Руководство по началу работы сервера DataPy серии БС

ДатаРу

Ваш доверенный партнер

Содержание

Оглавление

Глава 1. Подключение сервера

1.1. Подключение сервера к источнику питания

Для каждого серверного модуля необходимо выполнить следующие операции:

1. Определите место подключения к источнику питания.

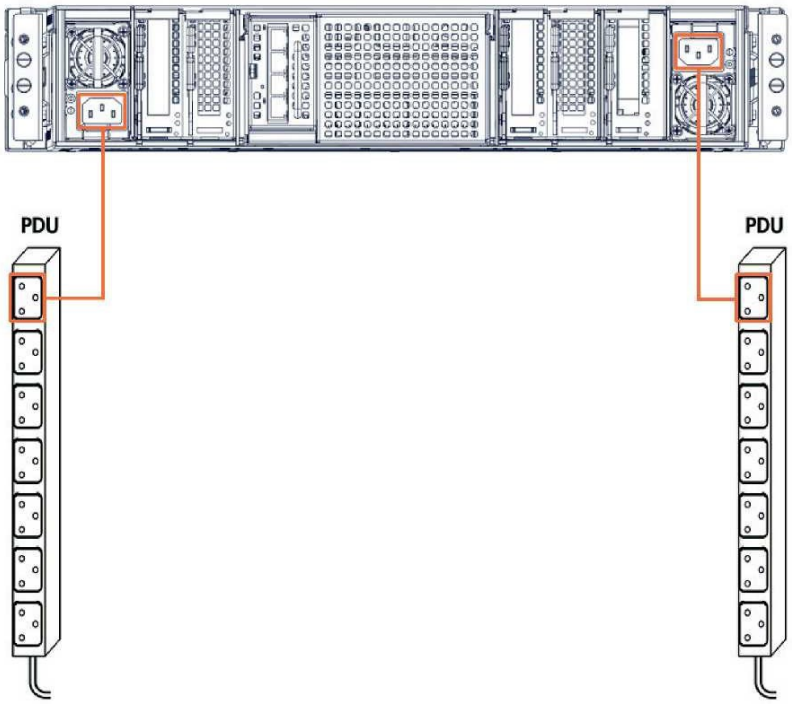
Важно **Выключатель питания на объекте должен находиться в положении ВЫКЛ при подключении блока распределения электропитания (БРЭ). Выключатель питания на объекте должен находиться в положении ВЫКЛ до момента включения системы.**

Вид сзади

2. Подключите модуль к Блоку Распределения Электропитания (БРЭ) a. Проложите каждый шнур питания вдоль фланца корпуса до БРЭ. b. Подключите каждый шнур питания к соответствующему БРЭ.

Примечание Требуется только один БРЭ. Подключение ко второму БРЭ используется для резерва.

Вид сзади



См. Руководства в документации для получения дополнительной информации.

1.2. Подключение сервера к локальной сети (LAN)

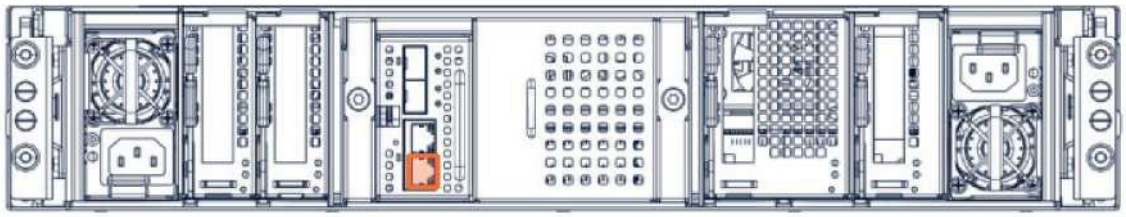
Корпус сервера

1. Для коммутации BMC (порт управления сервером), подключите один конец кабеля RJ45 к порту 0 Phy Ethernet Board (PEB) или Phy Ethernet Board SFP+ (PEBS) на задней стенке серверного модуля.

Вид сзади

Корпус PEB

Корпус PEBS



2. Подключите другой конец кабеля к локальной сети.

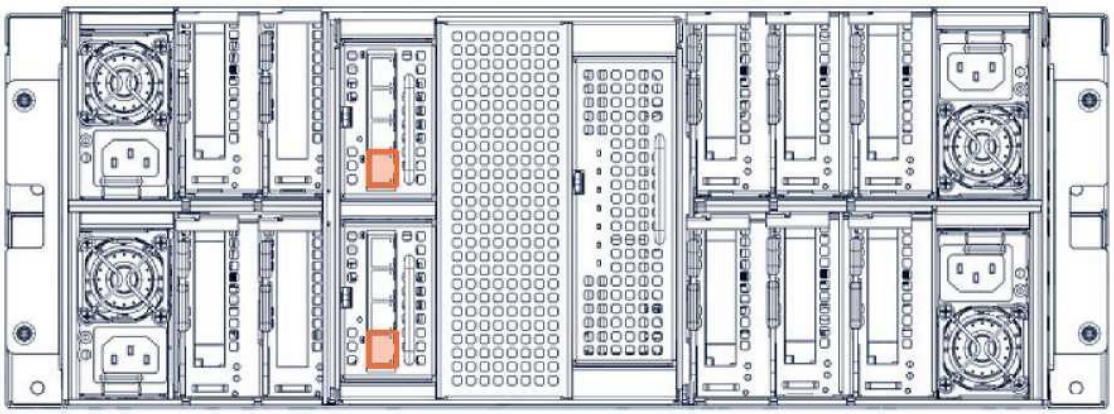
Корпус сервер БС4 и БС8

Примечание Для сервера БС4 и БС8 требуется подключение только главного серверного модуля.

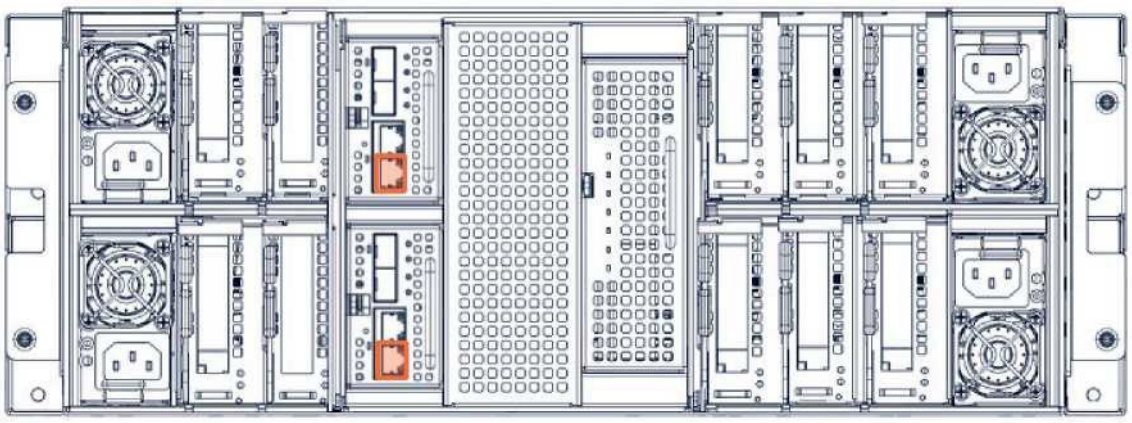
Для каждого серверного модуля, который вы хотите подключить, необходимо выполнить следующие операции:

1. Для коммутации BMC (порт управления сервером), подключите один конец кабеля RJ45 к PEB или порту 0 Phy Ethernet Board SFP+ (PEBS) на задней стенке серверного модуля.

Вид сзади



Корпус PEB



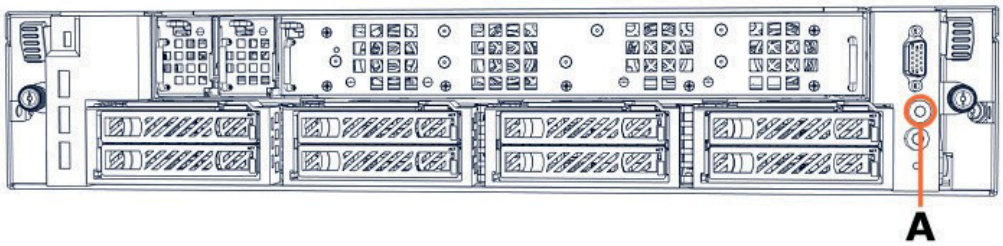
Корпус PEBS

2. Подключите другой конец кабеля к локальной сети.

1.3. Перевод сервера в режим ожидания

1. Попросите заказчика подключить каждый БРЭ к системе энергоснабжения на объекте. Теперь сервер подключен к системе энергоснабжения и готов к включению в режиме ожидания.
2. Попросите заказчика перевести выключатели системы энергоснабжения в положение ВКЛ.
3. Убедитесь в том, что светодиод состояния питания (A) с правой стороны панели управления (Management Board Right Side, MRB) моргает зеленым цветом.

Вид сзади



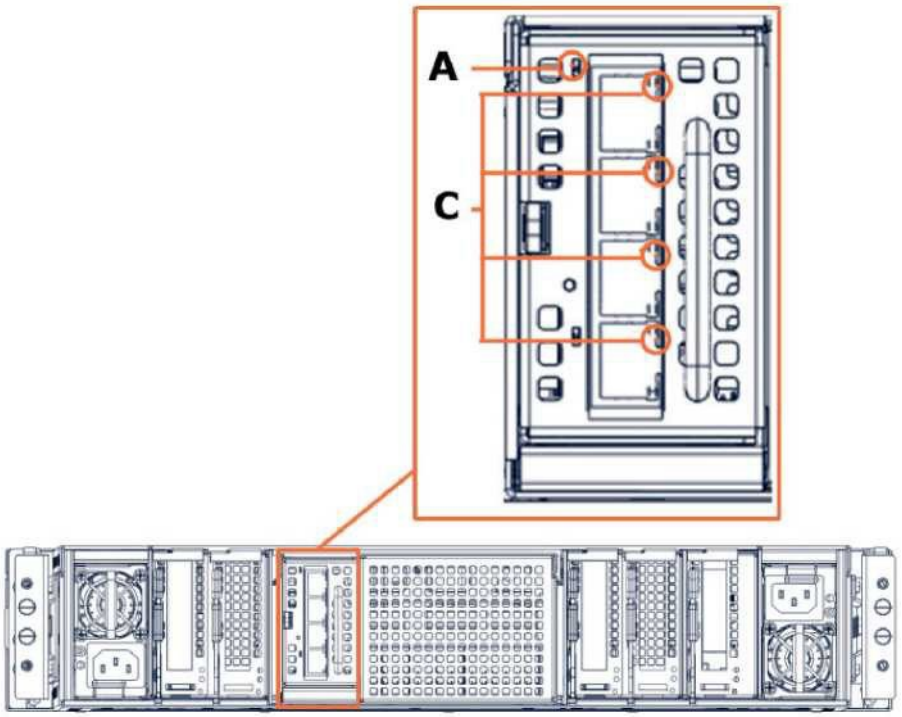
1.4. Проверка светодиодов сервера, расположенных на задней панели

Сервер БС2

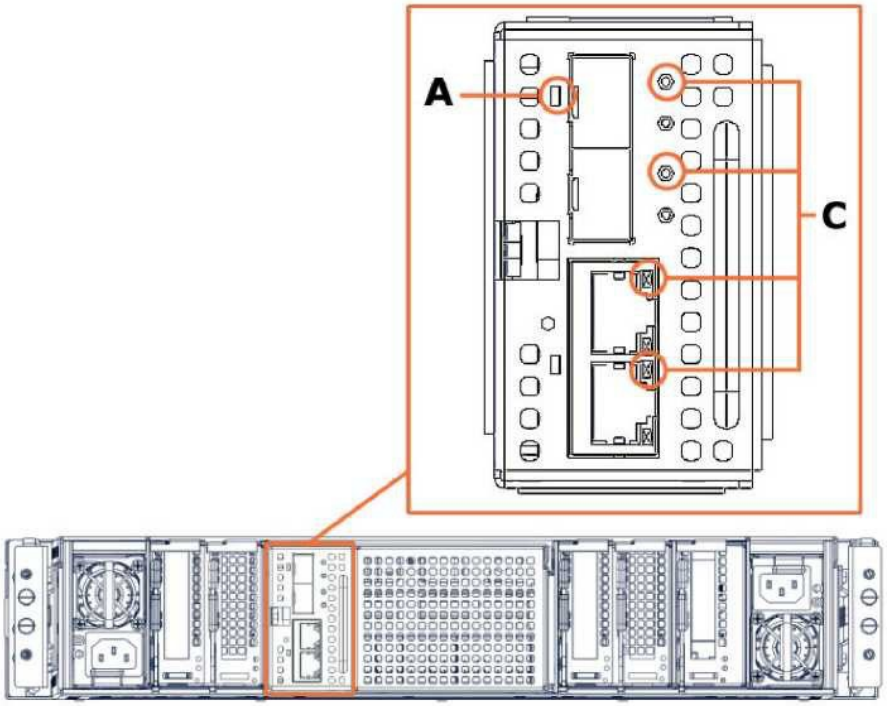
1. Убедитесь в том, что идентификационный светодиод (A) Phy Ethernet Board (PEB) или Phy Ethernet Board SFP+ (PEBS) светится.
2. Убедитесь в том, что светодиоды (C) PEB или PEBS Ethernet Link светятся для подключенных кабелей.

Вид сзади

Корпус PEB



Корпус PEBS

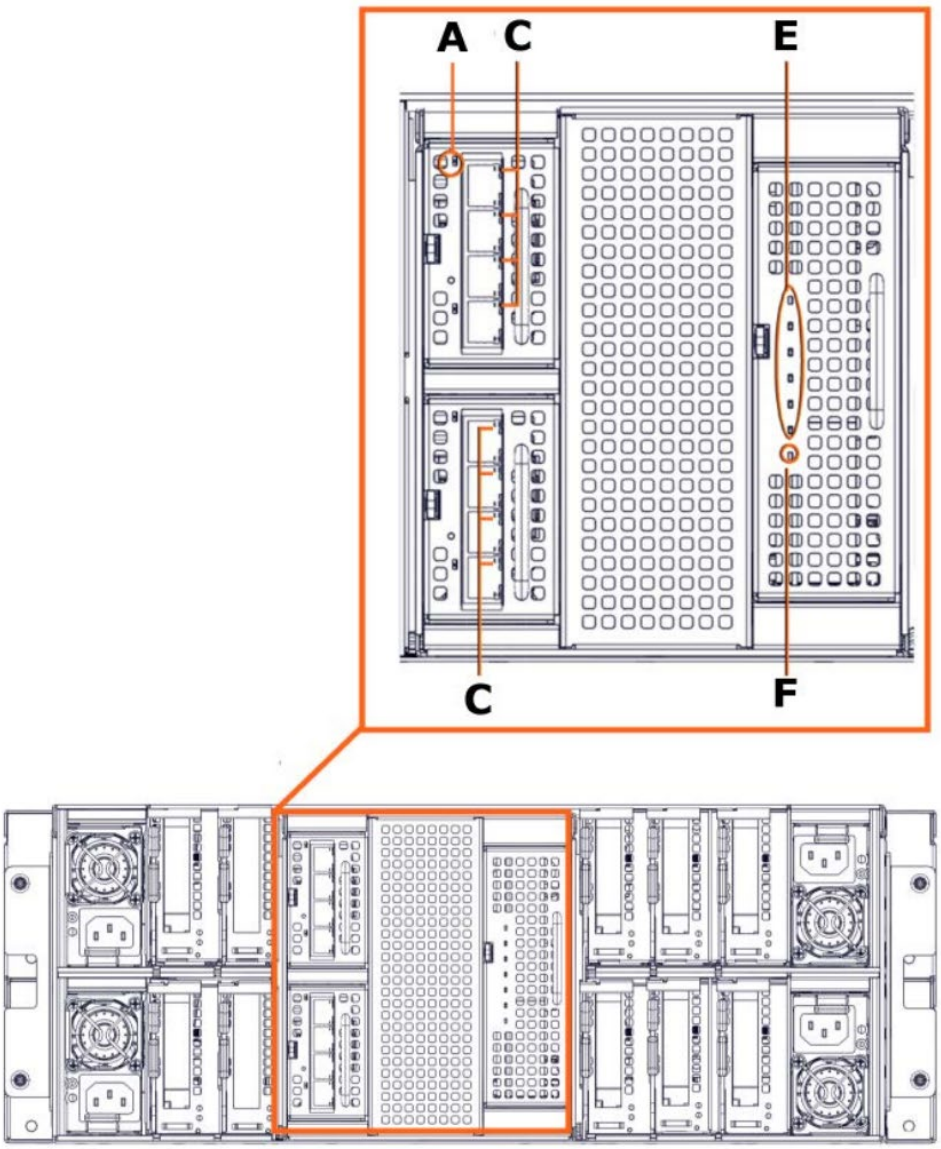


Сервер БС4 и БС8

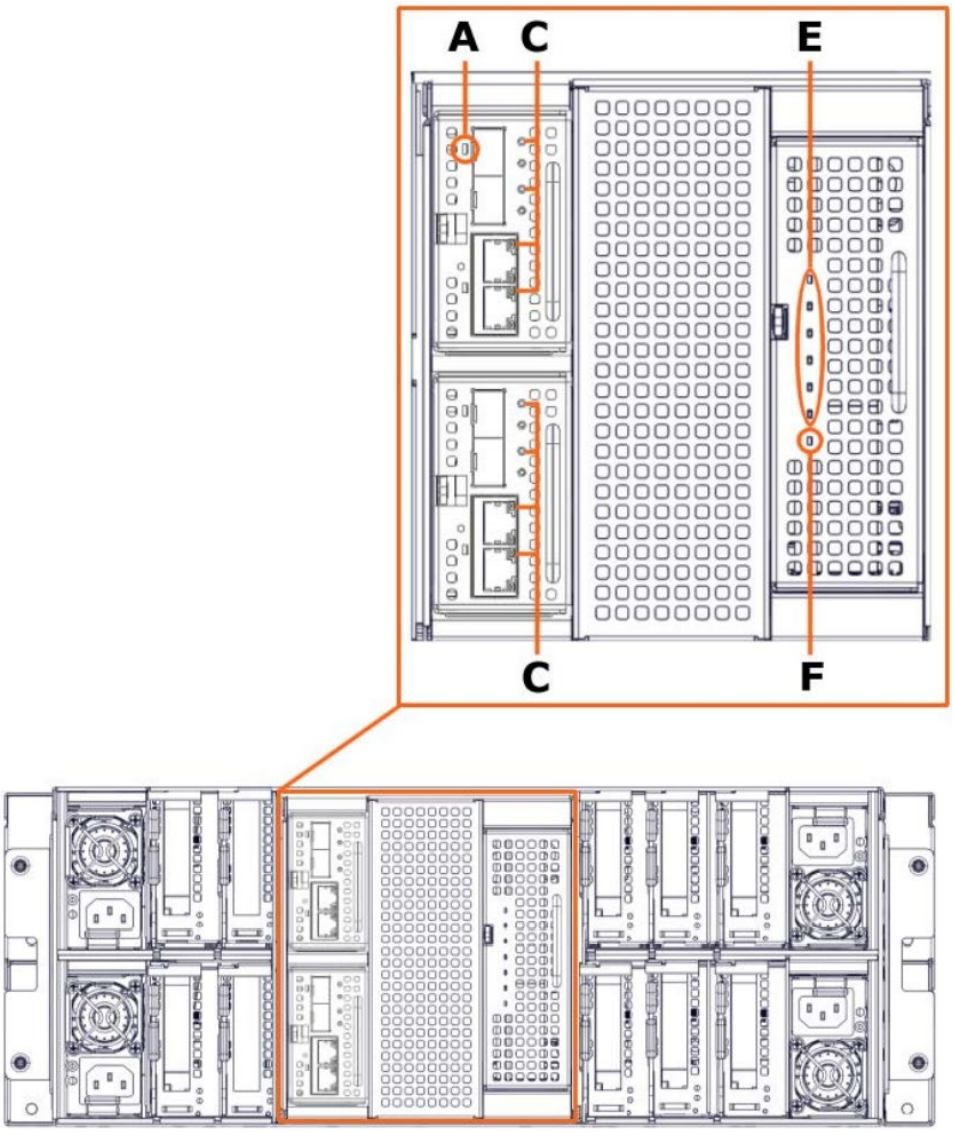
1. Подождите несколько секунд.
2. Убедитесь в том, что светодиод питания (F) sWitch Ethernet One Gigabit (WEO) светится зеленым и светодиоды работы (E) запитанных модулей светятся зеленым.
3. Убедитесь в том, что идентификационный светодиод (A) Phy Ethernet Board (PEB) или Phy Ethernet Board SFP+ (PEBS) светится.
4. Убедитесь в том, что светодиоды соединения (C) PEB или PEBS Ethernet Link светятся, когда кабель подключен.

Вид сзади

Корпус PEB



Корпус PEBS



1.5. Получение MAC-адреса сервера

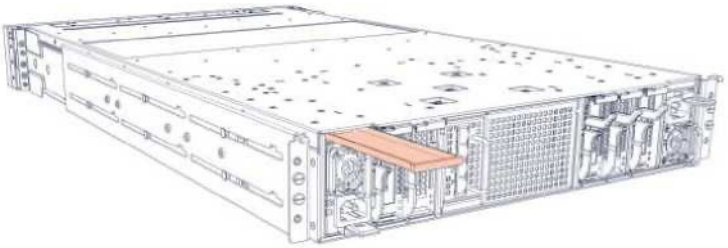
1. Найдите один из идентификаторов с указанием MAC-адреса сервера:

- Один идентификатор находится на передней части сервера в углублении.

Вид спереди

- Другой идентификатор находится на задней части сервера внутри небольшого выдвижного лотка.

Вид сзади



2. Установите MAC-адрес сервера.

Примечание MAC-адрес также может быть получен путем загрузки NFC-метки из MLB-сервера.

1.6. Настройка удаленного доступа

Каждый сервер оснащен встроенным контроллером управления для локального и/или удаленного администрирования с помощью веб-консоли администратора.

Коммуникационный интерфейс встроенного контроллера управления основан на базе TCP/IP. Изначально он имеет сетевые параметры, установленные по умолчанию.

См. Руководства в документации для получения дополнительной информации.

Необходимые условия

Сервер подключен к системе питания.

MAC-адрес был установлен.

Сервер подключен к локальной сети.

DHCP-сервер (где это актуально) установлен в той же подсети. Компьютер находится в той же подсети.

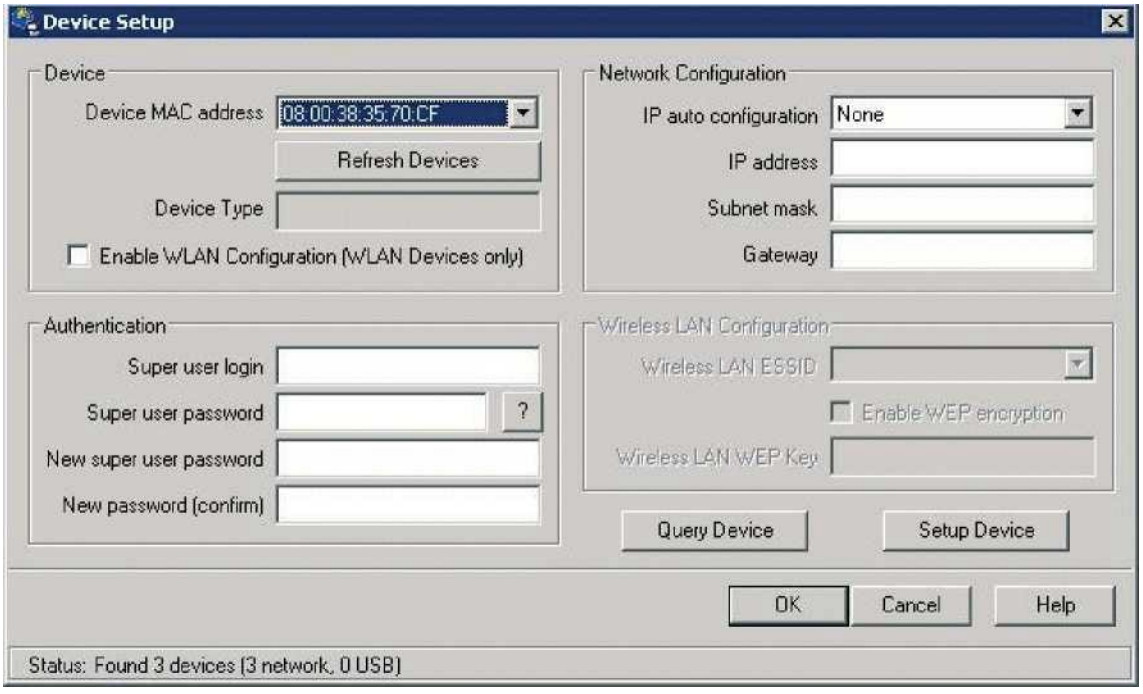
Имеется DVD-диск с файлами и документацией.

Примечание Для этой процедуры показаны только скриншоты psetup.
Следующие скриншоты приводятся только в качестве примеров.

Процедура

1. **Установите инструмент mc-setup или psetup**
   1. Вставьте DVD-диск с файлами и документацией в дисковод компьютера (удаленного или локального).
   2. В соответствии с операционной системой выполните следующие действия:
      - (ОС Linux) Установите mc-setup из установочного пакета в соответствии с версией ОС Linux (например: mc-setup-1.2.1.BD.1-1.fc<x>.i386.rpm, где <x> номер версии ядра Fedora).
      - (ОС Windows) Скопируйте файл psetup на компьютер (psetup устанавливать не нужно).

2. **Определите встроенный контроллер управления**
   1. Запустите инструмент. Появится экран Device Setup (Настройка устройства).

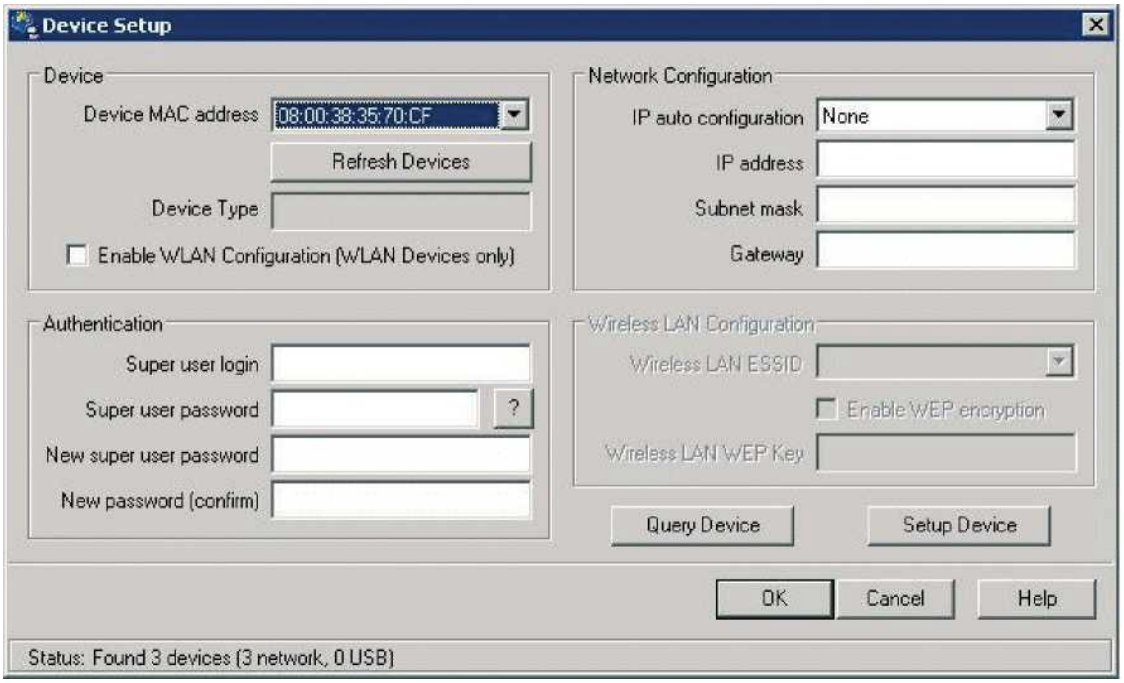


   2. Нажмите кнопку Refresh Devices (Обновить устройства). Инструмент автоматически обнаруживает все встроенные контроллеры управления, подключенные к подсети.
   3. Выберите MAC-адрес встроенного контроллера управления из выпадающего списка.

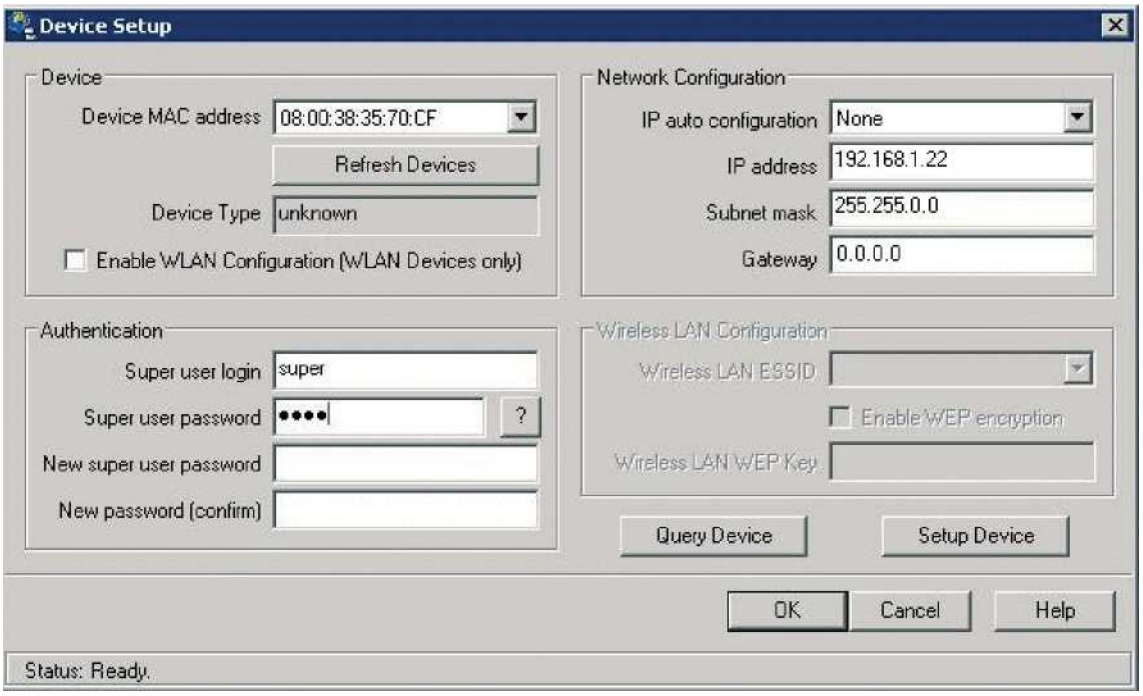
Примечание MAC-адрес контроллера управления указан на идентификаторах, размещенных на сервере, или может быть получен путем загрузки NFC- метки из MLB-сервера.

3. Сконфигурируйте сетевые настройки встроенного контроллера управления

1. Нажмите Query Device (Запросить информацию у устройства). Текущие сетевые настройки будут указаны в пункте Network Configuration (Конфигурация сети).



2. Для настройки статического IP-адреса выполните следующие операции:
   a. Заполните следующие поля.
   - Логин суперпользователя: super
   - Пароль суперпользователя: pass
   - Автоматическая конфигурация IP-адреса: None
   - IP-адрес, маска подсети и шлюз: должны быть указаны в соответствии с сетевыми настройками.



b. Нажмите Setup Device (Настроить устройство).

Важно **Хотя пароль суперпользователя может быть изменен с помощью этого инструмента, рекомендуется в первый раз войти в консоль аппаратного обеспечения сервера (Server Hardware Console) с логином и паролем суперпользователя, установленными по умолчанию. Логин и пароль суперпользователя по умолчанию можно изменить после завершения установки.**

4. Проверьте удаленный доступ к консоли аппаратного обеспечения (Hardware Console)

1. Если порт Ethernet системной платы подключен к компьютеру для локального конфигурирования, подключите его к локальной сети.
2. Откройте веб-браузер и введите IP-адрес, который был сконфигурирован. Если доступ к консоли аппаратного обеспечения (Hardware Console) был выполнен правильно, откроется страница аутентификации.

1.7. Проверка соединений локальной сети

Используйте удаленную рабочую станцию, подключенную к той же подсети, для проверки локальных соединений с помощью команды PING.

Рабочая станция под управлением ОС Windows

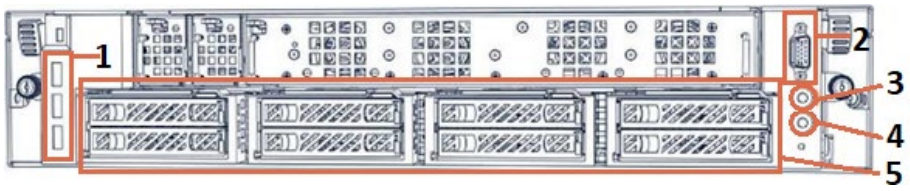
1. Нажмите Start > Run и введите cmd для того, чтобы открыть окно команд.
2. Введите ping <IP_address>, где <IP_address> - IP-адрес сервера, который был настроен с помощью инструмента psetup (Windows) или mc-setup (Linux).

Рабочая станция под управлением ОС Linux

1. Откройте окно shell-команды.
2. Введите ping <IP_address>, где <IP_address> - IP-адрес сервера, который был настроен с помощью инструмента psetup (Windows) или mc-setup (Linux).

1.8. Описание вычислительного модуля.

1.8.1. Вид спереди:



1 – три USB-порта на каждый модуль, из них не менее одного USB 3.0,

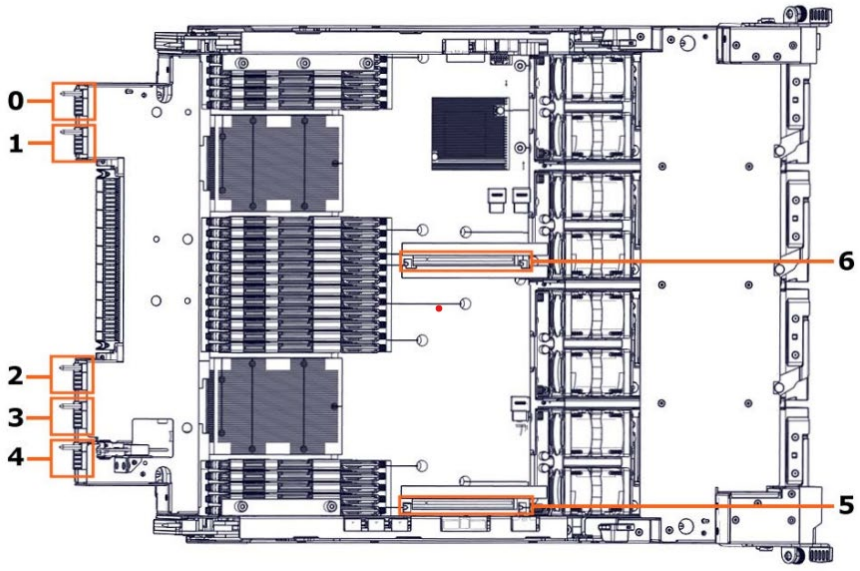
2 – порт DB15 VGA,

3 – кнопка включения,

4 – локатор,

5 – 8 дисковых корзин.

1.8.2. Вид сверху:



Каждый вычислительный модуль включает в себя:

Процессора семейства Intel Xeon Scalable Cascade Lake,

До 24 модулей памяти DIMM (до 3 ТБ на вычислительный модуль)

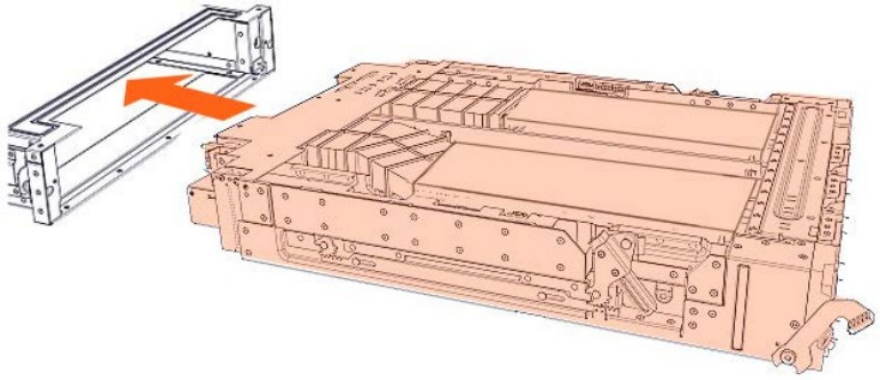
7 PCIe слотов различного назначения:

PCIe слот	Тип	
0	PCIe x8 слот (универсальный)	PCIe x16 слот (для высокопроизводительных адаптеров)
1	PCIe x8 слот (универсальный)	
2	PCIe x8 слот (универсальный)	PCIe x16 слот (для высокопроизводительных адаптеров)
3	PCIe x8 слот (универсальный)	
4	PCIe x16 слот предназначенный для RAID/SAS контроллера, либо NVME адаптера.	
5	Внутренний PCIe x16 разъём предназначенный для GPU, SAS карты или NVME адаптера	
6	Внутренний PCIe x16 разъём предназначенный для GPU	

1.8.3. Установка вычислительного модуля в шасси.

Внешний вид шасси с установленными вычислительными модулями:

Установка вычислительного модуля в шасси:



Глава 2. Начальная конфигурация

2.1. Настройка общих параметров

1. **Соберите информацию о начальной конфигурации**
   При настройке сервера в первый раз запишите следующую информацию:

Необходимые данные	Значение
Название платформы	
Название раздела	
Опция восстановления питания	
Опция полной скорости вентилятора	
IP-адрес (-а) DNS-сервера	
IP-адрес шлюза	
Номер порта TELNET	
Номер порта SSH	
Номер порта HTTPS	
Номер порта HTTP	
IP-адрес (-а) NTP-сервера	
IP-адрес (-а) SNMP-менеджера	
Номер (-а) порта SNMP-менеджера	
Сообщество SNMP-менеджера	
IP-адрес SysLog-менеджера	
Название или IP-адрес SMTP-сервера	
Адрес SMTP-отправителя	

2. **Запустите SHC**
   1. Запустите веб-браузер и введите стандартный или защищенный IP-адрес или имя хоста ведущего модуля в соответствии с настройками. Откроется страница аутентификации.
   2. Заполните поля Username (Пользователь) и Password (Пароль) и нажмите Log On (Войти в учетную запись). Откроется страница System Control (Управление системой).

3. **Укажите платформу**
   1. Во вкладке Configuration (Конфигурация) нажмите Global Settings > Platform (Общие настройки > Платформа), чтобы открыть страницу Platform (Платформа).
   2. Заполните поля и нажмите Apply (Применить).

Примечание Поле Module Count доступно только для чтения.

4. Укажите раздел

1. Во вкладке Configuration (Конфигурация) нажмите Global Settings > Managed Server (Общие настройки > Управляемый сервер), чтобы открыть страницу Managed Server Name (Название управляемого сервера).
2. Заполните поле и нажмите Apply (Применить).

5. Укажите DNS-сервера и шлюз, если необходимо

1. Во вкладке Configuration (Конфигурация) нажмите BMC Settings > Network (BMC-настройки > Сеть), чтобы открыть страницу Network Settings (Сетевые настройки).
2. Отредактируйте общие настройки в соответствии с требованиями заказчика и нажмите Apply (Применить).

6. Укажите режимы и порты для сетевого доступа

1. Во вкладке Configuration (Конфигурация) нажмите BMC Settings > Network (BMC-настройки > Сеть), чтобы открыть страницу Network Settings (Сетевые настройки).
2. Выберите необходимые режимы доступа, введите соответствующие номера портов и нажмите Apply (Применить).

7. Отключение режима серийного терминального доступа

1. Во вкладке Configuration (Конфигурация) нажмите BMC Settings > Network (BMC-настройки > Сеть), чтобы открыть страницу Network Settings (Сетевые настройки).
2. Снимите галочку в пункте Enable Serial Terminal Access (Включить серийный терминальный доступ) и нажмите Apply (Применить).

8. Отключение режима протокола настройки

1. Во вкладке Configuration (Конфигурация) нажмите BMC Settings > Network (BMC-настройки > Сеть), чтобы открыть станицу Network Settings (Сетевые настройки).
2. Поставьте галочку в пункте Disable Setup Protocol (Отключить протокол настройки) и нажмите Apply (Применить).

9. Отключение режима сброса порта Ethernet

1. Во вкладке Configuration (Конфигурация) нажмите BMC Settings > Network (BMC-настройки > Сеть), чтобы открыть станицу Network Settings (Сетевые настройки).
2. Выберите пункт Inhibit the PHY Reset of the shared Ethernet Controller и нажмите Apply (Применить).

10. Остановка SHC

1. Нажмите кнопку Logout (Выход из учетной записи).

11. Запуск SHC

1. Запустите веб-браузер и введите стандартный или защищенный IP-адрес или имя хоста ведущего модуля в соответствии с настройками. Откроется страница аутентификации.
2. Заполните поля Username (Пользователь) и Password (Пароль) и нажмите Log On (Войти в учетную запись). Откроется страница System Control (Управление системой).

12. Установка таймера контроллера управления

1. Во вкладке Configuration (Конфигурация) нажмите BMC Settings > Date-Time (BMC-настройки > Дата-Время), чтобы открыть страницу Date/Time (Дата/Время).
2. Если нужно изменить значение Time Zone (Часовая зона), поставьте галочку или уберите ее в пункте Adjust for daylight savings time (Переход на летнее время).
3. Нажмите на User Specified Time (Время, заданное пользователем) или Synchronize with NTP

Server (Синхронизация с NTP-сервером), заполните соответствующие поля и нажмите Apply (Применить).

2.2. Настройка передачи оповещений

События, не связанные с IPMI, записываются в журнал Board and Security Messages, а IPMI-события записываются в журнал System Event Log (SEL). Информация об этих событиях может быть передана в качестве оповещений SNMP-менеджеру и/или получателям по электронной почте.

При настройке передачи оповещений в первый раз необходимо выполнить следующее:

- Настроить SNMP-сервер для событий, не связанных с IPMI
- Настроить SNMP- и SMTP-сервер для IPMI-событий

2.2.1. Настройка сервера SNMP-менеджера для событий, не связанных с IPMI

1. Определите назначение сообщения

1. Во вкладке Configuration (Конфигурация) нажмите BMC Settings > Messages (BMC-настройки > Сообщения), чтобы открыть страницу SNMP Messages and Syslog Configuration (SNMP-сообщения и Конфигурация системного журнала).
2. Если необходимо, поставьте галочку в пункте SNMP Logging Enabled (Включить SNMP- журнал) и заполните поля Destination IP (IP назначения), Port # (Номер порта) и Community (Сообщество).
3. Если необходимо, поставьте галочку в пункте Enable Syslog Forwarding (Включить пересылку системного журнала) и заполните поле IP Address (IP-адрес).
4. Нажмите Apply (Применить).

2. Скачайте файл SNMP MIB

1. Во вкладке Configuration (Конфигурация) нажмите BMC Settings > Messages (BMC-настройки > Сообщения), чтобы открыть страницу SNMP Messages and Syslog Configuration (SNMP-сообщения и Конфигурация системного журнала).

2. Нажмите Download SNMP MIB (Скачать SNMP MIB).

3. Загрузите файл SNMP MIB в сервер SNMP-менеджера

1. Во вкладке Configuration (Конфигурация) нажмите BMC Settings > Messages (BMC-настройки > Сообщения), чтобы открыть страницу SNMP Messages and Syslog Configuration (SNMP-сообщения и Конфигурация системного журнала).
2. Заполните поля.
3. Нажмите Apply (Применить).

2.2.2. Настройка SNMP-менеджера и SMTP-сервера для IPMI-событий

Функция передачи оповещений позволяет передавать информацию о выбранных событиях в виде оповещений одному или нескольким SNMP-менеджерам и/или получателям по электронной почте.

1. **Для отправки оповещений SNMP-менеджеру, введите строку сообщества менеджера прерываний событий**
   1. Во вкладке Configuration (Конфигурация) нажмите Alert Settings > General (Настройки оповещений > Общие настройки), чтобы открыть страницу General Lan Alert (Общие сетевые оповещения).
   2. Заполните поле Community String (Строка сообщества), указав значение строки сообщества, используемое SNMP-менеджером, и нажмите Apply (Применить).

2. **Для отправки информации о событиях в виде оповещений получателям электронной почты настройте конфигурацию почтового сервера**
   1. Во вкладке Configuration (Конфигурация) нажмите Alert Settings > General (Настройки оповещений > Общие настройки), чтобы открыть страницу General Lan Alert (Общие сетевые оповещения).

Примечание После изменения каждое из этих значений будет автоматически обновлено на всех модулях раздела.

   2. Выберите поле SMTP Server (SMTP-сервер) с названием или IP-адресом исходящего SMTP-сервера, используемого для отправки оповещений по электронной почте.
   3. Заполните поле Email Sender Address (Адрес отправителя электронной почты), указав адрес отправителя почтового сервера, как он указан в заголовке электронной почты.
   4. Нажмите Apply (Применить).

3. **Сохраните параметры**

   Используйте bsmBMCcfg.sh, утилиту для резервного копирования с DVD-диска с файлами и документацией, для того, чтобы выполнить резервное копирование системы, PEF и данных конфигурации, если необходимо. Дополнительная информация доступа в документе Remote Hardware Management CLI Reference Guide, 86 A1 36FR.

4. **Настройте конфигурацию IP-адресов менеджера прерываний событий, адреса получателей электронной почты и/или расположения локальной сети**
   1. Во вкладке Configuration (Конфигурация) нажмите Alert Settings > LAN Destinations (Настройки оповещений > Расположение локальной сети), чтобы открыть страницу LAN Destinations (Расположение локальной сети).
   2. Выберите первые свободные строки назначения локальной сети (IP 0.0.0.0) и нажмите Modify (Изменить), чтобы открыть страницу IPMI LAN Destination Edit.

Примечание После изменения каждое из этих значений будет автоматически обновлено на всех модулях раздела.

   3. Введите необходимый ID назначения в поле Destination Number (Номер назначения).
   4. Нажмите на кнопку PET Alert.
   5. Заполните поля Acknowledge (Подтверждение), Timeout (Время ожидания) и Retries (Повторные попытки).
   6. Введите IP-адрес хост-сервера в поле Trap destination (Назначение прерывания) и нажмите Apply (Применить).

2.3. Обеспечение защиты сервера

Эта функция позволяет обеспечить защиту веб-подключений к консоли и контролировать режим шифрования KVM-протокола, который активируется при использовании консоли удаленной системы (Remote System Console).

1. **Обеспечьте защиту потоков данных**
   1. Во вкладке Configuration (Конфигурация) нажмите Security > Encryption (Безопасность > Шифрование), чтобы открыть страницу Encryption (Шифрование).
   2. Выберите Force HTTPS for Web Access (Использовать HTTPS для веб-доступа) и Force KVM Encryption (Использовать KVM-шифрование) и нажмите Apply (Применить).

2. **Получите и установите новый SSL-сертификат**
   1. Во вкладке Configuration (Конфигурация) нажмите Security > SSL Certificate (Безопасность > SSL-сертификат), чтобы открыть страницу Certificate Signing Request (Запрос подписи сертификата).
   2. Заполните поля и нажмите Create (Создать), чтобы создать CSR.
   3. Нажмите Download (Скачать), чтобы сохранить CSR на компьютер и отправить его органам по сертификации, которые проверят информацию и создадут и вернут подписанный сертификат.
   4. После получения подписанного сертификата используйте пункт Certificate Upload (Загрузка сертификата) для установки сертификата.

3. **Задайте количество одновременных подключений и политику окончания срока действия пароля**
   1. Во вкладке Configuration (Конфигурация) нажмите Security > User Logon Policy (Безопасность > Политика входа пользователей в учетную запись), чтобы открыть страницу User Logon Policy Management (Управление политикой входа пользователей в учетную запись).
   2. Выберите или очистите пункты, как это необходимо, и нажмите Apply (Применить).

4. **Определите максимальное количество попыток входа в учетную запись**
   1. Во вкладке Configuration (Конфигурация) нажмите Security > User Lockout (Безопасность > Запрет доступа пользователя), чтобы открыть страницу User Lockout (Запрет доступа пользователя).
   2. Заполните поля и нажмите Apply (Применить).

5. **Определите режим аутентификации**

1. Во вкладке Configuration (Конфигурация) нажмите Security > Authentication (Безопасность > Аутентификация), чтобы открыть страницу Authentication (Аутентификация).
2. Нажмите Local Authentication (Локальная аутентификация), LDAP или RADIUS, заполните соответствующие поля и нажмите Apply (Применить).

6. **Отключите кнопку питания**
   1. Во вкладке Configuration (Конфигурация) нажмите Security > Power Button Lockout (Безопасность > Блокировка кнопки питания), чтобы открыть страницу Power Button Lockout (Блокировка кнопки питания).
   2. Нажмите Activate Lockout (Активировать блокировку), чтобы отключить кнопку питания.
7. **Измените пароль суперпользователя**
   1. Во вкладке Configuration (Конфигурация) нажмите BMC User Management > Password (BMC-управление пользователями > Пароль), чтобы открыть страницу Password Modification (Изменение пароля).
   2. Заполните 3 поля.
   3. Нажмите Apply (Применить). Новый пароль создан и должен использоваться для следующего входа в учетную запись.

8. **Сохраните параметры**

   Используйте bsmBMCcfg.sh, утилиту для резервного копирования с DVD-диска с файлами и документацией для того, чтобы выполнить резервное копирование системы, PEF и данных конфигурации, если необходимо. Дополнительная информация доступа в документе Remote Hardware Management CLI Reference Guide, 86 A1 36FR.

9. **Остановите SHC**

   Нажмите кнопку Logout (Выйти из учетной записи).

Глава 3. Установка операционной системы (ОС)

3.1. Установка ОС Windows

Установите ОС Windows в соответствии с требованиями заказчика. Соответствующую лицензию можно приобрести в службе поддержки.

3.2. Установка ОС Linux

Установите ОС Linux в соответствии с требованиями заказчика. Соответствующую лицензию можно приобрести в службе поддержки.

Для установки ОС Linux на сервер необходимо соблюсти следующие требования:

- ПК с веб-браузером и Java
- Мин. 25 ГБ свободного объема памяти на сервере.
- Примечание: если сервер оснащен аппаратным RAID и/или оптоволоконным контроллером, доступная емкость должна быть видна в BIOS контроллера
- Мин. 4 Гбит/с RAM на сервере

3.3. Установка ОС VMware ESXi

ОС VMware ESXi уже установлена на сервере.
Загрузите ОС через консоль Remote System Console, выбрав соответствующую опцию загрузки в меню Boot Manager.

Глава 4. Начальная загрузка сервера

1. **Выполните изначальную настройку конфигурации, если она еще не выполнена**

2. **Запустите SHC**
   1. Запустите веб-браузер и введите стандартный или защищенный IP-адрес или имя хоста ведущего модуля в соответствии с настройками. Откроется страница аутентификации.
   2. Заполните поля Username (Имя пользователя) и Password (Пароль) и нажмите Log On (Войти в учетную запись). Откроется страница System Control (Управление системой).

3. Запустите консоль удаленной системы Remote System Console

Во вкладке System Control (Управление системой) нажмите Remote Console > Launch (Удаленная консоль > Запуск). Консоль Remote System Console откроется в новом окне.

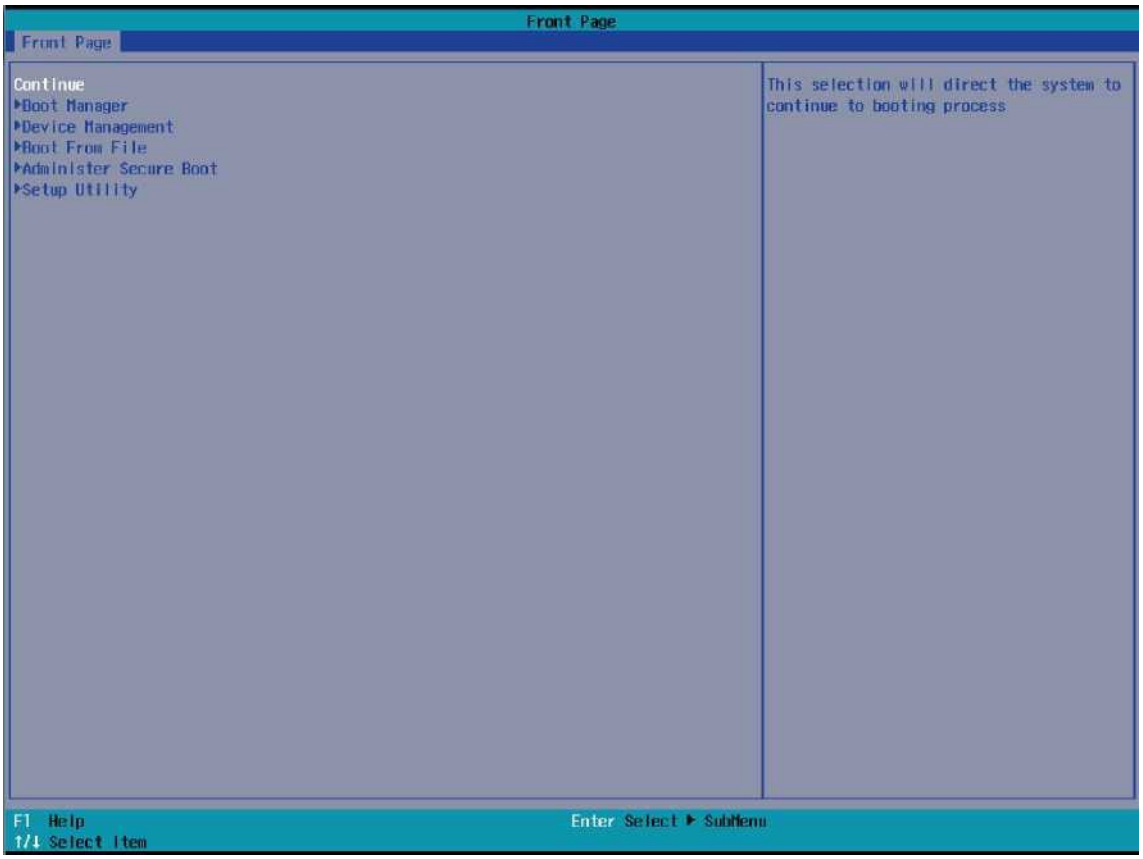
Важно	**Убедитесь, что вы выбрали вариант НЕТ, когда предупреждение системы безопасности Java будет запрашивать о блокировке потенциально опасных компонентов.**

Примечание	В некоторых версиях Java консоль Remote System Console не загружается из-за проверок безопасности Java. В таком случае URL-адрес консоли Remote System Console необходимо добавить в список Exception Site List в панели управления Java.

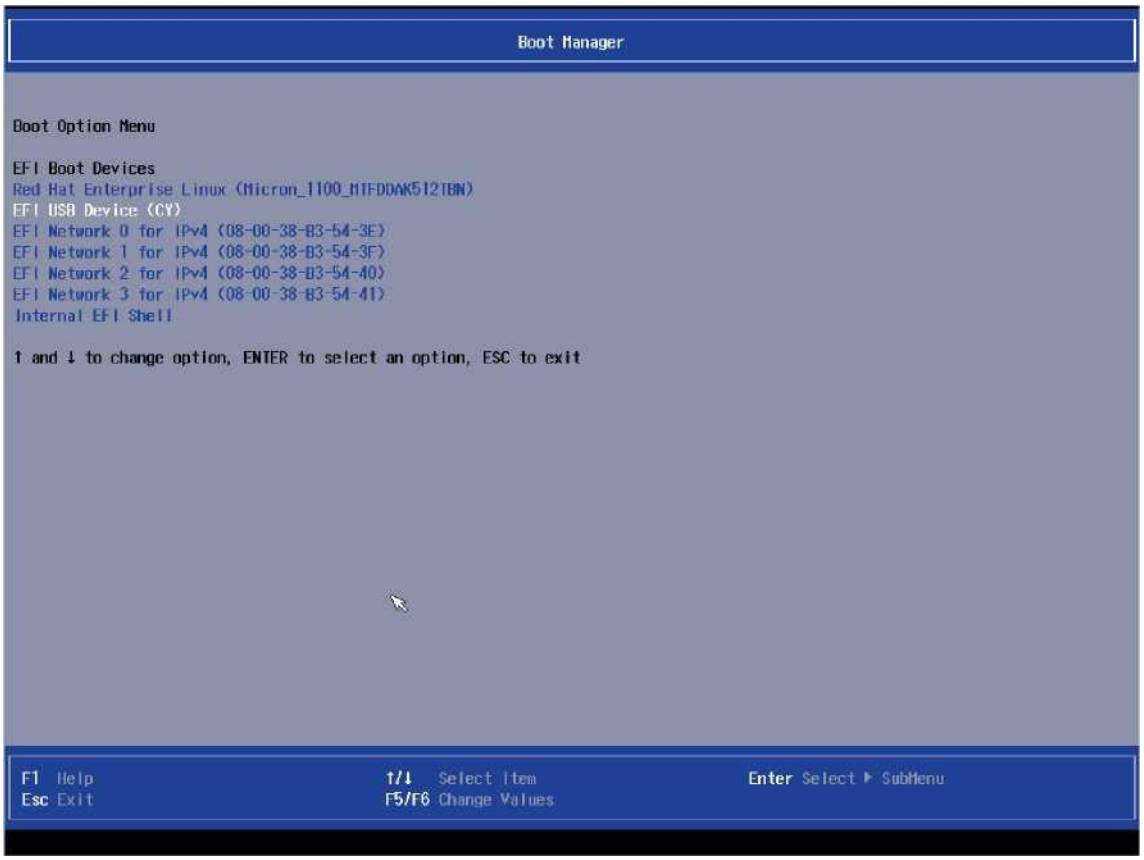
4. **Запуск интерфейса BIOS**
   1. Нажмите Power > Power Management (Питание > Управление питанием), чтобы открыть страницу Power Management (Управление питанием).
   2. Нажмите Power On (Включить питание), чтобы запустить порядок загрузки.
   3. Переключитесь на экран Remote Console (Удаленная консоль).
   4. Нажмите [Esc], когда отобразится сообщение Hit [Esc] для меню Boot Menu.

5. Выберите загрузочное устройство

1. С помощью стрелок навигации выберите Boot Manager (Менеджер загрузки) из основного меню и нажмите [Enter].



2. Выберите необходимое устройство и нажмите [Enter], чтобы выйти из настройки системы и завершить начальную загрузку сервера.



Примечание Изменение загрузочного устройства BIOS также может быть выполнено с помощью bsmBootDevice CLI. См. руководство Remote Hardware Management CLI Reference Guide, 86 A1 19FR для получения дополнительной информации.

Глава 5. Базовые операции

5.1. Отображение базовой информации

5.1.1. Обзор меток Near Field Communication (NFC)

Серверы БС оснащены NFC-метками, по одной для каждого серверного модуля.

Каждая NFC-метка содержит базовую информацию о серверном модуле или разделе.

Уровень информации	Информация	Формат/пример
Модуль	Дата	14:33:23 2017-11-20
	Версия BMC	33.01.0 Build-0155
	Версия BIOS	BIOS_SKL040.38.00.000
	IP-адрес	• 255.255.255.255 • 2001:0db8:85a3:0000:0000:8 a2e:0370:7334
	MAC-адрес	MM:MM:MM:SS:SS:SS
	Система	БС считывается из SYSTEM FRU - FRUID: 0x00
	Серийный номер	K009171C5 считывается из MODULE FRU - FRUID: 0x02
	Состояние загрузки	• BMC Boot • Bios Boot • OS Boot
	Описание BMC	{“M” или “S”}{ModuleId}{PartitionId} M=Master or S=Slave ModuleID 00 to 15 PartitionId 0000 to FFFF
Раздел	Состояние вентилятора	• Normal (Нормальное) • Warning (Предупреждающее) • Critical (Критическое) • Fatal (Фатальное)
	Состояние температуры	
	Состояние напряжения	
	Состояние системы питания	
	Состояние памяти DIMM	

5.1.2. Отображение информации с меток Near Field Communication (NFC)

Примечание Потребуется смартфон на базе Android с поддержкой технологии NFC или считыватель NFC-меток.

1. Разместите устройство с поддержкой технологии NFC напротив Management Board Left Side (MLB) серверного модуля.

2. Через несколько секунд данные NFC-метки будут загружены и отображены на устройстве.

5.2. Выполнение операций сброса

1. **Подключитесь к SHC**

2. **Запустите SHC**
   1. Запустите веб-браузер и введите стандартный или защищенный IP-адрес или имя хоста ведущего модуля в соответствии с настройками. Откроется страница аутентификации.
   2. Заполните поля Username (Пользователь) и Password (Пароль) и нажмите Log On (Войти в учетную запись). Откроется страница System Control (Управление системой).

3. **Выполните операции сброса**
   1. Во вкладке Maintenance (Обслуживание) нажмите Maintenance Operations > Unit Reset (Операции обслуживания > Сброс), чтобы открыть страницу Reset operations (Операции сброса).
   2. Нажмите кнопку Reset (Сброс).

5.3. Проверка контрольных датчиков

1. **Подключитесь к SHC**

2. **Запустите SHC**
   1. Запустите веб-браузер и введите стандартный или защищенный IP-адрес или имя хоста ведущего модуля в соответствии с настройками. Откроется страница аутентификации.
   2. Заполните поля Username (Пользователь) и Password (Пароль) и нажмите Log On (Войти в учетную запись). Откроется страница System Control (Управление системой).

3. **Проверка контрольных датчиков**
   1. Во вкладке Monitoring (Мониторинг) нажмите Sensor Status (Статус датчика), чтобы открыть страницу Sensor Status (Статус датчика).
   2. Во вкладке Module (Модуль) выберите вкладку Functional Unit (Функциональный блок) для отображения значений датчика

См. Руководства в документации для получения дополнительной информации.

5.4. Проверка и очистка журнала системных событий System Event Log (SEL)

1. **Подключитесь к SHC**

2. **Запустите SHC**
   1. Запустите веб-браузер и введите стандартный или защищенный IP-адрес или имя хоста ведущего модуля в соответствии с настройками. Откроется страница аутентификации.
   2. Заполните поля Username (Пользователь) и Password (Пароль) и нажмите Log On (Войти в учетную запись). Откроется страница System Control (Управление системой).

3. **Проверьте и очистите журнал системных событий (SEL)**
   Во вкладке Monitoring (Мониторинг) нажмите System Event Log (Журнал системных событий), чтобы открыть страницу System Event Log (Журнал системных событий).
   Используйте кнопку Refresh (Обновить), чтобы обновить данные в любое время.
   Используйте кнопку Clear (Очистить), чтобы очистить журнал. Записи будут удалены без возможности восстановления.

5.5. Проверка журнала Board and Security Messages Log

1. **Подключитесь к SHC**

2. **Запустите SHC**
   1. Запустите веб-браузер и введите стандартный или защищенный IP-адрес или имя хоста ведущего модуля в соответствии с настройками. Откроется страница аутентификации.
   2. Заполните поля Username (Пользователь) и Password (Пароль) и нажмите Log On (Войти в учетную запись). Откроется страница System Control (Управление системой).

3. **Проверка журнала Board and Security Messages Log**
   1. Во вкладке Monitoring (Мониторинг) нажмите Messages (Сообщения), чтобы открыть страницу Messages (Сообщения).
   2. Ознакомьтесь с сообщениями, если необходимо, используя навигационные стрелки и кнопки с номерами страниц.

Важно Этот журнал может записывать до 2 000 событий. После того, как максимальное количество записей достигнуто, старые сообщения будут автоматически заменяться новыми.

5.6. Получение информации контроллера управления

1. **Подключитесь к SHC**

2. **Запустите SHC**
   1. Запустите веб-браузер и введите стандартный или защищенный IP-адрес или имя хоста ведущего модуля в соответствии с настройками. Откроется страница аутентификации.
   2. Заполните поля Username (Пользователь) и Password (Пароль) и нажмите Log On (Войти в учетную запись). Откроется страница System Control (Управление системой).

3. **Получение информации контроллера управления**

   Во вкладке Maintenance (Обслуживание) нажмите Hardware Information > Management Controller (Информация об аппаратном обеспечении > Контроллер управления), чтобы открыть страницу Management Controller Information (Информация контроллера управления).

5.7. Отображение информации о версии прошивки

1. **Подключитесь к SHC**

2. **Запустите SHC**
   1. Запустите веб-браузер и введите стандартный или защищенный IP-адрес или имя хоста ведущего модуля в соответствии с настройками. Откроется страница аутентификации.
   2. Заполните поля Username (Пользователь) и Password (Пароль) и нажмите Log On (Войти в учетную запись). Откроется страница System Control (Управление системой).

3. **Отображение информации о версии прошивки**

   Во вкладке Maintenance (Обслуживание) нажмите Hardware Information > Firmware Version (Информация об аппаратном обеспечении > Версия прошивки), чтобы открыть страницу Firmware Version (Версия прошивки).

Глава 6. Использование сервера администрирования

6.1. Обзор инструмента администрирования

В соответствии с вашими потребностями различные инструменты администрирования могут быть установлены на сервере администрирования.

Инструмент администрирования	Описание	Установка
iCare	Предоставляет инструменты для контроля и обслуживания аппаратных ресурсов	Рекомендовано
External Adapter for VMware vRops	Предлагает функции управления несколькими серверами для vROps: настраиваемый по времени опрос, контроль рабочих показателей, самовосстановление и ведение журнала	Рекомендовано
VMware vCenter	Предлагает масштабируемую и расширяемую платформу для контроля за виртуальной средой	Опционально

См.

Руководства в документации для получения дополнительной информации.

6.2. Имена пользователей и пароли консоли

В следующей таблице перечислены имена пользователей и пароли по умолчанию для входа в различные консоли управления и администрирования:

	Имя пользователя	Пароль
Консоль Server Hardware Console (SHC)	super	pass
Консоль VMware Sphere Client Console	root	bullion
Консоль VMware Hypervisor Console	root	bullion
Консоль iCare Console	admin	pass

6.3. Порты iCare

iCare использует следующие номера портов в системах Windows и Linux.

См. Руководства по iCare для получения дополнительной информации.

Номера входящих портов

Порт	Служба
80/12080	httpd
162	snmptrapd
5432	сервер PostgreSQL

Номера выходящих портов

Порт	Служба
20/21	FTP
23	telnet
80	HTTP
623	IPMI

6.4. Использование внешнего адаптера для VMware vRops

Внешний адаптер bullion для серверов БС разработан для использования с VMware vRealize Operations Manager (vROps). vROps использует адаптеры для сбора и обработки данных из различных источников данных.

Внешний адаптер bullion собирает данные о рабочих показателях аппаратного обеспечения с одного или нескольких серверов и отправляет их на vROps. Он поддерживает следующие функции:

- Управление несколькими серверами
- Регулируемый по времени опрос
- Контроль соответствующих рабочих показателей
- Самовосстановление и ведение журнала

Рекомендуется установить и сконфигурировать внешний адаптер bullion для простого управления сервером. В документации, предлагаемой к серверу, содержатся инструкции по установке и настройки конфигурации.

6.5. Управление журналами событий с помощью iCare

6.5.1. Запуск консоли iCare

1. Два раза щелкните по иконке консоли iCare, расположенной на рабочем столе, или запустите веб-браузер и введите IP-адрес консоли iCare или хост-имя, после которого будет идти /icare (http://xxx.xxx.xxx.xxx/icare). Откроется страница входа в учетную запись.

Примечание Если IIS включено, порт TCP 80 не будет доступен, и iCare будет использовать порт TCP 12080.
В таком случае необходимо будет добавить номер порта к IP-адресу следующим образом: http://xxx.xxx.xxx.xxx:12080/icare.

2. Заполните поля Username (admin) (Имя пользователя) и Password (pass) Пароль и нажмите Log in (Войти в учетную запись). После аутентификации откроется вкладка Monitoring (Мониторинг).

6.5.2. Создание журналов System Event Logs (SEL)

1. Во вкладке Monitoring (Мониторинг) нажмите SEL Viewer, чтобы открыть страницу System Event Log (SEL) Viewer.
2. В каталоге Resource (Ресурсы) выберите ресурсы, в отношении которых вы хотите отправить запрос в базу данных.
3. Заполните шаблон System Event Log (SEL) Viewer.
4. Для использования существующего шаблона:
   a. Выберите пункт Display Query Template
   b. Из выпадающего списка Template Name (Название шаблона) выберите необходимый шаблон
   c. Нажмите Load (Загрузить)
5. Для создания новой подборки SEL
   a. Выберите Query Options (Опции запроса)
   b. Для сохранения подборки:
   - Нажмите Save Template (Сохранить шаблон)
   - Введите название в поле Template Name (Название шаблона)
   - Если необходимо, введите описание в поле Comment (Комментарии)
6. Нажмите Launch (Запустить). Откроется страница Filtered SEL (Отфильтрованные SEL).

6.5.3. Управление журналами System Event Log (SEL)

iCare предлагает функцию отслеживания событий SEL для каждого контролируемого ресурса. Когда в контролируемом ресурсе происходит событие, оно записывается в журнале System Event Log (SEL) и затем отправляется в базу данных консоли iCare.

Вы можете отправить запрос в базу данных, чтобы просмотреть события, что поможет вам проанализировать выход из строя аппаратного обеспечения или выполнить превентивное техническое обслуживание.

1. Откройте страницу Filtered SEL (Отфильтрованные SEL).
2. Выберите нужный ресурс и нажмите соответствующую кнопку +, чтобы раскрыть список событий SEL.
3. Выберите нужное событие и нажмите соответствующую кнопку +, чтобы раскрыть подробную информацию.
4. Выберите пункты, соответствующие событиям, которыми вы хотите управлять.

Примечание Нажмите ALL (ВСЕ), чтобы выбрать все события из списка.

5. В выпадающем меню Change Event Status (Изменить статус события) выберите новый статус, который вы хотите применить к выбранным событиям:
   - Измените с Received (Полученное) на In review (Пересматриваемое), чтобы указать, что событие находится на рассмотрении
   - Измените с In review (Пересматриваемое) на Concluded (Выполненное), чтобы указать, что событие было рассмотрено и закрыто
6. Заполните поле с комментариями, если это необходимо.
7. Нажмите Apply (Применить).

6.5.4. Создание журналов Board and Security Message Log

Каждый аппаратный ресурс в каталоге ресурсов записывает события. Эти события могут основываться на действиях и ошибках, аутентификации пользователей, подключениях удаленных консолей, нарушениях безопасности, удалениях журналов или обновлениях прошивки.

1. Во вкладке Monitoring (Мониторинг) нажмите Message Viewer (Просмотр сообщений), чтобы открыть страницу Message Viewer (Просмотр сообщений).
2. В каталоге Resource (Ресурсы) выберите ресурсы, в отношении которых вы хотите отправить запрос в базу данных.
3. Если необходимо, заполните поле Date Range (Диапазон дат) для того, чтобы отфильтровать сообщения по датам и времени.
4. Если необходимо, заполните поле Text Search (Поиск текста) для поиска сообщений по ключевым словам. Поиск выполняется без учета регистра и не принимает подстановки.
5. Нажмите Launch (Запустить). Откроется окно Filtered Messages (Отфильтрованные сообщения).

6.5.5. Управление журналами Board and Security Message Log

1. Откройте список сообщений журналов Board and Security Message Log.
2. Выберите необходимый ресурс и нажмите на соответствующую кнопку +, чтобы раскрыть список сообщений.
3. Нажмите на иконку принтера, чтобы распечатать в формате PDF список сообщений для выбранного аппаратного источника.