения об уровне разрешений см. в следующем разделе.

Уровень полномочий пользователя

Доступны следующие уровни разрешений пользователя:

Администратор
Для пользователя этого уровня не существует ограничений.

Только чтение
Уровень разрешений пользователя «Только чтение» обеспечивает доступ только для чтения. Такой пользователь не может выполнять передачу файлов, действия с питанием и перезапуском системы и функции удаленного присутствия.

Пользовательский
Пользовательский уровень разрешения позволяет настраивать полномочия пользователя, задавая параметры действий, которые пользователь может выполнять.

Выберите один или несколько следующих пользовательских уровней разрешений:

Конфигурация адаптера — сетевые подключения и безопасность
Пользователь может менять параметры конфигурации на страницах «Безопасность», «Сеть» и «Последовательный порт».

Управление учетными записями пользователей
Пользователь может добавлять, изменять и удалять пользователей, а также менять параметры глобального входа.

Доступ к удаленной консоли
Пользователь может осуществлять доступ к удаленной консоли.

Доступ к удаленной консоли и удаленному диску
Пользователь может осуществлять доступ к удаленной консоли и виртуальным носителям.

Удаленное питание/перезапуск сервера
Пользователь может включить и перезапускать сервер.

Конфигурация адаптера — базовая
Пользователь может менять параметры конфигурации на страницах «Свойства сервера» и «События».

Возможность очищать журналы событий
Пользователь может очищать журналы событий. Любой пользователь может просматривать журналы событий, однако для очистки журналов требуется разрешение этого уровня.

Конфигурация адаптера —расширенная (обновление микропрограмм, перезапуск BMC, восстановление конфигурации)

У пользователя нет ограничений по настройке XClarity Controller. Кроме того, пользователь имеет административные права доступа к XClarity Controller. Административные права доступа позволяют выполнять следующие расширенные функции: обновление микропрограмм, загрузка сети PXE, восстановление заводских значений XClarity Controller, изменение и восстановление параметров XClarity Controller из файла конфигурации и перезапуск и сброс XClarity Controller.

Когда пользователь настраивает уровень полномочий для ИД входа XClarity Controller, соответствующий уровень полномочий IPMI ИД пользователя IPMI настраивается с учетом следующих приоритетов:

- Если пользователь задает для ИД входа XClarity Controller уровень разрешений **Администратор**, привилегии IPMI задаются на уровне «Администратор».
- Если пользователь задает для ИД входа XClarity Controller уровень разрешений **Только чтение**, привилегии IPMI задаются на уровне «Пользователь».
- Если пользователь задает для ИД входа XClarity Controller любой из следующих типов доступа, привилегии IPMI задаются на уровне «Администратор»:
  - Доступ к управлению учетными записями пользователей
  - Доступ к удаленной консоли
  - Доступ к удаленной консоли и удаленному диску
  - Конфигурация адаптера — сетевые подключения и безопасность
  - Конфигурация адаптера — расширенная
- Если пользователь задает для ИД входа XClarity Controller уровень разрешений **Удаленный доступ к питанию/перезапуску сервера** или **Возможность очищать журналы событий**, привилегии IPMI задаются на уровне «Оператор».
- Если пользователь задает для ИД входа XClarity Controller уровень разрешений **Конфигурация адаптера — базовая**, привилегии IPMI задаются на уровне «Пользователь».

Параметры SNMPv3

Чтобы включить для пользователя доступ SNMPv3, установите флажок рядом с настройкой **Параметры SNMPv3**. Поясняются следующие варианты доступа пользователей:

Тип доступа
Поддерживаются только операции **GET**. XClarity Controller не поддерживает операции **SET** SNMPv3. SNMP3 может выполнять только операции запросов.

Адрес для ловушек
Укажите целевое расположение ловушек для пользователя. Это может быть IP-адрес или имя хоста. С помощью ловушек агент SNMP уведомляет станцию управления о событиях (например, если температура процессора превышает лимит).

Протокол аутентификации
В качестве протокола аутентификации поддерживается только **HMAC-SHA**. Этот алгоритм используется для аутентификации моделью безопасности SNMPv3.

Протокол конфиденциальности
Перенос данных между клиентом SNMP и агентом можно защитить с помощью шифрования. Поддерживаемые методы: **CBC-DES** и **AES**.

Примечания: Даже если пользователь SNMPv3 использует повторные строки пароля, можно будет по-прежнему получить доступ к XClarity Controller. Ниже приводится два примера для справки.

- Если в качестве пароля задано *11111111* (число из восьми цифр, содержащее восемь цифр 1), пользователь по-прежнему сможет получить доступ к XClarity Controller, если при вводе пароля случайно будет введено более восьми цифр 1. Например, если ввести пароль *1111111111* (число из десяти цифр, содержащее десять цифр 1), доступ по-прежнему предоставляется. Будет считаться, что у повторной строки тот же ключ.
- Если задан пароль *bertbert*, пользователь по-прежнему сможет получить доступ к XClarity Controller, если случайно был введен пароль *bertbertbert*. Считается, что у обоих паролей одинаковый ключ.

Дополнительные сведения см. на стр. 72 в документе «Интернет-стандарт RFC 3414» (https://tools.ietf.org/html/rfc3414).

Ключ SSH

XClarity Controller поддерживает аутентификацию с использованием открытых ключей SSH (тип ключа RSA). Чтобы добавить ключ SSH к локальной учетной записи пользователя, установите флажок рядом с параметром **Ключ SSH**. Предоставляются два следующих параметра:

Выбор файла ключа
Выберите файл ключа SSH для импорта в XClarity Controller с сервера.

Ввод ключа в текстовое поле
Вставьте или введите данные ключа SSH в текстовое поле.

Примечания:

- Некоторые инструменты Lenovo могут создавать временную учетную запись пользователя для доступа к XClarity Controller, если инструмент используется в серверной операционной системе. Эта временная учетная запись недоступна для просмотра и не использует никакие из 12 позиций учетных записей локальных пользователей. Эта учетная запись создается с произвольным именем пользователя (например, 20luN4SB) и паролем. Эту учетную запись можно использовать только для доступа к XClarity Controller во внутреннем интерфейсе Ethernet через USB и только для интерфейсов CIM-XML и SFTP. Создание и удаление этой временной учетной записи фиксируется в журнале аудита, равно как и любые действия, выполняемые инструментом с этими учетными данными.
- Для обозначения ИД механизма SNMPv3 XClarity Controller использует шестнадцатеричную строку. Эта шестнадцатеричная строка преобразуется из имени хоста XClarity Controller по умолчанию. См. следующий пример:

  Имя хоста XCC-7X06-S4AHJ300 сначала преобразуется в формат ASCII: 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  Шестнадцатеричная строка создается с использованием формата ASCII (пробелы игнорируются): 58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30

Удаление учетной записи пользователя

Используйте информацию в этом разделе для удаления учетной записи локального пользователя.

Чтобы удалить учетную запись локального пользователя, нажмите значок корзины в строке напротив учетной записи, которую требуется удалить. При наличии соответствующих разрешений можно удалить собственную учетную запись или учетную запись других пользователей, даже если в настоящее время они работают в системе. Исключение составляют случаи, когда речь идет о единственной оставшейся учетной записи с привилегиями управления учетными записями пользователей. Сеансы, выполнявшиеся на момент удаления учетных записей пользователей, не будут завершены автоматически.

Использование хэшированных паролей для аутентификации

Воспользуйтесь информацией из этого раздела, чтобы понять, как использовать хэшированные пароли для аутентификации.

Помимо использования паролей и учетных записей пользователей LDAP/AD XClarity Controller поддерживает сторонние хэшированные пароли для аутентификации. Специальный пароль имеет формат одностороннего хэша (SHA256) и поддерживается веб-интерфейсом XClarity Controller, средством OneCLI и интерфейсом командной строки. Однако помните, что аутентификация интерфейсов XCC SNMP, IPMI и CIM не поддерживает сторонние хэшированные пароли. Только средство OneCLI и интерфейс командной строки XCC могут создавать новые учетные записи с хэшированным паролем или выполнять обновление хэшированных паролей. XClarity Controller также позволяет средству OneCLI и интерфейсу командной строки XClarity Controller получить хэшированный пароль, если включена возможность чтения хэшированных паролей.

Настройка хэшированного пароля с помощью веб-интерфейса XClarity Controller

Нажмите **Безопасность** в разделе **BMC Configuration** и прокрутите раздел **Security Password Manager**, чтобы включить или отключить функцию стороннего пароля. Если эта функция включена, то для аутентификации при входе в систему будет использоваться сторонний хэшированный пароль. Кроме того, можно включить или отключить получение стороннего хэшированного пароля из XClarity Controller.

Примечание: По умолчанию функции *Сторонний пароль* и *Разрешить получение стороннего пароля* отключены.

Чтобы проверить тип пароля пользователя (*Собственный* или *Сторонний пароль*), нажмите **Пользователь/LDAP** в разделе **BMC Configuration** для получения дополнительных сведений. Сведения будут представлены в столбце **Дополнительный атрибут**.

Примечания:

- Пользователи не смогут изменить пароль, если он является сторонним паролем, и поля **Пароль** и **Подтверждение пароля** будут затемнены.
- Если срок действия стороннего пароля истек, в процессе входа в систему отобразится предупреждающее сообщение.

Настройка хэшированного пароля с помощью функции OneCLI

- Включение функции

  ```
  $ sudo OneCli config set IMM.ThirdPartyPassword Enabled
  ```

- Создание хэшированного пароля (без Salt). Ниже приведен пример входа в XClarity Controller с использованием пароля *password123*.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

- Создание пользователя с хэшированным паролем (с Salt). Ниже приведен пример входа в XClarity Controller с использованием пароля *password123*. Salt = abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  ```

```
$ sudo OneCli config set IMM.Loginid.3 Admin
$ sudo OneCli config set IMM.SHA256Password.3 $pwhash
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
```

- Получение хэшированного пароля и salt.

```
$ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled
$ sudo OneCli config show IMM.SHA256Password.3
$ sudo OneCli config show IMM.SHA256PasswordSalt.3
```

- Удаление хэшированного пароля и salt.

```
$ sudo OneCli config set IMM.SHA256Password.3 ""
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
```

- Задание хэшированного пароля для существующей учетной записи.

```
$ sudo OneCli config set IMM.Loginid.2 admin
$ sudo OneCli config set IMM.Password.2 Passw0rd123abc
$ sudo OneCli config set IMM.SHA256Password.2 $pwhash
$ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
```

Примечание: Хэшированный пароль вступает в силу сразу же после его создания. Исходный стандартный пароль больше не будет действовать. В этом примере исходный стандартный пароль *Passw0rd123abc* больше не может использоваться, пока не будет удален хэшированный пароль.

Настройка хэшированного пароля с помощью интерфейса командной строки

- Включение функции

```
> hashpw -sw enabled
```

- Создание хэшированного пароля (без Salt). Ниже приведен пример входа в XClarity Controller с использованием пароля *password123*.

```
$ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a
super
```

- Создание пользователя с хэшированным паролем (с Salt). Ниже приведен пример входа в XClarity Controller с использованием пароля *password123*. Salt = abc.

```
$ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`
$ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
> users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
-ssalt 'abc' -a super
```

- Получение хэшированного пароля и salt.

```
> hashpw -re enabled
> users -3 -ghp -gsalt
```

- Удаление хэшированного пароля и salt.

```
> users -3 -shp "" -ssalt ""
```

- Задание хэшированного пароля для существующей учетной записи.

```
> users -2 -n admin -p Passw0rd123abc -shp
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

Примечание: Хэшированный пароль вступает в силу сразу же после его создания. Исходный стандартный пароль больше не будет действовать. В этом примере исходный стандартный пароль *Passw0rd123abc* больше не может использоваться, пока не будет удален хэшированный пароль.

После настройки хэшированного пароля помните, что он не используется для входа в XClarity Controller. При входе в систему необходимо использовать пароль в виде обычного текста. В примере ниже используется пароль в виде обычного текста password123.

```
$ pwhash = ‘echo –n password123 | openssl dgst –sha256 | awk '{print $NF}''

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

Настройка параметров глобального входа

Воспользуйтесь информацией из этого раздела, чтобы настроить параметры политики входа и паролей, применимые ко всем пользователям.

Тайм-аут веб-сеанса после неактивности

Воспользуйтесь информацией из этого раздела, чтобы настроить тайм-аут веб-сеанса после неактивности.

В поле **Тайм-аут веб-сеанса после неактивности** можно указать продолжительность (в минутах) ожидания, прежде чем XClarity Controller отключит неактивный веб-сеанс. Максимальное время ожидания —1440 минут. Если задано значение 0, веб-сеанс никогда не истекает.

Микропрограмма XClarity Controller поддерживает до шести одновременных веб-сеансов. Чтобы освободить сеансы для использования другими пользователями, рекомендуется выходить из веб-сеанса по окончании работы, а не надеяться, что сеанс будет автоматически завершен тайм-аутом после неактивности.

Примечание: Если оставить браузер открытым на веб-странице XClarity Controller, которая обновляется автоматически, ваш веб-сеанс не будет автоматически закрыт из-за неактивности.

Параметры политики безопасности учетных записей

Воспользуйтесь информацией из этого раздела, чтобы изучить и выбрать параметры политики безопасности учетных записей для сервера.

Примечания: В Flex System параметрами политики безопасности учетных записей управляет модуль Flex System Chassis Management Module (CMM), и их невозможно изменить с помощью XCC. Если CMM используется для настройки политики безопасности учетных записей, обратите внимание на следующее:

- В отличие от XCC модуль CMM не имеет параметра *Период предупреждения об истечении срока действия пароля (в днях)*. Если значение *Период истечения срока действия пароля* превышает 5 дней в CMM, XCC задаст для периода предупреждения об истечении срока действия пароля значение «5 дней». И наоборот, если задано значение менее 5 дней, значение периода предупреждения об истечении срока действия будет совпадать со значением, введенным в поле *Период истечения срока действия пароля*.
- Диапазон значений параметра *Максимальное число ошибок при входе (раз)*, заданный в CMM, составляет от 0 до 100 раз. Однако диапазон, определенный в XCC, составляет от 0 до 10 раз. Таким образом, когда пользователь выбирает значение, превышающее 10 раз, в CMM, XCC по-прежнему задаст для максимального числа ошибок при входе значение «10 раз».

- Диапазон значений параметра *Минимальный интервал изменения пароля (в часах)*, заданный в CMM, составляет от 0 до 1440 ч. Однако диапазон, определенный в XCC, составляет от 0 до 240 ч. Таким образом, когда пользователь выбирает значение, превышающее 240 ч, в CMM, XCC по-прежнему задаст для минимального интервала изменения пароля значение 240 ч.

Ниже представлено описание полей с параметрами безопасности.

Принудительное изменение пароля при первом входе
После создания нового пользователя с паролем по умолчанию установите этот флажок, чтобы пользователь должен был менять свой пароль при первом входе в систему. Значение по умолчанию для этого поля — установленный флажок.

Принудительное изменение пароля учетной записи по умолчанию при следующем входе
Доступен заводской параметр, позволяющий сбросить профиль USERID по умолчанию после первого успешного входа. Если этот флажок установлен, необходимо изменить пароль по умолчанию, прежде чем пользоваться учетной записью. На новый пароль распространяются все правила действующего пароля. Значение по умолчанию для этого поля — установленный флажок.

Требуется сложный пароль
Флажок установлен по умолчанию, а сложный пароль должен соответствовать следующим правилам:

- Содержать только следующие символы (без пробелов):A–Z, a–z, 0–9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- Содержать по меньшей мере одну букву
- Содержать по меньшей мере одну цифру
- Содержать по меньшей мере две из следующих комбинаций:
  - По меньшей мере одну букву верхнего регистра;
  - По меньшей мере одну букву нижнего регистра;
  - По меньшей мере один специальный символ.
- Никакие другие символы (в частности, пробелы) использовать недопустимо.
- Пароль должен содержать не более двух одинаковых символов подряд (например, «ааа»).
- Пароль не может в точности повторять имя пользователя, состоять из повторяющегося один несколько раз имени пользователя либо имени пользователя в обратном порядке.
- Допустимая длина пароля — от 8 до 32 символов

Если флажок рядом с этим параметров не установлен, в качестве значения минимальной длины пароля можно указать от 0 до 32 символов. Если для минимальной длины пароля установлено значение 0, поле пароля учетной записи можно оставить пустым.

Период истечения срока действия пароля (в днях)
В этом поле указан максимальный срок действия пароля (период, по истечении которого пароль необходимо изменить). Поддерживается значение от 0 до 30 дней. Значение по умолчанию для этого поля — 14 дней.

Период ожидания истечения срока действия пароля (в днях)
В этом поле указано, за какое время (в днях) до истечения срока действия пароля пользователь начинает получать предупреждения. Если задано значение 0, предупреждения не отправляются. Поддерживается значение от 0 до 30 дней. Значение по умолчанию для этого поля — 14 дней.

Минимальная длина пароля

В этом поле указана минимальная длина пароля. В этом поле можно указать значение от 8 до 32. Значение по умолчанию для этого поля — 10.

Минимальный цикл повторного использования пароля
В этом поле указывается количество использовавшихся ранее паролей, которые нельзя использовать повторно. Можно сравнивать до десяти ранее использовавшихся паролей. Выберите 0, чтобы разрешить использовать любые созданные ранее пароли. Поддерживается значение от 0 до 10. Значение по умолчанию для этого поля — 5.

Минимальный интервал изменения пароля (в часах)
В этом поле указано, сколько следует ждать, прежде чем изменить пароль еще раз. Здесь можно указать значение от 0 до 240. Значение по умолчанию для этого поля — 1 час.

Максимальное число ошибок при входе (раз)
В этом поле указано максимально допустимое количество неудавшихся попыток входа, после чего пользователь будет заблокирован на определенное время. Поддерживается значение от 0 до 10. Значение по умолчанию для этого поля — пять неудачных попыток входа.

Период блокировки после максимального числа ошибок при входе (в минутах)
В этом поле указан период (в минутах), на который подсистема XClarity Controller запретит попытки удаленного входа при превышении максимально допустимого количества неудавшихся попыток входа. Здесь можно указать значение от 0 до 2880 минут. Значение по умолчанию для этого поля — 60 минут.

Настройка LDAP

Воспользуйтесь информацией из этого раздела для просмотра или изменения параметров LDAP XClarity Controller.

Поддержка LDAP включает:

- Поддержку протокола LDAP версии 3 (RFC 2251);
- Поддержку стандартных интерфейсов API клиентов LDAP (RFC 1823);
- Поддержку стандартного синтаксиса фильтра поиска LDAP (RFC 2254);
- Поддержку расширения протокола LDAP (версии 3) для протокола TLS (RFC 2830).

Реализация LDAP поддерживает следующие серверы LDAP:

- Microsoft Active Directory (Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Microsoft Active Directory Application Mode (Windows 2003 Server)
- Microsoft Lightweight Directory Service (Windows 2008, Windows 2012)
- Novell eDirectory Server, версия 8.7, 8.8 и 9.4
- OpenLDAP Server 2.1, 2.2, 2.3 и 2.4

Перейдите на вкладку **LDAP** для просмотра или изменения параметров LDAP XClarity Controller.

XClarity Controller может удаленно аутентифицировать доступ пользователя с помощью центрального сервера LDAP вместо локальных учетных записей пользователя (или в дополнение к ним), которые сохранены в самом контроллере XClarity Controller. Можно назначить привилегии для каждой учетной записи пользователя, используя строку IBMRBSPermissions. Кроме того, можно использовать сервер LDAP, чтобы назначить пользователей группам и выполнять групповую аутентификацию, помимо стандартной аутентификации пользователей (по проверке пароля). Например, можно назначить

XClarity Controller одной или нескольким группам; пользователь сможет пройти групповую аутентификацию, только если он относится хотя бы к одной группе, связанной с XClarity Controller.

Для настройки сервера LDAP выполните следующие действия:

1. В разделе **Сведения о сервере LDAP** в списке элементов доступны следующие параметры:

   - **Использовать сервер LDAP только для аутентификации (с локальной авторизацией)**: если выбран этот параметр, XClarity Controller будет использовать учетные данные только для аутентификации на сервере LDAP и извлечения информации о принадлежности к группе. Имена и привилегии групп можно настроить в разделе параметров Active Directory.
   - **Использовать сервер LDAP для аутентификации и авторизации**: если выбран этот параметр, XClarity Controller будет использовать учетные данные и для аутентификации на сервере LDAP, и для идентификации разрешений пользователя.

   Примечание: Серверы LDAP, которые следует использовать для аутентификации, можно настроить вручную или обнаружить с помощью записей DNS SRV в динамическом режиме.

   - **Использовать преднастроенные серверы**: можно настроить до четырех серверов LDAP, введя IP-адрес или имя хоста каждого из них, если DNS включена. Номер порта для каждого сервера указывать не обязательно. Если это поле оставлено пустым, для незащищенных подключений LDAP используется значение по умолчанию — 389. Для защищенных подключений значение порта по умолчанию — 636. Необходимо настроить по меньшей мере один сервер LDAP.
   - **Использовать DNS для поиска серверов**: можно настроить динамический режим обнаружения серверов LDAP. Механизмы, описанные в статье RFC2782 (DNS RR для указания расположения служб), используются для определения расположения серверов LDAP. Этот процесс известен под названием DNS SRV. Необходимо указать полное доменное имя, которое будет использоваться в качестве доменного имени в запросе DNS SRV.
     - **Лес AD**: в среде с универсальными группами в перекрестных доменах необходимо настроить имя леса (набора доменов) для обнаружения обязательных глобальных каталогов (GC). В среде без кросс-доменного членства в группах это поле можно оставить пустым.
     - **Домен AD**: потребуется указать полное доменное имя, которое будет использоваться в качестве доменного имени в запросе DNS SRV.

   Если требуется включить защищенный LDAP, установите флажок **Включить защищенный LDAP**. Для поддержки защищенного LDAP необходимо наличие действительного сертификата SSL; кроме того, требуется импортировать по меньшей мере один доверенный сертификат клиента SSL в XClarity Controller. Сервер LDAP должен поддерживать протокол TLS версии 1.2 — только в этом случае он будет совместим с защищенным клиентом LDAP контроллера XClarity Controller. Дополнительные сведения о работе с сертификатами см. в разделе «Обработка сертификатов SSL» на странице 40.

2. Заполните информацию в разделе **Дополнительные атрибуты**. Ниже приводятся пояснения этих атрибутов.

   Метод привязки

   Прежде чем начинать поиск на сервере LDAP или отправлять на него запросы, необходимо отправить запрос привязки. Это поле управляет выполнением первоначальной привязки к серверу LDAP. Доступны следующие методы привязки:

   - **Учетные данные не требуются**

     Используйте этот метод для привязки без различающегося имени или пароля. Использовать этот метод не рекомендуется, поскольку большинство серверов настроены на запрет поисковых запросов по отдельным записям пользователей.

   - **Использовать настроенные учетные данные**

Используйте этот метод для привязки с использованием настроенного различающегося имени и пароля клиента.

- **Использовать учетные данные входа**

  Используйте этот метод для привязки с учетными данными, предоставленными в процессе входа. ИД пользователя может быть предоставлен с помощью различающегося имени, частичного различающегося имени, полного доменного имени или идентификатора пользователя, соответствующего атрибуту поиска UID, который настроен в XClarity Controller. Если предоставленные учетные данные напоминают частичное различающееся имя (например, cn=joe), оно будет присоединено спереди настроенного различающегося имени корня в попытке создать различающееся имя, соответствующее записи пользователя. Если попытка привязки завершится сбоем, будет сделана заключительная попытка создания привязки путем присоединения cn= to спереди к учетным данным входа, а полученной строки — к настроенному различающемуся имени корня.

Если первоначальная привязка успешна, выполняется поиск записи на сервере LDAP, которая относится к пользователю, который выполняет вход в систему. При необходимости выполняется вторая попытка привязки, на этот раз с различающимся именем, которое извлекается из записи LDAP пользователя, и паролем, введенным в процессе входа. Если вторая попытка привязки завершается сбоем, пользователю отказано в доступе. Вторая привязка выполняется, только если используются методы привязки **Учетные данные не требуются** или **Использовать настроенные учетные данные**.

Различающееся имя корня

Это различающееся имя корневой записи в дереве каталога на сервере LDAP (например, dn=mycompany,dc=com). Это различающееся имя используется в качестве базового объекта для всех поисковых запросов.

Атрибут поиска UID

Если в качестве метода привязки задано значение **Учетные данные не требуются** или **Использовать настроенные учетные данные**, за первоначальной привязкой к серверу LDAP следует поисковый запрос, извлекающий конкретную информацию о пользователе, включая различающееся имя пользователя, разрешения на вход и принадлежность к группе. В поисковом запросе необходимо указать имя атрибута, представляющего идентификаторы пользователей на этом сервере. Имя атрибута настраивается в этом поле. На серверах Active Directory имя атрибута обычно имеет следующий вид: **sAMAccountName**. На серверах Novell eDirectory и OpenLDAP имя атрибута имеет вид **uid**. Если поле оставлено пустым, значение по умолчанию — **uid**.

Групповой фильтр

Поле **Групповой фильтр** используется для групповой аутентификации. Попытка групповой аутентификации предпринимается после успешной проверки учетных данных пользователя. Если групповая аутентификация завершается сбоем, пользователю отказывают в доступе. Если настроен групповой фильтр, он служит для указания принадлежности XClarity Controller к тем или иным группам. Это означает, что для успешного выполнения операции пользователь должен относиться по меньшей мере к одной группе, настроенной для групповой аутентификации. Если поле **Групповой фильтр** оставлено пустым, групповая аутентификация автоматически завершается успехом. Если групповой фильтр настроен, предпринимается попытка сопоставить по меньшей мере одну группу в списке группе, к которой относится пользователь. Если соответствие не найдено, пользователь не проходит аутентификацию, в доступе ему отказано. Если найдено хотя бы одно соответствие, групповая аутентификация завершается успешно.

При сравнении учитывается регистр. Длина фильтра ограничена 511 символами, фильтр может включать одно или несколько имен группы. Символ двоеточия (:) следует

использовать для разделения нескольких имен групп. Пробелы в начале и в конце строки игнорируются, однако все остальные пробелы считаются частью имени группы.

Примечание: Подстановочный символ (*) более не является подстановочным. Концепция подстановочных символов более не используется в целях устранения уязвимостей безопасности. Имя группы можно задать в качестве полного различающегося имени или с помощью части *cn*. Например, группу с различающимся именем cn=adminGroup, dc=mycompany, dc=com можно задать с использованием фактического различающегося имени или adminGroup.

Вложенное членство в группах поддерживается только в средах Active Directory. Например, если пользователь является участником групп GroupA и GroupB, а GroupA также является участником группы GroupC, считается, что пользователь также является участником группы GroupC. Поиск по вложенным группам прекращается после обработки 128 групп. Прежде чем переходить на более низкий уровень, выполняется поиск по группам одного уровня. Зацикливания не обнаруживаются.

Атрибут группового поиска

В средах Active Directory или Novell eDirectory значение в поле **Атрибут группового поиска** указывает на имя атрибута, используемое для идентификации групп, к которым относится пользователь. В среде Active Directory имя атрибута — **memberOf**. В среде eDirectory имя атрибута — **groupMembership**. В среде сервера OpenLDAP пользователи обычно назначаются группам, значение objectClass в которых равно PosixGroup. В этом контексте это поле задает имя атрибута, используемое для идентификации участников определенной группы PosixGroup. Это имя атрибута — **memberUid**. Если это поле оставлено пустым, имя атрибута в фильтре по умолчанию равно **memberOf**.

Атрибут разрешений на вход

Если пользователь успешно проходит аутентификацию на сервере LDAP, необходимо извлечь разрешения на вход для этого пользователя. Чтобы сделать это, фильтр поиска, отправляемый на сервер, должен содержать указание на имя атрибута, связанное с разрешениями на вход. В поле **Атрибут разрешений на вход** задается имя атрибута. Если это поле оставлено пустым, пользователю назначаются разрешения по умолчанию (только чтение), поскольку предполагается, что пользователь прошел индивидуальную и групповую аутентификацию.

Значение атрибута, возвращаемое сервером LDAP, выполняет поиск строки ключевых слов IBMRBSPermissions=. За строкой ключевых слов должна сразу следовать битовая строка, которая вводится в виде двенадцати нулей или единиц подряд. Каждый бит представляет набор функций Биты нумеруются в соответствии с расположением. Крайний левый бит — это битовая позиция 0, а крайний правый бит — это битовая позиция 11. Значение 1 битовой позиции включает функцию, связанную с этой битовой позицией. Значение 0 в битовой позиции отключает функцию, связанную с соответствующей битовой позицией.

Строка IBMRBSPermissions=010000000000 является наглядным примером утверждений выше. Строка IBMRBSPermissions= keyword используется, чтобы разрешить размещение в любом месте этого поля. Это позволяет администратору LDAP повторно использовать существующий атрибут и, следовательно, избежать расширения схемы LDAP. Кроме того, это позволяет использовать атрибут в первоначальных целях. Использовать строку ключевых слов можно в любом месте этого поля. Используемый атрибут позволяет составить строку свободного формата.a В случае успешного извлечения атрибута возвращаемое сервером LDAP значение интерпретируется в соответствии с информацией в следующей таблице.

Табл. 2. Биты разрешений

Таблица из трех столбцов, в которой объясняются позиции битов.

Табл. 2. Биты разрешений (продолж.)

Позиция бита	Функция	Объяснение
0	Всегда отказывать	Пользователь никогда не сможет пройти аутентификацию. Эту функцию можно использовать, чтобы заблокировать конкретного пользователя или пользователей, связанных с определенной группой.
1	Доступ уровня «Администратор»	Пользователю присваиваются привилегии администратора. У пользователя появляется доступ на чтение и запись в отношении каждой функции. Если настроить этот бит, настраивать другие биты по отдельности не потребуется.
2	Доступ «Только чтение»	Пользователь получает доступ «Только чтение» и не может выполнять никакие процедуры обслуживания (например, перезапускать систему, выполнять удаленные действия или обновления микропрограмм) или вносить изменения (то есть выполнять функции сохранения, очистки и восстановления). Позиция бита 2 и все остальные биты являются взаимно исключающими, позиция бита 2 имеет самый низкий приоритет. Если заданы какие-либо другие биты, этот бит будет игнорироваться.
3	Сетевые параметры и безопасность	Пользователь может менять параметры сети, сетевые протоколы, сетевой интерфейс, назначение портов и конфигурации последовательных портов.
4	Управление учетными записями пользователей	Пользователь может добавлять, изменять и удалять пользователей, а также менять параметры глобального входа в окне «Профили входа».
5	Доступ к удаленной консоли	Пользователь может осуществлять доступ к удаленной консоли сервера.
6	Доступ к удаленной консоли и удаленному диску	Пользователь может осуществлять доступ к удаленной консоли сервера и функциям удаленного диска для удаленного сервера.
7	Удаленный доступ к питанию/перезапуску сервера	Пользователь может осуществлять доступ к функциям включения и перезапуска удаленного сервера.
8	Базовая конфигурация адаптера	Пользователь может менять параметры конфигурации на страницах «Системные параметры» и «Оповещения».
9	Возможность очищать журналы событий	Пользователь может очищать журналы событий. **Примечание:** Все пользователи могут просматривать журналы событий, однако для очистки журналов требуется разрешение этого уровня.

Табл. 2. Биты разрешений (продолж.)

Позиция бита	Функция	Объяснение
10	Расширенная конфигурация адаптера	У пользователя нет ограничений по настройке XClarity Controller. Кроме того, пользователь имеет административные права доступа к XClarity Controller. Пользователь может выполнять следующие расширенные функции: обновление микропрограмм, загрузка сети PXE, восстановление заводских значений XClarity Controller, изменение и восстановление конфигурации адаптера из файла конфигурации, а также перезапуск и сброс XClarity Controller.
11	Зарезервирован	Эта позиция бита зарезервирована для будущего использования. Если ни один из битов не настроен, пользователь обладает правами только на чтение. Приоритет отдается разрешениям на вход, которые извлекаются непосредственно из записи пользователя. Если атрибут разрешений на вход отсутствует в записи пользователя, предпринимается попытка извлечь разрешения из групп, к которым относится пользователь. Это действие выполняется на этапе групповой аутентификации. Пользователю назначаются все биты во всех группах с включающим «ИЛИ». Бит доступа «Только чтение» (позиция 2) задается, только если для всех остальных битов задан нуль. Бит «Всегда отказывать» (позиция 0) задается для любой из групп, пользователю отказано в доступе. Бит «Всегда отказывать» (позиция 0) имеет приоритет над всеми остальными битами.

Если ни один из битов не настроен, для пользователя будет задано значение по умолчанию **Только чтение**.

Обратите внимание, что приоритет отдается разрешениям на вход, которые извлекаются непосредственно из записи пользователя. Если атрибут разрешений на вход отсутствует в записи пользователя, предпринимается попытка извлечь разрешения из групп, к которым относится пользователь, и которые соответствуют групповому фильтру (если он настроен). В этом случае пользователю назначаются все биты во всех группах с включающим «ИЛИ». Аналогично, бит доступа **Только чтение** будет задан, если все остальные биты равны нулю. Кроме того, обратите внимание, что если бит **Всегда отказывать** задается для любой из групп, пользователю будет отказано в доступе. Бит **Всегда отказывать** имеет приоритет над всеми остальными битами.

Примечание: Если предоставить пользователю возможность менять базовые, сетевые параметры и параметры конфигурации адаптера, связанные с безопасностью, целесообразно предоставить пользователю и возможность перезапускать контроллер XClarity Controller (позиция бита 10). В противном случае пользователь сможет изменить параметры (например, IP-адрес адаптера), но не сможет сделать так, чтобы они вступили в силу.

3. Выберите, нужно ли **Включить расширенную безопасность на основе ролей для пользователей Active Directory** в разделе **Параметры Active Directory** (если используется режим **Использовать сервер LDAP для аутентификации и авторизации**) или настроить параметр **Группы для локальной авторизации** (если используется режим **Использовать сервер LDAP только для аутентификации** (**с локальной авторизацией**).

   - **Включить расширенную безопасность на основе ролей для пользователей Active Directory**

     Если включена эта настройка, необходимо настроить имя сервера в произвольном формате так, чтобы оно функционировало как имя целевого объекта для конкретного контроллера

XClarity Controller. Целевое имя может быть связано с одной или несколькими ролями на сервере Active Directory посредством оснастки RBS. Это достигается созданием управляемых целей, присвоением им конкретных имен и связыванием их с определенными ролями. Если в этом поле настроено имя, оно обеспечит возможность определения конкретных ролей для пользователей и контроллеров XClarity Controller (целевых объектов), которые являются участниками той же роли. Когда пользователь выполняет вход в XClarity Controller и проходит аутентификацию через Active Directory, роли, участником которых является пользователь, извлекаются из каталога. Разрешения, назначаемые пользователю, извлекаются из ролей, участником которых является целевой объект, соответствующий имени сервера, которое настраивается здесь, или целевой объект, соответствующий любому контроллеру XClarity Controller. Несколько контроллеров XClarity Controller могут совместно использовать одно и то же целевое имя. Оно может использоваться для группировки нескольких XClarity Controller и присвоения им одной роли (или ролей) с помощью одного управляемого целевого объекта. Напротив, каждому контроллеру XClarity Controller можно присвоить уникальное имя.

- **Группы для локальной авторизации**

  Имена групп настраиваются для того, чтобы предоставить группам пользователей спецификации для локальной авторизации. Каждому имени группы можно назначить разрешения (роли) — такие же, как в таблице выше. Сервер LDAP связывает пользователей с именем группы. Когда пользователь выполняет вход, ему присваиваются разрешения, связанные с группой, к которой относится пользователь. Для настройки дополнительных групп щелкните значок «+», для удаления — значок «x».

Настройка сетевых протоколов

Воспользуйтесь информацией из этого раздела для просмотра или настройки сетевых параметров XClarity Controller.

Настройка параметров Ethernet

Воспользуйтесь информацией из этого раздела для просмотра или изменения способа обмена данными XClarity Controller по подключению Ethernet.

Контроллер XClarity Controller оснащен двумя сетевыми контроллерами. Один сетевой контроллер подключен к выделенному порту управления, а другой — к общему порту. Каждому сетевому контроллеру присваивается собственный записанный MAC-адрес. Если DHCP используется для назначения IP-адреса контроллеру XClarity Controller, то когда пользователь переключается между сетевыми портами или происходит отработка отказа и переход с выделенного сетевого порта на общий сетевой порт, сервер DHCP может присвоить контроллеру XClarity Controller другой IP-адрес. Рекомендуется, чтобы при использовании DHCP пользователи указывали имя хоста, а не IP-адрес, для осуществления доступа к XClarity Controller. Если сетевые порты XClarity Controller не изменяются, сервер DHCP может назначить контроллеру XClarity Controller другой IP-адрес, когда срок действия аренды DHCP истечет или когда XClarity Controller выполняет перезагрузку. Если пользователю требуется осуществлять доступ к XClarity Controller с помощью IP-адреса, который не изменится, следует настроить для XClarity Controller статический IP-адрес, а не DHCP.

Щелкните **Network** в разделе **BMC Configuration** для просмотра параметров Ethernet для XClarity Controller.

Конфигурация имени хоста XClarity Controller

Имя хоста XClarity Controller по умолчанию представляет собой комбинацию строки XCC, типа компьютера сервера и серийного номера сервера (например, «XCC-7X03-1234567890»). Имя хоста XClarity Controller можно изменить, введя значение в этом поле (не более 63 символов). Имя хоста не должно содержать точку (.) и может содержать только буквы, цифры, дефисы и нижние подчеркивания.

Порты Ethernet

Этот параметр управляет включением портов Ethernet, используемых контроллером управления, включая общие и выделенные порты.

После **отключения** всем портам Ethernet не будут назначать адреса IPv4 или IPv6, а также не будут вноситься какие-либо дальнейшие изменения в конфигурации Ethernet.

Примечание: Этот параметр не влияет на интерфейс USBLAN или порт управления USB в передней части сервера. Этим интерфейсам соответствуют их собственные параметры включения.

Настройка параметров сети IPv4

Чтобы воспользоваться подключением Ethernet IPv4, выполните следующие действия:

1. Включите параметр **IPv4**.

   Примечание: Выключение интерфейса Ethernet не позволяет осуществлять доступ к XClarity Controller из внешней сети.

2. В поле **Способ** выберите одно из следующих значений:
   - **Получить IP-адрес от DHCP**: контроллер XClarity Controller будет получать свой адрес IPv4 от сервера DHCP.
   - **Использовать статический IP-адрес**: XClarity Controller будет использовать заданное пользователем значение адреса IPv4.
   - **Сначала DHCP, затем статический IP-адрес**: XClarity Controller попытается получить свой адрес IPv4 от сервера DHCP, однако если попытка завершится неудачно, XClarity Controller будет использовать в качестве адреса IPv4 заданное пользователем значение.
3. В поле **Статический адрес** введите IP-адрес, который требуется присвоить XClarity Controller.

   Примечание: IP-адрес должен содержать четыре целых числа от 0 до 255 без пробелов с разделением точками. Это поле недоступно для настройки, если в качестве способа указано **Получить IP-адрес от DHCP**.

4. В поле **Маска сети** введите маску подсети, используемую XClarity Controller.

   Примечание: Маска подсети должна содержать четыре целых числа от 0 до 255 без пробелов или нескольких точек подряд с разделением точками. Значение по умолчанию — 255.255.255.0. Это поле недоступно для настройки, если в качестве способа указано **Получить IP-адрес от DHCP**.

5. В поле **Шлюз по умолчанию** введите маршрутизатор сетевого шлюза.

   Примечание: Адрес шлюза должен содержать четыре целых числа от 0 до 255 без пробелов или нескольких точек подряд с разделением точками. Это поле недоступно для настройки, если в качестве способа указано **Получить IP-адрес от DHCP**.

Настройка параметров расширенного Ethernet

Для настройки дополнительных параметров Ethernet перейдите на вкладку **Расширенный Ethernet**.

Примечание: В системе Flex System параметры виртуальной локальной сети контролируются CMM Flex System и не могут быть изменены в XClarity Controller.

Чтобы включить добавление меток виртуальной локальной сети (VLAN) установите флажок **Включить виртуальную локальную сеть**. Если виртуальная локальная сеть включена и настроен ИД виртуальной локальной сети, XClarity Controller принимает только пакеты с заданными ИД виртуальной локальной сети. Для идентификаторов виртуальной локальной сети можно настроить только числовые значения от 1 до 4094.

В списке **Выбор MAC-адреса** выберите одно из следующих значений:

- Использование записанного MAC-адреса

  Параметр «Записанный MAC-адрес» — это уникальный физический адрес, присваиваемый XClarity Controller производителем. Этот адрес доступен только для чтения.

- Использование пользовательского MAC-адреса

  Если значение задано, локально администрируемый адрес переопределяет записанный MAC-адрес. Локально администрируемый адрес должен представлять собой шестнадцатеричное значение от `000000000000` до `FFFFFFFFFFFF`. Это значение должно иметь формат *xx:xx:xx:xx:xx:xx*, где *x* — это шестнадцатеричное число от 0 до 9 или от «a» до «f». XClarity Controller не поддерживает использование адресов многоадресной рассылки. Первый байт адреса многоадресной рассылки — нечетное число (наименее значимому биту присваивается значение 1); поэтому первый байт должен быть четным числом.

В поле **Максимальная единица передачи** укажите максимальную единицу передачи пакета (в байтах) для сетевого интерфейса. Диапазон значений максимальной единицы передачи — от 60 до 1500. Значение по умолчанию — 1500.

Чтобы воспользоваться подключением Ethernet IPv6, выполните следующие действия:

Настройка параметров сети IPv6

1. Включите параметр **IPv6**.
2. Присвойте адрес IPv6 интерфейсу, используя один из следующих методов присвоения:
   - Использовать безагентскую автоматическую конфигурацию адресов
   - Использовать конфигурацию адресов с запоминанием состояния (DHCPv6)
   - Использовать статически присваиваемый IP-адрес

     Примечания: Если выбран параметр **Использовать статически присваиваемый IP-адрес**, потребуется ввести следующие сведения:

     – Адрес IPv6
     – Длина префикса
     – Шлюз

Настройка DNS

Воспользуйтесь информацией из этого раздела для просмотра или изменения параметров DNS XClarity Controller.

Примечание: В системе Flex System невозможно изменить параметры DNS для XClarity Controller. Модуль CMM управляет параметрами DNS.

Щелкните **Network** в разделе **BMC Configuration** для просмотра или изменения параметров DNS для XClarity Controller.

Если устанавливается флажок **Использовать дополнительные серверы адресов DNS**, не забудьте указать IP-адреса нескольких (до трех) серверов DNS в сети. Каждый IP-адрес должен содержать целые числа от 0 до 255, разделяемые точками. Такие адреса серверов DNS добавляются в верхнюю часть списка поиска, поэтому сначала поиск имени хоста выполняется на этих серверах, а затем — на том, который автоматически назначен сервером DHCP.

Настройка DDNS

Воспользуйтесь информацией из этого раздела для включения и отключения протокола динамической системы доменных имен (DDNS) на контроллере XClarity Controller.

Щелкните **Network** в разделе **BMC Configuration** для просмотра или изменения параметров DDNS для XClarity Controller.

Установите флажок **Включить DDNS**, чтобы включить DDNS. Если DDNS включена, XClarity Controller уведомляет сервер доменных имен о необходимости изменить в режиме реального времени активную конфигурацию сервера доменных имен для настроенных XClarity Controller имен хостов, адресов и прочих сведений, хранимых на сервере доменных имен.

Выберите параметр из списка элементов, чтобы указать, как должно выбираться доменное имя XClarity Controller.

- **Использовать пользовательское доменное имя**: можно указать доменное имя, к которому относится XClarity Controller.
- **Использовать доменное имя, полученное от сервера DHCP**: доменное имя, к которому относится XClarity Controller, задается сервером DHCP.

Настройка интерфейса Ethernet через USB

Воспользуйтесь информацией из этого раздела для управления интерфейсом Ethernet через USB, используемым для внутриполосного обмена данными между сервером и контроллером XClarity Controller.

Щелкните **Network** в разделе **BMC Configuration** для просмотра или изменения параметров интерфейса Ethernet через USB для XClarity Controller.

Интерфейс Ethernet через USB используется для внутриполосного обмена данными с XClarity Controller. Установите этот флажок, чтобы включить или отключить интерфейс Ethernet через USB.

Важно: Если выключить интерфейс Ethernet через USB, не удастся выполнить внутриполосное обновление микропрограммы XClarity Controller или микропрограммы сервера с помощью служебных программ Linux или Windows на флэш-носителях.

Выберите метод, используемый XClarity Controller для назначения адресов конечным точкам интерфейса Ethernet через USB.

- **Использовать локальный адрес канала IPv6 для интерфейса Ethernet через USB**: Этот метод использует адреса IPv6 на основе MAC-адреса, выделенного конечным точкам интерфейса Ethernet через USB. Как правило, локальный адрес канала IPv6 создается с использованием MAC-адреса (RFC 4862), однако Windows 2008 и более новые ОС 2016 года не поддерживают статический локальный адрес канала IPv6 на хост-стороне интерфейса. Вместо поведения Windows по умолчанию при выполнении воссоздаются произвольные локальные адреса каналов Если интерфейс Ethernet через USB контроллера XClarity Controller настроен для использования режима локального адреса канала IPv6, различные функции, основанные на использовании этого интерфейса, работать не будут, поскольку XClarity Controller не будет знать, какой адрес система Windows назначила интерфейсу. Если сервер работает под управлением Windows, воспользуйтесь любым другим методом конфигурации адреса Ethernet через USB или отключите поведение Windows по умолчанию, воспользовавшись следующей командой: *netsh interface ipv6 set global randomizeidentifiers=disabled*
- **Использовать локальный адрес канала IPv4 для интерфейса Ethernet через USB**: IP-адрес в диапазоне 169.254.0.0/16 присваивается контроллеру XClarity Controller и серверной стороне сети.

- **Настроить параметры IPv4 для интерфейса Ethernet через USB**: При использовании этого метода система задает IP-адреса и сетевую маску, которые назначаются контроллеру XClarity Controller и серверной стороне интерфейса Ethernet через USB.

Примечания:

1. Параметры конфигурации IP ОС не используются для настройки IP-адреса ОС интерфейса Ethernet через USB, однако используются для уведомления BMC о том, что IP-адрес ОС интерфейса Ethernet через USB изменился.
2. Перед настройкой трех IP-параметров для интерфейса Ethernet через USB необходимо вручную настроить IP-адрес ОС интерфейса Ethernet через USB в локальной операционной системе.

Сопоставление номеров внешних портов Ethernet номерам портов Ethernet через USB контролируется флажком **Включить перенаправление внешнего порта Ethernet в порт Ethernet через USB** и требует указания информации о сопоставлении для портов, которые следует перенаправить из интерфейса сети управления на сервер.

Настройка SNMP

Воспользуйтесь информацией из этого раздела для настройки агентов SNMP.

Выполните следующие шаги для настройки параметров оповещений SNMP в XClarity Controller.

1. Щелкните **Network** в разделе **BMC Configuration**.
2. Установите соответствующий флажок, чтобы включить **SNMPv1 Trap**, **SNMPv2 Trap** и/или **SNMPv3 Trap**.
3. Заполните следующие поля при включении ловушки **SNMPv1 Trap** или **SNMPv2**:
   a. В поле **Имя сообщества** введите имя сообщества; имя не может быть пустым.
   b. В поле **Хост** введите адрес хоста.
4. Заполните следующие поля при включении ловушки **SNMPv3**:
   a. В поле **ИД механизма** введите ИД механизма Поле «ИД механизма» не может быть пустым.
   b. В поле **Порт приемника ловушки** введите номер порта. Номер порта по умолчанию: 162.
5. При включении ловушек SNMP выберите типы событий, о которых вы хотите получать оповещения:
   - **Критическое**
   - **Внимание!**
   - **Системное**

   Примечание: Нажмите на каждую основную категорию, чтобы дополнительно выбрать типы событий подкатегории, о которых вы хотите получать оповещения.

Включение и отключение сетевого доступа IPMI

Воспользуйтесь информацией из этого раздела для управления сетевым доступом IPMI к XClarity Controller.

Щелкните **Network** в разделе **BMC Configuration** для просмотра или изменения параметров IPMI для XClarity Controller. Для просмотра или изменения параметров IPMI заполните следующие поля:

Доступ к IPMI через локальную сеть
Щелкните переключатель, чтобы включить или выключить сетевой доступ IPMI к XClarity Controller.

Важно:

- Если вы не используете никакие инструменты или приложения, осуществляющие доступ к XClarity Controller по сети с помощью протокола IPMI, в целях безопасности настоятельно рекомендуется отключить сетевой доступ IPMI.
- По умолчанию доступ к XClarity Controller с помощью IPMI через локальную сеть отключен.

Настройка параметров сети с использованием команд IPMI

Воспользуйтесь информацией из этого раздела для настройки параметров сети с помощью команд IPMI.

Поскольку каждый параметр сети BMC настраивается с использованием отдельных запросов IPMI и без какого-либо определенного порядка, у BMC отсутствует полное представление обо всех параметрах сети до тех пор, пока BMC не будет перезапущен, чтобы применить ожидающие изменения сети. Запрос на изменение параметра сети может быть успешным в момент запроса, однако при запросе дополнительных изменений он может стать недопустимым. Если ожидающие параметры сети несовместимы после перезапуска BMC, новые параметры не вступят в силу. После перезапуска BMC следует попытаться осуществить доступ к BMC с новыми параметрами, чтобы убедиться, что они применены должным образом.

Включение обслуживания и назначение портов

Воспользуйтесь информацией из этого раздела для просмотра или изменения номеров портов, используемых некоторыми службами в XClarity Controller.

Щелкните **Network** в разделе **BMC Configuration** для просмотра или изменения назначений портов XClarity Controller. Для просмотра или изменения назначений портов заполните следующие поля:

Интернет
Номер порта — 80. Это поле недоступно для настройки пользователем.

Сеть через HTTPS
В этом поле укажите номер порта для интерфейса «Сеть через HTTPS». Значение по умолчанию — 443.

REST через HTTPS
Номер порта автоматически изменится на указанный в поле «Сеть через HTTPS». Это поле недоступно для настройки пользователем.

CIM через HTTP
В этом поле укажите номер порта для интерфейса «CIM через HTTP». Значение по умолчанию — 5989.

Примечание: Интерфейс CIM по умолчанию отключен.

Удаленное присутствие
В этом поле укажите номер порта для удаленного присутствия. Значение по умолчанию — 3900.

IPMI через LAN
Номер порта — 623. Это поле недоступно для настройки пользователем.

Примечание: Интерфейс IPMI по умолчанию отключен.

SFTP

В этом поле укажите номер порта, используемый для протокола SFTP. Номер порта — 115. Это поле недоступно для настройки пользователем.

Примечание: Для внутриполосных обновлений OneCLI требуется IMM.SFTPPortControl=open.

SLP
В этом поле укажите номер порта, используемый для SLP. Номер порта — 427. Это поле недоступно для настройки пользователем.

Примечания: Существует два типа служб, о которых XClarity Controller составляет отчеты:

- служба management-hardware.Lenovo:lenovo-xclarity-controller
- служба wbem

SSDP
Номер порта — 1900. Это поле недоступно для настройки пользователем.

SSH
В этом поле укажите номер порта, настраиваемый для доступа в интерфейс командной строки через протокол SSH. Значение по умолчанию — 22.

Агент SNMP
В этом поле укажите номер порта для агента SNMP, выполняемого на контроллере XClarity Controller. Значение по умолчанию — 161. Допустимые значения номера порта — от 1 до 65535.

Ловушки SNMP
В этом поле укажите номер порта, используемый для ловушек SNMP. Значение по умолчанию — 162. Допустимые значения номера порта — от 1 до 65535.

Настройка ограничения доступа

Воспользуйтесь информацией из этого раздела для просмотра или изменения параметров блокировки доступа к XClarity Controller с IP-адресов или MAC-адресов.

Щелкните **Network** в разделе **BMC Configuration** для просмотра или изменения параметров контроля доступа к XClarity Controller.

Список блокировки и временное ограничение

Эти параметры позволяют блокировать определенные IP/MAC-адреса на указанный период времени.

- **Список заблокированных IP-адресов**
  - Можно ввести, разделяя запятыми, до трех адресов или диапазонов адресов IPv4 и до трех адресов или диапазонов адресов IPv6, доступ с которых к XClarity Controller запрещен. См. примеры адресов IPv4 ниже:
  - Пример отдельного адреса IPv4: 192.168.1.1
  - Пример адреса IPv4 в суперсети: 192.168.1.0/24
  - Пример диапазона адресов IPv4: 192.168.1.1–192.168.1.5
- **Список заблокированных MAC-адресов**
  - Можно ввести, разделяя запятыми, до трех MAC-адресов, доступ с которых к XClarity Controller запрещен. Например: 11:22:33:44:55:66.
- **Ограниченный доступ (однократно)**

  - Можно задать временной интервал одноразового использования, в течение которого доступ к XClarity Controller невозможен. При задании этого временного интервала необходимо соблюдать следующие условия:
  - Дата и время начала должны быть позже текущего времени XCC.
  - Дата и время окончания должны быть позже даты и времени начала.
- **Ограниченный доступ (ежедневно)**
  - Можно задать один или несколько ежедневных временных интервалов, в течение которых доступ к XClarity Controller невозможен. При задании каждого временного интервала необходимо соблюдать следующее условие:
  - Дата и время окончания должны быть позже даты и времени начала.

Список блокировки с внешней активацией

Эти параметры позволяют настроить автоматическую блокировку определенных IP-адресов (IPv4 и IPv6), с которым клиент последовательно пытался войти в XClarity Controller с различными неправильными сочетаниями имени пользователя и пароля.

Функция автоматической блокировки динамически определяет случаи чрезмерного количества ошибок при входе в систему с определенных IP-адресов и блокирует этим адресам доступ к XClarity Controller на заранее определенный период времени.

- **Максимальное количество ошибок при входе в систему с отдельного IP-адреса**
  - Максимальное количество попыток определяет количество ошибок при входе в систему, которые может совершить пользователь, вводя неверный пароль с определенного IP-адреса, прежде чем он будет заблокирован.
  - Если задано значение 0, IP-адрес не будет блокироваться на основании ошибок при входе в систему.
  - Счетчик ошибок при входе в систему для определенного IP-адреса будет обнулен после успешного входа с этого IP-адреса.
- **Период блокировки IP-адреса**
  - Минимальное количество времени (в минутах), которое должно пройти, прежде чем пользователь снова сможет попытаться выполнить вход с заблокированного IP-адреса.
  - Если задано значение 0, доступ с заблокированного IP-адреса остается заблокированным, пока администратор специально не разблокирует его.
- **Список блокировки**
  - В таблице «Список блокировки» отображаются все заблокированные IP-адреса. Можно разблокировать один или все IP-адреса из списка блокировки.

Настройка USB-порта на передней панели для управления

Воспользуйтесь информацией из этого раздела для настройки USB-порта на лицевой панели XClarity Controller для управления.

На некоторых серверах USB-порт на лицевой панели можно переключить и подключить либо к серверу, либо к XClarity Controller. Подключение к XClarity Controller, в основном, предназначено для использования на мобильном устройстве с мобильным приложением Lenovo XClarity. Если USB-кабель соединяет мобильное устройство и лицевую панель сервера, подключение Ethernet через USB будет установлено между мобильным приложением, выполняемым на устройстве, и XClarity Controller

Щелкните **Network** в разделе **BMC Configuration** для просмотра или изменения параметров USB-порта на лицевой панели XClarity Controller для управления.

Доступно четыре типа параметров на выбор:

Режим «Только хост»
USB-порт лицевой панели всегда подключен только к серверу.

Режим «Только BMC»
USB-порт лицевой панели всегда подключен только к XClarity Controller.

Общий режим: принадлежит BMC
USB-порт на лицевой панели совместно используется сервером и контроллером XClarity Controller, но переключен на контроллер XClarity Controller.

Общий режим: принадлежит хосту
USB-порт на лицевой панели совместно используется сервером и контроллером XClarity Controller, но переключен на хост.

Дополнительные сведения об этом мобильном приложении доступны на сайте:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_usemobileapp.html

Примечания:

- Если USB-порт на лицевой панели настроен для использования в общем режиме, порт подключен к контроллеру XClarity Controller, если питание отсутствует, и к серверу, если питание подается. При наличии питания управление USB-портом на лицевой панели может переходить от сервера к контроллеру XClarity Controller, и наоборот. В общем режиме порт также может переключаться между хостом и XClarity Controller: для этого достаточно нажать и удерживать более 3 секунд кнопку идентификации на лицевой панели (для вычислительных узлов это может быть кнопка управления USB).
- Если настроен общий режим и USB-порт в настоящее время подключен к серверу, XClarity Controller может поддерживать запрос на переключение USB-порта на лицевой панели обратно на контроллер XClarity Controller. При выполнении этого запроса USB-порт на лицевой панели останется подключенным к контроллеру XClarity Controller до тех пор, пока на контроллере не будет отсутствовать активность USB в течение периода, заданного тайм-аутом после неактивности.

Настройка параметров безопасности

Воспользуйтесь информацией из этого раздела для настройки протоколов безопасности.

Примечание: Минимальная версия TLS по умолчанию — TLS 1.2, однако XClarity Controller можно настроить для использования других версий TLS, если это необходимо для вашего браузера или приложений управления. Дополнительные сведения см. в разделе «Команда tls» на странице 162.

Щелкните **Security** в разделе **BMC Configuration**, чтобы получить доступ к свойствам безопасности, состоянию и настройкам XClarity Controller и при необходимости изменить их.

Обзор SSL

Этот раздел содержит обзор протокола безопасности SSL.

SSL — это протокол безопасности, обеспечивающий конфиденциальность связи. Благодаря протоколу SSL приложения «клиент–сервер» могут взаимодействовать без перехвата, искажения и подделки сообщений. Можно настроить контроллер XClarity Controller для использования протокола SSL для разных типов подключений, таких как HTTPS, LDAPS, CIM через HTTPS и сервер SSH, а также для управления необходимыми для SSL сертификатами.

Обработка сертификатов SSL

В данном разделе содержится информация об администрировании сертификатов, которые могут использоваться с протоколом безопасности SSL.

SSL можно использовать с самозаверяющим сертификатом или сертификатом, заверенным сторонним центром сертификации. Использование самозаверяющего сертификата — простейший способ использования SSL, однако при этом возникает небольшой риск безопасности. Этот риск возникает из-за того, что клиент SSL никак не может подтвердить идентичность сервера SSL при первом подключении, которое пытаются установить клиент и сервер. Например, сторонняя сущность может выдать себя за веб-сервер XClarity Controller и перехватить данные, передаваемые между фактическим веб-сервером XClarity Controller и веб-браузером пользователя. Если в период, когда установлено первоначальное соединение между браузером и XClarity Controller, самозаверяющий сертификат импортируется в хранилище сертификатов браузера, весь дальнейший обмен данными для такого браузера будет безопасным (при условии, что безопасность первоначального соединения не была нарушена в результате атаки).

Чтобы обеспечить более высокий уровень безопасности, можно использовать сертификат, заверенный центром сертификации (ЦС). Чтобы получить подписанный сертификат, необходимо выбрать команду **Создать запрос подписи сертификата (CSR)**. Выберите **Загрузить запрос подписи сертификата (CSR)** и отправьте запрос подписи сертификата (CSR) в ЦС, чтобы получить подписанный сертификат. Получив подписанный сертификат, щелкните **Импортировать подписанный сертификат**, чтобы импортировать его в XClarity Controller.

Функция ЦС заключатся в подтверждении идентичности XClarity Controller. Сертификат содержит цифровые подписи для ЦС и XClarity Controller. Если хорошо известный ЦС издает сертификат или сертификат ЦС был уже импортирован в веб-браузер, веб-браузер может подтвердить сертификат и положительно идентифицировать веб-сервер XClarity Controller.

XClarity Controller требует сертификат для использования с сервером HTTPS, интерфейсом CIM через HTTPS и защищенным клиентом LDAP. Кроме того, защищенный клиент LDAP также требует импорта одного или более доверенных сертификатов. Доверенный сертификат используется защищенным клиентом LDAP для положительной идентификации сервера LDAP. Доверенный сертификат — это сертификат центра сертификации, подписавшего сертификат сервера LDAP. Если на сервере LDAP используются самозаверяющие сертификаты, доверенным сертификатом может быть сам сертификат сервера LDAP. Если в конфигурации используется несколько серверов LDAP, необходимо импортировать дополнительные доверенные сертификаты.

Управление сертификатами SSL

В данном разделе содержится информация о некоторых действиях, которые можно выбрать для управления сертификатами с протоколом безопасности SSL.

Щелкните **Security** в разделе **BMC Configuration**, чтобы настроить управление сертификатами SSL.

При управлении сертификатами XClarity Controller доступны следующие действия:

Загрузка подписанного сертификата

Используйте эту ссылку для загрузки копии установленного в настоящее время сертификата. Сертификат можно загрузить в формате PEM или DER. Содержимое сертификата можно просматривать с использованием стороннего инструмента, такого как OpenSSL (www.openssl.org). Пример командной строки для просмотра содержимого сертификата с использованием OpenSSL может выглядеть так:

```
openssl x509 -in cert.der -inform DER -text
```

Загрузка запроса подписи сертификата (CSR)
Используйте эту ссылку для загрузки копии запроса подписи сертификата. Запрос CSR можно загрузить в формате PEM или DER.

Создание подписанного сертификата
Создайте самозаверяющий сертификат. По окончании операции можно включить SSL с помощью нового сертификата.

Примечание: При выполнении действия **Создание подписанного сертификата** откроется окно создания самозаверяющего сертификата для HTTPS. Отобразится запрос на заполнение обязательных и необязательных полей. *Необходимо* заполнить все обязательные поля. Введя необходимую информацию, нажмите **Создать**, чтобы завершить выполнение задачи.

Создать запрос CSR
Создайте запрос CSR. По окончании операции файл CSR можно загрузить и отправить на подпись в центр сертификации (ЦС).

Примечание: При выполнении действия **Создание запроса подписи сертификата (CSR)** откроется окно создания запроса подписи сертификата для HTTPS. Отобразится запрос на заполнение обязательных и необязательных полей. *Необходимо* заполнить все обязательные поля. Введя необходимую информацию, нажмите **Создать**, чтобы завершить выполнение задачи.

Импорт самозаверяющего сертификата
Используйте эту команду для импорта подписанного сертификата. Чтобы получить подписанный сертификат, необходимо создать запрос подписи сертификата (CSR) и отправить его в центр сертификации (ЦС).

Настройка сервера Secure Shell

Воспользуйтесь информацией из этого раздела, чтобы изучить и включить протокол безопасности SSH.

Щелкните **Network** в разделе **BMC Configuration**, чтобы настроить сервер Secure Shell.

Чтобы использовать протокол SSH, сначала необходимо создать ключ для включения сервера SSH.

Примечания:

- Чтобы использовать этот параметр, управление сертификатами не требуется.
- XClarity Controller изначально создаст ключ сервера SSH. Если требуется создать новый ключ сервера SSH, щелкните **Network** в разделе **BMC Configuration**; затем щелкните **Повторно создать ключ**.
- После этого действия необходимо перезапустить XClarity Controller, чтобы изменения вступили в силу.

Доступ с помощью IPMI через клавиатурную консоль

Воспользуйтесь информацией из этого раздела для управления доступом к XClarity Controller с помощью IPMI через клавиатурную консоль.

XClarity Controller предоставляет интерфейс IPMI по каналу клавиатурной консоли, не требующему аутентификации.

Нажмите **Безопасность** в разделе **BMC Configuration**, чтобы включить или отключить доступ с помощью IPMI через клавиатурную консоль.

Примечание: После изменения параметров необходимо перезапустить XClarity Controller, чтобы изменения вступили в силу.

Важно: Если вы не используете никакие инструменты или приложения на сервере, осуществляющем доступ к XClarity Controller по протоколу IPMI, в целях безопасности настоятельно рекомендуется отключить доступ с помощью IPMI через клавиатурную консоль. В XClarity Essentials для доступа к XClarity Controller не используется интерфейс IPMI через клавиатурную консоль. Если отключить интерфейс IPMI через клавиатурную консоль, следует включить его снова, прежде чем запускать XClarity Essentials на сервере. После этого интерфейс можно отключить.

Предотвращение перехода к предыдущим версиям системных микропрограмм

Воспользуйтесь информацией из этого раздела, чтобы не допустить перехода на предыдущие версии системных микропрограмм.

Эта функция позволяет разрешить возвращение к предыдущим версиям микропрограмм системы или запретить такое поведение.

Щелкните **Network** в разделе **BMC Configuration**, чтобы предотвратить возвращение к предыдущим версиям микропрограмм

Для включения или выключения этой функции щелкните **Network** в разделе **BMC Configuration**. Любые внесенные изменения вступят в силу незамедлительно, перезапускать XClarity Controller для этого не требуется.

Подтвердите физическое присутствие

Воспользуйтесь информацией из этого раздела для подтверждения и отмены подтверждения физического присутствия с веб-страницы XClarity Controller без физического присутствия на сервере.

Эта функция доступна, только если **Политика физического присутствия** включена с помощью UEFI. Если эта политика включена, вы сможете пользоваться функцией физического присутствия, нажав **Security** в разделе **BMC Configuration**.

Настройка управления ключами безопасности (SKM)

Воспользуйтесь информацией из этого раздела для создания ключей безопасности и управления ими.

Эта функция использует централизованный сервер управления ключами для предоставления ключей, разблокирующих оборудование хранилищ, чтобы получить доступ к данным, хранимым на дисках SED на сервере ThinkSystem. Сервер управления ключами включает SKLM — сервер управления ключами с дисками SED IBM — и KMIP — серверы управления ключами с дисками SED Thales/Gemalto (KeySecure и CipherTrust).

XClarity Controller использует сеть для извлечения ключей с сервера управления ключами; сервер управления ключами должен быть доступен контроллеру XClarity Controller. XClarity Controller образует канал обмена данными между сервером управления ключами и запрашивающим сервером ThinkSystem. Микропрограмма XClarity Controller пытается связаться с каждым из настроенных серверов управления ключами и прекращает попытки, как только подключение установлено.

XClarity Controller устанавливает связь с сервером управления ключами, если выполнены следующие условия:

- Одно или несколько имен хоста/IP-адресов сервера управления ключами настроены в XClarity Controller.
- Два сертификата (клиента и сервера) для обмена данными с сервером управления ключами установлены на контроллере XClarity Controller.

Примечание: Настройте для своего устройства по меньшей мере два сервера управления ключами (основной и дополнительный) с одним и тем же протоколом. Если основной сервер управления ключами не реагирует на попытку подключения от XClarity Controller; попытки подключения с дополнительных серверов управления ключами будут инициироваться до тех пор, пока не будет установлено успешное подключение.

Между контроллером XClarity Controller и сервером управления ключами должно быть установлено подключение TLS. XClarity Controller выполняет аутентификацию сервера управления ключами, сравнивая отправленный сервером управления ключами сертификат сервера с сертификатом сервера управления ключами, ранее импортированным в доверенное хранилище XClarity Controller. Сервер управления ключами выполняет аутентификацию каждого контроллера XClarity Controller, который устанавливает с ним связь, и проверяет, что контроллеру XClarity Controller разрешено осуществлять доступ к серверу управления ключами. Аутентификация выполняется путем сравнения сертификата клиента, отправленного контроллером XClarity Controller, со списком доверенных сертификатов, которые хранятся на сервере управления ключами.

Будет подключен по меньшей мере один сервер управления ключами, а группа устройств считается необязательной. Сертификат сервера управления ключами импортируется, а сертификат клиента необходимо задать. По умолчанию используется сертификат HTTPS. Если его нужно заменить, можно создать новый сертификат.

Примечание: Чтобы подключить сервер KMIP (KeySecure и CipherTrust), необходимо сгенерировать запрос на подпись сертификата (CSR), а его общее имя должно соответствовать имени пользователя, определенному на сервере KMIP. Затем необходимо импортировать сертификат, подписанный центром сертификации, которому доверяет сервер KMIP для CSR.

Настройка серверов управления ключами

Воспользуйтесь информацией из этого раздела для создания имени хоста или IP-адреса и соответствующей информации о портах для сервера управления ключами.

В разделе настройки сервера(ов) управления ключами доступны следующие поля:

Имя хоста или IP-адрес
В этом поле введите имя хоста (если DNS включена и настроена) или IP-адрес сервера управления ключами. Можно добавить до четырех серверов.

Порт
В этом поле введите номер порта для сервера управления ключами. Если это поле оставлено пустым, используется значение по умолчанию 5696. Допустимые значения номера порта: от 1 до 65535.

Настройка группы устройств

Воспользуйтесь информацией из этого раздела, чтобы настроить группу устройств, используемых на сервере SKLM.

Группа устройств на сервере SKLM позволяет пользователям управлять ключами SED (самошифруемого диска) на нескольких серверах в качестве группы. Необходимо создать группу устройств с тем же именем на сервере SKLM.

В разделе «Группа устройств» доступно следующее поле:

Группа устройств

Группа устройств позволяет пользователям управлять ключами для самошифруемых дисков (SED) на нескольких серверах в качестве группы. Необходимо создать группу устройств с тем же именем на сервере SKLM. Значение по умолчанию для этого поля — IBM_SYSTEM_X_SED.

Настройка управления сертификатами

В этом разделе содержатся сведения об управлении сертификатами для клиента и сервера.

Сертификаты клиента и сервера используются для аутентификации взаимодействия между сервером SKLM и контроллером XClarity Controller, размещенном на сервере ThinkSystem. В этом разделе рассматриваются вопросы управления сертификатами клиента и сервера.

Управление сертификатами клиента

В этом разделе содержатся сведения об управлении сертификатом клиента.

Сертификаты клиента классифицируются следующим образом:

- Самозаверяющий сертификат XClarity Controller.
- Сертификат, созданный в ответ на запрос на подпись сертификата (CSR) XClarity Controller и подписанный сторонним ЦС (вне организации).

Сертификат клиента необходим для обмена данными с сервером SKLM. Сертификат клиента содержит цифровые подписи для ЦС и XClarity Controller.

Примечания:

- При обновлении микропрограмм сертификаты сохраняются.
- Если сертификат клиента для обмена данными с сервером SKLM не создан, используется сертификат HTTPS-сервера XClarity Controller.
- Функция ЦС заключатся в подтверждении идентичности XClarity Controller.

Для создания сертификата клиента щелкните значок «плюс» ( ) и выберите один из следующих элементов:

- Создание нового ключа и самозаверяющего сертификата
- Создание нового ключа и запроса на подпись сертификата (CSR)

Элемент действия **Создать новый ключ и самозаверяющий сертификат** создает новый ключ шифрования и самозаверяющий сертификат. В окне «Создание нового ключа и самозаверяющего сертификата» введите или выберите сведения в нужных полях, а в необязательных полях укажите сведения, актуальные для вашей конфигурации (см. таблицу ниже). Нажмите кнопку **OK**, чтобы создать ключ шифрования и сертификат. Пока создается самозаверяющий сертификат, отображается окно с индикатором выполнения. Как только сертификат будет успешно установлен, отобразится окно с подтверждением.

Примечание: Новый ключ шифрования и сертификат заменяют существующий ключ и сертификат.

Табл. 3. Создание нового ключа и самозаверяющего сертификата

Таблица из двух столбцов с заголовками, в которой зафиксированы обязательные и необязательные поля действия «Создание нового ключа и самозаверяющего сертификата». Нижняя строка охватывает оба столбца.

Табл. 3. Создание нового ключа и самозаверяющего сертификата (продолж.)

Поле	Описание
Страна[1]	Выберите в списке страну физического расположения BMC.
Страна или регион[1]	Введите регион физического расположения BMC.
Город или муниципальная единица[1]	Введите город или муниципальную единицу физического расположения BMC.
Название организации[1]	Введите название компании или организации, которой принадлежит BMC.
Имя хоста BMC[1]	Введите имя хоста BMC, отображаемое в строке адреса веб-браузера.
Контактное лицо	Введите имя контактного лица, ответственного за BMC.
Адрес эл. почты	Введите адрес электронной почты контактного лица, ответственного за BMC.
Организационная единица	Укажите организационную единицу компании, которой принадлежит BMC.
Фамилия	Введите фамилию лица, ответственного за BMC. Это поле может содержать не более 60 символов.
Собственное имя	Введите имя лица, ответственного за BMC. Это поле может содержать не более 60 символов.
Инициалы	Введите инициалы лица, ответственного за BMC. Это поле может содержать не более 20 символов.
Квалификатор различающегося имени	Введите квалификатор различающегося имени для BMC. Это поле может содержать не более 60 символов.
1. Это обязательное поле.	

После создания сертификата клиента можно загрузить сертификат в хранилище на контроллере XClarity Controller, выбрав элемент действия **Загрузить сертификат**.

Элемент действия **Создать новый ключ и запрос на подпись сертификата** создает новый ключ шифрования и запрос CSR. В окне «Создание нового ключа и запроса на подпись сертификата» введите или выберите сведения в нужных полях, а в необязательных полях укажите сведения, актуальные для вашей конфигурации (см. таблицу ниже). Нажмите кнопку **OK**, чтобы создать новый ключ шифрования и запрос CSR.

Пока создается запрос CSR, отображается окно с индикатором выполнения, а по окончании процесса — окно с подтверждением. После создания CSR необходимо отправить CSR в ЦС для добавления цифровой подписи. Выберите элемент действия **Загрузить запрос на подпись сертификата (CSR)** и нажмите кнопку **OK**, чтобы сохранить CSR на сервере. Затем запрос CSR можно отправить в ЦС на подпись.

Табл. 4. Создание нового ключа и запроса на подпись сертификата

Таблица из двух столбцов с заголовками, в которой зафиксированы обязательные и необязательные поля действия «Создание нового ключа и запроса на подпись сертификата». Нижняя строка охватывает оба столбца.

Табл. 4. Создание нового ключа и запроса на подпись сертификата (продолж.)

Поле	Описание
Страна[1]	Выберите в списке страну физического расположения BMC.
Страна или регион[1]	Введите регион физического расположения BMC.
Город или муниципальная единица[1]	Введите город или муниципальную единицу физического расположения BMC.
Название организации[1]	Введите название компании или организации, которой принадлежит BMC.
Имя хоста BMC[1]	Введите имя хоста BMC, отображаемое в строке адреса веб-браузера.
Контактное лицо	Введите имя контактного лица, ответственного за BMC.
Адрес эл. почты	Введите адрес электронной почты контактного лица, ответственного за BMC.
Организационная единица	Укажите организационную единицу компании, которой принадлежит BMC.
Фамилия	Введите фамилию лица, ответственного за BMC. Это поле может содержать не более 60 символов.
Собственное имя	Введите имя лица, ответственного за BMC. Это поле может содержать не более 60 символов.
Инициалы	Введите инициалы лица, ответственного за BMC. Это поле может содержать не более 20 символов.
Квалификатор различающегося имени	Введите квалификатор различающегося имени для BMC. Это поле может содержать не более 60 символов.
Пароль запроса	Введите пароль для CSR. Это поле может содержать не более 30 символов.
Неструктурированное имя	Введите дополнительную информацию, например неструктурированное имя, присваиваемое BMC. Это поле может содержать не более 60 символов.
1. Это обязательное поле.	

ЦС ставит цифровую подпись на запрос CSR, используя инструмент обработки сертификатов пользователя, например *OpenSSL* или инструмент командной строки *Certutil*. Все сертификаты клиента, подписываемые с помощью инструмента обработки сертификата пользователя, имеют один и тот же *базовый* сертификат. Этот *базовый* сертификат необходимо также импортировать на сервер SKLM, чтобы все сертификаты с цифровой подписью пользователя принимались сервером SKLM.

Подписанный ЦС сертификат необходимо импортировать в BMC. Выберите элемент действия **Импорт подписанного сертификата** и выберите файл для отправки в качестве сертификата клиента, затем нажмите кнопку **OK**. Пока отправляется подписанный ЦС сертификат, отображается окно с индикатором выполнения. Как только сертификат будет успешно отправлен, отобразится окно отправки сертификата. Если сертификат не отправлен, отобразится окно с ошибкой отправки сертификата.

Примечания:

- В целях безопасности рекомендуется пользоваться сертификатами с цифровой подписью ЦС.

- Импортируемый на контроллер XClarity Controller сертификат должен соответствовать ранее созданному запросу CSR.

После импорта сертификата с подписью ЦС в BMC выберите элемент действия **Загрузить сертификат**. При выборе этого элемента действия сертификат с подписью ЦС загружается с контроллера XClarity Controller в хранилище вашей системы.

Управление сертификатами сервера

В этом разделе содержатся сведения об управлении сертификатом сервера.

Сертификат сервера создается на сервере SKLM, и его необходимо импортировать в XClarity Controller, чтобы функция безопасного доступа к дискам заработала. Чтобы импортировать сертификат, аутентифицирующий сервер SKLM в BMC, щелкните **Импортировать сертификат** в разделе «Состояние сертификата сервера» на странице «Доступ к дискам». Перенос файла в хранилище на контроллере XClarity Controller иллюстрируется индикатором выполнения.

После успешного переноса сертификата сервера на контроллер XClarity Controller, в области «Состояние сертификата сервера» отображается следующее содержимое: `A server certificate is installed`.

Если требуется удалить доверенный сертификат, нажмите соответствующую кнопку **Удалить**.

Расширенный журнал аудита

Воспользуйтесь информацией из этого раздела для управления расширенным журналом аудита.

Эта функция позволяет определить, следует ли включать записи журнала команды set IPMI (необработанные данные) из каналов LAN и KCS в журнал аудита.

Нажмите **Безопасность** в раздел **Конфигурация BMC** в веб-интерфейсе XCC, чтобы включить или отключить расширенный журнал аудита.

Примечание: Если команда set IPMI поступает из канала LAN, в сообщение в журнале будут включены имя пользователя и IP-адрес источника. Все команды IPMI с конфиденциальной информацией, связанной с безопасностью (например, паролем), исключаются из журнала.

Настройка шифрования

Воспользуйтесь информацией из этого раздела, чтобы изучить разные настройки шифрования.

Режим высокой безопасности

- Поддерживаются только строгие и современные шифры.
- Соответствует стандарту NIST.
- Соответствует стандарту PFS (Perfect Forward Secrecy).

Режим совместимости

- Поддерживает широкий диапазон шифров для максимальной совместимости.
- Не соответствует стандартам PFS и NIST.

Режим соответствия стандарту NIST

- Поддерживает широкий диапазон шифров для максимальной совместимости.
- Соответствует стандарту NIST.

- Соответствует стандарту PFS.

Поддержка версии TLS

- TLS 1.0 и выше
- TLS 1.1 и выше
- TLS 1.2 и выше
- TLS 1.3

Настройка шифрования TLS призвана ограничить поддерживаемые наборы шифров TLS для служб BMC.

Поддерживаемые наборы шифров TLS приводятся в следующей таблице

Режим безопасности	**Версия TLS**	**Набор шифров TLS**
Режим высокой безопасности	TLS 1.3 и ниже	• TLS_AES_256_GCM_SHA384
Режим высокой безопасности	TLS 1.2 и ниже	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Режим соответствия стандарту NIST	TLS 1.3 и ниже	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256
Режим соответствия стандарту NIST	TLS 1.2 и ниже	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Режим совместимости	TLS 1.3 и ниже	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256

Режим безопасности	Версия TLS	Набор шифров TLS
Режим совместимости	TLS 1.2 и ниже	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Режим совместимости	TLS 1.1 и ниже	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

Резервное копирование и восстановление конфигурации BMC

Сведения в этом разделе помогут восстановить или изменить вашу конфигурацию BMC.

Для выполнения следующих действий выберите **Резервное копирование и восстановление** в разделе **BMC Configuration**.

- Просмотр сводки по конфигурации контроллера управления
- Резервное копирование или восстановление конфигурации контроллера управления
- Просмотр состояния резервного копирования или восстановления
- Сброс конфигурации контроллера управления до заводского состояния
- Доступ к мастеру первоначальной настройки контроллера управления

Резервное копирование конфигурации BMC

Сведения в этом разделе помогут выполнить резервное копирование конфигурации BMC.

Выберите **Резервное копирование и восстановление** в разделе **BMC Configuration**. В самом верху страницы отображается раздел **Резервное копирование конфигурации BMC**.

Если ранее уже было выполнено резервное копирование, сведения о нем отображаются в поле **Последнее резервное копирование**.

Чтобы выполнить резервное копирование текущей конфигурации BMC, выполните шаги ниже:

1. Укажите пароль для файла резервной копии BMC.
2. Укажите, нужно ли зашифровать весь файл или только конфиденциальные данные.

3. Начните процесс резервного копирования, нажав кнопку **Начать резервное копирование**. Во время этого процесса не разрешено выполнять какие-либо действия по восстановлению или сбросу параметров.
4. По окончании этого процесса появится кнопка, позволяющая загрузить и сохранить файл.

Примечание: Когда пользователь настраивает нового пользователя/пароль XClarity Controller и выполняет резервное копирование конфигурации, также включаются учетная запись по умолчанию и пароль (USERID/PASSWORD). Последующее удаление учетной записи по умолчанию и пароля из резервной копии приведет к тому, что система отобразит сообщение, уведомляющее пользователя о сбое при восстановлении учетной записи/пароля XClarity Controller. Пользователи могут игнорировать это сообщение.

Восстановление конфигурации BMC

Сведения в этом разделе помогут восстановить вашу конфигурацию BMC.

Выберите **Резервное копирование и восстановление** в разделе **BMC Configuration**. Под разделом **Резервное копирование конфигурации BMC** находится раздел **Восстановление BMC из файла конфигурации**.

Чтобы восстановить ранее сохраненную конфигурацию BMC, выполните действия ниже:

1. Найдите и выберите файл резервной копии и введите пароль в ответ на соответствующий запрос.
2. Проверьте файл, нажав **Просмотр содержимого** для просмотра сведений.
3. После проверки содержимого нажмите **Начать восстановление**.

Сброс параметров BMC до заводских настроек

Воспользуйтесь информацией из этого раздела для сброса BMC до заводского состояния.

Выберите **Резервное копирование и восстановление** в разделе **BMC Configuration**. Под разделом **Восстановление BMC из файла конфигурации** находится раздел **Сброс BMC до заводского состояния**.

Чтобы сбросить BMC до заводского состояния, выполните следующие действия:

1. Щелкните **Начать сброс BMC до заводского состояния**.

   Примечания:

   - Выполнить это действие могут только пользователи с правами уровня «Администратор».
   - Подключение Ethernet временно разорвано. Необходимо снова выполнить вход в веб-интерфейс XClarity Controller по окончании операции сброса.
   - После нажатия кнопки **Начать сброс BMC до заводского состояния** все ранее сделанные изменения конфигурации будут потеряны. Если при восстановлении конфигурации BMC требуется включить LDAP, сначала необходимо импортировать доверенный сертификат безопасности.
   - По окончании процесса XClarity Controller будет перезапущен. Если это локальный сервер, подключение TCP/IP будет разорвано, и для восстановления подключения, возможно, потребуется изменить настройки сетевого интерфейса.
   - Сброс параметров BMC до заводских настроек не влияет на параметры UEFI.

Перезапуск контроллера XClarity Controller

В этом разделе содержится информация о перезапуске контроллера XClarity Controller.

Подробные сведения о перезапуске контроллера XClarity Controller см. в разделе «Действия кнопки питания» на странице 66

Глава 4. Мониторинг состояния сервера

Информация в этом разделе поможет понять, как просматривать и отслеживать информацию о сервере, к которому вы осуществляете доступ.

После входа в систему XClarity Controller отобразится страница состояния системы. На этой странице можно просмотреть состояние оборудования сервера, журналы событий и аудита, состояние системы, историю обслуживания и получателей оповещений.

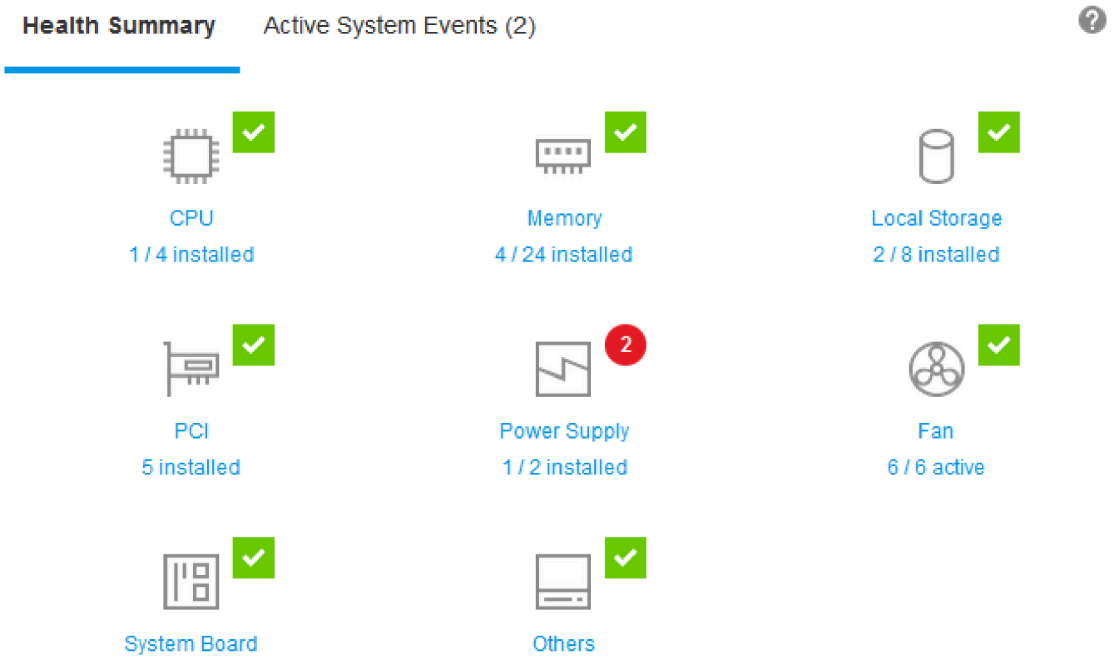
Просмотр сводки состояния/активных системных событий

Информация в этом разделе поможет понять, как просматривать сводку состояния/активные системные события.

При открытии домашней страницы XClarity Controller страница **Сводка состояния** отображается по умолчанию. На графическом представлении показано количество установленных аппаратных компонентов и их соответствующее состояние. Отслеживаются следующие аппаратные компоненты:

- Процессор (ЦП)
- Память
- Локальное хранилище
- Адаптеры PCI
- Блок питания
- Вентилятор
- Материнская плата
- Другие компоненты

Примечание: В системах с конфигурацией объединительной панели с обычной заменой **локальное хранилище** может отображаться как недоступное на значке состояния.



Если какой-либо из аппаратных компонентов не функционирует нормально, он будет помечен значком критической ошибки или предупреждения. Критическое состояние обозначается значком в виде красного круга, а предупреждение — желтым треугольником. Наводя указатель мыши на такой значок, можно просмотреть до трех активных в настоящее время событий для этого компонента.

Для просмотра других событий перейдите на вкладку **Активные системные события**. Отобразится окно с событиями, которые в настоящее время активны в системе. Щелкните **Просмотреть все журналы событий** для просмотра всего журнала событий.

Если аппаратный компонент помечен зеленым флажком, он функционирует нормально, активные события отсутствуют.

Текст под аппаратным компонентом указывает на количество установленных компонентов. Если щелкнуть текст, вы будете перенаправлены на страницу **Инвентаризация**.

Просмотр сведений о системе

В этом разделе рассказывается, как получить сводку стандартной информации о сервере.

На панели **Сведения о системе и системные параметры**, расположенной в левой части домашней страницы, представлена сводка общей информации о сервере, которая включает следующие сведения:

- Имя компьютера, состояние питания и операционной системы
- Тип/модель компьютера
- Серийный номер
- Название системы
- Владелец переднего USB-разъема
- Лицензия BMC
- IP-адрес BMC
- Имя хоста BMC
- Версия UEFI
- Версия BMC
- Версия LXPM
- Расположение

Сервер может находиться в одном из системных состояний, перечисленных в следующей таблице.

Табл. 5. Описания системных состояний

Таблица из двух столбцов с заголовками, описывающая системные состояния сервера.

Состояние	**Описание**
Питание системы выключено/Состояние неизвестно	Сервер выключен.
Система включена/запуск UEFI	Сервер включен, однако UEFI не работает.
Система работает в режиме UEFI.	Сервер включен, и UEFI работает.
Система остановлена в интерфейсе UEFI	Сервер включен; UEFI обнаружил проблему и прекратил работу.
Загрузка операционной системы или загрузка в неподдерживаемой операционной системе	Сервер может находиться в этом состоянии по одной из следующих причин: • Загрузчик операционной системы запущен; однако операционная система не работает • Интерфейс BMC Ethernet через USB отключен. • В операционной системе отсутствуют драйверы, поддерживающие интерфейс Ethernet через USB.
Операционная система загружена	Серверная операционная система работает.
Приостановка в ОЗУ	Сервер переведен в режим ожидания или спящий режим.
Система работает в режиме теста памяти	Сервер включен, запущены средства диагностики памяти.
Система работает в режиме настройки	Сервер включен, система загружена в меню настройки UEFI F1 или LXPM.
Система работает в режиме обслуживания LXPM.	Сервер включен, система загружена в режим обслуживания LXPM, в котором пользователи не могут осуществлять переход по меню LXPM.

Если требуется изменить название системы, щелкните значок с карандашом. Введите название системы, которое требуется использовать; затем нажмите зеленый флажок.

Если требуется изменить владельца переднего разъема USB, щелкните значок карандаша и выберите нужный режим **Владение передним разъемом USB** из раскрывающегося списка. Затем щелкните зеленый флажок.

Если у вашего сервера имеется какая-либо лицензия, отличная от XClarity Controller Enterprise, вы, возможно, сможете обновить ее, чтобы включить расширенные функции. Чтобы установить обновленную лицензию после приобретения щелкните значок со стрелкой, указывающей вверх.

Чтобы добавить, удалить или экспортировать лицензию, щелкните стрелку, указывающую вправо.

Чтобы изменить соответствующие параметры IP-адреса BMC, имени хоста BMC, версии UEFI, версии BMC и элементов местоположения, щелкните стрелку, указывающую вправо.

- В разделе **Network** вы будете направлены в раздел **Конфигурация Ethernet** для ввода IP-адреса и имени хоста.
- Для указания версий UEFI и BMC вы будете направлены на страницу **Обновление микропрограммы**.
- Для указания местоположения вы будете направлены в раздел **Свойства сервера** на странице **Конфигурация сервера**.

Просмотр сведений об использовании системы

При нажатии на левой панели кнопки **Использование** отображается сводка с общей информацией об использовании сервера.

Использование системы — это составной показатель, основанный на использовании процессора, памяти и подсистем ввода-вывода в режиме реального времени. Все данные об использовании ресурсов поступают со стороны ME (диспетчера узлов) и содержат следующую информацию.

- **Использование ЦП**
  - Совокупное время пребывание в C-состоянии
  - Измеренное время пребывания в состоянии C0 в процентах от используемого и максимальное время пребывание в состоянии C0 (в секунду).
- **Использование памяти**
  - Совокупный объем операций чтения-записи во всех каналах памяти.

  - Измеренная пропускная способность в процентах от используемой и максимально доступная пропускная способность памяти (в секунду).
- **Использование ресурсов ввода-вывода**
  - Совокупный объем операций чтения-записи в корневых портах шины PCIe*.
  - Измеренная пропускная способность в процентах от используемой и максимально доступная пропускная способность ввода-вывода (в секунду).

Просмотр журналов событий

Журнал событий представляет собой список всех аппаратных событий и событий управления за прошлые периоды.

Перейдите на вкладку **Журнал событий** в разделе **События**, чтобы отобразить страницу **Журнал событий**. Все события в этом журнале имеют отметку времени (добавляемую с помощью параметров даты и времени XClarity Controller). Некоторые события также создают оповещения, если соответствующий параметр настроен в разделе **Получатели оповещений**. События в журнале событий можно сортировать и фильтровать.

Ниже приводится описание действий, которые могут выполняться на странице **Журнал событий**.

- **Настроить таблицу**: выберите это действие, чтобы указать тип отображаемой в таблице информации. Может отображаться порядковый номер, помогающий определить последовательность событий при наличии нескольких событий с одинаковой отметкой времени.

  Примечание: Некоторые порядковые номера используются во внутренних процессах BMC, поэтому наличие пробелов в последовательностях номеров при сортировке событий по порядковому номеру — это нормально.
- **Очистить журналы**: выберите это действие, чтобы удалить журналы событий.
- **Обновить**: выберите это действие, чтобы обновить представление и отобразить любые записи журнала событий, которые, возможно, имели место с момента последнего отображения страницы.
- **Тип**: выберите, события каких типов следует показывать. Доступны следующие типы событий:

   показывает записи ошибок в журнале

   показывает записи предупреждений в журнале

   показывает информационные записи в журнале

  Щелкните каждый значок, чтобы выключить или включить типы ошибок для отображения. Последовательное нажатие на значок позволяет переключаться между режимом отображения и сокрытия событий. Синяя рамка вокруг значка указывает на то, что соответствующий тип события будет показан.
- **Фильтр по типу источника**: выберите этот элемент из раскрывающегося меню, чтобы отобразить только записи журнала событий выбранного вами типа.
- **Фильтр времени**: выберите этот элемент действий, чтобы указать интервал событий для отображения.

- **Поиск**: чтобы выполнить поиск по конкретным типам событий или ключевым словам, щелкните значок лупы и введите слово для поиска в поле **Поиск**. Обратите внимание, что данные вводятся с учетом регистра.

Примечание: Максимальное число записей в журнале событий — 1024. Если журнал событий полон, новая запись автоматически перезапишет самую старую.

Просмотр журналов аудита

Журнал аудита содержит записи о действиях пользователей за прошлые периоды, например о входе в систему на контроллере XClarity Controller, создании нового пользователя и изменении пароля пользователя.

Журнал аудита можно использовать для отслеживания и документирования аутентификации, изменений и системных действий.

В журнале событий и журнале аудита доступны схожие действия по обслуживанию системы и просмотру информации. Описание действий, которые можно выполнить на странице «Журнал аудита» для отображения или фильтрации определенных сведений, см. в разделе «Просмотр журналов событий» на странице 57.

Примечания:

- После запуска инструментов Lenovo в серверной операционной системе журнал аудита может содержать записи о действиях, выполненных пользователем (например, «20luN4SB»), имя которого вы вряд ли узнаете. Если какие-либо инструменты выполняются в серверной операционной системе, они могут создавать временную учетную запись пользователя для доступа к XClarity Controller. Учетная запись создается с произвольным именем пользователя и паролем; ее можно использовать только для доступа к XClarity Controller во внутреннем интерфейсе Ethernet через USB. Эту учетную запись можно использовать только для доступа к интерфейсам CIM-XML и SFTP XClarity Controller. Создание и удаление этой временной учетной записи фиксируется в журнале аудита, равно как и любые действия, выполняемые инструментом с этими учетными данными.
- Максимальное число записей в журнале аудита — 1024. Если журнал аудита полон, новая запись автоматически перезапишет самую старую.

Просмотр истории обслуживания

На странице **История обслуживания** приводится информация об истории обновлений микропрограмм, конфигурации и замены оборудования.

Содержимое истории обслуживания можно фильтровать, чтобы отобразить определенные типы событий или определенные интервалы времени.

Примечание: Максимальное число записей в журнале обслуживания — 250. Если журнал обслуживания полон, новая запись автоматически перезапишет самую старую.

Настройка получателей оповещений

Чтобы добавить или изменить уведомления по электронной почте или в системном журнале и получателей ловушек SNMP, следуйте рекомендациям из этого раздела.

Ниже приводится описание действий, которые могут выполняться на вкладке **Получатели оповещений**.

Следующие действия можно выполнить в разделе получателей **Электронная почта/системный журнал**.

- **Создать**: выберите это действие, чтобы создать дополнительных новых получателей электронной почты и системного журнала. Можно настроить до 12 получателей электронной почты и системного журнала.
  - **Создать получателя электронной почты**: выберите этот элемент действия для создания получателя электронной почты.
    - Введите имя и адрес электронной почты получателя.
    - Включите или выключите уведомление о событиях. Если вы решили выключить этот параметр, учетная запись останется настроенной, однако электронные сообщения отправляться не будут.
    - Выберите типы событий, о которых получатель будет получать уведомления. Если щелкнуть раскрывающийся список рядом с метками категорий «Критическое», «Внимание!» или «Системное», можно выбрать уведомления по конкретным компонентам в категории и отменить выбор.
    - Можно указать, следует ли включить содержимое журнала событий в электронное оповещение.
    - Индекс указывает, какое из 12 гнезд получателей будет назначено.
    - Здесь можно настроить сервер электронной почты, на который будут перенаправляться события. Кроме того, для этого можно щелкнуть действие «Сервер SMTP» вверху раздела. См. подробные сведения о настройке в разделе «Сервер SMTP».
  - **Создать получателя системного журнала**: выберите этот элемент действия для создания получателей системного журнала.
    - Введите имя и IP-адрес или имя хоста сервера системного журнала.
    - Включите или выключите уведомление о событиях. Если вы решили выключить этот параметр, учетная запись останется настроенной, однако электронные сообщения отправляться не будут.
    - Индекс указывает, какое из 12 гнезд получателей будет назначено.
    - Выберите типы событий, которые будут отправляться на сервер системного журнала. Если щелкнуть раскрывающееся меню рядом с метками категорий «Критическое», «Внимание!» или «Системное», можно выбрать уведомления по конкретным компонентам в категории и отменить выбор.
- **Сервер SMTP**: выберите этот элемент действия для настройки соответствующих параметров сервера электронной почты SMTP. Можно настроить только один сервер электронной почты. Одна и та же конфигурация электронной почты используется при отправке оповещений всем настроенным получателям электронной почты. BMC автоматически переключается с безопасного соединения на шифрованное соединение для передачи почты с помощью команды STARTTLS равномерно через порт 587, если целевой почтовый сервер поддерживает эту операцию.
  - Введите имя хоста или IP-адрес и номер сетевого порта сервера электронной почты.
  - Если сервер электронной почты требует аутентификации, установите флажок **Требовать аутентификации** и введите имя пользователя и пароль. Выберите тип аутентификации, требуемый сервером электронной почты: метод «вызов-ответ» (**CRAM-MD5**) или простые учетные данные (**LOGIN**).
  - Некоторые сети могут блокировать исходящие сообщения электронной почты, если значение обратного пути не соответствует ожидаемому. По умолчанию XClarity Controller будет использовать alertmgr@domain, где domain — это доменное имя, заданное в разделе DDNS сетевой веб-страницы XClarity Controller. Вместо значений по умолчанию можно указать собственные сведения об отправителе.

  - Можно протестировать подключение к серверу электронной почты, чтобы убедиться, что параметры электронной почты настроены правильно. В XClarity Controller отобразится сообщение о том, успешно ли установлено подключение.
- **Повторить попытку или отложить**: выберите этот вариант, чтобы настроить соответствующие параметры для повторной попытки или отсрочки.
  - Лимит повторных попыток указывает, сколько раз XClarity Controller будет пытаться отправить оповещение, если первоначальная попытка не была успешной.
  - Задержка между записями показывает, сколько XClarity Controller будет ждать после отправки оповещения одному получателю перед отправкой оповещения следующему получателю.
  - Задержка между попытками показывает, сколько XClarity Controller будет ждать после неудачной попытки, прежде чем повторить попытку отправить оповещение.
- **Протокол**: выберите этот элемент действия, чтобы настроить соответствующие параметры для протокола подключения.
  - Можно выбрать **Протокол TCP** или **Протокол UDP**. Обратите внимание, что этот параметр применяется ко всем получателям системного журнала.
- Если получатели электронных сообщений и системного журнала созданы, они будут перечислены в этом разделе.
  - Чтобы изменить настройки получателя электронных сообщений или системного журнала, щелкните значок с изображением карандаша под заголовком действия в строке рядом с получателем, которого требуется настроить.
  - Чтобы удалить получателя электронных сообщений или системного журнала, щелкните значок с изображением мусорной корзины.
  - Чтобы отправить тестовое оповещение получателю электронных сообщений или системного журнала, щелкните значок с изображением бумажного самолета.

В разделе пользователя **SNMPv3** можно выполнить следующие действия.

- **Создать**: выберите это действие для создания получателей ловушки SNMPv3.
  - Выберите учетную запись пользователя, которую требуется связать с ловушками SNMPv3. Это должна быть одна из двенадцати локальных учетных записей пользователя.
  - Укажите имя хоста или IP-адрес диспетчера SNMPv3, который будет получать ловушки SNMPv3.
  - В XClarity Controller для аутентификации с диспетчере SNMPv3 используется хэш-алгоритм HMAC-SHA. Это единственный поддерживаемый алгоритм.
  - Пароль конфиденциальности используется с протоколом конфиденциальности для шифрования данных SNMP.
  - **Глобальная настройка SNMPv3** применяется ко всем получателям ловушек SNMPv3. Эти параметры можно настроить при создании получателя ловушек SNMPv3 или нажав действие «Параметры SNMPv3» вверху сегмента пользователей **SNMPv3**.
    - Выберите, чтобы включить или выключить ловушки SNMPv3. Если выключено, эти параметры будут настроены, однако ловушки SNMPv3 отправляться не будут.
    - Сведения о контактном лице и расположении BMC являются обязательными, они настраиваются на веб-странице «Свойства сервера». Дополнительные сведения см. в разделе «Настройка местоположения и контактов» на странице 85.
    - Выберите типы событий, которые будут отправлять ловушки диспетчеру SNMPv3. Если щелкнуть раскрывающееся меню рядом с метками категорий «Критическое», «Внимание!» или «Системное», можно выбрать уведомления по конкретным компонентам в категории и отменить выбор.

Примечание: Перенос данных между клиентом SNMP и агентом можно защитить с помощью шифрования. Для **протокола конфиденциальности** поддерживаются методы CBC-DES и AES.

- Если получатели ловушек SNMPv3 созданы, они будут перечислены в этом разделе.
  - Чтобы изменить настройки получателя SNMPv3, щелкните значок с изображением карандаша под заголовком действия в строке рядом с получателем, которого требуется настроить.
  - Чтобы удалить получателя SNMPv3, щелкните значок с изображением мусорной корзины.

Фиксация данных экрана при последнем сбое ОС

Воспользуйтесь информацией из этого раздела для фиксации и просмотра экрана сбоя ОС.

Экран ОС фиксируется автоматически в случае тайм-аута Watchdog ОС. Если происходит событие, из-за которого ОС перестает выполняться, активируется функция Watchdog ОС и фиксируется содержимое экрана. XClarity Controller хранит только один захват экрана. В случае тайм-аута Watchdog ОС новый захват экрана перезаписывает предыдущий захват экрана. Для захвата экрана сбоя ОС необходимо включить функцию Watchdog ОС. Чтобы настроить время Watchdog ОС, воспользуйтесь дополнительной информацией в разделе «Настройка тайм-аутов сервера» на странице 85. Функция захвата экрана сбоя ОС доступна только в XClarity Controller с уровнем функциональности Advanced или Enterprise. См. сведения об уровне функциональности контроллера XClarity Controller, установленного на вашем сервере, в документации к вашему серверу.

Щелкните действие **Экран последнего сбоя** в разделе **Удаленная консоль** на домашней странице XClarity Controller, чтобы просмотреть изображение экрана ОС, зафиксированное в момент тайм-аута Watchdog ОС. Для просмотра захвата можно также щелкнуть **Обслуживание**, затем **Экран последнего сбоя** в разделе **Быстрые действия** на домашней странице. Если тайм-аут Watchdog ОС в системе не происходил, однако система зафиксировала экран ОС, отображается сообщение о том. что экран сбоя создан не был.

Глава 5. Настройка сервера

Воспользуйтесь информацией из этой главы, чтобы понять доступные параметры конфигурации сервера.

При настройке сервера доступны следующие параметры:

- Адаптеры
- Параметры загрузки
- Политика питания
- Свойства сервера

Просмотр сведений об адаптере и параметров конфигурации

Воспользуйтесь информацией в этом разделе для просмотра сведений об установленных на сервере адаптерах.

Щелкните **Адаптеры** в разделе **Конфигурация сервера**, чтобы просмотреть сведения об установленных на сервере адаптерах.

Примечания:

- Если адаптер не поддерживает мониторинг состояния, он не будет отображаться для мониторинга или конфигурации. Инвентарные сведения обо всех установленных адаптерах PCI доступны на странице **Ресурсы**.

Настройка режима и порядка загрузки системы

Воспользуйтесь информацией из этого раздела, чтобы настроить режим и порядок загрузки системы.

Выбрав **Параметры загрузки** в разделе **Конфигурация сервера**, можно настроить режим и порядок загрузки системы.

Примечание: Для изменения системных параметров, связанных с безопасностью, нельзя использовать внутриполосный способ без аутентификации. Например, НЕ ДОПУСКАЕТСЯ возможность настройки в режиме безопасной загрузки через внутриполосные API без аутентификации через ОС или оболочку UEFI. Это включает внутриполосное выполнение функции OneCLI и получение ей временных учетных данных с помощью IPMI, а также настройку параметров, связанных с безопасной загрузкой, TPM или паролем настройки UEFI через какие-либо инструменты или API. Для доступа к любым параметрам, связанным с безопасностью, должна требоваться соответствующая аутентификация с достаточным уровнем привилегий.

Доступно два режима загрузки системы:

Загрузка UEFI
Выберите этот вариант, чтобы настроить сервер, поддерживающий Unified Extensible Firmware Interface (UEFI). Если выполняется загрузка ОС с поддержкой UEFI, выбор этого параметра может ускорить загрузку благодаря отключению устаревших ОЗУ.

Устаревшая загрузка
Выберите этот вариант, если сервер настраивается для загрузки ОС, требующей устаревшую микропрограмму (BIOS). Выберите этот вариант только в том случае, если выполняется загрузка ОС без поддержки UEFI.

Чтобы настроить порядок загрузки системы, выберите устройство из списка **Доступные устройства** и щелкните стрелку вправо, чтобы добавить устройство в порядок загрузки. Чтобы удалить устройство из порядка загрузки, выберите устройство из списка порядка загрузки и щелкните стрелку влево, чтобы переместить устройство обратно в список доступных устройств. Чтобы изменить порядок загрузки, выберите устройство и с помощью стрелок «вверх» и «вниз» переместите устройство вверх или вниз в соответствии с приоритетом.

При внесении изменений в порядок загрузки перед применением изменения необходимо выбрать параметр перезапуска. Доступны следующие параметры:

- **Перезапустить сервер немедленно**: изменения порядка загрузки сохраняются, и сервер перезапускается немедленно, при этом операционная система не завершает работу.
- **Перезапустить сервер в нормальном режиме**: изменения порядка загрузки сохраняются, и перед перезапуском сервера операционная система завершает работу.
- **Перезапустить позже вручную**: изменения порядка загрузки сохраняются, но не вступают в силу до следующей перезагрузки сервера.

Настройка однократной загрузки

Чтобы временно проигнорировать настроенную загрузку и однократно выполнить загрузку на определенное устройство, воспользуйтесь информацией из этого раздела.

Щелкните **Параметры загрузки** в разделе **Конфигурация сервера** и выберите устройство из раскрывающегося меню, чтобы настроить устройство, на которое будет выполнена однократная загрузка системы при следующем перезапуске сервера. Доступны следующие варианты:

Сеть PXE
Настраивает сервер так, чтобы он пытался выполнить загрузку в сети PXE.

Основной съемный носитель
Сервер загружается с USB-устройства по умолчанию.

CD/DVD по умолчанию
Сервер загружается с CD/DVD-диска по умолчанию.

Настройка системы F1
Сервер загружается в диспетчер Lenovo XClarity Provisioning Manager.

Диагностический раздел
Сервер загружается в диагностический раздел диспетчера Lenovo XClarity Provisioning Manager.

Жесткий диск по умолчанию
Сервер загружается с дискового накопителя по умолчанию.

Основной удаленный носитель
Сервер загружается с подключенного виртуального носителя.

Без однократной загрузки
Используется настроенный порядок загрузки. Однократная загрузка не переопределяет настроенный порядок загрузки.

Если вы меняете тип загрузки и указываете, что она должна однократно выполняться с загрузочного устройства, можно также указать, следует ли выполнить устаревшую загрузку или загрузку UEFI. Установите флажок **Предпочитать устаревшую загрузку**, если требуется выполнять устаревшую загрузку BIOS. Снимите флажок, если требуется выполнить загрузку UEFI. Если выбирается однократное изменение порядка загрузки, перед применением изменения необходимо выбрать параметр перезапуска.

- **Перезапустить сервер немедленно**: изменение порядка загрузки сохраняется, и сервер перезапускается немедленно, при этом операционная система не завершает работу.
- **Перезапустить сервер в нормальном режиме**: изменение порядка загрузки сохраняется, и перед перезапуском сервера операционная система завершает работу.
- **Перезапустить позже вручную**: изменение порядка загрузки сохраняется, но не вступает в силу до следующей перезагрузки сервера.

Управление питанием сервера

Воспользуйтесь информацией из этого раздела, чтобы просмотреть сведения об управлении питанием и выполнить функции по управлению питанием.

Выберите **Power Policy** в разделе **Конфигурация сервера** для просмотра информации об управлении электропитанием и выполнения функций управления электропитанием.

Примечание: В раме, содержащей узлы блейд-серверов или серверов высокой плотности, охлаждение и питание рамы контролируется контроллером управления рамой, а не XClarity Controller.

Настройка резервирования питания

Воспользуйтесь информацией из этого раздела, чтобы настроить резервирование питания.

Доступные поля в разделе «Резервирование питания» включают следующее:

- **Избыточный (N+N)**: в этом режиме сервер продолжает функционировать даже при потере одного блока питания.
  - **Режим нулевого вывода**: если этот режим включен в конфигурации с резервированием, некоторые блоки питания будут автоматически переходить в режим ожидания при малой нагрузке. При этом оставшийся блок питания берет на себя полную электрическую нагрузку для повышения эффективности.
- **Избыточный (N+1)**: в этом режиме сервер продолжает функционировать даже при потере одного блока питания, если установлено четыре блока питания.
- **Неизбыточный режим**: в этом режиме не гарантируется, что сервер продолжит работать при потере питания. Сервер попытается применить регулирование, если блок питания не сможет продолжить работу.

Внеся изменения в конфигурацию, нажмите кнопку **Применить**.

Настройка политики ограничения мощности

Воспользуйтесь информацией из этого раздела, чтобы настроить политику ограничения мощности.

Можно включить или выключить функцию ограничения мощности. Если ограничение мощности включено, можно ограничить используемый сервером объем мощности. Если ограничение мощности выключено, максимальный объем мощности, используемый сервером, определяется политикой резервирования питания. Чтобы изменить эту настройку, сначала щелкните **Сброс**. Выберите предпочтительную настройку и нажмите **Применить**.

Ограничение мощности можно включить, используя измерения потребления питания от сети переменного или постоянного тока. В раскрывающемся меню выберите тип измерений, которые будут использоваться, чтобы определить лимит ограничения мощности. При переключении между переменным и постоянным током число на ползунке изменится соответственно.

Существует два способа изменить значение ограничения питания:

- **Способ 1**: переместите отметку на ползунке на нужное значение мощности, чтобы установить общий лимит мощности питания сервера.
- **Способ 2**: введите значение в поле ввода. Отметка на ползунке автоматически переместится в нужное положение.

Внеся изменения в конфигурацию, нажмите кнопку **Применить**.

Примечание: Параметр **Политики электропитания** недоступен, если XClarity Controller установлен в раму, которая содержит узлы блейд-серверов или серверов высокой плотности. Политика электропитания контролируется контроллером управления рамой, а не XClarity Controller.

Настройка политики восстановления питания

Чтобы настроить реакцию сервера на восстановление питания после отключения, воспользуйтесь информацией в этом разделе.

Три следующих параметра доступны для настройки политики восстановления питания:

Всегда выключен
Сервер остается выключен, даже если питание восстановлено.

Восстановить
Сервер будет автоматически включен после восстановления питания, если сервер был включен в момент сбоя в системе питания. В противном случае после восстановления питания питание сервера останется выключенным.

Всегда включен
Сервер включится автоматически после восстановления питания.

Внеся изменения в конфигурацию, нажмите кнопку **Применить**.

Примечание: Параметр **Политики восстановления питания** недоступен в раме, которая содержит узлы блейд-серверов или серверов высокой плотности. Политика восстановления питания контролируется контроллером управления рамой, а не XClarity Controller.

Действия кнопки питания

Информация в этом разделе поможет понять, какие связанные с питанием действия можно выполнять на сервере.

Щелкните **Действие кнопки питания** в разделе **Быстрое действие** страницы XClarity Controller.

В следующей таблице приводится описание связанных с питанием и перезапуском действий, которые можно выполнить на сервере.

Табл. 6. Связанные с питанием действия и описания

В следующей таблице из двух столбцов приводятся описания действий, связанных с питанием и перезапуском сервера.

Действие кнопки питания	Описание
Включить питание сервера	Выберите этот элемент действия, чтобы включить сервер и загрузить операционную систему.
Выключить сервер в нормальном режиме	Выберите этот элемент действия, чтобы завершить работу операционной системы и выключить питание сервера.

Табл. 6. Связанные с питанием действия и описания (продолж.)

Действие кнопки питания	**Описание**
Выключить сервер немедленно	Выберите этот элемент действия, чтобы выключить сервер, не завершая сначала работу операционной системы.
Перезапустить сервер в нормальном режиме	Выберите этот элемент действия, чтобы завершить работу операционной системы и выключить, а затем включить питание сервера.
Перезапустить сервер немедленно	Выберите этот элемент действия, чтобы выключить и снова включить сервер немедленно, не завершая сначала работу операционной системы.
Загрузить сервер в раздел настройки системы	Выберите этот элемент, чтобы включить или перезагрузить сервер и автоматически выполнить загрузку в раздел настройки системы без необходимости нажимать клавишу F1 во время загрузки.
Инициировать немаскируемое прерывание (NMI)	Выберите этот элемент действия, чтобы выполнить принудительное немаскируемое прерывание (NMI) зависшей системы. Если вы выберете этот элемент действия, операционная система платформы выполнит дамп памяти, который можно будет использовать для отладки зависшего состояния системы. Автоматическая перезагрузка в настройке NMI в меню настройки системы F1 определяет, будет ли XClarity Controller перезагружать сервер после NMI.
Запланировать действия кнопки питания	Выберите этот элемент действия, чтобы запланировать для сервера ежедневные и еженедельные действия, связанные с питанием и перезапуском.
Перезапустить контроллер управления	Выберите этот элемент действия, чтобы перезапустить XClarity Controller
Выключение и включение питания сервера	Выберите это действие, чтобы выключить и включить питание сервера.
Примечание: Если операционная система находится в заблокированном режиме или режиме экранной заставки, когда предпринимается попытка завершить работу операционной системы, XClarity Controller, возможно, не сможет выполнить нормальное завершение работы. XClarity Controller выполнит жесткий сброс или выключение системы по истечении интервала задержки выключения, в то время как операционная система может продолжать работать.	

Мониторинг потребления питания и управление потреблением питания с помощью команд IPMI

Воспользуйтесь информацией из этого раздела для мониторинга потребления питания и управления потреблением питания с помощью команд IPMI.

В этом разделе описано, как диспетчер Intel Intelligent Power Node Manager и интерфейс Data Center Manageability Interface (DCMI) можно использовать для мониторинга питания и температуры, а также управления электропитанием на основе политик для сервера, используя команды управления электропитанием IPMI.

Для серверов с Intel Node Manager SPS 3.0 пользователи XClarity Controller могут использовать команды управления электропитанием IPMI, предоставляемые модулем Intel Management Engine (ME),

чтобы контролировать функции диспетчера узлов и отслеживать потребление питания сервером. Управление питанием сервера также может осуществляться с помощью команд управления электропитанием DCMI. В этом разделе приводятся примеры команд управления электропитанием диспетчера узлов и DCMI.

Управление питанием сервера с использованием команд Node Manager

Воспользуйтесь информацией из этого раздела для управления питанием сервера с помощью диспетчера узлов.

У микропрограммы диспетчера узлов Intel Node Manager нет внешнего интерфейса; следовательно, команды диспетчера узлов должны быть сначала получены XClarity Controller, а затем отправлены диспетчеру узлов Intel Node Manager. XClarity Controller функционирует как реле и устройство переноса для команд IPMI, используя стандартный мост IPMI.

Примечание: При изменении политик диспетчера узлов с использованием команд IPMI диспетчера узлов могут возникнуть конфликты с функцией управления питанием XClarity Controller. По умолчанию мостовое соединение команд диспетчера узлов Node Manager отключено во избежание конфликтов.

Для пользователей, которые желают управлять питанием сервера с помощью диспетчера узлов, а не XClarity Controller, доступна команда IPMI OEM, состоящая из (сетевая функция: *0x3A*) и (команда: *0xC7*).

Чтобы включить собственный тип команд IPMI диспетчера узлов:`ipmitool -H` *<$XClarity_Controller_IP>* `-U` *<USERID>* `-P` *<PASSW0RD>* `raw` *0x3a 0xc7 0x01*

Чтобы выключить собственный тип команд IPMI диспетчера узлов:`ipmitool -H` *<$XClarity_Controller_IP>* `-U` *<USERID>* `-P` *<PASSW0RD>* `raw` *0x3a 0xc7 0x00*

Ниже представлены примеры команд управления электропитанием диспетчера узлов.

Примечания:

- Указав *канал 0* IPMI и целевой адрес *0x2c*, можно воспользоваться командой IPMITOOL для отправки команд в диспетчер узлов Intel на обработку. Сообщение запроса используется для запуска действия, а сообщение ответа возвращается запрашивающему объекту.
- Из-за пространственных ограничений команды отображаются в следующем формате.

Мониторинг питания с использованием команды «Получить глобальную статистику питания системы» (код команды 0xC8): Запрос:`ipmitool -H` *<$XClarity_Controller_IP>* `-U` *<USERID>* `-P` *<PASSW0RD>* `-b` *0x00* `-t` *0x2c* `raw` *0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00* Ответ:57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Ограничение мощности с использованием команды «Настроить политику диспетчера узлов Intel» (код команды 0xC1): Запрос:`ipmitool -H` *<$XClarity_Controller_IP>* `-U` *<USERID>* `-P` *<PASSW0RD>* `-b` *0x00* `-t` *0x2c* `raw` *0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00*Ответ:57 01 00

Энергосбережение с использованием команды «Настроить политику диспетчера узлов Intel» (код команды 0xC1): Запрос:`ipmitool -H` *<$XClarity_Controller_IP>* `-U` *<USERID>* `-P` *<PASSW0RD>* `-b` *0x00* `-t` *0x2c* `raw` *0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00*

Функция «Получить ИД устройства» с использованием команды «Получить ИД устройства модуля управления Intel»:Запрос:`ipmitool -H` *<$XClarity_Controller_IP>* `-U` *<USERID>* `-P` *<PASSW0RD>* `-b` *0x00* `-t` *0x2c* `raw` *0x06 0x01*Ответ:50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

Дополнительные команды диспетчера узлов Intel доступны в последнем выпуске статьи *Спецификация внешнего интерфейса диспетчера узлов системы интеллектуального питания Intel с использованием команд IPMI* по адресу https://businessportal.intel.com.

Управление питанием сервера с использованием команд DCMI

Воспользуйтесь информацией из этого раздела для управления питанием сервера с помощью команд DCMI.

DCMI предоставляет функции мониторинга и контроля, которые могут предоставляться через стандартные интерфейсы ПО управления. Функции управления питанием сервера также могут реализовываться с помощью команд DCMI.

Ниже представлены примеры наиболее распространенных функций и команд управления питанием DCMI. Сообщение запроса используется для запуска действия, а сообщение ответа возвращается запрашивающему объекту.

Примечание: Из-за пространственных ограничений команды отображаются в следующих форматах.

Получить показатель мощности: Запрос:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x2c 0x02 0xdc 0x01 0x00 0x00` Ответ:`dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40`

Настроить лимит мощности: Запрос:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P PASSW0RD raw 0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03` Ответ:`dc`

Получить ограничение мощности: Запрос:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x2c 0x03 0xdc 0x00 0x00` Ответ:`dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00`

Активировать лимит мощности: Запрос:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x2c 0x05 0xdc 0x01 0x00 0x00` Ответ:`dc`

Деактивировать лимит мощности: Запрос:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSW0RD> raw 0x2c 0x05 0xdc 0x00 0x00 0x00` Ответ:`dc`

Примечание: На некоторых серверах действия исключений для команды **Настроить лимит мощности** могут не поддерживаться. Так, может не поддерживаться параметр *Жесткое выключение системы и внесение событий в журнал SEL*.

Полный список команд, поддерживаемых спецификацией DCMI, см. в последнем выпуске статьи *Спецификация интерфейса управляемости ЦОД* раздела https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf.

Функции удаленной консоли

Информация в этом разделе поможет понять, как удаленно просматривать консоль сервера и взаимодействовать с ней.

В веб-интерфейсе XClarity Controller можно пользоваться функциональностью удаленной консоли для просмотра серверной консоли и взаимодействия с ней. Можно назначить образ диска (файл ISO или IMG) в качестве виртуальных дисков на сервере. Функциональность удаленной консоли доступна в выпусках XClarity Controller Advanced и Enterprise и только в веб-интерфейсе. Для использования функций удаленной консоли необходимо выполнить вход в XClarity Controller с ИД пользователя, имеющего права доступа Supervisor или привилегии на доступ к удаленной консоли. Дополнительные сведения об обновлении выпуска XClarity Controller Standard до XClarity Controller Advanced или XClarity Controller Enterprise см. в разделе «Обновление XClarity Controller» на странице 6.

Используйте функции удаленной консоли для решения следующих задач:

- Удаленный просмотр видео с графическим разрешением до 1280 x 1024 при частоте обновления 72 Гц или 75 Гц независимо от состояния сервера.
- Удаленный доступ к серверу с использованием клавиатуры и мыши удаленного клиента.
- Монтаж файлов ISO и IMG, размещенных в локальной или удаленной системе в качестве виртуальных дисков, доступных для использования сервером.
- Отправьте образ IMG или ISO в память XClarity Controller и установите его на сервере в качестве виртуальных дисков. В память контроллера XClarity Controller можно загрузить до двух файлов с максимальным совокупным размером 50 МБ.

Примечания:

- Если функция удаленной консоли запускается в многопользовательском режиме (XClarity Controller с набором компонентов XClarity Controller Enterprise поддерживает до шести одновременных сеансов), то функция удаленного диска не может использоваться в нескольких сеансах одновременно.
- Удаленная консоль может отображать только видео, создаваемые видеоконтроллером на материнской плате. Если установлен и используется вместо видеоконтроллера системы отдельный адаптер видеоконтроллера, на удаленной консоли XClarity Controller не может отображаться видеосодержимое с добавленного адаптера.
- Если в сети используются брандмауэры, сетевой порт должен быть открыт, чтобы обеспечить поддержку функции удаленной консоли. Для просмотра или изменения номера сетевого порта, используемого функцией удаленной консоли, выполните инструкции из раздела «Включение обслуживания и назначение портов» на странице 36.
- Функция удаленной консоли использует HTML5 для отображения видео с сервера на веб-страницах. Чтобы использовать эту функцию, ваш браузер должен поддерживать отображение видеосодержимого с использованием элементов HTML5.
- Если для доступа к BMC в браузере Internet Explorer используются самозаверяющие сертификаты и адрес IPv6, сеанс удаленной консоли может не запуститься из-за ошибки сертификата. Во избежание этой проблемы можно добавить самозаверяющий сертификат в Центры сертификации доверенных корневых сертификатов Internet Explorer:
  - Выберите **Security** в разделе **BMC Configuration** и загрузите самозаверяющий сертификат.
  - Измените расширение файла сертификата на *.crt и дважды щелкните файл интернет-сертификата.
  - Очистите кэш браузера IE11.
  - Щелкните **Установить сертификат**, чтобы установить сертификат в Хранилище сертификатов, выполнив шаги в мастере импорта сертификатов.

Включение функции удаленной консоли

В этом разделе приводятся сведения о функции удаленной консоли.

Как упоминалось ранее, функциональность удаленной консоли XClarity Controller доступна только в выпусках XClarity Controller Advanced и XClarity Controller Enterprise. Если у вас нет привилегий для работы с удаленной консолью, отобразится значок замка.

Если вы приобрели и получили ключ активации для обновления XClarity Controller Advanced, установите его, выполнив инструкции из раздела «Установка ключа активации» на странице 95.

Для использования функциональности удаленной консоли выполните следующие действия:

1. Щелкните изображение с белой указывающей по диагонали стрелой в разделе «Удаленная консоль» домашней страницы XClarity Controller или на веб-странице удаленной консоли.
2. Выберите один из следующих режимов:
   - Запускать удаленную консоль в однопользовательском режиме
   - Запускать удаленную консоль в многопользовательском режиме

   Примечание: XClarity Controller с набором функций XClarity Controller Enterprise в многопользовательском режиме поддерживает до шести одновременных видеосеансов.
3. Выберите, нужно ли разрешить другим отправлять запросы на отправку запроса о разрыве соединения пользователю удаленной консоли, если кому-то необходимо воспользоваться функцией удаленной консоли, которая уже используется в однопользовательском режиме, или если максимальное число пользователей использует функциональность удаленной консоли в многопользовательском режиме. Параметр **Временной интервал отсутствия ответа** указывает, сколько XClarity Controller будет ждать, прежде чем автоматически отключит пользователя, если ответ на запрос о разрыве соединения не получен.
4. Выберите, следует ли разрешать видеозапись трех последних загрузок сервера.
5. Выберите, следует ли разрешать видеозапись трех последних сбоев сервера.
6. Выберите, следует ли разрешить снимок экрана сбоя ОС с ошибкой HW.
7. Щелкните **Запустить удаленную консоль**, чтобы открыть страницу удаленной консоли на другой вкладке. Если все доступные сеансы удаленной консоли используются, отобразится диалоговое окно. В этом диалоговом окне пользователь может отправить запрос на разрыв соединения пользователю удаленной консоли, включившему для этой настройки значение **Разрешить другим запрашивать разъединение моего удаленного сеанса**. Пользователь может принять или отклонить запрос на разрыв соединения. Если пользователь не ответит в течение интервала, заданного в настройке **Временной интервал отсутствия ответа**, сеанс пользователя будет автоматически завершен XClarity Controller.

Удаленное управление питанием

В этом разделе описана отправка команд включения и перезапуска сервера из окна удаленной консоли.

Можно отправлять команды включения и перезапуска сервера из окна удаленной консоли, не возвращаясь на главную веб-страницу. Чтобы контролировать питание сервера с помощью удаленной консоли, щелкните **Power** и выберите одну из следующих команд:

Включить питание сервера
Выберите этот элемент действия, чтобы включить сервер и загрузить операционную систему.

Выключить сервер в нормальном режиме
Выберите этот элемент действия, чтобы завершить работу операционной системы и выключить питание сервера.

Выключить сервер немедленно
Выберите этот элемент действия, чтобы выключить сервер, не завершая сначала работу операционной системы.

Перезапустить сервер в нормальном режиме
Выберите этот элемент действия, чтобы завершить работу операционной системы и выключить, а затем включить питание сервера.

Перезапустить сервер немедленно
Выберите этот элемент действия, чтобы выключить и снова включить сервер немедленно, не завершая сначала работу операционной системы.

Загрузить сервер в раздел настройки системы

Выберите этот элемент, чтобы включить или перезагрузить сервер и автоматически выполнить загрузку в раздел настройки системы без необходимости нажимать клавишу F1 во время загрузки.

Захват экрана удаленной консоли

Воспользуйтесь информацией из этого раздела, чтобы понять, как пользоваться функцией захвата экрана удаленной консоли.

Функция захвата экрана в окне удаленной консоли фиксирует содержимое видеоизображения сервера. Чтобы захватить и сохранить изображение экрана, выполните следующие действия:

Шаг 1. В окне удаленной консоли нажмите **Захват экрана**.

Шаг 2. Во всплывающем окне щелкните **Сохранить файл** и нажмите кнопку **OK**. Файл будет назван rpviewer.png и сохранен в папку «Загрузки» по умолчанию.

Примечание: Изображение захвата экрана сохраняется в виде файла PNG.

Поддержка клавиатуры удаленной консоли

В окне удаленной консоли под заголовком **Клавиатура** доступны следующие параметры:

- Щелкните **Виртуальная клавиатура**, чтобы запустить виртуальную клавиатуру. Эта функция очень полезна, если вы пользуетесь планшетным устройством без физической клавиатуры. Следующие параметры можно использовать для создания комбинаций макросов и клавиш для отправки на сервер. Операционная система в используемой вами клиентской системе может заключать определенные комбинации клавиш (например, Ctrl+Alt+Del) в ловушку, вместо того чтобы передавать их на сервер. Другие клавиши, например F1 или Esc, могут перехватываться используемой программой или браузером. Макрос предоставляет механизм отправки на сервер нажатий клавиш, которые пользователю, возможно, отправить не удастся.
- Щелкните **Серверный макрос**, чтобы использовать макрос, определенный сервером. Некоторые серверные макросы предопределены в микропрограмме XClarity Controller. Другие серверные макросы можно определить с помощью Lenovo XClarity Essentials и загрузить из XClarity Controller. Эти макросы определяются для всех пользователей функции удаленной консоли.
- Щелкните **Настроить**, чтобы добавить или удалить пользовательские макросы. Пользовательские макросы определяются только для текущего пользователя удаленной консоли. Другие пользователи удаленной консоли не видят пользовательские макросы друг друга.
  - Щелкните значок «Добавить макросы» и нажмите нужные последовательности клавиш; затем щелкните **Добавить**, чтобы добавить новый макрос.
  - Чтобы удалить пользовательский макрос, выберите его из списка и щелкните значок корзины.
  - Чтобы отправить пользовательский макрос на сервер, выберите **Пользовательские макросы** и щелкните макрос, который требуется отправить.

Поддержка мыши удаленной консоли

Воспользуйтесь этой информацией, чтобы понять возможности удаленного управления с помощью мыши.

В окне удаленной консоли несколько параметров для управления мышью, включая абсолютный контроль над мышью, относительный контроль над мышью (без ускорения) и контроль над мышью (RHEL, более старые версии Linux).

Абсолютное и относительное управление мышью

Используйте эту информацию для доступа к абсолютным и относительным параметрам управления мышью.

Для доступа к абсолютным и относительным параметрам управления мышью выполните следующие действия:

Шаг 1. В окне удаленной консоли нажмите **Мышь**.

Шаг 2. Щелкните **Параметры мыши** в раскрывающемся меню.

Шаг 3. Выберите один из следующих режимов **Ускорение мыши**:

Абсолютное позиционирование (Windows, более новые версии Linux и Mac OS X)
Клиент отправляет сообщения с указанием расположения мыши на сервер, расположение которого по отношению к исходной области (верхний левый угол) зоны просмотра относительно.

Относительное позиционирование (без ускорения)
Клиент отправляет расположение мыши в качестве смещения относительно предыдущего положения мыши.

Относительное позиционирование (более старые версии Linux)
В этом режиме применяется фактор ускорения, чтобы лучше выравнивать положение мыши в некоторых целевых объектах Linux. Настройки ускорения устанавливаются, чтобы обеспечить максимальную совместимость с более старыми дистрибутивами Linux.

Запись/воспроизведение видеоизображения на экране

Используйте информацию в этом разделе для записи или воспроизведения видеоизображения на экране удаленного присутствия.

Веб-интерфейс XClarity Controller предоставляет схожую с DVR функцию, тем самым обеспечивая поддержку записи и воспроизведения видеоизображений с экрана удаленного присутствия. Эта функция поддерживает запись видео только в сетевую папку. В настоящее время поддерживаются протоколы NFS и CIFS. Ниже приводятся пошаговые инструкции по использованию функции записи и воспроизведения.

1. На веб-странице удаленной консоли нажмите кнопку **Запись экрана**, чтобы открыть окно настроек.
2. В окне настроек, возможно, потребуется указать следующие сведения.
   - Если выбран тип подключения CIFS, укажите параметры **Удаленная папка**, **Имя пользователя** и **Пароль**. Формат именования удаленной папки CIFS: **//<удаленный IP-адрес>/<имя папки>**. Например: //xxx.xxx.xxx.xxx/папка.
   - Если выбран тип подключения NFS, укажите параметр **Удаленная папка**. Формат именования удаленной папки NFS: **<удаленный IP-адрес>:/<имя папки>**. Например: xxx.xxx.xxx.xxx:/папка.
   - При необходимости укажите имя видеофайла. Если имя файла уже указано, отобразится сообщение об ошибке. Чтобы перезаписать существующее имя файла, выберите «Перезаписать имя файла». Если установлен флажок в поле «Авто», имя видеофайла будет сгенерировано автоматически.
   - Параметр «Максимальный размер файла» означает максимальный размер видеофайла, по достижении которого видеозапись остановится автоматически.
   - Параметр «Максимальная длительность записи» означает максимальную длительность видеозаписи, по достижении которой видеозапись остановится автоматически.

3. Нажмите **Начать запись**, чтобы начать видеозапись.
4. Нажмите **Остановить запись**, чтобы остановить видеозапись. Отобразится всплывающее окно с сообщением «Видеозапись завершена» и всей информацией о видеозаписи.
5. Скачайте записанные видео с NFS или CIFS в местную папку. В разделе «Предварительный просмотр удаленной консоли» на домашней странице XClarity Controller щелкните **Записанные видео** и выберите видео для воспроизведения.

Режимы экрана удаленной консоли

Воспользуйтесь информацией из этого раздела, чтобы настроить режимы экрана удаленной консоли.

Чтобы настроить режимы экрана удаленной консоли, щелкните **Режим экрана**.

Доступны следующие параметры меню:

Во весь экран
В этом режиме видео отображается на весь рабочий стол клиента. Если в этом режиме нажать клавишу Esc, вы выйдете из режима полного экрана. Поскольку меню удаленной консоли не отображается в режиме полного экрана, потребуется выйти из режима полного экрана, чтобы воспользоваться функциями меню удаленной консоли, например макросами клавиатуры.

По размеру экрана
Это настройка по умолчанию, действующая при запуске удаленной консоли. Если действует эта настройка, рабочий стол отображается полностью, без полос прокрутки. Сохраняется соотношение между сторонами.

Экран масштабирования
Если включено масштабирование, размер видеоизображения подбирается таким образом, чтобы изображение полностью занимало окно консоли.

Исходный экран
Видеоизображение имеет те же габариты, что и серверная часть. При необходимости отображаются полосы прокрутки, позволяющие просмотреть области видеоизображения, которые не помещаются в окно.

Цветной режим
Корректирует глубину цвета окна удаленной консоли. Существует два варианта цветного режима:

- Цветной: 7-, 9-, 12-, 15- и 23-разрядный
- Оттенки серого: 16, 32, 64 и 128 оттенков

Примечание: Корректировки цветного режима, как правило, вносятся, если ваше подключение к удаленному серверу имеет ограниченную полосу пропускания и вы хотите уменьшить потребность в пропускной способности.

Способы установки носителей

Воспользуйтесь информацией из этого раздела, чтобы понять, как выполнять подключение носителей.

Для подключения файлов ISO и IMG в качестве виртуальных дисков предоставляется три механизма.

- Для добавления виртуальных дисков на сервер из сеанса удаленной консоли можно нажать кнопку **Носители**.
- Непосредственно с веб-страницы удаленной консоли, не открывая сеанс удаленной консоли.

- Отдельный инструмент

Для использования функций виртуальных носителей пользователям требуются привилегии **Доступ к удаленной консоли и удаленному диску**.

Файлы можно подключать в качестве виртуальных носителей из локальной системы или с удаленного сервера. Доступ к ним можно осуществлять по сети или посредством загрузки этих файлов в память XClarity Controller с помощью компонента RDOC. Эти механизмы описаны ниже.

- Локальные носители — это файлы ISO или IMG, которые находятся в системе и используются для доступа к XClarity Controller. Этот механизм доступен только в сеансе удаленной консоли (а не непосредственно с веб-страницы удаленной консоли) и при наличии функций XClarity Controller уровня Enterprise. Для подключения локальных носителей щелкните **Активировать** в разделе **Подключить локальные носители**. Одновременно к серверу может быть подключено до четырех файлов.

  Примечания:

  – При использовании браузера Google Chrome доступен дополнительный параметр подключения **Файлы и папки подключения**, позволяющий перетаскивать файлы и папки.
  – Если выполняется несколько параллельных сеансов удаленной консоли с XClarity Controller, эту функцию можно активировать только для одного из сеансов.
- Файлы, расположенные в удаленной системе, можно также подключать как виртуальные носители. Одновременно в качестве виртуальных дисков можно подключать до четырех файлов. XClarity Controller поддерживает следующие протоколы обмена файлами:
  – **Файловая система CIFS**:
    – Введите URL-адрес расположения файла в удаленной системе.
    – Если требуется, чтобы файл присутствовал на сервере в качестве виртуального носителя, доступного только для чтения, установите этот флажок.
    – Введите учетные данные, необходимые XClarity Controller для осуществления доступа к файлу в удаленной системе.

      Примечание: XClarity Controller не поддерживает использование пробелов в имени пользователя, пароле или URL-адресе. Убедитесь, что настроенные для входа на сервер CIFS учетные данные и URL-адрес не содержат пробела в имени пользователя или пароле.
    – Параметры подключения являются дополнительными и определяются протоколом CIFS.
    – Если удаленный сервер относится к набору серверов, безопасность которых обеспечивается централизованно, введите доменное имя, к которому относится удаленный сервер.
  – **Файловая система NFS**:
    – Введите URL-адрес расположения файла в удаленной системе.
    – Если требуется, чтобы файл присутствовал на сервере в качестве виртуального носителя, доступного только для чтения, установите этот флажок.
    – Параметры подключения являются необязательными и определяются протоколом NFS. Поддерживаются протоколы NFSv3 и NFSv4. Например, чтобы использовать NFSv3, необходимо указать параметр nfsvers=3. Если сервер NFS использует для аутентификации операций NFS конфигурацию безопасности AUTH_SYS, необходимо указать параметр sec=sys.
  – **Файловая система HTTPFS**:
    – Введите URL-адрес расположения файла в удаленной системе

– Если требуется, чтобы файл присутствовал на сервере в качестве виртуального носителя, доступного только для чтения, установите этот флажок.

Примечание: Для сертификатов безопасности, созданных Microsoft IIS, в процессе подключения могут возникать ошибки. Если это происходит, обратитесь к разделу «Проблемы с подключением носителей» на странице 83.

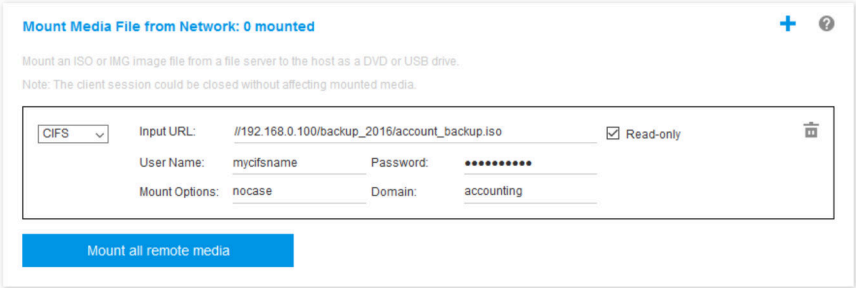
Щелкните **Подключить все удаленные носители**, чтобы подключить файл в качестве виртуального носителя. Чтобы удалить виртуальный носитель, щелкните значок корзины справа от подключенного носителя.

- С помощью компонента XClarity Controller RDOC можно отправить в память XClarity Controller и подключить в качестве виртуальных носителей до двух файлов. Общий размер обоих файлов не должен превышать 50 МБ. Эти файлы останутся в памяти XClarity Controller до удаления, даже если сеанс удаленной консоли завершен. Компонент RDOC поддерживает следующие механизмы отправки файлов:

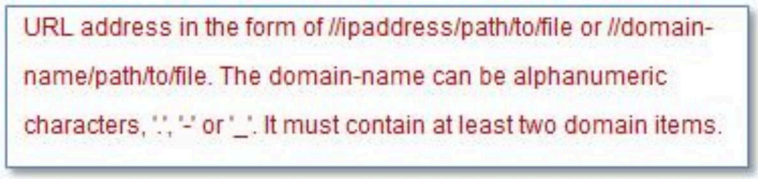
  – **Файловая система CIFS**: см. подробное описание выше.

  Пример:

  Чтобы подключить файл ISO с именем account_backup.iso, расположенный в каталоге backup_2016 сервера CIFS с IP-адресом 192.168.0.100, в качестве доступного только для чтения виртуального диска на сервере, необходимо заполнить поля, как показано на рисунке ниже. В этом примере сервер, расположенный по адресу 192.168.0.100, является членом набора серверов в домене «accounting». Доменное имя является необязательным. Если ваш сервер CIFS не является частью домена, оставьте поле **Домен** пустым. Параметр монтажа CIFS «nocase» задан в этом примере в поле **Параметры монтажа**, что указывает серверу CIFS на то, что проверку имени файла по верхнему/нижнему регистру следует игнорировать. Поле **Параметры подключения** является необязательным. Информация, вводимая пользователем в этом поле, не используется контроллером BMC и просто передается серверу CIFS, когда подается запрос на подключение. См. документацию по внедрению вашего сервера CIFS, чтобы определить, какие параметры поддерживаются вашим сервером CIFS.



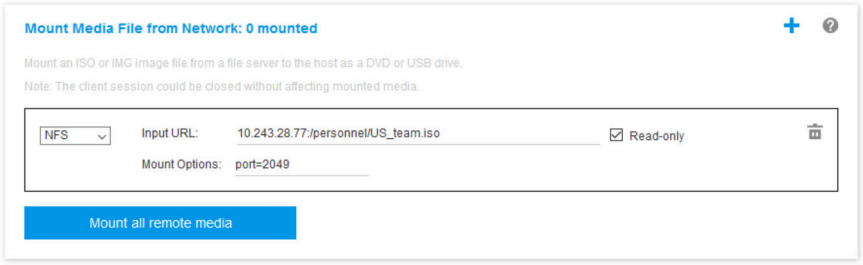
BMC предоставляет инструкции по указанию URL-адреса. Если вводится недопустимый URL-адрес, кнопка подключения будет серой (недоступной), и под полем URL-адреса будет отображаться ожидаемый формат URL-адреса красным цветом.



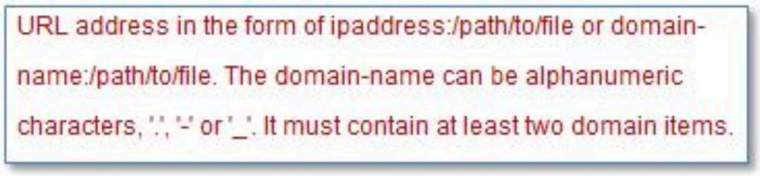
  – **Файловая система NFS**: см. подробное описание выше.

  Пример:

Чтобы установить файл ISO с именем US_team.iso, расположенный в каталоге «personnel» сервера NFS с IP-адресом 10.243.28.77, в качестве доступного только для чтения виртуального диска на сервере, необходимо заполнить следующие поля, как показано на рисунке ниже. Параметр подключения NFS «port=2049» указывает, что для передачи данных должен использоваться сетевой порт 2049. Поле **Параметры подключения** является необязательным. Информация, вводимая пользователем в этом поле, передается серверу NFS, когда подается запрос на подключение. См. документацию по внедрению вашего сервера NFS, чтобы определить, какие параметры поддерживаются вашим сервером NFS.



BMC предоставляет инструкции по указанию URL-адреса. Если вводится недопустимый URL-адрес, кнопка подключения будет серой (недоступной), и под полем URL-адреса будет отображаться ожидаемый формат URL-адреса красным цветом.

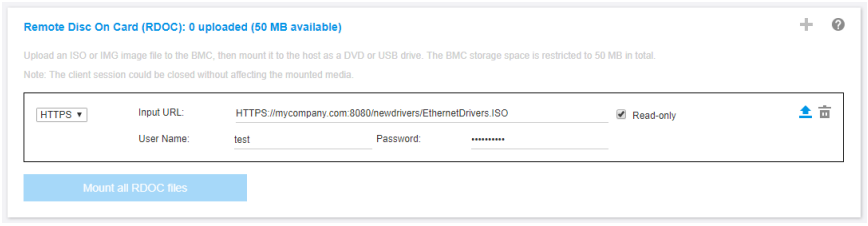


- **HTTPS — Hypertext Transfer Protocol Secure**:
  - Введите URL-адрес расположения файла в удаленной системе.
  - Если требуется, чтобы файл присутствовал на сервере в качестве виртуального носителя, доступного только для чтения, установите этот флажок.
  - Введите учетные данные, необходимые XClarity Controller для осуществления доступа к файлу в удаленной системе.

  Примечания:

  - Для сертификатов безопасности, созданных Microsoft IIS, в процессе подключения могут возникать ошибки. Если это происходит, обратитесь к разделу «Проблемы с подключением носителей» на странице 83.
  - XClarity Controller не поддерживает использование пробелов в имени пользователя, пароле или URL-адресе. Убедитесь, что настроенные для входа на сервер CIFS учетные данные и URL-адрес не содержат пробела в имени пользователя или пароле. **Пример**:

    Чтобы подключить файл ISO с именем EthernetDrivers.ISO, расположенный в каталоге newdrivers сервера HTTPS с доменным именем mycompany.com, с использованием сетевого порта 8080 в качестве доступного только для чтения виртуального диска на сервере, необходимо заполнить поля, как показано на рисунке ниже.



BMC предоставляет инструкции по указанию URL-адреса. Если вводится недопустимый URL-адрес, кнопка подключения будет серой (недоступной), и под полем URL-адреса будет отображаться ожидаемый формат URL-адреса красным цветом.

URL address in the form of https://ipaddress[:port]/path/to/file or HTTPS://domain-name[:port]/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items. The port number is optional

- **Протокол SFTP**
  - Введите URL-адрес расположения файла в удаленной системе.
  - Если требуется, чтобы файл присутствовал на сервере в качестве виртуального носителя, доступного только для чтения, установите этот флажок.
  - Введите учетные данные, необходимые XClarity Controller для осуществления доступа к файлу в удаленной системе.

  Примечания:

  - XClarity Controller не поддерживает использование пробелов в имени пользователя, пароле или URL-адресе. Убедитесь, что настроенные для входа на сервер CIFS учетные данные и URL-адрес не содержат пробела в имени пользователя или пароле.
  - Если XClarity Controller подключается к HTTPS-серверу, отображается всплывающее окно с информацией о сертификате безопасности, используемом сервером HTTPS. XClarity Controller не удается подтвердить аутентичность сертификата безопасности.
- **ЛОКАЛЬНО — файловая система CIFS**:
  - Найдите в системе файл ISO или IMG, который требуется установить.
  - Если требуется, чтобы файл присутствовал на сервере в качестве виртуального носителя, доступного только для чтения, установите этот флажок.

Щелкните **Подключить все файлы RDOC**, чтобы подключить файл в качестве виртуального носителя. Чтобы удалить виртуальный носитель, щелкните значок корзины справа от подключенного носителя.

Отдельный инструмент

Если пользователям требуется подключить устройства или образы (.iso/.img) с помощью XClarity Controller, они могут использовать отдельную часть кода rdmount в пакете OneCLI. В частности, rdmount откроет подключение к XClarity Controller и подключит устройство или образы в хосте.

rdmount имеет следующий синтаксис:

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

Пример подключения файла ISO:

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

Удаленный диск с использованием клиента Java

В этом разделе описано подключение локального носителя с использованием клиента Java.

Можно использовать клиент Java для назначения серверу CD- или DVD-диска, дисковода для дискет и USB-устройства флэш-памяти, находящегося на вашем компьютере, либо указать образ диска на своем компьютере для использования сервером. Диск можно использовать для перезагрузки (загрузки) сервера, обновления кода, установки на сервер нового ПО, а также установки или обновления операционной системы сервера. Можно осуществлять доступ к удаленному диску. Диски и образы дисков отображаются в качестве USB-накопителей на сервере.

Примечания: Удаленная консоль Java поддерживает одну из следующих сред Java и может быть открыта, только если клиент HTML5 не запущен.

1. Среда выполнения Oracle Java Runtime Environment 1.8/Java SE 8 или более новые версии
2. Поддерживается дистрибутив AdoptOpenJDK OpenJDK 8. с HotSpot JVM.

При использовании AdoptOpenJDK необходимо использовать https://openwebstart.com/ в OSX, Windows и Linux.

Создание файла образа

Чтобы создать новый файл образа из указанной исходной папки, выполните следующие действия:

1. Нажмите **Создать образ** на вкладке **Виртуальные носители** в окне «Клиент Java виртуальных носителей». Отобразится окно «Создание образа из папки».
2. Нажмите кнопку **Обзор**, связанную с полем **Исходная папка**, чтобы выбрать нужную исходную папку.
3. Нажмите кнопку **Обзор**, связанную с полем **Новый файл образа**, чтобы выбрать нужный файл образа.
4. Нажмите кнопку **Создать образ**.

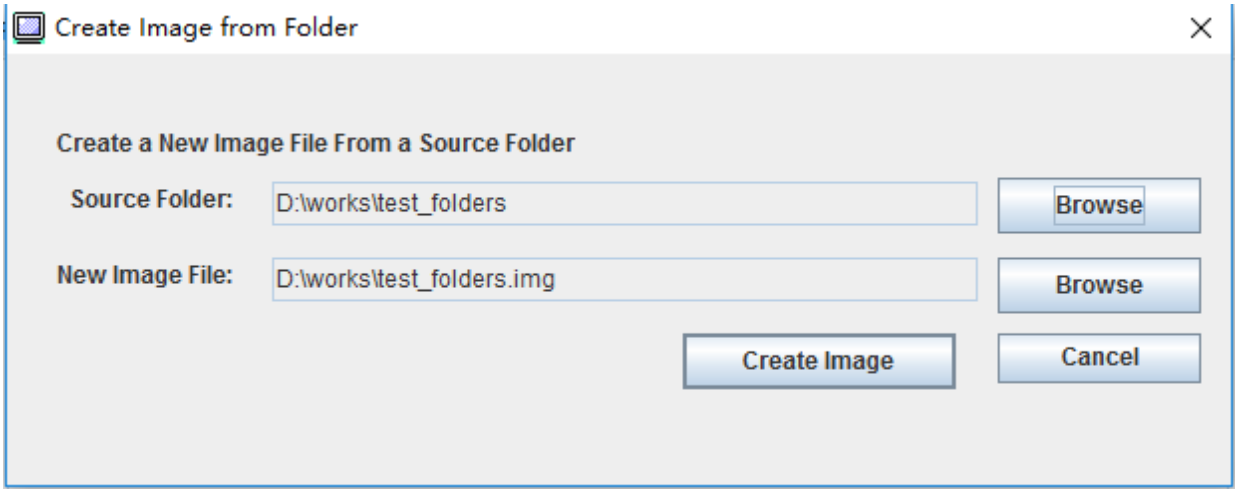


Рис. 1. Создание файла образа

Выбор подключаемых устройств

Чтобы подключить локальный образ, папку и CD-/DVD-/USB-диск, выполните следующие действия:

Нажмите **Выбрать подключаемые устройства** на вкладке **Виртуальные носители** в окне «Клиент Java виртуальных носителей». Отобразится окно «Выбор подключаемых устройств».

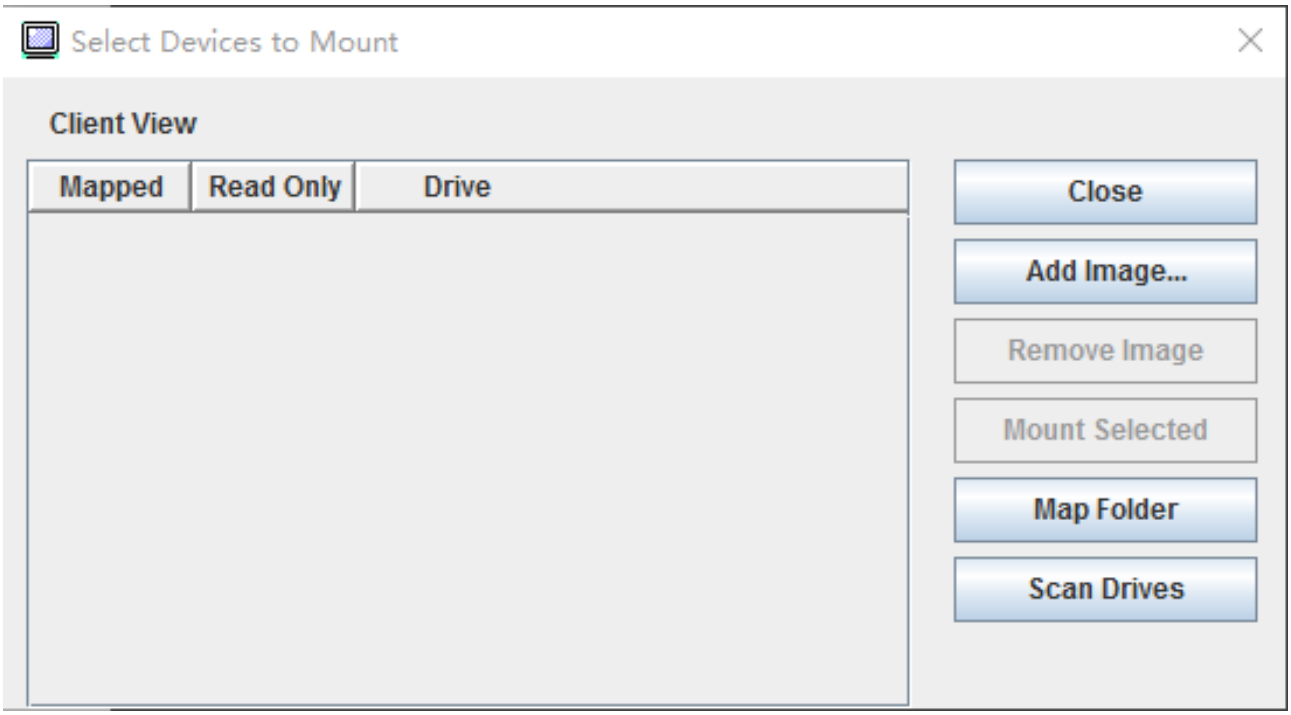


Рис. 2. Окно «Выбор подключаемых устройств»

Можно подключить локальный образ, папку и CD-/DVD-/USB-диск, выполнив следующие действия:

- **Подключение локального образа**:
  1. Нажмите кнопку **Добавить образ**, чтобы выбрать подключаемый образ.
  2. Установите флажок **Сопоставлено**.
  3. При необходимости установите флажок **Только чтение**, чтобы включить соответствующую функцию.
  4. Нажмите кнопку**Подключить выбранное**, и локальный образ будет успешно подключен.

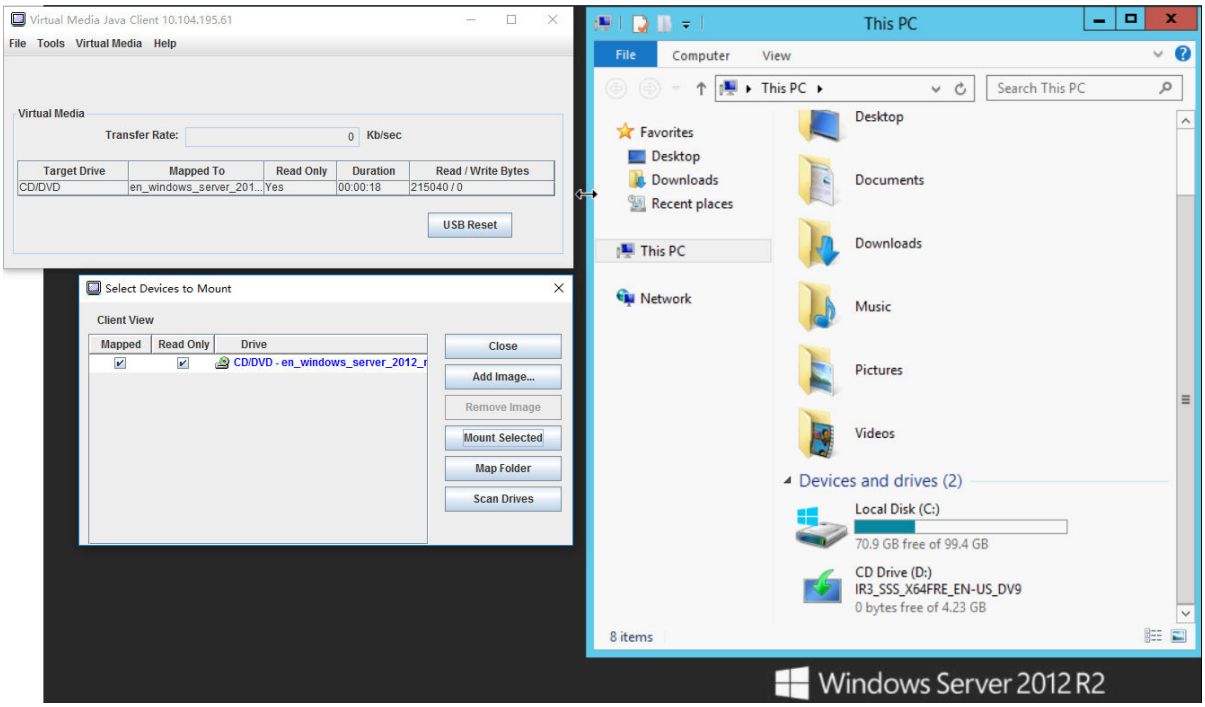


Рис. 3. Подключение локального образа

- **Подключение локальной папки**:
  1. Нажмите кнопку **Сопоставить папку**, чтобы выбрать локальную папку для подключения.
  2. Нажмите кнопку**Подключить выбранное**, и локальная папка будет успешно подключена.

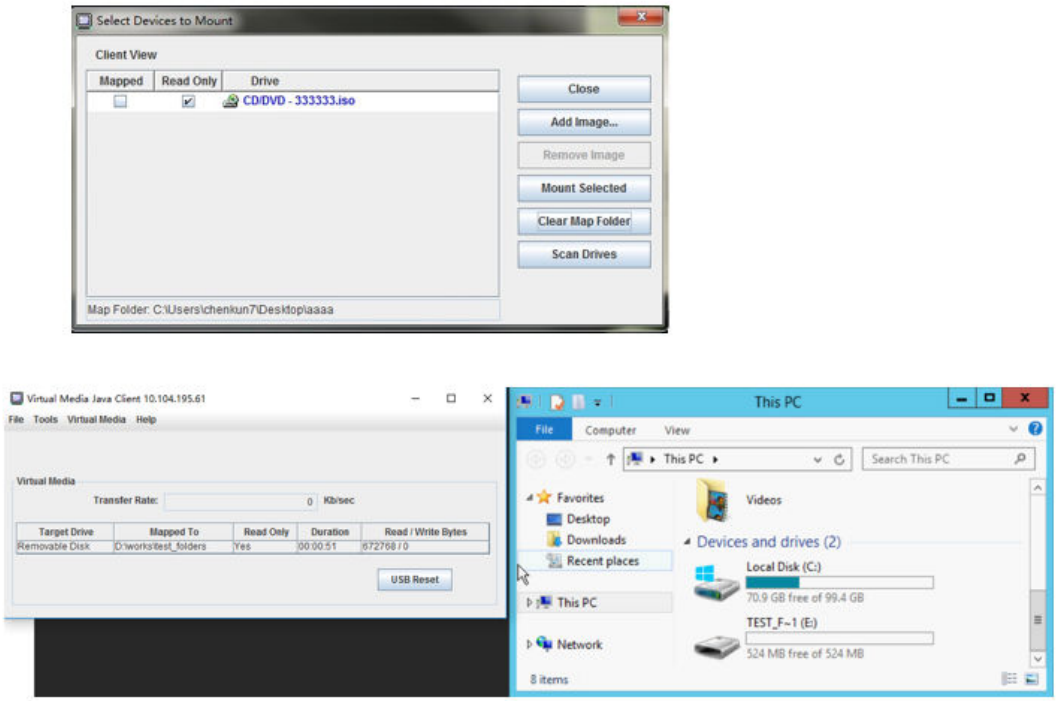


Рис. 4. Подключение локальной папки

- **Подключение CD-/DVD-/USB-диска**:
  1. Нажмите кнопку **Сканировать диски**, чтобы обнаружить подключенный CD-/DVD- или USB-диск.
  2. Установите флажок **Сопоставлено**.
  3. При необходимости установите флажок **Только чтение**, чтобы включить соответствующую функцию.
  4. Нажмите кнопку**Подключить выбранное**, и локальный образ будет успешно подключен.

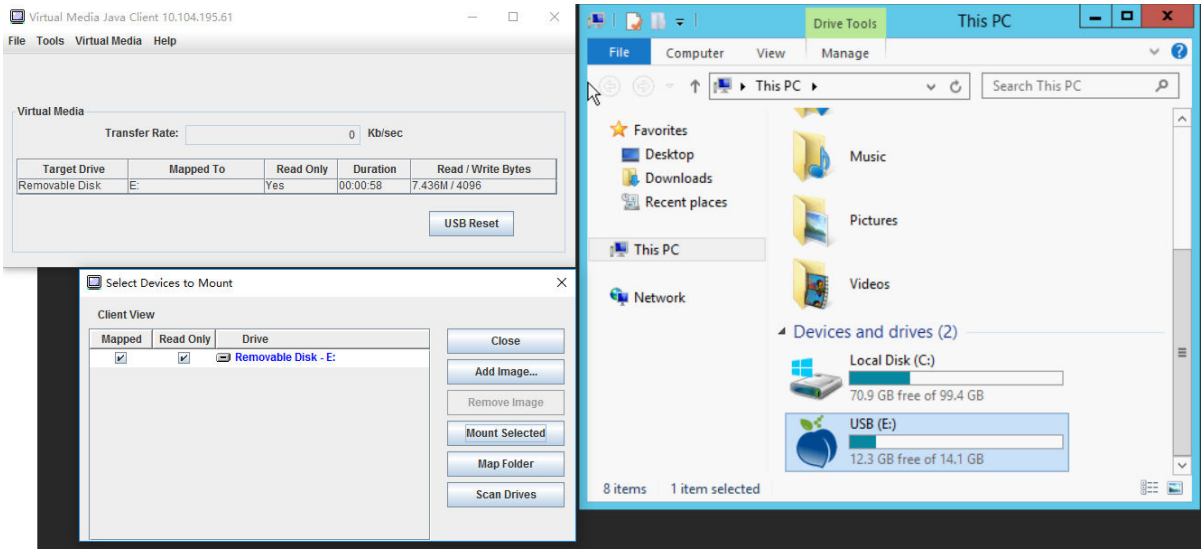


Рис. 5. Подключение CD-/DVD-/USB-диска

В окне «Выбор подключаемых устройств» отображается список доступных для подключения локальных устройств. В этом окне отображаются следующие поля и кнопки:

- Поле **Сопоставлено** содержит флажок, с помощью которого можно выбрать устройства для подключения или сопоставления.
- Поле **Только чтение** содержит флажок, с помощью которого можно выбрать сопоставленные или подключенные устройства, которые на хост-сервере будут доступны *только для чтения*.
- В поле **Диск** отображается путь к устройству на локальном компьютере.
- Нажмите кнопку **Закрыть**, чтобы закрыть окно «Выбор подключаемых устройств».
- Нажмите кнопку **Добавить образ**, чтобы найти файл образа на дискете или файл образа ISO в локальной файловой системе, который требуется добавить в список устройств.
- Нажмите кнопку **Удалить образ**, чтобы удалить образ, добавленный в список устройств.
- Нажмите кнопку **Подключить выбранное**, чтобы подключить или сопоставить все устройства, помеченные для подключения или сопоставления в поле **Сопоставленные**.

  Примечание: Папка будет подключена в качестве доступной только для чтения.
- Нажмите кнопку **Сканировать диски**, чтобы обновить список локальных устройств.

Выбор отключаемых устройств

Чтобы отключить устройства от хост-сервера, выполните следующие действия:

1. Нажмите **Отключить все** на вкладке **Виртуальные носители** в окне «Клиент Java виртуальных носителей».

2. После выбора варианта **Отключить все** отобразится окно подтверждения действия. После подтверждения *все* устройства хост-сервера будут отключены от сервера.

   Примечание: Невозможно отключать диски по одному.

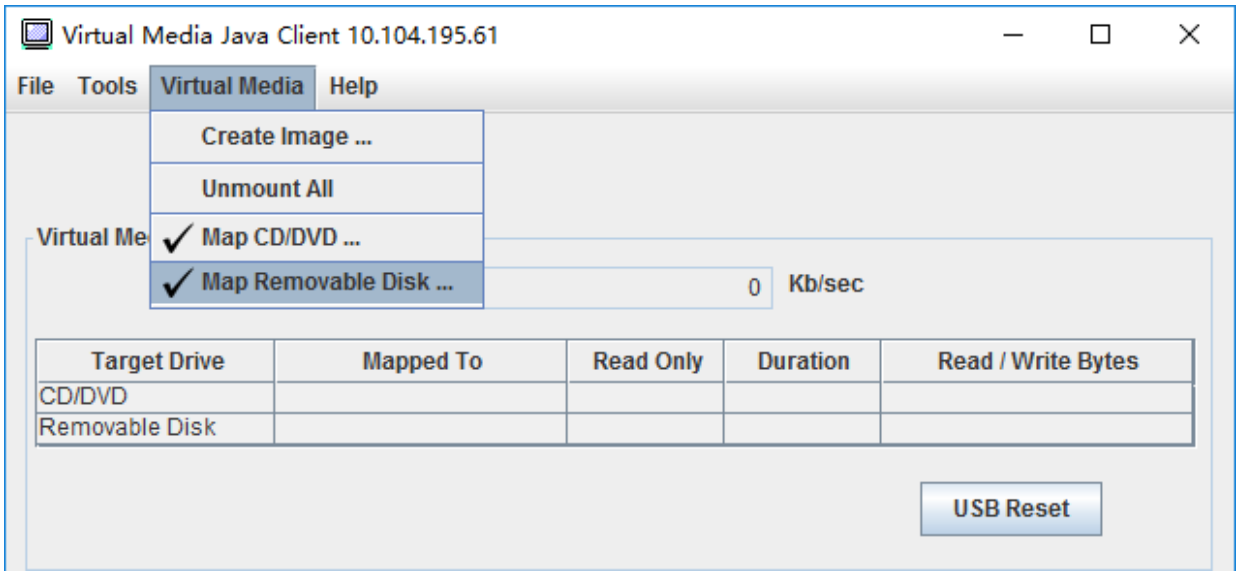


Рис. 6. Отключить все

Проблемы с подключением носителей

Воспользуйтесь информацией из этого раздела для устранения проблем с подключением носителей.

При использовании сертификатов безопасности, созданных Microsoft IIS, в процессе подключения могут возникать ошибки. В этом случае замените сертификат безопасности новым сертификатом, созданным с помощью openssl. При этом созданный PFX-файл загружается на сервер Microsoft IIS.

Ниже приведен пример создания нового сертификата безопасности с помощью openssl в операционной системе Linux.

```
$ openssl
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
Organizational Unit Name (eg, section) []:Lenovo
```

```
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt  server.csr  server.key

$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt  server.csr  server.key  server.pfx
```

Выход из сеанса удаленной консоли

В этом разделе описано завершение сеанса удаленной консоли.

Чтобы завершить сеанс удаленной консоли, закройте окна удаленной консоли и сеанса виртуальных носителей.

Загрузка данных по обслуживанию

Воспользуйтесь информацией из этого раздела для сбора информации об обслуживании вашего сервера Как правило, это процедура выполняется только по запросу специалиста по обслуживанию в процессе устранения проблем с сервером.

На домашней странице XClarity Controller щелкните параметр **Обслуживание** в разделе **Быстрое действие** и выберите **Скачать данные по обслуживанию**. Нажмите кнопку **OK**, чтобы скачать данные по обслуживанию.

Процедура сбора данных по обслуживанию и данных поддержки занимает несколько минут (именно столько времени требуется на генерирование данных по обслуживанию). Файл будет сохранен в вашу папку «Загрузки» по умолчанию. При выборе имени файла с данными по обслуживанию необходимо соблюдать следующие правила:<machine type and model>_<serial number>_xcc_<date>-<time>.tgz

Например: 7X2106Z01A_2345678_xcc_170511-175656.tgz.

Помимо формата tgz данные по обслуживанию также можно загрузить в формате tzz. Формат tzz использует другой алгоритм сжатия и может извлекаться с помощью служебной программы, например lzop.

Свойства сервера

Воспользуйтесь информацией из этого раздела, чтобы изменить или просмотреть соответствующие свойства сервера.

Настройка местоположения и контактов

Воспользуйтесь информацией из этого раздела, чтобы настроить различные параметры, помогающие идентифицировать систему для персонала по эксплуатации и поддержке.

Выберите **Свойства сервера** в разделе **Конфигурация сервера**, чтобы настроить сведения **Местоположения и контакты**.

Контакт
Позволяет указать имя и номер телефона лица, к которому следует обращаться при возникновении проблем в системе.

Примечание: Это поле совпадает с полем «Контакт» в конфигурации SNMPv3 и является необходимым для включения SNMPv3.

Имя стойки
Позволяет удобнее найти сервер благодаря указанию стойки, в которой он находится.

Примечание: Это поле не является обязательным и не настраивается на узле Flex.

Номер помещения
Позволяет удобнее найти сервер благодаря указанию помещения, в котором он находится.

Здание
Позволяет удобнее найти сервер благодаря указанию здания, в котором он находится.

Самый нижний U
Позволяет удобнее найти сервер благодаря указанию положения в стойке.

Примечание: Это поле не является обязательным и не настраивается на узле Flex.

Адрес
Позволяет указать полный почтовый адрес расположения сервера.

Примечание: После ввода соответствующей информации она отобразится одной строкой в поле **Расположение** раздела SNMPv3 и на домашней странице XClarity Controller.

Настройка тайм-аутов сервера

Воспользуйтесь информацией из этого раздела, чтобы настроить тайм-ауты для сервера.

Эти тайм-ауты используются для восстановления работы зависшего сервера.

Выберите **Свойства сервера** в разделе **Конфигурация сервера**, чтобы настроить тайм-ауты сервера. Доступны для выбора следующие тайм-ауты сервера:

Watchdog ОС

Watchdog ОС используется для мониторинга операционной системы, чтобы избежать ее зависания. Для использования этой функции требуется интерфейс Ethernet через USB. Подробные сведения см. в разделе «Настройка интерфейса Ethernet через USB» на странице 34. XClarity Controller обращается к операционной системе с интервалом, настроенным в параметре **Время Watchdog ОС**. Если операционная система не отвечает до следующей проверки, XClarity Controller исходит из того, что операционная система зависла. XClarity Controller фиксирует содержимое серверного дисплея, а затем перезагружает сервер в попытке восстановить его работу. XClarity Controller перезапускает сервер только один раз. Если операционная система продолжает зависать после перезагрузки, вместо того чтобы непрерывно перезагружать сервер, он будет оставлен в зависшем состоянии, чтобы можно было изучить и устранить проблему. Чтобы снова включить Watchdog ОС, выключите сервер и включите его снова. Чтобы включить Watchdog ОС, выберите интервал из раскрывающегося меню времени Watchdog ОС и нажмите кнопку **Применить**. Чтобы выключить Watchdog ОС, выберите **Нет** в раскрывающемся меню времени Watchdog ОС.

Watchdog загрузчика

Watchdog загрузчика отслеживает интервал между выполнением POST и началом работы операционной системы. Для использования этой функции требуется интерфейс Ethernet через USB. Подробные сведения см. в разделе «Настройка интерфейса Ethernet через USB» на странице 34. Как только выполнение POST завершено, XClarity Controller запускает таймер и начинает обращаться к операционной системе. Если операционная система не отвечает в течение времени, настроенного в параметрах Watchdog загрузчика, XClarity Controller предполагает, что загрузка ОС зависла. XClarity Controller перезагружает сервер в попытке восстановить его работу. XClarity Controller перезапускает сервер только один раз. Если загрузка операционной системы продолжает зависать после перезагрузки, вместо того чтобы непрерывно перезагружать сервер, он будет оставлен в зависшем состоянии, чтобы можно было изучить и устранить проблему. Watchdog загрузчика включается снова, если выключить и снова включить сервер или если сервер успешно загружает операционную систему. Чтобы включить Watchdog загрузчика, выберите интервал из раскрывающегося меню Watchdog загрузчика и нажмите кнопку **Применить**. Чтобы выключить Watchdog загрузчика, выберите **Нет** в раскрывающемся меню Watchdog загрузчика.

Включение задержки выключения питания

В поле «Задержка выключения питания» укажите период (в минутах) ожидания подсистемой XClarity Controller выключения операционной системы перед принудительным выключением питания. Чтобы задать значение тайм-аута задержки выключения питания, выберите интервал времени из раскрывающегося списка и нажмите кнопку **Применить**. Чтобы выключить принудительное выключение питания контроллера XClarity Controller, выберите **Нет** в раскрывающемся списке.

Сообщение при нарушении

Воспользуйтесь информацией из этого раздела, чтобы составить сообщение, отображаемое при входе пользователя в XClarity Controller.

Выберите **Свойства сервера** в разделе **Конфигурация сервера**. Воспользуйтесь параметром **Сообщение при нарушении**, чтобы настроить сообщение, отображаемое для пользователя. Завершив ввод данных, нажмите кнопку **Применить**.

Текст сообщения отображается в области «Сообщение» страницы входа в XClarity Controller, когда пользователь выполняет вход в систему.

Установка даты и времени на XClarity Controller

Информация из этого раздела поможет понять настройки даты и времени XClarity Controller. Предоставляются инструкции по настройке даты и времени XClarity Controller. Дата и время XClarity Controller используются для добавления отметок времени ко всем событиям, внесенным в журнал событий, и отправляемым оповещениям.

На домашней странице XClarity Controller щелкните значок часов в верхнем правом углу, чтобы просмотреть или изменить дату и время XClarity Controller. У XClarity Controller нет собственных часов реального времени. Можно настроить синхронизацию даты и времени XClarity Controller с сервером NTP (протокола сетевого времени) или с оборудованием часов реального времени сервера.

Синхронизация с NTP

Выполните следующие шаги для синхронизации часов XClarity Controller с сервером NTP:

- Выберите **Синхронизировать время с NTP** и укажите адрес сервера NTP.
- Нажмите значок «+», чтобы указать дополнительные серверы NTP.
- Укажите желаемую периодичность синхронизации XClarity Controller с сервером NTP.
- Время, полученное с сервера NTP, указано в формате UTC.
  - Если требуется, чтобы XClarity Controller корректировал время и дату для вашего региона, выберите в раскрывающемся меню смещение часового пояса для вашего языкового стандарта.
  - Если в вашем расположении действует летнее время, установите флажок **Автоматический переход на летнее время и обратно**.
- Завершив внесение изменений в конфигурацию, нажмите кнопку **Применить**.

Синхронизация с хостом

Время на оборудовании часов реального времени сервера может быть указано в формате UTC или уже переведено и сохранено в формате местного времени. Некоторые операционные системы сохраняют время часов реального времени в формате UTC, другие — в формате местного времени. Часы реального времени сервера не указывают, в каком формате сохранено время. Следовательно, если XClarity Controller настроен на синхронизацию с часами реального времени хоста, пользователь может выбрать, как XClarity Controller будет использовать время и дату, полученные от часов реального времени.

- Локальное (например: Windows): В этом режиме XClarity Controller расценивает время и дату, полученные от часов реального времени, как локальное время в соответствующем часовом поясе и переходом на летнее время, если таковой осуществляется.
- UTC (например: Linux): В этом режиме XClarity Controller расценивает время и дату, полученные от часов реального времени, как время в формате UTC без часового пояса или перехода на летнее время. В этом режиме можно корректировать время и дату для своего региона, выбирая в раскрывающемся меню смещение часового пояса для вашего языкового стандарта. Если в вашем расположении действует летнее время, можно также установить флажок **Автоматический переход на летнее время и обратно**..
- Завершив внесение изменений в конфигурацию, нажмите кнопку **Применить**.

Примечания:

- Когда выполняется переход на летнее время, любые действия, запланированные для выполнения контроллером XClarity Controller в интервале, когда часы переходят вперед, не выполняются. Например, если начальное летнее время в США — 2:00 утра 12 марта, а то или иное действие с питанием запланировано на 2:10 утра 12 марта, это действие выполнено не будет. Как только наступит 2:00 утра, XClarity Controller считает наступившее время как 3:00 утра.

- Изменить настройки даты и времени XClarity Controller в Flex System невозможно.

Глава 6. Настройка хранилища

Воспользуйтесь информацией из этой главы, чтобы понять доступные параметры конфигурации хранилища.

При настройке хранилища доступны следующие параметры:

- Подробно
- Настройка RAID

Сведения о массиве RAID

Воспользуйтесь информацией из этого раздела, чтобы использовать функцию получения сведений о массиве RAID.

Эта функция отображает сведения о физической структуре и конфигурации устройств хранения данных, а также информацию об их расположении, производителе, названии продукта, состоянии, емкости, интерфейсе, носителях, форм-факторе и прочие сведения.

Настройка RAID

Воспользуйтесь информацией из этого раздела, чтобы выполнить функции по настройке RAID.

Воспользуйтесь информацией из этого раздела для просмотра и настройки пулов памяти, соответствующих виртуальных дисков и дисков для адаптера RAID. Если система выключена, включите ее, чтобы просмотреть сведения о RAID.

Просмотр и настройка виртуальных дисков

Воспользуйтесь информацией из этого раздела для просмотра и настройки виртуальных дисков.

Когда вы выбираете команду **Настроить RAID** в разделе **Конфигурация сервера**, выполняется переход на вкладку **Конфигурация массива**, а существующие виртуальные диски отображаются по умолчанию. Логические диски сортируются по массивам дисков и контроллерам. Отображаются подробные сведения о виртуальном диске, такие как размер блока чередования виртуальных дисков и загружаемые сведения.

Чтобы настроить параметры RAID, щелкните **Включить режим редактирования**.

В режиме редактирования мощно щелкнуть меню действий контроллера, просмотреть существующие и создать новые виртуальные диски RAID.

В меню действий контроллера можно выполнить следующие действия:

Очистить конфигурацию RAID
Очищает всю конфигурацию и все данные на выбранном контроллере.

Управлять внешней конфигурацией
Импортирует любые обнаруженные внешние диски. Внешний диск — это диск, перенесенный в текущий контроллер RAID из другой конфигурации RAID

Примечание: Если внешние диски не обнаружены, вы получите соответствующее уведомление.

Сведения о текущих виртуальных дисках RAID для определенного контроллера отображаются как соответствующие «карточки виртуальных дисков». На каждой карточке отображается такая информация, как имя, статус, емкость и действия виртуальных дисков. Щелкнув значок карандаша, можно редактировать эту информацию, а щелкнув значок корзины, — удалить «карточку виртуальных дисков».

Примечание: Изменить емкость и уровень RAID невозможно.

Если щелкнуть название виртуальных дисков, отобразится окно свойств виртуальных дисков.

Чтобы создать новый виртуальный диск RAID, выполните действия ниже:

Примечание: Если места для хранения не осталось, создать новый виртуальный диск не удастся.

1. **Выберите диски или дисковый массив со свободным пространством для хранения**
   a. При создании виртуальных дисков в новом дисковом массиве необходимо указать уровень RAID. Если недостаточно дисков для выбора и вы нажимаете кнопку **Далее**, то под полем с уровнем RAID отображается сообщение об ошибке.

      Для некоторых уровней RAID необходимо использовать диапазон. Существует минимальное количество дисков, которые должны присутствовать в диапазоне.

      1) В таких ситуациях в веб-интерфейсе по умолчанию отображается **Диапазон 1**.
      2) Выберите диски и нажмите кнопку **Добавить элемент**, чтобы добавить диски в **Диапазон 1**. Если в разделе **Диапазон 1** недостаточно дисков, отключите ссылку **Добавить диапазон**.
      3) Щелкните **Добавить диапазон**, чтобы добавить **Диапазон 2**. Выберите диски и нажмите кнопку **Добавить элемент**, чтобы добавить элементы в **Диапазон 2**.
      4) Щелкните **Добавить элемент**, чтобы добавить диски в последний диапазон. Если требуется снова добавить диски в **Диапазон 1**, необходимо щелкнуть Диапазон 1 и выбрать диски для добавления в **Диапазон 1**.
      5) Если количество диапазонов достигло максимума, отключите ссылку **Добавить диапазон**.

   b. Чтобы создать виртуальные диски в существующем массиве дисков, необходимо выбрать массив дисков со свободной емкостью.
2. **Создание виртуальных дисков**
   a. По умолчанию создайте виртуальный диск, использующий всю доступную емкость для хранения. Значок **Добавить** неактивен, если использована вся емкость для хранения. Можно щелкнуть значок карандаша, чтобы изменить емкость или другие свойства.
   b. Когда вы отредактируете первый виртуальный диск так, чтобы использовать не всю емкость для хранения, значок **Добавить** станет активным. Щелкните этот значок, чтобы отобразить окно **Добавление виртуальных дисков**.
   c. Если виртуальных дисков несколько, значок **Удалить** также будет активен. Этот значок не отображается, если имеется только один виртуальный диск. При нажатии значка **Удалить** выделенная строка удаляется немедленно. Окно подтверждения не отображается, поскольку виртуальный диск еще не создан.
   d. Щелкните **Начать создание виртуальных дисков**, чтобы запустить процесс.

Примечание: Если контроллер не поддерживается, отобразится соответствующее сообщение.

Просмотр и настройка ресурсов хранения

Воспользуйтесь информацией из этого раздела для просмотра и настройки ресурсов хранения.

На вкладке **Ресурсы хранения** можно просматривать и настраивать дисковые массивы, соответствующие виртуальные диски и диски для контроллера RAID.

- **Для устройств хранения, поддерживающих конфигурацию RAID**:
  1. Если контроллер включает настроенные дисковые массивы, установленные диски будут отображаться с учетом дисковых массивов. Ниже описаны элементы, отображаемые в этом окне.
     - **Заголовок таблицы**: отображается ИД дискового массива, уровень RAID и общее количество дисков.
     - **Содержимое таблицы**: перечисляются базовые свойства, такие как имя диска, состояние RAID, тип, серийный номер, номер компонента, номер FRU и действия. На странице **Ресурсы** можно просмотреть все свойства, доступные для обнаружения XClarity Controller.
     - **Действия**: ниже показаны элементы действий, которые могут быть выполнены. Некоторые действия будут недоступны, если диск находится в другом состоянии.
       - **Назначение горячего резерва**: указывает, является ли диск глобальным или выделенным горячим резервом.
       - **Удаление горячего резерва**: удаляет диск из горячего резерва.
       - **Перевод дискового накопителя в автономный режим**: переводит диск в автономный режим.
       - **Перевод дискового накопителя в режим «В сети»**: переводит диск в режим «В сети».
       - **Перевод дискового накопителя в доступное для повторного использования состояние**: Делает диск доступным для повторного использования.
       - **Перевод дискового накопителя в отсутствующее состояние**: делает диск отсутствующим.
       - **Перевод диска в состояние, подходящее для включения в JBOD**: добавляет диск в дисковую структуру JBOD.
       - **Перевод диска в ненастроенное исправное состояние**: делает диск доступным для настройки в массиве или использования в качестве аварийного горячего резерва.
       - **Перевод диска в ненастроенное неисправное состояние**: делает диск неисправным и не позволяет использовать его в массиве или в качестве аварийного горячего резерва.
       - **Подготовка дискового накопителя к удалению**: настройка диска для удаления.
  2. Если контроллер включает диски, которые еще не были настроены, они будут отображаться в таблице **Диски, отличные от RAID**. Если щелкнуть **Преобразовать JBOD в готовое для настройки состояние**, отобразится окно со всеми дисками, поддерживающими этот элемент действий. Можно выбрать для преобразования один или несколько дисков.

Для устройств хранения, не поддерживающих конфигурацию RAID: возможно, XClarity Controller не сможет обнаружить свойства некоторых дисков.

Глава 7. Обновление микропрограммы сервера

Воспользуйтесь информацией из этого раздела для обновления микропрограммы сервера.

Обзор

Общие сведения об обновлении микропрограммы сервера.

Параметр **Обновление микропрограммы** на панели навигации предоставляет четыре функции:

- **Микропрограмма системы:** обзор состояния и версии микропрограммы системы. Также позволяет выполнить обновление микропрограммы системы.
- **Автоматическое продвижение основного XCC в резервный:** после включения микропрограмма ожидающего резервного банка будет синхронизирована с основным банком после того, как основной банк пройдет измерение показателя стабильности изображения (ISM).
- **Микропрограмма адаптера:** обзор установленной микропрограммы адаптера, а также ее состояния и версии. Кроме того, позволяет выполнить обновление микропрограммы адаптера.

Отображаются текущее состояние и версии микропрограмм BMC, UEFI, LXPM, дисков LXPM и адаптеров, включая основную и резервную версии BMC. Существует четыре категории состояний микропрограммы:

- **Активная:** микропрограмма активна.
- **Неактивная:** микропрограмма не активна.
- **В ожидании:** микропрограмма ожидает перехода в активное состояние.
- **Н/Д:** для этого компонента не установлена никакая микропрограмма.

Внимание:

- Перед обновлением UEFI необходимо обновить до последней версии XCC и IMM. Обновление в другом порядке может стать причиной нестандартного или неправильного поведения системы.
- Установка неправильного обновления микропрограммы может привести к неисправности сервера. Перед установкой обновления микропрограммы или драйвера устройства прочтите файлы Readme и истории изменений, сопровождающие загруженное обновление. Эти файлы содержат важную информацию об обновлении и процедуре его установки, включая описания особых процедур обновления с ранних версий микропрограммы или драйвера устройства до последней версии. Поскольку веб-браузер может содержать данные кэша XCC, рекомендуется перезагрузить веб-страницу после обновления микропрограммы XCC.
- Для некоторых обновлений микропрограммы требуется перезапуск системы, при котором выполняется активация микропрограммы или внутреннее обновление. Этот процесс при загрузке системы называется «режим обслуживания системы» и временно не позволяет пользователю выполнять действия кнопки питания. Также этот режим включается при обновлении микропрограммы. Пользователь не должен отключать питание при переходе системы в режим обслуживания.

Обновление микропрограммы системы, адаптера и блока питания

Пошаговая инструкция по обновлению микропрограммы системы, адаптера и блока питания.

Чтобы вручную применить обновление для **микропрограммы системы**, **адаптера** и **блока питания**, выполните следующие действия:

1. Нажмите **Обновить микропрограмму** в каждом компоненте. Откроется окно обновления микропрограммы сервера.
2. Щелкните **Обзор**, чтобы выбрать нужный файл обновления микропрограммы.
3. Перейдите к нужному файлу и нажмите кнопку **Открыть**. Вы вернетесь в окно обновления микропрограммы сервера, где будет отображаться выбранный файл.
4. Нажмите кнопку **Далее >**, чтобы начать отправку и проверку выбранного файла. Ход отправки и проверки файла отображается на шкале выполнения. В окне состояния можно убедиться, что выбран правильный файл для обновления. Для компонента **Микропрограмма системы** в окне состояния отображается информация о типе обновляемого файла микропрограммы, например BMC, UEFI или LXPM. После успешной отправки и проверки файла микропрограммы нажмите кнопку **Далее**, чтобы выбрать обновляемое устройство.
5. Щелкните **Обновить**, чтобы начать обновление микропрограммы. Ход обновления отображается на шкале выполнения. После успешного окончания обновления микропрограммы нажмите кнопку **Готово**. Если для того чтобы обновление вступило в силу, требуется перезапустить XClarity Controller, отобразится соответствующее предупреждение. Подробные сведения о перезапуске контроллера XClarity Controller см. в разделе «Действия кнопки питания» на странице 66.

Глава 8. Управление лицензиями

Управление лицензиями Lenovo XClarity Controller позволяет устанавливать и контролировать дополнительные компоненты управления сервером и системами.

Существует несколько уровней функциональности и компонентов микропрограммы XClarity Controller для вашего сервера. Уровень установленных на сервере компонентов микропрограммы варьируется в зависимости от типа оборудования.

Для обновления функциональности XClarity Controller можно приобрести и установить ключ активации.

Чтобы заказать ключ активации, свяжитесь со своим представителем по продажам или бизнес-партнером.

Используйте веб-интерфейс XClarity Controller или интерфейс командной строки XClarity Controller, чтобы вручную установить ключ активации, позволяющий использовать приобретенный вами дополнительный компонент. Перед активацией ключа:

- Ключ активации должен находиться в той же системе, которая используется для входа в XClarity Controller.
- Необходимо заказать лицензионный ключ и получить его код авторизации по почте или электронной почте.

См. сведения об управлении ключом активации с помощью веб-интерфейса XClarity Controller в разделах «Установка ключа активации» на странице 95, «Удаление ключа активации» на странице 96 или «Экспорт ключа активации» на странице 96. См. сведения об управлении ключом активации с помощью интерфейса командной строки XClarity Controller в разделе «Команда keycfg» на странице 135.

Чтобы зарегистрировать идентификатор при выполнении административных операций с лицензией XClarity Controller, щелкните следующую ссылку: http://thinksystem.lenovofiles.com/help/index.jsp

Дополнительные сведения об управлении лицензиями для серверов Lenovo доступны на веб-сайте **Lenovo Press** по следующему адресу:

https://lenovopress.com/redp4895-using-lenovo-features-on-demand

Внимание: Невозможно выполнить обновление выпуска XClarity Controller Standard до уровня Enterprise напрямую. Потребуется сначала выполнить обновление до уровня Advanced и только после этого активировать функциональность уровня Enterprise.

Установка ключа активации

Воспользуйтесь информацией из этого раздела для добавления дополнительного компонента на сервер.

Чтобы установить ключ активации, выполните следующие действия:

Шаг 1. Щелкните **Лицензия** в разделе **BMC Configuration**.

Шаг 2. Щелкните **Обновить лицензию**.

Шаг 3. В окне **Добавление новой лицензии** щелкните **Обзор**; затем выберите файл ключа активации, который требуется добавить, в окне «Отправка файла», щелкните **Открыть**, чтобы добавить файл, или **Отмена**, чтобы остановить установку. Чтобы завершить добавление ключа, нажмите кнопку **OK** в окне «Добавление ключа активации» или кнопку **Отмена**, чтобы остановить установку.

Окно «Успешно» говорит о том, что ключ активации установлен.

Примечания:

- Если ключ активации не действителен, отобразится окно с ошибкой.

Шаг 4. Нажмите кнопку **OK**, чтобы закрыть окно «Успешно».

Удаление ключа активации

Воспользуйтесь информацией из этого раздела для удаления дополнительного компонента с сервера.

Чтобы удалить ключ активации, выполните следующие действия:

Шаг 1. Щелкните **Лицензия** в разделе **BMC Configuration**.

Шаг 2. Выберите удаляемый ключ активации и нажмите кнопку **Удалить**.

Шаг 3. В окне «Подтверждение удаления ключа активации» нажмите кнопку **OK**, чтобы подтвердить удаление ключа активации, или **Отмена**, чтобы сохранить файл ключа.
Выбранный ключ активации удаляется с сервера и более не отображается на странице «Управление лицензиями».

Экспорт ключа активации

Воспользуйтесь информацией из этого раздела для экспорта дополнительного компонента с сервера.

Чтобы экспортировать ключ активации, выполните следующие действия:

Шаг 1. Щелкните **Лицензия** в разделе **BMC Configuration**.

Шаг 2. На странице управления лицензиями выберите ключ активации для экспорта и нажмите кнопку **Экспортировать**.

Шаг 3. В окне **Экспорт выбранной лицензии** щелкните **Экспортировать**, чтобы подтвердить экспорт ключа активации, или **Отмена**, чтобы отменить запрос на экспорт ключа.

Шаг 4. Выберите каталог для сохранения файла.
Выбранный ключ активации экспортируется с сервера.

Глава 9. Соответствующие стандарту Redfish API-интерфейсы REST Lenovo XClarity Controller

Lenovo XClarity Controller предоставляет ряд удобных соответствующих стандарту Redfish API-интерфейсов REST, которые можно использовать для доступа к данным и службам Lenovo XClarity Controller из приложений, работающих вне платформы Lenovo XClarity Controller.

Это позволяет легко интегрировать возможности Lenovo XClarity Controller в другое программное обеспечение независимо от того, в какой системе оно работает — в той же, что и сервер Lenovo XClarity Controller, или в удаленной системе в той же сети. Эти API-интерфейсы основаны на соответствующих отраслевому стандарту Redfish API-интерфейсах REST и доступны по протоколу HTTPS.

Руководство пользователя соответствующего стандарту Redfish API-интерфейса REST XClarity Controller можно найти по следующей ссылке: https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.restapi.doc/xcc_restapi_book.pdf.

Lenovo предоставляет примеры скриптов Redfish с открытым исходным кодом, которые можно использовать в качестве основы для разработки программного обеспечения, взаимодействующего с соответствующим стандарту Redfish API-интерфейсом REST Lenovo. Примеры скриптов можно найти по следующим адресам:

- Python: https://github.com/lenovo/python-redfish-lenovo
- PowerShell: https://github.com/lenovo/powershell-redfish-lenovo

Спецификации DMTF, связанные с соответствующим стандарту Redfish API-интерфейсом, можно найти по следующему адресу: https://redfish.dmtf.org/. На этом веб-сайте приводятся общие спецификации и другие справочные материалы по соответствующему стандарту Redfish API-интерфейсу REST.

Глава 10. Интерфейс командной строки

Воспользуйтесь информацией из этого раздела для ввода команд, позволяющих осуществлять мониторинг и управление XClarity Controller без использования веб-интерфейса XClarity Controller.

Используйте интерфейс командной строки XClarity Controller для доступа к XClarity Controller без использования веб-интерфейса. Он предоставляет подмножество функций управления, предоставляемых веб-интерфейсом.

Интерфейс командной строки доступен в сеансе SSH. Прежде чем отправлять какие-либо команды интерфейса командной строки, необходимо пройти аутентификацию в XClarity Controller.

Получение доступа к интерфейсу командной строки

Воспользуйтесь информацией из этого раздела, чтобы получить доступ к интерфейсу командной строки.

Чтобы получить доступ к интерфейсу командной строки, запустите сеанс SSH с IP-адресом контроллера XClarity Controller (см. дополнительные сведения в разделе «Настройка перенаправления последовательного порта в SSH» на странице 99).

Вход в сеанс командной строки

Воспользуйтесь информацией из этого раздела, чтобы выполнить вход в сеанс командной строки.

Чтобы войти в командную строку, выполните следующие действия:

Шаг 1. Установите соединение с XClarity Controller.

Шаг 2. В строке имени пользователя введите идентификатор пользователя.

Шаг 3. В строке пароля введите пароль, используемый для входа в XClarity Controller.

Вы выполнили вход в командную строку. Запрос командной строки имеет вид `system>`. Сеанс командной строки длится до тех пор, пока вы не введете `exit` в командной строке. Вы вышли из системы, сеанс завершен.

Настройка перенаправления последовательного порта в SSH

В этом разделе представлены сведения об использовании XClarity Controller в качестве последовательного сервера терминалов.

Перенаправление последовательных портов в SSH позволяет системному администратору использовать XClarity Controller в качестве последовательного терминального сервера. Последовательный порт сервера доступен из подключения SSH, если включено последовательное перенаправление.

Примечание: Команда интерфейса командной строки **console 1** используется для запуска сеанса последовательного перенаправления с портом COM.

Пример сеанса

```
$ ssh USERID@10.240.1.12
Password:
```

```
system>
```

Весь трафик из сеанса SSH направляется в COM2.

```
ESC (
```

Введите последовательность клавиш выхода, чтобы вернуться в интерфейс командной строки. В этом примере нужно нажать клавишу Esc и ввести левую скобку. Подсказка в интерфейсе командной строки укажет на возврат в интерфейс командной строки IMM.

```
system>
```

Синтаксис команд

Изучите инструкции из этого раздела, чтобы узнать, как вводить команды в интерфейсе командной строки.

Перед использованием команд ознакомьтесь со следующими инструкциями:

- Каждая команда имеет следующий формат:
  `command [arguments] [-options]`
- В синтаксисе команды учитывается регистр.
- Имя команды вводится символами нижнего регистра.
- Все аргументы необходимо указывать сразу после команды. Параметры следуют сразу за аргументами.
- Каждому параметру всегда предшествует дефис (-). Бывают короткие параметры (из одной буквы) и длинные параметры (из нескольких букв).
- Если параметр имеет аргумент, этот аргумент является обязательным, например:
  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`
  где **ifconfig** — это команда, eth0 — это аргумент, а -i, -g и -s — параметры. В этом примере все три параметра имеют аргументы.
- Скобки указывают на то, что аргумент или параметр является необязательным. Скобки не являются частью вводимой команды.

Возможности и ограничения

В этом разделе содержится информация о возможностях и ограничениях интерфейса командной строки.

Интерфейс командной строки имеет следующие возможности и ограничения:

- С помощью SSH можно проводить несколько параллельных сеансов интерфейса командной строки.
- Допускается одна команда на строку (лимит 1024 символа с пробелами).
- Отсутствует символ продолжения для длинных команд. Единственная функция редактирования — клавиша Backspace для стирания только что введенных символов.
- Клавиши со стрелками «вверх» и «вниз» можно использовать для просмотра последних восьми команд. Команда **history** позволяет отобразить список из восьми последних команд, которые затем можно использовать в качестве ярлыка для выполнения команды, как в следующем примере:
  ```
  system > history
   0 ifconfig eth0
  ```

```
 1 readlog
 2 readlog
 3 readlog
 4 history
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n XClarity ControllerA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system >
```

- В интерфейсе командной строки буфер выходных данных ограничен 2 КБ. Буферизация отсутствует. Выходные данные отдельной команды не должны превышать 2048 символов. Это ограничение не действует в режиме последовательного перенаправления (данные буферизуются с помощью последовательного перенаправления).
- Простые текстовые сообщения служат для обозначения состояния выполнения команды, как в следующем примере:
```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```
- В синтаксисе команды учитывается регистр.
- Между параметром и аргументом должен быть хотя бы один пробел. Пример неправильного синтаксиса: `ifconfig eth0 -i192.168.70.133`. Пример правильного синтаксиса: `ifconfig eth0 -i 192.168.70.133`.
- Все команды имеют параметры `-h`, `-help` и `?` , предоставляющие справку по синтаксису. Все следующие примеры дают один и тот же результат:
```
system> power -h
system> power -help
system> power ?
```
- Некоторые команды, описанные в следующих разделах, могут быть недоступны для вашей системной конфигурации. Полный список команд, поддерживаемых вашей конфигурацией, можно вывести с помощью параметра `help` или `?`, как показано в следующих примерах:
```
system> help
system> ?
```
- В системе Flex System некоторые параметры контролируются CMM и не могут быть изменены в XClarity Controller.

Перечисление команд по алфавиту

В этом разделе содержится сортированный по алфавиту список команд интерфейса командной строки. Предоставляются ссылки на разделы для каждой команды. В каждом разделе, посвященном команде, предоставляется информация о команде, ее функции, синтаксисе и использовании.

Полный список всех команд интерфейса командной строки XClarity Controller, сортированный в алфавитном порядке, выглядит следующим образом:

Команды служебной программы

В этом разделе приводится алфавитный список команд интерфейса командной строки для служебной программы.

В настоящее время доступно 3 команды служебной программы:

Команда exit

Используйте эту команду для выхода из сеанса интерфейса командной строки,

Используйте команду **exit** для выхода из системы и завершения сеанса интерфейса командной строки.

Команда help

Эта команда служит для отображения списка всех команд.

Используйте команду **help** для отображения списка всех команд с кратким описанием каждой. В командной строке можно также ввести ?.

Команда history

Эта команда позволяет вызвать список ранее использованных команд.

Используйте команду **history** для отображения индексированного списка восьми последних вызванных команд. Для вызова команд из списка можно использовать эти индексы (со знаком «!» в начале) в качестве ярлыков.

Пример:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Команды монитора

В этом разделе приводится алфавитный список команд интерфейса командной строки для монитора.

В настоящее время доступно 11 команд монитора:

Команда clearlog

Эта команда используется для очистки журнала событий IMM.

Для очистки журнала событий IMM воспользуйтесь командой **clearlog**. Для использования этой команды необходимо обладать полномочиями для очистки журналов событий.

Примечание: Эта команда предназначена для использования только специалистами по поддержке.

В следующей таблице показаны аргументы для этих параметров.

Табл. 7. Команда clearlog

В следующей однострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Табл. 7. Команда clearlog (продолж.)

Параметр	Описание
-t <all | platform | audit>	Тип событий; выберите тип событий для очистки. Если тип событий не задан, выбираются все типы событий.

Описание типов событий

- all: все типы событий, включая события платформы и события аудита.
- platform: события платформы.
- audit: события аудита.

Пример:
```
system> clearlog
All event log cleared successfully
system> clearlog -t all
All event log cleared successfully
system> clearlog -t platform
Platform event log cleared successfully
system> clearlog -t audit
Audit event log cleared successfully
```

Команда fans

Эта команда служит для отображения скорости вентиляторов сервера.

Используйте команду **fans** для отображения скорости каждого из вентиляторов сервера.

Пример:
```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

Команда ffdc

Эта команда используется для создания нового файла с данными по обслуживанию.

Используйте команду фиксации данных о первом сбое (**ffdc**) для создания и передачи данных по обслуживанию в службу поддержки.

Следующий список состоит из команд, которые следует использовать с командой **ffdc**:

- **generate**, создание нового файла с данными по обслуживанию
- **status**, проверка состояния файла с данными по обслуживанию
- **copy**, копирование существующих данных по обслуживанию
- **delete**, удаление существующих данных по обслуживанию

В следующей таблице показаны аргументы для этих параметров.

Табл. 8. Команда ffdc

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 8. Команда ffdc (продолж.)

Параметр	Описание	Значения
-t	Номер типа	1 (дамп процессора) и 4 (данные по обслуживанию). Дамп процессора содержит все доступные журналы и файлы. Данные по обслуживанию содержат только подмножество журналов и файлов. Значение по умолчанию — 1.
-f [1]	Удаленный каталог имен файлов или целевых объектов sftp.	Для sftp используйте полный путь или конечный / в имени каталога (~/ или /tmp/). Значение по умолчанию — это создаваемое системой имя.
-ip [1]	Адрес сервера tftp/sftp	
-pn [1]	Номер порта сервера TFTP/SFTP	Значение по умолчанию — 69/22.
-u [1]	Имя пользователя для сервера SFTP	
-pw [1]	Пароль для сервера SFTP	
1. Дополнительные аргументы для команд **generate** и **copy**		

Синтаксис:

```
ffdc [options]
option:
  -t 1 or 4
  -f
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

Пример:

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

Команда hreport

Используйте эту команду для отображения встроенного отчета о состоянии.

В следующей таблице показаны команды hreport.

Табл. 9. Команды hreport

В следующей многострочной таблице с двумя столбцами приводятся описания разных команд hreport.

Параметр	Описание
generate	Создание нового отчета о состоянии
status	Проверка состояния
copy	Копирование существующего отчета о состоянии
delete	Удаление существующего отчета о состоянии

В следующей таблице показаны аргументы для параметров generate и copy.

Табл. 10. Команды generate и copy

В следующей многострочной таблице с двумя столбцами приводятся параметры команд generate и copy и описания этих параметров.

Параметр	Описание
-f	Удаленное имя файла или целевой каталог sftp (по умолчанию используется созданное системой имя, для sftp используйте полный путь или конечный / в имени каталога (~/ или /tmp/))
-ip	Адрес сервера tftp/sftp
-pn	Номер порта сервера TFTP/SFTP (по умолчанию 69/22)
-u	Имя пользователя для сервера SFTP
-pw	Пароль для сервера SFTP

команда mhlog

Используйте эту команду для отображения записей в журнале истории обслуживания.

В следующей таблице показаны аргументы для этих параметров.

Табл. 11. Команда mhlog

В следующей многострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Параметр	Описание
-c <count>	Отображение сущностей count (1–250)
-i <index>	Отображение записей, начиная с индекса (1–250)
-f	Удаленное имя файла журнала
-ip	Адрес сервера tftp/sftp

Табл. 11. Команда mhlog (продолж.)

Параметр	Описание
-pn	Номер порта сервера TFTP/SFTP (по умолчанию 69/22)
-u	Имя пользователя для сервера SFTP
-pw	Пароль для сервера SFTP

Пример

На экране отобразится информация, подобная следующей:

```
Type            Message                                                                  Time
-------------   ------------                                                             ----
Hardware        SAS Backplane1(SN: XXXX9CE009L) is added.                               05/08/2020,04:23:18
Hardware        CPU 1(SKU NO: 50844440) is added.                                        05/08/2020,04:23:22
Hardware        CPU 2(SKU NO: 50844440) is added.                                        05/08/2020,04:23:22
Hardware        M2 Card(SN: R1SH9AJ0037) is added.                                       05/08/2020,04:23:22
Firmware        Primary XCC firmware is updated to TGBT99T by XCC Web.                   05/08/2020,06:40:37
Firmware        Primary XCC firmware is activated to TGBT99T .                           05/08/2020,06:41:26
Hardware        PSU1(SN: D1DG94C0075) is added.                                          05/08/2020,06:43:28
```

Команда led

Используйте эту команду для отображения и настройки состояний светодиодных индикаторов.

Команда **led** служит для отображения и настройки состояний светодиодных индикаторов сервера.

- Если выполнить команду **led** без параметров, отобразится состояние светодиодных индикаторов на лицевой панели.
- Параметр команды **led -d** необходимо использовать с параметром команды **led -identify on**.

В следующей таблице показаны аргументы для этих параметров.

Табл. 12. Команда led

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-l	Получение состояния всех светодиодных индикаторов системы и подкомпонентов системы	
-chklog	Выключение светодиодного индикатора журнала проверки	Выкл.
-identify	Светодиодный индикатор идентификации изменения состояния корпуса	Выкл., вкл., мигает
-d	Включение светодиодного индикатора идентификации на заданный период времени	Период времени (в секундах)

Синтаксис:

```
led [options]
option:
  -l
```

-chklog off
-identify *state*
-d *time*

Пример:

```
system> led
Fault                 Off
Identify              On            Blue
Chklog                Off
Power                 Off

system> led -l
Label                 Location                  State         Color
Battery               Planar                    Off
BMC Heartbeat         Planar                    Blink         Green
BRD                   Lightpath Card            Off
Channel A             Planar                    Off
Channel B             Planar                    Off
Channel C             Planar                    Off
Channel D             Planar                    Off
Channel E             Planar                    Off
Chklog                Front Panel               Off
CNFG                  Lightpath Card            Off
CPU                   Lightpath Card            Off
CPU 1                 Planar                    Off
CPU 2                 Planar                    Off
DASD                  Lightpath Card            Off
DIMM                  Lightpath Card            Off
DIMM 1                Planar                    Off
DIMM 10               Planar                    Off
DIMM 11               Planar                    Off
DIMM 12               Planar                    Off
DIMM 13               Planar                    Off
DIMM 14               Planar                    Off
DIMM 15               Planar                    Off
DIMM 16               Planar                    Off
DIMM 2                Planar                    Off
DIMM 3                Planar                    Off
DIMM 4                Planar                    Off
DIMM 5                Planar                    Off
DIMM 6                Planar                    Off
DIMM 7                Planar                    Off
DIMM 8                Planar                    Off
DIMM 9                Planar                    Off
FAN                   Lightpath Card            Off
FAN 1                 Planar                    Off
FAN 2                 Planar                    Off
FAN 3                 Planar                    Off
Fault                 Front Panel (+)           Off
Identify              Front Panel (+)           On            Blue
LINK                  Lightpath Card            Off
LOG                   Lightpath Card            Off
NMI                   Lightpath Card            Off
OVER SPEC             Lightpath Card            Off
PCI 1                 FRU                       Off
PCI 2                 FRU                       Off
PCI 3                 FRU                       Off
PCI 4                 FRU                       Off
Planar                Planar                    Off
Power                 Front Panel (+)           Off
PS                    Lightpath Card            Off
```

```
RAID                    Lightpath Card            Off
Riser 1                 Planar                    Off
Riser 2                 Planar                    Off
SAS ERR                 FRU                        Off
SAS MISSING             Planar                    Off
SP                      Lightpath Card            Off
TEMP                    Lightpath Card            Off
VRM                     Lightpath Card            Off
system>
```

Команда readlog

Эта команда служит для отображения журналов событий IMM.

Используйте команду **readlog** для отображения записей журнала событий IMM. Отображается пять журналов событий одновременно. Записи отображаются в порядке от самых недавних до самых старых.

Команда **readlog** служит для отображения пяти первых записей в журнале событий, начиная с самой недавней, при первом выполнении, а затем следующих пяти для каждого последующего вызова.

Команда **readlog -a** отображает все записи в журнале событий, начиная с самой недавней.

Команда **readlog -f** сбрасывает счетчик и отображает пять первых записей в журнале событий, начиная с самой недавней.

Команда **readlog -date *date*** отображает записи в журнале событий для заданной даты в формате мм/дд/гг. Может представлять собой список дат, разделенных вертикальной чертой (|).

Команда **readlog -sev *severity*** отображает записи в журнале событий для заданного уровня серьезности (E, W, I). Может представлять собой список уровней серьезности, разделенных вертикальной чертой (|).

Команда **readlog -i *ip_address*** задает адрес IPv4 или IPv6 IP сервера TFTP или SFTP, на котором сохранен журнал событий. Параметры команд **-i** и **-l** используются вместе для указания местоположения.

Команда **readlog -l *filename*** задает имя файла журнала событий. Параметры команд **-i** и **-l** используются вместе для указания местоположения.

readlog -pn *port_number* отображает или задает номер порта сервера TFTP или SFTP (значение по умолчанию: 69/22).

Команда **readlog -u *username*** задает имя пользователя для сервера SFTP.

Команда **readlog -pw *password*** задает пароль для сервера SFTP.

Синтаксис:

```
readlog [options]
option:
  -a
  -f
  -date date
  -sev severity
  -i ip_address
  -l filename
  -pn port_number
  -u username
  -pw password
```

Пример:

```
system> readlog -f
```

```
1 I 2017-06-17T09:31:59.217  Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685  Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581  Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5  I 2017-06-16T10:40:14.352  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

Команда syshealth

Эта команда позволяет получить сводку состояния или активных событий.

Используйте команду **syshealth** для отображения сводки состояния или активных событий на сервере. Отображаются следующие показатели: состояние питания, состояние системы, состояние оборудования (в том числе вентилятора, блока питания, устройств хранения, процессора и памяти), число перезапусков и состояние программного обеспечения IMM.

Синтаксис:

```
syshealth [argument]
argument:
  summary      -display the system health summary
  activeevents -display active events
  cooling - display cooling devices health status
  power - display power modules health status
  storage - display local storage health status
  processors - display processors health status
  memory - display memory health status
```

Пример:

```
system> syshealth summary
Power    On
State    OS booted
Restarts 29

system> syshealth activeevents
No Active Event Available!
```

Команда temps

Эта команда позволяет отобразить все сведения о температуре и пороговых значениях температуры.

Используйте команду **temps**, чтобы отобразить все показатели и пороговые значения температуры. Отображается тот же набор температурных значений, что и в веб-интерфейсе.

```
Example
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

         WR       W       T       SS      HS
-------------------------------------------
CPU1     N/A     N/A    80/27    N/A     N/A
CPU2     N/A     N/A    80/27    N/A     N/A
DASD1   66/19   73/23   82/28   88/31   92/33
Amb     59/15   70/21   83/28   90/32   95/35
system>
```

Примечания:

1. Выходные данные отображаются в столбцах со следующими заголовками:

   WR: сброс с предупреждением (движущийся в положительном направлении пороговый гистерезис)

   W: предупреждение (верхний некритический порог)

   T: температура (текущее значение)

   SS: мягкое выключение (верхний критический порог)

   HS: жесткое выключение (верхний невосстанавливаемый порог)
2. Все значения температуры указаны в градусах (F/C).
3. НД означает «недоступно».

Команда volts

Используйте эту команду для отображения сведений о напряжении на сервере.

Используйте команду **volts**, чтобы отобразить все показатели и пороговые значения напряжения. Отображается тот же набор значений напряжения, что и в веб-интерфейсе.

```
Example:
system> volts

     i HSL    SSL    WL     WRL    V      WRH    WH     SSH     HSH
-----------------------------------------------------------------
5v     5.02   4.00   4.15   4.50   4.60   5.25   5.50   5.75    6.00
3.3v   3.35   2.80   2.95   3.05   3.10   3.50   3.65   3.70    3.85
12v    12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40  12.65
-5v    -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40  -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80  -2.70
VRM1                          3.45
VRM2                          5.45
system>
```

Примечание: Выходные данные отображаются в столбцах со следующими заголовками:

HSL: жесткое выключение на нижнем пороге (нижний невосстанавливаемый порог)

SSL: мягкое выключение на нижнем пороге (нижний критический порог)

WL: предупреждение на нижнем пороге (нижний некритический порог)

WRL: сброс с предупреждением на нижнем пороге (движущийся в отрицательном направлении пороговый гистерезис)

V: напряжение (текущее значение)

WRH: сброс с предупреждением на верхнем пороге (движущийся в положительном направлении пороговый гистерезис)

WH: предупреждение на верхнем пороге (верхний некритический порог)

SSH: мягкое выключение на верхнем пороге (верхний критический порог)

HSH: жесткое выключение на верхнем пороге (верхний невосстанавливаемый порог)

Команда vpd

Эта команда позволяет отобразить данные о конфигурации и информационные сведения (важные данные продуктов, VPD), связанные с оборудованием и программным обеспечением сервера.

Воспользуйтесь командой **vpd**, чтобы отобразить важные данные продуктов о системе (sys), IMM (bmc), BIOS сервера (uefi), Lenovo XClarity Provisioning Manager (lxpm), микропрограммы сервера (fw), серверных компонентов (comp) и устройств PCIe (pcie). Отображается та же информация, что и в веб-интерфейсе.

Синтаксис:

```
vpd sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw   - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

Пример:

```
system> vpd bmc
Type            Status       Version      Build      ReleaseDate
----            -------       -----       ------
BMC (Primary)   Active       0.00        DVI399T    2017/06/06
BMC (Backup)    Inactive     1.00        TEI305J    2017/04/13

system>
```

Команды управления питанием и перезапуском сервера

В этом разделе приводится алфавитный список команд интерфейса командной строки для управления питанием и перезапуском.

В настоящее время доступно 4 команды управления питанием и перезапуском сервера:

Команда power

Эта команда описывает, как контролировать питание сервера.

Используйте команду **power** для управления питанием сервера. Чтобы создавать команды **power** необходимо обладать полномочиями на удаленный доступ к питанию и перезапуску сервера.

В следующей таблице представлено подмножество команд, которые можно использовать с командой **power**.

Табл. 13. Команда power

В следующей многострочной таблице с тремя столбцами приводятся команды power, их описание и соответствующие значения.

Команда	Описание	Значение
питание включено	Используйте эту команду для включения питания сервера.	вкл., выкл.
power off	Используйте эту команду для выключения питания сервера. **Примечание:** Параметр **-s** выключает операционную систему до выключения сервера.	вкл., выкл.
цикл электропитания	Используйте эту команду для выключения и последующего включения питания сервера. **Примечание:** Параметр **-s** выключает операционную систему до выключения сервера.	
power enterS3	Используйте эту команду для перевода операционной системы в режим S3 (сна). **Примечание:** Эта команда используется, только если операционная система включена. Режим S3 поддерживается не на всех серверах.	
power rp	Используйте этот параметр для настройки политики восстановления питания хоста.	alwayson|alwaysoff|restore
power S3resume	Используйте эту команду для вывода операционной системы из режима S3 (сна). **Примечание:** Эта команда используется, только если операционная система включена. Режим S3 поддерживается не на всех серверах.	
power state	Используйте эту команду для отображения состояния питания сервера и текущего состояния сервера.	вкл., выкл.

В следующей таблице представлены параметры для команд **power on**, **power off** и **power cycle**.

Табл. 14. Команда power

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Пара-метр	Описание	Значения
-s	Используйте этот параметр для выключения операционной системы до выключения сервера. **Примечание:** Параметр **-s** подразумевается при использовании параметра **-every** для команд **power off** и **power cycle**.	
-every	Используйте этот параметр с командами **power on**, **power off** и **power cycle** для управления электропитанием сервера. Можно настроить даты, время и периодичность (ежедневно или еженедельно) включения, выключения и выключения и последующего включения сервера.	**Примечание:** Значения для этого параметра представлены на отдельных строках из-за ограниченного пространства. Sun|Mon|Tue|Wed|Thu| Fri|Sat|Day|clear

Табл. 14. Команда power (продолж.)

Пара-метр	Описание	Значения
-t	Используйте этот параметр, чтобы указать время (в часах и минутах) включения сервера, выключения операционной системы и выключения и перезапуска сервера.	Используйте значения в следующем формате: чч:мм
-d	Используйте этот параметр, чтобы указать дату включения сервера. Это дополнительный параметр для команды **power on**. **Примечание:** Параметры **-d** и **-every** невозможно одновременно использовать с одной и той же командой.	Используйте значения в следующем формате: мм/дд/гггг
-clear	Используйте этот параметр, чтобы удалить запланированную дату включения. Это дополнительный параметр для команды **power on**.	

Синтаксис:
```
power on
power off [-s]
power state
power cycle [-s]
```

Ниже представлены примеры использования команды **power**.

Чтобы выключать операционную систему и сервер каждое воскресенье в 1:30, введите следующую команду:
```
system> power off
-every Sun -t 01:30
```

Чтобы выключать операционную систему и перезапускать сервер каждый день в 1:30, введите следующую команду:
```
system> power cycle
-every Day -t 01:30
```

Чтобы включать сервер каждый понедельник в 1:30, введите следующую команду:
```
system> power on
-every Mon -t 13:00
```

Чтобы включить сервер 31 декабря 2013 года в 23:30, введите следующую команду:
```
system> power on
-d 12/31/2013 -t 23:30
```

Чтобы очистить еженедельный цикл выключения и включения, введите следующую команду:
```
system> power cycle
-every clear
```

Команда reset

Эта команда описывает, как выполнить сброс сервера.

Используйте команду **reset** для перезапуска сервера. Для использования этой команды у вас должны быть полномочия на управление питанием и перезапуском системы.

В следующей таблице показаны аргументы для этих параметров.

Табл. 15. Команда reset

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-s	Выключение операционной системы перед сбросом сервера.	
-d	Задержка сброса на указанное количество секунд.	0 - 120
-nmi	Создание немаскируемого прерывания (NMI) на сервере.	

Синтаксис:
```
reset [option]
option:
-s
-d
-nmi
```

Команда fuelg

Эта команда служит для отображения информации о питании сервера.

Используйте команду **fuelg** для отображения информации об использовании питания сервера и настройки управления питанием сервера. Эта команда также служит для настройки политик на случай утери резерва питания. В следующей таблице показаны аргументы для этих параметров.

Табл. 16. Команда fuelg

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-pme	Включение и выключение управления электропитанием и ограничения мощности на сервере.	вкл., выкл.
-pcapmode	Настройка режима ограничения питания для сервера.	вход, выход
-pcap	Числовое значение в диапазоне значений ограничения питания, отображаемое при выполнении команды fuelg без параметров на целевом объекте.	числовое значение мощности (Вт)
-history	Отображение энергопотребления или журнала производительности	ПК, производительность
-period	Числовое значение для отображения журнала (1 час, 6 часов, 12 часов, 24 часа)	числовое значение в часах

Табл. 16. Команда fuelg (продолж.)

Параметр	Описание	Значения
-pm	Настройка режима политики на случай утери резерва питания.	• **bt**- базовый с регулированием • **rt**- резервирование с регулированием (по умолчанию) • **ort**- резервирование N_1 с регулированием
-zm	Включение или отключение режима нулевого вывода. Этот параметр можно настроить, только если в качестве режима политики выбрано резервирование с регулированием.	вкл., выкл.
-perf	Отображение информации о текущем использовании вычислительных ресурсов, включая систему, микропроцессор и ввод-вывод.	процент
-pc	Отображение текущего потребления питания	• **output**- отображение текущего потребления постоянного тока. Для стоечных и башенных серверов этот параметр включает энергопотребление системы, ЦП, памяти и других компонентов. Для блейд-серверов ITE параметр включает только энергопотребление системы. • **input**- отображение текущего входного энергопотребления, включая энергопотребление системы.

Синтаксис:
```
fuelg [options]
option:
  -pme on|off
  -pcapmode input|output
  -pcap
  -history
  -period
  -pm bt|r|rt
  -zm on|off
  -perf
  -pc input|output
```

Пример:
```
system> fuelg
-pme: on
system>
```

Команда pxeboot

Эта команда служит для отображения и настройки условия среды Preboot eXecution Environment.

Если выполнить команду **pxeboot** без параметров, вернется текущая настройка Preboot eXecution Environment. В следующей таблице показаны аргументы для этих параметров.

Табл. 17. Команда pxeboot

В следующей однострочной таблице с тремя столбцами приводится параметр, описание параметра и соответствующие значения для этого параметра.

Параметр	Описание	Значения
-en	Задает условие среды Preboot eXecution Environment для следующего перезапуска системы.	включено, выключено

Синтаксис:
```
pxeboot [options]
option:
  -en state
```

Пример:
```
system> pxeboot
-en disabled
system>
```

Команда serial redirect

В этом разделе содержится команда serial redirect.

Доступна лишь одна команда serial redirect: «Команда console» на странице 118.

Команда console

Эта команда используется для запуска сеанса консоли последовательного перенаправления.

Используйте команду **console** для запуска сеанса консоли последовательного перенаправления на указанном последовательном порту модуля IMM.

Синтаксис:
```
console 1
```

Команды конфигурации

В этом разделе приводится алфавитный список команд конфигурации интерфейса командной строки.

В настоящее время доступна 41 команда конфигурации:

Команда accseccfg

Используйте эту команду для отображения и настройки параметров безопасности учетной записи.

Если выполнить команду **accseccfg** без параметров, отобразятся все сведения о безопасности учетных записей. В следующей таблице показаны аргументы для этих параметров.

Табл. 18. Команда accseccfg

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 18. Команда accseccfg (продолж.)

Параметр	Описание	Значения
-am	Задает метод аутентификации пользователей.	local, ldap, localldap, ldaplocal
-lp	Период блокировки после максимального числа ошибок при входе (в минутах).	От 0 до 2880, 0 = срок действия периода блокировки неограничен
-pe	Период истечения срока действия пароля (в днях).	От 0 до 365, 0 = никогда не истекает
-pew	Период времени предупреждения об истечении срока действия пароля **Примечание:** Период предупреждения об истечении срока действия пароля должен быть меньше периода истечения срока действия пароля.	От 0 до 30, 0 = никогда не предупреждать
-pc	Включены правила сложности паролей.	вкл., выкл.
-pl	Длина пароля.	Если правила сложности паролей включены, длина пароля должна составлять от 8 до 32 символов. В противном случае он должен включать от 0 до 32 символов.
-ci	Минимальный интервал изменения пароля (в часах).	От 0 до 240, 0 = изменить сразу же
-lf	Максимальное число ошибок при входе.	От 0 до 10, 0 = никогда не блокировать
-chgdft	Изменение пароля по умолчанию после первого входа.	вкл., выкл.
-chgnew	Изменение пароля нового пользователя после первого входа.	вкл., выкл.
-rc	Цикл повторного использования пароля.	От 0 до 10, 0 = повторно использовать сразу же
-wt	Тайм-аут сеанса после неактивности в Интернете и Secure Shell (в минутах).	От 0 до 1440

Syntax:

```
accseccfg [options]
option:
   -legacy
   -high
   -custom
   -am authentication method
   -lp lockout_period
   -pe time_period
   -pr state
   -pc state
   -pd number_characters
   -pl number_characters
   -ci minimum_interval
   -lf number_failures
   -chgdft state
   -chgnew state
   -rc reuse_cycle
   -wt timeout
```

Пример:

```
system> accseccfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

Команда alertcfg

Используйте эту команду для отображения и настройки глобальных параметров удаленного оповещения IMM.

Если выполнить команду **alertcfg** без параметров, отобразятся все глобальные параметры удаленных оповещений. В следующей таблице показаны аргументы для этих параметров.

Табл. 19. Команда alertcfg

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 19. Команда alertcfg (продолж.)

Параметр	Описание	Значения
-dr	Задает время ожидания между повторными попытками отправки оповещения модулем IMM.	от 0 до 4 минут шагами по 0,5 минут
-da	Задает время ожидания до того, как IMM отправит оповещение следующему получателю в списке.	от 0 до 4 минут шагами по 0,5 минут
-rl	Задает количество дополнительных попыток отправки оповещения модулем IMM, если предыдущие попытки оказались безуспешными.	от 0 до 8

Синтаксис:
```
alertcfg [options]
  options:
   -rl retry_limit
   -dr retry_delay
   -da agent_delay
```

Пример:
```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

Команда asu

Эта команда используется для настройки параметров UEFI.

Команды программы Advanced Settings Utility служат для настройки параметров UEFI. Чтобы изменения параметров UEFI вступили в силу, основную систему необходимо перезагрузить.

В следующей таблице представлено подмножество команд, которые можно использовать с командой **asu**.

Табл. 20. Команда asu

В следующей многострочной таблице с тремя столбцами приводится подмножество команд, которые могут использоваться вместе с командой **asu**. Предоставляются описательные сведения и соответствующие значения команд.

Команда	Описание	Значение
delete	Используйте эту команду для удаления экземпляра или записи настройки. Эта настройка должна представлять собой экземпляр с возможностью удаления, например iSCSI.AttemptName.1.	*setting_instance*
справка	Используйте эту команду для отображения справочных сведений для одной или нескольких настроек.	*setting*

Табл. 20. Команда asu (продолж.)

Команда	Описание	Значение
set	Используйте эту команду для изменения значения настройки. Задание входного значения для параметров UEFI. **Примечания:** • Настройка одной или нескольких пар «параметр/значение». • Если эта настройка расширяется до отдельной настройки, она может содержать подстановочные символы. • Если значение содержит пробелы, оно должно быть заключено в кавычки. • Упорядоченные списки значений разделяются знаком «равно» (=). Например, set B*.Bootorder «CD/DVD Rom=Hard Disk 0=PXE Network.»	*значение настройки*
showgroups	Используйте эту команду для отображения доступных групп настроек. Эта команда служит для отображения названий известных групп. Названия групп могут варьироваться в зависимости от установленных устройств.	*setting*
show	Используйте эту команду для отображения текущего значения одной или нескольких настроек.	*setting*
showvalues	Используйте эту команду для отображения всех возможных значений одной или нескольких настроек. **Примечания:** • Эта команда отобразит сведения о допустимых значениях этой настройки. • Отобразится минимальное и максимальное количество допустимых экземпляров для этой настройки. • Если доступно, отобразится значение по умолчанию. • Значение по умолчанию заключено в треугольные скобки (< и >). • Текстовые значения показывают минимальную и максимальную длину и регулярное выражение.	*setting*
Примечания: • В синтаксисе команды *setting* — это название настройки, которое требуется просмотреть или изменить, а *value* — это значение, которое присваивается настройке. • *Setting* может выражаться несколькими именами (кроме случаев, когда используется команда **set**). • *Setting* может содержать подстановочные символы, например звездочку (*) или знак вопроса (?). • *Setting* может представлять собой группу, название настройки или **all**.		

Примеры синтаксиса команды **asu** представлены в следующем списке:

- Чтобы отобразить все параметры команды asu, введите `asu --help`.
- Чтобы отобразить подробную справку для всех команд, введите `asu -v --help`.
- Чтобы отобразить подробную справку для одной команды, введите `asu -v set --help`.

- Чтобы изменить значение, введите `asu set` *setting value*.
- Чтобы отобразить текущее значение, введите `asu show` *setting*.
- Чтобы отобразить параметры в длинном пакетном формате, введите `asu show -l -b all`
- Чтобы отобразить все возможные значения настройки, введите `asu showvalues` *setting*. Пример команды **show values**:
```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

В следующей таблице показаны аргументы для этих параметров.

Табл. 21. Параметры asu

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	**Описание**	**Значения**
-b	Отображение в пакетном формате.	
--справка[1]	Отображение сведений об использовании команды и параметров. Параметр --help размещается перед командой, например **asu --help show**.	
--справка[1]	Отображение справки для команды. Параметр --help размещается после команды, например **asu show --help**.	
-l	Имя настройки в длинном формате (включает заданную конфигурацию).	
-m	Имя настройки в смешанном формате (включает идентификатор конфигурации).	
-v[2]	Подробные выходные данные.	
1. Параметр --help может использоваться с любой командой. 2. Параметр -v можно поместить только между **asu** и командой.		

Синтаксис:
```
asu [options] command [cmdopts]
options:
   -v verbose output
   --help display main help
cmdopts:
   --help help for the command
```

Примечание: См. дополнительные параметры команд в разделах, посвященных отдельным командам.

Используйте команды транзакций asu для настройки нескольких параметров UEFI и создания и выполнения команд в пакетном режиме. Используйте команды **tropen** и **trset** для создания файла

транзакций с несколькими применяемыми настройками. Транзакция с заданным идентификатором открывается по команде **tropen**. Параметры добавляются в набор по команде **trset**. Выполненная транзакция фиксируется по команде **trcommit**. Завершив работу с транзакцией, можно удалить ее с помощью команды **trrm**.

Примечание: Операция восстановления параметров UEFI создаст транзакцию с идентификатором, используя произвольный трехзначный номер.

В следующей таблице представлены команды транзакций, которые можно использовать с командой **asu**.

Табл. 22. Команды транзакций asu

В следующей многострочной таблице с тремя столбцами приводятся команды транзакций, их описание и соответствующие значения.

Команда	Описание	Значение
tropen *id*	Эта команда создает новый файл транзакций с несколькими доступными для настройки параметрами.	*Id* — это идентифицирующая строка, которая может содержать от 1 до 3 буквенно-числовых символов.
trset *id*	Эта команда добавляет в транзакцию один или несколько параметров или пар значений.	*Id* — это идентифицирующая строка, которая может содержать от 1 до 3 буквенно-числовых символов.
trlist *id*	Эта команда отображает содержимое файла транзакции на первом месте. Это полезно, если файл транзакции создан в оболочке интерфейса командной строки.	*Id* — это идентифицирующая строка, которая может содержать от 1 до 3 буквенно-числовых символов.
trcommit *id*	Эта команда фиксирует и выполняет содержимое файла транзакции. Отображаются результаты выполнения и любые ошибки.	*Id* — это идентифицирующая строка, которая может содержать от 1 до 3 буквенно-числовых символов.
trrm *id*	Эта команда удаляет файл транзакции после фиксации.	*Id* — это идентифицирующая строка, которая может содержать от 1 до 3 буквенно-числовых символов.

Пример настройки нескольких параметров UEFI:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

Команда backup

Используйте эту команду для создания резервного файла, содержащего текущие параметры безопасности системы.

В следующей таблице показаны аргументы для этих параметров.

Табл. 23. Команда backup

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-f	Имя резервного файла	Допустимое имя файла
-pp	Пароль или фраза-пароль, используемые для шифрования паролей внутри резервного файла	Допустимый пароль или фраза-пароль с разделителями в виде кавычек
-ip	IP-адрес сервера TFTP/SFTP	Допустимый IP-адрес
-pn	Номер порта сервера TFTP/SFTP	Допустимый номер порта (по умолчанию 69/22)
-u	Имя пользователя для сервера SFTP	Допустимое имя пользователя
-pw	Пароль для сервера SFTP	Допустимый пароль
-fd	Имя файла XML-описания команд интерфейса командной строки для резервного копирования	Допустимое имя файла

Синтаксис:

```
backup [options]
  option:
   -f    filename
   -pp   password
   -ip   ip address
   -pn   port number
   -u    username
   -pw   password
   -fd   filename
```

Пример:

```
system> backup f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

Команда dhcpinfo

Используйте эту команду для просмотра назначенной сервером DHCP IP-конфигурации для eth0.

Используйте команду **dhcpinfo** для просмотра назначенной сервером DHCP IP-конфигурации для eth0, если интерфейс настраивается автоматически сервером DHCP. Для включения и отключения DHCP можно использовать команду **ifconfig**.

Синтаксис:

```
dhcpinfo eth0
```

```
Example:
system> dhcpinfo eth0
   -server :  10.240.0.10
   -n      :  XCC-7X19-123456789A
   -i      :  10.243.4.66
   -i6     :  ::
   -g      :  10.243.0.1
   -s      :  255.255.240.0
   -d      :  labs.lenovo.com
   -d6     :
   -dns1   :  10.240.0.10
   -dns2   :  10.240.0.11
   -dns3   :  0.0.0.0
   -dns61  :  ::
   -dns62  :  ::
   -dns63  :  ::
```

В следующей таблице приводятся выходные данные из этого примера.

Табл. 24. Команда dhcpinfo

В следующей многострочной таблице с двумя столбцами описаны параметры, использованные в предыдущем примере.

Параметр	**Описание**
-server	Сервер DHCP, назначивший конфигурацию
-n	Назначенное имя хоста
-i	Назначенный адрес IPv4
-g	Назначенный адрес шлюза
-s	Назначенная маска подсети
-d	Назначенное доменное имя
-dns1	Основной IP-адрес IPv4 сервера DNS
-dns2	Дополнительный IP-адрес IPv4 сервера DNS
-dns3	Третий IP-адрес IPv4 сервера DNS
-i6	Адрес IPv6
-d6	Доменное имя IPv6
-dns61	Основной IP-адрес IPv6 сервера DNS
-dns62	Дополнительный IP-адрес IPv6 сервера DNS
-dns63	Третий IP-адрес IPv6 сервера DNS

Команда dns

Используйте эту команду для просмотра и настройки DNS-конфигурации IMM.

Примечание: В системе Flex System невозможно изменить параметры DNS для IMM. Модуль CMM управляет параметрами DNS.

Если выполнить команду **dns** без параметров, отобразятся все сведения о конфигурации DNS. В следующей таблице показаны аргументы для этих параметров.

Табл. 25. Команда dns

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-state	Состояние DNS	вкл., выкл.
-ddns	Состояние DDNS	включено, выключено
-i1	Основной IP-адрес IPv4 сервера DNS	IP-адрес в десятичном формате IP-адресов с точкой.
-i2	Дополнительный IP-адрес IPv4 сервера DNS	IP-адрес в десятичном формате IP-адресов с точкой.
-i3	Третий IP-адрес IPv4 сервера DNS	IP-адрес в десятичном формате IP-адресов с точкой.
-i61	Основной IP-адрес IPv6 сервера DNS	IP-адрес в формате IPv6.
-i62	Дополнительный IP-адрес IPv6 сервера DNS	IP-адрес в формате IPv6.
-i63	Третий IP-адрес IPv6 сервера DNS	IP-адрес в формате IPv6.
-p	Приоритет IPv4/IPv6	ipv4, ipv6

Синтаксис:
```
dns [options]
option:
  -state state
  -ddns state
  -i1 first_ipv4_ip_address
  -i2 second_ipv4_ip_address
  -i3 third_ipv4_ip_address
  -i61 first_ipv6_ip_address
  -i62 second_ipv6_ip_address
  -i63 third_ipv6_ip_address
  -p priority
```

Примечание: В следующем примере показана конфигурация IMM с выключенной службой DNS.

Пример:
```
system> dns
   -state   :  disabled
   -i1      :  0.0.0.0
   -i2      :  0.0.0.0
   -i3      :  0.0.0.0
   -i61     :  ::
   -i62     :  ::
   -i63     :  ::
   -ddns    :  enabled
   -dnsrc   :  DHCP
   -ddn     :
   -ddncur  :  labs.lenovo.com
   -p       :  ipv6
   -dscvry  :  enabled

system>
```
В следующей таблице описаны параметры, использованные в предыдущем примере.

Табл. 26. вывод команды dns

В следующей многострочной таблице с двумя столбцами описаны параметры, использованные в предыдущем примере.

Параметр	Описание
-state	Состояние DNS (`on` или `off`)
-i1	Основной IP-адрес IPv4 сервера DNS
-i2	Дополнительный IP-адрес IPv4 сервера DNS
-i3	Третий IP-адрес IPv4 сервера DNS
-i61	Основной IP-адрес IPv6 сервера DNS
-i62	Дополнительный IP-адрес IPv6 сервера DNS
-i63	Третий IP-адрес IPv6 сервера DNS
-ddns	Состояние DDNS (`enabled` или `disabled`)
-dnsrc	Предпочтительное доменное имя (`dhcp` или `manual`)
-ddn	Указанный вручную DDN
-ddncur	Текущий DDN (только чтение)
-p	Предпочтительные серверы DNS (`ipv4` или `ipv6`)

Команда encaps

Используйте эту команду, чтобы позволить BMC выйти из режима инкапсуляции.

В следующей таблице показаны аргументы для этих параметров.

Табл. 27. Команда encaps

В следующей однострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Параметр	Описание
lite off	Предоставление BMC возможности выйти из режима инкапсуляции и открыть глобальный доступ для всех пользователей

Команда ethtousb

Воспользуйтесь командой **ethtousb** для отображения и настройки сопоставления портов Ethernet и Ethernet через USB.

Эта команда позволяет сопоставить номер внешнего порта Ethernet другому номеру порта для интерфейса Ethernet через USB.

Если выполнить команду **ethtousb** без параметров, отобразятся сведения об интерфейсе Ethernet через USB. В следующей таблице показаны аргументы для этих параметров.

Табл. 28. Команда ethtousb

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-en	Состояние интерфейса Ethernet через USB	включено, выключено
-m*x*	Настройка сопоставления портов для индекса *x*	Пара портов, разделяемая двоеточием (:), в формате *port1:port2* Где: • Номер индекса порта *x* задается в виде целого числа от 1 до 10 в параметре команды. • *port1* пары портов — это номер внешнего порта Ethernet. • *port2* пары портов — это номер порта Ethernet через USB.
-rm	Удаление сопоставления портов для заданного индекса	от 1 до 10 Индексы сопоставления портов отображаются с помощью команды **ethtousb** без параметров.

Синтаксис:
```
ethtousb [options]
option:
  -en state
  -mxport_pair
  -rm map_index
```

Пример:
```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
system>
```

Команда firewall

Используйте эту команду для настройки брандмауэра, чтобы ограничить доступ с определенных адресов и при необходимости ограничить временной период доступа. Если параметр не задан, будут отображаться текущие параметры.

В следующей таблице показаны аргументы для этих параметров.

Табл. 29. Команда firewall

В следующей многострочной таблице с тремя столбцами приводятся параметры этой команды и соответствующие описания.

Табл. 29. Команда firewall (продолж.)

Параметр	Описание	Значения
-bips	1–3 IP-адреса блока (разделенные запятой, CIDR или диапазон)	Допустимые IP-адреса **Примечание:** Для адресов IPv4 и IPv6 можно использовать формат CIDR, чтобы заблокировать диапазон адресов.
-bmacs	Блокировка 1–3 MAC-адресов (разделенных запятой)	Допустимые MAC-адреса **Примечание:** Фильтрация MAC-адресов работает только с определенными адресами.
-bbd	Дата начала блока	Дата в формате <ГГГГ-ММ-ДД>
-bed	Дата окончания блока	Дата в формате <ГГГГ-ММ-ДД>
-bbt	Время начала блока	Время в формате <ЧЧ:ММ>
-bet	Время окончания блока	Время в формате <ЧЧ:ММ>
-bti	Блокировка 1–3 временных интервалов (разделенных запятой) Например, если задано значение *firewall - bti 01:00–02:00,05:05–10:30*, доступ будет заблокирован ежедневно с 01:00 до 02:00 и с 05:05 до 10:30	Диапазон времени в формате <ЧЧ:ММ-ЧЧ:ММ>
-clr	Очистка правила брандмауэра для определенного типа	ip, mac, datetime, interval, all
Следующие параметры предназначены для блокировки IP-адресов		
-iplp	Период блокировки IP-адресов минутах.	Числовое значение от 0 до 2880, 0 = никогда не истекает
-iplf	Максимальное количество ошибок при входе в систему, прежде чем IP-адрес будет заблокирован. **Примечание:** Если значение отлично от 0, оно должно быть больше или равно значению параметра <Максимальное количество ошибок при входе в систему>, которое устанавливается командой <*accseccfg -lf*>	Числовое значение от 0 до 32, 0 = никогда не блокировать
-ipbl	Отображение/настройка списка блокируемых IP-адресов.	del, clrall, show • **-del**: удаление адреса IPv4 или IPv6 из списка блокировки • **-clrall**: очистить все блокируемые IP-адреса • **-show**: показать все блокируемые IP-адреса

Пример:

```
· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips  192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.
· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
```

· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”: Delete all blocking IP addresses.
· “firewall –ipbl –show”:   Show all blocking IP addresses.

Команда gprofile

Используйте эту команду для отображения и настройки групповых профилей для IMM.

В следующей таблице показаны аргументы для этих параметров.

Табл. 30. Команда gprofile

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-clear	Удаление группы	включено, выключено
-n	Имя группы	Строка *group_name* длиной до 63 символов. Значение *group_name* должно быть уникальным.
-a	Уровень полномочий в зависимости от роли	администратор, оператор, <список ролей> rbs: nsc|am|rca|rcvma|pr|bc|cel|ac Значения ролей указываются в виде списка разделенных вертикальными чертами значений.
-h	Отображение сведений об использовании команды и параметров	

Синтаксис:
```
gprofile [1 - 16 group_profile_slot_number] [options]
options:
-clear state
-n  group_name
-a  authority level:
    -nsc network and security
    -am user account management
    -rca remote console access
    -rcvma remote console and remote disk access
    -pr remote server power/restart access
    -bc basic adapter configuration
    -cel ability to clear event logs
    -ac advanced adapter configuration
-h help
```

Команда hashpw

Используйте эту команду с параметром -sw для включения/отключения функции стороннего пароля или с параметром -re для включения/отключения возможности получения стороннего пароля.

В следующей таблице показаны аргументы для этих параметров.

Табл. 31. Команда hashpw

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 31. Команда hashpw (продолж.)

Параметр	Описание	Значения
-sw	Состояние переключателя стороннего пароля	включено, выключено
-re	Состояние чтения стороннего пароля **Примечание:** Если переключатель включен, можно настроить чтение.	включено, выключено

Пример:

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f -a super
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account      Login ID      Advanced Attribute               Role            Password Expires
 -------      --------      ------------------              ------           ----------------
    1           USERID                   Native                 Administrator      Password doesn't expire
5           guest5    Third-party Password              Administrator                  90 day(s)
```

Команда ifconfig

Используйте эту команду для настройки интерфейса Ethernet.

Введите `ifconfig eth0`, чтобы отобразить текущую конфигурацию интерфейса Ethernet. Чтобы изменить конфигурацию интерфейса Ethernet, введите параметры, за которыми следуют их значения. Чтобы изменить конфигурацию интерфейса, необходимо обладать по меньшей мере правами настройки сетевых параметров и безопасности адаптера.

Примечание: В системе Flex System параметры виртуальной локальной сети контролируются CMM Flex System и не могут быть изменены в IMM.

В следующей таблице показаны аргументы для этих параметров.

Табл. 32. Команда ifconfig

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-b	Записанный MAC-адрес (только чтение, не настраивается)	
-state	Состояние интерфейса	выключено, включено
-c	Метод конфигурации	dhcp, static, dthens (dthens соответствует параметру **используйте dhcp-сервер, в случае сбоя используйте статическую конфигурацию** в веб-интерфейсе)
-i	Статический IP-адрес	Адрес в допустимом формате.
-g	Адрес шлюза	Адрес в допустимом формате.
-s	Маска подсети	Адрес в допустимом формате.
-n	Имя хоста	Строка длиной до 63 символов. Строка может содержать буквы, цифры, точки, нижние подчеркивания и дефисы.

Табл. 32. Команда ifconfig (продолж.)

Параметр	Описание	Значения
-r	Скорость обмена данными	10, 100, авто
-d	Дуплексный режим	полный, половинный, авто
-m	MTU	Число в диапазоне от 60 до 1500.
-l	LAA	Формат MAC-адреса. Адреса многоадресной рассылки использовать запрещено (первый байт должен быть четным).
-dn	Доменное имя	Доменное имя в допустимом формате.
-auto	Параметр автоматического согласования, определяющий доступность для настройки сетевых параметров «Скорость передачи данных» и «Дуплексный режим».	true, false
-ghn	Получение имени хоста из DHCP	выключено, включено
-nic	переключение режима NIC[1]	shared, dedicated, shared:nixX[2]
-failover[2]	Режим аварийного переключения	none, shared, shared:nicX
-nssync[3]	Синхронизация сетевых параметров	включено, выключено
-address_table	Таблица автоматически генерируемых адресов IPv6 с указанием длины префикса **Примечание:** Этот параметр отображается, только если включены IPv6 и безагентская автоматическая конфигурация.	Это значение доступно только для чтения и не может быть настроено.
-ipv6	Состояние IPv6	выключено, включено
-lla	Локальный адрес канала **Примечание:** Локальный адрес канала отображается, только если IPv6 включен.	Локальный адрес канала определяется IMM. Это значение доступно только для чтения и не может быть настроено.
-ipv6static	Состояние статического IPv6	выключено, включено
-i6	Статический IP-адрес	Статический IP-адрес для канала Ethernet 0 в формате IPv6.
-p6	Длина префикса адреса	Число в диапазоне от 1 до 128.
-g6	Шлюз или маршрут по умолчанию	IP-адрес для шлюза или маршрута по умолчанию канала Ethernet 0 в IPv6.
-dhcp6	Состояние DHCPv6	включено, выключено
-sa6	Состояние безагентской автоматической конфигурации IPv6	включено, выключено
-vlan	Включение или выключение меток виртуальной локальной сети	включено, выключено

Табл. 32. Команда ifconfig (продолж.)

Параметр	Описание	Значения
-vlanid	Метка идентификации сетевых пакетов для IMM	Число в диапазоне от 1 до 4094.

Примечания:

1. -nic также показывает состояние nic. [active] указывает, какую карту nic использует XCC в данный момент

   Например:
   ```
   -nic: shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot 5 [active]
   ```
   Указывает, что nic3 находится в общем режиме в гнезде 5, nic2 — в гнезде slot3, nic1 является выделенным портом XCC, а XCC использует nic3.
2. Значение shared:nicX доступно на серверах с установленной дополнительной мезонинной сетевой картой. Мезонинная сетевая карта может использоваться модулем IMM.
3. Если модуль IMM настроен для использования выделенного сетевого порта управления, параметр -failover укажет модулю IMM, что необходимо переключиться на общий сетевой порт, если выделенный порт отключен.
4. Если режим отработки отказа включен, параметр -nssync указывает модулю IMM, что необходимо использовать в общем сетевом порте те же сетевые параметры, что и в выделенном сетевом порте управления.

Синтаксис:

```
ifconfig eth0 [options]
options:

  -state interface_state
  -c config_method
  -i static_ipv4_ip_address
  -g ipv4_gateway_address
  -s subnet_mask
  -n hostname
  -r data_rate
  -d duplex_mode
  -m max_transmission_unit
  -l locally_administered_MAC
  -b burned_in_MAC_address
  -dn domain_name
  -auto state
  -nic state
  -failover mode
  -nssync state
  -address_table
  -lla ipv6_link_local_addr
  -dhcp6 state
  -ipv6 state
  -ipv6static state
  -sa6 state
  -i6 static_ipv6_ip_address
  -g6 ipv6_gateway_address
  -p6 length
  -vlan state
  -vlanid VLAN ID
```

Пример:

```
system> ifconfig eth0
-state    :   enabled
```

```
-c         :   dthens
-ghn       :   disabled
-i         :   192.168.70.125
-g         :   0.0.0.0
-s         :   255.255.255.0
-n         :   IMM00096B9E003A
-auto      :   true
-r         :   auto
-d         :   auto
-vlan      :   disabled
-vlanid  :   1
-m         :   1500
-b         :   00:09:6B:9E:00:3A
-l         :   00:00:00:00:00:00
-dn        :
-ipv6      :  enabled
-ipv6static :  disabled
-i6        :  ::
-p6        :  64
-g6        :  ::
-dhcp6    :  enabled
-sa6       :  enabled
-lla       :  fe80::6eae:8bff:fe23:91ae
-nic :  shared:nic3
       nic1: dedicate
       nic2: ext card slot #3
       nic3: ext card slot #5  [active]
-address_table    :

system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
```

Команда keycfg

Используйте эту команду для отображения, добавления или удаления ключей активации.

Ключи активации контролируют доступ к дополнительным функциям IMM.

Примечания:

- Если команда **keycfg** выполняется без каких-либо параметров, отображается список установленных ключей активации. Отображаются следующие сведения о ключах: номер индекса для каждого ключа активации, тип ключа активации, дата окончания срока действия ключа, оставшееся количество использований, статус и описание ключа.
- Добавьте новые ключи активации посредством передачи файлов.
- Удалите старые ключи, указав номер и тип ключа. При удалении ключей по типу удаляется только первый ключ заданного типа.

В следующей таблице показаны аргументы для этих параметров.

Табл. 33. Команда keycfg

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 33. Команда keycfg (продолж.)

Параметр	Описание	Значения
-add	Добавление ключа активации	Значения параметров команд -ip, -pn, -u, -pw и -f
-ip	IP-адрес сервера TFTP с добавляемым ключом активации	Допустимый IP-адрес для сервера TFTP
-pn	Номер порта для сервера TFTP/SFTP с добавляемым ключом активации	Допустимый номер порта для сервера TFTP/SFTP (по умолчанию 69/22)
-u	Имя пользователя для сервера SFTP с добавляемым ключом активации	Допустимое имя пользователя для сервера SFTP
-pw	Пароль для сервера SFTP с добавляемым ключом активации	Допустимый пароль для сервера SFTP
-f	Имя файла для добавляемого ключа активации	Допустимое имя для файла ключа активации
-del	Удаление ключа активации по номеру индекса	Допустимый номер индекса ключа активации из списка **keycfg**
-deltype	Удаление ключа активации по типу ключа	Допустимое значение типа ключа

Синтаксис:
```
keycfg [options]
option:
  -add
     -ip tftp/sftp server ip address
     -pn pn port number of tftp/sftp server (default 69/22)
     -u  username for sftp server
     -pw password for sftp server
     -f  filename
     -del   n ( where n is a valid ID number from listing)
     -deltype x ( where x is a Type value)
```

Пример:
```
system> keycfg
ID  Type  Valid           Uses           Status    Description
1   4     10/10/2010      5               "valid"   "IMM remote presence"
2   3     10/20/2010      2               "valid"   "IMM feature
3   32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"   "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

Примечание: Поле **Описание** для ИД 3 отображается на отдельных строках из-за ограниченного пространства.

Команда ldap

Используйте эту команду для отображения и настройки параметров конфигурации протокола LDAP.

В следующей таблице показаны аргументы для этих параметров.

Табл. 34. Команда ldap

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-a	Метод аутентификации пользователей	только локальная, только LDAP, сначала локальная, затем LDAP, сначала LDAP, затем локальная
-aom	Режим «Только аутентификация»	включено, выключено
-b	Метод привязки	анонимный, привязка с ClientDN и паролем, привязка с учетными данными для входа
-c	Различающееся имя клиента	Строка *client_dn* длиной до 127 символов
-d	Домен поиска	Строка *search_domain* длиной до 63 символов
-f	Групповой фильтр	Строка *group_filter* длиной до 127 символов
-fn	Имя леса	Для сред Active Directory. Строка длиной до 127 символов.
-g	Атрибут группового поиска	Строка *group_search_attr* длиной до 63 символов
-l	Атрибут разрешений на вход	Строка *string* длиной до 63 символов
-p	Пароль клиента	Строка *client_pw* длиной до 15 символов
-pc	Подтверждение пароля клиента	Строка *confirm_pw* длиной до 15 символов Использование команды: ldap -p *client_pw* -pc *confirm_pw* При изменении пароля клиента этот параметр является обязательным. Он сравнивает аргумент *confirm_pw* с аргументом *client_pw*. Если аргументы не соответствуют, выполнение команды завершится ошибкой.
-ep	Зашифрованный пароль	Резервное копирование/восстановление пароля (только для внутреннего использования)
-r	Различающееся имя корневой записи	Строка *root_dn* длиной до 127 символов
-rbs	Расширенная безопасность на основе ролей для пользователей Active Directory	включено, выключено
-s1ip	Имя хоста/IP-адрес сервера 1	Строка длиной до 127 символов или IP-адрес *host name/ip_addr*
-s2ip	Имя хоста/IP-адрес сервера 2	Строка длиной до 127 символов или IP-адрес *host name/ip_addr*
-s3ip	Имя хоста/IP-адрес сервера 3	Строка длиной до 127 символов или IP-адрес *host name/ip_addr*
-s4ip	Имя хоста/IP-адрес сервера 4	Строка длиной до 127 символов или IP-адрес *host name/ip_addr*
-s1pn	Номер порта сервера 1	Числовой номер порта *port_number* (до 5 цифр)
-s2pn	Номер порта сервера 2	Числовой номер порта *port_number* (до 5 цифр)

Табл. 34. Команда ldap (продолж.)

Параметр	Описание	Значения
-s3pn	Номер порта сервера 3	Числовой номер порта *port_number* (до 5 цифр)
-s4pn	Номер порта сервера 4	Числовой номер порта *port_number* (до 5 цифр)
-t	Целевое имя сервера	Если параметр rbs включен, в этом поле задается целевое имя, которое может быть связано с одной или несколькими ролями на сервере Active Directory посредством оснастки RBS.
-u	Атрибут поиска UID	Строка *search_attrib* длиной до 63 символов
-v	Получение адреса сервера LDAP через DNS	Выкл., вкл.
-h	Отображает сведения об использовании команды и параметры	

Синтаксис:

```
ldap [options]
options:
   -a loc|ldap|locld|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -fn forest_name
   -g group_search_attr
   -l string
   -p client_pw
   -pc confirm_pw
   -ep encrypted_pw
   -r root_dn
   -rbs enable|disabled
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
   -s4ip host name/ip_addr
   -s1pn port_number
   -s2pn port_number
   -s3pn port_number
   -s4pn port_number
   -t name
   -u search_attrib
   -v off|on
   -h
```

Команда ntp

Используйте эту команду для отображения и настройки протокола NTP.

В следующей таблице показаны аргументы для этих параметров.

Табл. 35. Команда ntp

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 35. Команда ntp (продолж.)

Параметр	Описание	Значения
-en	Включение и выключение протокола NTP.	включено, выключено
-i[1]	Имя или IP-адрес NTP-сервера. Это индекс NTP-сервера.	Имя NTP-сервера, которое следует использовать для синхронизации часов. Диапазон индексов NTP-сервера включает индексы от -i1 до -i4.
-f	Периодичность (в минутах) синхронизации часов IMM с NTP-сервером.	от 3 до 1440 минут
-synch	Запрос немедленной синхронизации с NTP-сервером.	С этим параметром не используются никакие значения.

1. -i равно i1.

Синтаксис:
```
ntp [options]
options:
-en state
-i  hostname/ip_addr
-f  frequency
-synch
```

Пример:
```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

Команда portcfg

Используйте эту команду для настройки функции последовательного направления в IMM.

Необходимо настроить IMM так, чтобы настройки соответствовали параметрам внутреннего последовательного порта сервера. Чтобы изменить конфигурацию последовательного порта, введите параметры, за которыми следуют их значения. Чтобы изменить конфигурацию последовательного порта, необходимо обладать по меньшей мере правами настройки сетевых параметров и безопасности адаптера.

Примечание: Внешний последовательный порт сервера может использоваться модулем IMM только для функции IPMI. Интерфейс командной строки не поддерживается последовательным портом. Параметры **serred** и **cliauth**, присутствовавшие в интерфейсе командной строки Remote Supervisor Adapter II, не поддерживаются.

Если выполнить команду **portcfg** без параметров, отобразится конфигурация последовательного порта. В следующей таблице показаны аргументы для этих параметров.

Примечание: Число битов данных (8) задается на аппаратном уровне и не может быть изменено.

Табл. 36. Команда portcfg

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 36. Команда portcfg (продолж.)

Параметр	Описание	Значения
-b	Скорость (бит/с)	9600, 19200, 38400, 57600, 115200
-p	Четность	нет, нечетный, четный
-s	Стоп-биты	1, 2
-climode	Режим интерфейса командной строки	0, 1, 2 Где: • 0 = none: интерфейс командной строки выключен • 1 = cliems: интерфейс командной строки включен с помощью последовательностей клавиш, совместимых с EMS • 2 = cliuser: интерфейс командной строки включен с помощью последовательностей клавиш, определяемых пользователем

Синтаксис:
```
portcfg [options]
 options:
   -b baud_rate
   -p parity
   -s stopbits
   -climode mode
```

Пример:
```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

Команда portcontrol

Используйте эту команду для включения и выключения сетевого порта службы.

В настоящее время эта команда поддерживает только управление портом для протокола IPMI. Введите **portcontrol**, чтобы отобразить состояние порта IPMI. Чтобы включить или отключить сетевой порт IPMI, введите параметр **-ipmi** и значение **on** или **off** сразу после него.

Табл. 37. Команда portcontrol

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-all	Включение или отключение всех интерфейсов и протоколов обнаружения	вкл., выкл.
-cim	Включение или отключение обнаружения CIM	вкл., выкл.

Табл. 37. Команда portcontrol (продолж.)

Параметр	Описание	Значения
-ipmi	Включение или отключение доступа к ipmi через LAN	вкл., выкл.
-ipmi-kcs	Включение или отключение доступа к ipmi с сервера	вкл., выкл.
-rest	Включение или отключение обнаружения REST	вкл., выкл.
-slp	Включение или отключение обнаружения SLP	вкл., выкл.
-snmp	Включение или отключение обнаружения SNMP	вкл., выкл.
-ssdp	Включение или отключение обнаружения SSDP	вкл., выкл.
-cli	Включение или отключение обнаружения CLI	вкл., выкл.
-web	Включение или отключение обнаружения WEB	вкл., выкл.

Синтаксис:
```
portcontrol [options]
 options:
   -ipmi on/off
```

Пример:
```
system> portcontrol
cim : on
ipmi : on
ipmi-kcs : on
rest : on
slp : on
snmp : off
ssdp : on
cli : on
web : on
```

Команда ports

Используйте эту команду для отображения и настройки портов IMM.

Если выполнить команду **ports** без параметров, отобразится информация обо всех портах IMM. В следующей таблице показаны аргументы для этих параметров.

Табл. 38. Команда ports

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-open	Отображение открытых портов	
-reset	Сброс портов до параметров по умолчанию	
-httpp	Номер порта HTTP	Номер порта по умолчанию: 80
-httpsp	Номер порта HTTPS	Номер порта по умолчанию: 443
-sshp	Номер порта устаревшего интерфейса командной строки SSH	Номер порта по умолчанию: 22
-snmpap	Номер порта агента SNMP	Номер порта по умолчанию: 161
-snmptp	Номер порта ловушек SNMP	Номер порта по умолчанию: 162
-rpp	Номер порта удаленного присутствия	Номер порта по умолчанию: 3900
-cimhp	Номер порта CIM через HTTP	Номер порта по умолчанию: 5988
-cimhsp	Номер порта CIM через HTTPS	Номер порта по умолчанию: 5989

Синтаксис:
```
ports [options]
option:
  -open
  -reset
  -httpp port_number
  -httpsp port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

Пример:
```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-cimhp 5988
-cimhsp 5989
system>
```

Команда rdmount

Используйте эту команду для установки образов удаленных дисков или сетевых папок

В следующей таблице показаны аргументы для этих параметров.

Табл. 39. Команда rdmount

В следующей многострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Примечания:

- С помощью компонента XClarity Controller RDOC можно отправить в память XClarity Controller и подключить в качестве виртуальных носителей до двух файлов. Общий размер обоих файлов не должен превышать 50 МБ. Отправленные образы доступны только для чтения, если не используется параметр –rw.
- При использовании протоколов HTTP, SFTP или FTP для подключения или сопоставления образов, общий размер всех образов не должен превышать 50 МБ. Если используются протоколы SAMBA и NFS ограничений по размеру нет.

Параметр	**Описание**
-r	Операция rdoc (если используется, должен быть первым параметром) -r -map: подключение образов RDOC -r -unmap<имя_файла>: отключение подключенных образов RDOC -r -maplist: отображение подключенных образов RDOC с помощью веб-браузера XClarity Controller и интерфейса командной строки
-map	-t тип файловой системы <samba|nfs|http|sftp|ftp> -ro только чтение -rw чтение и запись -u пользователь -p пароль -l расположение файла (формат URL-адреса) -o параметр (дополнительная строка параметров для установок samba и nfs) -d домен (домен для установки samba)
-maplist	отображение сопоставленных образов
-unmap <id|fname>	использование ИД с сетевыми образами, имени файла — с rdoc
-mount	подключение сопоставленных образов
-unmount	отключение подключенных образов

Команда restore

Используйте эту команду для восстановления системных параметров из резервного файла.

В следующей таблице показаны аргументы для этих параметров.

Табл. 40. Команда restore

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 40. Команда restore (продолж.)

Параметр	Описание	Значения
-f	Имя резервного файла	Допустимое имя файла
-pp	Пароль или фраза-пароль, используемые для шифрования паролей внутри резервного файла	Допустимый пароль или фраза-пароль с разделителями в виде кавычек
-ip	IP-адрес сервера TFTP/SFTP	Допустимый IP-адрес
-pn	Номер порта сервера TFTP/SFTP	Допустимый номер порта (по умолчанию 69/22)
-u	Имя пользователя для сервера SFTP	Допустимое имя пользователя
-pw	Пароль для сервера SFTP	Допустимый пароль

Синтаксис:
```
restore [options]
option:
  -f filename
  -pp password
  -ip ip_address
  -pn port_number
username
  -pw password
```

Пример:
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

Команда restoredefaults

Используйте эту команду для восстановления заводских значений по умолчанию для всех параметров IMM.

- Параметры для команды **restoredefaults** отсутствуют.
- Перед обработкой команды вам потребуется ее подтвердить.

Синтаксис:
```
restoredefaults
```

Пример:
```
system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults
```

Команда roles

Используйте эту команду для отображения или настройки ролей.

В следующей таблице показаны аргументы для этих параметров.

Табл. 41. Команда roles

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-n	Роль для настройки	Не более 32 символов
-p	Настройка привилегий	custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us • **am**: доступ к управлению учетными записями пользователей • **rca**: удаленный доступ к консоли • **rcvma**: удаленный доступ к консоли и диску (виртуальному носителю) • **pr**: удаленный доступ к питанию/перезапуску сервера • **cel**: возможность очищать журналы событий • **bc**: конфигурация адаптера (базовая) • **nsc**: конфигурация адаптера (сетевые подключения и безопасность) • **ac**: конфигурация адаптера (расширенная) • **us**: безопасность UEFI **Примечание:** указанные выше пользовательские флаги разрешений можно использовать в любом сочетании
d	Удаление строки	

Синтаксис

```
   roles [-options] - display/configure roles
   - role_account -role number[3-31]
options:
   -n        - role name (limited to 32 characters)
   -p        - privilege (custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us)
      am     - User account management access
      rca    - Remote console access
      rcvma  - Remote console and remote disk (virtual media) access
      pr     - Remote server power/restart access
      cel    - Ability to clear event logs
      bc     - Adapter Configuration (basic)
      nsc    - Adapter Configuration (network and security)
      ac     - Adapter Configuration (advanced)
      us     - UEFI Security
      Note: the above custom permission flags can be used in any combination
   -d        - delete a row
```

Пример

```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok
```

```
system> roles
Account              Role                              Privilege                      Assigned To
------- ----------------------------------   -------------------------     ------------------------------
    0                    Administrator                      all                          USERID
    1                         ReadOnly                        none
    2                         Operator                custom:pr|cel|bc|nsc
    3                             test1                custom:am|rca|rcvma
```

Команда seccfg

Используйте эту команду для выполнения отката микропрограммы.

В следующей таблице показаны аргументы для этих параметров.

Табл. 42. Команда seccfg

В следующей многострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Параметр	Описание	Значение
-fwrb	Позволяет выполнить откат микропрограммы до предыдущих версий	да, нет
-rppen	Включить удаленное физическое присутствие (только чтение)	/
-rppto	Тайм-аут удаленного физического присутствия (только чтение)	/
-rpp	Физическое присутствие (если включается BIOS)	да, нет
-aubp	включите или выключите функцию автоматического резервного копирования в первичное продвижение	включено, выключено

Команда set

Используйте эту команду для изменения некоторых настроек IMM.

- Некоторые параметры IMM можно изменить с помощью простой команды **set**.
- Некоторые из этих параметров, например переменные среды, используются в интерфейсе командной строки.

В следующей таблице показаны аргументы для этих параметров.

Табл. 43. Команда set

В следующей однострочной таблице с тремя столбцами приводится описание команды и соответствующая информация.

Табл. 43. Команда set (продолж.)

Параметр	Описание	Значения
значение	Задание значения для указанного пути или настройки	Подходящее значение для указанного пути или настройки.

Синтаксис:
```
set [options]
option:
  value
```

Команда smtp

Используйте эту команду для отображения и настройки параметров интерфейса SMTP.

Если выполнить команду **smtp** без параметров, отобразятся все сведения об интерфейсе SMTP. В следующей таблице показаны аргументы для этих параметров.

Табл. 44. Команда smtp

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-auth	Поддержка аутентификации SMTP	включено, выключено
-authepw	Зашифрованный пароль аутентификации SMTP	Строка допустимого пароля
-authmd	Метод аутентификации SMTP	CRAM-MD5, LOGIN
-authn	Имя пользователя аутентификации SMTP	Строка (не более 256 символов)
-authpw	Пароль для аутентификации SMTP	Строка (не более 256 символов)
-pn	Номер порта SMTP	Допустимый номер порта
-s	IP-адрес или имя хоста сервера SMTP	Допустимый IP-адрес или имя хоста (не более 63 символов)

Синтаксис:
```
smtp [options]
option:
  -auth enabled|disabled
  -authepw password
  -authmd CRAM-MD5|LOGIN
  -authn username
  -authpw password
  -s ip_address_or_hostname
  -pn port_number
```

Пример:
```
system> smtp
-s test.com
-pn 25
system>
```

Команда snmp

Используйте эту команду для отображения и настройки сведений об интерфейсе SNMP.

Если выполнить команду **snmp** без параметров, отобразятся все сведения об интерфейсе SNMP. В следующей таблице показаны аргументы для этих параметров.

Табл. 45. Команда snmp

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-a3	Агент SNMPv3	вкл., выкл. **Примечания:** Чтобы включить агент SNMPv3, необходимо выполнить следующие условия: • Контакт IMM, заданный с использованием параметра команды -cn. • Расположение IMM, заданное с использованием параметра команды -l.
-t1	Ловушки SNMPv1	вкл., выкл.
-t2	Ловушки SNMPv2	вкл., выкл.
-t	Ловушки SNMPv3	вкл., выкл.
-l	Расположение IMM	Строка (не более 47 символов). **Примечания:** • Аргументы, содержащие пробелы, должны быть заключены в кавычки. В аргументах запрещено использовать пробелы в начале или в конце. • Очистите расположение IMM, не указав никаких аргументов или указав в качестве аргумента пустую строку, например «».
-cn	Имя контакта IMM	Строка (не более 47 символов). **Примечания:** • Аргументы, содержащие пробелы, должны быть заключены в кавычки. В аргументах запрещено использовать пробелы в начале или в конце. • Очистите имя контакта IMM, не указав никаких аргументов или указав в качестве аргумента пустую строку, например «».
-c	Имя сообщества SNMP	Строка (не более 15 символов). **Примечания:** • Аргументы, содержащие пробелы, должны быть заключены в кавычки. В аргументах запрещено использовать пробелы в начале или в конце. • Очистите имя сообщества SNMP, не указав никаких аргументов или указав в качестве аргумента пустую строку, например «».
-ct	Имя сообщества ловушек SNMPv2	Строка (не более 15 символов). **Примечания:** • Аргументы, содержащие пробелы, должны быть заключены в кавычки. В аргументах запрещено использовать пробелы в начале или в конце. • Очистите имя контакта IMM, не указав никаких аргументов или указав в качестве аргумента пустую строку, например «».

Табл. 45. Команда snmp (продолж.)

Параметр	Описание	Значения
-ci	IP-адрес или имя хоста сообщества SNMP	Допустимый IP-адрес или имя хоста (не более 63 символов). **Примечания:** • IP-адрес или имя хоста может содержать только точки, нижние подчеркивания, знаки минус, буквы и цифры. Запрещается использовать внедренные пробелы или последовательные точки. • Очистите IP-адрес или имя хоста сообщества SNMP, не указав никакой аргумент.
-cti	IP-адрес/имя хоста сообщества ловушек SNMPv2	Допустимый IP-адрес или имя хоста (не более 63 символов). **Примечания:** • IP-адрес или имя хоста может содержать только точки, нижние подчеркивания, знаки минус, буквы и цифры. Запрещается использовать внедренные пробелы или последовательные точки. • Очистите IP-адрес или имя хоста сообщества SNMP, не указав никакой аргумент.
-eid	ИД механизма SNMP	Строка (от 1 до 27 символов)

Синтаксис:
```
snmp [options]
option:
 -a3 state
  -t state
  -l location
  -cn contact_name
  -t1 state
  -c community name
  -ci community IP address/hostname
  -t2 state
  -ct community name
  -cti community IP address/hostname
  -eid engine id
```

Пример:
```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
-eid XCC-7Z70-DSYM09X
system>
```

Команда snmpalerts

Используйте эту команду для управления оповещениями, которые отправляются через SNMP.

Если команда **snmpalerts** выполняется без параметров, отображаются все настройки оповещений SNMP. В следующей таблице показаны аргументы для этих параметров.

Табл. 46. Команда snmpalerts

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-status	Состояние оповещения SNMP	вкл., выкл.
-crt	Настройка критических событий, отправляющих уведомления	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Пользовательские настройки критических оповещений задаются с использованием разделенного вертикальными полосами списка значений в формате **snmpalerts -crt custom:te|vo**, где используются следующие пользовательские значения: • te: превышен критический температурный порог • vo: превышен критический порог напряжения • po: критический сбой питания • di: сбой жесткого диска • fa: сбой вентилятора • cp: сбой микропроцессора • me: сбой памяти • in: несовместимость оборудования • re: сбой резерва питания • ot: все остальные критические события
-crten	Отправка оповещений о критических событиях	включено, выключено
-wrn	Настройка событий типа «предупреждение», отправляющих уведомления	all, none, custom:rp|te|vo|po|fa|cp|me|ot Пользовательские настройки оповещений типа «предупреждение» задаются с использованием разделенного вертикальными полосами списка значений в формате **snmpalerts -wrn custom:rp|te**, где используются следующие пользовательские значения: • rp: предупреждение резерва питания • te: предупреждение о превышении температурного порога • vo: предупреждение о превышении порога напряжения • po: предупреждение о превышении порога питания • fa: некритическое событие вентилятора • cp: ухудшенное состояние микропроцессора • me: предупреждение памяти • ot: все остальные события типа «предупреждение»
-wrnen	Отправка оповещений о событиях типа «предупреждение»	включено, выключено

Табл. 46. Команда snmpalerts (продолж.)

Параметр	Описание	Значения
-sys	Настройка рутинных событий, отправляющих уведомления	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Пользовательские настройки стандартных оповещений задаются с использованием разделенного вертикальными полосами списка значений в формате **snmpalerts -sys custom:lo|tio**, где используются следующие пользовательские значения: • lo: успешный удаленный вход • tio: тайм-аут операционной системы • ot: все остальные информационные и системные события • po: включение/выключение питания системы • bf: сбой загрузки операционной системы • til: тайм-аут Watchdog загрузчика операционной системы • pf: прогнозируемый сбой (PFA) • el: журнал событий на 75 % полон • ne: изменение сети
-sysen	Отправка оповещений о рутинных событиях	включено, выключено

Синтаксис:
```
snmpalerts [options]
   options:
     -status status
     -crt event_type
     -crten state
     -wrn event_type
     -wrnen state
     -sys event_type
     -sysen state
```

Команда srcfg

Используйте эту команду для обозначения последовательности клавиш для входа в интерфейс командной строки из режима последовательного перенаправления.

Чтобы изменить конфигурацию последовательного перенаправления, введите параметры, за которыми следуют их значения. Чтобы изменить конфигурацию последовательного перенаправления, необходимо обладать по меньшей мере правами настройки сетевых параметров и безопасности адаптера.

Примечание: Оборудование IMM не предоставляет возможность сквозного прохода от одного последовательного порта к другому. Следовательно, параметры `-passthru` и `entercliseq`, присутствующие в интерфейсе командной строки Remote Supervisor Adapter II, не поддерживаются.

Если выполнить команду **srcfg** без параметров, отобразится текущая последовательность нажатий клавиш для последовательного перенаправления. В следующей таблице показаны аргументы для параметра команды `srcfg -entercliseq`.

Табл. 47. Команда srcfg

В следующей однострочной таблице с тремя столбцами приводится параметр, описание параметра и сведения о значениях для этого параметра.

Табл. 47. Команда srcfg (продолж.)

Параметр	Описание	Значения
-entercliseq	Введите последователь-ность нажатия клавиш в интерфейсе командной строки	Определяемая пользователем последовательность нажатия клавиш для входа в интерфейс командной строки. **Примечание:** Эта последовательность может включать от одного до 15 символов. Символ каретки (^) имеет особое значение в этой последовательности. Он обозначает Ctrl для нажатий клавиш, сопоставляемых последовательностям Ctrl (например, ^[— клавиша Esc и ^M — возврат каретки). Все вхождения ^ интерпретируются как часть последовательности Ctrl. См. полный список последовательностей CTRL в таблице преобразования ASCII-код — клавиша. Значение по умолчанию для этого поля — ^[(, что означает клавишу Esc, за которой следует (.

Синтаксис:
```
srcfg [options]
options:
-entercliseq entercli_keyseq
```

Пример:
```
system> srcfg
-entercliseq ^[Q
system>
```

Команда sshcfg

Используйте эту команду для отображения и настройки параметров SSH.

Если выполнить команду **sshcfg** без параметров, отобразятся все атрибуты SSH. В следующей таблице показаны аргументы для этих параметров.

Табл. 48. Команда sshcfg

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-cstatus	Состояние интерфейса командной строки SSH	включено, выключено
-hk gen	Создание закрытого ключа сервера SSH	
-hk rsa	Отображение открытого ключа RSA сервера	

Синтаксис:
```
sshcfg [options]
option:
  -cstatus state
  -hk gen
  -hk rsa
```

Пример:
```
system> sshcfg
-cstatus enabled
```

```
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

Команда ssl

Используйте эту команду для отображения и настройки параметров SSL.

Чтобы включить клиент SSL, необходимо установить сертификат клиента. Если выполнить команду **ssl** без параметров, отобразятся атрибуты SSL. В следующей таблице показаны аргументы для этих параметров.

Табл. 49. Команда ssl

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-ce	Включение или выключение клиента SSL	вкл., выкл.
-se	Включение или выключение сервера SSL	вкл., выкл.
-cime	Включение или выключение интерфейса CIM через HTTPS на сервере SSL	вкл., выкл.

Синтаксис:
```
portcfg [options]
 options:
  -ce state
  -se state
  -cime state
```

Атрибуты: следующие атрибуты отображаются на экране состояния параметра для команды **ssl** и выводятся только из интерфейса командной строки:

Включение безопасного транспорта сервера
Этот экран состояния доступен только для чтения, задать его непосредственно невозможно.

Состояние веб-ключа/ключа CMD сервера
Этот экран состояния доступен только для чтения, задать его непосредственно невозможно. Доступны следующие возможные выходные значения командной строки:

Закрытый ключ и сертификат/CSR недоступны

Закрытый ключ и заверенный ЦС сертификат установлены

Закрытый ключ и автоматически созданный самозаверяющий сертификат установлены

Закрытый ключ и самозаверяющий сертификат установлены

Закрытый ключ сохранен, CSR доступен для загрузки

Состояние ключа CSR сервера SSL
Этот экран состояния доступен только для чтения, задать его непосредственно невозможно. Доступны следующие возможные выходные значения командной строки:

Закрытый ключ и сертификат/CSR недоступны

Закрытый ключ и заверенный ЦС сертификат установлены

Закрытый ключ и автоматически созданный самозаверяющий сертификат установлены

Закрытый ключ и самозаверяющий сертификат установлены

Закрытый ключ сохранен, CSR доступен для загрузки

Состояние ключа LDAP клиента SSL

Этот экран состояния доступен только для чтения, задать его непосредственно невозможно. Доступны следующие возможные выходные значения командной строки:

Закрытый ключ и сертификат/CSR недоступны

Закрытый ключ и заверенный ЦС сертификат установлены

Закрытый ключ и автоматически созданный самозаверяющий сертификат установлены

Закрытый ключ и самозаверяющий сертификат установлены

Закрытый ключ сохранен, CSR доступен для загрузки

Состояние ключа CSR клиента SSL

Этот экран состояния доступен только для чтения, задать его непосредственно невозможно. Доступны следующие возможные выходные значения командной строки:

Закрытый ключ и сертификат/CSR недоступны

Закрытый ключ и заверенный ЦС сертификат установлены

Закрытый ключ и автоматически созданный самозаверяющий сертификат установлены

Закрытый ключ и самозаверяющий сертификат установлены

Закрытый ключ сохранен, CSR доступен для загрузки

Команда sslcfg

Используйте эту команду для отображения и настройки SSL для IMM и управления сертификатами.

Если выполнить команду **sslcfg** без параметров, отобразятся все сведения о конфигурации SSL. Команда **sslcfg** служит для создания нового ключа шифрования и самозаверяющего сертификата или запроса на подпись сертификата (CSR). В следующей таблице показаны аргументы для этих параметров.

Табл. 50. Команда sslcfg

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-server	Состояние сервера SSL	включено, выключено **Примечание:** Сервер SSL можно включить только при наличии действительного сертификата.
-client	Состояние клиента SSL	включено, выключено **Примечание:** Клиент SSL можно включить только при наличии действительного сертификата сервера или клиента.
-cim	Состояние CIM через HTTPS	включено, выключено **Примечание:** CIM через HTTPS можно включить только при наличии действительного сертификата сервера или клиента.

Табл. 50. Команда sslcfg (продолж.)

Параметр	Описание	Значения
-cert	Создание самозаверяющего сертификата	server, client, sysdir, storekey **Примечания:** • Значения для параметров команд **-c**, **-sp**, **-cl**, **-on**, and **-hn** при создании самозаверяющего сертификата являются обязательными. • Значения для параметров команд **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in** и **-dq** при создании самозаверяющего сертификата являются необязательными.
-csr	Создание запроса CSR	server, client, sysdir, storekey **Примечания:** • Значения для параметров команд **-c**, **-sp**, **-cl**, **-on** и **-hn** при создании запроса CSR являются обязательными. • Значения для параметров команд **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd** и **-un** при создании запроса CSR являются необязательными.
-i	IP-адрес сервера TFTP/ SFTP	Допустимый IP-адрес **Примечание:** Необходимо задать IP-адрес для сервера TFTP или SFTP при отправке сертификата или загрузке сертификата или запроса CSR.
-pn	Номер порта сервера TFTP/SFTP	Допустимый номер порта (по умолчанию 69/22)
-u	Имя пользователя для сервера SFTP	Допустимое имя пользователя
-pw	Пароль для сервера SFTP	Допустимый пароль
-l	Имя файла с сертификатом	Допустимое имя файла **Примечание:** При загрузке или отправке сертификата или запроса CSR имя файла является обязательным. Если имя файла для загрузки не указано, используется и отображается имя файла по умолчанию.
-dnld	Загрузка файла сертификата	Этот параметр не принимает аргументы, однако необходимо все равно задать значения для параметра команды **-cert** или **-csr** (в зависимости от типа загружаемого объекта). Этот параметр не принимает аргументы, однако необходимо все равно задать значения для параметра команды **-i** и параметр команды **-L** (необязательно).
-upld	Импорт файла сертификата	Этот параметр не принимает аргументы, однако необходимо все равно задать значения для параметров команд **-cert**, **-i** и **-l**.
-tc*x*	Доверенный сертификат *x* для клиента SSL	import, download, remove **Примечание:** Номер доверенного сертификата *x* задается в виде целого числа от 1 до 3 в параметре команды.
-c	Страна	Код страны (2 буквы) **Примечание:** Обязателен при создании самозаверяющего сертификата или CSR.
-sp	Регион	Строка с разделителями в виде кавычек (не более 60 символов) **Примечание:** Обязателен при создании самозаверяющего сертификата или CSR.

Табл. 50. Команда sslcfg (продолж.)

Параметр	Описание	Значения
-cl	Город или муниципальная единица	Строка с разделителями в виде кавычек (не более 50 символов) **Примечание:** Обязателен при создании самозаверяющего сертификата или CSR.
-on	Название организации	Строка с разделителями в виде кавычек (не более 60 символов) **Примечание:** Обязателен при создании самозаверяющего сертификата или CSR.
-hn	Имя хоста IMM	Строка (не более 60 символов) **Примечание:** Обязателен при создании самозаверяющего сертификата или CSR.
-cp	Контактное лицо	Строка с разделителями в виде кавычек (не более 60 символов) **Примечание:** Необязателен при создании самозаверяющего сертификата или CSR.
-ea	Адрес электронной почты контактного лица	Действительный адрес электронной почты (не более 60 символов) **Примечание:** Необязателен при создании самозаверяющего сертификата или CSR.
-ou	Организационная единица	Строка с разделителями в виде кавычек (не более 60 символов) **Примечание:** Необязателен при создании самозаверяющего сертификата или CSR.
-s	Фамилия	Строка с разделителями в виде кавычек (не более 60 символов) **Примечание:** Необязателен при создании самозаверяющего сертификата или CSR.
-gn	Имя	Строка с разделителями в виде кавычек (не более 60 символов) **Примечание:** Необязателен при создании самозаверяющего сертификата или CSR.
-in	Инициалы	Строка с разделителями в виде кавычек (не более 20 символов) **Примечание:** Необязателен при создании самозаверяющего сертификата или CSR.
-dq	Квалификатор доменного имени	Строка с разделителями в виде кавычек (не более 60 символов) **Примечание:** Необязателен при создании самозаверяющего сертификата или CSR.
-cpwd	Пароль запроса	Строка (длиной от 6 до 30 символов) **Примечание:** Необязателен при создании CSR.
-un	Неструктурированное имя	Строка с разделителями в виде кавычек (не более 60 символов) **Примечание:** Необязателен при создании CSR.

Синтаксис:

```
sslcfg [options]
option:
  -server state
  -client state
  -cim state
  -cert certificate_type
  -csr certificate_type
  -i ip_address
port number
user name
  -pw password
  -l filename
  -dnld
```

-upld
-tc *xaction*
-c *country_code*
-sp *state_or_province*
-cl *city_or_locality*
-on *organization_name*
-hn *bmc_hostname*
-cp *contact_person*
-ea *email_address*
-ou *organizational_unit*
-s *surname*
-gn *given_name*
-in *initials*
-dq *dn_qualifier*
-cpwd *challenge_password*
-un *unstructured_name*

Примеры:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

Примеры сертификата клиента:

- Чтобы создать CSR для хранилища ключей, введите следующую команду:
  ```
  system> sslcfg
  -csr storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```

Пример выше отображается на нескольких строках из-за нехватки места.

- Чтобы загрузить сертификат из IMM на другой сервер, введите следующую команду:
  ```
  system> sslcfg
  -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
  ok
  ```
- Чтобы отправить сертификат, обработанный центром сертификации (ЦС), введите следующую команду:
  ```
  system> sslcfg
  -cert storekey -upld -i 192.168.70.230 -l tklm.der
  ```
- Чтобы создать самозаверяющий сертификат, введите следующую команду:
  ```
  system> sslcfg
  -cert storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou "
  ok
  ```

Пример выше отображается на нескольких строках из-за нехватки места.

Пример сертификата сервера SKLM:

- Чтобы импортировать сертификат сервера SKLM, введите следующую команду:
```
system> storekeycfg
-add -ip 192.168.70.200 -f tklm-server.der
ok
```

Команда storekeycfg

Используйте эту команду для настройки имени хоста или IP-адреса и сетевого порта сервера SKLM.

Можно настроить до четырех целевых объектов сервера SKLM. Команда **storekeycfg** также служит для установки и удаления сертификатов, которые используются IMM для аутентификации на сервере SKLM.

В следующей таблице показаны аргументы для этих параметров.

Табл. 51. Команда storekeycfg

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-add	Добавление ключа активации	Значения — это параметры команд -ip, -pn, -u, -pw и -f
-ip	Имя хоста или IP-адрес сервера TFTP/SFTP	Допустимое имя хоста или IP-адрес сервера TFTP/SFTP
-pn	Номер порта сервера TFTP или SFTP	Допустимый номер порта для сервера TFTP/SFTP (значение по умолчанию — 69/22)
-u	Имя пользователя для сервера SFTP	Допустимое имя пользователя для сервера SFTP
-pw	Пароль для сервера SFTP	Допустимый пароль для сервера SFTP
-f	Имя файла для ключа активации	Допустимое имя для файла ключа активации
-del	Используйте эту команду для удаления ключа активации по номеру индекса	Допустимый номер индекса ключа активации из списка keycfg
-dgrp	Добавление группы устройств	Имя группы устройств
-sxip	Добавление имени хоста или IP-адреса для сервера SKLM	Допустимое имя хоста или IP-адрес сервера SKLM. Числовое значение 1, 2, 3 или 4.
-sxpn	Добавление номера порта сервера SKLM	Допустимый номер порта для сервера SKLM. Числовое значение 1, 2, 3 или 4.

Табл. 51. Команда storekeycfg (продолж.)

Параметр	Описание	Значения
-testx	Проверка конфигурации и подключения к серверу SKLM	Числовое значение 1, 2, 3 или 4
-h	Отображение сведений об использовании команды и параметров	

Синтаксис:
```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

Примеры:

Чтобы импортировать сертификат сервера SKLM, введите следующую команду:
```
system> storekeycfg
add -ip 192.168.70.200 -f tklm-server.der
system> ok
```

Чтобы настроить адрес сервера SKLM и номер порта, введите следующую команду:
```
system> storekeycfg
-s1ip 192.168.70.249
system> ok
```

Чтобы настроить имя группы устройств, введите следующую команду:
```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

Команда syncrep

Используйте эту команду для запуска синхронизации микропрограммы из удаленного репозитория.

В следующей таблице показаны аргументы для этих параметров.

Табл. 52. Команда syncrep

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 52. Команда syncrep (продолж.)

Параметр	Описание	Значения
-t	Протокол для подключения репозитория	samba, nfs
-l	Расположение удаленного репозитория	В формате URL-адреса
-u	Пользователь	
-p	Пароль	
-o	Параметр	Дополнительная строка параметров для подключения samba и nfs
-d	Домен	Домен для подключения samba
-q	Запрос текущего состояния обновления	
-c	Отмена процесса синхронизации	

Синтаксис

```
syncrep [options]  Launch firmware sync from remote repository
options:
     -t <samba|nfs> protocol to connect repository
     -l location of remote repository (URL format)
     -u User
     -p Password
     -o option (extra option string for samba and nfs mounts)
     -d domain (domain for samba mount)
     -q query current update status
     -c cancel the sync process
```

Пример

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

Команда thermal

Используйте эту команду для отображения и настройки политики температурного режима главной системы.

Если выполнить команду **thermal** без параметров, отобразится политика температурного режима. В следующей таблице показаны аргументы для этих параметров.

Табл. 53. Команда thermal

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 53. Команда thermal (продолж.)

Параметр	Описание	Значения
-mode	Выбор температурного режима	нормальный, производительность, минимальный, эффективность, пользовательский
-table	Таблица с данными о поставщиках, идентификации устройств (ИД) и альтернативных температурных режимах	

Синтаксис:
```
thermal [options]
option:
  -mode thermal_mode
  -table vendorID_devicetable_number
```

Пример:
```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

Команда timeouts

Используйте эту команду для отображения или изменения значений тайм-аута.

- Для отображения тайм-аутов введите `timeouts`.
- Чтобы изменить значения тайм-аутов, введите параметры, за которыми следуют их значения.
- Чтобы изменить значения тайм-аутов, необходимо обладать по меньшей мере правами на конфигурацию адаптера.

В следующей таблице показаны аргументы для значений тайм-аутов. Эти значения соответствуют параметрам тайм-аутов сервера в раскрывающемся списке с градуированной шкалой, доступном в веб-интерфейсе.

Табл. 54. Команда timeouts

В следующей многострочной таблице с четырьмя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Тайм-аут	Единицы	Значения
-f	Задержка выключения питания	мин.	выключено, 0,5, 1, 2, 3, 4, 5, 7,5, 10, 15, 20, 30, 60, 120
-l	Тайм-аут загрузчика	мин.	выключено, 0,5, 1, 1,5, 2, 2,5, 3, 3,5, 4, 4,5, 5, 7,5, 10, 15, 20, 30, 60, 120
-o	Тайм-аут операционной системы	мин.	выключено, 2,5, 3, 3,5, 4
-s	Снимок экрана сбоя ОС с ошибкой HW	/	выключено, включено

Синтаксис:
```
timeouts [options]
```

```
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
-s OS failure screen capture with HW error
```

Пример:

```
system> timeouts
-o disabled
-l 3.5
-f disabled
-s disabled
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
-f disabled
-s disabled
```

Команда tls

Используйте эту команду для настройки минимального уровня TLS.

В следующей таблице показаны аргументы для этих параметров.

Табл. 55. Команда tls

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-min	Выберите минимальный уровень TLS	1.0, 1.1, 1.2[1], 1.3
-h	Список вариантов использования и параметров	

Примечания:

1. Если в качестве режима шифрования задан режим соответствия стандарту NIST-800-131A, необходимо задать версию TLS 1.2.

Использование:

```
tls [-options] - configures the minimum TLS level
   -min <1.0 | 1.1 | 1.2 | 1.3> - Selects the minimum TLS level
   -h - Lists usage and options
```

Примеры:

Чтобы проанализировать использование команды tls, вызовите следующую команду:

```
system> tls
-h
system>
```

Чтобы получить текущую версию tls, вызовите следующую команду:

```
system> tls
-min 1.2
```

```
system>
```

Чтобы изменить текущую версию tls на 1.2, вызовите следующую команду:

```
system> tls
-min 1.2
ok
system>
```

Команда trespass

Используйте эту команду для настройки и отображения сообщений при нарушении.

Команду **trespass** можно использовать для настройки и отображения сообщений при нарушении. Сообщение о нарушении будут отображаться для любого пользователя, выполняющего вход через интерфейс WEB или CLI.

В следующей таблице показаны аргументы для этих параметров.

Табл. 56. Команда uefipw

В следующей многострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Параметр	Описание
-s	Настройка сообщений при нарушении
-h	Список вариантов использования и параметров

Синтаксис:

```
usage:
   trespass display the trespass message
   -s <trespass message> configure trespass message
   -h - Lists usage and options
```

Пример:

Примечание: Сообщение при нарушении не содержит пробелов.

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage

The trespass message contains spaces:
system> trespass -s "testing message"
ok
system> trespass
testing message
```

Команда uefipw

Используйте эту команду для настройки паролей администратора UEFI. Пароль доступен только для записи.

Команду **uefipw** можно использовать с параметром «-p», чтобы настроить пароль администратора UEFI для XCC, или с параметром «-ep» для LXCA, чтобы настроить пароль администратора UEFI в интерфейсе CLI. Пароль доступен только для записи.

В следующей таблице показаны аргументы для этих параметров.

Табл. 57. Команда uefipw

В следующей многострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Параметр	Описание
-cp	Текущий пароль (не более 20 символов)
-p	Новый пароль (не более 20 символов)
-cep	Текущий пароль зашифрован
-ep	Новый пароль зашифрован

Синтаксис:
```
usage:
   uefipw [-options] - Configure the UEFI admin password
options:
   -cp      - current password (limited to 20 characters)
   -p       - new password (limited to 20 characters)
   -cep     - current password encrypted
   -ep      - new password encrypted
```

Команда usbeth

Используйте эту команду для включения или выключения внутриполосного интерфейса локальной сети через USB.

Синтаксис:
```
usbeth [options]
options:
-en <enabled|disabled>
```

Пример:
```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

Команда usbfp

Используйте эту команду, чтобы контролировать использование BMC порта USB на лицевой панели

В следующей таблице показаны аргументы для этих параметров.

Табл. 58. Команда usbfp

В следующей многострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Параметр	Описание
-mode <bmc | server | shared>	Укажите режим использования: BMC, сервер или общий
-it <minutes>	Тайм-аут после неактивности в минутах (общий режим)

Табл. 58. Команда usbfp (продолж.)

Параметр	Описание
-btn <on | off>	Включение использования кнопки идентификации для смены владельца (общий режим)
-own <bmc | server >	Указание в качестве владельца BMC или сервера (общий режим)

Команда users

Используйте эту команду для доступа ко всем учетным записям пользователей и их уровням разрешений.

Команда **users** также служит для создания новых и изменения существующих учетных записей пользователей. Если выполнить команду **users** без параметров, отобразится список пользователей и базовая информация о них. В следующей таблице показаны аргументы для этих параметров.

Табл. 59. Команда users

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-user_index	Номер индекса учетной записи пользователя	от 1 до 12 включительно или `all` для всех пользователей.
-n	Имя учетной записи пользователя	Уникальная строка, содержащая только цифры, буквы, точки и нижние подчеркивания. От 4 до 16 символов.
-p	Пароль учетной записи пользователя	Строка, содержащая по меньшей мере один буквенный и один небуквенный символ. От 6 до 20 символов. Значение Null создает учетную запись без пароля — пароль должен задать пользователь при первом входе.
-a	Уровень полномочий	Возможны следующие уровни полномочий: • `super` (администратор) • `ro` (только чтение) • Любое сочетание следующих значений, разделенных |: – `am` (доступ к управлению учетными записями пользователей) – `rca` (удаленный доступ к консоли) – `rcvma` (удаленный доступ к консоли и виртуальному носителю) – `pr` (удаленный доступ к питанию/перезапуску сервера) – `cel` (возможность очищать журналы событий) – `bc` (конфигурация адаптера — [базовая]) – `nsc` (конфигурация адаптера — [сетевые подключения и безопасность]) – `ac` (конфигурация адаптера — [расширенная])
-ep	Пароль шифрования (для резервного копирования и восстановления)	Допустимый пароль

Табл. 59. Команда users (продолж.)

Параметр	Описание	Значения
-clear	Удаление указанной учетной записи пользователя При наличии соответствующих разрешений можно удалить собственную учетную запись или учетную запись других пользователей, даже если в настоящее время они работают в системе. Исключение составляют случаи, когда речь идет о единственной оставшейся учетной записи с привилегиями управления учетными записями пользователей. Сеансы, выполнявшиеся на момент удаления учетных записей пользователей, не будут завершены автоматически.	Необходимо указать номер индекса удаляемой учетной записи пользователя в следующем формате: `users -clear -`*user_index*
-curr	Отображение пользователей, которые в настоящее время выполнили вход	
-sauth	Протокол аутентификации SNMPv3	HMAC-SHA, нет
-spriv	Протокол конфиденциальности SNMPv3	CBC-DES, AES, нет
-spw	Пароль конфиденциальности SNMPv3	Допустимый пароль
-sepw	Пароль конфиденциальности SNMPv3 (зашифрованный)	Допустимый пароль
-sacc	Тип доступа SNMPv3	get, set
-strap	Имя хоста ловушки SNMPv3	Допустимое имя хоста

Табл. 59. Команда users (продолж.)

Параметр	Описание	Значения
-pk	Отображение открытого ключа SSH для пользователя	Номер индекса учетной записи пользователя. **Примечания:** • Отображаются все назначенные пользователю ключи SSH и идентифицирующий номер индекса ключа. • При использовании параметров открытого ключа SSH необходимо использовать параметр `-pk` после индекса пользователя (параметр *-userindex*) в следующей форме: `users -2 -pk`. • Все ключи указываются в формате OpenSSH. • Для узлов Flex команды пользователей ограничены локальными учетными записями IPMI и SNMP. Параметр `-pk` для систем Flex System не поддерживается.
-e	Отображение всего ключа SSH в формате OpenSSH *(параметр открытого ключа SSH)*	Этот параметр не принимает аргументы и должен использоваться отдельно ото всех остальных параметров `users -pk`. **Примечание:** При использовании параметров открытого ключа SSH необходимо использовать параметр `-pk` после индекса пользователя (параметр *-userindex*) в следующей форме: `users -2 -pk -e`.
-remove	Удаление открытого ключа SSH для пользователя *(параметр открытого ключа SSH)*	Номер индекса удаляемого открытого ключа необходимо указывать как определенный параметр *-key_index* или `-all` для всех присваиваемых пользователю ключей. **Примечания:** • При использовании параметров открытого ключа SSH необходимо использовать параметр `-pk` после индекса пользователя (параметр *-userindex*) в следующей форме: `users -2 -pk -remove -1`. • Для узлов Flex команды пользователей ограничены локальными учетными записями IPMI и SNMP. Параметр `-remove` для систем Flex System не поддерживается.
-add	Добавление открытого ключа SSH для пользователя *(параметр открытого ключа SSH)*	Разделенный кавычками ключ в формате OpenSSH **Примечания:** • Параметр `-add` используется отдельно ото всех остальных параметров команды `users -pk`. • При использовании параметров открытого ключа SSH необходимо использовать параметр `-pk` после индекса пользователя (параметр *-userindex*) в следующей форме: `users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/ aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/ qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="` • Для узлов Flex команды пользователей ограничены локальными учетными записями IPMI и SNMP. Параметр `-add` для систем Flex System не поддерживается.

Табл. 59. Команда users (продолж.)

Параметр	Описание	Значения
-upld	Отправка открытого ключа SSH *(параметр открытого ключа SSH)*	Для указания расположения ключа требуются параметры -i и -l. **Примечания:** • Параметр -upld используется отдельно ото всех остальных параметров команды users -pk (кроме -i и -l). • Чтобы заменить ключ новым, необходимо указать *-key_index*. Чтобы добавить ключ в конец списка текущих ключей, не указывайте индекс ключа. • При использовании параметров открытого ключа SSH необходимо использовать параметр -pk после индекса пользователя (параметр *-userindex*) в следующей форме: users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key. • Для узлов Flex команды пользователей ограничены локальными учетными записями IPMI и SNMP. Параметр -upld для систем Flex System не поддерживается.
-dnld	Загрузка заданного открытого ключа SSH *(параметр открытого ключа SSH)*	Чтобы указать ключ для загрузки, требуется *-key_index*, а чтобы указать расположение загрузки на другом компьютере с сервером TFTP — параметры -i и -l. **Примечания:** • Параметр -dnld используется отдельно ото всех остальных параметров команды users -pk (кроме -i, -l и *-key_index*). • При использовании параметров открытого ключа SSH необходимо использовать параметр -pk после индекса пользователя (параметр *-userindex*) в следующей форме: users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key.
-i	IP-адрес сервера TFTP/SFTP для отправки и загрузки файла ключа *(параметр открытого ключа SSH)*	Допустимый IP-адрес **Примечание:** Параметры команд users -pk -upld и users -pk -dnld требуют параметра -i.
-pn	Номер порта сервера TFTP/SFTP *(параметр открытого ключа SSH)*	Допустимый номер порта (по умолчанию 69/22) **Примечание:** Необязательный атрибут для параметров команд users -pk -upld и users -pk -dnld.
-u	Имя пользователя для сервера SFTP *(параметр открытого ключа SSH)*	Допустимое имя пользователя **Примечание:** Необязательный атрибут для параметров команд users -pk -upld и users -pk -dnld.
-pw	Пароль для сервера SFTP *(параметр открытого ключа SSH)*	Допустимый пароль **Примечание:** Необязательный атрибут для параметров команд users -pk -upld и users -pk -dnld.
-l	Имя файла для отправки и загрузки файла ключа через TFTP или SFTP *(параметр открытого ключа SSH)*	Допустимое имя файла **Примечание:** Параметры команд users -pk -upld и users -pk -dnld требуют параметра -l.

Табл. 59. Команда users (продолж.)

Параметр	Описание	Значения
-af	Принятие подключений от хоста *(параметр открытого ключа SSH)*	Разделяемый запятыми список имен хоста и IP-адресов (не более 511 символов). Допустимые символы: буквенно-числовые, запятая, звездочка, знак вопроса, восклицательный знак, точка, дефис, двоеточие и знак процента.
-cm	Комментарий *(параметр открытого ключа SSH)*	Строка с разделителями в виде кавычек (до 255 символов). **Примечание:** При использовании параметров открытого ключа SSH необходимо использовать параметр `-pk` после индекса пользователя (параметр *-userindex*) в следующей форме: `users -2 -pk -cm "This is my comment."`.

Синтаксис:

```
users [-options] - display/configure user accounts
options:
   -[1-12]  - user account number
   -l       - display password expiration days
   -n       - username (limited to 16 characters)
   -p       - password (limited to 32 characters)
   -shp     - set hashpassword (total 64 characters)
   -ssalt   - set salt (limited to 64 characters)
   -ghp     - get hashpassword
   -gsalt   - get salt
   -ep      - encrypted password (used with backup/restore )

   -a       - authority level (super, ro, custom:am|rca|rcvma|pr|cel|bc|nsc|ac)
       -am    - User account management access
       -rca   - Remote console access
       -rcvma - Remote console and remote disk (virtual media) access
       -pr    - Remote server power/restart access
       -cel   - Ability to clear event logs
       -bc    - Adapter Configuration (basic)
       -nsc   - Adapter Configuration (network and security)
       -ac    - Adapter Configuration (advanced)

   -clear   - clear user account
   -curr    - display current users
   -sauth   (none|HMAC-SHA)           - snmpv3 authentication protocol
   -spriv   (none|CBC-DES|AES)        - snmpv3 privacy protocol
   -spw     password                    - snmpv3 privacy password
   -sepw    encryptedpassword          - snmpv3 privacy password (encrypted)
   -sacc    (Get)                  - snmpv3 Access type
   -strap   hostname                    - snmpv3 trap hostname

   -pk      - SSH public keys options:
       -e       - Displays the entire key in OpenSSH format
       -remove  - Removes the specified key for the specified user
       -add     - Adds a public key for the specified user
       -upld    - Used to upload a public key in OpenSSH/RFC4716 format
       -dnld    - Used to download the specified public key to a TFTP/SFTP server
       -i       - IP address of the TFTP/SFTP
       -pn      - port number of tftp/sftp server (default 69/22)
       -u       - username for sftp server
       -pw      - password for sftp server
       -l       - Filename of the key file when uploading or downloading via TFTP/SFTP
       -af      - accept connections from host, in the format: from="<list>", where
                  <list> is a comma-separated list of hostnames and IP addresses
                  (limited to 511 characters)
```

```
       -cm      - comment (limited to 255 characters, must be quote-delimited)
```

Примечание: -пользовательские флаги разрешений можно использовать в любых сочетаниях.

Пример:

```
system> users
 Account      Login ID      Advanced Attribute              Role            Password Expires
 -------      --------      ------------------            ------            ----------------
    1           USERID                  Native                Administrator                  89 day(s)
system> users -2 -n sptest -p PasswOrd12 -a super
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Account      Login ID      Advanced Attribute            Role              Password Expires
 -------      --------      ------------------           ------             ----------------
    1           USERID                  Native           Administrator                  90 day(s)
2           sptest                  Native                Administrator            Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -a super
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system> users -2 -n sptest -p PasswOrd12 -a custom:am|rca
The user is required to change the password when the user logs in to the management server for the first time
ok
```

Команды управления IMM

В этом разделе приводится алфавитный список команд интерфейса командной строки для управления IMM.

В настоящее время доступно 7 команд управления IMM:

Команда alertentries

Используйте эту команду для управления получателями оповещений.

- Если команда **alertentries** выполняется без параметров, отображаются все настройки записей оповещений.
- Команда **alertentries -number -test** создает тестовое оповещение для номера индекса указанного получателя.
- Команда **alertentries -number** (где number — это число от 0 до 12) отображает параметры записей оповещений для указанного номера индекса получателя и позволяет изменить параметры оповещений для этого получателя.

В следующей таблице показаны аргументы для этих параметров.

Табл. 60. Команда alertentries

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 60. Команда alertentries (продолж.)

Параметр	Описание	Значения
-number	Номер индекса получателя оповещений для отображения, добавления, изменения или удаления	от 1 до 12
-status	Состояние получателя оповещения	вкл., выкл.
-type	Тип оповещения	email, syslog
-log	Включение журнала событий в электронное оповещение	вкл., выкл.
-n	Имя получателя оповещения	Строка
-e	Адрес электронной почты получателя оповещения	Допустимый адрес электронной почты
-ip	IP-адрес или имя хоста системного журнала	Допустимый IP-адрес или имя хоста
-pn	Номер порта системного журнала	Допустимый номер порта
-del	Удаление указанного номера индекса получателя	
-test	Создание тестового оповещения для указанного номера индекса получателя	
-crt	Настройка критических событий, отправляющих уведомления	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Пользовательские настройки критических оповещений задаются с использованием разделенного вертикальными полосами списка значений в формате **alertentries -crt custom:te|vo**, где используются следующие пользовательские значения: • te: превышен критический температурный порог • vo: превышен критический порог напряжения • po: критический сбой питания • di: сбой жесткого диска • fa: сбой вентилятора • cp: сбой микропроцессора • me: сбой памяти • in: несовместимость оборудования • re: сбой резерва питания • ot: все остальные критические события
-crten	Отправка оповещений о критических событиях	включено, выключено

Табл. 60. Команда alertentries (продолж.)

Параметр	Описание	Значения
-wrn	Настройка событий типа «предупреждение», отправляющих уведомления	all, none, custom:rp|te|vo|po|fa|cp|me|ot Пользовательские настройки оповещений типа «предупреждение» задаются с использованием разделенного вертикальными полосами списка значений в формате **alertentries -wrn custom:rp|te**, где используются следующие пользовательские значения: • rp: предупреждение резерва питания • te: предупреждение о превышении температурного порога • vo: предупреждение о превышении порога напряжения • po: предупреждение о превышении порога питания • fa: некритическое событие вентилятора • cp: ухудшенное состояние микропроцессора • me: предупреждение памяти • ot: все остальные события типа «предупреждение»
-wrnen	Отправка оповещений о событиях типа «предупреждение»	включено, выключено
-sys	Настройка рутинных событий, отправляющих уведомления	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Пользовательские настройки стандартных оповещений задаются с использованием разделенного вертикальными полосами списка значений в формате **alertentries -sys custom:lo|tio**, где используются следующие пользовательские значения: • lo: успешный удаленный вход • tio: тайм-аут операционной системы • ot: все остальные информационные и системные события • po: включение/выключение питания системы • bf: сбой загрузки операционной системы • til: тайм-аут Watchdog загрузчика операционной системы • pf: прогнозируемый сбой (PFA) • el: журнал событий на 75 % полон • ne: изменение сети
-sysen	Отправка оповещений о рутинных событиях	включено, выключено

Синтаксис:

```
alertentries [options]
   options:
   -number recipient_number
      -status status
      -type alert_type
      -log include_log_state
      -n recipient_name
      -e email_address
      -ip ip_addr_or_hostname
      -pn port_number
      -del
      -test
      -crt event_type
      -crten state
```

```
-wrn event_type
-wrnen state
-sys event_type
-sysen state
```

Пример:

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

Команда batch

С помощью этой команды можно выполнить одну или несколько команд интерфейса командной строки, которые содержатся в файле.

- Строки комментариев в пакетном файле начинаются со знака #.
- При выполнении пакетного файла команды, выполнение которых завершилось ошибкой, возвращаются вместе с кодом возврата ошибки.
- Команды пакетного файла, содержащие нераспознанные параметры команд, могут вызывать создание предупреждений.

В следующей таблице показаны аргументы для этих параметров.

Табл. 61. Команда batch

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-f	Имя пакетного файла	Допустимое имя файла
-ip	IP-адрес сервера TFTP/SFTP	Допустимый IP-адрес
-pn	Номер порта сервера TFTP/SFTP	Допустимый номер порта (по умолчанию 69/22)
-u	Имя пользователя для сервера SFTP	Допустимое имя пользователя
-pw	Пароль для сервера SFTP	Допустимый пароль

Синтаксис:
```
batch [options]
option:
  -f filename
  -ip ip_address
  -pn port_number
 username
  -pw password
```

Пример:
```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

Команда clearcfg

Используйте эту команду, чтобы вернуть заводские настройки по умолчанию для конфигурации IMM.

Для отправки этой команды необходимо обладать правами настройки конфигурации адаптера по меньшей мере уровня Advanced. После очистки конфигурации IMM модуль IMM перезапускается.

Команда clock

Используйте эту команду для отображения текущих даты и времени. Можно настроить смещение UTC и параметры летнего времени.

BMC получает время от сервера хоста или сервера NTP.

Получаемое от хоста время может быть в формате местного времени или UTC. В качестве параметра хоста нужно указать UTC, если NTP не используется и хост использует формат UTC. Смещение UTC можно указать в формате +0200, +2:00, +2 или 2 (для положительных смещений) либо -0500, -5:00 или -5 для отрицательных смещений. Смещение UTC и параметры летнего времени используются с NTP или если в качестве режима хоста задан UTC.

Для смещения UTC +2, -7, -6, -5, -4 и -3 требуются специальные настройки летнего времени.

- Для смещения +2 используются следующие настройки летнего времени: off, ee (Восточная Европа), tky (Турция), bei (Бейрут), amm (Амман), jem (Иерусалим).
- Для смещения -7 используются следующие настройки летнего времени: off, mtn (горное), maz (Масатлан).
- Для смещения -6 используются следующие настройки летнего времени: off, mex (Мексика), cna (центральная Северная Америка).
- Для смещения -5 используются следующие настройки летнего времени: off, cub (Куба), ena (восточная Северная Америка).
- Для смещения -4 используются следующие настройки летнего времени: off, asu (Асунсьон), cui (Куяба), san (Сантьяго), cat (Канада — Атлантика).
- Для смещения -3 используются следующие настройки летнего времени: off, gtb (Готхоб), bre (Бразилия — восток).

Синтаксис:
```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
```

```
Windows systems use local, Linux uses utc
```

Пример:
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

Команда identify

Используйте эту команду для включения, выключения и перевода в режим мигания светодиодного индикатора идентификации на раме.

Параметр **-d** можно использовать вместе с параметром **-s on** для включения светодиодного индикатора на время в секундах, заданное с помощью параметра **-d**. По истечение указанного срока в секундах светодиодный индикатор выключается.

Синтаксис:
```
identify [options]
options:
-s on/off/blink
-d seconds
```

Пример:
```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

Команда info

Используйте эту команду для отображения и настройки сведений об IMM.

Если выполнить команду **info** без параметров, отобразятся все сведения о местоположении и контактах IMM. В следующей таблице показаны аргументы для этих параметров.

Табл. 62. Команда info

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-name	Имя IMM	Строка
-contact	Имя контактного лица IMM	Строка
-location	Расположение IMM	Строка
-room[1]	Идентификатор помещения IMM	Строка
-rack[1]	Идентификатор стойки IMM	Строка
-rup[1]	Положение IMM в стойке	Строка
-ruh	Высота отсека стойки	Только чтение
-bbay	Расположение отсека для блейд-серверов	Только чтение

1. Это значение доступно только для чтения и не может быть сброшено, если IMM находится в системе Flex System.

Синтаксис:
```
info [options]
option:
  -name xcc_name
  -contact contact_name
  -location xcc_location
  -room room_id
  -rack rack_id
  -rup rack_unit_position
  -ruh rack_unit_height
  -bbay blade_bay
```

Команда spreset

Используйте эту команду для перезапуска IMM.

Для отправки этой команды необходимо обладать правами настройки конфигурации адаптера по меньшей мере уровня Advanced.

Команды без агентов

В этом разделе приводится алфавитный список команд без агентов.

В настоящее время доступно 3 команды без агентов:

Команда storage

Используйте эту команду для отображения и настройки (если поддерживается платформой) сведений об устройствах хранения сервера, управление которыми осуществляется с помощью IMM.

В следующей таблице показаны аргументы для этих параметров.

Табл. 63. Команда storage

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Табл. 63. Команда storage (продолж.)

Параметр	Описание	Значения
-list	Перечисляет все целевые объекты хранения, управляемые IMM.	*controllers*|*pools*|*volumes*|*drives* Где *target* — это: • *controllers*: список поддерживаемых контроллеров RAID[1] • *pools*: список пулов памяти, связанных с контроллером RAID[1] • *volumes*: список томов хранилища, связанных с контроллером RAID[1] • *drives*: список устройств хранения данных, связанных с контроллером RAID[1]
-list -target *target_id*	Список объектов *target* хранилища, управляемых IMM по *target_id*.	*pools*|*volumes*|*drives ctrl[x]*|*pool[x]* Где *target* и *target_id* — это: • *pools ctrl[x]*: список пулов памяти, связанных с контроллером RAID, по target_id[1] • *volumes ctrl[x]*|*pool[x]*: список томов хранилища, связанных с контроллером RAID, по target_id[1] • *drives ctrl[x]*|*pool[x]*: список устройств хранения, связанных с контроллером RAID, по target_id[1]
-list flashdimms	Список флэш-модулей DIMM, управляемых IMM.	
-list devices	Отображает состояние всех дисков и флэш-модулей DIMM, управляемых IMM.	
-show *target_id*	Отображает сведения для выбранного объекта target, управляемого IMM.	Где *target_id* — это: *ctrl[x]*|*vol[x]*|*disk[x]*|*pool[x]* |*flashdimm[x]* [3]
-show *target_id* info	Отображает подробные сведения для выбранного объекта target, управляемого IMM.	Где *target_id* — это: *ctrl[x]*|*vol[x]*|*disk[x]*|*pool[x]* |*flashdimm[x]* [3]
-show *target_id firmware*[3]	Отображает сведения о микропрограмме для выбранного объекта target, управляемого IMM.	Где *target_id* — это: *ctrl[x]*|*disk[x]*|*flashdimm[x]*[2]
-showlog *target_id<m:n*|*all>*[3]	Отображает журналы событий для выбранного объекта target, управляемого IMM.	Где *target_id* — это: *ctrl[x]*[4] *m:n*|*all* Где *m:n* — количество журналов событий от одного до максимального Где *all* — это все журналы событий
-config ctrl -scanforgn -target *target_id*[3]	Обнаружение конфигурации внешнего RAID.	Где *target_id* — это: *ctrl[x]*[5]

Табл. 63. Команда storage (продолж.)

Параметр	Описание	Значения
-config ctrl -imptforgn -target *target_id*[3]	Импорт конфигурации внешнего RAID.	Где *target_id* — это: *ctrl[x]*[5]
-config ctrl -clrforgn -target *target_id*[3]	Очистка конфигурации внешнего RAID.	Где *target_id* — это: *ctrl[x]*[5]
-config ctrl -clrcfg -target *target_id*[3]	Очистка конфигурации RAID.	Где *target_id* — это: *ctrl[x]*[5]
-config drv -mkoffline -target *target_id*[3]	Изменение состояния диска с «в сети» на «не в сети».	Где *target_id* — это: *disk[x]*[5]
-config drv -mkonline -target *target_id*[3]	Изменение состояния диска с «не в сети» на «в сети».	Где *target_id* — это: *disk[x]*[5]
-config drv -mkmissing -target *target_id*[3]	Обозначение диска не в сети в качестве исправного ненастроенного диска.	Где *target_id* — это: *disk[x]*[5]
-config drv -prprm -target *target_id*[3]	Подготовка исправного ненастроенного диска к извлечению.	Где *target_id* — это: *disk[x]*[5]
-config drv -undoprprm -target *target_id*[3]	Отмена подготовки исправного ненастроенного диска к извлечению.	Где *target_id* — это: *disk[x]*[5]
-config drv -mkbad -target *target_id*[3]	Изменение исправного ненастроенного диска на неисправный ненастроенный диск.	Где *target_id* — это: *disk[x]*[5]
-config drv -mkgood -target *target_id*[3]	Изменение неисправного ненастроенного диска на исправный ненастроенный диск. или Преобразование диска JBOD в исправный ненастроенный диск.	Где *target_id* — это: *disk[x]*[5]
-config drv -addhsp *-[выделенные пулы]* -target *target_id*[3]	Назначение выделенного диска в качестве горячего резерва для отдельного контроллера или существующих пулов памяти.	Где *target_id* — это: *disk[x]*[5]
-config drv -rmhsp -target *target_id*[3]	Извлечение горячего резерва.	Где *target_id* — это: *disk[x]*[5]
-config vol -remove -target *target_id*[3]	Извлечение отдельного тома.	Где *target_id* — это: *vol[x]*[5]

Табл. 63. Команда storage (продолж.)

Параметр	Описание	Значения
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target *target_id*[3]	Изменение свойств отдельного тома.	• [-N *volume_name*] — это имя тома • [-w <*0*|*1*|*2*>] — это политика записи кэша: – Введите *0* для политики сквозной записи – Введите *1* для политики обратной записи – Введите *2* для политики записи с резервным блоком батареи (BBU) • [-r <*0*|*1*|*2*>] — это политика чтения кэша: – Введите *0* для политики запрета упреждающего чтения – Введите *1* для политики упреждающего чтения – Введите *2* для политики адаптивного упреждающего чтения • [-i <*0*|*1*>] — это политика ввода-вывода кэша: – Введите *0* для политики прямого ввода-вывода – Введите *1* для политики кэшированного ввода-вывода • [-a <*0*|*2*|*3*>] — это политика доступа: – Введите *0* для политики чтения и записи – Введите *2* для политики «только чтение» – Введите *3* для политики «Заблокировано» • [-d <*0*|*1*|*2*>] — это политика кэширования дисков: – Введите *0*, если политика не меняется – Введите *1*, чтобы включить политику[6] – Введите *2*, чтобы выключить политику • [-b <*0*|*1*>] — это фоновая инициализация: – Введите *0*, чтобы включить инициализацию – Введите *1*, чтобы выключить инициализацию • *-target_id* — это *vol[x]*[5]
-config vol -add<[-R] [-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r][3],[7]	Создание отдельного тома для нового пула памяти, если целевым объектом является контроллер. или Создание отдельного тома с существующим пулом памяти, если целевым объектом является пул памяти.	• [-R <*0*|*1*|*5*|*1E*|*6*|*10*|*50*|*60*|*00*|*1ERLQ0*|*1E0RLQ0*>] Этот параметр определяет уровень RAID и используется только с новым пулом памяти • [-D disk *[id11]:disk[id12]:..disk[id21]:disk[id22]:..*] Этот параметр определяет группу дисков (включая охваченные объекты) и используется только с новым пулом памяти • [-H disk *[id1]:disk[id2]:..*] Этот параметр определяет группу горячего резервирования и используется только с новым пулом памяти. • [-1 hole] Этот параметр определяет номер индекса свободного пространства для существующего пула памяти

Табл. 63. Команда storage (продолж.)

Параметр	Описание	Значения
		• [-N *volume_name*] — это имя тома • [-w <*0*|*1*|*2*>] — это политика записи кэша: – Введите *0* для политики сквозной записи – Введите *1* для политики обратной записи – Введите *2* для политики записи с резервным блоком батареи (BBU) • [-r <*0*|*1*|*2*>] — это политика чтения кэша: – Введите *0* для политики запрета упреждающего чтения – Введите *1* для политики упреждающего чтения – Введите *2* для политики адаптивного упреждающего чтения
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target *target_id*[3]	Создание отдельного тома для нового пула памяти, если целевым объектом является контроллер. или Создание отдельного тома с существующим пулом памяти, если целевым объектом является пул памяти.	• [-i <*0*|*1*>] — это политика ввода-вывода кэша: – Введите *0* для политики прямого ввода-вывода – Введите *1* для политики кэшированного ввода-вывода • [-a <*0*|*2*|*3*>] — это политика доступа: – Введите *0* для политики чтения и записи – Введите *2* для политики «только чтение» – Введите *3* для политики «Заблокировано» • [-d <*0*|*1*|*2*>] — это политика кэширования дисков: – Введите *0*, если политика не меняется – Введите *1*, чтобы включить политику [6] – Введите *2*, чтобы выключить политику • [-f <*0/1/2*>] — это тип инициализации: – Введите *0*, чтобы обозначить отсутствие инициализации – Введите *1* для быстрой инициализации – Введите *2* для полной инициализации • [-S *volume_size*] — это размер нового тома в МБ • [-P *strip_size*] — это размер чередования тома, например 128K или 1M • -target *target_id*: – *ctrl[x]* (новый пул памяти)[5] – *pool[x]* (существующий пул памяти)[5]

Табл. 63. Команда storage (продолж.)

Параметр	Описание	Значения
-config vol -getfreecap [-R] [-D disk] [-H disk] -target *target_id*[3]	Получение объема свободного пространства в дисковой группе.	• [-R *<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>*] Этот параметр определяет уровень RAID и используется только с новым пулом памяти • [-D disk *[id11]:[id12]:..[id21]:[id22]:..*] Этот параметр определяет группу дисков (включая охваченные объекты) и используется только с новым пулом памяти • [-H disk *[id1]:[id2]:..*] Этот параметр определяет группу горячего резервирования и используется только с новым пулом памяти. • -target *target_id*: – *ctrl[x]*[5]
-help	Отображение сведений об использовании команды и параметров	

Примечания:
1. Эта команда поддерживается только на серверах, где IMM может осуществлять доступ к контроллеру RAID.
2. Сведения о микропрограмме отображаются только для связанных контроллеров, дисков и флэш-модулей DIMM. Сведения о микропрограмме для связанных пулов и томов не отображаются.
3. Информация отображается на нескольких строках из-за нехватки места.
4. Эта команда поддерживается только на серверах, поддерживающих журналы RAID.
5. Эта команда поддерживается только на серверах, поддерживающих конфигурации RAID.
6. Значение *Enable* не поддерживает конфигурации RAID первого уровня.
7. Здесь приводится неполный список доступных параметров. Остальные параметры команды **storage -config vol -add** перечислены в следующей строке.

Синтаксис:
```
storage [options]
option:
  -config ctrl|drv|vol -option [-options] -target target_id
  -list controllers|pools|volumes|drives
  -list pools -target ctrl[x]
  -list volumes -target ctrl[x]|pool[x]
  -list drives -target ctrl[x]|pool[x]
  -list devices
  -list flashdimms
  -show target_id
  -show {ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]} info
  -show {ctrl[x]|disk[x]|flashdimm[x]}firmware
  -showlog ctrl[x]m:n|all
  -h help
```

Примеры:
```
system> storage
-config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage
-config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage
```

```
-config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage
-config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage
-config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage
-config drv -addhsp -target disk[0-0]
ok
system>
system> storage
-config drv -mkbad -target disk[0-0]
ok
system>
system> storage
-config drv -mkgood -target disk[0-0]
ok
system>
system> storage
-config drv -mkmissing -target disk[0-0]
ok
system>
system> storage
-config drv -mkoffline -target disk[0-0]
ok
system>
system> storage
-config drv -mkonline -target disk[0-0]
ok
system>
system> storage
-config drv -prprm -target disk[0-0]
ok
system>
system> storage
-config drv -rmhsp -target disk[0-0]
ok
system>
system> storage
-config drv -undoprprm -target disk[0-0]
ok
system>
system> storage
-config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage
-config vol -add -R 1 -D disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage
-config vol -getfreecap -R 1 -D disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage
```

```
-config vol -remove -target vol[0-1]
ok
system>
system> storage
-config vol -set -N LD_volume -w 0 -target vol[0-0]
ok
system>
system> storage
-list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage
-list drives
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage
-list volumes
system>storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
system> storage
-list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list drives -target pool[0-0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
system> storage
-list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
system> storage
-list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
```

```
system> storage
-show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
Storage Pool 0
Storage Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
```

```
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>
system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage
-show vol[0-0] info
Name: LD_volume
```

```
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

Команда adapter

Эта команда служит для отображения инвентарных сведений об адаптере PCIe.

Если команда **adapter** не поддерживается, сервер реагирует на отправку такой команды следующим сообщением:
`Your platform does not support this command.`
При снятии, замене или настройке любых адаптеров необходимо перезапустить сервер (по меньшей мере один раз), чтобы увидеть обновленную информацию об адаптере.

В следующей таблице показаны аргументы для этих параметров.

Табл. 64. Команда adapter

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	Описание	Значения
-list	Перечисление всех адаптеров PCIe на сервере	
-show *target_id*	Отображение подробной информации о целевом адаптере PCIe	*target_id [info|firmware|ports|chips]* Где: • *info*: отображение сведений об оборудовании адаптера • *firmware*: отображение всех сведений о микропрограммах адаптера • *ports*: отображение всех сведений о портах Ethernet адаптера • *chips*: отображение всех сведений о микросхеме графического процессора адаптера
-h	Отображение сведений об использовании команды и параметров	

Синтаксис:
```
adapter [options]
option:
  -list
  -show target_id [info|firmware|ports|chips]
  -h help
```

Примеры:
```
system> adapter
```

```
list
ob-1     Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2     GPU Card 1
slot-1   Raid Controller 1
slot-2   Adapter 01:02:03
system> adapter
show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
```

```
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
```

Команда m2raid

Используйте эту команду для получения информации о запасах, связанную с M.2, и управлении виртуальными томами.

В следующей таблице показаны аргументы для этих параметров.

Табл. 65. Команда m2raid

В следующей многострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Параметр	Описание
-h/?	Печать справочных сведений для этой команды
-version	Отображение информации о микропрограмме контроллера
-disks	Отображение информации о мультимедийных дисках
-volumes	Отображении информации о виртуальных томах
-create	Создание виртуального тома, параметрам VD_Name, RaidLevel и StripeSize можно задать значения
-delete	Удаление виртуального тома
-import	Импорт внешнего виртуального тома. После импорта виртуального тома он будет автоматически восстановлен при перезагрузке системы.

Использование

```
m2raid [-options] - raid configuration for M.2 adapter with Mirroring Enablem
options:
   -version                    - displays controller firmware version.
   -disks                      - displays information of media disks.
   -volumes                    - displays information of virtual volumes
   -create -VD_Name <nameStr> -RaidLevel <0|1> -StripeSize <32|64>  - create virt
   -delete -VD_ID <0|1>       - delete the virtual volume
   -import -VD_ID <0|1>       - import a foreign virtual volume
```

Пример

```
system> m2raid -version
    ThinkSystem M.2 with Mirroring Enablement Kit
 Firmware Version = 2.3.10.1193

system> m2raid -disks
    M.2 Bay0          32GB M.2 SATA SSD     LEN     100%
M.2 Bay1          32GB M.2 SATA SSD     LEN      100%

system> m2raid -volumes
    VD_ID    VD_Name    RaidLevel    StripSize    VD Capacity    Status
     0       M2RAID       1              64k          29 GB           Optimal
```

```
system> m2raid -delete -VD_ID 0
VD_ID 0 is deleted

system> m2raid -create -VD_Name M2RAID -RaidLevel 1 -StripeSize 64
New volume is created

system> m2raid -import -VD_ID 0
VD_ID 0 is imported
```

Команды поддержки

В этом разделе приводится алфавитный список команд поддержки.

Доступна лишь одна команда поддержки: «Команда dbgshimm» на странице 189.

Команда dbgshimm

Используйте эту команду для разблокировки сетевого доступа к оболочке безопасной отладки.

Примечание: Эта команда предназначена для использования только специалистами по поддержке.

В следующей таблице показаны аргументы для этих параметров.

Табл. 66. Команда dbgshimm

В следующей многострочной таблице с двумя столбцами приводятся параметры этой команды и соответствующие описания.

Параметр	Описание
status	Отображение состояния
включить	Включение доступа к отладке (по умолчанию, если параметр не задан)
отключить	Выключение доступа к отладке

Глава 11. Интерфейс IPMI

В этой главе описан интерфейс IPMI, который поддерживается XClarity Controller.

Сведения о стандартных командах IPMI см. в спецификации интерфейса IPMI (версия 2.0 и выше). В этом документе характеризуются параметры OEM, используемые со стандартными IPMI-командами IPMI и OEM, которые поддерживаются микропрограммой XClarity Controller.

Управление XClarity Controller с помощью IPMI

Воспользуйтесь информацией из этого раздела для управления XClarity Controller с использованием интерфейса управления платформой (IPMI).

XClarity Controller поставляется с идентификатором пользователя, для которого изначально настроено имя пользователя USERID и пароль PASSW0RD (ноль, а не буква «O»). Этот пользователь имеет уровень доступа «Администратор».

Важно: В целях безопасности измените это имя пользователя и пароль во время первоначальной настройки.

В системе Flex System пользователь может настроить модуль CMM Flex System для централизованного управления учетными записями пользователей IPMI XClarity Controller. В этом случае вы, возможно, не сможете осуществлять доступ к XClarity Controller с использованием IPMI до тех пор, пока CMM не настроит идентификаторы пользователей IPMI.

Примечание: Учетные данные пользователя User ID, настраиваемого CMM, могут отличаться от вышеописанной комбинации USERID/PASSW0RD. Если модуль CMM не настроил никаких учетных записей пользователя IPMI, сетевой порт, связанный с протоколом IPMI, будет закрыт.

XClarity Controller также предоставляет следующие функции удаленного управления сервером IPMI:

Интерфейсы командной строки IPMI
Интерфейс командной строки IPMI предоставляет прямой доступ к функциям управления сервером по протоколу IPMI 2.0. IPMItool можно использовать для отправки команд по управлению питанием сервера, просмотру сведений о сервере и идентификации сервера. Дополнительные сведения об IPMItool см. в разделе «Использование IPMItool» на странице 191.

Перенаправление последовательного порта через локальную сеть
Чтобы управлять серверами из удаленного расположения, воспользуйтесь IPMItool для установки последовательного подключения по локальной сети (SOL). Дополнительные сведения об IPMItool см. в разделе «Использование IPMItool» на странице 191.

Использование IPMItool

Воспользуйтесь информацией из этого раздела для получения доступа к информации об инструменте IPMItool.

IPMItool предоставляет различные инструменты, которые можно использовать для настройки системы IPMI и управления ею. IPMItool можно использовать во внутриполосном и внеполосном режиме для настройки и управления XClarity Controller.

Дополнительные сведения и загрузка IPMItool доступны на сайте https://github.com/ipmitool/ipmitool.

Команды IPMI с параметрами OEM

Получение/задание параметров конфигурации локальной сети

Чтобы реализовать возможности, предоставляемые XCC для некоторых сетевых настроек, некоторые параметры необходимо задать так, как показано ниже.

DHCP

В дополнение к стандартным методам получения IP-адреса XCC поддерживает режим, в котором XCC пытается получить IP-адрес с сервера DHCP в течение определенного периода и если эти попытки завершаются неудачей, система переходит на использование статического IP-адреса.

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	#	Данные параметров
Источник IP-адреса	4	data 1 [7:4] — зарезервировано [3:0] — источник адреса 0h = не задано 1h = статический адрес (настраивается вручную) 2h = адрес, полученный XCC при выполнении DHCP 3h = адрес, полученный BIOS или программным обеспечением системы 4h = адрес, полученный XCC при выполнении другого протокола назначения адресов. XCC использует значение 4h, чтобы указать режим адреса DHCP с переходом на статический в случае сбоя.

Выбор интерфейса Ethernet

Оборудование XCC включает двойные контроллеры MAC Ethernet 10/100 с интерфейсами RMII. Оборудование XCC также включает двойные контроллеры MAC Ethernet 1 Гбит/с с интерфейсами RGMII. Один из контроллеров MAC, как правило, подключен к общей карте NIC сервера, а другой используется в качестве выделенного порта управления системой. В определенный момент времени на сервере может быть активен только один порт Ethernet. Невозможно одновременно включить оба порта.

На некоторых серверах специалисты по проектированию систем могут принять решение о подключении в планарном корпусе системы только один из этих интерфейсов Ethernet. В таких системах XCC поддерживает только интерфейс Ethernet, который подключен к планарному корпусу. Запрос на использование неподключенного порта возвращает код выполнения CCh.

Идентификаторы пакетов для всех дополнительных сетевых карт нумеруются следующим образом:

- дополнительная карта 1, ИД пакета = 03h (eth2),
- дополнительная карта 2, ИД пакета = 04h (eth3),

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	**#**	**Данные параметров**
Параметр OEM Этот номер параметра используется XCC, чтобы указать, какой из возможных портов Ethernet (логических пакетов) следует использовать. Этот параметр в команде «Получение/задание параметров конфигурации локальной сети» не использует средство выбора наборов и не требует средство выбора блоков, так что для этих полей необходимо задать значение 00h. Данные отклика возвращают 3 байта или 4 байта, если устройство находится в пакете NCSI. Байт 1 = код выполнения Байт 2 = редакция Байт 3 = 00h для eth0 или 01h для eth1 и т. д... Байт 4 = (необязательно) номер канала, если устройство находится в пакете NCSI	C0h	data1 00h = eth0 01h = eth1 02h = eth2 и т. д... FFh = отключить все внешние сетевые порты) XCC поддерживает второй дополнительный байт данных, который указывает, какой канал в пакете используется data2 00h = канал 0 01h = канал 1 и т. д... Если в запросе не указано значение data2, подразумевается канал 0

Байт data1 используется для указания логического пакета. Это может быть выделенная карта NIC для управления системой или интерфейс NCSI в используемой совместно с сервером карте NIC.

Байт data2 используется для указания канала для логического пакета, если пакет представляет собой устройство NCSI. Если значение data2 в запросе не указано и логический пакет представляет собой устройство NCSI, подразумевается канал 0. Если значение data2 в запросе указано, но логический пакет не является устройством NCSI, информация о канале игнорируется.

Примеры:

Приложение A. Если канал 2 общей карты NIC в планарном корпусе (ИД пакета = 0, eth0) следует использовать в качестве порта управления, вводные данные будут иметь следующий вид: 0xC0 0x00 0x02

Приложение B. Если следует использовать первый канал первой мезонинной сетевой карты, вводные данные должны иметь следующий вид: 0xC0 0x02 0x0

Включение/выключение Ethernet через USB

Параметр ниже используется для включения или выключения внутриполосного интерфейса XCC.

В следующей многострочной таблице с тремя столбцами приводятся параметры, описание параметров и соответствующие значения для этих параметров.

Параметр	**#**	**Данные параметров**
Параметр OEM (Этот номер параметра используется XCC для включения или выключения интерфейса Ethernet через USB.) Этот параметр в команде «Получение параметров конфигурации локальной сети» не использует средство выбора наборов и не требует средство выбора блоков, так что для этих полей необходимо задать значение 00h. Данные отклика возвращают 3 байта: Байт 1 = код выполнения Байт 2 = редакция Байт 3 = 00h (выключено) или 01h (включено)	C1h	data 1 0x00 = выключено 0x01 = включено

Байт data1 используется для указания логического пакета. Это может быть выделенная карта NIC для управления системой или интерфейс NCSI в используемой совместно с сервером карте NIC.

Байт data2 используется для указания канала для логического пакета, если пакет представляет собой устройство NCSI. Если значение data2 в запросе не указано и логический пакет представляет собой устройство NCSI, подразумевается канал 0. Если значение data2 в запросе указано, но логический пакет не является устройством NCSI, информация о канале игнорируется.

Примеры:

Приложение A. Если канал 2 общей карты NIC в планарном корпусе (ИД пакета = 0, eth0) следует использовать в качестве порта управления, вводные данные будут иметь следующий вид: 0xC0 0x00 0x02

Приложение B. Если следует использовать первый канал первой мезонинной сетевой карты, вводные данные должны иметь следующий вид: 0xC0 0x02 0x0

Параметр IPMI для получения DUID-LLT

Дополнительное доступное только для чтения значение, которое необходимо предоставлять через IPMI, — DUID. Согласно RFC3315, такой формат DUID основан на адресе уровня ссылки плюс время.

Параметр	#	Данные параметров
Параметр OEM (Этот номер параметра используется XCC для включения или выключения интерфейса Ethernet через USB.) Этот параметр в команде «Получение параметров конфигурации локальной сети» не использует средство выбора наборов и не требует средство выбора блоков, так что для этих полей необходимо задать значение 00h. Данные отклика возвращают 3 байта: Байт 1 = код выполнения Байт 2 = редакция параметра (как в спецификации IPMI) Байт 3 = длина следующих байтов данных (в настоящее время 16 байтов) Байт 4-n DUID_LLT	C2h	

Параметры конфигурации Ethernet

Параметры ниже можно использовать для настройки конкретных параметров Ethernet.

Параметр	#	Данные параметров
Параметр OEM (Этот номер параметра используется XCC для включения или выключения настройки автоматического согласования для интерфейса Ethernet.) Данные отклика возвращают 3 байта: Байт 1 = код выполнения Байт 2 = редакция Байт 3 = 00h (выключено) или 01h (включено)	C3h	data 1 0x00 = выключено 0x01 = включено Примечание. В системах Flex и Stark настройку автосогласования изменить невозможно, поскольку в этом случае может нарушиться путь сетевой связи через CMM и SMM.
Параметр OEM (Этот номер параметра используется XCC для получения или задания скорости обмена данными по интерфейсу Ethernet.) Данные отклика возвращают 3 байта: Байт 1 = код выполнения Байт 2 = редакция Байт 3 = 00h (10 Мбит/с) или 01h (100 Мбит/с)	C4h	data 1 0x00 = 10 Мбит 0x01 = 100 Мбит
Параметр OEM (Этот номер параметра используется XCC для получения или задания параметра Duplex интерфейса Ethernet.) Данные отклика возвращают 3 байта: Байт 1 = код выполнения Байт 2 = редакция Байт 3 = 00h (полудуплекс) или 01h (полный дуплекс)	C5h	data 1 0x00 = полудуплекс 0x01 = полный дуплекс

Параметр	#	Данные параметров
Параметр OEM (Этот номер параметра используется XCC для получения или задания максимальной единицы передачи интерфейса Ethernet.) Данные отклика возвращают 3 байта: Байт 1 = код выполнения Байт 2 = редакция Байт 3–4 = размер максимальной единицы передачи	C6h	data 1 Размер максимальной единицы передачи
Параметр OEM (Этот номер параметра используется XCC для получения или задания администрируемого локально MAC-адреса.) Данные отклика возвращают 3 байта: Байт 1 = код выполнения Байт 2 = редакция Байт 3–8 = MAC-адрес	C7h	data 1–6 Mac-адрес

Параметр IPMI для получения локального адреса ссылки

Это доступный только для чтения параметр для получения локального адреса ссылки IPV6.

Параметр	#	Данные параметров
Параметр OEM Этот параметр служит для получения локального адреса ссылки XCC. Данные отклика возвращают следующее: Байт 1 = код выполнения Байт 2 = редакция параметра (как в спецификации IPMI) Байт 3 = длина префикса адреса IPV6 Байт 4–19 — локальный адрес ссылки в двоичном формате	C8h	

Параметр IPMI для включения/выключения IPv6

Это доступный для чтения/записи параметр, позволяющий включить/выключить IPV6 в XCC.

Параметр	#	Данные параметров
Параметр OEM Этот параметр служит для включения/выключения IPv6 в XCC Данные отклика возвращают следующее: Байт 1 = код выполнения Байт 2 = редакция параметра (как в спецификации IPMI) Байт 3 = 00h (выключено) или 01h (включено)	C9h	data 1 0x00 = выключено 0x01 = включено

Сквозная передача по Ethernet через USB во внешнюю сеть

Параметр ниже служит для настройки сквозной передачи по Ethernet через USB во внешнюю сеть.

Параметр	#	Данные параметров
Параметр OEM Этот параметр в команде «Получение/задание параметров конфигурации локальной сети» не использует средство выбора наборов и не требует средство выбора блоков, так что для этих полей необходимо задать значение 00h. Данные отклика Get возвращают следующее: Байт 1 = код выполнения Байт 2 = редакция Байт 3 = зарезервировано (00h) Байты 4:5 = номер порта Ethernet через USB (сначала LSByte) Байты 6:7 = внешний номер порта Ethernet (сначала LSByte) Число последующих байтов может варьироваться (1, 4 или 16) в зависимости от режима адресации: • Байт 8 = предварительно определенные режимы: 00h = сквозная передача отключена 01h = используется IP-адрес CMM Байты 8:11 = внешний сетевой IP-адрес IPv4 в двоичном формате Байты 8:23 = внешний сетевой IP-адрес IPv6 в двоичном формате Коды выполнения: 00h — успешно 80h — параметр не поддерживается C1h — команда не поддерживается C7h — недопустимая длина данных запроса	CAh	Задание параметров конфигурации локальной сети: data 1 зарезервировано (= 00h) data 2:3 Номер порта Ethernet через USB, сначала LSByte data 4:5 Внешний номер порта Ethernet, сначала LSByte Число последующих байтов может варьироваться (1, 4 или 16) в зависимости от режима адресации: data 6 00h = отключить сквозную передачу 01h = использовать IP-адрес CMM data 6:9 Внешний сетевой IP-адрес IPv4 в двоичном формате data 6:21 Внешний сетевой IP-адрес IPv6 в двоичном формате
Параметр OEM Этот параметр служит для задания и получения IP-адреса локальной сети через USB и маски сети XCC: Данные отклика возвращают следующее: Байт 1 = код выполнения	CBh	Data 1:4 IP-адрес интерфейса локальной сети через USB на стороне XCC. Data 5:8 Маска сети интерфейса локальной сети через USB на стороне XCC

Параметр	#	Данные параметров
Байт 2 = редакция параметра (как в спецификации IPMI) Байт 3:10 = сначала IP-адрес и значение маски сети (MS-byte)		
Параметр OEM Этот параметр служит для задания и получения IP-адреса локальной сети через USB операционной хост-системы: Данные отклика возвращают следующее: Байт 1 = код выполнения Байт 2 = редакция параметра (как в спецификации IPMI) Byte 3:6 = сначала IP-адрес (MS-byte)	CCh	Data 1:4 IP-адрес интерфейса локальной сети через USB на стороне хоста.

Запрос количества логических пакетов

Параметр ниже используется для запроса данных о количестве пакетов NCSI.

Параметр	#	Данные параметров
Параметр OEM Этот параметр в команде «Получение/задание параметров конфигурации локальной сети» не использует средство выбора наборов и не требует средство выбора блоков, так что для этих полей необходимо задать значение 00h. Операция запроса количества пакетов Операция запроса информации о пакетах выполняется путем отправки запроса с двумя байтами данных 0x00 вместе с номером параметра D3h. Запрос количества пакетов: --> 0x0C 0x02 0x00 0xD3 0x00 0x00 Отклик XCC включает по байту информации для каждого из присутствующих пакетов: биты 7:4 = число каналов NCSI в пакете биты 3:0 = номер логического пакета Отклик --> 0x00 0x00 0x40 0x01 0x32 указывает, что присутствует 3 логических пакета: у пакета 0 — 4 канала NCSI пакет 1 не является картой NIC NCSI, так что он не поддерживает каналы NCSI у пакета 2 — 3 канала NCSI	D3h	Получение/задание параметров конфигурации локальной сети:

Получение/задание данных логических пакетов

Параметр ниже служит для чтения и задания приоритета, назначенного каждому пакету.

Параметр	#	Данные параметров
Параметр OEM Этот параметр в команде «Получение/задание параметров конфигурации локальной сети» не использует средство выбора наборов и не требует средство выбора блоков, так что для этих полей необходимо задать значение 00h. Эта команда поддерживает 2 операции: • Чтение приоритета пакета • Задание приоритета пакета Операция чтения приоритета пакета Операция чтения приоритета пакета выполняется путем отправки запроса с двумя байтами данных 0x00 вместе с номером параметра D4h. Чтение приоритета пакета: --> 0x0C 0x02 0x01 0xD4 0x00 0x00 Отклик --> 0x00 0x00 0x00 0x12 0x23 логический пакет 0 = приоритет 0 логический пакет 2 = приоритет 1 логический пакет 3 = приоритет 2 Операция задания приоритета пакета Операция задания приоритета пакета выполняется путем отправки запроса с 1 или более параметров вместе с номером параметра D4h. Задание приоритета пакета: --> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23	D4	Получение/задание параметров конфигурации локальной сети: Бит [7–4] = приоритет логического пакета (1 = самый высокий, 15 = самый низкий) Бит [3–0]= номер логического пакета

Параметр	#	Данные параметров
задать логический пакет 0 = приоритет 0 задать логический пакет 2 = приоритет 1 задать логический пакет 3 = приоритет 2 Отклик: только код выполнения, без дополнительных данных		

Получение/задание статуса сетевой синхронизации XCC

Параметр	#	Данные параметров
Параметр OEM Этот байт служит для настройки синхронизации сетевых настроек выделенного и общего режима NIC Этот параметр в команде «Получение параметров конфигурации локальной сети» не использует средство выбора наборов и не требует средство выбора блоков, так что для этих полей необходимо задать значение 00h. Данные отклика возвращают 3 байта: Байт 1 = код выполнения Байт 2 = редакция Байт 3 = 00h (включено) или 01h (выключено)	D5h	data 1 0x00 = синхронизация 0x01 = независимая работа

Этот байт служит для настройки синхронизации сетевых настроек выделенного и общего режима NIC. Значение по умолчанию — 0h. Это значит, что XCC будет автоматически обновлять сетевые настройки при изменении режима и использовать параметры совместного использования NIC (на плате) в качестве основного ориентира. Если задано значение 1h, каждая сетевая настройка будет использоваться по отдельности. Это значит, что можно задать разные сетевые настройки для каждого режима, например включить VLAN в выделенном режиме и выключить VLAN в общем режиме NIC.

Получение/задание сетевого режима XCC

Параметр	#	Данные параметров
Параметр OEM Этот параметр служит для получения/задания сетевого режима карты NIC для управления XCC. Данные отклика возвращают 4 байта: Байт 1 = код выполнения Байт 2 = редакция Байт 3 = примененный/ указанный сетевой режим Байт 4 = ИД пакета примененного сетевого режима Байт 5 = ИД канала примененного сетевого режима	D6h	Задание параметров конфигурации локальной сети: data 1 Задаваемый сетевой режим Получение параметров конфигурации локальной сети: data 1 Получаемый сетевой режим, это необязательные данные, по умолчанию запрашивается текущий сетевой режим

OEM-команды IPMI

XCC поддерживает следующие OEM-команды IPMI. Для выполнения каждой команды требуется разный уровень привилегий, как указано ниже.

Код	Команды Netfn 0x2E	Привилегия
0xCC	Сброс параметров XCC до значений по умолчанию	PRIV_USR

Код	Команды Netfn 0x3A	Привилегия
0x00	Запрос версии микропрограммы	PRIV_USR
0x0D	Информация о плате	PRIV_USR
0x1E	Варианты задержки восстановления питания рамы	PRIV_USR
0x38	NMI и сброс	PRIV_USR
0x49	Запуск сбора данных	PRIV_USR
0x4A	Отправка файла	PRIV_USR
0x4D	Состояние сбора данных	PRIV_USR
0x50	Получение информации о сборке	PRIV_USR

Код	Команды Netfn 0x3A	Привилегия
0x55	Получение/задание имени хоста	PRIV_USR
0x6B	Запрос уровня редакции микропрограммы FPGA	PRIV_USR
0x6C	Запрос уровня редакции оборудования платы	PRIV_USR
0x6D	Запрос уровня редакции микропрограммы PSoC	PRIV_USR
0x98	Управление USB-портом на передней панели	PRIV_USR
0xC7	Встроенный переключатель NM IPMI	PRIV_ADM

Сброс XCC до команды по умолчанию

Эта команда позволяет сбросить параметры конфигурации XCC до значений по умолчанию.

Сетевая функция = 0x2E			
Код	**Команда**	**Запрос, данные отклика**	**Описание**
0xCC	Сброс параметров XCC до значений по умолчанию	**Запрос:** Байт 1 — 0x5E Байт 2 — 0x2B Байт 3 — 0x00 Байт 4 — 0x0A Байт 5 — 0x01 Байт 6 — 0xFF Байт 7 — 0x00 Байт 8 — 0x00 Байт 9 — 0x00 **Отклик:** Байт 1 — код выполнения Байт 2 — 0x5E Байт 3 — 0x2B Байт 4 — 0x00 Байт 5 — 0x0A Байт 6 — 0x01 Байт 7 — данные отклика 0 = Успешно Ненулевое значение = Сбой	Эта команда позволяет сбросить параметры конфигурации XCC до значений по умолчанию.

Команды для получения информации о плате/микропрограмме

В этом разделе перечислены команды, позволяющие запрашивать информацию о плате и микропрограмме.

Функция сети = 0x3A			
Код	**Команда**	**Запрос, данные отклика**	**Описание**
0x00	Запрос версии микропрограммы	**Запрос**: Нет данных по запросу **Отклик**: Байт 1 — код выполнения Байт 2 — основная версия Байт 3 — дополнительная версия	Эта команда возвращает номера основной и дополнительной версий микропрограммы. Если команда отправляется с дополнительным 1 байтом данных запроса, отклик XCC также возвращает третье поле (редакцию) версии. (Основная.Дополнительная. Редакция)
0x0D	Запрос информации о плате	**Запрос**: недоступен **Отклик**: Байт 1 — ИД системы Байт 2 — редакция платы	Эта команда возвращает ИД платы и редакцию планарного корпуса.
0x50	Запрос информации о сборке	**Запрос**: недоступен **Отклик**: Байт 1 — код выполнения. Байты 2:10 — имя сборки ASCIIZ Байты 11:23 — дата сборки ASCIIZ Байты 24:31 — время сборки ASCII	Эта команда возвращает имя, дату и время сборки. Строки с именем и датой сборки имеют нулевое окончание. Формат даты сборки — ГГГГ-ММ-ДД. Например, ZUBT99A “2005-03-07” “23:59:59”

Функция сети = 0x3A			
Код	**Команда**	**Запрос, данные отклика**	**Описание**
0x6B	Запрос уровня редакции микропро-граммы FPGA	**Запрос**: Байт 1 — тип устройства FPGA* Тип устройства FPGA 0 = локальное (активный уровень) 1 = процессорная карта 1 (активный уровень) 2 = процессорная карта 2 (активный уровень) 3 = процессорная карта 3 (активный уровень) 4 = процессорная карта 4 (активный уровень) 5 = локальное основное ПЗУ 6 = локальное резервное ПЗУ **Отклик**: Байт 1 — код выполнения Байт 2 — уровень основной редакции Байт 3 — уровень дополнительной редакции Байт 4 — уровень дополнительной подредакции (тестовый байт на платформах XCC)	Эта команда возвращает уровень редакции микропрограммы FPGA. Если байт 1 пропущен, выбирается локальная версия (активный уровень)
0x6C	Запрос уровня редакции оборудова-ния платы	**Запрос**: Нет данных. **Отклик**: Байт 1 — код выполнения Байт 2 — уровень редакции	Эта команда возвращает уровень редакции оборудования платы, на которой размещена схема FPGA.
0x6D	Запрос уровня редакции микропро-граммы PSoC	**Запрос**: Нет **Отклик**: Байт 1 — код выполнения	Эта команда возвращает уровень редакции всех обнаруженных устройств PSoC. Примечание: bin# представляет физическое расположение. Для получения более подробной

Функция сети = 0x3A			
Код	**Команда**	**Запрос, данные отклика**	**Описание**
		Байт 2 — bin# Байт 3 — APID Байт 4 — Редакция Байты 5–6 — ИД FRU Байты 6:N — повторение байтов 2–6 для каждого из обнаруженных PSoC	информации обратитесь к спецификации системы.

Команды для управления системой

Спецификация IPMI предоставляет базовые инструменты для управления питанием и сбросом. Lenovo добавляет еще ряд функций управления.

<table>
<tr><th colspan="4">Сетевая функция = 0x2E</th></tr>
<tr><th>Код</th><th>Команда</th><th>Запрос, данные отклика</th><th>Описание</th></tr>
<tr><td>0x1E</td><td>Варианты задержки восстано-вления питания рамы</td><td>Запрос:
<table><tr><td>Байт 1</td><td>Тип запроса:

0x00 = задание параметров задержки

0x01 = запрос параметров задержки</td></tr><tr><td>Байт 2</td><td>(если байт 1 = 0x00)

0x00 = отключено (по умолчанию)

0x01 = произвольно

0x02 — 0xFF зарезервиро-вано</td></tr></table>Отклик:

Байт 1 — код выполнения

Байт 2 — параметры задержки (только для запроса)</td><td>Эта настройка используется, если согласно политике восстановления питания рамы питание на раму подается всегда либо питание рамы возобновляется (если ранее было включено) после подачи/ восстановления питания от сети переменного тока. Доступно 2 варианта на выбор: отключено (настройка по умолчанию, без задержки при включении питания) и произвольно. Если задана произвольная задержка, то между подачей/ восстановлением питания от сети переменного тока и автоматическим включением сервера происходит произвольная задержка продолжительностью от 1 до 15 секунд.

Эта команда поддерживается XCC только для стоечных серверов.</td></tr>
<tr><td>0x38</td><td>NMI и сброс</td><td>Запрос:

Байт 1 — число секунд

0 = только NMI

Байт 2 — тип сброса

0 = «мягкий» сброс

1 = выключение и включение питания

Отклик:

Байт 1 — код выполнения</td><td>Эта команда используется для выполнения немаскируемого прерывания системы. При необходимости после немаскируемого прерывания систему можно сбросить (перезагрузить) или выключить и включить ее питание.

Если в поле «Число секунд» указано ненулевое значение, сброс или выключение и включение питания системы произойдет через указанное число секунд.

Байт 2 запроса является необязательным. Если байт 2 не указан или имеет значение 0x00, выполняется «мягкий» сброс. Если байт 2 имеет значение 0x01, питание системы</td></tr>
</table>

Сетевая функция = 0x2E			
Код	**Команда**	**Запрос, данные отклика**	**Описание**
			выключается и включается снова.

Прочие команды

В этом разделе приводятся команды, которые невозможно отнести ни к какому другому разделу.

<table>
<tr><th colspan="4">Функция сети = 0x3A</th></tr>
<tr><th>Код</th><th>Команда</th><th>Запрос, данные отклика</th><th>Описание</th></tr>
<tr><td>0x55</td><td>Получение/ задание имени хоста</td><td>Длина запроса = 0:

Пустые данные в запросе

Отклик:<table><tr><td>Байт 1</td><td>Код выполнения</td></tr><tr><td>Байты 2–65</td><td>Текущее имя хоста.

ASCIIZ, строка с нулевым окончанием.</td></tr></table>Длина запроса 1–64:<table><tr><td>Байты 1–64</td><td>Имя хоста DHCP

ASCIIZ оканчивается 00h</td></tr></table></td><td>Используйте эту команду для получения/задания имени хоста.

При задании имени хоста желаемое значение должно оканчиваться 00h. Максимальная длина имени хоста — 63 символа и значение null.</td></tr>
<tr><td>0x98</td><td>Управление USB-портом на передней панели</td><td>Запрос:

Байт 1<table><tr><td>01h:</td><td>Получение текущего владельца USB-порта на лицевой панели</td></tr></table>Отклик:

Байт 1 — код выполнения

Байт 2<table><tr><td>00h:</td><td>Принадлежит хосту</td></tr><tr><td>01h:</td><td>Принадлежит BMC</td></tr></table>Запрос:

Байт 1<table><tr><td>02h:</td><td>Получение конфигура-ции USB-</td></tr></table></td><td>Эта команда используется для запроса состояния/ конфигурации USB-порта на лицевой панели, настройки режима/тайм-аута USB-порта на лицевой панели и переключения между владельцами USB-порта (хостом и BMC)

В конфигурации USB-порт на лицевой панели может функционировать в одном из трех режимов: выделен хосту, используется исключительно BMC или работает в общем режиме, когда владелец может переключаться между хостом и BMC.

Если включен общий режим, USB-порт подключен к BMC, когда питание сервера выключено, и к серверу, когда питание сервера включено.

Если включен общий режим и питание сервера, BMC возвращает USB-порт серверу после тайм-аута конфигурации из-за неактивности.</td></tr>
</table>

<table>
<tr><th colspan="4">Функция сети = 0x3A</th></tr>
<tr><th>Код</th><th>Команда</th><th>Запрос, данные отклика</th><th>Описание</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>порта на лицевой панели</td></tr>
</table>
Отклик:

Байт 1 — код выполнения

Байт 2

<table>
<tr><td>00h:</td><td>Выделено хосту</td></tr>
<tr><td>01h:</td><td>Выделено BMC</td></tr>
<tr><td>02h:</td><td>Режим совместного использова-ния</td></tr>
</table>
Байт 3:4 — тайм-аут после неактивности, в минутах (сначала MSB)

Байт 5 — включение кнопки идентификации

<table>
<tr><td>00h:</td><td>Отключено</td></tr>
<tr><td>01h:</td><td>Включено</td></tr>
</table>
Байт 6 — гистерезис (дополнительно) в секундах

Запрос:

Байт 1

03h: задание конфигурации USB-порта на лицевой панели

Байт 2

<table>
<tr><td>00h:</td><td>Выделено хосту</td></tr>
<tr><td>01h:</td><td>Выделено BMC</td></tr>
<tr><td>02h:</td><td>Режим совместного использова-ния</td></tr>
</table>
Байт 3:4 — тайм-аут после неактивности, в минутах
</td><td>Если сервер оборудован кнопкой идентификации, пользователи могут включать/выключать функцию смены владельца USB-порта на лицевой панели с помощью кнопки идентификации, удерживая ее более 3 секунд.

Гистерезис в секундах задается при автоматическом переключении порта при выключении и включении питания. Это необязательный параметр.

Серверы SD530

На платформе SD530 этот порт является дополнительным и при наличии он подключается напрямую к XCC и только к XCC. Переключить порт на хост невозможно.

• Если команда отправляется с байтом 1 = 1, XCC будет всегда отвечать, что порт принадлежит BMC.
• Если команда отправляется с байтом 1 = 2, XCC будет всегда отвечать, что порт выделен BMC.
• Если команда отправляется с байтом 1 = 3 или байтом 1 = 4, XCC будет отвечать кодом выполнения D6h.

Прочие серверы

На платформе, отличной от SD530, использование USB-порта на лицевой панели модулем XCC можно отключить, перейдя в режим «Только хост».

Если команда отправляется с байтом 1 = 5 или байтом 1 = 6, XCC будет отвечать кодом выполнения D6h.</td></tr>
</table>

<table>
<tr><th colspan="4">Функция сети = 0x3A</th></tr>
<tr><th>Код</th><th>Команда</th><th>Запрос, данные отклика</th><th>Описание</th></tr>
<tr><td></td><td></td><td>(сначала MSB)

Байт 5 — включение кнопки идентификации

<table><tr><td>00h:</td><td>Отключено</td></tr><tr><td>01h:</td><td>Включено</td></tr></table>
Байт 6 — гистерезис (дополнительно) в секундах

Отклик:

Байт 1 — код выполнения Байт 2

<table><tr><td>00h:</td><td>Переключение на хост</td></tr><tr><td>01h:</td><td>Переключение на BMC</td></tr></table>
Отклик:

Байт 1 — код выполнения

Байт 1

<table><tr><td>05h:</td><td>Включение/выключение USB-порта на лицевой панели</td></tr></table>
Байт 2

<table><tr><td>00h:</td><td>Выключить</td></tr><tr><td>01h:</td><td>Включить</td></tr></table>
Отклик:

Байт 1 — код выполнения

Запрос:

Байт 1

<table><tr><td>06h:</td><td>Чтение состояния включения/выключения USB-порта на лицевой панели</td></tr></table></td><td></td></tr>
</table>

<table>
<tr><th colspan="4">Функция сети = 0x3A</th></tr>
<tr><th>Код</th><th>Команда</th><th>Запрос, данные отклика</th><th>Описание</th></tr>
<tr><td></td><td></td><td>Отклик:

Байт 1 — код выполнения

Байт 2</td><td></td></tr>
<tr><td>0xC7</td><td>Встроенный переключа-тель NM IPMI</td><td>Длина запроса = 0:

Пустые данные в запросе

Отклик:

<table><tr><td>Байт 1</td><td>Код выполнения</td></tr><tr><td>Байты 2</td><td>Текущее состояние «Включено/ Выключено»</td></tr></table>
Длина запроса = 1:

<table><tr><td>Байт 1</td><td>Атрибут «Включено/ Выключено» встроенного интерфейса NM IPMI

00h — выключить

01h — включить</td></tr></table>
Отклик:

<table><tr><td>Байт 1</td><td>Код выполнения</td></tr></table></td><td>Эта команда служит для включения/выключения функции моста XCC для встроенных IPMI-команд Intel.</td></tr>
</table>

Глава 12. Серверы Edge

В этом разделе описаны функции серверов Edge.

Примечания:

1. При первом входе в систему необходимо изменить пароль XCC.
2. По умолчанию доступ к IPMI через локальную сеть отключен.
3. По умолчанию доступ к IPMI через KCS отключен.

Режим блокировки системы

Если **режим блокировки системы** в активном состоянии, это означает, что система находится в режиме блокировки. Можно активировать и разблокировать систему. В противном случае загрузить хост-систему не удастся.

Примечание: Режим блокировки системы доступен только для SE350 с пакетом безопасности, но не для SE350 в стандартной версии. Уточнить версию можно на вкладке **Главная** в разделе **Сведения о системе и параметры системы**.

Нажмите **Безопасность** в разделе **BMC Configuration** и прокрутите до **Режим блокировки системы**.

Режим блокировки системы

Чтобы активировать систему и выйти из **режима блокировки системы**, выполните следующие действия.

1. Нажмите кнопку **Неактивен** — отобразится окно **Активация хранилища ключей** с **текстом запроса**.
2. Обратитесь к своему ИТ-администратору и введите **текст запроса**.
3. Получите **ответ на запрос** у своего ИТ-администратора и введите его в окне **Активация хранилища ключей**.
4. Нажмите кнопку **OK**, а затем — **Применить**.
5. Если все настройки работают правильно, **Режим блокировки системы** станет **Неактивен**.

Примечание: Если режим блокировки системы находится в активном состоянии, доступ к секретам системы, таким как, например, ключи SED, **запрещен**.

Чтобы принудительно перевести систему в режим блокировки, выполните следующие действия.

1. Нажмите кнопку **Активен**.
2. Нажмите кнопку **OK**, а затем — **Применить**.

Обнаружение движения

Можно включить эту функцию, чтобы защитить свой сервер путем обнаружения физических перемещений сервера.
Если обнаружение движения включено, в зависимости от предпочтений и конфигурации можно задать следующие параметры.

- **Уровень чувствительности**: выберите один из трех уровней чувствительности (**Низкий**, **Средний** или **Высокий**) в зависимости от предпочтений
- **Ориентация**: выберите одну из конфигураций: **На столе**, **Монтаж на стену (горизонтальный)**, **Монтаж на стену (вертикальный)**, **Полка** и **Монтаж на потолок**.

Примечание: Обнаружение движения автоматически отключается, когда система переходит в режим блокировки.

Обнаружение вторжения в раму
Можно включить эту функцию, чтобы защитить свой сервер путем обнаружения физических перемещений верхнего кожуха.

Дополнительные конфигурации
Если установлен пакет LOM с поддержкой беспроводного соединения, для обнаруженного события повреждения можно выбрать три параметра.
В редких случаях, когда **текст запроса** не удается проверить на портале ThinkShield Key Vault Portal, может потребоваться сбросить внутренний счетчик устройства, прежде чем активировать устройство по просьбе ИТ-администратора.

Диспетчер SED AK

В системе, установленной с помощью SED (самошифруемого диска), эта функция контролирует BMC для развертывания ключа SED. Ключ SED можно использовать для шифрования загрузочных дисков и дисков данных, а также автоматической загрузки системы

Примечание: Эта операция не разрешена, если система не активирована (подтвержден режим блокировки системы) либо у текущего пользователя нет прав на управление ключом SED.

Примечание: Режим блокировки системы доступен только для SE350 с пакетом безопасности, но не для SE350 в стандартной версии. Уточнить версию можно на вкладке **Главная** в разделе **Сведения о системе и параметры системы**.

Примечание: SE350 также поддерживает функцию автоматического создания резервных копий при условии работоспособности вспомогательного комплекта ThinkSystem M.2 или вспомогательного комплекта зеркального отображения ThinkSystem M.2. Если оборудование повреждено, но SED и комплект M.2 работоспособны, их можно установить в другую систему SE350 и восстановить SED AK. Однако Lenovo рекомендует создать резервную копию SED AK, чтобы подготовиться к полному сбою оборудования.

Нажмите **Безопасность** в разделе **BMC Configuration** и прокрутите до пункта **Диспетчер ключа аутентификации (AK) SED**.

Изменение SED AK
Создание SED AK на основе парольной фразы: задайте пароль и повторно введите его для подтверждения. Щелкните **Создать повторно**, чтобы получить новый SED AK.
Создание случайного SED AK: щелкните **Создать повторно**, чтобы получить случайный SED AK.
Резервное копирование SED AK. Задайте пароль и повторно введите его для подтверждения. Щелкните **Начать резервное копирование** для выполнения резервного копирования SED AK. Затем загрузите файл SED AK и сохраните его в безопасном месте для использования в будущем.

Примечание: Если для восстановления конфигурации используется файл резервной копии SED AK, система запросит пароль, заданный здесь.

Восстановление SED AK. Эту операцию можно выполнить, только когда SED функционирует неправильно. Существует два способа восстановления SED AK:

- **Восстановление SED AK с помощью парольной фразы:** используйте пароль, заданный в режиме **Создание SED AK на основе парольной фразы**, для восстановления SED AK.
- **Восстановление SED AK из файла резервной копии:** отправьте файл резервной копии, созданный в режиме **Резервное копирование SED AK**, и введите соответствующий пароль файла резервной копии для восстановления SED AK.

Пограничные сети

Страница этой функции поддерживается, только если установлен пакет LOM с поддержкой беспроводного подключения.

См. дополнительные сведения в таблицах предустановок топологии сети в разделе https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html.

Подключение Wi-Fi
Щелкните **Включено**, и вы сможете настроить параметры в соответствии с конфигурацией Wi-Fi.

Подключение LTE
Эта функция позволяет контролировать подключение LTE для платы пограничной сети.

Адрес платы пограничной сети

Состояние **IPv4 или IPv6**	Состояние **сервера DHCP**	**Метод**
Отключено	**Отключено**	**Получать IP-адрес из DHCP**
Включено	**Включено**	**Использовать статический IP-адрес**
Включено	**Отключено**	**Получать IP-адрес из DHCP** или **Использовать статический IP-адрес** в зависимости от использования.

Сетевой мост BMC
Можно настроить следующие параметры доступа к BMC: **Нисходящие порты**, **Порты Wi-Fi**, **Восходящие порты** или **Нет**.

Примечание: Настройка **Нет** означает, что функция отключена.

Устранение неполадок с платой пограничной сети
Перезапустить немедленно: нажав на эту кнопку, можно перезапустить сетевую плату.
Восстановить заводские настройки: нажав на эту кнопку, можно сбросить параметры сетевой платы до значений по умолчанию.

Приложение A. Получение помощи и технической поддержки

Если вам нужна помощь, обслуживание или техническая поддержка в связи с продуктами, Lenovo может предложить самые различные источники помощи.

Актуальную информацию о системах, дополнительных устройствах, услугах и поддержке Lenovo можно найти в Интернете по следующему адресу:

http://datacentersupport.lenovo.com

Примечание: В этом разделе есть ссылки на веб-сайты IBM и информация о получении обслуживания. Рекомендуемый Lenovo сервис-центр для ThinkSystem — компания IBM.

Перед обращением в службу поддержки

Прежде чем обратиться в службу поддержки, убедитесь, что вы предприняли следующие действия, чтобы попытаться устранить неполадку самостоятельно. Если вы решите, что вам все же нужна помощь, соберите информацию, которая потребуется специалисту по техническому обслуживанию для более быстрого решения вашей проблемы.

Попытайтесь решить проблему самостоятельно

Многие проблемы можно решить без внешней помощи, выполнив процедуры по устранению неполадок, описанные Lenovo в справке в Интернете и в документации к продукту Lenovo. В документации к продукту Lenovo также описываются диагностические тесты, которые можно выполнить. В документации к большинству систем, операционных систем и программ содержатся процедуры устранения неполадок и расшифровка сообщений об ошибках и кодов ошибок. Если вы подозреваете, что неполадка связана с программным обеспечением, посмотрите документацию операционной системы или программы.

Документацию по продуктам ThinkSystem можно найти по следующему адресу:

http://thinksystem.lenovofiles.com/help/index.jsp

Прежде чем обратиться в службу поддержки, попытайтесь решить проблему самостоятельно:

- Проверьте, все ли кабели подсоединены.
- Проверьте все выключатели и убедитесь, что компьютер и все дополнительные устройства включены.
- Проверьте наличие обновлений программного обеспечения, микропрограммы и драйверов устройств операционной системы для вашего продукта Lenovo. Согласно условиям и положениям гарантии Lenovo вы, владелец продукта Lenovo, ответственны за поддержание и обновление программного обеспечения и микропрограмм продукта (если это не покрывается дополнительным контрактом на техническое обслуживание). Специалист по техническому обслуживанию попросит вас обновить программное обеспечение и микропрограмму, если в одном из обновлений программного обеспечения есть задокументированное решение неполадки.
- Если вы установили новое оборудование или программное обеспечение в среду, проверьте на странице http://www.lenovo.com/serverproven/, что оборудование и программное обеспечение поддерживается вашим продуктом.
- Перейдите на сайт http://datacentersupport.lenovo.com и поищите информацию, которая может помочь решить проблему.

– Просмотрите сведения форумов Lenovo по адресу https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg — возможно, кто-то уже сталкивался с аналогичной проблемой.

Многие проблемы можно решить без внешней помощи, выполнив процедуры по устранению неполадок, описанные Lenovo в справке в Интернете и в документации к продукту Lenovo. В документации к продукту Lenovo также описываются диагностические тесты, которые можно выполнить. В документации к большинству систем, операционных систем и программ содержатся процедуры устранения неполадок и расшифровка сообщений об ошибках и кодов ошибок. Если вы подозреваете, что неполадка связана с программным обеспечением, посмотрите документацию операционной системы или программы.

Сбор необходимой информации для обращения в службу поддержки

Если вы полагаете, что необходимо гарантийное обслуживание вашего продукта Lenovo, специалисты по техническому обслуживанию смогут помочь вам более эффективно, если вы подготовитесь к обращению. Дополнительные сведения о гарантии на ваш продукт также доступны по адресу http://datacentersupport.lenovo.com/warrantylookup.

Соберите следующую информацию, которую нужно будет предоставить специалисту по техническому обслуживанию. Эти данные помогут специалисту по техническому обслуживанию быстро предложить решение вашей неполадки и обеспечить вам уровень обслуживания согласно договору.

- Если применимо, номера договоров на обслуживание оборудования и программного обеспечения
- Номер типа компьютера (идентификатор компьютера Lenovo, 4 цифры)
- Номер модели
- Серийный номер
- Текущие уровни UEFI и микропрограммы системы
- Другая относящаяся к делу информация, такая как сообщения об ошибках и журналы

В качестве альтернативы обращению в службу поддержки Lenovo можно перейти по ссылке https://www-947.ibm.com/support/servicerequest/Home.action и отправить электронный запрос на обслуживание. Отправка электронного запроса на обслуживание запускает процесс поиска решения вашей проблемы; для этого предоставленная информация передается специалистам по техническому обслуживанию. Специалисты по техническому обслуживанию Lenovo могут начать работать над вашим решением, как только вы заполните и отправите электронный запрос на обслуживание.

Сбор данных по обслуживанию

Для точного определения основной причины проблем с сервером или по запросу специалистов службы поддержки Lenovo вам, возможно, потребуется собрать данные по обслуживанию, которые затем могут использоваться для дальнейшего анализа. Данные по обслуживанию включают такую информацию, как журналы событий и инвентарь оборудования.

Данные по обслуживанию можно собирать с помощью следующих инструментов:

- **Lenovo XClarity Controller**

  Для сбора данных по обслуживанию сервера можно использовать веб-интерфейс Lenovo XClarity Controller или интерфейс командной строки. Файл можно сохранить и отправить в службу поддержки Lenovo.

  – Дополнительные сведения об использовании веб-интерфейса для сбора данных по обслуживанию см. по ссылке http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_c_servicesandsupport.html.

  - Дополнительные сведения об использовании интерфейса командной строки для сбора данных по обслуживанию см. по ссылке http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/nn1ia_r_ffdccommand.html.

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator можно настроить для автоматического сбора и отправки диагностических файлов в службу поддержки Lenovo, когда определенные обслуживаемые события происходят в Lenovo XClarity Administrator и на управляемых конечных точках. Можно отправлять диагностические файлы в Поддержка Lenovo с помощью функции Call Home или в другой сервис-центр с помощью SFTP. Кроме того, можно вручную собрать диагностические файлы, открыть запись неполадки и отправить диагностические файлы в центр поддержки Lenovo.

  Дополнительные сведения о настройке автоматических уведомлений о неполадках в Lenovo XClarity Administrator см. по ссылке http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/admin_setupcallhome.html.

- **Lenovo XClarity Provisioning Manager**

  Используйте функцию сбора данных по обслуживанию в Lenovo XClarity Provisioning Manager для сбора системных данных по обслуживанию. Можно собрать существующие данные системного журнала или выполнить новую диагностику для сбора новых данных.

- **Lenovo XClarity Essentials**

  Lenovo XClarity Essentials можно запустить во внутриполосном режиме из операционной системы. В дополнение к аппаратным данным по обслуживанию Lenovo XClarity Essentials может собирать сведения об операционной системе, такие как журнал событий операционной системы.

  Чтобы получить данные по обслуживанию, можно выполнить команду `getinfor`. Дополнительные сведения о выполнении `getinfor` см. в разделе http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_getinfor_command.html.

Обращение в службу поддержки

Для получения помощи в решении той или иной проблемы можно обратиться в службу поддержки.

Можно воспользоваться услугами обслуживания оборудования, предоставляемыми авторизованным сервис-центром Lenovo. Чтобы найти сервис-центр, уполномоченный компанией Lenovo выполнять гарантийное обслуживание, откройте веб-страницу по адресу https://datacentersupport.lenovo.com/us/en/serviceprovider и воспользуйтесь поиском с фильтрацией для разных стран. Номера телефонов службы поддержки Lenovo по регионам см. на стр. https://datacentersupport.lenovo.com/us/en/supportphonelist.

Приложение B. Замечания

Lenovo может предоставлять продукты, услуги и компоненты, описанные в этом документе, не во всех странах. Сведения о продуктах и услугах, доступных в настоящее время в вашем регионе, можно получить у местного представителя Lenovo.

Ссылки на продукты, программы или услуги Lenovo не означают и не предполагают, что можно использовать только указанные продукты, программы или услуги Lenovo. Допускается использовать любые функционально эквивалентные продукты, программы или услуги, если при этом не нарушаются права Lenovo на интеллектуальную собственность. Однако при этом ответственность за оценку и проверку работы других продуктов, программ или услуг возлагается на пользователя.

Lenovo может располагать патентами или рассматриваемыми заявками на патенты, относящимися к предмету данной публикации. Предоставление этого документа не является предложением и не дает лицензию в рамках каких-либо патентов или заявок на патенты. Вы можете послать запрос на лицензию в письменном виде по следующему адресу:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO ПРЕДОСТАВЛЯЕТ ДАННУЮ ПУБЛИКАЦИЮ «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ОТНОСИТЕЛЬНО ЕЕ КОММЕРЧЕСКОГО ИСПОЛЬЗОВАНИЯ ИЛИ ПРИГОДНОСТИ ДЛЯ КАКИХ-ЛИБО ЦЕЛЕЙ. Законодательство некоторых стран не допускает отказ от явных или предполагаемых гарантий для ряда операций; в таком случае данное положение может к вам не относиться.

В приведенной здесь информации могут встретиться технические неточности или типографские опечатки. В публикацию время от времени вносятся изменения, которые будут отражены в следующих изданиях. Lenovo может в любой момент без предварительного уведомления вносить изменения в продукты и (или) программы, описанные в данной публикации.

Продукты, описанные в этом документе, не предназначаются для имплантации или использования в каких-либо устройствах жизнеобеспечения, отказ которых может привести к травмам или смерти. Информация, содержащаяся в этом документе, не влияет на спецификации продукта и гарантийные обязательства Lenovo и не меняет их. Ничто в этом документе не служит явной или неявной лицензией или гарантией возмещения ущерба в связи с правами на интеллектуальную собственность Lenovo или третьих сторон. Все данные, содержащиеся в этом документе, получены в специфических условиях и приводятся только в качестве иллюстрации. Результаты, полученные в других рабочих условиях, могут существенно отличаться.

Lenovo может использовать и распространять присланную вами информацию любым способом, каким сочтет нужным, без каких-либо обязательств перед вами.

Любые ссылки в данной информации на веб-сайты, не принадлежащие Lenovo, приводятся только для удобства и никоим образом не означают поддержки Lenovo этих веб-сайтов. Материалы на этих веб-сайтах не входят в число материалов по данному продукту Lenovo, и всю ответственность за использование этих веб-сайтов вы принимаете на себя.

Все данные по производительности, содержащиеся в этой публикации, получены в управляемой среде. Поэтому результаты, полученные в других рабочих условиях, могут существенно отличаться. Некоторые измерения могли быть выполнены в разрабатываемых системах, и нет гарантии, что в общедоступных системах результаты этих измерений будут такими же. Кроме того, результаты некоторых измерений могли быть получены экстраполяцией. Реальные результаты могут отличаться. Пользователи должны проверить эти данные для своих конкретных условий.

Товарные знаки

Lenovo, логотип Lenovo, ThinkSystem, Flex System, System x, NeXtScale System и x Architecture — товарные знаки Lenovo в США и других странах.

Intel и Intel Xeon — товарные знаки корпорации Intel Corporation в США и других странах.

Internet Explorer, Microsoft и Windows являются товарными знаками группы компаний Microsoft.

Linux — зарегистрированный товарный знак Linus Torvalds.

Прочие названия фирм, продуктов или услуг могут быть товарными знаками или марками обслуживания других компаний.

Важные примечания

Скорость процессора указывает внутреннюю тактовую частоту микропроцессора; на производительность приложений влияют и другие факторы.

Скорость дисковода для компакт-дисков или DVD-дисков — это переменная скорость чтения. Действительная скорость изменяется; как правило, она меньше максимальной скорости.

При описании системы хранения, действительного и виртуального хранилища, объема каналов один КБ равен 1024 байт, один МБ равен 1 048 576 байт, а один ГБ равен 1 073 741 824 байт.

При описании емкости жесткого диска или объема коммуникационных устройств один МБ равен 1 000 000 байт, а один ГБ равен 1 000 000 000 байт. Общий объем памяти, доступный пользователям, зависит от рабочей среды.

Максимальная внутренняя емкость жесткого диска подразумевает замену любого стандартного жесткого диска и заполнение всех отсеков жестких дисков самыми вместительными дисками, поддерживаемыми в данный момент компанией Lenovo.

Для достижения максимального объема памяти может потребоваться замена стандартных модулей на дополнительные модули памяти.

У каждой ячейки твердотельной памяти есть присущее ей конечное число циклов записи, которое она может выполнить. Поэтому у твердотельных устройств есть параметр максимального количества циклов записи, выражаемый в общем количестве записанных байт `total bytes written` (TBW). Устройство, которое преодолело этот порог, может не отвечать на команды системы или может перестать поддерживать запись. Lenovo не отвечает за замену устройства, которое превысило максимальное гарантированное количество циклов программирования или стирания, как описано в официальных опубликованных спецификациях для устройства.

Компания Lenovo не предоставляет никаких гарантий, связанных с продуктами, которые выпускаются не Lenovo. Поддержка (если таковая есть) продуктов, произведенных другой компанией, должна осуществляться соответствующей компанией, а не Lenovo.

Некоторое программное обеспечение может отличаться от розничной версии (если доступно) и может не содержать руководств по эксплуатации или всех функций.

Загрязнение частицами

Внимание! Взвешенные частицы (включая металлическую стружку) и активные газы отдельно или в сочетаниях с другими факторами окружающей среды, такими как влажность или температура, могут представлять опасность для описанного в этом документе устройства.

К рискам, которые представляют избыточные уровни частиц или концентрация опасных газов, относятся повреждения, которые могут вызвать неисправность или выход устройства из строя. Изложенные в данном документе спецификации устанавливают ограничения для частиц и газов и позволяют предотвратить такие повреждения. Ограничения не должны рассматриваться или использоваться как однозначные, так как различные другие факторы, такие как температура и влажность воздуха, могут повлиять на воздействие частиц или коррозийных и газовых загрязнений. При отсутствии определенных ограничений, приведенных в этом документе, необходимо реализовать правила, поддерживающие определенные уровни частиц и газов, обеспечивающие безопасность здоровья человека. Если компания Lenovo определила, что повреждение устройства вызвали уровни частиц или газов в окружающей среде, при ремонте или замене устройства или его компонентов в такой среде компания может потребовать устранения таких условий загрязнения. Реализация таких мер возлагается на клиента.

Табл. 67. Ограничения для частиц и газов

Загрязнение	**Ограничения**
Частицы	• В соответствии со стандартом ASHRAE 52.2[1] воздух в помещении должен постоянно фильтроваться фильтром с пылезадерживающей способностью 40 % (MERV 9). • Воздух, который поступает в центр обработки данных, должен фильтроваться с эффективностью 99,97 % или выше с помощью высокоэффективных фильтров частиц (HEPA), соответствующих стандарту MIL-STD-282. • Относительная влажность в среде загрязняющих частиц должна быть выше 60 %[2]. • В помещении не должны находиться электропроводные загрязнители, такие как частицы цинка.
Газы	• Медь: класс G1 согласно стандарту ANSI/ISA 71.04-1985[3] • Серебро: скорость коррозии меньше 300 Å в течение 30 дней

[1] ASHRAE 52.2-2008 — *метод проверки общей вентиляции воздуха — очистка устройств с эффективным удалением по размеру частиц*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] Относительная влажность растворения загрязняющих частиц — это относительная влажность, при которой пыль поглощает достаточное количество воды, чтобы стать влажной и попасть под действие ионной проводимости.

[3] ANSI/ISA-71.04-1985. *Условия окружающей среды для измерения процесса и систем управления: загрязняющие вещества в воздухе*. Instrument Society of America, Research Triangle Park, North Carolina, U.S. A.

Заявление о соответствии нормативным документам в области телекоммуникаций

Этот продукт может быть не сертифицирован в вашей стране для подключения любым образом к интерфейсам общедоступных телекоммуникационных сетей. Перед установлением такого

соединения по закону может требоваться дополнительная сертификация. Если у вас есть вопросы, обратитесь к местному представителю или торговцу продукцией Lenovo.

Замечания об электромагнитном излучении

При подключении к оборудованию монитора необходимо использовать специальный кабель монитора и устройства подавления помех, входящие в комплект монитора.

Дополнительные замечания об электромагнитном излучении можно найти по следующему адресу:

http://thinksystem.lenovofiles.com/help/index.jsp

Заявление о директиве RoHS Бюро стандартов, метрологии и контроля Тайваня (Китай)

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1.〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3.〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

Контактная информация отдела импорта и экспорта на Тайване (Китай)

Ниже приведена контактная информация отдела импорта и экспорта на Тайване (Китай).

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

Индекс

K

Л

М

Н

О

П

Р

С

Т

У

Ф

Х

Ц

Э

A

B

C

D

E

F

H

I

L

M

O

R

S

T

U

X

Lenovo

Шифр: SP47A30085

Printed in China

(1P) P/N: SP47A30085