Стоечный сервер Huawei

Руководство пользователя iBMC (версии V250-V259)

Выпуск 02

Дата 05.06.2018

HUAWEI TECHNOLOGIES CO., LTD.

Товарные знаки


и другие товарные знаки Huawei являются зарегистрированными товарными знаками компании Huawei Technologies Co., Ltd.

Другие товарные знаки и торговые наименования, упомянутые в настоящем документе, принадлежат их владельцам.

Внимание

Приобретаемые продукты, услуги и функции предусмотрены договором, заключенным между компанией Huawei и заказчиком. Все продукты, услуги и функции, полностью или частично, описанные в данном документе, могут не входить в объем закупок или использования. Если иное не указано, любые формулировки, сведения и рекомендации, содержащиеся в данном документе, представляются с условием «как есть», исключая гарантии, поручительства или какие-либо объяснения, явные или подразумеваемые.

Информация, содержащаяся в документе, может быть изменена без предварительного уведомления. При подготовке этого документа было приложено максимум усилий для обеспечения точности его содержимого. Но все положения, информация и рекомендации, содержащиеся в данном документе, не устанавливают жестких гарантий любого типа.

Huawei Technologies Co., Ltd.

Адрес: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Веб-сайт: http://e.huawei.com

О документе

Целевая аудитория

В данном документе приведено описание базового программного обеспечения интеллектуального контроллера управления материнской платой (iBMC, intelligent Baseboard Management Controller). Документ включает следующее:

- Функции и возможности iBMC
- Веб-интерфейс пользователя (WebUI) iBMC
- Интерфейс командной строки (CLI, Command Line Interface) iBMC
- Команды, используемые на iBMC

Данный документ предназначен для серверов RH1288 V3, RH2288 V3, RH2288H V3, RH1288A V2, RH2288A V2, 5288 V3, RH5885 V3, RH5885H V3, RH8100 V3, 1288H V5, 2288H V5, 2488 V5 и 8100 V5.

Данный документ предназначен для следующей аудитории:

- Инженеров по установке серверов
- Инженеров по техобслуживанию серверов

ПРИМЕЧАНИЕ

- В данном документе приведено описание команд, используемых только для развертывания и обслуживания серверов производства компании Huawei. Он не включает в себя команды, используемые при изготовлении, сборке и заводском контроле и ремонте.
- Данный документ не содержит команды, связанные с технической реализацией или локализацией неисправностей. Неправильное использование данных команд может привести к неисправностям устройства или к прерыванию обслуживания. Для получения справочной информации по данным командам, обратитесь в службу техподдержки компании Huawei.

Данный документ предназначен для лиц, занимающихся установкой, управлением и устранением неполадок серверов. Предполагается, что вы обладаете достаточной квалификацией, можете выполнять обслуживание серверов и определять потенциальные опасности в продуктах с опасными энергетическими уровнями.

Лист регистрации изменений

Обновления документа выполняются в порядке накопления. Таким образом, последний выпуск документа содержит все обновления, сделанные в предыдущих выпусках.

Обновления в выпуске 02 (05.06.2018)

Второй официальный выпуск.

Обновления в выпуске 01 (30.06.2017)

Первый официальный выпуск.

Содержание

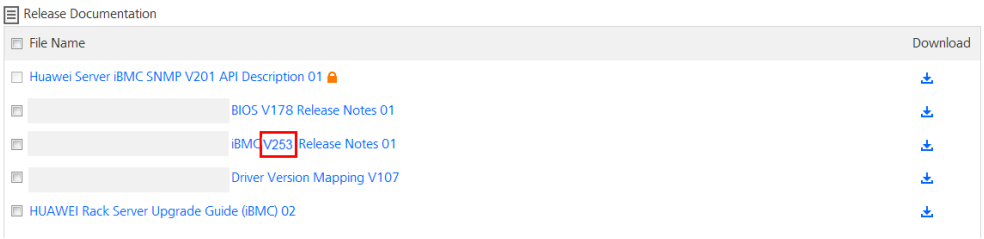
1 Общая информация

Версия iBMC *X.XX* также упоминается в документе как *VXXX*. Например, версия **2.01** также упоминается как **V201**.

Узнать номер версии iBMC можно следующим образом:

- Примечания к версии iBMC
  a. Перейдите на веб-сайт технической поддержки серверов Huaweihttp://support.huawei.com/enterprise/en/index.html.
  б. Выберите **Support** > **IT** > **Server** и выберите модель сервера.
  в. Нажмите **Downloads** и выберите версию сервера.
  г. В области **Release Documentation** будет указан список примечаний к версии iBMC.

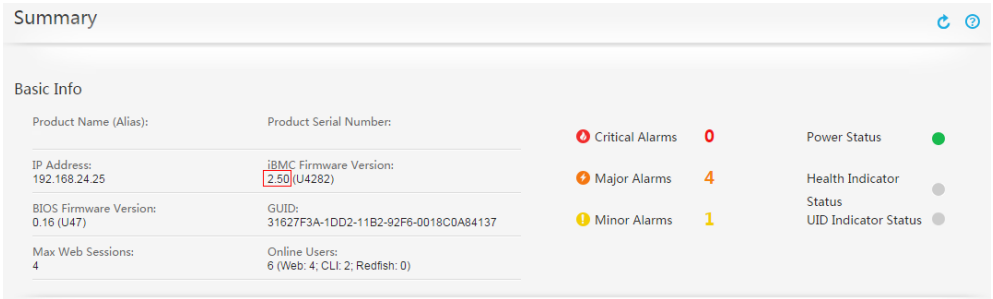
  В названии документа будет указан номер версии iBMC.



- Веб-интерфейс пользователя (WebUI) iBMC

  Войдите в веб-интерфейс iBMC и перейдите в меню **Information**.

  Параметр **iBMC Firmware Version** из области **Basic Info** – это номер версии iBMC.



- Интерфейс командной строки (CLI) iBMC

  В CLI iBMC выполните команду **ipmcget -d version**.

На экране появится следующее:

```
......
Active iBMC   Version:          (U4282)2.50
Active iBMC     Build:          002
......
```

2 Программное обеспечение iBMC

О данной главе

В данном разделе приведено описание ПО iBMC.

2.1 Функции iBMC

В данном разделе приведено описание ПО iBMC.

2.2 Конструкция системы

2.3 Управление безопасностью

2.1 Функции iBMC

В данном разделе приведено описание ПО iBMC.

iBMC – это интеллектуальная система управления, созданная компанией Huawei, которая позволяет дистанционно управлять серверами.

iBMC соответствует стандарту IPMI (Intelligent Platform Management Interface) и поддерживает протокол SNMP (Simple Network Management Protocol). Система предоставляет различные функции, такие как перенаправление с помощью KVM, перенаправление с помощью текстовой консоли, удаленная виртуальная среда, мониторинг и управление аппаратными средствами.

iBMC имеет следующие функциональные особенности:

- Различные интерфейсы управления для системной интеграции

  iBMC предоставляет IPMI, интерфейс командной строки (CLI), интерфейс управления центром обработки данных (DCMI), интерфейсы Redfish, протокол защищенной передачи гипертекста (HTTPS) и SNMP.
- Обнаружение и устранение неисправностей

  iBMC реализует обнаружение неисправностей и управление аварийными сигналами, обеспечивая стабильную бесперебойную работу системы в режиме 24/7.
- Виртуальный KVM-переключатель и виртуальная среда

  iBMC предоставляет виртуальный KVM-переключатель и виртуальную среду, что упрощает дистанционное обслуживание.

- Веб-интерфейс пользователя (WebUI)

  iBMC предоставляет веб-интерфейс пользователя для настройки и запроса информации об устройствах.

- Скриншоты системных отказов и воспроизведение видео

  iBMC позволяет создавать скриншоты и видео в случае отказа системы. Скриншоты и видео помогают определить причину сбоя системы.

- Мгновенные снимки экрана и видео

  iBMC имеет функцию создания мгновенных снимков экрана и записи видео, что упрощает регулярное профилактическое обслуживание, сбор информации и аудит.

- Поддержка DNS и LDAP

  iBMC поддерживает систему доменных имен (DNS) и протокол LDAP (Lightweight Directory Application Protocol) для реализации управления доменами и службы каталогов.

- Резервирование в режиме активный/резервный

  iBMC работает в режиме активном/резервном для обеспечения надежности системы. В случае сбоя активной iBMC, резервная iBMC немедленно перенимает на себя сервисы.

- Интеллектуальное управление питанием

  В iBMC использует механизм ограничения энергопотребления для повышения плотности серверов и динамическое энергосбережение для снижения операционных расходов (OPEX).

- Мониторинг компонентов на ЖК-дисплее

  ЖК-дисплей напрямую получает информацию о компонентах от iBMC. Пользователи используют ЖК-дисплей для мониторинга статуса компонентов, просмотра аварийных сигналов и установки параметров сети iBMC.

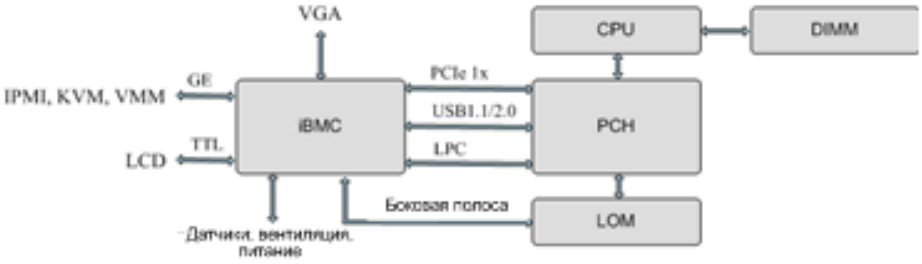
Клиент (локальный ПК), используемый для доступа к iBMC работает под управлением следующих версий ОС, браузера и среды Java (JRE), представленных в Табл. 3-65.

2.2 Конструкция системы

В iBMC используется микросхема Huawei Hi1710, которая оптимизирована для управления на уровне плат. Микросхема Hi1710 состоит из одноядерного ЦП A9, который работает с максимальной частотой 800 МГц, однокристального микрокомпьютера 8051 и сопроцессора с частотой 200 МГц. Для получения и передачи пакетов MCTP, микросхема Hi1710 поддерживает удаленную консоль KVM, IPMI и PCIe. Она предоставляет локальные порты VGA, GE и RMII, а также широкий выбор портов управления платой и периферийных портов.

На Рис. 2-1 показана архитектура системы iBMC.

Рис. 2-1 Архитектура системы



- Модуль KVM выполняет дистанционное управление клавиатурой и мышью. Когда модуль KVM получает видеоданные из системы x86 по порту VGA, он сжимает эти данные и отправляет их удаленному клиенту KVM по сети. Когда модуль KVM получает данные с клавиатуры и мыши от удаленного клиента KVM, он передает данные в систему x86 с помощью смоделированной USB-клавиатуры и мыши.
- iBMC получает рабочие данные системы от системы x86 через интерфейс PCIe и предоставляет интерфейс для экспорта рабочих данных системы.
- iBMC взаимодействует с системой x86 через локальный интерфейс ПК (LPC) для реализации управления IPMI.
- iBMC предоставляет интерфейсы GE, через которые осуществляется удаленное управление по сети с использованием IPMI и HTTPS.
- Для мониторинга температуры и напряжения сервера iBMC использует датчики. Он также выполняет интеллектуальное управление модулями вентиляторов и блоками питания (PSU) сервера.
- iBMC поддерживает технологию внеполосного интерфейса сетевого контроллера (NC-SI – network controller sideband interface) и функцию VLAN, которые обеспечивают более гибкую организацию сети.
- Подключение iBMC к ЖК-дисплею выполняется через последовательный порт TTL. Пользователи используют ЖК-дисплей для мониторинга статуса компонентов, просмотра аварийных сигналов, запроса и настройки данных сетевого порта iBMC.

2.3 Управление безопасностью

Возможности системы безопасности

iBMC предоставляет следующие возможности:

- Изоляция между плоскостью управления и плоскостью услуг

  Сервер, как правило, имеет две сетевых плоскости: плоскость управления и плоскость услуг. iBMC только управляет безопасностью на плоскости управления. Безопасность плоскостей услуг и управления поддерживают другие серверные компоненты или клиентские решения.

  Внеполосной интерфейс сетевого контроллера (NC-SI – Network Controller Sideband Interface) позволяет iBMC и плоскости услуг использовать одну сетевую интерфейсную плату (NIC – network interface card). Поскольку плоскости управления и услуг используют один физический сетевой порт, они логически изолированы VLAN и являются невидимыми друг для друга.

В WebUI iBMC выберите **Configuration** > **Network** для настройки совместно используемого сетевого порта и изоляции между плоскостью управления и плоскостью услуг. Подробная информация приведена в разделе 3.7.5 Сеть.

- Защита протоколов и портов от атак

  iBMC предоставляет минимально необходимые сервисные сетевые порты. По умолчанию ненужные сервисы отключены, порты сетевых служб для отладки отключены во время нормальной работы сервера, а сетевые порты для небезопасных протоколов отключены.

  Как правило серверы поддерживают различные сервисы, включая веб-сервисы, SSH, дистанционное управление, агент SNMP и RMCP/RMCP+. Протокол удаленного управления (RMCP – Remote Management Control Protocol) не является надежным и он по умолчанию отключен. Для изменения конфигурации порта и протокола выберите **Configuration** > **Services** в WebUI iBMC. Подробная информация приведена в разделе 3.7.6 Страница Services.

- Ограничения на вход в зависимости от сценария

  iBMC ограничивает веб-доступ к интерфейсу управления сервером в зависимости от времени, местоположения (IP- или MAC-адреса) и роли.

  Для пользователей из белого списка может быть настроено максимум три правила входа. Правила входа используются для локальных пользователей и пользователей LDAP, однако они не действуют для аккаунта администратора безопасности. При соблюдении любого из трех правил, пользователи могут выполнить вход на iBMC. Каждое правило входа включает три условия: длительность входа, сегмент IP-адресов источника и сегмент MAC-адресов источника. Правила входа выполняются только при соблюдении всех трех условий. При истечении срока действия аккаунта будет выполнен принудительный выход зарегистрированных пользователей из системы.

  ПРИМЕЧАНИЕ

  Пользователь с ID 1 является зарезервированным пользователем, который определен в спецификациях IPMI. Данный пользователь не обладает никакими правами и ему не разрешен вход в iBMC.

  Для настройки правил входа выберите **Configuration** > **Local Users** в WebUI iBMC. Подробная информация приведена в разделе 3.7.1 Локальные пользователи.

- Безопасность аккаунта пользователя

  При настройке параметров безопасности аккаунта пользователя необходимо учитывать правило сложности пароля, срок действия пароля, количество ограниченных к применению предыдущих паролей и максимальное количество неудачных попыток входа в систему до блокировки аккаунта.

  Срок действия пароля (в днях) применяется ко всем локальным пользователям. Пользователь может выполнить вход в iBMC только в течение данного срока действия. При истечении срока действия пароля пользователя, доступ к iBMC для него будет закрыт, однако пользователь, срок действия пароля которого истекает в данный момент времени, и который выполнил вход, может продолжить работать с iBMC.

  Значение срока действия пароля может быть установлено в диапазоне от 0 до 365. **0** означает, что пароль не имеет срока действия. Срок действия пароля пользователя начинается с даты его создания. Срок действия включает количество дней, когда сервер не работал, и будет изменен при изменении системного времени iBMC. При изменении системного времени iBMC, iBMC выполняет автоматическое обновление времени, с которого начинается срок действия пароля каждого пользователя. Если срок действия пароля истекает в течение 10 дней или меньше, то iBMC выводит на экран сообщение «Password will expire after *xx* days.

Please change the password immediately!» при входе пользователя в WebUI iBMC. После истечения срока действия пароля пользователя iBMC записывает это событие в журнал безопасности.

Для изменения настроек безопасности аккаунта пользователя выберите **Configuration** > **Security** в WebUI iBMC. Подробная информация приведена в разделе 3.7.4 Экран Security.

iBMC предоставляет следующие возможности, связанные с паролями:

- Пароль администратора безопасности не имеет срока действия.
- Пароль администратора iBMC можно изменить в BIOS. По умолчанию пользователь с ID 2 в BIOS является администратором iBMC.

- Управление сертификатами

  iBMC поддерживает управление сертификатами SSL и LDAP.

  В WebUI iBMC администраторы могут обновлять SSL-сертификаты, тогда как другие пользователи могут только просматривать базовую информацию сертификата. В целях обеспечения безопасности, исходный сертификат и ключи рекомендуется своевременно заменить настроенным сертификатом и парой открытого и закрытого ключей.

  Для управления сертификатом SSL выберите **Configuration** > **SSL Certificate** в WebUI iBMC. Подробная информация приведена в разделе 3.7.9 Сертификат SSL.

  iBMC поддерживает импорт сертификата LDAP, который предназначен для безопасной и надежной передачи данных LDAP. Для импорта сертификата LDAP выберите **Configuration** > **LDAP** в WebUI iBMC. Подробная информация приведена в разделе 3.7.2 LDAP.

- Управление журналом операций

  iBMC записывает все операции без запроса, выполненные на iBMC. Журналы операций делятся на журналы системных процессов Linux и журналы пользовательских процессов. В каждом журнале пользовательских процессов содержится время выполнения операции, интерфейс, на котором выполнялась операция, IP-адрес источника, имя пользователя и операция.

  Когда размер журнала операций достигает 200 КБ система автоматически создает резервную копию. Система поддерживает хранение только одной копии файла журнала операций. При создании второй копии файла журнала операций, более ранняя версия будет удалена.

  Для просмотра, экспорта данных и управления журналом операций выберите **System** > **Operation Logs** в WebUI iBMC. Подробная информация приведена в разделе 3.8.1 Страница Operation Logs.

- Зашифрованная передача

  iBMC позволяет включить безопасность транспортного уровня (TLS – Transport Layer Security) для простого протокола электронной почты (SMTP – Simple Mail Transfer Protocol) в целях обеспечения безопасности передаваемых данных. Чтобы включить TLS для SMTP выберите **Alarm&SEL** > **Alarm Settings** на WebUI iBMC. Подробная информация приведена в разделе 3.4.3 Настройка аварийных сигналов.

  iBMC позволяет активировать функцию шифрования данных KVM, которая выполняет шифрование данных, передаваемых на и из удаленной виртуальной консоли . Для включения функции шифрования данных KVM выберите **Remote Console** на WebUI iBMC. Подробная информация приведена в разделе 3.9.1 Удаленная виртуальная консоль Java.

Руководство по применению

- Для конфигурирования данных на iBMC используется частная сеть.
- Не допускается подключать iBMC к сети Интернет.
- Отключите ненужные и небезопасные протоколы и порты.
- Периодически выполняйте проверку журналов безопасности.

Исходные параметры

- Имя пользователя и пароль iBMC

  По умолчанию установлено имя пользователя **root** для серверов V3 и **Administrator** для серверов V5, а исходный пароль указан на табличке с маркировкой продукта.

  В целях безопасности после первого входа рекомендуется изменить исходный пароль и периодически менять пароль в дальнейшем. Новый пароль должен соответствовать всем требованиям и быть достаточно сложным.

  Для изменения пароля пользователя выберите **Configuration** > **Local Users** в WebUI iBMC. Подробная информация приведена в разделе 3.7.1 Локальные пользователи.

- Пароль U-Boot

  По умолчанию для серверов V3 установлен пароль U-Boot **Huawei12#$**, а для серверов V5 пароль **Admin@9000**. В целях безопасности пароль, установленный по умолчанию, необходимо изменить. Для изменения пароля необходимо связаться со службой техподдержки компании Huawei.

- Версии SNMP и имена сообществ

  По умолчанию SNMPv3 включен, а SNMPv1 и SNMPv2c отключены, поскольку они представляют угрозу безопасности. При использовании SNMPv1, SNMPv2c и услуги прерываний, измените первоначальные имена сообществ и периодически обновляйте имена сообществ, чтобы обеспечить безопасность системы. Новые имена сообществ должны соответствовать всем требованиям и быть достаточно сложными.

  В Табл. 2-1 приведены имена сообществ SNMP по умолчанию для серверов V3 и V5.

Табл. 2-1 Имена сообществ SNMP

Имя сообщества	Значение по умолчанию для серверов V3	Значение по умолчанию для серверов V5
Имя сообщества SNMP только для чтения	**roAdmin12#$**	**roAdministrator@9000**
Имя сообщества SNMP чтения–записи	**rwAdmin12#$**	**rwAdministrator@9000**
Имя сообщества прерываний	**TrapAdmin12#$**	**TrapAdmin12#$**

Для изменения имен сообществ выберите **Configuration** > **System** в WebUI iBMC. Подробная информация приведена в разделе 3.7.7 Страница System.

- Протоколы и сервисы отключены по умолчанию

  RMCP отключены по умолчанию, поскольку они создают угрозу безопасности из-за наличия дефектов в их механизмах безопасности. Соблюдайте осторожность при использовании данных сервисов.

  Для включения или отключения сервисов выберите **Configuration** > **Services** в WebUI iBMC. Подробная информация приведена в разделе 3.7.6 Страница Services.

- Шифрование и аутентификация

  По умолчанию для алгоритма аутентификации SNMPv3 установлено значение **SHA**, а для алгоритма шифрования SNMPv3 – **AES**. Вы можете использовать и другие алгоритмы SNMPv3; однако, при использовании небезопасных алгоритмов, таких как SHA1, MD5 или DES, необходимо ознакомиться с потенциальными рисками безопасности. Для изменения алгоритмов SNMPv3 выберите **Configuration** > **System** в WebUI iBMC. Подробная информация приведена в разделе 3.7.7 Страница System.

  В целях безопасности функция TLS для SMTP включена по умолчанию. Для включения или отключения данной функции выберите **Alarm&SEL** > **Alarm Settings** в WebUI iBMC. Подробная информация приведена в разделе 3.4.3 Настройка аварийных сигналов.

  Функция шифрования данных KVM отключена по умолчанию. Включите данную функцию для обеспечения безопасности передаваемых данных KVM. Для включения или отключения данной функции выберите **Remote Console** в WebUI iBMC. Подробная информация приведена в разделе 3.9.1 Удаленная виртуальная консоль Java.

  Для обеспечении безопасности передачи электронных сообщений, при первом использовании электронной почты необходимо включить функцию аутентификации пользователей SMTP. Для включения или отключения данной функции выберите **Alarm&SEL** > **Alarm Settings** в WebUI iBMC. Подробная информация приведена в разделе 3.4.3 Настройка аварийных сигналов.

3 Веб-интерфейс пользователя (WebUI) iBMC

О данной главе

В данном разделе приведено описание веб-интерфейса пользователя (WebUI) iBMC.

3.1 Вход в WebUI iBMC

В данном разделе для описания порядка входа в WebUI iBMC используется браузер Internet Explorer 11.

ПРИМЕЧАНИЕ

- Одновременно в WebUI iBMC могут работать максимум четыре пользователя.
- По умолчанию время ожидания составляет 5 минут. Если ни одна из операций не будет выполнена в WebUI в течение 5 минут, то будет выполнен автоматический выход пользователя из WebUI.

- При вводе пользователем неправильного пароля последовательно в течение 5 раз подряд, система заблокирует аккаунт пользователя. Аккаунт пользователя будет автоматически разблокирован по истечении пяти минут. Администратор системы может также разблокировать аккаунт пользователя с помощью интерфейса командной строки.
- В целях безопасности после первого входа рекомендуется изменить исходный пароль и периодически менять пароль в дальнейшем.

Шаг 1 Версии ОС и браузера клиента iBMC (локальный ПК) должны отвечать требованиям. При использовании функции дистанционного управления убедитесь, что используемая версия среды Java (JRE) отвечает требованиям.

Для получения информации о требованиях к версии, обратитесь к Табл. 3-65.

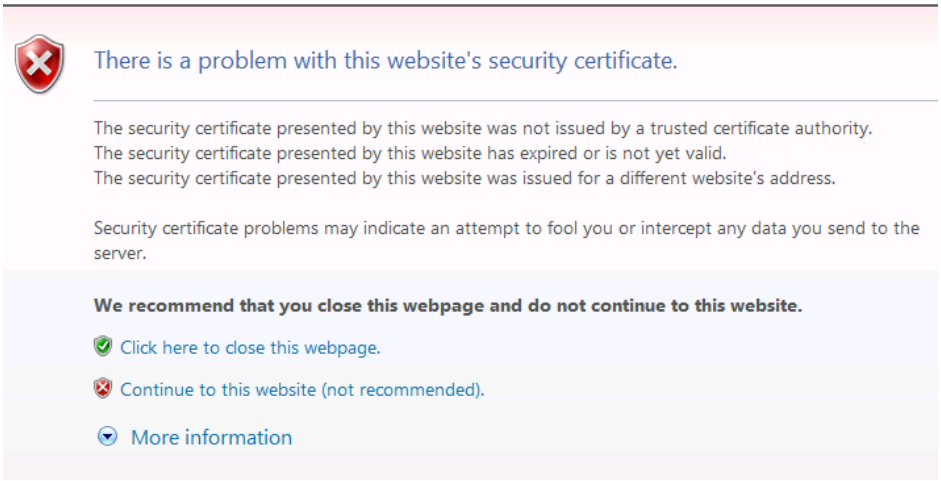
Шаг 2 Установите IP-адрес для ПК. IP-адрес должен находиться в том же сегменте сети, что и сетевой порт управления iBMC.

Шаг 3 Подключите ПК к сетевому порту управления iBMC с помощью сетевого кабеля.

Шаг 4 Откройте Internet Explorer, в адресной строке введите: https://*IP address of the iBMC management network port* и нажмите **Enter**. Более подробная информация о порядке получения IP-адреса приведена в разделе 4.2.2 Проверка IP-адреса сетевого интерфейса управления.

На экране появится информация, показанная на Рис. 3-1.

Рис. 3-1 Проблемы безопасности веб-сайта



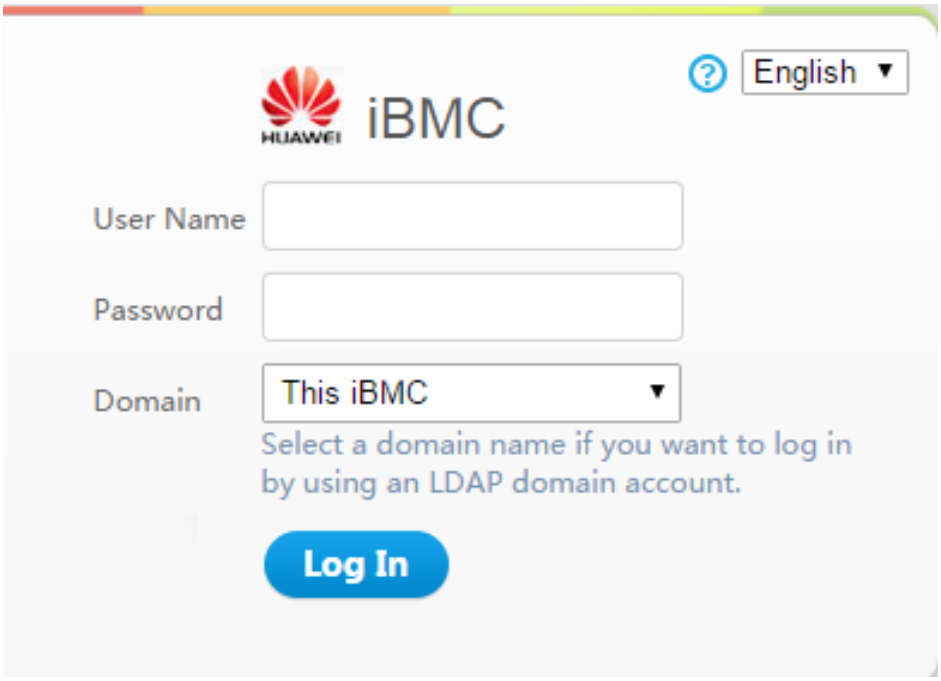
ПРИМЕЧАНИЕ

- Данное сообщение появляется на экране только при входе в WebUI iBMC через Internet Explorer.
- Если вы не хотите, чтобы данное сообщение появлялось на экране, добавьте iBMC к **Exception Site List** на **Java Control panel** или установите самый низкий уровень безопасности Java.

Шаг 5 Выберите **Continue to this website (not recommended)**.

На экране появится страница входа, как показано на Рис. 3-2.

Рис. 3-2 Пользовательский интерфейс для входа в iBMC



Шаг 6 Выполните вход в WebUI iBMC.

Выполните вход в WebUI iBMC, используя один из следующих способов:

- Вход в качестве локального пользователя.
  а. Выберите язык.
  б. Введите имя пользователя и пароль.

  ПРИМЕЧАНИЕ

  По умолчанию для серверов V3 установлено имя пользователя **root**, и пароль по умолчанию **Huawei12#$**. По умолчанию для серверов V5 установлено имя пользователя **Administrator**, и пароль по умолчанию **Admin@9000**.

  в. Выберите **This iBMC** или **Automatic matching** из выпадающего списка **Domain**.
  г. Нажмите **Log In**.

     На экране появится страница **Overview** с именем пользователя в верхнем правом углу.

  ПРИМЕЧАНИЕ

  Система может выводить сообщение о неправильном имени пользователя или пароля при попытке входа в систему через Internet Explorer после обновления системы. В таком случае, нажмите **Ctrl**+**Shift**+**DEL**, затем **Delete** для очистки кэш-памяти браузера, и выполните повторный вход в систему.

  Если выполнить вход не удалось, то выберите **Tools** > **Internet Options** > **Advanced** в строке меню и нажмите **Reset** для восстановления настроек по умолчанию Internet Explorer. После этого выполните повторный вход в систему.

- Вход в систему в качестве пользователя облегченного протокола доступа к каталогам (LDAP – Lightweight Directory Access Protocol).

  Перед входом убедитесь, что выполнены следующие настройки:

- В сети имеется контроллер домена, домен пользователей, который создан на контроллере домена, и пользователи LDAP, которые принадлежат к домену пользователей, также были созданы.

ПРИМЕЧАНИЕ

Для получения более подробной информации о порядке создания контроллера домена, домена пользователей и пользователей LDAP, обратитесь к документации контроллера домена. iBMC предоставляет доступ только для пользователей LDAP.

- В WebUI iBMC функция LDAP включена, установлен домен пользователей, и созданы пользователи LDAP, принадлежащие домену пользователей. Подробная информация приведена на странице **LDAP.**

а. Выберите язык.

б. Введите имя пользователя и пароль LDAP.

ПРИМЕЧАНИЕ

- При вводе имени пользователя LDAP в поле **User Name**, для параметра **Domain** должно быть установлено значение **Automatic matching** или должен быть выбран соответствующий домен.
- При вводе *LDAP user name@Domain name*, то для параметра **Domain** должно быть установлено значение **Automatic matching.**

в. Выберите домен пользователей LDAP из выпадающего списка **Domain.**

ПРИМЕЧАНИЕ

В выпадающем списке **Domain** доступны следующие опции:

- **This iBMC**: Выберите данную опцию для входа в качестве локального пользователя. iBMC автоматически находит пользователя в списке локальных пользователей.
- **Configured domain server:** Выберите сервер домена для входа в качестве пользователя LDAP. iBMC находит пользователя на сервере домена.
- **Automatic matching**: При выборе данной опции, iBMC сначала осуществляет поиск пользователя из списка локальных пользователей. Если соответствие не найдено, то iBMC выполняет поиск на сервере домена в последовательности, которая приведена в выпадающем списке **Domain**.

г. Нажмите **Log In.**

На экране появится страница **Overview** с именем пользователя в врехнем правом углу.

----Конец

3.2 Начало работы

3.2.1 Основные операции

В Табл. 3-1 приведено описание основных операций в WebUI iBMC.

Табл. 3-1 Основные операции

Операция	Процедура
Выбор языка.	На странице входа из выпадающего списка выберите язык.

Операция	Процедура
Просмотр основной информации сервера.	Выберите **Information** > **Overview**. В области **Basic Info** будет представлена информация сервера, включая: • Модель сервера и серийный номер • IP-адрес и версия встроенного ПО iBMC • Версия встроенного ПО BIOS и глобальный уникальный идентификатор (GUID – globally unique identifier) • Максимально допустимое количество веб-сеансов и количество онлайн-пользователей • Статус аварийных сигналов и индикаторов
Получение интерактивной справочной информации.	На странице **System** нажмите .
Запрос пользовательской информации.	После входа в iBMC, нажмите на имя пользователя (например, **root**) после в верхнем правом углу. На экране появится окно **Current User Info** с пользовательской информацией.
Выход из WebUI iBMC.	Нажмите **Logout** в верхнем правом углу.
Просмотр аварийной информации.	В верхнем правом углу WebUI iBMC нажмите на значок аварийной сигнализации. На экране появится страница **Current Alarms** с указанием уровня серьезности аварийных сигналов, описанием, кодами ошибок аварийных сигналов и временем генерирования сигналов, а также приведены соответствующие предложения по устранению аварийных сигналов.
Обновление текущей страницы.	Нажмите в верхнем правом углу WebUI iBMC.

3.2.2 Вход

Описание функции

Доступ к WebUI iBMC можно получить со страницы **Login**.

При вводе пользователем неправильного пароля последовательно в течение 5 раз подряд, система заблокирует аккаунт пользователя. Аккаунт пользователя будет автоматически разблокирован по истечении пяти минут.

ПРИМЕЧАНИЕ

Перед использованием Internet Explorer 11 для входа в WebUI iBMC необходимо включить режим совместимости:

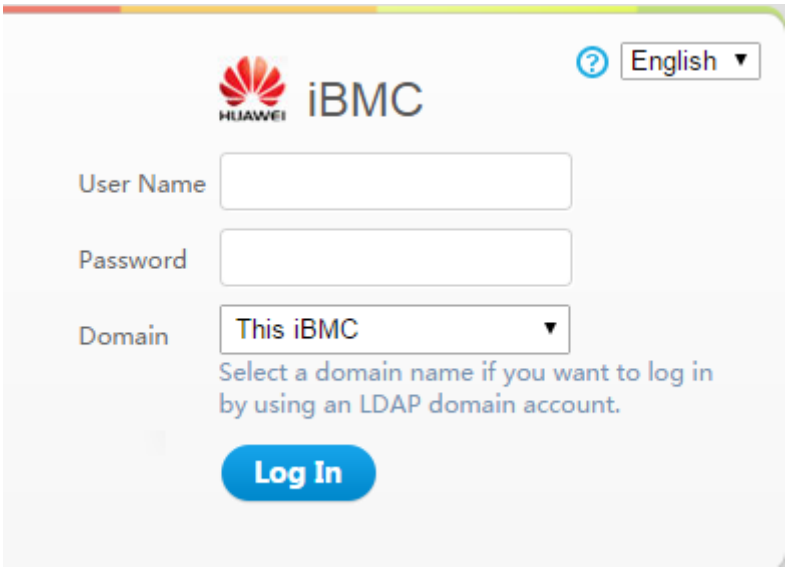
1. Нажмите в верхнем правом углу веб-браузера.
2. Выберите **Compatibility View Settings** из меню быстрого вызова.
3. В диалоговом окне **Compatibility View Settings** введите IP-адрес iBMC в текстовом поле **Add this website** и нажмите **Add**.
4. Отмените выбор **Use Microsoft compatibility lists**.

После запуска режим совместимости, WebUI iBMC будет правильно отображаться на экране, при входе в iBMC с помощью Internet Explorer 11.

Страница входа

Откройте веб-браузер, в адресной строке введите: https://*IP address of the iBMC management network port* и нажмите **Enter**.

Появится страница входа в систему.



Описание параметров

Табл. 3-2 Параметры на странице входа

Параметр	Описание
User Name	Имя пользователя для входа в WebUI iBMC. **ПРИМЕЧАНИЕ** • По умолчанию установлено имя пользователя **root** для серверов V3 и **Administrator** для серверов V5, а а табличке с маркировкой продукта указан пароль по умолчанию. В целях безопасности после первого входа рекомендуется изменить исходный пароль и периодически менять пароль в дальнейшем. • При входе в качестве локального пользователя выберите **This iBMC** или **Automatic matching** из **Domain**. • При входе в качестве пользователя LDAP, имя пользователя может быть представлено в любом из следующих форматов: • Имя пользователя LDAP При вводе имени пользователя LDAP для параметра **Domain** должно быть установлено значение **Automatic matching** или

Параметр	Описание
	должен быть выбран соответствующий домен. • LDAP имя пользователя@имя домена При вводе имени пользователя в формате **LDAP имя пользователя@имя домена**, для параметра **Domain** должно быть установлено значение **Automatic matching**.
Password	Пароль для входа в WebUI iBMC.

Процедура

Вход в качестве локального пользователя

1. На странице входа выберите язык.
2. Введите имя пользователя и пароль.

   Подробная информация о параметрах приведена в Табл. 3-2.
3. Выберите **This iBMC** или **Automatic matching** из выпадающего списка **Domain**.
4. Нажмите **Log In**.

   На экране появится страница **Overview** с именем пользователя в верхнем правом углу.

ПРИМЕЧАНИЕ

Система может выводить сообщение о неправильном имени пользователя или пароля при попытке входа в систему через Internet Explorer после обновления системы. В таком случае, нажмите **Ctrl**+**Shift**+**DEL**, затем **Delete** для очистки кэш-памяти браузера, и выполните повторный вход в систему.

Если выполнить вход не удалось, то выберите **Tools** > **Internet Options** > **Advanced** в строке меню и нажмите **Reset** для восстановления настроек по умолчанию Internet Explorer. После этого выполните повторный вход в систему.

Вход в качестве пользователя LDAP

Перед входом убедитесь, что выполнены следующие настройки:

- В сети имеется контроллер домена, домен пользователей, который создан на контроллере домена, и пользователи LDAP, которые принадлежат к домену пользователей, также были созданы.

ПРИМЕЧАНИЕ

Для получения более подробной информации о порядке создания контроллера домена, домена пользователей и пользователей LDAP, обратитесь к документации контроллера домена. iBMC предоставляет доступ только для пользователей LDAP.

- В WebUI iBMC функция LDAP включена, установлен домен пользователей, и созданы пользователи LDAP, принадлежащие домену пользователей. Подробная информация приведена на странице **LDAP**.

1. Выберите язык.
2. На странице **User Login** введите имя пользователя LDAP и пароль.

ПРИМЕЧАНИЕ

- При вводе имени пользователя LDAP в поле **User Name**, для параметра **Domain** должно быть установлено значение **Automatic matching** или должен быть выбран соответствующий домен.

- При вводе *LDAP user name@Domain name*, то для параметра **Domain** должно быть установлено значение **Automatic matching**.

3. Выберите домен пользователей LDAP из выпадающего списка **Domain**.

ПРИМЕЧАНИЕ

В выпадающем списке **Domain** доступны следующие опции:

- **This iBMC**: Выберите данную опцию для входа в качестве локального пользователя. iBMC автоматически находит аккаунт пользователя в списке локальных пользователей.
- **Configured domain server:** Выберите сервер домена для входа в качестве пользователя LDAP. iBMC автоматически находит пользователя на сервере домена.
- **Automatic matching**: При выборе данной опции, iBMC сначала осуществляет поиск аккаунта пользователя из списка локальных пользователей. Если соответствие не найдено, то iBMC выполняет поиск на сервере домена в последовательности, которая приведена в выпадающем списке **Domain**.

4. Нажмите **Login**.

   На экране появится страница **Overview** с именем пользователя в верхнем правом углу.

3.3 Информация

3.3.1 Страница Overview

На странице **Overview** приведена основная информация о сервере, указаны виртуальные кнопки, и ярлыки для выполнения обычных операций.

GUI

Выберите **Information** из главного меню и выберите **Overview** из дерева навигации.

На экране появится страница **Overview**.

Страница **Overview** состоит из четырех областей, как показано на Рис. 3-3.

Четыре области страницы **Overview** приведены на Рис. 3-3, Рис. 3-4 и Рис. 3-5.

В Табл. 3-3 приведено описание информации, отображаемой в каждой из областей.

ПРИМЕЧАНИЕ

Содержание страницы **Overview** различается в зависимости от режима работы сервера RH8100 V3 или 8100 V5. На странице **Overview** серверов RH8100 V3 или 8100 V5, работающих в двухсистемном режиме, представлены параметры **VGA/USB/DVD** и ярлык **Node Redirect**.

Рис. 3-3 Страница **Overview** сервера RH8100 V3, работающего в односистемном режиме

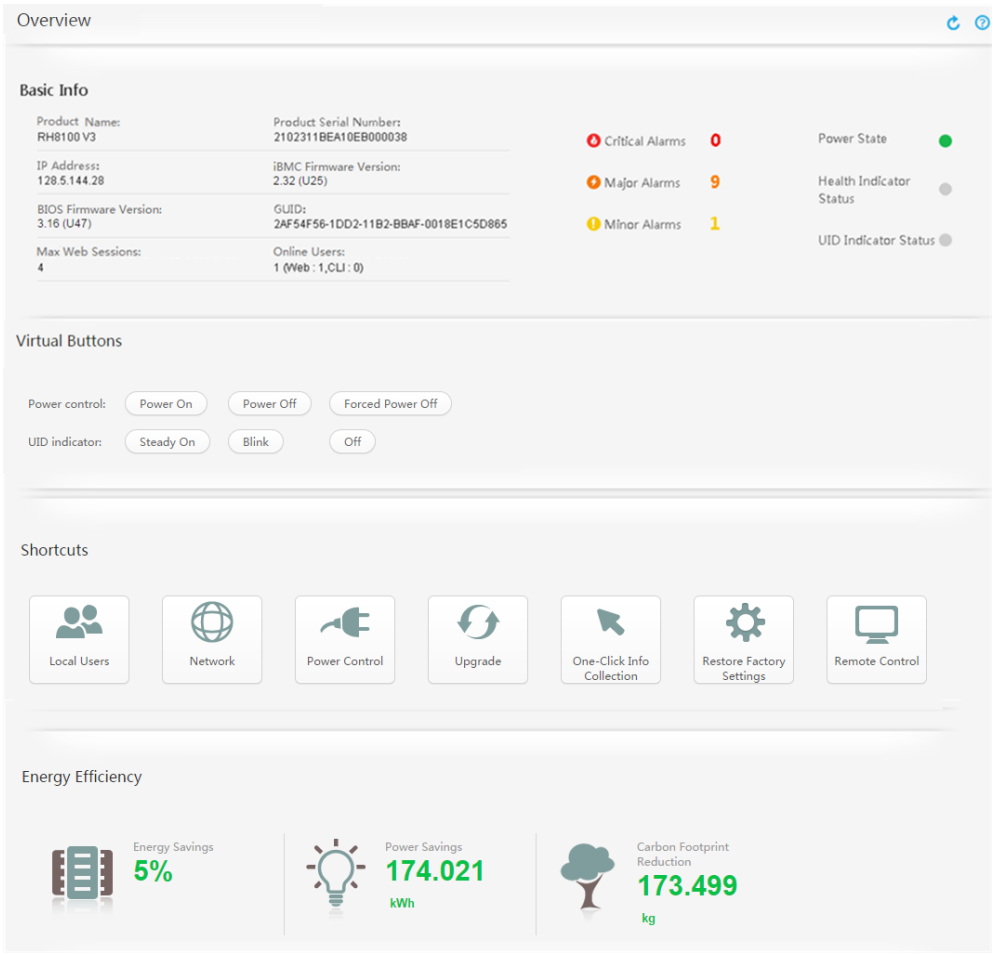


Рис. 3-4 Станица **Overview** сервера RH8100 V3, работающего в двухсистемном режиме

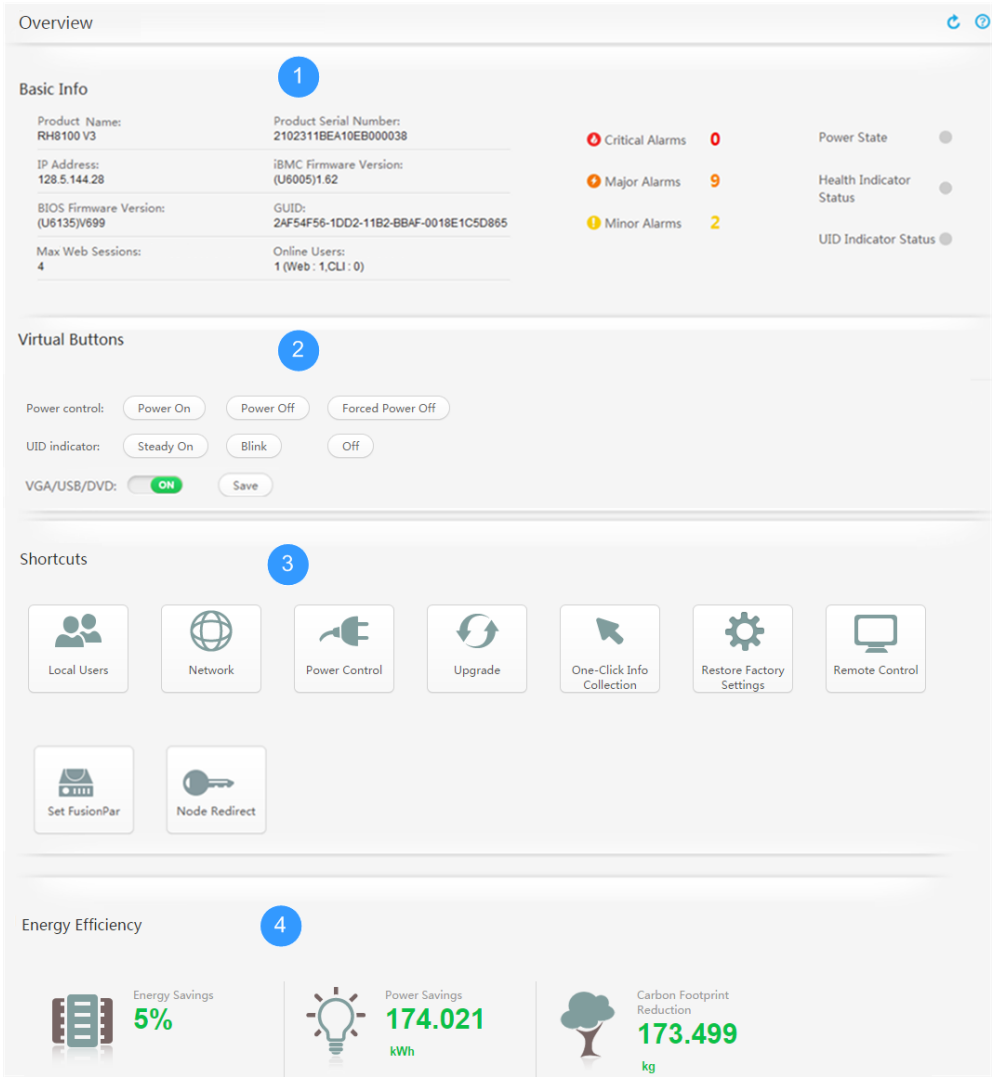
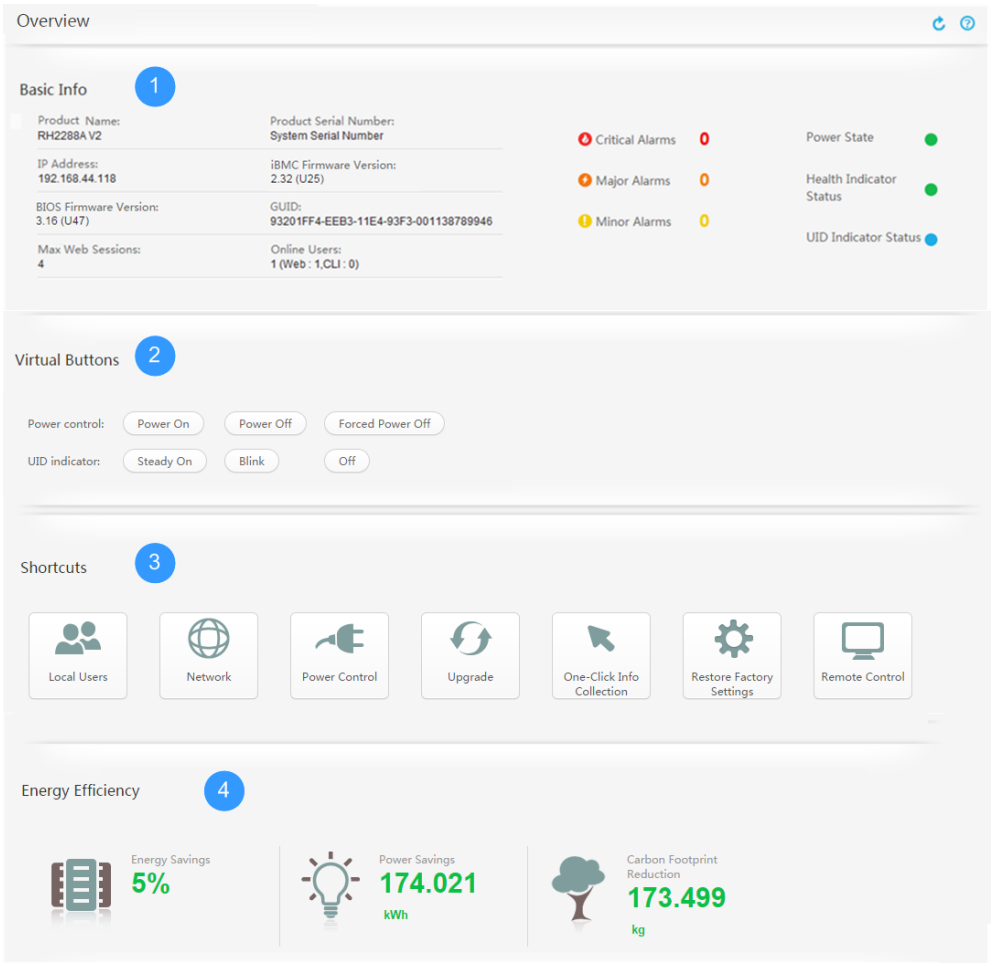


Рис. 3-5 Страница **Overview** других серверов (в зависимости от моделей продукта)



Описание параметров

Табл. 3-3 Описание страницы **Overview**

№	Область	Отображаемая информация
1	Basic Info	Краткая информация о сервере, включая: • **Product Name**: модель сервера. • **Product Serial Number**: серийный номер сервера. • **IP Address**: IP-адрес для входа в iBMC. • **iBMC Firmware Version**: версия встроенного ПО iBMC. • **BIOS Firmware Version**: версия встроенного ПО BIOS. • **GUID**: глобальный уникальный идентификатор сервера. • **Max Web Sessions**: максимальное количество одновременных пользователей в WebUI iBMC. • **Online Users**: количество онлайн-пользователей. Например, **4 (Web: 1; CLI: 2; Redfish: 1)** означает, что в системе имеется 4 онлайн-пользователя: один из них выполнил вход в

№	Область	Отображаемая информация
		систему через веб-интерфейс, два пользователя выполнили вход через интерфейс командной строки, и один через Redfish. • **Power Status**: зеленый цвет означает, что ОС сервера запущена. Серый цвет означает, что работа ОС сервера остановлена. • **Health Indicator Status**: состояние работоспособности сервера. Статус индикатора должен быть таким же, что и на сервере. • **UID Indicator Status**: место размещения сервера в шасси. Статус индикатора должен быть таким же, что и на сервере. • **Critical Alarms**: общее количество критических аварийных сигналов. Аварийные сигналы критического уровня свидетельствуют о наличии неисправности, в результате которой может произойти отключение сервера и прерывание работы всех системных служб. При появлении критических аварийных сигналов необходимо немедленно предпринять меры по локализации и устранению неисправностей. • **Major Alarms**: общее количество серьезных аварийных сигналов. Аварийные сигналы серьезного уровня свидетельствуют о неисправностях, которые оказывают значительное влияние на работу системы. Неисправность такого уровня может привести к системному сбою или прерыванию работы сервисов. • **Minor Alarms**: общее количество незначительных аварийных сигналов. Незначительные аварийные сигналы свидетельствуют о наличии неисправностей, которые не оказывают особого влияния на работу системы. Однако необходимо как можно скорее предпринять меры по их устранению, чтобы предотвратить более серьезную неисправность.
2	Virtual Buttons	Наиболее часто используемые виртуальные кнопки. • **Power control** – **Power On**: включение питания сервера. – **Power Off**: выключение питания сервера. – **Forced Power Off**: принудительное выключение питания сервера. • **UID indicator** – **Steady On**: активация индикатора UID для определения местоположения сервера в шасси. – **Blink**: определение сервера в шасси среди серверов с одинаковым местоположением. – **Off**: деактивация индикатора UID. • **VGA/USB/DVD** (только для серверов RH8100 V3): отображается только когда сервер RH8100 V3 работает в двухсистемном режиме. Если данный параметр  , то порт VGA, USB-порт, и DVD-диск сервера подключены к текущему узлу и отключены от другого узла.

№	Область	Отображаемая информация
3	Shortcut	Ярлыки для выполнения операций, связанных с: • **Local Users** • **Network** • **Power Control** • **Upgrade** • **One-Click Info Collection** Подробная информация о порядке бора данных приведена в разделе 3.11 Сбор информации одним щелчком кнопки мыши. • **Restore Factory Settings** Восстановление заводских настроек, включая но не ограничиваясь: – Состояние подключения последовательного порта – Настройки ограничения энергопотребления – Имена пользователей, пароли, сроки действия, настройки групп пользователей и настройки блокировки пользователей – Режим назначения IP-адресов, IP-адреса, маски подсети и шлюзы по умолчанию – Настройки SNMP – Прерывания SNMP и настройки SNMP дляфункции передачи данных аварийной сигнализации После восстановления заводских настроек, сертификаты LDAP и SSL, загруженные пользователями, будут удалены. • **Remote Control** • **Set FusionPar** (только для сервера RH8100 V3) • **Node Redirect** (только для сервера RH8100 V3, работающего в двухсистемном режиме)
4	Energy Saving Statistics Energy Efficiency	Данные энергосбережения сервера. • **Energy Savings**: коэффициент энергосбережения сервера. • **Power Savings**: питание, сэкономленное сервером. • **Carbon Footprint Reduction**: показатель сокращения углеродосодержащих выбросов сервера. **ПРИМЕЧАНИЕ** • Коэффициент энергосбережения сервера по умолчанию составляет 5%. Его расчет выполняется в зависимости от настроек энергосбережения BIOS. • Показатель энергосбережения = Фактическая потребляемая мощность×(1/(1–коэффициент энергосбережения) –1) • Экономия энергии в 1 кВт×ч приводит к сокращению углеродосодержащих выбросов на 0,997 кг Для обновления статистики энергосбережения выберите **Power** > **Power Capping** и нажмите **Reset Statistics**.

3.3.2 Страница System Info

Описание функции

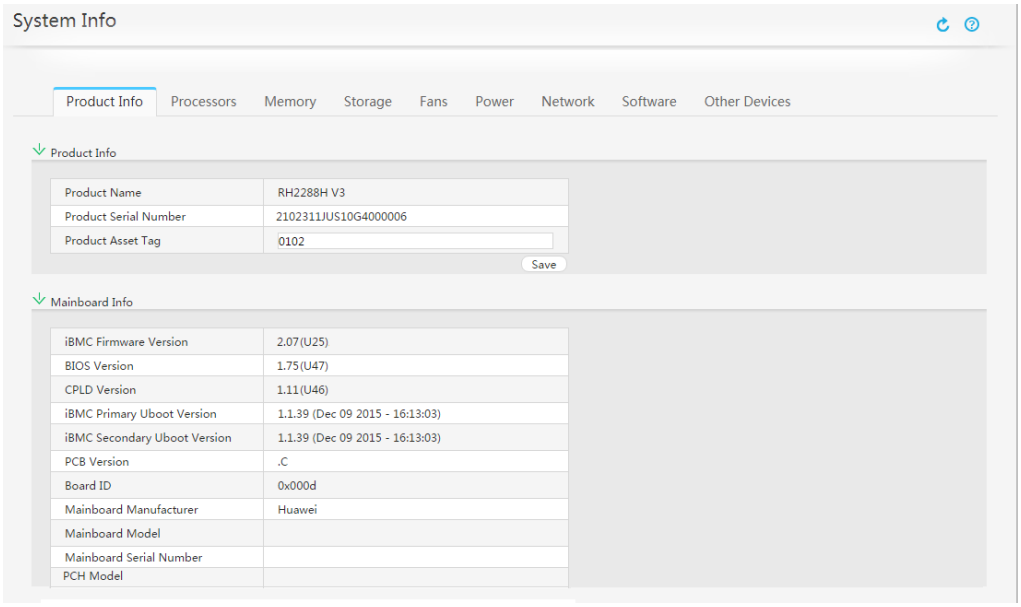
На странице **System Info** приведена системная информация сервера. На данной странице также можно выполнить настройку и управление RAID-контроллером.

GUI

Перейдите к **Information** и выберите **System Info** из дерева навигации.

На экране появится страница **System Info**.

Рис. 3-6 Страница **System Info** стоечных серверов



Описание параметров

Табл. 3-4 Вкладка **Product Info**

Параметр	Описание
Product Info	
Product Name	Модель сервера
Серийный номер продукта	Серийный номер сервера
Product Asset Tag	Инвентарный номер сервера • Значение: Строка с максимальной длиной 48 байтов, состоящая из цифр, букв и специальных символов. **ПРИМЕЧАНИЕ** У обычных пользователей нет полномочий на настройку инвентарного

Параметр	Описание
	номера продукта.
Mainboard Info	
iBMC Firmware Version	Версия встроенного ПО iBMC
BIOS Version	Версия BIOS
CPLD Version	Версия сложной программируемой логической интегральной схемы (CPLD – Complex programmable logical device).
iBMC Primary Uboot Version	Версия первичного образа универсального загрузчика системы (U-Boot – Universal Boot Loader)
iBMC Secondary Uboot Version	Версия вторичного образа U-Boot
PCB Version	Версия печатной платы (PCB – Printed Circuit Board)
Board ID	Идентификатор платы
Mainboard Manufacturer	Производитель материнской платы
Mainboard Model	Модель материнской платы
Mainboard Serial Number	Серийный номер материнской платы
PCH model	Модель PCH **ПРИМЕЧАНИЕ** Данный параметр доступен только для серверов V5.

Табл. 3-5 Вкладка **Processors**

Параметр	Описание
Processors	Представлена следующая информация о каждом процессоре, установленном на сервере: • Название, производитель, модель, идентификатор процессора, скорость синхронизации, и BOM-код каждого процессора • Количество ядер/потоков, поддерживаемых каждой моделью процессора • **Cache**: объем кэш-памяти L1, L2 и L3 каждого процессора • **Status**: Статус ЦП. • **Other Parameters**: Другие параметры ЦП

Табл. 3-6 Вкладка **Memory**

Параметр	Описание
Memory	Данные DIMM, включая следующее: • Максимальное и фактическое количество DIMM • Название, местоположение, производитель, объем, частота тактовых импульсов, серийный номер, тип, минимальное напряжение, количество рангов, битовая ширина, поддерживаемые технологии, и BOM-код каждого DIMM

Табл. 3-7 Вкладка **Storage**

Параметр	Описание
Views	Отображение устройств памяти сервера в древовидной структуре. **ПРИМЕЧАНИЕ** Если на экране отображается **NA**, то загрузите последнюю документацию по iBMA и программные пакеты с веб-сайта Huaweihttp://e.huawei.com/en/, затем установите и запустите iBMA 2.0.
	RAID controller information: • Название RAID-контроллера, тип, имя драйвера и версия, версия встроенного ПО, поддержка внеполосного управления, состояние работоспособности, режим, версия конфигурации, объем памяти, интерфейсы устройства, адрес SAS, поддерживаемый диапазон размера блока данных, статус связанной кэш-памяти, сохранение истории сбоев PD, статус копирования, копирование по статусу ошибки SMART, и статус JBOD. • Название BBU и статус. **ПРИМЕЧАНИЕ** Если плата RAID-контроллера не поддерживает внеполосное управление и, при этом, не установлен iBMA 2.0, то на экране отображается только имя RAID-контроллера и тип.
	Logical drive information: Название, статус, уровень и емкость RAID, размер блока данных, статус кэширования SSCD, политика чтения по умолчанию, текущая политика чтения, политика записи по умолчанию, текущая политика записи, политика ввода-вывода по умолчанию, текущая IP-политика, статус кэш-памяти диска, политика доступа, тип инициализации, статус BGI, статус кэш-памяти L2, статус проверки согласованности, буква диска с установленной ОС и является ли данный диск загрузочным диском. **ПРИМЕЧАНИЕ** Если плата RAID-контроллера не поддерживает внеполосное управление и, при этом, не установлен iBMA 2.0, то логические диски под управлением платы RAID-контроллера не отображаются на экране.

Параметр	Описание
	Disk information: Производитель, емкость, модель, серийный номер, версия встроенного ПО и номер, тип носителя, тип интерфейса, максимальная скорость, скорость канала, адрес SAS (0), адрес SAS (1), состояние питания, температура, статус «горячего резерва», статус модернизации, состояние работоспособности, износ носителя, статус местоположения и количество часов во включенном состоянии. **ПРИМЕЧАНИЕ** • Если плата RAID-контроллера не поддерживает внеполосное управление и, при этом, не установлен iBMA 2.0, то на экране отображаются только типы интерфейсов физических дисков платы RAID-контроллера. • Система поддерживает функцию запроса количества часов во включенном состоянии только для дисков SATA и SAS-дисков Seagate.
Configure	Настройка RAID-контроллера.
	Настройка RAID-контроллера: • Копирующее архивирование • Копирующее архивирование при появлении ошибки SMART • JBOD Способ настройки: выберите значение из выпадающего списка **Value** и нажмите **Save**. Для возврата к заводским настройкам нажмите **Restore settings**.
	Настройка логического диска: • Создание логического диска • Удаление логического диска • Изменение логического диска Способ настройки: выберите пункт и установите соответствующие параметры.
	Настройка физического диска: • Статус «горячего» резерва • Статус встроенного ПО • Статус местоположения Способ настройки: выберите значение из выпадающего списка **Value** и нажмите **Save**.

ПРИМЕЧАНИЕ

При выключении или в процессе запуска ОС, данные на вкладке **Storage** будут недействительны. После запуска ОС, iBMC выполняет повторное обнаружение всех дисков. При перестройке структуры диска в процессе идентификации, данные диска будут действительны только после завершения идентификации диска. Если обнаружить диск не удалось, то будет сгенерирован аварийный сигнал «Drive Fault».

Табл. 3-8 Вкладка **Fans**

Параметр	Описание
Fans	Информация о вентиляторах: • Максимальное и фактическое количество вентиляторов • Имя, номер модели, скорость вращения, коэффициент скорости и BOM-код каждого вентилятора **ПРИМЕЧАНИЕ** Если установлен несовместимый или неисправный модуль вентилятора, то для параметра **Model** будет отображено значение **FAULT**.

Табл. 3-9 Вкладка **Power**

Параметр	Описание
Power	Информация об источнике питания: • Максимальное и фактическое количество блоков питания (PSU) • ID слота, производитель, тип, серийный номер, версия встроенного ПО, номинальная мощность, режим подачи питания и BOM-код каждого источника питания

Табл. 3-10 Вкладка **Network**

Параметр	Описание
ПРИМЕЧАНИЕ • Полная сетевая информация отображается на странице **Network** только после запуска iBMA 2.0. • Если iBMA 2.0 не установлен на сервере, то загрузите последнюю документацию iBMA и пакеты ПО с веб-сайта Huawei,http://e.huawei.com/en/ и установите iBMA 2.0.	
NIC	Информация о LOM, NIC и PCIe NIC. Информация о NIC включает: имя NIC, название производителя, модель, модель микросхемы, производителя микросхемы, версию PCB, ID платы, задействованные ресурсы, версию встроенного ПО, имя драйвера и его версию. **ПРИМЕЧАНИЕ** Нажмите → после NIC для просмотра данных соответствующего порта. В списке представлена информация, включая имена сетевых портов, количество портов, их статус, информация по IPv4-адресам, информация по IPv6-адресам, MAC-адреса, статус VLAN, а также типы сетевых портов.
FC Adapter	Информация об адаптере FC. Информация включает: имя адаптера, название производителя, модуль, модель микросхемы, версию встроенного ПО, имя драйвера и его версию.

Параметр	Описание
	ПРИМЕЧАНИЕ Нажмите на  адаптера FC для просмотра подробной информации.
Bridge	Информация о порте моста. Информация включает имя порта, статус, информацию IPv4 и IPv6 (адрес/маска подсети/шлюз), MAC-адрес, и информацию VLAN (ID VLAN, а также приоритеты VLAN). **ПРИМЕЧАНИЕ** Нажмите на  порт моста для просмотра подробной информации.
Team	Информация об агрегированном сетевом порте. Информация включает имя порта, статус, рабочий режим, информацию IPv4 и IPv6 (адрес/маска подсети/шлюз), MAC-адрес, и информацию VLAN (ID VLAN, статус поддержки VLAN, а также статус поддержки приоритетов VLAN). **ПРИМЕЧАНИЕ** Нажмите на  агрегированного порта для просмотра подробной информации.

Табл. 3-11 Вкладка **Software**

Параметр	Описание
ПРИМЕЧАНИЕ • Полная сетевая информация отображается на странице **System Software** только после запуска iBMA 2.0. • Если iBMA 2.0 не установлен на сервере, то загрузите последнюю документацию iBMA и пакеты ПО с веб-сайта Huawei,http://e.huawei.com/en/ и установите iBMA 2.0.	
Computer Name	Название компьютера, определенное ОС сервера.
Computer Description	Дополнительная информация о сервере.
OS Version	Версия ОС.
OS Kernel Version	Версия ядра при использовании ОС Linux.
Domain/Workgroup	Имя домена или рабочей группы в ОС сервера.
iBMA Service	Версия iBMA.
iBMA Running Status	Рабочий статус iBMA.
iBMA Driver	Версия драйвера iBMA.

Табл. 3-12 Вкладка **Other Devices**

Параметр	Описание
PCIe Card	Информация о плате PCIe: • Максимальное и фактическое количество плат PCIe • Описание, производитель, номер слота, ID производителя, ID устройства и перечень задействованных ресурсов к каждой плате PCIe **ПРИМЕЧАНИЕ** Нажмите на  платы PCIe для просмотра информации о подкартах платы.
HDD Backplane	Информация об объединительной плате жестких дисков: • Максимальное и фактическое количество объединительных плат жестких дисков • Название, производитель, тип, версия PCB, версия CPLD и ID каждой объединительной платы жестких дисков
Riser Card	Информация о райзер-карте: • Максимальное и фактическое количество райзер-карт • Название, производитель, слот, тип, ID платы каждой райзер-карты
SD Card	Информация о карте microSD: • Максимальное и фактическое количество карт microSD • Производитель, серийный номер, емкость каждой карты microSD **ПРИМЕЧАНИЕ** Для сервера RH8100 V3, работающего в односистемном режиме, на экране отображаются только карты microSD первичного iBMC. Для сервера RH8100 V3, работающего в двухсистемном режиме, отображаются все карты microSD. **ПРИМЕЧАНИЕ** Серверы V5 не поддерживают SD-карты.
Security Module	Информация о модулях защиты: • Максимальное и фактическое количество модулей защиты • Тип спецификации, версия спецификации, производитель, версия производителя, а также статус самотестирования каждого модуля защиты
Raid Card	Информация о плате RAID-контроллера: • Максимальное и фактическое количество плат RAID-контроллера • Название, местоположение, производитель, номер, тип, поддерживаемые уровни RAID, версия PCB, версия CPLD, ID платы и задействованные ресурсы каждой платы RAID-контроллера
SD Card Controller	Информация о контроллере карты microSD: • Максимальное и фактическое количество контроллеров

Параметр	Описание
	карт microSD • Производитель и версия каждого контроллера карты microSD **ПРИМЕЧАНИЕ** Серверы V5 не поддерживают контроллеры SD-карты.
LCD	Версия встроенного ПО ЖК-дисплея. **ПРИМЕЧАНИЕ** Серверы RH5885 V3 не поддерживают ЖК-дисплей. Информация о ЖК-дисплее не отображается на экране. Серверы RH5885H V3 поддерживают ЖК-дисплей. На экран будет выведена информация о ЖК-дисплее.
CPU Board	Информация о плате ЦП: • Максимальное и фактическое количество текущих плат ЦП • Название, производитель, номер слота, тип, версия PCB, версия CPLD, ID платы и питание каждой платы ЦП **ПРИМЕЧАНИЕ** Только сервер 8100 V5 поддерживает отображение питания платы ЦП.
Memory Board	Информация о плате памяти: • Максимальное и фактическое количество плат памяти • Название, производитель, номер слота, тип, версия PCB, ID каждой платы памяти **ПРИМЕЧАНИЕ** Сервер RH5885 V3 не поддерживает платы памяти. Поэтому информация о платах памяти не отображается. Сервер RH5885H V3 поддерживает платы памяти. На экране отображается информация о плате памяти.
IO Board	Информация о плате ввода-вывода: • Максимальное и фактическое количество плат ввода-вывода • Название, производитель, тип, версия PCB, версия CPLD, ID платы и питание каждой платы ввода-вывода **ПРИМЕЧАНИЕ** Только серверы 8100 V5 поддерживают отображение питания платы ввода-вывода.
M.2 Adapter	Информация об адаптере M.2, включая название, описание, версию PCB и ID платы. **ПРИМЕЧАНИЕ** Только серверы RH2288 V3 и RH2288H V3 поддерживают адаптеры M.2.

Запрос системной информации

1. В строке меню выберите **Information**.
2. В дереве навигации выберите **System Info**.

На экране появится страница **System Info**.

3. На данной странице приведена информация о сервре и его компонентах.

Запрос свойств платы RAID-контроллера

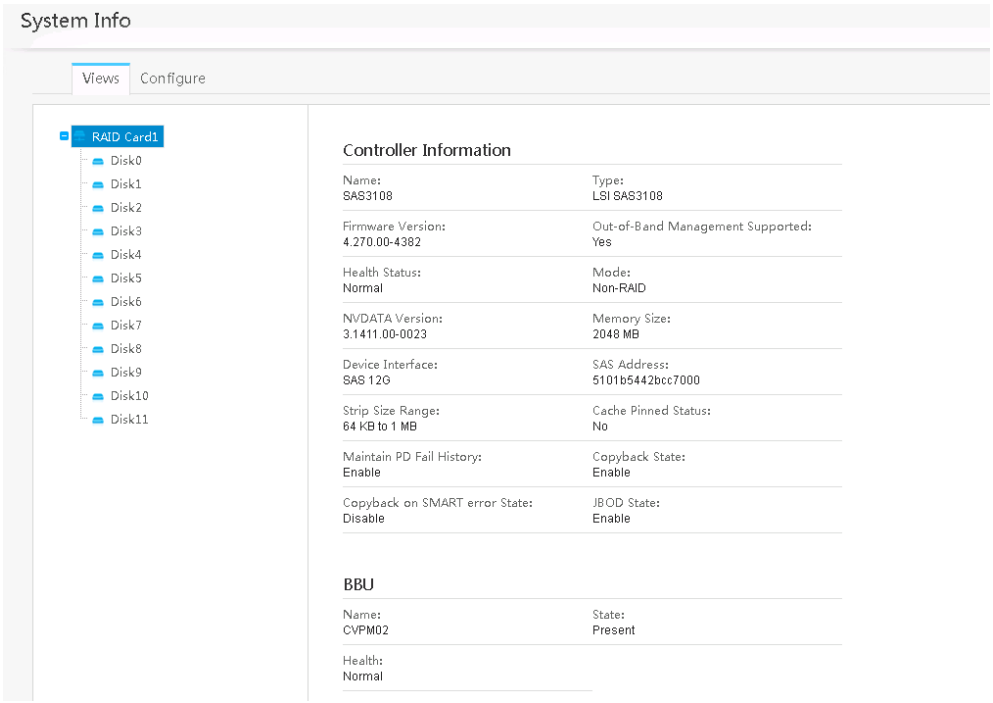
ПРИМЕЧАНИЕ

Данная операция может быть выполнена только если плата RAID-контроллера поддерживает внеполосное управление или если выполнен запуск iBMA 2.0.

1. На странице **System Info** перейдите на вкладку **Storage**.
2. На вкладке **Views** выберите плату RAID-контроллера.

   Свойства RAID-контроллера будет отображены на панели справа, как показано на Рис. 3-7.

Рис. 3-7 Запрос свойств платы RAID-контроллера



Запрос свойств RAID-массива

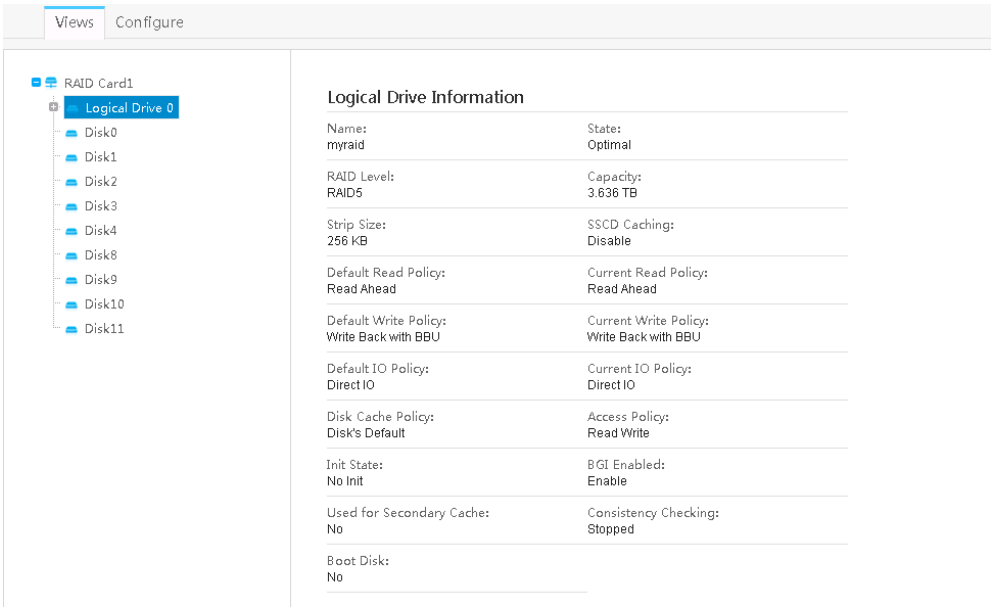
ПРИМЕЧАНИЕ

Данная операция может быть выполнена только если плата RAID-контроллера поддерживает внеполосное управление или если выполнен запуск iBMA 2.0.

1. На странице **System Info** перейдите на вкладку **Storage**.
2. На вкладке **Views** выберите RAID-массив.

   Свойства RAID-массива будет отображены на панели справа, как показано на Рис. 3-8.

Рис. 3-8 Запрос свойств RAID-массива



Запрос свойств жесткого диска

ПРИМЕЧАНИЕ

Данная операция может быть выполнена только если плата RAID-контроллера поддерживает внеполосное управление или если выполнен запуск iBMA 2.0.

1. На странице **System Info** перейдите на вкладку **Storage**.
2. На вкладке **Views** выберите жесткий диск (диск из RAID-массива или независимый жесткий диск).

   Свойства жесткого диска будут отображены на панели справа, как показано на Рис. 3-9 и Рис. 3-10.

Рис. 3-9 Запрос свойств диска RAID-массива

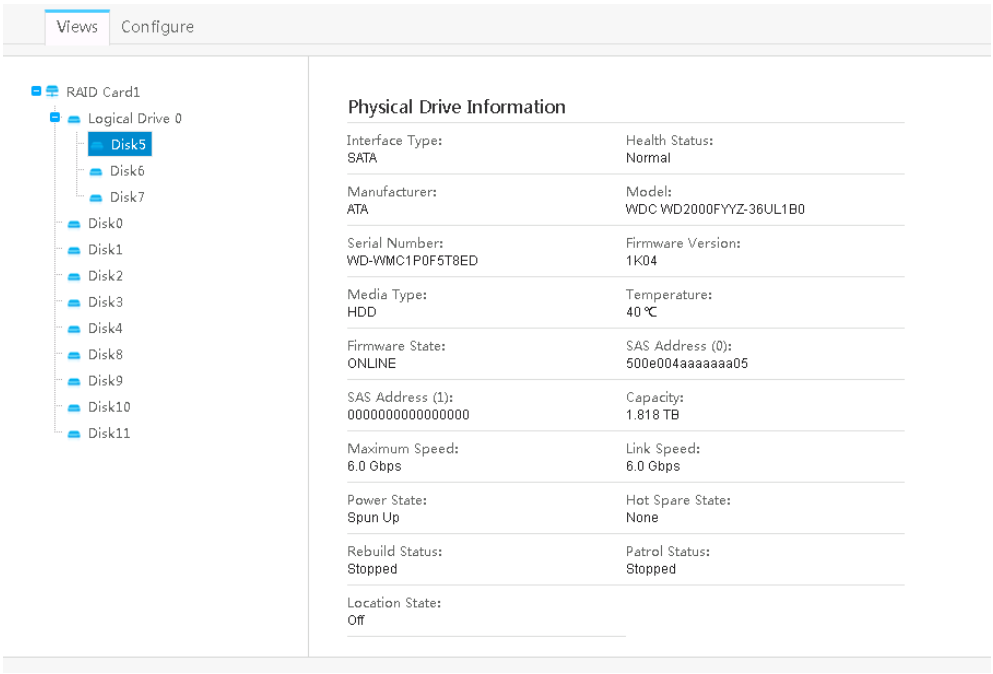
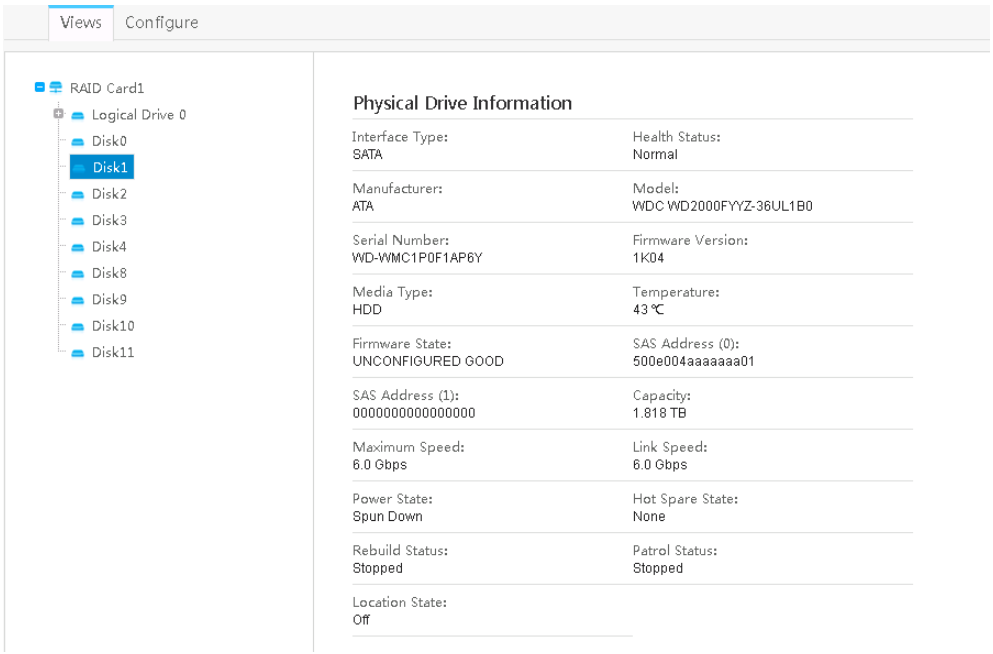


Рис. 3-10 Запрос свойств независимого жесткого диска



Изменение свойств платы RAID-контроллера

ПРИМЕЧАНИЕ

Данная операция может быть выполнена только если плата RAID-контроллера поддерживает внеполосное управление или если выполнен запуск iBMA 2.0.

1. На странице **System Info** перейдите на вкладку **Storage**.
2. Перейдите на вкладку **Configure**.

   На экране появится страница конфигурации RAID-контроллера.
3. Выберите плату RAID-контроллера.
4. Нажмите  после **RAID Controller**.

   На экране появится окно настройки RAID-контроллера, как показано на Рис. 3-11. В Табл. 3-13 приведено описание параметров.

Рис. 3-11 Изменение свойств платы RAID-контроллера

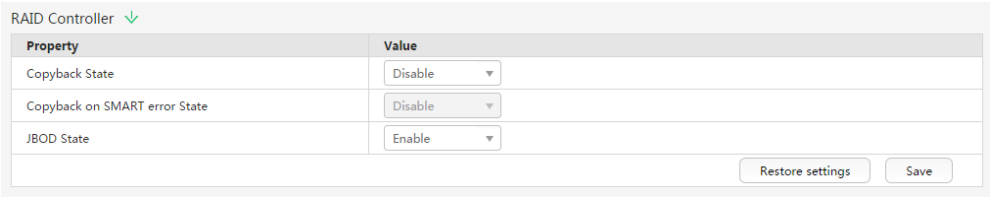


Табл. 3-13 Описание параметров

Параметр	Описание
Copyback State	Функция копирования позволяет копировать данные с исходного диска на целевой диск. Если диск из RAID-массива с поддержкой избыточности становится неисправным, то диск с поддержкой «горячего» резерва автоматически начинает работу и запускает синхронизацию данных. После установки нового диска для замены неисправного, выполняется копирование данных с резервного диска на новый. По завершении копирования данных резервный диск переходит в статус выполнения «горячего» резервирования данных.
Copyback on SMART error State	Запуск копирования данных при появлении на диске первой ошибки технологии повышения надёжности работы на основе предсказания сбоев в работе (SMART – Self-Monitoring Analysis and Reporting Technology).
JBOD State	Просто несколько жестких дисков (JBOD – Just a bunch of disks) позволяет напрямую передавать команды с RAID-контроллера на подключенные жесткие диски без необходимости конфигурирования логических дисков. Эта функция позволяет сервисам верхнего уровня или ПО управления получить доступ к физическим дискам и управлять физическими дисками.

5. Установите все необходимые параметры и нажмите **Save**.

Создание логического диска

ПРИМЕЧАНИЕ

Данная операция может быть выполнена только если плата RAID-контроллера поддерживает внеполосное управление или если выполнен запуск iBMA 2.0.

1. На странице **System Info** перейдите на вкладку **Storage**.
2. Перейдите на вкладку **Configure**.

   На экране появится страница конфигурации RAID-контроллера.
3. Выберите плату RAID-контроллера.
4. Нажмите → после **Logical Drive**.

   На экране появится страница конфигурации логического диска.
5. Нажмите на кнопку перед **Create**.

   На экране появится окно настройки логического диска, как показано на Рис. 3-12. В Табл. 3-14 приведено описание параметров.

Рис. 3-12 Создание логического диска

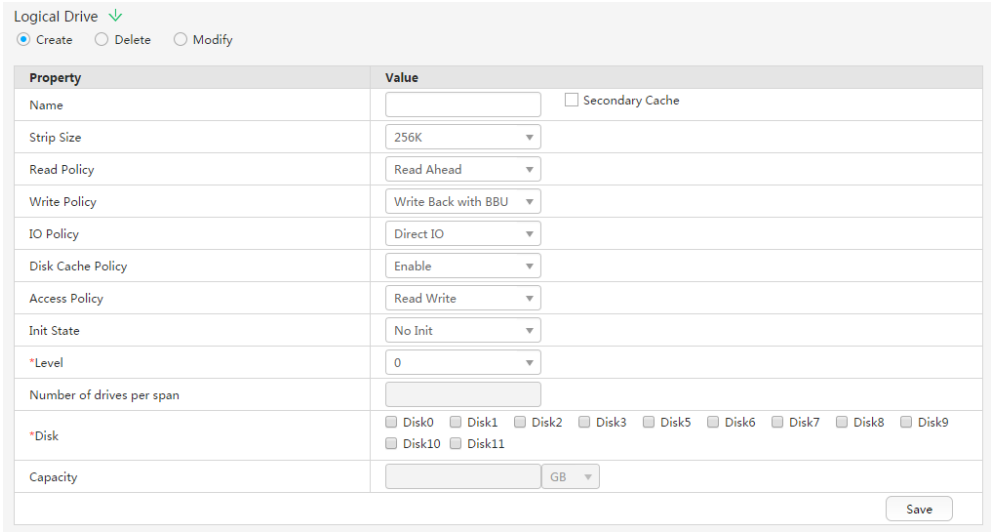


Табл. 3-14 Описание параметров

Параметр	Описание
Name	Идентификатор логического диска
Secondary Cache	Кэширование данных
Strip Size	Размер блока данных каждого физического диска.
Read Policy	Политика чтения данных с логического диска. Значение: • **Read Ahead**: RAID-контроллер предварительно считывает последовательные данные или данные, которые предполагается использовать, и сохраняет их в кэш-памяти.

Параметр	Описание
	• **No Read Ahead**: функция опережающего считывания данных отключена.
Write Policy	Политика записи данных на логический диск. Значение: • **Write Through**: после получения всех данных контроллер отправляет на хост сообщение, в котором говорится о том, что передача данных завершена. • **Write Back with BBU**: если блок резервной аккумуляторной батареи (BBU – battery backup unit) не сконфигурирован или сконфигурированный BBU неисправен, то RAID-контроллер автоматически переходит в режим Write Through (одновременная запись в кэш-память и на диск). • **Write Back**: после получения всех данных в кэш-память, контроллер отправляет на хост сообщение, в котором говорится о том, что передача данных завершена.
IO Policy	Политика ввода-вывода (I/O – input/output) при чтении данных со специальных логических дисков. Данная политика не оказывает никакого влияния на предварительное считывание данных из кэш-памяти. Значение: • **Cached IO**: все запросы на чтение и запись обрабатываются кэш-памятью RAID-контроллера. Система поддерживает выбор данного параметра только если сконфигурирован CacheCade 1.1. • **Direct IO**: данная опция имеет различные значения в сценариях считывания и записи данных. – В сценариях считывания, данные непосредственно считываются с физических дисков (если для параметра **Read Policy** установлено значение **Read Ahead**, то запросы на считывание данных обрабатываются кэш-памятью RAID-контроллера). – В сценриях записи, все запросы на запись обрабатываются кэш-памятью RAID-контроллера (если для параметра **Write Policy** установлено значение **Write Through**, то запись данных осуществляется непосрелдственно на физические диски).
Disk Cache Status	Значения статуса кэш-памяти диска могут быть следующими:

Параметр	Описание
	• **Enable**: запись данных в кэш-память перед записью данных на жесткий диск. Данная опция повышает производительность записи данных. Однако данные будут потеряны, если система не поддерживает механизм защиты от сбоев питания. • **Disable**: запись данных на жесткий диск без кэширования данных. При сбое питания данные не будут потеряны. • **Disk's default**: политика кэширования, установленная по умолчанию.
Access Policy	Политика доступа к логическому диску. Значение: • **Read/Write:** операции чтения и записи разрешены • **Read Only**: логческий диск только для чтения • **Blocked**: доступ к логическому диску запрещен
Init State	Инициализация созданного логического диска. Значение: • **No Init**: инициализация не выполняется. • **Quick Init**: запись нулей в первые и последние 10 МБ логического диска. После этого статус логического диска изменится на **Optimal.** • **Full Init**: инициализация логического диска. Перед завершением инициализации, статус логического диска будет **initialization.**
Level	Уровень RAID логического диска.
Number of drives per span	Установите данный параметр при использовании уровней RAID 10, 50 или 60.
Disk	Диски, которые добавляются к логическому диску.
Capacity	Объем логического диска.

6. Установите все необходимые параметры и нажмите **Save.**

Удаление логических дисков

ПРИМЕЧАНИЕ

Данная операция может быть выполнена только если плата RAID-контроллера поддерживает внеполосное управление или если выполнен запуск iBMA 2.0.

1. На странице **System Info** перейдите на вкладку **Storage.**
2. Перейдите на вкладку **Configure.**

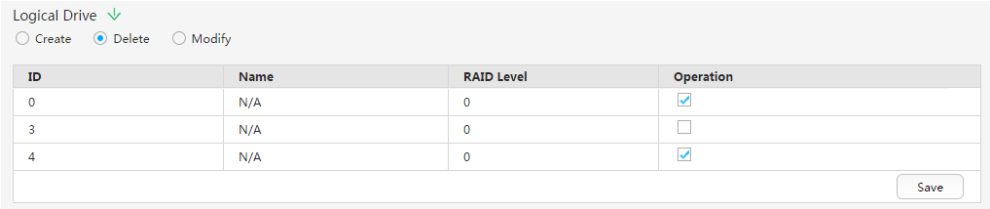
   На экране появится страница конфигурации RAID-контроллера.

3. Выберите плату RAID-контроллера.
4. Нажмите → после **Logical Drive**.

   На экране появится страница конфигурации логического диска.
5. Нажмите на кнопку перед **Delete**.

   На экране появится окно настройки логического диска, как показано на Рис. 3-13.

Рис. 3-13 Удаление логических дисков



6. Выберите логические диски для удаления и нажмите **Save**.

Изменение свойств логического диска

ПРИМЕЧАНИЕ

Данная операция может быть выполнена только если плата RAID-контроллера поддерживает внеполосное управление или если выполнен запуск iBMA 2.0.

1. На странице **System Info** перейдите на вкладку **Storage**.
2. Перейдите на вкладку **Configure**.

   На экране появится страница конфигурации RAID-контроллера.
3. Выберите плату RAID-контроллера.
4. Нажмите → после **Logical Drive**.

   На экране появится страница конфигурации логического диска.
5. Нажмите на кнопку перед **Modify**.

   На экране появится окно настройки логического диска, как показано на Рис. 3-14. В Табл. 3-15 приведено описание параметров.

Рис. 3-14 Изменение свойств логического диска

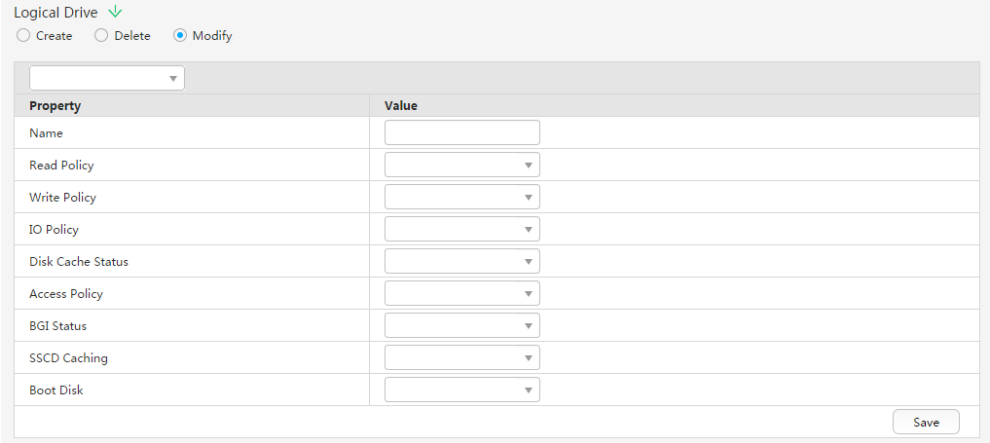


Табл. 3-15 Описание параметров

Параметр	Описание
Name	Идентификатор логического диска
Read Policy	Политика чтения данных с логического диска. Значение: • **Read Ahead**: RAID-контроллер предварительно считывает последовательные данные или данные, которые предполагается использовать, и сохраняет их в кэш-памяти. • **No Read Ahead**: функция опережающего считывания данных отключена.
Write Policy	Политика записи данных на логический диск. Значение: • **Write Through**: после получения всех данных контроллер отправляет на хост сообщение, в котором говорится о том, что передача данных завершена. • **Write Back with BBU**: если блок резервной аккумуляторной батареи (BBU – battery backup unit) не сконфигурирован или сконфигурированный BBU неисправен, то RAID-контроллер автоматически переходит в режим Write Through (одновременная запись в кэш-память и на диск). • **Write Back**: после получения всех данных в кэш-память, контроллер отправляет на хост сообщение, в котором говорится о том, что передача данных завершена.
IO Policy	Политика ввода-вывода (I/O – input/output) при чтении данных со специальных логических дисков. Данная политика не оказывает никакого влияния на

Параметр	Описание
	предварительное считывание данных из кэш-памяти. Значение: • **Cached IO**: все запросы на чтение и запись обрабатываются кэш-памятью RAID-контроллера. Система поддерживает выбор данного параметра только если сконфигурирован CacheCade 1.1. • **Direct IO**: данная опция имеет различные значения в сценариях считывания и записи данных. – В сценариях считывания, данные непосредственно считываются с физических дисков (если для параметра **Read Policy** установлено значение **Read Ahead**, то запросы на считывание данных обрабатываются кэш-памятью RAID-контроллера). – В сценриях записи, все запросы на запись обрабатываются кэш-памятью RAID-контроллера (если для параметра **Write Policy** установлено значение **Write Through**, то запись данных осуществляется непосрелдственно на физические диски).
Disk Cache Status	Значения статуса кэш-памяти диска могут быть следующими: • **Enable**: запись данных в кэш-память перед записью данных на жесткий диск. Данная опция повышает производительность записи данных. Однако данные будут потеряны, если система не поддерживает механизм защиты от сбоев питания. • **Disable**: запись данных на жесткий диск без кэширования данных. При сбое питания данные не будут потеряны. • **Disk's default**: политика кэширования, установленная по умолчанию.
Access Policy	Политика доступа к логическому диску. Доступны следующие опции: Значение: • **Read/Write**: операции чтения и записи разрешены • **Read Only**: логический диск только для чтения • **Blocked**: доступ к логическому диску запрещен
BGI Status	Инициализация в фоновом режиме.
SSCD Caching	Использование диска CacheCade в качестве

Параметр	Описание
	кэш-памяти.
Boot Disk	Является ли логический диск загрузочным диском.

6. Выберите логический диск для изменения.
7. Установите все необходимые параметры и нажмите **Save**.

Изменение свойств диска-участника

ПРИМЕЧАНИЕ

Данная операция может быть выполнена только если плата RAID-контроллера поддерживает внеполосное управление или если выполнен запуск iBMA 2.0.

1. На странице **System Info** перейдите на вкладку **Storage**.
2. Перейдите на вкладку **Configure**.

   На экране появится страница конфигурации RAID-контроллера.
3. Выберите плату RAID-контроллера.
4. Нажмите → после **Physical Drive**.

   На экране появится окно настройки физического диска, как показано на Рис. 3-15. В Табл. 3-16 приведено описание параметров, доступных на этом экране.

Рис. 3-15 Изменение свойств физического диска

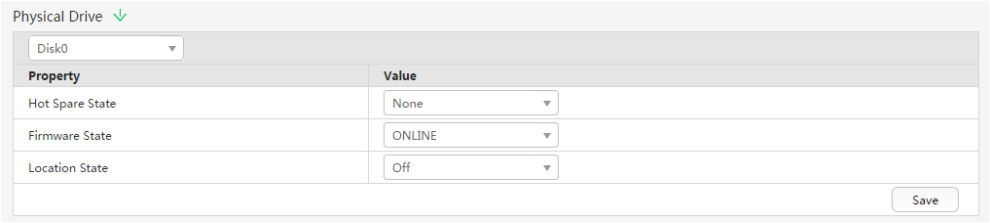


Табл. 3-16 Описание параметров

Параметр	Описание
Hot Spare State	Статус «горячего» резерва физического диска. Значения: • **None**: диск не является диском «горячего» резерва. • **Global**: глобальный диск «горячего» резерва. • **Dedicated**: выделенный диск «горячего» резерва.
Firmware State	Статус физического диска. Значения: • **UNCONFIGURED**: диск недоступен. • **ONLINE**: диск в сети.

Параметр	Описание
	• **OFFLINE**: диск не в сети. • **GOOD**: диск не занят. • **JBOD**: ОС напрямую управляет диском.
Location State	Индикатор местоположения диска.

5. Выберите диск для изменения.
6. Установите все необходимые параметры и нажмите **Save**.

3.3.3 Мониторинг в режиме реального времени

Описание функции

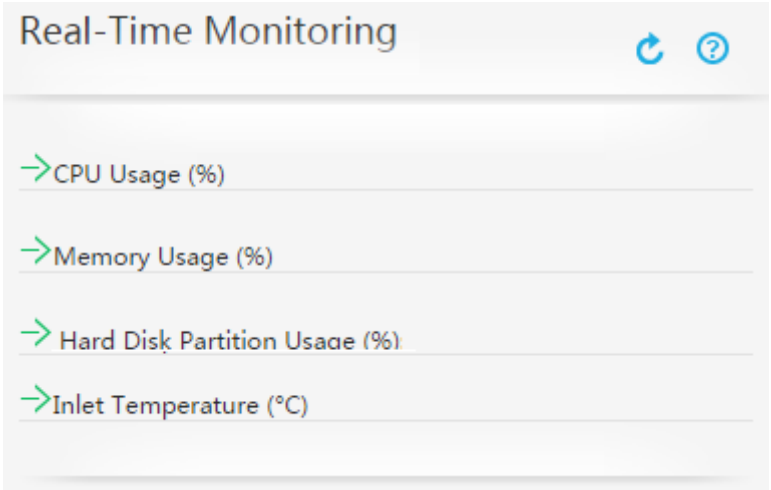
На странице **Real-Time Monitoring** приведена следующая информация:

- Коэффициент использования ЦП за последний час
- Коэффициент использования памяти за последний час
- Объем и коэффициент использования всех разделов дисков
- Архивные данные по температуре воздуха на входе

GUI

Выберите **Information** из главного меню и выберите **Real-Time Monitoring** из дерева навигации.

На экране появится страница **Real-Time Monitoring**.



Описание параметров

Табл. 3-17 Использование ЦП

Параметр	Описание
CPU Usage (%)	Процент ресурсов ЦП, используемых работающими приложениями. **ПРИМЕЧАНИЕ** Если на экране не отображается использование ЦП, то установите и запустите iBMA 2.0.

Табл. 3-18 Использование памяти

Параметр	Описание
Memory Usage (%)	Процент ресурсов памяти, используемых работающими приложениями. **ПРИМЕЧАНИЕ** Если на экране не отображается использование памяти, то установите и запустите iBMA 2.0.

Табл. 3-19 Использование разделов жесткого диска

Параметр	Описание
Hard Disk Partition Usage (%)	В области **Hard Disk Partition Usage** приведена следующая информация: • Процентное отношение используемого пространства раздела к общему пространству раздела • Информация о разделах диска • Общий объем и занятый объем каждого раздела **ПРИМЕЧАНИЕ** Если на экране не отображается использование разделов диска, то установите и запустите iBMA 2.0.

Табл. 3-20 Температура воздуха на входе

Параметр	Описание
Inlet Temperature (°C)	Выборка данных температуры воздуха на входе происходит каждые 10 минут в течение последней недели.

Процедура

1. Выберите **Information** из главного меню и выберите **Real-Time Monitoring** из дерева навигации.

   На экране появится страница **Real-Time Monitoring**.

2. Нажмите  после **CPU Usage (%)**, **Memory Bandwidth Usage (%)**, **Hard Disk Partition Usage (%)** или **Inlet Temperature (°C)**.

ПРИМЕЧАНИЕ

- Для сворачивания данных мониторинга в режиме реального времени нажмите  .
- Для очистки данных статистики нажмите кнопку **Clear Historical Records** из области **Inlet Temperature (°C)**.

3.3.4 Страница Sensor Info

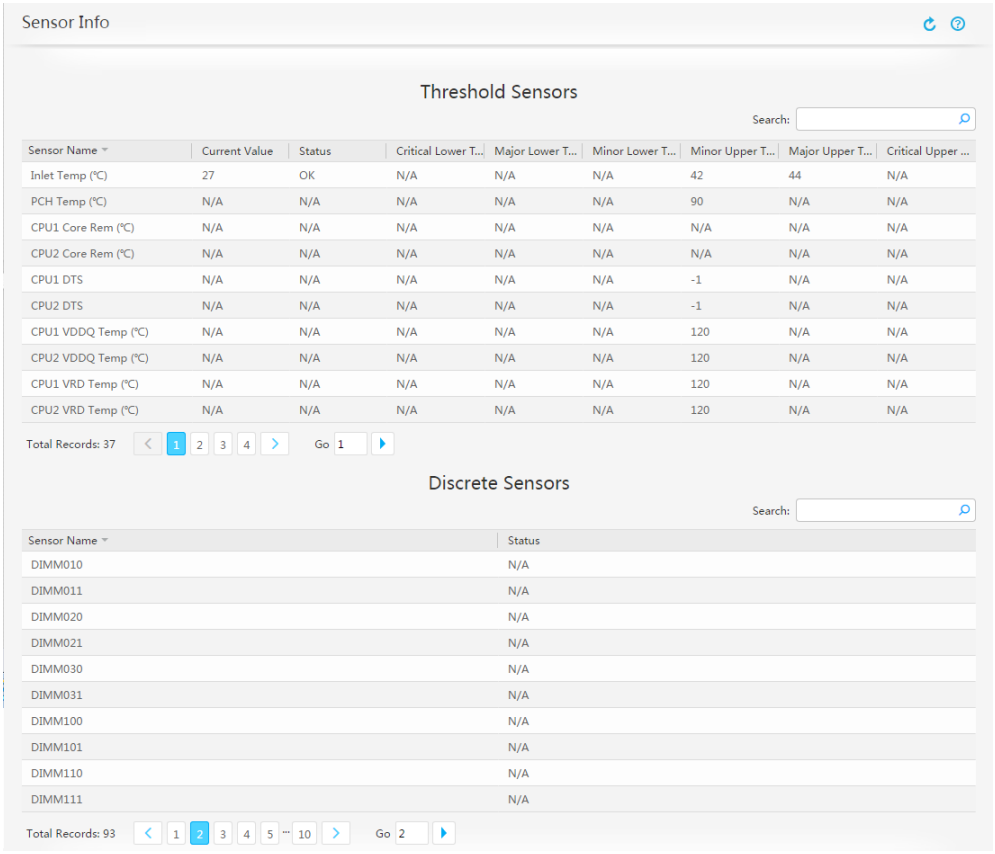
Описание функции

На странице **Sensor Info** приведена информация о пороговых датчиков и дискретных датчиков.

GUI

Выберите **Information** из главного меню и выберите **Sensor Info** из дерева навигации.

На экране появится страница **Sensor Info**.



Описание параметра

Табл. 3-21 Параметры на странице **Sensor Info**

Параметр	Описание
Sensor Name	Логический модуль или физическое устройство, которое осуществляет мониторинг индикаторов сервера.
Current Value	Текущее значение индикатора. Значение **N/A** означает, что датчик не получил данные с индикатора.
Status	Статус порогового датчика. • **OK**: датчик работает исправно. • **N/A**: датчик не получил данные с индикатора. • **NC**: датчик обнаружил незначительную аварию. • **CR**: датчик обнаружил серьезную аварию. • **NR**: датчик обнаружил критическую аварию. Статус дискретного датчика. • **N/A**: датчик не определил значение или статус. Контролируемое устройство не установлено. • **0x***XXXX*: шестнадцатеричное число, определенное на основе спецификаций интерфейса для интеллектуальной платформы управления (IPMI), которое необходимо для указания статуса датчика, например, **0x8000**. Подробная информация приведена в руководстве по аварийным сигналам вашего сервера.
Critical Lower Threshold	Нижнее пороговое значение, установленное для датчика, генерирующего критический аварийный сигнал.
Major Lower Threshold	Нижнее пороговое значение, установленное для датчика, генерирующего серьезный аварийный сигнал.
Minor Lower Threshold	Нижнее пороговое значение, установленное для датчика, генерирующего незначительный аварийный сигнал.
Minor Upper Threshold	Верхнее пороговое значение, установленное для датчика, генерирующего незначительный аварийный сигнал.
Major Upper Threshold	Верхнее пороговое значение, установленное для датчика, генерирующего серьезный аварийный сигнал.
Critical Upper Threshold	Верхнее пороговое значение, установленное для датчика, генерирующего критический аварийный сигнал.

Процедура

1. Выберите **Information** из главного меню и выберите **Sensor Info** из дерева навигации.

   На экране появится страница **Sensor Info**.

2. Просмотр информации датчика.

ПРИМЕЧАНИЕ

Для поиска информации датчика, введите ключевое слово в текстовой строке **Search**.

3.4 Аварийные сигналы и события системы

3.4.1 Текущие аварийные сигналы

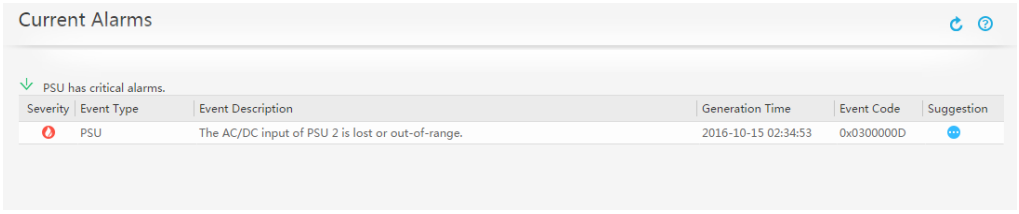
Описание функции

На странице **Current Alarms** приведена информация о всех активных аварийных сигналах, которые еще не устранены.

GUI

Выберите **Alarm & SEL** из главного меню и выберите **Current Alarms** из дерева навигации.

На экране появится страница **Current Alarms**.



Описание параметров

Табл. 3-22 Параметры из списка текущих аварийных сигналов

Параметр	Описание
Severity	Уровень серьезности аварийного сигнала. Значения: **Critical**, **Major** или **Minor** • : аварийные сигналы критического уровня свидетельствуют о наличии неисправности, в результате которой может произойти отключение сервера и прерывание работы всех системных служб. При появлении критических аварийных сигналов необходимо немедленно предпринять меры по локализации и устранению неисправностей. • : аварийные сигналы серьезного уровня свидетельствуют о неисправностях, которые оказывают значительное влияние на работу системы. Неисправность такого уровня может привести к системному сбою или прерыванию работы сервисов. • : незначительные аварийные сигналы свидетельствуют о наличии неисправностей, которые не оказывают особого влияния на работу системы. Однако необходимо как можно

Параметр	Описание
	скорее предпринять меры по их устранению, чтобы предотвратить более серьезную неисправность.
Object Type	Тип компонента, для которого генерируется аварийный сигнал.
Description	Дополнительная информация об аварийном сигнале.
Generated	Дата и время появления аварийного сигнала.
Event Code	Уникальный идентификатор аварийного сигнала.
Handling Suggestion	Инструкции по порядку устранения аварийного сигнала. Нажмите для просмотра инструкций.

Процедура

1. Выберите **Alarm & SEL** из главного меню и выберите **Current Alarms** из дерева навигации.

   На экране появится страница **Current Alarms**.
2. Просмотр аварийной информации.

   Для просмотра подробной информации по аварийному сигналу нажмите после типа события, а для закрытия этих данных нажмите .

3.4.2 События системы

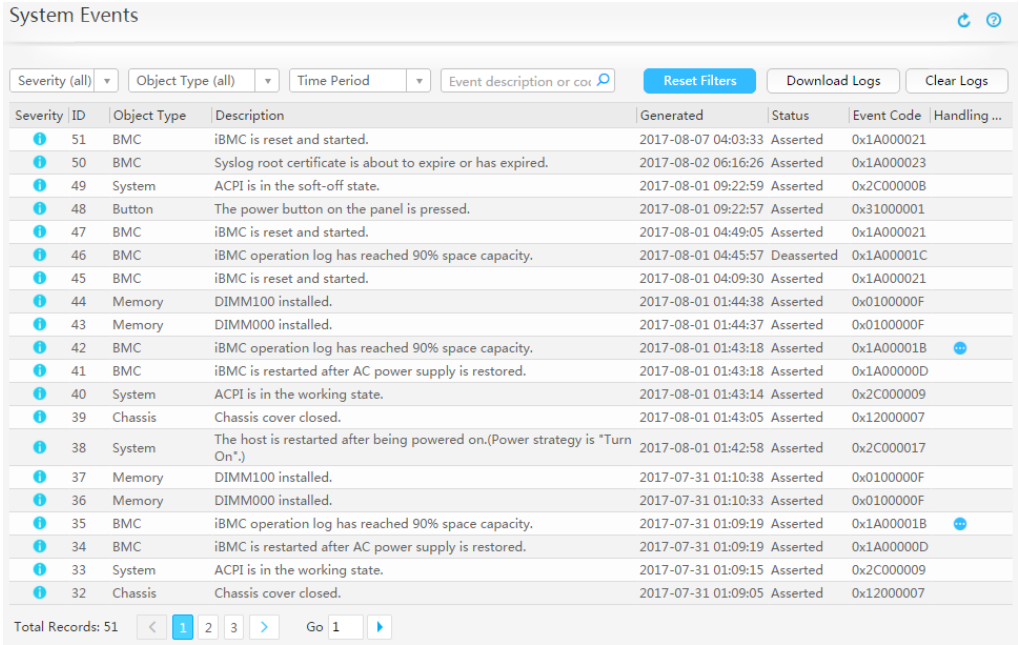
Описание функции

На странице **System Events** можно просматривать, загружать и удалять события системы.

GUI

Выберите **Alarm & SEL** из главного меню и выберите **System Events** из дерева навигации.

На экране появится страница **System Events**.



Описание параметра

Табл. 3-23 Параметры из списка событий системы

Параметр	Описание
Severity	Уровень серьезности события системы. Значения: **All**, **Critical**, **Major**, **Minor** или **Normal**
ID	Серийный номер события системы.
Object Type	Тип компонента, для которого сгенерировано событие системы.
Description	Дополнительная информация о событии системы.
Generated	Дата и время появления события системы.
Status	Статус события системы. Значения: **Asserted** или **Deasserted**
Event Code	Уникальный идентификатор события системы.
Handing Suggestion	Инструкции по порядку обработки события системы. Нажмите для просмотра инструкций.

Процедура

Поиск событий системы

1. Выберите **Alarm & SEL** из главного меню и выберите **System Events** из дерева навигации.

   На экране появится страница **System Events**.

2. Укажите критерии поиска.

   Подробная информация о параметрах приведена в Табл. 3-24.

Табл. 3-24 Описание критериев поиска

Параметр	Описание
Severity	Уровень серьезности события системы. Значения: **All**, **Critical**, **Major**, **Minor** или **Informational**
Object Type	Компонент, для которого сгенерировано событие системы. Значение: диапазон значений различается в зависимости от используемой модели сервера.
Time Period	Период времени, в течение которого были сгенерированы события системы. Значения: • **Today** • **Recent 7 days** • **Recent 30 days** • **Custom** **ПРИМЕЧАНИЕ** При выборе **Custom** необходимо указать начальную и конечную дату.
Event description or code	Описание или код события системы. Введите описание или код события и нажмите или нажмите **Enter**.

Удаление всех событий системы

ВНИМАНИЕ

Удаленные события системы нельзя восстановить. Будьте внимательны при удалении событий системы.

1. На странице **System Events** нажмите **Clear Logs**.

   На экране появится сообщение с вопросом о необходимости очистки журналов.
2. Нажмите **Yes**.

Загрузка событий системы

1. На странице **System Events** нажмите **Download Logs**.

   На экране появится диалоговое окно **Save**.
2. Укажите каталог для сохранения загруженного файла.
3. Нажмите **Save**.

   Загруженный файл будет сохранен в указанный каталог на локальном ПК.

3.4.3 Настройка аварийных сигналов

Описание функции

На странице **Alarm Settings** можно выполнить следующие настройки:

- Syslog-уведомления: отправка журналов на сторонний сервер через syslog-сообщения.
- Уведомления с оповещениями: отправка аварийных сигналов, событий и свойств оповещений на сторонний сервер через trap-сообщения.

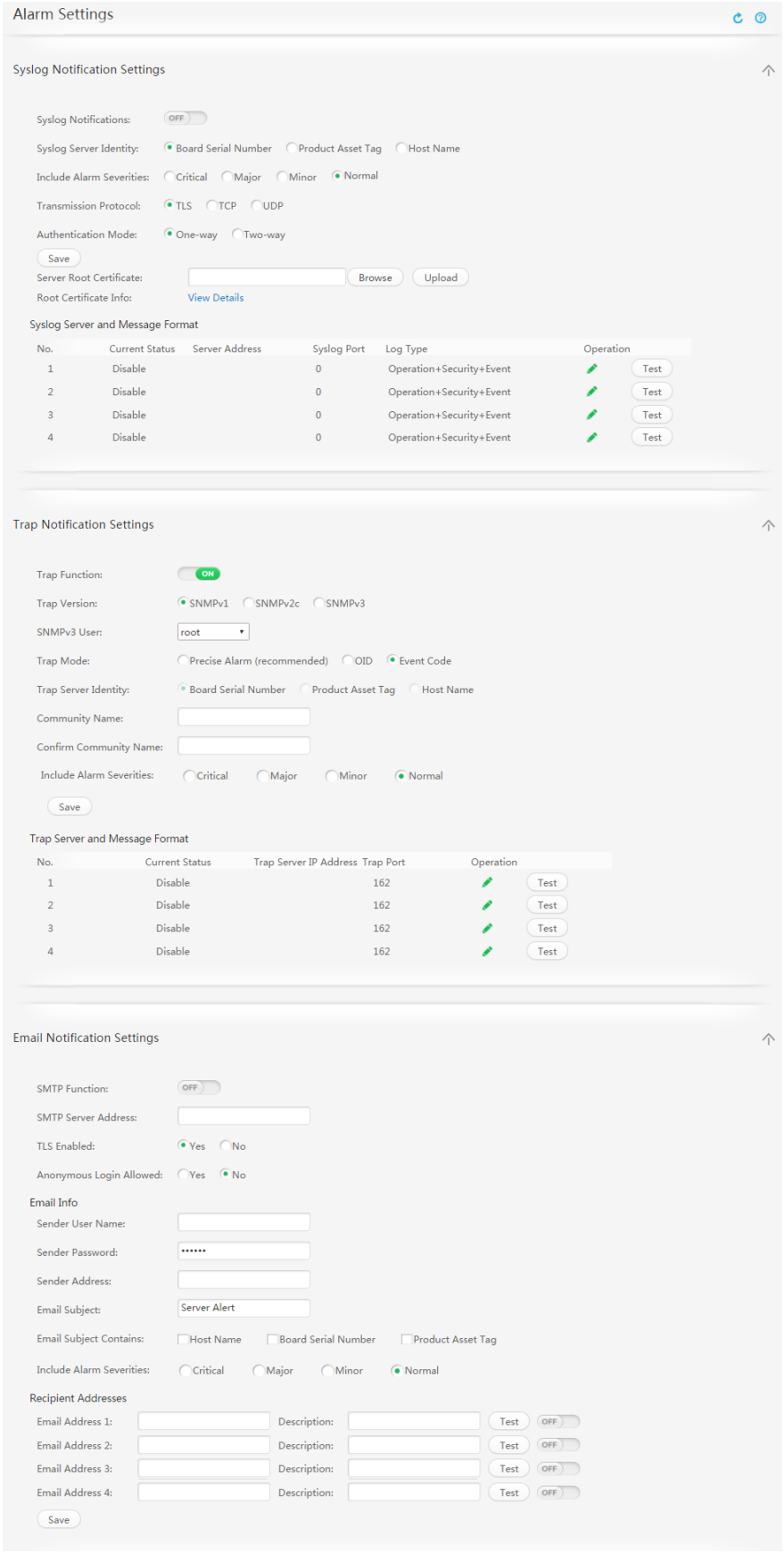
ПРИМЕЧАНИЕ

Оповещения – это сообщения, которые отправляет iBMC на сторонний сервер без явного запроса. Оповещения используются для сообщения о событиях, а также критических, серьезных и незначительных аварийных сигналах.

- Уведомления электронной почты: отправка сообщений электронной почты на указанные почтовые ящики через SMTP-сервер при возникновении аварийного сигнала.

GUI

В строке меню выберите **Alarm & SEL**. В дереве навигации выберите **Alarm Settings**. На экране появится страница **Alarm Settings**.



Описание параметра

Табл. 3-25 Область **Syslog Notification Settings**

Параметр	Описание
Syslog Notifications	Функция отправки уведомлений через syslog-сообщения. Нажмите  или  и нажмите **Save**. • Для включения данной функции установите для параметра значение  . • Для отключения данной функции установите для параметра значение  .
Syslog Server Identity	Источник отправки syslog-сообщений. Значения: • Серийный номер платы • Инвентарный номер продукта • Имя хоста
Include Alarm Severities	Уровни серьезности аварийных сигналов, отправляемых в syslog-сообщениях. Значения: • **Critical**: только критические аварийные сигналы. • **Major**: серьезные и критические аварийные сигналы. • **Minor**: незначительные, серьезные и критические аварийные сигналы. • **Normal**: события и незначительные, серьезные и критические аварийные сигналы.
Transmission Protocol	Протокол, используемый для передачи syslog-сообщений между iBMC и syslog-сервером. Значения: • **TLS**: протокол, ориентированный на соединение, который обеспечивает конфиденциальность и целостность передаваемых данных. • **TCP**: протокол, ориентированный на соединение, который отправляет данные только после установления надежного соединения между отправителем и получателем. • **UDP**: протокол без установления соединения, который отправляет данные без установления соединения между отправителем и получателем.
Authentication Mode	Режим аутентификации syslog-сертификатов. Данный параметр устанавливается только если **Transmission Protocol** имеет значение **TLS**. Значения: • **One-way**: аутентификация только сертификата syslog-сервера.

Параметр	Описание
	• **Two-way**: аутентификация сертификатов syslog-сервера и клиента.
Server Root Certificate	Сертификат, используемый для проверки сообщений, отправленных с syslog-сервера до установления соединения.
Root Certificate Info	Информация о загруженном корневом сертификате сервера. Информация о сертификате содержит следующее: • Орган, выдавший корневой сертификат. • Пользователь, которому был выдан корневой сертификат. • Срок действия корневого сертификата. • Серийный номер корневого сертификата.
Local Certificate	Сертификат, используемый для аутентификации клиента Syslog (iBMC) до установления соединения с Syslog-сервером. Перед установлением соединения iBMC отправляет пакет с информацией о локальном сертификате на Syslog-сервер. Установка соединения выполняется только после успешной аутентификации.
Certificate Password	Пароль, используемый для дешифровки сертификата клиента. Данный пароль создается вместе с сертификатом клиента, сгенерированным сервером сертификатов.
Local Certificate Info	Информация о сертификате клиента, который будет загружен. Информация о сертификате включает: орган, выдавший сертификат, пользователя, срок действия и серийный номер сертификата.
Syslog-сервер и формат сообщений	
No.	Канал для отправки сообщений системного журнала. Система поддерживает установку максимум четырех каналов.
Current Status	Текущий статус канала, который может быть включен или отключен.  означает что канал отключен, а  означает, что канал включен.
Server Address	Адрес syslog-сервера.
Syslog Port	Номер порта syslog-сервера.
Log Type	Типы журналов, которые содержатся в syslog-сообщении.
Test	Функция тестирования доступности syslog-канала. Нажмите **Test** для тестирования канала. Если на экране появится сообщение «Operation successful», то это говорит о том, что канал доступен.
Нажмите  . На экране появятся следующие параметры:	
Current Status	Текущий статус канала, который может быть включен или

Параметр	Описание
	отключен. Нажмите  или  и нажмите **Save**. • Для включения данной функции установите для параметра значение  . • Для отключения данной функции установите для параметра значение  .
Server Address	Адрес syslog-сервера. Значения: **IPv4 address**, **IPv6 address** или **domain name** **ПРИМЕЧАНИЕ** Если для параметра **Transmission** установлено значение **TLS**, то необходимо указать имя домена. Кроме того, в меню **Configuration** > **Network** необходимо правильно сконфигурировать информацию DNS.
Syslog Port	Номер порта syslog-сервера. Диапазон значений: От 1 до 65535
Log Type	Типы журналов, которые содержатся в syslog-сообщении. Значения: **All**, **Operation**, **Security** и **Event**

Табл. 3-26 Параметры из области **Trap Notification Settings**

Параметр	Описание
Trap Function	Функция отправки аварийных сообщений с сообщениях с оповещениями. • Для включения данной функции установите для параметра значение  . • Для отключения данной функции установите для параметра значение  .
Trap Version	Для отправки оповещений используются следующие версии SNMP. Значения: • **SNMPv1**: первая официальная версия SNMP, определенная в документе RFC 1157. • **SNMPv2c**: версия, в которую добавлена архитектура управления на уровне сообществ для SNMPv2. • **SNMPv3**: версия с поддержкой безопасности и удаленных конфигураций для SNMP. **ПРИМЕЧАНИЕ** • Для отправки оповещений рекомендуется использовать версию SNMPv3. При использовании SNMPv1 и SNMPv2c необходимо соблюдать осторожность, поскольку они несут определенные риски безопасности. • Подробная информация о порядке установки алгоритмов

Параметр	Описание
	аутентификации и шифрования для SNMPv3 приведена разделе 3.7.7 Страница System. Значение по умолчанию: **SNMPv1**
SNMPv3 User	Имя пользователя SNMPv3. Данный параметр устанавливается только если **Trap Version** имеет значение **SNMPv3.** Для серверов V3 установлено имя пользователя по умолчанию **root**, а для серверов V5 имя пользователя **Administrator.**
Trap Mode	Режим отправки оповещений. Значение: • **Precise Alarm (recommended)**: OID узла SNMP, который находится во взаимно-однозначном соответствии с событием, и используется как ID события оповещения. По сравнению с **OID** и **Event Code**, данный режим предоставляет более точную ифнормацию. • **OID**: OID узла SNMP, используемый в качестве ID события оповещения. • **Event Code**: код события, используемый в качестве ID события оповещения. Значение по умолчанию: Для серверов V3 по умолчанию установлено значение **Event Code**, а для серверов V5 значение **Precise Alarm (recommended).**
Trap Server Identity	Источник отправки сообщений с оповещениями. Значения: • Серийный номер платы • Инвентарный номер продукта • Имя хоста
Community Name	Строка с именем сообщества SNMP для аутентификации при использовании SNMPv1 или SNMPv2c. Диапазон значений различается в зависимости от того, включена ли проверка сложности пароля. • Если проверка сложности пароля отключена, то в качестве значения может использоваться строка длиной от 1 до 18 символов, состоящая из букв, цифр и специальных символов (за исключением пробелов). • Если проверка сложности пароля включена, то имя сообщества должно удовлетворять следующим требованиям: – Должно содержать от 8 до 18 символов – Содержать как минимум две опции из следующих: прописные буквы от A до Z, строчные буквы от a до z, цифры от 0 до 9 – Оно должно включать, как минимум, один из следующих специальных символов: `~!@#$%^&*()-_=+\\[{}];:'",<.>/? – По крайней мере два новых символа по сравнению с

Параметр	Описание
	предыдущим именем сообщества. – Не должно содержать пробелы. Значение по умолчанию: **TrapAdmin12#$**
Confirm Community Name	Имя сообщества для подтверждения.
Include Alarm Severities	Уровни серьезности аварийных сигналов, которые отправляются на сторонний сервер, в сообщениях с оповещением. Значения: • **Critical**: только критические аварийные сигналы. • **Major**: серьезные и критические аварийные сигналы. • **Minor**: незначительные, серьезные и критические аварийные сигналы. • **Normal**: события и незначительные, серьезные и критические аварийные сигналы.
Trap-сервер и формат сообщений	
No.	Trap-канал для отправки аварийных сигналов. Система поддерживает установку максимум четырех каналов.
Test	Функция тестирования доступности trap-канала. Нажмите **Test** для тестирования канала. Если на экране появится сообщение «Operation successful», то это говорит о том, что канал доступен.
Нажмите  . На экране появятся следующие параметры:	
Current State	Текущий статус trap-канала. Нажмите  или  и нажмите **Save**. • Для включения данной функции установите для параметра значение  . • Для отключения данной функции установите для параметра значение  .
Trap Server IP Address	Адрес сервера, который получает аварийные сигналы, отправленные в trap-сообщениях. В качестве адреса сервера может быть указан IPv4- или IPv6-адрес.
Trap Port	Номер порта, который получает аварийные сигналы, отправленные в trap-сообщениях. Диапазон значений: От 1 до 65535 Значение по умолчанию: **162** **ПРИМЕЧАНИЕ** Для установки номера trap-порта в значение по умолчанию **162**, нажмите **Restore Defaults**.

Параметр	Описание
Message Delimiter	Разделитель, который отделяет ключевые слова в trap-сообщениях. Например, «**;**».
Select Message Content	Содержание trap-сообщений.
Display Keyword in Message	Отображение указанных ключевых слов в trap-сообщении. **ПРИМЕЧАНИЕ** Пример будет приведен справа от флажка, в зависимости от выбранных параметров: **Message Delimiter**, **Select Message Content** или **Display Keyword in Message**.

Табл. 3-27 Параметры из области **Email Notification Settings**

Параметр	Описание
SMTP Function	Функция отправки уведомлений в сообщениях электронной почты через SMTP-сервер. Нажмите  или  и нажмите **Save**. • Для включения данной функции установите для параметра значение  . • Для отключения данной функции установите для параметра значение  .
SMTP Server Address	IPv4- или IPv6-адрес SMTP-сервера. **ПРИМЕЧАНИЕ** iBMC не поддерживает разрешение имени домена. Имя домена сервера SMTP не поддерживается в текстовом поле **SMTP Server Address**.
TLS Enabled	Функция включения безопасности транспортного уровня (TLS – Transport Layer Security) для передачи данных. Если TLS отключен, то данные передаются в виде обычного текста. **ПРИМЕЧАНИЕ** • По умолчанию SMTP-сервер поддерживает TLS. Рекомендуется включить функцию TLS для обеспечения безопасности. • После включения TLS в WebUI iBMC включите TLS и настройте аутентификацию личных данных на SMTP-сервере. SMTP-сервер сможет получать сообщения электронной почты только от iBMC только после включения TLS.
Anonymous Login Allowed	Функция, разрешающая анонимный вход в систему. Если данная функция включена, то SMTP-сервер передает аварийные сообщения по электронной почте без аутентификации имени пользователя и пароля. Если данная функция не включена, то SMTP-сервер передает аварийные сообщения по электронной почте только после ввода правильного имени пользователя и пароля. Имя пользователя и пароль должны быть установлены на

Параметр	Описание
	SMTP-сервере. **ПРИМЕЧАНИЕ** По умолчанию на SMTP-сервере не разрешен анонимный вход в систему. Для обеспечения безопасности, не используйте функцию анонимного входа в систему.
Email Info	
Sender User Name/Sender Password	Имя пользователя и пароль, используемые когда для параметра **Anonymous Login Allowed** установлено значение **No**. Имя пользователя и пароль должны совпадать с именем пользователя и паролем, установленными на SMTP-сервере. Диапазон значений: • User name (имя пользователя): строка, длиной от 1 до 64 символов, состоящая из букв, цифр и специальных символов. Данное поле не должно быть пустым. • Password (пароль): строка, длиной от 1 до 50 символов
Sender Address	Адрес электронной почты, с которого отправляются аварийные сигналы. Значение: строка, длиной до 255 символов Значение может содержать буквы, цифры и специальные символы.
Email Subject/Email Subject Contains	Тема сообщения электронной почты. Значение: строка, длиной от 0 до 255 символов, состоящая из букв, цифр и специальных символов. Введите тему в поле **Email Subject** и выберите ключевые слова, которые будут содержаться в теме электронного сообщения. Например при выборе **Host Name** и **Board serial number**, в теме электронного сообщения будет содержаться имя хоста и серийный номер платы.
Include Alarm Severities	Уровни серьезности аварийных сигналов, отправляемых через SMTP-сервер. Значение: • **Critical**: только критические аварийные сигналы. • **Major**: серьезные и критические аварийные сигналы. • **Minor**: незначительные, серьезные и критические аварийные сигналы. • **Normal**: события и незначительные, серьезные и критические аварийные сигналы.
Recipient Addresses	Адрес электронной почты получателя сообщений. Адреса должны быть установлены на SMTP-сервере. Значение: строка, длиной до 255 символов в формате ***xx@xxx.xx***. Значение может содержать буквы, цифры и специальные

Параметр	Описание
	символы.
Description	Дополнительная информация об адресах-получателях электронных сообщений. Значение: строка, длиной от 0 до 255 символов, состоящая из букв, цифр и специальных символов.
Test	Функция проверки успешности отправки сообщений электронной почты получателю.
Enable	Функция включения или отключения адресов электронной почты. Нажмите  или  и нажмите **Save**. • Для включения данной функции установите для параметра значение  . • Для отключения данной функции установите для параметра значение  .

Процедура

Настройка уведомлений системных журналов

1. Выберите **Alarm & SEL** из главного меню и выберите **System Events** из дерева навигации.

   На экране появится страница **Alarm Settings**.
2. Установите параметры уведомлений системных журналов.

   Подробная информация о параметрах приведена в Табл. 3-25.
3. Нажмите **Save**.

   Если на экране появится сообщение «Operation Successful», то это говорит о том, что уведомления системных журналов установлены успешно.

Настройка оповещений

1. Установите параметры оповещений.

   Подробная информация о параметрах приведена в Табл. 3-26.
2. Нажмите **Save**.

   Если на экране появится сообщение «Operation Successful», то это говорит о том, что оповещения установлены успешно.

Настройка уведомлений электронной почты

1. Установите параметры уведомлений электронной почты.

   Подробная информация о параметрах приведена в Табл. 3-27.
2. Нажмите **Save**.

   Если на экране появится сообщение «Operation Successful», то это говорит о том, что уведомления электронной почты установлены успешно.

3.5 Диагностика

3.5.1 Воспроизведение

Описание функции

На странице **Playback** можно выполнить следующие операции:

- Воспроизвдение видеофайла сервера, хранящегося на локальном ПК.
- Воспроизведение видео, которое было автоматически записано на сервере.
- Захват изображения во время воспроизведения видео.

ПРИМЕЧАНИЕ

- Видеофайл должен быть в формате *.rep.
- Функция записи видео включена по умолчанию. Выборка важной служебной информации во время записи видео.

В Табл. 3-28 приведено описание элементов управления в окне воспроизведения видео.

Табл. 3-28 Элементы управления в окне воспроизведения видео

Нажмите...	**Для...**
 Кнопка **Play**	Воспроизведение выбранного видео.
 Кнопка **Pause**	Приостановка воспроизведения выбранного видео.
 Кнопка **Fast Forward**	Быстрая перемотка видео с 1-, 2- или 4-кратным ускорением.
 Кнопка **Rewind**	Обратная перемотка видеофайла с 1-, 0,5- или 0,25-кратным ускорением.
 Кнопка **Full Screen**	Максимальное увеличение страницы управления воспроизведением видео. **ПРИМЕЧАНИЕ** При воспроизведении видео в полноэкранном режиме, нажмите правой кнопкой мыши на экране для открытия меню быстрого вызова.
 Кнопка **Open**	Откройте видеофайл *.rep, который хранится на локальном ПК.
 Кнопка **Cut Screen**	Захват изображения во время воспроизведения видео.
	Воспроизведение видеофайла с указанной точки. (ползунок показывает ход воспроизведения).

Нажмите...	Для...
Ползунок	
 Кнопка **Loop**	Функция воспроизведения по кругу. Данная функция доступна только для локальных видеофайлов.

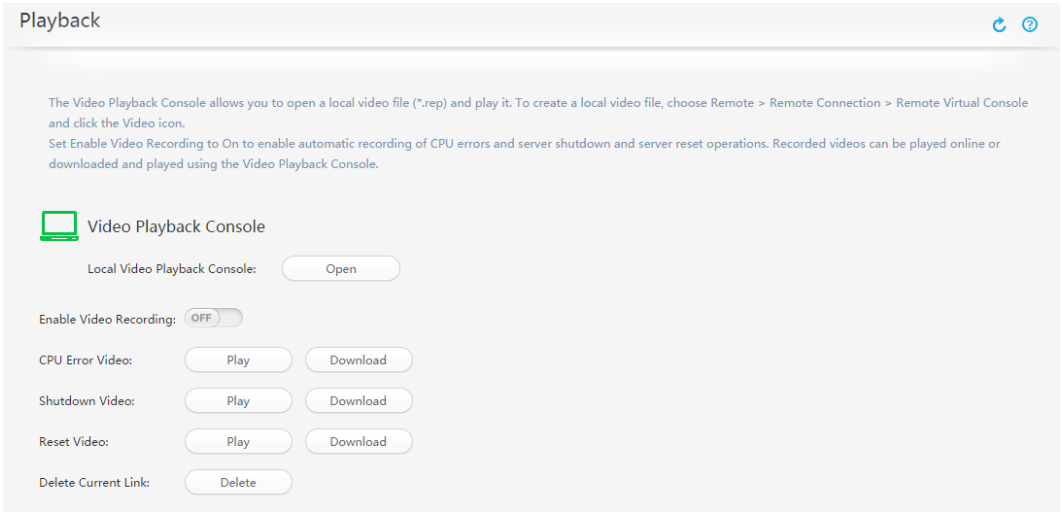
Функции записи и воспроизведения видео можно использовать для обслуживания и устранения неполадок сервера. Рис. 3-16 показана процедура использования функций записи и воспроизведения видео.

Рис. 3-16 Процедура использования функций записи и воспроизведения видео

GUI

Выберите **Diagnostics** из главного меню и выберите **Playback** из дерева навигации.

На экране появится страница **Playback**.



Процедура

Воспроизведение локального видео

1. На странице **Playback** нажмите **Open** после **Local Video Playback Console**.
   На экране появится окно **Video Player**.

   ПРИМЕЧАНИЕ

   Если перед открытием окна **Video Player**, на экране появится диалоговое окно с предупреждением о нарушении безопасности, то нажмите **Yes**.
2. В окне **Video Player** нажмите  .
   На экране появится диалоговое окно **Open**.
3. Выберите видеофайл, который хранится на локальном ПК и нажмите **Open**.
   Video Player начнет проигрывать видео.
   - Для быстрой перемотки видео с 1-, 2- или 4-кратным ускорением нажмите  .
   - Для обратной перемотки видео с 1-, 0,5- или 0,25-кратным ускорением нажмите  .
   - Для управления процессом воспроизведения видео перетащите  влево или вправо.
   - Для повтора воспроизведения видео нажмите  .
4. Нажмите **Open**.
   Video Player начнет проигрывать видео.

   ПРИМЕЧАНИЕ

   - Для быстрой перемотки видео с 1-, 2- или 4-кратным ускорением нажмите  .
   - Для обратной перемотки видео с 1-, 0,5- или 0,25-кратным ускорением нажмите  .
   - Для управления процессом воспроизведения видео перетащите  влево или вправо.
   - Для повтора воспроизведения видео нажмите  .
   - Для отображения окна **Video Player** в полноэкранном режиме нажмите  .

Отключение или включение функции записи видео

ПРИМЕЧАНИЕ

Функция записи видео включена по умолчанию. Во время записи видео может быть записана важная служебная информация.

Для включения функции записи видео, выполните следующие шаги:

1. Установите для параметра **Video Recording** значение  .
   На экране появится следующее сообщение:

   ```
   Are you sure you want to continue?
   ```
2. Нажмите **Yes**.

После включения функции записи видео, сервер будет продолжать автоматически записывать видео даже при условии, что:

- Сервер выключен или выполняется его перезагрузка.
- На экране появляется сообщение «CPU CAT ERROR».

Все видео хранятсяв папке **/tmp**.

ПРИМЕЧАНИЕ

Для отключения функции записи видео, установите для параметра **Video Recording** значение 

.

Воспроизведение или загрузка видео, которое было автоматически записано на сервере

- Для воспроизведения видео нажмите кнопку **Play**.
- Для загрузки видео нажмите кнопку **Download** и сохраните видео на локальный ПК.

Если видео воспроизводится другим лицом, то нажмите **Stop** после **Stop Other User's Video Playback** для остановки воспроизведения.

Захват изображения во время воспроизведения видео

1. Нажмите  во время воспроизведения видео.
   На экране появится диалоговое окно **Save As**.
2. Выберите локальный каталог для сохранения изображения и нажмите **Save**.
   Все изображения сохраняются в файлах в формате *.jpg в указанном каталоге.

3.5.2 Скриншот

Описание функции

На странице **Screenshot** можно выполнить следующие операции:

- Включить или отключить функцию последнего скриншота.
  Функция последнего скриншота позволяет автоматически выполнять скриншот экрана сервера перед его выключением или перезагрузкой.
- Скриншот рабочего стола сервера в режиме реального времени.

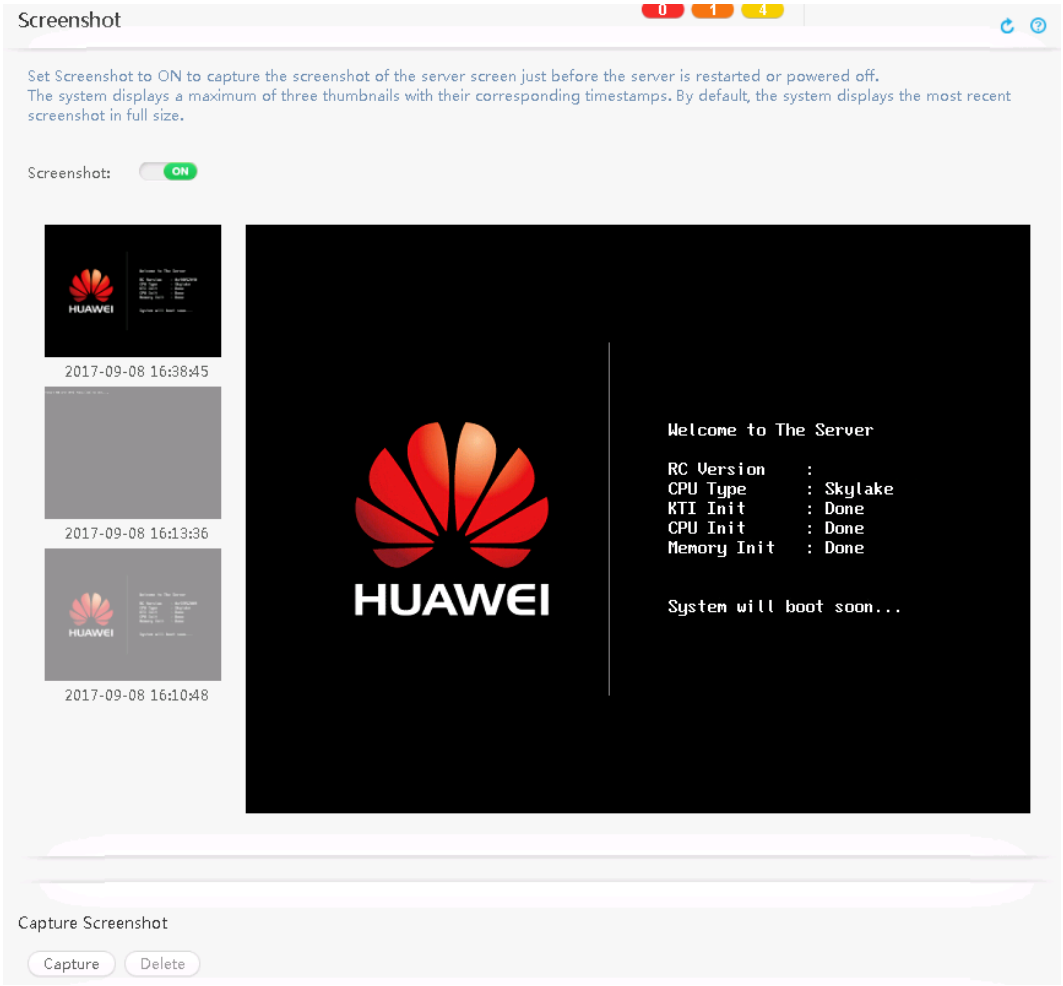
ПРИМЕЧАНИЕ

Функция выполнения последнего скриншота включена по умолчанию. При создании скриншота можно получить важную служебную информацию.

GUI

Выберите **Diagnostics** из главного меню и выберите **Screenshot** из дерева навигации.

На экране появится страница **Screenshot**.



Процедура

Отключение или включение функции последнего скриншота

1. Для включения функции последнего скриншота установите для параметра **Screenshot** кнопку ON. Для отключения функции последнего скриншота установите для параметра **Screenshot** OFF.
   На экране появится следующая информация:
   ```
   Are you sure you want to perform this operation?
   ```
2. Нажмите **Yes**.
   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Просмотр последнего скриншота

1. В строке меню выберите **Diagnostics**.
2. В дереве навигации выберите **Screenshot**.
   На экране появится страница **Screenshot**.
3. Просмотр скриншотов.

- Система выдает максимум три миниатюры с соответствующими отметками времени. По умолчанию, система отображает самые последние скриншоты в полном размере.
- Нажмите на миниатюру для увеличения изображения.

Создание скриншота

1. Нажмите кнопку **Capture** под **Capture Screenshot**.

   На экране появится скриншот рабочего стола сервера. В верхнем левом углу скриншота будет указано время его создания.

При создании нескольких скриншотов, на экране появится только последний скриншот и время его создания.

Удаление скриншота

1. Нажмите кнопку **Delete** под **Capture Screenshot**.

   На экране появится диалоговое окно с просьбой подтвердить ваши действия.
2. Нажмите **Yes**.

3.5.3 Черный ящик

Описание функции

На экране **Black Box** можно включить или отключить функцию черного ящика, а также выгрузить данные из памяти черного ящика.

Черный ящик состоит из памяти и ПО мониторинга неисправностей.

- Память представляет из себя встроенный чип памяти, на который записывается информация о сбоях, независимо от жестких дисков на сервере.

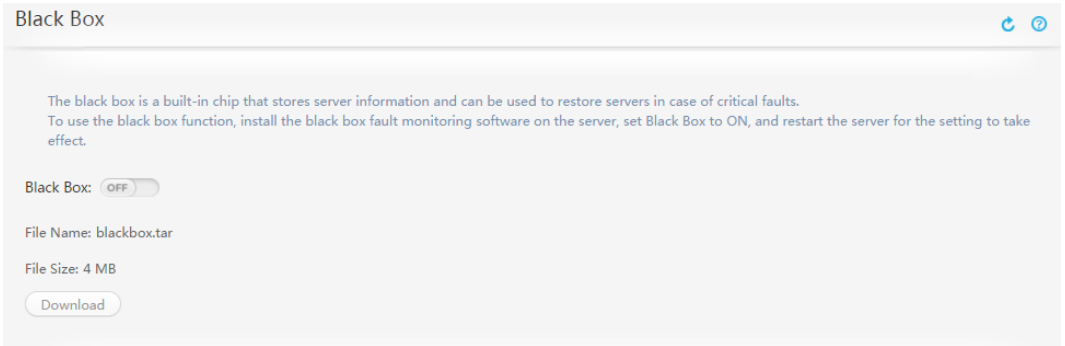
  В памяти объемом не более 4 МБ хранятся данные ядра при сбое ОС.
- ПО мониторинга неисправностей записывает данные ядра при сбое ОС.

  Перед использованием функции черного ящика убедитесь, что на сервере установлено ПО мониторинга неисправностей (например, iBMA). Подробная информация о порядке установки и использования iBMA приведена в документе *Руководство пользователя iBMA*.

GUI

Выберите **Diagnostics** из главного меню и выберите **Black Box** из дерева навигации.

На экране появится страница **Black Box**.



Описание параметра

Табл. 3-29 Параметры на странице **Black Box**

Параметр	Описание
Black Box	Функция черного ящика. Функция отключена по умолчанию. •  : функция черного ящика включена. •  : функция черного ящика отключена.
File Name	Файл данных сервера, записанный в памяти черного ящика.
File Size	Размер файла данных сервера, записанный в памяти черного ящика.

Процедура

Включение функции черного ящика

ПРИМЕЧАНИЕ

После включения или отключения функции черного ящика необходимо выполнить перезагрузку сервера, чтобы настройки вступили в силу.

1. В строке меню выберите **Diagnostics**.
2. В дереве навигации выберите **Black Box**.

   На экране появится страница **Black Box**.
3. Установите для параметра **Black Box** значение  .
4. Перезагрузите сервер.

Отключение функции черного ящика

1. Установите для параметра **Black Box** значение  .
2. Перезагрузите сервер.

Выгрузка данных из черного ящика

ПРИМЕЧАНИЕ

Убедитесь, что функция черного ящика включена.

1. В Internet Explorer выберите **Tools** > **Internet Options**.

   На экране появится страница **Internet Options**.
2. Перейдите на вкладку **Security** выберите из списка **Internet**, нажмите **Custom Level** и выберите **Enable** для **Automatic prompting for file downloads** под **Download**.
3. В WebUI iBMC выберите **Diagnostics** > **Black Box**.
4. Нажмите **Download**.

   На экране появится диалоговое окно **Save**.
5. Выберите локальный каталог для сохранения файла.
6. Нажмите **Save**.

Загруженный файл с данными черного ящика будет сохранен в указанный каталог на локальном ПК.

ПРИМЕЧАНИЕ

iBMC загружает только файл данных черного ящика с сервера на локальный ПК, но не анализирует этот файл. Подробная информация о процедуре анализа файла данных черного ящика приведена в руководстве по установке сервера.

3.5.4 Данные последовательного порта

Описание функции

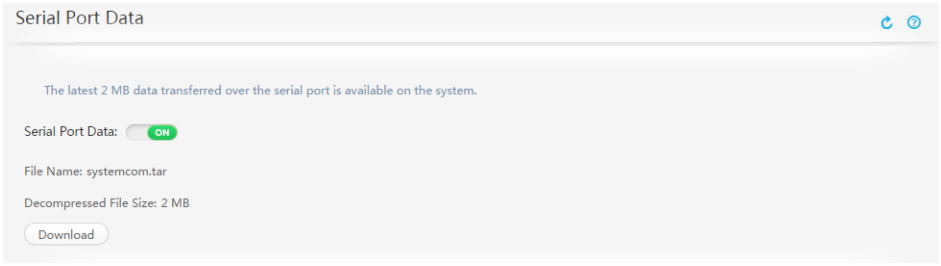
На странице **Serial Port Data** можно включить или отключить функцию для сохранения записанных данных, переданных по последовательному порту, и загрузить последние 2 МБ данных.

Функция сохранения данных, передаваемых по последовательному порту, включена по умолчанию.

GUI

Выберите **Diagnostics** из главного меню и выберите **Serial Port Data** из дерева навигации.

На экране появится страница **Serial Port Data**.



Процедура

1. В строке меню Internet Explorer выберите **Tools** > **Internet Options**.

   На экране появится страница **Internet Options**.
2. Перейдите на вкладку **Security**, выберите из списка **Internet** и нажмите **Custom level**. В появившемся диалоговом окне нажмите на кнопку **Enable** для **Automatic prompting for file downloads** под **Downloads**.
3. В WebUI iBMC из главного меню выберите **Diagnostics**.
4. В дереве навигации выберите **Serial Port Data**.

   На экране появится страница **Serial Port Data**.
5. Установите для параметра **Serial Port Data** значение 

.
6. Нажмите **Download**.

   На экране появится диалоговое окно **Save**.
7. Выберите локальный каталог для сохранения загруженного файла.
8. Нажмите **Save**.

   Загруженный файл будет сохранен в указанный каталог на локальном ПК.

3.5.5 Журналы диагностики неисправностей

Описание функции

На странице **Fault Diagnosis Logs** можно выполнить загрузку отчетов об ошибках, выдаваемых ЦП.

Функция выполнения диагностики неисправностей включена по умолчанию. Для включения или отключения данной функции настройте **FDM** в BIOS.

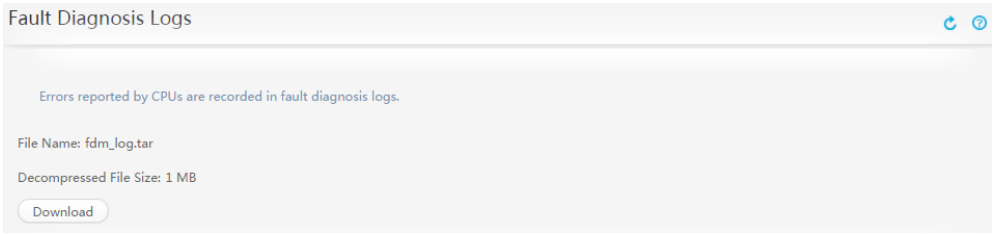
Путь к параметрам **FDM** зависит от платформы BIOS:

- Romley BIOS: **Advanced** > **RAS Configuration** > **FDM**
- Brickland BIOS: **Advanced** > **Runtime Error Logging** > **FDM**
- Grantley BIOS: **Advanced** > **System Event Log** > **FDM**
- Purley BIOS: **Advanced** > **System Event Log** > **FDM**

GUI

Выберите **Diagnostics** из главного меню и выберите **Fault Diagnosis Logs** из дерева навигации.

На экране появится страница **Fault Diagnosis Logs**.



Процедура

1. В строке меню Internet Explorer выберите **Tools** > **Internet Options**.

   На экране появится страница **Internet Options**.
2. Перейдите на вкладку **Security**, выберите из списка **Internet** и нажмите **Custom level**. В появившемся диалоговом окне нажмите на кнопку **Enable** для **Automatic prompting for file downloads** под **Downloads**.
3. В WebUI iBMC из главного меню выберите **Diagnostics**.
4. В дереве навигации выберите **Fault Diagnosis Logs**.

   На экране появится страница **Fault Diagnosis Logs**.
5. Нажмите **Download**.

   На экране появится диалоговое окно **Save**.
6. Выберите локальный каталог для сохранения загруженного файла.
7. Нажмите **Save**.

   Загруженный файл будет сохранен в указанный каталог на локальном ПК.

3.5.6 Память с возможностью замены в «горячем» режиме (только для RH8100 V3)

Описание функции

На вкладке **Memory Hot-Swap** можно выполнить «горячую» замену двухрядных модулей памяти (DIMM) и контролировать процесс «горячей» замены.

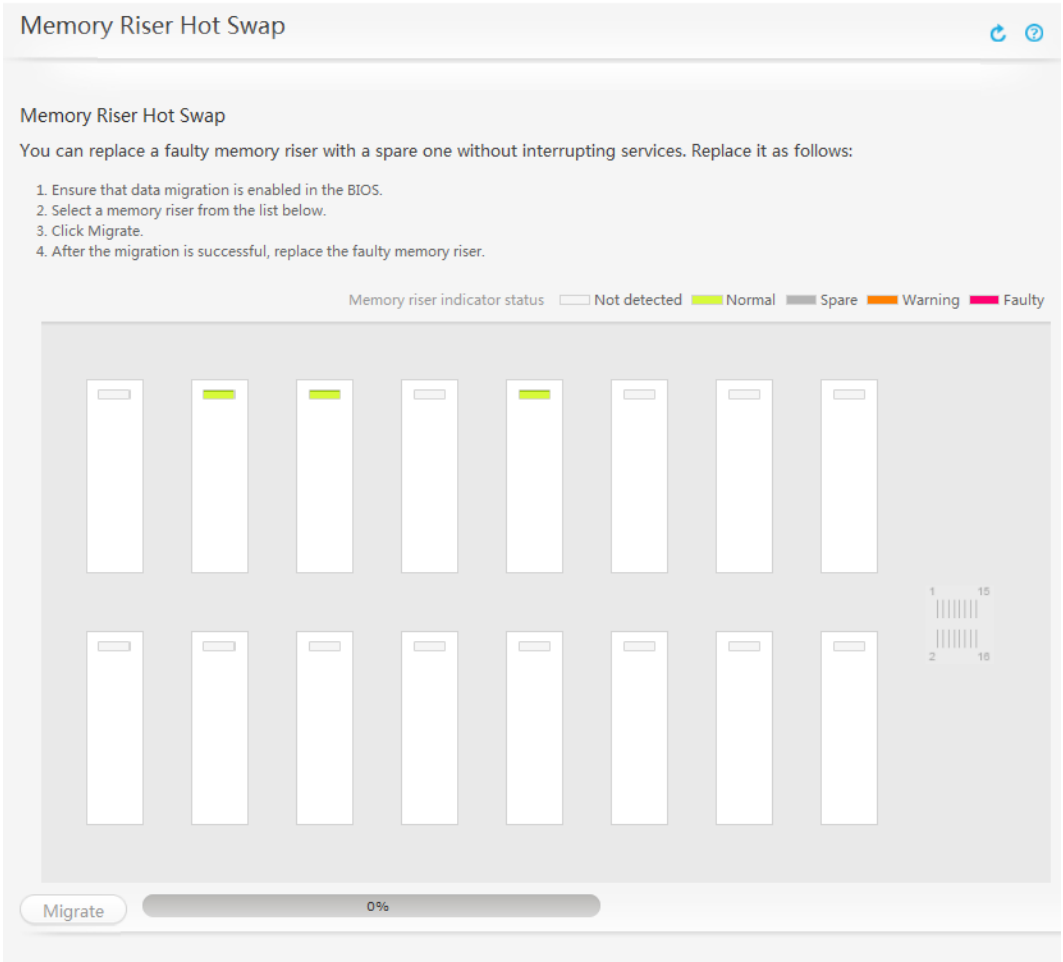
ПРИМЕЧАНИЕ

Вкладка **Memory Hot-Swap** недоступна для сервера RH8100 V3, в котором используются процессоры Broadwell.

GUI

Выберите **Diagnostics** из главного меню и выберите **Memory Hot-swap** из дерева навигации.

На экране появится страница **Memory Riser Hot Swap**.



Процедура

1. В строке меню выберите **Diagnostics**.
2. В дереве навигации выберите **Memory Hot-Swap**.

На экране появится страница **Memory Riser Hot Swap**.

3. Выберите дорожку памяти зеленого или оранжевого цвета.
4. Нажмите **Migrate**.

   Система запускает процесс миграции, а индикатор выполнения отображает ход миграции.

3.6 Питание

3.6.1 Управление питанием

Описание функции

На странице **Power Control** можно выполнить следующие операции:

- Включение питания, отключение питания или перезагрузка ОС сервера, а также запуск ОС для создания немаскируемого прерывания (NMI).
- Установите политику восстановления питания для ОС сервера.

NMI – это специальное прерывание, которое не может быть замаскировано, с использованием стандартной технологии маскирования прерываний. NMI генерируется, как правило, при появлении невосстанавливаемой аппаратной ошибки. Некоторые NMI могут быть замаскированы с использованием специальных методов.

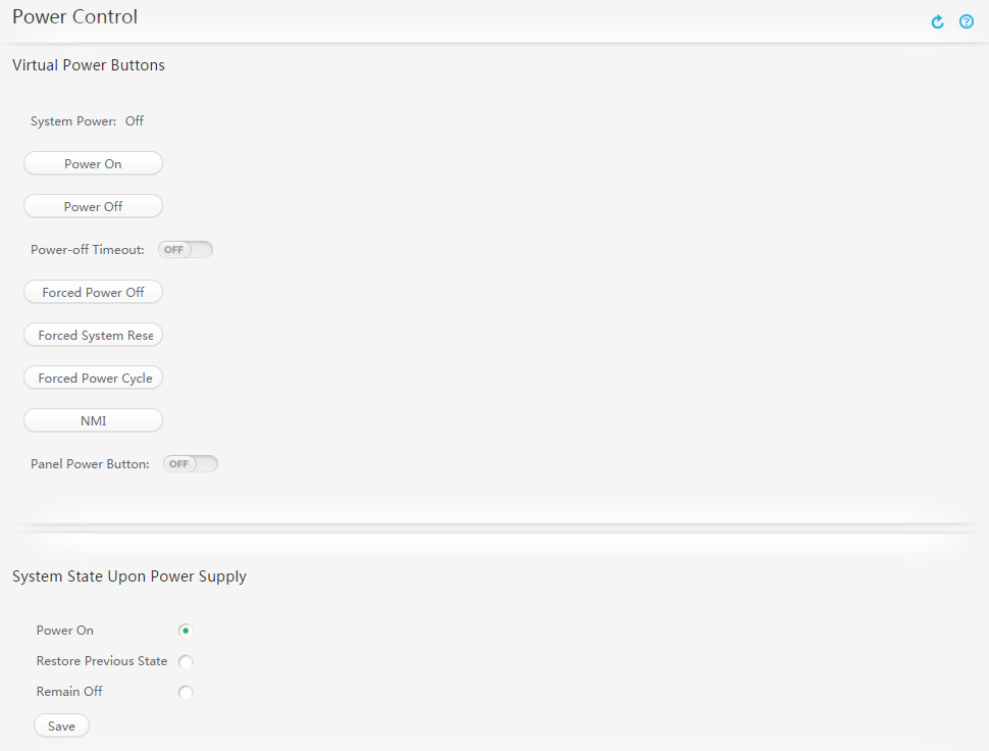
ВНИМАНИЕ

Перед выполнением контроля питания на сервере убедитесь, что данная операция не оказывает никакого влияния на сервисы.

GUI

Выберите **Power** из главного меню и выберите **Power Control** из дерева навигации.

На экране появится страница **Power Control**.



Описание элементов страницы

Табл. 3-30 Элементы из области **Virtual Power Buttons**

Элемент	Описание
System Power	Текущий статус ОС сервера.
Power On	Запуск ОС сервера.
Power Off	Выключение ОС сервера.
Power-off Timeout	iBMC работает в соответствии с настройками функции **Power-off Timeout** после нажатия кнопки **Power Off** для выключения ОС сервера. • Если функция **Power-off Timeout** включена, то iBMC принудительно выключает ОС, когда выключение ОС не происходит в течение вказанного периода времени. • Если опция **Power-off Timeout** отключена, то iBMC никак не мешает процессу выключения ОС. Диапазон значений и значение по умолчанию **Timeout Period** различаются в зависимости от используемой модели сервера. Подробная информация приведена в WebUI. • Для включения функции задержки при отключении питания, установите для данного параметра  . Нажмите  , введите значение в текстовом поле и нажмите **Save**. • Для отключения функции задержки при отключении питания, установите для данного параметра значение

Элемент	Описание
	 .
Forced Power Off	**ВНИМАНИЕ** Принудительное выключение может привести к потере или повреждению данных. В течение 6 секунд после нажатия данной кнопки будеьт выполнено принудительное отключение питания ОС сервера.
Forced System Reset	**ВНИМАНИЕ** Принудительная перезагрузка может привести к повреждению пользовательских программ или к тому, что данные не будут сохранены. Resets the server OS. **ПРИМЕЧАНИЕ** • Параметр **Forced System Reset** не работает, если уже произошло выключение ОС. • Данная операция влияет на выполняемую операцию отключения питания.
Forced Power Cycle	**ВНИМАНИЕ** Принудительное питание может привести к повреждению или потере данных. Принудительное выключение ОС сервера и повторный запуск ОС примерно через 6 секунд.
NMI	Запуск немаскируемого прерывания (NMI). Нажмите данную кнопку для запуска NMI только в том случае, если ОС не работает исправно. Не нажимайте данную кнопку, если ОС работает исправно. **ВНИМАНИЕ** Нажимайте данную кнопку только для внутреннего процесса ввода в действие. Прежде чем нажать данную кнопку, убедитесь, что ОС поддерживает программу обработки прерываний. В противном случае может произойти сбой ОС.
Panel Power Button	Отключение кнопки питания на панели сервера. Нажмите  или  и нажмите **Save**. При установке для данного параметра  , кнопка питания на панели сервера не будет работать.

Табл. 3-31 Опции из области **System State Upon Power Supply**

Опция	Описание
Power On	Автоматический запуск ОС после восстановления подачи питания.
Restore Previous State	Возврат ОС к предыдущему состоянию перед сбоем питания. • Если ОС сервера была запущена перед сбоем питания, ОС сервера будет запущена автоматически после

Опция	Описание
	восстановления подачи питания. • Если ОС сервера была выключена перед сбоем питания, то ОС сервера также будет выключена и после восстановления подачи питания.
Remain Off	ОС сервера будет выключена даже после восстановления подачи питания.

Процедура

Табл. 3-32 Операции управления питанием

Операция	Процедура
Запуск ОС сервера.	1. На странице **Power Control** нажмите на кнопку **Power On** под **Virtual Power Buttons**. На экране появится следующее сообщение: `Are you sure you want to perform this operation?` 2. Нажмите **Yes**. Время запуска ОС различается в зависимости от конфигурации сервера. Запуск ОС выполнен успешно, если на экране появится сообщение «Operation successful». После запуска ОС значение параметра **System Power** изменится на **On**.
Выключение ОС сервера.	1. На странице **Power Control** нажмите на кнопку **Power Off** под **Virtual Power Buttons**. На экране появится следующее сообщение: `Are you sure you want to perform this operation?` 2. Нажмите **Yes**. Выключение ОС выполнено успешно, если на экране появится сообщение «Operation successful». После выключения ОС значение параметра **System Power** изменится на **Off**.
Принудительное выключение ОС сервера.	1. На странице **Power Control** нажмите на кнопку **Forced Power Off** под **Virtual Power Buttons**. На экране появится следующее сообщение: `Are you sure you want to perform this operation?` 2. Нажмите **Yes**. Принудительное выключение ОС выполнено успешно, если на экране появится сообщение «Operation successful». После принудительного выключения ОС значение параметра **System Power** изменится на **Off**.
Принудительная перезагрузка ОС	1. На странице **Power Control** нажмите на кнопку **Forced System Reset** под **Virtual Power Buttons**.

Операция	Процедура
сервера.	На экране появится следующее сообщение: `Are you sure you want to perform this operation?` 2. Нажмите **Yes**. Принудительная перезагрузка ОС сервера выполнена успешно, если на экране появится сообщение «Operation successful».
Цикл включения и отключения питания ОС сервера.	1. На странице **Power Control** нажмите на кнопку **Forced Power Cycle** под **Virtual Power Buttons**. На экране появится следующее сообщение: `Are you sure you want to perform this operation?` 2. Нажмите **Yes**. Время, необходимое на выполнение данной операции, различается в зависимости от конфигурации сервера. Выключение ОС с последующим запуском выполнено успешно, если на экране появится сообщение «Operation successful». Во время данного процесса значение параметра **System Power** изменится сначала с **On** на **Off** и затем снова станет **On**.
Запуск NMI	**ВНИМАНИЕ** Выполняйте данную операцию только в том случае, если ОС не работает исправно. Прежде чем нажать данную кнопку, убедитесь, что ОС поддерживает программу обработки прерываний. В противном случае может произойти сбой ОС. 1. На странице **Power Control** нажмите на вкладку **NMI** под **Virtual Power Buttons**. На экране появится следующее сообщение: `Generating an NMI may cause data corruption or data loss. Are you sure you want to continue?` 2. Нажмите **Yes**. Время, необходимое на выполнение данной операции, различается в зависимости от конфигурации сервера. Запуск NMI выполнен успешно, если на экране появится сообщение «Operation successful».
Установка политики восстановления подачи питания.	1. На вкладке **Power Control** выберите политику восстановления подачи питания под **System State Upon Power Supply**. Подробная информация приведена в Табл. 3-31. 2. Нажмите **Save**. Настройка выполнена успешно, если на экране появится сообщение «Operation successful».
Установка периода ожидания отключения питания.	1. На странице **Power Control** для параметра **Power-off Timeout** должно быть установлено значение  . 2. Нажмите  и введите значение в текстовом поле.

Операция	Процедура
	Нажмите  для просмотра диапазона значений. Диапазон значений различается в зависимости от используемой модели сервера. Значение по умолчанию – **600**. 3. Нажмите **Save**. Настройка выполнена успешно, если на экране появится сообщение «Operation successful».
Проверка периода ожидания отключения питания.	На странице **Power Control** проверьте значение параметра **Timeout Period (s)** после **Power-off Timeout** из области **Virtual Power Buttons**.

3.6.2 Ограничение питания

Описание функции

На странице **Power Capping** можно выполнить следующие операции:

- Просмотр информации о питании сервера.
- Включение или отключение функции ограничения питания, установка значения ограничения питания, а также указание действий, которые необходимо предпринять при сбое ограничения питания.
- Просмотр графиков среднего значения питания и пикового значения питания за прошлую неделю или день, просмотр данных питания, полученных в каждый период выборки, и повторно собранных статистических данных питания.

  Система получает данные питания сервера каждые 10 минут.

ВНИМАНИЕ

- Соблюдайте осторожность при установке значения ограничения питания. Небольшое значение ограничения питания может повлиять на производительность и операции системы.
- Если для параметра **Forced Shutdown After Power Capping Failure** установлено 

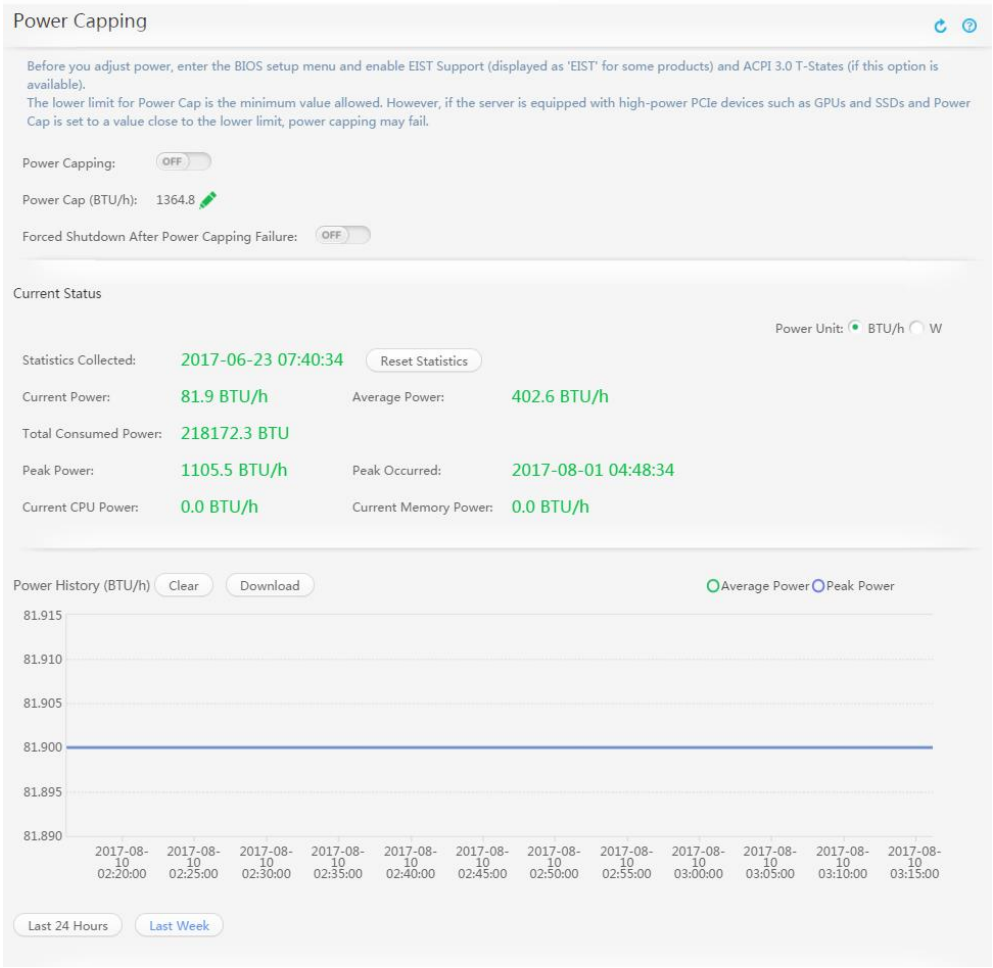
, то это может повлиять на сервисы (серверы RH5885 V3, RH5885H V3 и RH8100 V3 не поддерживают функцию принудительного выключения при сбое ограничения питания).
- Функция **Power Capping** недоступна для iBMC системы B, если RH8100 V3 работает в двухсистемном режиме.

GUI

Выберите **Power** из главного меню и выберите **Power Capping** из дерева навигации.

На экране появится страница **Power Capping**.

Рис. 3-17 Страница **Power Capping**



Параметры

Табл. 3-33 Параметры из области **Power Capping**

Параметр	Описание
Power Capping	Включение или отключение функции ограничения питания. **ПРИМЕЧАНИЕ** Перед настройкой функции ограничения питания в BIOS должны быть установлены следующие параметры: • Для параметров **EIST Support** или **EIST** должно быть установлено значение **Enabled**. • Для параметров **ACPI 3.0 T-States** или **ACPI T-States** (если таковые имеются) должно быть установлено значение **Enabled**. Функция ограничения питания недоступна для сервера RH8100 V3, работающего в двухсистемном режиме. Статистика потребления питания всего сервера RH8100 V3 отображается

Параметр	Описание
	независимо от того, работает ли сервер RH8100 V3 в односистемном или двухсистемном режиме. Нажмите  или  и нажмите **Save**. • Для включения данной функции установите для параметра  . • Для отключения данной функции установите для параметра  .
Power Cap (BTU/h)	Максимальное энергопотребление работающего сервера. Данный параметр недоступен для сервера RH8100 V3, работающего в двухсистемном режиме. Нажмите  для просмотра диапазона значений. Диапазон значений различается в зависимости от используемой модели сервера. Значение ограничения питания не может быть ниже нижнего рекомендованного значения.
Forced Shutdown After Power Capping Failure (серверы RH5885 V3, RH5885H V3 и RH8100 V3 не поддерживают данную функцию)	Функция автоматического выключения системы через 15 секунд после отключения питания. Нажмите  или  и нажмите **Save**. Установите для данного параметра значение  для автоматического выключения системы через 15 секунд после отключения питания.

Табл. 3-34 Параметры из области **Current Status**

Параметр	Описание
Power Unit	Выбор единицы измерения питания, например: **W** или **BTU/h**. **ПРИМЕЧАНИЕ** 1 BTU/h = 0,293 W
Statistics Collected	Время начала сбора статистических данных питания.
Current Power	Текущее питание сервера.
Average Power	Данные средней мощности, собранные с момента включения сервера или с момента последнего старта сбора статистики.
Total Consumed Power	Данные общей потребляемой мощности, собранные с момента включения сервера или с момента последнего старта сбора статистики.
Peak Power	Данные максимальной потребляемой мощности, собранные с момента включения сервера или с момента последнего старта сбора статистики.

Параметр	Описание
Peak Occurred	Время появления пикового значения мощности с момента включения сервера или с момента последнего старта сбора статистики.
Current CPU Power	Текущее энергопотребление ЦП сервера.
Current Memory Power	Текущее энергопотребление памяти сервера.

Табл. 3-35 Параметры из области **Power History**

Параметр	Описание
Линейный график потребляемой мощности	
Average power	Значения пиковой мощности, собранные за последнюю неделю, день или период от последнего старта сбора статистики до 10 минут назад.
Peak power	Значения средней мощности, собранные за последнюю неделю, день или период от последнего старта сбора статистики до 10 минут назад.

Процедура

Просмотр питания сервера

1. В строке меню выберите **Power**.
2. В дереве навигации выберите **Power Capping**.
   На экране появится страница **Power Capping**.
3. В области **Current State** будут показаны данные питания сервера.

Повторный сбор статистики питания сервера

1. Нажмите **Reset Statistics**.
   На экране появится следующая информация:

   ```
   If you perform this operation, the system will delete the original power statistics and recollect power statistics (the system will also recollect power saving statistics on the Information Summary page). Are you sure you want to perform this operation?
   ```

2. Нажмите **Yes**.
   После этого система удалит архивные статистические данные питания сервера.

Установка ограничения питания

1. Нажмите 

после **Power Capping**.
   На экране появится следующая информация:

```
Are you sure you want to enable or disable power capping?
```

2. Нажмите **Yes**.

   Функция ограничения питания включена, если на экране появится «Operation Successful» и 

изменится на 

.

3. Нажмите  и введите значение в текстовом поле **Power Cap**.

   Указанное значение должно находиться в пределах диапазона значений, который указан после текстового поля.

4. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Отключение функции ограничения питания

1. Нажмите 

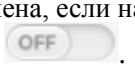
после **Power Capping**.

   На экране отобразится следующая информация:

```
Are you sure you want to enable or disable power capping?
```

2. Нажмите **Yes**.

   Функция ограничения питания отключена, если на экране появится «Operation Successful» и 

изменится на 

.

Включение принудительного отключения после сбоя питания

1. Нажмите 

после **Forced Shutdown After Power Capping Failure**.

   На экране появится следующая информация:

```
Are you sure you want to change the policy used in the event of power capping failure?
```

2. Нажмите **Yes**.

   Если на экране появится сообщение «Operation Successful» и значение 

изменится на 

, то произойдет принудительное отключение питания сервера по истечении 15 секунд после сбоя питания.

Удаление архивных статистических данных питания

1. Нажмите **Reset Statistics**.

   На экране появится следующая информация:

```
Reset History Power Data?
```

2. Нажмите **Yes**.

   Система удалит архивные статистические данные о питании сервера и незамедлительно собирает статистику питания сервера.

Загрузка архивных статистических данных питания

1. Нажмите **Download**.

   На экране появится диалоговое окно **Save**.

2. Выберите локальный каталог для сохранения файла с архивными данными питания.

3. Нажмите **Save**.

Загруженный файл с архивными данными питания будет сохранен в указанный каталог на локальном ПК.

Просмотр архивных данных питания за последнюю неделю

1. В области **Power History** нажмите **Last week**.

   На экране появятся статистические данные пиковой и средней мощности за последнюю неделю. Если период от последнего времени начала сбора статистики до текущего времени составляет менее одной недели, то на экране появятся только статистические данные мощности, созданные с момента начала последнего сбора статистики .

Просмотр архивных данных питания за последний день

В области **Power History** нажмите **Last day**.

На экране появятся статистические данные пиковой и средней мощности за последний день.

3.6.3 Настройки энергосбережения

Описание функции

На странице **Energy Saving Settings** можно настроить P-состояния (рабочую частоту ЦП) и T-состояния (рабочий цикл ЦП) для сокращения энергопотребления.

ВНИМАНИЕ

Настройки энергосбережения могут повлиять на производительность системы. Соблюдайте осторожность при конфигурировании параметров энергосбережения.

Перед настройкой функции ограничения питания в BIOS должны быть установлены следующие параметры:

- Для параметров **EIST Support** или **EIST** должно быть установлено значение **Enabled**.
- Для параметров **ACPI 3.0 T-States** или **ACPI T-States** (если таковые имеются) должно быть установлено значение **Enabled**.

GUI

Выберите **Power** из главного меню и выберите **Energy Saving Settings** из дерева навигации.

На экране появится страница **Energy Saving Settings**.

Область **Energy Saving Settings** состоит из двух разделов: **Power Adjustment** и **PSU settings**.

Рис. 3-18 Страница **Energy Saving Settings** RH8100 V3

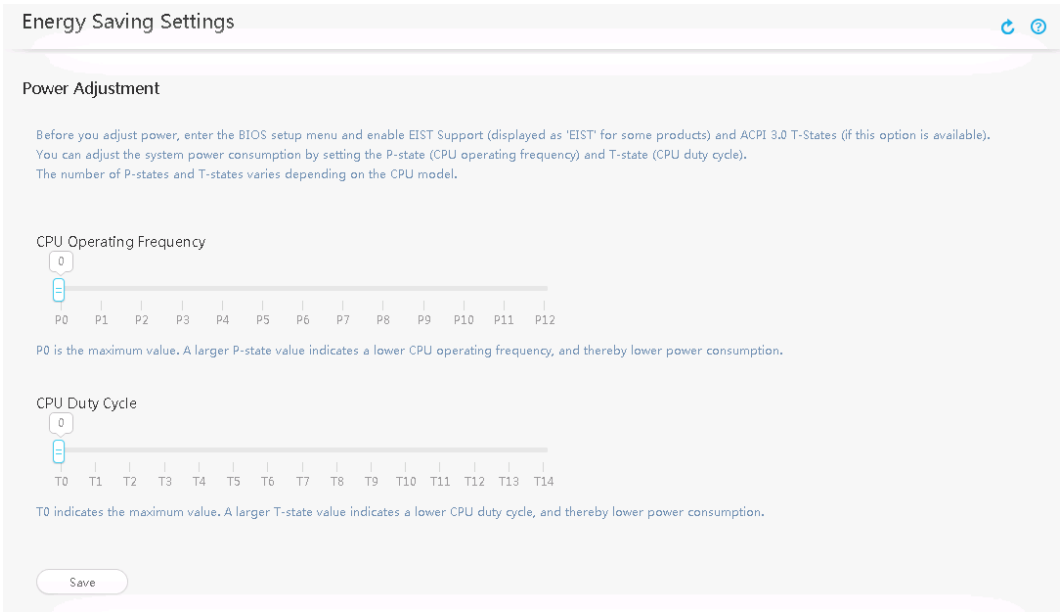
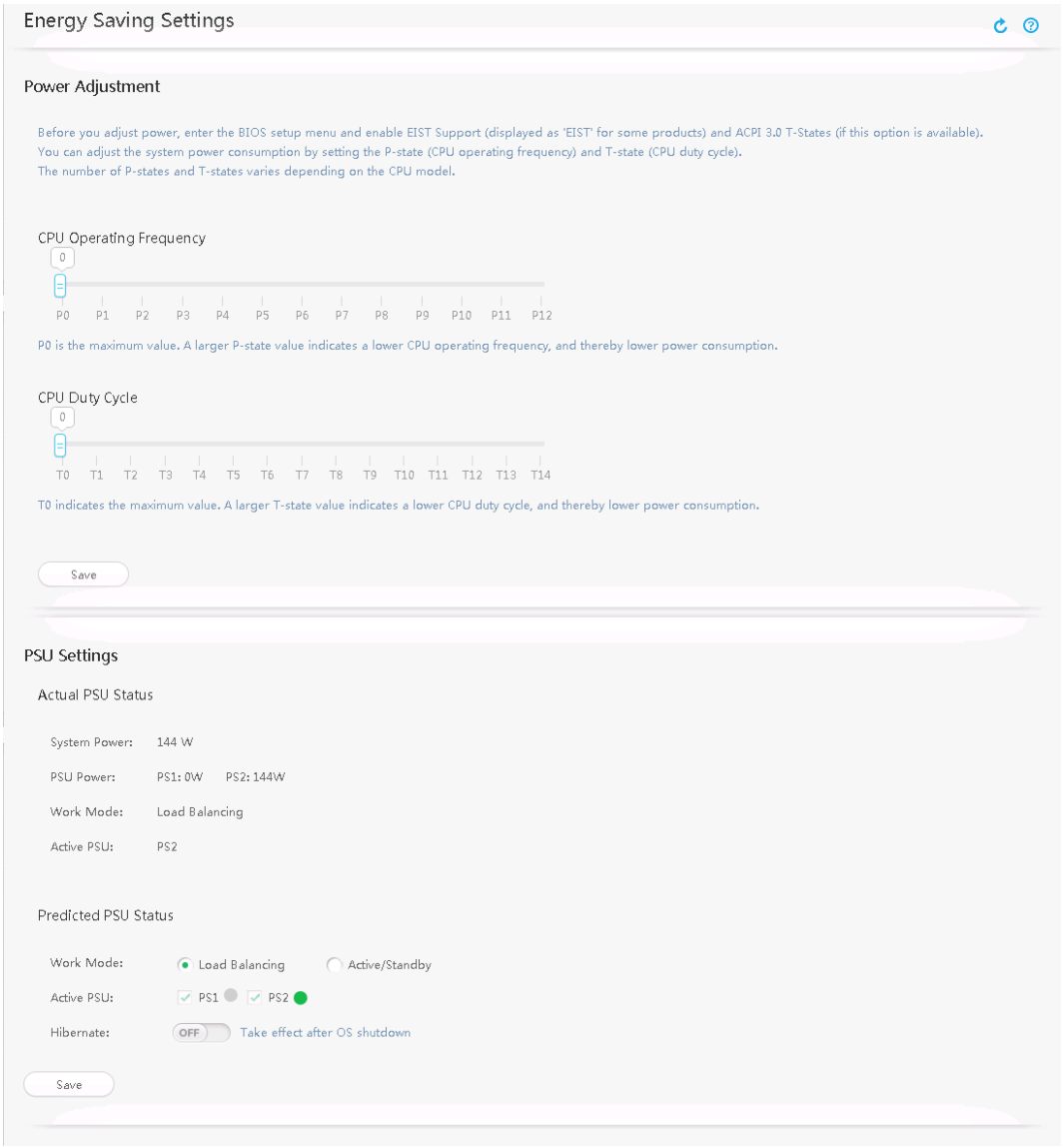


Рис. 3-19 Страница **Energy Saving Settings** других стоечных серверов



Описание параметра

Табл. 3-36 Параметры из области **Power Adjustment**

Параметр	Описание
CPU Operating Frequency	Для настройки рабочей частоты ЦП перетащите ползунок (P-состояние). Количество P-состояний различается в зависимости от модели ЦП. P0 – это максимальное значение. Более высокое значение P-состояния указывает на более низкую рабочую частоту ЦП и, следовательно, меньшее энергопотребление. **ПРИМЕЧАНИЕ** Если фактическая мощность сервера превышает значение ограничения

Параметр	Описание
	питания после того, как была выполнена настройка P-состояния и T-состояния, то P-состояние и T-состояние будут автоматически настроены на нормальные значения.
CPU Duty Cycle	Для настройки рабочего цикла ЦП перетащите ползунок (T-состояние). Количество T-состояний различается в зависимости от модели ЦП. T0 – это максимальное значение. Более высокое значение T-состояния указывает на более низкий рабочий цикл ЦП и, следовательно, меньшее энергопотребление. **ПРИМЕЧАНИЕ** Если фактическая мощность сервера превышает значение ограничения питания после того, как была выполнена настройка P-состояния и T-состояния, то P-состояние и T-состояние будут автоматически настроены на нормальные значения.

Табл. 3-37 Параметры в разделе **PSU settings** (сервер RH8100 V3 не поддерживает данную функцию)

Параметр	Описание
Actual PSU Status	
System Power	Текущая мощность сервера.
PSU Power	Текущая мощность всех блоков питания (PSU) сервера.
Work Mode	Текущий режим работы PSU.
Active PSU	Активные PSU. **ПРИМЕЧАНИЕ** Если для параметра **Work Mode** установлено значение **Load Balancing**, то отображаются все обнаруженные PSU.
Predicted PSU Status	
Work Mode	Режим работы PSU. Значения: • **Loading Balancing**: несколько блоков питания одновременно подают питание для системы и разделяют энергопотребление системы. Этот режим обеспечивает высокую мощность для всей системы и оказывает незначительное влияние на резервные блоки питания, если один из блоков питания неисправен. Однако блоки питания в данном режиме имеют низкую энергоэффективность и потребляют больше электроэнергии. • **Active/Standby**: один или несколько активных блоков питания подают питание для системы, а другие блоки питания являются резервными. В данном режиме обеспечивается более высокая энергоэффективность и меньшая потребляемая мощность. В данном режиме также продлевается срок службы блока

Параметр	Описание
	питания. Однако данный режим поддерживает более низкую мощность. Значение по умолчанию: **Распределение нагрузки** **ПРИМЕЧАНИЕ** • При низком энергопотреблении системы выберите **Active/Standby** для снижения потребляемой мощности сервера. • Если потребляемая мощность системы выше или равна 75% от номинальных мощностей активных блоков питания, то режим работы PSU автоматически изменится на **Loading Balancing**. • В настоящее время режим **active/standby** (резервирование «1+1») используется только если в системе сконфигурировано два PSU.
Active PSU	Активные PSU.
Hibernate	**ВНИМАНИЕ** После включения режима глубокой гибернации и сервер выключен, если все активные PSU будут удалены или перестанут подавать питание из-за сбоев, то потеря всей мощности сервера произойдет примерно за 10 секунд, после чего произойдет автоматическое включение PSU, находящихся в режиме глубокой гибернации. Включение режима глубокой гибернации. После включения режима глубокой гибернации, если сервер выключен, то некоторые PSU переходят в режим глубокой гибернации и перестают подавать питание. После включения режима глубокой гибернации или включения сервера, PSU в режиме глубокой гибернации продолжат подавать питание. Нажмите OFF или ON и нажмите **Save.** • Для включения данной функции установите для параметра ON. • Для отключения данной функции установите для параметра OFF. Настройки вступят в силу только после выключения ОС. **ПРИМЕЧАНИЕ** Настройка режима глубокой гибернации доступна только для серверов 1288H V5, 2288H V5 и 2488 V5.

Процедура

Конфигурирование политики энергосбережения ЦП

1. В строке меню выберите **Power**.
2. В дереве навигации выберите **Energy Saving Settings**.
   На экране появится страница **Energy Saving Settings**.
3. Для настройки рабочей частоты ЦП или рабочего цикла перетащите ползунок.
   Подробная информация о параметрах приведена в Табл. 3-36.

ПРИМЕЧАНИЕ

- Перетащите ползунок.

- Настройка максимальной рабочей частоты ЦП оказывает большее влияние на энергопотребление и меньшее влияние на производительность системы, чем настройка рабочего цикла ЦП. Поэтому сначала необходимо выполнить настройку максимальной рабочей частоты ЦП.

4. Нажмите **Save**.

   На экране появится следующая информация:

   ```
   Are you sure you want to perform this operation?
   ```

5. Нажмите **Yes**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Setting the PSU Working Mode (не поддерживается в серверах RH8100 V3)

1. В строке меню выберите **Power**.
2. В дереве навигации выберите **Energy Saving Settings**.

   На экране появится страница **Energy Saving Settings**.
3. В области **Predicted PSU Status** указите рабочий режим PSU, активный PSU, а также будет ли включен режим глубокой гибернации.

   Подробная информация о параметрах приведена в Табл. 3-36.

ПРИМЕЧАНИЕ

Настройка режима глубокой гибернации доступна только для серверов 1288H V5, 2288H V5 и 2488 V5.

4. Нажмите **Save**.

   На экране появится следующая информация:

   ```
   Are you sure you want to perform this operation?
   ```

5. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

3.7 Конфигурирование

3.7.1 Локальные пользователи

Описание функции

На странице **Local Users** можно выполнять просмотр и управление пользователями iBMC.

Кроме того, имя пользователя по умолчанию **root** для серверов V3 и **Administrator** для серверов V5. iBMC поддерживает до 15 пользователей. Система поддерживает добавление, редактирование или их удаление на данной странице.

GUI

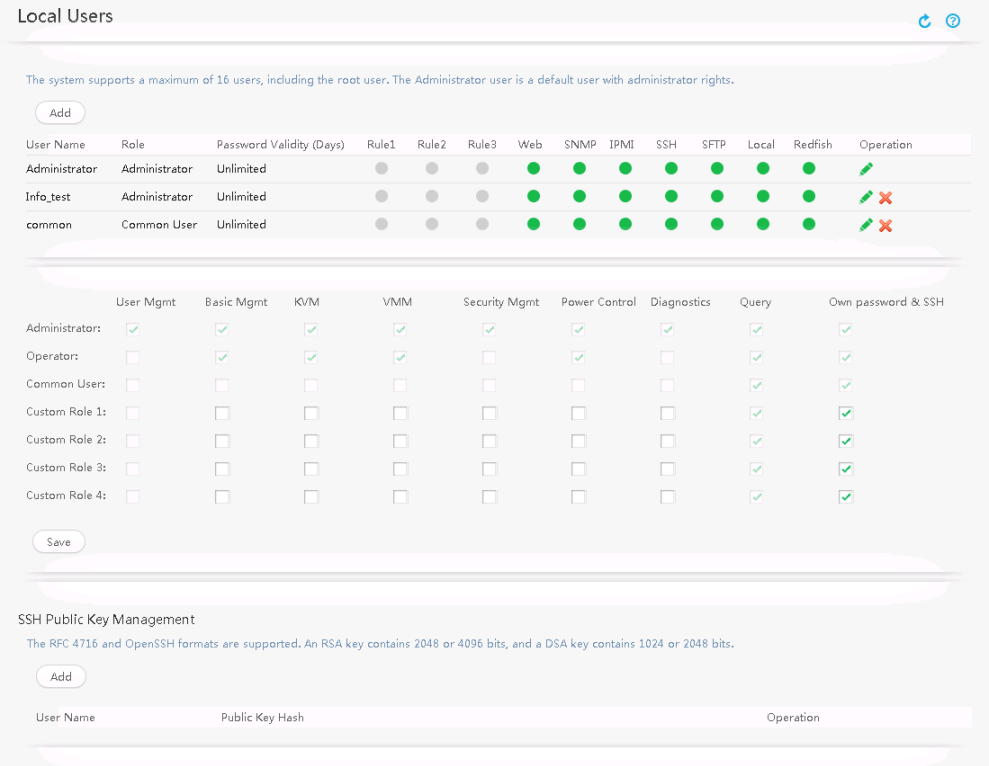
Выберите **Configuration** из главного меню и выберите **Local Users** из дерева навигации.

Откроется страница **Local User**. Страница состоит из трех областей.

- Local user list: список пользователей iBMC.

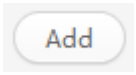
- User rights: список прав, назнавенных пользователям **Administrator**, **Operator**, **Common User**, а также четыре обычные роли.
- SSH public key management: список пользователей SSH, сконфигкрированных с публичными ключами. Система поддерживает добавление или удаление публичных ключей SSH.

Рис. 3-20 Страница **Local Users**



Описание параметра

Табл. 3-38 Параметры, связанные с локальными пользователями

Параметр	Описание
	Добавление локального пользователя.
	Изменение информации о локальном пользователе.
	Удаление локального пользователя.
	Сохранение конфигурации локального пользователя.
User Name	Имя пользователя для входа в iBMC. По умолчанию установлено имя пользователя **root** для серверов V3 и **Administrator** для серверов V5, а исходный пароль указан на табличке с маркировкой продукта. В целях

Параметр	Описание
	безопасности после первого входа рекомендуется изменить исходный пароль и периодически менять пароль в дальнейшем.
Role	Роль, назначенная пользователю. Роль определяет операции, которые может выполнять пользователь.
Password Validity (Days)	Срок действия пароля пользователя.
Rule	Правила входа в систему, которые применяются к пользователю.
Login Interface	Интерфейс при помощи которого пользователь входит в iBMC.

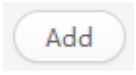
Табл. 3-39 Параметры, связанные с привилегиями

Параметр	Описание
Administrator	Пользователь, который может выполнять все операции. Полномочия пользователя **Administrator** нельзя изменить.
Operator	Пользователи, которые могут выполнять базовое управление, управление KVM, управление VMM, контроль питания, запрос информации и конфигурирование своих собственных паролей. Полномочия пользователя **Operator** нельзя изменить.
Common User	Пользователи, которые могут запрашивать информацию и конфигурировать свои собственные пароли Полномочия пользователя **Common User** нельзя изменить.
Custom Role 1 to 4	Пользователь, который может выполнять только определенные операции.
User Mgmt	Конфигурирование пользователей и паролей. **User Mgmt** поддерживает следующие операции: • Конфигурирование локальных пользователей, онлайн-пользователей и пользователей LDAP • Конфигурирование двухфакторной аутентификации • Восстановление заводских настроек
Basic Mgmt	Выполнение базовой конфигурации сервера внеполосного управления. **Basic Mgmt** поддерживает следующие операции: • Конфигурирование сети • Конфигурирование аварийных отчетов • Идентификация сервера • Обновление встроенного ПО • Загрузка и удаление SEL • Настройка загрузочного устройства

Параметр	Описание
	• Конфигурирование устройств хранения • Обновление языка На страницах **Alarm Settings**, **Network**, **System**, **System Info** и **Language Update** неавторизованные пользователи могут только выполнять запрос данных.
KVM	Дистанционное управление с помощью Java или встроенной удаленной консоли HTML5 или независимой удаленной консоли, выполнение конфигурирования VNC (доступно только для серверов V5) и настройка переадресации на последовательном порте.
VMM	Использование функции виртуальной среды.
Security Mgmt	Конфигурирование и запрос функций системы безопасности. **Security Mgmt** поддерживает следующие операции: • Запрос журналов операций и журналов безопасности • Выбор алгоритмов и протоколов • Управление сертификатом SSL • Конфигурирование услуг • Сбор информации одним щелчком кнопки мыши • Импорт и экспорт файлов конфигурации • Конфигурирование баннера безопасности при входе На страницах **Services**, **SSL Certificate** и **Import/Export** неавторизованные пользователи могут только запрашивать данные.
Power Control	Операции включения и выключения питания, перезагрузка, а также конфигурирование питания и энергосбережения. На страницах **Power Control**, **Power Capping** и **Energy Saving Settings** неавторизованные пользователи могут только запрашивать данные.
Diagnostics	Обнаружение неисправностей и ввод в эксплуатацию. **Diagnostics** поддерживает следующие операции: • Доступ к интерфейсу техобслуживания и ввода в эксплуатацию • Sensor simulation • Автоматическая запись видео • Создание скриншотов вручную и автоматически • Данные последовательного порта • Черный ящик
Query	Запрос информации за исключением настроек безопасности, пользовательских настроек и системной информации.
Own password & SSH	Конфигурирование своих собственных паролей и управление публичным ключом SSH. Пользователи системы по умолчанию обладают данными

Параметр	Описание
	полномочиями. Данные полномочия могут быть назначены и для обычных пользователей.

Табл. 3-40 Управление публичным ключом SSH

Параметр	Описание
User Name	Пользователь с публичным ключом SSH.
Public Key Hash	Строка, преобразованная из публичного ключа SSH с использованием хэш-алгоритмов.
	Удаление публичного ключа пользователя SSH.
	Импорт публичного ключа пользователя SSH.

Процедура

Просмотр пользовательской информации

1. В строке меню выберите **Configuration**.
2. В дереве навигации выберите **Local Users**.

   Откроется страница **Local User**.
3. Просмотр информации о локальных пользователях.

Добавление пользователей

Система поддержвает добавление максимум 15 пользователей iBMC.

1. Нажмите **Add**.

   На экране появится страница для добавления пользователя, как показано на Рис. 3-21. Подробная информация о параметрах приведена в Табл. 3-41.

Рис. 3-21 Добавление пользователя

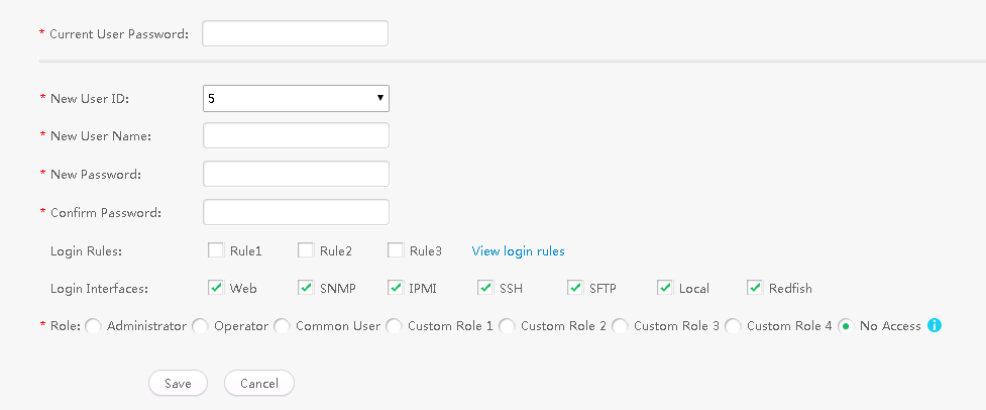


Табл. 3-41 Параметры связанные с добавлением пользователя

Параметр	Описание
Cancel	Страница для настройки локального пользователя без сохранения настроек.
Save	Сохранение информации.
Current User Password	Пароль текущего пользователя.
New User ID	ID добавляемого пользователя.
New User Name	Имя добавляемого пользователя. Значение: строка длиной от 1 до 16 символов Пароль должен соответствовать следующим требованиям: • Содержать буквы, цифры и специальные символы (за исключением <>&,'"/\%). • Не может начинаться со знака # и не должен содержать пробел.
New Password	Пароль для входа в iBMC. Значение: строка, длиной до 20 символов В целях безопасности необходимо периодически менять пароль. Если проверка сложности пароля включена, то пароль должен удовлетворять требованиям и быть достаточно сложным.
Confirm Password	Пароль для входа в iBMC. Значение должно быть таким же, что и для параметра **Password**.
Login Rules	Правила входа в систему, которые применяются к пользователю. Для просмотра настроенных правил нажмите **View login rules**.
Login Interfaces	Интерфейс при помощи которого пользователь входит в iBMC.

Параметр	Описание
	Значения: • **Web**: пользователь использует веб-браузер для входа в WebUI iBMC. • **SNMP**: пользователь использует инструмент SNMP (например браузер MIB) для входа в iBMC. • **IPMI**: пользователь использует инструмент IPMI (например IPMItool) для входа в CLI iBMC. • **SSH**: пользователь использует инструмент SSH (например PuTTY) для входа в CLI iBMC. • **SFTP**: пользователь использует инструмент SFTP (например Xftp) для входа в файловую систему iBMC. • **Local**: пользователь использует последовательный порт сервера для входа в CLI iBMC или может воспользоваться ЖК-дисплеем для входа на интерфейс управления iBMC. • **Redfish**: пользователь для входа в iBMC может воспользоваться инструментом Redfish. **ПРИМЕЧАНИЕ** По умолчанию для нового пользователя выбраны все интерфейсы входа.
Role	Роль, назначенная пользователю. Пользовательская роль определяет операции, которые может выполнять пользователь. Значения: • **Administrator**: пользователи с ролью **Administrator** выполняют все операции. • **Operator**: пользователи с ролью **Operator** выполняют базовые операции, удаленный контроль, доступ к удаленной среде, управление питанием, запрос информации и конфигурировать свои собственные данные. • **Common User**: пользователи с ролью **Common User** запрашивают информацию и конфигурируют свои собственные данные. • **Custom Role**: пользователи, которым назначены роли от **Custom Role 1** до **Custom Role 4** могут выполнять только заданные операции. • **No Access**: пользователи с ролью **No Access** не могут выполнять никаких операций. **ПРИМЕЧАНИЕ** Для новых пользователей по умолчанию система задает роль **No Access**.

2. Установите параметры пользователя. Подробная информация о параметрах приведена в Табл. 3-41.

ПРИМЕЧАНИЕ

- Пользователь с ID 1 является резервным пользователем, который определен в спецификациях IPMI. Данный пользователь не обладает правами на вход в iBMC.

- Для серверов V3 пользователь с ID 2 это пользователь **root**, а для серверов V5 это пользователь **Administrator**.

3. Нажмите **Save**.

   В списке пользователей появится информация о новом пользователе.

Modifying User Information

1. В списке локальных пользователей выберите пользователя, параметры которого необходимо изменить, и нажмите  .

   На экране появится страница для изменения пользовательской информации, как показано на Рис. 3-22. Подробная информация о параметрах приведена в Табл. 3-42.

Рис. 3-22 Изменение информации пользователя

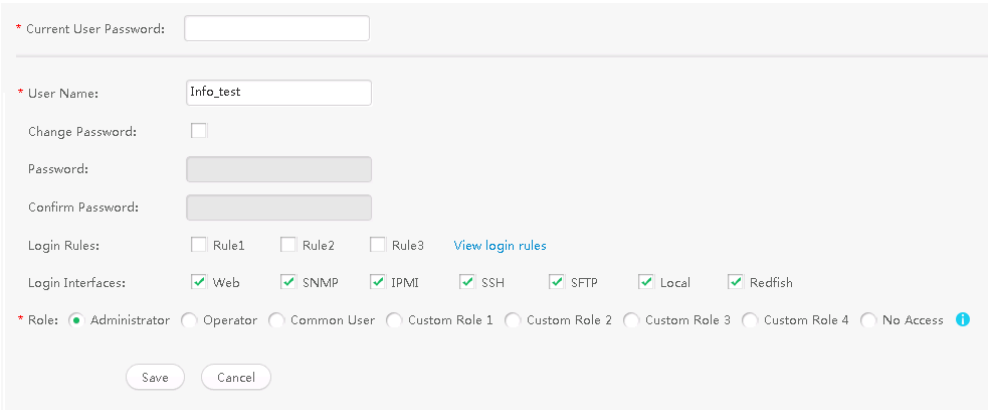
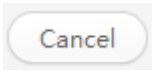
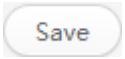


Табл. 3-42 Параметры связанные с редактированием пользователя

Параметр	Описание
	Страница для настройки локального пользователя без сохранения настроек.
	Сохранение информации. **ПРИМЕЧАНИЕ** Изменение имени пользователя, пароля или роли пользователя приведет к принудительному выходу пользователя из системы.
Current User Password	Пароль текущего пользователя.
User Name	Имя пользователя, параметры которого необходимо изменить.
Change Password	Изменения пароля пользователя. Выберите флажок и введите новый пароль в полях **Password** и **Confirm Password**. Если проверка сложности пароля включена, то пароль должен удовлетворять требованиям и быть достаточно сложным.
Login Rules	Правила входа в систему, которые применяются к пользователю.

Параметр	Описание
	Для просмотра настроенных правил нажмите **View login rules**.
Login Interfaces	Интерфейс при помощи которого пользователь входит в iBMC. Значения: • **Web**: пользователь использует веб-браузер для входа в WebUI iBMC. • **SNMP**: пользователь использует инструмент SNMP (например браузер MIB) для входа в iBMC. • **IPMI**: пользователь использует инструмент IPMI (например IPMItool) для входа в CLI iBMC. • **SSH**: пользователь использует инструмент SSH (например PuTTY) для входа в CLI iBMC. • **SFTP**: пользователь использует инструмент SFTP (например Xftp) для входа в файловую систему iBMC. • **Local**: пользователь использует последовательный порт сервера для входа в CLI iBMC или может воспользоваться ЖК-дисплеем для входа на интерфейс управления iBMC. • **Redfish**: пользователь для входа в iBMC может воспользоваться инструментом Redfish.
Role	Роль, назначенная пользователю. Пользовательская роль определяет операции, которые может выполнять пользователь.

2. Введите текущий пароль пользователя и измените информацию пользователя.

   Подробная информация о параметрах приведена в Табл. 3-42.
3. Нажмите **Save**.

   Информация пользователя успешно изменена.

Удаление пользователя

1. В списке локальных пользователей выберите пользователя для удаления и нажмите  .

   На экране появится диалоговое окно с просьбой ввести пароль текущего пользователя.
2. Введите пароль текущего пользователя и нажмите **OK**.

   Пользователь будет удален из списка пользователей.

Конфигурирование специальных ролей

Полномочия ролей, заданных в системе по умолчанию (**Administrator**, **Operator** и **Common User**) нельзя изменить, однако администратор может установить полномочия для специальных ролей.

1. Выберите необходимые параметры из списка функций.

   В Табл. 3-39 приведено описание полномочий.
2. Нажмите **Save**.

   На экране появится диалоговое окно с просьбой ввести пароль текущего пользователя.

3. Введите пароль текущего пользователя и нажмите **OK**.

Импорт открытого ключа SSH

ПРИМЕЧАНИЕ

- После того, как закрытый ключ сгенерирован на клиенте, необходимо импортировать соответствующий открытый ключ в iBMC для обеспечения безопасного доступа пользователей SSH к iBMC.
- Каждый пользователь имеет только один открытый ключ. Старый ключ будет заменен недавно импортированным открытым ключом.
- Открытые ключи могут быть в формате RFC 4716 или OpenSSH. Тип открытого ключа RSA или DSA. Ключ RSA содержит 2048 или 4096 бит, а ключ DSA содержит 1024 или 2048 бит.

1. Под **SSH Public Key Management** нажмите **Add**.

   На экране появятся параметры, как показано на Рис. 3-23. Табл. 3-43 приведено описание параметров.

Рис. 3-23 Импорт открытого ключа SSH

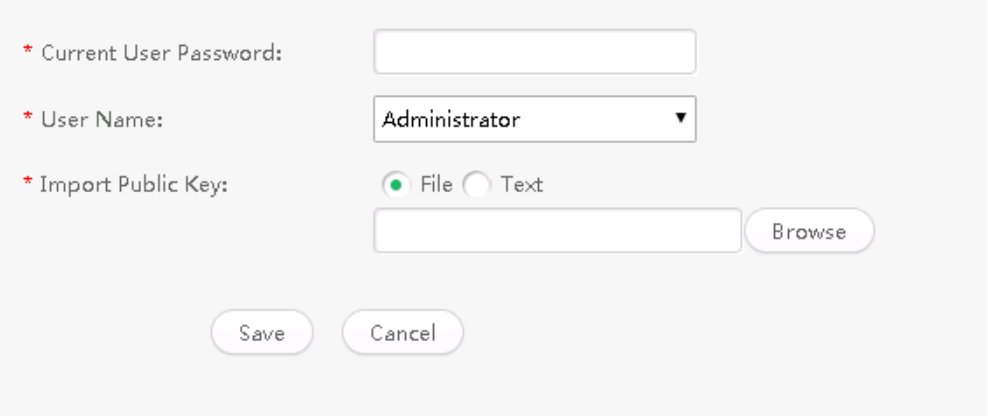


Табл. 3-43 Параметры, связанные с импортом открытых ключей SSH

Параметр	Описание
Current User Password	Пароль пользователя, использующего iBMC в данный момент времени.
User Name	Пользователь для которого выполняется импорт открытого ключа SSH.
Import Public Key	Режим импорта открытого ключа SSH. Значения: • **File**: импорт файла с открытым ключом SSH с локального клиента. • **Text**: введите информацию об открытом ключе SSH в текстовое поле.

2. Установите параметры. Подробная информация приведена в Табл. 3-43.
3. Нажмите **Save**.

Открытый ключ SSH успешно импортирован, если на экране появится информация «Public key imported successfully».

3.7.2 LDAP

Описание функции

На странице **LDAP** можно выполнить просмотр и настройку пользовательской информации (LDAP – Lightweight Directory Access Protocol).

iBMC предоставляет доступ только для пользователей LDAP. Пользователи LDAP могут войти в WebUI iBMC или использовать инструмент SSH для перехода к CLI iBMC. Использование учетной записи пользователя домена для доступа к iBMC повышает безопасность системы.

ВНИМАНИЕ

- В версии iBMC 2.46 или более ранней версии, имена групп, имена пользователей и CN, сконфигурированные на сервере LDAP для iBMC не могут содержать следующие специальные символы: \";<>#+=,
- На сервере LDAP параметры **DisplayName** и **CN** должны быть уникальными.

iBMC поддерживает максимум шесть серверов доменов. Во время входа в WebUI iBMC сервер домена можно указать вручную или он может быть найден автоматически. Во время доступа к CLI iBMC поиск сервера домена выполняется автоматически.

ПРИМЕЧАНИЕ

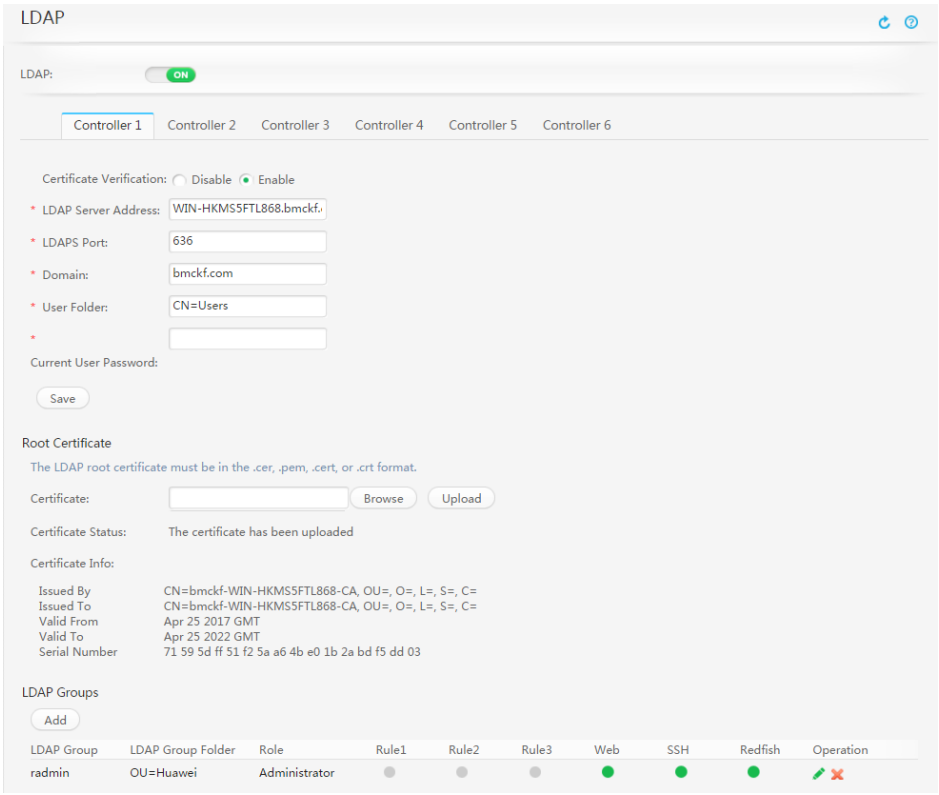
iBMC поддерживает активный Windows-каталог (AD – Active Directory) и Linux OpenLDAP.

GUI

Выберите **Configuration** из главного меню и выберите **LDAP** из дерева навигации.

На экране появится страница **LDAP**.

Рис. 3-24 Страница **LDAP**

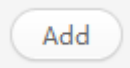
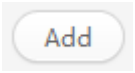


Описание параметра

Табл. 3-44 Параметры на странице **LDAP**

Параметр	Описание	
LDAP	Функция LDAP позволяет пользователям домена получить доступ к iBMC. Нажмите OFF или ON и нажмите **Save**. • ON: включение функции LDAP. • OFF: отключение функции LDAP.	
Domain Controller 1 iBMC поддерживает максимум шесть контроллеров доменов (серверов). Когда пользователь предпринимает попытку доступа к WebUI iBMC через LDAP, пользователь может выбрать контроллер домена или **Automatic matching**. Контроллеры доменов 1–3 имеют одинаковые параметры. **ПРИМЕЧАНИЕ** Параметры со знаком звездочки (*) являются обязательными.		
Basic Parameters	Certificate Verification	Проверка сертификата сервера LDAP, который может быть включен или отключен. В целях безопасности рекомендуется включить проверку

Параметр	Описание	
		сертификатов. После включения функции проверки сертификатов необходимо импортировать корневой сертификат LDAP, установить AD, DNS, указать орган выдавший сертификат CA на сервере LDAP и импортировать сертификат CA на сервер LDAP и iBMC.
	LDAP Server Address	IP-адрес сервера LDAP. Формат: IPv4 или IPv6-адрес. После включения функции проверки сертификата, установите данный параметр для сервера LDAP FQDN (*Host name*.*Domain name*) с укажите информацию об адресе DNS на странице **Network.**
	LDAPS Port	Номер порта сервиса LDAP. Значение: целое значение в диапазоне от 1 до 65535 Значение по умолчанию: **636** Зашифрованная передача включена по умолчанию. Н а сервере LDAP необходимо выполнить соответствующие настройки.
	Domain	Пользовательский домен, которому принадлежит LDAP-пользователь, определенный в контроллере домена. Значение: строка, длиной до 255 символов Значение может содержать буквы, цифры и специальные символы.
	User Folder	Имя папки пользователя, которое должно совпадать с именем папки с данными участника приложений на сервере LDAP. Например **CN=employee, OU=company** или **OU=department, OU=company.** Диапазон значений: строка длиной от 64 до 255 символов. Конкретная длина зависит от количества байтов каждого символа.
	Current User Password	Пароль текущего пользователя.
Root Certificate	Certificate	Загрузка корневого сертификата LDAP. Это могут быть файлы с расширением .cer, .pem, .cert, или .crt. **ПРИМЕЧАНИЕ** Системе требуется больше времени для загрузки файлов сертификатов, размер которых превышает 100 МБ. Обновите страницу для получения последнего статуса.
	Certificate Status	Импорт сертификата LDAP на сервер.
	Certificate Info	Информация о сертификате.

Параметр	Описание	
LDAP Groups		Добавление группы LDAP. Нажмите  для добавления группы LDAP.
		Регион для настройки существующей группы LDAP.
		Изменение группы LDAP.
	LDAP Group	Имя группы LDAP, к которой принадлежит пользователь LDAP. Диапазон значений: строка длиной от 64 до 255 символов. Конкретная длина зависит от количества байтов каждого символа.
	LDAP Group Folder	Имя папки с группой LDAP. Оно должно совпадать с названием организации, к которой принадлежит группа пользователей на сервере LDAP. Например **OU=department, OU=company**. Диапазон значений: строка длиной от 64 до 255 символов. Конкретная длина зависит от количества байтов каждого символа.
	Role	Роль, назначенная группе LDAP. Значение: **Administrator**, **Operator**, **Common user** или **Custom Role**.
	Login Rule	Правила входа в систему, которые применяются к группе LDAP.
	Login Interface	Интерфейсы, через которые участники группы LDAP смогут войти в iBMC. Значения: • **Web**: пользователи используют веб-браузер для входа в WebUI iBMC. • **SSH**: пользователи используют инструмент SSH (например PuTTY) для входа в CLI iBMC. • **Redfish**: пользователи для входа в iBMC используют инструмент Redfish.

Процедура

iBMC поддерживает максимум три сервера домена. Для настройки сервера домена, установите параметры контроллера LDAP, импортируйте корневой сертификат и добавьте группы LDAP.

Включение LDAP и установка параметров контроллера LDAP.

1. В строке меню выберите **Configuration**.
2. В дереве навигации выберите **LDAP**.

На экране появится страница **LDAP**.

3. Установите для параметра **LDAP Function** значение  .
4. Установка параметров контроллера LDAP. Подробная информация приведена в Табл. 3-44.
5. Нажмите **Save**.

   На экране появится сообщение «Operation Successful».

Импорт корневого сертификата LDAP.

1. В области **Import LDAP Root Certificate** нажмите **Browse** после **Certificate** и выберите сертификат LDAP.
2. Нажмите **Upload**.

   В случае успешной загрузки сертификата значение параметра **Certificate Status** изменится на **The certificate has been uploaded** и на экране появится информация об импортированном сертификате. Подробная информация приведена в Табл. 3-45.

Табл. 3-45 Параметры из области **Import LDAP Root Certificate**

Параметр	Описание
Issued By	Орган, выдавший сертификат LDAP. У параметров **Issued By** и **Issued To** одинаковые пункты.
Issued To	Пользователь (текущий сервер) сертификата LDAP, включая: • **CN**: имя пользователя. • **OU**: департамент пользователя. • **O**: компания, которой принадлежит пользователь. • **L**: город пользователя. • **S**: район или регион размещения пользователя. • **C**: страна пользователя.
Valid From	Дата, с которой сертификат LDAP считается действительным.
Valid To	Дата истечения срока действия сертификата LDAP.
Serial Number	Серийный номер сертификата LDAP, который используется для идентификации и переноса сертификата.

Добавление группы LDAP.

Система поддерживает добавление максимум 5 групп LDAP для iBMC.

1. В области **LDAP Group** нажмите **Add**.

   На экране появится страница для добавления группы LDAP, как показано на Рис. 3-25.

Рис. 3-25 Добавление группы LDAP

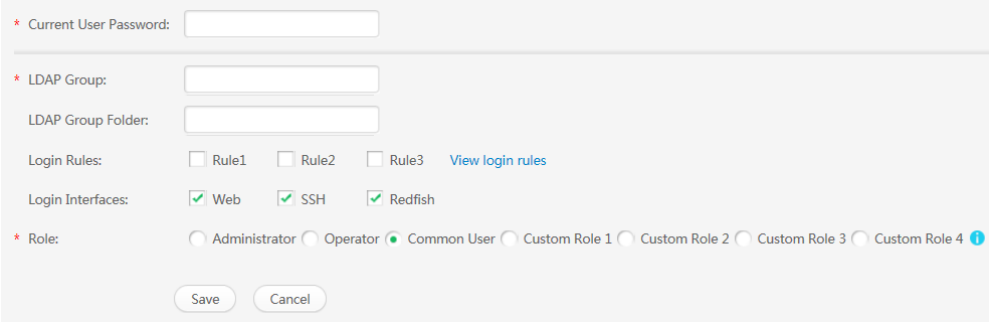


Табл. 3-46 Параметры для добавления группы LDAP

Параметр	Описание
Current User Password	Пароль пользователя, использующего iBMC в данный момент времени.
LDAP Group	Имя группы LDAP, к которой принадлежит пользователь LDAP. Диапазон значений: строка длиной от 64 до 255 символов. Конкретная длина зависит от количества байтов каждого символа.
LDAP Group Folder	Имя папки с группой LDAP. Оно должно совпадать с названием организации, к которой принадлежит группа пользователей на сервере LDAP. Например **OU=department, OU=company**. Диапазон значений: строка длиной от 64 до 255 символов. Конкретная длина зависит от количества байтов каждого символа.
Login Rules	Правила входа в систему, которые применяются к группе LDAP.
Login Interface	Интерфейсы, через которые участники группы LDAP смогут войти в iBMC. Значения: • **Web**: пользователи используют веб-браузер для входа в WebUI iBMC. • **SSH**: пользователи используют инструмент SSH (например PuTTY) для входа в CLI iBMC. • **Redfish**: пользователи для входа в iBMC используют инструмент Redfish.
Role	Роль, назначенная группе LDAP. Значение: **Administrator**, **Operator**, **Common user** или **Custom Role**.

2. Установите параметры группы LDAP.

3. Нажмите **Save**.

   Информация о новой группе LDAP будет отображена в списке групп LDAP.

Удаление группы LDAP.

1. В области **LDAP group** нажмите на  для группы LDAP, которую необходимо удалить.

   На экране появится диалоговое окно с просьбой ввести пароль текущего пользователя.
2. Введите пароль текущего пользователя.

Редактирование группы LDAP.

1. В области **LDAP group** нажмите  для редактирования группы.
2. Введите пароль текущего пользователя и измените параметры группы LDAP. Подробная информация приведена в Табл. 3-46.
3. Нажмите **Save**.

3.7.3 Двухфакторная аутентификация

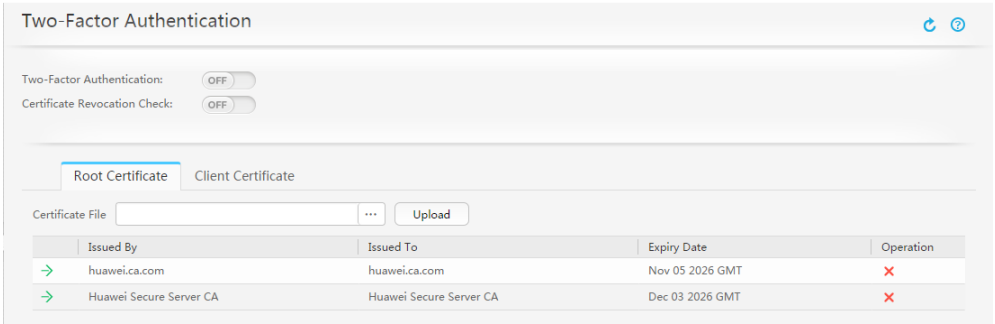
Описание функции

Двухфакторная аутентификация позволяет пользователям получить доступ только при условии правильно введенного сертификата клиента и пароля. Она обеспечивает более безопасный доступ чем при обычной аутентификации только по паролю учетной записи.

Для реализации безопасного соединения между клиентом и WebUI iBMC, необходимо загрузить корневой сертификат и клиентские сертификаты, выданные CA на iBMC.

GUI

Нажмите **Configuration** и из дерева навигации выберите **Two-Factor Authentication**. На экране появится страница **Two-Factor Authentication**.



Описание

Табл. 3-47 Двухфакторная аутентификация

Параметр	Описание

Параметр	Описание
Two-Factor Authentication	Включение двухфакторной аутентификации. Если двухфакторная аутентификация включена, то пользователи смогут войти в WebUI iBMC только если сертификат и пароль сертификата будут правильными. Нажмите  или  и нажмите **Save**. •  двухфакторная аутентификация включена. •  двухфакторная аутентификация отключена. **ПРИМЕЧАНИЕ** • После включения двухфакторной аутентификации необходимо выполнить импорт корневого сертификата и клиентского сертификата. В противном случае при последующих попытках входа может произойти сбой аутентификации. • После включения двухфакторной аутентификации произойдет автоматическое отключение сервиса SSH и его нельзя будет запустить вручную.
Certificate Revocation Check	Данный параметр определяет необходимость проверки срока действия сертификата во время аутентификации. Если параметр включен, то в процессе аутентификации будет выполняться проверка срока действия клиентского сертификата. Если клиентский сертификат окажется недействительным, то пользователь не сможет войти на WebUI iBMC. Нажмите  или  и нажмите **Save**. •  проверка срока действия сертификата включена. •  проверка срока действия сертификата отключена. **ПРИМЕЧАНИЕ** При проверке аннулирования сертификата используется протокол протокол проверки статуса сертификата в сети (OCSP – Online Certificate Status Protocol). Перед включением проверки аннулирования сертификата убедитесь, что соединение между iBMC и сервером OCSP находится в норме. В противном случае веб-сервис может быть недоступен.
Root Certificate	Перечень корневых сертификатов, загруженных на iBMC и информация о корневых сертификатах. iBMC поддерживает максимум 16 корневых сертификатов.
Client Certificate	Перечень клиентских сертификатов, загруженных на iBMC и информация о клиентских сертификатах, например имя пользователя, роль, отпечаток пальца к сертификату клиента (хэш-значение файла сертификата клиента) и статус. iBMC поддерживает сертификаты клиентов максимум для 16 пользователей.

Процедура

Включение двухфакторной аутентификации и загрузки сертификатов на iBMC

ПРИМЕЧАНИЕ

- Перед выполнением данной операции необходимо подать заявление на получение корневого и клиентского сертификата в официальный CA.
- Система поддерживает загрузку корневых и клиентских сертификатов, закодированных по схеме Base64. Корневые и клиентские сертификаты могут быть в следующих форматах: *.cer, *.crt и *.pem.

1. В строке меню выберите **Configuration**.
2. Из дерева навигации выберите **Two-Factor Authentication**.

   На экране появится страница **Two-Factor Authentication**.
3. Установите для параметра **Two-Factor Authentication** 

.
4. Перейдите на вкладку **Root Certificate** нажмите  после **Certificate File** и выберите корневой сертификат для загрузки.
5. Нажмите **Upload**.

   При успешной загрузке сертификата на экране появится **Imported successfully**.
6. Перейдите на вкладку **Client Certificate** нажмите  после имени пользователя и выберите сертификат клиента для загрузки.
7. Нажмите **Upload**.

   При успешной загрузке сертификата на экране появится **Imported successfully**.

Включение функции проверки аннулирования сертификата

1. Установите для параметра **Certificate Revocation Check** значение 

.

Включение аутентификации по сертификату для доступа к iBMC

ПРИМЕЧАНИЕ

После загрузки сертификатов для включения функции аутентификации по сертификату пользователей, которые предпринимают попытки входа в WebUI iBMC, выполните следующие действия:

1. Откройте браузер на клиенте, например Google Chrome.
2. Нажмите  в верхнем правом углу и выберите **Settings**.
3. В окне **Settings** нажмите **Manage certificates** под **HTTPS/SSL**.
4. Выполните импорт сертификата клиента.
5. В адресной строке браузера введите адрес для входа в iBMC.
6. Выберите сертификат клиента в соответствии с инструкциями.

   После этого вход в WebUI iBMC будет выполнен успешно.

Удаление корневого сертификата

1. На вкладке **Root Certificate** нажмите на  после корневого сертификата, который необходимо удалить.

   На экране появится диалоговое окно с просьбой подтвердить ваши действия.
2. Нажмите **Yes**.

Удаление сертификата клиента

1. На вкладке **Client Certificate** нажмите на  после пользователя, чей клиентский сертификат необходимо удалить.

   На экране появится диалоговое окно с просьбой подтвердить ваши действия.
2. Нажмите **Yes**.

Просмотр подробной информации о корневом сертификате

1. На вкладке **Root Certificate** нажмите на  перед сертификатом.

   На экране появится подробная информация о сертификате.

3.7.4 Экран Security

Описание функции

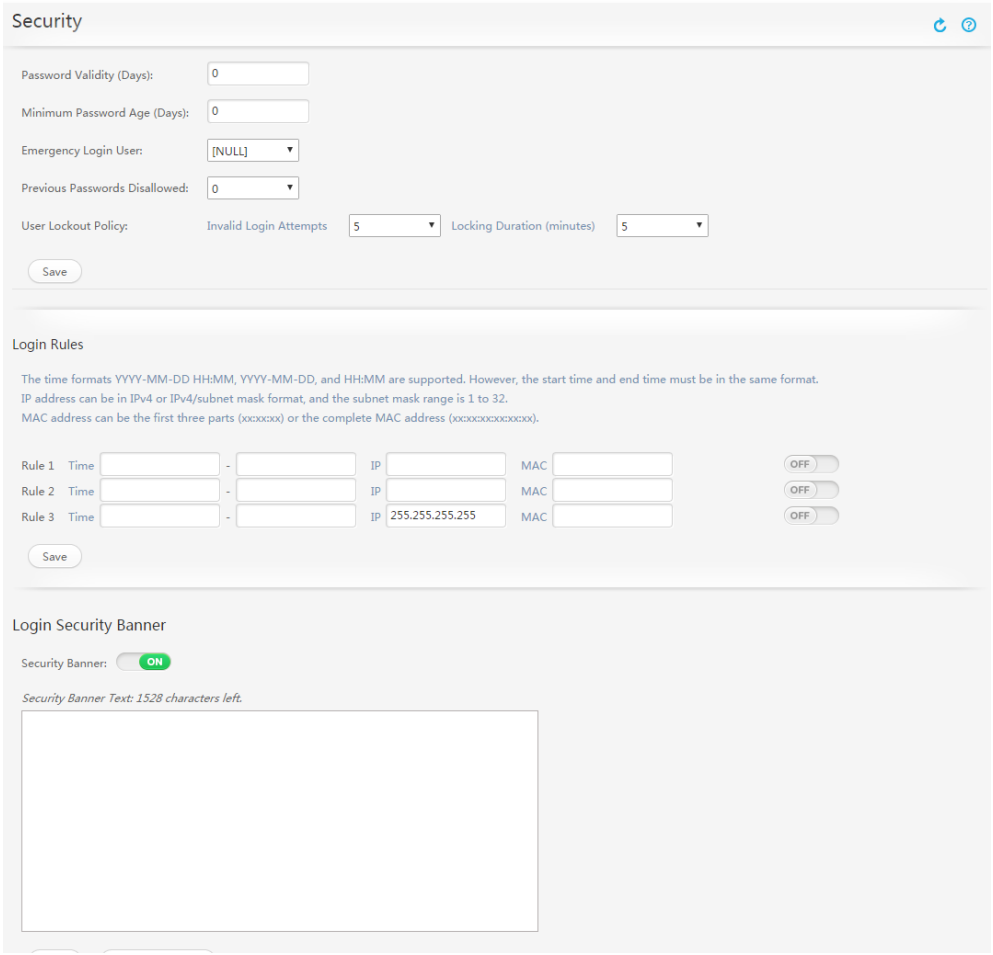
На экране **Security** выполняется просмотр и настройка правил защиты пользователя для iBMC.

GUI

Выберите **Configuration** из главного меню и выберите **Security** из дерева навигации.

На экране появится страница **Security**.

Рис. 3-26 Страница **Security**



Описание параметров

Табл. 3-48 Параметры пароля

Параметр	Описание
Password Complexity Check	Проверка сложности пароля определяет удовлетворяет ли пароль требованиям и является ли он достаточно сложным. Данный параметр включен по умолчанию. Он используется для SNMPv1/v2, имен trap-сообществ SNMP и паролей VNC. **ПРИМЕЧАНИЕ** Проверку сложности паролей VNC поддерживают только серверы V5. Если проверка сложности пароля включена, то пароль должен соответствовать следующим требованиям: • должен содержать от 8 до 20 символов • должен включать пробел и один из следующих специальных символов:

Параметр	Описание
	`~!@#$%^&*()-_=+\|[{}];:'",<.>/? • Он должен включать символы, как минимум, двух видов: – Заглавные буквы: от A до Z – Строчные буквы: от a до z – Цифры: от 0 до 9 • Пароль не должен совпадать с именем пользователя в прямом и обратном порядке расположения символов. • Пароль должен иметь по крайней мере два новых символа по сравнению с предыдущим именем сообщества. Пароль VNC также должен соответствовать определенным требованиям: • содержать, как минимум, один пробел или один из следующих специальных символов: `~!@#$%^&*()-_=+|[{}];:'",<.>/? • Должен содержать, как минимум, символы следующих двух видов: – Заглавные буквы: от A до Z – Строчные буквы: от a до z – Цифры: от 0 до 9 **ВНИМАНИЕ** В целях безопасности рекомендуется включить проверку сложности пароля.
SSH Password Authentication	При использовании аутентификации пароля SSH пользователи могут выполнять входв в iBMC по SSH при помощи пароля или публичного ключа. Значения: • **Disable**: вход пользователей выполняется по SSH с помощью только публичных ключей. • **Enable**: вход пользователей выполняется по SSH при помощи паролей или публичных ключей.
Password Validity (Days)	Срок действия (в днях) пароля пользователя. Диапазон значений: от 0 до 365 **0** означает, что у пароля нет срока действия.
Minimum Password Age (Days)	Минимальное время (в днях) в течение которого необходимо использовать пароль. В течение данного периода пароль нельзя изменить. Диапазон значений: от 0 до 365 **0** означает, что у пароля нет минимального срока действия пароля. **ПРИМЕЧАНИЕ** Значение минимального срока действия пароля должно быть, по меньшей мере, на 10 дней меньше срока действия пароля. • Если для параметра **Password Expiration (Days)** указано значение **10** или меньше, то для параметра **Minimum Password Age (Days)**

Параметр	Описание
	может быть установлено только значение **0**. • Если для параметра **Minimum Password Age (Days)** установлено значение **354** или более, то для параметра **Password Expiration (Days)** может быть установлено только значение **0**.
Emergency Login User	Имя пользователя для входа в iBMC в экстренных случаях. Данный пользователь не имеет ограниченных правил на вход в систему или интерфейсы входа, и у пароля такого пользователя нет срока действия. **ПРИМЕЧАНИЕ** В качестве пользователя для осуществления экстренного входа в систему может быть указан только администратор.
Previous Passwords Disallowed	Количество предыдущих паролей, которые не могут использоваться в качестве нового пароля. Диапазон значений: от 0 до 5 **0** означает, что можно использовать все предыдущие пароли.
User Lockout Policy	Максимально допустимое количество попыток входа в систему при неправильно введенных данных и длительность блокировки учетной записи. • Максимально допустимое количество попыток входа в систему при неправильно введенных данных – это целое число в диапазоне от 1 до 5 или значение **Unlimited** (блокировка учетной записи отключена). • Длительность блокировки учетной записи (в минутах) – это целое число в диапазоне от 1 до 5. После блокировки учетной записи пользователя, пользователь может повторно войти в систему только после истечения длительности блокировки учетной записи. **ПРИМЕЧАНИЕ** • Для целях безопасности функцию блокировки учетной записи рекомендуется включить. • Для разблокировки учетной записи пользователя в экстренных ситуациях, выполните команду **unlock** на CLI. Подробная информация приведена в документе *Руководство пользователя iBMC* сервера.

Табл. 3-49 Параметры из области **login rule**

Параметр	Описание
Time	**ВНИМАНИЕ** • Начальный и конечный год не может быть больше 2050. • Начальное и конечное время для правил входа должно быть указано в одном формате. Период времени в течение которого пользователь может выполнять вход в систему. Значение может быть указано в одном из следующих форматов:

Параметр	Описание
	• *YYYY-MM-DD*: Пример значения: от **2013-08-30** до **2013-12-30** • *HH*:*MM*: Пример значения: от **08:30** до **20:30** • *YYYY-MM-DD HH*:*MM*: Пример значения: от **2013-08-30 08:30** до **2013-12-30 20:30**
IP	IP-адрес или диапазон IP-адресов, для которых разрешен вход в систему. Значение может быть представлено в одном из следующих форматов: • IPv4 (*xxx.xxx.xxx.xxx*): IP-адрес. • IPv4/маска подсети (*xxx.xxx.xxx.xxx*/*mask*): сегмент IP-адресов.
MAC	MAC-адрес или диапазон MAC-адресов, для которых разрешен вход в систему. Значение может быть представлено в одном из следующих форматов: • *xx:xx:xx:xx:xx:xx*: MAC-адрес. • *xx:xx:xx*: сегмент MAC-адресов.

Табл. 3-50 Праметры из области **login security banner settings**

Параметр	Описание
Login Security Banner	Включение или отключение баннера безопасности при входе в систему. •  : включение баннера безопасности при входе в систему. На странице входа появится баннер безопасности. •  : отключение баннера безопасности при входе в систему.
Security Banner	Текст на баннере безопасности, который отображается на странице входа. Значение: строка, длиной до 1600 символов.

Процедура

Настройка правил использования паролей

1. В строке меню выберите **Configuration**.
2. В дереве навигации выберите **Security**.
   На экране появится страница **Security**.
3. Настройте нужные параметры. Подробная информация приведена в Табл. 3-48.
4. Нажмите **Save**.

На экране появится диалоговое окно с просьбой подтвердить ваши действия.

5. Нажмите **Yes**.

Настройка правил входа в систему

iBMC поддерживает максимум три правила входа. Пользователи, которые соответствуют любому из трех правил, смогут войти в iBMC.

Правила входа действуют для локальных пользователей, групп LDAP, сервисов SNMPv3 или интерфейсов CLP (ssh), KVM_VMM RMCP и интерфейсов Redfish только тогда, когда они отвечают следующим двум условиям:

- Правила входа в систему сконфигурированы и включены в области **Login Rules**.
- Правила входа были выбраны в области конфигурирования.

ПРИМЕЧАНИЕ

Каждое правило входа включает три условия: длительность входа, сегмент IP-адресов источника и сегмент MAC-адресов источника. При конфигурировании правила входа не нужно указывать все три условия.

1. В области **Login Rules** установите правила входа.

   Подробная информация приведена в Табл. 3-49.

2. Установите правила входа 

.
3. Нажмите **Save**.

   На экране появится диалоговое окно с просьбой подтвердить ваши действия.

4. Нажмите **Yes**.

Настройка баннера безопасности при входе в систему

1. В области **Login Security Banner Settings** установите для параметра **Security Banner** 

.
2. Введите сообщение в поле **Security Banner Text**.
3. Нажмите **Save**.

   На экране появится диалоговое окно с просьбой подтвердить ваши действия.

4. Нажмите **Yes**.

Восстановление сообщения безопасности по умолчанию при входе в систему

1. В области **Login Security Banner Settings** установите для параметра **Security Banner** 

.
2. Нажмите **Restore Defaults**.
3. Нажмите **Save**.

   На экране появится диалоговое окно с просьбой подтвердить ваши действия.

4. Нажмите **Yes**.

3.7.5 Сеть

Описание функции

На странице **Network** можно выполнить следующие операции:

- Установить имя хоста сервера.

- Установить режим и IP-адрес сетевого порта управления для сервера.

ВНИМАНИЕ

Изменение IP-адреса сетевого порта управления приведет к потере соединения сети. Изменять IP-адрес рекомендуется только в случае крайней необходимости.

- Установить режим получения информации системы доменных имен (DNS – domain name system).

ПРИМЕЧАНИЕ

DNS поддерживает как IPv4-адреса, так и IPv6-адреса.

Если RH8100 V3 функционирует в односистемном режиме, LAN материнской платы (LOM) на HFC-1 не предоставляет функцию интерфейса боковой полосы сетевого контроллера (NC-SI – Network Controller Sideband Interface). Таким образом, сетевые порты на LOM HFC-1 не отображаются в зоне **LOM**.

- Установить VLAN.
- Указать информацию NTP.
- Указать часовой пояс.

ПРИМЕЧАНИЕ

Когда сервер отключен, а затем происходит его включение или загружается драйвер, сетевой порт повторно подключается из-за функции энергосбережения сетевой интерфейсной платы X540 или BCM5719. В данном сценарии функция NC-SI временно недоступна.

GUI

Выберите **Configuration** из главного меню и выберите **Network** из дерева навигации.

На экране появится страница **Network**.

Рис. 3-27 Страница **Network** RH8100 V3

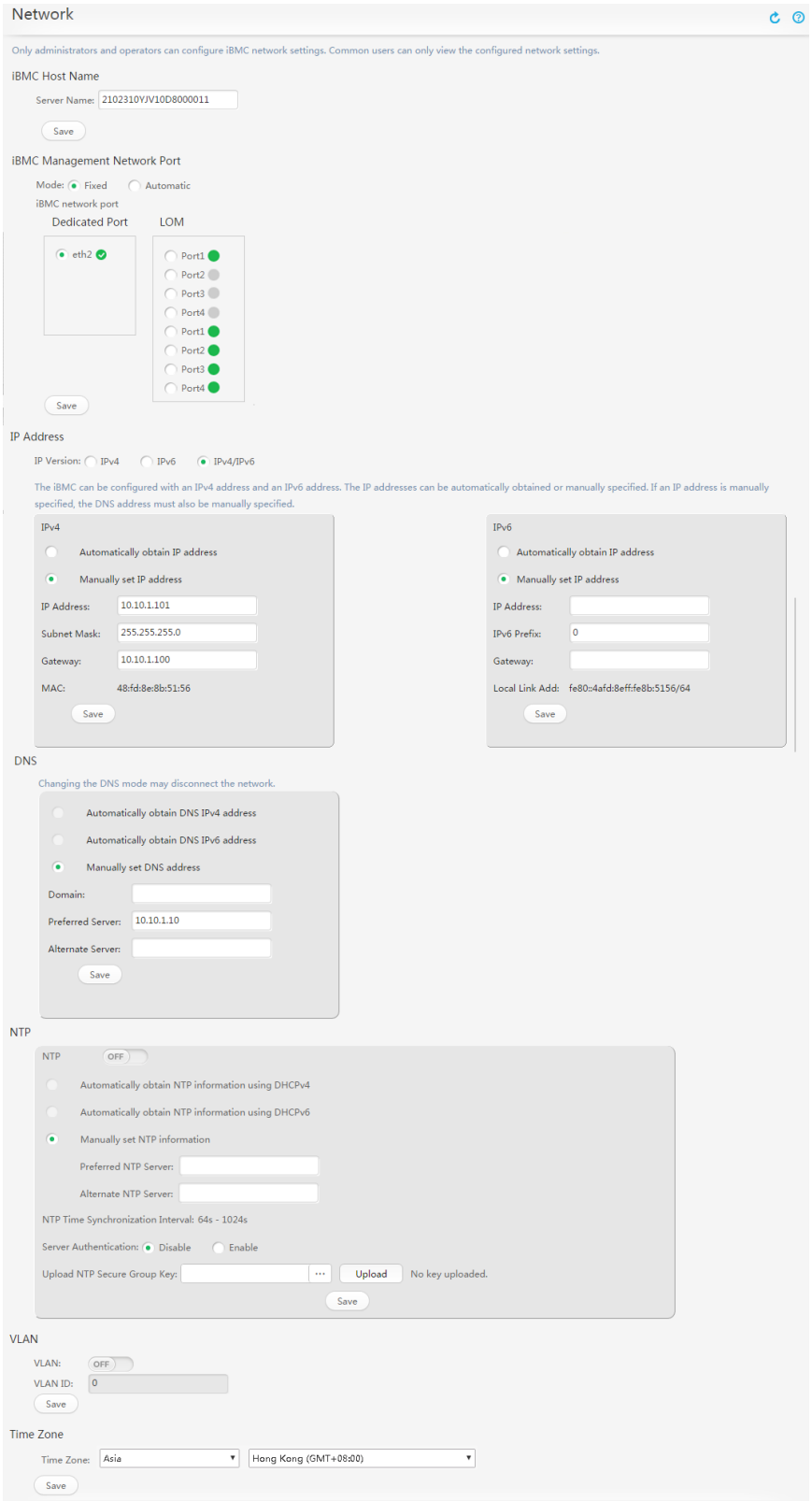
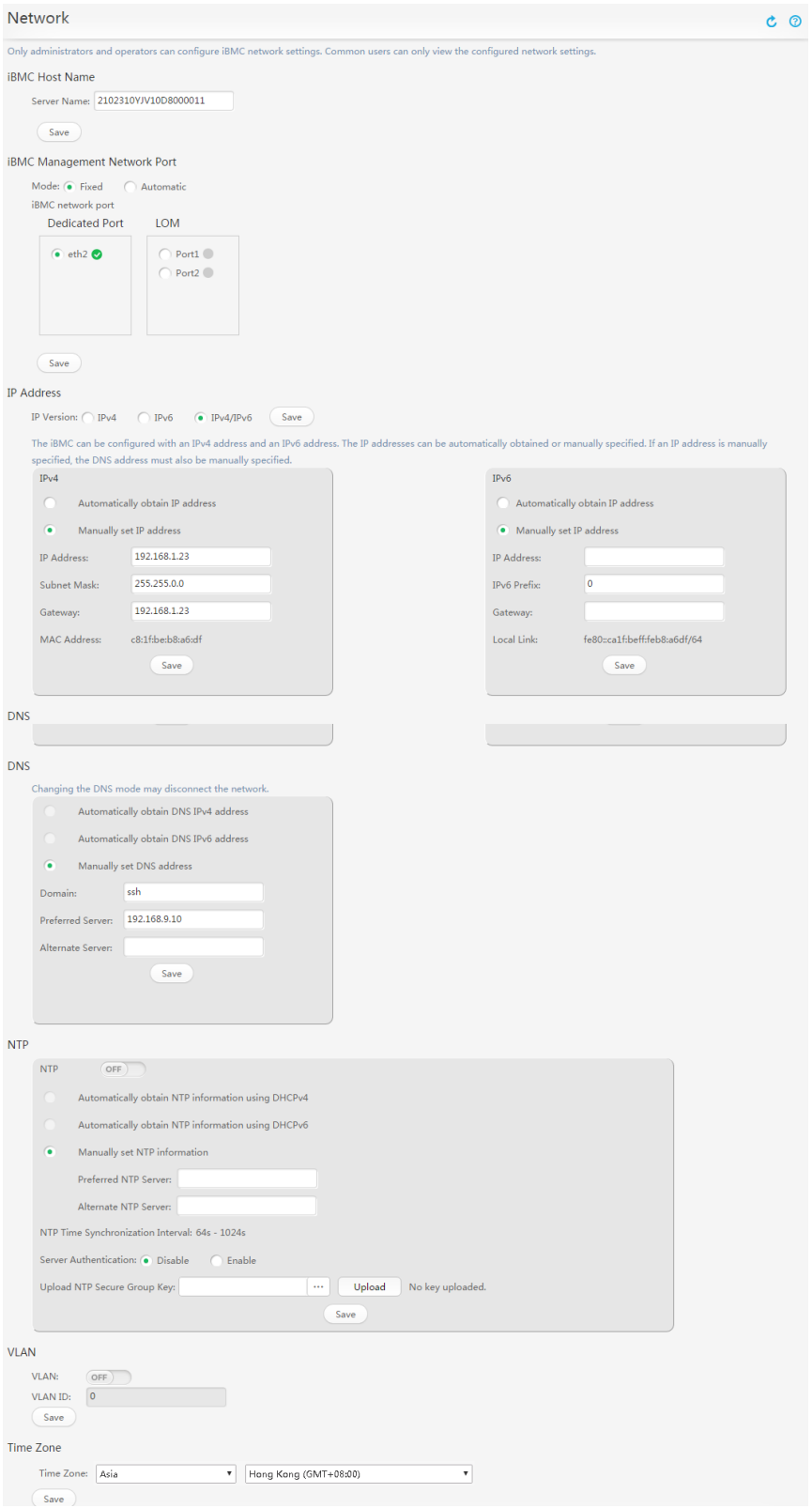


Рис. 3-28 Страница **Network** других стоечных серверов



Описание параметра

Табл. 3-51 Параметры на странице **Network**

Параметр	Описание
Server Name	Имя хоста iBMC. Значение: строка длиной от 1 до 64 символов Значение может включать буквы, цифры и дефис (-), но не может начинаться или заканчиваться дефисом. Значение по умолчанию: huawei
Mode	Тип сетевого порта управления, т.е. сетевого порта iBMC. Значение: • **Fixed**: при выборе данной опции необходимо также указать выделенный сетевой порт, LOM или порт технологии шины для подключения периферийных устройств (PCIe – Peripheral Component Interconnect Express) в качестве сетевого порта iBMC. – Dedicated network port: выделенный сетевой порт iBMC – LOM network port: сервисный сетевой порт на LOM – PCIe port (недоступен для RH8100 V3): сервисный сетевой порт на плате PCIe • **Automatic**: при выборе данной опции iBMC автоматически выбирает сетевой порт iBMC, в зависимости от статуса. Если доступно несколько сетевых портов, iBMC выбирает сетевой порт в соответствии со следующим приоритетом: выделенный сетевой порт > сетевой порт LOM > порт PCIe (недоступен для RH8100 V3). **ПРИМЕЧАНИЕ** • Если сетевой порт на плате PCIe выбран в качестве сетевого порта iBMC, то может использоваться только плата PCIe Huawei, которая подключена с использованием кабелей NC-SI. • Если порт на LOM выбран в качестве сетевого порта iBMC, то LOM должен поддерживать NC-SI. • При выборе порта LOM или порта PCIe вручную или автоматически, один и тот же физический порт служит управляющим портом и сервисным сетевым портом. В целях безопасности необходимо сконфигурировать данные виртуальной локальной сети (VLAN – virtual local area network) для изоляции плоскости управления и плоскости обслуживания, при условии что выбраны значения **Fixed** или **Automatic** и сконфигурированы порты LOM и PCIe. • Если сетевой порт выбран в качестве сетевого порта управления iBMC, то  будет отображено за сетевым портом. Значения по умолчанию: **Fixed**
Сетевой порт iBMC	Если для параметра **Select Mode** выбрано значение **Fixed**, то необходимо указать сетевой порт управления. Если для параметра **Select Mode** выбрано значение **Automatic**, то необходимо выбрать сетевые порты для автосогласования.

Параметр	Описание
IP Version	Версии IP-адресов: • IPv4 • IPv6 • IPv4/IPv6 Значение по умолчанию: **IPv4/IPv6**
IPv4	
Automatically obtain IP address	Выберите данный параметр, чтобы для сетевого порта iBMC был автоматически назначен IPv4-адрес.
Manually set IP address	Выберите данный параметр для установки IPv4-адреса сетевого порта iBMC. Информация об IPv4-адресе включает: **IP Address**, **Subnet Mask**, **Gateway** и **MAC Address**. **ПРИМЕЧАНИЕ** **MAC Address** – это физический адрес NIC.
IPv6	
Automatically obtain IP address	Выберите данный параметр, чтобы для сетевого порта iBMC был автоматически назначен IPv6-адрес.
Manually set IP address	Выберите данный параметр для установки IPv6-адреса сетевого порта iBMC. Информация об IPv6-адресе включает: **IP Address**, **IPv6 Prefix**, **Gateway**, **Local Link** и **IP Address List**. **ПРИМЕЧАНИЕ** • **Local Link** используется для локальной связи. • **IP Address List** поддерживает максимум 15 IPv6-адресов, при использовании автоматической настройки адресов без сохранения состояния (SLAAC – stateless address autoconfiguration).
DNS	
Automatically obtain DNS IPv4 address	Выберите данный параметр, чтобы для сервера DNS был автоматически назначен IPv4-адрес.
Automatically obtain DNS IPv6 address	Выберите данный параметр, чтобы для сервера DNS был автоматически назначен IPv6-адрес.
Manually set DNS address	Выберите данный параметр для ввода информации о DNS вручную. Информация о DNS включает: **Domain**, **Preferred Server** и **Alternate Server**. **ВНИМАНИЕ** Если IP-адрес сетевого порта iBMC указан вручную, то информация о DNS также должна быть указана вручную.
Domain	Имя домена для сервера. Значение: строка длиной от 0 до 67 символов Значение может содержать буквы, цифры и специальные символы, включая пробелы.

Параметр	Описание
Preferred Server	IP-адрес предпочтительного сервера DNS.
Alternate Server	IP-адрес альтернативного сервера DNS.
NTP	
NTP	NTP позволяет серверу синхронизировать время с сервером NTP. Нажмите  или  и нажмите **Save**. Значение: •  : включение NTP. •  : отключение NTP.
Automatically obtain NTP information using DHCPv4	Выберите данный параметр, чтобы для сервера NTP был автоматически назначен IPv4-адрес. **ПРИМЕЧАНИЕ** При выборе данного параметра, информация о часовом поясе должна быть указана вручную.
Automatically obtain NTP information using DHCPv6	Выберите данный параметр, чтобы для сервера NTP был автоматически назначен IPv6-адрес.
Manually set NTP information	Выберите данный параметр, чтобы указать предпочтительный и альтернативный сервер NTP вручную.
Preferred NTP server	IP-адрес предпочтительного сервера NTP. Значение: • IPv4 address • IPv6 address • Domain name
Alternate NTP server	IP-адрес альтернативного сервера NTP. Значение: • IPv4 address • IPv6 address • Domain name
Server Authentication	Закрытый ключ для загрузки на iBMC и проверки идентификации, если параметр **Server Authentication** включен.
NTP Time Synchronization Interval	Интервал в течение которого система выполняет синхронизацию времени с сервером NTP. Система автоматически указывает интервал синхронизации времени, в зависимости от сетевого статуса. Если сеть находится в хорошем состоянии, то в качестве интервала синхронизации времени указывается максимальное значение.
Server	Аутентификация, которая может быть включена или отключена

Параметр	Описание
Authentication	для связи между сервером и сервером NTP. Значение по умолчанию: Disabled
Upload NTP Secure Group Key	Если параметр **Server Authentication** включен, то для проверки идентификации необходимо загрузить закрытый ключ на iBMC. **ПРИМЕЧАНИЕ** Для генерирования закрытых ключей система поддерживает загрузку генератора ключей (например ntp-keygen).
VLAN	
VLAN	Настройка VLAN. Нажмите  или  и нажмите **Save**. Значения: •  VLAN включена. •  VLAN отключена. **ПРИМЕЧАНИЕ** • Система не поддерживает настройку VLAN, только если выделенный сетевой порт используется в рамках режима **Fixed**. • Для изоляции между сервисной сетью и управляющей сетью рекомендуется включить VLAN и установить ID VLAN. Значение по умолчанию: 
VLAN ID	VLAN которой принадлежит сетевой порт iBMC.
Time Zone	Часовой пояс для iBMC. Установить часовой пояс можно следующими способами: • Выберите **Others** из **Time Zone** и выберите сдвиг по времени **GMT-***hh:mm* или **GMT+***hh:mm*. Сдвиг по времени находится в диапазоне от **GMT-12:00** до **GMT+14:00**. • Выберите название часового пояса: *Global time zone name+City name* **ПРИМЕЧАНИЕ** • При выборе **Automatically obtain NTP information through DHCPv4** система автоматически отобразит информацию о часовом поясе. • В часовых поясах, использующих летнее время (DST), iBMC автоматически указывает время на один час вперед, когда начинается DST, и возвращается к стандартному времени, когда заканчивается DST. Значение по умолчанию: **Others+GMT**

Процедура

Настройка имени хоста

1. На странице **Network** укажите имя хоста сервера.

   Подробная информация приведена в Табл. 3-51.

2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

3. Нажмите **Restart Now** для незамедлительной перезагрузки iBMC или нажмите **Restart Later**, чтобы выполнить перезагрузку iBMC позже.

ПРИМЕЧАНИЕ

Сброс iBMC приведет к автоматическому генерированию сертификата SSL.

Выбор сетевого порта управления

1. На странице **Network** выберите тип сетевого порта управления и укажите сетевой порт.

   Подробная информация приведена в Табл. 3-51.

2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка IPv4-адреса для сетевого порта управления

1. В области **IPv4** на странице **Network** укажите информацию о IPv4 для сетевого порта управления.

   Подробная информация приведена в Табл. 3-51.

2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка IPv6-адреса для сетевого порта управления

1. В области **IPv6** на странице **Network** укажите информацию о IPv6 для сетевого порта управления.

   Подробная информация приведена в Табл. 3-51.

2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Автоматическое получение информации о DNS

1. Нажмите **Automatically obtain DNS IPv4 address** если сетевой порт управления использует IPv4-адрес или нажмите **Automatically obtain DNS IPv6 address** если сетевой порт управления использует IPv6-адрес.

2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка информации NTP вручную

1. Нажмите на кнопку **Manually set DNS IP address**.
2. Установите значения параметров **Domain**, **Preferred Server** и **Alternate Server**. Подробная информация приведена в Табл. 3-51.
3. Нажмите **Save**.

Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка ID VLAN для сетевого порта управления

ВНИМАНИЕ

Указанный ID VLAN вступает в силу только для сетевого порта управления общего пользования.

1. В области **IPv4** на странице **Network** укажите ID VLAN для сетевого порта управления. Подробная информация приведена в Табл. 3-51.
2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка информации о NTP

1. В **NTP** укажите параметры в зависимости от сервисных требований.

   Подробная информация приведена в Табл. 3-51.
2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка часового пояса

1. В **Time zone** выберите часовой поясе.
2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

3.7.6 Страница Services

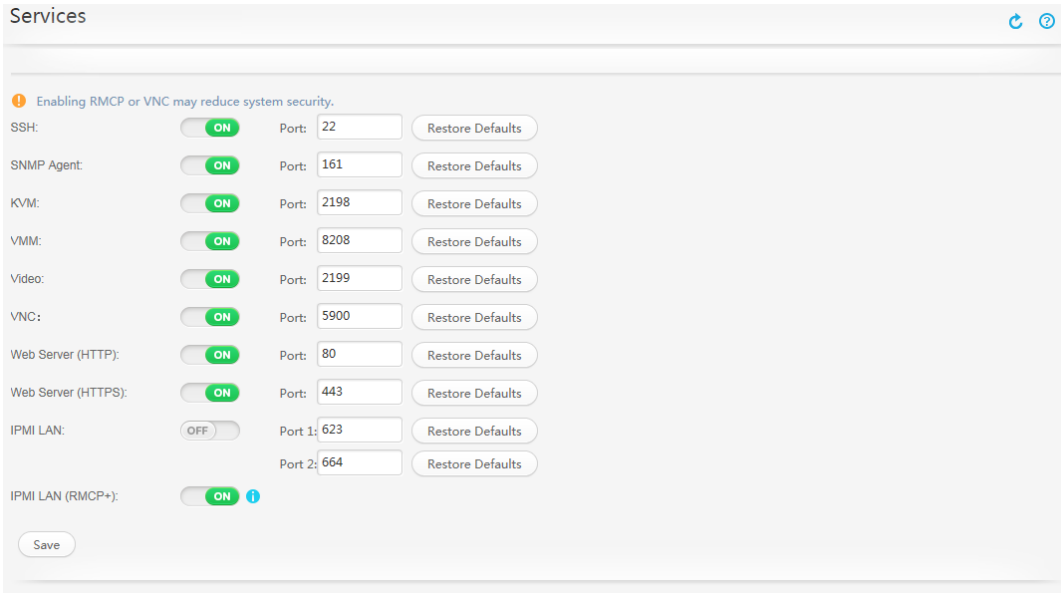
Описание функции

На странице **Services** можно просмотреть и установить сервисную информацию системы.

GUI

Выберите **Configuration** из главного меню и выберите **Services** из дерева навигации.

На экране появится страница **Services**.



Описание параметров

Табл. 3-52 Параметры на странице **Port Settings**

Параметр	Описание
Services	Системные сервисы, которые могут быть включены или отключены: • **SSH**: установка безопасного канала между локальным компьютером и сервером. iBMC поддерживает максимум пять одновременных соединений SSH. **ПРИМЕЧАНИЕ** SSH поддерживает алгоритмы шифрования: **AES128-CTR**, **AES192-CTR** и **AES256-CTR**. При входе в iBMC через SSH используется один из поддерживаемых алгоритмов шифрования. • **SNMP Agent**: трансляция и передача запросов между управляющими устройствами и управляемыми устройствами. • **KVM**: пользователи могут удаленно управлять сервером при помощи локальной клавиатуры, видео и мыши (KVM). iBMC поддерживает максимум два одновременных пользователя. • **VMM**: пользователь может использовать виртуальный DVD-дисковод или дисковод для флоппи-дисков (FDD) для управления и доступа к серверу. iBMC поддерживает только одного пользователя одновременно. **ПРИМЕЧАНИЕ** VMM – это диспетчер виртуальных машин (Virtual Machine Manager). • **Video**: пользователи могут использовать функцию воспроизведения видео. Подробная информация приведена

Параметр	Описание
	в разделе 3.5.1 Воспроизведение. iBMC поддерживает только одного пользователя одновременно. • **Web Server (HTTP)**: поддержка просмотра сети Интернет и трансляция страниц на базе протокола передачи гипертекста(HTTP – Hypertext Transfer Protocol). Для установки соединения между браузером и iBMC сервис Web Server (HTTP) включен по умолчанию. После установления соединения используется безопасный протокол HTTPS. • **VNC**: пользователи могут удаленно управлять сервером при помощи локальной клавиатуры, видео и мыши (KVM). VNC – это виртуальная сетевая консоль. Система поддерживает максимум пять одновременных пользователей. • **Web Server (HTTP)**: поддержка просмотра сети Интернет и трансляции страниц на базе протокола передачи гипертекста (HTTP – Hypertext Transfer Protocol). Для установки соединения между браузером и iBMC сервис Web Server (HTTP) включен по умолчанию. После установления соединения используется безопасный протокол HTTPS. • **Web Server (HTTPS)**: поддержка просмотра сети Интернет и трансляции страниц на базе протокола передачи гипертекста по SSL (HTTPS – Hypertext Transfer Protocol over Secure Socket Layer). iBMC поддерживает максимум четыре одновременных соединения HTTPS. • **IPMI LAN (RMCP)**: интерфейс интеллектуальной платформы управления по LAN (IPMI – Intelligent Platform Management Interface) с поддержкой протокола удаленного управления (RMCP – Remote Management Control Protocol). Использование сервиса IPMI LAN (RMCP) может привести к определенным рискам в системе безопасности. Вместо этого, в целях обеспечения безопасности рекомендуется использовать сервис IPMI LAN(RMCP+). Сервис IPMI LAN (RMCP) отключен по умолчанию. • **IPMI LAN (RMCP+)**: интерфейс интеллектуальной платформы управления по LAN (IPMI – Intelligent Platform Management Interface) с поддержкой протокола удаленного управления (RMCP+ – Remote Management Control Protocol). **ПРИМЕЧАНИЕ** Только серверы V5 поддерживают сервис VNC. Нажмите  или  и нажмите **Save**. •  : включение сервера. •  : отключение сервера
Port	Номер порта, используемый сервисом. Диапазон значений: от 1 до 65535

Параметр	Описание
	Значение по умолчанию: • SSH: **22** • SNMP Agent: **161** • KVM: **2198** • VMM: **8208** • Video: **2199** • VNC: **5900** • Web Server (HTTP): **80** • Web Server (HTTPS): **443** • IPMI LAN (RMCP): **623** для порта 1 (первичный порт) и **664** для порта 2 (вторичный порт) • IPMI LAN (RMCP+): Сервисы RMCP+ и RMCP используют один и тот же порт. **ПРИМЕЧАНИЕ** • Если в качестве порта браузера, не установленного по умолчанию, сконфигурирован порт HTTP/HTTPS, то браузеры Chrome или Firefox не могут использовать данный порт для установления соединения. Для решения данной проблемы необходимо настроить браузер таким образом, чтобы он мог использовать порты не по умолчанию для установления соединений. • Одновременное отключение сервисов SSH, HTTPS, RMCP и RMCP+ может привести к разъединению сети. Если все сервисы отключены, то можно подключиться к серверу по последовательному порту и включить веб-сервисы. • Только серверы V5 поддерживают сервис VNC.

Процедура

Настройка номеров портов для системных сервисов

1. В строке меню выберите **Configuration**.
2. В дереве навигации слева выберите **Services**.

   На экране справа появится страница **Services**.
3. Включите необходимые системные сервисы и установите номера портов для этих сервисов.

   Подробная информация приведена в Табл. 3-52.

ПРИМЕЧАНИЕ

Для использования номеров портов по умолчанию для сервисов, нажмите **Restore Default** после порта.

Сервис	Действие
SSH	Введите номер порта в текстовом поле **Port**.
SNMP Agent	Введите номер порта в текстовом поле **Port**.
KVM	Введите номер порта в текстовом поле **Port**.

Сервис	Действие
VMM	Введите номер порта в текстовом поле **Port**.
Video	Введите номер порта в текстовом поле **Port**.
VNC	Введите номер порта в текстовом поле **Port**.
Web Server (HTTP)	Введите номер порта в текстовом поле **Port**.
Web Server (HTTPS)	Введите номер порта в текстовом поле **Port**.
IPMI LAN (RMCP)	1. Введите номер порта в текстовом поле **Port 1**. 2. Введите номер порта в текстовом поле **Port 2**.
IPMI LAN(RMCP+)	Сервисы RMCP+ и RMCP используют один и тот же порт.

4. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

3.7.7 Страница System

Описание

На странице **System** приведена следующая информация:

- Информация о простом протоколе управления сетью (SNMP – Simple Network Management Protocol)
- Версии системы безопасности транспортного уровня (TLS – Transport Layer Security)
- Функции управления пользователями на обслуживающей стороне
- Период ожидания веб-сессий и режим установления веб-сессий
- Местоположение устройств
- Пороговые значения использования ЦП и памяти
- FusionPar
- Режим RAID

GUI

Выберите **Configuration** из главного меню и выберите **System** из дерева навигации.

На экране появится страница **System**.

Рис. 3-29 Страница **System** RH8100 V3

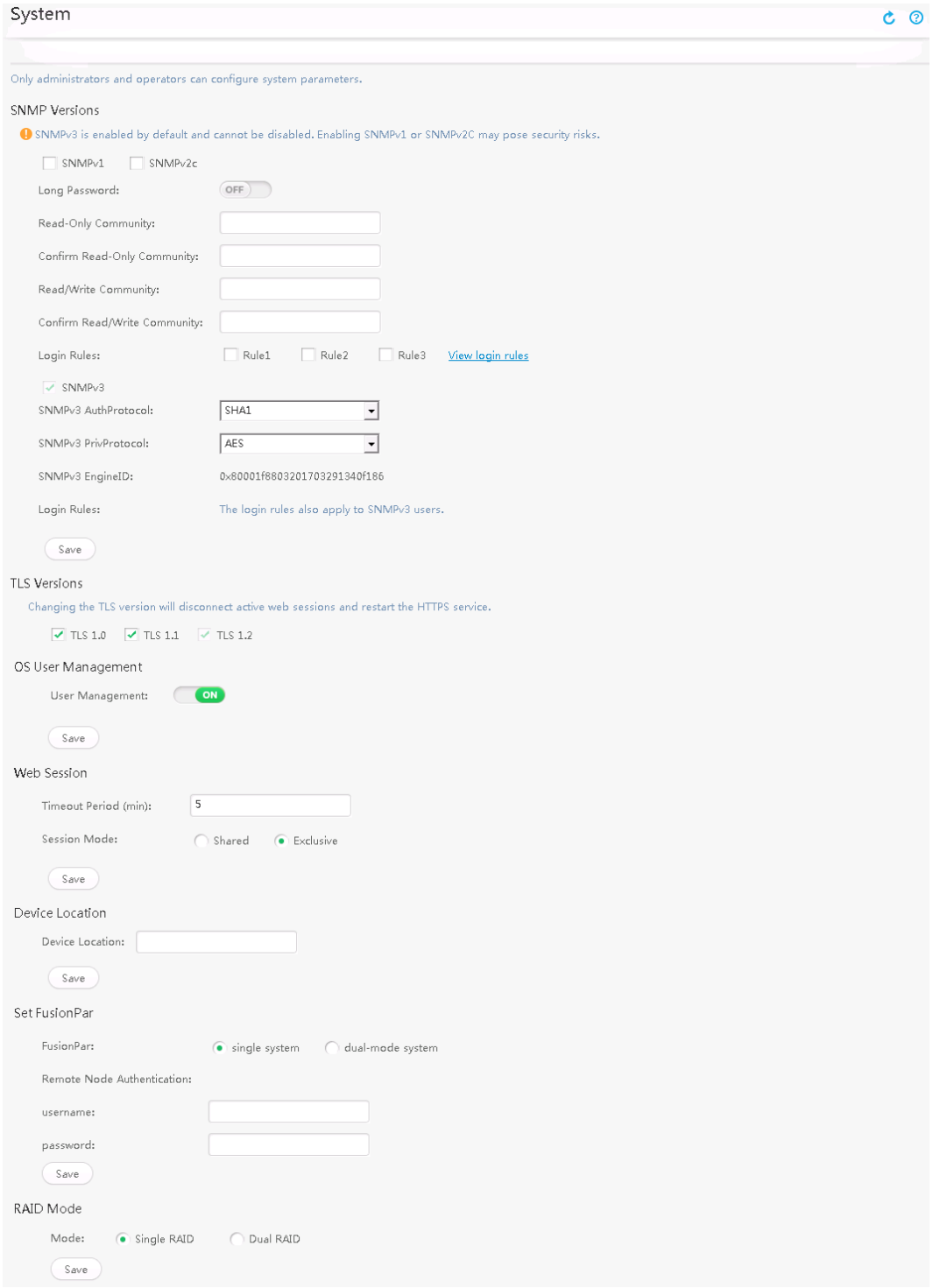


Рис. 3-30 Страница **System** RH5885 V3

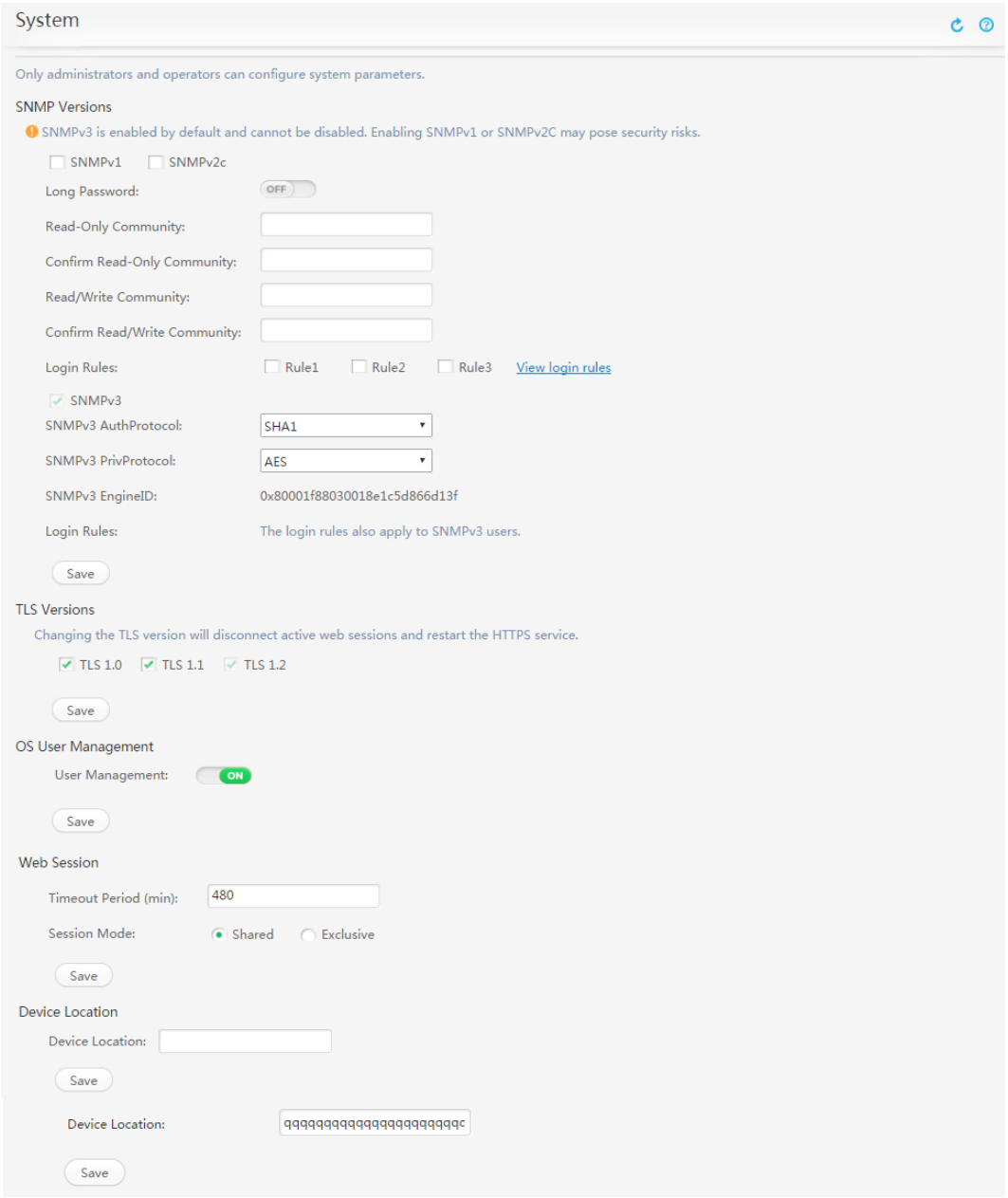


Рис. 3-31 Страница **System** других стоечных серверов V3

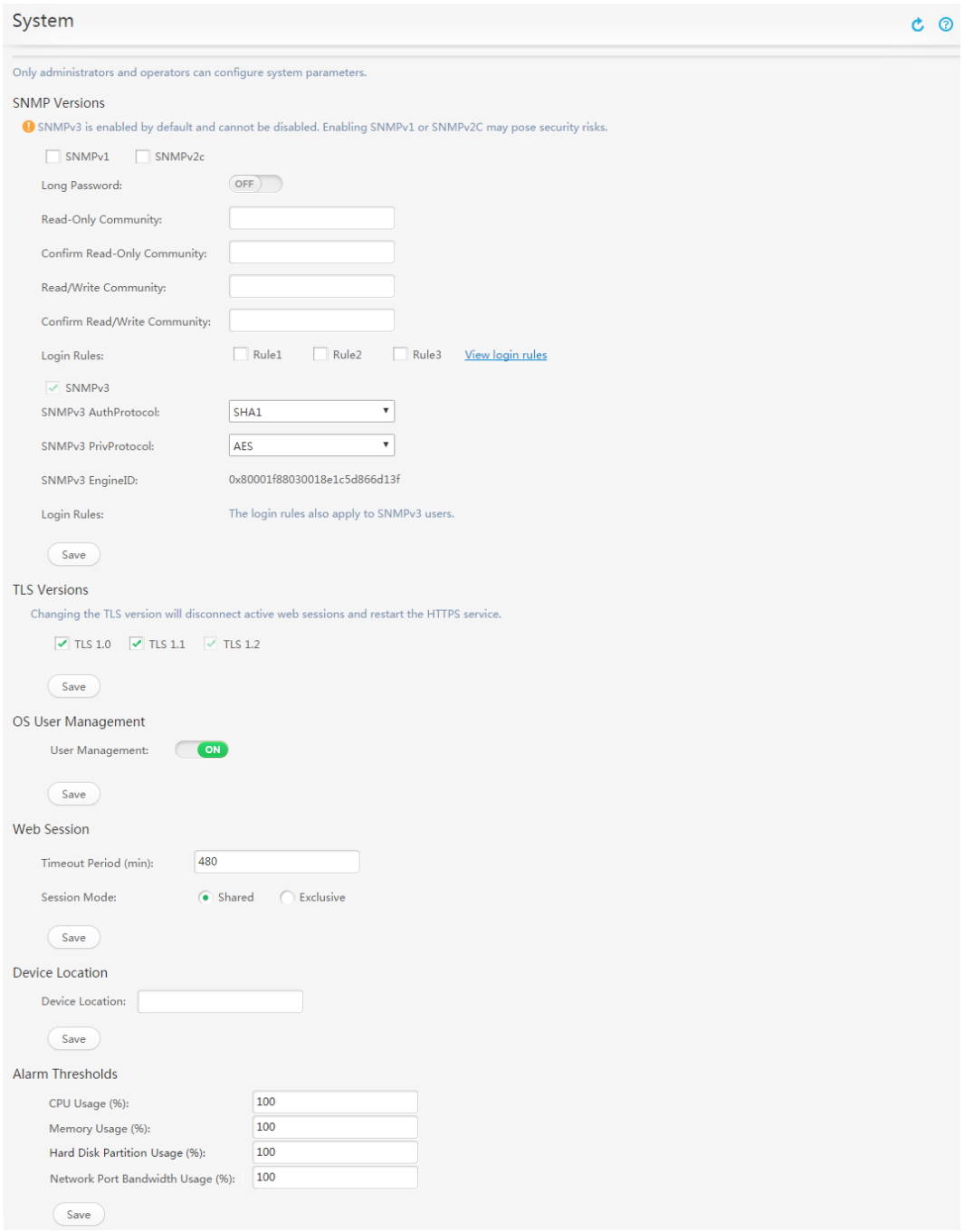
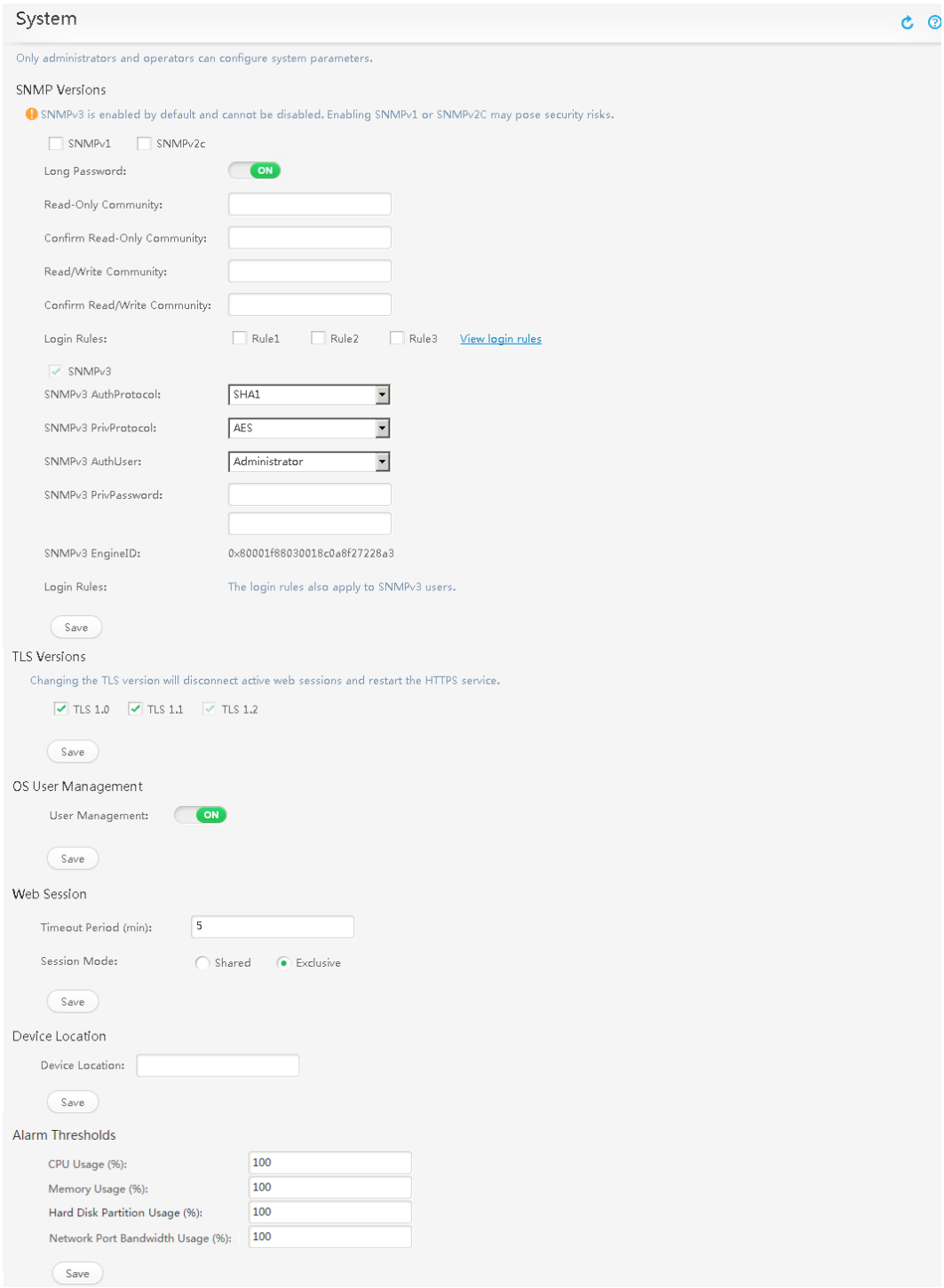


Рис. 3-32 Страница **System** стоечных серверов V5



Описание параметров

Табл. 3-53 Параметры на странице **System**

Параметр	Описание
SNMP Version	
SNMPv1	Первая официальная версия SNMP, определенная в документе RFC 1157. Использование SNMPv1 может привести к появлению определенных рисков безопасности. Для обеспечения безопасности рекомендуется использовать SNMPv3. **ПРИМЕЧАНИЕ** Если SNMPv1 включен, то рекомендуется изменить имя сообщества SNMP при первом входе в систему и периодически менять его в дальнейшем.
SNMPv2c	Усовершенствованная версия SNMPv2. SNMPv2c – это экспериментальный протокол, который определен в RFC 1901 и который поддерживает архитектуру управления на базе сообществ. Использование SNMPv2c может привести к появлению определенных рисков безопасности. Для обеспечения безопасности рекомендуется использовать SNMPv3. **ПРИМЕЧАНИЕ** Если сервис SNMPv2c включен, то рекомендуется изменить имя сообщества SNMP при первом входе в систему и периодически менять его в дальнейшем.
Long Password	Включение или отключение функции длинного пароля. Включите данную функцию при вводе минимум 16 символов для имен сообществ. Значение по умолчанию:  для серверов V3 и  для серверов V5. Нажмите  или  и нажмите **Save**. •  : включение функции Long Password. •  : отключение функции Long Password.
Read-Only Community	Имя сообщества только для чтения. Значение по умолчанию: **roAdmin12#$** для серверов V3 и **roAdministrator@9000** для серверов V5. **ПРИМЕЧАНИЕ** Данный параметр является действительным только при использовании SNMPv1 или SNMPv2c. Если проверка сложности пароля отключена, то в качестве значения может использоваться строка длиной от 1 до 32 символов, состоящая из букв, цифр и специальных символов (за исключением пробелов). Если проверка сложности пароля включена, то пароль должен соответствовать следующим требованиям:

Параметр	Описание
	• Содержать от 8 до 32 символов. • Содержать, как минимум, один из следующих специальных символов: `~!@#$%^&*()-_=+\\|[{}];:'",<.>/? • Содержать символы, как минимум, двух видов: – Заглавные буквы: от A до Z – Строчные буквы: от a до z – Цифры: от 0 до 9 • Не должен содержать пробелы.
Confirm Read-Only Community	Имя сообщества только для чтения, повторно введенное для подтверждения.
Read/Write Community	Имя сообщества чтения-записи. Значение по умолчанию: **rwAdmin12#$** для серверов V3 и **rwAdministrator@9000** для серверов V5. **ПРИМЕЧАНИЕ** Данный параметр является действительным только при использовании SNMPv1 или SNMPv2c. Если проверка сложности пароля отключена, то в качестве значения может использоваться строка длиной от 1 до 32 символов, состоящая из букв, цифр и специальных символов (за исключением пробелов). Если проверка сложности пароля включена, то пароль должен соответствовать следующим требованиям: • Содержать от 8 до 32 символов. • Содержать, как минимум, один из следующих специальных символов: `~!@#$%^&*()-_=+\\|[{}];:'",<.>/? • Содержать символы, как минимум, двух видов: – Заглавные буквы: от A до Z – Строчные буквы: от a до z – Цифры: от 0 до 9 • Не должен содержать пробелы.
Confirm Read/Write Community	Имя сообщества чтения-записи, повторно введенное для подтверждения.
Login Rules	Правила входа для пользователей SNMPv1 и SNMPv2c. Правила входа устанавливаются на странице **Configuration** > **Security**. Для просмотра правил входа нажмите `Click here to ensure that log rules have been configured and enabled`.
SNMPv3	Третья официальная версия SNMP с улучшенными возможностями безопасности и удаленным конфигурированием по сравнению с более ранними версиями.

Параметр	Описание
	ПРИМЕЧАНИЕ SNMPv3 включен по умолчанию и его нельзя отключить.
SNMPv3 AuthProtocol	Алгоритм аутентификации SNMPv3. Значение: • MD5 • SHA1 Значение по умолчанию: **SHA1** **ПРИМЕЧАНИЕ** • Данная настройка используется только для **SNMPv3** и **SNMPv3 Trap**. • Использование MD5 может привести к появлению определенных рисков безопасности. Рекомендуется использовать значение SHA1.
SNMPv3 PrivProtocol	Алгоритм шифрования SNMPv3. Значение: • DES • AES Значение по умолчанию: **AES** **ПРИМЕЧАНИЕ** • Данная настройка используется только для **SNMPv3** и **SNMPv3 Trap**. • Использование DES может привести к появлению определенных рисков безопасности. Рекомендуется использовать значение AES.
SNMPv3 EngineID	Уникальный идентификатор устройства SNMP агента SNMP.
SNMPv3 AuthUser	Имя пользователя для аутентификации. **ПРИМЕЧАНИЕ** Данный параметр доступен только для серверов V5.
SNMPv3 PrivPassword	Пароль шифрования SNMP v3 для пользователя аутентификации. **ПРИМЕЧАНИЕ** Данный параметр доступен только для серверов V5. Значение по умолчанию: то же, что и пароль пользователя. Значение: • Если функция проверки сложности пароля отключена, то пароль не может быть пустым. В качестве пароля должна использоваться строка, длиной до 20 символов. • Если проверка сложности пароля включена, то пароль должен соответствовать следующим требованиям: – Содержать от 8 до 20 символов. – Содержать, как минимум, один пробел или один из следующих специальных символов: `~!@#$%^&*()-_=+|[{}];:'",<.>/? – Содержать, как минимум, символы двух видов:

Параметр	Описание
	– Строчные буквы: от a до z – Буквы: от A до Z – Цифры: от 0 до 9 – Пароль не должен совпадать с именем пользователя в прямом и обратном порядке расположения символов. – Новый пароль должен отличаться от старого пароля, как минимум, расположением двух символов. • Запрещено использовать пароль, если он находится в справочнике слабых паролей. **ПРИМЕЧАНИЕ** Во время настройки пароля шифрования SNMP v3 не выполняется проверка архивных паролей и сроков их действия. Рекомендуется, чтобы пароль шифрования SNMPv3 и пароль пользователя отличались друг от друга. Если эти два пароля не отличаются друг от друга, то это может привести к появлению определенных рисков безопасности.
Login Rules	Правила входа в систему, которые применяются к пользователям SNMPv3. Правила входа в систему, сконфигурированные и включенные для локальных пользователей, применяются и для пользователей SNMPv3.

Табл. 3-54 Другие параметры на странице **System**

Параметр	Описание
TLS Version	Версия протокола TLS, который используется для обеспечения безопасности и целостности данных, во время обмена данными между двумя приложениями. Для обеспечения безопасного соединения между веб-браузером и веб-сервером необходимо включить TLS. **ПРИМЕЧАНИЕ** • JRE 1.8 использует TLS 1.2 по умолчанию. • JRE 1.7 использует TLS 1.0 по умолчанию. Если TLS 1.0 отключен, то для JRE 1.7 не может использоваться удаленная KVM.
OS User Management	Функция управления пользователями сервисной системы. При включении данной функции, сервисная система будет отправлять команды управления, например команды добавления или удаления пользователей, управление ролями пользователей и паролями для управления пользователями iBMC. Значение по умолчанию:  В целях безопасности рекомендуется установить для данного параметра  . Нажмите  или  и нажмите **Save**.

Параметр	Описание
	•  сервисная система может управлять пользователями. •  сервисная система не может управлять пользователями.
Web Session	
Timeout Period (min)	Максимальный период простоя (в минутах), после которого будет выполннен выход пользователя из WebUI iBMC. Диапазон значений: от 5 до 480
Session Mode	Режим в котором учетная запись пользователя используется для входа в WebUI iBMC. • **Share**: каждая учетная запись пользователя может использоваться для входа в WebUI iBMC, до четырех клиентов одновременно. • **Exclusive**: каждая учетная запись пользователя может использоваться для входа в WebUI iBMC с одного клиента в любой момент времени.
Device Location	
Device Location	Информация о местоположении сервера. Значение: строка, длиной от 0 до 64 символов, состоящая из букв, цифр и следующих специальных символов: `~!@#$%^&*()-_=+|[{}];:'",<.>/? Значение по умолчанию не указано.
Alarm Thresholds	
CPU Usage (%)	Аварийное пороговое значение использования ЦП (в процентах). Если коэффициент использования ЦП превышает пороговое значение, то iBMC выдает нормальное событие. Диапазон значений: от 0 до 100 **ПРИМЕЧАНИЕ** Если на экране не отображается аварийное пороговое значение использования ЦП, то установите и запустите iBMA 2.0.
Memory Usage (%)	Аварийное пороговое значение использования памяти (в процентах). Если коэффициент использования памяти превышает пороговое значение, то iBMC выдает нормальное событие. Диапазон значений: от 0 до 100 **ПРИМЕЧАНИЕ** Если на экране не отображается аварийное пороговое значение использования памяти, то установите и запустите iBMA 2.0.
Hard Disk Partition Usage (%)	Аварийное пороговое значение использования разделов жесткого диска. Если использование разделов жесткого диска превышает пороговое значение, то iBMC выдает нормальное событие.

Параметр	Описание
	Диапазон значений: от 0 до 100 **ПРИМЕЧАНИЕ** Если на экране не отображается аварийное пороговое значение использования разделов жесткого диска, то установите и запустите iBMA 2.0.
Network Port Bandwidth Usage (%)	Аварийное пороговое значение использования полосы пропускания сетевого порта. Если использование полосы пропускания сетевого порта превышает аварийное пороговое значение, то iBMC выдает нормальное событие. Диапазон значений: от 0 до 100 **ПРИМЕЧАНИЕ** Если на экране не отображается аварийное пороговое значение использования полосы пропускания сетевого порта, то установите и запустите iBMA 2.0.
FusionPar (уникальная функция RH8100 V3)	Сервер может быть настроен для работы в качестве отдельной системы или в качестве двух независимых систем. Значения: • Single-system mode • Dual-system mode В двухсистемном режиме не поддерживается создание разделов дисков с использованием iBMC системы B. Когда RH8100 V3 переключается из двухсистемного режима в односистемный режим, сетевой порт управления в системе B не будет иметь IP-адреса, а для пароля пользователя **root** будет восстановлено значение по умолчанию (указан на табличке с маркировкой продукта). Когда RH8100 V3 переключается из односистемного режима в двухсистемный режим, а для IP-адреса сетевого порта управления в системе B будет восстановлено значение по умолчанию **192.168.2.101**. **ПРИМЕЧАНИЕ** • Если сервер RH8100 V3 работает в односистемном режиме и ОС запущена, то произойдет сбой при переключении из односистемного режима в двухсистемный. • Если сервер RH8100 V3 работает в двухсистемном режиме и ОС системы A или B запущена, то произойдет сбой при переключении из двухсистемного режима в односистемный.
RAID Mode (уникальная функция RH8100 V3)	RAID может ыбть сконфигурирован в качестве отдельного RAID или сдвоенного RAID. Значение: • Single RAID Выберите **Single RAID** если в слоте 1 установлен вычислительный модуль. • Dual RAID Выберите **Dual RAID** только если на сервере установлены два RAID-контроллера и в слотах 1 и 5 установлены вычислительные модули. **ПРИМЕЧАНИЕ**

Параметр	Описание
	• Функция **RAID Mode** не поддерживается, если сервер сконфигурирован с фронтальным модулем ввода-вывода B или C. • Если для сервера, работающего в односистемном режиме, сконфигурирован фронтальный модуль ввода-вывода A, то для параметра **RAID Mode** можно установить значение **Single RAID** или **Dual RAID**. • Если для сервера, работающего в двухсистемном режиме, сконфигурирован фронтальный модуль ввода-вывода A, то при помощи системы A iBMC можно только выполнить переключение режима RAID с single RAID на dual RAID. Система не поддерживает установку режима RAID при помощи системы B iBMC. • Перед выполнением переключения между двумя режимами RAID необходимо убедиться, что ОС запущена.

Процедура

Конфигурирование настроек SNMP

1. На странице **System** установите параметры SNMP.

   Подробная информация приведена в Табл. 3-53.

   .
2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка версии TLS

ВНИМАНИЕ

Настройка данного параметра приведет к разъединению всех себ-сеансов.

1. В области **TLS Version** на странице **System** выберите версии TLS.
2. Нажмите **Save**.

Включение сервисной системы для управления пользователями iBMC

1. В области **OS User Management** установите для параметра **User Management** значение 

.
2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка периода ожидания и режима сессий для веб-сервера

1. На странице **Web Session** установите значения параметров **Timeout Period (min)** и **Session Mode**. Подробная информация приведена в Табл. 3-54.
2. Нажмите **Save**.

Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка местоположения устройства

1. На странице **Device Location** введите информацию о местоположении сервера в **Device Location**.

   Подробная информация приведена в Табл. 3-54.

2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Установка аварийных пороговых значений

1. В области **Alarm Thresholds** установите аварийные пороговые значения для коэффициента использования ЦП и памяти.

   Подробная информация приведена в Табл. 3-54.

2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Настройка разбиения жесткого диска на разделы (эксклюзивная функция RH8100 V3)

1. В области **FusionPar** укажите информацию о разбиении жесткого диска на разделы для сервера.

   Подробная информация приведена в Табл. 3-54.

2. Нажмите **Save**.

   На экране отобразится следующая информация:

   Перед переключением между односистемным и двухсистемным режимом необходимо убедиться что все сервисные системы выключены и не выполняется обновление iBMC в данный момент времени. На экране появится сообщение «Are you sure to perform the switching?»

   Если переключение выполнено успешно, то будет выполнена перезагрузка iBMC. После переключения значения параметров имени пользователя, пароля и IP-адреса резервного iBMC вернутся к заводским настройкам.

3. Нажмите **Save**.

   Настройки разбиения жесткого диска на разделы вступят в силу только после перезагрузки iBMC.

Настройка режима RAID (эксклюзивная функция RH8100 V3)

1. На странице **System** установите режим RAID.

   Подробная информация приведена в Табл. 3-54.

2. Нажмите **Save**.

   На экране появится следующая информация:

   Перед переключением между режимом single RAID и dual RAID необходимо убедиться что все сервисные системы включены. В противном случае произойдет сбой переключения. Неправильное выполнение переключения между режимами RAID приведет к потере данных. Перед выполнением переключения необходимо извлечь все жесткие диски, или выполнять переключение между режимами RAID после включения сервисной системы и перед запуском операционной системы.

3. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

3.7.8 Страница Boot Device

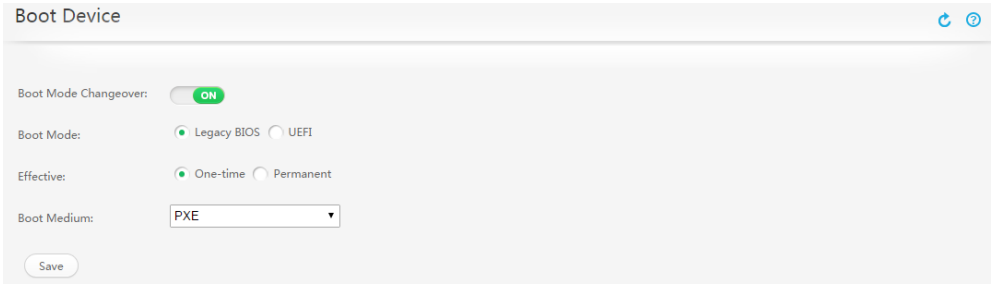
Описание

На странице **Boot Device** можно установить первое загрузочное устройство для ОС сервера.

GUI

Выберите **Configuration** из главного меню и выберите **Boot Device** из дерева навигации.

На экране появится страница **Boot Device**.



Описание параметра

Табл. 3-55 Параметры на странице **Boot Device**

Параметр	Описание
Boot Mode Changeover	Можно ли изменить режим загрузки. Нажмите OFF или ON и нажмите **Save**. • ON: Режим загрузки можно изменить. Режим загрузки, установленный в iBMC. • OFF: Режим загрузки нельзя изменить. Режим загрузки, установленный в BIOS. **ПРИМЕЧАНИЕ** • Кнопка **Boot Mode Changeover** доступна только в продуктах серии V5. • Обычные пользователи не обладают соответствующими полномочиями и они не могут выполнять переключение между режимами загрузки.
Boot Mode	• **Legacy BIOS**: запуск ОС выполняется из BIOS. • **UEFI**: запуск ОС выполняется с единого расширяемого интерфейса прошивки (UEFI – Unified Extensible Firmware Interface).

Параметр	Описание
	ПРИМЕЧАНИЕ Параметр **Boot Mode** доступен только в продуктах серии V5.
Effective	• **One-time**: загрузочное устройство используется только для загрузки при следующем перезапуске сервера. • **Permanent**: настройки параметров загрузки вступают в силу на постоянной основе.
Boot Medium	**Hard Drive**: загрузка ОС с жесткого диска.
	DVD-ROM: загрузка ОС с компакт-диска или DVD-диска.
	FDD/Removable Device: загрузка ОС с виртуального флоппи-диска (FDD) или переносного диска.
	PXE: загрузка ОС из среды выполнения предварительной загрузки (PXE – Preboot Execution Environment).
	BIOS Setup: отображение меню BIOS Setup при запуске сервера.
	No Override: загрузка ОС с первого загрузочного устройства, указанного в BIOS.

Процедура

1. В строке меню выберите **Configuration**.
2. В дереве навигации выберите **Boot Device**.

   На экране появится страница **Boot Device**.
3. Установите первое загрузочное устройство. Подробная информация приведена в Табл. 3-55.
4. Нажмите **Save**.

   Настройки выполнены успешно, если на экране появится сообщение «Save Success».

3.7.9 Сертификат SSL

Описание

На странице **SSL Certificate** можно выполнить следующие операции:

- Просмотр информации сертификата SSL (Secure Sockets Layer), которая включает информацию о корневых сертификатах, промежуточных сертификатах и сертификатах сервера.
- Настройку информации о сертификате SSL.

- Импорт новых сертификатов.

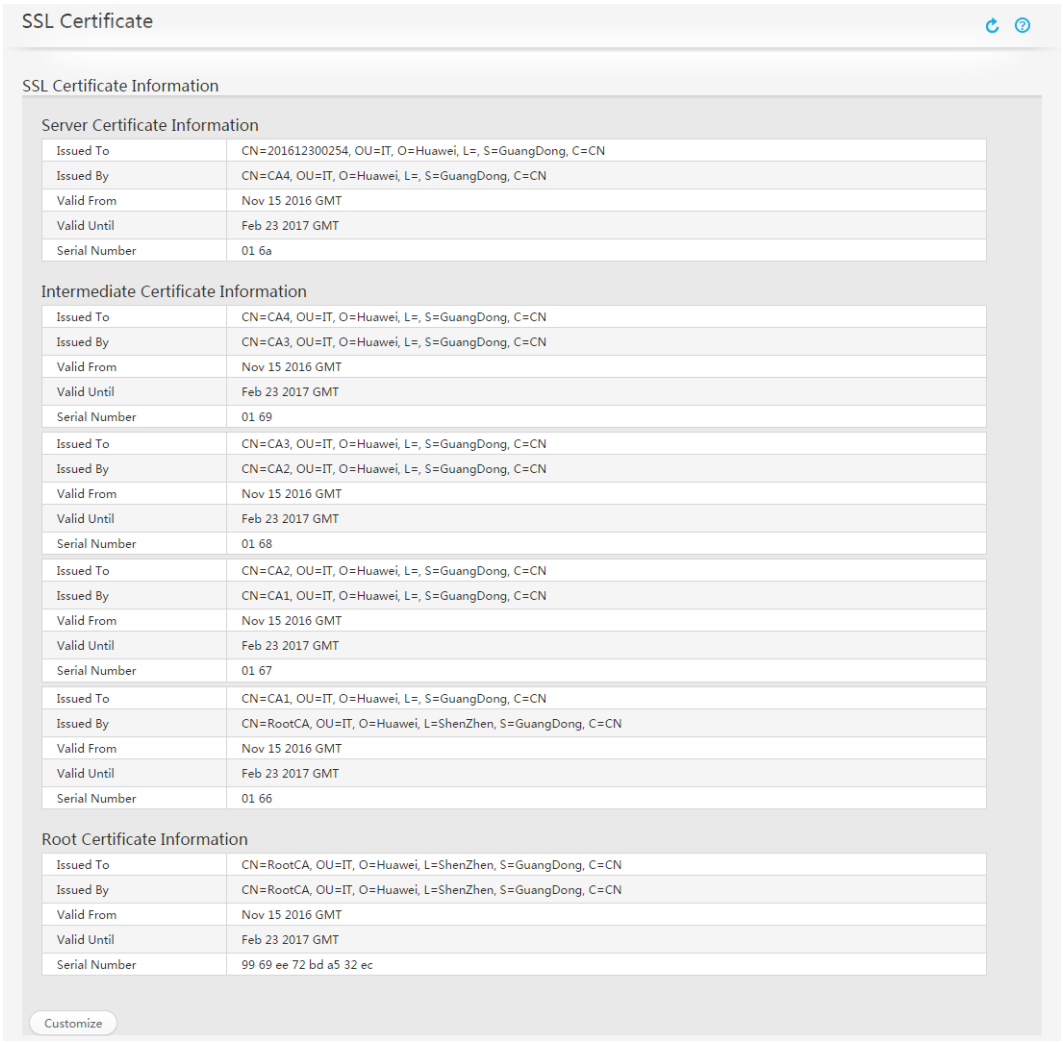
SSL-сертификат устанавливает безопасный SSL-канал по HTTPS между веб-браузером на стороне клиента и веб-сервером для передачи зашифрованных данных между клиентом и сервером и предотвращения раскрытия информации. SSL обеспечивает безопасность передаваемой информации и используется для проверки подлинности доступа к веб-сайту. Серверы позволяют заменять сертификаты SSL. В целях безопасности замените исходный сертификат и ключи на свой собственный сертификат и пару публичных и приватных ключей, и незамедлительно обновите сертификат.

ПРИМЕЧАНИЕ

Сертификат SSL может быть, как отдельным сертификатом, так и цепочкой сертификатов, состоящей из 10 уровней.

GUI

В строке меню выберите **Configuration**. В дереве навигации выберите **SSL Certificate**. На экране появится страница **SSL Certificate**.



Описание параметров

Табл. 3-56 Параметры из области **SSL Certificate Information**

Параметр	Описание
Issued To	Информация о пользователе сертификата SSL, включая: • **CN**: имя пользователя. **ПРИМЕЧАНИЕ** Установите для **CN** полное доменное имя сервера (FQDN – fully qualified domain name), т.е. *Имя хоста*.*Имя домена*. • **OU**: департамент пользователя. • **O**: компания или организация пользователя. • **L**: город пользователя. • **S**: район или регион размещения пользователя. • **C**: страна пользователя.
Issued By	Информация об органе, выдавшем сертификат SSL. Поля **Issued By** и **Issued To** должны быть одинаковыми.
Valid From	Дата вступления сертификата SSL в силу.
Valid To	Дата истечения срока действия сертификата SSL.
Serial Number	Серийный номер сертификата SSL, который используется для идентификации и переноса сертификата.

Процедура

Просмотр информации о текущем сертификате SSL

1. В дереве навигации выберите **Configuration** > **SSL Certificate**.
   На экране появится страница **SSL Certificate**.
2. В области **SSL Certificate Information** просмотрите информацию о текущем сертификате SSL, используемом сервером.

Настройка информации о сертификате SSL и импорт сертификата

ПРИМЕЧАНИЕ

Данная операция выполняется при подаче заявки на получение сертификата SSL.

1. На странице **SSL Certificate** нажмите **Customize**.
   На экране появится страница настройки информации о сертификате SSL.
2. В области **1. Generation CSR** укажите параметры настройки информации о сертификате и нажмите **Save**.
   В появившемся диалоговом окне экспортируйте файл CSR на локальный ПК.
   В Табл. 3-57 приведено описание параметров настройки информации о сертификате.

Табл. 3-57 Параметры настройки информации о сертификате

Параметр	Описание
Country(C)	Страна пользователя. Обязательный параметр. Значение состоит только из букв.
State(S)	Район или регион размещения пользователя. Значение состоит максимум из 128 символов, включая: буквы, цифры, дефисы (-), символы подчеркивания (_), десятичные точки (.), и пробелы.
City/Location(L)	Город пользователя. Значение состоит максимум из 128 символов, включая: буквы, цифры, дефисы (-), символы подчеркивания (_), десятичные точки (.), и пробелы.
Organization Name(O)	Компания пользователя. Значение состоит максимум из 64 символов, включая: буквы, цифры, дефисы (-), символы подчеркивания (_), десятичные точки (.), и пробелы.
Organizational Unit(OU)	Департамент пользователя. Значение состоит максимум из 64 символов, включая: буквы, цифры, дефисы (-), символы подчеркивания (_), десятичные точки (.), и пробелы.
Common Name(CN)	Имя пользователя. Обязательный параметр. Значение состоит максимум из 64 символов, включая: буквы, цифры, дефисы (-), символы подчеркивания (_), десятичные точки (.), и пробелы.

3. Отправьте экспортированный файл CSR органу, выдавшему сертификат SSL, для подачи заявки на получения нового сертификата SSL.

   После получения официального сертификата SSL, сохраните его на локальный ПК.

4. В области **Import Server Certificate** нажмите **Browse**, выберите файл сертификата SSL и нажмите **Import**.

   Сертификат успешно загружен на сервер, если на экране появится следующая информация:

   ```
   Certificate imported successfully. The new certificate takes effect after the iBMC is restarted.
   ```

   Нажмите **Restart Now** для незамедлительной перезагрузки iBMC или нажмите **Restart Later**, чтобы выполнить перезагрузку iBMC позже.

ПРИМЕЧАНИЕ

- Импортируемый файл сертификата должен быть в формате *.crt, *.cer, или *.pem и не должен превышать 1 МБ.
- Файл CSR связан с сертификатом сервера, выдаваемым организацией CA. Не генерируйте новый файл CSR перед импортом сертификата сервера. В противном случае новый файл CSR будет перезаписан поверх исходного файла CSR, и его нельзя будет восстановить. Новый файл CSR используется для подачи заявки на получение нового сертификата сервера от организации CA.

Импорт сертификата SSL

ПРИМЕЧАНИЕ

- Данная операция выполняется только когда сертификат SSL доступен на клиенте.
- В целях безопасности рекомендуется использовать надежный алгоритм шифрования, например RSA2048, для настраиваемого сертификата SSL.

1. На странице **SSL Certificate** нажмите **Customize**.

   На экране появится страница настройки информации о сертификате SSL.

2. В области **Import Custom Certificate (Optional)** выполняется импорт сертификата SSL.

   а. Нажмите **Browse** после **Certificate** и выберите файл сертификата SSL для импорта.

   Файл сертификата должен быть в формате .pfx и .p12 и не может превышать 100 КБ.

   б. В текстовом поле **Certificate Password** введите пароль для обеспечения безопасности в процессе передачи сертификата.

   Если сертификат защищен паролем, то необходимо ввести пароль. В противном случае сертификат не будет загружен.

   в. Нажмите **Import**.

ПРИМЕЧАНИЕ

Если размер загружаемого файла превышает 100 МБ, то на экране появится сообщение об ошибке запроса страницы. Обновите страницу.

Сертификат успешно загружен на сервер, если на экране появится следующая информация:

```
Certificate imported successfully. The new certificate takes effect after the iBMC is restarted.
```

Нажмите **Restart Now** для незамедлительной перезагрузки iBMC или нажмите **Restart Later**, чтобы выполнить перезагрузку iBMC позже.

Добавление корневого сертификата к браузеру

ПРИМЕЧАНИЕ

Если сертификат SSL сгенерирован самостоятельно (не получен из организации CA), то проверьте, есть ли на браузере корневой сертификат .

Далее, в качестве примера, для описания порядка просмотра и добавления корневого сертификата в браузер, используется Internet Explorer.

1. Откройте Internet Explorer.
2. На панели инструментов выберите **Tools** > **Internet Options**.

   На экране появится диалоговое окно **Internet Options**.

3. На вкладке **Content** нажмите **Certificates**.

   На экране появится диалоговое окно **Certificates**.

4. На вкладке **Trusted Root Certification Authorities** проверьте, указан ли орган, выдавший сертификат SSL.
   - Если да, перейдите к 5.
   - Если нет, перейдите к 6.
5. Проверьте не истек ли срок действия сертификата SSL.

- Если да, перейдите к 6.
- Если нет, перейдите к 7.

6. На вкладке **Trusted Root Certification Authorities** нажмите **Import**.

   Выполните импорт корневого сертификата, в соответствии с инструкциями.

7. Откройте Internet Explorer снова и проверьте отображается ли значок в адресной строке.
   - Если да, то никаких действий больше выполнять не требуется.
   - Если нет, обратитесь за помощью в службу техподдержки Huawei.

3.7.10 Импорт/Экспорт

Описание функции

На странице **Import/Export** можно выполнить импорт и экспорт iBMC, BIOS и файлов конфигурации RAID-контроллера.

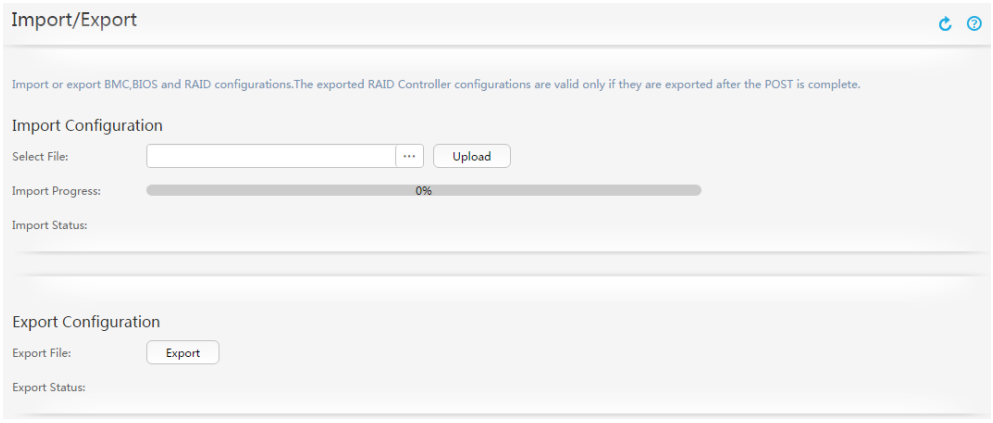
ПРИМЕЧАНИЕ

- Настройки RAID-контроллера вступят в силу только после завершения самотестирования при запуске системы (POST – system power-on self test).
- Если импортированные элементы конфигурации связаны с изменением версии TLS или сетевой конфигурации, установленные веб-соединения будут разъединены. Если на экране появится сообщение «Import failed», то необходимо выполнить повторный вход на WebUI iBMC и просмотреть журнал операций, чтобы определить успешность выполнения операции импортирования.

Данную операцию может выполнять только администратор системы.

Описание страницы

Перейдите к **Configuration** из меню и выберите **Import/Export** из дерева навигации.



Процедура

Импорт файла конфигурации

1. В области **Import Configuration** нажмите ... после **Select File** и выберите файл конфигурации для испорта.
2. Нажмите **Upload**.

Импорт файла конфигурации выполнен успешно, если на экране появится сообщение «File imported successfully. The configuration will take effect after iBMC is restarted».

3. Файл конфигурации успешно загружен на сервер, если на экране появится следующая информация:

```
File imported successfully. The configuration will take effect after iBMC is restarted.
```

Нажмите **Restart Now** для незамедлительной перезагрузки iBMC или нажмите **Restart Later**, чтобы выполнить перезагрузку iBMC позже.

Экспорт файла конфигурации

1. Нажмите **Export** в области **Export Configuration**, укажите каталог для сохранения экспортируемого файла и нажмите **OK**.

   Экспорт файла конфигурации выполнен успешно, если на экране появится сообщение «File exported successfully.

3.8 Система

3.8.1 Страница Operation Logs

Описание

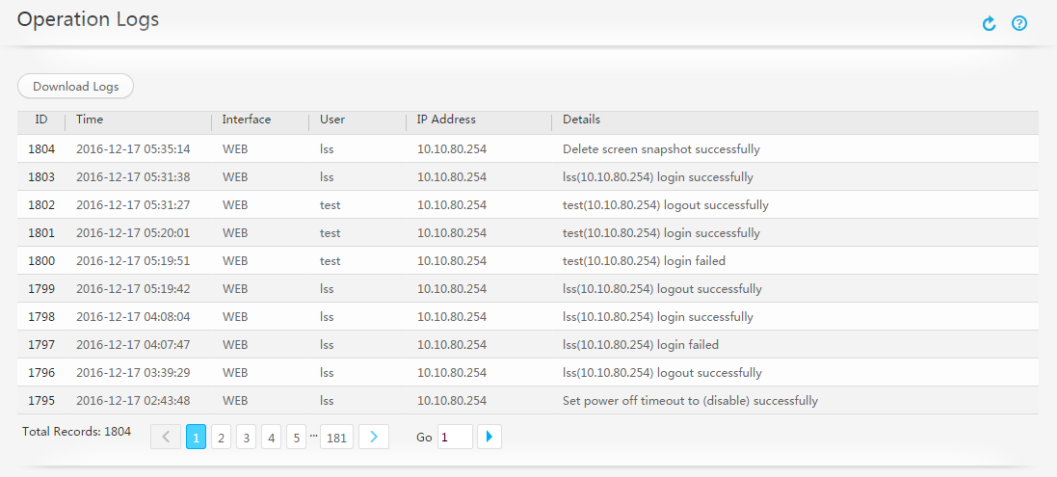
Страница **Operation Logs** позволяет просматривать и загружать журналы, записанные во время выполнения системных операций, включая информацию о запуске системы, изменении статусов, а также настройках, выполненных пользователями на iBMC. iBMC предоставляет объем 200 КБ для хранения до 2000 записей журнала операций.

ПРИМЕЧАНИЕ

Журналы операций, которые записывают успешные операции запуска системы, выключения и сброса, показывают, что данные операции были успешно инициированы, однако это не обязательно означает, что операции были успешно выполнены на оборудовании.

Описание страницы

В строке меню выберите **System**. В дереве навигации выберите **Operation Logs**. На экране появится страница **Operation Logs**.



Описание параметра

Табл. 3-58 Параметры на странице **Operation Logs**

Параметр	Описание
ID	ID операции. Последняя выполненная операция представлена в списке первой.
Time	Время выполнения операции.
Interface	Интерфейс, с которого была выполнена операция.
User	Пользователь, выполнивший операцию. Значение параметра **User** отображается как **N/A** (имя пользователя не отображается) в следующих случаях: • Кнопка идентификации пользователя (UID – User Identification) или кнопка питания нажаты. • В качестве интерфейса используется SNMPv1 или SNMPv2c. • В качестве интерфейса используется IPMI и IP-адрес :**HOST** или **SMM** (журнал записывает IPMI-сообщение, отправленное сервисной системой). • Для серверов V3 IP-адрес iBMC и пароль пользователя **root** были изменены с помощью джампера. Для серверов V5 IP-адрес iBMC и пароль пользователя **Administrator** были сброшены с помощью джампера. • Выполнена замена компонента в «горячем» режиме.
IP Address	IP-адрес, с которого была выполнена операция. • Значение **SMM** говорит о том, что операция была запущена управляющим модулем. • Значение **HOST** говорит о том, что операция была запущена сервисной системой. • Значение **127.0.0.1** говорит о том, что операция была запущена локальным хостом, в следующих случаях: – Кнопка UID, райзер-кнопка памяти или кнопка питания

Параметр	Описание
	нажаты. – В качестве интерфейса используется ЖК-дисплей или локальный последовательный порт. – Для серверов V3 IP-адрес iBMC и пароль пользователя **root** были изменены с помощью джампера. Для серверов V5 IP-адрес iBMC и пароль пользователя **Administrator** были изменены с помощью джампера. – Выполнена замена компонента в «горячем» режиме.
Details	Подробная информация об операции. Если после обновления с использованием WebUI iBMC или CLI или IPMI, происходит перезагрузка iBMC, то регистрация операции выполняется в следующем формате: • Interface: N/A • User: N/A • IP address: 127.0.0.1 • Details: The iBMC was successfully reset due to an upgrade.
Примечание: Если значения параметров **User** и **IP address** не удалось проанализировать, то они отображаются как **unknown**.	

Процедура

Страница Operation Logs

1. В строке меню выберите **System**.
2. В дереве навигации выберите **Operation Logs**.

   На экране появится страница **Operation Logs**.

Загрузка журнала операций

1. Нажмите **Download Logs**.

   На экране появится диалоговое окно **Save**.
2. Выберите локальный каталог для сохранения загруженного файла журнала операций.
3. Нажмите **Save**.

   Загруженный файл будет сохранен в указанный каталог.

3.8.2 Страница Run Logs

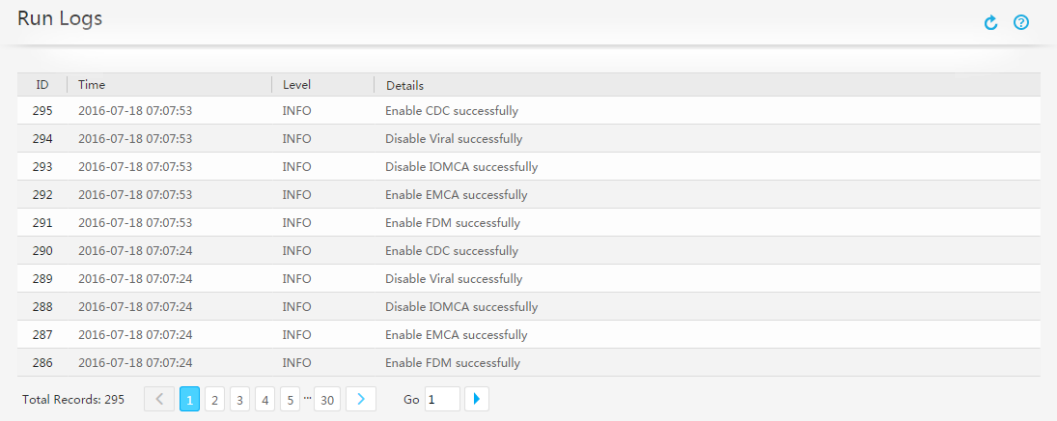
Описание

На странице **Run Logs** представлены журналы RAS. iBMC предоставляет объем 200 КБ для хранения до 2000 записей рабочего журнала.

GUI

Выберите **System** из главного меню и выберите **Run Logs** из дерева навигации.

На экране появится страница **Run Logs**.



Описание параметра

Табл. 3-59 Параметры на странице **Run Logs**

Параметр	Описание
Time	Время появления ошибки при выполнении операции.
Level	Уровень серьезности аварийного сигнала ошибки при выполнении операции.
Details	Подробная информация об ошибке при выполнении операции.

Процедура

1. В строке меню выберите **System**.
2. В дереве навигации выберите **Run Logs**.
   На экране появится страница **Run Logs**.
3. Просмотрите все журналы выполнения операций.

3.8.3 Страница Security Logs

Описание

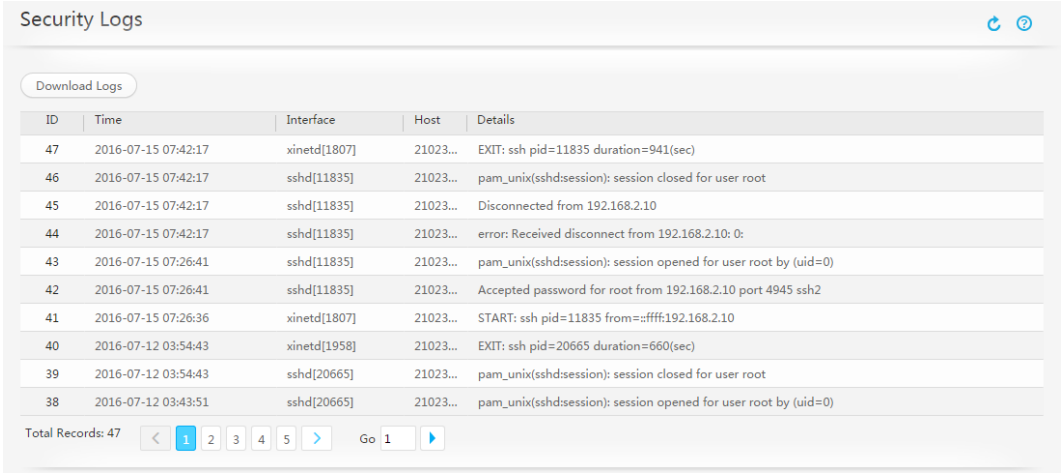
iBMC предоставляет объем 200 КБ для хранения до 2000 записей журнала безопасности. На странице **Security Logs** можно выполнить следующие операции:

- Просмотр журналов входа и выхода iBMC через последовательный порт SSH и просмотр параметров настройки операций.
- Просмотр журналов о запросе и выполнении операций по SNMP.
- Загрузка журнала безопасности.

Описание страницы

Выберите **System** из главного меню и выберите **Security Logs** из дерева навигации.

На экране появится страница **Security Logs**.



Описание параметра

Табл. 3-60 Параметры на странице **Security Logs**

Параметр	Описание
ID	ID операции. Последняя выполненная операция представлена в списке первой.
Time	Время выполнения операции.
Interface	Интерфейс, с которого была выполнена операция.
Host	Имя хоста iBMC.
Details	Подробная информация об операции.

Процедура

Просмотр журналов безопасности

1. На вкладке **Security Logs** просмотрите журналы входа и выхода iBMC.

Загрузка журнала безопасности

1. На странице **Security Logs** нажмите **Download Logs**.
   На экране появится диалоговое окно **Save**.
2. Укажите каталог для сохранения загруженного файла.
3. Нажмите **Save**.
   Загруженный файл будет сохранен в указанный каталог.

3.8.4 Страница Work Records

Описание

На странице **Work Records** можно добавлять и просматривать рабочие записи. iBMC предоставляет объем 200 КБ для хранения до 2000 записей рабочего журнала.

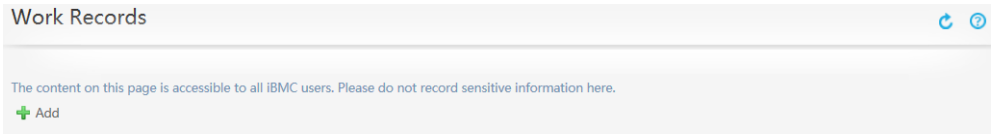
ПРИМЕЧАНИЕ

- Рабочие записи содержат максимум 255 символов. Система поддерживает добавление максимум 20 рабочих записей. Если количество записей превышает 20, то система будет выполнять перезапись новых рабочих записей поверх существующих.
- Рабочие записи могут просматривать и редактировать все пользователи.

GUI

Перейдите к **System** из главного меню и выберите **Work Records** из дерева навигации.

На экране появится страница **Work Records**.



Процедура

Добавление рабочей записи

1. В строке меню выберите **System**.
2. В дереве навигации выберите **Work Records**.
   На экране появится страница **Work Records**.
3. Нажмите **Add** и добавьте рабочую запись в появившемся текстовом поле.
4. Нажмите **Save**.

Изменение рабочей записи

1. Нажмите  для изменения рабочей записи в текстовом поле.
2. Нажмите **Save**.

Удаление рабочей записи

1. Нажмите  для удаления рабочей записи.
   На экране появится следующая информация:

   ```
   Are you sure you want to perform this operation?
   ```
2. Нажмите **Yes**.

3.8.5 Страница Online Users

Описание

На странице **Online Users** можно выполнить следующие операции:

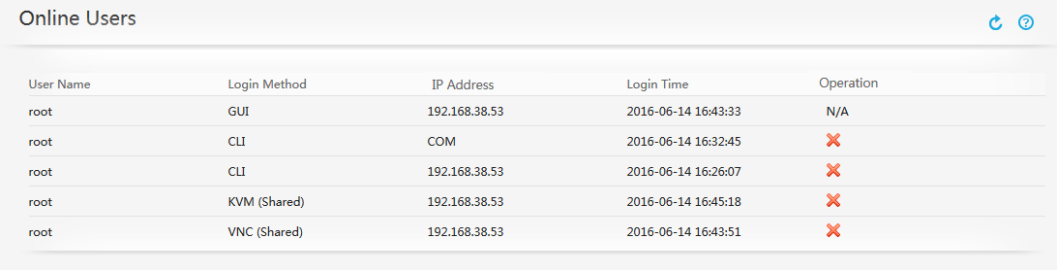
- Просмотр пользователей, которые выполнили вход в iBMC.
- Принудительный выход онлайн-пользователей из системы.

Только администратор может выполнить принудительный выход онлайн-пользователей из системы.

Описание

Выберите **System** из главного меню и выберите **Online Users** из дерева навигации.

На экране появится страница **Online Users**.



Описание параметров

Табл. 3-61 Параметры на странице **Online Users**

Параметр	Описание
User Name	Имя пользователя, вошедшего в iBMC или KVM.
Login Method	Способ входа пользователя. Для выбора доступны следующие режимы: • **GUI**: пользователь вошел в iBMC через WebUI. • **CLI**: пользователь вошел в iBMC через CLI. • **KVM**: пользователь вошел в ОС через удаленную виртуальную консоль. • **Redfish**: пользователь вошел в iBMC через интерфейс Redfish. • **VNC**: пользователь вошел в ОС через виртуальную сетевую консоль. Данный способ входа поддерживают только серверы V5.
IP Address	IP-адрес для подключения и входа в iBMC. Значения: IP-адрес или **COM** **ПРИМЕЧАНИЕ** Значение **COM** Говорит о том, что пользователь вошел в iBMC через последовательный порт. Через последовательный порт одновременно войти в систему могут максимум пять пользователей.
Login Time	Время входа пользователя в iBMC.
Operation	Принудительный выход пользователя.

Процедура

Просмотр онлайн-пользователей

1. В строке меню выберите **System**.
2. В дереве навигации выберите **Online Users**.

   На экране появится страница **Online Users**.
3. На странице **Online Users** представлена информация обо всех пользователях, которые вошли в iBMC.

Выход пользователя

1. На странице **Online Users** нажмите  после пользователя.

   На экране появится диалоговое окно с просьбой подтвердить ваши действия.
2. Нажмите **OK**.

   Будет выполнен принудительный выход пользователя из системы, и информация о пользователе больше не будет отображаться на странице **Online Users**.

3.8.6 Страница Firmware Upgrade

Описание

На странице **Firmware Upgrade** можно выполнять следующие операции:

- Просмотр информации о версии встроенного ПО сервера.
- Перезагрузка iBMC.
- Переключение между активными и резервными образами iBMC.
- Обновление встроенного ПО сервера.

iBMC имеет два образа, развернутые в режиме активный-резервный. Сначала выполняется обновление активного образа, и уже затем резервного. После обновления резервного образа выполняется перезапуск iBMC и автоматическое переключение на резервный файл образа. Если автоматическое переключение не выполняется, то необходимо вручную переключить сервисы на резервный образ.

ВНИМАНИЕ

- В процессе обновления не отключайте питание сервера и не выполняйте перезагрузку iBMC.
- После обновления встроенного ПО iBMC необходимо выполнить перезагрузку iBMC, чтобы новая версия вступила в силу. Однако нет никакой необходимости выполнять перезагрузку сервера. Поэтому это никак не повлияет на услуги, работающие на сервере.
- Не нужно выполнять перезагрузку сервера после обновления встроенного ПО ЖК-дисплея и блока питания. Однако необходимо выполнить перезагрузку сервера, чтобы новая версия вступила в силу, после обновления следующего встроенного ПО:
- Встроенное ПО BIOS
- Встроенное ПО сложной программируемой логической интегральной схемы (CPLD – Complex programmable logical device) материнской платы
- Встроенное ПО CPLD платы ЦП (встроенное ПО, за исключением RH8100 V3)
- Встроенное ПО CPLD фронтальной платы ввода-вывода (встроенное ПО, за исключением RH8100 V3)
- Встроенное ПО CPLD задней платы ввода-вывода (встроенное ПО, за исключением RH8100 V3)
- Встроенное ПО объединительной платы жестких дисков.
- Встроенное ПО CPLD райзер-карты PCIe с возможностью замены в «горячем» режиме

Перед обновлением встроенного ПО необходимо обновить все работающие сервисы на сервере. Это позволит предотвратить прерывание обслуживания при перезагрузке сервера.

- Для обновления встроенного ПО CPLD передней платы ввода-вывода в двухсистемном режиме, необходимо войти в систему B iBMC, а затем войти в систему A iBMC, чтобы обновить встроенное ПО CPLD задней платы ввода-вывода.

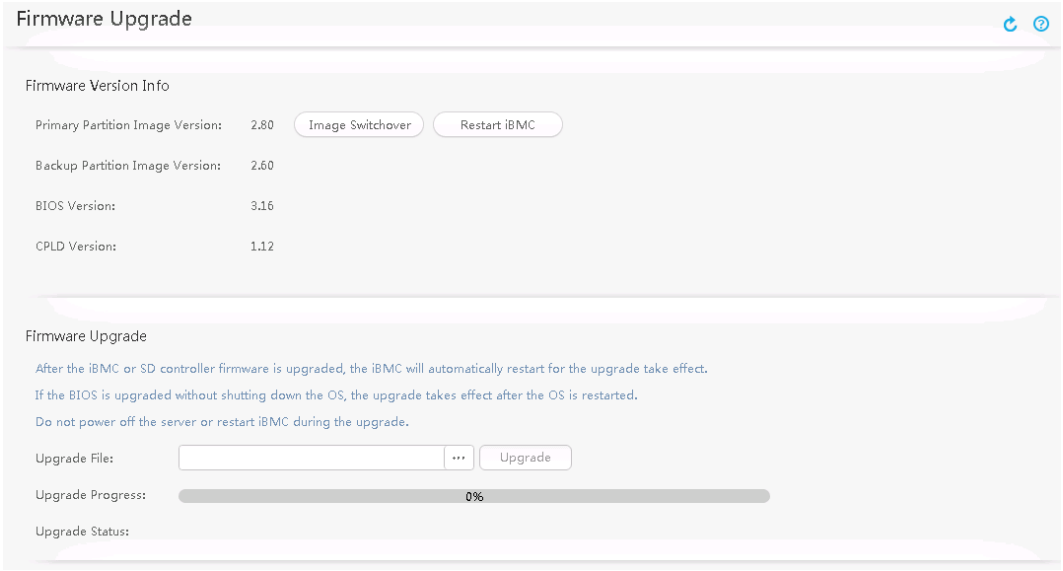
В iBMC Help приведено описание порядка обновления встроенного ПО на WebUI iBMC. Для получения более подробной информации о порядке получения пакетов обновлений встроенного ПО и справочной документации, обратитесь к руководству, поставляемому вместе с сервером.

На Рис. 3-33 показан процесс обновления встроенного ПО.

Рис. 3-33 Процесс обновления встроенного ПО

GUI

В строке меню выберите **System**. В дереве навигации выберите **Firmware Upgrade**. На экране появится страница **Firmware Upgrade**.



Описание параметров

Табл. 3-62 Параметры на странице Firmware Upgrade

Параметр	Описание
Firmware Version Info	
Primary Partition Image Version	Номер версии встроенного ПО iBMC основного раздела диска.
Backup Partition Image Version	Номер версии встроенного ПО iBMC резервного раздела диска.
BIOS Version	Номер версии BIOS.
CPLD Version	Версия встроенного ПО CPLD.
Image Switchover	Переключение между образами iBMC основного и резервного раздела дисков.
Restart iBMC	Перезапуск iBMC, чтобы обновления вступили в силу.
Обновление встроенного ПО **ПРИМЕЧАНИЕ** • В процессе обновления встроенного ПО iBMC серверов V3, KVM, функции создания скриншотов и функции видео недоступны. • Для применения встроенного ПО после завершения обновления iBMC или SD-карты, будет выполнен перезапуск iBMC. • Если обновление BIOS выполняется без выключения ОС, то обновление вступит в силу после перезагрузки ОС. • Не выключайте питание сервера или не выполняйте перезагрузку iBMC в процессе обновления.	
Upgrade File	Выберите локальный каталог, в котором будет храниться пакет с обновлениями встроенного ПО. Пакет с обновлениями встроенного ПО это файл в формате *.hpm.

Параметр	Описание
	Методы настройки: 1. Нажмите  . Выберите локальный каталог, в котором будет храниться пакет с обновлениями встроенного ПО. Нажмите **Open**. На экране появится страница **Firmware Upgrade**. 2. Нажмите **Upgrade**. На экране появится следующее сообщение: `Are you sure you want to perform this operation?` 3. Нажмите **Yes** и iBMC начнет обновление.
Upgrade Progress	Процесс обновления встроенного ПО.
Upgrade Status	Статус обновления встроенного ПО.

Процедура

Просмотр версий встроенного ПО

1. В строке меню выберите **System**.
2. В дереве навигации выберите **Firmware Upgrade**.

   На экране появится страница **Firmware Upgrade**.
3. Посмотрите версии iBMC, BIOS и CPLD.

Обновление встроенного ПО iBMC.

1. На странице **Firmware Upgrade** выберите пакет с обновлениями из **Upgrade File**, в соответствии с методами, представленными в Табл. 3-62.
2. Нажмите **Upgrade**.

   На экране отобразится следующая информация:

   ```
   Are you sure you want to perform this operation?
   ```
3. Нажмите **Yes**.

   iBMC начинает обновление а в области **Upgrade Progress** отображается процесс обновления.

   После завершения обновления на экране под **Upgrade Status** будет отображено следующее сообщение:

   ```
   The upgrade is complete.
   ```
4. Повторите шаги с 1 по 3 для обновления активного образа iBMC.

Обновление другого встроенного ПО

1. На странице **Firmware Upgrade** выберите пакет с обновлениями из **Upgrade File**, в соответствии с методами, представленными в Табл. 3-62.
2. Нажмите **Upgrade**.

   На экране отобразится следующая информация:

   ```
   Are you sure you want to perform this operation?
   ```
3. Нажмите **Yes**.

iBMC начинает обновление а в области **Upgrade Progress** отображается процесс обновления.

После завершения обновления на экране под **Upgrade Status** будет отображено следующее сообщение:

```
The upgrade is complete.
```

После завершения обновления встроенного ПО BIOS на экране под **Upgrade Status** будет отображено следующее сообщение:

```
File upload successfully. The upgrade takes effect automatically after the next power-off or restart
```

Выполнение переключения образов для встроенного ПО iBMC

Выполнять переключение образов встроенного ПО iBMC рекомендуется только при необходимости. Переключение образов выполняется опционально в процессе обновления.

1. На странице **Firmware Upgrade** нажмите **Image Switchover**.

   На экране появится следующее сообщение:

   ```
   iBMC will restart after the switchover is complete. Continue?
   ```

2. Нажмите **Yes**.

   Используется исходный файл образа резервной копии встроенного ПО iBMC.

   На экране появится страница со следующим сообщением:

   ```
   iBMC is restarting. Please wait a few minutes.
   ```

   После перезапуска iBMC на экране появится страница входа.

Перезапуск iBMC

Выполняйте перезапуск iBMC при необходимости. Данная операция не является обязательной в процессе обновления.

1. На странице **Firmware Upgrade** нажмите **Restart iBMC**.

   На экране отобразится следующая информация:

   ```
   Are you sure you want to perform this operation?
   ```

2. Нажмите **Yes**. После этого будет выполнен перезапуск iBMC.

   На экране появится страница со следующим сообщением:

   ```
   iBMC is restarting. Please wait a few minutes.
   ```

   После перезапуска iBMC на экране появится страница входа.

3.8.7 Страница Language Update

Описание

На странице **Language Update** можно установить и удалить пакет языков, изменить язык, используемый в iBMC.

ПРИМЕЧАНИЕ

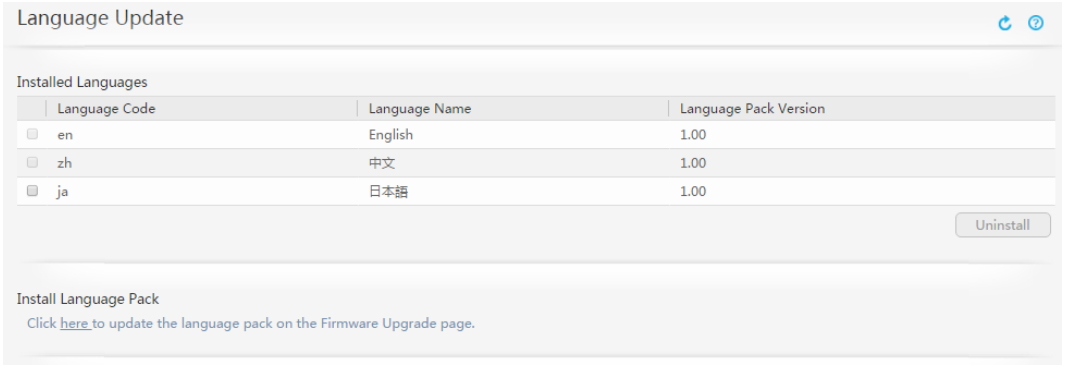
- Только iBMC версии 2.56 и более поздние версии поддерживают установку и удаление пакета языков.
- Только администраторам и пользователям, которые могут выполнять обычные настройки, разрешено устанавливать или удалять пакет языков.
- Только пакет с японским языком можно удалить и обновить.

- Пакеты с английским и китайским языком удалить нельзя.

GUI

Выберите **System** из главного меню и выберите **Language Update** из дерева навигации.

На экране появится страница **Language Update**.



Параметры

Табл. 3-63 Страница **Language Update**

Параметры	Описание
Installed Languages	
Language Code	Код языка. Например **en** означает английский язык, **zh** – это китайский, а **ja** японский язык.
Language Name	Язык, соответствующий коду.
Language Pack Version	Версия пакета языков, установленная на iBMC.
here	Нажмите **here** для перехода со страницы **Firmware Upgrade** на обновление пакета языков.

Процедура

Запрос установленных пакетов языков

1. В главном меню выберите **System**.
2. Из дерева навигации выберите **Language Update**.
   На экране появится страница **Language Update**.
   Под **Installed Language Packs** представлены установленные пакеты языков.

Установка или обновление пакета с языками

1. Загрузка целевого пакета языков.
   a. Перейдите на веб-сайт корпоративной поддержки компании Huawei.
   б. Выберите **Support** > **Software Download** > **Server**.

На экране появятся серверные продукты.

в. Выберите целевой сервер.

На экране появится страница выбранного сервера.

г. Перейдите на вкладку **Downloads.**

На экране появится список версий сервера.

д. Выберите необходимую версию.

е. Загрузите пакет языков, например **2288H_V5-iBMC-LANG-JA-V257.zip** на локальный ПК.

2. Обновление пакета языков.

а. Выполните вход в веб-интерфейс iBMC.

б. Выберите **System** > **Firmware Upgrade**.

На экране появится страница **Firmware Upgrade**.

в. Выберите пакет целевого языка из **Upgrade File**.

г. Нажмите **Upgrade**.

На экране появится следующая информация:

```
Are you sure you want to perform this operation?
```

д. Нажмите **Yes**.

iBMC начинает обновление пакета языков, а в области **Upgrade Progress** появится процесс обновления.

После завершения обновления на экране под **Upgrade Status** появится следующее сообщение:

```
The upgrade is complete.
```

Выберите язык из выпадающего списка в врехнем правом углу страницы.

Удаление пакета языков

1. На вкладке **Language Update** под **Installed Language Packs** выберите пакет языков для удаления.
2. Нажмите **Uninstall**.

Пакет языков успешно удален, если на экране появится сообщение «Operation successful».

3.9 Страница Remote Console

Описание

На странице **Remote Console** можно увидеть максимальное количество сеансов и количество активных сеансов удаленной консоли, виртуальные носители и сервис VNC, а также получить доступ к ОС сервера, используя удаленную виртуальную консоль.

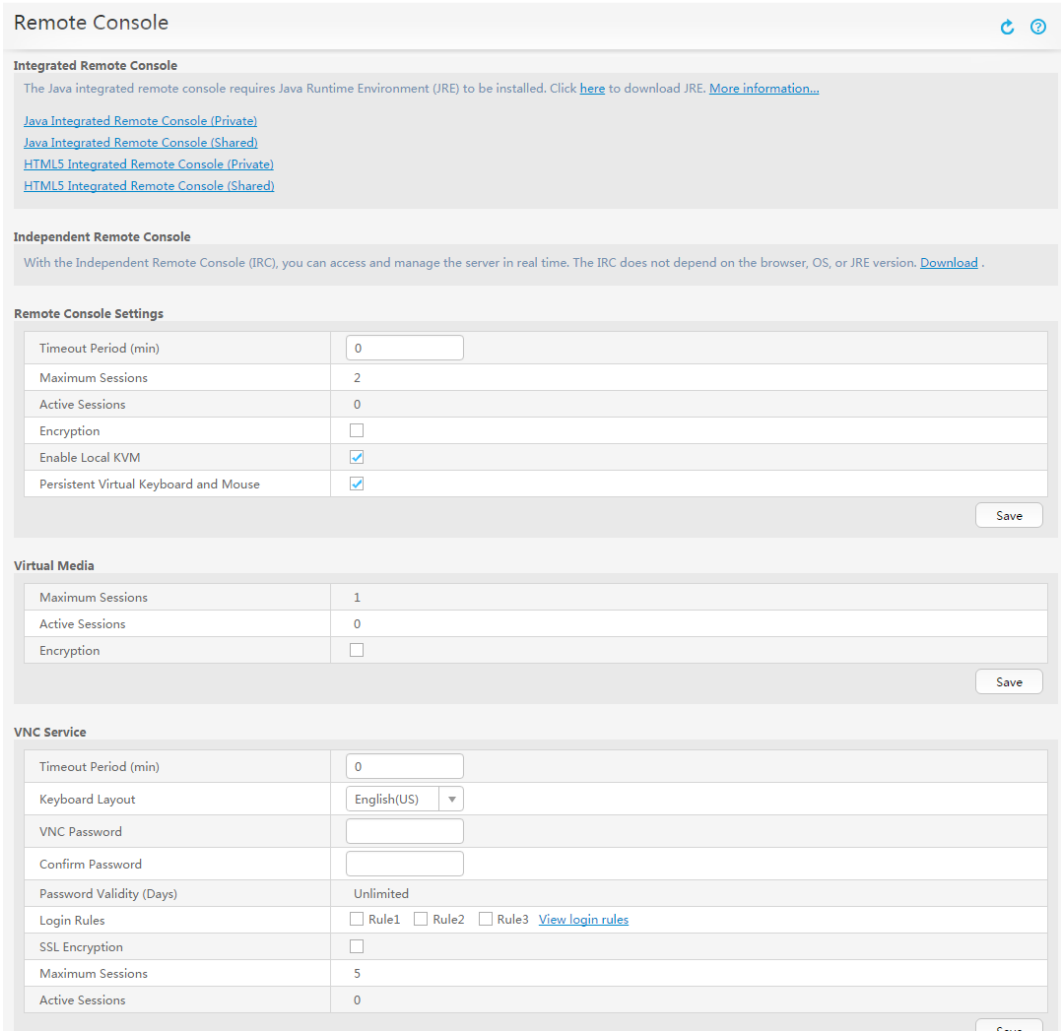
ПРИМЕЧАНИЕ

Только серверы V5 поддерживают сервис VNC.

GUI

В главном меню выберите **Remote Console**.

На экране появится страница **Remote Console**.



Описание параметра

Табл. 3-64 Параметры на странице **Remote Console**

Параметр	Описание
Интегрированная удаленная консоль	
Here	Для работы встроенной удаленной консоли Java необходимо установить среду Java Runtime Environment (JRE). Нажмите **Here** для ее загрузки.
More information	Нажмите **More information** для получения информации о порядке устранения общих проблем удаленной консоли.
HTML5 Integrated Remote Console (Private)	Приватный режим позволяет только одному пользователю использовать удаленную консоль для доступа и выполнения операций на сервере.
HTML5 Integrated Remote Console	В режиме совместного использования два пользователя могут одновременно использовать удаленную консоль для доступа и

Параметр	Описание
(Shared)	выполнения операций на сервере. Каждый пользователь может просматривать операции, выполняемые другим пользователем.
HTML5 Integrated Remote Console (Private)	Приватный режим позволяет только одному пользователю использовать удаленную консоль для доступа и выполнения операций на сервере.
HTML5 Integrated Remote Console (Shared)	В режиме совместного использования два пользователя могут одновременно использовать удаленную консоль для доступа и выполнения операций на сервере. Каждый пользователь может просматривать операции, выполняемые другим пользователем.
Независимая удаленная консоль	
Download	Независимая удаленная консоль (IRC – Independent Remote Console) позволяет пользователям получить доступ и управлять сервером в режиме реального времени. IRC не зависит ни от версии браузера, ни от ОС, ни от версии JRE.
Настройки удаленной консоли	
Timeout Period (min)	Максимальное время простоя (в минутах) после последней операции (включая операции чтения данных на виртуальном CD-диске) на удаленной консоли. Если в течение определенного периода времени ни будет выполнена ни одна операция, то будет выполнено автоматическое разъединение удаленной консоли. Диапазон значений: от 0 до 480 Значение **0** означает неограниченное время.
Maximum Sessions	Максимальное количество пользователей, которым разрешено использовать удаленную консоль для подключения к серверной системе. Параметр имеет фиксированное значение **2**.
Active Sessions	Количество пользователей, подключенных в настоящее время к серверу через удаленную консоль. Для получения на страницу **Online Users** и получения информации о пользователях, нажмите на номер.
Encryption	Функция шифрования данных KVM перед передачей. При включении данной функции выполняется шифрование данных с использованием алгоритма AES128 перед передачей между сервером и клиентом. По умолчанию шифрование данных KVM отключено. Для целях безопасности рекомендуется включить данную функцию. **ПРИМЕЧАНИЕ** KVM-шифрование может быть отключено только после отключения шифрования VMM и сохранения настроек.
Enable local KVM	Функция включения или отключения локальной KVM. • При включении **Enable local KVM** локальная KVM и удаленная виртуальная консоль могут использоваться для

Параметр	Описание
	доступа к серверу. • Если параметр **Enable local KVM** не выбран, то локальная KVM недоступна. Только удаленная виртуальная консоль будет использоваться для доступа к серверу. По умолчанию параметр **Enable local KVM** выбран.
Persistent Virtual Keyboard and Mouse	Функция включения или отключения постоянного подключения клавиатуры и мыши. • При включении данной функции виртуальная клавиатура iBMC и мышь будут всегда подключены к USB-контроллеру UHCI iBMC. • Если данная функция отключена, то виртуальная клавиатура iBMC и мышь динамически подключаются к контроллеру UHCI iBMC только при запуске приложения Remote Console и подключении к iBMC. Это позволяет экономить электроэнергию, когда ОС сервера не работает, соответственно нет необходимости в подключении виртуальной USB-клавиатуры и мыши. По умолчанию параметр **Persistent Virtual Keyboard and Mouse** выбран.
Виртуальные носители	
Maximum Sessions	Максимальное количество одновременных пользователей, которым разрешено использовать виртуальные носители (виртуальные DVD-диски или флоппи-диски) удаленной виртуальной консоли. Параметр имеет фиксированное значение **1**.
Active Sessions	Количество пользователей, которым разрешено использовать виртуальные носители (виртуальные DVD-диски или флоппи-диски) удаленной виртуальной консоли. Для получения информации о пользователях перейдите на страницу **Online Users** и нажмите номер.
Encryption	Функция шифрования данных виртуального носителя перед передачей. При включении функции выполняется шифрование данных виртуального носителя с использованием алгоритма AES128 перед передачей между сервером и клиентом. По умолчанию шифрование данных виртуального носителя отключено. Для целях безопасности рекомендуется включить данную функцию. **ПРИМЕЧАНИЕ** VMM-шифрование может быть включено только после включения шифрования KVM и сохранения настроек.
Сервис VNC Сервис VNC позволяет подключаться к ОС сервера и выполнять операции на клавиатуре, видео и мыши сервера. **ПРИМЕЧАНИЕ**	

Параметр	Описание
Только серверы V5 поддерживают сервис VNC.	
Timeout Period (min)	Максимальное время ожидания (в минутах) после выполнения последней операции на интерфейсе VNC. Если в течение определенного периода времени не будет выполнена ни одна операция, то произойдет автоматическое разъединение от интерфейса VNC. Диапазон значений: от 0 до 480 Значение **0** означает неограниченное время.
Keyboard Layout	Раскладка клавиатуры ОС, управляемой VNC. Значение: • Japanese • English Значение по умолчанию: **Japanese**
VNC Password	Пароль для входа в интерфейс VNC. • Если проверка сложности пароля отключена, то в качестве пароля VNC может использоваться строка, длиной от 1 до 8 символов. • Если проверка сложности пароля включена, то в качестве пароля VNC может использоваться строка, состоящая из 8 символов. Пароль VNC также должен соответствовать определенным требованиям: – содержать, как минимум, один пробел или один из следующих специальных символов: `~!@#$%^&*()-_=+|[{}];:'",<.>/? – Должен содержать, как минимум, символы следующих двух видов: – Заглавные буквы: от A до Z – Строчные буквы: от a до z – Цифры: от 0 до 9
Confirm Password	Имя сообщества для подтверждения. **ПРИМЕЧАНИЕ** После нажатия **Save** на экране появится диалоговое окно **User Password**. Пароль VNC можно установить успешно только после ввода пароля для входа в iBMC.
Password Validity (Days)	Срок действия пароля VNC.
Login Rule	Правила входа, применяемые к пользователям VNC. Для просмотра настроенных правил нажмите **View login rules**.
SSL Encryption	Функция включения или отключения шифрования SSL. В целях безопасности рекомендуется включить данную функцию. Если шифрование SSL отключено, то клиент VNC запускает процесс удаленного буфера кадров (RFB – Remote

Параметр	Описание
	Frame Buffer). **ПРИМЕЧАНИЕ** Если шифрование SSL включено, то только клиенты VNC с включенной функцией шифрования SSL могут подключаться к ОС сервера. Если клиент VNC не поддерживает функцию шифрования SSL, то для реализации шифрования SSL используется туннелирование SSL. По умолчанию параметр **SSL Encryption** выбран.
Maximum Sessions	Максимальное количество пользователей, которым разрешено получить доступ к интерфейсу VNC. Параметр имеет фиксированное значение **5.**
Active Sessions	Количество пользователей одновременно получивших доступ к интерфейсу VNC. Для получения информации о пользователях перейдите на страницу **Online Users** и нажмите номер.

В Табл. 3-65 приведено описание операционных систем, браузеров, и сред JRE, которые необходимы для использования удаленной виртуальной консоли.

ПРИМЕЧАНИЕ

- Для загрузки JRE необходимой версии, перейдите на официальный веб-сайт ПО.
- При использовании JRE версии 1.7 или 1.8 и если приложение удаленной консоли останавливается при попытке его запустить, обратитесь к разделу 3.10.1 Сбой при открытии удаленной виртуальной консоли.

Табл. 3-65 Рабочая среда

ОС	Браузер	JRE
Windows 7 (32-bit) Windows 7 (64-bit)	Internet Explorer 9.0/10.0/11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0/54.0	
	Google Chrome 21.0/44.0	
Windows 8 (32-bit) Windows 8 (64-bit)	Internet Explorer 10.0/11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0/54.0	
	Google Chrome 21.0/44.0	
Windows 10 (64-bit)	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0/54.0	
Windows 2012 R2 64-бит	Internet Explorer 11.0	JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0/54.0	
Windows 2016 (64-bit)	Internet Explorer 11.0	JRE 1.8 U45

ОС	Браузер	JRE
	Mozilla Firefox 39.0/54.0	JRE 1.8 U144
Windows Server 2008 R2 (64-bit)	Internet Explorer 9.0/10.0/11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0/54.0	
	Google Chrome 21.0/44.0	
Windows Server 2012 (64-bit)	Internet Explorer 10.0/11.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0/54.0	
	Google Chrome 21.0/44.0	
64-битная Red Hat 6.0	Mozilla Firefox 39.0/54.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
MAC X v10.7	Safari 8.0	JRE 1.7 U45 JRE 1.8 U45 JRE 1.8 U144
	Mozilla Firefox 39.0/54.0	

Процедура

Открытие удаленной виртуальной консоли

ПРИМЕЧАНИЕ

При вводе пароля ОС или BIOS на виртуальной удаленной консоли:

- Если используемая клавиатура соответствует настройкам клавиатуры ОС, то используйте фактическую клавиатуру.
- Если используемая клавиатура не соответствует настройкам клавиатуры ОС, то используйте клавиатуру ОС.

Открыть удаленную консоль можно любым из следующих способов:

- На странице **Remote Console** нажмите **Java Integrated Remote Console (Shared)**, **Java Integrated Remote Console (Private)**, **HTML5 Integrated Remote Console (Shared)** или **HTML5 Integrated Remote Console (Private)**.

  В режиме совместного использования два пользователя могут одновременно использовать удаленную консоль для доступа и выполнения операций на сервере. Каждый пользователь может просматривать операции, выполняемые другим пользователем.

  Приватный режим позволяет только одному пользователю использовать удаленную консоль для доступа и выполнения операций на сервере. При выборе данного режима, функция создания скриншотов вручную будет недоступна.
- Откройте ьраузер и введите:
  - https://*IPaddress*/remoteconsole
  - https://*IPaddress*/kvmvmm.asp
  - https://*IPaddress*/bmc/pages/remote/kvm.php

- https://*IPaddress*/login.html?redirect_type=1

ПРИМЕЧАНИЕ

IPaddress – это IP-адрес iBMC.

На экране появится страница входа WebUI iBMC. Выполните следующие операции:

а. Выберите язык.

б. Введите имя пользователя и пароль.

Имя пользователя и пароль по умолчанию для серверов V3: **root** и **Huawei12#$**, соответственно. Имя пользователя и пароль по умолчанию для серверов V5: **Administrator** и **Admin@9000**, соответственно.

в. Выберите **This iBMC** или **LDAP** при необходимости.

г. Нажмите **Log In**.

Просмотр количества сеансов связи

1. В главном меню выберите **Remote Console**.

   На экране появится страница **Remote Console**.

2. На ней будет отображена информация о максимальном количестве сеансво связи и количестве активных сеансов связи удаленной консоли, виртуальных носителях и сервисе VNC.

3. Выберите номер сеанса связи для переключения на страницу **Online Users** и просмотрите информацию о пользователях.

Настройки удаленной консоли

1. На странице **Remote Console** установите параметры в области **Remote Console Setting**.

   Подробная информация приведена в Табл. 3-64.

2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

Включение шифрования при передачи информации виртуальных носителей

На странице **Remote Console** выберите **Encryption** в области **Virtual Media** и нажмите **Save**.

Настройка сервиса VNC

1. На странице **Remote Console** установите параметры в области **VNC Service**.

   Подробная информация приведена в Табл. 3-64.

2. Нажмите **Save**.

   Настройка выполнена успешно, если на экране появится сообщение «Operation successful».

3.9.1 Удаленная виртуальная консоль Java

Описание

Благодаря удаленной виртуальной консоли Java, вы можете получить доступ к серверу и управлять сервером дистанционно, устанавливать или восстановить ОС, а также устанавливать драйверы на сервер.

Благодаря встроенной удаленной консоли можно:

- Использовать клавиатуру и мышь локального ПК для дистанционного управления сервером.
- Включить сервер для удаленного доступа к локальному ПК по сети, с использованием флоппи-диска (FDD) или DVD-диска. Для сервера использование виртуального FDD или виртуального DVD-диска это то же самое, что и использование физического USB-устройства.

ПРИМЕЧАНИЕ

В качестве носителя на локальном ПК может использоваться локальный жесткий диск FDD или DVD-диск, или флоппи-диск, или файл образа DVD, который хранится на локальном ПК или сетевом диске.

В Табл. 3-66 приведено описание значков на экране KVM.

Табл. 3-66 Значки на экране KVM

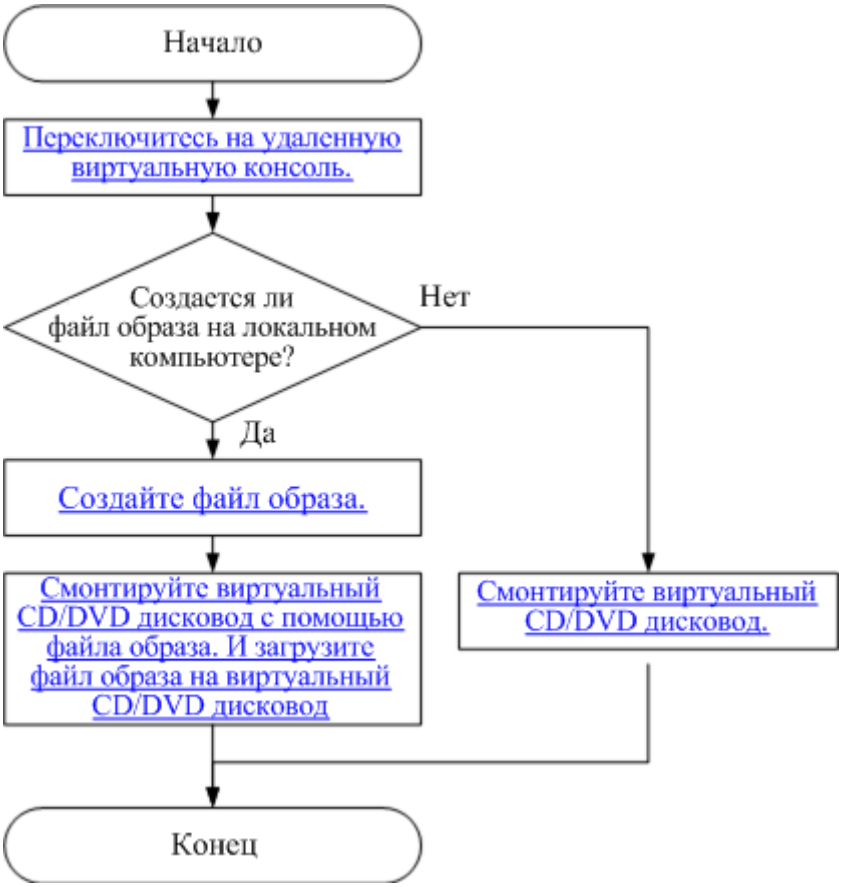
Значок	Описание
	Блокировка панели инструментов.
	Скрытие панели инструментов.
	Рабочий стол сервера в полноэкранном режиме. **ПРИМЕЧАНИЕ** Для переключения с полноэкранного в оконный режим, переместите указатель в верхнюю часть полноэкранного режима или нажмите **Ctrl+Alt+Shift** для отображения панели инструментов и нажмите  .
	Синхронизация местоположения мыши. **ПРИМЕЧАНИЕ** Данная кнопка доступна на панели инструментов только когда рабочий стол сервера отображается в полноэкранном режиме.
	Изменение режима мыши. **ПРИМЕЧАНИЕ** Данная кнопка доступна на панели инструментов только когда рабочий стол сервера отображается в полноэкранном режиме.
	Возврат отображения рабочего стола сервера к оконному режиму. **ПРИМЕЧАНИЕ** Данная кнопка доступна на панели инструментов только когда рабочий стол сервера отображается в полноэкранном режиме.
	Отображение меню управления питанием, включая:

Значок	Описание
	• Power On • Forced Power Off • Normal Power Off • Forced System Reset • Forced Power Cycle
	Запись видео операций, выполняемых на сервере.
	Управление мышью сервера. Поддерживаются следующие операции: • **Mouse Acceleration** Ускорение мыши рабочего стола сервера для синхронизации работы с мышью на локальном ПК. **ПРИМЕЧАНИЕ** В более ранних версиях, чем SUSE 12, данная операция не поддерживается. • **Single Mouse** Скрытие мыши локального ПК и отображение мыши рабочего стола сервера. • **Mouse & Key Reset** Имитация удаления и установки USB-клавиатуры и мыши. Когда клавиатура и мышь на рабочем столе сервера перестают отвечать, нажмите **Mouse & Key Reset** для восстановления. Настройки по умолчанию: **Mouse Acceleration**
	Выбор и использование виртуального DVD-диска.
	Выбор и использование виртуального жесткого диска FDD.
	Использование DVD-диска или FDD для создания файла образа.
	Отправка или настройка комбинации клавиш. Поддерживаются следующие комбинации клавиш: • **Ctrl+Shift**: переключение между способами ввода. • **Ctrl+Esc**: расширение или сворачивание меню **Start**. • **Ctrl+Alt+Del**: блокировка окна ОС, выход пользователя, изменение пароля, открытие Диспетчера задач или перезагрузка сервера. • **Alt+Tab**: переключение между работающими приложениями. • **Ctrl+Space**: включение или отключение способов ввода. • **ResetKeyboad**: моделирование отжатия кнопки на клавиатуре.
Image Clarity	Настройка четкости изображения рабочего стола сервера.

Значок	Описание
num ■	Статус клавиши **Num Lock** сервера.
caps ■	Статус клавиши **Caps Lock** сервера.
scroll ■	Статус клавиши **Scroll Lock** сервера. При нажатии клавиш **Ctrl+S** по ошибке после перехода к символьному режиму Linux, экран будет заблокирован. Нажмите **Scroll Lock** для разблокировки экрана. **ПРИМЕЧАНИЕ** Если при управлении сервером с использованием удаленной виртуальной консоли возникла ошибка ввода клавиатуры, сначала проверьте статус значков num ■, caps ■ и scroll ■.
	Справочная информация.
Примечание: Значки на экране удаленной виртуальной консоли и их функции различаются в зависимости от используемой модели сервера.	

На Рис. 3-34 показан процесс использования виртуального DVD-диска на панели инструментов. Процесс использования файла образа или виртуального FDD не отличаются от данного процесса.

Рис. 3-34 Процедура



GUI

Выберите **Remote Console** из главного меню и нажмите **Java Integrated Remote Console (Shared)** или **Java Integrated Remote Console (private)**.

Появится экран KVM.

ПРИМЕЧАНИЕ

После выбора **Java Integrated Remote Console (Shared)** два пользователя могут одновременно получить доступ к серверу и выполнять операции на сервере. Каждый пользователь может просматривать операции, выполняемые другим пользователем, что может привести к определенным рискам безопасности.

Экран KVM состоит из трех областей, как показано на Рис. 3-35. В Табл. 3-67 приведено описание этих областей.

Рис. 3-35 Экран KVM

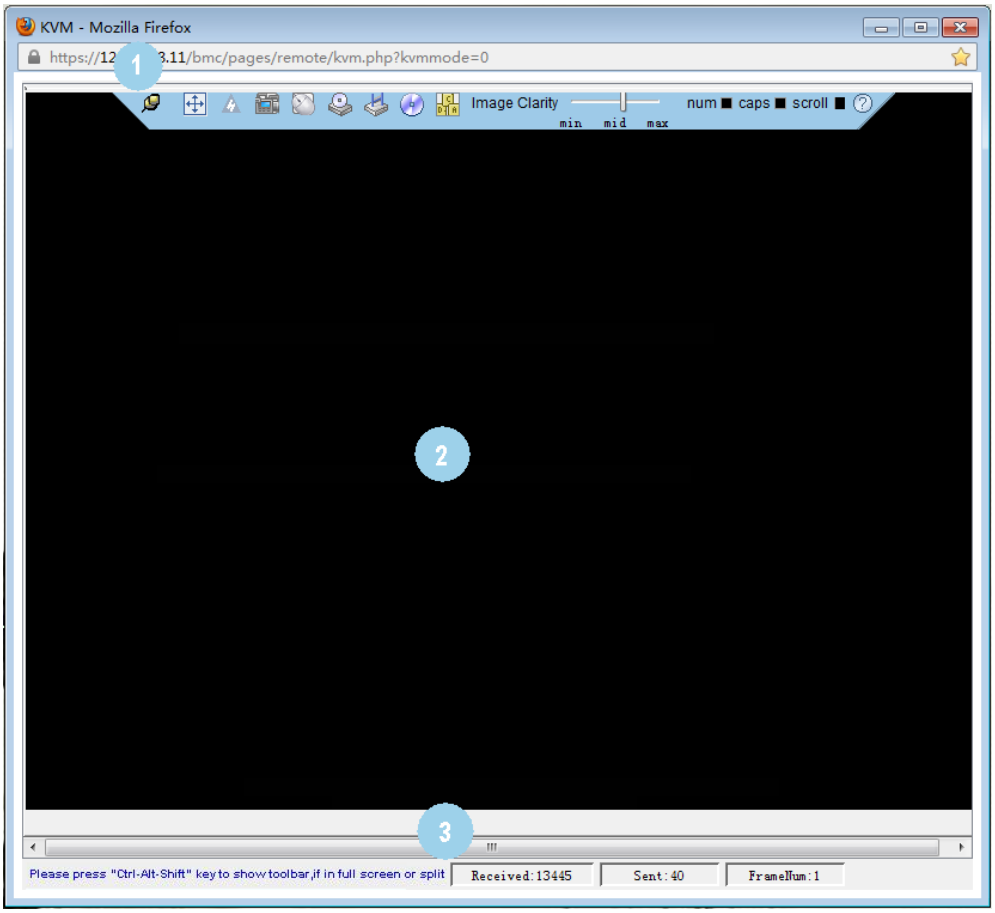


Табл. 3-67 Области на экране KVM

№	Площадь	Функция
1	Панель инструментов	Значки на панели инструментов используются для удаленного управления сервером.
2	Рабочий стол сервера	С помощью клавиатуры или мыши вашего локального ПК можно управлять сервером в режиме реального времени.
3	Строка состояния	Отображебние подсказок для рабочего стола сервера и данных связи между сервером и локальным ПК в режиме реального времени.

Процедура

Отправка комбинации клавиш

1. На экране KVM-консоли на панели инструментов нажмите  .
   На экране появится диалоговое окно комбинации клавиш.

2. Выберите комбинацию клавиш.

   Сервер выполнит операцию в соответствии с комбинацией клавиш.

ПРИМЕЧАНИЕ

Если необходимо настроить комбинацию клавиш, введите клавиши в текстовом поле после **Custom** и нажмите **Send**.

Монтировка DVD-диска

Монтировка DVD-диска на локальном ПК на сервер.

1. На экране KVM-консоли на панели инструментов нажмите  .

   Откроется диалоговое окно, показанное на Рис. 3-36.

   Рис. 3-36 Смонтируйте виртуальный DVD-диск.

2. Выберите **CD/DVD**.
3. Из выпадающего списка выберите букву диска DVD-диска на локальном ПК, например **G:**.
4. Нажмите **Connect**.

   Начнется монтировка DVD-диска локального ПК на сервер.

ПРИМЕЧАНИЕ

Для отмены монтировки DVD-диска нажмите **Disconnect**. Затем нажмите **Yes** в появившемся диалоговом окне **Confirm**.

Загрузка файла образа с локального ПК через виртуальный DVD-диск

Монтировка DVD-диска локального ПК и загрузка файла образа с локального ПК на сервер.

1. На экране KVM-консоли на панели инструментов нажмите  .

   Откроется диалоговое окно, показанное на Рис. 3-36.
2. Выберите **Image File**.
3. Нажмите **Browse**.

   На экране появится диалоговое окно **Open**.
4. Выберите файл образа, который хранится на локальном ПК и нажмите **Open**.

   Откроется диалоговое окно, показанное на Рис. 3-36.
5. Нажмите **Connect**.

   Виртуальный DVD-диск успешно смонтирован на сервер и файл образа успешно загружен.

ПРИМЕЧАНИЕ

- Для загрузки другого файла образа нажмите **Eject** и извлеките существующий файл образа DVD, выберите новый файл образа DVD и нажмите **Insert**.

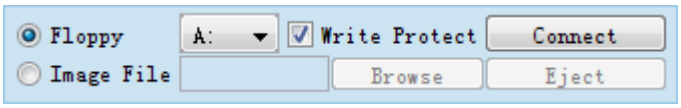
- Для размонтировки DVD-диска нажмите **Disconnect**. Затем нажмите **Yes** в появившемся диалоговом окне **Confirm**.

Монтировка виртуального FDD

Монтировка FDD на локальном ПК для сервера.

1. На экране KVM-консоли на панели инструментов нажмите  .
   Откроется диалоговое окно, показанное на Рис. 3-37.

   Рис. 3-37 Монтировка виртуального FDD

2. Выберите **Floppy**.
3. Выберите буКву диска FDD на локальном ПК из выпадающего списка, например **A:**.
4. Установите галочку **Write Protect**.

ПРИМЕЧАНИЕ

Write Protect – это механизм, который предотвращает изменение или стирание важных данных. При выборе **Write Protect** данные не могут быть записаны на указанный FDD.

5. Нажмите **Connect**.
   FDD смонтирован на сервер.

ПРИМЕЧАНИЕ

Для размонтировки FDD нажмите **Disconnect**. Затем нажмите **Yes** в появившемся диалоговом окне **Confirm**.

Загрузка файла образа с локального ПК через виртуальный FDD

Монтировка FDD локального ПК и загрузка файла образа с локального ПК на сервер.

1. На экране KVM-консоли на панели инструментов нажмите  .
   Откроется диалоговое окно, показанное на Рис. 3-37.
2. Выберите **Image File**.
3. Нажмите **Browse**.
   На экране появится диалоговое окно **Open**.
4. Выберите файл образа, который хранится на локальном ПК и нажмите **Open**.
   Откроется диалоговое окно, показанное на Рис. 3-37.
5. Нажмите **Connect**.
   Файл образа будет успешно загружен на сервер.

ПРИМЕЧАНИЕ

- Для загрузки другого файла образа нажмите **Eject** для извлечения существующего виртуального FDD, выберите новый файл образа и нажмите **Insert**.
- Для размонтировки виртуального FDD нажмите **Disconnect**. Затем нажмите **Yes** в появившемся диалоговом окне **Confirm**.

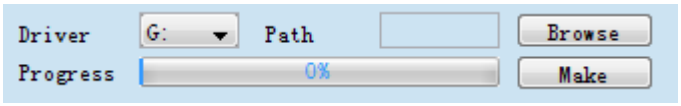
Создание файла образа

Создание файла образа с помощью флоппи-диска на FDD или DVD на DVD-диске локального ПК. Созданный файл образа хранится на локальном ПК.

Перед выполнением данной операции необходимо убедиться, что флоппи-диск вставлен в FDD или DVD-диск вставлен в DVD-привод локального ПК.

1. На экране KVM-консоли на панели инструментов нажмите  .
   Откроется диалоговое окно, показанное на Рис. 3-38.

   Рис. 3-38 Создание файла образа

2. Из выпадающего списка **Driver** выберите букву диска FDD или DVD-диска на локальном ПК.
3. Нажмите **Browse**. На экране появится диалоговое окно **Save**.
4. Выберите каталог для сохранения файла образа и в текстовой строке **File Name** укажите имя файла.

ПРИМЕЧАНИЕ

Система поддерживает создание только файлов образов *.iso, с использованием DVD-диска и файлов образов*.img с использованием FDD.

5. Нажмите **Save**.
   Откроется диалоговое окно, показанное на Рис. 3-38.
6. Нажмите **Make**.
   Progress – это ход создания файла образа.

ПРИМЕЧАНИЕ

Для остановки создания файла образа нажмите **Stop**.

Монтировка виртуального каталога

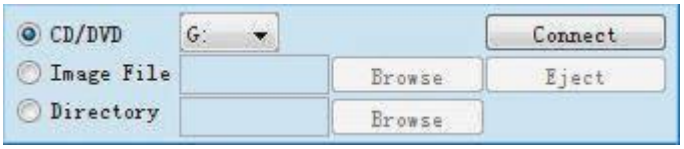
Монтировка каталогов на локальном ПК на сервер, чтобы сервер могу получить доступ к локальным каталогам в режиме «только для чтения».

ВНИМАНИЕ

Перед монтировкой каталога, скопируйте необходимые файлы в каталог. После монтировки каталога, вы не сможете добавлять файлы в каталог или удалять файлы из каталога.

1. На экране KVM нажмите  на панели инструментов.
   Откроется диалоговое окно, показанное на Рис. 3-39.

Рис. 3-39 Монтировка виртуального каталога



2. Выберите **Directory**.
3. Нажмите **Browse**.

   На экране появится диалоговое окно выбора локального каталога.
4. Выберите каталог и нажмите **Open**.
5. Нажмите **Connect**.

ПРИМЕЧАНИЕ

- Если подключение выполнено успешно, то виртуальный каталог будет отображен в списке ОС сервера. Вы можете копировать файлы из данного каталога.
- Для размонтировки виртуального каталога нажмите **Disconnect**.

Включение сервера

1. На экране KVM нажмите на панели инструментов и выберите **Power On** из меню.

   Появится диалоговое окно **Confirm**.
2. Нажмите **Yes**.

   включается питания сервера

ПРИМЕЧАНИЕ

Время запуска ОС различается в зависимости от конфигурации сервера.

Выключение сервера

ВНИМАНИЕ

- Перед выключением питания сервера необходимо убедиться, что все сервисы остановлены.
- Выберите режим выключения питания, в зависимости от требований. Подробная информация о различиях между режимами выключения питания приведена в разделе 3.6.1 Управление питанием.

1. На экране KVM нажмите на панели инструментов и выберите **Normal Power Off** из меню.

   Появится диалоговое окно **Confirm**.
2. Нажмите **Yes**.

   Питание сервера будет выключено.

Принудительная перезагрузка или периодическое включение и выключение питания сервера

ВНИМАНИЕ

- Принудительная перезагрузка может привести к повреждению пользовательских программ или к потере несохраненных данных.
- Перед выполнением принудительной перезагрузки системы или принудительным включением и выключением питания сервера, необходимо убедиться в отсутствии сервисных рисков.
- Выберите режим (**Forced System Reset** или **Forced Power Cycle**) в зависимости от сервисных требований. Подробная информация о различиях между двумя режимами приведена в разделе 3.6.1 Управление питанием.

1. На экране KVM нажмите на панели инструментов и выберите **Forced System Reset** или **Forced Power Cycle** из меню.

   Появится диалоговое окно **Confirm**.
2. Нажмите **Yes**.

   После этого сервер начнет перезагрузку или включение и выключение питания.

ПРИМЕЧАНИЕ

Длительность перезагрузки или включения и выключения питания сервера зависит от конфигурации сервера.

Возврат клавиатуры и мыши в исходное состояние

Моделирование удаления и установки USB-клавиатуры и мыши, когда клавиатура и мышь на рабочем столе сервера перестают отвечать.

1. На экране KVM нажмите на панели инструментов и выберите **Mouse & Key Reset** из меню.

   Появится диалоговое окно **Confirm**.
2. Нажмите **Yes**.

   После этого произойдет сброс USB-клавиатуры и мыши.

Запись видео рабочего стола сервера

Запись видео рабочего стола отображается на удаленной виртуальной консоли.

1. На экране KVM-консоли на панели инструментов нажмите .

   На экране появится диалоговое окно **Confirm**.
2. Нажмите **Yes**.

   На экране появится диалоговое окно **Save**.
3. Выберите каталог для сохранения записываемого видеофайла и в текстовой строке **File Name** укажите имя файла.
4. Нажмите **Save**.

   Появится экран KVM и начнется запись видео.
5. После записи видео нажмите .

   На экране появится диалоговое окно **Confirm**.
6. Нажмите **Yes**.

   Видеофайл будет сохранен в указанный каталог.

Видеофайл – это файл с расширением .rep. На странице **Play Back** можно воспроизвести видеофайл.

Использование функции Single Mouse

Если мышь локального ПК не синхронизирована с рабочим столом сервера, то для того, чтобы скрыть мышь на локальном ПК используется функция single-mouse. При этом мышь будет отображаться только на рабочем столе сервера.

1. На экране KVM нажмите  на панели инструментов и выберите **Single Mouse** из меню.

   На экране появится диалоговое окно **Confirm**.
2. Нажмите **Yes**.

   На экране KVM отображается только мышь рабочего стола сервера.

Ускорение удаленной мыши

Ускорение мыши рабочего стола сервера для синхронизации работы с мышью на локальном ПК.

1. На экране KVM нажмите  на панели инструментов и выберите **Mouse Acceleration** из меню.

   На экране появится диалоговое окно **Confirm**.
2. Нажмите **Yes**.

   Работа мыши сервера синхронизирована с мышью на локальном ПК.

3.9.2 Встроенная удаленная консоль HTML5

Описание функции

Благодаря удаленной виртуальной консоли Java, вы можете получить доступ к серверу и управлять сервером дистанционно, устанавливать или восстановить ОС, а также устанавливать драйверы на сервер.

Благодаря встроенной удаленной консоли можно:

- Использовать клавиатуру и мышь локального ПК для дистанционного управления сервером.
- Включить сервер для удаленного доступа к локальному ПК по сети, с использованием флоппи-диска (FDD) или DVD-диска. Для сервера использование виртуального FDD или виртуального DVD-диска это то же самое, что и использование физического USB-устройства.

ПРИМЕЧАНИЕ

В качестве носителя на локальном ПК может использоваться локальный жесткий диск FDD или DVD-диск, или флоппи-диск, или файл образа DVD, который хранится на локальном ПК или сетевом диске.

В Табл. 3-66 приведено описание значков на экране KVM.

Табл. 3-68 Описание значков

Значок	Описание
	Блокировка панели инструментов.
	Скрытие панели инструментов.
	Рабочий стол сервера в полноэкранном режиме.
	Отмена полноэкранного отображения рабочего стола сервера.
	Меню управления питанием, включая: • Power On • Forced Power Off • Power Off • Forced System Reset • Forced Power Cycle
	Установка первого загрузочного устройства, с которого будет выполняться загрузка ОС. Система поддерживает следующие параметры: • **No Override**: загрузка ОС с первого загрузочного устройства, указанного в BIOS. • **Hard Drive**: загрузка ОС с жесткого диска. • **DVD-ROM**: загрузка ОС с компакт-диска или DVD-диска. • **FDD/Removable Device**: загрузка ОС с виртуального флоппи-диска (FDD) или переносного диска. • **PXE**: загрузка ОС из среды выполнения предварительной загрузки (PXE – Preboot Execution Environment). • **BIOS Setup**: отображение меню BIOS Setup при запуске сервера.
	Отправка или настройка комбинации клавиш. Поддерживаются следующие комбинации клавиш: • **Alt+Tab**: переключение между работающими приложениями. • **Ctrl+Esc**: расширение или сворачивание меню **Start.** • **Ctrl+Shift**: переключение между способами ввода. • **Ctrl+Space**: включение или отключение способов ввода. • **Ctrl+Alt+Del**: блокировка окна ОС, выход пользователя, изменение пароля, открытие Диспетчера задач или перезагрузка сервера.
	Управление мышью сервера. Поддерживаются следующие операции:

Значок	Описание
	• **Mouse Acceleration** Ускорение мыши рабочего стола сервера для синхронизации работы с мышью на локальном ПК. **ПРИМЕЧАНИЕ** В более ранних версиях, чем SUSE 12, данная операция не поддерживается. • **Single Mouse** Скрытие мыши локального ПК и отображение мыши рабочего стола сервера. • **Mouse & Key Reset** Имитация удаления и установки USB-клавиатуры и мыши. Когда клавиатура и мышь на рабочем столе сервера перестают отвечать, нажмите **Mouse & Key Reset** для восстановления. Настройки по умолчанию: **Mouse Acceleration**
	Выбор и использование виртуального DVD-диска.
	Выбор и использование виртуального жесткого диска FDD.
	Запись видео операций, выполняемых на сервере.
	Справочная информация.
	Настройка четкости изображения рабочего стола сервера.
	Статус клавиши **Num Lock** сервера.
	Статус клавиши **Caps Lock** сервера.
	Статус клавиши **Scroll Lock** сервера. **ПРИМЕЧАНИЕ** Если при управлении сервером с использованием удаленной виртуальной консоли возникла ошибка ввода клавиатуры, сначала проверьте статус значков  ,  и  .

GUI

Выберите **Remote Console** из главного меню и нажмите **HTML5 Integrated Remote Console (private)** или **HTML5 Integrated Remote Console (Shared)**.

Появится экран KVM.

ПРИМЕЧАНИЕ

После выбора **HTML5 Integrated Remote Console (Shared)** два пользователя могут одновременно получить доступ к серверу и выполнять операции на сервере. Каждый пользователь может просматривать операции, выполняемые другим пользователем, что может привести к определенным рискам безопасности.

Экран **KVM** состоит из трех областей, как показано на Рис. 3-40. Табл. 3-68 приведено описание этих областей.

Рис. 3-40 Экран KVM

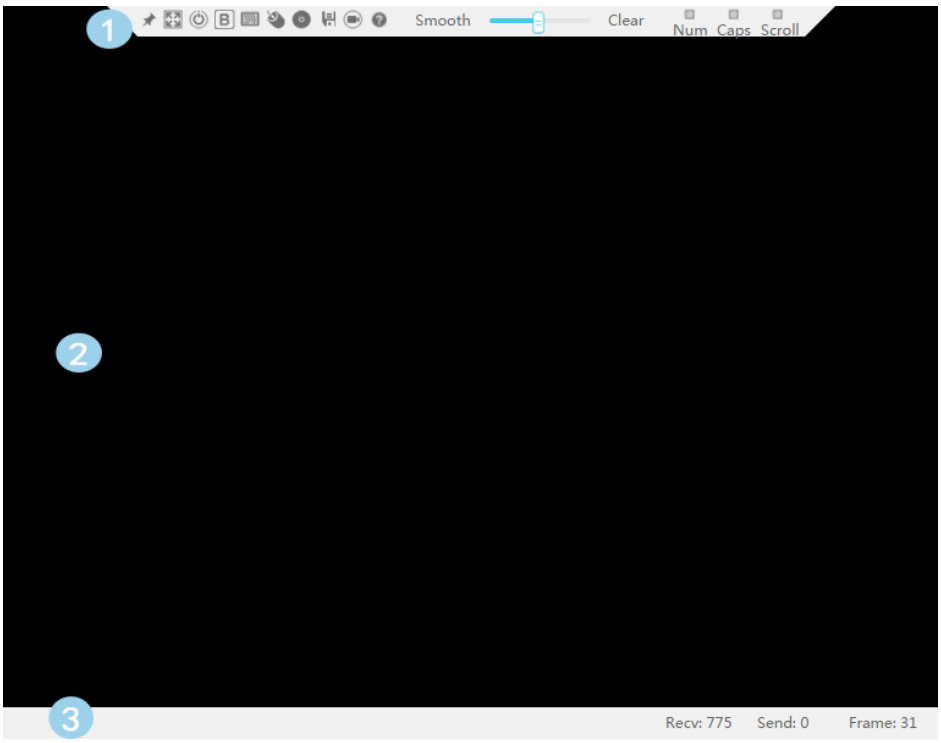


Табл. 3-69 Области на экране KVM

№	Область	Функция
1	Панель инструментов	Значки на панели инструментов используются для удаленного управления сервером.
2	Рабочий стол сервера	С помощью клавиатуры или мыши вашего локального ПК можно управлять сервером в режиме реального времени.
3	Строка состояния	Отображебние подсказок для рабочего стола сервера и данных связи между сервером и локальным ПК в режиме реального времени.

Процедура

Включение сервера

На экране **KVM** нажмите  на панели инструментов и выберите **Power On** из меню.

Питание сервера будет включено.

ПРИМЕЧАНИЕ

Время запуска ОС различается в зависимости от конфигурации сервера.

Выключение сервера

ВНИМАНИЕ

- Перед выключением питания сервера необходимо убедиться, что все сервисы остановлены.
- Выберите режим выключения питания, в зависимости от требований. Подробная информация о различиях между режимами выключения питания приведена в разделе 3.6.1 Управление питанием.

На экране **KVM** нажмите  на панели инструментов и выберите **Forced Power Off** или **Power Off**.

Питание сервера будет выключено.

Принудительная перезагрузка или периодическое включение и выключение питания сервера

ВНИМАНИЕ

- Принудительная перезагрузка может привести к повреждению пользовательских программ или к потере несохраненных данных.
- Перед выполнением принудительной перезагрузки системы или принудительным включением и выключением питания сервера, необходимо убедиться в отсутствии сервисных рисков.
- Выберите режим (**Forced System Reset** или **Forced Power Cycle**) в зависимости от сервисных требований. Подробная информация о различиях между двумя режимами приведена в разделе 3.6.1 Управление питанием.

На экране **KVM** нажмите  на панели инструментов и выберите **Forced System Reset** или **Forced Power Cycle**.

После этого сервер начнет перезагрузку или включение и выключение питания.

ПРИМЕЧАНИЕ

Длительность перезагрузки или включения и выключения питания сервера зависит от конфигурации сервера.

Установка первого загрузочного устройства, с которого будет выполняться загрузка ОС

1. На экране **KVM** нажмите  на панели инструментов.
   На экране появятся параметры загрузочного устройства.
2. Выберите первое загрузочное устройство, в соответствии с требованиями.
   Подробная информация приведена в Табл. 3-68.

Отправка комбинации клавиш

1. На экране KVM-консоли на панели инструментов нажмите  .
   На экране появится диалоговое окно комбинации клавиш.
2. Выберите комбинацию клавиш.
   Сервер выполнит операцию в соответствии с комбинацией клавиш.

ПРИМЕЧАНИЕ

Если необходимо настроить комбинацию клавиш, введите клавиши в текстовом поле после **Custom** и нажмите **Send**.

Ускорение удаленной мыши

Ускорение мыши рабочего стола сервера для синхронизации работы с мышью на локальном ПК.

На экране **KVM** нажмите  на панели инструментов и выберите **Mouse Acceleration**.

Работа мыши сервера синхронизирована с мышью на локальном ПК.

Использование функции Single Mouse

Если мышь локального ПК не синхронизирована с рабочим столом сервера, то для того, чтобы скрыть мышь на локальном ПК используется функция single-mouse. При этом мышь будет отображаться только на рабочем столе сервера.

На экране **KVM** нажмите  на панели инструментов и выберите **Single Mouse.**

Возврат клавиатуры и мыши в исходное состояние

Моделирование удаления и установки USB-клавиатуры и мыши, когда клавиатура и мышь на рабочем столе сервера перестают отвечать.

На экране **KVM** нажмите  на панели инструментов и выберите **Mouse & Key Reset**.

После этого будет выполнен возврат USB-клавиатуры и мыши в исходное состояние.

Монтировка DVD-диска

Монтировка DVD-диска на локальном ПК на сервер.

1. На экране **KVM** нажмите  на панели инструментов.
   Появится экран, показанный на Рис. 3-41.

   Рис. 3-41 Монтировка DVD-диска

2. Выберите **Image File**.
3. Нажмите  .
   На экране локального ПК появится диалоговое окно **Open**.
4. Выберите файл ***.iso** и нажмите **Connect**.
   Откроется экран, показанный на Рис. 3-41.
   Файл образа будет успешно загружен на сервер.

ПРИМЕЧАНИЕ

- Для загрузки другого файла образа нажмите **Eject**, выберите файл ***.iso** для загрузки и нажмите **Insert**.
- Для размонтировки DVD-диска нажмите **Disconnect**.

Монтировка файла

Монтировка файла на локальном ПК на сервер, чтобы сервер могу получить доступ к файлу в режиме «только для чтения».

1. На экране **KVM** нажмите  на панели инструментов.
   Откроется экран, показанный на Рис. 3-42.

   Рис. 3-42 Монтировка файла на локальный ПК

2. Выберите **Local File**.
3. Нажмите  .
   На экране локального ПК появится диалоговое окно **Open**.
4. Выберите файл для монтировки.
   Появится экран, показанный на Рис. 3-42.
5. Нажмите **Connect**.

Файл на ПК будет успешно смонтирован на сервер.

ПРИМЕЧАНИЕ

- После успешной монтировки файла, откройте и просмотрите файл в ОС сервера.
- Для размонтировки файла нажмите **Disconnect**.

Загрузка файла образа с локального ПК через виртуальный FDD

Монтировка FDD локального ПК и загрузка файла образа с локального ПК на сервер.

1. На экране **KVM** нажмите  на панели инструментов.
   Появится экран, показанный на Рис. 3-43.

   Рис. 3-43 Монтировка файла образа с использованием виртуального FDD

2. Нажмите  .
   На экране локального ПК появится диалоговое окн **Open**.
3. Выберите файл ***.img** и нажмите **Connect**.
   Откроется экран, показанный на Рис. 3-43.
4. Нажмите **Connect**.
   Файл образа будет успешно смонтирован на сервер.

ПРИМЕЧАНИЕ

- Для загрузки другого файла образа нажмите **Eject** для извлечения существующего виртуального FDD, выберите новый файл образа и нажмите **Insert**.
- Для размонтировки виртуального FDD нажмите **Disconnect**.

Запись видео рабочего стола сервера

Запись видео рабочего стола отображается на удаленной виртуальной консоли.

1. На экране KVM-консоли на панели инструментов нажмите  .
   Когда значок изменится на  начнется запись видео.
2. Нажмите  для остановки записи видео.
   Видеофайл будет автоматически загружен и сохранен на локальный ПК.

Видеофайл – это файл с расширением .rep. На странице **Play Back** можно воспроизвести видеофайл.

3.10 Устранение неисправностей удаленной виртуальной консоли

3.10.1 Сбой при открытии удаленной виртуальной консоли

Признаки неисправности

Симптомы	Возможные причины
Не удается открыть удаленную виртуальную консоль.	• Версия JRE не правильная. • Версия JRE несовместима с iBMC.

Решение

Шаг 1 Проверьте установлена ли правильна версия JRE.

iBMC поддерживает JRE версии 1.7 и 1.8.

- Если да, выполните шаг 3.
- Если нет, выполните шаг 2.

Шаг 2 Установите версию JRE, поддерживаемую iBMC.

Установите JRE версии 1.7 или 1.8 и выполните шаг 3.

Шаг 3 Измените конфигурацию безопасности Java.

1. Проверьте версию Java клиента.

   На CLI Windows или устройстве Linux выполните команду **java –version**.
2. Откройте Java Control Panel.
   - В ОС Windows откройте Java Control Panel через панель управления.
   - В Linux:
     i. Откройте клиент.
     ii. Перейдите к каталогу установки Java, например **/usr/java/jre1.7/bin**.
     iii. Запустите панель управления Java.
3. Решите проблему несовместимости между JRE и iBMC.

   Решить проблему несовместимости можно путем изменения конфигурации безопасности Java.
   - При использовании версии JRE 1.7, выполните следующее:
     i. На панели управления Java установите уровень безопасности **Medium** и нажмите **OK**.
     ii. Выполните перезагрузку веб-браузера.
   - При использовании версии JRE 1.8, выполните следующее:
     i. На вкладке **Security** нажмите **Edit Site List**.
     ii. Добавьте IP-адрес iBMC и номер порта (443 по умолчанию), например *https://192.168.2.10:443/* к списку.
     iii. Сохраните настройки и перезагрузите браузер.

iv. Войдите на удаленную виртуальную консоль и проигнорируйте любое отображаемое сообщение о безопасности.

----Конец

3.10.2 Не удалось открыть удаленную виртуальную консоль в Google Chrome

Признаки неисправности

Симптомы	Возможные причины
Не удалось открыть удаленную виртуальную консоль в Google Chrome, и на экране появляется сообщение о том, что плагин не поддерживается.	Интерфейс программирования приложений Netscape Plugin (NPAPI – Netscape Plugin Application Programming Interface) не поддерживается или не включен Google Chrome.

ПРИМЕЧАНИЕ

Для запуска удаленной виртуальной консоли требуется плагин Java, соответствующий NPAPI. Перед открытием удаленной виртуальной консоли в Google Chrome убедитесь, что NPAPI включен.

Решение

Google Chrome версии 45 и более поздние версии больше не поддерживают NPAPI.

1. Проверьте версию Google Chrome.
   - При использовании Google Chrome версии 42, 42 или 44, перейдите к шагу 2.
   - Если установлен Google Chrome версии 45 или более поздней версии, то рекомендуется использовать другой веб-браузер.
2. Включите NPAPI для Google Chrome.
   a. Введите **chrome://flags/#enable-npapi** в адресной строке Google Chrome и нажмите **Enter**.
   б. Перезагрузите Google Chrome.

3.10.3 Не удалось открыть удаленную виртуальную консоль из-за старого плагина Firefox в ОС Linux

Признаки неисправности

Симптомы	Возможные причины
Когда запуск удаленной виртуальной консоли выполняется при использовании Firefox в Linux, то на экране появится сообщение о том, что необходимо обновить плагин Firefox.	Слишком старая версия плагина Firefox.

Решение

Шаг 1 Перейдите в каталог с плагином Firefox.

Например, выполните команду **cd /usr/lib/mozilla/plugins**.

Шаг 2 Создайте программную ссылку к файлу **libnpjp2.so** в установочном каталоге java.

Например, выполните команду **ln -s /usr/java/jre1.6.0_25/lib/libnpjp2.so**.

Шаг 3 Выполните перезагрузку Firefox.

----Конец

3.10.4 На удаленной виртуальной консоли недоступны мышь и клавиатура

Признаки неисправности

Симптомы	Возможные причины
На удаленной виртуальной консоли не работают клавиатура и мышь.	RAID-контроллер LSISAS3108 настроен, отсутствует постоянное подключение клавиатуры и мыши.

Решение

Шаг 1 На странице **Component Info** проверьте сконфигурирован ли сервер с RAID-контроллером LSISAS3108.

- Если да, выполните шаг 2.
- Если нет, выполните шаг 4.

Шаг 2 На странице **Remote** проверьте включено ли постоянное подключение клавиатуры и мыши.

- Если да, выполните шаг 4.
- Если нет, выполните шаг 3.

Шаг 3 Включите постоянное подключение клавиатуры и мыши и выполните перезагрузку сервера. После перезагрузки сервера проверьте, решена ли проблема.

- Если да, то никаких действий больше выполнять не требуется.
- Если нет, выполните шаг 4.

Шаг 4 Обратитесь за помощью в службу технической поддержки Huawei.

----Конец

3.10.5 Не удалось открыть удаленную виртуальную консоль, после появления значка запуска Java Web

Признаки неисправности

Симптомы	Возможные причины
После появления и закрытия страницы запуска Java web, удаленная виртуальная консоль не открывается.	При запуске удаленной виртуальной консоли в режиме Java web, временные файлы недоступны.

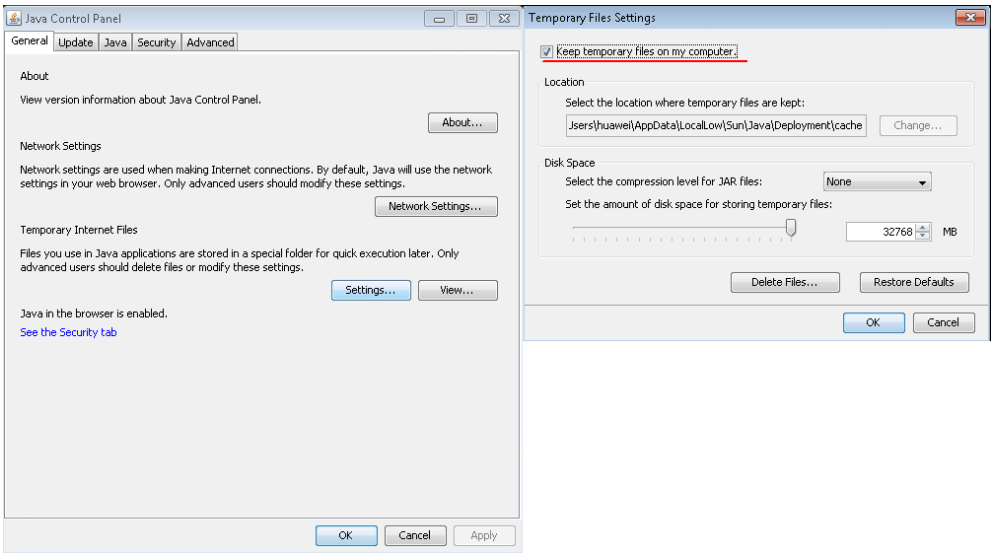
Решение

Шаг 1 Откройте Java Control Panel на локальном ПК.

Шаг 2 Нажмите **Settings** на кладке **General**.

Шаг 3 В окне **Temporary Files Settings** выберите **Keep temporary files on my computer** и нажмите **OK**, как показано на Рис. 3-44.

Рис. 3-44 Настройка режима отображения архивных файлов



Шаг 4 Сохранение настроек и перезагрузка браузера.

----Конец

3.10.6 Неавторизованный пользователь на удаленной виртуальной консоли

Признаки неисправности

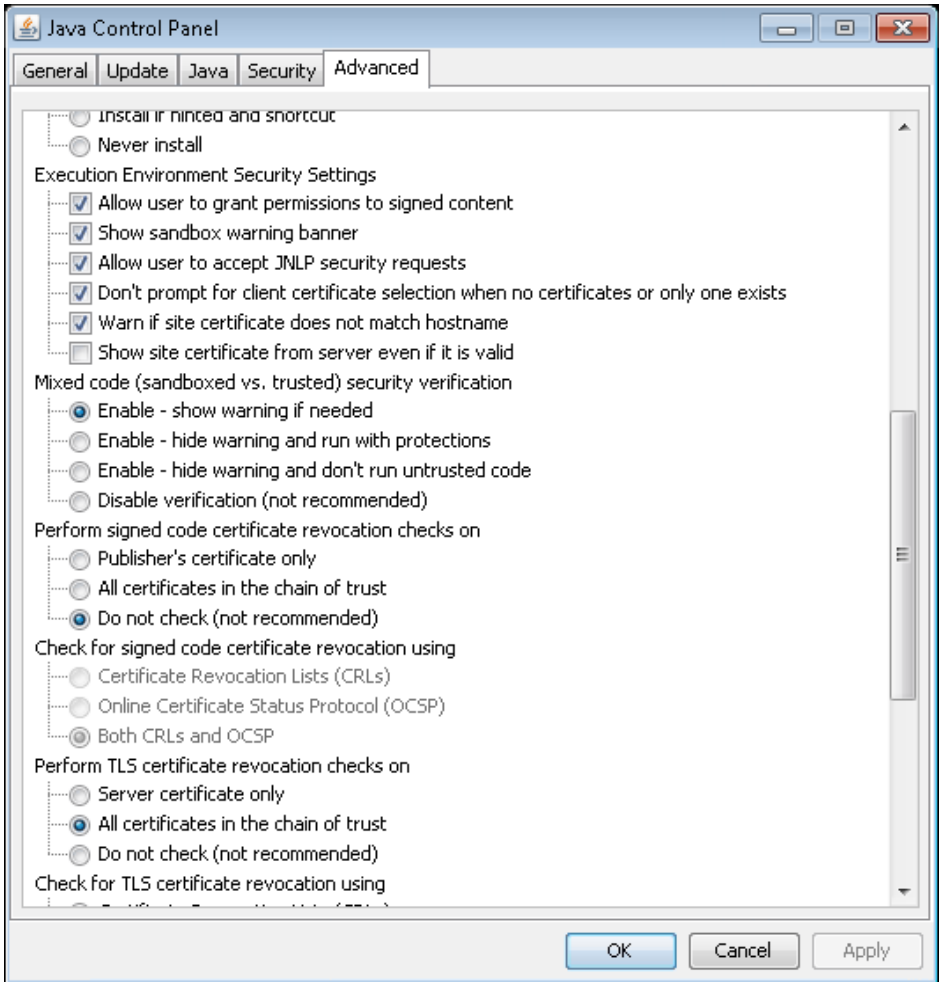
Симптомы	Возможные причины
1. Когда пользователь пытается открыть удаленную виртуальную консоль, на экране появляется значок запуска Java web. 2. Удаленная виртуальная консоль откроется по истечении длительного периода времени, как только значок Java web исчезнет с экрана. 3. После появления на экране удаленной виртуальной консоли, на экране появляется сообщение «Unauthorized User».	В процессе запуска KVM должна быть выполнена авторизация, когда клиент подключается к сети Интернет. Если клиентская сеть находится в режиме offline, то время аутентификации может истечь, что приведет к сбою запуска.

Решение

Решить данную проблему можно любым из следующих способов:

- Подключите клиент, который используется для доступа к удаленной виртуальной консоли е сети Интернет.
- Укажите параметры Java.
  а. Откройте Java Control Panel на локальном ПК.
  б. На вкладке **Advanced** выберите **Do not check** для параметра **Perform signed code certificate revocation checks on** как показано на Рис. 3-45.

Рис. 3-45 Изменение параметров Java



в. Сохранение настроек и перезагрузка браузера.

3.11 Сбор информации одним щелчком кнопки мыши

Табл. 3-70 Сбор информации одним щелчком кнопки мыши

Каталог	Подкаталог	Имя файла	Содержание файла
–	–	dump_app_log	Перечень информации, собранной iBMC.
		dump_log	Результаты сбора информации одним щелчком кнопки мыши.
AppDump	Lcd	Lcd_dfl.log	Информация о ЖК-модуле.
	User	User_dfl.log	Информация о

Каталог	Подкаталог	Имя файла	Содержание файла	
			пользовательском модуле.	
	card_manage	card_manage_dfl.log	Информация о модуле Card_Manage.	
		card_info	Информация о платах, сконфигурированных на сервере.	
	BMC	BMC_dfl.log	Информация о модуле BMC.	
		fruinfo.txt	Информация об утилитах.	
		net_info.txt	Информация о конфигурации сетевого интерфейса	
		psu_info.txt	Информация о блоках питания сервера.	
	PowerMgnt	PowerMgnt_dfl.log	Информация о модуле управления питанием.	
		UPGRADE	UPGRADE_dfl.log	Информация о модуле обновлений.
	upgrade_info		Версия устройств, связанных с BMC.	
	BIOS	BIOS_dfl.log	Информация о BIOS.	
		bios_info	Конфигурационная информация BIOS.	
		ClpConfig0.ini	Информация о конфигурации iBMC на BIOS.	
		ClpResponse0.ini	Информация об ответной информации iBMC, сконфигурированной на BIOS.	
		options0.ini	Конфигурационная информация BIOS.	
		changed0.ini	Список измененных пунктов конфигурации BIOS.	
		display0.ini	Отображаемая информация BIOS.	
		registry.json	Регистрационный файл BIOS, содержащий конфигурационную информацию BIOS.	
		currentvalue.json	Информация о текущей конфигурации BIOS.	
		setting.json	Информация о настройках	

Каталог	Подкаталог	Имя файла	Содержание файла	
			BIOS, созданных с использованием Redfish, которые не вступили в силу.	
		result.json	Результаты настроек BIOS, созданные с использованием Redfish.	
	discovery	discovery_dfl.log	Информация о модуле обнаружения.	
	diagnose	diagnose_dfl.log	Информация о модуле распознавания.	
		diagnose_info	Информация о диагностике неисправностей по порту 80.	
	Snmp	Snmp_dfl.log	Информация о модуле Snmp.	
	cooling_app	cooling_app_dfl.log	Информация о модуле охлаждения.	
		fan_info.txt	Информация о моделях вентиляторов и скорости их вращения.	
	CpuMem	CpuMem_dfl.log	Информация о модуле CpuMem.	
		cpu_info	Подробная информация о ЦП, сконфигурированных для сервера.	
		mem_info	Подробная информация о DIMM, сконфигурированных для сервера.	
	kvm_vmm	kvm_vmm_dfl.log	Информация о модуле KVM_VMM.	
	ipmi_app	ipmi_app_dfl.log	Информация о модуле IPMI.	
	Dft	Dft_dfl.log	Информация о модуле DFT.	
	net_nat	net_nat_dfl.log	Информация о модуле Net_NAT.	
	PcieSwitch	PcieSwitch_dfl.log	Информация о модуле PcieSwitch.	
		sensor_alarm	sensor_alarm_dfl.log	Информация о модуле Sensor_Alarm.
	sensor_info.txt		Список всех датчиков сервера.	
	current_event.txt		Текущее рабочее состояние и аварийные сигналы сервера.	

Каталог	Подкаталог	Имя файла	Содержание файла	
	sel.tar		Заархивированный пакет текущих и архивных журналов событий системы (SEL).	
	sensor_alarm_sel.bin.md5		Код проверки целостности для исходных SEL.	
	sensor_alarm_sel.bin.bak.md5		Код проверки целостности для резервных и исходных SEL.	
	sensor_alarm_sel.bin.sha256		Код проверки целостности для исходных SEL.	
	sensor_alarm_sel.bin.bak.sha256		Код проверки целостности для резервных и исходных SEL.	
	sensor_alarm_sel.bin.bak		Исходная информация о резервном копировании и проверка значения текущих SEL.	
	sensor_alarm_sel.bin		Исходная информация и проверка значения текущих SEL.	
	sel.db		Информация о базе данных текущих SEL.	
	LedInfo		Статус индикатора тока сервера.	
	sensor_alarm_sel.bin.tar.gz		Заархивированный пакет с архивными SEL.	
	MaintDebug	MaintDebug_dfl.log	Информация о модуле MaintDebug.	
	FileManage	FileManage_dfl.log	Информация о модуле FileManage.	
	switch_card	switch_card_dfl.log	Информация о модуле Switch_Card.	
		phy_register_info	Информация о регистре PHY задних плат.	
		port_adapter_info	Информация об интерфейсном устройстве задних плат.	
	StorageMgnt	StorageMgnt_dfl.log	Информация о модуле StorageMgnt.	
		RAID_Controller_Info.txt	Информация о RAID-контроллере, логическом диске и жестком диске.	
	rimm	rimm_dfl.log	Информация о модуле StorageMgnt.	

Каталог	Подкаталог	Имя файла	Содержание файла	
	redfish	redfish_dfl.log	Информация о модуле Redfish.	
	dfm	dfm.log	Информация об объектах, управляемых DFM.	
		dfm_debug_log dfm_debug_log.1	Журнал регистрации событий отладки структуры PME.	
	3rdDump	–	error_log	Журнал ошибок Apache.
			access_log	Журнал доступа Apache.
httpd.conf			Конфигурационный файл Apache HTTP.	
httpd-port.conf			Конфигурационный файл порта Apache HTTP.	
httpd-ssl.conf			Конфигурационный файл Apache HTTPS.	
httpd-ssl-port.conf			Конфигурационный файл порта Apache HTTPS.	
httpd-ssl-protocol.conf			Конфигурационный файл с версией протокола Apache HTTPS.	
CoreDump	–	core-* (файлы, начинающиеся с «core-»)	Файл дампинга памяти. Основной файл дампинга прикладной программы. Создается один или несколько файлов в зависимости от рабочего статуса системы.	
RTOSDump	sysinfo	cmdline	Параметры командной строки ядра.	
		cpuinfo	Информация о микросхеме ЦП ядра iBMC.	
		devices	Информация о устройствах iBMC.	
		df_info	Информация об использовании разделов iBMC.	
		diskstats	Информация о статусе дисков iBMC.	
		filesystems	Информация о файловой системе iBMC.	

Каталог	Подкаталог	Имя файла	Содержание файла	
		free_info	Информация о доступной памяти iBMC.	
		interrupts	Информация о прерываниях iBMC.	
		ipcs_q	Информация об очереди процессов iBMC.	
		ipcs_q_detail	Подробная информация об очереди процессов iBMC.	
		ipcs_s	Информация о ручной сигнализации процесса iBMC.	
		ipcs_s_detail	Подробная информация о ручной сигнализации процесса iBMC.	
		loadavg	Информация о рабочей нагрузке системы iBMC.	
		locks	Список заблокированных файлов фдра iBMC.	
		meminfo	Информация об использовании памяти iBMC.	
		modules	Список модулей iBMC.	
		mtd	Информация о конфигурации разделов iBMC.	
		partitions	Информация о разделах iBMC.	
		ps_info	ps -elf Подробная информация о процессах iBMC.	
		slabinfo	Информация о slab iBMC.	
		stat	Использование ЦП iBMC.	
		top_info	top -bn 1 Информация о работающих текущих процессах.	
		uname_info	uname -a Текущий статус процессов iBMC.	
		uptime	Рабочее время системы iBMC	
		version	Версия операционной системы, работающей в режиме реального времени (RTOS) iBMC.	

Каталог	Подкаталог	Имя файла	Содержание файла
		vmstat	Статистическая информация виртуальной памяти iBMC.
	versioninfo	ibmc_revision.txt	Информация об исправлениях iBMC.
		app_revision.txt	Информация о версии iBMC.
		build_date.txt	Время создания версии iBMC.
		fruinfo.txt	Информация об электронной метке FRU.
		RTOS-Release	Информация о выпуске RTOS.
		RTOS-Revision	Маркировка с версией RTOS.
		server_config.txt	Информация о текущей конфигурации сервера.
	networkinfo	ifconfig_info	Сетевая информация. Для получения данной информации выполните команду **ifconfig**.
		ipinfo_info	Информация о конфигурации сети iBMC.
		_data_var_dhcp_dhclient.leases	Файл аренды DHCP.
		dhclient.leases	Файл аренды DHCP.
		dhclient6.leases	Файл аренды DHCP.
		dhclient6_eth0.leases	Файл аренды DHCP.
		dhclient6_eth1.leases	Файл аренды DHCP.
		dhclient6_eth2.leases	Файл аренды DHCP.
		dhclient.conf	Файл конфигурации DHCP.
		dhclient_ip.conf	Файл конфигурации DHCP.
		dhclient6.conf	Файл конфигурации DHCP.
		dhclient6_ip.conf	Файл конфигурации DHCP.
		resolv.conf	Файл конфигурации DNS.
		ipinfo.sh	Сценарий конфигурации сети iBMC.
		netstat_info	netstat -a Текущие сетевые порты и статус их подключения.
		route_info	route Текущая информация о

Каталог	Подкаталог	Имя файла	Содержание файла
			маршрутизации.
		services	Информация о сервисном порте.
	other_info	extern.conf	Конфигурация файла журнала iBMC.
		remotelog.conf	Конфигурационный файл Syslog.
		ssh	Конфигурация сервиса SSH.
		sshd_config	Конфигурационный файл сервиса SSHD.
		logrotate.status	Файл, в котором записан статус logrotate.
		login	Правила входа в систему для привилегированных учетных записей.
		sshd	Правила входа в систему для привилегированных учетных записей SSH.
		sfcb	Правила входа в систему для привилегированных учетных записей CIM.
		datafs_log	Журнал проверки данных.
		ntp.conf	Конфигурация сервиса NTP.
		vsftpd	Правила входа в систему для привилегированных учетных записей FTP.
	driver_info	dmesg_info	Информация о запуске системы (результаты выполнения команды **dmesg**).
		lsmod_info	Информация р загруженных драйверах.
		kbox_info	Информация kbox.
		edma_drv_info	Статистика драйвера edma.
		cdev_drv_info	Статистика драйвера символьного устройства.
		veth_drv_info	Статистика драйвера виртуальной сетевой карты.
LogDump	–	LSI_RAID_Controller_Log LSI_RAID_Controlle	Журналы контроллера RAID LSI.

Каталог	Подкаталог	Имя файла	Содержание файла	
		r_Log.1.gz LSI_RAID_Controller_Log.2.gz		
		PD_SMART_INFO_C*	Журнал SMART жестких дисков. * – это серийный номер RAID-контроллера.	
		linux_kernel_log linux_kernel_log.1	Журналы ядра Linux.	
		operate_log operate_log.tar.gz	Журнал операций пользователя.	
		remote_log remote_log.1.gz	Журналы операций и журналы SELдля тестирования Syslog.	
		security_log security_log.1	Журналы безопасности.	
		strategy_log strategy_log.tar.gz	Журналы работы системы.	
		fdm.bin fdm.bin.tar.gz	Журнал первичных неисправностей FDM.	
		fdm_me_log fdm_me_log.tar.gz	Журнал неисправностей ME.	
		fdm_pfae_log	Журнал с предупреждениями FDM.	
		fdm_mmio_log fdm_mmio_log.tar.gz	Журналы конфигурации платы FDM.	
		maintenance_log maintenance_log.tar.gz	Журналы техобслуживания.	
		ipmi_debug_log ipmi_debug_log.tar.gz	Журналы модуля IPMI.	
		ipmi_mass_operation_log ipmi_mass_operation_log.tar.gz	Журналы операций модуля IPMI.	
		app_debug_log_all app_debug_log_all.1.gz app_debug_log_all.2.	Журналы отладки приложений.	

Каталог	Подкаталог	Имя файла	Содержание файла
		gz app_debug_log_all.3.gz	
		agentless_driver_log agentless_driver_log.1.gz agentless_driver_log.2.gz agentless_driver_log.3.gz	Журналы отладки драйвера Agentless.
		kvm_vmm_debug_log kvm_vmm_debug_log.tar.gz	Журналы модуля KVM.
		ps_black_box.log	Журналы черного ящика блока питания.
OSDump	–	systemcom.tar	Информация о последовательном порте SOL.
		img*.jpeg	Образ последнего скриншота ОС сервера.
		*.rep	Автоматически записанные видеофайлы.
DeviceDump	i2c_info	*_info	Информация о памяти устройства I2C или об области памяти.
Register	–	cpld_reg_info	Информация о регистре сложной программируемой логической интегральной схемы (CPLD – Complex programmable logical device).
OptPme	pram **ПРИМЕЧАНИЕ** В данной папке содержатся файлы из каталога /opt/pme/pram. Файлы, которые не входят в данную папку, представляют собой промежуточные файлы, созданные во время работы программы, и у	filelist	Список файлов в каталоге **/opt/pme/pram**.
		BIOS_FileName	Информация SMBIOS.
		BIOS_OptionFileName	Конфигурационная информация BIOS.
		BMC_dhclient.conf	Файл конфигурации DHCP.
		BMC_dhclient.conf.md5	Код проверки целостности.
		BMC_dhclient.conf.sha256	Код проверки целостности.

Каталог	Подкаталог	Имя файла	Содержание файла
	которых нет проблем с информационной безопасностью.	BMC_dhclient6.conf	Файл конфигурации DHCP.
		BMC_dhclient6.conf.md5	Код проверки целостности.
		BMC_dhclient6.conf.sha256	Код проверки целостности.
		BMC_dhclient6_ip.conf	Файл конфигурации DHCP.
		BMC_dhclient6_ip.conf.md5	Код проверки целостности.
		BMC_dhclient6_ip.conf.sha256	Код проверки целостности.
		BMC_dhclient_ip.conf	Файл конфигурации DHCP.
		BMC_dhclient_ip.conf.md5	Код проверки целостности.
		BMC_dhclient_ip.conf.sha256	Код проверки целостности.
		BMC_HOSTNAME	Имя хоста.
		BMC_HOSTNAME.md5	Код проверки целостности.
		BMC_HOSTNAME.sha256	Код проверки целостности.
		CpuMem_cpu_utilise	Использование ЦП сервера.
		CpuMem_mem_utilise	Использование памяти сервера.
		cpu_utilise_webview.dat	Данные кривой использования ЦП.
		env_web_view.dat	Данные кривой температуры окружающей среды.
		fsync_reg.ini	Файл конфигурации синхронизации файлов.
		lost+found	Папка.
		md_so_maintenance_log	Журнал техобслуживания.
		md_so_maintenance_log.tar.gz	Пакет журнала техобслуживания.
		md_so_operate_log	Журнал операций пользователя.

Каталог	Подкаталог	Имя файла	Содержание файла
		md_so_operate_log.md5	Код проверки целостности.
		md_so_operate_log.sha256	Код проверки целостности.
		md_so_operate_log.tar.gz	Пакет журнала операций пользователя.
		md_so_strategy_log	Журнал политик.
		md_so_strategy_log.md5	Код проверки целостности.
		md_so_strategy_log.sha256	Код проверки целостности.
		md_so_strategy_log.tar.gz	Пакет журнала политик.
		memory_webview.dat	Операционная информация об управляемом объекте.
		per_config.ini	Файл постоянной конфигурации iBMC.
		per_config.ini.md5	Код проверки целостности.
		per_config.ini.sha256	Код проверки целостности.
		per_config_permanent.ini	Файл постоянной конфигурации iBMC.
		per_config_permanent.ini.md5	Код проверки целостности.
		per_config_permanent.ini.sha256	Код проверки целостности.
		per_config_reset.ini	Файл постоянной конфигурации iBMC.
		per_config_reset.ini.bak	Файл постоянной конфигурации iBMC.
		per_config_reset.ini.bak.md5	Код проверки целостности.
		per_config_reset.ini.bak.sha256	Код проверки целостности.
		per_config_reset.ini.md5	Код проверки целостности.
		per_config_reset.ini.sha256	Код проверки целостности.
		per_def_config.ini	Файл постоянной конфигурации

Каталог	Подкаталог	Имя файла	Содержание файла
			iBMC.
		per_def_config.ini.md5	Код проверки целостности.
		per_def_config.ini.sha256	Код проверки целостности.
		per_def_config_permanent.ini	Файл постоянной конфигурации iBMC.
		per_def_config_permanent.ini.md5	Код проверки целостности.
		per_def_config_permanent.ini.sha256	Код проверки целостности.
		per_def_config_reset.ini	Файл долговечности конфигурации iBMC.
		per_def_config_reset.ini.bak	Файл постоянной конфигурации iBMC.
		per_def_config_reset.ini.bak.md5	Код проверки целостности.
		per_def_config_reset.ini.bak.sha256	Код проверки целостности.
		per_def_config_reset.ini.md5	Код проверки целостности.
		per_def_config_reset.ini.sha256	Код проверки целостности.
		per_power_off.ini	Файл постоянной конфигурации iBMC.
		per_power_off.ini.md5	Код проверки целостности.
		per_power_off.ini.sha256	Код проверки целостности.
		per_reset.ini	Файл постоянной конфигурации iBMC.
		per_reset.ini.bak	Файл постоянной конфигурации iBMC.
		per_reset.ini.bak.md5	Код проверки целостности.
		per_reset.ini.bak.sha256	Код проверки целостности.
		per_reset.ini.md5	Код проверки целостности.
		per_reset.ini.sha256	Код проверки целостности.

Каталог	Подкаталог	Имя файла	Содержание файла
		pflash_lock	Блокировка флэш-файла.
		PowerMgnt_record	Операционная информация об управляемом объекте.
		powerview.txt	Файл статистики питания.
		proc_queue	Папка с ID очереди процессов.
		ps_web_view.dat	Операционная информация об управляемом объекте.
		sel.db	База данных SEL.
		sel_db_sync	Блокировка синхронизации базы данных SEL.
		semid	Папка с ID ручной сигнализации процессов.
		sensor_alarm_sel.bin	Исходный файл SEL.
		sensor_alarm_sel.bin.md5	Код проверки целостности.
		sensor_alarm_sel.bin.sha256	Код проверки целостности.
		sensor_alarm_sel.bin.tar.gz	Папка с пакетами архивных SEL.
		Snmp_snmpd.conf	Файл конфигурации SNMP.
		Snmp_snmpd.conf.md5	Код проверки целостности.
		Snmp_snmpd.conf.sha256	Код проверки целостности.
		Snmp_http_configure	Конфигурационная папка HTTP.
		Snmp_http_configure.md5	Код проверки целостности.
		Snmp_http_configure.sha256	Код проверки целостности.
		Snmp_https_configure	Конфигурационная папка HTTPS.
		Snmp_https_configure.md5	Код проверки целостности.
		Snmp_https_configure.sha256	Код проверки целостности.
		Snmp_https_tsl	Конфигурационная папка TLS HTTPS.

Каталог	Подкаталог	Имя файла	Содержание файла	
		Snmp_https_tsl.md5	Код проверки целостности.	
		Snmp_https_tsl.sha256	Код проверки целостности.	
		up_cfg	Конфигурационная папка с обновлениями.	
		User_login	Правила входа в систему для привилегированных учетных записей.	
		User_login.md5	Код проверки целостности.	
		User_login.sha256	Код проверки целостности.	
		User_sshd	Правила входа в систему для привилегированных учетных записей SSH.	
		User_sshd.md5	Код проверки целостности.	
		User_sshd.sha256	Код проверки целостности.	
		User_sshd_config	Конфигурационный файл SSH.	
		User_sshd_config.md5	Код проверки целостности.	
		User_sshd_config.sha256	Код проверки целостности.	
		User_vsftp	Правила входа в систему для привилегированных учетных записей FTP.	
		User_vsftp.md5	Код проверки целостности.	
		User_vsftp.sha256	Код проверки целостности.	
		eo.db	База данных SEL.	
	save **ПРИМЕЧАНИЕ** В данной папке содержатся файлы из каталога /opt/pme/save. В файле *.md5 содержится код проверки целостности. В файле *.sha256 содержится код проверки целостности. Файл *.bak – это резервный файл.	filelist	Список файлов в каталоге **/opt/pme/pram**.	
		BIOS_FileName	Информация SMBIOS.	
		BMC_dhclient.conf.bak	Резервный файл конфигурации DHCP.	
		BMC_dhclient.conf.bak.md5	Код проверки целостности.	
		BMC_dhclient.conf.bak.sha256	Код проверки целостности.	
		BMC_dhclient.conf.md5	Код проверки целостности.	

Каталог	Подкаталог	Имя файла	Содержание файла	
	Файл *.tar.gz – это распакованный пакет. Файл per_*.ini – это файл постоянной конфигурации. Файл *sel.* – это файл журнала событий системы (Файлы, которые не входят в данную папку, представляют собой промежуточные файлы, созданные во время работы программы, и у них нет проблем с информационной безопасностью).	BMC_dhclient.conf.sha256	Код проверки целостности.	
		BMC_dhclient6.conf.bak	Резервный файл конфигурации DHCP.	
		BMC_dhclient6.conf.bak.md5	Код проверки целостности.	
		BMC_dhclient6.conf.bak.sha256	Код проверки целостности.	
		BMC_dhclient6.conf.md5	Код проверки целостности.	
		BMC_dhclient6.conf.sha256	Код проверки целостности.	
		BMC_dhclient6_ip.conf.bak	Резервный файл конфигурации DHCP.	
		BMC_dhclient6_ip.conf.bak.md5	Код проверки целостности.	
		BMC_dhclient6_ip.conf.bak.sha256	Код проверки целостности.	
		BMC_dhclient6_ip.conf.md5	Код проверки целостности.	
		BMC_dhclient6_ip.conf.sha256	Код проверки целостности.	
		BMC_dhclient_ip.conf.bak	Резервный файл конфигурации DHCP.	
		BMC_dhclient_ip.conf.bak.md5	Код проверки целостности.	
		BMC_dhclient_ip.conf.bak.sha256	Код проверки целостности.	
		BMC_dhclient_ip.conf.md5	Код проверки целостности.	
		BMC_dhclient_ip.conf.sha256	Код проверки целостности.	
		BMC_HOSTNAME.bak	Резервный файл конфигурации имени хоста.	
		BMC_HOSTNAME.bak.md5	Код проверки целостности.	
		BMC_HOSTNAME.bak.sha256	Код проверки целостности.	
		BMC_HOSTNAME.	Код проверки целостности.	

Каталог	Подкаталог	Имя файла	Содержание файла
		md5	
		BMC_HOSTNAME.sha256	Код проверки целостности.
		CpuMem_cpu_utilise	Операционная информация об управляемом объекте.
		CpuMem_mem_utilise	Операционная информация об управляемом объекте.
		md_so_operate_log.bak	Журнал операций пользователя.
		md_so_operate_log.bak.md5	Код проверки целостности.
		md_so_operate_log.md5	Код проверки целостности.
		md_so_operate_log.bak.sha256	Код проверки целостности.
		md_so_strategy_log.bak	Журнал политик.
		md_so_operate_log.sha256	Код проверки целостности.
		md_so_strategy_log.bak.md5	Код проверки целостности.
		md_so_strategy_log.bak.sha256	Код проверки целостности.
		md_so_strategy_log.md5	Код проверки целостности.
		md_so_strategy_log.sha256	Код проверки целостности.
		per_config.ini	Файл постоянной конфигурации iBMC.
		per_config.ini.bak	Файл постоянной конфигурации iBMC.
		per_config.ini.bak.md5	Код проверки целостности.
		per_config.ini.bak.sha256	Код проверки целостности.
		per_config.ini.md5	Код проверки целостности.
		per_config.ini.sha256	Код проверки целостности.
		per_def_config.ini	Файл постоянной конфигурации

Каталог	Подкаталог	Имя файла	Содержание файла
			iBMC.
		per_def_config.ini.bak	Файл постоянной конфигурации iBMC.
		per_def_config.ini.bak.md5	Код проверки целостности.
		per_def_config.ini.bak.sha256	Код проверки целостности.
		per_def_config.ini.md5	Код проверки целостности.
		per_def_config.ini.sha256	Код проверки целостности.
		per_power_off.ini	Файл постоянной конфигурации iBMC.
		per_power_off.ini.bak	Файл постоянной конфигурации iBMC.
		per_power_off.ini.bak.md5	Код проверки целостности.
		per_power_off.ini.bak.sha256	Код проверки целостности.
		per_power_off.ini.md5	Код проверки целостности.
		per_power_off.ini.sha256	Код проверки целостности.
		PowerMgnt_record	Операционная информация об управляемом объекте.
		sensor_alarm_sel.bin	Исходный файл SEL.
		sensor_alarm_sel.bin.bak	Исходный файл SEL.
		sensor_alarm_sel.bin.bak.md5	Код проверки целостности.
		sensor_alarm_sel.bin.bak.sha256	Код проверки целостности.
		sensor_alarm_sel.bin.md5	Код проверки целостности.
		sensor_alarm_sel.bin.sha256	Код проверки целостности.
		sensor_alarm_sel.bin.tar.gz	Пакет с архивными SEL.
		Snmp_http_configure	Резервный файл конфигурации

Каталог	Подкаталог	Имя файла	Содержание файла
		.bak	HTTP.
		Snmp_http_configure.bak.md5	Код проверки целостности.
		Snmp_http_configure.bak.sha256	Код проверки целостности.
		Snmp_http_configure.md5	Код проверки целостности.
		Snmp_http_configure.sha256	Код проверки целостности.
		Snmp_https_configure.bak	Резервный файл конфигурации HTTPS.
		Snmp_https_configure.bak.md5	Код проверки целостности.
		Snmp_https_configure.bak.sha256	Код проверки целостности.
		Snmp_https_configure.md5	Код проверки целостности.
		Snmp_https_configure.sha256	Код проверки целостности.
		Snmp_https_tsl.bak	Резервный файл конфигурации TLS HTTPS.
		Snmp_https_tsl.bak.md5	Код проверки целостности.
		Snmp_https_tsl.bak.sha256	Код проверки целостности.
		Snmp_https_tsl.md5	Код проверки целостности.
		Snmp_https_tsl.sha256	Код проверки целостности.
		Snmp_snmpd.conf.bak	Резервный файл конфигурации Snmp.
		Snmp_snmpd.conf.bak.md5	Код проверки целостности.
		Snmp_snmpd.conf.bak.sha256	Код проверки целостности.
		Snmp_snmpd.conf.md5	Код проверки целостности.
		Snmp_snmpd.conf.sha256	Код проверки целостности.

Каталог	Подкаталог	Имя файла	Содержание файла	
		User_login.bak	Правила входа в систему для привилегированных учетных записей	
		User_login.bak.md5	Код проверки целостности.	
		User_login.bak.sha256	Код проверки целостности.	
		User_login.md5	Код проверки целостности.	
		User_login.sha256	Код проверки целостности.	
		User_sshd.bak	Правила входа в систему для привилегированных учетных записей SSH.	
		User_sshd.bak.md5	Код проверки целостности.	
		User_sshd.bak.sha256	Код проверки целостности.	
		User_sshd.md5	Код проверки целостности.	
		User_sshd.sha256	Код проверки целостности.	
		User_sshd_config.bak	Конфигурационная папка SSH.	
		User_sshd_config.bak.md5	Код проверки целостности.	
		User_sshd_config.bak.sha256	Код проверки целостности.	
		User_sshd_config.md5	Код проверки целостности.	
		User_sshd_config.sha256	Код проверки целостности.	
		User_vsftp.bak	Правила входа в систему для привилегированных учетных записей FTP.	
		User_vsftp.bak.md5	Код проверки целостности.	
		User_vsftp.bak.sha256	Код проверки целостности.	
		User_vsftp.md5	Код проверки целостности.	
		User_vsftp.sha256	Код проверки целостности.	
		eo.db	База данных SEL.	
		eo.db.md5	Код проверки целостности.	
		eo.db_backup	База данных SEL.	

Каталог	Подкаталог	Имя файла	Содержание файла	
		eo.db.md5_backup	Код проверки целостности.	

4 Интерфейс командной строки (CLI) iBMC

О данной главе

В данном разделе приведено описание порядка доступа к CLI, а также описание команд, поддерживаемых iBMC.

4.1 Обзор CLI

В данном разделе приведено описание синтаксиса команд.

4.2 Доступ к CLI

В данном разделе приведено описание порядка доступа к CLI.

4.3 Команды iBMC

В данном разделе приведено описание всех команд iBMC.

4.4 Команды Trap

В данном разделе приведено описание всех trap-команд.

4.5 Команды Syslog

В данном разделе приведено описание порядка использования команд для запроса и настройки параметров syslog.

4.6 Команды сервера

В данном разделе приведено описание всех команд, связанных с сервером.

4.7 Системные команды

В данном разделе приведено описание всех системных команд.

4.8 Команды управления пользователями

В данном разделе приведено описание всех команд управления пользователями.

4.9 Команды NTP

В данном разделе приведено описание команд, связанных с протоколом сетевого времени (NTP – Network Time Protocol).

4.10 Команды на индикаторы

В данном разделе приведено описание всех команд на индикаторы.

4.11 Команды на вентилятор

В данном разделе приведено описание всех команд на вентилятор.

4.12 Команды на датчики

В данном разделе приведено описание всех команд на датчики.

4.13 Команды PSU

В данном разделе приведено описание всех команд PSU.

4.14 Команды U-Boot

В данном разделе приведен список команд U-Boot, а также порядок доступа к CLI U-Boot.

4.15 Команды SOL

В данном разделе приведено описание команд SOL (Serial Over LAN).

4.1 Обзор CLI

В данном разделе приведено описание синтаксиса команд.

4.1.1 Синтаксис

Наиболее часто используемые команды iBMC подразделяются на два типа:

- Команды запроса **ipmcget**

  Синтаксис команды **ipmcget** следующий:

  ipmcget [**-t** *target*] **-d** *dataitem* [**-v** *value*]
- Команды установления соединения **ipmcset**

  Синтаксис команды **ipmcset** следующий:

  ipmcset [**-t** *target*] **-d** *dataitem* [**-v** *value*]

Далее приведено описание параметров команд **ipmcget** и **ipmcset**:

- [ ]: информация, заключенная в квадратные скобки, является опциональной для каждой команды.
- **-t** *target*: получение и указание цели на управляемом устройстве. В качестве цели может выступать датчик или индикатор.
- **-d** *dataitem*: получение, установка конкретных свойств управляемого устройства или компонентов на управляемом устройстве.
- **-v** *value*: получение, установка значений параметров компонентов на управляемом устройстве.

В Табл. 4-1 приведены оглашения о формате команд для командной строки.

Табл. 4-1 Соглашения о формате команд для командной строки

Формат	Описание
Полужирный	Ключевые слова командной строки выделяются **полужирным** шрифтом.
Курсив	Параметры команды обозначаются *курсивом.*
[ ]	Ключевые слова или аргументы, заключенные в квадратные скобки [ ], являются опциональными.
{ x | y | ... }	Опциональные элементы сгруппированы в скобках и разделены вертикальными чертами. Выбирается один из вариантов.
[x | y | ...]	Опциональные элементы сгруппированы в скобках и разделены вертикальными чертами. Выбор нескольких вариантов, либо ни одного из них.
{ x | y | ... }*	Опциональные элементы сгруппированы в скобках и разделены вертикальными чертами. Выбирается минимум один вариант или максимум все варианты.
[x | y | ...]*	Опциональные элементы сгруппированы в скобках и разделены вертикальными чертами. Выбирается несколько вариантов, либо ни один из них.

4.1.2 Помощь

Интерфейс командной строки iBMC предоставляет справочную информацию по командам. В процессе ввода команды, при вводе определенного символа и нажатия кнопки **Enter**, в интерфейсе командной строки будут автоматически отображены параметры команд и их синтаксис.

Далее приведен пример.

Команда запроса:

```
iBMC:/->ipmcget
Usage: ipmcget [-t target] -d dataitem [-v value]
   -t <target>
      fru0                      Get the information of the fru0
      sensor                    Print detailed sensor information
      smbios                    Get the information of smbios
      trap                      Get SNMP trap status
      service                   Get service information
      maintenance               Get maintenance information
      syslog                    Get syslog status
      user                      Get the information of user
      securitybanner            Get login security banner information
      storage                   Get storage device information
      config                    Get configuration information
      vmm                       Get virtual media information
      certificate               Get SSL certificate information
      sol                       Get SOL information
      securityenhance           Get security enhance information
```

```
  -d <dataitem>
     faninfo                   Get fan mode and the percentage of the fan speed
     port80                    Get the diagnose code of port 80
     diaginfo                  Get diagnostic info of management subsystem
     systemcom                 Get system com data
     blackbox                  Get black box data
     bootdevice                Get boot device
     shutdowntimeout            Get graceful shutdown timeout state and value
     powerstate                Get power state
     health                    Get health status
     healthevents               Get health events
     sel                       Print System Event Log (SEL)
     operatelog                 Print operation log
     version                   Get iBMC version
     serialnumber               Get system serial number
     userlist                  List all user info
     fruinfo                   Get fru information
     time                      Get system time
     macaddr                   Get mac address
     serialdir                 Get currently connected serial direction
     rollbackstatus             Get rollback status
     passwordcomplexity          Get password complexity check enable status
     ledinfo                   Get led information
     ipinfo                    Get ip information
     ethport                   Get usable eth port
     psuinfo                   Get PSU component information
     autodiscovery              Get autodiscovery configuration
     poweronpermit              Get poweronpermit configuration
     raid                      Deprecated. Please use 'ipmcget -t storage ...' to get
more inforamtion
     ldinfo                    Deprecated. Please use 'ipmcget -t storage ...' to get
more inforamtion
     pdinfo                    Deprecated. Please use 'ipmcget -t storage ...' to get
more inforamtion
     minimumpasswordage          Get minimum password age configuration
     ntpinfo                   Get NTP information
```

Команда установки:

```
iBMC:/->ipmcset
Usage: ipmcset [-t target] -d dataitem [-v value]
   -t <target>
     fru0                      Operate with fru0
     trap                      Operate SNMP trap
     service                    Operate with service
     user                      Operate with user
     maintenance                Operate with maintenance
     sensor                    Operate with sensor
     securitybanner             Operate login security banner information
     syslog                    Operate syslog
     ntp                       Operate ntp
     storage                    Configure storage device
     config                    Operate configuration
     vmm                       Operate virtual media
```

```
      certificate               Operate certificate
      sol                      Operate SOL
      securityenhance            Operate security enhance

   -d <dataitem>
      fanmode                   Set fan mode,you can choose manual or auto
      fanlevel                  Set fan speed percent
      reset                    Reboot iBMC system
      identify                  Operate identify led
      upgrade                  Upgrade component
      clearcmos                 Clear CMOS
      bootdevice                Set boot device
      shutdowntimeout            Set graceful shutdown timeout state and value
      frucontrol                Fru control
      powerstate                Set power state
      sel                      Clear SEL
      adduser                   Add user
      password                  Modify user password
      deluser                   Delete user
      privilege                 Set user privilege
      serialdir                 Set serial direction
      printscreen               Print current screen to iBMC
      rollback                  Perform a manual rollback
      timezone                  Set time zone
      passwordcomplexity          Set password complexity check enable state
      ipaddr                   Set ip address
      ipconfig                  Set ip address mask gateway
      ipmode                   Set ip mode
      gateway                   Set gateway
      ipaddr6                   Set ipv6 address
      ipmode6                   Set ipv6 mode
      gateway6                  Set ipv6 gateway
      ipv6config                Set ipv6 fix gateway
      netmode                   Set net mode
      activeport                Set EthGroup active port
      vlan                     Set sideband vlan
      restore                   Restore factory setting
      notimeout                 Set no timeout state
      emergencyuser              Set emergency user
      autodiscovery              Set autodiscovery configuration
      poweronpermit              Set poweronpermit configuration
      workkey                  Update system workkey
      minimumpasswordage          Set minimum password age configuration
      locate                   Deprecated. Please use 'ipmcset -t storage ...'.
      psuworkmode                Set PSU work mode
```

При неправильном вводе параметра функция справки подскажет правильный синтаксис команды.

Далее приведен пример.

```
iBMC:/->ipmcset -d inff
Input parameter[-d] error
   -d <dataitem>
      fanmode                   Set fan mode,you can choose manual or auto
      fanlevel                  Set fan speed percent
```

```
reset                    Reboot iBMC system
identify                 Operate identify led
upgrade                  Upgrade component
clearcmos                Clear CMOS
bootdevice               Set boot device
shutdowntimeout          Set graceful shutdown timeout state and value
frucontrol               Fru control
powerstate               Set power state
sel                      Clear SEL
adduser                  Add user
password                 Modify user password
deluser                  Delete user
privilege                Set user privilege
serialdir                Set serial direction
printscreen              Print current screen to iBMC
rollback                 Perform a manual rollback
timezone                 Set time zone
passwordcomplexity       Set password complexity check enable state
ipaddr                   Set ip address
ipconfig                 Set ip address mask gateway
ipmode                   Set ip mode
gateway                  Set gateway
ipaddr6                  Set ipv6 address
ipmode6                  Set ipv6 mode
gateway6                 Set ipv6 gateway
ipv6config               Set ipv6 fix gateway
netmode                  Set net mode
activeport               Set EthGroup active port
vlan                     Set sideband vlan
restore                  Restore factory setting
notimeout                Set no timeout state
emergencyuser            Set emergency user
autodiscovery            Set autodiscovery configuration
poweronpermit            Set poweronpermit configuration
workkey                  Update system workkey
minimumpasswordage       Set minimum password age configuration
locate                   Deprecated. Please use 'ipmcset -t storage ...'.
psuworkmode              Set PSU work mode
```

4.2 Доступ к CLI

В данном разделе приведено описание порядка доступа к CLI.

В дополнение к пользователям по умолчанию и пользователям, добавленным вручную, система iBMC генерирует следующих системных пользователей для определенных сервисов:

- **ftp**: используется, когда сервис FTP работает во внутренней сети системы.
- **root**: используется в процессе работы приложения.
- **sshd**: используется когда система запускает сервис SSH.
- **apache**: используется, когда система запускает сервис httpd.
- **snmpd_user**: используется, когда система запускает сервис snmpd_user.

- **ipmi_user**: используется, когда система запускает сервис ipmi_user.
- **kvm_user**: используется, когда система запускает сервис kvm_user.

ПРИМЕЧАНИЕ

- Для серверов V5 пользователь **root** используется только для запуска приложений. Он не используется для входа в систему.
- Эти системные пользователи не могут выполнить вход в iBMC и, следовательно, не оказывают никакого влияния на систему.
- Учетные записи данных пользователей используются для управления системой и не предназначены для конечных пользователей.

4.2.1 Изменение пароля пользователя по умолчанию в BIOS

ВНИМАНИЕ

- По умолчанию для серверов V3 установлен пароль BIOS **Huawei12#$**, а для серверов V5 пароль **Admin@9000**.
- В BIOS можно изменить только пароль пользователя по умолчанию iBMC. По умолчанию в iBMC установлено имя пользователя **root** для серверов V3 и **Administrator** для серверов V5, а на табличке с маркировкой продукта указан пароль по умолчанию.
- Пароль пользователя по умолчанию iBMC, указанный в BIOS может содержать максимум 16 символов.
- В целях безопасности после первого входа в систему рекомендуется изменять исходный пароль и периодически менять пароль в дальнейшем.
- Если параметр **OS User Management** отключен на странице, отображаемой после выбора **Configuration** > **System** в WebUI iBMC а для параметра **BMC User Name** отображается значение **NA** на экране **Server Mgmt** BIOS, то пароль пользователя по умолчанию iBMC в BIOS изменить нельзя.

Операции на платформе Grantley

Экран BIOS различается в зависимости от используемой модели сервера. В следующих шагах, в качестве примера, выбран BIOS на базе платформы Grantley.

Шаг 1 Перезагрузите сервер.

Шаг 2 В процессе запуска когда появится следующий экран, нажмите **Delete** несколько раз подряд. Появится экран запуска BIOS.

Рис. 4-1 Экран запуска BIOS

Шаг 3 Введите пароль BIOS. Пароль по умолчанию приведен на табличке с маркировкой продукта, как показано на Рис. 4-2.

ПРИМЕЧАНИЕ

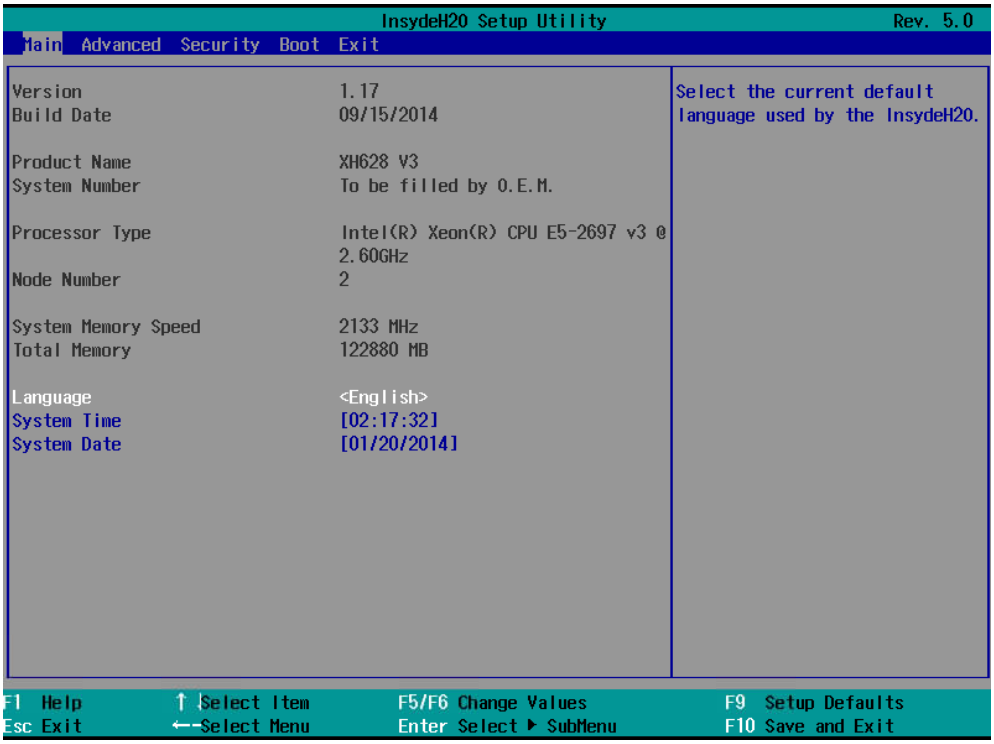
По умолчанию для входа в BIOS используется пароль **Huawei12#$**.

Рис. 4-2 Ввод пароля

Шаг 4 Войдите в BIOS.

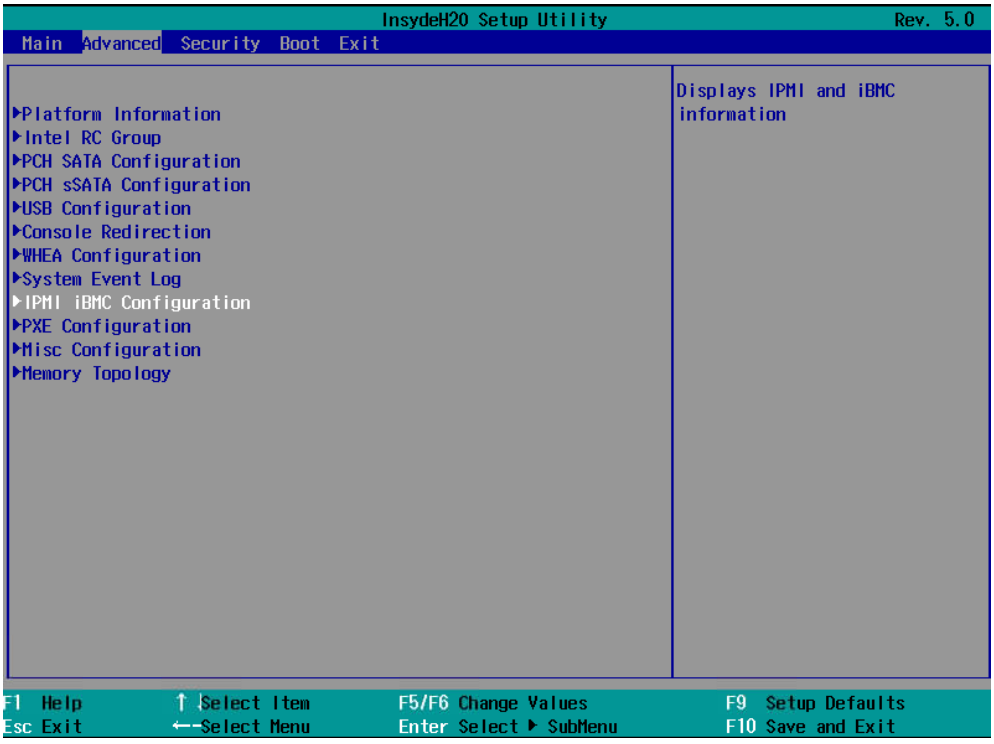
Появится экран BIOS, как показано на Рис. 4-3.

Рис. 4-3 Главный экран BIOS



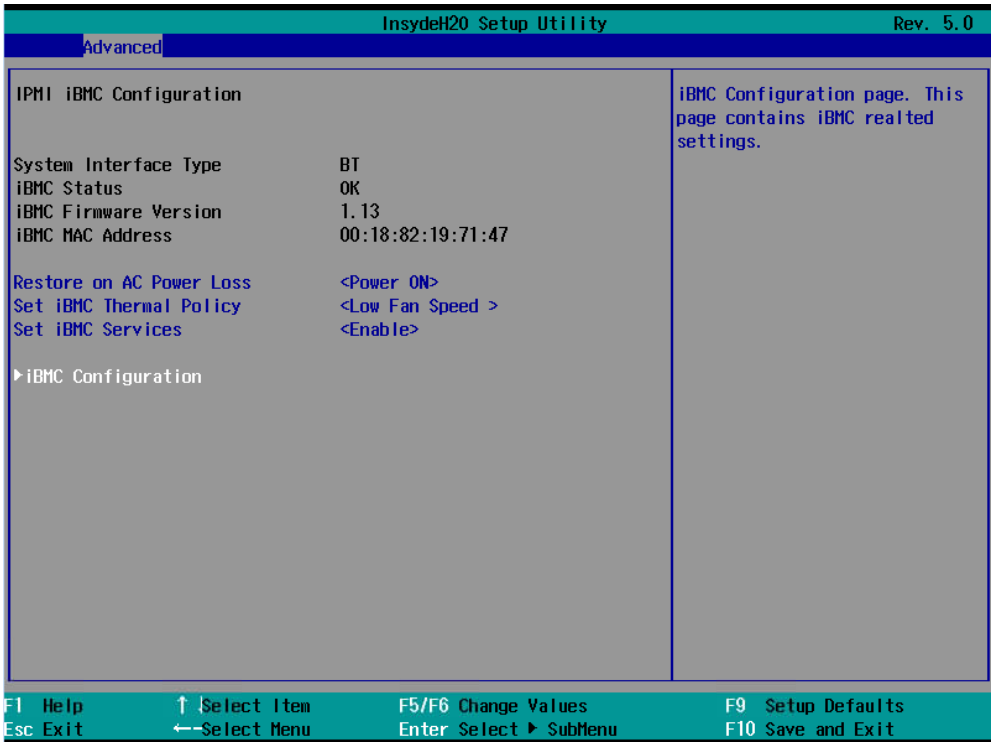
Шаг 5 С помощью клавиш со стрелками выберите экран **Advanced**, как показано на Рис. 4-4.

Рис. 4-4 Экран **Advanced**



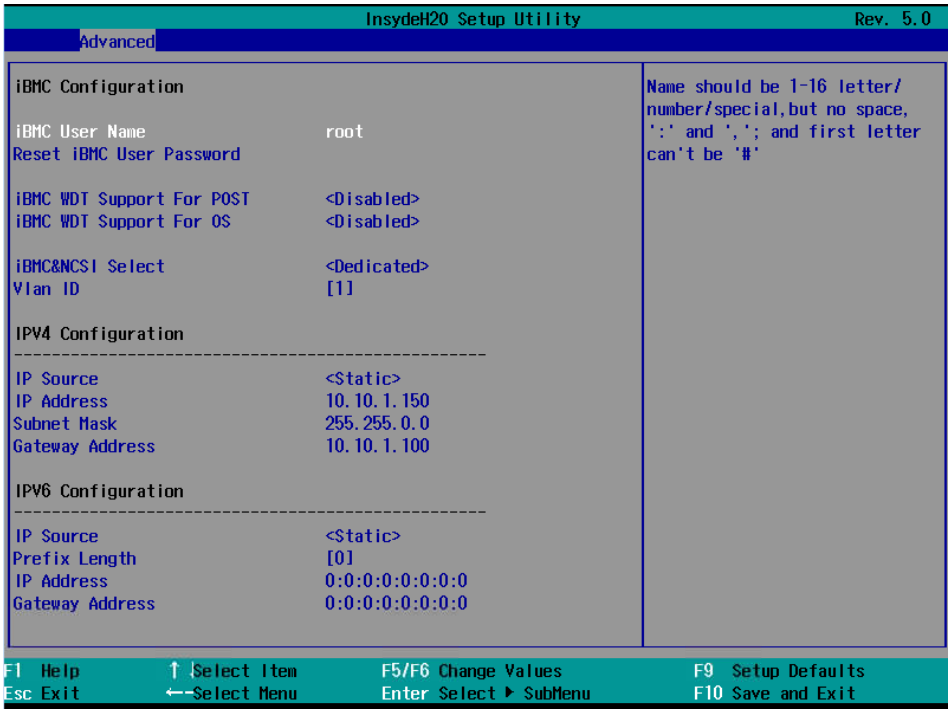
Шаг 6 На экране **Advanced** с помощью клавиш со стрелками выберите **IPMI iBMC Configuration** и нажмите **Enter**, как показано Рис. 4-5.

Рис. 4-5 Экран **IPMI iBMC Configuration**



Шаг 7 На экране **IPMI iBMC Configuration** с помощью клавиш со стрелками выберите **iBMC Configuration** и нажмите **Enter**, как показано на Рис. 4-6.

Рис. 4-6 Экран **iBMC Configuration**



На этом экране отображается IP-адрес сервера.

Шаг 8 Выберите **Reset iBMC User Password** и нажмите **Enter**.

На экране появится диалоговое окно **Reset iBMC User Password**.

Шаг 9 Введите пароль iBMC и нажмите **Enter**.

Пароль должен соответствовать определенным требованиям:

- содержать от 8 до 16 символов.
- содержать, как минимум, один пробел или один из следующих специальных символов:

  `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- содержать, как минимум, символы двух видов:
  - Заглавные буквы: от A до Z
  - Строчные буквы: от a до z
  - Цифры: от 0 до 9
- Пароль не должен совпадать с именем пользователя в прямом и обратном порядке расположения символов.

Шаг 10 Повторите пароль и нажмите **Enter**.

На экране появится диалоговое окно **Changes have been saved**.

Шаг 11 Нажмите **Enter**.

Сохранение настроек

----Конец

Операции на платформе Brinkland

Экран BIOS различается в зависимости от используемой модели сервера. В следующих шагах, в качестве примера, выбран BIOS на базе платформы Brinkland.

Шаг 1 Перезагрузите сервер.

ПРИМЕЧАНИЕ

Время загрузки сервера зависит от его конфигурации. Загрузка полностью сконфигурированного сервера занимает 20 минут.

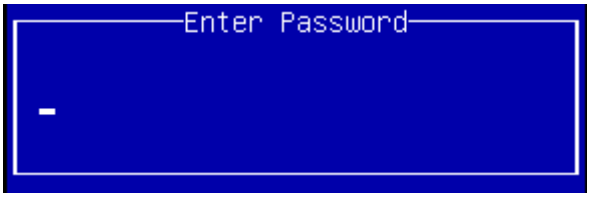
Шаг 2 После появления экрана запуска BIOS, нажмите **Del** для перехода к экрану **BIOS Setup Utility**.

Шаг 3 Введите пароль, как показано на Рис. 4-7.

ПРИМЕЧАНИЕ

- По умолчанию для входа в BIOS используется пароль **Huawei12#$**. В целях безопасности измените пароль по умолчанию при первом входе в систему и периодически меняйте пароль в дальнейшем.
- При вводе неправильного пароля BIOS три раза подряд, BIOS будет заблокирован. Для перезапуска BIOS нажмите **Ctrl+Alt+Del**.

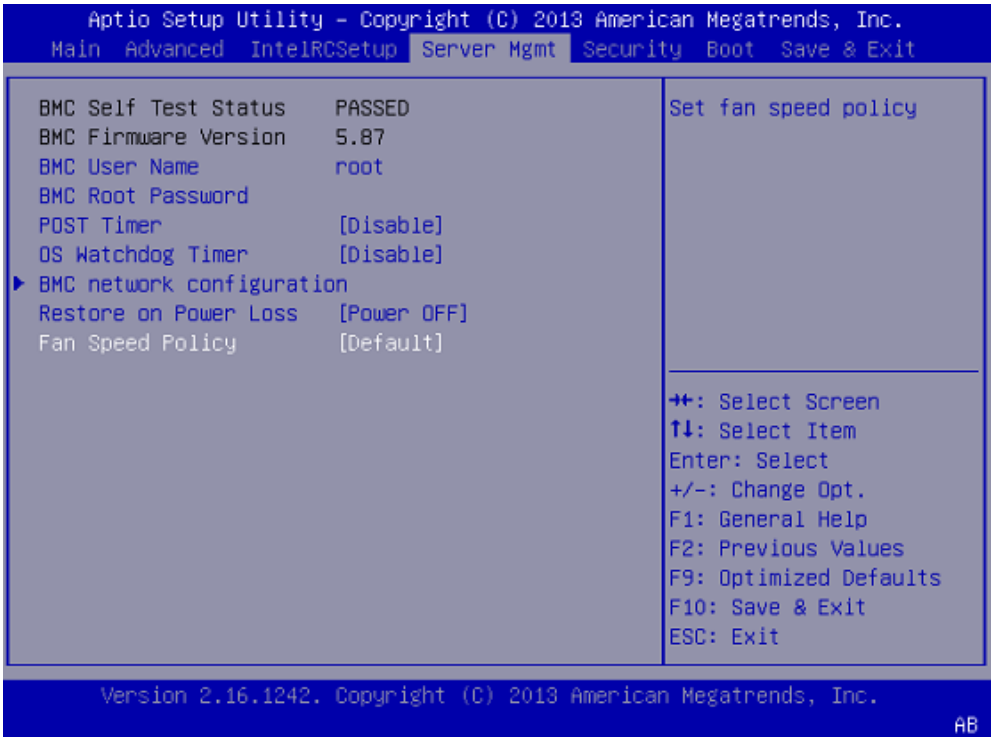
Рис. 4-7 Ввод пароля



Шаг 4 Выберите **Server Mgmt** и нажмите **Enter**.

На экране появится окно **Server Mgmt**, как показано на Рис. 4-8.

Рис. 4-8 Экран **Server Mgmt**



Шаг 5 Выберите **BMC Root Password** и нажмите **Enter**.

Шаг 6 Измените пароль iBMC и нажмите **Enter**.

- Пароль должен содержать от 8 до 16 символов.
- Пароль должен содержать, как минимум, один пробел или один из следующих специальных символов:

  `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Пароль должен содержать, как минимум, два следующих символа:
  - Заглавные буквы: от A до Z
  - Строчные буквы: от a до z
  - Цифры: от 0 до 9
- Пароль не должен совпадать с именем пользователя в прямом и обратном порядке расположения символов.

Шаг 7 Повторите пароль и нажмите **Enter**.

На экране появится диалоговое окно **Changes have been saved**.

Шаг 8 Нажмите **Enter**.

Сохранение настроек

----Конец

4.2.2 Проверка IP-адреса сетевого интерфейса управления

Способы

Для проверки IP-адреса сетевого интерфейса управления, можно использовать любой из следующих способов:

- IP-адрес по умолчанию
- Запрос и установка IP-адреса сетевого интерфейса управления в BIOS.
- Запрос и установка IP-адреса сетевого интерфейса управления с помощью CLI управляющего ПО, после входа в iBMC через последовательный порт.

ПРИМЕЧАНИЕ

Через последовательный порт одновременно войти в систему могут максимум пять пользователей.

IP-адрес по умолчанию

В Табл. 4-2 представлены IP-адреса по умолчанию сетевого порта управления iBMC.

Табл. 4-2 IP-адрес по умолчанию

Тип продукта	№ слота	IP-адрес
RH8100 V3	8-сокетная отдельная система	192.168.2.100
	4-сокетная сдвоенная система	• Исходный сетевой порт управления: 192.168.2.100 • Вторичный сетевой порт управления: 192.168.2.101
Стоечный сервер	–	192.168.2.100

Запрос и установка IP-адреса в BIOS для серверов RH8100 V3

Шаг 1 Перезагрузите сервер.

ПРИМЕЧАНИЕ

Время загрузки сервера зависит от его конфигурации. Загрузка полностью сконфигурированного сервера занимает 20 минут.

Шаг 2 После появления экрана запуска BIOS, нажмите **Del** для перехода к экрану **BIOS Setup Utility**.

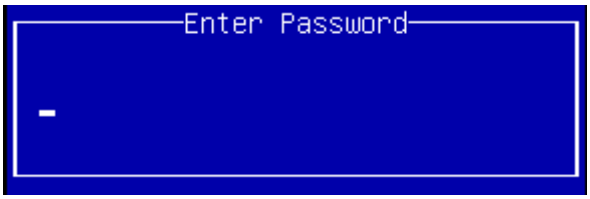
Шаг 3 Введите пароль, как показано на Рис. 4-9.

ПРИМЕЧАНИЕ

- По умолчанию для входа в BIOS используется пароль **Huawei12#$**. В целях безопасности измените пароль по умолчанию при первом входе в систему и периодически меняйте пароль в дальнейшем.

- При вводе неправильного пароля BIOS три раза подряд, BIOS будет заблокирован. Для разблокировки BIOS нажмите **Ctrl+Alt+Del**.

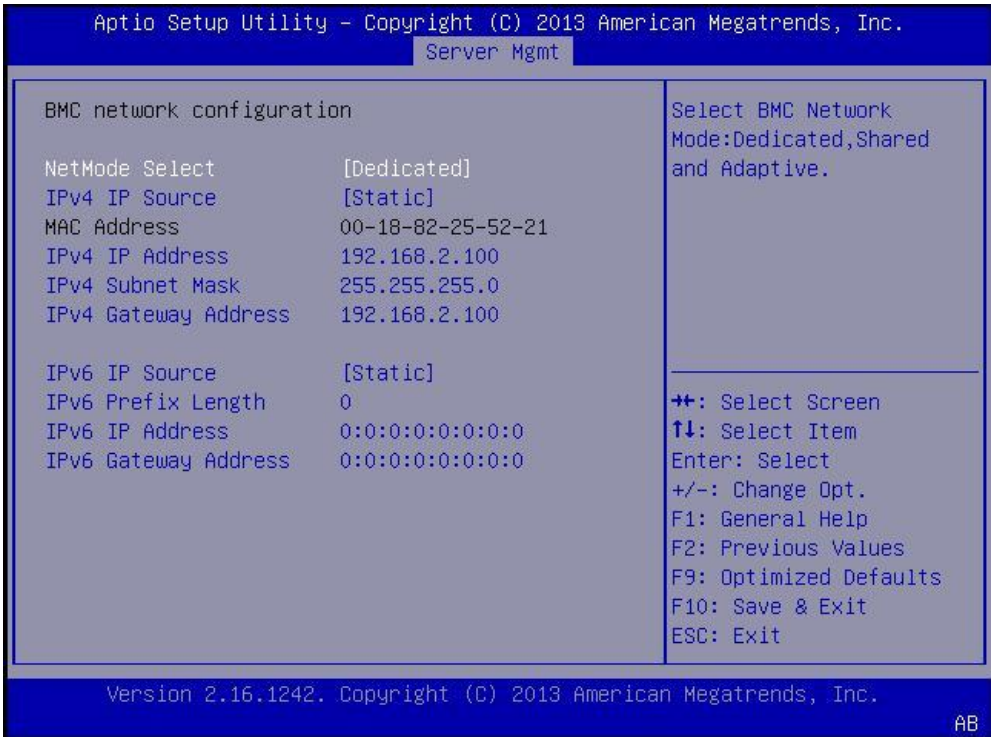
Рис. 4-9 Ввод пароля



Шаг 4 Выберите **Server Mgmt** > **BMC network configuration** и нажмите **Enter**.

На экране **BMC network configuration** будет отображена информация о IP-адресе BMC, как показано на Рис. 4-10.

Рис. 4-10 Экран конфигурации сети BMC



Шаг 5 Выберите параметр и нажмите **Enter**.

В появившемся диалоговом окне можно изменить значение параметра.

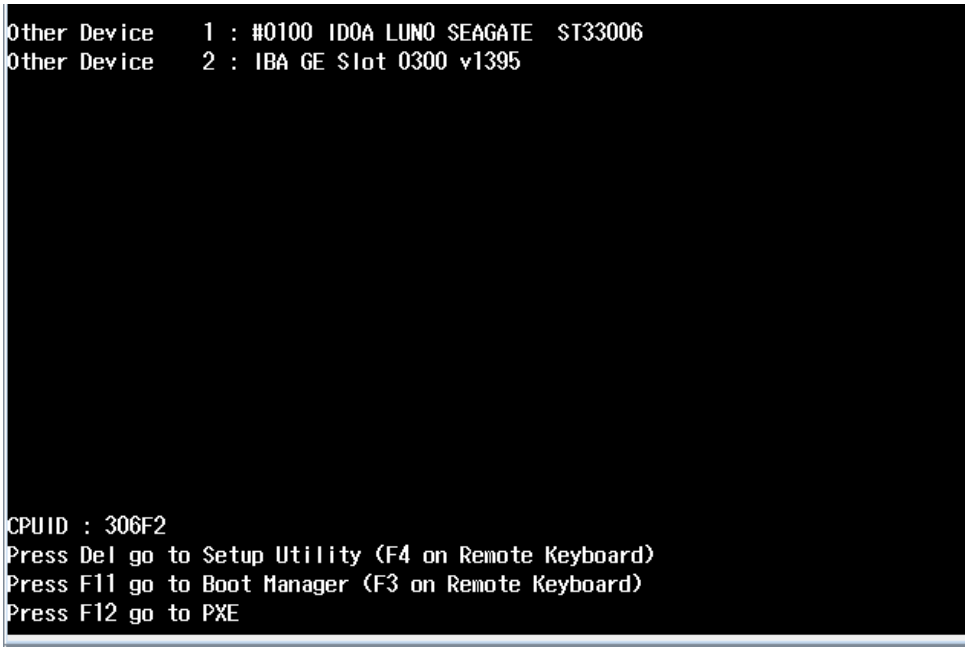
----Конец

Запрос и установка IP-адреса в BIOS для других стоечных серверов

Шаг 1 Перезагрузите сервер.

Шаг 2 В процессе запуска когда появится следующий экран, нажмите **Delete** несколько раз подряд. Появится экран запуска BIOS.

Рис. 4-11 Экран запуска BIOS



Шаг 3 Введите пароль. Пароль по умолчанию приведен на табличке с маркировкой продукта, как показано на Рис. 4-12.

Рис. 4-12 Ввод пароля

Шаг 4 Перейдите на вкладку **Advanced** > **IPMI BMC Configuration**.

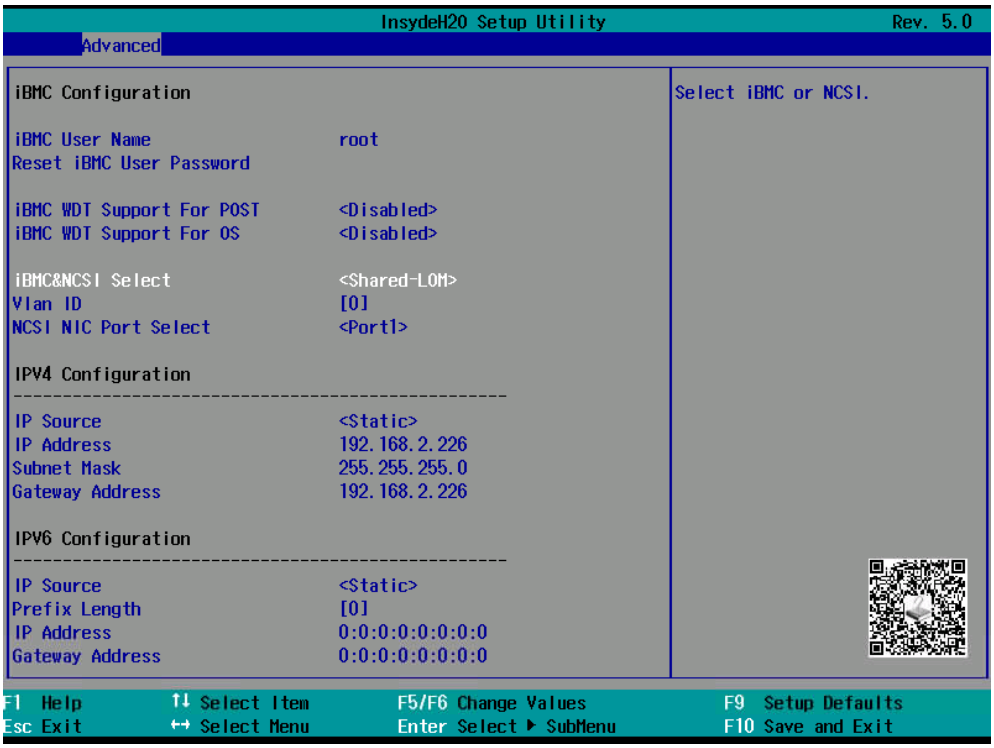
Появится окно **IPMI BMC Configuration**.

Шаг 5 Выберите **iBMC Configuration** и нажмите **Enter**.

На экране будет отображен интерфейс **iBMC Configuration**, как показано на Рис. 4-13.

На нем приведена информация об ip-адресе порта управления.

Рис. 4-13 Интерфейс конфигурации BMC



Шаг 6 Выберите параметр и нажмите **Enter**.

В появившемся диалоговом окне можно изменить значение параметра.

----Конец

4.2.3 Доступ к CLI управляющего ПО

В данном разделе приведено описание порядка доступа к CLI управляющего ПО.

Предварительные условия

Перед входом на CLI необходимо внимательно ознакомиться со следующей информацией.

- С помощью SSH максимум пять пользователей могут одновременно выполнить вход.
- Чтобы открыть CLI через сетевой порт необходимо подключить сетевой интерфейс устройства конфигурирования к сетевому интерфейсу сервера с помощью сетевого кабеля и убедиться, что IP-адреса двух сетевых интерфейсов находятся в одном сегменте сети.

ПРИМЕЧАНИЕ

Не подключайте два порта управления одновременно, так как для входа в iBMC необходим лишь один порт управления.

- Чтобы открыть CLI через последовательный порт необходимо подключить последовательный порт устройства конфигурирования к последовательному порту сервера с помощью последовательного кабеля.

  Через последовательный порт одновременно войти в систему могут максимум пять пользователей.

Стоечный сервер имеет адаптивный сетевой интерфейс управления 1000 Мбит/с на задней панели шасси. Подключиться к сетевому интерфейсу можно при помощи сетевого кабеля.

Режимы входа

- SSH
- Локальный последовательный порт

ПРИМЕЧАНИЕ

- По умолчанию в iBMC установлено имя пользователя **root** для серверов V3 и **Administrator** для серверов V5, а на табличке с маркировкой продукта указан пароль по умолчанию.
- При вводе пользователем неправильного пароля последовательно в течение 5 раз подряд, система заблокирует учетную запись пользователя. Разблокировка произойдет автоматически через 5 минут, или администратор может разблокировать учетную запись пользователя с помощью интерфейса командной строки.
- В целях безопасности после первого входа в систему рекомендуется изменять исходный пароль и периодически менять пароль в дальнейшем.
- По умолчанию период ожидания CLI составляет 15 минут.

Вход через SSH

Для безопасного удаленного доступа и других сетевых сервисов в небезопасной сети используется протовол SSH.

ПРИМЕЧАНИЕ

SSH поддерживает следующие алгоритмы шифрования: **AES128-CTR**, **AES192-CTR** и **AES256-CTR**. При входе в iBMC через SSH используется поддерживаемый алгоритм шифрования.

1. Загрузите инструмент связи SSH на локальный клиент.
2. Подключите клиент к сетевому порту управления сервера напрямую или через сеть.
3. Задайте IP-адрес клиента, чтобы клиент мог взаимодействовать с сетевым портом управления iBMC на сервере.
4. В клиенте откройте инструмент SSH и установите соответствующие параметры, такие как IP-адрес.
5. Подключитесь к iBMC и введите имя пользователя и пароль.

ПРИМЕЧАНИЕ

- Локальные и LDAP-пользователи могут войти в интерфейс командной строки iBMC через SSH.
- Чтобы войти в iBMC, LDAP-пользователям не нужно вводить информацию о сервере домена, так как система настраивает её автоматически.

Вход через последовательный порт

Через последовательный порт одновременно войти в систему могут максимум пять пользователей.

ВНИМАНИЕ

Перед входом в CLI iBMC через последовательный порт убедитесь, что данный порт сконфигурирован в качестве последовательного порта iBMC. Для переключения между последовательными портами войдите в CLI по SSH и выполните команду 4.3.11 Запрос и перенаправление последовательного порта (serialdir) или используйте джампер, в соответствии с документацией к серверному продукту.

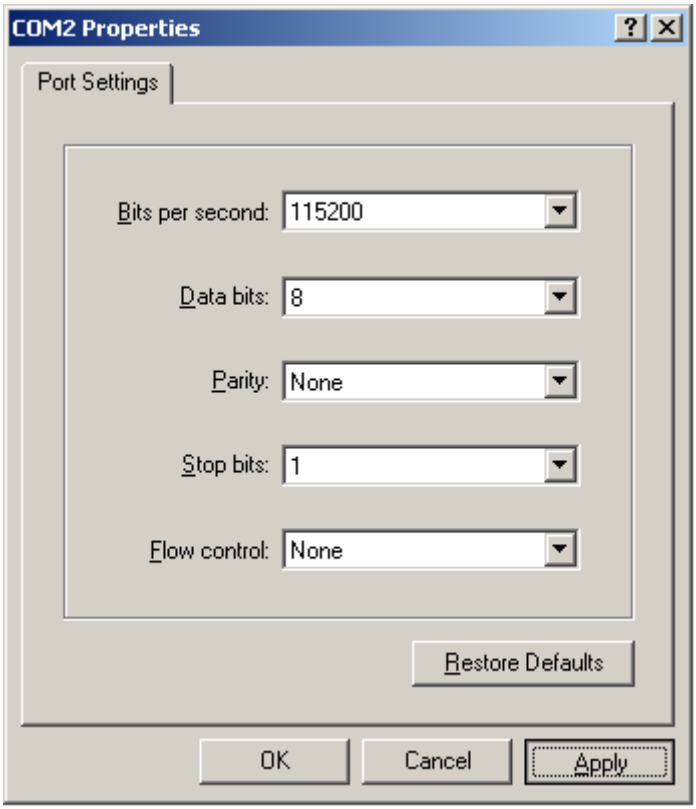
Шаг 1 Подключите последовательный кабель.

Шаг 2 Войдите в CLI с помощью HyperTerminal и настройте следующие параметры:

- Baud rate: 115200
- Data bits: 8
- Parity check: None
- Stop bits: 1
- Flow control: None

Подробная информация о порядке установки параметров приведена на Рис. 4-14.

Рис. 4-14 Свойства **HyperTerminal**



Шаг 3 На странице входа введите имя пользователя и пароль.

----Конец

4.3 Команды iBMC

В данном разделе приведено описание всех команд iBMC.

4.3.1 Запрос IP-информации iBMC (ipinfo)

Функция

Команда **ipinfo** используется для запроса IP-адреса сетевого порта управления iBMC.

Формат

ipmcget -d ipinfo

Параметры

–

Инструкции по использованию

–

Пример

Запросите IP-адрес iBMC.

```
iBMC:/->ipmcget -d ipinfo
```

Ответная информация системы RH8100 V3:

```
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  192.168.2.100
Subnet Mask         :  255.255.0.0
Default Gateway      :  192.168.2.25
MAC Address         :  00:18:e1:c5:d8:26
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address        :  2001::2001/15
Default Gateway IPv6  :  2001::2003
Link-Local Address    :  fe80::218:e1ff:fec5:d826/64
VLAN Information     :
VLAN State          :  disabled

EthGroup ID         :  2
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  10.0.0.1
Subnet Mask         :  255.255.255.252
Default Gateway      :
MAC Address         :
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address 1       :  2001::2001/15
Default Gateway IPv6  :  2001::2003
Link-Local Address    :  fe80::218:e1ff:fec5:d826/64
IPv6 Address 2       :  2411:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 3       :  2311:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 4       :  2211:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 5       :  2111:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 6       :  2901:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 7       :  2801:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 8       :  2701:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 9       :  2601:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 10      :  2501:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 11      :  2401:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 12      :  2301:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 13      :  2201:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 14      :  2101:db8:1:0:218:e1ff:fec5:d826/64
```

```
IPv6 Address 15      :  2001:db8:1:0:218:e1ff:fec5:d826/64
VLAN Information     :
VLAN State           :  enabled
VLAN ID              :  4094
```

ПРИМЕЧАНИЕ

- GROUP1 используется для внешнего доступа.
- GROUP2 используется для внутренней передачи данных.

Ответная информация системы для других стоечных серверов:

```
EthGroup ID          :  1
Net Mode             :  Manual
Net Type             :  Dedicated
IPv4 Information     :
IP Mode              :  static
IP Address           :  192.168.2.100
Subnet Mask          :  255.255.0.0
Default Gateway IP   :  192.168.0.25
MAC Address          :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode            :  static
IPv6 Address 1       :  2001::2001/15
Default Gateway IPv6 :  2001::2003
Link-Local Address   :  fe80::218:e1ff:fec5:d826/64
IPv6 Address 2       :  2411:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 3       :  2311:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 4       :  2211:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 5       :  2111:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 6       :  2901:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 7       :  2801:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 8       :  2701:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 9       :  2601:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 10      :  2501:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 11      :  2401:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 12      :  2301:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 13      :  2201:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 14      :  2101:db8:1:0:218:e1ff:fec5:d826/64
IPv6 Address 15      :  2001:db8:1:0:218:e1ff:fec5:d826/64
VLAN Information     :
VLAN State           :  disabled
```

4.3.2 Настройка IPv4-адреса iBMC (ipaddr)

Функция

Команда **ipaddr** используется для настройки IPv4-адреса, маски подсети и адреса шлюза для iBMC.

Формат

ipmcset -d ipaddr -v <*ipaddr*> <*mask*> [*gateway*]

Параметры

Параметр	Описание	Значение
ipaddr	IPv4-адрес для iBMC.	IPv4-адрес в формате *xxx.xxx.xxx.xxx*.
mask	Маска подсети для iBMC.	IPv4-адрес в формате *xxx.xxx.xxx.xxx*.
gateway	Адрес шлюза для iBMC.	IPv4-адрес в формате *xxx.xxx.xxx.xxx*.

Инструкции по использованию

После изменения IP-адреса новый IP-адрес вступает в силу немедленно. Для повторного входа следует использовать новый IP-адрес.

Не устанавливайте для *ipaddr* значения от **10.0.0.0** до **10.0.0.3**, потому что эти IP-адреса зарезервированы для внутренней связи.

Пример

Установка для IP-адреса сетевого интерфейса управления iBMC значения **192.168.0.25**, для маски подсети – значения **255.255.255.0** и для шлюза – значения **192.168.0.25**.

```
iBMC:/->ipmcset -d ipaddr -v 192.168.0.25 255.255.255.0 192.168.0.25
Set IP address successfully.
Set MASK address successfully.
Set GateWay successfully.
```

Запрос измененного IP-адреса сетевого интерфейса управления iBMC.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  192.168.0.25
Subnet Mask         :  255.255.255.0
Default Gateway      :  192.168.0.25
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  dhcp
IPv6 Address        :
Default Gateway IPv6  :
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             :  1
```

4.3.3 Настройка режима IPv4 iBMC (ipmode)

Функция

Команда **ipmode** используется для указания порядка назначения IPv4-адреса iBMC.

Формат

ipmcset -d ipmode -v <dhcp | static>

Параметры

Параметр	Описание	Значение
dhcp	Сервер DHCP динамически назначает IP-адрес для iBMC.	–
static	iBMC использует статический IP-адрес.	–

Инструкции по использованию

После изменения режима IPv4 новая конфигурация вступает в силу немедленно.

Пример

Активация iBMC для использования IPv4-адреса, динамически назначенного сервером DHCP.

```
iBMC:/->ipmcset -d ipmode -v dhcp
Set dhcp mode successfully.
```

Запрос IP-адреса iBMC.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  dhcp
IP Address          :  192.168.0.12
Subnet Mask         :  255.255.0.0
Default Gateway      :  192.168.0.25
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  dhcp
IPv6 Address         :
Default Gateway IPv6  :
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             :  1
```

ПРИМЕЧАНИЕ

Для просмотра нового IP-адреса 192.168.0.12, полученного сетевым интерфейсом управления iBMC от сервера DHCP, выполните команду **ipinfo** .

4.3.4 Настройка IPv4-адреса шлюза iBMC (gateway)

Функция

Команда **gateway** используется для настройки IPv4-адреса шлюза iBMC.

Формат

ipmcset -d gateway -v <*gateway*>

Параметры

Параметр	Описание	Значение
gateway	IPv4-адрес шлюза iBMC.	IPv4-адрес в формате *xxx.xxx.xxx.xxx*.

Инструкции по использованию

После изменения адреса шлюза новый адрес вступает в силу немедленно.

Пример

Установка значения **192.168.0.1** в качестве адреса шлюза iBMC.

```
iBMC:/->ipmcset -d gateway -v 192.168.0.1
Set gateway successfully.
```

Запрос нового адреса шлюза iBMC.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  192.168.0.25
Subnet Mask         :  255.255.255.0
Default Gateway      :  192.168.0.1
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  dhcp
IPv6 Address        :
Default Gateway IPv6  :
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             :  1
```

4.3.5 Настройка IPv6-адреса iBMC (ipaddr6)

Функция

Команда **ipaddr6** используется для настройки IPv6-адреса, длины префикса и адреса шлюза iBMC.

Формат

ipmcset -d ipaddr6 -v <*ipaddr6*/*prefixlen*> [*gateway6*]

Параметры

Параметр	Описание	Значение
ipaddr6	IPv6-адрес для iBMC.	Длина IP-адреса составляет 128 бит и состоит из восьми 16-битовых полей: **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**. Большинство IPv6-адресов не занимают все 128 бит и их можно сократить. Кроме того, нотация с двумя двоеточиями (::) может использоваться для представления смежных 16-битовых полей нулей, а ведущие нули в поле можно опустить. Например, IPv6-адреса **2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b** могут быть сокращены до **2001:db8:3c4d:15::1a2f:1a2b**.
prefixlen	Длина префикса для iBMC.	от 0 до 128
gateway6	IPv6-адрес шлюза для iBMC.	Длина IP-адреса составляет 128 бит и состоит из восьми 16-битовых полей: **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**. Большинство IPv6-адресов не занимают все 128 бит и их можно сократить. Кроме того, нотация с двумя двоеточиями (::) может использоваться для представления смежных 16-битовых полей нулей, а ведущие нули в поле можно опустить. Например, IPv6-адреса **2001:0db8:3c4d:0015:0000:0000:1a2f:1a20** могут быть сокращены до **2001:db8:3c4d:15::1a2f:1a20**.

Инструкции по использованию

После изменения IPv6-адреса новый IP-адрес вступает в силу немедленно.

Кроме IPv6-адреса для доступа к iBMC может использоваться **Link-Local Address**. Для получения **Link-Local Address** выполните команду **ipmcget**.

Пример

Установка значения **2011::6516** в качестве IPv6-адреса iBMC, длины префикса – **64** и значения шлюза IPv6 – **2011:1**.

```
iBMC:/->ipmcset -d ipaddr6 -v 2011::6516/64 2011:1
Set IPV6 address successfully.
Set IPV6 prefix successfully.
Set IPv6 gateway6 successfully.
```

v

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  192.168.0.25
Subnet Mask         :  255.255.0.0
Default Gateway      :  192.168.0.1
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address        :  2011::6516
Default Gateway IPv6  :  2011::1
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             :  1
```

4.3.6 Настройка режима IPv6 iBMC (ipmode6)

Функция

Команда **ipmode6** используется для указания порядка назначения IPv6-адреса iBMC.

Формат

ipmcset -d ipmode6 -v <dhcp | static>

Параметры

Параметр	Описание	Значение
dhcp	Сервер DHCP динамически выделяет IP-адрес для iBMC.	–
static	iBMC использует статический IP-адрес.	–

Инструкции по использованию

После изменения режима IPv6 новая конфигурация вступает в силу немедленно.

Пример

Активация iBMC для использования IPv6-адреса, динамически выделенного сервером DHCP.

```
iBMC:/->ipmcset -d ipmode6 -v dhcp
Set dhcp mode successfully.
```

Запрос IP-адреса iBMC.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  dhcp
IP Address          :  192.168.0.12
Subnet Mask         :  255.255.0.0
Default Gateway      :  192.168.0.25
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  dhcp
IPv6 Address        :
Default Gateway IPv6  :
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             :  1
```

4.3.7 Настройка IPv6-адреса шлюза iBMC (gateway6)

Функция

Команда **gateway6** используется для настройки IPv6-адреса шлюза сетевого порта управления iBMC.

Формат

ipmcset -d gateway6 -v <*gateway6*>

Параметры

Параметр	Описание	Значение
gateway6	IPv6-адрес шлюза сетевого порта управления iBMC.	Длина IP-адреса составляет 128 бит и состоит из восьми 16-битовых полей: **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**. Большинство IPv6-адресов не занимают все 128 бит и их можно сократить. Кроме того, нотация с двумя двоеточиями (::) может использоваться для представления смежных

Параметр	Описание	Значение
		16-битовых полей нулей, а ведущие нули в поле можно опустить. Например, IPv6-адреса **2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b** могут быть сокращены до **2001:db8:3c4d:15::1a2f:1a2b**.

Инструкции по использованию

После изменения адреса шлюза новый адрес вступает в силу немедленно.

Пример

Установка значения **2001::1** в качестве IPv6-адреса шлюза iBMC.

```
iBMC:/->ipmcset -d gateway6 -v 2001::1
Set gateway6 successfully.
```

Запрос нового адреса шлюза iBMC.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  dhcp
IP Address          :  192.168.0.12
Subnet Mask         :  255.255.0.0
Default Gateway      :  192.168.0.25
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address        :  2001::65
Default Gateway IPv6  :  2001::1
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             :  1
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  192.168.0.25
Subnet Mask         :  255.255.255.0
Default Gateway      :  192.168.0.25
MAC Address         :  00:18:e1:c5:d8:26
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address        :  2001::65
Default Gateway IPv6  :  2001::1
Link-Local Address    :  fe80::218:e1ff:fec5:d826/64
```

```
VLAN Information     :
VLAN State          :  disabled

EthGroup ID         :  2
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  10.0.0.1
Subnet Mask         :  255.255.255.252
Default Gateway      :
MAC Address         :
IPv6 Information     :
IPv6 Mode           :  static
IPv6 Address        :
Default Gateway IPv6  :
Link-Local Address    :  fe80::218:e1ff:fec5:d887/64
VLAN Information     :
VLAN State          :  enabled
VLAN ID             :  4094
```

4.3.8 Настройка режима сетевого порта (netmode)

Функция

Команда **netmode** используется для указания сетевого порта iBMC.

Формат

ipmcset -d netmode -v <*option*>

Параметры

Параметр	Описание	Значение
option	Сетевой порт iBMC.	• **1**: **Manual** • **2**: **Adaptive** Значение по умолчанию: **1**

Инструкции по использованию

- Если для параметра *option* установлено значение **1**, необходимо вручную настроить сетевой порт управления iBMC.
- Если для параметра *option* установлено значение **2**, необходимо указать сетевые порты для автосогласования. Выделенный порт iBMC имеет приоритет над другими указанными сетевыми портами. Если выделенный сетевой порт iBMC недоступен, сетевой порт будет выбран из других доступных портов.

Пример

Включение вручную указанного сетевого порта iBMC.

```
iBMC:/->ipmcset -d netmode -v 1
Set net mode Manual successfully.
```

Запрос режима сетевого порта iBMC.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  128.5.197.98
Subnet Mask         :  255.255.224.0
Default Gateway      :  128.5.197.98
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  dhcp
IPv6 Address         :
Default Gateway IPv6  :
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             :  1
```

4.3.9 Настройка активного порта iBMC (activeport)

Функция

Команда **activeport** используется для настройки активного сетевого порта управления iBMC.

Формат

ipmcset -d activeport -v <*option*> [*portid*]

Параметры

Параметр	Описание	Значение
option	Тип порта	• **0**: выделенный сетевой порт • **1**: порт на LOM • **2**: порт на плате PCIe • **3**: сетевой порт агрегации **ПРИМЕЧАНИЕ** Диапазон значений зависит от модели сервера.
portid	Номер порта	–

Инструкции по использованию

Для выделенного сетевого порта iBMC нет необходимости указывать *portid*.

Пример

Установка выделенного сетевого порта в качестве порта iBMC.

```
iBMC:/->ipmcset -d activeport -v 0
Set active port successfully.
```

Запрос информации о порте iBMC.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  128.5.197.98
Subnet Mask         :  255.255.224.0
Default Gateway      :  128.5.197.98
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  dhcp
IPv6 Address        :
Default Gateway IPv6  :
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
VLAN ID             :  1
```

4.3.10 Настройка ID VLAN для сетевого порта (vlan)

Функция

Команда **vlan** используется для настройки ID VLAN порта внеполосного интерфейса сетевого контроллера (NC-SI) iBMC. NC-SI позволяет сетевому порту работать в качестве порта iBMC.

Формат

ipmcset -d vlan -v <off | *id*>

Параметры

Параметр	Описание	Значение
off	Отключение VLAN.	–
vlanid	Идентификация VLAN, к которой принадлежит сетевой порт.	от 1 до 4094 от 1 до 4093

Инструкции по использованию

–

Пример

#Установка значения **405** в качестве ID VLAN сетевого порта управления iBMC.

```
iBMC:/->ipmcset -d vlan -v 405
Set vlan state successfully.
```

Запрос интформации о vlan сетевого порта.

```
iBMC:/->ipmcget -d ipinfo
EthGroup ID         :  1
Net Mode            :  Manual
Net Type            :  Dedicated
IPv4 Information     :
IP Mode             :  static
IP Address          :  128.5.197.98
Subnet Mask         :  255.255.224.0
Default Gateway      :  128.5.197.98
MAC Address         :  00:18:e1:c5:d8:66
IPv6 Information     :
IPv6 Mode           :  dhcp
IPv6 Address        :
Default Gateway IPv6  :
Link-Local Address    :  fe80::218:e1ff:fec5:d866/64
VLAN Information     :
VLAN State          :  disabled
```

4.3.11 Запрос и перенаправление последовательного порта (serialdir)

Функция

Команда **serialdir** используется для запроса и настройки перенаправления последовательного порта.

Формат

ipmcget -d serialdir

ipmcset -d serialdir -v <*option*>

Параметры

Параметр	Описание	Значение
<*option*>	Используемый последовательный порт.	• **0**: перенаправление последовательного порта на панели сервера на последовательный порт системы. • **1**: перенаправление последовательного порта на панели сервера на последовательный порт iBMC. • **2**: перенаправление порта SOL на последовательный порт системы. • **3**: перенаправление порта SOL на последовательный порт iBMC. Диапазон значений данного параметра зависит от модели сервера. Перед настройкой последовательного порта выполните команду **ipmcget -d serialdir** для запроса диапазона значений данного параметра.

Инструкции по использованию

Настройка перенаправления порта SOL имеет приоритет над настройкой последовательного порта на панели сервера. При перенаправлении порта SOL на последовательный порт системы или iBMC, который в настоящее время перенаправляется из последовательного порта на панели сервера, последовательный порт на панели сервера станет временно недоступен. Исходные настройки последовательного порта на панели сервера будут восстановлены только после отключения порта SOL.

Пример

Перенаправление последовательного порта на панели сервера на последовательный порт iBMC.

```
iBMC:/->ipmcset -d serialdir -v 1
Set serial port direction successfully.
```

Запрос информации о перенаправлении последовательного порта.

```
iBMC:/->ipmcget -d serialdir
Currently connected serial direction :
Num         Source               Destination
1           PANEL COM            BMC COM
```

4.3.12 Перезапуск системы iBMC (reset)

Функция

Команда **reset** используется для перезапуска системы iBMC.

Формат

ipmcset -d reset

Параметры

–

Инструкции по использованию

- В односистемном режиме выполнение команды **restart** на основной системе iBMC приведет к одновременному перезапуску основной и вспомогательной системы iBMC.
- В двусистемном режиме команды **restart** приведет к перезапуску только той системы iBMC, на которой выполняется эта команда.

Пример

Перезапуск системы iBMC.

```
iBMC:/->ipmcset -d reset
This operation will reboot iBMC system. Continue? [Y/N]:y
Resetting...
```

4.3.13 Обновление встроенного ПО (upgrade)

Функция

Команда **upgrade** используется для обновления встроенного ПО сервера, которое включает встроенное ПО iBMC, BIOS, SD-карты, а также сложного программируемого логического устройства (CPLD).

Формат

ipmcset -d upgrade -v <*filepath*>

Параметры

Параметр	Описание	Значение
filepath	Абсолютный путь к файлу обновления. **ПРИМЕЧАНИЕ** Поддерживается только файл **xxx.hpm**.	Пример значения: **/tmp/image.hpm**.

Инструкции по использованию

Используйте инструмент передачи файлов, чтобы загрузить файл обновления в определенный каталог iBMC на целевом сервере и выполните эту команду.

- В односистемном режиме выполнение команды **upgrade** на основной системе iBMC приведет к одновременному обновлению основной и вспомогательной системы iBMC.

- В двусистемном режиме команда **upgrade** приведет к обновлению только той системы iBMC, на которой выполняется эта команда.

После завершения обновления контроллера iBMC или SD-карты iBMC автоматически перезагрузится, чтобы обновление вступило в силу.

Пример

Обновление встроенного ПО.

```
iBMC:/->ipmcset -d upgrade -v /tmp/image.hpm
Please make sure the iBMC is working while upgrading!
Updating...
100%
Update successfully.
```

4.3.14 Фото экрана (printscreen)

Функция

Команда **printscreen** используется для создания скриншота экрана сервера.

Формат

ipmcset -d printscreen [-v wakeup]

Параметры

Параметр	Описание	Значение
wakeup	Выход системы из спящего режима.	–

Инструкции по использованию

Сделанный скриншот автоматически сохраняется в виде файла **manualscreen.jpeg** в каталоге **/tmp/web**. Передайте файл клиенту с помощью инструмента передачи файлов, а затем просмотрите его.

ВНИМАНИЕ

При запуске команды **printscreen** несколько раз сохранится только последний скриншот.

Пример

Скриншот экрана сервера.

```
iBMC:/->ipmcset -d printscreen
Download print screen image to /tmp/manualscreen.jpeg successfully.
```

4.3.15 Возврат к предыдущей версии ПО iBMC (rollback)

Функция

Команда **rollback** используется для переключения встроенного ПО iBMC из файла образа основного раздела диска в файл образа вспомогательного раздела.

Формат

ipmcset -d rollback

Параметры

–

Инструкции по использованию

- В односистемном режиме выполнение команды **rollback** на основной системе iBMC приведет к одновременному возврату к предыдущей версии основной и вспомогательной системы iBMC.
- В двусистемном режиме команда **rollback** приведет к возврату к предыдущей версии только той системы iBMC, на которой выполняется эта команда.
- Эта команда переключает встроенное ПО iBMC из файла образа основного раздела диска в файл образа вспомогательного раздела. Если файлы образов в основном и вспомогательном разделах имеют одну и ту же версию, версия не изменяется после выполнения данной команды.

Пример

Возврат к предыдущей версии ПО iBMC.

```
iBMC:/->ipmcset -d rollback
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Set rollback successfully, system will reboot soon!
```

4.3.16 Запрос результата возврата к предыдущей версии ПО iBMC (rollbackstatus)

Функция

Команда **rollbackstatus** используется для запроса результата возврата к предыдущей версии ПО iBMC.

Формат

ipmcget -d rollbackstatus

Параметры

–

Инструкции по использованию

–

Пример

Запрос результата возврата к предыдущей версии ПО iBMC.

```
iBMC:/->ipmcget -d rollbackstatus
Last rollback success!
```

4.3.17 Настройка статуса обслуживания (service -d state)

Функция

Команда **service -d state** используется для настройки статуса обслуживания для iBMC.

Формат

ipmcset -t service -d state -v <*option*> <**enabled** | **disabled**>

Параметры

Параметр	Описание	Значение
option	Тип сервиса.	• SSH • SNMP • KVM • VMM • Video • HTTP • HTTPS • RMCP • RMCP+ • SSDP
enabled	Активация сервиса	–
disabled	Деактивация сервиса	–

Инструкции по использованию

Значение параметра *option* не чувствительно к регистру.

Активация сервиса HTTP может привести к появлению определенных рисков безопасности.

Пример

Активация сервиса HTTP.

```
iBMC:/->ipmcset -t service -d state -v http enabled
Set http service state(enabled) successfully.
```

4.3.18 Настройка номера сервисного порта (service -d port)

Функция

Команда **service -d port** используется для настройки номера сервисного порта.

Формат

ipmcset -t service -d port -v <*option*> <*port1value*> [*port2value*]

Параметры

Параметр	Описание	Значение
option	Тип сервиса	• SSH • SNMP • KVM • VMM • Video • HTTP • HTTPS • RMCP
port1value	Номер порта	от 1 до 65535
port2value	Номер сервисного порта. Данный номер порта доступен только для сервиса RMCP.	от 1 до 65535

Инструкции по использованию

Если для номера порта веб-сервера (HTTP) или (HTTPS) установлено значение **65535**, Google Chrome не может установить сеанс через этот порт.

Пример

Установка значения **443** для порта HTTPS.

```
iBMC:/->ipmcset -t service -d port -v https 443
Set https service port to 443 successfully.
```

4.3.19 Запрос сервисной информации (service -d list)

Функция

Команда **service -d list** используется для запроса сервисной информации.

Формат

ipmcget -t service -d list

Параметры

–

Инструкции по использованию

–

Пример

Запрос сервисной информации.

```
iBMC:/->ipmcget -t service -d list
service name   |  state        |  port
SSH            |  Enabled      |  22
SNMP           |  Enabled      |  168
KVM            |  Disabled     |  2001
VMM            |  Disabled     |  8001
Video          |  Enabled      |  2200
HTTP           |  Enabled      |  80
HTTPS          |  Enabled      |  443
RMCP           |  Disabled     |  1004,184
RMCP+          |  Enabled      |  1004,184
SSDP           |  Enabled      |  1004,184
```

4.3.20 Настройка статуса включения сообщения безопасности при входе в систему (securitybanner -d state)

Функция

Команда **securitybanner -d state** используется для настройки отображения сообщения системы безопасности при входе на iBMC.

Формат

ipmcset -t securitybanner -d state -v <enabled | disabled>

Параметры

Параметр	Описание	Значение
enabled	Сообщение системы безопасности будет отображаться на странице входа.	–
disabled	Сообщение системы безопасности не будет отображаться на странице входа.	–

Инструкции по использованию

–

Пример

Настройка для iBMC отображения сообщения системы безопасности на странице входа.

```
iBMC:/->ipmcset -t securitybanner -d state -v enabled
Enable login security banner state successfully.
```

4.3.21 Настройка сообщения системы безопасности при входе (securitybanner -d content)

Функция

Команда **securitybanner -d content** используется для настройки сообщения системы безопасности при входе в iBMC.

Формат

ipmcset -t securitybanner -d content -v <**default** | *"option"*>

Параметры

Параметр	Описание	Значение
default	Сообщение системы безопасности, установленное по умолчанию.	–
option	Настройка сообщения системы безопасности.	Строка от 0 до 1600 символов

Инструкции по использованию

–

Пример

Установка сообщения системы безопасности при входе как сообщения по умолчанию.

```
iBMC:/-> ipmcset -t securitybanner -d content -v default
Set login security banner content successfully.
```

4.3.22 Запрос сообщения системы безопасности при входе (securitybanner -d info)

Функция

Команда **securitybanner -d info** используется для запроса сообщения системы безопасности при входе в iBMC.

Формат

ipmcget -t securitybanner -d info

Параметры

–

Инструкции по использованию

–

Пример

Запрос сообщения системы безопасности при входе.

```
iBMC:/-> ipmcget -t securitybanner -d info
Login security banner information state: enabled.

Login security banner information:
WARNING! This system is PRIVATE and PROPRIETARY and may only be accessed by authorized
users. Unauthorized use of the system is prohibited. The owner, or its agents, may monitor
any activity or communication on the system. The owner, or its agents, may retrieve
any information stored within the system. By accessing and using the system, you are
consenting to such monitoring and information retrieval for law enforcement and other
purposes.
```

4.3.23 Импортирование сертификата SSL (certificate -d import)

Функция

Команда **certificate -d import** используется для импорта сертификата SSL (Secure Sockets Layer – уровень защищенных сокетов) в iBMC.

Формат

ipmcset -t certificate -d import -v <*filepath* | *file_URL*> <*type*> [*passphrase*]

Параметры

Параметр	Описание	Значение
filepath	Каталог, в который будет импортирован сертификат SSL. **ПРИМЕЧАНИЕ** Файл сертификата должен быть в формате *.pfx или *.p12 и не может превышать 100 КБ.	Абсолютный путь к сертификату на iBMC, например, **/tmp/test.pfx**.
file_URL	URL-адрес импортируемого сертификата SSL.	Формат: *protocol*://*username*:*password@IP:[port]*/*directory/filename* Где: • *protocol* должен быть в формате **https**, **sftp**, **cifs** или **scp**. • *username* – имя пользователя, используемого для входа на целевой сервер. • *password* – пароль, используемый для входа на целевой сервер. • *IP:[port]* – IP-адрес и номер порта целевого сервера. • *directory/filename* – абсолютный путь к сертификату SSL на целевом сервере. Например, **https://root:Huawei12#$@10.10.10.1:443/tmp/test.pfx**.
type	Тип сертификата SSL.	Установлено фиксированное значение **1**.
passphrase	Пароль сертификата SSL.	Значение данного параметра можно не указывать.

Инструкции по использованию

–

Пример

Импорт сертификата SSL.

```
iBMC:/-> ipmcset -t certificate -d import -v /tmp/test-01.pfx 1 Huawei12#$
Import certificate successfully
Reset iBMC for the certificate to take effect.
```

4.3.24 Запрос информации сертификата SSL (certificate -d info)

Функция

Команда **certificate -d info** используется для запроса информации сертификата SSL.

Формат

ipmcget -t certificate -d info

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации сертификата SSL.

```
iBMC:/-> ipmcget -t certificate -d info
SSL Certificate Information:
Issued    To: CN=Server, OU=IT, O=Huawei, L=ShenZhen, S=GuangDong, C=CN
Issued    By: CN=Server, OU=IT, O=Huawei, L=ShenZhen, S=GuangDong, C=CN
Valid   From: Jul 25 2014 GMT
Valid     To: Jul 22 2024 GMT
Serial Number: 07
```

4.3.25 Экспорт файла конфигурации (config -d export)

Функция

Команда **config -d export** используется для экспорта файлов конфигурации iBMC, BIOS и RAID-контроллера.

Формат

ipmcget -t config -d export -v <*filepath* | *file_URL*>

Параметры

Параметр	Описание	Значение
filepath	Каталог для экспорта файла конфигурации.	Абсолютный путь к файлу конфигурации на iBMC. Пример значения: **/tmp/config.xml**
file_URL	URL-адрес	Формат:

Параметр	Описание	Значение
	экспортируемого файла конфигурации.	*protocol*://*username*:*password@IP:[port]*/*directory/filename* Где: • *protocol* должен быть **https**, **sftp**, **cifs**, **scp** или **nfs**. • *username* – имя пользователя, используемого для входа на целевой сервер. • *password* – пароль для входа на целевой сервер. • *IP:[port]* – IP-адрес и номер порта целевого сервера. • *directory/filename* – абсолютный путь к файлу конфигурации на целевом сервере. Пример значения: **https://root:Huawei12#$@10.10.10.1:443/tmp/config.xml**

Инструкции по использованию

–

Пример

Экспорт файла конфигурации.

```
iBMC:/-> ipmcget -t config -d export -v /tmp/testconfig.xml
NOTE: The exported RAID Controller configurations are valid only if they are exported
after the POST is complete.
Collecting configuration...
100%
Export configuration successfully.
```

4.3.26 Импорт файла конфигурации (config -d import)

Функция

Команда **config -d import** используется для импорта файлов конфигурации iBMC, BIOS и RAID-контроллера.

Формат

ipmcset -t config -d import -v <*filepath* | *file_URL*>

Параметры

Параметр	Описание	Значение
filepath	Каталог для импорта файла конфигурации.	Абсолютный путь к файлу конфигурации на iBMC. Пример значения: **/tmp/config.xml**
file_URL	URL-адрес импортируемого файла конфигурации.	Формат: *protocol*://*username*:*password@IP:[port]*/*directory/filename* Где: • *protocol* должен быть **https**, **sftp**, **cifs**, **scp** или **nfs**. • *username* – имя пользователя, используемого для входа на целевой сервер. • *password* – пароль для входа на целевой сервер. • *IP:[port]* – IP-адрес и номер порта целевого сервера. • *directory/filename* – абсолютный путь к файлу конфигурации на целевом сервере. Пример значения: **https://root:Huawei12#$@10.10.10.1:443/tmp/config.xml**

Инструкции по использованию

–

Пример

Импорт файла конфигурации.

```
iBMC:/-> ipmcset -t config -d import -v /tmp/testconfig.xml
Setting configuration...
100%
Import configuration successfully.
Reset OS for the BIOS config to take effect.
```

4.3.27 Импорт файла CRL (crl)

Функция

Команда **crl** используется для импорта файла со списком аннулированных сертификатов (CRL), который применяется для проверки целостности пакета обновления.

Формат

ipmcset -d crl -v <*localpath*/*URL*> <*type*>

Параметры

Параметр	Описание	Значение
localpath	Каталог, в который импортируется файл CRL на iBMC. **ПРИМЕЧАНИЕ** Формат файла должен быть ***.crl**, а размер менее 100 КБ.	Абсолютный каталог на iBMC, например, **/tmp/cms.crl**.
URL	URL-адрес импортируемого файла CRL.	Имеет следующий формат: *protocol*://*username*:*password@IP:[port]*/*directory/filename* Где • *protocol* должен быть **https**, **sftp**, **cifs**, **scp** или **nfs**. • *username* – имя пользователя, используемого для входа на целевой сервер. • *password* – пароль для входа на целевой сервер. • *IP:[port]* – IP-адрес и номер порта целевого сервера. • *directory/filename* – абсолютный каталог, в который сохраняется файл CRL на целевом сервере. Пример значения: **https://root:Huawei12#$@10.10.10.1:443/tmp/cms.crl**
type	Тип файла CRL.	Установлено фиксированное значение **1**.

Инструкции по использованию

Данная команда доступна только для серверов V5.

Пример

Импорт файла CRL.

```
iBMC:/-> ipmcset -d crl -v /tmp/cms.crl 1
Import CRL file successfully.
```

4.3.28 Монтировка файла на виртуальный CD-диск (vmm -d connect)

Функция

Команда **vmm -d connect** используется для монтировки файла на виртуальный CD-диск.

Формат

ipmcset -t vmm -d connect -v <*file_URL*>

Параметры

Параметр	Описание	Значение
file_URL	Исходный каталог монтируемого файла.	Формат: *protocol*://[*username*:*password@*]*IP:[port]*/*directory/filename* Где: • Значение *protocol* должно быть **nfs** или **cifs**. • *username* – имя пользователя, используемого для входа на целевой сервер. • *password* – пароль, используемый для входа на целевой сервер. • *IP:[port]* – IP-адрес и номер порта целевого сервера. • *directory/filename* – абсолютный каталог, в который сохраняется файл на целевом сервере. Например, nfs://192.168.44.178/home/admin/nfsserver/rhel-server-6.3-x86_64-dvd.iso. **ПРИМЕЧАНИЕ** file_URL может содержать до 255 символов.

Инструкции по использованию

–

Пример

Монтировка **rhel-server-6.3-x86_64-dvd.iso** на виртуальный CD-диск.

```
iBMC:/-> ipmcset -t vmm -d connect -v
nfs://192.168.44.178/home/admin/nfsserver/rhel-server-6.3-x86_64-dvd.iso

Connect virtual media...
```

```
.............
Connect virtual media successfully.
```

4.3.29 Отключение виртуального CD-диска (vmm -d disconnect)

Функция

Команда **vmm -d disconnect** используется для отключения виртуального диска CD-ROM.

Формат

ipmcset -t vmm -d disconnect

Параметры

–

Инструкции по использованию

–

Пример

Отключение виртуального CD-диска.

```
iBMC:/-> ipmcset -t vmm -d disconnect
Disconnect virtual media...
.....
Disconnect virtual media successfully.
```

4.3.30 Запрос информации о виртуальном носителе (vmm -d info)

Функция

Команда **vmm -d info** используется для запроса информации о виртуальном носителе iBMC.

Формат

ipmcget -t vmm -d info

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации о виртуальном носителе.

```
iBMC:/-> ipmcget -t vmm -d info
Virtual Media Information:
Maximum Number of Virtual Media Sessions:    1
Number of Activated Sessions          :    0
Activated Sessions URL                :
```

4.3.31 Запрос и настройка режима охлаждения

Функция

Команда **coolingpowermode** используется для настройки и запроса режима охлаждения сервера.

Формат

ipmcget -t maintenance -d coolingpowermode

ipmcset -t maintenance -d coolingpowermode -v <*option*>

Параметры

Параметр	Описание параметра	Значение
option	Режим охлаждения сервера.	• **0**: низкий режим охлаждения. • **1**: высокий режим охлаждения.

Инструкции по использованию

Данная команда может использоваться только на RH8100 V3. В двусистемном режиме работы режим охлаждения может быть установлен только на активной системе.

Пример

Установка низкого режима охлаждения сервера.

```
iBMC:/-> ipmcset -t maintenance -d coolingpowermode -v 0
Set cooling power mode to [Power saving mode] successfully.
```

Запрос текущего режима охлаждения.

```
iBMC:/-> ipmcget -t maintenance -d coolingpowermode
Power saving mode
```

4.4 Команды Trap

В данном разделе приведено описание всех trap-команд.

4.4.1 Запрос и настройка статуса прерываний SNMP (trap -d state)

Функция

Команда **trap -d state** используется для настройки и запроса статуса прерываний SNMP.

Формат

ipmcget -t trap -d state [-v <*destination*>]

ipmcset -t trap -d state -v <*destination*> <**disabled** | **enabled**>

Параметры

Параметр	Описание	Значение
destination	Пункт назначения для прерываний SNMP.	от 1 до 4
disabled	Отключение прерываний SNMP.	–
enabled	Включение прерываний SNMP.	–

Инструкции по использованию

–

Пример

Отключение прерываний SNMP для пункта назначения 1.

```
iBMC:/->ipmcset -t trap -d state -v 1 disabled
Set trap dest1 disabled successfully.
```

Запрос статуса прерываний SNMP пункта назначения 1.

```
iBMC:/->ipmcget -t trap -d state -v 1
trap dest1 state : disabled
```

4.4.2 Настройка номера порта прерываний SNMP (trap -d port)

Функция

Команда **trap -d port** используется для настройки номера порта прерываний SNMP iBMC.

Формат

ipmcset -t trap -d port -v <*destination*> <*portvalue*>

Параметры

Параметр	Описание	Значение
destination	Пункт назначения для прерываний SNMP.	Диапазон значений: от 1 до 4
portvalue	Номер порта прерываний SNMP.	Диапазон значений: от 1 до 65535 Значение по умолчанию: **162**

Инструкции по использованию

–

Пример

Установка значения **1024** для номера порта прерываний SNMP пункта назначения 1.

```
iBMC:/->ipmcset -t trap -d port -v 1 1024
Set trap dest1 port successfully.
```

4.4.3 Настройка имени сообщества прерываний SNMP (trap -d community)

Функция

Команда **trap -d community** используется для настройки имени сообщества прерываний SNMP.

Формат

ipmcset -t trap -d community

Параметры

Параметр	Описание	Значение
Community	Строка сообщества прерываний SNMP.	Значение по умолчанию: **TrapAdmin12#$** Диапазон значений различается в зависимости от того, включена ли проверка сложности пароля. • Если проверка сложности пароля отключена, то в качестве значения может использоваться строка длиной от 1 до 18 символов, состоящая из букв, цифр и специальных символов (за исключением пробелов). • Если проверка сложности пароля включена, то значение должно соответствовать следующим требованиям: – Пароль должен содержать от 8 до 18 символов – Содержать как минимум два параметра из следующих: прописные буквы от A до Z, строчные буквы от a до z, цифры от 0 до 9 – Он должен включать, как минимум, один из следующих специальных символов: `~!@#$%^&*()-_=+|[{}];:'",<.>/? – Не должен содержать пробелы.

Инструкции по использованию

–

Пример

Установка значения **mytrap** для имени сообщества прерываний SNMP.

```
iBMC:/->ipmcset -t trap -d community
New Community:
Confirm Community:
Set SNMP trap community successfully.
```

4.4.4 Настройка IP-адреса прерываний SNMP (trap -d address)

Функция

Команда **trap -d address** используется для настройки IP-адреса прерываний SNMP.

Формат

ipmcset -t trap -d address -v <*destination*> <*ipaddr*>

Параметры

Параметр	Описание	Значение
destination	Пункт назначения для прерываний SNMP.	от 1 до 4
ipaddr	IP-адрес для получения trap-сообщений SNMP.	Это может быть IPv4-адрес (в формате **xxx.xxx.xxx.xxx**), IPv6-адрес (в формате **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**) или значение может быть не указано (в формате "").

Инструкции по использованию

Если значение *ipaddr* не указано, то данная команда используется для удаления IP-адреса.

Пример

Настройка значения **10.10.10.10**. IP-адреса получения trap-сообщений

```
iBMC:/->ipmcset -t trap -d address -v 1 10.10.10.10
Set trap dest1 address successfully.
```

Удаление IP-адреса прерываний SNMP пункта назначения 1.

```
iBMC:/->ipmcset -t trap -d address -v 1 ""
Set trap dest1 address successfully.
```

4.4.5 Запрос информации о пункте назначения прерываний SNMP (trap -d trapiteminfo)

Функция

Команда **trap -d trapiteminfo** используется для запроса информации о пункте назначения прерываний SNMP, которая включает статус прерываний SNMP, IP-адрес и номер порта.

Формат

ipmcget -t trap -d trapiteminfo

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации о пункте назначения прерываний SNMP.

```
iBMC:/->ipmcget -t trap -d trapiteminfo

TrapItem Num    | state     | port      | alert address
1             | enabled   | 1024      | 10.10.10.10
2             | disabled  | 162       |
3             | disabled  | 162       |
4             | disabled  | 162       |
```

4.4.6 Запрос и настройка версии прерываний SNMP (trap -d version)

Функция

Команда **trap -d version** используется для настройки и запроса версии прерываний SNMP.

Формат

ipmcget -t trap -d version

ipmcset -t trap -d version -v <*V1* | *V2C* | *V3*>

Параметры

Параметр	Описание	Значение
V1	SNMPv1.	–
V2C	SNMPv2c.	–
V3	SNMPv3.	–

Инструкции по использованию

Значение по умолчанию: *V1*. Однако, рекомендуется использовать значение *V3*. При использовании V1 и V2C необходимо соблюдать осторожность, поскольку они несут определенные риски безопасности.

Пример

Настройка значения SNMPv2c для версии прерываний SNMP.

```
iBMC:/->ipmcset -t trap -d version -v V2C
Set trap V2C success.
```

Запрос версии прерываний SNMP.

```
iBMC:/->ipmcget -t trap -d version
Trap version : V2C
```

4.4.7 Запрос и настройка уровней серьезности аварийных сигналов прерываний SNMP (trap -d severity)

Функция

Команда **trap -d severity** используется для настройки и запроса уровней серьезности аварийных сигналов, отправляемых в trap-сообщениях SNMP.

Формат

ipmcget -t trap -d severity

ipmcset -t trap -d severity -v <*level*>

Параметры

Параметр	Описание	Значение
severityvalue	Уровень серьезности аварийных сигналов, отправляемых в trap-сообщениях SNMP.	• **none**: аварийные сигналы не отправляются. • **all**: отправлены все аварийные сигналы и события. • **normal**: отправлены только события. • **minor**: отправлены только аварийные сигналы незначительного уровня. • **major**: отправлены только аварийные сигналы серьезного уровня. • **critical**: отправлены только аварийные сигналы критического уровня.

Инструкции по использованию

Система поддерживает несколько уровней серьезности, например, **ipmcset -t trap -d severity -v normal minor**.

Пример

Активация незначительных аварийных сигналов, отправляемых в trap-сообщениях SNMP.

```
iBMC:/->ipmcset -t trap -d severity -v minor
Set trap severity successfully.
```

Запрос уровня серьезности аварийных сигналов, отправленных в trap-сообщениях SNMP.

```
iBMC:/->ipmcget -t trap -d severity
Trap severity :  minor
```

4.4.8 Запрос и настройка пользователя прерываний SNMP (trap -d user)

Функция

Команда **trap -d user** используется для настройки и запроса пользователя прерываний SNMP.

Формат

ipmcget -t trap -d user

ipmcset -t trap -d user -v <*username*>

Параметры

Параметр	Описание	Значение
username	Пользователь trap SNMPv3.	Имя пользователя, которое уже определено в системе.

Инструкции по использованию

То же имя пользователя и пароль должны быть указаны на станции управления сетью (NMS) SNMP.

Имя пользователя для trap-протокола версии V3 установлено по умолчанию **root**, а для серверов V5 – **Administrator**.

Пример

Установка значения **root** для пользователя прерываний SNMPv3.

```
iBMC:/->ipmcset -t trap -d user -v root
Set trap user root successfully.
```

Запрос пользователя прерываний SNMPv3.

```
iBMC:/->ipmcget -t trap -d user
Trap user : root
```

4.4.9 Запрос и настройка протокола аутентификации и конфиденциальности прерываний SNMP V3 (trap -d protocol)

Функция

Команда **trap -d protocol** используется для запроса и настройки протоколов аутентификации и конфиденциальности прерываний SNMPv3.

Формат

ipmcget -t trap -d protocol

ipmcset -t trap -d protocol -v <*option*>

Параметры

Параметр	Описание	Значение
option	Протоколы аутентификации и конфиденциальности для прерываний SNMPv3.	• **1**: Протокол аутентификации – MD5, протокол конфиденциальности – DES. • **2**: Протокол аутентификации – MD5, протокол конфиденциальности – AES. • **3**: Протокол аутентификации – SHA, протокол конфиденциальности – DES. • **4**: Протокол аутентификации – SHA, протокол конфиденциальности – AES. Значение по умолчанию: **4**

Инструкции по использованию

- Те же протоколы аутентификации и конфиденциальности должны быть указаны на сервере SNMP.
- Настроенные протоколы аутентификации и конфиденциальности также одновременно применяются к SNMPv3.
- Использование **MD5** и **DES** может привести к появлению определенных рисков безопасности. Рекомендуется использовать **SHA** и **AES**.

Пример

Настройка протоколов аутентификации и конфиденциальности прерываний SNMPv3.

```
iBMC:/->ipmcset -t trap -d protocol -v 4
Set SNMP trap authentication and privacy protocol successfully.
```

Запрос протоколов аутентификации и конфиденциальности прерываний SNMPv3.

```
iBMC:/->ipmcget -t trap -d protocol
Trap protocol     :
  Authentication  : SHA
  Privacy         : AES
```

4.4.10 Запрос и настройка режима прерываний SNMP (trap -d mode)

Функция

Команда **trap -d mode** используется для настройки и запроса режима прерываний SNMP.

Формат

ipmcget -t trap -d mode

ipmcset -t trap -d mode -v <*option*>

Параметры

Параметр	Описание	Значение
option	Режим trap SNMP.	• **0** – режим прерываний SNMP Event Code. • **1** – режим прерываний SNMP OID. • **2** – режим прерываний SNMP Precise Alarm (рекомендуется).

Инструкции по использованию

Precise Alarm (recommended) предоставляет более точную информацию, чем **OID** и **Event Code**. Подробная информация приведена в документе *HUAWEI Server iBMC Intelligent Management System SNMP API Description*.

Пример

Установка значения Event Code для режима прерываний SNMP.

```
iBMC:/->ipmcset -t trap -d mode -v 0
Set trap mode Event Code success.
```

Запрос текущего режима прерываний SNMP.

```
iBMC:/->ipmcget -t trap -d mode
Trap mode: Event Code
```

4.5 Команды Syslog

В данном разделе приведено описание порядка использования команд для запроса и настройки параметров syslog.

4.5.1 Запрос и настройка статуса активации syslog (syslog -d state)

Функция

Команда **syslog -d state** используется для настройки и запроса статуса активации отчетности syslog для iBMC.

Формат

ipmcget -t syslog -d state [-v <*destination*>]

ipmcset -t syslog -d state -v [<*destination*>] <**disabled** | **enabled**>

Параметры

Параметр	Описание	Значение
destination	Количество каналов отчетности syslog.	от 1 до 4 Команда применяется для всех каналов, если данный параметр не определен.
disabled	Функция создания отчетов syslog отключена.	–
enabled	Функция создания отчетов syslog включена.	–

Инструкции по использованию

–

Пример

Отключение функции создания отчетов syslog для канала 1.

```
iBMC:/->ipmcset -t syslog -d state -v 1 disabled
Set syslog dest1 disabled successfully.
```

Запрос статуса активации функции создания отчетов syslog канала 1.

```
iBMC:/-> ipmcget -t syslog -d state -v 1
syslog dest1 state: disabled
```

4.5.2 Запрос и настройка режима аутентификации сертификата (syslog -d auth)

Функция

Команда **syslog -d auth** используется для настройки и запроса режима аутентификации сертификата.

Формат

ipmcget -t syslog -d auth

ipmcset -t syslog -d auth -v <*option*>

Параметры

Параметр	Описание	Значение
option	Режим аутентификации сертификата.	• **1**: односторонняя аутентификация • **2**: взаимная аутентификация

Инструкции по использованию

- Односторонняя аутентификация: Аутентификацию проходит только сертификат сервера syslog.
- Взаимная аутентификация: Аутентификацию проходят сертификаты сервера syslog и клиента.

Пример

Настройка взаимного режима аутентификаци сертификата.

```
iBMC:/->ipmcset -t syslog -d auth -v 2
Set syslog auth type successfully.
```

Запрос текущего режима аутентификации сертификата.

```
iBMC:/-> ipmcget -t syslog -d auth
Syslog auth type: mutual authentication
```

4.5.3 Запрос и настройка идентификатора хоста syslog (syslog -d state)

Функция

Команда **syslog -d identity** используется для настройки и запроса идентификатора хоста, применяемого при создании отчетов syslog.

Формат

ipmcget -t syslog -d identity

ipmcset -t syslog -d identity -v <*option*>

Параметры

Параметр	Описание	Значение
option	Используемый	• **1**: серийный номер платы

Параметр	Описание	Значение
	идентификатор хоста.	• **2**: инвентарный номер продукта • **3**: имя хоста

Инструкции по использованию

–

Пример

Установка имени хоста для идентификатора хоста syslog.

```
iBMC:/-> ipmcset -t syslog -d identity -v 3
Set syslog identity successfully.
```

Запрос идентификатора хоста syslog.

```
iBMC:/-> ipmcget -t syslog -d identity
Syslog identity: host name
```

4.5.4 Запрос и настройка типа протокола (syslog -d protocol)

Функция

Команда **syslog -d protocol** используется для настройки и запроса протокола, применяемого для отчетности syslog.

Формат

ipmcget -t syslog -d protocol

ipmcset -t syslog -d protocol -v <*option*>

Параметры

Параметр	Описание	Значение
option	Используемый протокол.	• **1**: UDP • **2**: TCP • **3**: TLS

Инструкции по использованию

- **TLS**: протокол, ориентированный на соединение, который обеспечивает конфиденциальность и целостность передаваемых данных.
- **TCP**: протокол, ориентированный на соединение, который устанавливает надежное соединение между отправителем и получателем до передачи данных.

- **UDP**: протокол без соединения, который не устанавливает соединение между отправителем и получателем до передачи данных.

Пример

Установка значения **TLS** для протокола создания отчетов syslog.

```
iBMC:/-> ipmcset -t syslog -d protocol -v 3
Set syslog protocol successfully.
```

Запрос текущего протокола создания отчетов syslog.

```
iBMC:/-> ipmcget -t syslog -d protocol
Syslog protocol: TLS
```

4.5.5 Запрос и настройка уровней журналов для создания отчетов (syslog -d severity)

Функция

Команда **syslog -d severity** используется для настройки и запроса уровней журналов, предоставляемых в качестве пакетов syslog.

Формат

ipmcget -t syslog -d severity

ipmcset -t syslog -d severity -v <*level*>

Параметры

Параметр	Описание	Значение
level	Уровни отчетных журналов.	• **none**: отсутствие аварийных сигналов в отчетах. • **normal**: отчеты по всем аварийным сигналам, включая записи о неисправностях и авариях. • **minor**: отчеты о незначительных, серьезных и критических сбоях. • **major**: отчеты о серьезных и критических сбоях. • **critical**: отчеты о критических сбоях.

Инструкции по использованию

–

Пример

Установка уровня журнала **critical** для отчетов syslog.

```
iBMC:/->ipmcset -t syslog -d severity -v critical
Set syslog severity successfully.
```

Запрос уровня журнала отчетов syslog.

```
iBMC:/-> ipmcget -t syslog -d severity
Syslog severity:  critical
```

4.5.6 Запрос и загрузка корневого сертификата сервера (syslog -d rootcertificate)

Функция

Команда **syslog -d rootcertificate** используется для загрузки корневого сертификата сервера syslog на iBMC или запроса текущей информации корневого сертификата.

Формат

ipmcget -t syslog -d rootcertificate

ipmcset -t syslog -d rootcertificate -v <*filepath*>

Параметры

Параметр	Описание	Значение
filepath	Абсолютный путь к корневому сертификату на iBMC.	Например, **/tmp/rootcertificate.cer**

Инструкции по использованию

Перед выполнением команды загрузки загрузите вручную сгенерированный корневой сертификат в файловую систему iBMC.

Пример

Загрузка корневого сертификата сервера.

```
iBMC:/-> ipmcset -t syslog -d rootcertificate -v /tmp/rootcertificate.cer
Set syslog root certificate successfully.
```

Запрос информации корневого сертификата сервера.

```
iBMC:/-> ipmcget -t syslog -d rootcertificate
Server Root Certificate:
Issued    To: CN=SERVER, OU=IT, O=HW, L=, S=GD, C=CH
```

```
Issued    By: CN=Huawei, OU=IT, O=Huawei, L=ShenZhen, S=GuangDong, C=CN
Valid   From: Mar 24 2016 GMT
Valid     To: Mar 24 2017 GMT
Serial Number: 0b
```

4.5.7 Запрос и загрузка локального сертификата (syslog -d clientcertificate)

Функция

Команда **syslog -d clientcertificate** используется для загрузки сертификата клиента syslog (локальный) на iBMC или запроса текущей информации о локальном сертификате.

Формат

ipmcget -t syslog -d clientcertificate

ipmcset -t syslog -d clientcertificate -v <*filepath*> <*password*>

Параметры

Параметр	Описание	Значение
filepath	Абсолютный путь к корневому сертификату на iBMC.	Например, **/tmp/rootcertificate.cer**
password	Пароль, используемый для дешифровки локального сертификата.	Пароль автоматически генерируется при использовании сервера сертификата для генерации локального сертификата.

Инструкции по использованию

Перед выполнением команды загрузки вручную загрузите локальный сертификат в файловую систему iBMC.

Пример

Загрузка локального сертификата.

```
iBMC:/-> ipmcset -t syslog -d client -v /tmp/clientcertificate.pfx syslogpw
Set syslog client certificate successfully.
```

Запрос информации локального сертификата.

```
iBMC:/-> ipmcget -t syslog -d clientcertificate
Syslog Client Certificate Information:
Issued    To: CN=Server, OU=IT, O=Huawei, L=ShenZhen, S=GuangDong, C=CN
```

```
Issued    By: CN=huangmin, OU=it3, O=huawei3, L=, S=guangdong2, C=cn
Valid   From: Feb 17 2015 GMT
Valid     To: Feb 17 2016 GMT
Serial Number: 25
```

4.5.8 Настройка адреса сервера Syslog (syslog -d address)

Функция

Команда **syslog -d address** используется для настройки адреса сервера syslog.

Формат

ipmcset -t syslog -d address -v <*destination*> <*ipaddr*>

Параметры

Параметр	Описание	Значение
destination	Количество каналов отчетности syslog.	от 1 до 4
ipaddr	Адрес сервера syslog.	В качестве данного параметра может использоваться IPv4-адрес или IPv6-адрес, имя домена или значение данного параметра можно не указывать.

Инструкции по использованию

Если значение *ipaddr* не указано, то данная команда используется для удаления IP-адреса.

Пример

Настройка адреса сервера syslog как **host** для канала 1.

```
iBMC:/-> ipmcset -t syslog -d address -v 1 host
Set syslog dest1 address successfully.
```

Запрос адреса сервера syslog.

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num       | state     | port      | dest address        | log type
1              | disabled  | 0         | host                | operationlogs securitylogs
eventlogs
2              | disabled  | 0         |                     | operationlogs securitylogs
eventlogs
3              | disabled  | 0         |                     | operationlogs securitylogs
eventlogs
4              | disabled  | 0         |                     | operationlogs securitylogs
```

```
eventlogs
```

Удаление IP-адреса сервера syslog канала 1.

```
iBMC:/-> ipmcset -t syslog -d address -v 1 ""
Set syslog dest1 address successfully.
```

4.5.9 Настройка номера порта сервера Syslog (syslog -d port)

Функция

Команда **syslog -d port** используется для настройки номера порта сервера syslog.

Формат

ipmcset -t syslog -d port -v <*destination*> <*portvalue*>

Параметры

Параметр	Описание	Значение
destination	Количество каналов отчетности syslog.	от 1 до 4
portvalue	Номер порта сервера syslog.	от 1 до 65535

Инструкции по использованию

–

Пример

Настройка номера порта сервера syslog как **65535** для канала 1.

```
iBMC:/-> ipmcset -t syslog -d port -v 1 65535
Set syslog dest1 port successfully.
```

Запрос номеров портов сервера syslog.

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num       | state     | port      | dest address        | log type
1             | disabled   | 65535     | host               | operationlogs
securitylogs eventlogs
2             | disabled   | 0         |                    | operationlogs securitylogs
eventlogs
3             | disabled   | 0         |                    | operationlogs securitylogs
eventlogs
4             | disabled   | 0         |                    | operationlogs securitylogs
eventlogs
```

4.5.10 Настройка типов журналов для отчетности (syslog -d logtype)

Функция

Команда **syslog -d logtype** используется для настройки типов журналов, предоставляемых в качестве пакетов syslog.

Формат

ipmcset -t syslog -d logtype -v <*destination*> <*type*>

Параметры

Параметр	Описание	Значение
destination	Количество каналов отчетности syslog.	от 1 до 4
type	Типы отчетных журналов.	• **none**: отчетные журналы отсутствуют. • **all**: отчет по всем журналам. • **operationlogs**: отчет по журналам операций. • **securitylogs**: отчет по журналам безопасности. • **eventlogs**: отчет по журналам событий.

Инструкции по использованию

–

Пример

Настройка типов журналов для канала 4 как журналы событий и операций.

```
iBMC:/-> ipmcset -t syslog -d logtype -v 4 operationlogs eventlogs
Set syslog log type successfully.
```

Запрос типов журналов, предоставляемых посредством канала 4.

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num       | state     | port      | dest address        | log type
1             | disabled   | 65535     | host               | operationlogs
securitylogs eventlogs
2             | disabled   | 0         |                    | operationlogs securitylogs
eventlogs
3             | disabled   | 0         |                    | operationlogs securitylogs
eventlogs
4             | disabled   | 0         |                    | operationlogs eventlogs
```

4.5.11 Проверка доступности сервера Syslog (syslog -d test)

Функция

Команда **syslog -d test** используется для проверки доступности сервера syslog.

Формат

ipmcset -t syslog -d test -v <*destination*>

Параметры

Параметр	Описание	Значение
destination	Количество каналов отчетности syslog.	от 1 до 4

Инструкции по использованию

–

Пример

Проверка доступности сервера syslog для канала 1.

```
iBMC:/-> ipmcset -t syslog -d test -v 1
Test syslog dest1 successfully.
```

4.5.12 Запрос конфигурационной информации всех каналов отчетности Syslog (syslog -d iteminfo)

Функция

Команда **syslog -d iteminfo** используется для запроса конфигурационной четырех каналов отчетности syslog.

Формат

ipmcget -t syslog -d iteminfo

Параметры

–

Инструкции по использованию

–

Пример

Запрос конфигурационной информации каналов отчетности iBMC.

```
iBMC:/-> ipmcget -t syslog -d iteminfo

Item Num       | state     | port      | dest address        | log type
1             | disabled   | 65535     | host               | operationlogs
securitylogs eventlogs
2             | disabled   | 0         |                    | operationlogs securitylogs
eventlogs
3             | disabled   | 0         |                    | operationlogs securitylogs
eventlogs
4             | disabled   | 0         |                    | operationlogs eventlogs
```

4.6 Команды сервера

В данном разделе приведено описание всех команд, связанных с сервером.

4.6.1 Запрос и настройка загрузочного устройства (bootdevice)

Функция

Команда **bootdevice** используется для запроса и настройки загрузочного устройства.

Формат

ipmcget -d bootdevice

ipmcset -d bootdevice -v <*option*> [*once* | *permanent*]

Параметры

Параметр	Описание	Значение
option	Номер загрузочного устройства.	• **0**: отмена принудительного запуска. • **1**: запуск с PXE. • **2**: запуск с жесткого диска по умолчанию. • **5**: запуск с диска CD/DVD по умолчанию. • **6**: доступ к меню настройки BIOS при запуске сервера. • **0xF**: запуск с FDD или первого мобильного накопителя.
once	Установка параметра загрузки вступает в силу только для следующего запуска. После следующего запуска восстанавливается параметр загрузки по умолчанию.	–

Параметр	Описание	Значение
permanent	Настройки параметров загрузки вступают в силу на постоянной основе.	–

Инструкции по использованию

–

Пример

ПРИМЕЧАНИЕ

Отображаемая информация содержит параметр **Unspecified**, который указывает на то, что параметры принудительной загрузки устройства не установлены.

Запуск устройства с жесткого диска по умолчанию.

```
iBMC:/->ipmcset -d bootdevice -v 2 once
Set boot device successfully.
```

Запрос измененного загрузочного устройства.

```
iBMC:/->ipmcget -d bootdevice
Boot    device:  Force boot from default Hard-drive
Effective  type:  Once
```

4.6.2 Настройка режима перезапуска сервера (frucontrol)

Функция

Команда **frucontrol** используется для указания процедуры перезапуска сервера.

Формат

ipmcset [-t fru0] **-d frucontrol** -v <*option*>

Параметры

Параметр	Описание	Значение
option	Режим перезапуска.	• **0**: принудительный перезапуск сервера. • **2**: цикл принудительного включения-отключения (отключение и включение питания) сервера.

Инструкции по использованию

Эта команда недоступна для сервера в состоянии отключенного питания.

Пример

Принудительный перезапуск сервера.

```
iBMC:/->ipmcset -d frucontrol -v 0
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
FRU control fru0 (forced system reset) successfully.
```

Цикл принудительного включения-отключения питания сервера.

```
iBMC:/->ipmcset -d frucontrol -v 2
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
FRU control fru0 (forced power cycle) successfully.
```

4.6.3 Запрос и настройка состояния питания сервера (powerstate)

Функция

Команда **powerstate** используется для запроса и настройки состояния питания сервера.

Формат

ipmcget [-t fru0] **-d powerstate**

ipmcset [-t fru0] **-d powerstate -v** <*option*>

Параметры

Параметр	Описание	Значение
option	Операция, выполняемая на сервере.	• 0: безопасное отключение питания сервера • 1: включение питания сервера • 2: принудительное отключение питания сервера

Инструкции по использованию

Команда отключения питания недоступна для сервера в состоянии отключенного питания.

Пример

Включение питания сервера.

```
iBMC:/->ipmcset -d powerstate -v 1
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Control fru0 power on successfully.
```

Запрос состояния питания сервера.

```
iBMC:/->ipmcget -d powerstate
Power state   : On
Hotswap state : M4
```

4.6.4 Запрос и настройка периода ожидания отключения питания сервера (shutdowntimeout)

Функция

Команда **shutdowntimeout** используется для запроса и настройки периода ожидания отключения питания сервера.

После выполнения операции отключения питания iBMC ожидает завершения работы ОС. Если ОС не завершит работу в течение указанного времени, iBMC принудительно отключит сервер.

Формат

ipmcget [-t fru0] **-d shutdowntimeout**

ipmcset [-t fru0] **-d shutdowntimeout -v** <*time*>

Параметры

Параметр	Описание	Значение
time	Максимальное время (в секундах) для завершения работы ОС.	Диапазон значений: 0, 10 до 6000 Значение **0** говорит о том, что период ожидания завершения работы отключен.

Инструкции по использованию

- Если для **Power-off Timeout Period** установлено 

на WebUI iBMC, вы можете использовать эту команду, чтобы отключить режим ожидания выключения или установить период ожидания выключения по мере необходимости.
- Если для **Power-off Timeout Period** установлено 

на WebUI iBMC, вы можете использовать эту команду для установки периода ожидания выключения.

  После настройки **Power-off Timeout Period** изменяется на 

на WebUI iBMC.

Пример

Настройка для периода ожидания выключения значения 600 секунд для сервера.

```
iBMC:/->ipmcset -d shutdowntimeout -v 600
Set shutdown timeout successfully.
```

Запрос периода ожидания выключения.

```
iBMC:/->ipmcget -d shutdowntimeout
Graceful shutdown timeout state:   enabled
Graceful shutdown timeout value:   600 s
```

Запрос периода ожидания выключения (для **power-off timeout period** установлено значение **OFF** на WebUI iBMC).

```
iBMC:/->ipmcget -d shutdowntimeout
Graceful shutdown timeout state:   disabled
```

Отключение ожидания выключения для сервера.

```
iBMC:/->ipmcset -d shutdowntimeout -v 0
Set shutdown timeout successfully.
```

4.6.5 Запрос MAC-адреса сетевого интерфейса на материнской плате (macaddr)

Функция

Команда **macaddr** используется для запроса MAC-адреса сетевого интерфейса на материнской плате.

Формат

ipmcget -d macaddr

Параметры

–

Инструкции по использованию

–

Пример

Запрос MAC-адреса сетевого интерфейса на материнской плате.

```
iBMC:/->ipmcget -d macaddr
Type      | Name      | Mac Address
LOM       | Port1     | 20:0b:c7:2a:e6:0b
LOM       | Port2     | 20:0b:c7:2a:e6:0c
LOM       | Port3     | 20:0b:c7:2a:e6:0d
LOM       | Port4     | 20:0b:c7:2a:e6:0e
```

4.6.6 Запрос доступного сетевого порта (ethport)

Функция

Команда **ethport** используется для запроса информации о доступном сетевом порте.

Формат

ipmcget -d ethport

Параметры

–

Инструкции по использованию

–

Пример

Запрос доступного сетевого порта.

```
iBMC:/->ipmcget -d ethport
Type      | Name      | Port ID  | Link Status
Dedicated  | eth2      | na      | Link Up
LOM       | Port1     | 1       | Link Down
LOM       | Port2     | 2       | Link Down
LOM       | Port3     | 3       | Link Down
LOM       | Port4     | 4       | Link Down
```

4.6.7 Очистка флеш-памяти BIOS (clearcmos)

Функция

Команда **clearcmos** используется для удаления всей информации, определенной пользователем во флеш-памяти BIOS.

Формат

ipmcset -d clearcmos

Параметры

–

Инструкции по использованию

–

Пример

Очистка флеш-памяти BIOS.

```
iBMC:/->ipmcset -d clearcmos
WARNING: The operation may have many adverse effects
Do you want to continue?[Y/N]:y
Clear CMOS successfully.
```

4.6.8 Запрос информации о RAID-контроллере (ctrlinfo)

Функция

Команда **ctrlinfo** используется для запроса информации о плате контроллера RAID.

Формат

ipmcget -t storage -d ctrlinfo -v <*option*>

Параметры

Параметр	Описание	Значение
option	Идентификатор RAID-контроллера.	• От **0** до **255**: определенная плата контроллера RAID. • **all**: все платы контроллера RAID.

Инструкции по использованию

–

Пример

Запрос информации о плате 0 контроллера RAID.

```
iBMC:/->ipmcget -t storage -d ctrlinfo -v 0
RAID Controller #0 Information
---------------------------------------------------------------------
Controller Name                           : SAS3108
Controller Type                           : LSI SAS3108
Component Name                            : RAID Card1
Support Out-of-Band Management              : Yes
Controller Mode                           : RAID
Controller Health                         : Normal
Firmware Version                          : 4.650.00-6121
NVDATA Version                            : 3.1602.00-0002
Memory Size                               : 1024 MB
Device Interface                          : SAS 12G
SAS Address                               : 5e00000157737cd6
Minimum Strip Size Supported                : 64 KB
Maximum Strip Size Supported                : 1 MB
Controller Cache Is Pinned                  : No
Maintain PD Fail History across Reboot        : Yes
Copyback Enabled                          : No
Copyback on SMART error Enabled             : No
JBOD Enabled                              : No
DDR ECC Count                             : 0

BBU Status                                : Present
BBU Type                                  : CVPM02
BBU Health                                : Normal
```

```
PHY Status                              :
   PHY #0 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #1 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #2 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #3 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #4 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #5 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #6 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0

   PHY #7 :
      Invalid Dword Count         : 0
      Loss Dword Sync Count       : 0
      PHY Reset Problem Count     : 0
      Running Disparity Error Count : 0
----------------------------------------------------------------------
```

4.6.9 Запрос информации о логическом диске (ldinfo)

Функция

Команда **ldinfo** используется для запроса информации о логических дисках, управляемых платой контроллера RAID.

Формат

pmcget -t storage -d ldinfo -v <*ctrlid*> <*option*>

Параметры

Параметр	Описание	Значение
ctrlid	ID контроллера RAID, который управляет целевым логическим диском.	от **0** до **255**
option	ID логического диска.	• От **0** до **255**: определенный логический диск. • **all**: все логические диски, управляемые контроллером RAID.

Инструкции по использованию

–

Пример

Запрос информации о логическом диске 0, управляемом контроллером RAID 0.

```
iBMC:/->ipmcget -t storage -d ldinfo -v 0 0
Logical Drive Information
---------------------------------------------------------------------
Target ID                          : 0
Name                               : example1
Type                               : RAID1
State                              : Optimal
Default Read Policy                  : Read Ahead
Default Write Policy                 : Write Back with BBU
Default Cache Policy                 : Direct IO
Current Read Policy                  : Read Ahead
Current Write Policy                 : Write Back with BBU
Current Cache Policy                 : Direct IO
Access Policy                       : Read Write
Span depth                         : 1
Number of drives per span            : 2
Strip Size                         : 256 KB
Total Size                         : 100.234 GB
Disk Cache Policy                   : Enabled
```

```
Init State                          : No Init
Consistency Checking                  : No
BGI Enabled                         : Yes
Bootable                            : No
Used for Secondary Cache              : No
SSCD Caching Enable                   : No
PD participating in LD (ID#)           : 0,1
Dedicated Hot Spare PD (ID#)           : N/A
----------------------------------------------------------------------
```

Запрос информации о всех логических дисках, управляемых RAID-контроллером 0.

```
iBMC:/->ipmcget -t storage -d ldinfo -v 0 all
Logical Drive Information
----------------------------------------------------------------------
Target ID                           : 0
Name                                : example1
Type                                : RAID1
State                               : Optimal
Default Read Policy                   : Read Ahead
Default Write Policy                  : Write Back with BBU
Default Cache Policy                  : Direct IO
Current Read Policy                   : Read Ahead
Current Write Policy                  : Write Back with BBU
Current Cache Policy                  : Direct IO
Access Policy                       : Read Write
Span depth                          : 1
Number of drives per span             : 2
Strip Size                          : 256 KB
Total Size                          : 100.234 GB
Disk Cache Policy                    : Enabled
Init State                          : No Init
Consistency Checking                  : No
BGI Enabled                         : Yes
Bootable                            : No
Used for Secondary Cache              : No
SSCD Caching Enable                   : No
PD participating in LD (ID#)           : 0,1
Dedicated Hot Spare PD (ID#)           : N/A
----------------------------------------------------------------------

Logical Drive Information
----------------------------------------------------------------------
Target ID                           : 1
Name                                : example2
Type                                : RAID0
State                               : Optimal
Default Read Policy                   : Read Ahead
Default Write Policy                  : Write Back with BBU
Default Cache Policy                  : Direct IO
Current Read Policy                   : Read Ahead
Current Write Policy                  : Write Back with BBU
Current Cache Policy                  : Direct IO
Access Policy                       : Read Write
Span depth                          : 1
```

```
Number of drives per span              : 5
Strip Size                            : 256 KB
Total Size                            : 1.149 TB
Disk Cache Policy                      : Enabled
Init State                            : No Init
Consistency Checking                   : No
BGI Enabled                           : Yes
Bootable                              : No
Used for Secondary Cache               : No
SSCD Caching Enable                    : No
PD participating in LD (ID#)           : 2,8,9,10,11
Dedicated Hot Spare PD (ID#)           : N/A
------------------------------------------------------------------------
```

4.6.10 Запрос информации о физическом диске (pdinfo)

Функция

Команда **pdinfo** используется для запроса информации о физических дисках.

Формат

ipmcget -t storage -d pdinfo -v <*option*>

Параметры

Параметр	Описание	Значение
option	ID физического диска.	• От **0** до **255**: определенный физический диск. • **all**: все физические диски.

Инструкции по использованию

–

Пример

Запрос информации о физическом диске 2.

```
iBMC:/->ipmcget -t storage -d pdinfo -v 2
Physical Drive Information
------------------------------------------------------------------------
ID                                   : 2
Device Name                           : Disk2
Manufacturer                          : TOSHIBA
Serial Number                         : EB00PC208N0R
Model                                : MBF2300RC
Firmware Version                       : 0109
Health Status                         : Normal
Firmware State                        : UNCONFIGURED GOOD
```

```
Power State                          : Spun Up
Media Type                           : HDD
Interface Type                        : SAS
Interface Speed                       : 6.0Gbps
Link Speed                           : 6.0Gbps
Drive Temperature                     : 62(Celsius)
Capacity                             : 278.465 GB
Hot Spare                            : None
Rebuild in Progress                   : No
Patrol Read in Progress               : No
Remnant Media Wearout                 : N/A
SAS Address(0)                        : 50000393d84baa46
SAS Address(1)                        : 0000000000000000
Location State                        : Off

Media Error Count                     : 0
Prefail Error Count                   : 0
Other Error Count                     : 0
------------------------------------------------------------------------
```

Запрос информации о всех физических дисках.

```
iBMC:/->ipmcget -t storage -d pdinfo -v all
Physical Drive Information
------------------------------------------------------------------------
ID                                   : 0
Device Name                           : Disk0
Manufacturer                          : TOSHIBA
Serial Number                         : EB00PC208KL3
Model                                : MBF2300RC
Firmware Version                      : 0109
Health Status                         : Normal
Firmware State                        : ONLINE
Power State                          : Spun Up
Media Type                           : HDD
Interface Type                        : SAS
Interface Speed                       : 6.0Gbps
Link Speed                           : 6.0Gbps
Drive Temperature                     : 53(Celsius)
Capacity                             : 278.465 GB
Hot Spare                            : None
Rebuild in Progress                   : No
Patrol Read in Progress               : No
Remnant Media Wearout                 : N/A
SAS Address(0)                        : 50000393d84b6f92
SAS Address(1)                        : 0000000000000000
Location State                        : Off

Media Error Count                     : 0
Prefail Error Count                   : 0
Other Error Count                     : 0
------------------------------------------------------------------------

Physical Drive Information
------------------------------------------------------------------------
```

```
ID                                : 1
Device Name                        : Disk1
Manufacturer                       : TOSHIBA
Serial Number                      : EB72PC600G1C
Model                             : MBF2300RC
Firmware Version                    : 0109
Health Status                      : Normal
Firmware State                     : ONLINE
Power State                        : Spun Up
Media Type                         : HDD
Interface Type                      : SAS
Interface Speed                    : 6.0Gbps
Link Speed                         : 6.0Gbps
Drive Temperature                   : 69(Celsius)
Capacity                           : 278.465 GB
Hot Spare                          : None
Rebuild in Progress                 : No
Patrol Read in Progress             : No
Remnant Media Wearout               : N/A
SAS Address(0)                     : 5000039418218546
SAS Address(1)                     : 0000000000000000
Location State                     : Off

Media Error Count                   : 0
Prefail Error Count                 : 0
Other Error Count                   : 0
------------------------------------------------------------------------

Physical Drive Information
------------------------------------------------------------------------
ID                                : 2
Device Name                        : Disk2
Manufacturer                       : TOSHIBA
Serial Number                      : EB00PC208N0R
Model                             : MBF2300RC
Firmware Version                    : 0109
Health Status                      : Normal
Firmware State                     : ONLINE
Power State                        : Spun Up
Media Type                         : HDD
Interface Type                      : SAS
Interface Speed                    : 6.0Gbps
Link Speed                         : 6.0Gbps
Drive Temperature                   : 62(Celsius)
Capacity                           : 278.465 GB
Hot Spare                          : None
Rebuild in Progress                 : No
Patrol Read in Progress             : No
Remnant Media Wearout               : N/A
SAS Address(0)                     : 50000393d84baa46
SAS Address(1)                     : 0000000000000000
Location State                     : Off

Media Error Count                   : 0
Prefail Error Count                 : 0
```

```
Other Error Count                    : 0
----------------------------------------------------------------------
```

4.6.11 Запрос информации о дисковом массиве (arrayinfo)

Функция

Команда **arrayinfo** используется для запроса информации о дисковом массиве.

Формат

ipmcget -t storage -d arrayinfo -v <*control_id*> <*option*>

Параметры

Параметр	Описание	Значение
control_id	ID контроллера RAID, которому принадлежит дисковый массив.	от 0 до 255
option	Запрашиваемый дисковый массив.	• **all**: запрос информации о всех определенных дисковых массивах. • От 0 до 255: запрос информации об определенном дисковом массиве.

Инструкции по использованию

–

Пример

Запрос информации о дисковом массиве 1 RAID-контроллера 0.

```
iBMC:/->ipmcget -t storage -d arrayinfo -v 0 1
Disk Array Information
----------------------------------------------------------------------
Array ID                            : 1
Used Space                          : 1.149 TB
Free Space                          : 215.749 GB
Logcial Drive(s) ID                   : 1
Physical Drive(s) ID                  : 2,8,9,10,11
----------------------------------------------------------------------
```

Запрос информации о всех дисковых массивах RAID-контроллера 0.

```
iBMC:/->ipmcget -t storage -d arrayinfo -v 0 all
Disk Array Information
----------------------------------------------------------------------
Array ID                            : 0
```

```
Used Space                          : 200.469 GB
Free Space                          : 356.461 GB
Logcial Drive(s) ID                   : 0
Physical Drive(s) ID                  : 0,1
---------------------------------------------------------------------

Disk Array Information
---------------------------------------------------------------------
Array ID                            : 1
Used Space                          : 1.149 TB
Free Space                          : 215.749 GB
Logcial Drive(s) ID                   : 1
Physical Drive(s) ID                  : 2,8,9,10,11
---------------------------------------------------------------------

Disk Array Information
---------------------------------------------------------------------
Array ID                            : 2
Used Space                          : 446.103 GB
Free Space                          : 0 MB
Logcial Drive(s) ID                   : 2
Physical Drive(s) ID                  : 7
---------------------------------------------------------------------
```

4.6.12 Создание логического диска (createld)

Функция

Команда **createld** используется для создания логического диска из свободного физического диска.

Формат

ipmcset -t storage -d createld -v <*control_id*> **-rl** <*raidlevel*> **-pd** <*pd_id*> **[-cachecade] [-sc** <*span_num*>**] [-name** <*ldname*>**] [-size** <*capative*>{m|g|t} **] [-ss** <*stripesize*>**] [-rp** <*rpvalue*>**] [-wp** <*wpvalue*>**] [-iop** <*iopvalue*>**] [-ap** <*apvalue*>**] [-dcp** <*dcpvalue*>**] [-init** <*initmode*>**]**

Параметры

Параметр	Описание	Значение
control_id	ID контроллера RAID.	от 0 до 255
raidlevel	Уровень RAID логического диска.	• **r0**: RAID 0 • **r1**: RAID 1 • **r5**: RAID 5 • **r6**: RAID 6 • **r10**: RAID 10 • **r50**: RAID 50

Параметр	Описание	Значение
		• **r60**: RAID 60 **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, значение этого параметра должно быть **r0** или **r1**.
pd_id	ID диска-участника логического диска.	Для разделения ID нескольких дисков используйте запятую (,), например, **0,1,2**. **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, диск-участник должен быть диск SSD.
span_num	Количество объединений логического диска.	• Если уровень RAID равен 0, 1, 5 или 6, этот параметр можно не настраивать. • Если уровень RAID равен 10, 50 или 60, следует настроить этот параметр. Значение по умолчанию – 2. **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, этот параметр недействителен.
ldname	Имя создаваемого логического диска.	Значение параметра не может превышать 15 символов.
capative	Емкость создаваемого логического диска.	Единицей емкости может быть: • **m**: МБ • **g**: ГБ • **t**: ТБ **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, этот параметр недействителен.
stripesize	Размер полосы данных (в байтах) логического диска.	Значение: • 64K • 128K • 256K • 512K • 1M По умолчанию используется значение **256K**. **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, этот параметр недействителен.
rpvalue	Политика чтения данных с логического диска.	• **ra**: Read Ahead • **nra**: No Read Ahead Значение по умолчанию – **ra**. **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, этот параметр недействителен.

Параметр	Описание	Значение
wpvalue	Политика записи данных логического диска.	• **wt**: Write Through • **wb**: Write Back • **wbwithbbu**: Write Back with BBU Значение по умолчанию – **wbwithbbu**. **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, этот параметр недействителен.
iopvalue	Политика ввода-вывода данных на логический диск.	• **cio**: Cached IO • **dio**: Direct IO Значение по умолчанию – **dio**. **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, этот параметр недействителен.
apvalue	Политика доступа к логическому диску.	• **rw**: логический диск доступен для записи и чтения. • **ro**: логический диск доступен только для чтения. • **blocked**: логический диск скрыт. Значение по умолчанию – **rw**. **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, этот параметр недействителен.
dcpvalue	Политика использования кэш-памяти логического диска.	• **enabled**: для логического диска разрешено использовать кэш-память. • **disabled**: для логического диска не разрешено использовать кэш-память. • **default**: используется политика по умолчанию, то есть используется политика дисков-участников. Значение по умолчанию – **enabled**. **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, этот параметр недействителен.
initmode	Режим инициализации логического диска.	• **no**: логический диск не инициализируется. • **quick**: выполняется быстрая инициализация. • **full**: выполняется полная инициализация. Значение по умолчанию – **no**. **ПРИМЕЧАНИЕ** Если команда содержит **-cachecade**, этот параметр недействителен.

Инструкции по использованию

Если команда содержит **-cachecade**, будет создан диск CacheCade.

Пример

Создание общего логического диска под контроллером RAID 0.

```
iBMC:/-> ipmcset -t storage -d createld -v 0 -rl r1 -pd 0,1 -name example -size 100g
-ss 512k -rp ra -wp wb -ap rw -iop cio -dcp enabled -init quick
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

Создание диска Cachecade под контроллером RAID 0.

```
iBMC:/-> ipmcset -t storage -d createld -v 0 -rl r0 -pd 0,1,2 -name cachecade -cachecade
-wp wb
WARNING: The operation may have many adverse effects.
    Do you want to continue?[Y/N]:y
```

4.6.13 Добавление логического диска (addld)

Функция

Команда **addld** используется для добавления логического диска к дисковому массиву.

Формат

ipmcset -t storage -d addld -v <*control_id*> **-array** <*arrayid*> **[-name** <*ldname*>**] [-size** <*capative*>{m|g|t} **] [-ss** <*stripesize*>**] [-rp** <*rpvalue*>**] [-wp** <*wpvalue*>**] [-iop** <*iopvalue*>**] [-ap** <*apvalue*>**] [-dcp** <*dcpvalue*>**] [-init** <*initmode*>**]**

Параметры

Параметр	Описание	Значение
control_id	ID RAID-контроллера.	от 0 до 255
arrayid	ID дискового массива, к которому будет добавлен логический диск.	от 0 до 255
ldname	Имя добавляемого логического диска.	Значение параметра не может превышать 15 символов.
capative	Емкость добавляемого логического диска.	Единица емкости может быть: • **m**: МБ • **g**: ГБ • **t**: ТБ По умолчанию емкость равна оставшемуся

Параметр	Описание	Значение
		пространству дискового массива.
stripesize	Размер полосы данных (в байтах) логического диска.	Значение: • 64K • 128K • 256K • 512K • 1M По умолчанию используется значение **256K**.
rpvalue	Политика чтения данных с логического диска.	• **ra**: Read Ahead • **nra**: No Read Ahead Значение по умолчанию – **ra**.
wpvalue	Политика записи данных логического диска.	• **wt**: Write Through • **wb**: Write Back • **wbwithbbu**: Write Back with BBU Значение по умолчанию – **wbwithbbu**.
iopvalue	Политика ввода-вывода данных на логический диск.	• **cio**: Cached IO • **dio**: Direct IO Значение по умолчанию – **dio**.
apvalue	Политика доступа к логическому диску.	• **rw**: логический диск доступен для записи и чтения. • **ro**: логический диск доступен только для чтения. • **blocked**: логический диск скрыт. Значение по умолчанию – **rw**.
dcpvalue	Политика использования кэш-памяти логического диска.	• **enabled**: для логического диска разрешено использовать кэш-память. • **disabled**: для логического диска не разрешено использовать кэш-память. • **default**: используется политика по умолчанию, то есть используется политика дисков-участников. Значение по умолчанию – **enabled**.
initmode	Режим инициализации логического диска.	• **no**: логический диск не инициализируется. • **quick**: быстрая инициализация. • **full**: полная инициализация. Значение по умолчанию – **no**.

Инструкции по использованию

–

Пример

Добавление логического диска к дисковому массиву 1 контроллера RAID 0.

```
iBMC:/-> ipmcset -t storage -d addld -v 0 -array 1 -name example -size 500g -ss 256k
-rp ra -wp wb -ap rw -iop cio -dcp enabled -init quick
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.6.14 Удаление логического диска (deleteld)

Функция

Команда **deleteld** используется для удаления логического диска, управляемого контроллером RAID.

Формат

ipmcset -t storage -d deleteld -v <*control_id*> <*ldid*>

Параметры

Параметр	Описание	Значение
control_id	ID RAID-контроллера.	от 0 до 255
ldid	ID удаляемого логического диска.	от 0 до 255

Инструкции по использованию

–

Пример

Удаление логического диска 1, управляемого контроллером RAID 0.

```
iBMC:/-> ipmcset -t storage -d deleteld -v 0 0
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.6.15 Изменение свойств логического диска (ldconfig)

Функция

Команда **ldconfig** используется для изменения свойств логического диска.

Формат

ipmcset -t storage -d ldconfig -v <*control_id*> <*ldid*> <**[-name** <*ldname*>**] [-rp** <*rpvalue*>**] [-wp** <*wpvalue*>**] [-iop** <*iopvalue*>**] [-ap** <*apvalue*>**] [-bgi** <*bgistate*>**] [-boot] [-sscd** <*initmode*>**]**

Параметры

Параметр	Описание	Значение
control_id	ID RAID-контроллера.	от 0 до 255
ldid	ID изменяемого логического диска.	от 0 до 255
ldname	Имя изменяемого логического диска.	Значение параметра не может превышать 15 символов.
rpvalue	Политика чтения данных с логического диска.	• **ra**: Read Ahead • **nra**: No Read Ahead
wpvalue	Политика записи данных логического диска.	• **wt**: Write Through • **wb**: Write Back • **wbwithbbu**: Write Back with BBU
iopvalue	Политика ввода-вывода данных на логический диск.	• **cio**: Cached IO • **dio**: Direct IO
apvalue	Политика доступа к логическому диску.	• **rw**: логический диск доступен для записи и чтения. • **ro**: логический диск доступен только для чтения. • **blocked**: логический диск скрыт.
bgistate	Статус BGI логического диска.	• enabled • disabled
initmode	Настройка кэширования SSD (использовать ли диск CacheCade в качестве кеша).	• enabled • disabled

Инструкции по использованию

Если команда содержит **-boot**, логический диск является загрузочным устройством.

Пример

Изменение свойств логического диска 1 под контроллером RAID 0.

```
iBMC:/-> ipmcset -t storage -d ldconfig -v 0 1 -name example -rp ra -wp wb -ap rw -iop
cio -dcp enabled -bgi enabled -boot
WARNING: The operation may have many adverse effects.
    Do you want to continue?[Y/N]:y
```

4.6.16 Изменение свойств контроллера RAID (ctrlconfig)

Функция

Команда **ctrlconfig** используется для изменения свойств контроллера RAID.

Формат

ipmcset -t storage -d ctrlconfig -v <*control_id*> <**[-cb** <*cbstate*>**] [-smartercb** <*smartercbstate*>**] [-jbod** <*jbodstate*>**] [-restore]**

Параметры

Параметр	Описание	Значение
control_id	ID RAID-контроллера.	от 0 до 255
cbstate	Настройка копирования RAID-контроллера.	• enabled • disabled
smartercbstate	Копирование при обнаружении ошибки SMART на диске-участнике RAID-контроллера.	• enabled • disabled
jbodstate	Настройка JBOD RAID-контроллера.	• enabled • disabled

Инструкции по использованию

Если команда содержит **-restore**, свойства контроллера RAID будут восстановлены до значений по умолчанию.

Пример

Включение копирования для контроллера RAID 0.

```
iBMC:/-> ipmcset -t storage -d ctrlconfig -v 0 -cb enabled
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.6.17 Изменение свойств физического диска (pdconfig)

Функция

Команда **pdconfig** используется для изменения свойств физического диска, управляемого контроллером RAID.

Формат

ipmcset -t storage -d pdconfig -v <*pdid*> **[-state** <*pdstate*>**] [-hotspare** <*hotsparetype*> **[-ld** <*ldid*>**]] [-locate]** <*locatestate*>

Параметры

Параметр	Описание	Значение
pdid	ID физического диска.	от 0 до 255
pdstate	Статус физического диска.	• **online**: диск в сети. • **offline**: диск не в сети. • **ug**: диск не занят. • **jbod:** диск является диском JBOD.
hotsparetype	Статус «горячего» резерва физического диска.	• **none**: диск не является диском «горячего» резерва. • **global**: диск является диском глобального «горячего» резерва. • **dedicated**: диск является специальным диском «горячего» резерва.
ldid	ID логического диска. Если **hotsparetype** – **dedicated**, необходимо настроить логический диск, связанный с этим физическим диском.	0~255
locatestate	Статус индикатора местоположения физического диска.	• **start**: индикатор местоположения мигает. • **stop**: индикатор местоположения отключен.

Инструкции по использованию

–

Пример

Настройте для статуса физического диска 1 значение **online**.

```
iBMC:/-> ipmcset -t storage -d pdconfig -v 1 -state online
WARNING: The operation may have many adverse effects.
Do you want to continue?[Y/N]:y
```

4.7 Системные команды

В данном разделе приведено описание всех системных команд.

4.7.1 Запрос системного имени (systemname)

Функция

Команда **systemname** используется для запроса системного имени.

Формат

ipmcget -t smbios -d systemname

Параметры

–

Инструкции по использованию

–

Пример

Запрос системного имени.

```
iBMC:/->ipmcget -t smbios -d systemname
System name is: xxxxx
```

4.7.2 Настройка часового пояса (timezone)

Функция

Команда **timezone** используется для настройки часового пояса.

Формат

ipmcset -d timezone -v <*timezone*>

Параметры

Параметр	Описание	Значение
timezone	Часовой пояс.	Установить часовой пояс можно следующими способами: • Смещение времени Диапазон значений: – -12:00 до +14:00. Например, +8:00 или -4:30. – GMT-12:00 до GMT+14:00. Например, GMT+8:00 или GMT-4:30. • Название зоны Диапазон значений: Названия зон глобального часового пояса. Например, Азия/Шанхай или Америка/Нью-Йорк. Вы можете выполнить команду **ipmcset -d timezone -v** <*a*> для запроса поддерживаемого часового пояса.

Инструкции по использованию

В часовых поясах, использующих летнее время (DST), iBMC автоматически указывает время на один час вперед, когда начинается DST, и возвращается к стандартному времени, когда заканчивается DST.

Пример

Настройка для часового пояса iBMC значения **+8:00**.

```
iBMC:/->ipmcset -d timezone -v +8:00
Set time zone successfully.
```

Настройка для часового пояса iBMC значения **GMT+8:00**.

```
iBMC:/->ipmcset -d timezone -v GMT+8:00
Set time zone successfully.
```

Запрос часового пояса iBMC.

```
iBMC:/->ipmcget -d time
2014-06-28 Saturday 16:43:51 GMT+08:00
```

Настройка для часового пояса iBMC значения **Asia/Shanghai**.

```
iBMC:/->ipmcset -d timezone -v Asia/Shanghai
Set time zone successfully.
```

Запрос часового пояса iBMC.

```
iBMC:/->ipmcget -d time
2017-09-06 Wednesday 16:43:51 Asia/Shanghai(GMT+08:00)
```

4.7.3 Запрос времени iBMC (time)

Функция

Команда **time** используется для запроса времени iBMC.

Формат

ipmcget -d time

Параметры

–

Инструкции по использованию

–

Пример

Запрос времени iBMC.

```
iBMC:/->ipmcget -d time
2014-06-28 Saturday 16:43:51 GMT+08:00
```

Запрос времени iBMC.

```
iBMC:/->ipmcget -d time
2017-09-06 Wednesday 16:43:51 Asia/Shanghai(GMT+08:00)
```

4.7.4 Запрос информации о версии устройства (version)

Функция

Команда **version** используется для запроса информации о версии устройства.

Формат

ipmcget -d version

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации о версии устройства.

```
iBMC:/->ipmcget -d version
```

Ответная информация системы RH8100 V3:

```
------------------- iBMC INFO -------------------
IPMC             CPU:         Hi1710
IPMI         Version:          2.0
CPLD         Version:          (U6029)1.04
Active iBMC   Version:          (U6005)5.30
Active iBMC     Build:          001
Active iBMC     Built:          10:56:13 Aug  1 2014
Backup iBMC   Version:          5.30
SDK          Version:          1.36
SDK            Built:          15:07:46 Jul 30 2014
Active Uboot   Version:          1.1.26 (Jun 20 2014 - 14:28:52)
Backup Uboot   Version:          1.1.26 (Jun 20 2014 - 14:28:52)
IPMB         Address:          0x20
----------------- Product INFO -----------------
Product           ID:          0x0008
Product          Name:          RH8100 V3
BIOS         Version:          (U6145)V019
-------------- Mother Board INFO ---------------
RH8100        BoardID:          0x005b
RH8100           PCB:          .A
---------------- Raid Card INFO ----------------
SR130         BoardID:          0x002c
SR130            PCB:          .A
--------------- Riser Card INFO ----------------
BC61PRBA      BoardID:          0x0080
-------------- HDD Backplane INFO --------------
BC11THBG      BoardID:          0x007a
BC11THBG         PCB:          .A
---------------- CPU Board INFO -----------------
CpuBoard      BoardID:          0x0090
CpuBoard         PCB:          .A
CpuBoard  CPLD Version:          (U1028)1.04
CpuBoard      BoardID:          0x0090
CpuBoard         PCB:          .A
CpuBoard  CPLD Version:          (U1028)1.04
CpuBoard      BoardID:          0x0090
CpuBoard         PCB:          .A
CpuBoard  CPLD Version:          (U1028)1.04
CpuBoard      BoardID:          0x0090
CpuBoard         PCB:          .A
CpuBoard  CPLD Version:          (U1028)1.04
-------------- Memory Board INFO --------------
MemoryBoard    BoardID:          0x0094
MemoryBoard       PCB:          .A
MemoryBoard    BoardID:          0x0094
MemoryBoard       PCB:          .A
---------------- IO Board INFO -----------------
BioBoard      BoardID:          0x005a
BioBoard         PCB:          .A
BioBoard  CPLD Version:          (U1044)1.04
------------------- LCD INFO --------------------
```

```
LCD          Version:         (J7)1.00
```

Ответная информация системы для других стоечных серверов:

```
------------------- iBMC INFO -------------------
IPMC             CPU:         Hi1710
IPMI          Version:         2.0
CPLD          Version:         (U46)1.03
Active iBMC   Version:          (U25)5.16
Active iBMC     Build:         001
Active iBMC     Built:         14:52:23 Apr 18 2014
Backup iBMC   Version:         5.16
SDK           Version:         1.25
SDK             Built:         20:24:25 Apr 10 2014
Active Uboot  Version:          1.1.17 (Feb 10 2014 - 16:42:52)
Backup Uboot  Version:          1.1.17 (Feb 10 2014 - 16:42:52)
----------------- Product INFO -----------------
Product           ID:          0x0001
Product          Name:         RH2288 V3
BIOS          Version:         (U47)000
-------------- Mother Board INFO ---------------
Mainboard     BoardID:         0x000d
Mainboard        PCB:          .A
```

4.7.5 Запрос информации FRU (fruinfo)

Функция

Команда **fruinfo** используется для запроса информации обо всех быстрозаменяемых блоках (FRU).

Формат

ipmcget [-t fru0] **-d fruinfo**

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации обо всех FRU.

```
iBMC:/->ipmcget -d fruinfo
FRU Device Description : Builtin FRU Device (ID 0, Mainboard)
 Board Mfg. Date      : 2014/04/03 Thu 16:12:00
 Board Manufacturer   : Huawei Technologies Co., Ltd.
 Board Product Name   : board
 Board Serial Number  : 022HLV10E3000003
```

```
Board FRU File ID    : 1.17
Product Manufacturer  : Huawei Technologies Co., Ltd.
Product Name         : pname
Product Serial Number : serialnumber
Product FRU File ID   : 1.17
```

4.7.6 Запрос рабочего состояния системы (health)

Функция

Команда **health** используется для запроса информации о рабочем состоянии системы.

Формат

ipmcget [-t fru0] **-d health**

Параметры

–

Инструкции по использованию

–

Пример

Запрос рабочего состояния системы.

```
iBMC:/->ipmcget -d health
System in health state.
```

4.7.7 Запрос информации о рабочих событиях системы (healthevents)

Функция

Команда **healthevents** используется для запроса информации о рабочих событиях системы.

Формат

ipmcget [-t fru0] **-d healthevents**

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации о рабочих событиях системы.

```
iBMC:/->ipmcget -d healthevents
Event Num  | Event Time          | Alarm Level  | Event Code   | Event Description
1         | 2016-10-17 06:27:14  | Minor       | 0x01000021   | Failed to obtain data
of the CPU 1 DIMM VDDQ2 voltage.
2         | 2016-10-17 10:24:43  | Critical    | 0x01000015   |  DIMM020 DIMM
configuration error or training failed.
3         | 2016-10-17 10:24:43  | Major       | 0x01000017   |  DIMM012 DIMM  triggered
an uncorrectable error, .
4         | 2016-10-17 10:24:43  | Critical    | 0x01000015   |  DIMM001 DIMM
configuration error or training failed.
5         | 2016-10-17 08:47:27  | Major       | 0x03000009   | [Mock]PSU 1 failure.
6         | 2016-10-17 07:40:57  | Minor       | 0x0D000003   | The NIC 1 temperature
(150 degrees C) exceeds the overtemperature threshold (100 degrees C).
7         | 2016-10-17 07:04:47  | Major       | 0x2100000B   | Data rebuild failed at
SD card 2.
8         | 2016-10-17 06:33:21  | Major       | 0x2C000029   | The OS is forcibly
powered off and on due to the watchdog timeout.
```

4.7.8 Запрос информации порта 80 (port80)

Функция

Команда **port80** используется для запроса текущей и архивной информации о порте 80.

Формат

ipmcget -d port80

Параметры

–

Инструкции по использованию

–

Пример

Запрос текущей и архивной информации порта 80. Значение в квадратных скобках – это текущее значение.

```
iBMC:/->ipmcget -d port80
port80 diagnose code:
[00]-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
```

```
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
00-00-00-00-00-00-00-00--00-00-00-00-00-00-00-00
```

4.7.9 Запрос серийного номера SMBIOS (serialnumber)

Функция

Команда **serialnumber** используется для запроса серийного номера SMBIOS.

Формат

ipmcget [-t smbios] **-d serialnumber**

Параметры

–

Инструкции по использованию

–

Пример

Запрос серийного номера SMBIOS.

```
iBMC:/->ipmcget -d serialnumber
System SN is:44444444444444444444
```

4.7.10 Запрос и удаление информации SEL (sel)

Функция

Команда **sel** используется для запроса и удаления информации журнала системных событий (SEL).

Формат

ipmcget -d sel -v <*option*> [*sel_id*]

ipmcset [-t fru0] **-d sel -v clear**

Параметры

Параметр	Описание	Значение
option	Настраиваемая операция.	• list: перечисление всех записей SEL системы. • info: запрос информации об использовании записей SEL. • suggestion: запрос предложений определенного SEL. **ПРИМЕЧАНИЕ** Система хранит максимум 4000 журналов. Когда создается 4001 журнал, система автоматически удаляет самые ранние 2000 журналов, а нумерация новых журналов начинается с 2001.
sel_id	ID SEL, чьи предложения должны быть получены.	Предложения могут быть получены из результата операции **list**. **ПРИМЕЧАНИЕ** Этот параметр доступен только тогда, когда выполнена операция **suggestion**.
clear	Удаление всех SEL. Удаленные SEL не могут быть восстановлены.	–

Инструкции по использованию

–

Пример

Запрос информации об использовании записей SEL.

```
iBMC:/->ipmcget -d sel -v info
SEL Information
Version             :1.0.0
Current Event Number  :  147
Max Event Number      :  4000
```

Запрос предложений SEL, ID которого 146.

```
iBMC:/->ipmcget -d sel -v suggestion 146
ID                :  146
Generation Time    :  2016-10-26 03:26:23
Severity          :  Minor
Event Code         :  0x12000013
Status            :  Asserted
Event Description   :  [Mock]Failed to obtain data of the air inlet temperature
Suggestion         :  1. Restart the iBMC.
                      2. Remove and reconnect power cables or remove and reinstall the
board in the chassis.
```

4.7.11 Запрос журналов операций (operatelog)

Функция

Команда **operatelog** используется для запроса журнала системных операций.

Формат

ipmcget -d operatelog

Параметры

–

Инструкции по использованию

–

Пример

Запрос журнала операций.

```
iBMC:/->ipmcget -d operatelog
2013-11-12 18:27:36 CLI,root@128.5.197.2,Cooling,Set fan manual mode expired time (300)
seconds
2013-11-12 18:27:36 CLI,root@128.5.197.2,Cooling,Set fan mode (manual)
2013-11-12 18:23:19 CLI,root@128.5.197.2,Cooling,Set fan manual mode expired time (60)
seconds
2013-11-12 18:23:19 CLI,root@128.5.197.2,Cooling,Set fan mode (manual)
2013-11-12 18:18:48 CLI,root@128.5.197.2,Cooling,Set fan level (80)
2013-11-12 18:18:45 CLI,root@128.5.197.2,Cooling,Set fan manual mode expired time (30)
seconds
2013-11-12 18:18:45 CLI,root@128.5.197.2,Cooling,Set fan mode (manual)
2013-11-12 18:18:28 CLI,root@128.5.197.2,Cooling,Set fan level (80)
2013-11-12 18:17:43 CLI,root@128.5.197.2,Cooling,Set fan level (80)
2013-11-12 18:13:37 CLI,root@128.5.197.2,Led,Set UID identify force on
2013-11-12 17:56:11 CLI,root@128.5.197.2,User,Modify user(mytest|user5) password
2013-11-12 17:56:02 CLI,root@128.5.197.2,User,Add user5's username (mytest)
2013-11-12 17:51:44 CLI,root@128.5.197.2,diagnose,Download black box data
2013-11-12 17:51:24 CLI,root@128.5.197.2,diagnose,Download System COM data
2013-11-12 17:29:43 CLI,root@128.5.197.2,BMC,Set time zone to (+8:00)
2013-11-12 09:18:11 CLI,root@128.5.197.2,Payload,Set graceful shutdown timeout to (600)
seconds
2013-11-12 08:59:00 CLI,root@128.5.197.2,sensor_alarm,Set SNMP trap severity filter
alarm to (Minar )
2013-11-12 08:45:45 CLI,root@128.5.197.2,sensor_alarm,Set SNMP trap destination 1
address to (10.10.10.10)
2013-11-12 08:41:55 CLI,root@128.5.197.2,sensor_alarm,Set SNMP trap community to
(mytrap)
2013-11-12 08:22:22 CLI,root@128.5.197.2,sensor_alarm,Enable SNMP trap destination 1
Input 'q' to quit:
```

4.7.12 Загрузка данных Systemcom (systemcom)

Функция

Команда **systemcom** используется для загрузки файла SOL.

Формат

ipmcget -d systemcom

Параметры

–

Инструкции по использованию

Перед выполнением этой команды убедитесь, что функция загрузки данных посредством последовательного порта включения на странице **Serial Port Data** веб-интерфейса iBMC.

Пример

Загрузка файла SOL.

```
iBMC:/->ipmcget -d systemcom
Download System Com data to /tmp/systemcom.tar successfully.
```

4.7.13 Загрузка файла черного ящика (blackbox)

Функция

Команда **blackbox** используется для загрузки файла черного ящика.

Формат

ipmcget -d blackbox

Параметры

–

Инструкции по использованию

Черный ящик хранит базовую информацию сервера до критической ошибки, например, сбоя ОС.

Перед выполнением этой команды убедитесь, что функция черного ящика включена на **Diagnosis** > **Black Box** веб-интерфейса iBMC. Подробная информация приведена в разделе 3.5.3 Черный ящик.

ВНИМАНИЕ

Функция черного ящика может использоваться только после того, как на сервере установлено программное обеспечение для мониторинга сбоев (например, iBMA). Подробная информауия об анализе данных черного ящика приведена в документе *Руководство пользователя iBMA*.

Пример

Загрузка данных черного ящика.

```
iBMC:/->ipmcget -d blackbox
Downloading...
100%
Download Black Box data to /tmp/blackbox.tar successfully.
```

4.7.14 Загрузка BIOS (download)

Функция

Команда **maintenance -d download** используется для загрузки файла BIOS **bios.bin** в **/tmp**.

Файл **bios.bin** помогает помогает находить сбои запуска ОС и ошибки BIOS.

Формат

ipmcset -t maintenance -d download –v <*option*>

Параметры

Параметр	Описание	Значение
option	Каталог назначения, в который загружаются данные BIOS.	Значение должно быть **1**, что означает **/tmp**.

Инструкции по использованию

При возникновении сбоя загрузите файл **bios.bin** и свяжитесь со службой технической поддержки Huawei.

Чтобы предотвратить таймаут, отключите функцию режима ожидания CLP перед загрузкой данных BIOS. Подробная информация приведена в разделе 5.11 Отключение функции времени ожидания CLP (notimeout).

Пример

Загрузка файла BIOS **bios.bin** в **/tmp/**.

```
iBMC:/->ipmcset -t maintenance -d download –v 1
Download /tmp/bios.bin.
Downloading BIOS...
```

```
Download BIOS successfully.
```

4.7.15 Обновление BIOS (upgradebios)

Функция

Команда **maintenance -d upgradebios** используется для обновления BIOS.

Формат

ipmcset -t maintenance -d upgradebios -v *filepath*

Параметры

Параметр	Описание	Значение
filepath	Путь к файлу обновления BIOS.	–

Инструкции по использованию

Обе команды **maintenance -d upgradebios** и **upgrade** могут использоваться для обновления BIOS, различия в следующем:

- Если используется команда **maintenance -d upgradebios**, после обновления восстанавливаются настройки BIOS по умолчанию.
- Если используется команда **upgrade**, настройки системы не изменятся. Подробная информация приведена в разделе 4.3.13 Обновление встроенного ПО (upgrade).

Пример

Обновление BIOS с помощью файла **/tmp/biosimage.hpm**.

```
iBMC:/->ipmcset -t maintenance -d upgradebios -v /tmp/biosimage.hpm
Please make sure the iBMC is working while upgrading.
Updating...
System needs two minutes time to prepare.
<100%>
Update successfully.
```

4.7.16 Настройки состояния сетевого порта iBMC (ethlink)

Функция

Команда **maintenance -d ethlink** используется для настройки состояния сетевого порта iBMC.

Формат

ipmcset -t maintenance -d ethlink -v <*ethname*> <*action*>

Параметры

Параметр	Описание	Значение
ethname	Настраиваемый сетевой порт iBMC.	• eth0 • eth1 • eth2 • eth3 Количество сетевых портов iBMC зависит от модели сервера.
action	Состояние сетевого порта.	• enable • disable

Инструкции по использованию

–

Пример

Включение сетевого порта iBMC **eth2**.

```
iBMC:/->ipmcset -t maintenance -d ethlink -v eth2 enable
WARNING: This operation will enable eth2.
Do you want to continue?[Y/N]:y
Enable eth2 successfully.
```

4.7.17 Выполнение сбора информации одним щелчком кнопки мыши (diaginfo)

Функция

Команда **diaginfo** используется для выполнения сбора информации одним щелчком кнопки мыши. Подробная информация приведена в разделе 3.11 Сбор информации одним щелчком кнопки мыши.

Формат

ipmcget -d diaginfo

Параметры

–

Инструкции по использованию

–

Пример

Сбор информации одним щелчком кнопки мыши.

```
iBMC:/->ipmcget -d diaginfo
Download diagnose info to /tmp/ successfully.
```

4.7.18 Восстановление заводских настроек iBMC (restore)

Функция

Команда **restore** используется для восстановления заводских настроек iBMC. После выполнения команды производится перезапуск iBMC.

Формат

ipmcset -d restore

Параметры

–

Инструкции по использованию

–

Пример

Восстановление заводских настроек iBMC.

```
iBMC:/->ipmcset -d restore
WARNING: The iBMC will automatically restart and restore factory settings. Continue?
[Y/N]:Y
Restore factory setting successfully.
```

4.7.19 Включение и отключение функции времени ожидания CLP

Функция

Команда **notimeout** используется для включения или отключения функции времени ожидания CLP. После выполнения этой команды вам необходимо выйти и повторно войти в iBMC, чтобы настройки вступили в силу.

По умолчанию, функция времени ожидания CLP отключена.

Формат

ipmcset -d notimeout -v <enabled | disabled>

Параметры

Параметр	Описание	Значение
enabled	Включение функции времени ожидания CLP.	–

Параметр	Описание	Значение
disabled	Отключение функции времени ожидания CLP.	–

Инструкции по использованию

–

Пример

Включение функции времени ожидания CLP.

```
iBMC:/->ipmcset -d notimeout -v enabled
Set no timeout state successfully.
```

Отключение функции времени ожидания CLP.

```
iBMC:/->ipmcset -d notimeout -v disabled
Set no timeout state successfully.
```

4.7.20 Обновление рабочей таблицы (Workkey) системы (workkey)

Функция

Команда **workkey** используется для обновления рабочей таблицы системы.

Формат

ipmcset -d workkey

Параметры

–

Инструкции по использованию

–

Пример

Обновление рабочей таблицы системы.

```
iBMC:/->ipmcset -d workkey
Update system workkey successfully.
```

4.7.21 Запрос и настройка конфигурации автоматического обнаружения (autodiscovery)

Функция

Команда **autodiscovery** используется для запроса и настройки функции автоматического обнаружения.

Формат

ipmcget -d autodiscovery

ipmcset -d autodiscovery -v <enable>/<disable> [option(0/1)] [netport]

Параметры

Параметр	Описание	Значение
enabled/disable	Включение или отключение функции автоматического обнаружения.	• **enable**: включение автоматического обнаружения. • **disable**: отключение автоматического обнаружения.
option	Сетевой сегмент.	• **0**: вещание на 255.255.255.255 • **1**: адрес вещания подсети
netport	Номер порта.	от 0 до 65535

Инструкции по использованию

–

Пример

Запрос конфигурации функции автоматического обнаружения.

```
iBMC:/->ipmcget -d autodiscovery
State        : disabled
Broadcast    : 255.255.255.255
NetPort      : 26957
```

Включение функции автоматического обнаружения.

```
iBMC:/->ipmcset -d autodiscovery -v enable 0 26957
Set state to (enable) successfully.
Set broadcast to (255.255.255.255) successfully.
Set netport to (26957) successfully.
```

4.7.22 Запрос и настройка конфигурации контролируемого включения питания (poweronpermit)

Функция

Команда **poweronpermit** используется для запроса и настройки функции контролируемого включения питания.

Формат

ipmcget -d poweronpermit

ipmcset -d poweronpermit -v <**enable** | **disable**> [*ip*] [*netport*]

Параметры

Параметр	Описание	Значение
Опция включения (Enable)	Включение функции контролируемого включения питания.	–
Опция отключения (disable)	Отключение функции контролируемого включения питания.	–
ip	IP-адрес сервера.	–
netport	Номер порта.	от 0 до 65535

Инструкции по использованию

–

Пример

Запрос конфигурации функции контролируемого включения питания.

```
iBMC:/->ipmcget -d poweronpermit
State        : enabled
ManagerIP    : 192.168.1.1
ManagerPort  : 26957
```

Включение функции контролируемого включения питания.

```
iBMC:/->ipmcset -d poweronpermit -v enable 192.168.1.1 26957
Set poweronpermit successfully.
```

4.7.23 Запрос и настройка статуса включения печати BIOS (biosprint)

Функция

Команда **biosprint** используется для запроса и настройки отладки BIOS. Если функция отладки BIOS включена, инфорамция об отладке будет отправлена на последовательный порт во время процесса POST.

Формат

ipmcget -t maintenance -d biosprint

ipmcset -t maintenance -d biosprint -v <*option*>

Параметры

Параметр	Описание	Значение
<*option*>	Выполняемая операция.	• **1**: принудительное включение отладки BIOS. • **2**: применение настроек на BIOS.

Инструкции по использованию

RH1288A V2 и RH2288A V2 не поддерживают эту команду.

Пример

Включение печати BIOS.

```
iBMC:/->ipmcset -t maintenance -d biosprint -v 1
WARNING: Setting BIOS debug info enbale will make system start slow. Do you want to
continue?[Y/N]y
Set BIOS debug info enable successfully
```

Запрос статуса печати BIOS.

```
iBMC:/->ipmcget -t maintenance -d biosprint
BIOS debug info enable
```

4.8 Команды управления пользователями

В данном разделе приведено описание всех команд управления пользователями.

4.8.1 Запрос информации обо всех пользователях (userlist/list)

Функция

Команда **userlist** используется для запроса информации обо всех пользователях.

Формат

ipmcget -d userlist

ipmcget -t user -d list

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации обо всех пользователях.

```
iBMC:/->ipmcget -t user -d list
ID     Name            Privilege     Interface
PublicKeyHash                              State
2      root            ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
3      test1           CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
4      test2           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
5      test3           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
6      test4           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Disabled
7      test5           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
8      test6           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
9      test7           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Disabled
10     test8           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
11     test9           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Disabled
12     test10          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Disabled
13     test11          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Disabled
14     test12          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Disabled
15     test13          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Disabled
16     test14          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Disabled
17     test15          ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
```

4.8.2 Добавление пользователя (adduser)

Функция

Команда **adduser** используется для добавления пользователя.

Формат

ipmcset [-t user] -d adduser -v <*username*>

Параметры

Параметр	Описание	Значение
username	Имя добавляемого пользователя.	Значение: строка, длиной до 16 символов. • Строка может содержать цифры, буквы и другие символы, исключая пробелы и следующие специальные символы: , \ : < > & ' " / % • Строка не может начинаться с знака номера (#).

Инструкции по использованию

Система поддерживает добавление максимум 15 пользователей. Вам необходимо установить пароли разных уровней сложности для новых пользователей на основе того, включена ли функция проверки сложности пароля (запрос с помощью команды 4.8.6 Запрос и настройка статума функции проверки сложности пароля (passwordcomplexity)).

- Если функция проверки сложности пароля отключена, то пароль не может быть пустым. В качестве пароля должна использоваться строка, длиной до 20 символов.
- Если проверка сложности пароля включена, то пароль должен соответствовать следующим требованиям:
  - Содержать от 8 до 20 символов.
  - Содержать, как минимум, один пробел или один из следующих специальных символов:

    ` ~ ! @ # $ % ^ & * () - _ = + \ | [{}] ; : ' " ,<.> / ?
  - Содержать, как минимум, символы двух видов:
    - Строчные буквы: от a до z
    - Буквы: от A до Z
    - Цифры: от 0 до 9
  - Пароль не должен совпадать с именем пользователя в прямом и обратном порядке расположения символов.
  - Новый пароль должен отличаться от старого пароля, как минимум, расположением двух символов.

Только администраторы могут добавлять нового пользователя, и необходим пароль текущего пользователя.

ПРИМЕЧАНИЕ

По умолчанию уровень привилегии нового пользователя – **No Access**, и новый пользователь поддерживает все интерфейсы входа.

Пример

Добавление пользователя и настройка имени **test**.

```
iBMC:/->ipmcset -d adduser -v test
Input your password:
Password:
Confirm password:
Add user successfully.
```

Запрос списка пользователей после добавления.

```
iBMC:/->ipmcget -d userlist
ID     Name            Privilege     Interface
PublicKeyHash                              State
2      root            ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
3      test            NO ACCESS     Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA                                        Enabled
4                      NO ACCESS                                          NA
Disabled
5                      NO ACCESS                                          NA
Disabled
6                      NO ACCESS                                          NA
Disabled
7                      NO ACCESS                                          NA
Disabled
8                      NO ACCESS                                          NA
Disabled
9                      NO ACCESS                                          NA
Disabled
10                     NO ACCESS                                          NA
Disabled
11                     NO ACCESS                                          NA
Disabled
12                     NO ACCESS                                          NA
Disabled
13                     NO ACCESS                                          NA
Disabled
14                     NO ACCESS                                          NA
Disabled
15                     NO ACCESS                                          NA
Disabled
16                     NO ACCESS                                          NA
Disabled
17                     NO ACCESS                                          NA
Disabled
```

Предыдущая информация указывает, что пользователь **test** успешно добавлен.

4.8.3 Изменение пароля пользователя (password)

Функция

Команда **password** используется для изменения пароля пользователя.

Формат

ipmcset [-t user] -d password -v *username*

Параметры

Параметр	Описание	Значение
username	Существующий пользователь, пароль которого необходимо изменить.	–

Инструкции по использованию

Вы можете изменять пароли разных уровней сложности на основе того, включена ли функция проверки сложности пароля (запрос с помощью команды 4.8.6 Запрос и настройка статума функции проверки сложности пароля (passwordcomplexity)).

- Если функция проверки сложности пароля отключена, то пароль не может быть пустым. В качестве пароля должна использоваться строка, длиной до 20 символов.
- Если проверка сложности пароля включена, то пароль должен соответствовать следующим требованиям:
  - Содержать от 8 до 20 символов.
  - Содержать, как минимум, один пробел или один из следующих специальных символов:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
  - Содержать, как минимум, символы двух видов:
    - Строчные буквы: от a до z
    - Буквы: от A до Z
    - Цифры: от 0 до 9
  - Пароль не должен совпадать с именем пользователя в прямом и обратном порядке расположения символов.
  - Новый пароль должен отличаться от старого пароля, как минимум, расположением двух символов.

Администраторы имеют право изменять пароли всех пользователей, а операторы и обычные пользователи имеют право изменять только свои собственные пароли. При изменении пароля необходим пароль текущего пользователя.

Пример

Изменение пароля **user**.

```
iBMC:/->ipmcset -d password -v user
Input your password:
New password:
```

```
Confirm password:
Set user password successfully.
```

4.8.4 Удаление пользователя (deluser)

Функция

Команда **deluser** используется для удаления пользователя.

Формат

ipmcset [-t user] -d deluser -v *username*

Параметры

Параметр	Описание	Значение
username	Имя существующего пользователя, которого необходимо удалить.	–

Инструкции по использованию

Только администраторы могут удалять пользователя, и необходим пароль текущего пользователя.

Пример

Удаление пользователя с именем **test**.

```
iBMC:/->ipmcset -d deluser -v test
Input your password:
Delete user successfully.
```

4.8.5 Настройка прав пользователя (privilege)

Функция

Команда **privilege** используется для настройки прав пользователя.

Формат

ipmcset [-t user] -d privilege -v <*username*> <*privalue*>

Параметры

Параметр	Описание	Значение
username	Существующий пользователь, права которого необходимо настроить.	–

Параметр	Описание	Значение
privalue	Права	• 15: отсутствие прав доступа • 2: права пользователя • 3: права оператора • 4: права администратора • 5: пользовательские права Role1 • 6: пользовательские права Role2 • 7: пользовательские права Role3 • 8: пользовательские права Role4

Инструкции по использованию

Только администраторы могут настраивать права пользователя, и необходим пароль текущего пользователя.

Пример

Предоставление пользователю **test** прав **Administrator**.

```
iBMC:/->ipmcset -d privilege -v test 4
Input your password:
Set user privilege successfully.
```

4.8.6 Запрос и настройка статума функции проверки сложности пароля (passwordcomplexity)

Функция

Команда **passwordcomplexity** используется для запроса и настройки статуса функции проверки сложности пароля.

Формат

ipmcget [-t user] -d passwordcomplexity

ipmcset [-t user] -d passwordcomplexity -v <enabled | disabled>

Параметры

Параметр	Описание	Значение
enabled	Включение функции проверки сложности пароля.	–
disabled	Отключение функции проверки сложности пароля.	–

Инструкции по использованию

ВНИМАНИЕ

- По умолчанию функция проверки сложности пароля включена.
- Отключение функции проверки сложности пароля снижает безопасность системы. Следует с осторожностью настраивать этот параметр.

- Если функция проверки сложности пароля отключена, то пароль не может быть пустым. В качестве пароля должна использоваться строка, длиной до 20 символов.
- Если проверка сложности пароля включена, то пароль должен соответствовать следующим требованиям:
  - Содержать от 8 до 20 символов.
  - Содержать, как минимум, один пробел или один из следующих специальных символов:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
  - Содержать, как минимум, символы двух видов:
    - Строчные буквы: от a до z
    - Буквы: от A до Z
    - Цифры: от 0 до 9
  - Пароль не должен совпадать с именем пользователя в прямом и обратном порядке расположения символов.
  - Новый пароль должен отличаться от старого пароля, как минимум, расположением двух символов.

Только администраторы могут настраивать статус функции проверки сложности пароля.

Пример

Запрос статуса функции проверки сложности пароля.

```
iBMC:/->ipmcget -d passwordcomplexity
Password complexity check state : enabled
```

Включение функции проверки сложности пароля.

```
iBMC:/->ipmcset -d passwordcomplexity -v enabled
Set password complexity check state successfully.
```

4.8.7 Блокировка пользователя (user -d lock)

Функция

Команда **lock** используется для блокировки определенного пользователя. Заблокированный пользователь не может войти в систему.

Формат

ipmcset -t user -d lock -v *username*

Параметры

Параметр	Описание	Значение
username	Имя блокируемого пользователя.	–

Инструкции по использованию

Только администраторы имеют разрешение на блокировку пользователей.

При блокировке пользователя необходимо ввести пароль текущего администратора.

Пример

Блокировка пользователя **admin**.

```
iBMC:/->ipmcset -t user -d lock -v admin
Input your password:
Lock user:admin successfully.
```

4.8.8 Разблокировка пользователя (user -d unlock)

Функция

Команда **unlock** используется для разблокировки пользователя, находящегося в блокировке.

Формат

ipmcset -t user -d unlock -v *username*

Параметры

Параметр	Описание	Значение
username	Имя разблокируемого пользователя.	–

Инструкции по использованию

Только администраторы могут выполнять эту операцию, необходим пароль администратора.

Пример

Разблокировка пользователя **root**.

```
iBMC:/->ipmcset -t user -d unlock -v root
Input your password:
Set user:root unlock status successfully.
```

4.8.9 Запрос и настройка периода действия пароля (minimumpasswordage)

Функция

Команда **minimumpasswordage** используется для запроса и настройки периода действия пароля.

Формат

ipmcget -d minimumpasswordage

ipmcset -d minimumpasswordage -v *time*

Параметры

Параметр	Описание	Значение
time	Срок действия пароля (дней).	Диапазон значений: от 0 до 365 **0** означает, что у пароля нет срока действия.

Инструкции по использованию

Только администраторы могут настраивать период действия пароля.

Пример

Настройка для периода действия пароля значения один день.

```
iBMC:/->ipmcset -d minimumpasswordage -v 1
Set minimum password age successfully, minimumpasswordage(1) days.
```

4.8.10 Настройка пользователя для экстренного входа в систему (emergencyuser)

Функция

Команда **emergencyuser** используется для настройки пользователя, который не ограничен никакими правилами входа.

Формат

ipmcset [-t user] -d emergencyuser -v *username*

Параметры

Параметр	Описание	Значение
username	Имя пользователя для экстренного входа в систему.	–

Инструкции по использованию

Только администратор может устанавливать пользователя для экстренного входа в систему.

Пример

Настройка пользователя **root** для экстренного входа.

```
iBMC:/->ipmcset -d emergencyuser -v root
Set emergency user to (root) successfully.
```

4.8.11 Импорт открытого ключа SSH пользователя (addpublickey)

Функция

Команда **addpublickey** используется для импорта открытого ключа SSH пользователя.

Формат

ipmcset -t user -d addpublickey -v *username filepath file URL*

Параметры

Параметр	Описание	Значение
username	Пользователь, для которого импортируется открытый ключ SSH.	Существующее имя пользователя.
filepath	Путь, с которого импортируется открытый ключ.	Значение должно быть указано в формате ***/Path/File name*.**
file URL	URL-адрес импортируемого файла открытого ключа.	Значение в следующем формате: *protocol*://*username*:*password*@IP:[port]/*directory/filename* Где: • Значение *protocol* должно быть **https** или **http**. • Значения *username* и *password* – это имя пользователя и пароль для доступа на целевой сервер. • Значение *directory/filename* – это путь файла открытого ключа на целевом сервере.

Инструкции по использованию

Администраторы могут импортировать открытые ключи SSH для всех пользователей. Обычные пользователи могут импортировать только свои открытые ключи SSH.

Пример

Импорт открытого ключа SSH для пользователя **ssh_user**.

```
iBMC:/->ipmcset -t user -d addpublic -v ssh_user /tmp/id_dsa_1024.key
Input your password:
Add user public key successfully.
```

4.8.12 Удаление открытого ключа SSH пользователя (delpublickey)

Функция

Команда **delpublickey** используется для удаления открытого ключа SSH пользователя.

Формат

ipmcset -t user -d delpublickey -v *username*

Параметры

Параметр	Описание	Значение
username	Имя пользователя, для которого удаляется открытый ключ SSH.	–

Инструкции по использованию

Администраторы могут удалять открытые ключи SSH всех пользователей. Обычные пользователи могут удалять только свои открытые ключи SSH.

Пример

Удаление открытого ключа пользователя **ssh_user_01**.

```
iBMC:/->ipmcset -t user -d delpublickey -v ssh_user_01
Input your password:
Delete user public key successfully.
```

4.8.13 Запрос и настройка статуса включения аутентификации пароля пользователя SSH (sshpasswordauthentication)

Функция

Команда **sshpasswordauthentication** используется для включения или отключения аутентификации пароля пользователя SSH.

Формат

ipmcget -t user -d sshpasswordauthentication

ipmcset -t user -d sshpasswordauthentication -v <**enabled** | **disabled**>

Параметры

Параметр	Описание	Значение
enabled	Включение аутентификации пароля пользователя SSH.	–
disabled	Отключение аутентификации пароля пользователя SSH.	–

Инструкции по использованию

–

Пример

Включение аутентификации пароля пользователя SSH.

```
iBMC:/->ipmcset -t user -d sshpasswordauthentication -v enabled
Set SSH password authentication successfully.
```

Запрос статуса включения аутентификации пароля пользователя SSH.

```
iBMC:/-> ipmcget -t user -d sshpasswordauthentication
SSH Password Authentication : enabled
```

4.8.14 Настройка пользовательских интерфейсов для входа в систему iBMC (interface)

Функция

Команда **interface** используется для настройки пользовательских интерфейсов, которые могут использоваться определенными пользователями для входа в iBMC.

Формат

ipmcset -t user -d interface -v *username* <**enabled** | **disabled**> <*option1 option2 ... optionN*>

Параметры

Параметр	Описание	Значение
username	Имя конфигурируемого пользователя.	–
enabled	Включение интерфейсов.	–
disabled	Отключение интерфейсов.	–
option1 *option2 ...* *optionN*	Типы конфигурируемых интерфейсов.	Можно настроить несколько типов интерфейсов одновременно. Варианты: • **1**: Web • **2**: SNMP • **3**: IPMI • **4**: SSH • **5**: SFTP • **7**: локальный • **8**: Redfish

Инструкции по использованию

–

Пример

Включение интерфейсов для входа в iBMC: **Web, SNMP, IPMI, SSH, SFTP, Local** для пользователя **test**.

```
iBMC:/->ipmcset -t user -d interface -v test enabled 1 2 3 4 5 7
Input your password:
Set user login interface successfully.
```

Запрос информации о пользователе **ssh_user_01**.

```
iBMC:/->ipmcget -t user -d list
ID     Name            Privilege     Interface
PublicKeyHash
2      root            ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
3      xxx             CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
4      commonuser       USER          Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
5      admin           ADMINISTRATOR  Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
6      operator         OPERATOR      Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
7      custom1          CUSTOM ROLE1   Web,SNMP,IPMI,SSH,SFTP,Local,Redfish
NA
8      test            USER          Web,SNMP,IPMI,SSH,SFTP,Local                NA
```

```
9                    NO ACCESS                                          NA
10                   NO ACCESS                                          NA
11                   NO ACCESS                                          NA
12                   NO ACCESS                                          NA
13                   NO ACCESS                                          NA
14                   NO ACCESS                                          NA
15                   NO ACCESS                                          NA
16                   NO ACCESS                                          NA
17                   NO ACCESS
```

4.8.15 Настройка статуса проверки слабого пароля (weakpwddic)

Функция

Команда **weakpwddic** используется для включения или отключения проверки слабого пароля.

Формат

ipmcset -t user -d weakpwddic -v <**enabled** | **disabled**>

Параметры

Параметр	Описание	Значение
enabled	Включение проверки слабого пароля.	–
disabled	Отключение проверки слабого пароля.	–

Инструкции по использованию

Данная команда доступна только для серверов V5.

Пример

Включение проверки слабого пароля.

```
iBMC:/-> ipmcset -t user -d weakpwddic -v enabled
Enable weak password dictionary check successfully.
```

4.8.16 Экспорт справочника слабых паролей (weakpwddic -v export)

Функция

Команда **weakpwddic -v export** используется для экспорта справочника слабых паролей системы iBMC.

Формат

ipmcset -t user -d weakpwddic -v export <*filepath* | *file_URL*>

Параметры

Параметр	Описание	Значение
filepath	Локальный каталог, в котором хранится справочник слабых паролей.	Абсолютный каталог на iBMC, например, **/tmp/weakpwddictionary**.
file_URL	Удаленный путь справочника слабых паролей.	Имеет следующий формат: *protocol*://*username*:*password@IP*:*[port]*/*directory/filename* Где • *protocol* должен быть **https**, **sftp**, **cifs**, **scp** или **nfs**. • *username* – это имя пользователя, используемого для входа на целевой сервер. • *password* – это пароль для входа на целевой сервер. • *IP:[port]* – это IP-адрес и номер порта целевого сервера. • *directory/filename* – это абсолютный каталог, в котором хранится справочник слабых паролей на целевом сервере. Пример значения: **https://root:Huawei12#$@10.10.10.1:443/tmp/weakpwddictionary**

Инструкции по использованию

Данная команда доступна только для серверов V5.

Пример

Экспорт справочника слабых паролей.

```
iBMC:/-> ipmcset -t user -d weakpwddic -v export /tmp/weakpwddictionary
Export weak password dictionary successfully.
```

4.8.17 Импорт справочника слабых паролей (weakpwddic -v import)

Функция

Команда **weakpwddic -v import** используется для импорта справочника слабых паролей в систему iBMC.

Формат

ipmcset -t user -d weakpwddic –v import <*filepath* | *file_URL*>

Параметры

Параметр	Описание	Значение
filepath	Каталог, в который импортируется справочник слабых паролей на iBMC.	Абсолютный каталог на iBMC, например, **/tmp/weakpwddictionary**.
file_URL	Удаленный путь справочника слабых паролей.	Имеет следующий формат: *protocol*://*username*:*password@IP:[port]*/*directory/filename* Где • *protocol* должен быть **https**, **sftp**, **cifs**, **scp** или **nfs**. • *username* – это имя пользователя, используемого для входа на целевой сервер. • *password* – это пароль для входа на целевой сервер. • *IP:[port]* – это IP-адрес и номер порта целевого сервера. • *directory/filename* – это абсолютный каталог, в котором хранится справочник слабых паролей на целевом сервере. Пример значения: **https://root:Huawei12#$@10.10.10.1:443/tmp/weakpwddictionary**

Инструкции по использованию

Данная команда доступна только для серверов V5.

Пример

Импорт справочника слабых паролей.

```
iBMC:/-> ipmcset -t user -d weakpwddic -v import /tmp/weakpwddictionary
Import weak password dictionary successfully.
```

4.8.18 Настройка пароля шифрования для пользователя SNMPv3 (snmpprivacypassword)

Функция

Команда **snmpprivacypassword** используется для настройки пароля шифрования данных для пользователя, который применяет SNMPv3 для подключения к iBMC.

Формат

ipmcset -t user -d snmpprivacypassword -v *username*

Параметры

Параметр	Описание	Значение
username	Существующий пользователь, пароль которого необходимо изменить.	–

Инструкции по использованию

Данная команда доступна только для серверов V5.

Только администратор может устанавливать и изменять пароли всех пользователей, а операторы и обычные пользователи могут изменять только свои собственные пароли. При изменении пароля необходим пароль текущего пользователя.

Правила настройки пароля различаются в зависимости от того, включена ли проверка сложности пароля (запрос с помощью команды 4.8.6 Запрос и настройка статума функции проверки сложности пароля (passwordcomplexity)).

- Если проверка сложности пароля отключена, то пароль должен представлять строку длиной до 20 символов.
- Если проверка сложности пароля включена, то пароль должен соответствовать следующим требованиям:
  - Он может включать от 8 до 20 символов.
  - содержать, как минимум, один пробел или один из следующих специальных символов:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
  - Содержать как минимум два типа следующих символов: прописные буквы от A до Z, строчные буквы от a до z, цифры от 0 до 9.
  - Пароль не должен совпадать с именем пользователя в прямом и обратном порядке расположения символов.
  - Старый и новый пароли должны отличаться минимум двумя символами.
- Запрещено использовать пароль, если он находится в справочнике слабых паролей. Вы можете выполнить 4.8.6 Запрос и настройка статума функции проверки сложности пароля (passwordcomplexity) для запроса слабых паролей.

Пример

Пароль шифрования SNMP v3 для пользователя аутентификации.

```
iBMC:/->ipmcset -t user -d snmpprivacypassword -v Administrator
Input your password:
Password:
Confirm password:
Set snmp privacy password successfully.
```

4.9 Команды NTP

В данном разделе приведено описание команд, связанных с протоколом сетевого времени (NTP – Network Time Protocol).

4.9.1 Запрос информации NTP (ntpinfo)

Функция

Команда **ntpinfo** используется для запроса информации NTP iBMC.

Формат

ipmcget -d ntpinfo

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации NTP iBMC.

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : dhcpv4
Preferred Server   : 192.168.2.26
Alternative Server : 192.168.2.77
Synchronize       : successful
Auth Enable       : disabled
Group Key         : not imported
```

4.9.2 Настройка статуса NTP (ntp -d status)

Функция

Команда **ntp -d status** используется для включения или отключения функции NTP.

Формат

ipmcset -t ntp -d status -v *status*

Параметры

Параметр	Описание	Значение
status	Статус NTP.	• enabled

Параметр	Описание	Значение
		• disabled

Инструкции по использованию

–

Пример

Включение функции NTP.

```
iBMC:/->ipmcset -t ntp -d status -v enabled
Set NTP enable status (enabled) successfully.
```

Запрос информации NTP.

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : dhcpv6
Preferred Server   : 2016:ed8:77b5:0:192:168:2:26
Alternative Server : 2016:ed8:77b5:0:192:168:9:77
Synchronize       : successful
Auth Enable       : disabled
Group Key         : not imported
```

4.9.3 Настройка способа получения информации NTP (ntp -d mode)

Функция

Команда **ntp -d mode** используется для настройки способа получения информации NTP.

Формат

ipmcset -t ntp -d mode -v *mode*

Параметры

Параметр	Описание	Значение
mode	Способ получения информации NTP.	• **manual**: получение информации NTP вручную. • **dhcpv4**: автоматическое получения информации NTP с использованием DHCPv4. • **dhcpv6**: автоматическое получение информации NTP с использованием

Параметр	Описание	Значение
		DHCPv6.

Инструкции по использованию

Если для параметра *mode* установлено значение **DHCPv4**, то не нужно указывать часовой пояс.

Пример

Получение информации NTP вручную.

```
iBMC:/->ipmcset -t ntp -d mode -v manual
Set NTP mode (manual) successfully.
```

Запрос информации NTP.

```
iBMC:/->ipmcget -d ntpinfo
Status : enabled
Mode             : manual
Preferred Server   : 192.168.2.26
Alternative Server : 192.168.2.99
Synchronize       : successful
Auth Enable       : disabled
Group Key         : not imported
```

4.9.4 Настройка адреса для предпочтительного сервера NTP (ntp -d preferredserver)

Функция

Команда **ntp -d preferredserver** используется для установки предпочтительного сервера NTP.

Формат

ipmcset -t ntp -d preferredserver -v *addr*

Параметры

Параметр	Описание	Значение
addr	IP-адрес предпочтительного сервера NTP.	Значение может быть представлено в одном из следующих форматов: • IPv4-адрес • IPv6-адрес • Имя домена

Инструкции по использованию

–

Пример

Установка адреса предпочтительного сервера NTP **dhcp1.com**.

```
iBMC:/->ipmcset -t ntp -d preferredserver -v dhcp1.com
Set NTP preferred server (dhcp1.com) successfully.
```

Запрос информации NTP.

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : 2016:ed8:77b5:0:192:168:9:78
Synchronize       : sucessful
Auth Enable       : disabled
Group Key         : not imported
```

4.9.5 Настройка адреса альтернативного сервера NTP (ntp -d alternativeserver)

Функция

Команда **ntp -d alternativeserver** используется для установки альтернативного сервера NTP.

Формат

ipmcset -t ntp -d alternativeserver -v *addr*

Параметры

Параметр	Описание	Значение
addr	Адрес альтернативного сервера NTP.	Значение может быть представлено в одном из следующих форматов: • IPv4-адрес • IPv6-адрес • Имя домена

Инструкции по использованию

–

Пример

Установка адреса альтернативного сервера NTP **2001::1234**.

```
iBMC:/-> ipmcset -t ntp -d alternativeserver -v 2001::1234
Set NTP alternative server (2001::1234) successfully.
```

Запрос информации NTP.

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : 2001::1234
Synchronize       : sucessful
Auth Enable       : disabled
Group Key         : not imported
```

4.9.6 Настройка аутентификации сервера NTP (ntp -d authstatus)

Функция

Команда **ntp -d authstatus** используется для настройки статуса аутентификации сервера NTP.

- Если аутентификация включена, то она выполняется перед установлением соединения между iBMC и сервером NTP.
- Если аутентификация отключена, то перед установлением соединения между iBMC и сервером NTP выполнять аутентификацию не требуется.

Формат

ipmcset -t ntp -d authstatus -v *status*

Параметры

Параметр	Описание	Значение
status	Необходимость выполнения аутентификации.	• enabled • disabled

Инструкции по использованию

Если аутентификация включена, то на iBMC необходимо загрузить групповой ключ.

Пример

Включение аутентификации для серверов NTP.

```
iBMC:/->ipmcset -t ntp -d authstatus -v enabled
Set NTP enable status (enabled) successfully.
```

Запрос информации NTP.

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : 2001::1234
Synchronize       : sucessful
Auth Enable       : enabled
Group Key         : not imported
```

4.9.7 Загрузка группового ключа NTP (ntp -d groupkey)

Функция

Команда **ntp -d groupkey** используется для загрузки группового ключа NTP на iBMC. Групповой ключ NTP используется для проверки аутентификации при установлении связи между iBMC и сервером NTP.

Формат

ipmcset -t ntp -d groupkey -v *filepath*

Параметры

Параметр	Описание	Значение
filepath	Файл, в котором содержится груповой ключ.	Данный параметр представлен в формате *путь к файлу + имя файла*.

Инструкции по использованию

Перед выполнением данной команды необходимо сохранить файл с групповым ключом в каталог iBMC.

Пример

Загрузка группового ключа NTP в iBMC.

```
iBMC:/->ipmcset -t ntp -d groupkey -v /tmp/ntp.keys
Set NTP group key (/tmp/ntp.keys) successfully.
```

Запрос информации NTP.

```
iBMC:/->ipmcget -d ntpinfo
Status           : enabled
Mode             : manual
Preferred Server   : dhcp1.com
Alternative Server : 2001::1234
```

```
Synchronize       : sucessful
Auth Enable       : enabled
Group Key         : imported
```

4.10 Команды на индикаторы

В данном разделе приведено описание всех команд на индикаторы.

4.10.1 Запрос статуса текущего индикатора (ledinfo)

Функция

Команда **ledinfo** используется для запроса статуса текущего индикатора.

Формат

ipmcget -d ledinfo

Параметры

–

Инструкции по использованию

–

Пример

Запрос статуса индикатора

```
iBMC:/->ipmcget -d ledinfo
LED Name             : SysHealLed
LED Mode             : Local Control
LED State            : BLINKING
Off Duration         : 100 ms
On Duration          : 100 ms
LED Color            : RED
LED Color Capabilities : RED GREEN
Default LED Color in
     Local Control   : GREEN
     Override State  : GREEN

LED Name             : UIDLed
LED Mode             : Local Control
LED State            : OFF
LED Color            : BLUE
LED Color Capabilities : BLUE
Default LED Color in
     Local Control   : BLUE
     Override State  : BLUE
```

4.10.2 Настройка индикатора UID (identify)

Функция

Команда **identify** используется для настройки индикатора UID.

Формат

ipmcset -d identify [**-v** {*time* | **force** }]

Параметры

Параметр	Описание	Значение
time	Продолжительность включения индикатора UID.	В качестве значения используется целое число. Единица измерения: секунды. Диапазон значений от 0 до 255. 0: индикатор выключен.
force	Постоянное включение индикатора UID.	–

Инструкции по использованию

Если ни один из параметров не установлен, то индикатор UID по умолчанию будет включен на 15 секунд.

Пример

Постоянное включение индикатора UID.

```
iBMC:/->ipmcset -d identify -v force
Identify UID led successfully.
```

4.10.3 Настройка статуса индикатора местоположения (locate)

Функция

Команда **locate** используется для настройки статуса индикатора местоположения жесткого диска.

Формат

ipmcget -d locate -v <*ID*> <*Action*>

Параметры

Параметр	Описание	Значение
ID	ID жесткого диска.	от **0** до **255**
Action	Статус индикатора местоположения.	• **start**: включение индикатора местоположения жесткого диска.

Параметр	Описание	Значение
		• **start**: выключение индикатора местоположения жесткого диска.

Инструкции по использованию

Если параметр **Action** имеет значение **start**, то индикатор местоположения жесткого диска буцет постоянно мигать.

Пример

Включение индикатора местоположения жесткого диска 5.

```
iBMC:/->ipmcset -d locate -v 5 start
start locating physical drive (ID:5) successfully
```

4.11 Команды на вентилятор

В данном разделе приведено описание всех команд на вентилятор.

4.11.1 Настройка скорости вращения вентилятора (fanlevel)

Функция

Команда **fanlevel** используется для настройки скорости вращения вентилятора.

Формат

ipmcset -d fanlevel -v <*fanlevel*> [*fanid*]

Параметры

Параметр	Описание	Значение
fanlevel	Процентное соотношение текущей скорости вращения вентилятора к полной скорости вращения вентилятора.	В качестве значения используется целое число. Диапазон значений зависит от модели сервера.
fanid	ID вентилятора.	Диапазон значений зависит от модели сервера.

Инструкции по использованию

Если ID вентилятора не указан, то данная команда действует для всех вентиляторов.

Пример

Установка скорости вращения вентилятора 2 на 50% от максимальной скорости.

```
iBMC:/->ipmcset -d fanlevel -v 50 2
Set fan(2) level to (50%) successfully.
Current Mode         :  Auto
iBMC:/->ipmcset -d fanlevel -v 50
Set fan level successfully.
Current Mode         :  Auto
Global Manual Fan Level:  50%
```

4.11.2 Настройка режима вентилятора (fanmode)

Функция

Команда **fanmode** используется для установки режима вентилятора.

Формат

ipmcset -d fanmode -v <*mode*> [*timeout*]

Параметры

Параметр	Описание	Значение
mode	Режим работы вентилятора	• 0: автоматический режим. При этом не нужно устанавливать значение переменной *timeout*. • 1: ручной режим. При этом необходимо установить значение переменной *timeout*.
timeout	Время ожидания переключения с ручного режима на автоматический.	В качестве значения используется целое число. Единица измерения: секунды. Значение **0** означает отсутствие времени ожидания. Значение по умолчанию: 30s.

Инструкции по использованию

Режим работы вентилятора переключается на автоматический при перезапуске iBMC, сервер выключен или истекло время ожидания переключения с ручного режима в автоматический режим.

Пример

Установка ручного режима работы вентилятора, с последующим переключнием на автоматический режим по истечении 60 секунд.

```
iBMC:/->ipmcset -d fanmode -v 1 60
Set fan mode successfully.
Current Mode:      manual
```

```
Time out    :      60 секунд
```

4.11.3 Запрос статуса вентилятора (faninfo)

Функция

Команда **faninfo** используется для запроса статуса вентилятора.

Формат

ipmcget -d faninfo

Параметры

–

Инструкции по использованию

–

Пример

Запрос статуса вентилятора.

```
iBMC:/->ipmcget -d faninfo
Get fan mode and fan level successfully!
Current mode: manual,timeout 297 seconds.
Manual fan level is 80.
```

4.12 Команды на датчики

В данном разделе приведено описание всех команд на датчики.

4.12.1 Запрос информации о всех датчиках (sensor -d list)

Функция

Команда **list** используется для запроса информации о всех датчиках.

Формат

ipmcget -t sensor -d list

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации о всех датчиках (В зависимости от типа сервера используются различные датчики).

```
iBMC:/->ipmcget -t sensor -d list
sensor id  | sensor name      | value     | unit        | status | lnr       | lc        |
lnc        | unc      | uc         | unr       | phys   | nhys
0x1        | Inlet Temp       | 24.000    | degrees C   | ok     | na        | na        |
na         | 42.000   | 44.000     | na        | 2.000  | 2.000
0x2        | Outlet Temp      | 30.000    | degrees C   | ok     | na        | na        |
na         | na       | na         | na        | 2.000  | 2.000
0x3        | PCH Temp         | 32.000    | degrees C   | ok     | na        | na        |
na         | 90.000   | na         | na        | 3.000  | 3.000
0x4        | CPU1 Core Rem    | 30.000    | degrees C   | ok     | na        | na        |
na         | na       | na         | na        | 0.000  | 0.000
0x5        | CPU2 Core Rem    | 30.000    | degrees C   | ok     | na        | na        |
na         | na       | na         | na        | 0.000  | 0.000
0x6        | CPU1 DTS         | -65.000   | unspecified | ok     | na        | na        |
na         | -1.000   | na         | na        | 3.000  | 3.000
0x7        | CPU2 DTS         | -66.000   | unspecified | ok     | na        | na        |
na         | -1.000   | na         | na        | 3.000  | 3.000
0x8        | CPU1 Prochot     | 30.000    | degrees C   | ok     | na        | na        |
na         | na       | 90.000     | na        | 0.000  | 0.000
0x9        | CPU2 Prochot     | 30.000    | degrees C   | ok     | na        | na        |
na         | na       | 90.000     | na        | 0.000  | 0.000
0xa        | CPU1 VDDQ Temp   | 32.000    | degrees C   | ok     | na        | na        |
na         | 120.000  | na         | na        | 3.000  | 3.000
0xb        | CPU2 VDDQ Temp   | 32.000    | degrees C   | ok     | na        | na        |
na         | 120.000  | na         | na        | 3.000  | 3.000
0xc        | CPU1 VRD Temp    | 33.000    | degrees C   | ok     | na        | na        |
na         | 120.000  | na         | na        | 3.000  | 3.000
0xd        | CPU2 VRD Temp    | 31.000    | degrees C   | ok     | na        | na        |
na         | 120.000  | na         | na        | 3.000  | 3.000
0xe        | CPU1 MEM Temp    | 27.000    | degrees C   | ok     | na        | na        |
na         | 90.000   | na         | na        | 3.000  | 3.000
0xf        | CPU2 MEM Temp    | 27.000    | degrees C   | ok     | na        | na        |
na         | 90.000   | na         | na        | 3.000  | 3.000
0x10       | +3.3V            | 3.260     | Volts       | ok     | na        | 2.980     |
na         | na       | 3.620     | na        | 0.160  | 0.160
0x11       | +5.0V            | 4.980     | Volts       | ok     | na        | 4.530     |
na         | na       | 5.490     | na        | 0.240  | 0.240
0x12       | +12.0V           | 12.120    | Volts       | ok     | na        | 10.800    |
na         | na       | 13.200    | na        | 0.480  | 0.480
0x13       | +1.8V CPU1       | 1.800     | Volts       | ok     | na        | 1.470     |
na         | na       | 1.850     | na        | 0.020  | 0.020
0x14       | +1.8V CPU2       | 1.790     | Volts       | ok     | na        | 1.470     |
na         | na       | 1.850     | na        | 0.020  | 0.020
0x15       | +1.2V VDDQ1      | 1.180     | Volts       | ok     | na        | 1.140     |
na         | na       | 1.260     | na        | 0.020  | 0.020
0x16       | +1.2V VDDQ2      | 1.180     | Volts       | ok     | na        | 1.140     |
na         | na       | 1.260     | na        | 0.020  | 0.020
```

```
0x17      | +1.2V VDDQ3     | 1.180     | Volts       | ok    | na        | 1.140     |
na        | na      | 1.260     | na        | 0.020  | 0.020
0x18      | +1.2V VDDQ4     | 1.180     | Volts       | ok    | na        | 1.140     |
na        | na      | 1.260     | na        | 0.020  | 0.020
0x19      | FAN1 F Speed    | 6720.000  | RPM         | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x1a      | FAN1 R Speed    | 6720.000  | RPM         | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x1b      | FAN2 F Speed    | 6600.000  | RPM         | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x1c      | FAN2 R Speed    | 6600.000  | RPM         | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x1d      | FAN3 F Speed    | 6720.000  | RPM         | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x1e      | FAN3 R Speed    | 6720.000  | RPM         | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x1f      | FAN4 F Speed    | 6600.000  | RPM         | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x20      | FAN4 R Speed    | 6600.000  | RPM         | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x21      | RearDisk1 Temp  | 26.000    | degrees C   | ok    | na        | na        |
na        | 53.000  | na        | na        | 2.000  | 2.000
0x22      | Power1          | 124.000   | Watts       | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x23      | Power2          | 52.000    | Watts       | ok    | na        | na        |
na        | na      | na        | na        | 0.000  | 0.000
0x24      | CPU1 Status     | 0x0       | discrete    | 0x8080| na        | na        |
na        | na      | na        | na        | na    | na
0x25      | CPU2 Status     | 0x0       | discrete    | 0x8080| na        | na        |
na        | na      | na        | na        | na    | na
0x26      | CPU1 Memory     | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x27      | CPU2 Memory     | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x28      | FAN1 F Status   | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x29      | FAN1 R Status   | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x2a      | FAN2 F Status   | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x2b      | FAN2 R Status   | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x2c      | FAN3 F Status   | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x2d      | FAN3 R Status   | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x2e      | FAN4 F Status   | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x2f      | FAN4 R Status   | 0x0       | discrete    | 0x8000| na        | na        |
na        | na      | na        | na        | na    | na
0x30      | PS1 Presence    | 0x0       | discrete    | 0x8002| na        | na        |
na        | na      | na        | na        | na    | na
0x31      | PS2 Presence    | 0x0       | discrete    | 0x8002| na        | na        |
na        | na      | na        | na        | na    | na
0x32      | DIMM000         | 0x0       | discrete    | 0x8040| na        | na        |
```

```
na        | na      | na        | na        | na    | na
0x33      | DIMM001         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x34      | DIMM002         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x35      | DIMM010         | 0x0       | discrete    | 0x8040 | na        | na        |
na        | na      | na        | na        | na    | na
0x36      | DIMM011         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x37      | DIMM012         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x38      | DIMM020         | 0x0       | discrete    | 0x8040 | na        | na        |
na        | na      | na        | na        | na    | na
0x39      | DIMM021         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x3a      | DIMM022         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x3b      | DIMM030         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x3c      | DIMM031         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x3d      | DIMM032         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x3e      | DIMM100         | 0x0       | discrete    | 0x8040 | na        | na        |
na        | na      | na        | na        | na    | na
0x3f      | DIMM101         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x40      | DIMM102         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x41      | DIMM110         | 0x0       | discrete    | 0x8040 | na        | na        |
na        | na      | na        | na        | na    | na
0x42      | DIMM111         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x43      | DIMM112         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x44      | DIMM120         | 0x0       | discrete    | 0x8040 | na        | na        |
na        | na      | na        | na        | na    | na
0x45      | DIMM121         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x46      | DIMM122         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x47      | DIMM130         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x48      | DIMM131         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x49      | DIMM132         | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x4a      | AreaIntrusion   | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na    | na
0x4b      | RTC Battery     | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x4c      | PCIE Status     | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x4d      | ACPI State      | 0x0       | discrete    | 0x8001 | na        | na        |
na        | na      | na        | na        | na    | na
```

```
0x4e      | SysFWProgress    | 0x0       | discrete    | 0x8000 | na        | na
| na        | na      | na        | na        | na    | na
0x4f      | Power Button     | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x50      | SysRestart       | 0x0       | discrete    | 0x8080 | na        | na        |
na        | na      | na        | na        | na    | na
0x51      | Boot Error       | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x52      | Watchdog2        | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x53      | Mngmnt Health    | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x54      | UID Button       | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x55      | PwrOk Sig. Drop  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x56      | PwrOn TimeOut    | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x57      | PwrCap Status    | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x58      | HDD Backplane    | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x59      | HDD BP Status    | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x5a      | Riser1 Card      | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x5b      | Riser2 Card      | 0x0       | discrete    | 0x8002 | na        | na        |
na        | na      | na        | na        | na    | na
0x5c      | SAS Cable        | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x5d      | FAN1 F Presence  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x5e      | FAN1 R Presence  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x5f      | FAN2 F Presence  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x60      | FAN2 R Presence  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x61      | FAN3 F Presence  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x62      | FAN3 R Presence  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x63      | FAN4 F Presence  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x64      | FAN4 R Presence  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x65      | RAID Presence    | 0x0       | discrete    | 0x8002 | na        | na        |
na        | na      | na        | na        | na    | na
0x66      | CPU Usage        | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x67      | Memory Usage     | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x68      | LCD Status       | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na    | na
0x69      | LCD Presence     | 0x0       | discrete    | 0x8001 | na        | na        |
```

```
na        | na      | na        | na        | na     | na
0x6a      | RAID Status     | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x6b      | DISK0           | 0x0       | discrete    | 0x8001 | na        | na        |
na        | na      | na        | na        | na     | na
0x6c      | DISK1           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x6d      | DISK2           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x6e      | DISK3           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x6f      | DISK4           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x70      | DISK5           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x71      | DISK6           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x72      | DISK7           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x73      | DISK8           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x74      | DISK9           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x75      | DISK10          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x76      | DISK11          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x77      | DISK12          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x78      | DISK13          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x79      | DISK14          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x7a      | DISK15          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x7b      | DISK16          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x7c      | DISK17          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x7d      | DISK18          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x7e      | DISK19          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x7f      | DISK20          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x80      | DISK21          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x81      | DISK22          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x82      | DISK23          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x83      | DISK24          | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x84      | DISKA           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
```

```
0x85      | DISKB           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x86      | DISKC           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x87      | DISKD           | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x88      | Eth1 Link Down  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x89      | Eth2 Link Down  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x8a      | Eth3 Link Down  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x8b      | Eth4 Link Down  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x8c      | PS1 Status      | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x8d      | PS1 Fan Status  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x8e      | PS2 Status      | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x8f      | PS2 Fan Status  | 0x0       | discrete    | 0x8000 | na        | na        |
na        | na      | na        | na        | na     | na
0x90      | PCIE SW1 Temp   | na        | degrees C   | na     | na        | na        |
na        | 100.000  | na        | na        | 2.000  | 2.000
0x91      | PCIE SW2 Temp   | na        | degrees C   | na     | na        | na        |
na        | 100.000  | na        | na        | 2.000  | 2.000
0x93      | LOM P1 Link Down | 0x0      | discrete    | 0x8100 | na        | na        |
na        | na      | na        | na        | na     | na
0x94      | LOM P2 Link Down | 0x0      | discrete    | 0x8100 | na        | na        |
na        | na      | na        | na        | na     | na
0x95      | LOM P3 Link Down | 0x0      | discrete    | 0x8100 | na        | na        |
na        | na      | na        | na        | na     | na
0x96      | LOM P4 Link Down | 0x0      | discrete    | 0x8100 | na        | na        |
na        | na      | na        | na        | na     | na
```

Табл. 4-3 Описание полей информации о датчиках

Поле	Значение	Пример	Примечания
sensor name	Sensor name	CPU1 Core Rem: датчик температуры ядра ЦП 1.	–
value	Current value	35.000: значение текущего датчика.	na: текущий датчик не обнаруживает никакой информации, поскольку соответствующее устройство может не присутствовать.
unit	Единица измерения текущего значения	degrees C: значение измеряется в град. Цельсия.	discrete: дискретный датчик без каких-либо единиц измерения.
status	Состояние	ok: датчик	na: текущий датчик не обнаруживает

Поле	Значение	Пример	Примечания
		работает правильно. nc: датчик обнаружил незначительную аварию. cr: датчик обнаружил серьезную аварию. nr: датчик обнаружил критическую аварию.	никакой информации, поскольку соответствующее устройство может не присутствовать. 0x*XXXX*, например 0x8000. Значение определяется в соответствии со стандартами IPMI и для представления состояния текущего датчика используется шестнадцатеричное значение. Подробная информация приведена в поле Generic Offset Табл. 42-2 Generic Event/Reading Type Codes и поле Sensor specific Offset Табл. 42-3 Sensor Type Codes стандартов IPMI.
lnr	Нижнее пороговое значение для критических аварийных сигналов	na	na: текущий датчик не поддерживает пороговое значение.
lc	Нижнее пороговое значение для серьезных аварийных сигналов	na	na: текущий датчик не поддерживает пороговое значение.
lnc	Нижнее пороговое значение для незначительных аварийных сигналов	na	na: текущий датчик не поддерживает пороговое значение.
unc	Верхнее пороговое значение для незначительных аварийных сигналов	84.000: положительное пороговое значение появления незначительного аварийного сигнала текущего датчика составляет 84.	na: текущий датчик не поддерживает пороговое значение.
uc	Верхнее пороговое	88.000: положительное	na: текущий датчик не поддерживает

Поле	Значение	Пример	Примечания
	значение для серьезных аварийных сигналов	пороговое значение появления серьезного аварийного сигнала текущего датчика составляет 88.	пороговое значение.
unr	Верхнее пороговое значение для критических аварийных сигналов	na	na: текущий датчик не поддерживает пороговое значение.
phys	Положительное отставание фаз	3: положительное отставание фаз текущего датчика равно 3.	na: текущий датчик не поддерживает отставание фаз.
nhys	Отрицательное отставание фаз	3: отрицательное отставание фаз текущего датчика равно 3.	na: текущий датчик не поддерживает отставание фаз.

ПРИМЕЧАНИЕ

Представленный выше командный вывод приведен только в качестве примера. Фактические пороговые значения датчиков могут отличаться от представленных.

4.12.2 Команда проверки датчика (sensor -d test)

Функция

Команда **test** используется для моделирования статуса датчика или значения, без генерирования аварийного сигнала.

Формат

ipmcset -t sensor -d test -v <sensorname/stopall> [value/stop]

Параметры

Параметр	Описание	Значение
sensorname/stopall	Имя датчика.	• *sensorname*: имя датчика. • **stopall**: остановка всех проверок.

Параметр	Описание	Значение
value/stop	Аналоговое значение.	• *value*: аналоговое значение проверки датчика. • **stop**: остановка всех проверок.

Инструкции по использованию

–

Пример

Моделирование значения датчика температуры ЦП1 Core Rem 100°C.

```
iBMC:/->ipmcset -t sensor -d test -v "CPU1 Core Rem" 100
Sensor test successfully.
```

4.13 Команды PSU

В данном разделе приведено описание всех команд PSU.

4.13.1 Настрока режима работы PSU (psuworkmode)

Функция

Команда **psuworkmode** используется для запроса рабочего режима PSU.

Формат

ipmcset -d psuworkmode -v <*option*> [*active_psuid*]

Параметры

Параметр	Описание	Значение
option	режим работы PSU.	• **0**: режим распределения нагрузки • **1**: режим активный-резервный
active_psuid	ID активного PSU, когда PSU работает в режиме активный-резервный.	1~2

Инструкции по использованию

–

Пример

Настройка режима работы PSU.

```
iBMC:/->ipmcset -d psuworkmode -v 1 1
Set Power Work Mode (Active Standby) successfully
```

4.13.2 Запрос основной информации PSU (psuinfo)

Функция

Команда **psuinfo** используется для запроса информации PSU.

Формат

ipmcget -d psuinfo

Параметры

–

Инструкции по использованию

–

Пример

Запрос информации PSU.

```
iBMC:/-> ipmcget -d psuinfo
Current PSU Information :
Slot   Manufacturer    Type                      SN                            Version
Rate     InputMode
1     HUAWE          HUAWE 750W PLATINUM PS       N/A                          07
750      AC/DC
2     HUAWE          HUAWE 750W PLATINUM PS       N/A                          07
750      AC/DC

Current PSU WorkMode   :
Actual PSU Status      :
   Work Mode         : Load Balancing
Predicted PSU Status   :
   Work Mode         : Load Balancing
```

4.14 Команды U-Boot

В данном разделе приведено описание списка команд U-Boot, а также порядок доступа к CLI U-Boot.

4.14.1 Вход на U-Boot

Сценарий

Вход на U-Boot iBMC через последовательный порт.

ВНИМАНИЕ

Команды U-Boot используются для загрузки базового ПО и отладки базовых устройств. Только квалифицированный персонал может использовать команды U-Boot.

Предварительные условия

- Имя пользователя и пароль для входа в iBMC

  По умолчанию установлено имя пользователя **root** для серверов V3 и **Administrator** для серверов V5, а в табличке с маркировкой продукта указан пароль по умолчанию.
- Пароль для входа в U-boot iBMC.

  Для серверов V3 установлен пароль по умолчанию **Huawei12#$**, а для серверов V5 пароль по умолчанию **Admin@9000**.

ВНИМАНИЕ

В целях безопасности после первого входа рекомендуется изменить исходный пароль и периодически менять пароль в дальнейшем.

Процедура

Шаг 1 Выполните вход в интерфейс командной строки iBMC через последовательный порт.

ПРИМЕЧАНИЕ

Через последовательный порт одновременно войти в систему может максимум пять пользователей.

Шаг 2 Перезапуск iBMC.

```
iBMC:/->ipmcset -d reset
This operation will reboot iBMC system. Continue? [Y/N]:
```

Шаг 3 Введите **Y** и нажмите **Enter**.

После этого будет выполнен перезапуск iBMC.

Шаг 4 Нажмите **Ctrl+B** сразу после того, как система выведет на экран сообщение «`Hit 'ctrl + b' to stop autoboot`».

На экране появится следующая информация:

```
ENTER PASSWD:
```

Шаг 5 Введите пароль для входа в U-Boot. Для серверов V3 установлен пароль по умолчанию **Huawei12#$**, а для серверов V5 пароль по умолчанию **Admin@9000**.

Появится интерфейс командной строки U-Boot.

----Конец

4.14.2 Список команд U-Boot

ПРИМЕЧАНИЕ

Команды U-boot используются только для отладки. Далее представлены команды U-boot. Для получения информации по данным командам обратитесь в компанию Huawei.

В CLI U-boot iBMC введите **?** или **help** и нажмите **Enter**. Справка по всем командам U-boot:

```
Hi1710 UBOOT> help
?      - alias for 'help'
appfs cp- appfs cp  -copy appfs to flash

appfs up- appfs up  -update app file system

base   - print or set address offset
bdinfo  - print Board Info structure
boot   - boot default, i.e., run 'bootcmd'
bootd  - boot default, i.e., run 'bootcmd'
bootm  - boot application image from memory
bootp  - boot image via network using BOOTP/TFTP protocol
cfgfs cp- cfgfs cp  -copy cfgfs to flash

cfgfs up- cfgfs up  -update data file system

cmp    - memory compare
coninfo - print console devices and information
cp     - memory copy
crc32  - checksum calculation
datafs cp- datafs cp  -copy datafs to flash

datafs up- datafs up  -update data file system

ddr test- ddr test <ADDR> <LEN> <ALGO>

dt     - memory test
dts    - just for test
echo   - echo args to console
editenv - edit environment variable
erase  - erase FLASH memory
exit   - exit script
false  - do nothing, unsuccessfully
flinfo  - print FLASH memory information
fsinfo  - print information about filesystems
fsload  - load binary file from a filesystem image
go     - start application at address 'addr'
help   - print command description/usage
hiddr test- use for save ddr auto test ret

iminfo  - print header information for application image
itest  - return true/false on integer compare
loadb  - load binary file over serial line (kermit mode)
loads  - load S-Record file over serial line
loady  - load binary file over serial line (ymodem mode)
loop   - infinite loop on address range
```

```
ls     - list files in a directory (default /)
lswread - read value of lsw register
lswwrite- write value to lsw register
md     - memory display
mm     - memory modify (auto-incrementing address)
mtdparts- define flash/nand partitions
mtest   - simple RAM read/write test
mw     - memory write (fill)
nfs    - boot image via network using NFS protocol
nm     - memory modify (constant address)
passwd  - passwd -   Modify uboot passwd

phyread - read value of phy register
phywrite- write value to phy register
ping   - send ICMP ECHO_REQUEST to network host
printenv- print environment variables
protect - enable or disable FLASH write protection
rarpboot- boot image via network using RARP/TFTP protocol
reboot  - Perform RESET of the CPU
reset   - Perform RESET of the BMC
rootfs_cp- rootfs_cp  -copy rootfs to flash

rootfs_up- rootfs_up  -update root file system

run    - run commands in an environment variable
saveenv - save environment variables to persistent storage
setenv  - set environment variables
sleep   - delay execution for some time
spi test- spi test <data>

test   - minimal test like /bin/sh
tftpboot- boot image via network using TFTP protocol
true   - do nothing, successfully
uboot0 up- uboot up  -update uboot

uboot1 up- uboot up  -update uboot

uboot cp0- uboot cp  -copy uboot to flash

uboot cp1- uboot cp  -copy uboot to flash

version - display u-boot version
Hi1710_UBOOT>
```

4.15 Команды SOL

В данном разделе приведено описание команд SOL (Serial Over LAN).

4.15.1 Создание сеанса SOL (sol -d activate)

Функция

Команда **sol -d activate** используется для установления сеанса связи SOL с последовательным портом системы или последовательным портом iBMC сервера.

Формат

ipmcset -t sol -d activate -v <*option*> <*mode*>

Параметры

Параметр	Описание	Значение
option	Последовательный порт, к которому выполняется подключение.	• **1**: последовтельный порт системы • **2**: последовательный порт iBMC
mode	Режим сеанса SOL.	• **0**: режим совместного доступа Режим совместного доступа позволяет одновременно устанавливать два сеанса связи SOL. Каждый пользователь может просматривать операции, выполняемые другим пользователем. • **1**: частный режим Частный режим позволяет только одному пользователю устанавливать сеанс связи SOL.

Инструкции по использованию

Только iBMC 2.56 и более поздние версии поддерживают данную команду.

Нажмите **Esc** и затем **(** с интервалом менее 1 секунды для выхода из сеанса связи SOL и перехода к интерфейсу командной строки.

Пример

Установка сеанса связи SOL в режиме совместного доступа с последовательным портом системы.

```
iBMC:/->ipmcset -t sol -d activate -v 1 0
[Connect SOL successfully! Use 'Esc(' to exit.]
Warning! The SOL session is in shared mode, the operation can be viewed on another terminal.

sles11sp1:~ #
sles11sp1:~ # Esc( [Close SOL]

SOL connection closed.
```

4.15.2 Деактивация сеанса SOL (sol -d deactivate)

Функция

Команда **sol -d deactivate** используется для принудительной деактивации сеанса SOL.

Формат

ipmcset -t sol -d deactivate -v <*index*>

Параметры

Параметр	Описание	Значение
index	Порядковый номер сеанса SOL.	• **1**: сеанс 1. • **2**: сеанс 2.

Инструкции по использованию

Только iBMC 2.56 и более поздние версии поддерживают данную команду.

Сеанс SOL, установленный с использованием IPMITOOL не может быть отключен.

Пример

Деактивация сеанса SOL 1.

```
iBMC:/->ipmcset -t sol -d deactivate -v 1
Close SOL session successfully.
```

4.15.3 Настройка времени ожидания сеанса SOL (sol -d timeout)

Функция

Команда **sol -d timeout** используется для настройки времени ожидания сеансов SOL. Если в течение определенного периода времени ни будет выполнена ни одна операция, то сеанс SOL будет автоматически разъединен и на экране появится CLI iBMC.

Формат

ipmcset -t sol -d timeout -v <*value*>

Параметры

Параметр	Описание	Значение
value	Максимальное время ожидания (в минутах) после выполнения последней операции сеанса SOL. Если в течение определенного периода времени ни будет выполнена ни одна операция, то сеанс SOL будет автоматически разъединен.	Диапазон значений: от 0 до 480 Значение **0** означает неограниченное время. Значение по умолчанию: **15**

Инструкции по использованию

Только iBMC 2.56 и более поздние версии поддерживают данную команду.

Пример

Установите время ожидания сеанса SOL 20 минут.

```
iBMC:/->ipmcset -t sol -d timeout -v 20
Set SOL timeout period successfully.
```

4.15.4 Запрос списка сеансов SOL (sol -d session)

Функция

Команда **sol -d session** используется для запроса списка сеансов SOL.

Формат

ipmcget -t sol -d session

Параметры

–

Инструкции по использованию

Только iBMC 2.56 и более поздние версии поддерживают данную команду.

Пример

Запрос списка сеансов SOL.

```
iBMC:/->ipmcget -t sol -d session
Index  Type    Mode    LoginTime             IP                   Name
1      CLI     Shared  2017-09-14 11:19:55  172.100.1.40:50013   root
2      N/A     N/A      N/A                   N/A                  N/A
```

4.15.5 Запрос данных конфигурации сеанса SOL (sol -d info)

Функция

Команда **sol -d info** используется для запроса данных конфигурации сеанса SOL, например периода ожидания сеанса SOL.

Формат

ipmcget -t certificate -d info

Параметры

–

Инструкции по использованию

Только iBMC 2.56 и более поздние версии поддерживают данную команду.

Пример

Запрос данных конфигурации сеанса SOL.

```
iBMC:/->ipmcget -t sol -d info
Timeout Period(Min)       :   20
```

5 Общие команды техобслуживания

О данной главе

Общие команды техобслуживания выполняются на интерфейсе CLP. На CLI iBMC выполните команду **clp_commands** для переключения на интерфейс CLP.

5.1 Просмотр справочной информации (help)

Функция

Команда **help** используется для просмотра справочной информации.

Формат

help

[*command*] **--help**

Параметры

Параметр	Описание	Значение
command	Команда должна быть запрошена.	–

Инструкции по использованию

–

Пример

Просмотр команд, поддерживаемых в текущем пути.

```
iBMC:/->help
Commands:
help     :      Used to get context sensitive help.
exit     :      Used to terminate the CLP session.
ipmcget   :      Used to get BMC runtime status.
ipmcset   :      Used to set BMC runtime status or send control command.
notimeout :      Used to set no timeout limit to login shell.
maint_debug_cli : Used to maintance in debug mode.
ping     :      Used to test IPv4 network status.
ping6    :      Used to test IPv6 network status.
ifconfig  :      Used to check network device information.
ps       :      Used to check processes status.
free     :      Used to check memory status.
top      :      Used to check system resource used information. None parameter is
allowed
df       :      Used to check disk used information.
route    :      Used to check route information. None parameter is allowed
netstat   :      Used to check network port status.
```

ПРИМЕЧАНИЕ

Команда **maint_debug_cli** в основном используется для обнаружения неисправностей на объектах связи и, в основном, используется только администраторами и операторами. Подробная информация о порядке использования данной команды приведена в документе *Справочник по расширенным командам iBMC сервера Huawei*.

Просмотр способа использования команды **ping**.

```
iBMC:/->ping --help
BusyBox v1.18.4 (2014-08-09 16:28:25 CST) multi-call binary.

Usage: ping [OPTIONS] HOST

Send ICMP ECHO REQUEST packets to network hosts

Options:
    -4,-6        Force IP or IPv6 name resolution
    -c CNT       Send only CNT pings
    -s SIZE      Send SIZE data bytes in packets (default:56)
    -I IFACE/IP  Use interface or IP address as source
    -W SEC       Seconds to wait for the first response (default:10)
             (after all -c CNT packets are sent)
    -w SEC       Seconds until ping exits (default:infinite)
```

```
            (can exit earlier with -c CNT)
   -q       Quiet, only displays output at start
            and when finished
```

5.2 Разъединение клиента от iBMC (exit)

Функция

Команда **exit** используется для разъединения клиента от iBMC.

Формат

exit

Параметры

–

Инструкции по использованию

–

Пример

Разъединение клиента от iBMC.

```
iBMC:/->exit

Connection closed by foreign host.
```

5.3 Проверка сетевого соединения (ping, ping6)

Функция

Команда **ping** или **ping6** используется для проверки сетевого соединения.

Формат

ping <*IPv4 Address*>

ping6 <*IPv6 Address*>

Параметры

Параметр	Описание	Значение
IPv4-адрес	Целевой IPv4-адрес	–

Параметр	Описание	Значение
IPv6-адрес	Целевой IPv6-адрес	–

Инструкции по использованию

Подробная информация приведена в руководстве пользователя команд **ping** или **ping6** для ОС Linux.

Пример

Проверка соединения между текущим устройством и целевым устройством при помощи IP-адреса.

```
iBMC:/->ping 192.168.44.178
PING 192.168.44.178 (192.168.44.178) 56(84) bytes of data.
64 bytes from 192.168.44.178: icmp req=1 ttl=64 time=8.19 ms
64 bytes from 192.168.44.178: icmp req=2 ttl=64 time=0.398 ms
64 bytes from 192.168.44.178: icmp req=3 ttl=64 time=0.263 ms
64 bytes from 192.168.44.178: icmp req=4 ttl=64 time=0.285 ms
64 bytes from 192.168.44.178: icmp req=5 ttl=64 time=0.418 ms

iBMC:/->ping6 2014::39ad:9345:1a6e:d0e1
PING 2014::39ad:9345:1a6e:d0e1(2014::39ad:9345:1a6e:d0e1) 56 data bytes
64 bytes from 2014::39ad:9345:1a6e:d0e1: icmp seq=1 ttl=64 time=0.821 ms
64 bytes from 2014::39ad:9345:1a6e:d0e1: icmp seq=2 ttl=64 time=0.840 ms
64 bytes from 2014::39ad:9345:1a6e:d0e1: icmp seq=3 ttl=64 time=0.843 ms
64 bytes from 2014::39ad:9345:1a6e:d0e1: icmp seq=4 ttl=64 time=0.744 ms
64 bytes from 2014::39ad:9345:1a6e:d0e1: icmp seq=5 ttl=64 time=0.774 ms
64 bytes from 2014::39ad:9345:1a6e:d0e1: icmp seq=6 ttl=64 time=1.02 ms
```

5.4 Выполнение команды free (free)

Функция

Команда **free** используется для запуска команды **free** в ОС Linux.

Формат

Для получения подробной информации обратитесь к синтаксису команды **free** в ОС Linux.

Параметры

Данная команда поддерживает все параметры для команды **free**.

Инструкции по использованию

–

Пример

```
iBMC:/->free
             total        used        free      shared     buffers
  Mem:      125572       94780       30792           0       14780
 Swap:          0           0           0
Total:      125572       94780       30792
```

5.5 Выполнение команды ps (ps)

Функция

Команда **ps** используется для запуска команды **ps** в ОС Linux.

Формат

Для получения подробной информации обратитесь к синтаксису команды **ps** в ОС Linux.

Параметры

Данная команда поддерживает все параметры для команды **ps**.

Инструкции по использованию

–

Пример

```
iBMC:/->ps
  PID USER      VSZ STAT COMMAND
    1 root     1980 S    init [3]
    2 root        0 SW<  [kthreadd]
    3 root        0 SW<  [ksoftirqd/0]
    4 root        0 SW<  [events/0]
    5 root        0 SW<  [khelper]
   64 root        0 SW<  [kblockd/0]
  103 root        0 SW   [pdflush]
  104 root        0 SW   [pdflush]
  105 root        0 SW<  [kswapd0]
  106 root        0 SW<  [aio/0]
  107 root        0 SW<  [nfsiod]
  227 root        0 SW<  [mtdblockd]
  255 root        0 SW<  [spi-dma-wq]
  256 root        0 SW<  []
  270 root        0 SW<  [rpciod/0]
  279 root        0 SWN  [jffs2 gcd mtd5]
  333 root        0 SW<  [hw wdt gpio]
  344 root    53760 S    /ipmc/fsync
  362 root     4460 S    /ipmc/uusync
  363 root      418m S    /ipmc/bmcipmi.out
  379 root    21488 S    /usr/sfcb/sbin/sfcbd -d
```

```
 381 root     5104 S   /usr/sfcb/sbin/sfcbd -d
 387 root    13296 S   /usr/sfcb/sbin/sfcbd -d
 389 root    21800 S   /usr/sfcb/sbin/sfcbd -d
 400 root    67004 S   /web/linux/webs
 403 root    13348 S   /usr/sfcb/sbin/sfcbd -d
 404 root    13336 S   /usr/sfcb/sbin/sfcbd -d
 412 root    78204 S   /vmm/vmm
 432 root     104m S   /kvm/kvm
 434 root    47456 S   /kvm/video
 443 root     4136 S   /ipmc/nsupdate
 458 root    13388 S   /usr/sfcb/sbin/sfcbd -d
 465 root     2576 S   /bin/sh /usr/script/monitor
 476 root     1644 S   syslogd -m 0
 484 root     1564 S   klogd -x
 502 root     3252 S   crond
 543 root    70700 S   /ipmc/cooling
 640 root     2960 S   /usr/sbin/xinetd -reuse
 945 root    14988 S   -hwsmash
1014 root    61096 S   /usr/net-snmp/sbin/snmpd -Ln -f
1902 root     9472 S   sshd: root@pts/0
1918 root    14988 S   -hwsmash
2048 root     9472 R   sshd: root@pts/1
2064 root    14992 S   -hwsmash
3345 root     2444 S   sleep 60
3346 root     2900 R   /bin/ps
```

5.6 Выполнение команды Netstat (netstat)

Функция

Команда **netstat** используется для запуска команды **netstat** в ОС Linux.

Формат

Для получения подробной информации обратитесь к синтаксису команды **netstat** в ОС Linux.

Параметры

Данная команда поддерживает все параметры для команды **netstat**.

Инструкции по использованию

–

Пример

```
iBMC:/->netstat -t
 Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp       0    116 192.168.64.110:ssh     192.168.29.200:65069   ESTABLISHED
tcp       0      0 192.168.64.110:ssh     192.168.29.200:65068   ESTABLISHED
```

5.7 Выполнение команды df (df)

Функция

Команда **df** используется для запуска команды **df** в ОС Linux.

Формат

Для получения подробной информации обратитесь к синтаксису команды **df** в ОС Linux.

Параметры

Данная команда поддерживает все параметры для команды **df**.

Инструкции по использованию

–

Пример

```
iBMC:/->df
Filesystem         1k-blocks     Used Available Use% Mounted on
rootfs                50580    50580        0 100% /
/dev/root             50580    50580        0 100% /
/dev/mtdblock5        15872     1308    14564   8% /data
tmpfs                 62784      292    62492   0% /dev/shm
tmpfs                 62784      292    62492   0% /dev/shm
tmpfs                 49152      160    48992   0% /tmp
tmpfs                  4096       12     4084   0% /ipmc/usr
```

5.8 Выполнение команды ifconfig (ifconfig)

Функция

Команда **ifconfig** используется для запуска команды **ifconfig** в ОС Linux.

Формат

Для получения подробной информации обратитесь к синтаксису команды **ifconfig** в ОС Linux.

Параметры

Данная команда поддерживает только параметры **lo**, **eth***n* (*n* – номер индекса сетевого порта), или **-a** или параметра **no**.

Инструкции по использованию

–

Пример

```
iBMC:/->ifconfig eth1
eth1     Link encap:Ethernet  HWaddr 00:18:82:11:03:21
         inet6 addr: fe80::218:82ff:fe11:321/64 Scope:Link
         UP BROADCAST DEBUG RUNNING  MTU:1500  Metric:1
         RX packets:28 errors:0 dropped:0 overruns:0 frame:0
         TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:1832 (1.7 KiB)  TX bytes:2558 (2.4 KiB)
         Interrupt:28
```

5.9 Выполнение команды route (route)

Функция

Команда **route** используется для запуска команды **route** в ОС Linux.

Формат

Для получения подробной информации обратитесь к синтаксису команды **route** в ОС Linux.

Параметры

-n: использование IP-адреса или номер порта, вместо протокола связи или имени хоста.

-e: отображение дополнительной информации.

-A inet{6}: выбор семейства адресов.

Инструкции по использованию

–

Пример

```
iBMC:/->route --help
Usage: route [option]

Check kernel routing tables

Options:
    -n              Don't resolve names
    -e              Display other/more information
    -A inet{6}       Select address family
```

5.10 Выполнение команды top (top)

Функция

Команда **top** используется для запуска команды **top** в ОС Linux.

Формат

Для получения подробной информации обратитесь к синтаксису команды **top** в ОС Linux.

Параметры

Данная команда не поддерживает никакие параметры.

Инструкции по использованию

–

Пример

```
iBMC:/->top
top - 16:26:41 up 3 days, 15:48,  3 users,  load average: 0.09, 0.08, 0.08
Tasks:  46 total,   1 running,  45 sleeping,   0 stopped,   0 zombie
Cpu(s):  2.2%us,  3.4%sy,  0.0%ni, 94.3%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:    125572k total,    94920k used,    30652k free,    14780k buffers
Swap:       0k total,       0k used,       0k free,    35916k cached

 PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
1133 root      20   0  2408  968  784 R  3.7  0.8   0:00.09 top
   1 root      20   0  1980  652  572 S  0.0  0.5   0:01.95 init
   2 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kthreadd
   3 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
   4 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 events/0
   5 root      15  -5     0    0    0 S  0.0  0.0   0:03.81 khelper
  64 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kblockd/0
 103 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
 104 root      20   0     0    0    0 S  0.0  0.0   0:13.65 pdflush
```

5.11 Отключение функции времени ожидания CLP (notimeout)

Функция

Команда **notimeout** используется для отключения функции времени ожидания CLP.

Формат

notimeout

Параметры

–

Инструкции по использованию

–

Пример

Отключение функции времени ожидания CLP.

```
iBMC:/->notimeout
iBMC:/->
```

6 Стандартные операции

О данной главе

Данный раздел описывает как выполнять общие операции для iBMC.

6.1 Вход в систему сервера через последовательный порт с помощью PuTTY

Сценарий

Вход на сервер через последовательный порт с использованием PuTTY осуществляется в следующих сценариях:

- Сервер сконфигурирован впервые на новом сайте, и необходимо выполнить первоначальную настройку.
- Сервер не может быть подключен удаленно, так как в сети имеется неисправность и сначала необходимо определить данную неисправность.

Предварительные условия

Условия

- ПК подключен к серверу через последовательный кабель.
- Установлен PuTTY версии 0.60 или более поздней версии.

Данные

Необходимо подготовить следующие данные:

- Имя пользователя для входа на сервер.
- Пароль пользователя для входа на сервер.

Программное обеспечение

PuTTy.exe это бесплатная программа. Найти ее можно самостоятельно. Версия PuTTY для входа в систему сервера должна быть 0.60 или выше.

Процедура

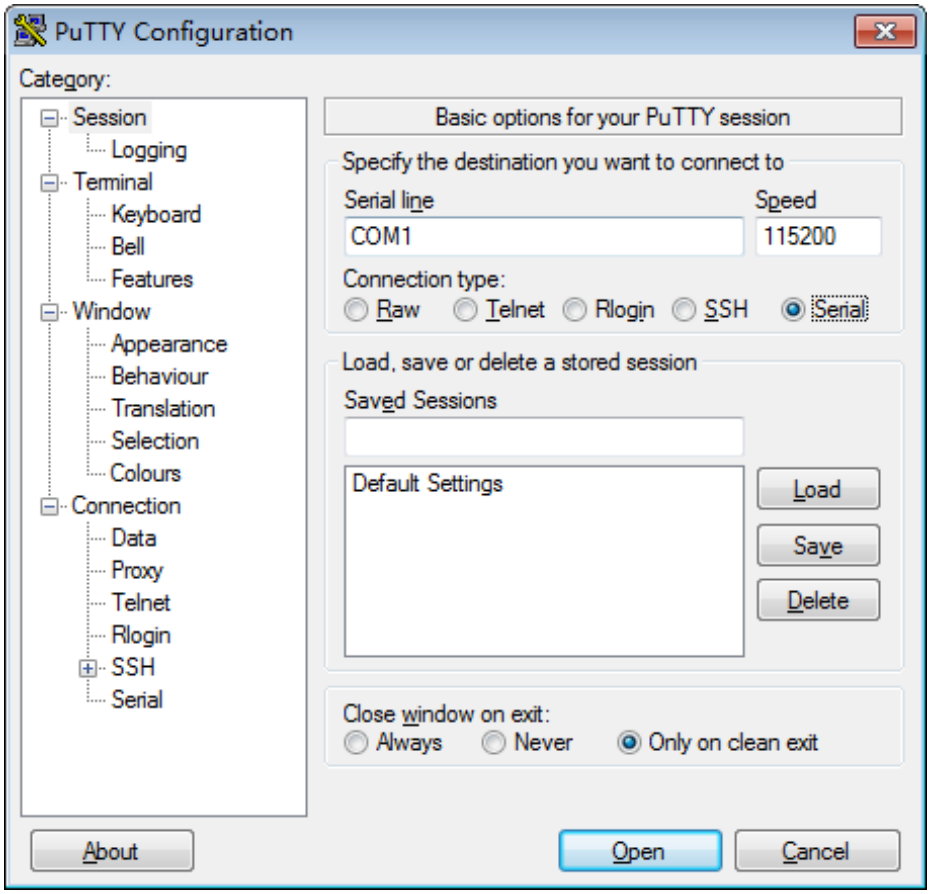
1. Дважды щелкните кнопкой мыши **PuTTY.exe**.

   На экране появится окно **PuTTY Configuration**.
2. В дереве навигации выберите **Connection** > **Serial**.
3. Настройте параметры входа.

   Далее приведен пример настройки параметров:
   - Serial Line to connect to: COM*n*
   - Speed (baud): 115200
   - Data bits: 8
   - Stop bits: 1
   - Parity: –
   - Flow control: –

   n – это номер последовательного порта, значение которого должно быть целым числом.
4. В дереве навигации выберите **Session**.
5. Выберите **Connection type** в **Serial**, как показано на Рис. 6-1.

Рис. 6-1 Окно **PuTTY Configuration**



6. Нажмите **Open**.

   На экране появятся окна **PuTTY** и **login as:**, в которых необходимо ввести имя пользователя.

7. Введите имя пользователя и пароль, следуя инструкциям.

   После успешного входа имя хоста сервера будет отображаться слева в строке приглашения.

----Конец

6.2 Вход в систему сервера через сетевой порт с помощью PuTTY

Сценарий

Для дистанционного входа на сервер по локальной сети (LAN), а также для конфигурирования и обслуживания сервера используется PuTTY.

Предварительные условия

Условия

Компьютер нормально подключен к порту сети управления на сервере с помощью сетевого кабеля.

Данные

Необходимо подготовить следующие данные:

- IP-адрес сервера, к которому будет выполняться подключение.
- Имя пользователя и пароль для входа на сервер.

Программное обеспечение

PuTTy.exe это бесплатная сторонняя программа. Найти ее можно самостоятельно.

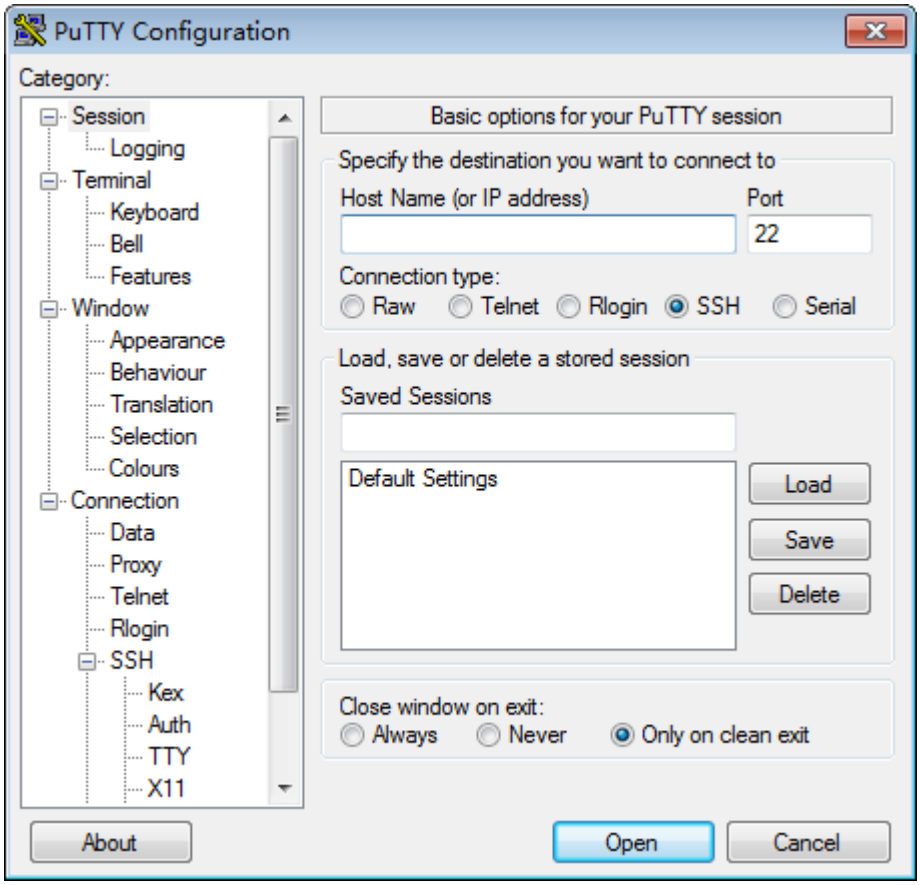
Процедура

1. Настройте IP-адрес и маску подсети или добавьте информацию о маршруте для связи ПК с сервером.

   Для проверки связи между ПК и сервером выполните команду **Ping *Server IP address*** в CLI ПК.
2. Дважды щелкните кнопкой мыши **PuTTY.exe**.

   На экране появится окно **PuTTY Configuration**, показанное на Рис. 6-2.

Рис. 6-2 Окно **PuTTY Configuration**



3. Настройте параметры входа.

   Описание параметров:

   - Host Name (или IP address): IP-адрес сервера, к которому будет выполняться подключение. Например, **191.100.34.32**.
   - Port: рекомендуется использовать значение по умолчанию **22.**
   - Connection type: рекомендуется использовать значение по умолчанию **SSH.**
   - Close window on exit: рекомендуется использовать значение по умолчанию **Only on clean exit**.

ПРИМЕЧАНИЕ

Установите значение параметров **Host Name** и **Saved Sessions** и нажмите **Save**. При следующем входе на сервер дважды щелкните кнопкой мыши по сохраненным настройкам в разделе **Saved Sessions**.

4. Нажмите **Open.**

   На экране появятся окна **PuTTY** и **login as:**, в которых необходимо ввести имя пользователя.

ПРИМЕЧАНИЕ

- При первом входе на целевой сервер на экране появится окно **PuTTY Security Alert**. Если данный сайт является доверенным, то нажмите **Yes**. На экране появится окно **PuTTY.**
- Если во время входа на сервер было введено неправильное имя пользователя, PuTTY необходимо будет подключить снова.

5. Введите имя пользователя и пароль, следуя инструкциям.

   После успешного входа имя хоста сервера будет отображаться слева в строке приглашения.

----Конец

6.3 Возврат к настройкам по умолчанию iBMC

Сценарий

Возврат к настройкам по умолчанию iBMC применяется при повреждении конфигурационных данных iBMC или при невозможности запустить или подключиться к iBMC.

Для возврата к настройкам по умолчанию iBMC можно воспользоваться командами U-Boot или перемычкой.

ВНИМАНИЕ

- Данную операцию могут выполнять только инженеры технической поддержки Huawei или сертифицированные специалисты.
- Возврат настроек iBMC по умолчанию выполняется только на объекте.
- Данные всех пользователей, включая имена пользователей, пароли и IP-адреса, будут утеряны и произойдет возврат к настройкам по умолчанию. Выполнять данную операцию надо с осторожностью.

Возврат настроек по умолчанию iBMC можно осуществить командами U-Boot или перемычкой. В Табл. 6-1 перечислены модели продуктов и поддерживаемые способы восстановления.

ПРИМЕЧАНИЕ

Для восстановления настроек iBMC по умолчанию на iBMC можно воспользоваться следующими методами:

- Если вы можете войти в U-boot через последовательный порт, используйте команды U-boot для восстановления настроек iBMC по умолчанию.
- Если нет возможности подключиться к U-Boot и iBMC, используйте перемычку для восстановления настроек iBMC по умолчанию.

Табл. 6-1 Модели продуктов и поддерживаемые методы восстановления.

Категория	Модель продукта	U-Boot	Джампер
Стоечные серверы	RH1288A V2	Поддерживается	Поддерживается
	RH2288A V2	Поддерживается	Поддерживается
	RH1288 V3	Поддерживается	Поддерживается
	RH2288 V3	Поддерживается	Поддерживается

Категория	Модель продукта	U-Boot	Джампер
	RH2288H V3	Поддерживается	Поддерживается
	RH5885 V3	Поддерживается	–
	RH5885H V3	Поддерживается	–
	5288 V3	Поддерживается	Поддерживается
	RH8100 V3	Поддерживается	–
Компоненты блейд-серверов	CH121 V3	Поддерживается	Поддерживается
	CH220 V3	Поддерживается	–
	CH140 V3	–	Поддерживается
	CH242 V3 DDR4	Поддерживается	Поддерживается
	CH226 V3	–	Поддерживается
	CH225 V3	Поддерживается	Поддерживается
	CX710	Поддерживается	Поддерживается
	CX220	Поддерживается	–
	CH121 V5	Поддерживается	Поддерживается
Серверные узлы высокой плотности	HMM	Поддерживается	Поддерживается
	XH310 V3	Поддерживается	Поддерживается
	XH628 V3	Поддерживается	Поддерживается
	XH622 V3	Поддерживается	Поддерживается
	XH620 V3	Поддерживается	Поддерживается

Процедура

- Для восстановления настроек по умолчанию iBMC с помощью команд U-Boot выполните следующие шаги:
  а. Выполните вход в систему сервера с помощью PuTTY.

     Подробная информация приведена в разделе 6.1 Вход в систему сервера через последовательный порт с помощью PuTTY.

  б. Чтобы перезагрузить iBMC, нажмите и удерживайте кнопку UID на сервере в течение 6 секунд.

  в. Когда появится сообщение «Hit 'ctrl + b' to stop autoboot: 1», нажмите **Ctrl** + **B**.

  г. Введите пароль U-Boot по умолчанию.

     Для серверов V3 установлен пароль U-Boot по умолчанию **Huawei12#$**, а для серверов V5 – **Admin@9000**.

     Если появится надпись «u-boot>», вы успешно вошли в U-Boot.

  д. Выполните следующую команду для запроса версии U-Boot:

printenv ver

е. Восстановите datafs.

- Если версия U-Boot – 1.1.37 или ниже, выполните следующие команды:

  fsload /usr/upgrade/datafs.jffs2

  datafs_cp

- Если версия U-Boot выше, чем 1.1.37, выполните следующие команды:

  datafs_reset

ж. Выполните следующую команду для перезапуска iBMC:

reset

Процесс перезагрузки длится около 3 минут. После перезагрузки, на iBMC будут восстановлены настройки по умолчанию.

- Для восстановления настроек по умолчанию iBMC с помощью перемычки выполните следующие шаги:

а. Резервное копирование данных.

ВНИМАНИЕ

Выполните резервирование данных перед восстановлением настроек iBMC по умолчанию.

б. Найдите перемычку.

ID перемычки зависит от используемой модели сервера. В Табл. 6-2 предоставлена информация о джамперах основных серверов Huawei. Более подробная информация о местоположении джампера на материнской плате приведена в описании материнской платы в руководстве пользователя сервера.

Табл. 6-2 Названия перемычек и их местоположение

Категория	Модель продукта	ID джампера	Название джампера
Стоечные серверы	RH2288A V2	J117	CLR_BMC_PW
	RH1288A V2	J117	CLR_BMC_PW
	RH1288 V3	J36	CLR_BMC_PW
	RH2288 V3	J36	CLR_BMC_PW
	RH2288H V3	J36	CLR_BMC_PW
	5288 V3	J36	CLR_BMC_PW
	1288H V5	J176	BMC_RCV
	2288H V5	J176	BMC_RCV
Компоненты блейд-серверов	CH121 V3	J19	JTAG SW
	CH140 V3	J19	JTAG SW

Категория	Модель продукта	ID джампера	Название джампера
	CH242 V3 DDR4	J2	SYS_RST
	CH226 V3	J19	JTAG SW
	CH225 V3	J19	JTAG CLR_PSW
	CH121 V5	J76	CLR_BMC_PW
	CH242 V5	J76	CLR_BMC_PW
Серверные узлы высокой плотности	HMM	J17	CLR_MM_PW
	XH628 V3	J36	CLR_BMC_PW
	XH622 V3	J36	CLR_BMC_PW
	XH620 V3	J36	CLR_BMC_PW
	XH310 V3	J36	CLR_BMC_PW

в. Замыкание джампера выполняется при помощи колпачка или специальным инструментом.

г. Чтобы перезагрузить iBMC, нажмите и удерживайте кнопку UID на сервере в течение 6 секунд при замкнутом джампере.

Процесс перезагрузки длится около 3 минут. После перезагрузки, на iBMC будут восстановлены настройки по умолчанию.

----Конец

6.4 Конфигурирование функции перехвата на веб-интерфейсе iBMC

Сценарий действий

На странице **Alarm Settings** веб-интерфейса iBMC можно сконфигурировать функцию перехвата, чтобы получить возможность в iBMC использовать trap-пакеты для передачи аварийной информации, информации о событиях и свойств перехвата на сторонние сервера.

ПРИМЕЧАНИЕ

Данные перехвата это информация, которую система сама отправляет на сторонний сервер, не ожидая каких-либо запросов. Trap-информация включает события, критические, серьезные и незначительные аварийные сигналы.

Предварительные условия

Данные

Получите следующие данные:

- Версия SNMP trap
- Идентификатор, используемый для определения сервера-источника перехвата в передаваемых trap-сообщениях (**Board Serial Number**, **Product Asset Tag** и **Host Name**)
- Название сообщества, используемого протоколом SNMP trap
- Адрес сервера, который получает аварийные сигналы, отправленные в trap-сообщениях.

Процедура

Шаг 1 Выполните вход в веб-интерфейс iBMC. Подробная информация приведена в разделе 3.1 Вход в WebUI iBMC.

Шаг 2 Выберите **Alarm & SEL** > **Alarm Settings**.

Шаг 3 В поле **Alarm Trap Notification Settings**, нажмите 

для включения функции перехвата.

Если 

поменяется на 

, то функция перехвата включена.

Шаг 4 Настройте свойства перехвата.

1. Установите для **Trap Version** версию протокола SNMP trap для передачи информации о событиях.

   Возможные варианты для **Trap Version** : **SNMPv1** (SNMP Trap v1), **SNMPv2c** (SNMP Trap v2c) и **SNMPv3** (SNMP Trap v3).

   Значение по умолчанию: **SNMPv1**

   ПРИМЕЧАНИЕ

   Из-за наличия собственного механизма, протоколы SNMPv1 и SNMPv2c могут создавать риски для системы безопасности. По возможности, старайтесь избегать их. Рекомендуется использовать версию SNMPv3 trap.

2. В выпадающем списке **Choose Trap SNMPv3 User** выберите пользователя iBMC для SNMP Trap v3. Имя пользователя для trap-протокола версии V3 установлено по умолчанию **root**, а для серверов V5 – **Administrator** (дополнительно).
3. Для определения режима перехвата при передаче информации, настройте параметр **Trap Mode**.
   - **Precise Alarm (recommended)**: OID узла SNMP, который находится во взаимно-однозначном соответствии с событием, и используется как ID события перехвата. По сравнению с **OID** и **Event Code**, данный режим предоставляет более точную информацию.
   - **OID**: OID узла SNMP, используемый в качестве ID события перехвата.
   - **Event Code**: Код события, используемый в качестве ID события перехвата.
4. Для **Trap Server Identity** установите идентификатор, используемый для определения сервера-источника перехвата в передаваемых trap-сообщениях.

   Возможные варианты для **Trap Server Identity : Board Serial Number**, **Product Asset Tag** и **Host Name**.

5. В текстовом окне **Community Name**, введите название сообщества, используемого протоколом SNMP trap (дополнительно).

   Только когда **Trap Version** имеет значение **SNMPv1** или **SNMPv2c**, необходимо указывать **Community Name**.

   Название сообщества служит паролем аутентификации, используемым в SNMP Trap v1 и SNMP Trap v2c.

6. В текстовом окне **Confirm Community Name**, введите название сообщества еще раз (дополнительно).

Шаг 5 Установите **Include Alarm Severities**.

Шаг 6 Настройте сервер перехвата и формат пакетов.

1. В поле **Trap Server and Message Format** выберите канал передачи аварийных сообщений.

   Система поддерживает установку максимум четырех каналов передачи аварийных сообщений.

2. Нажмите  , чтобы вывести поле редактирования канала.

1. Нажмите  для включения канала передачи аварийных сообщений.

   Если  поменяется на  , канал передачи аварийных сообщений включен.

2. В текстовом окне **Trap Server Address**, введите адрес сервера для приема аварийных сообщений, отправленных функцией перехвата.

   В качестве адреса сервера может быть указан IPv4- или IPv6-адрес.

3. В текстовом окне **Trap Server Address**, введите адрес сервера для приема аварийных сообщений, отправленных функцией перехвата.

   Значение по умолчанию – **162**.

4. В правой части **Packet Delimiter**, выберите разделитель для разграничения основных полей trap-пакета.

1. В правой части **Select Packet Content**, выберите ключевые слова в передаваемых сообщениях.

2. Выберите или отмените выбор пункта **Display Keyword in Packet**, чтобы определить, должны ли содержаться указанные ключевые слова в trap-пакете.

3. Нажмите **Save**.

   Если появится сообщение **Operation successful**, функция перехвата и настройки этой функции вступили в силу.

4. Нажмите **Test**, чтобы проверить канал.

   Если на экране появится сообщение **Operation successful**, канал доступен.

----Конец

6.5 Конфигурирование функции SMTP на веб-интерфейсе iBMC

Сценарий действий

На странице **Alarm Setting** веб-интерфейса iBMC можно сконфигурировать функцию SMTP (Simple Mail Transfer Protocol / Простой протокол пересылки почты), чтобы iBMC мог передавать аварийные сообщения и события на указанный почтовый ящик через SMTP-сервер.

Предварительные условия

Данные

Получите следующие данные:

- Адрес SMTP-сервера
- Информация отправителя:
  - Имя пользователя и пароль отправителя
  - Адрес эл.почты отправителя
  - Тема сообщения
- Информация получателя:
  - Адрес эл.почты получателя
  - Описание адреса эл.почты получателя

Процедура

Шаг 1 Выполните вход в веб-интерфейс iBMC. Подробная информация приведена в разделе 3.1 Вход в WebUI iBMC.

Шаг 2 Выберите **Alarm & SEL** > **Alarm Setting**.

Шаг 3 В поле **Alarm Trap Notification Settings**, нажмите 

для включения функции SMTP.

Если 

поменяется на 

, функция SMTP включена.

Шаг 4 В текстовом окне **SMTP Server Address**, введите адрес SMTP-сервера.

В качестве адреса сервера может быть указан IPv4- или IPv6-адрес.

Шаг 5 Установите **Allows TLS Enabled**, чтобы включить или отключить функцию TLS (Transport Layer Security/ Безопасность транспортного уровня).

- **Yes:** включение функции TLS. Данные передаются в зашифрованном виде.
- **No**: выключение функции TLS. Данные передаются в незашифрованном виде.

ПРИМЕЧАНИЕ

- По умолчанию SMTP поддерживает TLS. Рекомендуется включить функцию TLS для обеспечения безопасности.
- После включения функции TLS на веб-интерфейсе iBMC, необходимо настроить функцию TLS и аутентификацию на SMTP-сервере так, чтобы SMTP-сервер мог получать почтовые сообщения от iBMC.

Шаг 6 Установите **Allows Anonymous Login**.

- **Allows Anonymous Login** определяет, поддерживает ли SMTP-сервер аутентификацию без указании имени пользователя. Значение **Yes** означает, что при передаче аварийных сообщений с помощью SMTP-сервера указывать имя пользователя и пароль не требуется. Функция anonymous authentication требует поддержки анонимной регистрации на SMTP-сервере.
- Значение **No** означает отказ в анонимной аутентификации. Если вы выбрали опциональную кнопку **No**, надо будет обязательно вводить имя пользователя и пароль, зарегистрированный на SMTP-сервере. Каждый раз при передаче iBMC аварийных сообщений на SMTP-сервер, для аутентификации требуется вводить имя пользователя и пароль.

ПРИМЕЧАНИЕ

По умолчанию на SMTP-сервере не разрешена анонимная аутентификация. В целях безопасности рекомендуется для **Allows Anonymous Login** устанавливать **No**.

Шаг 7 Настройка информации эл.почты

1. Введите значения в полях **Sender's User Name** и **Sender's Password**.

ПРИМЕЧАНИЕ

- Если для **Allows Anonymous Login** выбрано **Yes**, указывать **Sender's User Name** и **Sender's Password** не надо.
- Если пароль на SMTP сервере был изменен, необходимо открыть страницу **Alarm Setting** и ввести новый пароль в текстовое поле **Sender's Password**.

2. Укажите **Sender's Address**.
3. Укажите **Email Subject**.

   Для определения содержания прикрепляемой информации в теме почтового сообщения можно выбрать **Host Name**, **Board serial number** и **Product asset tag**.

Шаг 8 Установите **Select Alarm Severities**.

iBMC может передавать аварии пяти уровней серьезности: **All**, **Critical**, **Major**, **Minor** и **Normal**

После того, как вы выбрали уровень серьезности аварии, iBMC будет передавать аварийные сигналы и события определенного уровня серьезности по указанному адресу почты (если они определены) через SMTP-сервер.

ПРИМЕЧАНИЕ

Далее приведено описание указанных вариантов:

- **All**: означает, что передаются события, незначительные, серьезные и критические аварийные сигналы.
- **Critical**: означает, что передаются только критические аварийные сигналы.
- **Major**: означает, что передаются только серьезные аварийные сигналы.
- **Minor**: означает, что передаются только незначительные аварийные сигналы.
- **Normal**: означает, что передаются только события.

Шаг 9 Установите адрес эл.почты для приема аварийных сообщений.

Нажмите 

. Если 

поменяется на 

, то адрес активирован.

1. Введите адрес эл.почты для приема аварийных сообщений.
2. Введите описание адреса эл.почты для приема аварийных сообщений.

Шаг 10 Нажмите **Save**.

После сохранения конфигурации, для проверки адреса эл.почты можно нажать **Test.** Если появится сообщение **Operation successful**, функция SMTP и настройки этой функции вступили в силу.

Шаг 11 Нажмите **Test**, чтобы проверить адреса электронной почты.

Если появится сообщение **Operation succeeded**, тестовое сообщение было отправлено на соответствующий почтовый ящик. Для проверки необходимо убедиться, что сообщение дошло до адресата.

----Конец

6.6 Конфигурирование функции LDAP

Сценарий

Включение и конфигурирование функции LDAP (Lightweight Directory Access Protocol/ Облегченный протокол доступа к каталогам) на веб-интерфейсе iBMC. Функция LDAP позволяет пользователям домена получить доступ к iBMC.

ПРИМЕЧАНИЕ

- LDAP это универсальное решение аутентификации, которое позволяет быстро реагировать на запросы пользователя.
- Для получения более подробной информации о порядке создания контроллера домена, домена пользователей и пользователей LDAP, обратитесь к документации контроллера домена. iBMC разрешает доступ только пользователям LDAP.

Предварительные условия

Данные

До начала конфигурирования получите следующую информацию:

- Информация о доступных серверах LDAP
  - Адрес сервера LDAP
  - Название домена сервера LDAP
  - Название хоста сервера LDAP
  - Папка пользователей приложения сервера LDAP
- Пароль для входа в WebUI iBMC
- Название группы LDAP, к которой принадлежит пользователь LDAP.

Процедура

Конфигурирование сервера LDAP

iBMC поддерживает взаимодействие с активным Windows-каталогом (AD) и Linux OpenLDAP. Далее в качестве примера конфигурирования сервера LDAP используется вариант с Windows Server 2008. Если сервер LDAP доступен, можно пропустить этот шаг.

1. Установите Windows Server 2008 на сервер.

2. Выберите **Start** > **Computer** > **Manage**.

   Откроется диалоговое окно **Server Manager.**

3. Добавьте пользователя в организацию **Users**.

   Например, установите имя пользователя **test** и пароль **Huawei12#$**.

4. Нажмите правой кнопкой на **Active Directory Users and Computers** и добавьте название домена, например, **softest.com**.

5. Нажмите правой кнопкой на **softest.com** и выберите **New** > **Organizational Unit** для добавления организационной единицы, например **Huawei**.

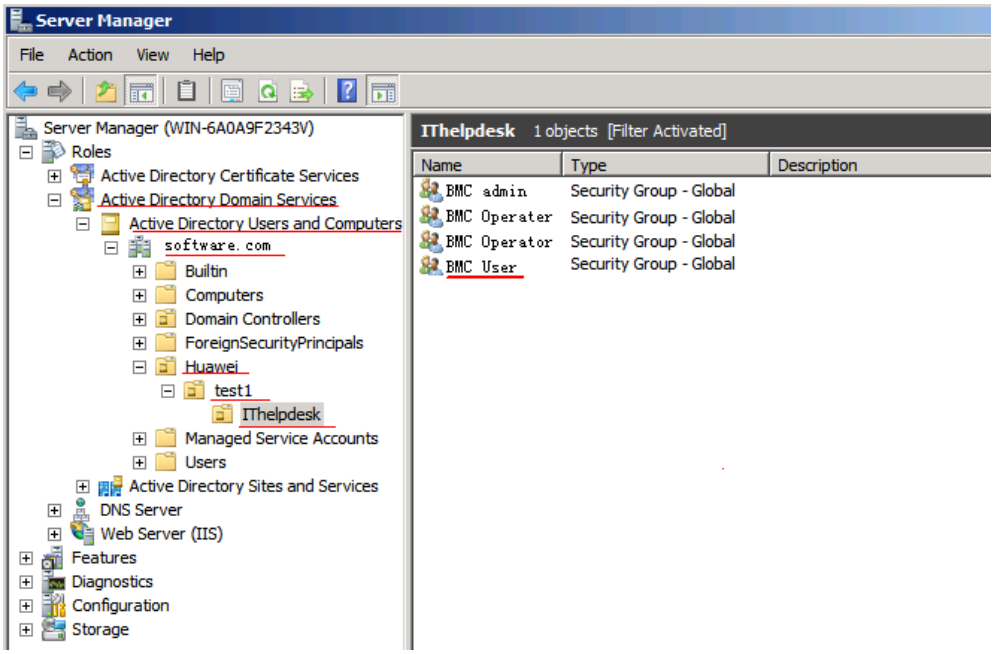
6. Нажмите правой кнопкой на добавленную организационную единицу (**Huawei**) и выберите **New** > **Organizational Unit** для добавления организационной единицы нижнего уровня, например **test1**.

   Аналогичным способом можно создать многоуровневую организацию, например **Huawei -> test1 -> IThelpdesk**.

7. Нажмите правой кнопкой на организационной единице нижнего уровня (например, **IThelpdesk**), и выберите **New** > **Group** для создания группы LDAP, например **BMC User**.

   Можно создавать несколько групп LDAP, например, **BMC admin** и **BMC Operator**, как показано на Рис. 6-3.

   Рис. 6-3 Вновь созданные организационные единицы и группы LDAP

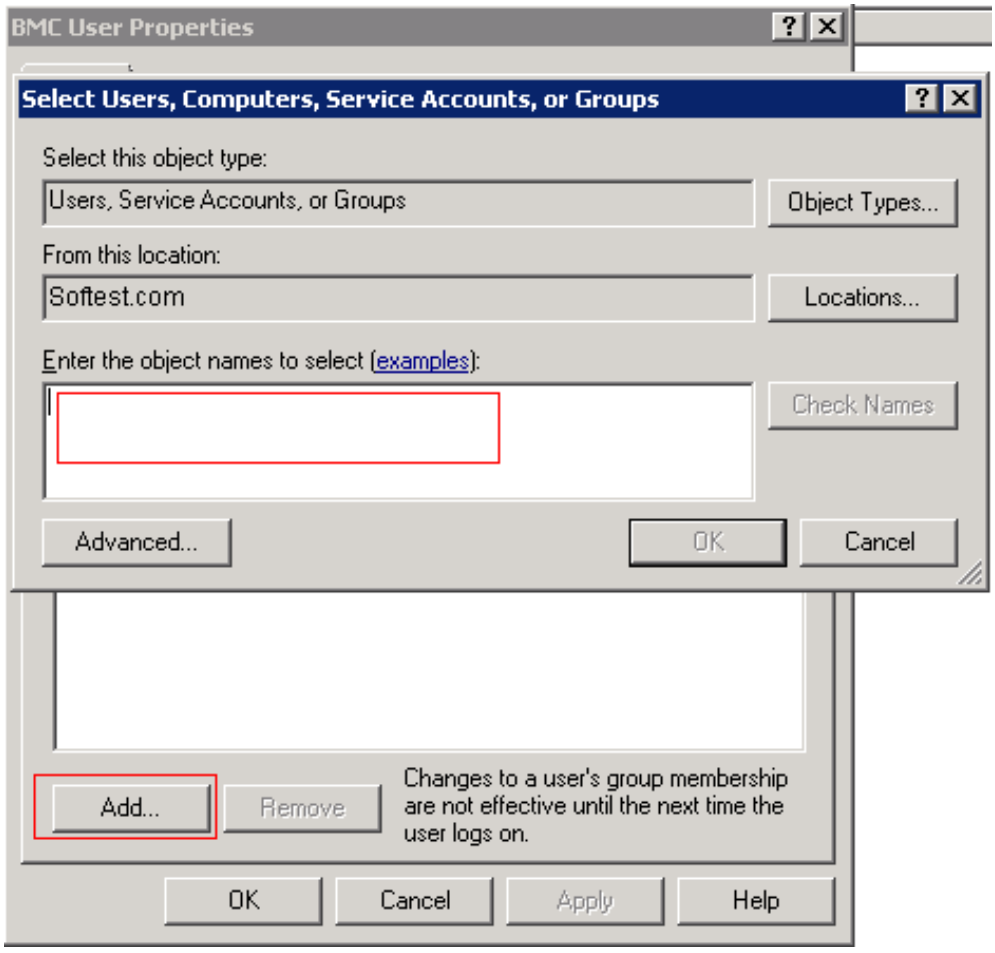


8. Нажмите правой кнопкой на **BMC User** и выберите **Properties** из контекстного меню.

9. Выберите вкладку **Member Of** и нажмите **Add**.

   Откроется диалоговое окно, показанное на Рис. 6-4.

Рис. 6-4 Добавление пользователя



10. Введите пользователя, созданного на шаге 3, например **test**, и нажмите **OK**.

Вход в веб-интерфейс iBMC

Подробная информация приведена в разделе 3.1 Вход в WebUI iBMC.

Конфигурирование сервера LDAP на iBMC

11. На веб-интерфейсе iBMC выберите **Configuration** > **LDAP**.
12. Установите **LDAP** в 

, чтобы включить функцию LDAP.
13. В **LDAP Server Address** введите IP-адрес сервера LDAP, например **192.168.66.66**.
14. Введите номер порта сервера LDAP.
15. Введите название домена сервера LDAP, например, **softest.com**.

    Название домена должно совпадать с названием домена, установленным на сервере LDAP.
16. В **User Folder**, укажите папку пользователей приложения сервера LDAP, например **CN=Users**.

    Имя папки пользователя должно совпадать с именем папки с данными участника приложений на сервере LDAP.
17. В **User Password**, укажите пароль для входа на iBMC.

18. Нажмите **Save**.

Импорт корневого сертификата LDAP (дополнительно)

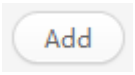
Можно определить, надо ли импортировать корневой сертификат LDAP. В целях безопасности рекомендуется, чтобы проверка сертификата была включена.

19. Установите адрес DNS в качестве адреса сервера LDAP. Подробная информация приведена в разделе 6.7 Конфигурирование DNS на веб-интерфейсе iBMC (вручную).
20. На странице **LDAP** установите для **Certificate Verification** значение **Enable**.
21. Нажмите **Browse** после **Upload Certificate** и выберите корневой сертификат для загрузки.

    Корневой сертификат должен быть файл с расширением .cer, .pem, .cert, или .crt.
22. Нажмите **Upload**.

    После успешной загрузки сертификата на экране появится сообщение «The certificate has been uploaded».

Конфигурирование группы LDAP

23. В поле **LDAP Groups** нажмите 

или  .
24. Введите пароль пользователя iBMC в **User Password**.

    Перед настройкой данных LDAP, укажите пароль для входа на iBMC.
25. В **LDAP Group**, укажите название группы пользователей LDAP, например, **BMC User** (то есть название группы пользователей LDAP, установленный на шаге 7).
26. В **LDAP Group Folder** укажите название папки, в которой хранятся приложения группы LDAP.

    Папка группы LDAP должна совпадать с организационной единицей, установленной для пользователя на сервере LDAP, например, **Huawei/test1/IThelpdesk** (то есть, организационная единица нижнего уровня, установленная на шаге 7). Максимальная длина 255 символов.
27. Выберите правила входа.
28. Выберите интерфейс входа.
29. Выберите права группы LDAP.
30. Нажмите **Save**.

Вход в iBMC с использованием учетной записи домена.

31. Введите имя пользователя (**test**) и пароль (**test/Huawei12#$**), которые действуют на сервере LDAP.
32. В выпадающем списке названия домена, выберите название домена сервера LDAP, например, **softest.com**.
33. Нажмите **Log In**.

----Конец

6.7 Конфигурирование DNS на веб-интерфейсе iBMC (вручную)

Сценарий действий

На странице **Network Settings** веб-интерфейса iBMC можно сконфигурировать Систему доменных имен (DNS) так, чтобы пользователи могли по адресу доменного имени подключиться к iBMC.

ПРИМЕЧАНИЕ

- Адрес доменного имени это комбинация из названия хоста и доменного имени. Например, если название хоста **huawei**, а доменное имя**manager.com**, адрес доменного имени будет**huawei.manager.com**.
- DNS это распределенная база данных, которая устанавливает соответствие между доменными именами и IP-адресами в сети Интернет. Это позволяет пользователям подключаться к Интернет не запоминая IP-адресов, которые могут непосредственно считываться хостами.

Предварительные условия

Данные

Получите следующие данные:

- Имя хоста iBMC.
- Информация о DNS-сервере:
  - Адрес DNS-сервера
  - Доменное имя DNS-сервера

Процедура

Шаг 1 Выполните вход в веб-интерфейс iBMC. Подробная информация приведена в разделе 3.1 Вход в WebUI iBMC.

Шаг 2 Выберите **Config** > **Network Settings**.

Шаг 3 В поле **Config iBMC Host Name** установите для **Server Name** имя хоста iBMC, например, **huawei**.

Шаг 4 Нажмите **Save**.

Шаг 5 Выберите **Config** > **Network Settings**.

Шаг 6 В поле **Set DNS Parameters** нажмите **Manually set DNS address**.

Нажав **Manually set DNS address**, можно вручную задать доменное имя DNS-сервера, предпочтительный адрес DNS-сервера и альтернативный адрес DNS-сервера.

Шаг 7 Определите DNS-адрес.

1. Установите для **Domain** доменное имя DNS-сервера, например, **manager.com**.
2. Установите для **Preferred Server** IP-адрес предпочтительного DNS-сервера, например, **192.168.66.66**.
3. Установите для **Alternate Server** IP-адрес альтернативного DNS-сервера.
4. Нажмите **Save**.

Шаг 8 На локальном компьютере, подключенном к iBMC, установите для local DNS address адрес DNS-сервера.

Убедитесь, что local DNS address совпадает с DNS-адресом iBMC. Иначе, локальный компьютер не сможет подключиться к iBMC через Интернет.

Шаг 9 В адресной строке браузера, введите адрес доменного имени, например **huawei.manager.com,** и нажмите **Enter**. Если появится веб-страница iBMC, конфигурирование выполнено успешно.

----Конец

6.8 Вход в интерфейс командной строки iBMC путем конфигурирования закрытого ключа пользователя SSH

Сценарий действий

При входе пользователя в iBMC через SSH возможны два варианта.

- Аутентификация по паролю: Пользователь должен вводить пароль при каждом входе в систему. Данный метод довольно неудобный и есть возможность кражи пароля.
- Аутентификация по закрытому ключу: После конфигурирования пользователям не надо вводить пароль при каждом входе в систему. Для входа в iBMC через SSH пользователь должен использовать клиент с правильным закрытым ключом, таким образом обеспечивается безопасность.

В данном разделе описывается, как управлять закрытыми ключами SSH и как войти в iBMC через SSH с аутентификацией закрытого ключа.

Подготовка

Предварительные условия

- Локальный клиент может связаться с сервером iBMC.
- Для пользователя на iBMC был установлен интерфейс SSH.

Данные

- Тип открытого ключа SSH: RSA или DSA
- IP-адрес сетевого порта управления iBMC
- Номер сервисного порта SSH

Программное обеспечение

- Инструмент регистрации, типа **putty.exe**.
- Инструмент генерации закрытого ключа, типа **puttygen.exe.**

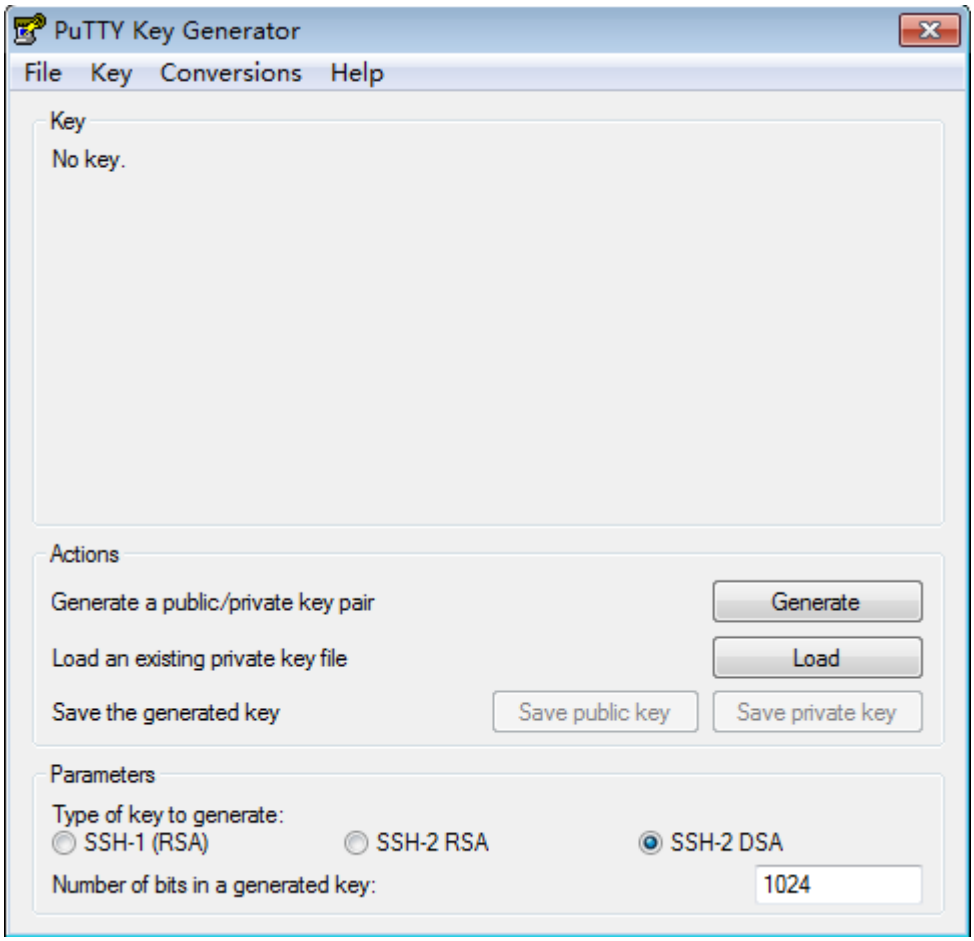
Выше указанные инструменты это бесплатные программы. Скачайте их сами.

Процедура

Генерация закрытого ключа SSH

1. На клиенте (например, компьютере), откройте генератор закрытого ключа, например **puttygen.exe**, как показано на Рис. 6-5.

   Рис. 6-5 Интерфейс генератора закрытого ключа.



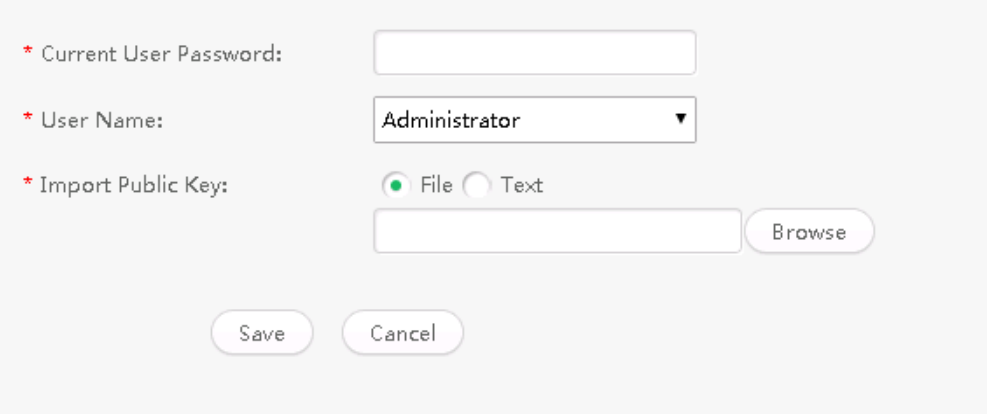
2. В области **Parameters** выберите тип закрытого ключа, например **SSH-2 DSA**.
3. Выберите длину закрытого ключа, например **1024**.
4. Нажмите **Generate**.
5. Нажмите **Save public key** и **Save private key**, чтобы сохранить сгенерированные открытый и закрытый ключи на клиенте.

Импорт открытого ключа в iBMC

6. Выполните вход в веб-интерфейс iBMC. Подробная информация приведена в разделе 3.1 Вход в WebUI iBMC.
7. В веб-интерфейсе iBMC выберите **Config** > **Local User**.
8. В области **SSH Public Key Management** нажмите **Add**.

   Появится окно импорта открытого ключа SSH, как показано на Рис. 6-6.

Рис. 6-6 Импорт открытого ключа SSH



9. Введите имя текущего пользователя.
10. Выберите пользователя, для которого выполняется импорт открытого ключа SSH.
11. Выберите **File** в качестве метода импорта.

    Выберите метод импорта в зависимости от текущих требований.
12. Нажмите **Browse** и выберите открытый ключ, сгенерированный на этапе Генерация открытого ключа SSH.
13. Нажмите **Save**.

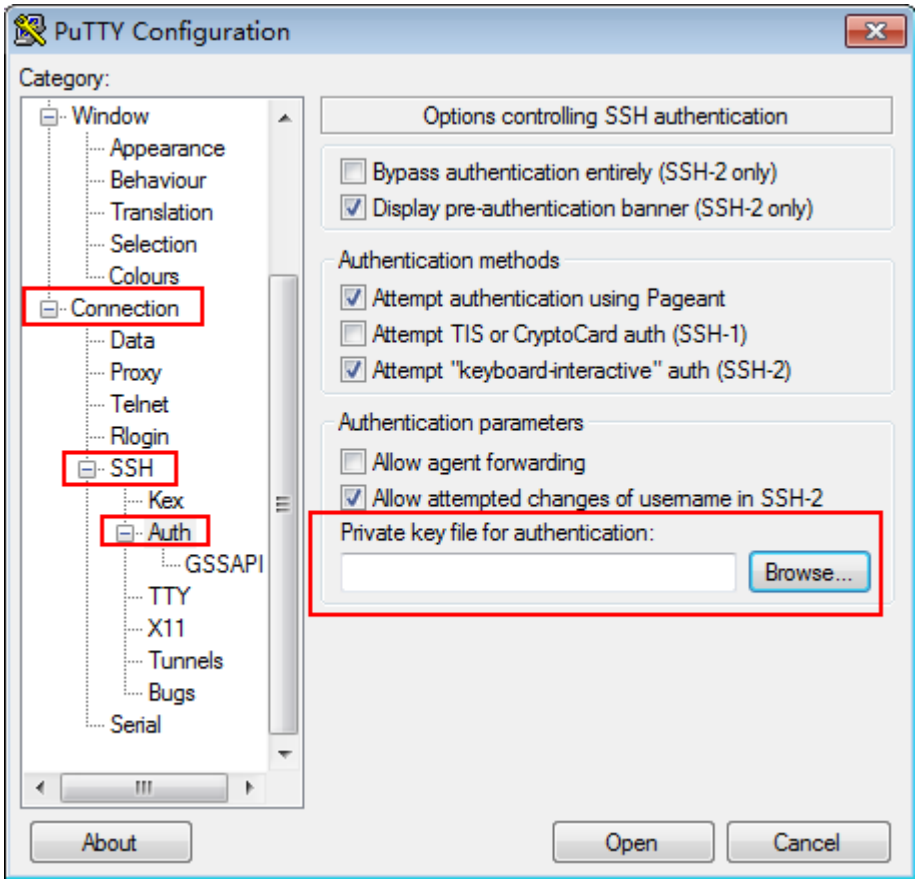
    По завершению импорта появится сообщение об успешном выполнении операции.

Конфигурирование инструмента SSH

14. На клиенте, откройте инструмент регистрации, например **putty.exe**.
15. Выполните импорт закрытого ключа, сгенерированного на этапе Генерация закрытого ключа SSH.

    На Рис. 6-7 показан интерфейс для импорта закрытого ключа.

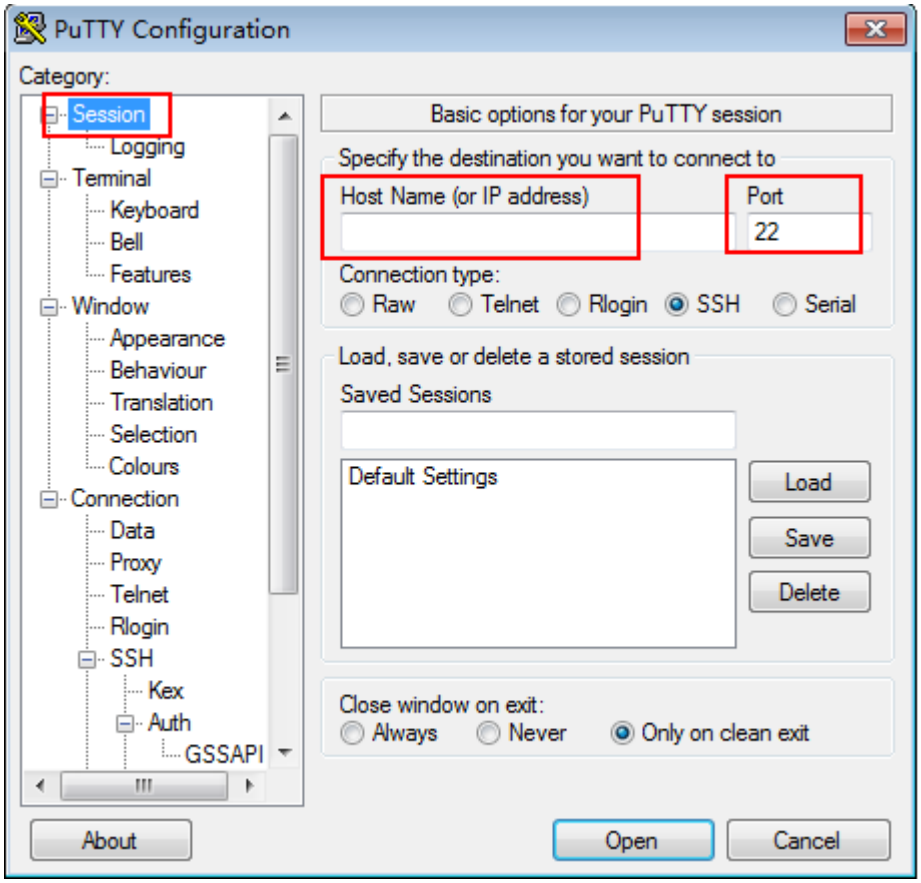
Рис. 6-7 Импорт закрытого ключа



16. Установите данные регистрации в инструменте SSH.

    Данные регистрации включают адрес iBMC и номер сервисного порта SSH, как показано на Рис. 6-8.

Рис. 6-8 Настройка данных регистрации



Войдите в интерфейс командой строки iBMC.

17. Нажмите **Open**.
18. Введите имя пользователя SSH.

    На экране появится командная строка iBMC.

----Конец

6.9 Конфигурирование сертификата SSL iBMC

Сценарий действий

Сертификат SSL устанавливает безопасный канал SSL по HTTPS между веб-браузером на стороне клиента и веб-сервером для передачи зашифрованных данных между клиентом и сервером, который предотвращает раскрытие информации. SSL обеспечивает безопасность передаваемых данных и используется для проверки подлинности доступа к веб-сайту. Серверы Huawei позволяют заменять сертификаты SSL. В целях безопасности замените исходный сертификат и ключи на свой собственный сертификат и пару публичных и приватных ключей, и незамедлительно обновите сертификат.

В данном разделе приведено описание порядка замены сертификата SSL.

Подготовка

Предварительные условия

Локальный клиент может связаться с сервером iBMC.

Процедура

Вход в веб-интерфейс iBMC

Подробная информация приведена в разделе 3.1 Вход в WebUI iBMC.

Выполните операции согласно существующим требованиям:

- Если клиент имеет сертификат SSL, выданный официальными органами, перейдите к Импорт файла сертификата SSL.
- Если клиент имеет сертификат SSL, сгенерированный самими пользователями, выполните пункты Импорт файла сертификата SSL и Добавление корневого сертификата в браузер клиента.
- Для использования сертификата SSL, содержащего специальную информацию и выданного официальными органами, выполните пункты Настройка информации о сертификате, Получение сертификата SSL и Импорт файла сертификата SSL.
- Для использования сертификата SSL, содержащего специальную информацию и сгенерированного самими пользователями, выполните пункты Настройка информации о сертификате, Получение сертификата SSL, Импорт файла сертификата SSL и Добавление корневого сертификата в браузер клиента.

Настройка информации о сертификате

1. В веб-интерфейсе iBMC выберите **Config** > **SSL Certificate**.
2. Нажмите **Customize**.
3. В области **Шаге 1: Generation CSR**, настройте специализированную информацию о сертификате.

   Специализированная информация включает страну, регион (область), город, компанию (организацию) и подразделение (организационную единицу) и общее название.
4. Нажмите **Save**.
5. В появившемся диалоговом окне, экспортируйте файл CSR на клиент.

Получение сертификата SSL

Получить сертификат SSL можно любым из следующих способов:

- Обратитесь за сертификатом подписи SSL в официальную сертификационную организацию (рекомендуется).
- Используйте инструмент для генерации сертификата (например, OpenSSL), чтобы самостоятельно сгенерировать сертификат подписи SSL и корневой сертификат.

  Инструмент генерации сертификата и руководство можно скачать в интернете.

Импорт файла сертификата SSL

6. На странице **SSL Certificate** нажмите **Customize**.
7. Если имеется сертификат SSL, выданный официальными органами, перейдите к **Шагу 2.** В области **Import Server Certificate**, нажмите **Browse**, выберите сертификат подписи SSL, сгенерированный в пункте Получение сертификата SSL, и нажмите **Save**.

После завершения импорта сертификата, появится сообщение «Succeeded in importing the certificate. Reset iBMC for the certificate to take effect».

8. Если используется сертификат SSL, сгенерированный самими пользователями, перейдите к области **Custom Certificate**, нажмите **Browse**, выберите сертификат подписи SSL, полученный в пункте Получение сертификата SSL, введите пароль, используемый при передаче, в текстовое поле **Certificate Password** и нажмите **Save**.

   После завершения импорта сертификата, появится сообщение «Succeeded in importing the certificate. Reset iBMC for the certificate to take effect».

9. Перезапустите iBMC.

Добавление корневого сертификата в браузер клиента

ПРИМЕЧАНИЕ

Если импортированный сертификат SSL сгенерирован вручную (не выдан официальным органом), после импорта сертификата SSL проверьте, имеет ли браузер клиента корневой сертификат.

Далее, в качестве примера, для описания порядка просмотра и добавления корневого сертификата в браузер, используется Internet Explorer.

10. Откройте Internet Explorer.
11. На панели инструментов выберите **Tools** > **Internet Options**.

    На экране появится диалоговое окно **Internet Options**.
12. На вкладке **Content** нажмите **Certificate**.

    На экране появится диалоговое окно **Certificate**.
13. На вкладке **Trusted Root Certificate Issuer** проверьте, указан ли орган, выдавший сертификат SSL.
    - Если да, перейдите к 14.
    - Если нет, перейдите к 15.
14. Проверьте не истек ли срок действия сертификата SSL.
    - Если да, перейдите к 15.
    - Если нет, перейдите к 16.
15. На вкладке **Trusted Root Certificate Issuer** нажмите **Import**. Выполните импорт корневого сертификата, в соответствии с инструкциями.
16. Откройте Internet Explorer снова и проверьте отображается ли значок в адресной панели.
    - Если да, то никаких действий больше выполнять не требуется.
    - Если нет, обратитесь за помощью в службу технической поддержки Huawei.

----Конец

6.10 Конфигурирование формирование отчета Syslog iBMC

Сценарий действий

На странице **Alarm Setting** веб-интерфейса iBMC, можно настроить iBMC, чтобы он передавал данные журнала событий на сторонний сервер в виде syslog-пакетов.

Подготовка

Предварительные условия

Локальный клиент может связаться с сервером iBMC.

Данные

Перед началом конфигурации создайте план всех требуемых для конфигурации данных.

- Syslog attributes:
  - Информация используемая для идентификации хоста-источника. Например, **board serial number**, **product asset tag** или **host name**.
  - Протокол передачи, такие как **TLS**, **TCP** или **UDP**.
  - Метод аутентификации Syslog, типа **one-way authentication** и **mutual authentication**.
  - Уровни регистрируемых событий.
- Syslog server information and log types:
  - Статус канала передачи отчета.
  - Адрес сервера.
  - Номер порта сервера.
  - Типы событий, фиксируемые в отчете.

Программное обеспечение

Необходимо скачать бесплатную программу генерации сертификата **OpenSSL** в интернете.

Процедура

Генерирование сертификатов

Вручную сгенерируйте сертификаты с помощью программы генерации сертификатов.

- Для подтверждения сертификата сервера syslog и корневого сертификата сервера требуется односторонняя аутентификация (one-way authentication).
- Для подтверждения сертификата сервера syslog, корневого сертификата сервера, сертификата клиента syslog и корневого сертификата клиента требуется взаимная аутентификация (mutual authentication).

Для получения более подробной информации о генерации сертификатов, скачайте в интернете руководство по **OpenSSL**.

Загрузка сертификатов на сервер syslog

Загрузка сертификатов на сервер syslog вручную.

- Для односторонней аутентификации, загрузите сертификат на сервер syslog.
- Для взаимной аутентификации, загрузите сертификат сервера и коневой сертификат на сервер syslog.

Вход в веб-интерфейс iBMC

Подробная информация приведена в разделе 3.1 Вход в WebUI iBMC.

Настройка атрибутов syslog

1. На веб-интерфейсе iBMC выберите **Alarm & SEL** > **Alarm Setting**.

2. В поле **Alarm Syslog Notification Settings**, нажмите 

для включения функции формирования отчета syslog.

   Если 

поменяется на 

, функция формирования отчета syslog активирована.
3. Настройте параметры **Syslog Server Identity**, **Alarm Severities**, **Transmission Protocol** и **Authentication Mode**.
4. Загрузите сертификаты.
   - Если для **Authentication Mode** установлено **One way authentication**, загрузите на iBMC корневой сертификат сервера, сгенерированный в пункте Генерация сертификатов.
   - Если для **Authentication Mode** установлено **Mutual authentication**, загрузите на iBMC корневой сертификат сервера и сертификат клиента, сгенерированный в пункте Генерация сертификатов.

Настройка сервер syslog и формата пакетов

5. Выберите канал для передачи пакетов syslog.
6. Нажмите 
, чтобы вывести поле редактирования канала.
7. Нажмите 

для включения канала передачи.

   Если 

поменяется на 

, канал включен.
8. Настройте **Server Address**, **Syslog Port** и **Log Type**.
9. Нажмите **Test**.

   Если на экране появится сообщение «Operation successful», то это говорит о том, что канал доступен.

----Конец

6.11 Вход в систему сервера с помощью VNC

Сценарий

Когда вы не знаете требования совместимости операционной системы и версию приложение Java, применяемое на клиенте (локальном ПК), используйте протокол Virtual Network Computing (VNC) для выхода на рабочий стол сервера через iBMC.

Если версия iBMC – 2.56 или выше, для входа в систему сервера можно использовать VNC, не беспокоясь о применяемой на ПК версии ОС и Java.

Служба VNC поддерживает передачу данных с SSL шифрованием и без. В данном разделе, для примера, используется передача VNC без SSL шифрования.

Предварительные условия

Условия

Клиент (локальный ПК) подключен к сетевому порту управления iBMC сервера, к которому выполняется подключение.

Данные

- IP-адрес сетевого порта управления iBMC и номер порта (номер порта службы VNC)
- Имя пользователя и пароль для входа в iBMC

Программное обеспечение

На локальный ПК установлена сторонняя программа клиента VNC, например, RealVNC.

ПРИМЕЧАНИЕ

Поддерживаемые сторонние клиенты VNC: RealVNC, TightVNC, UltraVNC и TigerVNC.

Процедура

Включение службы VNC

Службу VNC можно включить через веб-интерфейс iBMC, интерфейсы командной строки CLI, IPMI и Redfish. В данном разделе для примера используется веб-интерфейс iBMC.

1. Выполните вход в веб-интерфейс iBMC.

   Подробная информация приведена в разделе 3.1 Вход в WebUI iBMC.
2. Выберите **Configuration** > **Services**.
3. Установите для службы VNC 

, укажите номер порта и нажмите **Save**.

   Служба VNC по умолчанию отключена. По умолчанию номер порта VNC – **5900**.

Установка параметров VNC

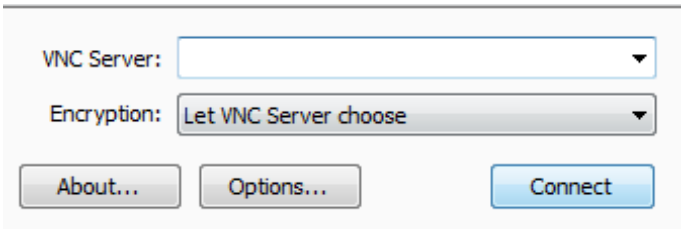
4. На веб-интерфейсе iBMC выберите **Remote Console**.
5. Установите пароль VNC и отмените выбор **SSL Encryption**.

Настройка клиента VNC

6. Откройте клиент VNC, например, RealVNC.

   Откроется страница клиента VNC, показанная на Рис. 6-9.

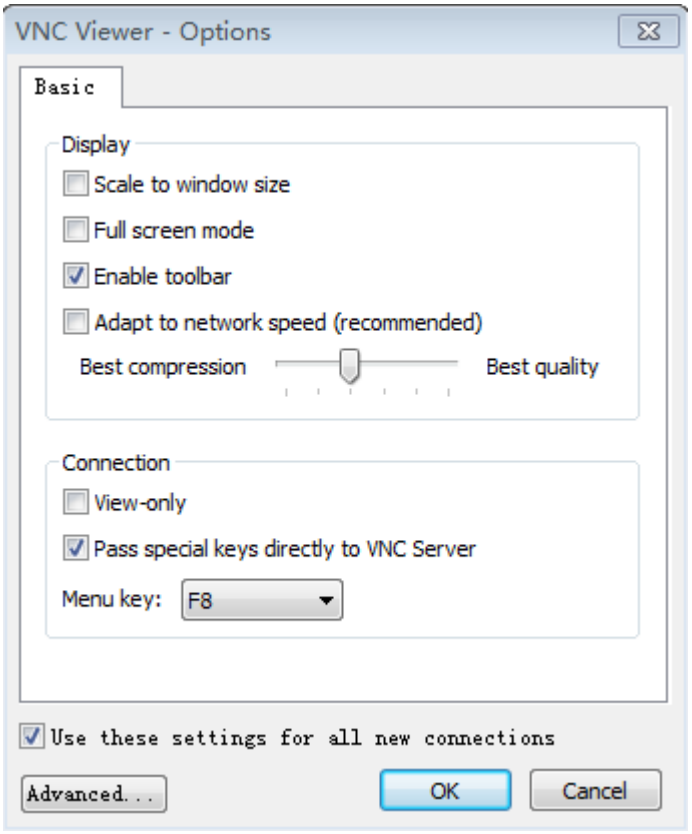
   Рис. 6-9 Клиент VNC



7. Нажмите **Options**.

   Появится диалоговое окно базовых настроек VNC, как показано на Рис. 6-10.

Рис. 6-10 Базовые настройки клиента VNC



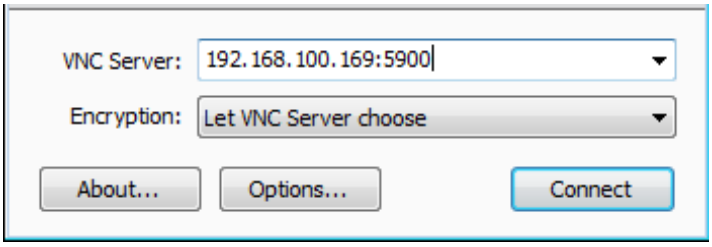
8. Установите параметры в соответствии с требованиями и нажмите **OK**.

Использование клиента VNC для подключения к ОС сервера

9. На клиенте VNC введите *IP-адрес сетевого порта управления iBMC*: *Номер порта VNC*, например **192.168.100.169:5900** в **VNC Server**.

   IP-адрес сетевого порта управления iBMC может быть адресом IPv4 или IPv6.

Рис. 6-11 Клиент VNC

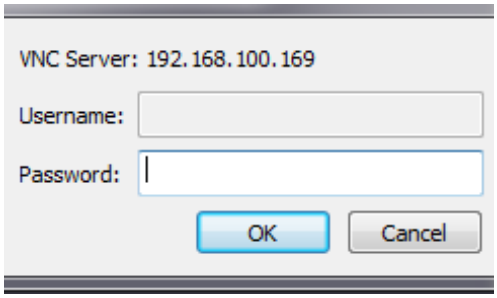


10. Нажмите **Connect**.

    В открывшемся диалоговом окне **Encryption** нажмите **Continue**.

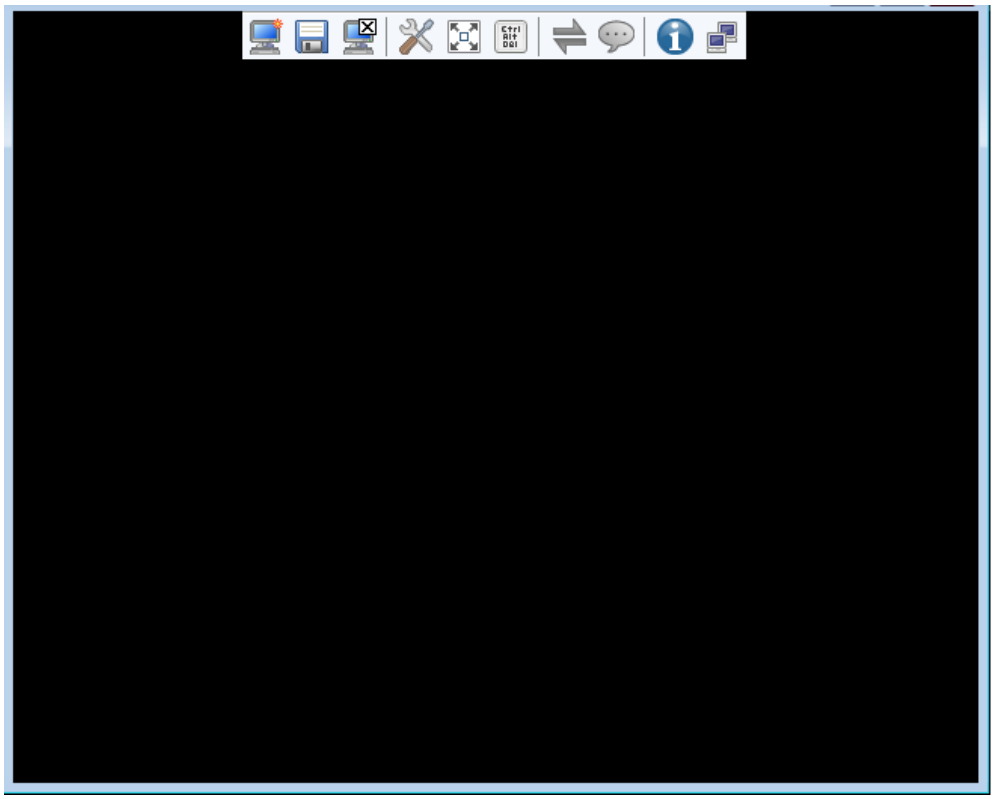
    Откроется диалоговое окно, показанное на Рис. 6-12.

Рис. 6-12 Аутентификация клиента VNC



11. Введите пароль VNC в текстовое окно **Password** и нажмите **OK**.
    Откроется рабочий стол сервера, показанный на Рис. 6-13.

Рис. 6-13 Рабочий стол сервера



----Конец

7 Независимая удаленная консоль

О данной главе

В данном разделе приведено описание порядка использования независимой удаленной консоли.

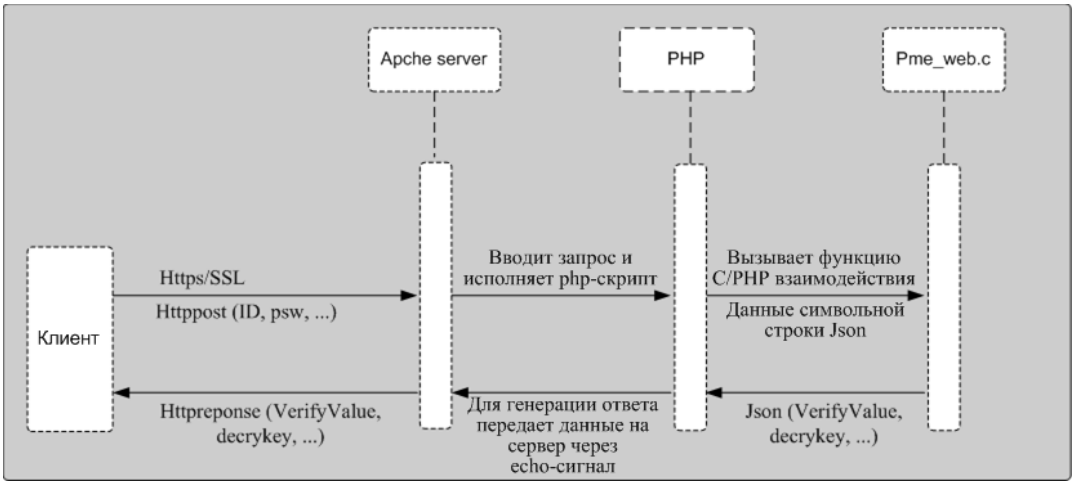
7.1 Краткое описание

Независимая удаленная консоль – это инструмент дистанционного управления, разработанный на базе программного обеспечения управления iBMC сервером Huawei. Он выполняет те же функции, что и **Remote Control**, предоставляемые WebUI iBMC. Данный инструмент позволяет удаленно осуществлять доступ к серверу и управлять им, не беспокоясь о совместимости браузера клиента и JRE.

Базовые принципы

На Рис. 7-1 представлены базовые принципы работы независимой удаленной консоли.

Рис. 7-1 Базовые принципы



Совместимость

Независимая удаленная консоль работает в среде, требования к которой представлены в Табл. 7-1.

Табл. 7-1 Требования к среде

Тип клиентской ОС	Версия клиентской ОС	Управляющее ПО
Windows	Windows 7 (32-bit/64-bit)	iBMC 2.28 или более поздней версии
	Windows 8 (32-bit/64-bit)	
	Windows 10 (32-bit/64-bit)	
	Windows Server 2008 R2 (32-bit/64-bit)	
	Windows Server 2012 (64-bit)	
OC Ubuntu	Ubuntu 14.04 LTS	
	Ubuntu 16.04 LTS	
Mac	Mac OS X El Capitan	

Загрузка

Для загрузки независимой удаленной консоли нажмите Independent Remote Console.

7.2 Вход на сервер с помощью независимой удаленной консоли (Windows)

Сценарий

Независимая удаленная консоль позволяет получить удаленный доступ и управлять сервером с локального ПК.

В данном разделе приведено описание порядка использования независимой удаленной консоли, работающей под управлением ОС Windows для входа на сервер.

Предварительные условия

Условия

Клиент (например ПК) подключен к сетевому порту управления iBMC сервера, к которому выполняется подключение.

Данные

- IP-адрес сетевого порта управления iBMC и номер порта (номер порта HTTPS)
- Имя пользователя и пароль для входа в iBMC

Программное обеспечение

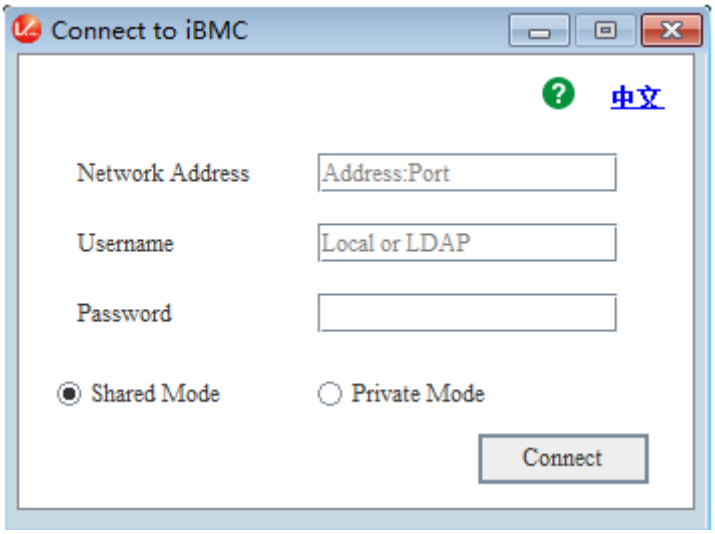
На клиент (ПК) загружен и распакован пакет программного обеспечения.

Процедура

Шаг 1 Настройте IP-адрес для клиента (ПК), чтобы обеспечить связь между клиентом и iBMC. Настроенный IP-адрес и IP-адрес сетевого порта управления iBMC должны находиться в одном сетевом сегменте.

Шаг 2 Дважды щелкните кнопкой мыши **KVM.exe**. На экран появится интерфейс независимой удаленной консоли, как показано на Рис. 7-2.

Рис. 7-2 Интерфейс входа



Шаг 3 Введите сетевой адрес, имя пользователя и пароль.

Сетевой адрес можно может быть представлен в следующих форматах:

- IP-адрес (IPv4 или IPv6) сетевого порта управления iBMC: номер порта
- Адрес имя домена iBMC: номер порта

ПРИМЕЧАНИЕ

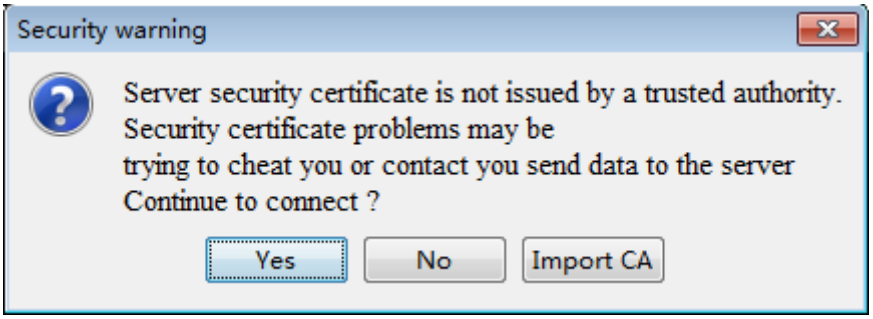
- Введите IPv6-адрес в скобках и IPv4-адрес напрямую. Например **[2001::64]:444**, and **192.168.100.1:444**.
- Номер порта по умолчанию **443** можно пропустить.

Шаг 4 Выберите режим входа и нажмите **Connect.**

- **Shared Mode**: два пользователя могут одновременно подключиться и управлять сервером. Пользователи могут видеть операции друг друга.
- **Private Mode**: один пользователь может подключиться и управлять сервером.

На экране повится информация, показанная на Рис. 7-3.

Рис. 7-3 Информация о рисках безопасности



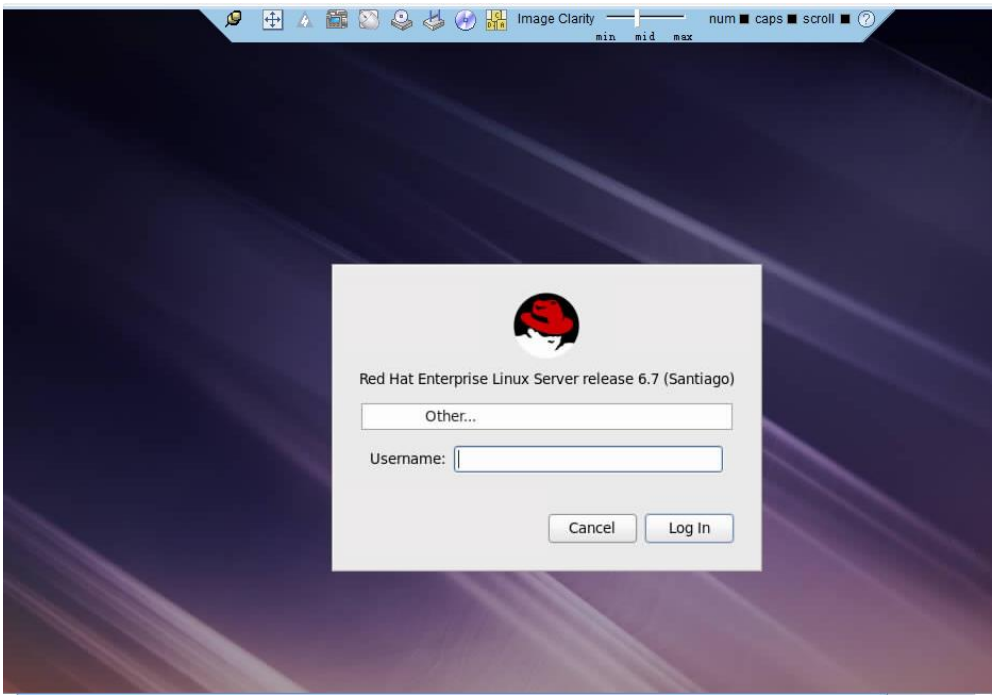
Шаг 5 Выполните следующие операции, исходя из реальной ситуации:

- Нажмите **Yes**, чтобы открыть KVM-консоль.

- Нажмите **No**, чтобы вернуться к интерфейсу входа.
- Нажмите **Import CA**, чтобы импортировать сертификат CA (***.cer**, ***.crt** или ***.pem**). После импорта сертификата CA диалоговое окно о рисках безопасности больше не будет появляться на экране.

На экране появится удаленная виртуальная консоль, показанная на Рис. 7-4.

Рис. 7-4 Удаленная виртуальная консоль сервера



----Конец

7.3 Вход на сервер с помощью независимой удаленной консоли (Ubuntu)

Сценарий

Независимая удаленная консоль позволяет получить удаленный доступ и управлять сервером с локального ПК.

В данном разделе приведено описание порядка использования независимой удаленной консоли, работающей под управлением Ubuntu для входа на сервер.

Предварительные условия

Условия

Клиент (например ПК) подключен к сетевому порту управления iBMC сервера, к которому выполняется подключение.

Данные

- IP-адрес сетевого порта управления iBMC и номер порта (номер порта HTTPS)
- Имя пользователя и пароль для входа в iBMC

Программное обеспечение

На клиент (ПК) загружен и распакован пакет программного обеспечения.

Процедура

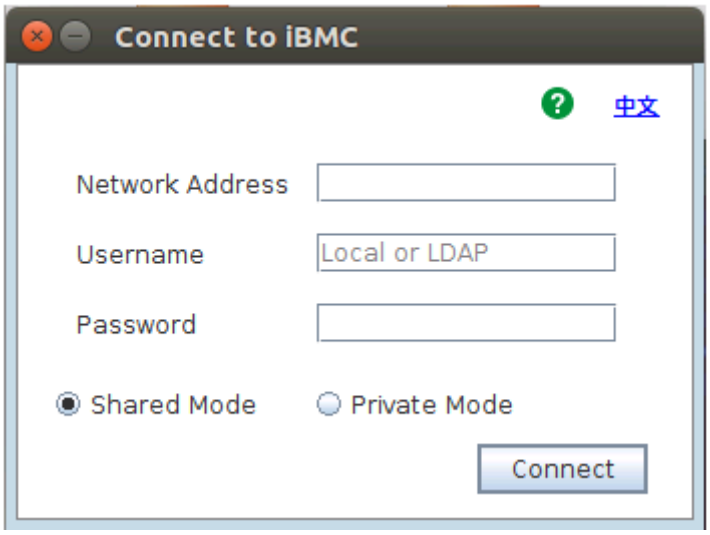
Шаг 1 Настройте IP-адрес для клиента (ПК), чтобы обеспечить связь между клиентом и iBMC. Настроенный IP-адрес и IP-адрес сетевого порта управления iBMC должны находиться в одном сетевом сегменте.

Шаг 2 Откройте консоль и укажите рабочую папку, в которой будут храниться файлы независимой удаленной консоли.

Шаг 3 Выполните команду **chmod 777 KVM.sh** чтобы настроить права пользования независимой удаленной консолью.

Шаг 4 Выполните команду **./KVM.sh** для запуска независимой удаленной консоли. На экран появится интерфейс независимой удаленной консоли, как показано на Рис. 7-5.

Рис. 7-5 Интерфейс входа



Шаг 5 Введите сетевой адрес, имя пользователя и пароль.

Сетевой адрес можно вводить в одном из следующих форматов:

- IP-адрес (IPv4 или IPv6) сетевого порта управления iBMC: номер порта
- Адрес имя домена iBMC: номер порта

ПРИМЕЧАНИЕ

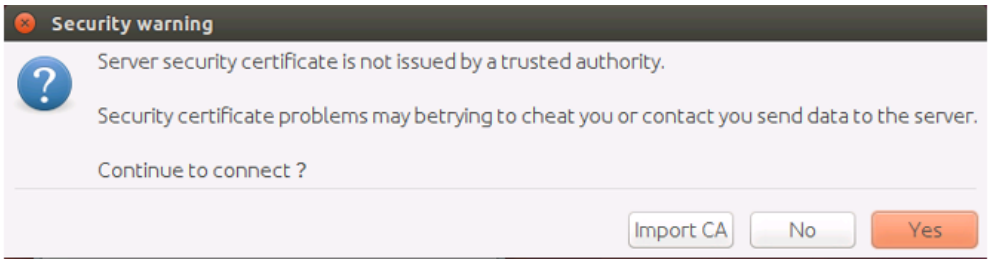
- Введите IPv6-адрес в скобках и IPv4-адрес напрямую. Например **[2001::64]:444**, and **192.168.100.1:444**.
- Номер порта по умолчанию **443** можно пропустить.

Шаг 6 Выберите режим входа и нажмите **Connect**.

- **Shared Mode**: позволяет двум пользователям одновременно подключиться и управлять сервером. Пользователи могут видеть операции друг друга.
- **Private Mode**: один пользователь может подключиться и управлять сервером.

На экране отобразится информация, показанная на Рис. 7-6.

Рис. 7-6 Информация о рисках безопасности

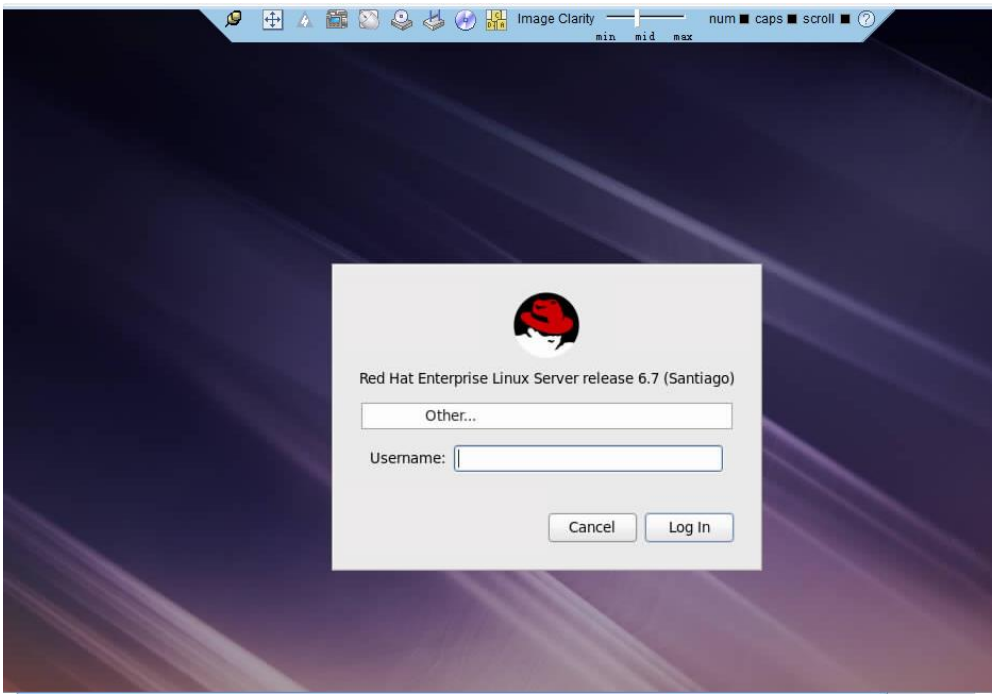


Шаг 7 Выполните следующие операции, исходя из реальной ситуации:

- Нажмите **Yes**, чтобы открыть KVM-консоль.
- Нажмите **No**, чтобы вернуться к интерфейсу входа.
- Нажмите **Import CA**, чтобы импортировать сертификат CA (***.cer**, ***.crt** или ***.pem**). После импортирования сертификата CA диалоговое окно о рисках безопасности больше не будет появляться на экране.

На экране появится удаленная виртуальная консоль, показанная на Рис. 7-7.

Рис. 7-7 Удаленная виртуальная консоль сервера



----Конец

7.4 Вход на сервер с помощью независимой удаленной консоли (Mac)

Сценарий

Независимая удаленная консоль позволяет получить удаленный доступ и управлять сервером с локального ПК.

В данном разделе приведено описание порядка использования независимой удаленной консоли, работающей под управлением Mac для входа на сервер.

Предварительные условия

Условия

Клиент (например ПК) подключен к сетевому порту управления iBMC сервера, к которому выполняется подключение.

Данные

- IP-адрес сетевого порта управления iBMC и номер порта (номер порта HTTPS)
- Имя пользователя и пароль для входа в iBMC

Программное обеспечение

На клиент (ПК) загружен и распакован пакет программного обеспечения.

Процедура

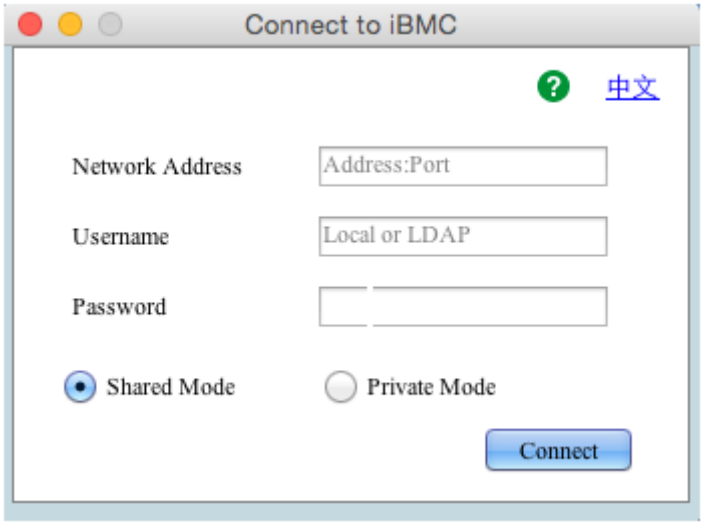
Шаг 1 Настройте IP-адрес для клиента (ПК), чтобы обеспечить связь между клиентом и iBMC. Настроенный IP-адрес и IP-адрес сетевого порта управления iBMC должны находиться в одном сетевом сегменте.

Шаг 2 Откройте консоль и укажите рабочую папку, в которой будут храниться файлы независимой удаленной консоли.

Шаг 3 Выполните команду **chmod 777 KVM.sh** чтобы настроить права пользования независимой удаленной консолью.

Шаг 4 Выполните команду **./KVM.sh** для запуска независимой удаленной консоли. На экран появится интерфейс независимой удаленной консоли, как показано на Рис. 7-8.

Рис. 7-8 Интерфейс входа



Шаг 5 Введите сетевой адрес, имя пользователя и пароль.

Сетевой адрес можно вводить в одном из следующих форматов:

- IP-адрес (IPv4 или IPv6) сетевого порта управления iBMC: номер порта
- Адрес имя домена iBMC: номер порта

ПРИМЕЧАНИЕ

- Введите IPv6-адрес в скобках и IPv4-адрес напрямую. Например **[2001::64]:444**, and **192.168.100.1:444**.
- Номер порта по умолчанию **443** можно пропустить.

Шаг 6 Выберите режим входа и нажмите **Connect.**

- **Shared Mode**: два пользователя могут одновременно подключиться и управлять сервером. Пользователи могут видеть операции друг друга.
- **Private Mode**: один пользователь может подключиться и управлять сервером.

На экране отобразится информация, показанная на Рис. 7-9.

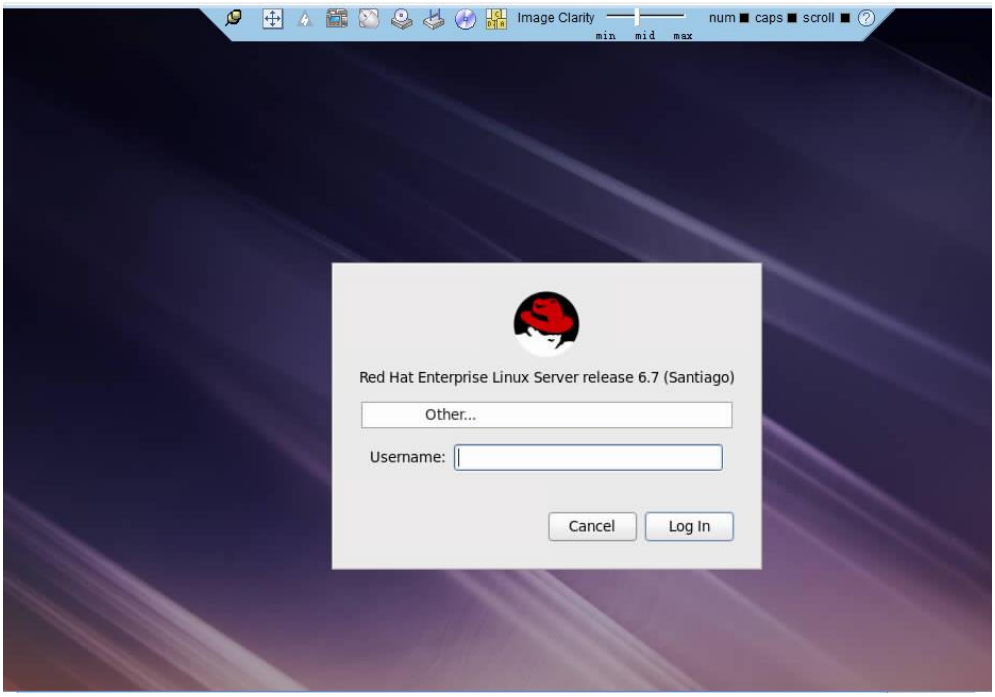
Рис. 7-9 Информация о рисках безопасности

Шаг 7 Выполните следующие операции, исходя из реальной ситуации:

- Нажмите **Yes**, чтобы открыть KVM-консоль.
- Нажмите **No**, чтобы вернуться к интерфейсу входа.
- Нажмите **Import CA**, чтобы импортировать сертификат CA (***.cer**, ***.crt** или ***.pem**). После импортирования сертификата CA диалоговое окно о рисках безопасности больше не будет появляться на экране.

На экране появится удаленная виртуальная консоль, показанная на Рис. 7-10.

Рис. 7-10 Удаленная виртуальная консоль сервера



----Конец

8 Описание файлов конфигурации

В данном разделе приведено описание параметров файлов конфигурации iBMC, BIOS и RAID-контроллера.

В Табл. 8-1, Табл. 8-2 и Табл. 8-3 приведено описание параметров файлов конфигурации iBMC, BIOS и RAID-контроллера.

Табл. 8-1 Параметры iBMC

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
Local user	User	UserName	Имя пользователя.
	User	PassWord	Пароль пользователя.
	User	Privilege	Права пользователя.
	User	UserRoleId	Роль пользователя.
	User	PermitRuleIds	Правила входа пользователя.
	User	LoginInterface	Интерфейс входа пользователя.
	User	IsUserEnable	Включение пользователя.
	UserRole	KVMMgnt	Права KVM.
	UserRole	UserMgnt	Права управления пользователем.
	UserRole	VMMMgnt	Права VMM.
	UserRole	BasicSetting	Права на выполнение базовых настроек.
	UserRole	ReadOnly	Права только на чтение.
	UserRole	PowerMgnt	Права на управление питанием.
	UserRole	DiagnoseMgnt	Права на отладку и диагностику.
	UserRole	SecurityMgnt	Права конфигурирования безопасности.

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
Two-factor authentication	MutualAuthentication	MutualAuthenticationState	Включение двухфакторной аутентификации.
	MutualAuthentication	MutualAuthenticationOCSP	Включение проверки подлинности двухфакторной аутентификации.
LDAP configuration	LDAP	Enable	Включение LDAP.
	LDAP	CertStatus	Включение проверки сертификата LDAP.
	LDAP	HostAddr	Адрес сервера LDAP.
	LDAP	Port	Номер порта LDAPS.
	LDAP	UserDomain	Имя домена.
	LDAP	Folder	Папка, в которой хранятся приложения пользователя.
	LDAPGroup	GroupName	Имя группы LDAP.
	LDAPGroup	GroupFolder	Папка приложений для группы LDAP.
	LDAPGroup	GroupPermitRuleIds	Права входа для группы LDAP.
	LDAPGroup	GroupLoginInterface	Интерфейс входа для группы LDAP.
	LDAPGroup	GroupPrivilege	Права группы LDAP.
Security hardening	PasswdSetting	EnableStrongPassword	Включение функции проверки сложности пароля.
	SecurityEnhance	SSHPasswordAuthentication	Включение аутентификации пароля SSH.
	SecurityEnhance	PwdExpiredTime	Срок действия пароля.
	SecurityEnhance	MinimumPwdAge	Минимальный срок действия пароля.
	SecurityEnhance	ExcludeUser	Пользователь, который может входить в систему в экстренных случаях.
	SecurityEnhance	OldPwdCount	Предыдущий пароль, который нельзя использовать.
	SecurityEnhance	AuthFailMax	Максимальное количество допустимых неудачных попыток входа перед блокировкой учетной записи пользователя.
	SecurityEnhance	AuthFailLockTime	Период блокировки

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
			пользователя.
	PermitRule	TimeRuleInfo	Правила входа в зависимости от времени.
	PermitRule	IpRuleInfo	Правила входа на базе IP-адреса.
	PermitRule	MacRuleInfo	Правила входа на базе MAC-адреса.
	SecurityEnhance	PermitRuleIds	Включение правил.
	SecurityEnhance	BannerState	Включение настройки отображаемой информации безопасности при входе в систему.
	SecurityEnhance	BannerContent	Информация безопасности при входе в систему.
Network configuration	BMC	HostName	Имя хоста iBMC.
	EthGroup	NetMode	Режим сетевого порта.
	EthGroup	ActivePort	Сетевой порт управления.
	EthGroup	IpVersion	Включение IP-адреса.
	EthGroup	IpMode	Порядок назначения IPv4-адреса.
	EthGroup	IpAddr	IPv4-адрес.
	EthGroup	SubnetMask	Маска подсети IPv4.
	EthGroup	DefaultGateway	IP-адрес IPv4 шлюза по умолчанию.
	EthGroup	Ipv6Mode	Порядок назначения IPv6-адресов.
	EthGroup	Ipv6Addr	IPv6-адрес.
	EthGroup	Ipv6Prefix	Длина префикса IPv6-адреса.
	EthGroup	Ipv6DefaultGateway	IP-адрес IPv6 шлюза по умолчанию.
	DNSSetting	IPVer	IP-версия, связанная с DNS.
	DNSSetting	Mode	Порядок назначения адресов DNS.
	DNSSetting	PrimaryDomain	Предпочтительный сервер DNS.
	DNSSetting	BackupDomain	Альтернативный сервер DNS.
	DNSSetting	DomainName	Имя домена DNS.

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
	EthGroup	VlanState	Включение VLAN.
	EthGroup	VlanID	ID VLAN.
	NTP	EnableStatus	Включение NTP.
	NTP	Mode	Режим NTP.
	NTP	PreferredServer	Адрес предпочтительного сервера NTP.
	NTP	AlternativeServer	Адрес альтернативного сервера NTP.
	NTP	AuthEnableStatus	Включение аутентификации сервера NTP.
	BMC	TimeZone	Часовой пояс.
Service configuration	PortConfig	State	Включение FTP.
	PortConfig	Port	Номер порта FTP.
	PortConfig	State	Включение SSH.
	PortConfig	Port	Номер порта SSH.
	Snmp	State	Включение агента SNMP.
	Snmp	PortID	Агент SNMP.
	Kvm	State	Включение KVM.
	Kvm	Port	Номер порта KVM.
	Vmm	State	Включение VMM.
	Vmm	Port	Номер порта VMM.
	Video	State	Включение функции видео.
	Video	Port	Номер порта видео.
	PortConfig	State	Включение HTTP.
	PortConfig	Port	Номер порта HTTP.
	PortConfig	State	Включение HTTPS.
	PortConfig	Port	Номер порта HTTPS.
	RmcpConfig	LanState	Включение IPMI LAN (RMCP).
	RmcpConfig	Port1	Порт 1 IPMI LAN (RMCP).
	RmcpConfig	Port2	Порт 2 IPMI LAN (RMCP).
	RmcpConfig	LanPlusState	Включение IPMI LAN(RMCP+).

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
System configuration	Snmp	V1State	Поддержка SNMPv1.
	Snmp	V2CState	Поддержка SNMPv2c.
	Snmp	LongPasswordEnable	Включение функции длинного пароля.
	Snmp	ROCommunity	Строка сообщества только для чтения.
	Snmp	RWCommunity	Строка сообщества чтения-записи.
	Snmp	SNMPV1V2CPermitRuleIds	Правила входа SNMP.
	Snmp	AuthProtocol	Алгоритм аутентификации SNMPv3.
	Snmp	PrivProtocol	Алгоритм шифрования SNMPv3.
	SecurityEnhance	TLSVersion	Версия TLS.
	SecurityEnhance	EnableUserMgnt	Включенеи функции управления пользователем на стороне обслуживания.
	Session	Timeout	Время ожидания веб-сеанса.
	Session	Mode	Режим веб-сеанса.
	BMC	LocationInfo	Местоположение оборудования.
	MeInfo	CpuUtiliseThre	Аварийное пороговое значение использования ЦП.
	MeInfo	MemUtiliseThre	Аварийное пороговое значение использования памяти.
	MeInfo	DiskPartitionUsageThre	Аварийное пороговое значение использования раздела жесткого диска.
	Partition	RAIDMode	Режим работы RAID (только для RH8100).
System boot option	Bios	StartOption	Первое загрузочное устройство.
	Bios	StartOptionFlag	Настройки загрузки будут использоваться постоянно или только один раз.
Alarm settings	SyslogConfig	EnableState	Включение Syslog.
	SyslogConfig	MsgIdentity	Хост Syslog.
	SyslogConfig	MsgSeverity	Уровень серьезности аварийного

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
			сигнала Syslog.
	SyslogConfig	NetProtocol	Протокол передачи Syslog.
	SyslogConfig	AuthType	Режим аутентификации Syslog.
	SyslogItemCfg	EnableState	Включение сервера Syslog.
	SyslogItemCfg	DestAddr	Адрес сервера Syslog.
	SyslogItemCfg	DestPort	Номер порта сервера Syslog.
	SyslogItemCfg	LogSrcMask	Тип журнала Syslog.
	TrapConfig	TrapEnable	Включение функции Trap.
	TrapConfig	TrapVersion	Версия Trap.
	TrapConfig	Trapv3Userid	Имя пользователя SNMPv3.
	TrapConfig	TrapMode	Режим использования функции Trap.
	TrapConfig	TrapIdentity	Идентификатор хоста Trap.
	TrapConfig	CommunityName	Имя сообщества Trap.
	TrapConfig	SendSeverity	Уровень серьезности для отправки аварийного сообщения Trap.
	TrapItemCfg	ItemEnable	Включение сервера Trap.
	TrapItemCfg	DestIpAddr	Адрес сервера Trap.
	TrapItemCfg	DestIpPort	Номер порта сервера Trap.
	TrapItemCfg	Separator	Разделитель, используемый в сообщении.
	TrapItemCfg	Time	Содержание сообщения (время).
	TrapItemCfg	SensorName	Содержание сообщения (имя датчика).
	TrapItemCfg	Severity	Содержание сообщения (уровень серьезности).
	TrapItemCfg	EventCode	Содержание сообщения (код события).
	TrapItemCfg	EventDesc	Содержание сообщения (описание события).
	TrapItemCfg	ShowKeyWord	Отображение ключевых слов в сообщении.
	SmtpConfig	SmtpEnable	Включение SMTP.

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
	SmtpConfig	SmtpServer	Адрес SMTP.
	SmtpConfig	TlsSendMode	Включение TLS.
	SmtpConfig	AnonymousMode	Включение режима входа анонимного пользователя.
	SmtpConfig	LoginName	Имя отправителя электронной почты.
	SmtpConfig	LoginPasswd	Пароль отправителя электронной почты.
	SmtpConfig	SenderName	Адрес электронной почты отправителя
	SmtpConfig	TempletTopic	Тема сообщения электронной почты.
	SmtpConfig	TempletIpaddr	Включение имени хоста в тему сообщения электронной почты.
	SmtpConfig	TempletBoardSn	Включение серийного номера платы в тему сообщения электронной почты.
	SmtpConfig	TempletAsset	Включение инвентарного номера продукта в тему сообщения электронной почты.
	SmtpConfig	SendSeverity	Уровни серьезности аварийных сигналов, которые необходимо отправить.
	SmtpItemCfg	EmailName	Адрес получателя.
	SmtpItemCfg	EmailDesc	Информация об аварийном сигнале.
	SmtpItemCfg	ItemEnable	Включение функции отправки аварийных уведомлений по электронной почте получателю.
Power control	Payload	PowerOffTimeoutEN	Включение периода ожидания при отключенном питании.
	Payload	PowerOffTimeout	Период ожидания при отключенном питании.
	Payload	PwrButtonLock	Отключение кнопки питания на передней панели сервера.
	Payload	PowerRestorePolicy	Политику восстановления подачи питания при подключении источника питания.

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
Power	PowerCapping	Enable	Включение функции ограничения питания.
	PowerCapping	LimitValue	Значение ограничения питания.
	PowerCapping	FailAction	Принудительное выключения сервера при сбое ограниченного энергопотребления.
Energy saving settings	SysPower	ExpectedMode	Режим работы источника питания.
	SysPower	ExpectedActive	Активный источник питания.
Remote control	Kvm	EncryptState	Включение шифрования KVM.
	Vmm	EncryptState	Включение шифрования VMM.
	Kvm	KeyboardMode	Включение постоянного соединения виртуальной клавиатуры и мыши.
	Kvm	KvmTimeout	Время ожидания удаленной консоли.
	Kvm	LocalKVMState	Включение локальной KVM.
Video playback	Video	VideoSwitch	Включение записи видео.
Screenshot	Kvm	ScreenSwitch	Включение последнего скриншота.
Black box	Diagnose	BlackBoxState	Включение функции черного ящика.
Serial port data	Diagnose	SolDataState	Включение данных последовательного порта.
Others	PortConfig	State	Включение NAT.
	ExPortConfig	State	Включение SSDP.
	PortConfig	Port	Номер порта NAT.
	Bios	BiosPrintFlag	Настройки переключателя печати BIOS.
	Cooling	Mode	Режим настройки скорости вращения вентиляторов.
	Cooling	Level	Уровень скорости вентилятора.
	Stateless	Enable	Включение вычислений без отслеживания состояния.
	Stateless	SysManagerID	ID удаленного управления (конфигурирование вычислений

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
			без отслеживания состояния).
	Stateless	AutoPowerOn	Включение автоматического управления при подаче питания (конфигурирование вычислений без отслеживания состояния).
	Stateless	BroadcastNetSegment	Сегмент широковещательной сети, используемый для автоматического обнаружения (конфигурирование вычислений без отслеживания состояния).
	Stateless	BroadcastPort	Номер широковещательного порта, используемый для автоматического обнаружения (конфигурирование вычислений без отслеживания состояния).
	Stateless	SysManagerIP	IP-адрес сервера, который выполняет управление питанием (конфигурирование вычислений без отслеживания состояния).
	Stateless	SysManagerPort	Номер порта сервера, который выполняет управление питанием (конфигурирование вычислений без отслеживания состояния).

Табл. 8-2 Параметры BIOS

Параметр	Описание
ProcessorHyperThreadingDisable	Включение гиперпотоковой обработки процессора.
ProcessorFlexibleRatioOverrideEnable	Включение функции установки верхнего предела частоты ЦП. Функция отключена по умолчанию.
ProcessorFlexibleRatio	Верхний предел частоты ЦП. По умолчанию это номинальная частота ЦП.
MonitorMwaitEnable	Включение функции Monitor и энергосберегающего режима Mwait.
ProcessorVmxEnable	Включение виртуализации ЦП.
ProcessorLtsxEnable	Включение Intel TXT.

Параметр	Описание
MlcStreamerPrefetcherEnable	Включение функции предварительной загрузки оборудования. Перед обработкой инструкций или данных ЦП предварительно загружает эти инструкции или данные и сохраняет их в кэше L2. Это позволяет сократить время считывания памяти, устранить потенциальные узкие места и, следовательно, повысить производительность системы.
MlcSpatialPrefetcherEnable	Включение функции предварительной загрузки данных в кэш-память. Эта функция позволяет осуществлять предварительную выборку данных, смежных с данными, которые необходимо считывать. Это значительно повышает скорость считывания данных.
DCUStreamerPrefetcherEnable	Включение функции предварительной загрузки данных в устройство DCU. Эта функция позволяет предварительно загружать данные ЦП, что сокращает время чтения данных.
DCUIPPrefetcherEnable	Включение IP устройства DCU. Данная функция позволяет системе проверять архивные записи для данных, которые необходимо предварительно загрузить, что сокращает время чтения данных.
CustomPowerPolicy	Меню выбора энергосберегающего режима. Настройка не поддерживается.
PowerSaving	Параметр, настроенный Huawei для технологии динамического управления энергопотреблением (DEMT), объединяет алгоритмы настройки частоты UniBIOS, разработанные Huawei, и улучшает результаты тестирования энергоэффективности. Данный параметр является действительным только для определенных ОС.
ProcessorEistEnable	Включение технологии уменьшения напряжения питания и тактовой частоты во время низкой нагрузки на процессор (EIST – Enhanced Intel SpeedStep® Technology). EIST позволяет выполнять динамическую настройку частоты ЦП, в зависимости от рабочей нагрузки, что позволяет снизить теплоотдачу.
TurboMode	Включение турбо режима ЦП.
PStateDomain	Переключатель PStateDomain. Данный переключатель настраивает частоты ядра или для определенных пакетов данных.
ProcessorCcxEnable	Меню управления C-состоянием ЦП для контроля потребления энергии процессорами в режиме ожидания.
TStateEnable	Переключатель T-состояния ЦП. Данная функция недоступна, поскольку она ограничивает частоту ЦП.
PackageCState	Настройка C-состояния пакета.
C3Enable	Установленный переключатель C3-состояния ЦП.
C6Enable	Установленный переключатель C6-состояния ЦП.

Параметр	Описание
ProcessorC1eEnable	Установленный переключатель C1e-состояния ЦП.
OSCx	Настройка C2/C3 ACPI.
QpiLinkSpeed	Скорость LINK QPI.
ClusterOnDieEn	Установленный переключатель ClusterOnDie режима Memory Snoop.
EarlySnoopEn	Установленные переключатели EarlySnoop и HomeSnoop режима Memory Snoop.
DdrFreqLimit	Настройки частоты памяти.
RankMargin	Переключатель Rank Margin Tool.
rmtPatternLength	Длина изображения RMT, которая устанавливается при включенном Rank Margin Tool.
MemTestOnFastBoot	Переключатель тестирования памяти, установленный для быстрой загрузки.
ADREn	Переключатель ADR памяти.
CustomRefreshRateEn	Переключатель скорости обновления памяти.
CustomRefreshRate	Скорость обновления памяти.
refreshMode	Режим обновления памяти. 1 указывает на удвоенный режим обновления памяти, а 0 означает, что данный режим не поддерживается. Если данный параметр имеет значение 1, то частота обновления памяти будет удвоена, когда температура DIMM памяти превысит 85ºC.
mcODTOverride	Настройки памяти mc (ODT – on die termination). ODT – это механизм, который позволяет DRAM-контроллеру динамически управлять значением сопротивления контактов DQ/DQS/DM на устройствах DRAM различными способами. Возможные значения: 50 Ом или 100 Ом.
NumaEn	Неравномерный доступ к памяти (NUMA – Non Uniform Memory Access) – это режим доступа к распределенной памяти. Это осуществляет разумное распределение памяти между несколькими узлами, а процессор позволяет одновременно обращаться к различным адресам памяти.
IsocEn	Включение режима изохронного управления потоком, который обеспечивает качество трафика в/от PCH и влияет на производительность памяти, поскольку некоторые полосы пропускания зарезервированы для DMI.
RASMode	Режим памяти RAS. Независимый режим, режим зеркалирования или режим Lockstep.
enableSparing	Установленный переключатель Rank Sparing.

Параметр	Описание
multiSparingRanks	ЦП Haswell поддерживает несколько разрядов памяти. Пользователь может выбрать количество разрядов памяти для канала.
spareErrTh	Пороговое значение корректируемых ошибок памяти. Когда количество корректируемых ошибок памяти достигает данного порогового значения, будет запущен SMI, и будут приняты меры на основе настроенной функции RAS.
PatrolScrub	Управление функцией очистки памяти patrol scrub. Механизм проверяет память с определенной скоростью и исправляет найденные корректируемые ошибки, чтобы предотвратить накопление ошибок до некорректируемых ошибок.
PatrolScrubDuration	Длительность патрулирования памяти в часах.
DemandScrubMode	Управление функцией Demand Scrub. Когда HA считывает данные памяти, он исправляет найденные ошибки и записывает правильные данные в память.
DeviceTaggingMode	Управление функцией Device Tagging. Эта функция позволяет запускать SMI, когда количество ошибок на чипе памяти превышает пороговое значение. Во время обработки SMI микросхема четности может использоваться для замены неисправной микросхемы.
thermalthrottlingsupport	Режим регулировки температуры памяти. Тепловое регулирование с замкнутым контуром (CLTT – Closed Loop Thermal Throttling) применяется для DIMM с датчиками температуры. Настройка динамической памяти в зависимости от температуры датчика. Тепловое регулирование с открытым контуром (OLTT – Open Loop Thermal Throttling) применяется для DIMM без датчиков температуры. Настройка статической памяти в зависимости от конфигурации.
PcieAcpiHotPlugEnable	Включение «горячего» подключения PCI-E IIO.
EnableAzaliaVCpOptimizationste	Включение azalia_on_vcp.
PCIeSRIOVSupport	Включение функции виртуализации PCIe.
VTdSupport	Включение технологии виртуализации (VT-d – Intel VT for Directed I/O).
InterruptRemap	Включение функции перераспределения прерываний, которая связана с технологией VT-d.
CoherencySupport	Включение функции поддержки когерентности, которая связана с технологией VT-d.
IsochCoherencySupport	Включение функции поддержки когерентности (Isoch), которая связана с технологией VT-d.

Параметр	Описание
IdeController	Включение SATA-контроллера.
SataCnfigure	Режим SATA-контроллера.
PchsSata	Включение sSATA-контроллера.
sSataInterfaceMode	Режим sSATA-контроллера.
XHCIMode	Переключатель USB-контроллера 3.0.
CREnable	Переключатель переадресации последовательного порта.
CRTerminalType	Переключатель выбора типа шрифта для переадресации последовательного порта.
CRBaudRate	Переключатель выбора скорости передачи для переадресации последовательного порта.
CRInfoWaitTime	Время отображения информации об инициализации для переадресации последовательного порта.
CRAfterPost	Вступление в силу функции переадресации последовательного порта после POST BIOS.
PXE1setting	Переключатель PXE LOM 1.
PXE2setting	Переключатель PXE LOM 2.
WheaSupport	Включение WHEA для диагностики неисправностей.
WheaEinjType	Включение введения ошибок WHEA для диагностики неисправностей.
SystemErrorEn	Включение диагностики неисправностей.
FDM	Включение функции отправки отчетов по результатам диагностики неисправностей на BMC.
PoisonEn	Разрядный переключатель Poison.
EMcaLogEn	Переключатель EMCA log (ELOG). BIOS создает записи ELOG, в которых записывается подробная информация об ошибках для прогнозирования возможных неисправностей OC/VMM. Эти записи хранятся в резервной памяти, предоставляемой BIOS, доступ к которой осуществляется через входной адрес. Существует также журнал WHEA, соответствующий ELOG, структура журнала WHEA определена в спецификациях ACPI.
EMcaCSmiEn	Переключатель сигнала с CMCI на SMI. Если он отключен, то когда в памяти будут обнаружены корректируемые ошибки, то будет срабатывать только CMCI. SMI будет срабатывать только тогда, когда количество ошибок достигнет порогового значения. Если данный параметр включен, то каждая корректируемая ошибка вызывает SMI, который обрабатывается BIOS. В конце функции обработки SMI BIOS решает, отправлять ли

Параметр	Описание
	сигнал MCE в ОС. Это позволяет собрать более полезную информацию.
PowerStateRestoreOnACLoss	Политика управления питанием для сервера x86 при включении питания AC. • ON: автоматическая подача питания. • OFF: отключение питания. • Last State: восстановление последнего статуса.
BmcWdtEnable	Включение функции «сторожевой собаки» POST.
BmcWdtTimeout	Время ожидания функции «сторожевой собаки» POST.
BmcWdtAction	Действия функции «сторожевой собаки» POST.
OSWdtEnable	Включение функции «сторожевой собаки» ОС.
OSWdtTimeout	Время ожидания функции «сторожевой собаки» ОС.
OSWdtAction	Действия функции «сторожевой собаки» ОС.
SysDbgLevel	Отладочный переключатель BIOS.
serialDebugMsgLvl	Уровень отладки BIOS.
Pci64BitResourceAllocation	Если данная функция включена, то адресное пространство MMIO PCI больше 4 ГБ.
ClkGenSpreadSpectrum	Переключатель расширения спектра.
WakeOnPME	Переключатель технологии дистанционного включения по сети.
NICTrunk	Перед запуском ОС вызывается функция DisableNic2ndhandle для отключения второго оптического порта 82599. В настоящее время данная функция недоступна.
Language	Используемый язык.
ComBaseOutput	Базовые настройки последовательного порта ввода-вывода.
OemMemTurbo	Переключатель разгона мощности памяти.
SoftRaidModeSelect	Переключатель выбора SoftRAID.
BootType	Тип загрузки. Параметр может принимать значения: Legacy, UEFI или DUAL.
QuickBoot	Настройки быстрой загрузки. Если данный параметр выключен, то тестирование памяти будет выполняться каждый раз после каждого запуска при появлении первого экрана.
QuietBoot	Отображение загрузочной информации до появления логотипа BIOS.

Параметр	Описание
PXEOnly	Ограничение загрузки сервера только с PXE и пропуск других параметров загрузки (например жесткий диск и CD-диск).
VideoSelected	Встроенная видеокарта или внешняя видеокарта.
NoBootDevCtr	Автоматическая перезагрузка платы при недоступности устройства загрузки.
BootTypeOrder[0]	Порядок загрузки.
BootTypeOrder[1]	Порядок загрузки.
BootTypeOrder[2]	Порядок загрузки.
BootTypeOrder[3]	Порядок загрузки.

Табл. 8-3 Параметры RAID-контроллера

Тип	Экспортированный параметр	Экспортированный подпараметр	Описание
Storage	RaidController	CopybackEnabled	Статус функции копирования RAID-контроллера.
	RaidController	SMARTerCopybackEnabled	Автоматическое выполнение копирования при обнаружении RAID-контроллером SMART-ошибки физического диска.
	RaidController	JBODEnabled	Статус функции JBOD RAID-контроллера.

9 Часто задаваемые вопросы

О данной главе

9.1 После установки Windows на сервере V5 обнаружены неизвестные устройства

Признаки неисправности

Симптомы	Возможные причины
После установки Windows и соответствующих пакетов драйверов на сервер V5, в окне **Device Manager** обнаружено неизвестное устройство, как показано на Рис. 9-1.	Функция черного ящика включена на iBMC сервера V5 по умолчанию. Однако в ОС Windows нет необходимых драйверов.

Рис. 9-1 Неизвестное устройство в ОС Windows сервера V5

Решение

Шаг 1 Установите iBMA в ОС Windows. Для получения более подробной информации обратитесь к документу Руководство пользователя iBMA.

Шаг 2 Если после запуска iBMA проблема все еще не устранена, то обратитесь в службу техподдержки компании Huawei.

----Конец