

Power Systems

*Установка и настройка
консоли аппаратного
обеспечения*



Power Systems

*Установка и настройка
консоли аппаратного
обеспечения*



Примечание

Перед тем, как приступить к работе с этой информацией и описанным в ней продуктом, обязательно ознакомьтесь со сведениями, приведенными в документе “Примечания, касающиеся безопасности” на стр. vii, “Примечания” на стр. 175 и в руководстве *IBM Systems - Информация по технике безопасности*, G229-9054, и *Руководстве пользователя и замечаниям по эксплуатации IBM*, Z125-5823.

Содержание

Примечания, касающиеся безопасности	vii
---	-----

Установка и настройка HMC	1
Новое в книге Установка и настройка HMC	1
Задачи установки и настройки	2
Установка и настройка новой консоли HMC с новым сервером	2
Обновление или модернизация кода HMC	2
Добавление второй HMC в существующую конфигурацию	3
Установка HMC	3
Подключение автономной HMC	4
Установка HMC 7310-CR4 в стойку	5
Инвентаризация компонентов	6
Определение расположения	7
Маркировка расположения без трафарета монтажа в стойке	8
Установка направляющих в стойке	8
Установка HMC на направляющих	11
Установка кабельного кронштейна	13
Подключение смонтированной в стойке HMC	14
Расположения портов HMC	15
Установка 7042-CR5 и 7042-CR6 в стойку	19
Установка 7042-CR7 и 7042-CR8 в стойку	24
Установка HMC 7042-CR9 в стойку	33
Установка 7063-CR1 в стойку	42
Предварительные требования для установки монтируемой в стойке системы 7063-CR1	43
Инвентаризация системы	43
Определение расположения в стойке и его маркировка для системы 7063-CR1	43
Установка HMC в стойку с помощью фиксированных направляющих	44
Присоединение фиксированных направляющих к шасси системы и стойке	45
Установка системы в стойку, подключение и прокладка кабелей питания	46
Установка HMC в стойку с помощью направляющих	47
Присоединение направляющих к системе и стойке	48
Установка системы в стойку, подключение и прокладка кабелей питания	51
Подключение смонтированной в стойке HMC 7063-CR1	52
Настройка HMC 7063-CR1	53
Установка Виртуальное устройство HMC	54
Установка Виртуальное устройство HMC в среде x86	55
Установка Виртуальное устройство HMC с помощью гипервизора KVM	55
Установка Виртуальное устройство HMC с помощью гипервизора Xen	55
Установка Виртуальное устройство HMC с помощью VMware ESXi	56
Установка Виртуальное устройство HMC в PowerVM (логический раздел)	57
Работа со службой активации для Виртуальное устройство HMC	57
Настройка профайла конфигурации для службы активации	58
Установка монитора и клавиатуры	64
Инвентаризация компонентов	66
Маркировка расположения без трафарета монтажа в стойке	66
Установка монитора и клавиатуры в стойку	66
Установка коммутатора консоли (необязательно)	71
Настройка HMC с помощью интерфейса HMC Classic или HMC Enhanced	73
Выбор параметров сети в HMC	73
Сетевые соединения HMC	73
Типы сетевых соединений HMC	73
Выбор способа соединения для сервисного сервера	77
Простые соединения	79
Использование Internet SSL для соединения с удаленным сервисным центром	79
Выбор протокола соединения с Интернетом	80

Списки адресов Internet SSL	80
Использование виртуальной частной сети для соединения с сервисным центром	81
Список адресов серверов VPN	81
Использование телефона и модемов для соединения с удаленным сервисным центром	81
Использование нескольких серверов вызова сервисного центра.	82
Подготовка к настройке НМС	82
Форма настройки НМС перед установкой.	84
Настройка НМС	91
Настройка НМС с помощью быстрого выполнения мастера пошаговой настройки	91
Запуск НМС и выполнение шагов мастера пошаговой настройки	91
Проверка конфигурации	92
Настройка НМС с помощью меню НМС	92
Запуск НМС	93
Изменение даты и времени	94
Настройка типов сетей НМС	94
Изменение параметров брандмауэра НМС	100
Настройка записи маршрутизации в качестве стандартного шлюза	101
Настройка служб имен доменов	101
Настройка доменных суффиксов	102
Настройка НМС для использования удаленной идентификации с помощью LDAP	102
Настройка НМС для использования Центров рассылки ключей (KDC) для удаленной идентификации Kerberos	102
Настройка НМС для связи с сервисным центром и службой поддержки.	103
Настройка Администратора событий для вызова сервисного центра	108
Задание паролей для управляемой системы	109
Проверка соединения между НМС и управляемой системой	110
Действия после настройки	110
Резервное копирование наиболее важных данных НМС	110
Создание полной резервной копии жесткого диска НМС в удаленной системе.	111
Обновление, модернизация и миграция машинного кода НМС	112
Определение версии и выпуска машинного кода НМС	112
Получение и применение обновлений машинного кода для НМС через Internet-соединение	113
Шаг 1. Убедитесь в наличии соединения с Internet	113
Шаг 2. Просмотр текущего уровня машинного кода НМС	113
Шаг 3. Просмотр доступных уровней машинного кода НМС	113
Шаг 4. Применение обновления машинного кода НМС	114
Шаг 5. Проверка правильности установки обновления машинного кода НМС	114
Получение и применение обновлений машинного кода для НМС на DVD или через сервер FTP	114
Шаг 1. Просмотр текущего уровня машинного кода НМС	114
Шаг 2. Просмотр доступных уровней машинного кода НМС	114
Шаг 3. Получение обновления машинного кода НМС	114
Шаг 4. Применение обновления машинного кода НМС	115
Шаг 5. Проверка правильности установки обновления машинного кода НМС	115
Модернизация программного обеспечения НМС	115
Шаг 1. Получение модернизации	116
Шаг 2. Просмотр текущего уровня машинного кода НМС	116
Шаг 3. Создание резервной копии данных профайла управляемой системы	116
Шаг 4. Резервное копирование данных НМС	116
Шаг 5. Запись информации о текущей конфигурации НМС	117
Шаг 6. Запись состояния удаленной команды	117
Шаг 7. Сохранение данных модернизации	118
Шаг 8. Модернизация программного обеспечения НМС.	118
Шаг 9. Проверка правильности установки модернизации машинного кода НМС.	118
Обновление НМС из удаленного расположения с помощью образов сетевого обновления.	119
Настройка НМС с помощью интерфейса НМС Enhanced+	119
Выбор параметров сети в НМС.	120
Сетевые соединения НМС	120
Типы сетевых соединений НМС	120
Выбор способа соединения для сервисного сервера	124
Использование Internet SSL для соединения с удаленным сервисным центром	126
Выбор протокола соединения с Интернетом	126

Списки адресов Internet SSL	126
Использование виртуальной частной сети для соединения с сервисным центром	127
Список адресов серверов VPN	128
Использование телефона и модемов для соединения с удаленным сервисным центром	128
Использование нескольких серверов вызова сервисного центра	128
Подготовка к настройке НМС	129
Форма настройки НМС перед установкой	130
Настройка НМС	137
Настройка НМС с помощью быстрого выполнения мастера пошаговой настройки	137
Запуск НМС и выполнение шагов мастера пошаговой настройки	137
Проверка конфигурации	138
Настройка НМС с помощью меню НМС	138
Запуск НМС	139
Изменение даты и времени	140
Настройка типов сетей НМС	141
Изменение параметров брандмауэра НМС	147
Настройка записи маршрутизации в качестве стандартного шлюза	148
Настройка служб имен доменов	149
Настройка доменных суффиксов	149
Настройка НМС для использования удаленной идентификации с помощью LDAP	149
Настройка НМС для использования Центров рассылки ключей (KDC) для удаленной идентификации Kerberos	150
Настройка локальной консоли для отправки сервисному центру сообщений об ошибках	151
Настройка Администратора событий для вызова сервисного центра	157
Задание паролей для управляемой системы	158
Проверка соединения между НМС и управляемой системой	159
Действия после настройки	159
Резервное копирование наиболее важных данных НМС	159
Создание полной резервной копии жесткого диска НМС в удаленной системе	160
Обновление, модернизация и миграция машинного кода НМС	161
Определение версии и выпуска машинного кода НМС	162
Получение и применение обновлений машинного кода для НМС через Internet-соединение	162
Шаг 1. Убедитесь в наличии соединения с Internet	162
Шаг 2. Просмотр текущего уровня машинного кода НМС	163
Шаг 3. Просмотр доступных уровней машинного кода НМС	163
Шаг 4. Применение обновления машинного кода НМС	163
Шаг 5. Проверка правильности установки обновления машинного кода НМС	163
Получение и применение обновлений машинного кода для НМС на DVD или через сервер FTP	164
Шаг 1. Просмотр текущего уровня машинного кода НМС	164
Шаг 2. Просмотр доступных уровней машинного кода НМС	164
Шаг 3. Получение обновления машинного кода НМС	164
Шаг 4. Применение обновления машинного кода НМС	165
Шаг 5. Проверка правильности установки обновления машинного кода НМС	165
Модернизация программного обеспечения НМС	166
Шаг 1. Получение модернизации	166
Шаг 2. Просмотр текущего уровня машинного кода НМС	166
Шаг 3. Создание резервной копии данных профайла управляемой системы	166
Шаг 4. Резервное копирование данных НМС	166
Шаг 5. Запись информации о текущей конфигурации НМС	167
Шаг 6. Запись состояния удаленной команды	168
Шаг 7. Сохранение данных модернизации	168
Шаг 8. Модернизация программного обеспечения НМС	168
Шаг 9. Проверка правильности установки модернизации машинного кода НМС	169
Обновление НМС из удаленного расположения с помощью образов сетевого обновления	169
Расположения портов НМС	170
Примечания.	175
Специальные возможности серверов IBM Power Systems	176
Замечания о правилах работы с личными данными	177
Товарные знаки.	178
Замечания об уровне электронного излучения	178

Информация о классе А	178
Информация о классе В	182
Положения и условия	185

Примечания, касающиеся безопасности

В настоящем руководстве используются следующие замечания по технике безопасности:

- **ОПАСНО** - это замечание касается ситуаций, создающих угрозу жизни или здоровью человека.
- **ОСТОРОЖНО** - это замечание касается потенциально опасных аварийных ситуаций.
- **Внимание** - это замечание касается ситуаций, создающих угрозу повреждения программы, устройства, системы или данных.

Информация о безопасности международной торговли

В некоторых странах действует требование, согласно которому информация по технике безопасности, приводимая в документации к продукту, должна быть доступна на государственном языке данной страны. Если это требование применимо для вашей страны, пакет документов, поставляемый вместе с продуктом (например печатная документация, документация на диске DVD или в составе продукта), будет содержать документацию по технике безопасности. Эта документация содержит информацию о безопасности на государственном языке вашей страны со ссылками на источник на английском языке (США). Перед началом установки, использования или обслуживания данного продукта следует ознакомиться с информацией по технике безопасности, приведенной в этой документации. В случае возникновения каких-либо сомнений в отношении информации по технике безопасности, приведенной в английской документации, вы также можете обратиться к этой документации.

Для замены или получения дополнительных копий документации по технике безопасности обратитесь по телефону горячей линии IBM: 1-800-300-8751.

Информация о безопасности для Германии

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

Техника безопасности при работе с лазером

Серверы IBM® могут использовать карты ввода-вывода или компоненты на основе оптоволоконных соединений, в которых применяются лазеры или светодиоды.

Требования к лазерам

Серверы IBM можно устанавливать внутри стойки или за ее пределами.

ОПАСНО: При работе с системой или вблизи нее соблюдайте следующие меры предосторожности:

Ток электрических, телефонных и коммуникационных кабелей представляет опасность для человека. Для того чтобы избежать поражения током, выполняйте следующие рекомендации:

- Если в комплект поставки IBM входят кабели питания, для подключения данного блока к электропитанию используйте только имеющийся в комплекте поставки кабель IBM. Не используйте эти кабели для других продуктов.
- Не открывайте и не пытайтесь отремонтировать блок питания.
- Не подключайте и не отключайте кабели и не проводите установку или обслуживание продукта при неполадках в электрической сети.
- Продукт может быть оборудован несколькими силовыми кабелями. Во избежание поражения электрическим током отключайте все силовые кабели.
 - В случае питания от сети переменного тока отключите все кабели питания от источника питания.

- Для стоек с панелью распределения питания (PDP) постоянного тока отключите источник питания, предоставляемый заказчиком, от PDP.
- При подключении питания к продукту убедитесь, что все кабели питания подсоединены правильным образом.
 - Для стоек с питанием переменного тока все кабели питания включайте в правильно подсоединенные и заземленные электрические розетки. Убедитесь, что напряжение и чередование фаз розетки отвечает заданным требованиям.
 - Для стоек с панелью распределения питания (PDP) постоянного тока подключите источник питания, предоставляемый заказчиком, к PDP. Проверьте полярность при подключении питания постоянного тока и проводов возврата питания.
- Устройства, которые соединены с этим продуктом, должны быть подключены к правильно установленным розеткам.
- При возможности отключение и подключение сигнальных кабелей следует производить одной рукой.
- Никогда не включайте оборудование при пожаре, наводнении и повреждении здания.
- Не пытайтесь включить систему до тех пор, пока не будут выполнены все требования техники безопасности.
- Предполагайте наличие опасности поражения электрическим током. Выполните все проверки целостности, заземления и питания в ходе установки подсистемы, чтобы обеспечить соответствие системы всем требованиям техники безопасности.
- Не продолжайте проверку в случае обнаружения неисправностей.
- Перед открытием крышек устройства, если обратное не указано в инструкциях по установке и настройке: отключите кабели питания переменного тока, выключите прерыватели, расположенные на панели распределения питания (PDP), и отключите все телекоммуникационные системы, сети и модемы.

ОПАСНО:

- Подключение и отключение кабелей при установке, перемещении или снятии крышек продукта или подключенного к нему устройства должно проводиться в соответствии со следующими инструкциями.

Отключение:

1. Выключите все устройства (если иное не оговорено в инструкциях).
2. В случае питания от сети переменного тока отсоедините кабели питания из розеток.
3. Для стоек с панелью распределения питания (PDP) выключите прерыватели, расположенные на PDP, и отключите источник питания постоянного тока, предоставленный заказчиком.
4. Выньте сигнальные кабели из разъемов.
5. Отсоедините все кабели от устройств.

Подключение:

1. Выключите все устройства (если иное не оговорено в инструкциях).
2. Подсоедините все кабели к устройствам.
3. Подключите сигнальные кабели к разъемам.
4. В случае питания от сети переменного тока подсоедините кабели питания к розеткам.
5. Для стоек с панелью распределения питания (PDP) постоянного тока включите источник питания, предоставляемый заказчиком, и включите прерыватели, расположенные на PDP.
6. Включите устройства.

В системе или ее окрестности могут быть острые края, углы и стыки. Проявляйте осторожность при перемещении оборудования, чтобы избежать порезов, царапин и прочих травм. (D005)

(R001 - часть 1 из 2):

ОПАСНО: При работе возле системы ИТ-стоек или с самой системой соблюдайте следующие меры предосторожности:

- Неправильное обращение с тяжелым оборудованием может привести к травмированию персонала или повреждению оборудования.
- Всегда опускайте выравнивающие опоры стойки.
- Всегда устанавливайте стабилизирующие скобы стойки.

- Для обеспечения устойчивости стойки размещайте самые тяжелые устройства в нижней части стойки. Заполнение стойки устройствами всегда следует начинать снизу.
- Устройства для монтирования в стойке нельзя использовать в качестве полок или рабочего пространства. Не размещайте предметы на поверхности смонтированных в стойку устройств. Кроме того, не облокачивайтесь на смонтированные в стойке устройства и не используйте их для опоры (например, работая на лестнице).



- У устройств, монтируемых в стойке, может быть несколько силовых кабелей.
 - Если требуется отключить питание при обслуживании стойки, работающей от сети переменного тока, убедитесь, что отсоединены все кабели питания.
 - Для стоек с панелью распределения питания (PDP) постоянного тока выключите прерыватель цепи питания системных блоков или отключите источник питания, предоставляемый заказчиком, если обслуживание предусматривает отключение питания.
- Все устройства, монтируемые в стойке, должны быть подключены к устройствам питания этой же стойки. Не подключайте устройства из одной стойки к источнику питания из другой стойки.
- При подключении устройства к неправильно установленной электрической розетке на металлические части устройства может быть подан ток опасного напряжения. Потребитель должен убедиться, что розетка установлена и заземлена должным образом.

(R001 - часть 2 из 2):

ОСТОРОЖНО:

- Нельзя устанавливать блок в стойку, температура внутри которой превышает рекомендованную производителем рабочую температуру для монтируемых в стойке устройств.
- Нельзя устанавливать блок в стойку с нарушенной вентиляцией. Убедитесь, что воздух может беспрепятственно охлаждать устанавливаемый блок.
- При подключении оборудования к сети электропитания следует учитывать мощность цепи питания, чтобы перегрузка не привела к повреждению проводки или срабатыванию токовой защиты. Для вычисления требований к мощности цепи питания стойки обратитесь к сведениям о параметрах энергопотребления, указанным на этикетках, прикрепленных к установленному в стойке оборудованию.
- *(Для выдвижных ящиков.)* Не выдвигайте ящики и не монтируйте в стойке устройства, если на стойке не установлены стабилизирующие скобы. Выдвигайте блоки по одному. Это может нарушить равновесие стойки.



- *(Для закрепленных ящиков.)* Этот ящик является закрепленным и не может выдвигаться для обслуживания, если это не указано производителем. Попытка полностью или частично выдвинуть такой ящик может нарушить равновесие стойки или привести к выпадению ящика.

ОСТОРОЖНО:

Чем ниже находится центр тяжести стойки, тем она устойчивее. При перемещении заполненной стойки в пределах помещения или здания выполняйте следующие общие указания.

- Удалите устройства из верхней части стойки, чтобы уменьшить ее массу. При возможности оставьте в ней только те компоненты, которые она содержала изначально. Если эти компоненты неизвестны, соблюдайте следующие меры предосторожности:
 - Удалите все устройства в отсеках 32U (ИД соответствия RACK-001 или 22U (ИД соответствия RR001) и выше.
 - Убедитесь, что самые тяжелые устройства находятся в нижней части стойки.
 - Убедитесь, что стойка не содержит пустых отсеков, расположенных ниже уровня 32U (ИД соответствия RACK-001) или 22U (ИД соответствия RR001), если это не разрешено полученной конфигурацией.
- Если стойка прикреплена к другим стойкам, отсоедините ее.
- Если перемещаемая стойка оснащена съемными боковыми опорами, то их необходимо установить перед перемещением стойки.
- Расчистите предполагаемый путь.
- Убедитесь, что предполагаемый путь пригоден для массы стойки. Масса стойки приведена в документации по ней.
- Убедитесь, что размер дверных проемов не меньше 760 x 230 мм (30 x 80 дюймов).
- Убедитесь, что все устройства, полки, блоки накопителей и кабели закреплены.
- Убедитесь, что выравнивающие опоры находятся в наивысшем положении.
- Убедитесь, что скоба стабилизатора извлечена из стойки.
- Не наклоняйте стойку более чем на десять градусов.
- Переместив стойку, выполните следующие действия:
 - Опустите выравнивающие опоры.
 - Установите скобу стабилизатора в стойку.
 - Если перед перемещением вы извлекали устройства из стойки, установите их снова, начиная с нижней части стойки.
- Если требуется перемещение стойки на большое расстояние, восстановите первоначальное состояние стойки. Поместите стойку в исходный упаковочный материал или аналогичный ему. Опустите выравнивающие опоры, чтобы поставить поддон на ролики и прикрепить стойку к поддону.

(R002)

(L001)



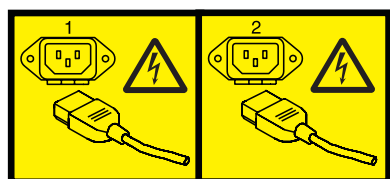
ОПАСНО: Эта метка указывает на компоненты с опасным напряжением или током. Не открывайте крышки, на которых размещена эта метка. (L001)

(L002)



ОПАСНО: Устройства для монтирования в стойке нельзя использовать в качестве полок или рабочего пространства. (L002)

(L003)



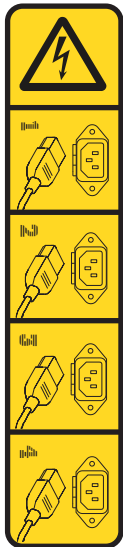
или



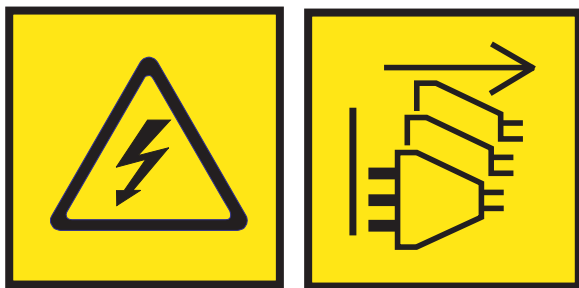
или



или



или



ОПАСНО: Несколько кабелей питания. Продукт может быть оснащено несколькими кабелями питания переменного и постоянного тока. Для обеспечения отсутствия опасных напряжений отсоединяйте все кабели питания. (L003)

(L007)



ОСТОРОЖНО: Горячая поверхность рядом. (L007)

(L008)



ОСТОРОЖНО: Опасные подвижные детали. (L008)

Все лазеры сертифицированы в США как продукты класса 1 и подчиняются требованиям, перечисленным в Постановлении 21 CFR, Подраздел J, Департамента здравоохранения и медицинских услуг (DHHS). В других странах они сертифицированы как продукты класса 1 и подчиняются требованиям, перечисленным в Стандарте 60825 Международной электротехнической комиссии (IEC). Все компоненты имеют маркировку, содержащую сертификационный номер лазера и контрольную информацию.

ОСТОРОЖНО:

Продукт может содержать одно или несколько из следующих устройств: дисковод CD-ROM, дисковод DVD-ROM, дисковод DVD-RAM или лазерный модуль. Эти устройства относятся к лазерным продуктам класса 1. Учтите следующее:

- Не снимайте крышки. В результате снятия крышек с лазерных продуктов возникает угроза лазерного излучения. Устройство не содержит компонентов, которые может обслуживать пользователь.
- Использование сторонних приспособлений или нарушение указанных инструкций может привести к опасному радиационному облучению.

(C026)

ОСТОРОЖНО:

Система обработки данных содержит оборудование, соединенное с лазерными устройствами класса уровня мощности выше 1. Запрещается заглядывать в волоконно-оптический кабель и открывать гнезда. Несмотря на то, что волоконно-оптический кабель можно проверить, подсветив его с одной стороны и заглянув с другой, такая процедура может быть опасной для глаз. Таким образом, такой способ проверки волоконно-оптических кабелей не рекомендуется. Для проверки волоконно-оптического кабеля следует использовать источник света и измеритель мощности. (C027)

ОСТОРОЖНО:

Продукт содержит лазер класса 1M. Не следует рассматривать его с помощью оптических устройств. (C028)

ОСТОРОЖНО:

В некоторые лазерные устройства встроен лазерный диод класса 3A или 3B. Учтите следующее: при открытии корпуса распространяется лазерное излучение. Не допускайте попадания луча в глаза, не рассматривайте луч с помощью оптических устройств и избегайте прямого контакта с лучом. (C030)

ОСТОРОЖНО:

Батареи содержат литий. Во избежание взрыва, батарею запрещается нагревать или перезаряжать.

Запрещается:

- ____ бросать или погружать батарею в воду
- ____ нагревать более чем до 100°C (212°F)
- ____ ремонтировать или разбирать батарею

Замена батарей допускается только на батареи разрешенного фирмой IBM типа. Уничтожение или переработка батарей должны производиться в соответствии с местными правилами. В США существует сеть отделений фирмы IBM, занимающихся сбором отслуживших свой срок батарей. Дополнительную информацию вы можете узнать по телефону 1-800-426-4333. При этом сообщите номер изделия, указанный на корпусе батареи. (C003)

ОСТОРОЖНО:

Предупреждение относительно предоставленного IBM подъемника производителя:

- Работа с ПОДЪЕМНИКОМ разрешена только специальному персоналу.
- Подъемный инструмент предназначен для работы с верхними отсеками стоек (подъем, установка и удаление блоков (нагрузки)). Он не должен использоваться под нагрузкой при транспортировке по главным пандусам, а также в качестве замены таким инструментам как подъемные транспортные платформы, вилочные погрузчики и другие средства для подобных операций. Когда это не осуществимо, необходимо использовать специально обученных лиц (например, такелажники или переносчики).
- Перед началом работы необходимо прочитать руководство оператора подъемного инструмента. Если не прочитать, не понять, не соблюдать правила безопасности и не следовать инструкциям, что это может привести повреждению имущества и/или собственной травме. При наличии вопросов обратитесь в службу поддержки производителя. Бумажная копия руководства должна находиться вместе с системой в выделенной для этого области. Последнее издание руководства доступно на веб-сайте производителя.
- Проверяйте функционирование тормоза стабилизатора перед каждым использованием. Не перенагружайте движущийся или вращающийся ПОДЪЕМНИК тормозом стабилизатора.
- Не перемещайте подъемный инструмент с поднятой платформой за исключением незначительных смещений при позиционировании.
- Не превышайте номинальную грузоподъемность. В Таблице грузоподъемности приведены максимальные нагрузки на центр и на край расширенной платформы.
- Выполняйте подъем только при правильном центрировании на платформе. Не размещайте более 200 фунтов (91 кг) на краю скользящего выступа платформы, учитывая также центр тяжести (CoG) нагрузки.
- Избегайте угловой нагрузки наклонной подставки. Перед использованием закрепите приспособление для изменения угла наклона платформы на главной плоскости во всех четырех положениях только с помощью специального оборудования. Грузы должны сдвигаться на ровные платформы и с них без существенного усилия, поэтому не следует давить или наклонять. Держите приспособление для изменения угла наклона платформы ровно во всех случаях, кроме окончательной незначительной корректировки.
- Не стойте под нависающим грузом.
- Не работайте на неровной поверхности (с наклоном), такой как пандусы.
- Не складывайте грузы друг на друга.
- Не работайте под действием алкоголя или наркотиков.
- Не ставьте лестницу рядом с ПОДЪЕМНИКОМ.
- Есть риск опрокидывания. Не давите на грузы и не наклоняйте их при поднятой платформе.
- Не используйте в качестве лифта или ступеньки для себя. Не ездите на нем.
- Не становитесь ни на какую часть подъемника.
- Не лезьте на мачту.
- Не работайте с поврежденным или неисправным ПОДЪЕМНИКОМ.
- Существует риск защемления под платформой. Опускайте груз только в области, свободные от персонала и препятствий. Держите руки и ноги открытыми в процессе выполнения операций.
- Никаких вилочных устройств. Никогда не поднимайте и не перемещайте пустой ПОДЪЕМНИК с помощью тележки с поддонами, домкрата или вилочного погрузчика.
- Мачта возвышается над платформой. Учитывайте высоту потолка, кабельные лотки, противопожарные спринклеры, осветительные приборы и другие объекты наверху.
- Не оставляйте ПОДЪЕМНИК с поднятым грузом без присмотра.
- Наблюдайте и сохраняйте руки, пальцы и одежду открытыми при движении оборудования.
- Поворачивайте ворот только с помощью ручного привода. Если рукоятку ворота не получается легко повернуть одной рукой, значит она перегружена. Не продолжайте поворачивать ворот после перемещения платформы в нижнее или верхнее положение. Чрезмерное раскручивание приведет к отсоединению рукоятки или повреждению кабеля. Всегда придерживайте рукоятку при опускании, раскручивании. Всегда убеждайтесь в том, что ворот удерживает груз, перед тем как отпустить рукоятку.
- Авария ворота может вызвать серьезную травму. Он не предназначен для перемещения людей. При подъеме оборудования должен ясно слышаться звук щелчков. Перед тем как отпустить рукоятку, убедитесь в том, что ворот заблокирован. Перед работой с этим воротом прочитайте инструкции. Никогда не допускайте свободного раскручивания. Свободное вращение вызовет неравномерное наматывание кабеля вокруг барабана ворота, повреждение кабеля и может привести к серьезным травмам. (C048)

Информация по электропитанию и кабельному соединению для NEBS (Network

Equipment-Building System) GR-1089-CORE

Следующие комментарии относятся к серверам IBM, официально соответствующим требованиям NEBS (Network Equipment-Building System) GR-1089-CORE:

Оборудование пригодно для установки в следующих частях:

- оборудование сетевой телекоммуникации
- места расположения, соответствующие правилам NEC (National Electrical Code)

Предназначенные для работы внутри помещений порты данного оборудования пригодны только для соединения с расположенными в помещениях (или укрытиях) проводами или кабелями. Эти предназначенные для работы внутри помещений порты данного оборудования *не должны* быть подсоединены металлическим способом к интерфейсам, соединенным с внешней установкой OSP или с ее проводами. Эти интерфейсы предназначены для использования только внутри помещений (порты типа 2 и типа 4, согласно описанию в GR-1089-CORE) и должны быть изолированы от открытых кабелей внешней установки OSP. Дополнительная установка основных фильтров не является достаточной защитой при подключении этих интерфейсов к проводке OSP металлическим способом.

Примечание: Все кабели Ethernet должны быть экранированы и заземлены с обоих концов.

Если система работает на переменном токе, использовать внешний фильтр защиты от перенапряжения (SPD) нет необходимости.

Система, работающая на постоянном токе, задействует механизм изолированного обратного провода (DC-I). Возвратная клемма аккумулятора постоянного тока *не должна* соединяться с проводом заземления корпуса или каркаса.

Если система работает на постоянном токе, то ее следует установить в сети с общим заземлением (CBN) (см. GR-1089-CORE).

Установка и настройка НМС

Приведены инструкции по установке аппаратного обеспечения НМС (Консоль аппаратного обеспечения) подключению его к управляемой системе и настройке для использования. Рассмотренные задачи можно выполнить самостоятельно или обратиться за помощью в сервисный центр. В последнем случае услуга может оказаться платной.

Примечание: Виртуализация не поддерживается на сервере IBM Power System S824L (8247-42L).

Новое в книге Установка и настройка НМС

Новая или существенно измененная с предыдущего издания информация по установке и настройке НМС.

Август 2017 года

- Начиная с версии 8.7.0, консоль аппаратного обеспечения (НМС) не поддерживает интерфейс НМС Classic. Функции, которые были ранее были доступны в интерфейсе с НМС Classic, теперь можно выполнить с помощью интерфейса НМС Enhanced+.
- Добавлены следующие разделы:
 - “Установка 7063-CR1 в стойку” на стр. 42
 - “Настройка связи BMC” на стр. 146
- Добавлен раздел “Установка 7063-CR1 в стойку” на стр. 42.

Октябрь 2016 года

- Обновлен раздел “Расположения портов НМС” на стр. 15.

Май 2016 года

- Добавлен раздел “Установка НМС 7042-CR9 в стойку” на стр. 33.

Октябрь 2015

- Добавлен раздел “Установка Виртуальное устройство НМС” на стр. 54.
- Обновлены следующие разделы:
 - “Списки адресов Internet SSL” на стр. 80
 - “Подготовка к настройке НМС” на стр. 82

Июнь 2015 года

- Процедуры и функции интерфейса НМС Enhanced + Tech Preview (предварительная версия), предоставлявшиеся в НМС версии 8.2.0, совпадают с функциями интерфейса НМС Enhanced+, предоставленного в НМС версии 8.3.0. В документации называется только НМС Enhanced+, но данные материалы относятся также и к интерфейсу НМС Enhanced + Tech Preview (предварительная версия).
- Процедуры и функции интерфейса НМС Enhanced, предоставлявшиеся в НМС версии 8.2.0, теперь входят в состав интерфейса НМС Enhanced+, предоставленного в НМС версии 8.3.0.
- Добавлен раздел “Настройка НМС с помощью интерфейса НМС Enhanced+” на стр. 119.
- Обновлен раздел “Настройка Администратора событий для вызова сервисного центра” на стр. 108.

Октябрь 2014 года

- Добавлены следующие разделы:
 - “Установка 7042-CR7 и 7042-CR8 в стойку” на стр. 24
 - “Настройка Администратора событий для вызова сервисного центра” на стр. 108

- Обновлен раздел “Запуск НМС” на стр. 93.

Июнь 2014

- Добавлена информация для серверов IBM Power Systems с процессором POWER8.

Задачи установки и настройки

Рассмотрены задачи, связанные с различными задачами установки и настройки НМС.

В этом разделе приведено общее описание задач, выполняемых в ходе установки и настройки НМС. НМС можно установить и настроить различными способами. Выберите ситуацию, наилучшим образом соответствующую выполняемой задаче.

Примечание: Для переноса серверов с процессорами POWER8 требуется НМС версии 8.1.0. Дополнительные сведения содержатся в разделе “Определение версии и выпуска машинного кода НМС” на стр. 112.

Установка и настройка новой консоли НМС с новым сервером

Общее описание задач, выполняемых в случае установки и настройки новой НМС с новым сервером.

Таблица 1. Задачи, выполняемые в случае установки и настройки новой НМС с новым сервером

Задача	Где искать связанную информацию
1. Соберите информацию и заполните справочную таблицу по подготовке к установке.	“Форма настройки НМС перед установкой” на стр. 84 “Подготовка к настройке НМС” на стр. 82
2. Извлеките аппаратное обеспечение из упаковки.	
3. Подсоедините к НМС необходимые кабели.	“Подключение автономной НМС” на стр. 4 “Подключение смонтированной в стойке НМС” на стр. 14
4. Включите НМС, нажав кнопку питания.	
5. Войдите в НМС и запустите веб-приложение.	
6. Настройте НМС с помощью меню или мастера пошаговой настройки.	“Настройка НМС с помощью быстрого выполнения мастера пошаговой настройки” на стр. 91 “Настройка НМС с помощью меню НМС” на стр. 92
7. Подключите сервер к НМС.	

Обновление или модернизация кода НМС

Общее описание задач, выполняемых в случае обновления или модернизации кода НМС.

В ходе обновления или модернизации кода существующей НМС необходимо выполнить следующие задачи:

Таблица 2. Задачи, выполняемые в случае обновления или модернизации кода НМС

Задача	Где искать связанную информацию
1. Получите обновление.	“Модернизация программного обеспечения НМС” на стр. 115
2. Просмотрите текущий уровень машинного кода НМС.	
3. Создайте резервную копию данных профайла управляемой системы.	
4. Создайте резервную копию данных НМС.	
5. Запишите информацию о текущей конфигурации НМС.	
6. Запишите состояние удаленной команды.	
7. Сохраните данные модернизации.	
8. Обновите программное обеспечение НМС.	
9. Проверьте правильность установки модернизации машинного кода НМС	

Добавление второй НМС в существующую конфигурацию

Общее описание задач, выполняемых в случае добавления второй НМС в конфигурацию управляемой системы.

В случае добавления второй НМС в существующую конфигурацию необходимо выполнить следующие задачи:

Таблица 3. Задачи, выполняемые в случае добавления второй НМС в существующую конфигурацию

Задача	Где искать связанную информацию
1. Убедитесь, что аппаратное обеспечение НМС поддерживает код НМС версии 7.	
2. Соберите информацию и заполните справочную таблицу по подготовке к установке.	“Форма настройки НМС перед установкой” на стр. 84
3. Извлеките аппаратное обеспечение из упаковки.	
4. Подсоедините к НМС необходимые кабели.	“Подключение автономной НМС” на стр. 4 “Подключение смонтированной в стойке НМС” на стр. 14
5. Включите НМС, нажав кнопку питания.	
6. Войдите в систему НМС.	
7. Уровни версий НМС должны совпадать. Измените уровень одной НМС, чтобы он соответствовал уровню другой.	“Определение версии и выпуска машинного кода НМС” на стр. 112 “Модернизация программного обеспечения НМС” на стр. 115
8. Настройте НМС с помощью меню или мастера пошаговой настройки.	“Настройка НМС с помощью меню НМС” на стр. 92
9. Настройте НМС для обслуживания с помощью мастера Настройка вызова сервисного центра.	“Настройка НМС для связи с сервисным центром и службой поддержки” на стр. 103
10. Подключите сервер к НМС.	

Установка НМС

Перед настройкой программного обеспечения НМС необходимо установить аппаратное обеспечение НМС. Здесь описывается установка панельной НМС или устанавливаемой в стойку НМС.

Подключение автономной НМС

Размещение НМС и подключение всех компонентов аппаратного обеспечения.

Автономную НМС с управляемой системой можно соединить с помощью кабеля.

1. Проверьте правильность расположения НМС.
2. Вставьте кабель монитора в разъем на мониторе и затяните винты.
3. Подключите кабель питания к монитору.
4. Проверьте, соответствует ли положение переключателя напряжения на НМС напряжению сети в вашем регионе. Переключатель напряжения находится рядом с разъемом питания, цвет - красный. Переведите переключатель в положение, соответствующее напряжению в вашем регионе.
5. Вставьте кабель питания в НМС.
6. Подключите клавиатуру и мышь к НМС.
7. Подключите модем:

Примечание: В процессе установки и настройки НМС модем должен автоматически выйти во внешнюю линию, когда НМС будут выполняться стандартные процедуры отправки вызовов. Так и должно быть.

Для подключения дополнительного внешнего модема выполните следующие действия:

Примечание: Информацию об ошибках можно отправлять компании IBM с помощью других способов соединения.

- a. Если этого еще не сделано, подключите кабель данных модема к внешнему модему НМС.
- b. Подключите кабель данных модема к системному порту на НМС, помеченному символом:



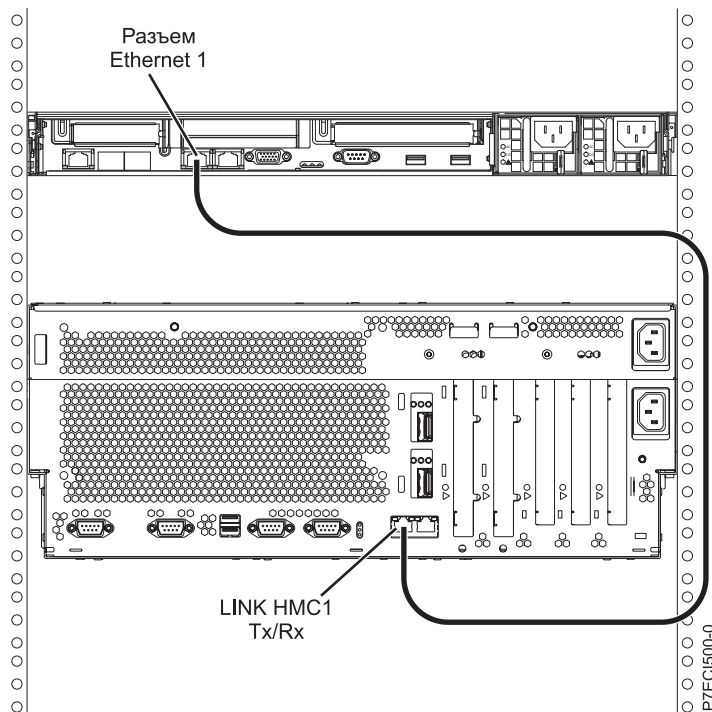
IPNA522-0

- c. Подключите линейный порт внешнего модема к аналоговому телефонному гнезду на стене через телефонный кабель.

При подключении к дополнительному встроенному модему используйте кабель данных для подключения встроенного модема НМС к соответствующему источнику данных. Например, подключайте линейный порт модема НМС к аналоговому телефонному гнезду на стене через телефонный кабель.

Примечание: Информацию об ошибках можно отправлять компании IBM с помощью других способов соединения.

8. Если управляемая система уже установлена, можно проверить, активно ли кабельное подключение Ethernet: в процессе установки нужно смотреть на зеленые лампочки состояния и на НМС, и на портах Ethernet управляемой системы.
9. Соедините **Разъем Ethernet 1** НМС с портом **LINK HMC1** управляемой системы.



10. Если к управляемому серверу подключается вторая HMC, то подключайте ее к порту Ethernet с меткой **LINK HMC2** на управляемом сервере.
11. При использовании внешнего модема вставьте кабель питания модема в модем HMC.
12. Вставьте кабели питания монитора, HMC и внешнего модема HMC в электрические розетки. В случае подключения HMC к новой управляемой системе не подключайте управляемую систему к источнику питания.

Далее следует настроить программное обеспечение HMC. Перейдите к “Настройка HMC” на стр. 91.

Понятия, связанные с данным:

“Выбор способа соединения для сервисного сервера” на стр. 77

Дополнительные сведения об опциях соединения при работе с сервисным центром.

“Сетевые соединения HMC” на стр. 73

Установка HMC 7310-CR4 в стойку

В данном разделе описан процесс установки HMC 7310-CR4 в стойку. Эта задача выполняется заказчиком.

Если для управления системой с процессором Power8 применяется HMC, то это должна быть HMC модели CR3 или выше, монтируемая в стойке.

Ниже показан вид сзади 7310-CR4:

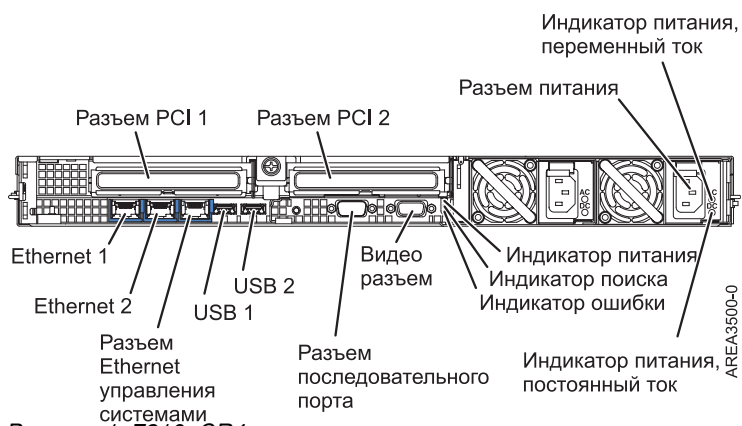


Рисунок 1. 7310-CR4 - вид сзади

Для установки НМС 7310-CR4 в стойку выполните следующие действия:

1. Сверьтесь со списком поставки. Обратитесь к разделу Инвентаризация компонентов.
2. Найдите комплект для монтажа аппаратных средств в стойке и блоки направляющих, поставляемые с системным блоком.

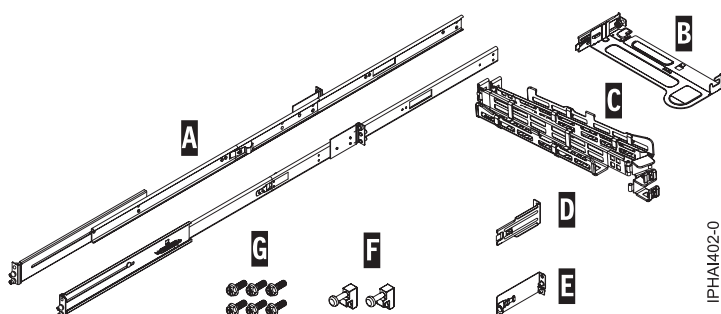


Рисунок 2. Комплект направляющих

Таблица 4. Детали из комплекта направляющих

детали из комплекта направляющих

- A** Направляющие
- B** Монтажная пластина кабельного кронштейна
- C** Кабельный кронштейн
- D** Кабельная скоба
- E** Скоба кабельного кронштейна и предохранительный фиксатор
- F** Защелки (2 шт.)
- G** Винты (6 шт.)

Важное замечание: Высота этого системного блока равна одному блоку EIA; эта информация понадобится для завершения установки.

Инвентаризация компонентов

Иногда возникает необходимость составить реестр компонентов. Для выполнения этой задачи используйте процедуру, описанную в этом разделе.

Если вы не сделали это, выполните описание компонентов перед началом установки:

1. Найдите описание деталей в коробке.

2. Убедитесь, что вы получили все заказанные компоненты.

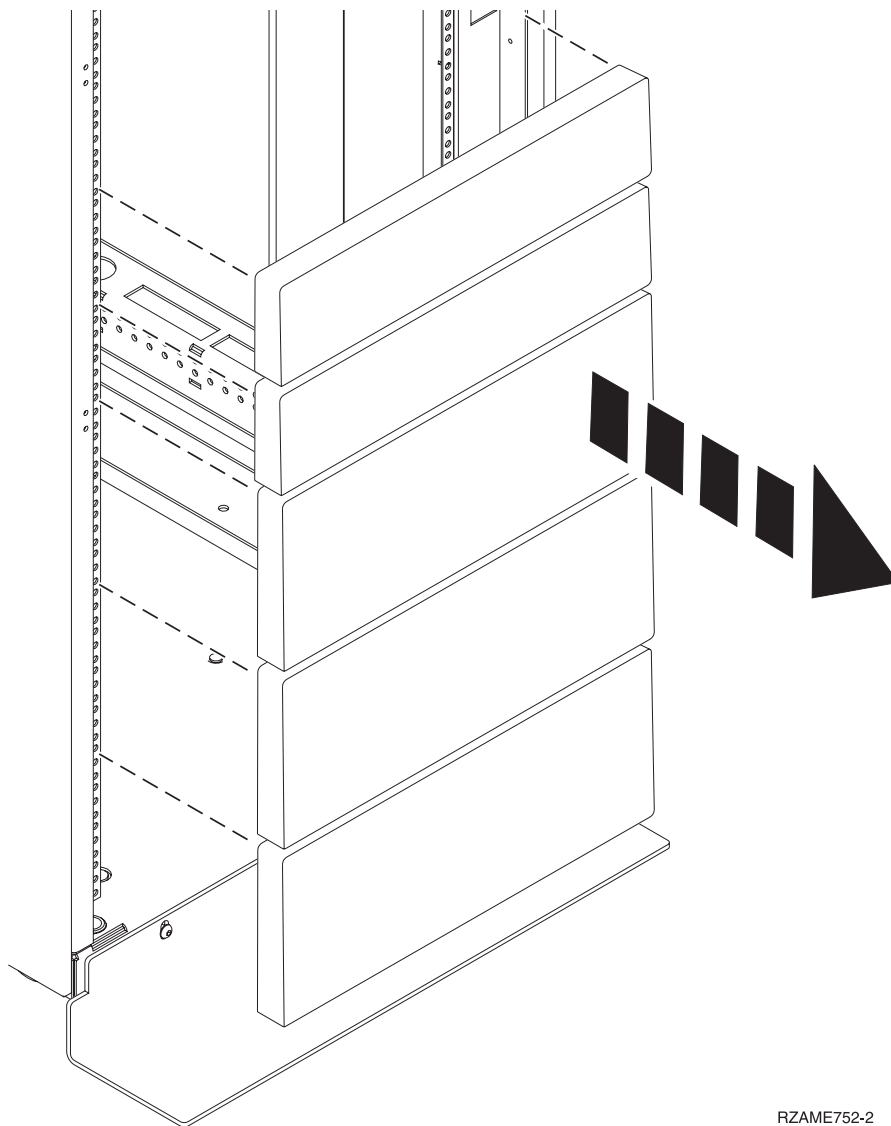
При обнаружении не предусмотренных в комплекте, отсутствующих или поврежденных компонентов обращайтесь к торговому посреднику IBM или в сервисный центр IBM .

Определение расположения

Иногда нужно определить место, куда должна быть установлена система в стойку. В этом разделе описаны процедуры выполнения этих задач.

Перед установкой НМС в стойку выполните следующие действия:

1. Спланируйте расположение блоков. Крупные и тяжелые блоки размещайте внизу стойки.
2. Снимите панели-заменители для доступа внутрь стойки по месту установки блока.



RZAME752-2

Рисунок 3. Удаление панелей-заменителей.

3. При необходимости удалите переднюю и заднюю дверцы.
4. При отсутствии схемы монтажа в стойке следуйте инструкциям, изложенным в разделе Метка расположения без схемы монтажа в стойке.

Маркировка расположения без трафарета монтажа в стойке:

Расположение можно пометить без трафарета.

В комплект поставки данной системы схема не входит. Высота этих системных блоков равна одному блоку EIA.

Для определения места монтажа выполните следующие действия:

1. Выберите место для размещения системы в стойке. Запишите расположение EIA.

Примечание: Блок EIA в стойке содержит группу из трех отверстий.

2. Стоя лицом к передней панели стойке и начиная справа, приклейте самоклеющуюся точку из комплекта поставки рядом с верхним отверстием блока EIA.

Примечание: Самоклеющиеся точки используются для помощи в идентификации расположений в стойке. Если у вас нет самоклеющихся точек, используйте для маркировки другие способы, например, маркер, карандаш или липкую ленту. При установке направляющих поставьте метку или приклейте самоклеющуюся точку на нижнем и среднем отверстиях блока EIA.

3. Приклейте другую самоклеющуюся точку рядом с нижним отверстием верхнего блока EIA.

Примечание: Пересчитывать отверстия нужно, начиная с отверстия, отмеченного первой точкой; после него отсчитываются два отверстия. Вторую точку приклейте рядом с третьим отверстием.

4. Повторите шаг 1 для соответствующих отверстий, расположенных с левой стороны стойки.
5. Зайдите в тыл стойки.
6. На правой стороне найдите единицу EIA, соотносящуюся с нижней помеченной единицей EIA спереди стойки.
7. Приклейте самоклеющуюся точку внизу блока EIA.
8. Приклейте самоклеющуюся точку на верхнее отверстие блока EIA.
9. Пометьте соответствующие отверстия на левой стороне стойки.

Установка направляющих в стойке

Инструкции по установке направляющих в стойку.

Для установки направляющих в стойку выполните следующие действия:

1. Установите правую направляющую (**A**) с меткой правая в задних правых положениях монтажного фланца (**B**). Два штыря направляющей должны выступать в нижнем и среднем отверстиях (**B**) блока EIA.

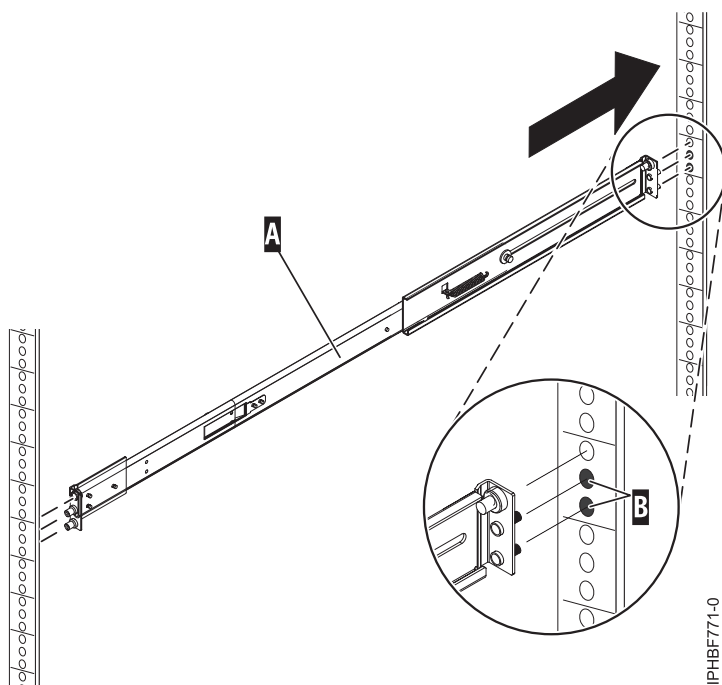


Рисунок 4. Установка правой направляющей в задней панели стойки

2. Нажмите на край направляющей (А), чтобы сжать ее подпружиненный механизм, и вставьте ее в передние правые положения монтажного фланца (В). Направляющая разожмется, и два ее штыря пройдут сквозь нижнее и среднее отверстия (В) блока EIA.

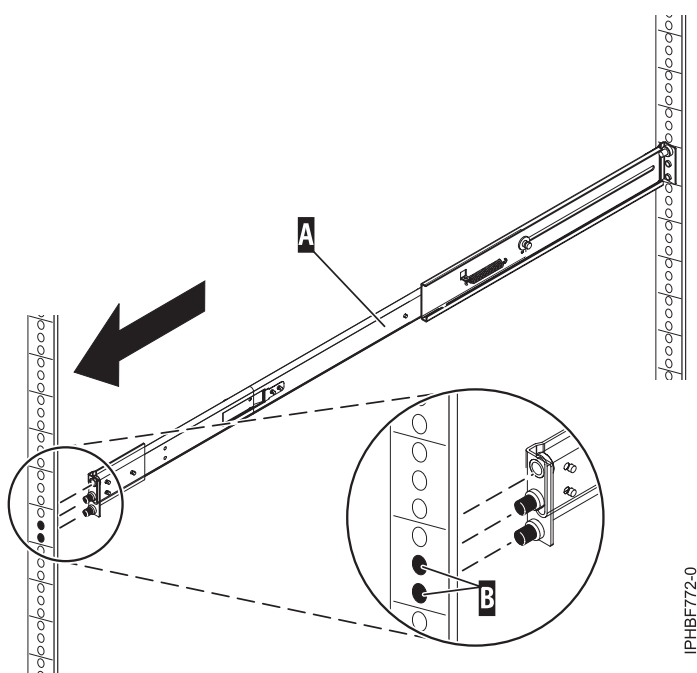


Рисунок 5. Установка правой направляющей в передней панели стойки

3. Повторите шаги 1 на стр. 8 – 2 для установки в стойку левой направляющей (с меткой левая).

4. Спереди стойки разместите защелку (C) над штырями. Вручную затяните невыпадающий винт (D) на верхнем штыре передней части правой направляющей (A).

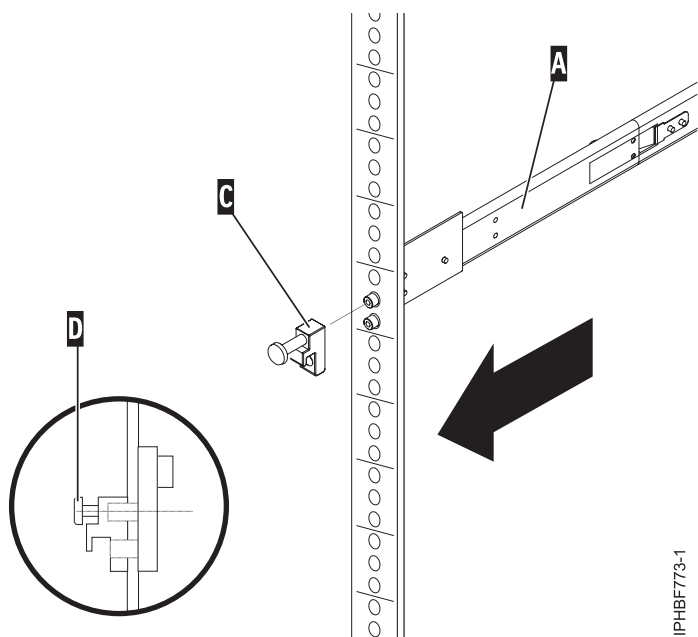


Рисунок 6. Установка защелки на передней части направляющих

5. Повторите предыдущий шаг для установки защелки на передней части левой направляющей.
6. Перейдите к задней части стойки. Вручную затяните винт (F) для крепления скобы кабельного кронштейна (E) к задней части левой направляющей (G).

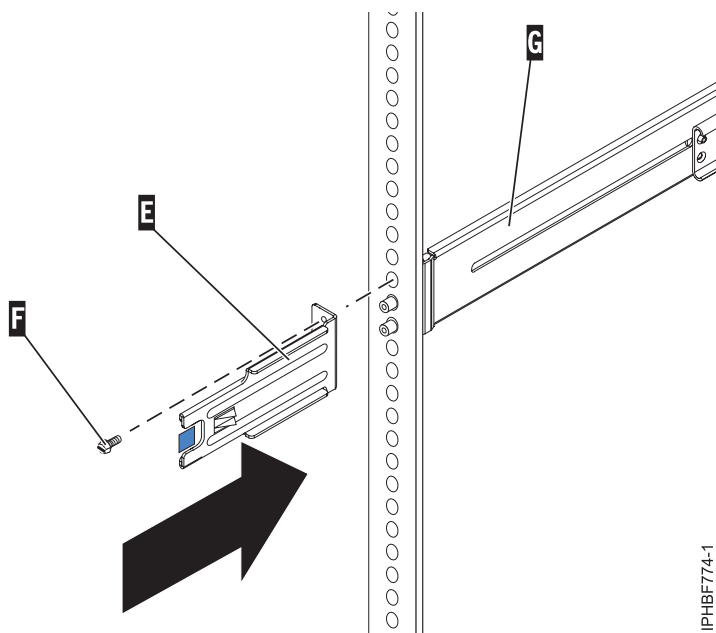


Рисунок 7. Крепление скобы кабельного кронштейна к задней части левой направляющей

7. Если перемещать систему не планируется, перейдите к разделу “Установка НМС на направляющих”.
- Если система будет перемещаться, вставьте винт (I) для крепления скобы кабельного кронштейна (H) к задней части правой направляющей (A). Вручную затяните винт.
- С помощью скобы кабельного кронштейна его можно закреплять во время транспортировки. Если механизм вводится в зацепление после установки кабельного кронштейна, систему не удастся выдвинуть из стойки.

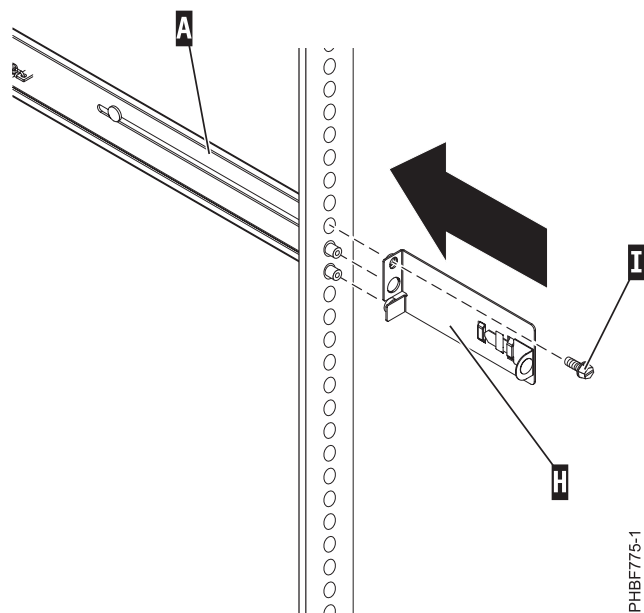


Рисунок 8. Крепление скобы кабельного кронштейна к задней части правой направляющей.

Установка НМС на направляющих

Иногда необходимо установить НМС на направляющих. Для выполнения этой задачи используйте процедуру, описанную в этом разделе.

Перед установкой НМС на направляющих убедитесь в том, что стабилизаторы выдвинуты и скоба стабилизаторов стойки прикреплена к нижней передней панели стойки для предотвращения ее от падения вперед при выдвигении направляющих из стойки.

Для установки НМС в блоке направляющих выполните следующие действия:

1. Снимите транспортировочную скобу, защищающую блоки питания, с задней правой части НМС. Для того чтобы снять транспортировочную скобу, сдвиньте ее вправо и, повернув, выньте из НМС.
2. Спереди стойки выдвиньте направляющие на полную длину, чтобы они защелкнулись в нужном положении в раздвинутом состоянии (A).

Внимание: Фиксаторы на передней части направляющей и скобы кабельных кронштейнов нужно устанавливать *перед* установкой НМС на направляющих. Если указанные элементы не установлены, то при установке возможно сжатие направляющих, в результате чего НМС может выпасть из стойки.

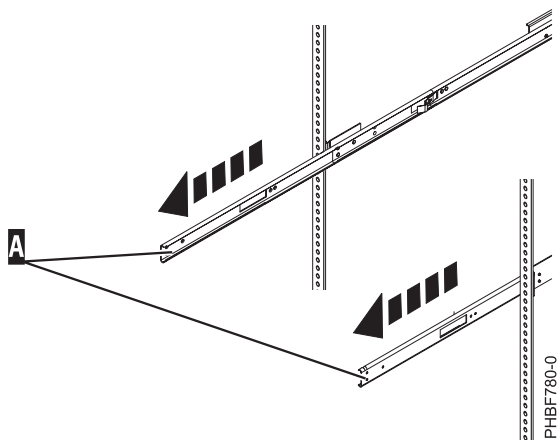


Рисунок 9. Раздвижение направляющих.

Важное замечание: Этот блок весит приблизительно 17 кг (37 фунтов). Убедитесь в том, что можно будет безопасно удерживать такой вес при установке НМС в стойку.

3. Поднимите НМС на уровень направляющих и расположите колесики **(B)** в задней части НМС между направляющими.

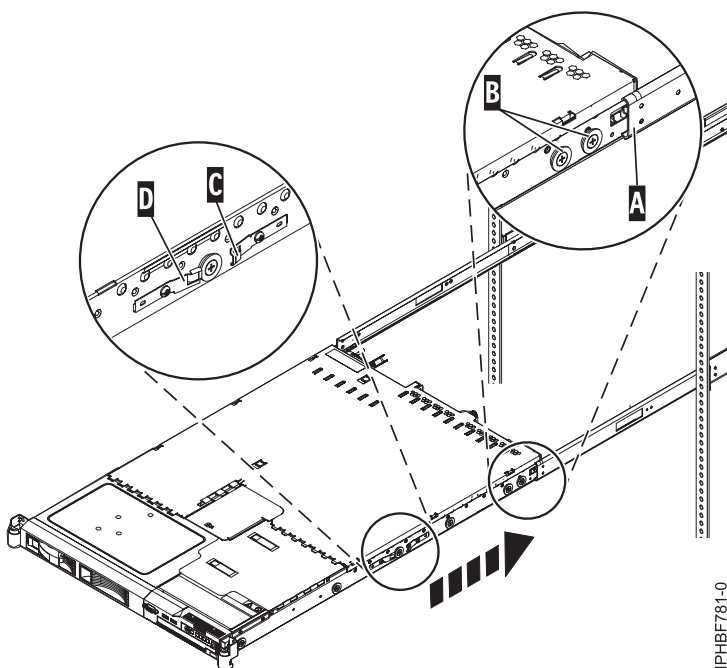


Рисунок 10. Установка НМС на направляющих.

4. Задвигайте НМС по направляющим, пока фиксаторы **(C)** не защелкнутся в нужном положении. Они фиксируют систему в рабочем положении на направляющих. Будет слышен отчетливый щелчок.
5. Нажмите на защелки **(D)** в передней части направляющих по обе стороны направляющих.
6. Попробуйте выдвинуть и задвинуть НМС, чтобы убедиться в том, что НМС движется свободно, без помех.

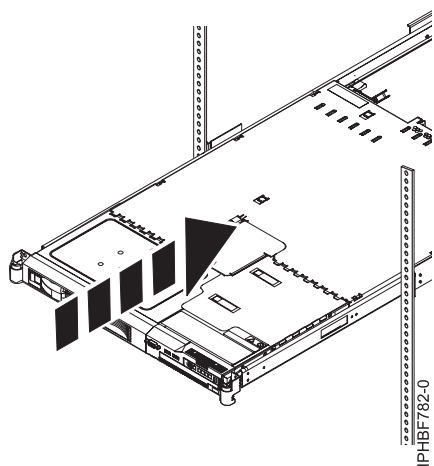


Рисунок 11. Задвиньте НМС в стойку

Важное замечание: Ни в коем случае не применяйте силу для того, чтобы задвинуть НМС по направляющим. Если НМС не скользит свободно по направляющим, просто целиком снимите НМС с направляющих. После снятия с направляющих НМС переместите НМС, а затем повторно вставьте НМС на направляющие. Повторяйте процесс до тех пор, пока НМС не будет свободно скользить в стойке.

7. Задвиньте НМС на место, пока защелки (**F**) стойки не защелкнутся в нужном положении.

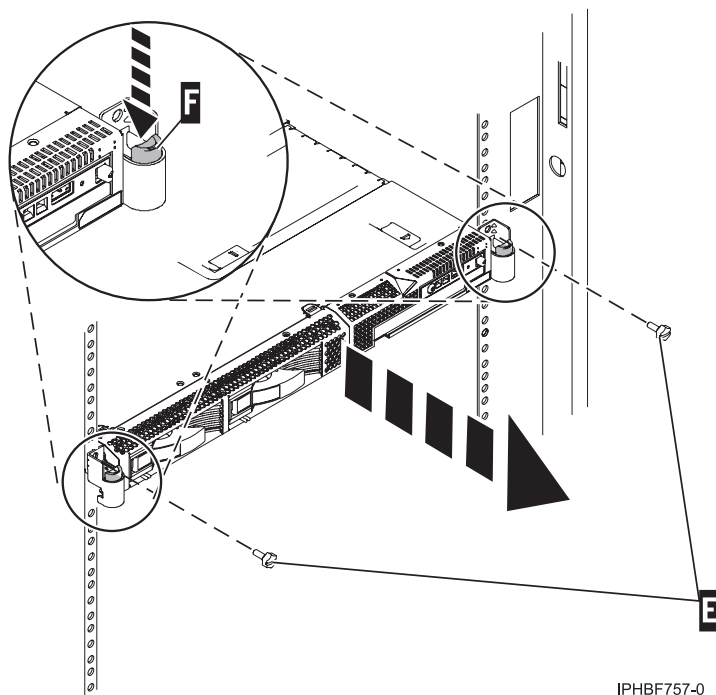


Рисунок 12. Защелки и винты стойки

8. Хорошо затяните все четыре винта, установленные в передней и задней части обеих направляющих.
9. Если стойку планируется перемещать, вставьте и затяните два винта (**E**).

Установка кабельного кронштейна

Иногда необходимо установить кабельный кронштейн. Для выполнения этой задачи используйте процедуру, описанную в этом разделе.

Для установки кабельного кронштейна выполните следующие действия:

1. С задней стороны стойки найдите фланец (А) кабельного кронштейна, расположенный на неподвижной задней части левого блока направляющих (если смотреть с задней стороны стойки).
2. Прикрепите зажим (В) кабельного кронштейна к направляющей, продвигая его по направляющей до защелкивания в нужном положении.

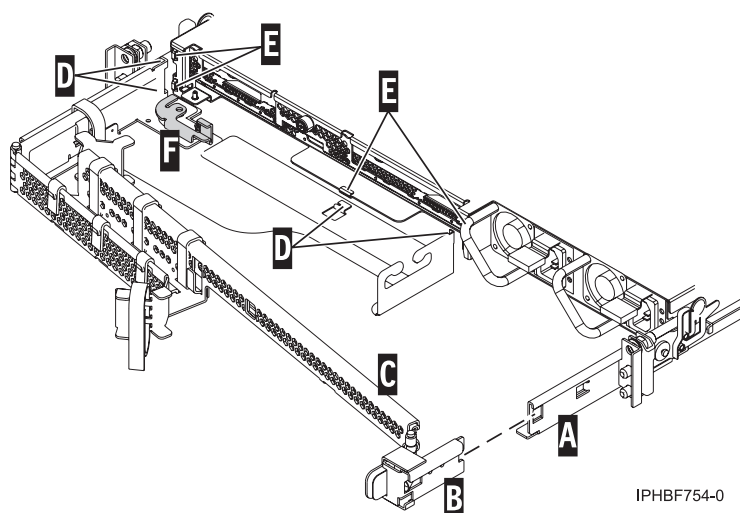


Рисунок 13. Кабельный кронштейн и системный блок.

3. Прикрепите второй конец кабельного кронштейна (С) к задней части НМС. Совместите фиксаторы (D) кабельного кронштейна с отверстиями (Е) на задней части НМС.
4. Сдвиньте кабельный кронштейн влево, закрепляя его на месте. Проверьте, все ли фиксаторы попали в отверстия.
5. Переведите стопорный рычаг (F) в положение фиксации. Убедитесь в том, что кабельный кронштейн (С) установлен без перекосов и движется свободно.

Подключение смонтированной в стойке НМС

Описывается физическая установка монтируемой в стойку НМС.

1. Проверьте правильность расположения НМС.
2. Установите НМС в стойку. Дополнительные сведения содержатся в разделе “Установка НМС 7310-CR4 в стойку” на стр. 5. По окончании установки перейдите к следующему шагу.
3. Вставьте кабель питания в НМС.
4. Подключите клавиатуру, монитор и мышь.
5. Подключите дополнительный модем:

Для подключения внешнего модема выполните следующие действия:

Примечание: Информацию об ошибках можно отправлять компании IBM с помощью других способов соединения. Дополнительные сведения содержатся в разделе “Выбор способа соединения для сервисного сервера” на стр. 77.

- а. Если вы хотите установить внешний модем в стойку, то сделайте это сейчас.
- б. Если этого еще не сделано, подключите кабель данных модема к внешнему модему НМС.
- с. Подключите кабель данных модема к системному порту на НМС, помеченному символом:



IPNA522-0

- d. Подключите линейный порт внешнего модема к аналоговому телефонному гнезду на стене через телефонный кабель.
- e. Вставьте кабель питания модема в модем НМС.

При подключении к встроенному модему используйте кабель данных для подключения встроенного модема НМС к соответствующему источнику данных. Например, подключайте линейный порт модема НМС к аналоговому телефонному гнезду на стене через телефонный кабель.

Примечание: Информацию об ошибках можно отправлять компании IBM с помощью других способов соединения. Дополнительные сведения содержатся в разделе “Выбор способа соединения для сервисного сервера” на стр. 77.

6. Подключите НМС к управляемому серверу через кабель Ethernet (иначе - перекрестный кабель):

Примечание: Дополнительная информация о сетевых соединениях НМС приведена в разделе “Сетевые соединения НМС” на стр. 73.

7. Если управляемая система уже установлена, можно проверить, активно ли кабельное подключение Ethernet: в процессе установки нужно смотреть на зеленые лампочки состояния и на НМС, и на портах Ethernet управляемой системы.
8. Подключите порт Ethernet НМС к порту Ethernet с меткой **НМС1** на управляемом сервере.
9. При подключении второго НМС к управляемому серверу подключите его к порту Ethernet с меткой **НМС2** на управляемом сервере.
10. Вставьте кабели питания монитора, НМС и внешнего модема НМС в электрические розетки.

Примечание: В случае подключения НМС к новой управляемой системе не подключайте управляемую систему к источнику питания.

Далее следует настроить программное обеспечение НМС. Перейдите к “Настройка НМС” на стр. 91.

Расположения портов НМС

Расположения компонентов можно найти с помощью кодов расположений. Диаграммы расположений портов НМС помогают сопоставить код расположения с положением порта НМС на сервере.

Расположения портов НМС модели 8247-21L, 8247-22L, 8284-21A или 8284-22A

С помощью этой диаграммы можно найти порты НМС в системе 8247-21L, 8247-22L, 8284-21A или 8284-22A.

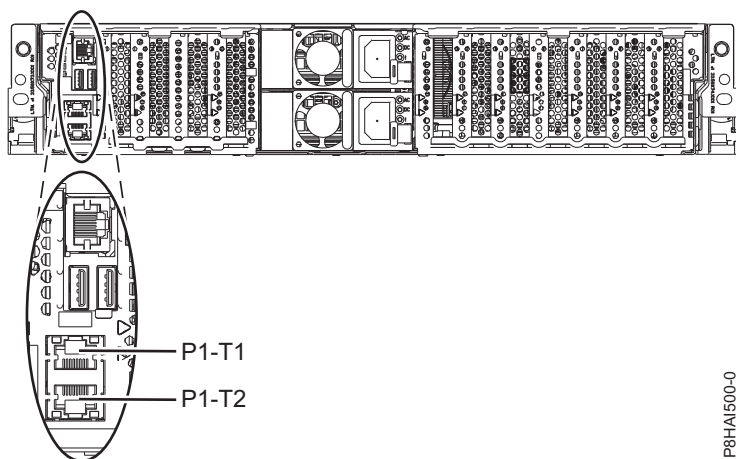


Рисунок 14. Расположения портов НМС 8247-21L, 8247-22L, 8284-21A или 8284-22A

Таблица 5. Расположения портов НМС 8247-21L, 8247-22L, 8284-21A или 8284-22A

Порт	Код физического расположения	Индикатор идентификации
Порт НМС 1	Un-P1-T1	Нет
Порт НМС 2	Un-P1-T2	Нет
Дополнительная информация о расположениях портов НМС в системе 8247-21L, 8247-22L, 8284-21A или 8284-22A приведена в разделе Расположение компонента и коды расположений для 8247-21L, 8247-22L или 8284-22A .		

Расположения портов НМС модели 8247-42L, 8286-41A и 8286-42A

С помощью этой диаграммы можно найти порты НМС в системе 8247-42L, 8286-41A или 8286-42A.

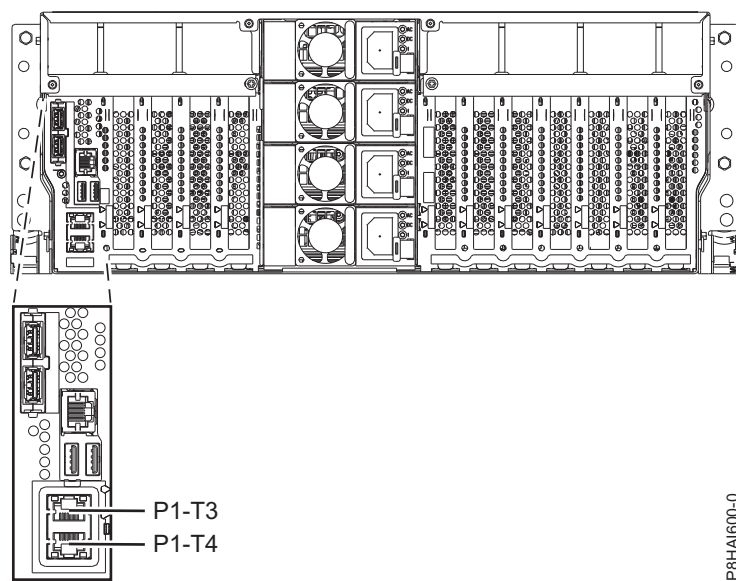


Рисунок 15. Стойка - расположения портов НМС 8247-42L, 8286-41A и 8286-42A

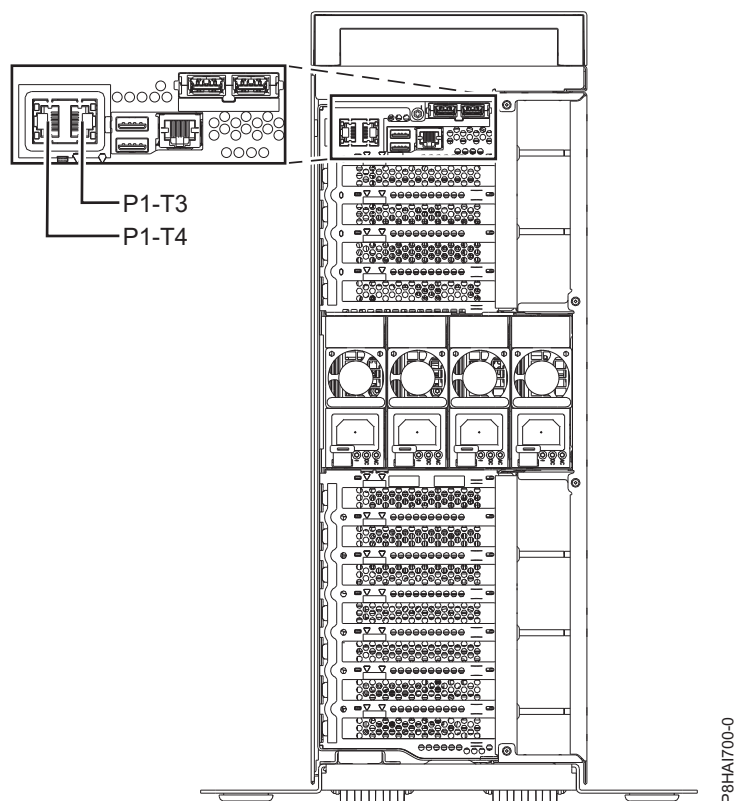


Рисунок 16. Расположения портов НМС для 8286-41А в виде системного блока

Таблица 6. Расположения портов НМС 8247-42L, 8286-41А и 8286-42А

Порт	Код физического расположения	Индикатор идентификации
Порт НМС 1	Un-P1-T3	Нет
Порт НМС 2	Un-P1-T4	Нет
Дополнительная информация о расположении портов НМС в системе 8247-42L, 8286-41А или 8286-42А приведена в разделе Расположение компонента и коды расположений для 8247-42L, 8286-41А и 8286-42А.		

Расположения портов НМС модели 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ

С помощью этой диаграммы и таблицы можно найти порты НМС в системе 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ.

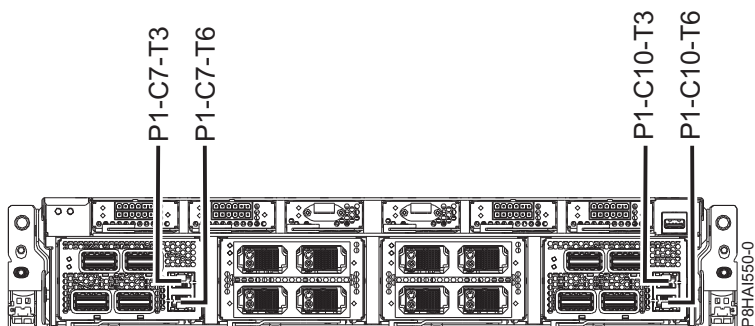


Рисунок 17. Расположения портов НМС 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ

Таблица 7. Расположения портов НМС 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ

Порт	Код физического расположения	Индикатор идентификации
Карта служебного процессора 1 - порт НМС 1	Un-P1-C7-T3	Нет
Карта служебного процессора 1 - порт НМС 2	Un-P1-C7-T6	Нет
Карта служебного процессора 2 - порт НМС 1	Un-P1-C10-T3	Нет
Карта служебного процессора 2 - порт НМС 2	Un-P1-C10-T6	Нет
Дополнительная информация о расположении портов НМС в системах 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ приведена в разделе Расположение компонента и коды расположений для 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ.		

Расположения портов НМС модели 8408-44Е и 8408-Е8Е

С помощью этой диаграммы и таблицы можно найти порты НМС в системе 8408-44Е или 8408-Е8Е.

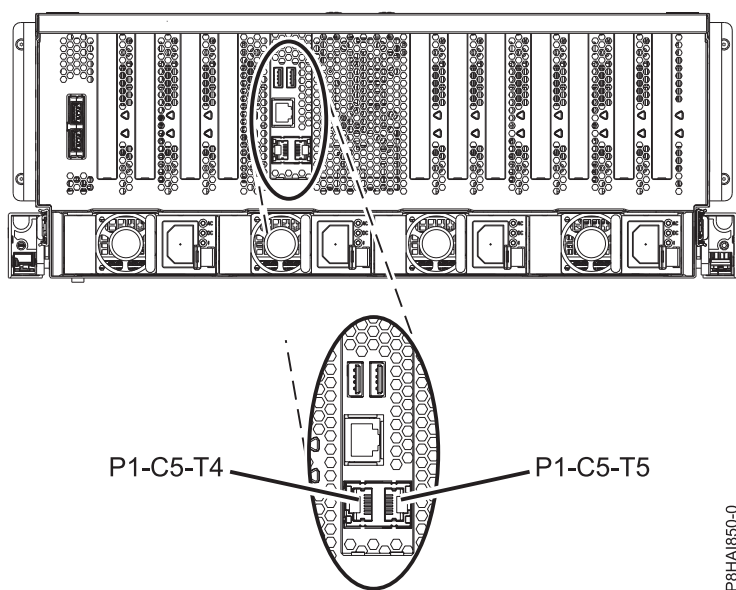


Рисунок 18. Расположения портов НМС 8408-44Е и 8408-Е8Е

Таблица 8. Расположения портов НМС 8408-44Е и 8408-Е8Е

Порт	Код физического расположения	Индикатор идентификации
Порт НМС 1	Un-P1-C5-T4	Нет
Порт НМС 2	Un-P1-C5-T5	Нет
Дополнительная информация о расположении портов НМС в системах 8408-44Е и 8408-Е8Е приведена в разделе Расположение компонента и коды расположений для 8404-44Е и 8408-Е8Е.		

Установка 7042-CR5 и 7042-CR6 в стойку

В данном разделе описан процесс установки НМС 7042-CR5 и 7042-CR6 в стойку.

Сверьтесь со списком поставки. Компоненты, необходимые для установки сервера в стойку, показаны на следующем рисунке. Если какие-то компоненты отсутствуют или повреждены, обратитесь к продавцу.

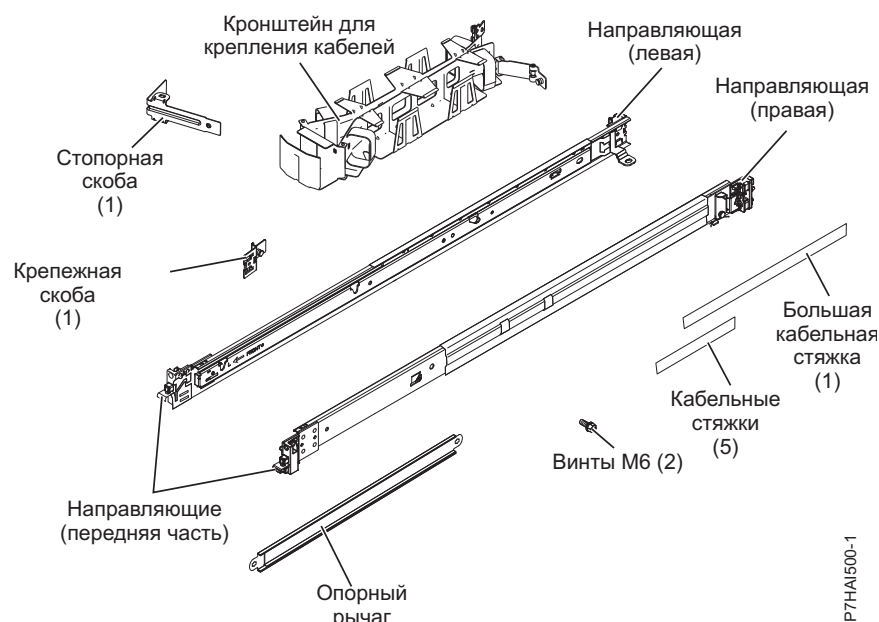


Рисунок 19. Список поставки

Примечание: Для крепления или обеспечения дополнительной устойчивости в местах с высоким уровнем вибрации можно использовать винты.

Для установки НМС 7042-CR5 или 7042-CR6 в стойку выполните следующие действия:

1. Каждая направляющая помечена или буквой R (правая), или буквой L (левая). Выберите одну из направляющих и надавите на передний подвижный фиксатор (1); затем вытяните переднюю защелку (2), чтобы выдвинуть переднюю боковую направляющую. Если в направляющей установлен винт с накатанной головкой (3), удалите его.

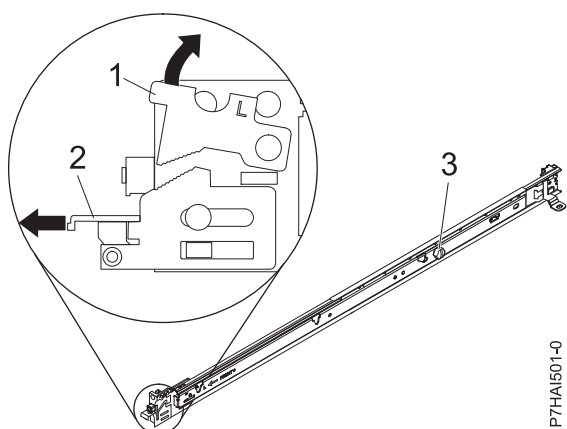


Рисунок 20. Направляющая и подвижный фиксатор

Примечание: Убедитесь, что подвижный фиксатор остался вытянутым и не защелкнулся.

2. Совместите три штыря на заднем конце направляющей с тремя отверстиями на выбранной высоте в задней части стойки. Вставьте направляющие так, чтобы штыри вошли в отверстия (1), а затем опустите их вниз (2), чтобы защелки не встали на место.

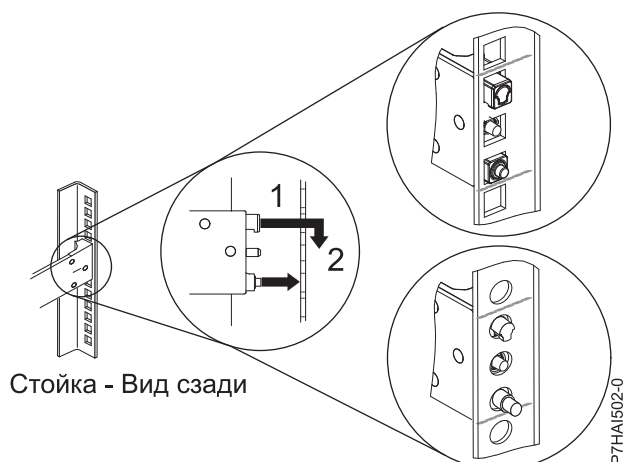
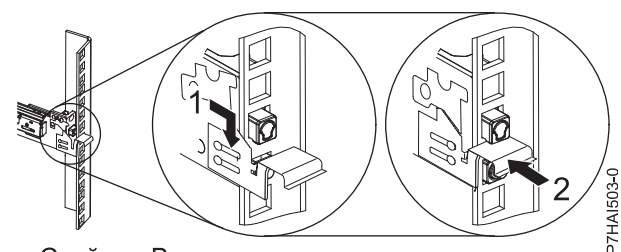


Рисунок 21. Совместите штыри с отверстиями в задней части стойки

3. Потяните направляющую вперед и вставьте два штыря (1) на переднем конце направляющей в два отверстия на той же высоте в передней части стойки. Надавливайте на направляющую, пока она не встанет на место (до щелчка). Нажмите на переднюю защелку (2). Повторите шаги 1 - 3 для установки в стойку другой направляющей. Убедитесь, что все передние защелки полностью зафиксированы.



Стойка - Вид спереди
Рисунок 22. Направляющая и штыри в передней части стойки

4. Потяните направляющие вперед (1) до двойного щелчка. Осторожно поднимите сервер и установите его в наклонном положении над направляющими, чтобы совместить головки штифтов (2) на задней части корпуса сервера с прорезями (3) в направляющих. Опускайте сервер, пока головки штифтов не войдут в две задние прорези, а затем медленно опустите переднюю часть сервера (4), чтобы остальные головки

штифтов также вошли в прорези на направляющих. Передвиньте переднюю защелку (5) над головками штифтов.

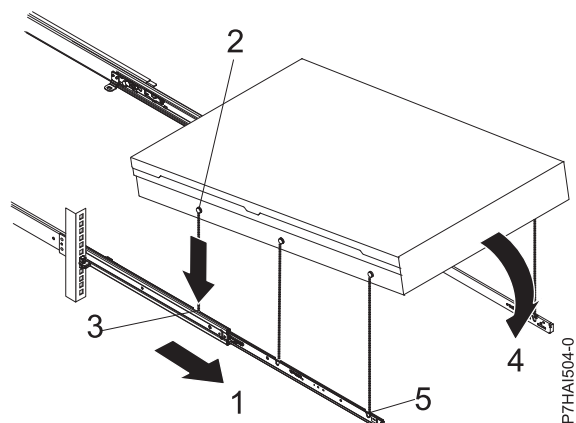


Рисунок 23. Направляющие выдвинуты, головки штифтов сервера совмещены с прорезями в направляющих

5. Поднимите синие защелки (1) на направляющих и задвигайте сервер (2) в стойку, пока он не встанет на место.

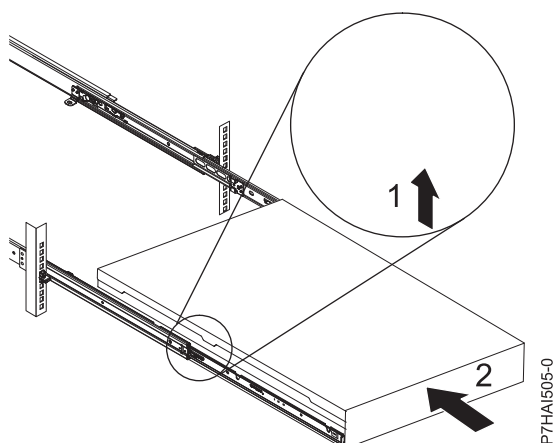


Рисунок 24. Защелки и сервер

6. На любой из двух сторон сервера можно установить кабельный кронштейн. На следующем рисунке показан кабельный кронштейн, установленный на левой стороне. Для установки кабельного кронштейна с правой стороны выполните инструкции и установите оборудование с противоположной стороны. Соедините один конец опорного рычага (1) с той направляющей, к которой планируется прикрепить кабельный кронштейн, чтобы другой конец опорного рычага (2) можно было повернуть к стойке.

Стойка - Вид сзади

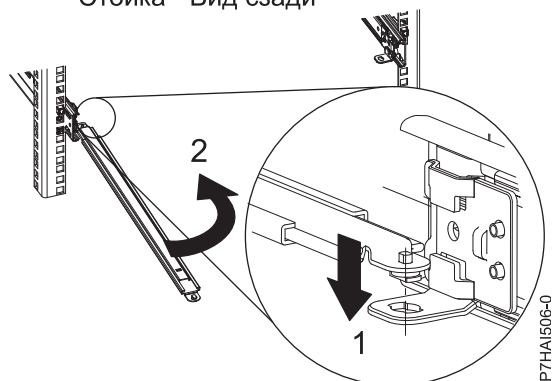


Рисунок 25. Соединение опорного рычага

7. Установите L-образную стопорную скобу (1) кабельного кронштейна на свободный конец опорного рычага. Поверните скобу (2), чтобы прикрепить ее к опорному рычагу.

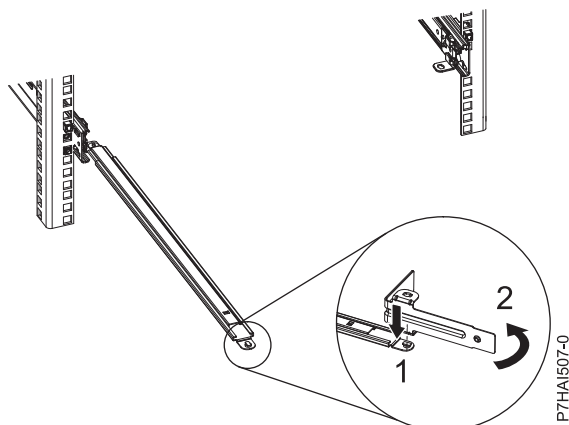


Рисунок 26. Стопорная скоба кабельного кронштейна, закрепленная на опорном рычаге

8. Для прикрепления другого конца опорного рычага к задней части направляющей вытяните штырь (1), а затем задвиньте скобу (2) в направляющую.

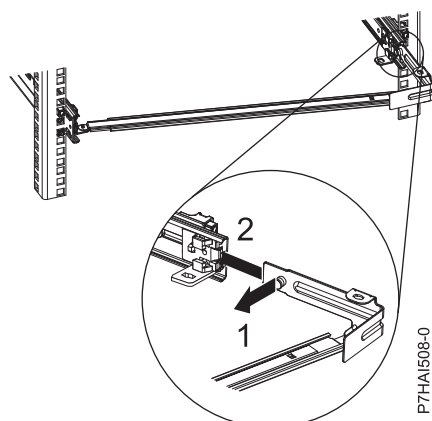
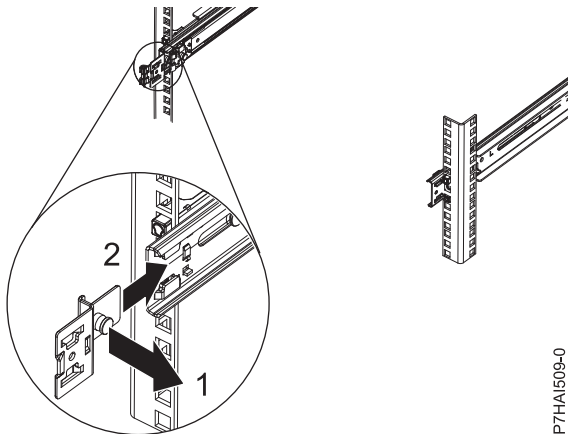


Рисунок 27. Штырь вытянут, скоба вставлена в направляющую

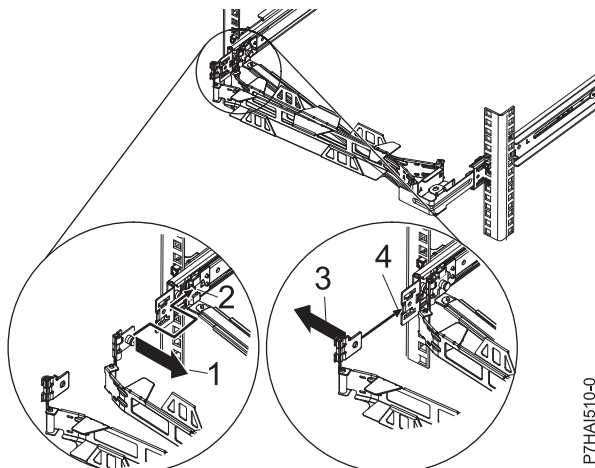
9. Вытяните штырь крепежной скобы (1) и вставьте крепежную скобу (2) в направляющую, на которой устанавливается кабельный кронштейн. Задвигайте скобу в направляющую, пока не защелкнутся пружинные штыри.



P7HAI509-0

Рисунок 28. Вытянутый штырь крепежной скобы и крепежная скоба, установленная в направляющей

10. Установите кабельный кронштейн на опорный рычаг. Вытяните штырь (1) кабельного кронштейна и вставьте фиксатор (2) кронштейна в прорезь на внутренней стороне направляющей. Нажимайте на фиксатор, пока он не защелкнется. Вытяните другой штырь (3) кабельного кронштейна и вставьте фиксатор кронштейна в прорезь (4) на внешней стороне направляющей. Нажимайте на фиксатор, пока он не защелкнется.



P7HAI510-0

Рисунок 29. Соединение кабельного кронштейна

11. Подсоедините к задней части сервера кабели питания и другие кабели (кабель клавиатуры, монитора и мыши, если это необходимо). Проложите эти кабели вдоль кабельного кронштейна (1) и закрепите их с помощью кабельной стяжки или зажимов с кольцом и крючком.

Примечание: При прокладке кабелей оставляйте слабину, чтобы избежать их натяжения при перемещении кронштейна.

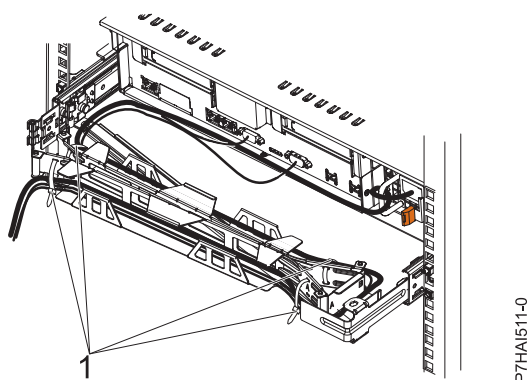


Рисунок 30. Подсоединение и прокладка кабеля питания

12. Задвигайте сервер в стойку, пока он не встанет на место.

Установка 7042-CR7 и 7042-CR8 в стойку

Рассмотрена установка консоли аппаратного обеспечения (HMC) 7042-CR7 и 7042-CR8 в стойку.

Сверьтесь со списком поставки. Компоненты, необходимые для установки сервера в стойку, показаны на следующих рисунках. Если какие-то компоненты отсутствуют или повреждены, обратитесь к продавцу.

Комплект поставки кабельного кронштейна

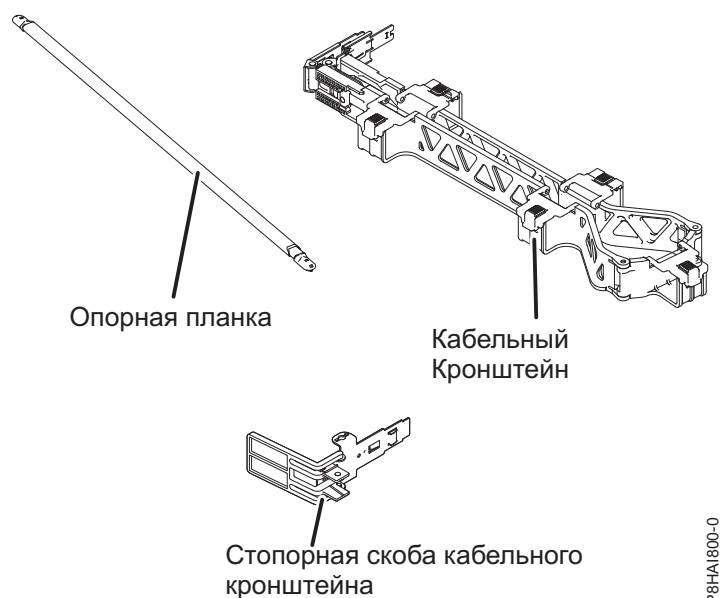
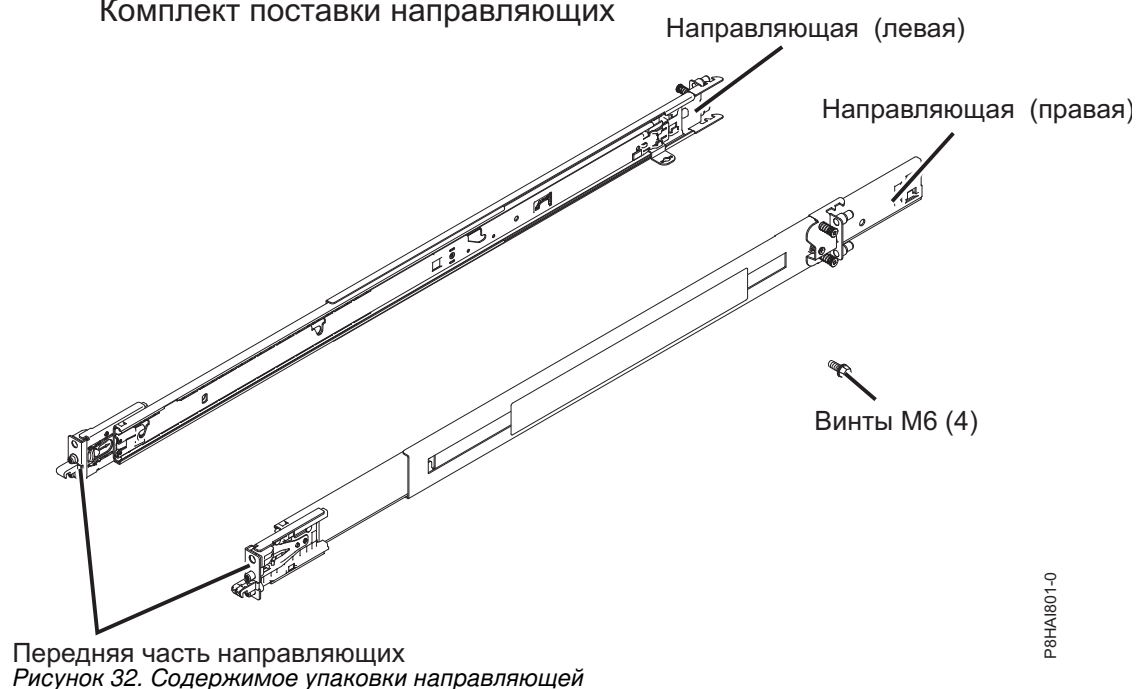


Рисунок 31. Содержимое упаковки кабельного кронштейна

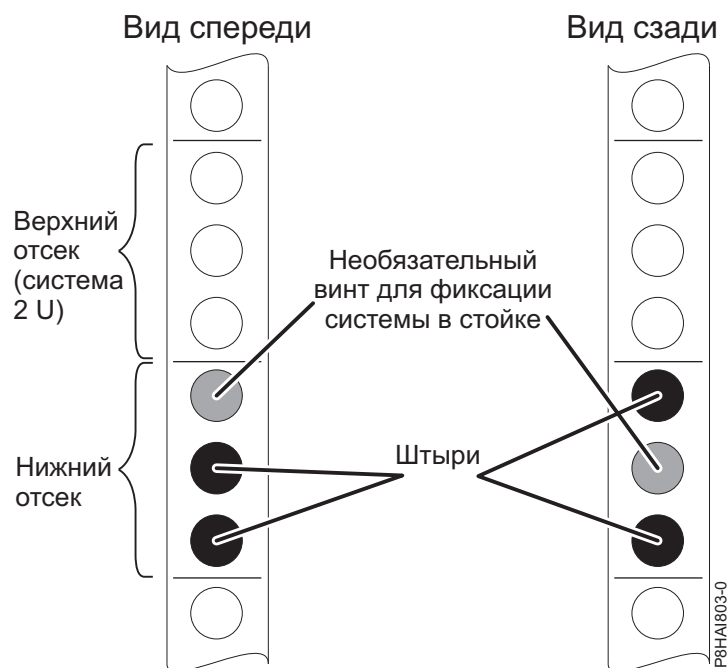
Комплект поставки направляющих



Примечание: Для установки потребуется упаковка направляющей и кабельного кронштейна.

Для установки HMC 7042-CR7 или 7042-CR8 в стойку выполните следующие действия:

1. Выберите отсек на один или два блока (в зависимости от устанавливаемого сервера) в стойке для установки сервера.



Примечание: В случае установки сервера двойной высоты установите направляющие в нижней части отсека в стойке.

- В конце каждой направляющей расположена метка **Left Front/Rear** или **Right Front/Rear**. Выберите одну из направляющих и потяните заднюю скобу назад пока она не встанет на место (до щелчка).

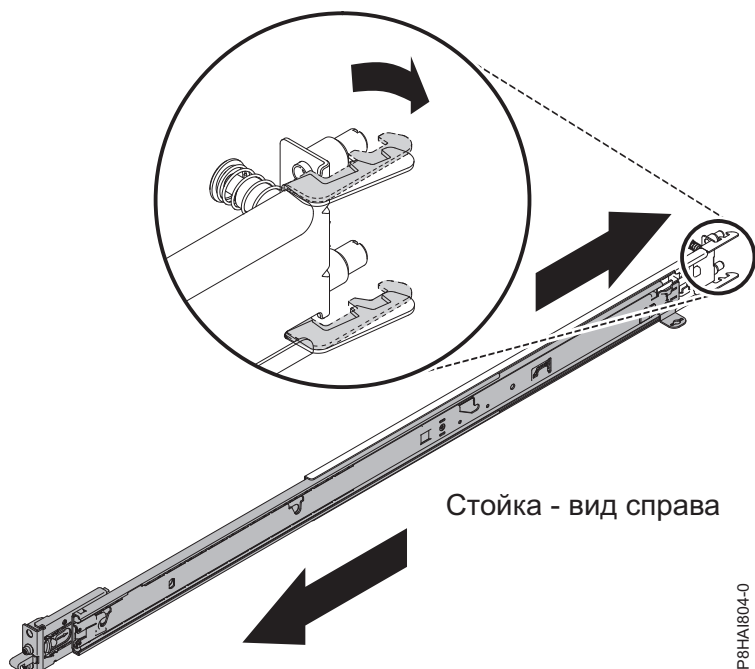


Рисунок 34. Направляющая и подвижный фиксатор

Примечание: Убедитесь, что подвижный фиксатор остался вытянутым и не защелкнулся.

- С передней части стойки совместите два штыря на заднем конце направляющей на выбранной высоте в задней части стойки. Вставьте направляющие так, чтобы штыри вошли в отверстия и вставьте направляющие в стойку, чтобы зафиксировать заднюю часть направляющих в стойке.

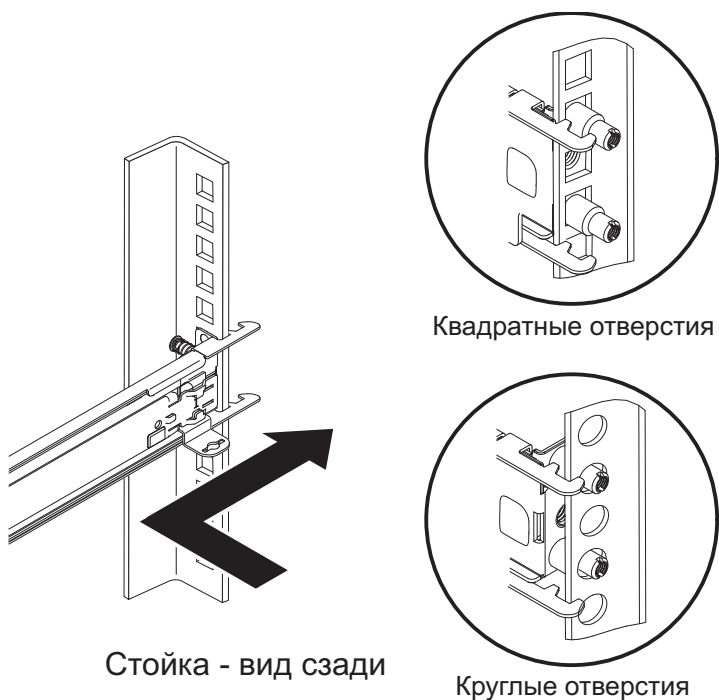


Рисунок 35. Совместите штыри с отверстиями в задней части стойки

Примечание: В случае установки направляющих в отсек 1 U, выше и ниже которого уже установлены устройства, направляющие следует вставить в заднюю стенку стойки.

- Откройте переднюю защелку направляющей. Если они закрыты, откройте защелки, нажав на синюю кнопку и потянув защелку назад.

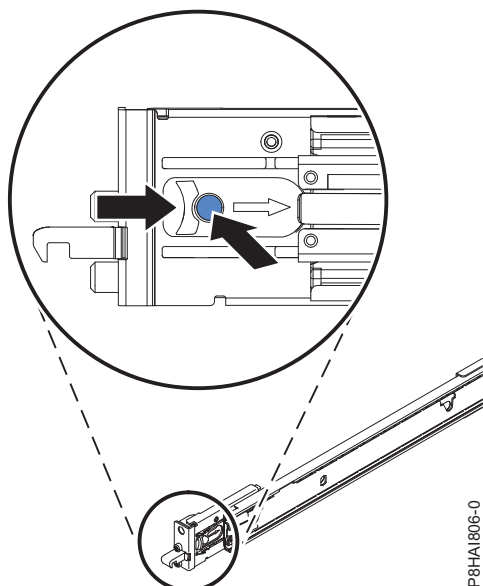


Рисунок 36. Передняя защелка направляющей

- Потяните направляющие вперед и найдите передние защелки в отсеках U в передней части направляющих EIA стойки. Отрегулируйте длину направляющих. Убедитесь, что передний конец повернут в положение с передней защелкой в передней части направляющей EIA стойки.

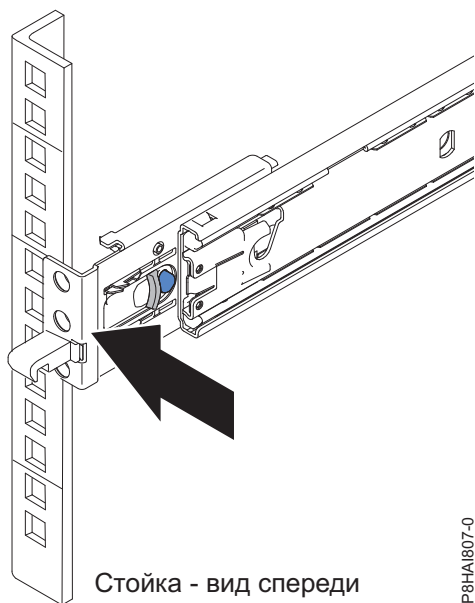
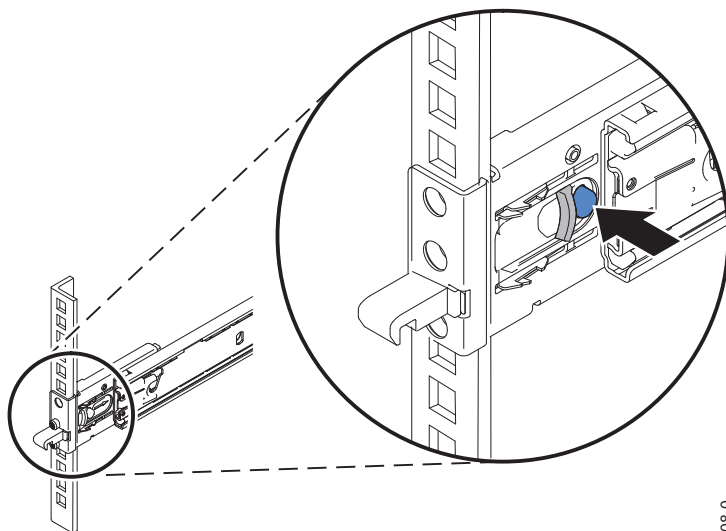


Рисунок 37. Направляющая и штыри в передней части стойки

- Нажмите синюю кнопку, чтобы закрыть скобу со штырьками. Переместите направляющую вверх и вниз, чтобы зафиксировать ее. Повторите шаги 1 - 5 для установки в стойку другой направляющей. Убедитесь, что все передние защелки полностью зафиксированы.



Стойка - вид спереди

Рисунок 38. Направляющая и штыри в передней части стойки

P8HA1808-0

- Потяните направляющие вперед (1) до двойного щелчка. Осторожно поднимите сервер и установите его в наклонном положении над направляющими, чтобы совместить головки штифтов (2) на задней части корпуса сервера с прорезями в направляющих. Опускайте сервер, пока головки штифтов не войдут в две задние прорези, а затем медленно опустите переднюю часть сервера (3), чтобы остальные головки штифтов также вошли в прорези на направляющих (с двойным щелчком). Убедитесь, что передняя защелка накрывает переднюю головку штифта и система зафиксирована в направляющих.

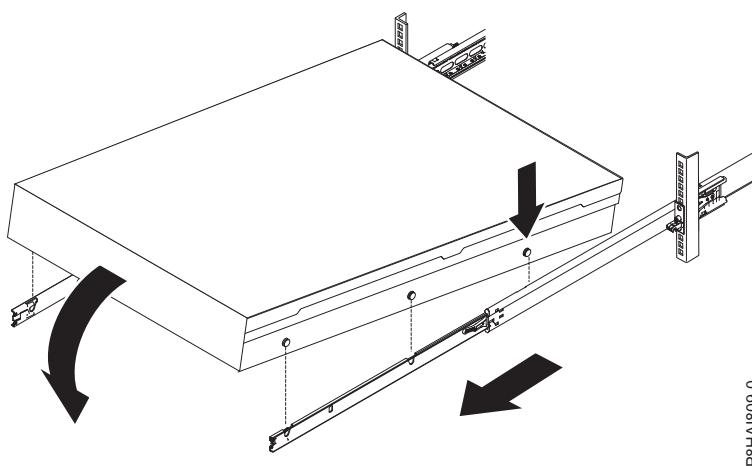
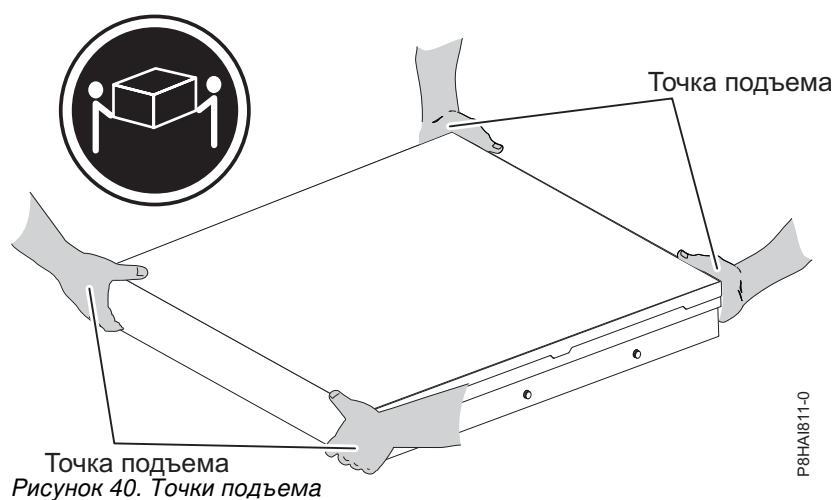


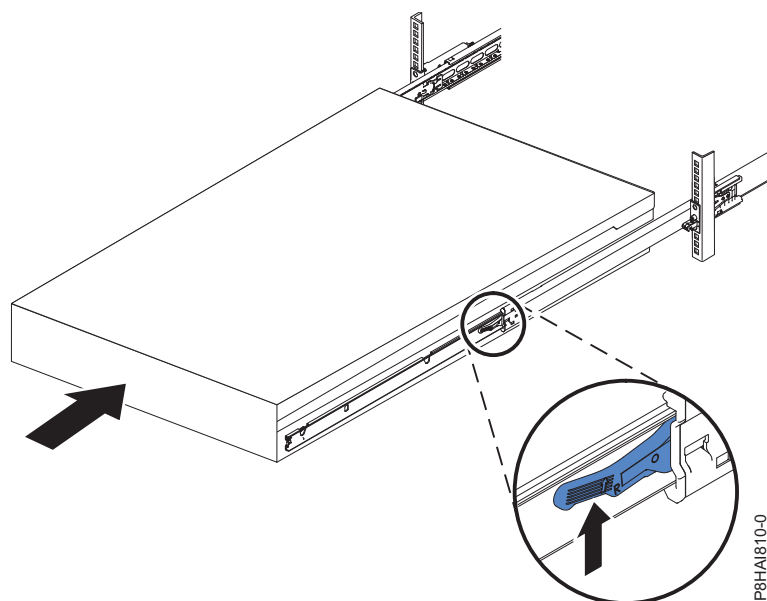
Рисунок 39. Направляющие выдвинуты, головки штифтов сервера совмещены с прорезями в направляющих

P8HA1809-0

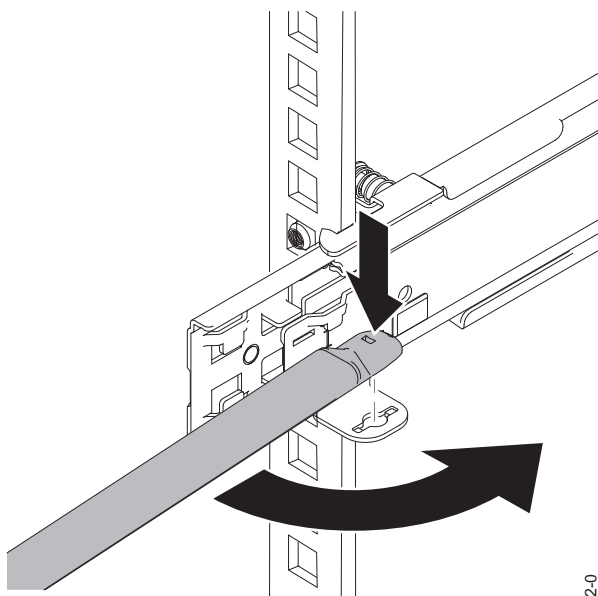


Примечание: При подъеме соблюдайте технику безопасности. Сервер 2 U должны поднимать по крайней мере два человека. Их руки должны быть расположены, как показано на рис. 40.

8. Поднимите стопорные рычаги (1) на направляющих и задвигайте сервер (2) в стойку, пока он не встанет на место.



9. На любой из двух сторон сервера можно установить кабельный кронштейн. На следующем рисунке показан кабельный кронштейн, установленный на левой стороне. Для установки кабельного кронштейна с правой стороны выполните инструкции и установите оборудование с противоположной стороны. Соедините один конец опорного рычага (1) с той направляющей, к которой планируется прикрепить кабельный кронштейн, чтобы другой конец опорного рычага (2) можно было повернуть к стойке.

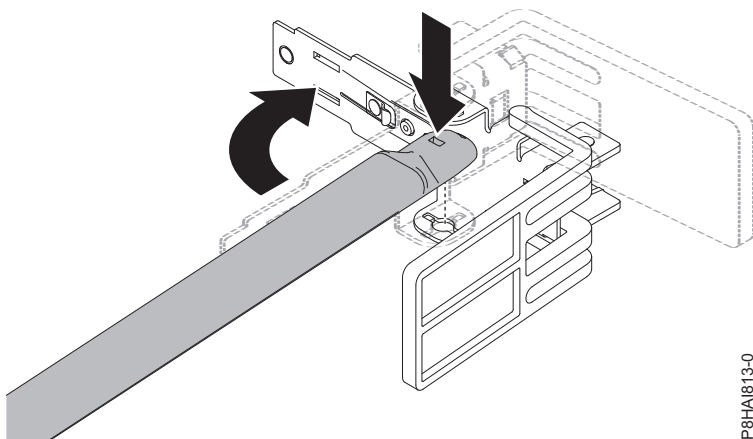


P8HA1812-0

Стойка - вид сзади

Рисунок 42. Соединение опорного рычага

10. Соедините другой конец опорного рычага со стопорной скобой кабельного кронштейна (1). Поверните скобу (2), чтобы прикрепить ее к опорному рычагу.



P8HA1813-0

Рисунок 43. Стопорная скоба кабельного кронштейна, закрепленная на опорном рычаге

11. На штырях кабельного кронштейна напечатаны заглавные буквы **I** и **O**, которые указывают на внутренний и внешний штыри. Установите кабельную стопорную скобу (с заглавной буквой **O**) на свободный конец опорного рычага. Убедитесь, что опорный рычаг установлен.

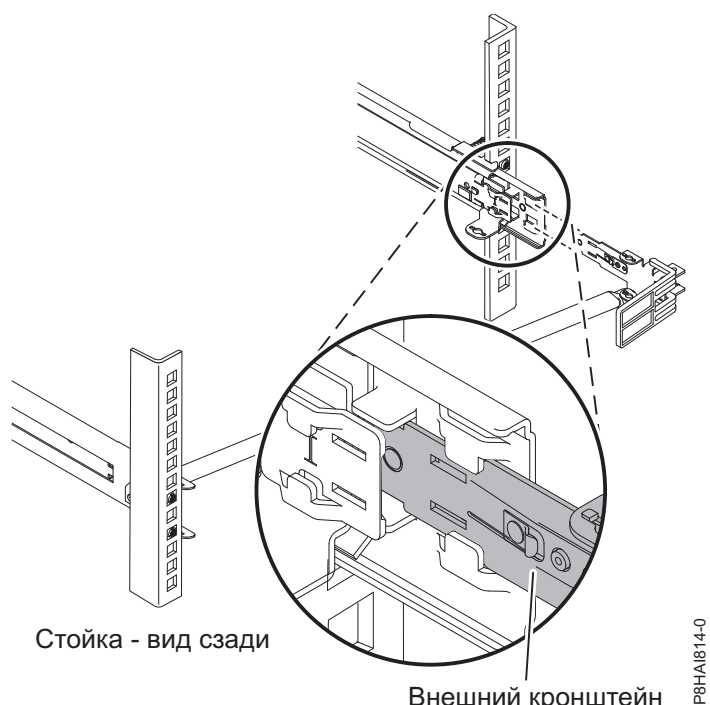


Рисунок 44. Подключение стопорной скобы к направляющей

12. Установите кабельный кронштейн на опорный рычаг. Вытяните внутренний и внешний штыри кабельного кронштейна, затем вставьте фиксатор кронштейна в прорезь на внутренней стороне направляющей. Нажимайте на фиксаторы, пока они не защелкнутся.

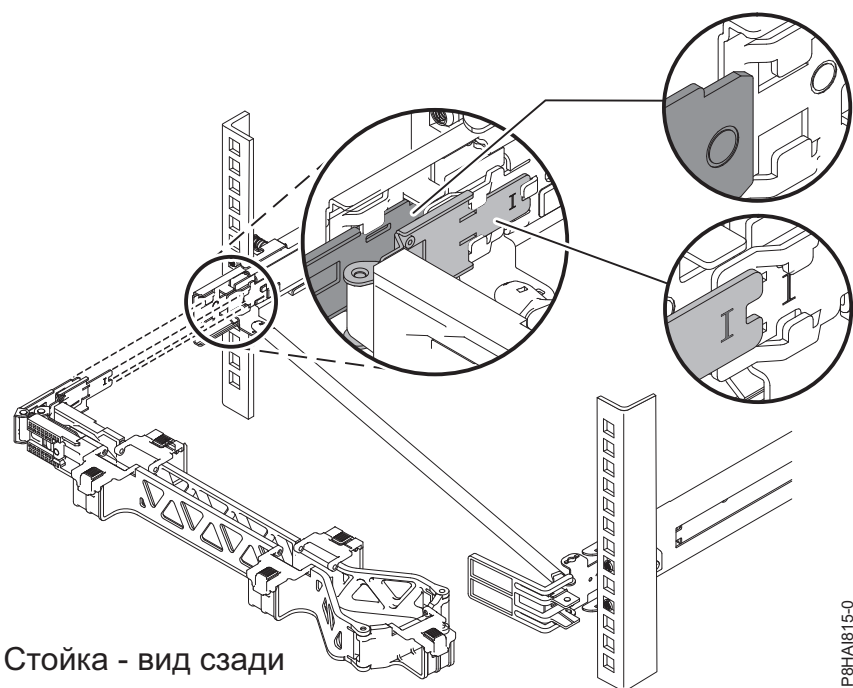
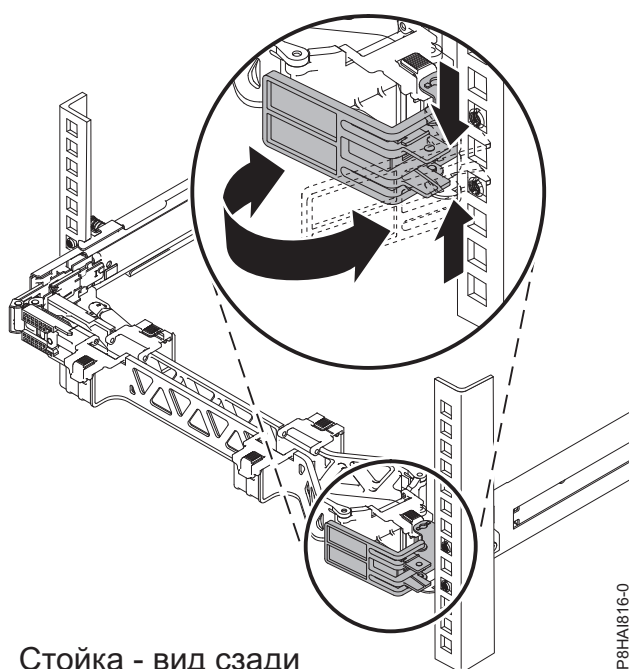


Рисунок 45. Соединение кабельного кронштейна

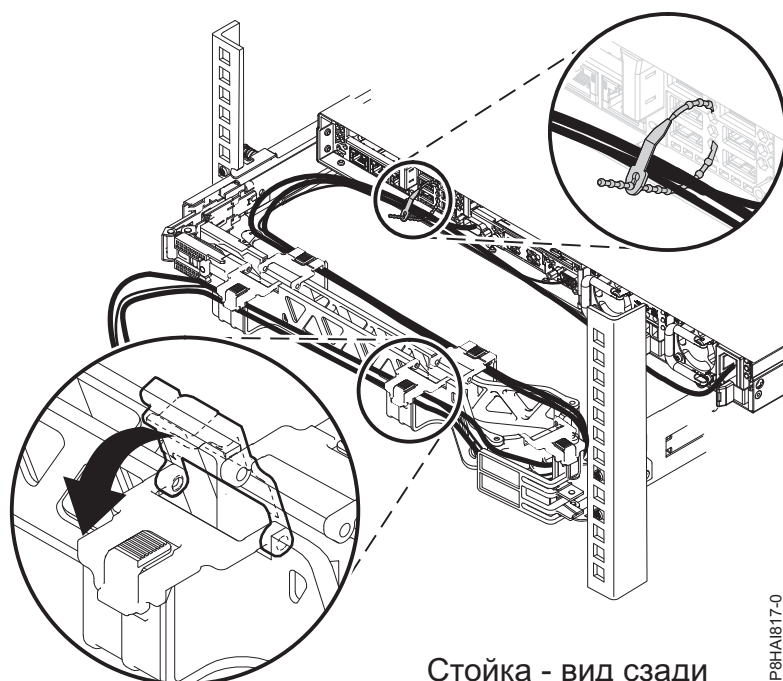
13. Для того чтобы облегчить поворот кабельного кронштейна на опорном рычаге можно открыть стопорную скобу, нажав на фиксаторы выше и ниже стопорной скобы, чтобы закрыть ее.



Стойка - вид сзади
Рисунок 46. Стопорная скоба кабельного кронштейна

14. Подсоедините к задней части сервера кабели питания и другие кабели (кабель клавиатуры, монитора и мыши, если это необходимо). Проложите эти кабели вдоль кабельного кронштейна и закрепите их с помощью кабельной стяжки или зажимов с кольцом и крючком.

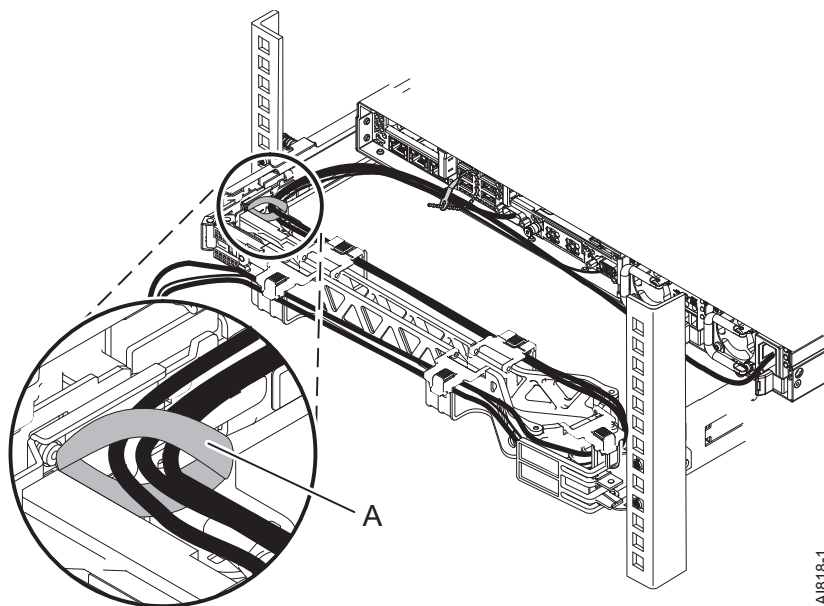
Примечание: Расположение кабельных стяжек зависит от конкретной системы. С помощью кабельных стяжек в задней части системы закрепите кабели, чтобы предотвратить их провисание.



Стойка - вид сзади
Рисунок 47. Подсоединение и прокладка кабеля питания

15. Кабели поставляются вместе с липучками для правильного перемещения кабельного кронштейна.

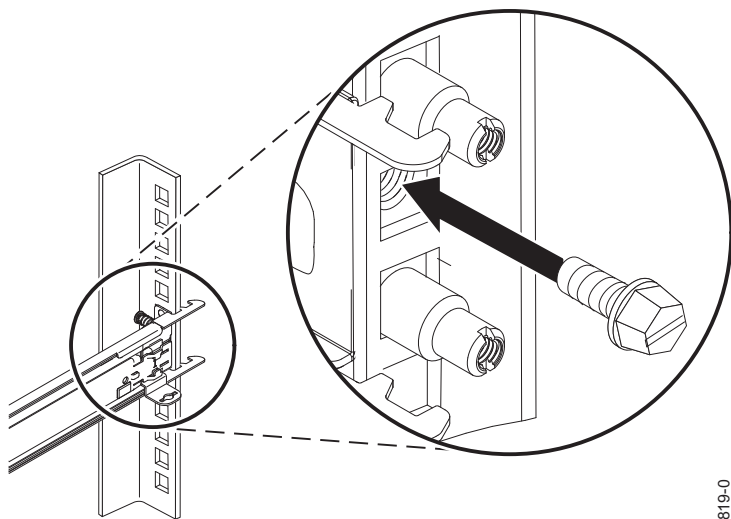
Примечание: Убедитесь, что кабели не провисают ниже отсека U, чтобы они не мешали системам внизу. При прокладке кабелей оставляйте слабинку, чтобы избежать их натяжения при перемещении кронштейна.



Стойка - вид сзади

Рисунок 48. Фиксатор на липучке

16. Если стойка перевозится с установленной системой или расположена в условиях повышенной вибрации, вставьте винты М6 в заднюю часть направляющих. При необходимости с помощью кабельной стяжки прикрепите свободный конец кабельного кронштейна к стойке.



Стойка - вид сзади

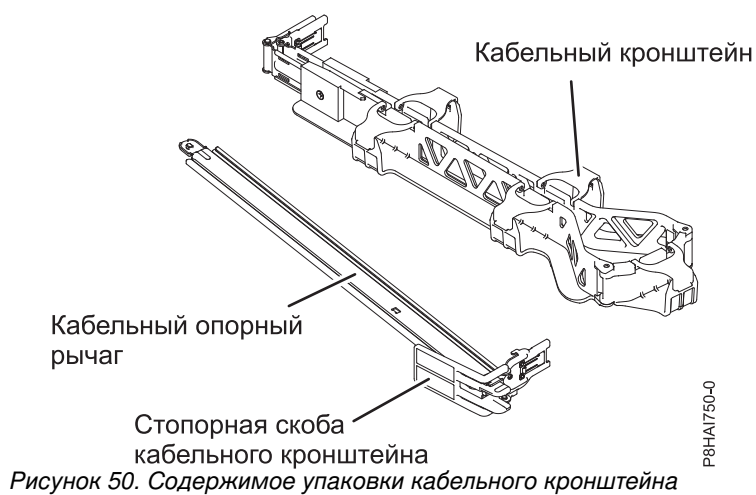
Рисунок 49. Подготовка сервера к перевозке

Установка НМС 7042-CR9 в стойку

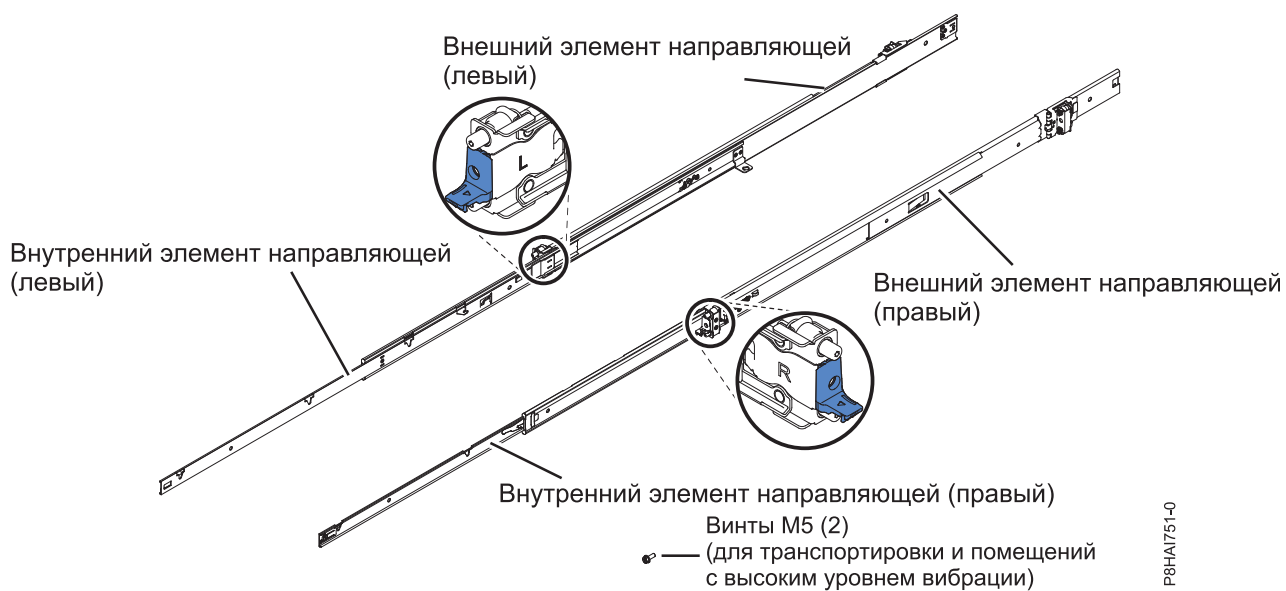
Рассмотрена установка консоли аппаратного обеспечения (НМС) 7042-CR9 в стойку.

Сверьтесь со списком поставки. Компоненты, необходимые для установки сервера в стойку, показаны на следующих рисунках. Если какие-то компоненты отсутствуют или повреждены, обратитесь к продавцу.

Содержимое упаковки кабельного кронштейна



Содержимое упаковки направляющей



Примечание: Для установки потребуется упаковка направляющей и кабельного кронштейна.

Для установки НМС 7042-CR9 в стойку выполните следующие действия:

1. Выберите отсек (в зависимости от устанавливаемого сервера) в стойке для установки сервера.

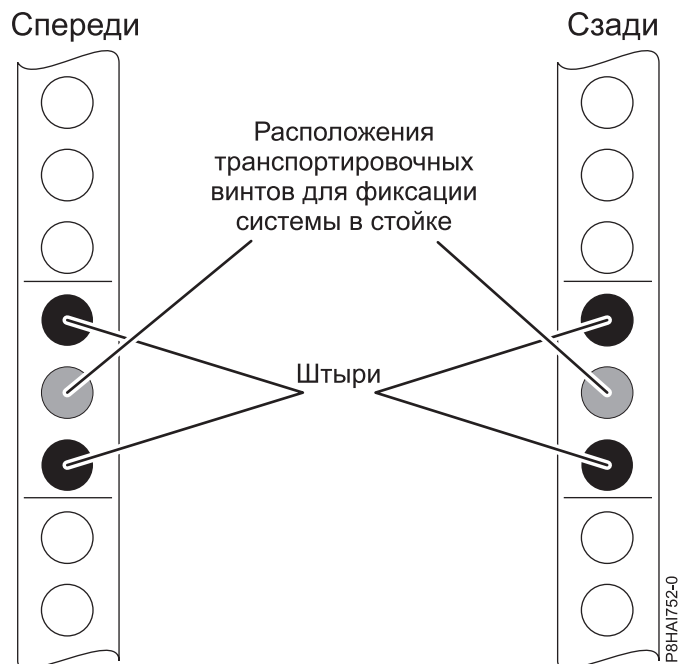


Рисунок 52. Определение отсека в стойке

Примечание: Требуется отсек высотой 1 U, в нижней части которого устанавливаются направляющие.

2. Вытяните внешний элемент направляющей назад до конца. Будет слышен отчетливый щелчок. Монтажный кронштейн в задней части стойки теперь повернут в открытое положение.

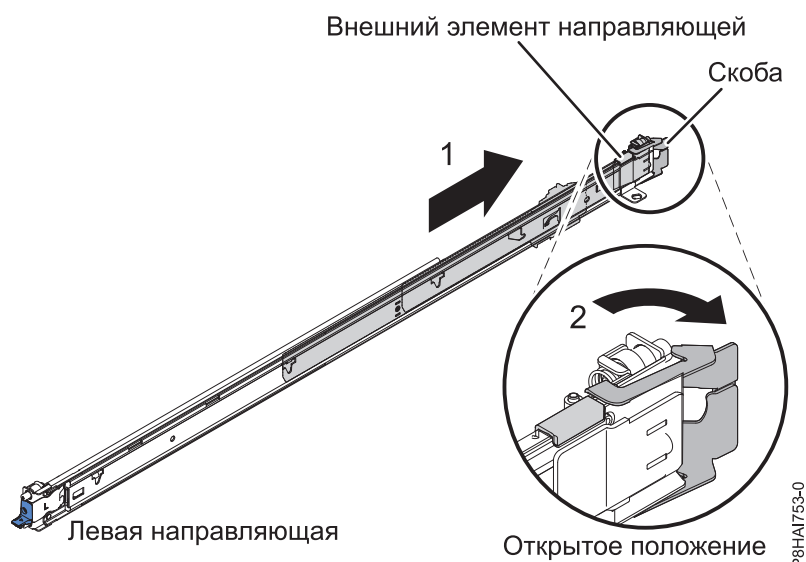


Рисунок 53. Направляющая и внешний элемент направляющей

Примечание: В конце каждой направляющей расположена метка **R (right)** или **L (left)**.

3. Совместите задний конец внешнего элемента направляющей с отверстиями в задней части стойки. Штыри направляющей должны войти в отверстия. Два штыря на направляющей выступают из верхнего и нижнего отверстий во фланце EIA. Перемещайте направляющую в сторону задней части стойки до тех пор, пока монтажный кронштейн не встанет на место.

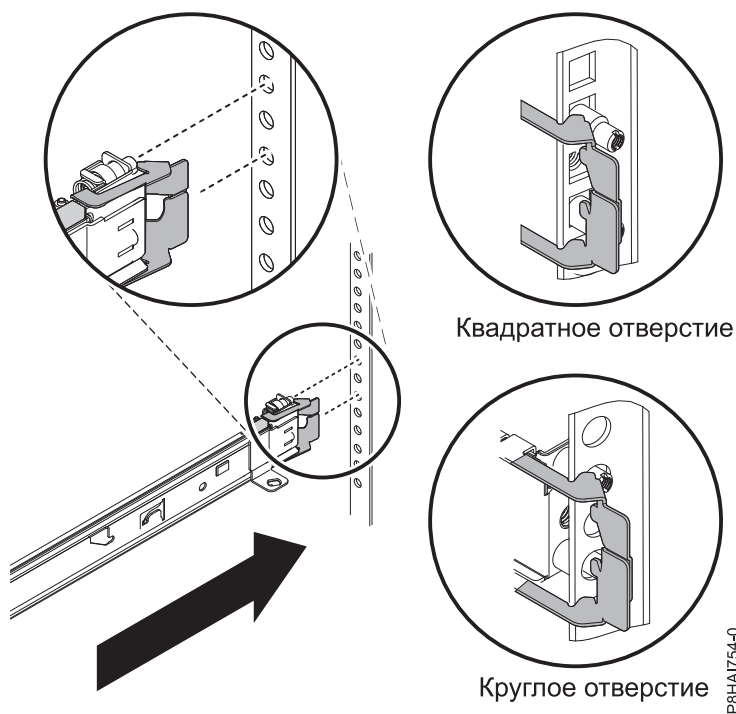


Рисунок 54. Совместите штыри с отверстиями в задней части стойки

4. Поверните переднюю защелку в открытое положение и совместите передний конец внешнего элемента направляющей с отверстиями в передней части стойки. Совместите штыри с отверстиями на фланцах EIA и потяните направляющую вперед, чтобы штыри выступали из отверстий. Закройте переднюю часть направляющей, повернув переднюю защелку в закрытое положение. Повторите шаги 2-4 для другого внешнего элемента направляющей.

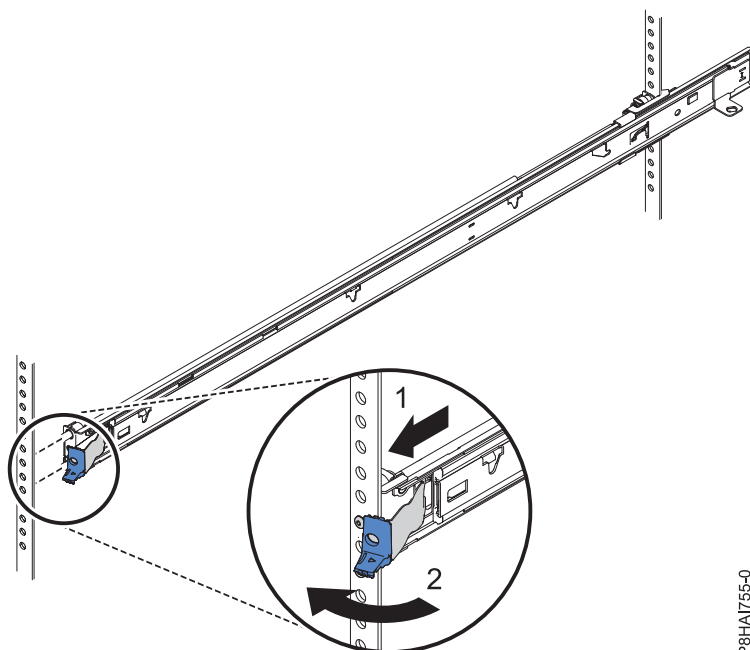


Рисунок 55. Передняя защелка направляющей

5. Нажмите защелки (1). При перемещении стойки или в случае установки стойки в помещении с высоким уровнем вибрации затяните винты M5 (2) на передней части сервера.

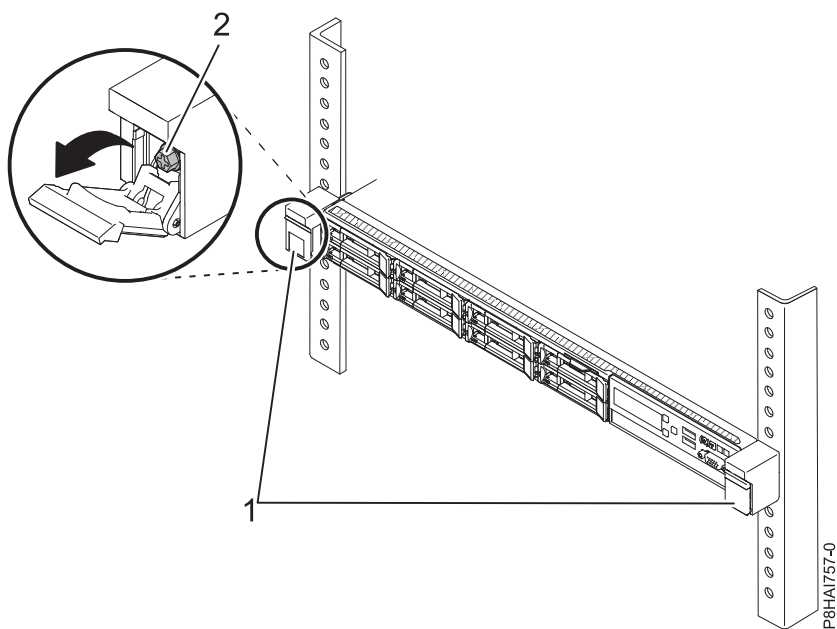


Рисунок 56. Направляющая и штыри в передней части стойки

6. Потяните направляющие вперед **(1)** до двойного щелчка. Осторожно поднимите сервер и установите его в наклонном положении над направляющими, чтобы совместить головки штифтов **(2)** на задней части корпуса сервера с прорезями в направляющих. Опускайте сервер, пока головки штифтов не войдут в две задние прорези, а затем медленно опустите переднюю часть сервера **(3)**, чтобы остальные головки штифтов также вошли в прорези на направляющих. Убедитесь, что передняя защелка накрывает переднюю головку штифта и система зафиксирована в направляющих.

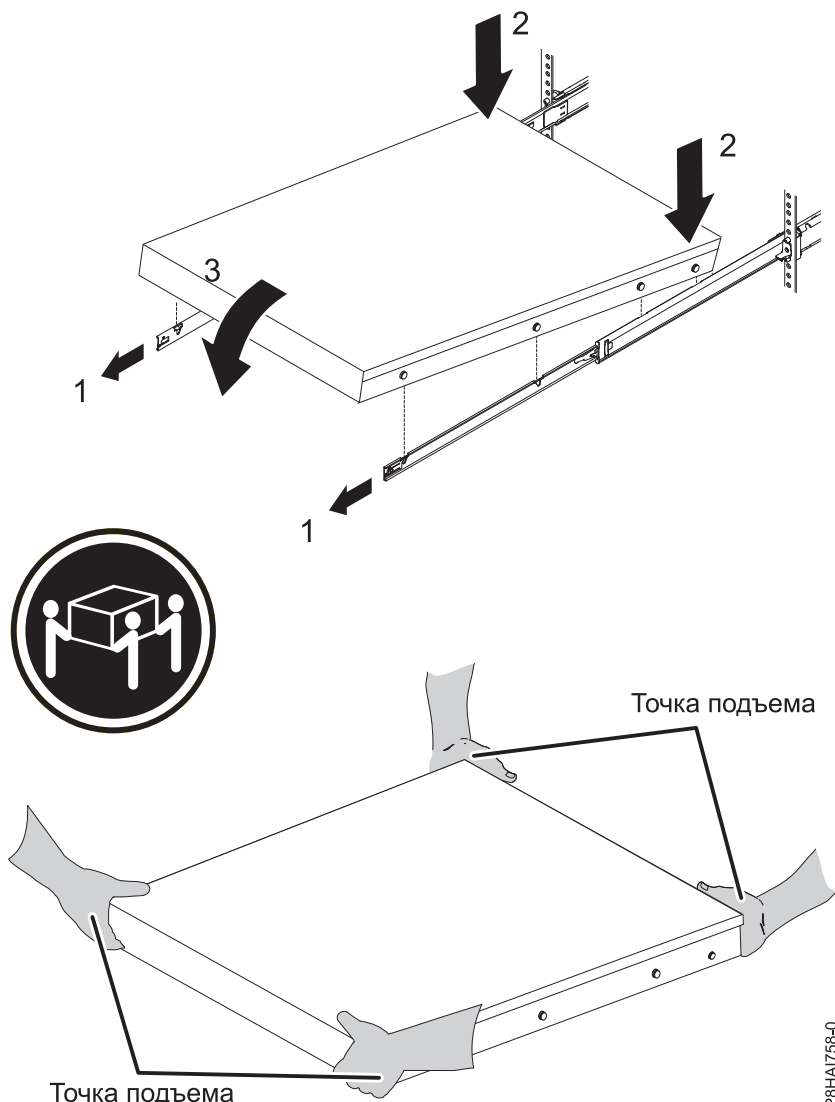


Рисунок 57. Направляющие выдвинуты, головки штифтов сервера совмещены с прорезями в направляющих и точками подъема

Примечание: При подъеме соблюдайте технику безопасности. Сервер 1 U должны поднимать по крайней мере два человека. Их руки должны быть расположены, как показано на рис. 57.

7. Поднимите стопорные рычаги (1) на направляющих и задвигайте сервер (2) в стойку, пока он не встанет на место.

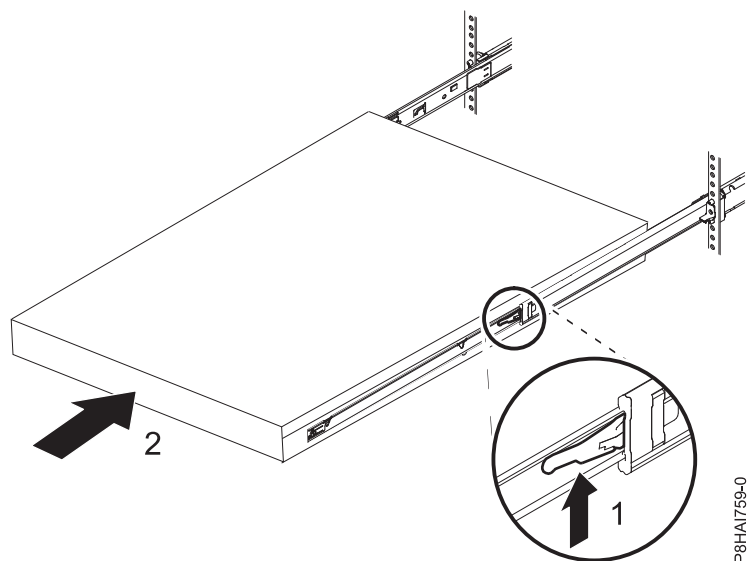


Рисунок 58. Защелки и сервер

8. На любой из двух сторон сервера можно установить кабельный кронштейн. На рис. 59 показан кабельный кронштейн, установленный на левой стороне. Рекомендуется установить кабельный кронштейн напротив блоков питания, чтобы обеспечить доступ к блокам питания. Для установки кабельного кронштейна с правой стороны выполните инструкции и установите оборудование с противоположной стороны. Поместите штырь (1) в горизонтальный прорезь в задней части направляющих. Затем поверните другой конец рычага (2) в сторону стойки.

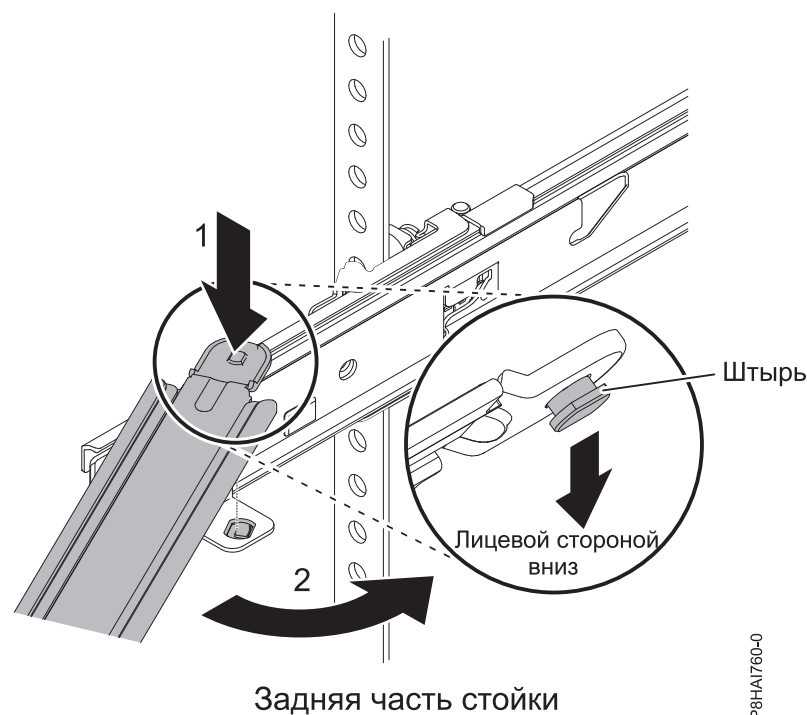


Рисунок 59. Соединение опорного рычага

Примечание: Кабельный опорный рычаг должен быть расположен сверху фиксатора направляющей.

9. Установите кабельную стопорную скобу (с заглавной буквой **O**) на свободный конец опорного рычага. Убедитесь, что опорный рычаг установлен.

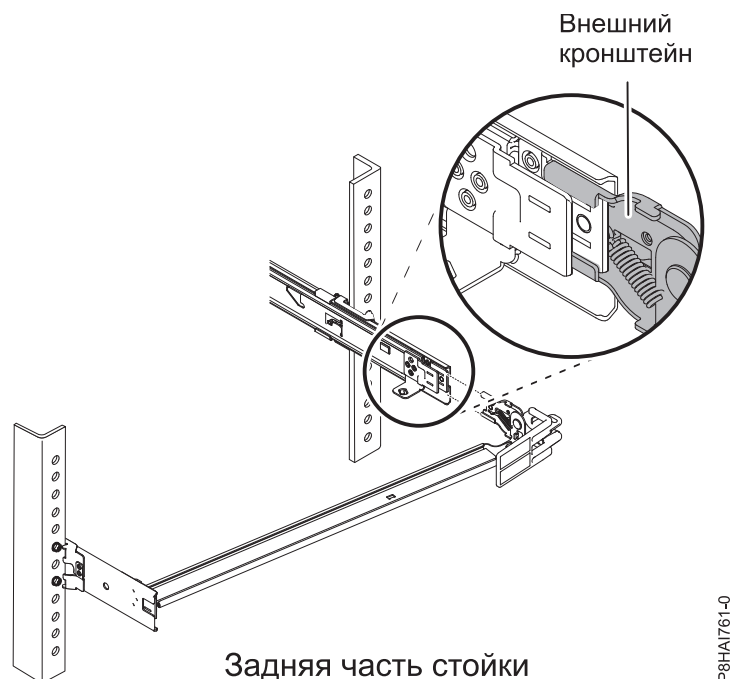


Рисунок 60. Подключение стопорной скобы к направляющей

P8HA1761-0

Примечание: На штырях кабельного кронштейна напечатана заглавная буква **O**, которая указывает на внешний штырь.

10. Установите кабельный кронштейн на опорный рычаг. Вставьте фиксатор кабельного кронштейна в прорезь на внутренней стороне направляющей. Нажимайте на фиксаторы, пока они не защелкнутся.

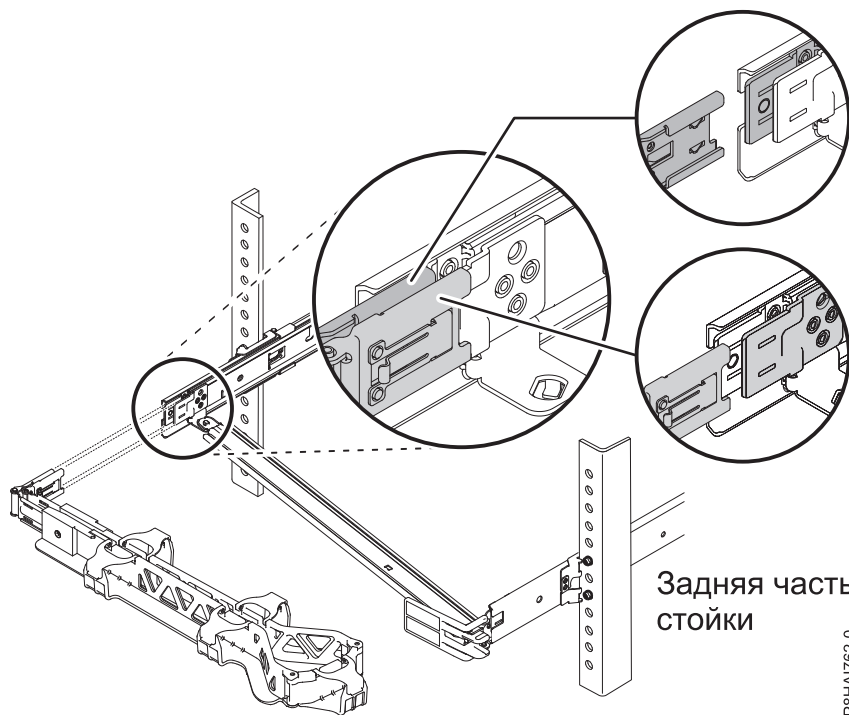
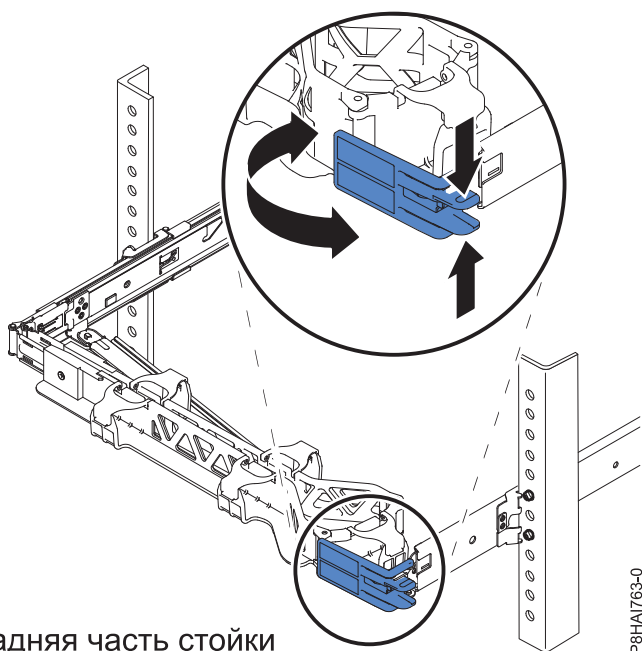


Рисунок 61. Соединение кабельного кронштейна

P8HA1762-0

11. Для того чтобы облегчить поворот кабельного кронштейна на опорном рычаге можно открыть стопорную скобу, нажав на фиксаторы выше и ниже опорного рычага.

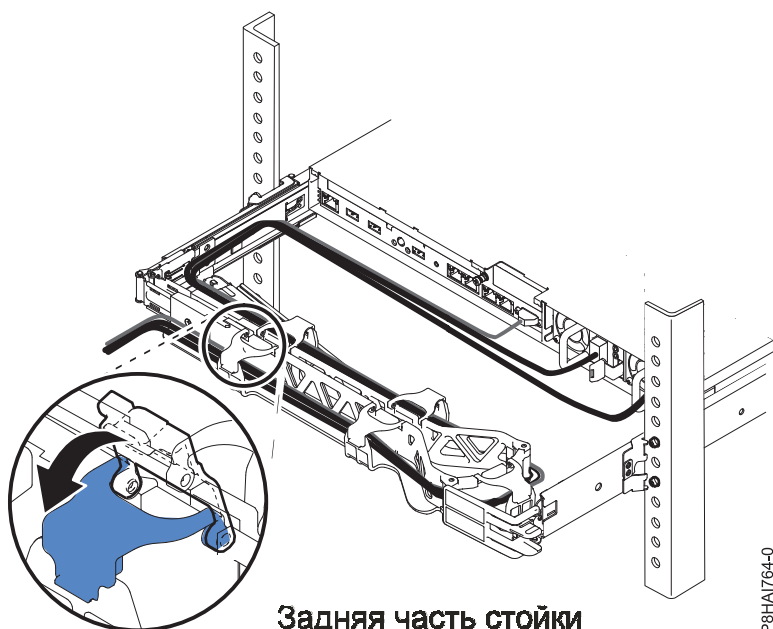


Задняя часть стойки

Рисунок 62. Стопорная скоба кабельного кронштейна

12. Подсоедините к задней части сервера кабели питания и другие кабели (кабель клавиатуры, монитора и мыши, если это необходимо). Проложите эти кабели вдоль кабельного кронштейна и закрепите их с помощью кабельной стяжки или зажимов с кольцом и крючком.

Примечание: Расположение кабельных стяжек зависит от конкретной системы. С помощью кабельных стяжек в задней части системы закрепите кабели, чтобы предотвратить их провисание.



Задняя часть стойки

Рисунок 63. Подключение и прокладка кабеля питания

13. Кабели поставляются вместе с хомутами для правильного перемещения кабельного кронштейна.

Примечание: Убедитесь, что кабели не провисают ниже отсека U, чтобы они не мешали системам внизу. При прокладке кабелей оставляйте слаbinу, чтобы избежать их натяжения при перемещении

кронштейна.

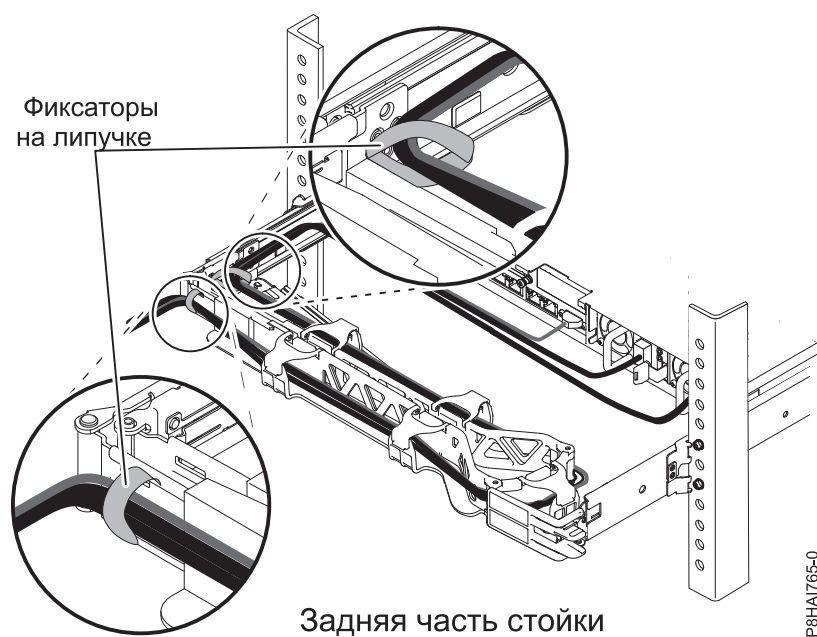


Рисунок 64. Фиксатор на липучке

14. Если стойка перевозится с установленной системой или расположена в условиях повышенной вибрации, вставьте винты М5 в заднюю часть направляющих. При необходимости с помощью кабельной стяжки прикрепите свободный конец кабельного кронштейна к стойке.

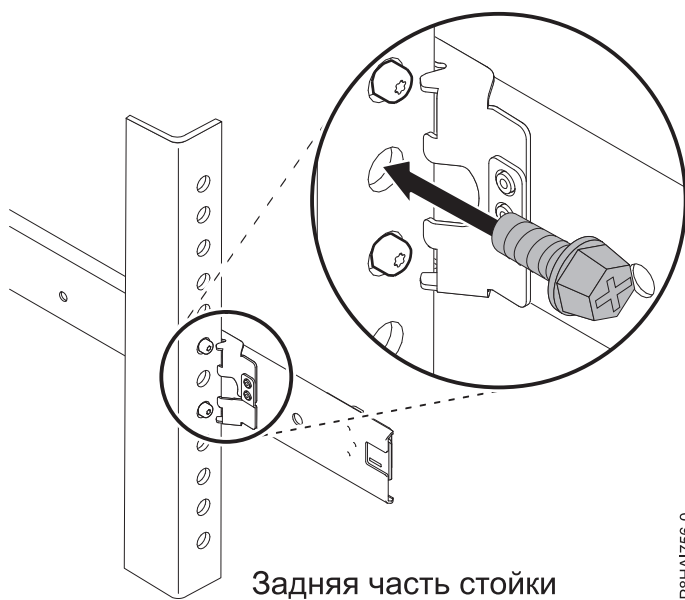


Рисунок 65. Подготовка сервера к перевозке

Установка 7063-CR1 в стойку

Рассмотрена установка консоли аппаратного обеспечения (НМС) 7063-CR1 в стойку.

Предварительные требования для установки монтируемой в стойке системы 7063-CR1

Рассмотрены предварительные требования для установки системы.

Перед тем как приступить к установке сервера, рекомендуется ознакомиться со следующими документами:

- Последняя версия этого документа опубликована в Интернете: Установка 7063-CR1 в стойке (http://www.ibm.com/support/knowledgecenter/POWER8/p8hai/p8hai_install7063_kickoff.htm).
- Инструкции по планированию установки сервера приведены в разделе Планирование системы (http://www.ibm.com/support/knowledgecenter/POWER8/p8had/p8had_8xx_kickoff.htm).

Перед тем как приступить к установке, подготовьте следующие компоненты:

- Крестовая отвертка
- Плоская отвертка
- Канцелярский нож
- Браслет заземления
- Стойке со свободным отсеком высотой в две единицы (2U) EIA (Electronic Industries Association).

Примечание: Если стойка не установлена, установите ее. Соответствующие инструкции приведены в разделе Стойки и компоненты стоек (http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/p8hbf_8xx_kickoff.htm).

Инвентаризация системы

Приведены инструкции по инвентаризации системы.

1. Убедитесь, что получены все заказанные коробки.
2. Распакуйте компоненты сервера.
3. Выполните опись компонентов перед установкой каждого компонента сервера. Для этого выполните следующие действия:
 - a. Найдите инвентарную опись сервера.
 - b. Проверьте, все ли заказанные компоненты получены.

Примечание: Информация о заказе поставляется вместе с продуктом. Информацию о заказе можно получить от торгового представителя или делового партнера IBM.

Если часть компонентов не соответствует заказу, отсутствует или повреждена, обратитесь по любому из следующих адресов:

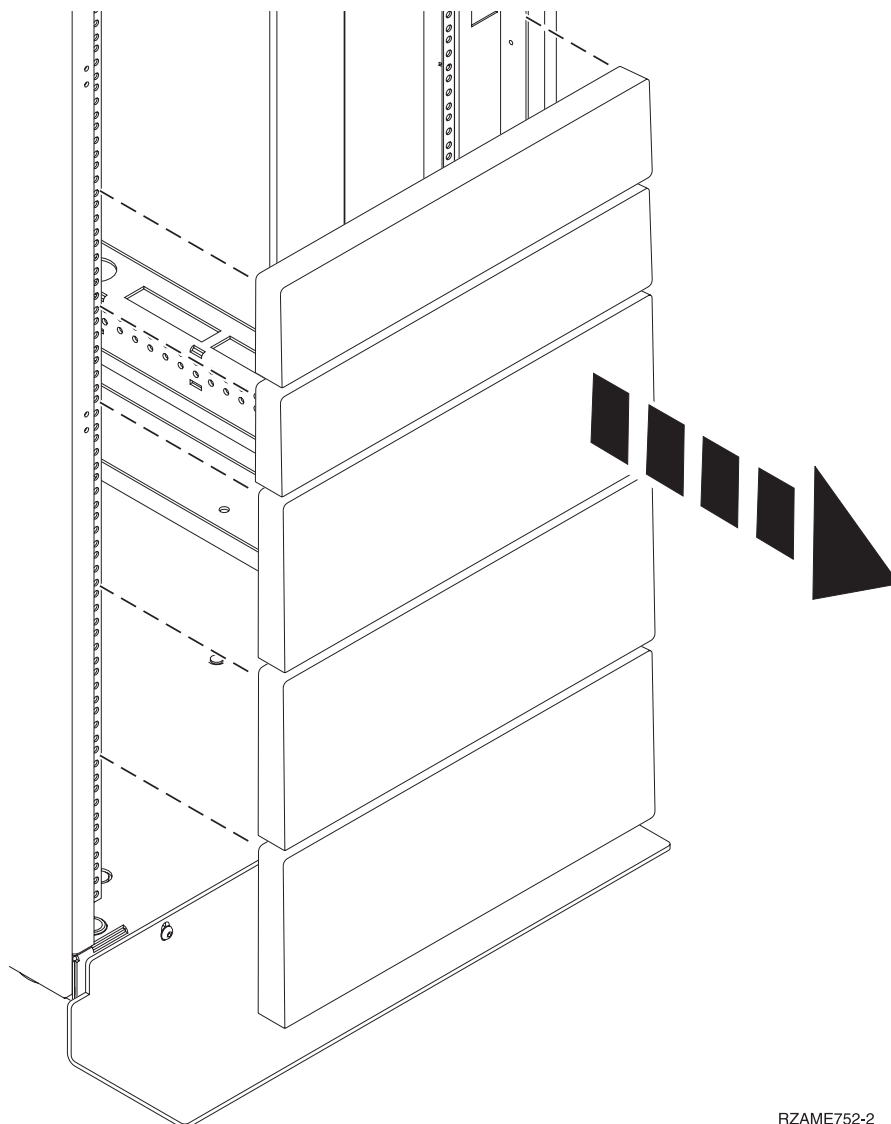
- Торговый посредник IBM.
- Автоматизированная информационная линия производителя IBM Rochester: 1-800-300-8751 (только США).
- Directory of worldwide contacts <http://www.ibm.com/planetwide>. Выберите свое расположение, чтобы просмотреть контактную информацию службы поддержки.

Определение расположения в стойке и его маркировка для системы 7063-CR1

Вам может потребоваться определить расположение для установки системного блока в стойке.

1. Ознакомьтесь с разделом Техника безопасности при работе со стойкой (<http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/racksafety.htm>).
2. Выберите место для размещения системного блока в стойке. В процессе планирования установки системного блока в стойке рекомендуется учитывать следующую информацию:
 - Самые большие и тяжелые блоки следует размещать внизу стойки.
 - Сначала устанавливайте блоки в нижней части стойки.
 - Укажите в плане отсеки в единицах EIA (Electronic Industries Alliance).

3. При необходимости удалите заглушки для получения доступа внутрь стойки там, где вы планируете разместить блок (см. рис. 66).



RZAME752-2

Рисунок 66. Снятие заглушек

4. Выберите место для размещения системы в стойке. Запишите расположение EIA.
5. Став лицом к стойке и работая с правой стороны стойки, с помощью скотча, маркера или карандаша отметьте нижнее отверстие каждого модуля EIA.
6. Повторите шаг 5 для соответствующих отверстий, расположенных с левой стороны стойки.
7. Зайдите в тыл стойки.
8. На правой стороне найдите единицу EIA, соотносящуюся с нижней помеченной единицей EIA спереди стойки.
9. Отметьте нижний модуль EIA.
10. Пометьте соответствующие отверстия на левой стороне стойки.

Установка НМС в стойку с помощью фиксированных направляющих

В случае установки НМС 7063-CR1 в стойку с помощью фиксированных направляющих выполните следующие задачи.

Присоединение фиксированных направляющих к шасси системы и стойке:

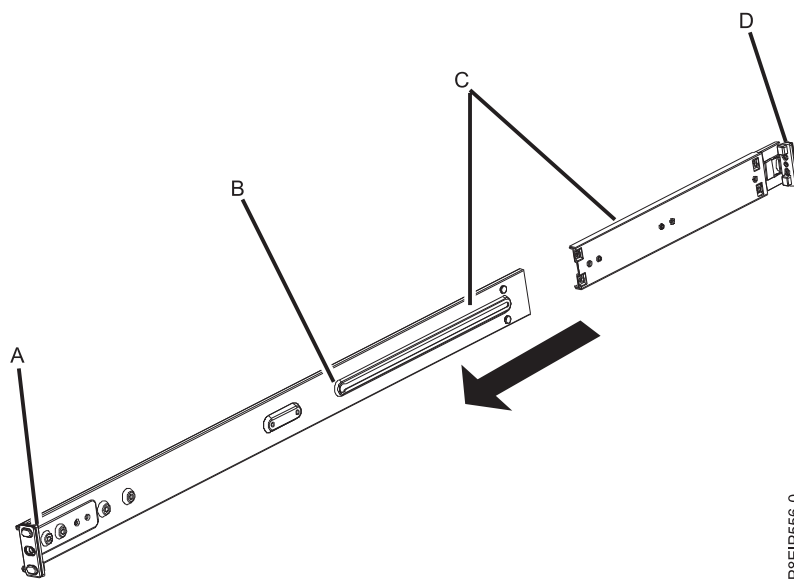
Направляющие необходимо установить на шасси и в стойку. Используйте эту процедуру для выполнения этой задачи.

Внимание: Для того чтобы избежать неправильной установки направляющих, травм и повреждения блока, убедитесь, что для стойки подготовлены подходящие направляющие и крепежные элементы. Направляющие и крепежные элементы должны соответствовать отверстиям в опорных фланцах (квадратные отверстия или отверстия с резьбой). Не устанавливайте неподходящее оборудование с помощью шайб или вставок. Если комплект направляющих и крепежных элементов отсутствует, обратитесь к посреднику IBM.

Примечание: Для установки системы требуется свободный отсек высотой 1 EIA (1U).

Проверьте наличие необходимых элементов для установки направляющих. В комплект направляющих входят следующие элементы:

- Винты направляющих, применяемые для прикрепления двух компонентов каждой направляющей
 - Винты, применяемые для прикрепления направляющих к стойке
 - Направляющие
 - Винты 10 - 32 x 0.635 см (0.25 дюйма), применяемые для прикрепления направляющих к шасси системы
1. Извлеките все элементы из упаковки и положите их на рабочую поверхность.
 2. Соедините две части каждой направляющей. Для соединения двух частей каждой направляющей выполните следующие задачи:
 - a. Определите две части левой направляющей. Выровняйте короткую и длинную части (C). Штифты направляющей должны быть направлены в одну сторону (A) и (D).



- b. Короткая часть направляющей имеет металлический штифт. Вставьте штифт в отверстие в длинной части направляющей (B). Задвиньте короткую часть направляющей в длинную часть.
- c. Совместите отверстия в двух частях направляющей. С помощью крестовой отвертки соедините две части, свободно закрутив винты в отверстия.

Примечание: Не затягивайте винты направляющей.

- d. Повторите эти шаги для правой направляющей.
3. Прикрепите направляющие шасси к шасси системы. Для прикрепления направляющих шасси к шасси системы выполните следующие действия:

- a. В левой части системы совместите металлические штыри на левой части шасси системы с квадратными отверстиями на левой направляющей. Задвигайте направляющую в сторону передней части стойки до тех пор, пока она не встанет на место.
 - b. Прикрепите направляющую к шасси системы с помощью двух винтов из комплекта направляющих.
 - c. Повторите процедуру для направляющей шасси на правой стороне системы.
4. Установите направляющие в стойку.
- a. Перейдите к передней стороне стойки.
 - b. Выберите левую направляющую и найдите ранее отмеченный блок EIA. На каждой направляющей находится метка **Back**, соответствующая задней части стойки. Убедитесь, что вы держите переднюю часть направляющей.
 - c. Раздвиньте направляющую из передней в заднюю часть стойки и совместите штифты на направляющей с ранее отмеченными отверстиями на фланце стойки.
 - d. Вставьте штифты в задний фланец стойки до щелчка.
 - e. Потяните переднюю часть направляющей в сторону переднего фланца стойки. Совместите штифты на направляющей с отверстиями на фланце стойки, затем вставьте их до щелчка.
 - f. С помощью отвертки затяните винты, установленные на шаге 2.
 - g. Повторите шаги 4a - 4f для правой направляющей.
5. Закрепите направляющие в стойке.
- a. Перейдите к задней части стойки.
 - b. Установите шайбу на каждый длинный винт из комплекта направляющих.
 - c. Закрутите винт с шайбой через среднее отверстие каждой направляющей с обеих сторон в задней части стойки.

Установка системы в стойку, подключение и прокладка кабелей питания:

После установки системы на направляющие в стойке подключите и проложите кабели питания.

Примечание: Для установки системы в стойку необходимо два человека.

1. Снимите защитную пластиковую пленку с верхней части шасси системы.
2. Перейдите к передней стороне стойки.
3. Вдвоем поднимите систему и выровняйте направляющие на шасси систем с направляющими, установленными в стойке.
4. Пока один человек удерживает систему, второй должен осторожно задвинуть систему в стойку, чтобы каждая направляющая встала на место до щелчка.
5. Надавите на систему спереди.
6. Закрепите систему в стойке, закрутив винты через ручки с обеих сторон шасси системы.
7. Вставьте кабели питания в источники питания.

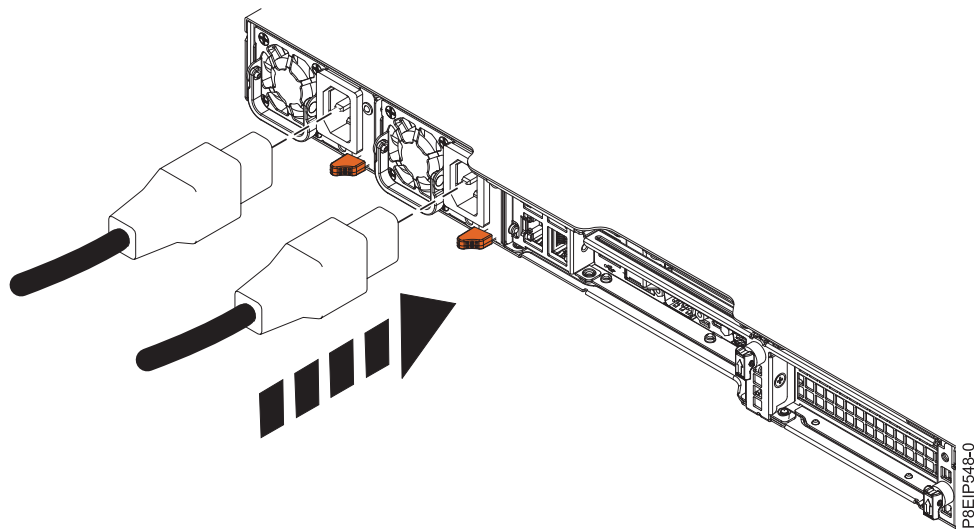


Рисунок 67. Вставка кабелей питания в источники питания

8. Подключите все кабели к задней части сервера.

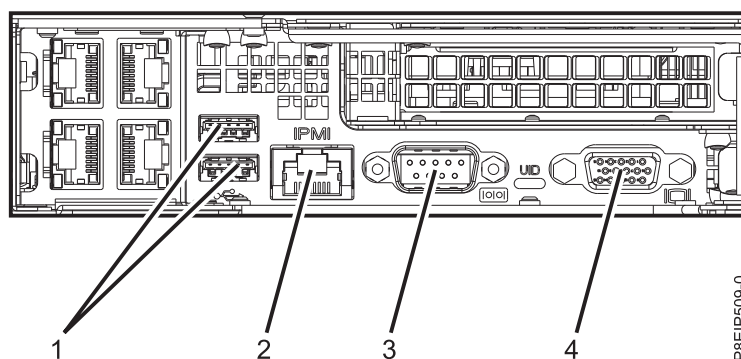


Рисунок 68. Задние порты

Таблица 9. Входные и выходные порты

Идентификатор	Описание
1	USB 2.0 применяется для подключения клавиатуры и мыши
2	IPMI (интерфейс интеллектуального управления платформой) Ethernet
3	Последовательный IPMI
4	Для подключения монитора применяется режим Video Graphics Array (VGA). Поддерживается только режим VGA 1024 x 768 с частотой 60 Гц. Длина кабеля не может превышать 3 метра. В настоящее время поддерживается только текстовый режим.

9. Подключите кабели питания системы и других устройств к источнику переменного тока (AC).
10. Перейдите к “Настройка НМС с помощью интерфейса НМС Enhanced+” на стр. 119.

Установка НМС в стойку с помощью направляющих

В случае установки НМС в стойку с помощью направляющих выполните следующие задачи.

Присоединение направляющих к системе и стойке:

Присоедините направляющие к сначала системе, а затем к стойке.

Внимание: Для того чтобы избежать неправильной установки направляющих, травм и повреждения блока, убедитесь, что для стойки подготовлены подходящие направляющие и крепежные элементы. Направляющие и крепежные элементы должны соответствовать отверстиям в опорных фланцах (квадратные отверстия или отверстия с резьбой). Не устанавливайте неподходящее оборудование с помощью шайб или вставок. Если комплект направляющих и крепежных элементов отсутствует, обратитесь к посреднику IBM.

Направляющие поставляют в полностью собранном виде. Для установки направляющих в стойку необходимо разобрать направляющие на четыре части.

1. Удалите нижние винты кросс-платы DASD с обеих сторон, чтобы освободить место для обслуживания кросс-платы без извлечения системы из стойки.

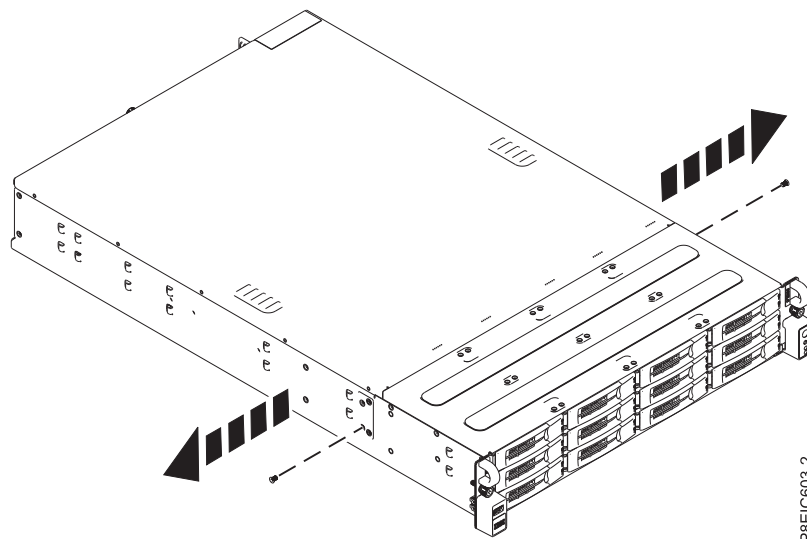


Рисунок 69. Удаление винтов кросс-платы DASD

2. Прикрепите направляющие системы с обеих сторон шасси системы. В задней части шасси системы совместите защелки на шасси системы (B) с разъемами на направляющей (A). Потяните направляющую вперед таким образом, чтобы защелки встали на место.

Примечание: Направляющие системы с меткой **L** устанавливаются с левой стороны системы, а направляющие с меткой **R** - с правой стороны (относительно передней части системы).

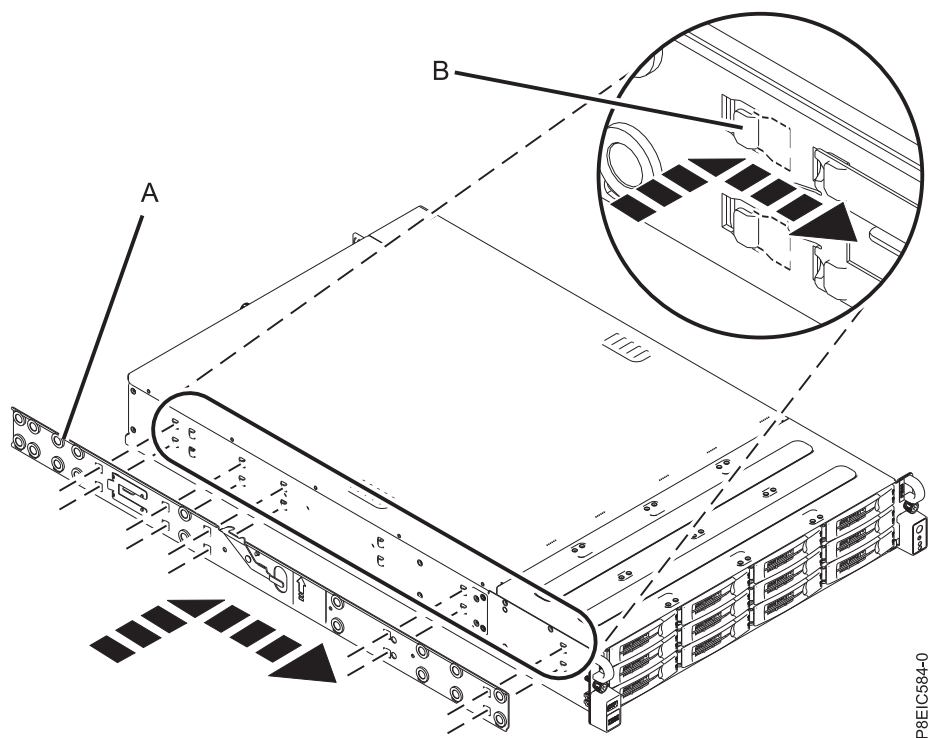


Рисунок 70. Присоединение направляющей к шасси на левой стороне системы

3. Установите крепежный винт на каждую направляющую системы, чтобы прикрепить направляющую к шасси системы.

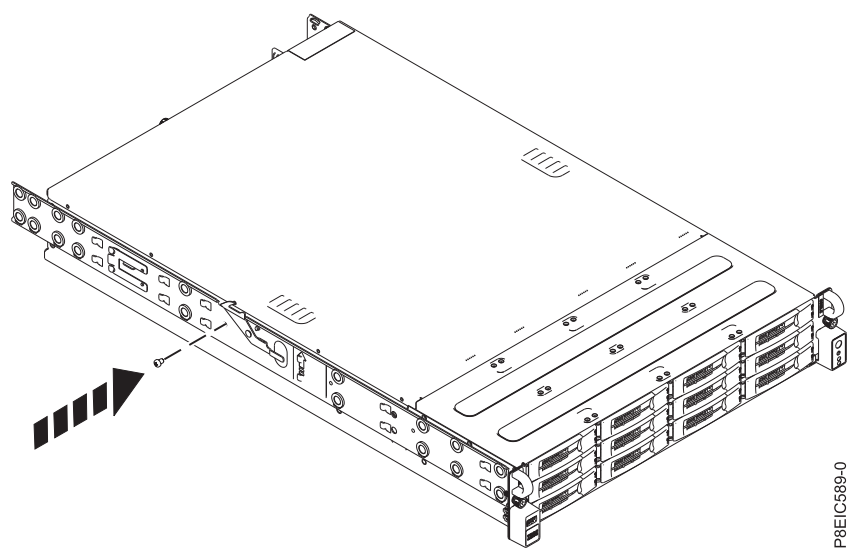
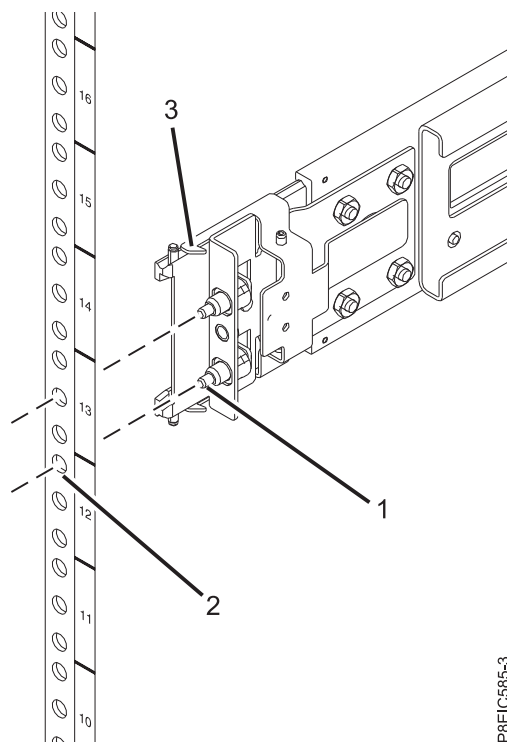


Рисунок 71. Присоединение крепежного винта направляющей к шасси на левой стороне системы

4. Установите направляющие в стойку. Каждая направляющая помечена буквой **R** (правая) или буквой **L** (левая), если смотреть спереди. Выберите правую направляющую, поднесите ее к передней части стойки и найдите выбранный блок EIA.
5. С передней части стойки вставьте штифты на передней части направляющей (1) в ранее помеченные отверстия в передней части стойки (2). Потяните направляющую вперед, чтобы гайка с зажимом (3)

попала во фланец направляющей и встала на место.



P8E/C585-3

Рисунок 72. Установка направляющей в передней части стойки

6. Повторите шаги 3 и 4 для левой направляющей.
7. Перейдите к задней части стойки. Потяните направляющую на себя, чтобы вставить два штыря (1) в отверстия в стойке (2). Тяните направляющую до тех пор, пока пружинная защелка (3) не встанет на место. С помощью винта (4) закрепите направляющую в стойке.

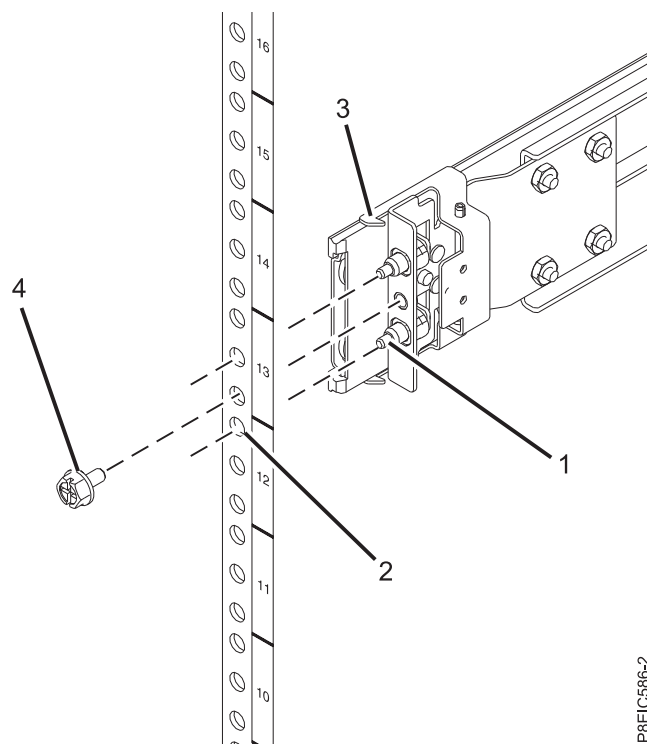


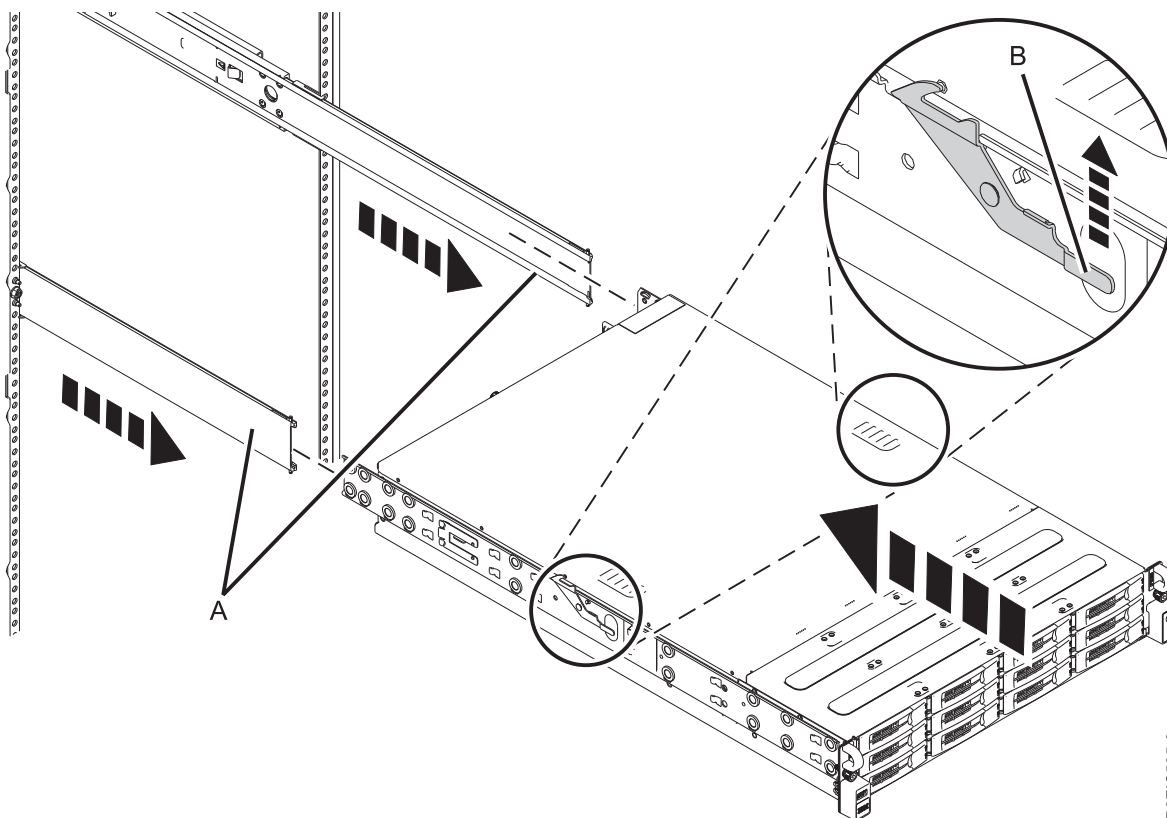
Рисунок 73. Установка направляющей в задней части стойки

Установка системы в стойку, подключение и прокладка кабелей питания:

После установки системы на направляющие в стойке подключите и проложите кабели питания.

Примечание: Для установки системы в стойку необходимо два человека.

1. Выдвиньте направляющие на полную длину, чтобы они защелкнулись в положении для обслуживания (A).
2. Вдвоем поднимите систему и выровняйте нижние цилиндрические штифты на шасси с выемками на направляющих с обеих сторон стойки.



P8E/C595-2

Рисунок 74. Выравнивание нижних цилиндрических штифтов на шасси с выемками на направляющих

3. Одновременно сдвиньте защелки с обеих сторон стойки (В), помеченные зеленой стрелкой.
4. Задвиньте систему в стойку.
5. Затяните винты с накатанными головками с обеих сторон системы, чтобы прикрепить систему к стойке.

Подключение смонтированной в стойке НМС 7063-CR1

Приведены инструкции по физической установке консоли аппаратного обеспечения (НМС).

1. Проверьте правильность расположения НМС.
2. Установите НМС в стойку. Дополнительная информация приведена в разделе “Установка 7063-CR1 в стойку” на стр. 42. После установки НМС в стойке перейдите к следующему шагу.
3. Вставьте кабель питания в НМС.
4. Подключите клавиатуру, монитор и мышь.
5. Подключите НМС к управляемому серверу через кабель Ethernet (иначе - перекрестный кабель):

Примечание: Дополнительная информация о сетевых соединениях НМС приведена в разделе “Сетевые соединения НМС” на стр. 73.

6. Если управляемая система уже установлена, можно проверить, активно ли кабельное подключение Ethernet: в процессе установки нужно смотреть на зеленые лампочки состояния и на НМС, и на портах Ethernet управляемой системы.
7. Подключите порт IPMI (интерфейс интеллектуального управления платформой) к сети.

Примечание: Это соединение необходимо для подключения к контроллеру управления платформой (ВМС) в НМС. Доступ к ВМС требуется для выполнения задач обслуживания и обновления встроенного программного обеспечения НМС. Дополнительная информация приведена в разделе “Типы сетевых соединений НМС” на стр. 73.

8. Подключите порт Ethernet НМС к порту Ethernet с меткой **НМС1** на управляемом сервере.

9. При подключении второго НМС к управляемому серверу подключите его к порту Ethernet с меткой **НМС2** на управляемом сервере.
10. Вставьте кабели питания монитора, НМС и внешнего модема НМС в электрические розетки.

Примечание: В случае подключения НМС к новой управляемой системе не подключайте управляемую систему к источнику питания.

Далее следует установить и настроить программное обеспечение НМС. Перейдите к “Настройка НМС 7063-CR1”.

Настройка НМС 7063-CR1

Приведены инструкции по установке и настройке консоли аппаратного обеспечения (НМС).

Требуемую версию НМС можно загрузить на веб-сайте Fix Central. С помощью съемного носителя (такого как диск DVD или накопитель USB) создайте загрузочный файл ISO на основе пакета НМС (образ ISO).

Примечание: Следующие варианты установки приведены в качестве примеров.

Установка НМС с помощью флэш-накопителя USB

Для того чтобы установить НМС с помощью флэш-накопителя в системе Linux, выполните следующие действия:

1. Загрузите требуемую версию НМС можно на веб-сайте Fix Central.
2. Выполните следующую команду: **dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync** (где **sdx** - это имя накопителя USB).

Примечание: Размер накопителя USB должен быть не менее 4 ГБ.

3. Вставьте накопитель USB и включите систему.

Установка НМС с помощью удаленного носителя из программы просмотра консоли

Для того чтобы установить с помощью удаленного носителя из программы просмотра консоли, выполните следующие действия:

1. Войдите в веб-интерфейс BMC (<http://<bmc-ip>>).
2. Выберите **Удаленное управление**.
3. Выберите **Перенаправление консоли**.
4. Выберите **Запустить консоль**.
5. В программе iKVM Viewer Java™ выберите **Виртуальные носители > Виртуальная память**.
6. В разделе **Тип логического накопителя** выберите **Файл ISO**.
7. Выберите **Открыть образ** и найдите файл ISO в системе.
8. Нажмите кнопку **Подключить**, чтобы смонтировать файл ISO.
9. Включите систему.

Установка НМС с помощью удаленного носителя из веб-интерфейса BMC

Для того чтобы установить с помощью удаленного носителя из веб-интерфейса BMC, выполните следующие действия:

1. Войдите в веб-интерфейс BMC (<http://<bmc-ip>>).
2. Выберите **Виртуальные носители**.
3. Выберите **Образ компакт-диска**.
4. Введите следующую информацию:

Общий хост

IP-адрес хоста SMB. Если применяется имя хоста, проверьте правильность конфигурации DNS в BMC.

Путь к образу

Путь SMB к системе. Пример: /<имя общего диска>/<остальной путь>/<имя образа>.iso

Пользователь (необязательно)

Имя пользователя для входа в систему хоста SMB.

Пароль (необязательно)

Пароль пользователя.

5. Нажмите кнопку **Сохранить**.
6. Выберите **Смонтировать**.
7. Теперь в устройстве 1 отображается следующее сообщение: **Смонтирован файл iso**.

Примечание: Если сообщение не показано, снова проверьте информацию и повторите шаги 5 - 7.

8. Включите систему.

Примечание: Server Message Block версии 3 (SMBv3) не поддерживается.

Далее следует настроить программное обеспечение НМС. Соответствующие инструкции приведены в разделе “Настройка НМС с помощью интерфейса НМС Enhanced+” на стр. 119.

Понятия, связанные с данным:

“Настройка связи BMC” на стр. 146

Можно настроить или просмотреть сетевые параметры BMC для консоли управления.

Установка Виртуальное устройство НМС

Рассмотрена процедура установки Виртуальное устройство консоли аппаратного обеспечения (НМС).

Виртуальное устройство НМС можно установить в существующей виртуализованной инфраструктуре x86 или POWER. Виртуальное устройство НМС поддерживает следующие гипервизоры виртуализации x86:

- Виртуальная машина на основе ядра (KVM)
- Xen
- VMware

Минимальные требования для запуска Виртуальное устройство НМС:

- 8 ГБ оперативной памяти
- 4 процессора
- 1 сетевой интерфейс (поддерживается до 4 интерфейсов)
- 160 ГБ дисковой памяти (рекомендуется 700 ГБ для получения правильных данных мониторинга производительности (PCM))

Примечания:

1. Виртуальное устройство НМС можно установить в системе на основе процессора с аппаратной поддержкой виртуализации Intel VT-x или AMD-V.
2. Диски DVD Виртуальное устройство НМС не являются загрузочными. Необходимо сначала смонтировать носитель, а затем скопировать файл .tgz. Способ монтирования диска DVD может зависеть от применяемой операционной системы.
3. Синтаксис команд, применяемых в следующих примерах, может зависеть от операционной системы.

Информация, связанная с данной:

НМС V8 - образы для сетевой установки и инструкции по установке

Установка Виртуальное устройство НМС в среде x86

Рассмотрена процедура установки Виртуальное устройство консоли аппаратного обеспечения (НМС) в среде x86.

Установка Виртуальное устройство НМС с помощью гипервизора KVM:

Рассмотрена установка Виртуальное устройство консоли аппаратного обеспечения (НМС) с помощью гипервизора KVM.

Для установки Виртуальное устройство НМС в KVM выполните следующие действия:

Примечание: В следующей процедуре применяется интерфейс командной строки и требуются права пользователя root. Синтаксис команды может зависеть от операционной системы.

1. Убедитесь, что пакеты виртуализации установлены в системах с Red Hat Enterprise Linux (RHEL) версии 6.7 и выше.
2. Загрузите файл <установочный файл vHMC KVM>.tar.gz в систему хоста.
3. Выполните следующую команду: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Выполните следующую команду: `cd /var/lib/libvirt/images/vHMC`.
5. Для извлечения образов виртуальных дисков выполните следующую команду: `tar -zxvf <установочный файл vHMC KVM>.tgz`

Примечание: В этой команде укажите полный путь к файлу .tar Виртуальное устройство НМС.

6. Файл **domain.xml** входит в состав файла <установочный файл vHMC KVM>.tar.gz. Выполните следующие действия:
 - a. Откройте файл **domain.xml** в редакторе и проверьте правильность пути к дискам. Этот файл содержит строку **DISK_PATH**.
 - b. Укажите **virtio** в качестве значения шины дискового устройства.
 - c. Можно указать другое имя VM. Имя по умолчанию в файле **domain.xml**: **vHMC**.
 - d. Убедитесь, что в файле **domain.xml** указан MAC-адрес. Этот файл содержит строку **MAC_ADDRESS**.

Примечание: Удалите эту строку, если MAC-адрес следует создавать в автоматическом режиме.

- e. Убедитесь, что мосты соответствуют устройствам Ethernet. В файле **domain.xml** по умолчанию указано одно устройство Ethernet.
7. Для того чтобы создать VM, выполните следующую команду: `virsh define <domain>.xml`.
 8. Для того чтобы запустить VM, выполните следующую команду: `virsh start vHMC`.
 9. Для того чтобы определить номер дисплея Virtual Network Computing (VNC) для консоли выполните следующую команду: `virsh vncdisplay vHMC`.
 10. Для того чтобы подключиться к консоли с помощью программы просмотра VNC, выполните следующую команду: `vncviewer HOSTNAME:ID`(где ID - это номер дисплея, например 0).

Примечание: Если требуется удаленный доступ, то необходимо выключить брандмауэр или открыть в нем порт 5900.

Установка Виртуальное устройство НМС с помощью гипервизора Xen:

Рассмотрена установка Виртуальное устройство консоли аппаратного обеспечения (НМС) с помощью гипервизора Xen.

Виртуальное устройство НМС поддерживает Xen версии 4.2 и выше.

Для установки Виртуальное устройство НМС с помощью гипервизора Xen выполните следующие действия:

Примечание: В следующей процедуре применяется интерфейс командной строки и требуются права пользователя root. Синтаксис команды может зависеть от операционной системы.

1. Убедитесь, что пакеты виртуализации установлены в системах с Red Hat Enterprise Linux (RHEL) версии 6.4 и выше.
2. Загрузите файл <установочный файл vHMC XEN>.tar.gz в систему хоста.
3. Выполните следующую команду: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Выполните следующую команду: `cd /var/lib/libvirt/images/vHMC`.
5. Для извлечения образов виртуальных дисков выполните следующую команду: `tar -zxvf <установочный файл vHMC XEN>.tgz`

Примечание: В этой команде укажите полный путь к файлу .tar Виртуальное устройство НМС.

6. Файл **vhmc.cfg** входит в состав файла <установочный файл vHMC XEN>.tar.gz. Откройте файл **vhmc.cfg** в текстовом редакторе и измените следующие значения:
 - a. Измените имя виртуальной НМС (необязательно): откройте файл **vhmc.cfg** в редакторе и проверьте правильность пути к дискам. Этот файл содержит строку **DISK_PATH**.
 - b. Замените строку **DISK_PATH** на путь к disk1.img:
`disk = [ 'file:DISKPATH,hda,w' ]`
 - c. Замените строку **ethernet adapter** и добавьте MAC-адрес (необязательно):
`vif = [ 'type=virtio, model=e1000, bridge=eth0' ]`
Необязательный MAC-адрес:
`vif = [ 'type=virtio, mac=MACADDRESS, model=e1000, bridge=eth0' ]`
7. Для того чтобы создать и запустить виртуальную машину, выполните следующую команду: `xl create vHMC.cfg`.
8. Убедитесь, что виртуальная машина добавлена в список существующих виртуальных машин. Для этого выполните следующую команду: `xl list`.
9. Для того чтобы открыть локальную консоль виртуальной машины, выполните следующую команду: `vncviewer localhost 0`.

Установка Виртуальное устройство НМС с помощью VMware ESXi:

Рассмотрена установка Виртуальное устройство консоли аппаратного обеспечения (НМС) с помощью VMware ESXi.

Виртуальное устройство НМС можно установить в VMware ESXi с помощью графического пользовательского интерфейса клиента vSphere путем развертывания шаблона Open Virtualization Format (OVF).

Примечание: Виртуальное устройство НМС можно установить в VMware ESXi версии 5.5 и выше.

Для установки Виртуальное устройство НМС в VMware ESXi с помощью клиента vSphere выполните следующие действия:

Примечание: Синтаксис команды может зависеть от операционной системы.

1. Получите файл архива Tar: <имя установочного файла vHMC VMware>.tgz.

2. С помощью команды `tar` извлеките файл OVA из архива Tar.
3. Запустите клиент vSphere и войдите в систему хоста ESXi.
4. В меню **Файл** выберите **Развернуть шаблон OVF**.
5. Нажмите кнопку **Обзор** и выберите файл OVA.
6. Нажмите кнопку **Далее**.
7. После завершения развертывания нажмите кнопку **Заккрыть** и щелкните на значке Виртуальное устройство HMC, чтобы включить Виртуальное устройство HMC.

Установка Виртуальное устройство HMC в PowerVM (логический раздел)

Рассмотрена процедура установки Виртуальное устройство консоли аппаратного обеспечения (HMC) в среде PowerVM.

Примечание: Если Виртуальное устройство HMC устанавливается в разделе с помощью файла образа ISO HMC, вы не будете обладать доступом к пользовательскому веб-интерфейсу из локальной графической консоли.

Для установки Виртуальное устройство HMC в PowerVM выполните следующие действия:

1. Выполните стандартную процедуру установки образа ISO в системе PowerVM. Дополнительная информация приведена в разделе Как настроить хранилище носителей VIOS/виртуальную библиотеку носителей.
2. После завершения установки и запуска системы необходимо выбрать язык в окне **Выбор языка**.
3. Примите условия лицензионного соглашения.

Примечание: Перед тем как приступить к выполнению команд, убедитесь, что контроллер команд готов к приему команд. Например, запускайте команду `lshmc -V` до тех пор, пока она не будет успешно выполнена.

4. Войдите в систему от имени пользователя `hscroot` и настройте сеть с помощью команды `chhmc`.

В следующем примере показана последовательность команд `chhmc`, с помощью которых можно настроить сеть, а также включить ssh и удаленный доступ в HMC.

```
chhmc -c network -s modify -i eth0 -a <IP-адрес hmc> -nm <маска сети hmc> --lparcomm on
chhmc -c network -s modify -h <имя хоста hmc> -d <имя домена hmc> -g <IP-адрес шлюза>
chhmc -c network -s add -ns <сервер имен> -ds <домены для поиска>
chhmc -c ssh -s enable
chhmc -c ssh.name -s add -a <IP-адрес>
chhmc -c SecureRemoteAccess.name -s add -a <IP-адрес>
hmcshutdown -r -t now
```

- **IP-адрес hmc** - это IP-адрес HMC.
- **маска сети hmc** - маска сети HMC.
- **имя хоста hmc** - имя хоста HMC.
- **имя домена hmc** - имя домена HMC.
- **IP-адрес шлюза** - IP-адрес шлюза в сети.
- **сервер имен** - адрес сервера имен в сети.
- **домены для поиска** - имена доменов, в которых консоль HMC должна выполнять поиск.
- Для того чтобы разрешить доступ со всех IP-адресов укажите **-a 0.0.0.0 -nm 0** вместо параметра **IP-адрес**.

5. Перезапустите систему.

Работа со службой активации для Виртуальное устройство HMC

Рассмотрено применение службы активации для Виртуальное устройство консоли аппаратного обеспечения (HMC).

Служба активации обеспечивает настройку различных компонентов виртуальной машины в ходе запуска системы. Службу активации можно использовать только для предварительно созданных образом дисков. Например, если Виртуальное устройство НМС создана с помощью файла ISO восстановления НМС, то служба активации выключена. Для применения службы активации необходимо настроить профайл конфигурации XML, обеспечивающий перевод Виртуальное устройство НМС в состояние готовности к управлению при первом запуске. Дополнительная информация о настройке профайла конфигурации XML приведена в разделе “Настройка профайла конфигурации для службы активации”. В файле конфигурации можно настроить следующие параметры:

- Клавиатура по умолчанию (США)
- Локаль по умолчанию (США)
- Лицензионное соглашение и соглашение на машинный код
- Выключить мастер настройки
- Выключить мастер вызова сервисного центра
- Настроить до четырех сетевых карт
- Настроить параметры брандмауэра для каждого интерфейса

Для того чтобы настроить службу активации, выполните следующие действия:

1. В текстовом редакторе создайте файл XML с именем **vHMC-Conf.xml** или воспользуйтесь примером файла из пакета **<установочный файл vHMC>.tgz**.
2. Создайте образ дискеты. В системах Linux эту задачу можно выполнить с помощью команды dd:
`dd if=/dev/zero of=/Floppy/Path/Floppy.img count=1440 bs=1k`
3. Отформатируйте файл с помощью команды mkfs.ext2:
`/sbin/mkfs.ext2 /Floppy/Path/Floppy.img`
4. Скопируйте файл **vHMC-Conf.xml** в образ дискеты:

```
mkdir /Path/to/Tempfolder/Temp
mount -o loop,rw /Floppy/Path/Floppy.img /Path/to/Tempfolder/Temp
cp /Path/to/vHMC-Conf.xml /Path/to/Tempfolder/Temp
umount /Path/to/Tempfolder/Temp
```

5. Для гипервизора KVM добавьте расположение дискеты в файл **domain.xml**:

```
<disk type='file' device='floppy'>
  <driver name='qemu' type='raw' cache='default' />
  <source file='Path/to/Floppy' />
  <target dev='fda' bus='fdc' />
  <address type='drive' controller='0' bus='0' target='0' unit='0' />
</disk>
```
6. Для того чтобы указать VM, выполните следующую команду: `virsh define PATH_TO_DOMAIN_XML`.
7. Для того чтобы запустить VM, выполните следующую команду: `virsh start NAME_OF_VM` (NAME_OF_VM описывается в файле Domain.xml).

Настройка профайла конфигурации для службы активации:

В этом разделе приведены инструкции по настройке файла конфигурации службы активации с помощью тегов XML.

Теги XML для файла конфигурации

Теги XML применяются в файле конфигурации службы активации для указания значений атрибутов. Эти значения можно вручную указать в файле конфигурации службы активации. В следующих разделах приведено описание каждого тега вместе с допустимыми значениями:

- “Теги НМС” на стр. 59
- “Теги Ethernet” на стр. 59
- “Теги брандмауэра” на стр. 61

- “Теги NTPServers” на стр. 62

Примечание: Служба активации не предоставляет параметры сервера DHCPD.

В следующих разделах приведен пример настройки файла конфигурации:

- “Пример файла конфигурации XML службы активации без NTPServers” на стр. 63
- “Пример файла конфигурации XML службы активации с NTPServers” на стр. 63

Теги НМС

Теги НМС содержат значения параметров НМС. В следующем примере показаны доступные теги НМС:

Тег лицензионного соглашения НМС:

Тег: <AcceptLicense></AcceptLicense>
 Допустимые значения:
 Yes -> Позволяет принять лицензионное соглашение НМС
 No -> Предлагает пользователю принять лицензионное соглашение

Тег локали НМС:

Тег: <Locale></Locale>
 Допустимые значения:
 en_US.UTF-8

Тег мастера настройки НМС:

Тег: <SetupWizard></SetupWizard>
 Допустимые значения:
 Yes -> Отображает мастер настройки НМС
 No -> Выключает мастер настройки НМС

Теги мастера настройки вызова сервисного центра НМС:

Тег: <SetupCallHomeWizard></SetupCallHomeWizard>
 Допустимые значения:
 Yes -> Отображает мастер настройки вызова сервисного центра НМС
 No -> Выключает мастер настройки вызова сервисного центра НМС

Тег настройки клавиатуры НМС:

Тег: <SetupKeyboard></SetupKeyboard>
 Допустимые значения:
 Yes -> Пользователю предлагается настроить клавиатуру:wq
 No -> Позволяет принять конфигурацию клавиатуры по умолчанию (США)

Теги Ethernet

Теги Ethernet позволяют указать значения параметров адаптеров Ethernet. Служба активации позволяет настроить не более четырех адаптеров Ethernet. В следующем примере показаны доступные теги Ethernet:

Тег
 включения Ethernet:

Тег: <Enable></Enable>
 Допустимые значения:
 Yes -> Адаптер настраивается
 No -> Адаптер не настраивается

Тег MACAddr Ethernet:

Тег: <MACAddr></MACAddr>
 Допустимые значения:
 XX:XX:XX:XX:XX:XX -> где X - это значение 0-F
 XX-XX-XX-XX-XX-XX -> где X - это значение 0-F

Тег IPVersion Ethernet:

Тег: <IPVersion></IPVersion>

Допустимые значения:

IPv4 -> Использовать конфигурацию IPv4

IPv6 -> Использовать конфигурацию IPv6

MIX -> Использовать конфигурации IPv4 и IPv6

Тег типа сети IPv4 Ethernet:

Тег: <IPv4NetworkType></IPv4NetworkType>

Допустимые значения:

Static -> Позволяет настроить адаптер с помощью статической конфигурации

Dhcp -> Позволяет настроить адаптер с помощью конфигурации DHCP

Тег адреса IPv4 Ethernet:

Тег: <IPv4Address></IPv4Address>

Допустимые значения:

Любой допустимый адрес IPv4

Тег маски сети IPv4 Ethernet:

Тег: <IPv4Netmask></IPv4Netmask>

Допустимые значения:

Любая допустимая маска сети IPv4

Тег шлюза IPv4 Ethernet:

Тег: <IPv4Gateway></IPv4Gateway>

Допустимые значения:

Любой допустимый адрес IPv4

Тег типа сети IPv6 Ethernet:

Тег: <IPv6NetworkType></IPv6NetworkType>

Допустимые значения:

Static -> Позволяет настроить адаптер с помощью статической конфигурации

Dhcp -> Позволяет настроить адаптер с помощью конфигурации DHCP

Тег адреса IPv6 Ethernet:

Тег: <IPv6Address></IPv6Address>

Допустимые значения:

Любой допустимый адрес IPv6

Тег шлюза IPv6 Ethernet:

Тег: <IPv6Gateway></IPv6Gateway>

Допустимые значения:

Любой допустимый адрес IPv6

Тег имени хоста Ethernet:

Тег: <Hostname></Hostname>

Допустимые значения:

Допустимая строка

Тег домена Ethernet:

Тег: <Domain></Domain>

Допустимые значения:

Любое допустимое значение домена

Пример: austin.ibm.com

Тег серверов DNS Ethernet:

Тег: <DNSServers></DNSServers>

Допустимые значения:

До трех допустимых адресов IPV4 или IPV6, разделенных запятыми.

Можно указать пустое значение сервера DNS.

Пример 1 IPV4: 9.3.2.1 IPV6: 2001:4860:4860::8888

Пример 2 IPV4: 9.3.2.1,9.5.4.1 IPV6: 2001:4860:4860::8888,2001:4860:4860::8844

Пример 3 IPV4: 9.3.2.1,9.5.4.1,9.4.3.2 IPV6: 2001:4860:4860::8888,2001:4860:4860::8844,
::ffff:903:201

Теги брандмауэра

Теги брандмауэра содержат параметры брандмауэра для соответствующего адаптера Ethernet. В следующем примере показаны доступные теги HMC:

Примечание: Во всех тегах применяются значения enabled и disabled.

Тег PEGASUS брандмауэра:

Тег: <PEGASUS></PEGASUS>

Допустимые значения:

Enabled -> Позволяет открыть порты PEGASUS

Disabled -> Позволяет выключить порты PEGASUS

Тег RPD брандмауэра:

Тег: <RPD></RPD>

Допустимые значения:

Enabled -> Позволяет открыть порты RMC

Disabled -> Позволяет выключить порты RMC

Тег FCS брандмауэра:

Тег: <FCS></FCS>

Допустимые значения:

Enabled -> Позволяет открыть порты FCS

Disabled -> Позволяет выключить порты FCS

Тег I5250 брандмауэра:

Тег: <I5250></I5250>

Допустимые значения:

Enabled -> Позволяет открыть порты 5250

Disabled -> Позволяет выключить порты 5250

Тег PING брандмауэра:

Тег: <PING></PING>

Допустимые значения:

Enabled -> Позволяет открыть порт PING

Disabled -> Позволяет выключить порт PING

Тег L2TP брандмауэра:

Тег: <L2TP></L2TP>

Допустимые значения:

Enabled -> Позволяет открыть порты L2TP

Disabled -> Позволяет выключить порты L2TP

Тег SLP брандмауэра:

Тег: <SLP></SLP>

Допустимые значения:

Enabled -> Позволяет открыть порты SLP
Disabled -> Позволяет выключить порты SLP

Тег RSCT брандмауэра:

Тег: <RSCT></RSCT>
Допустимые значения:
Enabled -> Позволяет открыть порты RSCT
Disabled -> Позволяет выключить порты RSCT

Тег SECUREREMOTEACCESS брандмауэра:

Тег: <SECUREREMOTEACCESS></SECUREREMOTEACCESS>
Допустимые значения:
Enabled -> Позволяет открыть порты защищенного удаленного доступа
Disabled -> Позволяет выключить порты защищенного удаленного доступа

Тег SSH брандмауэра:

Тег: <SSH></SSH>
Допустимые значения:
Enabled -> Позволяет открыть порт SSH
Disabled -> Позволяет выключить порт SSH

Тег VTTY брандмауэра:

Тег: <VTTY></VTTY>
Допустимые значения:
Enabled -> Позволяет открыть порты VTTY
Disabled -> Позволяет выключить порты VTTY

Тег NTP брандмауэра:

Тег: <NTP></NTP>
Допустимые значения:
Enabled -> Позволяет открыть порты NTP
Disabled -> Позволяет выключить порты NTP

Тег SNMPTraps брандмауэра:

Тег: <SNMPTraps></SNMPTraps>
Допустимые значения:
Enabled -> Позволяет открыть порты прерываний SNMP
Disabled -> Позволяет выключить порты прерываний SNMP

Тег SNMPAgents брандмауэра:

Тег: <SNMPAgents></SNMPAgents>
Допустимые значения:
Enabled -> Позволяет открыть порты агентов SNMP
Disabled -> Позволяет выключить порты агентов SNMP

Теги NTPServers

Тег NTPServers позволяет настроить в Виртуальное устройство НМС до пяти серверов NTP. Серверы NTP добавляются с помощью тега <ntpparam ntpserver="server" ntpversion="1-4"/>. В параметрах сервера можно указать значения IPv4 и IPv6 или имена доменов. В следующем примере показаны доступные теги NTPServers:

Тег NTPServers:

Тег: <NTPServers></NTPServers>
Принимает <ntpparam ntpserver="server" ntpversion="1-4"/>

Пример 1 <NTPServers>
<ntpparam ntpserver="9.4.34.1" ntpversion="4"/>

</NTPServers>

```
Пример 2 <NTPServers>
  <ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/>
  <ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
  <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>
</NTPServers>
```

Тег ntpparam

Тег: <ntpparam ntpserver="" ntpversion="" />

Значения атрибутов:

ntpserver: принимает значения IPv4/IPv6 и допустимые имена хостов

ntpversion: принимает числовое значение в диапазоне 1-4

Пример файла конфигурации XML службы активации без NTPServers

Ниже приведен пример файла конфигурации XML службы активации без NTPServers:

```
<vHMC-Configuration>
  <LicenseAgreement>
  </LicenseAgreement>
  <AcceptLicense>Yes</AcceptLicense>
  <Locale>en_US.UTF-8</Locale>
  <SetupWizard>No</SetupWizard>
  <SetupCallHomeWizard>No</SetupCallHomeWizard>
  <SetupKeyboard>No</SetupKeyboard>
<Ethernet>
  <Enable>No</Enable>
  <MACAddr></MACAddr>
  <IPVersion></IPVersion>
  <IPv4NetworkType></IPv4NetworkType>
  <IPv4Address></IPv4Address>
  <IPv4Netmask></IPv4Netmask>
  <IPv4Gateway></IPv4Gateway>
  <IPv6NetworkType></IPv6NetworkType>
  <IPv6Address></IPv6Address>
  <IPv6Gateway></IPv6Gateway>
  <Hostname></Hostname>
  <Domain></Domain>
  <DNSServers></DNSServers>
<Firewall>
  <PEGASUS>Enabled</PEGASUS>
  <RPD>Enabled</RPD>
  <FCS>Enabled</FCS>
  <I5250>Enabled</I5250>
  <PING>Enabled</PING>
  <L2TP>Disabled</L2TP>
  <SLP>Enabled</SLP>
  <RSCT>Enabled</RSCT>
  <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
  <SSH>Enabled</SSH>
  <VTTY>Disabled</VTTY>
  <NTP>Disabled</NTP>
  <SNMPTraps>Disabled</SNMPTraps>
  <SNMPAgents>Disabled</SNMPAgents>
</Firewall>
</Ethernet>
</vHMC-Configuration>
```

Пример файла конфигурации XML службы активации с NTPServers

Ниже приведен пример файла конфигурации XML службы активации с NTPServers

```

<vHMC-Configuration>
  <LicenseAgreement>
    </LicenseAgreement>
  <AcceptLicense>Yes</AcceptLicense>
  <Locale>en_US.UTF-8</Locale>
  <SetupWizard>No</SetupWizard>
  <SetupCallHomeWizard>No</SetupCallHomeWizard>
  <SetupKeyboard>No</SetupKeyboard>
<Ethernet>
  <Enable>No</Enable>
  <MACAddr></MACAddr>
  <IPVersion></IPVersion>
  <IPv4NetworkType></IPv4NetworkType>
  <IPv4Address></IPv4Address>
  <IPv4Netmask></IPv4Netmask>
  <IPv4Gateway></IPv4Gateway>
  <IPv6NetworkType></IPv6NetworkType>
  <IPv6Address></IPv6Address>
  <IPv6Gateway></IPv6Gateway>
  <Hostname></Hostname>
  <Domain></Domain>
  <DNSServers></DNSServers>
<Firewall>
  <PEGASUS>Enabled</PEGASUS>
  <RPD>Enabled</RPD>
  <FCS>Enabled</FCS>
  <I5250>Enabled</I5250>
  <PING>Enabled</PING>
  <L2TP>Disabled</L2TP>
  <SLP>Enabled</SLP>
  <RSCT>Enabled</RSCT>
  <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
  <SSH>Enabled</SSH>
  <VTTY>Disabled</VTTY>
  <NTP>Disabled</NTP>
  <SNMPTraps>Disabled</SNMPTraps>
  <SNMPAgents>Disabled</SNMPAgents>
</Firewall>
</Ethernet>
<NTPServers>
  <ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/>
  <ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
  <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>
</NTPServers>
</vHMC-Configuration>

```

Установка монитора и клавиатуры

Инструкции по установке в стойку монитора и клавиатуры, поставляемых вместе с HMC 7042-CR6. Эта задача выполняется заказчиком.

Если для управления системой с процессором POWER8 применяется HMC, то это должна быть HMC модели CR3 или выше, монтируемая в стойке. IBM eserver 7316-TF3 - плоский монитор с диагональю 17 дюймов, монтируемый в стойке вместе с клавиатурой. Специальная клавиатура, предлагаемая для разных языков, размещается в передней части лотка клавиатуры. Лоток монитора и клавиатуры занимает в стойке одну единицу пространства Electronics Industries Association (EIA). За лотком можно установить коммутатор консоли, позволяющий подключать к монитору и клавиатуре несколько серверов.

Для установки HMC 7042-CR6 в стойку выполните следующие действия:

Внимание: Установка направляющих в стойке является сложной процедурой. Для того чтобы установить их правильно, описанные ниже задачи должны выполняться в указанном порядке.

1. Сверьтесь со списком поставки. За инструкциями обратитесь к разделу Инвентаризация компонентов.

2. Найдите комплект для монтажа аппаратных средств в стойке и блоки направляющих, поставляемые с системным блоком.

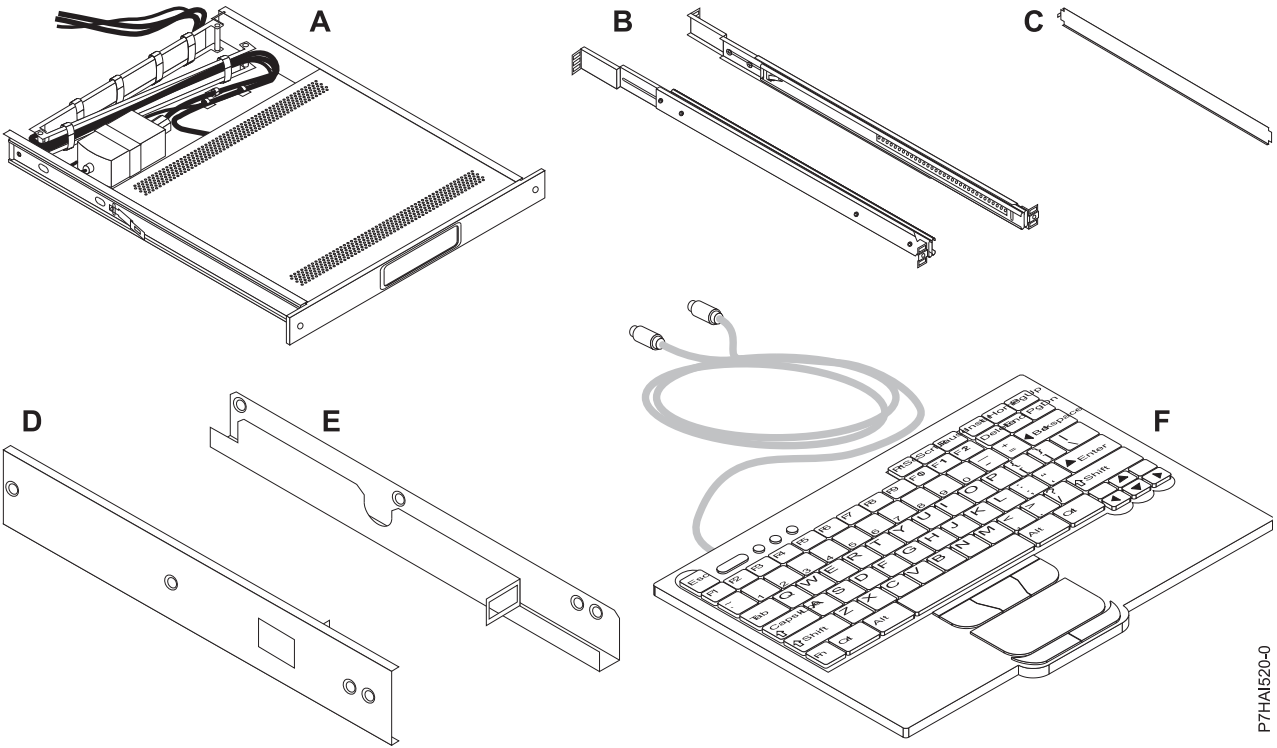


Рисунок 75. Установка деталей из комплекта

Таблица 10. Детали из установочного комплекта

Установочный комплект	Детали
A	Один лоток клавиатуры со встроенным монитором
B	Внешние рельсы (2)
C	Разделитель выравнивания направляющей (1)
D	Правый кронштейн крепления коммутатора консоли (1)
E	Левый кронштейн крепления коммутатора консоли (1)
F	Клавиатура со встроенным позиционирующим устройством (1)
G	Комплект прочих деталей: 12 квадратных гаек, 12 зажимных гаек, 10 крестообразных винтов, 4 (8-32) винтов и 2 винта с накатанными головками.
H	кабель питания, 1.8 м (6 футов) (1)
I	кабель питания с разъемом IEC (Международная электротехническая комиссия), 2.4 м (8 футов) (1)
J	Удлинитель клавиатуры (1)
K	Удлинитель мыши (1)
L	Компакт-диск с драйверами клавиатуры и мыши для Windows (не предназначен для систем Eserver pSeries, а также систем на основе AIX, Linux и OS/400)

Таблица 10. Детали из установочного комплекта (продолжение)

Установочный комплект	Детали
Важное замечание: Для установки монитора и клавиатуры в стойку требуются следующие инструменты: • Ножницы • Крестовая отвертка • Плоская отвертка.	

Инвентаризация компонентов

Иногда возникает необходимость составить реестр компонентов.

Если вы не сделали это, выполните опись компонентов перед началом установки:

1. Найдите описание деталей в коробке.
2. Убедитесь, что вы получили все заказанные компоненты.

При обнаружении не предусмотренных в комплекте, отсутствующих или поврежденных компонентов обращайтесь к торговому посреднику IBM или в сервисный центр IBM.

Маркировка расположения без трафарета монтажа в стойке

Расположение можно пометить без трафарета.

В комплект поставки данной системы схема не входит. Высота этих системных блоков равна одному блоку EIA.

Для определения места монтажа выполните следующие действия:

1. Выберите место для размещения системы в стойке. Запишите расположение EIA.

Примечание: Блок EIA в стойке содержит группу из трех отверстий.

2. Стоя лицом к передней панели стойке и начиная справа, приклейте самоклеющуюся точку из комплекта поставки рядом с верхним отверстием блока EIA.

Примечание: Самоклеющиеся точки используются для помощи в идентификации расположений в стойке. Если у вас нет самоклеющихся точек, используйте для маркировки другие способы, например, маркер, карандаш или липкую ленту. При установке направляющих проставьте метку или приклейте самоклеющуюся точку на нижнем и среднем отверстиях блока EIA.

3. Приклейте другую самоклеющуюся точку рядом с нижним отверстием верхнего блока EIA.

Примечание: Пересчитывать отверстия нужно, начиная с отверстия, отмеченного первой точкой; после него отсчитываются два отверстия. Вторую точку приклейте рядом с третьим отверстием.

4. Повторите шаг 1 на стр. 8 для соответствующих отверстий, расположенных с левой стороны стойки.
5. Зайдите в тыл стойки.
6. На правой стороне найдите единицу EIA, соотносящуюся с нижней помеченной единицей EIA спереди стойки.
7. Приклейте самоклеющуюся точку внизу блока EIA.
8. Приклейте самоклеющуюся точку на верхнее отверстие блока EIA.
9. Пометьте соответствующие отверстия на левой стороне стойки.

Установка монитора и клавиатуры в стойку

Инструкции по установке в стойку монитора и клавиатуры, поставляемых вместе с HMC 7042-CR6.

17-дюймовый плоский монитор IBM 7316-TF3 и клавиатура занимают 1.75 дюймов (1 EIA) в стойке. С помощью кронштейнов, входящих в этот комплект, вместе с монитором можно установить дополнительный коммутатор консоли.

Для установки монитора и клавиатуры НМС 7042-CR6 в стойку выполните следующие действия:

Внимание: Снимите дверцы стойки и боковые панели, чтобы обеспечить доступ к консоли.

Выполните следующие действия для установки монитора и клавиатуры в стойку:

1. Выберите расположение в стойке для размещения лотка монитора и клавиатуры. Дополнительная информация приведена в разделе Маркировка расположения.
2. Установите 4 квадратные гайки (на фланцы с квадратными отверстиями) или 4 гайки с зажимом (на фланцы с круглыми отверстиями) в те же позиции EIA спереди и сзади стойки.

Примечание: Если планируется установить коммутатор консоли, установите квадратную гайку или гайку с зажимом в центральное заднее положение, показанное на следующем рисунке.

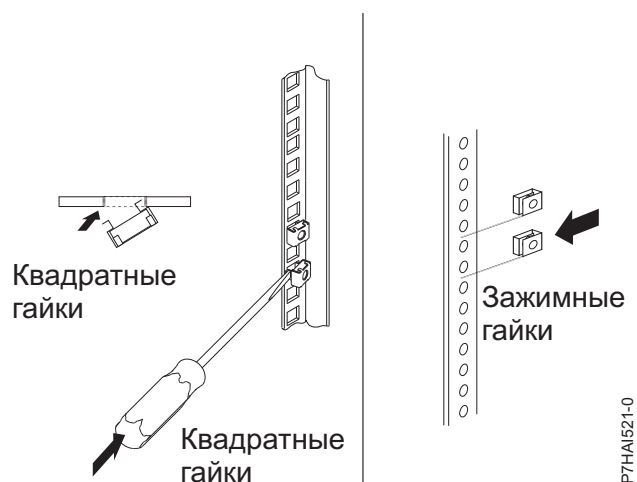


Рисунок 76. Установка квадратных гаек

3. Ослабьте два винта фиксации направляющей, расположенные на каждой внешней направляющей. Максимально раздвиньте направляющие.
4. Выровняйте кронштейны внешних направляющих с учетом ширины стойки. Затем прикрепите переднюю часть кронштейнов направляющих с учетом глубины стойки с помощью четырех винтов из комплекта прочего аппаратного обеспечения. Затяните винты вручную, чтобы обеспечить возможность выравнивания направляющих.

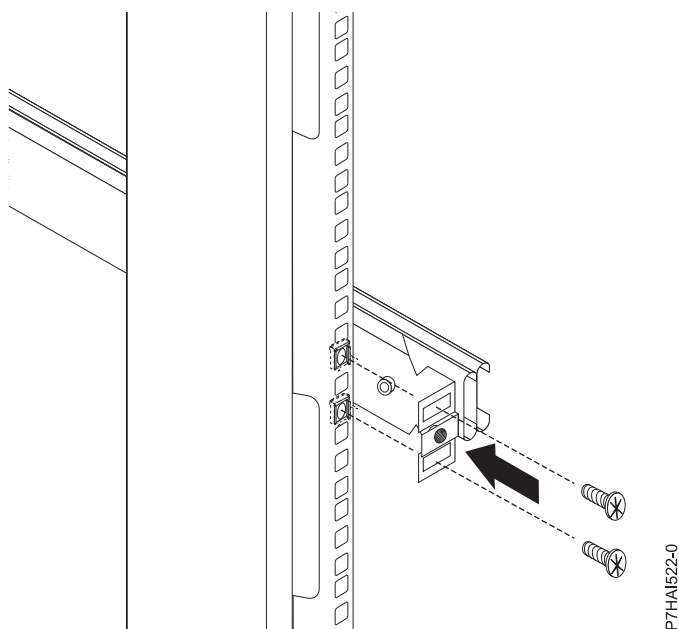


Рисунок 77. Выравнивание кронштейна боковой направляющей

Примечание: Убедитесь, что кронштейны направляющих выходят за пределы крепежных фланцев стойки. Не устанавливайте винты в средние отверстия переднего или заднего кронштейна направляющей. Эти отверстия предназначены для установки винтов с накатанными головками или монтажных кронштейнов коммутатора консоли.

5. Вручную затяните четыре винта на задней части кронштейнов направляющих, прикрепив их к стойке. Убедитесь, что кронштейны направляющих выходят за пределы крепежных фланцев стойки.
6. Затяните два винта фиксации направляющей, которые расположены на каждой внешней направляющей и были ослаблены на шаге 5.
7. Вставьте прокладку выравнивания направляющей в средние отверстия направляющей. Убедитесь, что прокладка обертывает направляющие. Затяните передние четыре винта и удалите прокладку.

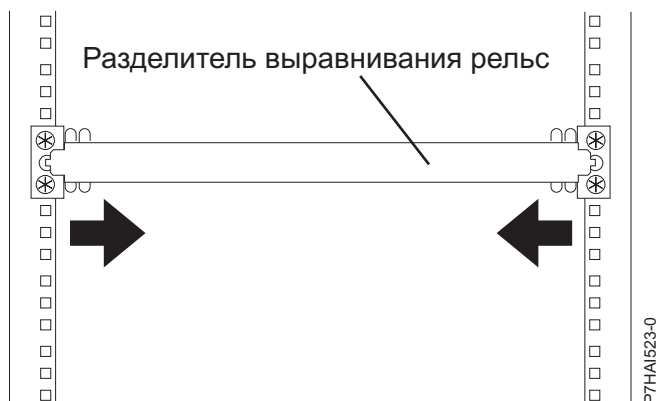


Рисунок 78. Установка разделителя выравнивания направляющей

8. Расширьте внутреннюю часть направляющих, смонтированных в стойке, затем задвиньте блоки с подшипниками вперед к передней части направляющих.
9. Задвиньте лоток монитора и клавиатуры в блоки с подшипниками на направляющих.

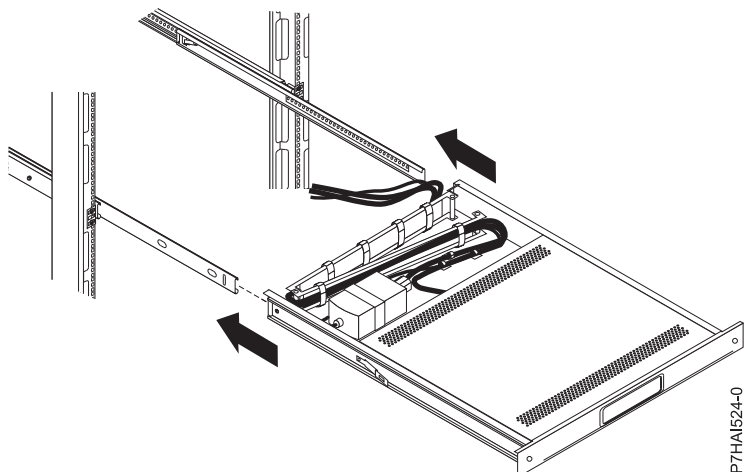


Рисунок 79. Вставка монитора и клавиатуры

10. Нажмите на защелки и установите лоток монитора и клавиатуры до конца в стойку. В начале может возникнуть сопротивление по мере выравнивания подшипников между внутренними и внешними направляющими. Выдвиньте лоток на половину, вставьте его обратно, чтобы установить в направляющие. Повторите это действие несколько раз до тех пор, пока лоток не будет плавно перемещаться по направляющим.

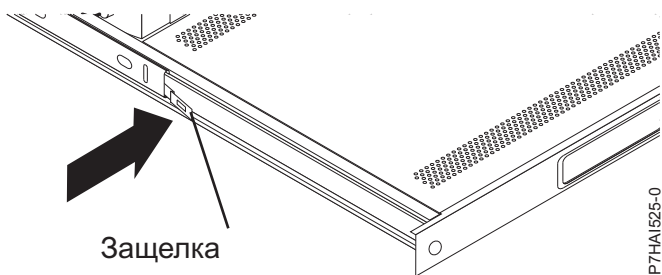


Рисунок 80. Использование защелки

Примечание:

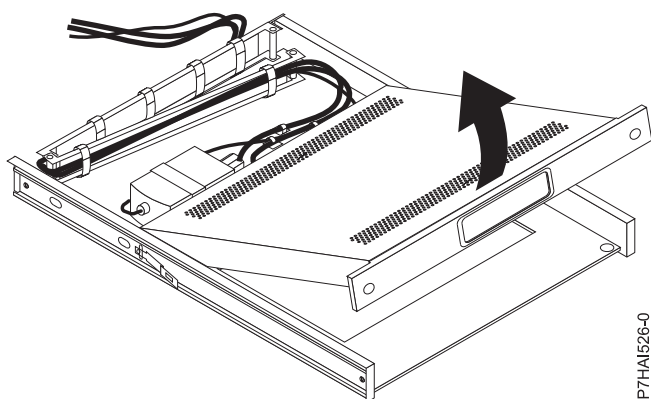
Видеокабель подключен к плоскому монитору. В ходе установки лотка в стойку убедитесь, что кабель монитора не защемлен или не порезан.

11. Установите лоток в стойку и затяните четыре винта заднего кронштейна направляющей.
12. Поместите клавиатуру на устойчивой плоской поверхности и снимите резиновые накладки, расположенные снизу с каждой стороны клавиатуры. Не оставляйте резиновые накладки на клавиатуре, поскольку они могут попасть под лоток.

Примечание:

Не открывайте ножки клавиатуры. Это может привести к повреждению монитора при его закрытии.

13. Полностью вытяните лоток из стойки.
14. Поднимите монитор в положение справа до конца.



P7H4526-0

Рисунок 81. Перемещение монитора в положение справа

15. Вставьте клавиатуру в лоток. Затем протяните кабель клавиатуры и мыши через зажим в нижней части лотка вверх через отверстие в правой части лотка и в сторону кабельного кронштейна. Протяните весь кабель через отверстие.
16. Разместите кабели клавиатуры и монитора в лотке за монитором. Убедитесь, что кабели не будут мешать устройствам после установки лотка в стойку. Ниже приведены инструкции по прокладыванию кабелей через кабельный кронштейн.
17. Опустите монитор и задвиньте лоток в стойку. С помощью винтов с накатанными головками зафиксируйте переднюю часть лотка.
18. С задней части стойки снимите транспортировочные стяжки, которые крепят кабельный кронштейн к лотку.
19. Протяните кабели монитора и клавиатуры через кабельный кронштейн. Зафиксируйте кабели с помощью существующих стяжек.
20. Снимите винт выравнивания направляющей, расположенный ближе всего к задней части стойки от левой направляющей. С помощью винта прикрепите кабельный кронштейн к направляющей.

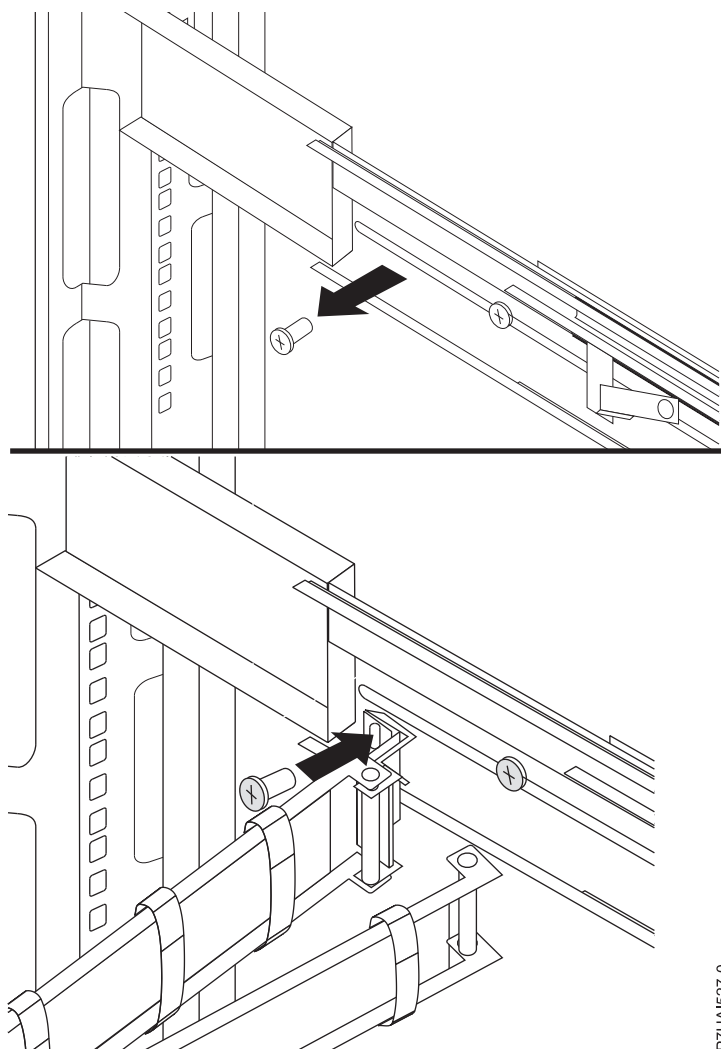


Рисунок 82. Подключение рукава с кабелями

21. Подключите разъемы монитора, клавиатуры и мыши к серверу или коммутатору консоли в стойке. В случае установки необязательного коммутатора консоли выполните инструкции из раздела Установка необязательного коммутатора консоли. В противном случае выполните процедуру с шага 21 для завершения установки лотка клавиатуры и монитора.
22. Подключите кабель питания к короткому кабельно-перемычке на кабельном кронштейне.
23. Подключите все кабели и сигнальные разъемы в подходящие устройства или разъемы.
24. Убедитесь, что все выключатели питания выключены. Подключите кабель питания к заземленной розетке или блоку распределения питания (PDU).

Примечание: Перед подключением кабеля питания переменного тока в розетку постоянного тока убедитесь, что напряжение локального источника питания лежит в диапазоне 100 - 240 вольт (переменный ток).

25. Вытяните лоток из передней части стойки. Протяните кабели в стойке и зафиксируйте их с помощью стяжек.

Установка коммутатора консоли (необязательно)

Инструкции по установке необязательного коммутатора консоли.

С помощью коммутатора консоли можно подключить несколько серверов к монитору и клавиатуре. Коммутатор консоли доступен отдельно, однако крепежные кронштейны для него входят в состав комплекта установки.

За счет установки коммутатора консоли за лотком монитора и клавиатуры можно разместить монитор и клавиатуру в одном отсеке стойки. Для установки коммутатора консоли за лотком воспользуйтесь кронштейнами, входящими в состав установочного комплекта.

Выполните следующие действия для установки коммутатора консоли за лотком:

1. С помощью винтов 8-32 прикрепите правую и левую боковые скобы к коммутатору консоли.

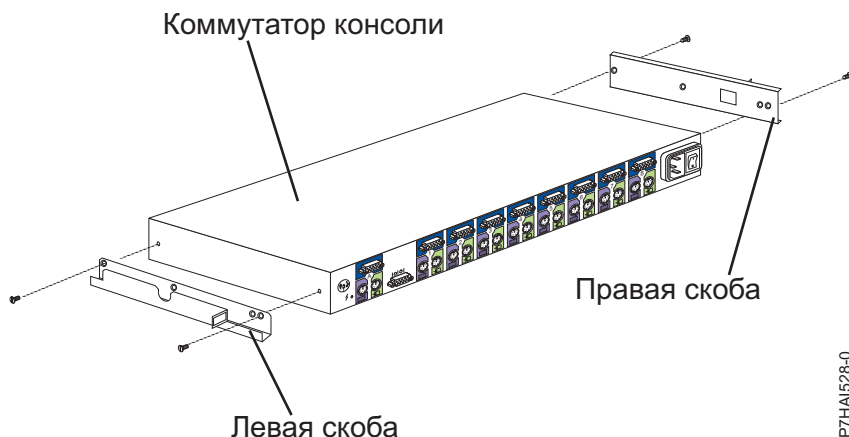


Рисунок 83. Установка коммутатора консоли

Примечание: Левая скоба содержит паз для размещения кабелей монитора, питания, клавиатуры и мыши. Скобы следует прикрепить к коммутатору консоли таким образом, чтобы канал на левой скобе был направлен вверх.

2. Установите коммутатор консоли за лотком монитора и клавиатуры с помощью четырех (по два с каждой стороны) крестообразных винтов из комплекта прочего аппаратного обеспечения.
3. Протяните кабели монитора, питания, клавиатуры и мыши через паз, предусмотренный на левой скобе коммутатора консоли. Затем подключите разъемы монитора, клавиатуры и мыши к коммутатору консоли.

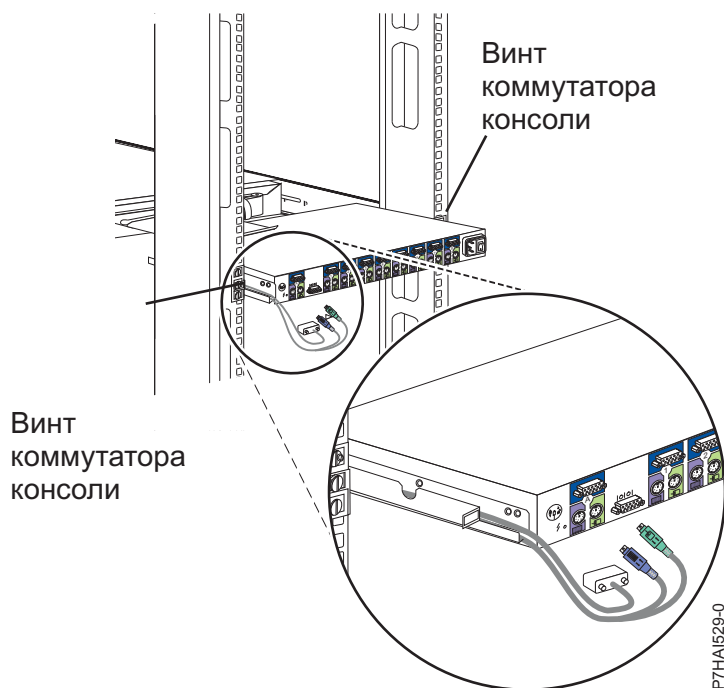


Рисунок 84. Прокладывание кабелей

4. Соедините кабели питания, промежуточные кабели и кабельные стяжки. Соответствующие инструкции приведены в разделе Подключение кабеля питания к короткому соединительному кабелю на кабельном кронштейне.

Настройка НМС с помощью интерфейса НМС Classic или НМС Enhanced

Рассматриваются настройка сетевых соединений, настройка НМС, действия после настройки и обновление НМС с помощью интерфейса НМС Classic или НМС Enhanced.

Примечания:

1. Начиная с версии 8.7.0, консоль аппаратного обеспечения (НМС) не поддерживает интерфейс НМС Classic. Функции, которые были ранее доступны в интерфейсе с НМС Classic, теперь можно выполнить с помощью интерфейса НМС Enhanced+.
2. Графический пользовательский интерфейс НМС Enhanced доступен в НМС версии 8.1.0.1 и 8.2.0. Для его открытия при входе в НМС необходимо выбрать опцию НМС Enhanced. Начиная с версии НМС 8.3.0 процедуры и функции интерфейса НМС Enhanced включены в интерфейс НМС Enhanced+.
3. В зависимости от предполагаемого уровня настройки конфигурации НМС, можно воспользоваться несколькими вариантами настройки НМС, выбирая из них наиболее подходящий для своих задач. Инструментальное средство Мастер пошаговой настройки из НМС позволяет легко и быстро выполнить настройку НМС. Мастер предоставляет возможность выбрать быстрое прохождение, при этом быстро создается рекомендуемая среда НМС. Кроме того, в нем предусмотрена возможность подробного ознакомления с доступными параметрами. Настройку можно также выполнить без помощи мастера в соответствии с инструкциями из раздела Настройка НМС с помощью меню НМС.

Выбор параметров сети в НМС

Знакомит с параметрами сети, которые можно использовать в НМС.

Сетевые соединения НМС

Для соединения НМС с управляемыми системами можно использовать разные типы сетевых соединений. Дополнительная информация о настройке НМС для подключения к сети приведена в разделе “Настройка НМС” на стр. 91. Дополнительная информация об использовании НМС в сети приведена в следующем разделе:

Типы сетевых соединений НМС:

Знакомит с использованием функций дистанционного управления НМС и служебных функций при помощи сети.

НМС поддерживает следующие типы логических связей:

Соединение НМС с управляемой системой

Используется для выполнения большинства функций управления аппаратными средствами; в нем НМС выдает запросы функции управления через служебный процессор управляемой системы. Другое название соединения между НМС и служебным процессором: *сеть обслуживания*. Оно требуется для работы с управляемой системой.

Соединение НМС с логическим разделом

Используется для получения информации, связанной с платформой (события при ошибках аппаратных средств, реестр аппаратных средств), от операционных систем, работающих в логических разделах, а также для координации определенных действий платформы (динамический LPAR, оперативный ремонт) с указанными операционными системами. Для работы с функциями обслуживания и извещений об ошибках используется именно этот тип соединения.

НМС к BMC

Примечание: Соединение с контроллером управления базовой платой (ВМС) применимо только к НМС модели 7063-CR1.

Применяется для выполнения задач обслуживания. Соединение ВМС используется для настройки и обслуживания встроенного программного обеспечения НМС в системе. Это соединение требуется для доступа к ВМС в НМС.

Соединение НМС с удаленными пользователями

Обеспечивает удаленный доступ к функциям НМС. Удаленные пользователи могут получить доступ к НМС следующим образом:

- С помощью веб-браузера для удаленного доступа ко всем функциям графического пользовательского интерфейса НМС.
- С помощью протокола SSH для доступа к функциям командной строки НМС.

Соединение НМС со службой сопровождения и поддержки

Используется для обмена данными, такими как отчеты об ошибках аппаратных средств, реестровые данные и обновления микрокодов, с обслуживающей системой. С его помощью можно также осуществлять автоматические вызовы сервисного центра.

НМС может поддерживать до четырех отдельных физических интерфейсов Ethernet, в зависимости от модели. Автономная версия НМС поддерживает три физических интерфейса НМС, используя один встроенный адаптер Ethernet и один или два встраиваемых адаптера. Каждый из указанных интерфейсов используется следующим образом:

- Один или несколько сетевых интерфейсов могут использоваться только для связи между НМС и управляемой системой; это означает, что в такой сети могут присутствовать только НМС и служебные процессоры управляемых систем. Несмотря на то, что сетевые интерфейсы для связи со служебными процессорами зашифрованы по протоколу Secure Sockets Layer (SSL) и защищены паролем, выделенная сеть обеспечивает более высокую степень защиты таких интерфейсов.
- Интерфейс открытой сети используется обычно для сетевых соединений между НМС и логическими разделами управляемых систем, обеспечивая связь между НМС и логическими разделами. Кроме того, интерфейс открытой сети обеспечивает удаленное управление НМС.
- При необходимости можно настроить третий интерфейс для подключения к логическим разделам и удаленного управления НМС. Третий интерфейс можно также использовать для отдельного соединения НМС с разными группами логических разделов. Например, можно создать отдельный сегмент локальной сети для задач администрирования, не связанный с общей локальной сетью, в которой выполняются деловые задачи. По этой сети администраторы смогут обращаться к НМС и другим управляемым компонентам. Иногда логические разделы размещаются в отдельных защищенных сегментах сети, возможно - за брандмауэром, и иногда требуются отдельные соединения НМС с этими сегментами сети.

Требования к веб-браузерам для НМС

Консоль аппаратного обеспечения (НМС) версии 8.7.0 поддерживается Google Chrome версии 57, Microsoft Internet Explorer (IE) версии 11.0, Mozilla Firefox версий 45 и 52 Extended Support Release (ESR), а также Safari версии 10.1.

Если браузер настроен для использования прокси-сервера, то в список исключений следует добавить локальные IP-адреса. За дополнительной информацией о списке исключений обратитесь к администратору сети. Если для подключения к НМС требуется использовать прокси-сервер, то включите переключатель Использовать HTTP 1.1 через прокси-соединения на вкладке Дополнительно в окне Свойства обозревателя.

Для работы Расширенного интерфейса управления системой (ASMI) при удаленном подключении к НМС необходимо включить cookie для текущего сеанса. В коде asm проху сохраняется информация о сеансе, которая используется в дальнейшем. Выполните инструкции по включению cookie сеансов.

Включение cookie сеансов в Internet Explorer.

1. Выберите Сервис, затем выберите Свойства обозревателя.

2. Выберите Конфиденциальность и нажмите кнопку Дополнительно
3. Убедитесь, что переключатель Всегда разрешать сеансовые cookie включен. Если он выключен, то включите переключатели Перекрыть автоматическую обработку файлов cookie и Всегда разрешать сеансовые cookie.
4. Включите переключатель Запрашивать в списках Основные cookie и Сторонние cookie.
5. Нажмите кнопку ОК.

Включение cookie сеансов в Firefox.

1. Выберите Инструменты, затем выберите Настройки.
2. Выберите Cookie
3. Включите переключатель Разрешить сайтам задавать cookie.
4. Выберите Исключения и добавьте НМС.
5. Нажмите кнопку ОК.

Частные и открытые сети в среде НМС:

НМС может быть настроена на открытые и частные сети. Частная сеть позволяет пользоваться избранным диапазоном немаршрутизируемых IP-адресов. *Общая*, или "открытая" сеть представляет собой сетевое соединение между НМС и любыми логическими разделами, а также другими системами обычной сети.

Частные сети

Из устройств в частной сети с НМС имеются только сама НМС и каждая из управляемых систем, к которым она подключена. НМС подключена к FSP (гибкому служебному процессору) каждой управляемой системы.

В большинстве систем FSP обеспечивает два порта Ethernet с метками **НМС1** и **НМС2**. Поэтому подключаться можно к двум НМС.

В некоторых системах предусмотрена такая возможность, как наличие двух FSP. В этой ситуации второй FSP выступает в роли "избыточного" резервного сервера. Основные требования установки системы с двумя FSP мало чем отличаются от требований к системе без второго FSP. НМС должна быть подключена к каждому FSP, поэтому при наличии дополнительного FSP или нескольких управляемых систем потребуются дополнительные аппаратные средства (например, коммутатор или концентратор LAN).

Примечание: Каждый порт FSP управляемой системы должен быть подключен только к одной НМС.

Общие сети

Открытая сеть может быть соединена с брандмауэром или маршрутизатором для подключения к Internet. Подключение к Internet позволяет НМС "обратиться к сервисный центр" в случае аппаратных сбоев, требующих отправки сообщений.

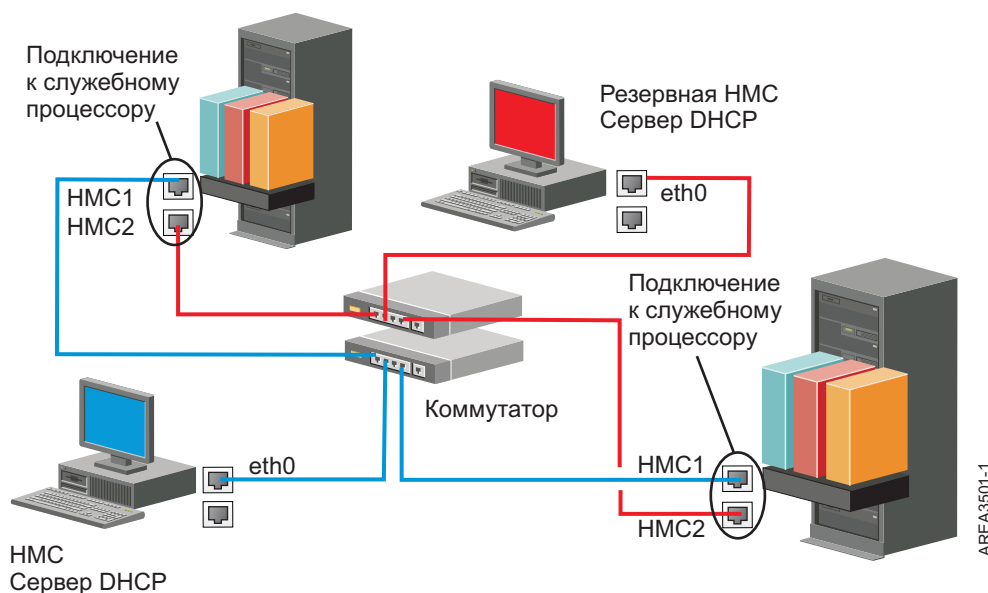
НМС предоставляет собственный брандмауэр на каждом из своих сетевых интерфейсов. Основной брандмауэр настраивается автоматически при запуске мастера пошаговой настройки НМС, но по окончании начальной установки и настройки НМС необходимо настроить брандмауэра, задав собственные параметры с учетом своих требований.

НМС в качестве сервера DHCP:

Данную НМС можно использовать в качестве сервера DHCP.

Примечание: При использовании IPv6 поиск необходимо выполнить вручную. Для IPv6 нет автоматической процедуры поиска.

Дополнительная информация о настройке HMC в качестве сервера DHCP приведена в разделе “Настройка HMC в качестве сервера DHCP” на стр. 99.

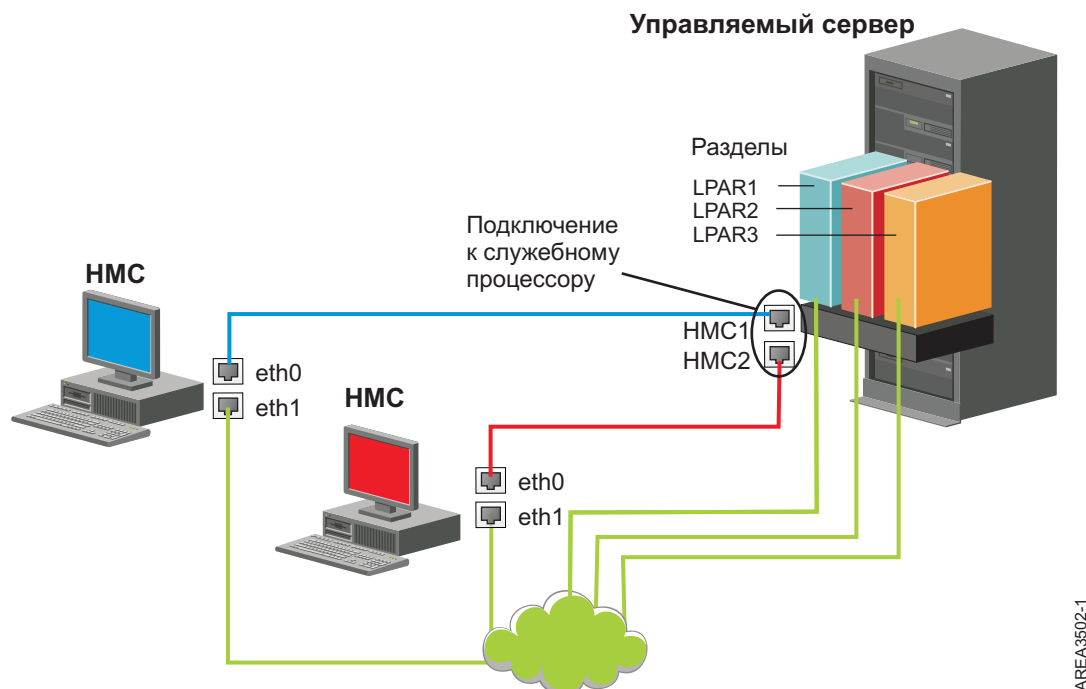


На рисунке показана среда дополнительной HMC с двумя управляемыми системами. Первая HMC подключена к первому порту на каждом FSP, дополнительная HMC - ко второму порту на каждой HMC. Каждая HMC настроена в качестве сервера DHCP с использованием отдельного диапазона IP-адресов. Соединения выполняются в разных частных сетях. Исходя из этого, важно, чтобы каждый порт был подключен только к одной HMC.

Каждый порт FSP управляемой системы, подключенный к HMC, требует уникального IP-адреса. С этой целью воспользуйтесь встроенной функцией сервера DHCP консоли HMC. После обнаружения процессором FSP активной сетевой ссылки, он выдает оповещающий запрос для нахождения сервера DHCP. Если настройка выполнена правильно, HMC в ответ на этот запрос назначает один из выбранных диапазонов адресов.

При наличии нескольких FSP требуется отдельный коммутатор или концентратор LAN для подключения HMC к частной сети FSP. В альтернативном варианте этот частный сегмент может существовать в виде нескольких портов в частной *виртуальной LAN* (VLAN) на более крупном управляемом переключателе. При наличии нескольких частных сетей VLAN они должны быть изолированными друг от друга, и между ними не должно быть перекрестного трафика.

В среде с несколькими HMC необходимо, кроме того, подключить каждый HMC к логическим разделам и к остальным HMC в одной и той же открытой сети.



На рисунке представлены две консоли HMC, подключенные к одному управляемому серверу в частной сети и к трем логическим разделам в открытой сети. Для того чтобы пользоваться тремя сетевыми интерфейсами, можно предусмотреть дополнительный адаптер Ethernet для HMC. Эту третью сеть можно использовать в качестве сети управления или можно подключить ее к серверу управления CSM (Cluster Systems Manager).

Дополнительная информация о настройке HMC в качестве сервера DHCP приведена в разделе “Настройка HMC в качестве сервера DHCP” на стр. 99.

Выбор способа соединения для сервисного сервера:

Дополнительные сведения об опциях соединения при работе с сервисным центром.

HMC можно настроить для передачи сервисной информации по аппаратному обеспечению в компанию IBM через Internet-соединение на основе LAN или соединение по телефонной линии через модем.

Примечание: Виртуальная частная сеть Internet (VPN) и соединение по телефонной линии через модем доступны только в HMC версии 8.2.0 и более ранних версий.

При настройке Internet-соединения на базе LAN обмен данными можно организовать двумя способами. В первом варианте используется стандартный протокол защищенных сокетов (SSL). Связь по протоколу SSL можно разрешить для подключения к Internet через сервер Proxy. SSL-соединение с большей вероятностью будет соответствовать корпоративным рекомендациям по обеспечению защиты. Во втором - соединении VPN.

Примечание: Если для открытого сетевого соединения интерфейса используется только Internet Protocol Version 6 (IPv6), нельзя использовать Internet VPN для соединения со службой поддержки. Дополнительная информация о применяемых протоколах приведена в разделе “Выбор протокола соединения с Интернетом” на стр. 80.

К преимуществам использования Internet-соединения можно отнести:

- Более высокая скорость передачи данных
- Более низкие расходы пользователя (например, затраты на выделенную телефонную линию)

- Более высокая надежность

При любом способе соединения действуют следующие характеристики защиты:

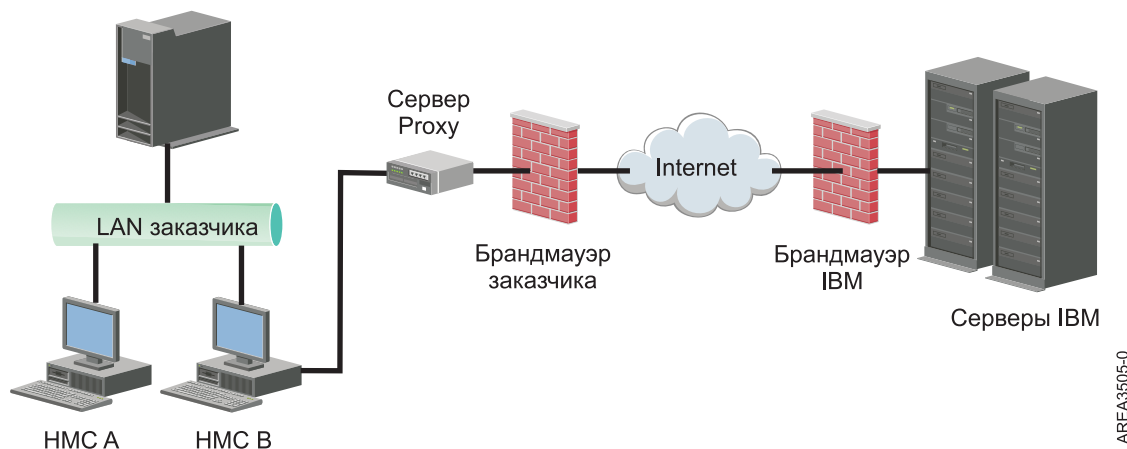
- Запросы Remote Support Facility всегда иницируются с НМС к IBM. Соединение для приема данных никогда не иницируется с системы сервисной поддержки IBM.
- Все данные, передаваемые между НМС и системой сервисной поддержки IBM, шифруются с помощью высококачественного шифрования. В зависимости от выбранного способа соединения, шифрование выполняется с помощью SSL или безопасного закрытия содержания по протоколу IPSec (ESP).
- При инициализации зашифрованного соединения НМС идентифицирует целевую систему как систему сервисной поддержки IBM.

Данные, отправляемые в систему сервисной поддержки IBM, состоят исключительно из сведений о неполадках аппаратных средств и данных конфигурации. Данные о прикладных программах и пользовательские данные в компанию IBM не передаются.

Использование непрямого Internet-соединения через прокси-сервер

Если по требованиям установки НМС должна находиться в частной сети, то соединение с Интернетом может выполняться через SSL прокси-сервер, используемый для направления запросов в Интернет. Еще одно потенциальное преимущество использования SSL прокси-сервера состоит в том, что прокси-сервер может поддерживать средства регистрации и контроля.

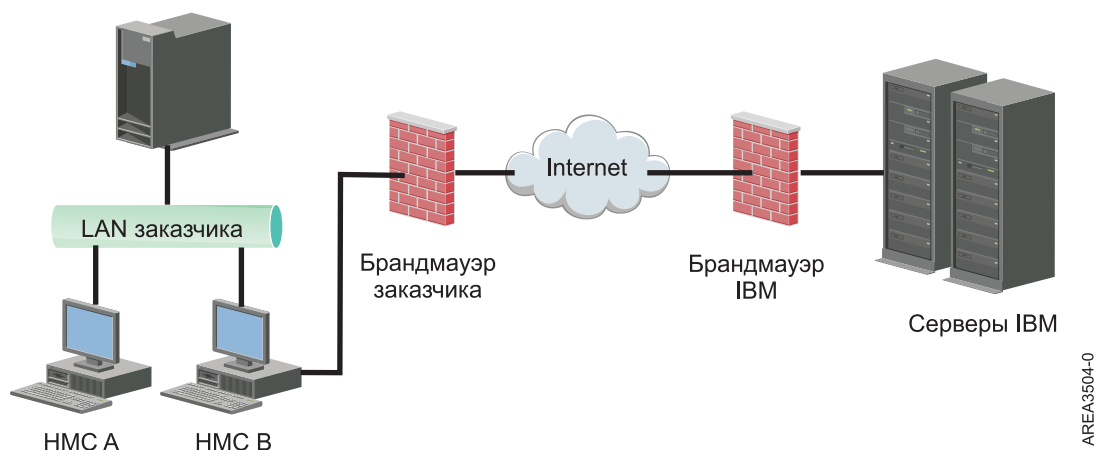
Для пересылки SSL сокетов сервер Proxy должен поддерживать основные функции заголовка сервера Proxy (как описано в RFC 2616) и метод CONNECT. По желанию можно настроить базовую идентификацию прокси (RFC 2617), чтобы НМС выполняла идентификацию перед пересылкой данных через прокси-сервер.



Для успешного обмена данными с НМС сервер Proxy клиента должен допускать соединение с портом 443. Можно настроить прокси-сервер таким образом, чтобы ограничить конкретные IP-адреса, с которыми НМС может устанавливать соединение. Список IP-адресов приведен в разделе “Списки адресов Internet SSL” на стр. 80.

Использование прямого SSL-соединения с Internet

Если можно устанавливать соединение НМС с Internet, и внешний брандмауэр можно настроить для передачи установленных исходящих пакетов TCP получателям, описанным в “Списки адресов Internet SSL” на стр. 80, то можно использовать прямое соединение с Internet.



Простые соединения:

Описываются IP-адреса HMC, используемые для простого соединения.

Доступна новая среда сервера вызова сервисного центра, выполняющая роль фронтального прокси-сервера текущей инфраструктуры вызова сервисного центра. Эта среда позволяет упростить работу за счет сокращения числа серверов IBM, поддержки IPv6 и расширенной защиты на основе NIST 800-131A. В брандмауэре требуется открыть меньшее число IP-адресов IBM. Трафик, связанный с вызовом сервисного центра, передается через прокси-сервер вызова сервисного центра.

Примечание: Простые соединения поддерживаются, начиная с HMC версии 8.3.0.

Для связи с сервисным центром IBM HMC, настроенная для работы с простыми соединениями, использует следующие адреса IPv4:

- 129.42.56.189
- 129.42.60.189
- 129.42.54.189

Для связи с сервисным центром IBM HMC, настроенная для работы с простыми соединениями, использует следующие адреса IPv6:

- 2620:0:6c0:200:129:42:56:189
- 2620:0:6c2:200:129:42:60:189
- 2620:0:6c4:200:129:42:54:189

Использование Internet SSL для соединения с удаленным сервисным центром:

Вся передача данных обрабатывается через сокет TCP, инициированные HMC: в процессе передачи используется скоростной SSL для шифрования передаваемых данных. TCP/IP адреса получателей публикуются (см. “Списки адресов Internet SSL” на стр. 80), что позволяет настраивать внешние брандмауэры для разрешения таких соединений.

Примечание: Для всей передачи данных используется стандартный порт HTTPS 443.

HMC можно включать для соединения с Internet напрямую или для непрямого соединения с Internet через клиентский прокси-сервер. Выбор подходящего решения зависит от защиты и требований к сетевому взаимодействию конкретной организации. HMC, настроенная для работы с соединениями Internet SSL, использует (прямо или через SSL прокси-сервер) следующие адреса.

Выбор протокола соединения с Интернетом:

Определите версию IP-адреса, используемую при соединении HMC с Internet-провайдером.

Большинство пользователей для связи с Internet-провайдером используют Internet Protocol Version 4 (IPv4). Для доступа к Internet адреса IPv4 имеют формат, состоящий из четырех байтов адреса IPv4, разделенных точками (например 9.60.12.123). Также можно использовать Internet Protocol Version 6 (IPv6). IPv6 часто используется администраторами сети для обеспечения уникального пространства адресов. Если вы не уверены в том, какой протокол используется в вашей системе, обратитесь к сетевому администратору. Дополнительная информация об использовании каждой версии приведена в “Установка IPv4-адреса” на стр. 99 и “Установка IPv6-адреса” на стр. 100.

Списки адресов Internet SSL:

Описываются адреса HMC, используемые при соединении с Internet по протоколу SSL.

Для связи с сервисным центром IBM HMC, настроенная для работы с соединениями Internet SSL, использует следующие адреса IPv4.

Следующие адреса IPv4 используются для всех регионов:

- 129.42.26.224
- 129.42.42.224
- 129.42.50.224
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216
- 170.225.15.41

Следующие адреса IPv4 используются для Северной и Южной Америк:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

Следующие адреса IPv4 используются для всех регионов, за исключением Северной и Южной Америк:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

Примечание: При настройке брандмауэра, который должен разрешать соединение HMC с указанными серверами, требуются только IP-адреса, специфические для географического региона.

Для связи с сервисным центром IBM HMC, настроенная для работы с соединениями Internet SSL, использует следующие адреса IPv6:

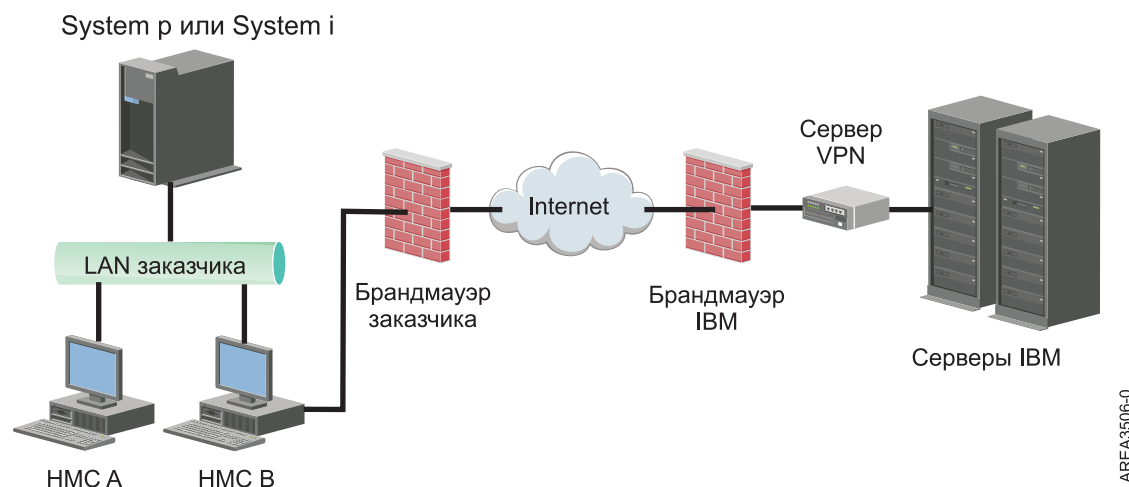
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

Использование виртуальной частной сети для соединения с сервисным центром:

Виртуальная частная сеть (VPN) обеспечивает защиту соединения с удаленным сервисным центром.

Примечание: Соединение этого типа доступно только в НМС версии 8.2.0 и более ранних версий.

VPN обеспечивает конфиденциальность отдельной сети по общедоступным соединениям путем применения шифрования и других способов защиты данных в физически разделенных сетевых соединениях стандартных частных сетей. Кроме использования для передачи исходящих сообщений, соединение VPN можно также настраивать по мере необходимости для поддержки запросов к сервисной службе.



Соединение с Интернетом обеспечивает администратор системы. При необходимости брандмауэр можно настроить таким образом, чтобы ограничить IP-адреса, к которым может подключаться НМС. При необходимости настройки брандмауэра для ограничения IP-адресов обратитесь к “Список адресов серверов VPN”, где приведен список возможных адресов.

Дополнительная информация о соединении с Internet с использованием VPN на основе LAN приведена в разделе “Настройка типов сетей НМС” на стр. 94.

Список адресов серверов VPN:

Приведен список серверов, используемых НМС, когда НМС настроена для работы по соединению с Internet VPN.

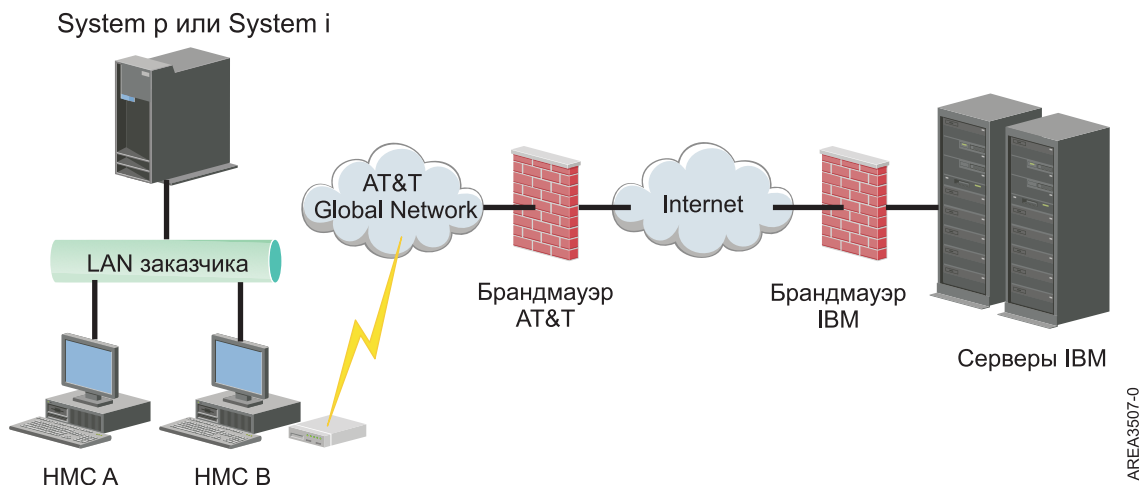
Если НМС настроена для работы по соединению с Internet VPN, она использует следующие серверы. Для всех соединений используются ESP и UDP на порте 500 и порте 4500 в случае использования брандмауэра преобразования сетевых адресов (NAT).

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

Использование телефона и модемов для соединения с удаленным сервисным центром:

При использовании модема для соединения с удаленным сервисным центром необходимо иметь выделенную аналоговую линию. НМС использует модем для соединения по телефонным линиям с глобальной сетью и для соединения со службой поддержки IBM.

Примечание: Соединение этого типа доступно только в НМС версии 8.2.0 и более ранних версий.



Дополнительная информация о соединении с удаленным сервисным центром с помощью телефона и модема приведена в разделе “Настройка типов сетей НМС” на стр. 94.

Использование нескольких серверов вызова сервисного центра:

Приведены необходимые сведения для использования нескольких серверов вызова сервисного центра.

Во избежание единственной точки сбоя настройте НМС для использования нескольких серверов вызова сервисного центра. Каждое сервисное событие будет обрабатываться первым доступным сервером. Если произойдет сбой соединения или передачи с этого сервера, то попытка отправки сервисного запроса будет повторяться со следующих доступных серверов до тех пор, пока она не будет успешно завершена или пока не произойдет сбой на всех серверах.

Сообщение о неполадке отправляется подключенной НМС, которая была распознана при анализе неполадок как главная консоль анализа для данной управляемой системы. Главная консоль также отправляет копию отчета о неполадке вспомогательным НМС. Вспомогательная НМС должна быть распознана в сети главной НМС. Вспомогательная НМС распознается главной НМС как дополнительный сервер вызова сервисного центра, если:

- Главная НМС настроена для использования "обнаруженных" серверов вызова сервисного центра, и сервер либо находится в той же подсети, что и главная НМС, либо управляет той же системой
- Сервер вызова сервисного центра был вручную добавлен в список консолей серверов, доступных для осуществления исходящих соединений

Подготовка к настройке НМС

Пользуясь этим разделом, соберите обязательные параметры конфигурации, которые понадобятся для выполнения шагов настройки.

Для того чтобы настроить НМС, ознакомьтесь со связанными концепциями, спланируйте варианты решения и подготовьте необходимую информацию.

В этом разделе приведена информация, необходимая для подключения НМС к следующим устройствам и системам:

- Служебные процессоры управляемых систем
- Логические разделы управляемых систем
- Удаленные рабочие станции

- Служба поддержки IBM для реализации функций “вызова сервисного центра”.

Примечание: Существуют дополнительные сведения о соединениях и защите. Дополнительная информация приведена в документе **ESA for HMC Connectivity Security for IBM POWER6, POWER7 and POWER8 Processor-Based Systems and IBM Storage Systems DS8000** : IBM Electronic Service Agent (<http://www-01.ibm.com/support/esa/security.htm>).

Для подготовки конфигурации НМС выполните следующие действия:

1. Приобретите и установите самый новый уровень версии НМС, который вы хотите установить.
2. Определите физическое расположение НМС по отношению к управляемым серверам. Если расстояние между НМС и управляемой системой превышает 7,5 метров, то необходимо настроить доступ к НМС через веб-браузер.
3. Определите серверы, которые должны работать под управлением НМС.
4. Определите, будет ли для управления серверами использоваться частная или открытая сеть. В частной сети следует использовать сервер DHCP, если не применяется конфигурация Cluster Systems Management (CSM). CSM не поддерживает IPv6. Для доступа к CSM нужно иметь две сети. Дополнительная информация о CSM приведена в соответствующей документации. Дополнительная информация об открытых и частных сетях приведена в разделе “Частные и открытые сети в среде НМС” на стр. 75.
5. В открытой сети адрес FSP следует указать вручную с помощью меню расширенного интерфейса управления системой (ASMI). Рекомендуется использовать частную сеть без возможности маршрутизации.
6. Если у вас две НМС, назначьте главную и вспомогательную НМС. Главная НМС должна находиться физически ближе к компьютеру и быть настроена для вызова сервисного центра.
7. Определите сетевые параметры, которые потребуется настроить для подключения НМС к удаленным системам, логическим разделам и сетевым устройствам.
8. Определите способ вызова сервисного центра. Можно выбрать исходящее соединение Secure Socket Layer (SSL), модем или соединение виртуальной частной сети (VPN).
9. Определите пользователей НМС, пароли пользователей, а также выполняемые ими роли. Пароли должны быть указаны для пользователей hscroot и hscpe.
10. Подготовьте следующую информацию об организации:
 - Имя компании
 - Имя администратора
 - Электронный адрес
 - Номера телефонов
 - Номера факсов
 - Адрес помещения, в котором предполагается установить НМС
11. Если планируется уведомлять операторов или администраторов об отправке информации в сервисный центр IBM, то укажите сервер SMTP и электронные адреса.
12. Необходимо задать следующие пароли:
 - Пароль доступа для идентификации НМС при обращении к FSP.
 - Пароль ASMI для **администратора**.
 - Пароль ASMI для **обычных** пользователей.

Укажите пароли при первом подключении НМС к новому серверу. В случае применения резервной или второй консоли НМС необходимо получить пароль пользователя НМС и указать его при первом подключении к FSP управляемого сервера.

После завершения подготовительной процедуры перейдите к разделу “Форма настройки НМС перед установкой” на стр. 84.

Форма настройки НМС перед установкой

В этой справочной таблице приведена информация, необходимая для подготовки к установке.

Параметры сети

Интерфейс LAN: Выберите доступные адаптеры (например, eth0, eth1), с помощью которых НМС будет соединяться с управляемыми системами, логическими разделами, сервисным центром и/или удаленными пользователями. Дополнительная информация приведена в разделе “Сетевые соединения НМС” на стр. 73. Соединение с НМС может устанавливаться в частной или открытой сети.

Пропускная способность и дуплексный режим адаптера Ethernet

Введите требуемую пропускную способность и дуплексный режим адаптера Ethernet. Параметр автоматическое определение определяет оптимальный параметр для данных аппаратных средств. Стандартное значение = Автоматическое определение Пропускная способность задает пропускную способность в дуплексном режиме адаптера Ethernet. Выберите автоматическое определение, если не требуется указывать конкретную пропускную способность. Любое устройство, подключенное к FSP (коммутаторы/НМС) должно работать в режиме Автоматически (быстродействие) / Автоматически (дуплексный), поскольку это режим FSP по умолчанию, который нельзя изменить.

Таблица 11. Пропускная способность и дуплексный режим адаптера Ethernet

	eth0	eth1	eth2	eth3
Выберите пропускную способность и дуплексный режим				
Пропускная способность (Автоматическое определение, 10/100/1000 дуплексный/полудуплексный)				

Дополнительная информация об открытых и частных сетях приведена в разделе “Частные и открытые сети в среде НМС” на стр. 75.

Таблица 12. Частные и открытые сети

	eth0	eth1	eth2	eth3
Для каждого адаптера укажите Частная или Открытая сеть				

Протокол динамической настройки хостов (DHCP) является автоматическим способом динамической настройки клиента. Данную НМС можно определить как сервер DHCP. Для первой или единственной НМС в частной сети разрешите НМС в качестве сервера DHCP. Как только это будет сделано, НМС автоматически настроит и найдет управляемые системы.

Для адаптеров Ethernet, заданных как частные сети, заполните следующую таблицу:

Таблица 13. Частные сети

	eth0	eth1
Определить эту НМС как сервер DHCP? (да/нет)		
Если "да," запишите диапазон IP-адресов, который необходимо использовать.		

В случае применения НМС 7063-CR1 необходимо подключить порт **IPMI** Ethernet к сети, чтобы обеспечить доступ к контроллеру управления платформой (ВМС) в НМС. Дополнительная информация приведена в разделе “Настройка связи ВМС” на стр. 146. Заполните следующую таблицу для соединения ВМС.

Таблица 14. Соединение ВМС

	IPMI
Вы хотите настроить это соединение в режиме DHCP? (да/нет)	
Если "нет", введите указанные статические адреса ниже:	
IP-адрес:	
Маска подсети:	
Шлюз:	

Для адаптеров Ethernet, заданных как *открытые* сети, заполните следующие таблицы. Более подробная информация о различных версиях протокола IP приведена в разделе “Выбор протокола соединения с Интернетом” на стр. 80.

Применение IPv6

Если вы используете IPv6, обсудите с администратором сети то, как необходимо получать IP-адреса. Затем заполните следующие таблицы:

Таблица 15. Применение IPv6

	eth0	eth1	eth2	eth3
Используете ли вы статически присвоенный IP-адрес? Если "да", укажите его здесь.				

Таблица 16. Применение IPv6

	eth0	eth1	eth2	eth3
Получаете ли вы IP-адреса от сервера DHCP? (Да/Нет)				

Таблица 17. Применение IPv6

	eth0	eth1	eth2	eth3
Получаете ли вы IP-адреса от маршрутизатора IPv6?				

Дополнительная информация о настройке адресов IPv6 приведена в разделе “Установка IPv6-адреса” на стр. 100. Дополнительная информация об использовании только адресов IPv6 приведена в разделе “Использование только адресов IPv6” на стр. 100.

Применение IPv4

Заполните следующие таблицы для адаптеров Ethernet, заданных как открытые сети с использованием IPv4.

Таблица 18. Применение IPv4

	eth0	eth1	eth2	eth3
Получать IP-адреса автоматически? (да/нет)				
Если "нет", введите указанный адрес ниже:				
Адрес интерфейса TCP/IP:				
Маска сети интерфейса TCP/IP:				
Параметры брандмауэра:				
Настроить параметры брандмауэра НМС? (да/нет)				
Если "да", перечислите приложения и IP-адреса, которые должны пропускаться через брандмауэр:				

Информация о TCP/IP

Уникальный адрес TCP/IP требуется для каждого узла, как для элемента поддержки (SE), так и для консоли аппаратного обеспечения (НМС). Заданная маска сети используется для создания уникального адреса (по умолчанию) для локальной частной LAN. Если узлы будут связаны в более крупную сеть с устанавливаемым адресом TCP/IP, можно указать адрес TCP/IP. Стандартное значение генерируется системой.

Параметры брандмауэра

Параметры брандмауэра НМС создают защитный барьер, который разрешает или запрещает доступ к конкретным сетевым приложениям на НМС. Эти параметры управления можно устанавливать для каждого физического интерфейса сети отдельно; таким образом можно регулировать, через какую НМС будет предоставляться доступ к сетевым приложениям в каждой сети.

Если хотя бы один адаптер настроен как адаптер открытой сети, то для разрешения доступа к LAN с НМС потребуется следующая дополнительная информация:

Таблица 19. Информация о локальном хосте

Информация о локальном хосте	
Имя хоста НМС:	
Имя домена:	
Описание НМС:	
Информация о шлюзе	
Адрес шлюза: (nnn.nnn.nnn.nnn)	
Устройство шлюза:	
Разрешение DNS	
Использовать DNS? (да/нет)	

Таблица 19. Информация о локальном хосте (продолжение)

Информация о локальном хосте	
Если “да”, укажите очередность обращения к серверам DNS ниже:	
1.	
2.	
Порядок просмотра доменных суффиксов:	
1.	
2.	

Информация о локальном хосте

Для того чтобы идентифицировать консоль аппаратного обеспечения (НМС) для сети, введите имя хоста и имя домена НМС. Введите полное имя хоста, кроме случаев, когда в сети используются только короткие имена. Пример имени домена: name.yourcompany.com

Информация о шлюзе

Для определения стандартного шлюза введите адрес TCP/IP, который будет использоваться для маршрутизации IP-пакетов. Адрес шлюза сообщает каждому компьютеру или сетевому устройству, когда пересылать данные, если целевая станция и отправитель находятся в разных подсетях.

Включение DNS

Система имен доменов (DNS) служит стандартным соглашением об именах для поиска компьютеров, использующих IP-протокол. Определив серверы DNS, можно вместо IP-адресов использовать имена хостов для идентификации серверов и консолей аппаратного обеспечения (НМС).

Очередность обращения к серверам DNS

Введите IP-адреса серверов DNS, которые нужно будет искать для преобразования имен хостов и IP-адресов. Очередность обращения доступна только тогда, когда DNS включен.

Порядок просмотра доменных суффиксов

Введите используемые доменные суффиксы. НМС использует доменные суффиксы, которые добавляются к неполным именам для обращений к DNS. Суффиксы просматриваются в порядке их следования в списке. Порядок просмотра доступен только тогда, когда DNS включен.

Уведомление по электронной почте

Введите информацию для контактов по электронной почте, если желательно получать извещения по email при неполадках аппаратных средств локальной системы.

Таблица 20. Уведомление по электронной почте

Поля	
Адреса электронной почты:	
Сервер SMTP:	
Порт:	
Уведомлять об ошибках:	
Только события при неполадках для сервисного центра	
События при всех неполадках	

Сервер SMTP

Введите адрес SMTP-сервера, который будет использоваться для отправки электронного сообщения. Пример имени сервера SMTP - relay.us.ibm.com.

SMTP - это протокол для отправки электронной почты. При использовании SMTP клиент отправляет сообщение и обменивается данными с сервером SMTP по протоколу SMTP.

Если вам не известен адрес SMTP сервера или нет уверенности в его правильности, обратитесь к администратору сети.

Порт Введите номер порта сервера, который нужно оповещать о системном событии, или воспользуйтесь стандартным портом.

Электронный адрес

Введите настроенные электронные адреса для отправки сообщений о системных событиях.

- **Только события при неполадках для сервисного центра** выбирают только для получения извещения при наступлении событий, создающих сервисную функцию.
- **События при всех неполадках** выбирают для получения извещения при наступлении любых событий.

Сервисная контактная информация

Таблица 21. Сервисная контактная информация

Сервисная контактная информация	
Имя компании	
Имя администратора	
Электронный адрес	
Номер телефона	
Другой номер телефона	
Номер факса	
Другой номер факса	
Адрес местонахождения	
Адрес местонахождения 2	
Город или населенный пункт	
Состояние	
Почтовый индекс	
Страна или регион	
Местонахождение НМС (если совпадает с вышеуказанным адресом администратора, укажите “то же”):	
Адрес местонахождения	
Адрес местонахождения 2	
Город или населенный пункт	
Состояние	
Почтовый индекс	
Страна или регион	

Связь с сервисным центром и доступ

Выберите тип соединения для контактов с сервисным центром. Описание указанных методов, включая требования к характеристикам защиты и конфигурации, приведено в разделе “Выбор способа соединения для сервисного сервера” на стр. 77.

Таблица 22. Тип соединения

Тип соединения	
	Secure Sockets Layer (SSL) через Internet
	Соединение по телефонной линии с локальной НМС
	Виртуальная частная сеть (VPN) через Internet

Secure Sockets Layer (SSL) через Internet:

При наличии существующего Internet-соединения с НМС им можно пользоваться для связи с сервисным центром. С сервисным центром можно связываться напрямую с использованием зашифрованного Secure Sockets Layer (SSL) по существующему Internet соединению. Если требуется настроить использование зашифрованного SSL с использованием непрямого соединения через SSL Proxy, выберите **Использовать SSL Proxy**.

Таблица 23. Secure Sockets Layer (SSL) через Internet

Secure Sockets Layer (SSL) через Internet	
Использовать SSL? (да/нет)	
Если "да", введите информацию ниже:	
Адрес:	
Порт:	
Идентифицировать с SSL Proxy?	
Если "да", введите информацию ниже:	
Пользователь:	
Пароль:	

Используемый протокол соединения с Internet

Более подробная информация о различных протоколах IP приведена в разделе “Выбор протокола соединения с Интернетом” на стр. 80.

___ IPv4

___ IPv6

___ IPv4 и IPv6

Соединение по телефонной линии с локальной НМС

Введите информацию телефонного соединения для настройки локального модема. Укажите номера телефонов для связи с сервисным центром. При соединении телефонные номера будут набираться в порядке их следования в списке.

Таблица 24. Соединение по телефонной линии с локальной НМС

Поля	
Префикс телефонного номера:	
Тональный:	
Импульсный:	

Таблица 24. Соединение по телефонной линии с локальной НМС (продолжение)

Поля	
Дождаться гудка?	
Включить громкую связь?	

Виртуальная частная сеть (VPN)

При наличии существующего Internet-соединения с НМС им можно пользоваться для связи с сервисным центром. С сервисным центром можно связываться напрямую через виртуальную частную сеть (VPN) с использованием существующего Internet соединения.

Примечание: При выборе виртуальной частной сети (VPN) через Internet никакие другие параметры выбирать не нужно.

Серверы сервисного центра

Определите, какие НМС необходимо настроить в качестве серверов для вызова сервисного центра и службы поддержки. Дополнительная информация об использовании нескольких серверов вызова сервисного центра приведена в разделе “Использование нескольких серверов вызова сервисного центра” на стр. 82.

___ Эту НМС

___ Другую НМС

Если вы выбрали **Другую НМС**, перечислите другие НМС, настроенные как серверы вызова сервисного центра:

Таблица 25. Другие НМС, настроенные как серверы вызова сервисного центра

Список имен хостов или IP-адресов НМС, настроенных как серверы вызова сервисного центра	

Дополнительные преимущества поддержки

Мои системы и премиальный поиск

Таблица 26. Дополнительные преимущества поддержки

Поля	
Укажите свой ИД в IBM	
Укажите свой ИД в IBM	

Для получения доступа к ценной персонализированной вспомогательной информации в разделах Мои системы и Премиальный поиск веб-сайта Electronic Services пользователи должны зарегистрировать ID IBM в данной системе. При отсутствии ID IBM зарегистрироваться для его получения можно на: www.ibm.com/account/profile.

Примечание: IBM предоставляет персонализированные веб-функции, в которых используется информация, собранная приложением IBM Electronic Service Agent. Для того чтобы иметь возможность пользоваться этими функциями, необходимо вначале зарегистрироваться на веб-сайте регистрации в IBM по адресу <http://www.ibm.com/account/profile>.

Для предоставления пользователям права на использование информации Electronic Service Agent с целью персонализации веб-функций введите ID IBM, зарегистрированный на веб-сайте регистрации IBM. Для ознакомления с ценной информацией поддержки, доступной для клиентов, зарегистрировавших ID IBM в своих системах, перейдите к разделу <http://www.ibm.com/support/electronic.systems>.

Настройка НМС

Рассмотрена настройка сетевых соединений, защиты, служебных приложений и некоторых параметров для пользователей.

В зависимости от предполагаемого уровня настройки конфигурации НМС, можно воспользоваться несколькими вариантами настройки НМС, выбирая из них наиболее подходящий для своих задач. Инструментальное средство Мастер пошаговой настройки из НМС позволяет легко и быстро выполнить настройку НМС. Мастер предоставляет возможность выбрать быстрое прохождение, при этом быстро создается рекомендуемая среда НМС. Кроме того, в нем предусмотрена возможность подробного ознакомления с доступными параметрами. Настройку можно также выполнить без помощи мастера в соответствии с инструкциями из раздела Настройка НМС с помощью меню НМС.

Перед выполнением настройки получите обязательную информацию о конфигурации, которая потребуется для успешного выполнения шагов. Список обязательной информации приведен в разделе “Подготовка к настройке НМС” на стр. 82. По завершении подготовки выполните инструкции из раздела “Форма настройки НМС перед установкой” на стр. 84 и вернитесь к этому разделу.

Настройка НМС с помощью быстрого выполнения мастера пошаговой настройки

В большинстве случаев НМС можно настроить для эффективной работы с помощью многочисленных стандартных параметров. Для того чтобы быстро и эффективно подготовить НМС к работе, воспользуйтесь данной справочной таблицей быстрого выполнения. После выполнения этих действий НМС будет настроена в качестве сервера протокола динамической настройки хостов (DHCP) частной (подключенной напрямую) сети.

Запуск НМС и выполнение шагов мастера пошаговой настройки:

Войдите в интерфейс НМС и настройте свою НМС с помощью мастера пошаговой настройки.

Примечание: В случае новой установки убедитесь, что управляемая система не подключена к источнику питания. Для консоли НМС, монтируемой в стойке, данное требование означает, что единственным устройством, подключаемым к шине распределения питания (PDB) до подключения источника питания, является НМС. Если речь идет о второй НМС, подключенной к той же управляемой системе, то управляемая система может быть подключена к источнику питания.

1. Включите НМС, нажав кнопку питания.
2. Дождитесь, пока НМС автоматически выберет стандартный язык и желательную локаль по истечении 30 секунд.
3. Примите условия лицензионных соглашений на Консоль аппаратного обеспечения. Если условия лицензионных соглашений на Консоль аппаратного обеспечения не будут приняты, выполнить настройку НМС не удастся.
4. Выберите **Войти и запустить веб-приложение Консоль аппаратного обеспечения**.
5. Войдите в НМС:

Примечание: Введите пароль, если его изменил системный администратор (**hmcadmin**).

- ИД: hscroot
- Пароль: abc123

Откроется мастер пошаговой настройки.

6. Нажмите **ОК** в окне входа в пошаговую настройку.

Примечание: Если после запуска НМС Мастер пошаговой настройки не показан, выберите **Мастер пошаговой настройки** в области навигации начальной страницы НМС.

7. Выполните шаги, предлагаемые мастером пошаговой настройки, в соответствии с заполненной перед установкой справочной таблицей. Для продолжения нажмите **Да** и выполните шаги, описанные в мастере Соединений и вызова сервисного центра.
8. В окне Обзор нажмите кнопку **Закончить**.
9. Подсоедините к управляемой системе перекрестный кабель Ethernet.
10. В области навигации НМС выберите **Управление службами**.
11. В области содержимого выберите **Предоставить пользователю права доступа**. Откроется окно Предоставление пользователю прав доступа.
12. Введите свой ИД IBM в поле и нажмите **ОК**.

Проверка конфигурации:

В окне Состояние отследите текущее состояние разных выбранных вами параметров конфигурации. Для некоторых параметров в течение нескольких минут может отражаться состояние Ожидание. Выберите **Просмотреть протокол** и просмотрите сообщения о состоянии по каждой задаче. Мастер пошаговой настройки можно закрыть в любой момент - для этого нужно нажать кнопку **Закрыть**. При этом запущенные задачи будут продолжать выполнение. НМС настроена.

Настройка НМС с помощью меню НМС

В этом разделе приведен полный список всех задач настройки НМС, направляющих пользователя в процессе настройки НМС. Выберите данный пункт, если Мастер пошаговой настройки не будет использован.

Для вступления в силу параметров конфигурации необходимо будет перезапустить НМС, поэтому имеет смысл распечатать данную таблицу, чтобы пользоваться ею при настройке НМС.

В данном документе имеются ссылки на задачи, не вошедшие в данный PDF. Для получения доступа к дополнительным материалам поддержки можно обратиться к разделу **Дополнительные ресурсы** на начальных страницах НМС.

Предварительные требования

Перед тем, как приступить к настройке НМС с помощью меню НМС, выполните подготовительные действия, описанные в разделе “Подготовка к настройке НМС” на стр. 82.

Таблица 27. Задачи настройки НМС вручную и источники связанной информации

Задача	Где искать связанную информацию
1. Запустите НМС.	“Запуск НМС” на стр. 93
2. Задайте дату и время.	
3. Измените стандартные пароли.	
4. Создайте дополнительных пользователей и вернитесь к этой справочной таблице.	
5. Настройте сетевые соединения.	“Настройка типов сетей НМС” на стр. 94
6. При использовании открытой сети и фиксированных IP-адресов установите идентификационную информацию.	

Таблица 27. Задачи настройки НМС вручную и источники связанной информации (продолжение)

Задача	Где искать связанную информацию
7. При использовании открытой сети и фиксированных IP-адресов настройте запись маршрутизации как стандартный шлюз.	“Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 101
8. При использовании открытой сети и фиксированных IP-адресов настройте службы имен доменов.	“Настройка служб имен доменов” на стр. 101
9. При использовании фиксированных IP-адресов и включении DNS настройте доменные суффиксы.	“Настройка доменных суффиксов” на стр. 102
10. Настройте сервер для соединения со службой поддержки IBM и вернитесь к данной справочной таблице после выполнения этого шага.	“Настройка НМС для связи с сервисным центром и службой поддержки” на стр. 103
11. Настройте Администратор событий для вызова сервисного центра.	“Настройка Администратора событий для вызова сервисного центра” на стр. 108
12. Подключите управляемую систему к источнику питания.	
13. Укажите пароли для управляемой системы, а также пароли ASMI (общий и администратора).	“Задание паролей для управляемой системы” на стр. 109
14. Задайте дату и время управляемой системы с помощью ASMI.	
15. Запустите управляемую систему и вернитесь к этой справочной таблице.	
16. Убедитесь, что в управляемой системе создан один логический раздел.	
17. Необязательно: Добавьте другую управляемую систему и вернитесь к этой справочной таблице.	
18. Необязательно: При установке нового сервера с НМС настройте логические разделы и установите операционную систему.	
19. Если вы не устанавливаете новый сервер, то выполните задачи заключительного этапа настройки для дополнительной настройки конфигурации.	“Действия после настройки” на стр. 110

Запуск НМС:

Войдите в НМС и выберите рабочий язык для интерфейса. Для первого входа в НМС воспользуйтесь стандартными ИД hscroot и паролем abc123.

Для запуска НМС выполните следующие действия:

1. Включите НМС, нажав кнопку питания.
2. Если предпочитаемым языком является английский, перейдите к шагу 4.
Если предпочтение отдается другому языку, введите номер **2** после предложения изменить локаль.

Примечание: Для ответа на предложение пользователю дается 30 секунд.

3. Выберите необходимую локаль в окне Выбор локали и нажмите кнопку **ОК**. Локаль определяет язык, который используется интерфейсом НМС.
4. Выберите **Войти и запустить веб-приложение Консоль аппаратного обеспечения**.
5. Войдите в НМС, используя приведенный ниже стандартный ИД и пароль пользователя:

ИД: hscroot

Пароль: abc123

Примечание: В НМС версии 8.1.0.1 можно выбрать следующие варианты входа в систему:

Вход в систему: Последний вход в систему, НМС Classic или НМС Enhanced

Выберите интерфейс программного обеспечения для входа в НМС. Интерфейс НМС Classic предоставляет доступ ко всем стандартным функциям НМС, а интерфейс НМС Enhanced предлагает переработанные и новые задачи и функции виртуализации.

Последний вход в систему

Отображает графический пользовательский интерфейс, выбранный в предыдущем сеансе входа в систему.

НМС Enhanced

Отображает новый расширенный графический пользовательский интерфейс с расширенными функциями PowerVM.

НМС Classic

Отображает стандартный графический пользовательский интерфейс без расширенных функций PowerVM.

Примечание: Если НМС работает в качестве сервера DHCP, то она применяет пароль по умолчанию при первом подключении к служебному процессору.

6. Нажмите Enter.

Изменение даты и времени:

Работающие от батарей часы хранят дату и время НМС. Иногда необходимо восстановить дату и время консоли, например, в случае замены батарей или при физическом перемещении системы в другой часовой пояс. Знакомит с процедурой изменения даты и времени для НМС.

При смене информации о дате и времени внесенные изменения не отразятся на системах и логических разделах под управлением НМС.

Для изменения даты и времени НМС выполните следующие действия:

1. Проверьте, входите ли вы в группу пользователей с одной из ролей:
 - Главный администратор
 - Сотрудник сервисного представительства
 - Оператор
 - Наблюдатель
2. В области навигации выберите **Управление НМС**.
3. На панели содержимого выберите **Изменить дату и время**.
4. При выборе пункта **UTC** в поле **Часы** значение времени будет настроено автоматически как сезонное время выбранного часового пояса. Введите дату, время и часовой пояс и нажмите **ОК**.

Настройка типов сетей НМС:

Настройка НМС для взаимодействия с управляемой системой, логическими разделами, удаленными пользователями и службой поддержки.

Настройка НМС для подключения к управляемой системе по открытой сети:

Процедура настройки НМС для подключения к управляемой системе по открытой сети.

Для того чтобы настроить НМС для подключения к управляемой системе по открытой сети, выполните следующие действия:

Таблица 28. Настройка НМС для подключения к управляемой системе по открытой сети

Задача	Где искать связанную информацию
1. Выберите интерфейс управляемой системы. Рекомендуемый интерфейс: eth0 .	“Форма настройки НМС перед установкой” на стр. 84
2. Выберите порты Ethernet для НМС.	“Идентификация порта Ethernet, определяемого как eth0” на стр. 97
3. Настройте адаптер Ethernet. Для этого выполните следующие задачи:	
a. Укажите пропускную способность.	“Установка пропускной способности” на стр. 98
b. Выберите тип открытой сети.	“Выбор типа сети (частная, открытая)” на стр. 99
c. Укажите статические адреса.	“Установка IPv4-адреса” на стр. 99
d. Укажите брандмауэр.	“Изменение параметров брандмауэра НМС” на стр. 100
e. Настройте шлюз по умолчанию.	“Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 101
f. Настройте DNS.	“Настройка служб имен доменов” на стр. 101
4. Настройте дополнительные адаптеры (если они установлены).	
5. Проверьте соединение между управляемым сервером и НМС.	“Проверка соединения между НМС и управляемой системой” на стр. 110

Настройка НМС для подключения к управляемой системе по частной сети:

Процедура настройки НМС для подключения к управляемой системе по частной сети.

Для того чтобы настроить НМС для подключения к управляемой системе по частной сети, выполните следующие действия:

Таблица 29. Настройка НМС для подключения к управляемой системе по частной сети

Задача	Где искать связанную информацию
1. Выберите интерфейс управляемой системы.	“Форма настройки НМС перед установкой” на стр. 84
2. Выберите порты Ethernet для НМС.	“Идентификация порта Ethernet, определяемого как eth0” на стр. 97
3. Настройте НМС в качестве сервера DHCP.	“Настройка НМС в качестве сервера DHCP” на стр. 99
4. Проверьте соединение между управляемым сервером и НМС.	“Проверка соединения между НМС и управляемой системой” на стр. 110

Настройка НМС для подключения к логическим разделам по открытой сети:

Для того чтобы настроить НМС для подключения к логическим разделам по открытой сети, выполните следующие действия:

Таблица 30. Настройка НМС для подключения к логическим разделам по открытой сети

Задача	Где искать связанную информацию
1. Выберите интерфейс управляемой системы.	“Форма настройки НМС перед установкой” на стр. 84
2. Выберите порты Ethernet для НМС.	“Идентификация порта Ethernet, определяемого как eth0” на стр. 97
3. Настройте адаптер Ethernet. Для этого выполните следующие задачи:	
a. Укажите пропускную способность.	“Установка пропускной способности” на стр. 98

Таблица 30. Настройка НМС для подключения к логическим разделам по открытой сети (продолжение)

Задача	Где искать связанную информацию
b. Выберите тип открытой сети.	“Выбор типа сети (частная, открытая)” на стр. 99
c. Укажите статические адреса.	“Установка IPv4-адреса” на стр. 99
d. Укажите брандмауэр.	“Изменение параметров брандмауэра НМС” на стр. 100
e. Настройте шлюз по умолчанию.	“Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 101
f. Настройте DNS.	“Настройка служб имен доменов” на стр. 101
4. Настройте дополнительные адаптеры (если они установлены).	
5. Проверьте соединение между управляемым сервером и НМС.	“Проверка соединения между НМС и управляемой системой” на стр. 110

Настройка НМС для подключения к удаленным пользователям по открытой сети:

Для того чтобы настроить НМС для подключения к удаленным пользователям по открытой сети, выполните следующие действия:

Таблица 31. Настройка НМС для подключения к удаленным пользователям по открытой сети

Задача	Где искать связанную информацию
1. Выберите интерфейс управляемой системы.	“Форма настройки НМС перед установкой” на стр. 84
2. Выберите порты Ethernet для НМС.	“Идентификация порта Ethernet, определяемого как eth0” на стр. 97
3. Настройте адаптер Ethernet. Для этого выполните следующие задачи:	
a. Укажите пропускную способность.	“Установка пропускной способности” на стр. 98
b. Выберите тип открытой сети.	“Выбор типа сети (частная, открытая)” на стр. 99
c. Укажите статические адреса.	“Установка IPv4-адреса” на стр. 99
d. Укажите брандмауэр.	“Изменение параметров брандмауэра НМС” на стр. 100
e. Настройте шлюз по умолчанию.	“Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 101
f. Настройте DNS.	“Настройка служб имен доменов” на стр. 101
g. Настройте суффиксы.	“Настройка доменных суффиксов” на стр. 102
4. Настройте дополнительные адаптеры (если они установлены).	

Настройка параметров сервера НМС для вызова сервисного центра:

Для настройки параметров сервера НМС для вызова сервисного центра и отправки сообщений о неполадках выполните следующие шаги:

Таблица 32. Настройка параметров сервера НМС для вызова сервисного центра

Задача	Где искать связанную информацию
1. Убедитесь, что у вас есть все необходимые сведения о клиенте	“Форма настройки НМС перед установкой” на стр. 84

Таблица 32. Настройка параметров сервера НМС для вызова сервисного центра (продолжение)

Задача	Где искать связанную информацию
2. Настройте НМС для отправки сообщений об ошибках или выберите существующий сервер для вызова сервисного центра	“Настройка локальной консоли для отправки сервисному центру сообщений об ошибках” на стр. 104 “Выбор из существующих серверов вызова сервисного центра для соединения со службой поддержки для данной НМС” на стр. 107
3. Убедитесь, что конфигурация вызова сервисного центра функционирует	“Проверка работоспособности соединения с сервисным центром и службой поддержки” на стр. 107
4. Предоставьте пользователям права доступа для просмотра собранных системных данных	“Предоставление пользователям права доступа для просмотра собранных системных данных” на стр. 107
5. Запланируйте передачу системных данных	“Передача служебной информации” на стр. 108

Идентификация порта Ethernet, определяемого как eth0:

Ethernet должна подключаться к управляемому серверу через порт Ethernet, определяемый как eth0 на вашем НМС.

Если в гнездах PCI НМС не установлены дополнительные адаптеры Ethernet, то основной встроенный порт Ethernet НМС всегда определяет как eth0 или eth1 при использовании НМС в качестве сервера DHCP для управляемых систем.

Если дополнительные адаптеры Ethernet в гнездах PCI установлены, то определение порта как eth0 будет зависеть от расположения и типа установленных адаптеров Ethernet.

Примечание: Существуют общие правила, которые в случае некоторых конфигураций могут не выполняться.

В следующей таблице описаны правила размещения адаптеров Ethernet для разных типов НМС.

Таблица 33. Типы НМС и соответствующие правила размещения Ethernet

Тип НМС	Правила размещения Ethernet
Смонтированные в стойке НМС с двумя встроенными портами Ethernet	НМС поддерживает только один дополнительный адаптер Ethernet. - Если дополнительный адаптер Ethernet установлен, то этот порт определяется как eth0. В этом случае первичный встроенный порт Ethernet определяется как eth1, а вторичный встроенный порт Ethernet - как eth2. - В случае двухпортового адаптера Ethernet в качестве порта eth0 обычно определяется порт с обозначением Act/Link A. Порт с обозначением Act/link B будет определен как eth1. Тогда первичный встроенный порт Ethernet определяется как eth2, а вторичный встроенный порт Ethernet - как eth3. - Если же адаптеры не установлены, то основной встроенный порт Ethernet определяется как eth0.

Таблица 33. Типы НМС и соответствующие правила размещения Ethernet (продолжение)

Тип НМС	Правила размещения Ethernet
Автономные модели с одним встроенным портом Ethernet	Рассмотренные определения будут зависеть от типа устанавливаемого адаптера Ethernet: • Если установлен только один адаптер Ethernet, то он будет определяться как <code>eth0</code>. • Для двухпортового адаптера Ethernet в качестве порта <code>eth0</code> будет определен порт с обозначением Act/link A. Порт с обозначением Act/link B будет определен как <code>eth1</code>. При этом основной встроенный порт Ethernet определяется как <code>eth2</code>. • Если ни один адаптер не установлен, то встроенный порт Ethernet определяется как <code>eth0</code>. • Установка нескольких адаптеров Ethernet рассматривается в разделе “Определение имени интерфейса для адаптера Ethernet”.

Определение имени интерфейса для адаптера Ethernet:

При настройке НМС в качестве сервера DHCP этот сервер сможет работать только с соединителями сетевой интерфейсной платы (NIC), которые НМС идентифицирует как `eth0` и `eth1`. Также необходимо выбрать соединитель NIC для подключения кабеля Ethernet. Обратитесь к соответствующей информации по выбору соединителей NIC, которые НМС идентифицирует как `eth0` и `eth1`.

Для того чтобы определить имя, присваиваемое НМС адаптеру Ethernet, выполните следующее:

1. Откройте терминал ограниченной оболочки. Выберите пункт **Управление НМС > Откройте Терминал ограниченной оболочки**.
2. Введите в командную строку следующее: `tail -f /var/log/messages`. Протокол сообщений смещается соответственно новым событиям.
3. Подключите кабель Ethernet. Если кабель уже подключен, отсоедините его, подождите 5 секунд и снова подключите. При подключении кабеля ограниченная оболочка перейдет на вывод некоторого сообщения. Следующий пример записи означает, что этот порт Ethernet идентифицируется как `eth0`: Aug 28 12:41:20 termite kernel: e1000: eth0: e1000_watchdog: NIC Link is Up 100.
4. Выполните эту процедуру для всех остальных портов Ethernet и запишите результаты.
5. Для остановки команды **tail** нажмите Ctrl+C.

Установка пропускной способности:

Знакомит с процессом установки пропускной способности и дуплексного режима адаптера Ethernet.

Стандартным параметром адаптера НМС является **Автоматическое определение**. Если адаптер подключен к коммутатору LAN, то необходимо настроить параметры портов коммутатора. Для настройки пропускной способности и дуплексного режима выполните следующие действия:

1. В области навигации выберите **Управление НМС**.
2. Нажмите кнопку **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. В разделе информации о локальной сети выберите **Автоматическое обнаружение** или укажите пропускную способность и дуплексный режим.
6. Нажмите **ОК**.

Выбор типа сети (частная, открытая):

Частная сеть обслуживания состоит из НМС и управляемых систем. Частная сеть обслуживания ограничивается консолями и системами, которыми они управляют. Это сеть, отдельная от сети компании. *Открытая сеть* состоит из частной сети обслуживания и сети компании. Кроме консолей и управляемых систем, в открытую сеть могут входить конечные точки сети, и сеть может охватывать несколько подсетей и сетевых устройств.

Для выбора частной или общей сети выполните следующее:

1. В области навигации выберите **Управление НМС**.
2. Нажмите кнопку **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Щелкните на вкладке **Сетевой адаптер**.
6. В разделе Информация о локальной сети выберите **Частная** или **Открытая**.
7. Нажмите **ОК**.

Настройка НМС в качестве сервера DHCP:

Протокол динамической настройки хостов (DHCP) является автоматическим способом динамической настройки клиента.

Для настройки НМС в качестве сервера DHCP выполните следующее:

1. В области навигации выберите **Управление НМС**.
2. В рабочей области выберите **Изменить параметры сети**. Откроется окно Настройка параметров сети.
3. Выберите нужный адаптер LAN и нажмите на **Сведения**.
4. Выберите **Частная** и укажите тип сети.
5. В разделе Сервер DHCP включите переключатель **Разрешить сервер DHCP**, чтобы разрешить НМС в качестве сервера DHCP.

Примечание: НМС можно настроить в качестве сервера DHCP только в частной сети. При использовании открытой сети выбрать опцию **Разрешить DHCP** невозможно.

6. Введите диапазон адресов сервера DHCP.
7. Нажмите **ОК**.

Если НМС настроена в качестве сервера DHCP в частной сети, необходимо проверить правильность настройки частной сети НМС DHCP. Информация о соединении НМС с частной сетью приведена в разделе “Выбор типа сети (частная, открытая)”.

Дополнительные сведения содержатся в разделе “НМС в качестве сервера DHCP” на стр. 75.

Установка IPv4-адреса:

Знакомит с процессом установки IPv4-адреса на НМС.

1. В области навигации выберите **Управление НМС**.
2. Нажмите кнопку **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Выберите вкладку **Основные параметры**.
6. Выберите адрес IPv4.
7. Если выбран пункт Указать IP-адрес, введите адрес интерфейса TCP/IP и маску сети интерфейса TCP/IP.

8. Нажмите кнопку **ОК**.

Установка IPv6-адреса:

Описан процесс установки IPv6-адреса на НМС.

1. В области навигации выберите **Управление НМС**.
2. Нажмите кнопку **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Выберите вкладку **Параметры IPv6**.
6. Выберите опцию автонастройка или добавьте постоянный IP адрес.
7. При добавлении IP адреса, введите адрес IPv6 и длину префикс, а затем нажмите **ОК**.
8. Нажмите кнопку **ОК**.

Использование только адресов IPv6:

Настройка НМС для использования только адресов IPv6.

1. В области навигации выберите **Управление НМС**.
2. Нажмите кнопку **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Выберите **Без адресов IPv4**.
6. Выберите вкладку **Параметры IPv6**.
7. Выберите **Использовать DHCPv6 для настройки параметров IP** или добавьте постоянные IP адреса. Затем нажмите **ОК**.

Для того чтобы изменения вступили в силу необходимо перезагрузить НМС.

Изменение параметров брандмауэра НМС:

В открытой сети брандмауэр обычно используется для управления внешним доступом к сети компании. В НМС также имеется брандмауэр на каждом Ethernet адаптере. Для удаленного управления НМС или предоставления удаленного доступа другим пользователям измените параметры брандмауэра адаптера Ethernet на консоли НМС, подключенной к вашей открытой сети.

Для настройки брандмауэра выполните следующие действия:

1. В области навигации выберите **Управление НМС**.
2. Нажмите кнопку **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Выберите вкладку **Брандмауэр**.
6. С помощью одного из приведенных ниже методов можно разрешить любой IP-адрес, использующий конкретные приложения через брандмауэр, или можно указать один или несколько IP-адресов:
 - Разрешить любой IP-адрес, использующий конкретное приложение через брандмауэр:
 - a. В верхнем окне выделите приложение.
 - b. Выберите **Разрешить входящие**. Приложение появится в нижнем окне - это говорит о том, что приложение выбрано.
 - Укажите IP-адреса, разрешенные через брандмауэр:
 - a. В верхнем окне выделите приложение.

- b. Выберите **Разрешить входящие по IP-адресу**.
 - c. В окне Разрешенные хосты введите IP-адрес и маску сети.
 - d. Выберите **Добавить** и нажмите кнопку **ОК**.
7. Нажмите кнопку **ОК**.

Включение доступа через удаленную оболочку с ограничениями:

При настройке брандмауэра можно включить доступ через удаленную оболочку с ограничениями.

Для включения доступа через удаленную оболочку с ограничениями выполните следующие действия:

1. В области навигации выберите **Управление НМС**.
2. Выберите **Удаленное выполнение команд**.
3. Выберите **Разрешить удаленное выполнение команд по протоколу ssh** и нажмите кнопку **ОК**.

Доступ через удаленную оболочку с ограничениями включен.

Включение удаленного доступа с помощью веб-браузера:

Можно настроить удаленный доступ к НМС с помощью веб-браузера.

Для включения удаленного доступа с помощью веб-браузера выполните следующие действия:

1. В области навигации выберите **Управление НМС**.
2. Выберите **Удаленная работа**.
3. Выберите **Включить** и нажмите кнопку **ОК**.

Удаленный доступ включен.

Настройка записи маршрутизации в качестве стандартного шлюза:

Знакомит с настройкой записи маршрутизации в качестве стандартного шлюза. Эта задача доступна только для открытой сети.

Для настройки записи маршрутизации в качестве стандартного шлюза выполните следующее:

1. В области навигации выберите **Управление НМС**.
2. В рабочей области выберите **Изменить параметры сети**. Откроется окно Настройка параметров сети.
3. Выберите вкладку **Маршрутизация**.
4. В области Информация о шлюзе по умолчанию введите адрес и устройства шлюза записи маршрутизации в качестве стандартного шлюза.
5. Нажмите **ОК**.

Настройка служб имен доменов:

При установке открытой сети настройте службы имен доменов.

При установке открытой сети настройте службы имен доменов. Система имен доменов (DNS) - это распределенная база данных для управления именами хостов и их соответствующими адресами протокола IP (IP-адресами). Для настройки служб имен доменов необходимо включить DNS и указать порядок просмотра доменных суффиксов.

1. В области навигации выберите **Управление НМС**.
2. В рабочей области выберите **Изменить параметры сети**. Откроется окно Изменение параметров сети.
3. Выберите вкладку **Службы имен**.
4. Для включения DNS выберите **DNS включено**.

5. Укажите порядок просмотра серверов DNS и доменных суффиксов и нажмите кнопку **Добавить**.
6. Нажмите **ОК**.

Настройка доменных суффиксов:

Список доменных суффиксов служит для поиска IP-адреса, начиная с первой записи списка.

Доменный суффикс - это строка после имени хоста, которая помогает находить его IP-адрес. Например, имя хоста `мое_имя` может быть не найдено. Но если в таблице доменных суффиксов присутствует строка `myloc.myscompany.com`, то сервер попытается найти также `myname.myloc.myscompany.com`.

Для настройки записи доменного суффикса выполните следующие действия:

1. В области навигации выберите **Управление НМС**.
2. В рабочей области выберите **Изменить параметры сети**. Откроется окно Настройка параметров сети.
3. Выберите вкладку **Службы имен**.
4. Введите строку в качестве записи доменного суффикса.
5. Выберите **Добавить**, и запись будет добавлена в список.

Настройка НМС для использования удаленной идентификации с помощью LDAP:

НМС можно настроить для использования удаленной идентификации с помощью LDAP (Упрощенный протокол доступа к каталогам).

Когда пользователь входит в НМС, сначала идентификация осуществляется путем сравнения с локальным файлом пароля. Если локальный файл пароля не обнаружен, НМС может связаться с удаленным сервером LDAP для идентификации. Для использования удаленной идентификации с помощью LDAP необходимо настроить НМС.

Примечание: Прежде чем настраивать НМС для использования удаленной идентификации с помощью LDAP, необходимо убедиться, что существует рабочее сетевое соединение между НМС и серверами LDAP. Дополнительная информация о настройке сетевых соединений НМС приведена в разделе “Настройка типов сетей НМС” на стр. 94.

Для настройки идентификации LDAP в Консоли аппаратного обеспечения НМС выполните следующие действия:

1. В области навигации выберите **Управление НМС**.
2. В области содержимого выберите **Настроить LDAP**. Откроется окно **Определение сервера LDAP**.
3. Выберите **Включить LDAP**.
4. Укажите сервер LDAP, который будет использоваться при идентификации (например, Microsoft Active Directory, Tivoli или Open LDAP).
5. Определите атрибут LDAP, используемый для идентификации пользователя. Значение по умолчанию - **uid**, но можно использовать собственное. Для Microsoft Active Directory применяется атрибут **sAMAccountName**.
6. Определите для сервера LDAP дерево отличительного имени, также известное как база поиска.
7. Нажмите кнопку **ОК**.
8. Если пользователь желает использовать идентификацию с помощью LDAP, он должен настроить свой профайл для использования удаленной идентификации LDAP вместо локальной идентификации.

Настройка НМС для использования Центров рассылки ключей (KDC) для удаленной идентификации Kerberos:

НМС можно настроить для использования Центров рассылки ключей для удаленной идентификации Kerberos

Когда пользователь входит в НМС, сначала идентификация осуществляется путем сравнения с локальным файлом пароля. Если локальный файл пароля не обнаружен, НМС может связаться с удаленным сервером Kerberos для идентификации. Для использования удаленной идентификации Kerberos необходимо настроить НМС.

Примечание: Прежде чем настраивать НМС для использования Центров рассылки ключей для удаленной идентификации Kerberos, необходимо убедиться, что существует рабочее сетевое соединение между НМС и Центрами рассылки ключей. Дополнительная информация о настройке сетевых соединений НМС приведена в разделе “Настройка типов сетей НМС” на стр. 94.

Для настройки НМС выполните следующие действия:

1. Включите службу Протокола сетевого времени (NTP) в НМС и задайте синхронизацию времени серверов НМС и KDC с одним и тем же сервером NTP. Для того чтобы включить службу NTP в НМС выполните следующее:
 - a. В области навигации выберите **Управление НМС**.
 - b. В области содержимого выберите **Изменить дату и время**.
 - c. Выберите вкладку **Конфигурация NTP**.
 - d. Выберите **Включить службу NTP в данной НМС**.
 - e. Нажмите кнопку **ОК**.
2. Настройте каждый профайл удаленного пользователя НМС для использования удаленной идентификации Kerberos, а не локальной идентификации.
3. Необязательно: можно импортировать файл служебных ключей в НМС. В файле служебных ключей содержится субъект хоста, идентифицирующий НМС для сервера KDC. Файлы служебных ключей также известны как *keytab*. Для того чтобы импортировать файл служебных ключей в НМС, выполните следующие действия:
 - a. В области навигации выберите **Управление НМС**.
 - b. В области содержимого выберите **Настроить KDC**. Откроется окно Настройки центра рассылки ключей.
 - c. Выберите **Действия > Импортировать служебный ключ**. Откроется окно Импорта служебного ключа.
 - d. Введите расположение файла служебного ключа.
 - e. Нажмите кнопку **ОК**.
4. Добавьте новый сервер KDC в НМС. Для этого выполните следующие действия:
 - a. В области навигации выберите **Управление НМС**.
 - b. В области содержимого выберите **Настроить KDC**. Откроется окно Настройки центра рассылки ключей.
 - c. Выберите **Действия > Добавить сервер KDC**. Откроется окно Импорта служебного ключа.
 - d. Введите область и имя хоста или IP-адрес сервера KDC.
 - e. Нажмите кнопку **ОК**.

Настройка НМС для связи с сервисным центром и службой поддержки:

Настройте НМС таким образом, чтобы она могла сообщать о встречающихся неполадках.

Настройка НМС для соединения со службой поддержки с помощью мастера настройки вызова сервисного центра:

Настройте НМС в качестве сервера вызова сервисного центра с помощью мастера.

В этой процедуре описывается, как настроить НМС в качестве сервисного сервера с помощью прямых (на основе LAN) и косвенных (на основе протокола SSL) соединений с Internet.

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Администратор сети проверил, что соединение разрешено. Дополнительные сведения содержатся в разделе “Подготовка к настройке НМС” на стр. 82.
- При настройке поддержки Internet через прокси-сервер также необходимы:
 - IP-адрес и порт прокси-сервера
 - Идентификационные данные сервера Proxu
- Применяется адаптер **eth1** (адаптер, применяемый для подключения к открытой сети). Дополнительные сведения содержатся в разделе “Выбор параметров сети в НМС” на стр. 73.
- Кабель Ethernet физически соединяет НМС с LAN.

Для настройки НМС в качестве сервера вызова сервисного центра с помощью мастера выполните следующие действия:

1. В области навигации выберите **Управление службами**.
2. В области содержимого выберите **Мастер настройки вызова сервисного центра**. Откроется мастер соединений и вызова сервисного центра Call-Home. Для настройки вызова сервисного центра Call-Home следуйте инструкциям мастера установки.

Настройка локальной консоли для отправки сервисному центру сообщений об ошибках:

Настройте НМС таким образом, чтобы она могла отправлять сервисному центру сообщения об ошибках с помощью соединений LAN.

Примечание: Виртуальная частная сеть Internet (VPN) и соединение по телефонной линии через модем доступны только в НМС версии 8.2.0 и более ранних версий.

Настройка НМС для связи со службой поддержки через Internet и SSL на основе LAN:

Описывается, как настроить НМС в качестве сервисного сервера с помощью прямых (на основе LAN) и косвенных (на основе протокола SSL) соединений с Internet.

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Администратор сети проверил, что соединение разрешено. Дополнительные сведения содержатся в разделе “Подготовка к настройке НМС” на стр. 82.
- Контактная информация клиента задана. Для проверки нужно воспользоваться НМС и нажать **Управление службами > Управление информацией о клиентах**.
- При настройке поддержки Internet через сервер Proxu также необходимы:
 - IP-адрес и порт прокси-сервера
 - Идентификационные данные сервера Proxu
- Необходим по крайней мере один настроенный открытый сетевой интерфейс. Дополнительная информация приведена в разделе “Частные и открытые сети в среде НМС” на стр. 75.
- Кабель Ethernet физически соединяет НМС с LAN.

Для настройки НМС в качестве сервисного сервера с помощью Интернета на основе LAN и SSL выполните следующие действия:

1. В области навигации выберите **Управление службами**.
2. В разделе Соединение выберите **Управление исходящими соединениями**. Откроется окно Консоли сервера вызова сервисного центра.
3. Выберите **Настроить**.
4. В окне Параметры исходящих соединений отметьте **Разрешить использование локальной системы в качестве сервисного сервера**.
5. Примите условия соглашения.

6. В окне Параметры исходящих соединений выберите страницу **Интернет**.
7. Поставьте отметку в окне **Разрешить существующие соединения с Internet для обслуживания**.
8. При использовании SSL прокси-сервера поставьте отметку в окне **Использовать SSL прокси-сервер**.
9. Если используется SSL прокси-сервер, введите его адрес и порт. Такую информацию можно получить у администратора системы.
10. Если отмечено окно **Использовать SSL прокси-сервер**, и прокси-сервер требует идентификации по идентификатору и паролю пользователя, поставьте отметку в окне **Идентификация на SSL прокси-сервере**. Введите идентификатор и пароль пользователя. Информацию об ИД и пароле пользователя получите у администратора системы.
11. Выберите **Протокол связи с Internet**, который необходимо использовать.
12. На странице **Интернет** выберите **Проверить**.
13. В окне Тестирование Internet нажмите кнопку **Запустить**.
14. Убедитесь, что проверка была успешно выполнена.
15. В окне Тестирование Internet нажмите кнопку **Завершить**.
16. В окне Параметры исходящих соединений нажмите **ОК**.

Связь со службой поддержки с помощью телефона и модемов:

Описывается, как настроить НМС в качестве сервисного сервера с помощью доступа к службе поддержки IBM через модем.

Примечание: Виртуальная частная сеть Internet (VPN) и соединение по телефонной линии через модем доступны только в НМС версии 8.2.0 и более ранних версий.

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Имеется выделенная аналоговая телефонная линия.
- Имеется информация, необходимая для настройки модема. Дополнительные сведения содержатся в разделе “Подготовка к настройке НМС” на стр. 82.
- Контактная информация клиента задана. Для проверки нужно воспользоваться НМС и нажать **Управление службами > Управление информацией о клиентах**.
- Убедитесь в наличии следующей информации:
 - Тип аналоговой линии - тональная или импульсная. Большинство линий являются тональными, однако пока еще сохраняются некоторые более старые линии ротационного или импульсного типа.
 - Если при поднятии трубки в линию выдается непрерывный гудок. Большинство телефонов работают с гудком, однако некоторые - без гудка.
 - Если при наборе необходима строка префиксов. Строка префиксов - это номер или последовательность номеров для выхода во внешнюю линию.

Для настройки НМС в качестве сервисного сервера с помощью доступа к службе поддержки IBM через модем выполните следующие действия:

1. В области навигации выберите **Управление службами**.
2. В разделе Соединение выберите **Управление исходящими соединениями**.
3. Выберите **Настроить**.
4. В окне Параметры исходящих соединений включите переключатель **Разрешить использование локальной системы в качестве сервисного сервера**.
5. Примите условия соглашения.
6. В окне Параметры исходящих соединений выберите вкладку **Локальный модем**.
7. На странице Локальный модем включите переключатель **Разрешить набор номера через локальный модем для обслуживания**.
8. На странице Локальный модем включите переключатель **Конфигурация модема**.

9. В окне Настройка параметров модема выберите **Тип набора - тональный или импульсный**. Если при поднятии трубки в линию выдается непрерывный гудок, включите переключатель **Дождаться гудка**. Введите необходимую строку префиксов набора для выхода во внешнюю линию.
10. Нажмите кнопку **ОК**.
11. На странице Локальный модем нажмите кнопку **Добавить**.
12. Выберите номер из списка.
13. Для местных номеров удалите код области из поля **Номер телефона**.
14. На панели Добавление телефонного номера нажмите кнопку **Добавить**.
15. На панели Настройка параметров модема выберите **Проверка**.
16. На панели Проверка номера телефона нажмите кнопку **Запустить**.
17. Убедитесь, что проверка была успешно выполнена.
18. В окне Проверка номера телефона нажмите кнопку **Завершить**.
19. Можно настроить до пяти телефонных номеров. Рекомендуется настроить, по крайней мере, два телефонных номера (основной и резервный). Попытки соединения с номерами будут выполняться в той же очередности, что и настройка. Для того чтобы добавить номера в список вызываемых номеров, повторите шаги данной процедуры.
20. В окне Параметры исходящих соединений нажмите **ОК**.

Подключение к службе поддержки с помощью VPN на основе LAN:

Настройка сервисного сервера с помощью VPN

Примечание: Виртуальная частная сеть Internet (VPN) и соединение по телефонной линии через модем доступны только в НМС версии 8.2.0 и более ранних версий.

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Администратор сети проверил, что соединение разрешено. Дополнительные сведения содержатся в разделе “Подготовка к настройке НМС” на стр. 82.
- Применяется адаптер **eth1** (адаптер, применяемый для подключения к открытой сети). Дополнительные сведения содержатся в разделе “Выбор параметров сети в НМС” на стр. 73.
- Кабель Ethernet физически соединяет НМС с LAN.
- Контактная информация клиента задана. Для проверки нажмите **Управление службам > Управление информацией о клиентах** на интерфейсе НМС.

Для того чтобы настроить сервисный сервер с помощью VPN, выполните следующие действия:

1. В области навигации выберите **Управление службами**.
2. В разделе Соединение выберите **Управление исходящими соединениями**.
3. Выберите **Настроить**
4. В окне Параметры исходящих соединений включите переключатель **Разрешить использование локальной системы в качестве сервисного сервера**.
5. Примите условия соглашения.
6. В окне Параметры исходящих соединений выберите вкладку **Internet**.
7. На странице Интернет через VPN выберите **Разрешить обслуживание по VPN через существующее соединение с Интернетом**.
8. На странице Интернет через VPN включите переключатель **Проверить**.
9. В окне Тестирование Internet VPN нажмите кнопку **Запустить**.
10. Убедитесь, что проверка была успешно выполнена.
11. В окне Тестирование Internet VPN нажмите кнопку **Завершить**.
12. В окне Параметры исходящих соединений нажмите **ОК**.

Выбор из существующих серверов вызова сервисного центра для соединения со службой поддержки для данной НМС:

Выберите из существующих серверов вызова сервисного центра НМС, которые были распознаны, или "обнаружены," данной НМС для отправки отчета об ошибках.

Обнаруженные НМС - это НМС, которые подключены как серверы вызова сервисного центра и либо находятся в той же подсети, либо управляют той же системой, что и данная НМС.

Для того чтобы выбрать обнаруженную НМС для вызова сервисного центра при возникновении ошибок данной НМС, выполните следующее:

1. В области навигации выберите **Управление службами**.
2. В области содержимого выберите **Управление исходящими соединениями**. Откроется окно Консоли сервера вызова сервисного центра.
3. Включите переключатель **Использовать обнаруженные консоли сервера вызова сервисного центра**. В НМС будет показан IP-адрес или имя хоста НМС, настроенных для вызова сервисного центра.
4. Нажмите кнопку **ОК**.

Также можно вручную добавить существующие серверы вызова сервисного центра НМС, которые находятся в другой подсети. Выберите IP-адрес или имя хоста НМС, настроенной для вызова сервисного центра и нажмите **Добавить**. Затем нажмите **ОК**.

Проверка работоспособности соединения с сервисным центром и службой поддержки:

Отправка тестовой неполадки для проверки работоспособности соединения с сервисным центром и службой поддержки

Для проверки работоспособности конфигурации вызова сервисного центра выполните следующие действия:

1. В области навигации выберите **Управление службами**.
2. В рабочей области выберите **Создать событие**.
3. Выберите **Проверка автоматического создания отчета о неполадках** и введите комментарий.
4. Выберите **Запросить обслуживание**. Дождитесь отправки запроса.
5. В окне Службное управление выберите **Управление событиями**.
6. Выберите **Все сообщенные неполадки**.
7. Проверьте, выбрано ли событие РМН и присвоен ли номер неполадке, о которой Вы сообщили.
8. Выберите событие и нажмите кнопку **Заккрыть**.
9. В окне Заккрыть введите свое имя и краткое замечание.

Предоставление пользователям права доступа для просмотра собранных системных данных:

Для просмотра данных о системе необходимо предоставить пользователям права доступа.

Прежде чем предоставить пользователям права доступа для просмотра собранных системных данных, необходимо получить ИД IBM. Более подробная информация о получении ИД IBM приведена в разделе "Форма настройки НМС перед установкой" на стр. 84.

Для предоставления пользователям прав доступа для просмотра собранных системных данных выполните следующие действия:

1. В области навигации выберите **Управление службами**.
2. В области содержимого выберите **Предоставить пользователю права доступа**.
3. Введите свой ИД IBM.
4. Нажмите кнопку **ОК**.

Передача служебной информации:

Передача служебной информации для использования ее в целях выявления неполадок.

IBM предоставляет персонализированные веб-функции, в которых используется информация, собранная приложением IBM Electronic Service Agent. Для того чтобы иметь возможность пользоваться этими функциями, необходимо вначале зарегистрироваться на веб-сайте регистрации в IBM по адресу <http://www.ibm.com/account/profile>. Для предоставления пользователям права пользоваться информацией Electronic Service Agent с целью персонализации веб-функций обратитесь к разделу “Предоставление пользователям права доступа для просмотра собранных системных данных” на стр. 107. Более подробная информация о преимуществах регистрации ИД IBM для систем приведена в разделе <http://www.ibm.com/support/electronic>.

Примечание: Как только НМС установлена и настроена, необходимо предоставить информацию для официального сервисного центра.

Для передачи служебной информации выполните следующие действия:

1. В области навигации выберите **Управление службами**.
2. В области содержимого выберите **Передать сервисные данные**.
3. Щелкните на одной из следующих вкладок:
 - **Передача.** На этой странице можно настроить расписание отправки данных для службы технической поддержки (день и время) и способ отправки.
 - **FTP.** На этой странице можно настроить данные для работы с сервером FTP, с брандмауэром или без него, для отправки служебной информации. Эта служебная информация включает расширенное описание ошибок и данные, связанные с неполадками в Консоли аппаратного обеспечения (НМС) или управляемой системе.
 - **Передача служебной информации в IBM.** На этой странице можно настроить отставку информации, хранящейся на жестком диске НМС и используемой для анализа неполадок. Это могут быть данные трассировки и протокола или дампы, которые могут быть переданы в систему IBM Support или записаны на дискету, флэш-память USB или на DVD. Перед отставкой информации в IBM Support необходимо включить телефонный сервер и функции удаленного обслуживания.
4. Выполните задачи в окне Передача сервисных данных и нажмите **ОК**.

Настройка Администратора событий для вызова сервисного центра:

Рассмотрена настройка задачи Администратор событий для вызова сервисного центра. Эта задача позволяет отслеживать и утверждать данные, передаваемые из НМС в IBM.

Режим Администратор событий для вызова сервисного центра включается и выключается с помощью интерфейса командной строки НМС. Включение задачи Администратор событий для вызова сервисного центра предусматривает выключение автоматического вызова сервисного центра. Для того чтобы запретить вызов сервисного центра без подтверждения, необходимо включить режим Администратор событий для вызова сервисного центра на всех НМС в среде.

Для включения или выключения задачи Администратор событий для вызова сервисного центра выполните следующую команду:

```
chhmc -c emch
```

```
-s {enable | disable}
```

```
[--callhome {enable | disable}]
```

```
[--help]
```

Примечание: Включение задачи Администратор событий для вызова сервисного центра блокирует события вызова сервисного центра до их утверждения для задачи вызова сервисного центра. При выключении задачи Администратор событий для вызова сервисного центра не происходит автоматического включения функции вызова сервисного центра. Такая конфигурация позволяет избежать непреднамеренной передачи данных в IBM. Для задания требуемой конфигурации предусмотрены следующие опции командной строки:

- Включить задачу Администратор событий для вызова сервисного центра: **chhmc -c emch -s enable**
- Выключить задачу Администратор событий для вызова сервисного центра и повторно включить автоматический вызов сервисного центра: **chhmc -c emch -s disable --callhome enable**
- Выключить задачу Администратор событий для вызова сервисного центра без повторного включения автоматического вызова сервисного центра: **chhmc -c emch -s disable --callhome disable**

Убедитесь, что НМС может обмениваться данными с другими НМС, развернутыми в этой среде. В ходе регистрации НМС администратор событий для вызова сервисного центра выполняет проверку связи.

НМС можно зарегистрировать с помощью администратора событий для вызова сервисного центра. После регистрации НМС администратор событий запрашивает в зарегистрированной НМС события, ожидающие вызова сервисного центра IBM. администратор событий отображает данные, отправляемые в IBM, и утверждает события. После утверждения администратор событий разрешает зарегистрированной НМС продолжить операцию вызова сервисного центра.

Задачу Администратор событий для вызова сервисного центра можно запустить из любой НМС или из нескольких НМС. Для регистрации консоли управления в задаче Администратор событий для вызова сервисного центра выполните следующие действия:

1. В области навигации выберите **Управление службами**.
2. В области содержимого выберите **Администратор событий для вызова сервисного центра**.
3. В окне **Администратор событий для вызова сервисного центра** выберите **Управление консолями**.
4. В окне **Управление зарегистрированными консолями** выберите **Добавить консоль** для ввода информации для регистрации консоли управления в Администраторе событий для вызова сервисного центра.
5. Нажмите кнопку **ОК**, чтобы сохранить изменения в списке зарегистрированных консолей управления.

Примечание: Администратор событий для вызова сервисного центра может работать, когда режим администратора событий выключен. Вы сможете зарегистрировать НМС и просмотреть события, однако администратор событий не будет управлять отправкой событий в сервисный центр.

Задание паролей для управляемой системы:

Вам необходимо задать пароли как для своего сервера, так и для расширенного интерфейса управления системой (ASM). Использование интерфейса НМС для задания этих паролей описывается далее.

При получении сообщения Ожидание идентификации НМС предлагает пользователю установить пароли для управляемой системы.

Если сообщение Ожидание идентификации не получено, выполните следующие шаги, чтобы установить пароли для управляемой системы.

Обновление пароля сервера:

Для обновления пароля своего сервера выполните следующее:

1. В области навигации выберите управляемую систему.
2. В области задач выберите **Операции**.
3. Нажмите кнопку **Изменить пароль**. Откроется окно Обновление пароля.
4. Введите требуемую информацию и нажмите **ОК**.

Обновление общего пароля расширенного управления системой (ASM):

Примечание: Пароль по умолчанию для ИД обычного пользователя - general, для ИД администратора - admin.

Для обновления общего пароля ASM выполните следующее:

1. Выберите управляемую систему в области навигации НМС.
2. В области задач выберите **Операции**.
3. Выберите **Расширенное управление системой (ASM)**. Откроется окно Запуск интерфейса ASM.
4. Выберите IP-адрес служебного процессора и нажмите **ОК**. Откроется интерфейс ASM.
5. На начальной странице ASM1 укажите свой ИД пользователя и пароль и нажмите **Войти в систему**.
6. В области навигации разверните **Профайл входа в систему**.
7. Выберите **Изменить пароль**.
8. Укажите необходимую информацию и нажмите **Продолжить**.

Восстановление пароля администратора расширенного управления системой (ASM):

Для сброса пароля администратора обратитесь в официальный сервисный центр.

Проверка соединения между НМС и управляемой системой:

Этот параметр позволяет проверить правильность соединения с сетью.

Проверку соединения с сетью могут выполнять пользователи со следующими ролями:

- Главный администратор
- Сотрудник сервисного представительства

Для проверки соединения между НМС и управляемой системой выполните следующее:

1. В области навигации выберите **Управление НМС**.
2. Выберите **Проверка соединения с сетью**.
3. Во вкладке Отправить пробный пакет введите имя хоста или IP-адрес любой системы, с которой нужно установить соединение. Для проверки открытой сети введите имя шлюза. Нажмите кнопку **Проверить связь**.

Проверка связи недоступна, если еще не созданы логические разделы. Для этого можно воспользоваться НМС. Дополнительная информация приведена в разделе Создание логических разделов.

Для того чтобы разобраться, как можно использовать НМС в сети, обратитесь к разделу “Сетевые соединения НМС” на стр. 73.

Дополнительная информация о настройке НМС для соединения с сетью приведена в разделе “Настройка НМС с помощью меню НМС” на стр. 92.

Действия после настройки

После установки и настройки НМС можно создать резервную копию данных НМС.

Резервное копирование наиболее важных данных НМС

Резервную копию важной информации о консоли можно сохранить на флэш-памяти USB, DVD-диске, в удаленной системе или на сервере FTP.

С помощью НМС можно выполнять резервное копирование всех важных данных, например:

- Файлы пользовательских параметров
- Информация пользователей
- Файлы конфигурации платформы НМС

- Файлы протокола НМС
- Обновления НМС через Установку исправлений

Функция резервного копирования сохраняет данные НМС, содержащиеся на жестком диске НМС на следующие носители:

- DVD диск
- флэш-память USB
- Удаленная система, вмонтированная в файловую систему НМС (например, NFS)
- Удаленный сайт с помощью FTP

Резервная копия НМС создается после внесения изменений в НМС или в информацию, связанную с логическими разделами.

Примечание: Прежде чем сохранять данные на съемном носителе, его следует отформатировать. Для форматирования носителя выберите **Управление НМС > Форматировать носитель** и выполните инструкции.

Резервное копирование НМС могут выполнять пользователи со следующими ролями:

- Главный администратор
- Оператор
- Сотрудник сервисного представительства

Для резервного копирования важнейших данных НМС выполните следующие действия:

1. В области навигации выберите **Управление НМС**.
2. Выберите **Создать резервную копию данных НМС**.
3. Выберите параметры архивации. Резервную копию можно сохранить на носителе в локальной системе, в смонтированной удаленной системе, или можно переслать данные резервной копии на удаленный сайт.
4. Для выполнения этой задачи следуйте инструкциям на экране.

Создание полной резервной копии жесткого диска НМС в удаленной системе

С помощью консоли НМС можно выполнять резервное копирование всего жесткого диска НМС в удаленную систему.

Для этого в удаленной системе должна быть настроена сетевая файловая система (NFS) или защищенная оболочка (ssh), и эта сеть должна быть доступной из НМС. Для выполнения указанной задачи необходимо завершить выполнение и перегрузить НМС. Эти задачи следует выполнять только с помощью НМС.

Резервное копирование жесткого диска НМС в удаленную систему могут выполнять пользователи со следующими ролями:

- Главный администратор
- Оператор
- Сотрудник сервисного представительства

Для резервного копирования жесткого диска НМС в удаленную систему выполните следующие действия:

1. Запишите номер интерфейса (eth0, eth1 и т. д.), MAC-адрес и IP-адрес каждого сетевого адаптера НМС. Для этого выберите **Управление НМС > Изменить сетевые параметры > Адаптеры LAN**.
2. Завершите работу и отключите питание НМС.
3. Подключите питание консоли НМС, вставив НМС съемный диск восстановления в дисковод DVD. При запуске интерфейса НМС с настроенного сервера загрузки из сети проследите за тем, чтобы в качестве сетевого интерфейса было выбрано одно из устройств, предусмотренных в последовательности запуска. Для просмотра списка загрузочных устройств нажмите F12 после включения питания НМС и выберите требуемый сетевой интерфейс для загрузки.
4. Выберите опцию резервного копирования и нажмите **Далее**.

5. Выберите сетевой интерфейс для обмена данными с удаленным сервером. Если для запуска НМС устанавливается связь с сервером загрузки из сети, и на тот же сервер будет выполняться резервное копирование данных, используйте стандартные параметры. Затем нажмите **Далее** и перейдите к шагу 7. Если стандартные параметры не выбраны, перейдите к следующему шагу.

Примечание: Номер интерфейса (eth0, eth1) может не совпадать с номером, записанным при выполнении шага 1. Для идентификации необходимого интерфейса можно использовать указанный MAC-адрес. Дополнительные сведения содержатся в разделе “Идентификация порта Ethernet, определяемого как eth0” на стр. 97.

6. В этом случае необходимо выбрать сетевой протокол для выбранного интерфейса. Для этого можно получить IP-адрес с сервера DHCP своей сети или назначить статический IP-адрес выбранному сетевому интерфейсу. Выберите нужное и нажмите кнопку **Далее**.
7. Если стандартные параметры не были выбраны, введите IP-адрес или имя хоста удаленного сервера. Резервный файл будет создан с помощью утилиты сжатия **gzip** и команды **tar**. В поле **Файл на удаленном хосте** укажите файл с расширением .tgz. Если были выбраны стандартные сетевые параметры, в сетевой загрузочной конфигурации нужно использовать настройку каталогов. Такая информация отображается в поле **Файл на удаленном хосте**. После ввода всей обязательной информации нажмите кнопку **Далее**.
8. Выберите требуемый способ переноса данных из НМС на удаленный сервер. Если данные будут зашифрованы, на удаленном хосте должен быть запущен сервер Secure Shell (SSH). При переносе данных без шифрования на удаленном хосте должен быть запущен сетевой файловый сервер (NFS), и должен быть экспортирован каталог, куда будет выполняться резервное копирование данных, для предоставления доступа для записи. Выберите нужное и нажмите кнопку **Далее**.
9. При выборе переноса данных с шифрованием необходимо ввести идентификатор и пароль пользователя удаленного сервера.
10. Проверьте правильность введенной информации и нажмите кнопку **Закончить**. По завершении резервного копирования будет отображен интерфейс НМС.

Если при включении питания НМС была нажата кнопка F1, и последовательность загрузки была изменена, необходимо перегрузить НМС и вновь изменить параметры. При изменении последовательности загрузки проследите за тем, чтобы жесткий диск был указан перед сетевым интерфейсом.

Обновление, модернизация и миграция машинного кода НМС

Для НМС периодически выходят обновления, позволяющие добавить новые возможности и улучшить существующие. В этом разделе приведено различий операций обновления, модернизации и миграции машинного кода НМС. Кроме того, рассмотрены процедуры обновления, модернизации и миграции машинного кода НМС.

После завершения каждой задачи выполняется перезагрузка НМС без остановки разделов.

Обновление кода НМС

Применение пакета обслуживания для текущего уровня НМС.

Не требуется выполнять задачу **Сохранить данные модернизации**.

Модернизация кода НМС

Замена программного обеспечения НМС новым выпуском или уровнем исправления.

Требуется загрузка с носителя восстановления.

Миграция кода НМС

Перемещение данных НМС из одной версии НМС в другую.

Миграция является частным случаем модернизации.

Определение версии и выпуска машинного кода НМС

Информация о том, как определить версию и выпуск машинного кода НМС.

Набор доступных функций, включая оперативное обслуживание встроенного программного обеспечения сервера, а также расширения для модернизации до нового выпуска, определяется уровнем машинного кода НМС.

Для просмотра версии и выпуска машинного кода НМС выполните следующее:

1. В области навигации выберите **Обновления**.
2. В рабочей области просмотрите и запишите информацию, приведенную под заголовком Уровень кода НМС, включая: версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.

Получение и применение обновлений машинного кода для НМС через Internet-соединение

Знакомит с получением обновлений машинного кода для НМС при наличии соединения с Internet.

Для получения обновлений машинного кода для НМС выполните шаги 1 - 5.

Шаг 1. Убедитесь в наличии соединения с Internet:

Для того чтобы загрузить на НМС или сервер обновления с системы или веб-сайта службы поддержки, необходимо иметь одну из возможностей:

- SSL-соединение с или без SSL proxy
- Internet VPN

Для того чтобы убедиться в наличии соединения с Internet, выполните следующее:

1. В области навигации выберите **Управление службами**.
2. Выберите **Управление исходящими соединениями**.
3. Откройте вкладку, соответствующую типу исходящего соединения, выбранному для НМС (Internet VPN или SSL-соединение).

Примечание: Если соединение со службой поддержки отсутствует, настройте его перед продолжением выполнения этого сценария. Инструкции по настройке соединения со службой поддержки приведены в разделе Настройка сервера для связи с сервисным центром IBM.

4. Нажмите кнопку **Проверить**.
5. Убедитесь, что проверка была успешно выполнена. Если проверка не была пройдена, устраните неполадку соединения перед продолжением выполнения этой процедуры. Кроме того, можно получить обновление на DVD.
6. Перейдите к “Шаг 2. Просмотр текущего уровня машинного кода НМС”.

Шаг 2. Просмотр текущего уровня машинного кода НМС:

Для просмотра текущего уровня машинного кода НМС выполните следующее:

1. В области навигации выберите **Обновления**.
2. В рабочей области просмотрите и запишите информацию, приведенную под заголовком Уровень кода НМС, включая версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
3. Перейдите к “Шаг 3. Просмотр доступных уровней машинного кода НМС”.

Шаг 3. Просмотр доступных уровней машинного кода НМС:

Для просмотра доступных уровней машинного кода НМС выполните следующее:

1. С компьютера или сервера, подключенного к Internet, перейдите на веб-сайт <http://www.ibm.com/eserver/support/fixes>.
2. Выберите нужное семейство серверов в списке Product.
3. Выберите **Hardware Management Console** в списке Product or fix type.
4. Нажмите кнопку **Continue**. Будет показан консоли аппаратного обеспечения.
5. Прокрутите список до нужного уровня версии НМС и для просмотра доступных уровней.

Примечание: При необходимости обратитесь в службу поддержки.

6. Перейдите к “Шаг 4. Применение обновления машинного кода НМС”.

Шаг 4. Применение обновления машинного кода НМС:

Для применения обновления машинного кода НМС выполните следующее:

1. Перед установкой обновлений для машинного кода НМС следует создать резервную копию важной информации о консоли на НМС. Соответствующие инструкции приведены в разделе “Резервное копирование наиболее важных данных НМС” на стр. 110. Затем перейдите к следующему шагу.
2. В области навигации выберите **Обновления**.
3. Выберите **Обновление НМС**. Откроется окно Установка исправления.
4. Следуйте инструкциям по установке обновления.
5. Для того чтобы обновления вступили в силу, завершите работу и перезапустите НМС.
6. Выберите **Войти и запустить веб-приложение Консоль аппаратного обеспечения**.
7. Войдите в интерфейс НМС.

Шаг 5. Проверка правильности установки обновления машинного кода НМС:

Для проверки правильности установки обновления машинного кода НМС выполните следующее:

1. В области навигации выберите **Обновления**.
2. В рабочей области под заголовком Уровень кода НМС отображается версия НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
3. Убедитесь, что версия и выпуск совпадают с версией установленного обновления.
4. Если показана другая версия кода, выполните следующие действия:
 - a. Выберите сетевое соединение в НМС.
 - b. Повторно обновите встроенное программное обеспечение, используя другое хранилище.
 - c. Если ошибка возникнет снова, обратитесь на следующий уровень поддержки.

Получение и применение обновлений машинного кода для НМС на DVD или через сервер FTP

Знакомит с получением обновлений машинного кода на DVD или через сервер FTP.

Для получения обновлений машинного кода НМС выполните шаги 1 - 5.

Шаг 1. Просмотр текущего уровня машинного кода НМС:

Для просмотра текущего уровня машинного кода НМС выполните следующее:

1. В области навигации выберите **Обновления**.
2. В рабочей области просмотрите и запишите информацию, приведенную под заголовком Уровень кода НМС, включая версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
3. Перейдите к “Шаг 2. Просмотр доступных уровней машинного кода НМС”.

Шаг 2. Просмотр доступных уровней машинного кода НМС:

Для просмотра доступных уровней машинного кода НМС выполните следующее:

1. На компьютере или сервере с подключением к Интернету откройте веб-страницу консоли программного обеспечения <http://www-933.ibm.com/support/fixcentral/>.
2. Прокрутите список до нужного уровня версии НМС и для просмотра доступных уровней.

Примечание: При необходимости обратитесь в службу поддержки IBM .

3. Перейдите к “Шаг 3. Получение обновления машинного кода НМС”.

Шаг 3. Получение обновления машинного кода НМС:

Для получения обновления машинного кода НМС выполните следующее:

Обновление машинного кода НМС можно заказать на веб-сайте Fix Central или в службе поддержки. Кроме того, его можно загрузить на сервер FTP.

Заказ обновления машинного кода НМС через веб-сайт Fix Central

1. На компьютере или сервере с подключением к Интернету откройте веб-страницу консоли программного обеспечения <http://www-933.ibm.com/support/fixcentral/>.
2. В продуктах, поддерживаемых НМС, выберите последний уровень НМС.
3. Прокрутите страницу вниз до области File name(s) / Package area и найдите обновление, которое требуется заказать.
4. В столбце Заказ выберите **Перейти**.
5. Щелкните на ссылке **Continue** для получения идентификатора IBM.
6. Для того чтобы отправить заказ, следуйте инструкциям, появляющимся на экране.

Загрузка обновления машинного кода НМС на съемные носители

1. На компьютере или сервере с подключением к Интернету откройте веб-страницу консоли программного обеспечения <http://www-933.ibm.com/support/fixcentral/>.
2. В продуктах, поддерживаемых НМС, выберите последний уровень НМС.
3. Прокрутите страницу вниз до области Имя (имена) файла / Пакетная область и найдите обновление, которое требуется загрузить.
4. Выберите обновление, которое требуется загрузить.
5. Примите условия лицензионного соглашения и сохраните обновление на съемном носителе.

По окончании перейдите к “Шаг 4. Применение обновления машинного кода НМС”.

Шаг 4. Применение обновления машинного кода НМС:

Для применения обновления машинного кода НМС выполните следующее:

1. Перед установкой обновлений для машинного кода НМС создайте резервную копию данных НМС. Дополнительная информация приведена в разделе “Резервное копирование наиболее важных данных НМС” на стр. 110
2. Если вы получили или создали обновление на DVD-RAM, вставьте его в дисковод DVD на консоли НМС. Если вы получили или создали обновление на накопителе USB, то установите его.
3. В области навигации выберите **Обновления**.
4. Выберите **Обновление НМС**. Откроется окно Установка исправления НМС.
5. Следуйте инструкциям по установке обновления.
6. Для того чтобы обновления вступили в силу, завершите работу, перезапустите и вновь войдите на НМС.
7. Перейдите к “Шаг 5. Проверка правильности установки обновления машинного кода НМС”.

Шаг 5. Проверка правильности установки обновления машинного кода НМС:

Для проверки правильности установки обновления машинного кода НМС выполните следующее:

1. В области навигации выберите **Обновления**. В рабочей области под заголовком Уровень кода НМС отображается версия НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
2. Убедитесь, что версия и выпуск совпадают с версией установленного обновления.
3. Если показана другая версия кода, выполните следующие действия:
 - a. Повторно обновите машинный код. Если для выполнения этой процедуры был создан диск DVD, замените его.
 - b. Если ошибка возникнет снова, обратитесь на следующий уровень поддержки.

Модернизация программного обеспечения НМС

Знакомит с модернизацией программного обеспечения на НМС до следующего выпуска с сохранением данных конфигурации НМС.

Для обновления машинного кода в НМС выполните шаги 1 - 9.

Шаг 1. Получение модернизации:

Обновление машинного кода НМС можно заказать на веб-сайте Fix Central.

Для того чтобы получить обновление с веб-сайта Fix Central, выполните следующие действия:

1. На компьютере или сервере с подключением к Интернету откройте веб-страницу консоли программного обеспечения <http://www-933.ibm.com/support/fixcentral/>.
2. Нажмите кнопку **Continue**. Будет показан консоль аппаратного обеспечения.
3. Найдите версию НМС, которую вы хотите обновить.
4. Найдите раздел загрузки и заказа.

Примечание: Если у вас нет доступа к Internet, закажите обновление на DVD в службе сопровождения и поддержки IBM.

5. Для того чтобы отправить заказ, следуйте инструкциям, появляющимся на экране.
6. Получив обновление, перейдите к шагу “Шаг 2. Просмотр текущего уровня машинного кода НМС”.

Шаг 2. Просмотр текущего уровня машинного кода НМС:

Для определения текущего уровня машинного кода НМС выполните следующие действия:

1. В области навигации выберите **Обновления**.
2. В рабочей области просмотрите и запишите информацию, приведенную под заголовком Уровень кода НМС, включая версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
3. Перейдите к “Шаг 3. Создание резервной копии данных профайла управляемой системы”.

Шаг 3. Создание резервной копии данных профайла управляемой системы:

Для того чтобы скопировать данные профайлов управляемой системы, выполните следующее:

1. области навигации выберите **Управление системами**.
2. Выберите **Серверы**.
3. Выберите сервер, который должен иметь состояние *Рабочий* или *Резервный*.
4. В разделе Задачи выберите **Настройка > Управление данными о разделах > Резервное копирование**.
5. Введите и запишите имя файла с резервной копией.
6. Нажмите кнопку **ОК**.
7. Повторите шаги для каждой управляемой системы.
8. Перейдите к “Шаг 4. Резервное копирование данных НМС”.

Шаг 4. Резервное копирование данных НМС:

Перед установкой новой версии программного обеспечения НМС следует выполнить резервное копирование данных НМС; это позволит восстановить предыдущие версии программного обеспечения в случае ошибок в процессе модернизации ПО. После успешной установки новой версии программного обеспечения НМС сохраненную информацию применять не следует.

Примечание: Для сохранения данных консоли на съемном носителе необходимо предварительно подготовить соответствующий носитель.

Для резервного копирования данных НМС выполните следующее:

1. Если резервную копию предполагается создать на съемном носителе, отформатируйте носитель:
 - a. Вставьте носитель в накопитель.
 - b. В области навигации выберите **Управление службами**
 - c. Выберите **Отформатировать носитель**.
 - d. Выберите тип носителя.

- e. Выберите тип форматирования.
 - f. Нажмите кнопку **ОК**.
2. В области навигации выберите **Управление НМС**.
 3. Выберите **Создать резервную копию данных НМС**. Откроется окно резервного копирования данных НМС.
 4. Выберите параметры архивации. Резервную копию можно сохранить на носителе в локальной системе, в удаленной системе, смонтированной в файловой системе НМС, (например, NFS) или отправить на удаленный сервер FTP.
 - Для создания резервной копии на носителе выберите **Сохранить на носителе в локальной системе** и следуйте показанным инструкциям.
 - Для создания резервной копии в смонтированной удаленной системе выберите **Сохранить в смонтированной удаленной системе** и следуйте показанным инструкциям.
 - Для создания резервной копии на сервере FTP выберите **Отправить резервную копию важнейших данных на удаленный сервер** и следуйте показанным инструкциям.
 5. Перейдите к “Шаг 5. Запись информации о текущей конфигурации НМС”.

Шаг 5. Запись информации о текущей конфигурации НМС:

Перед обновлением версии программного обеспечения НМС в качестве меры предосторожности следует записать информацию о конфигурации НМС.

Для регистрации существующей конфигурации НМС выполните следующее:

1. Для просмотра запланированных операций для управляемой системы или ее логических разделов откройте **Управление системами**. Если вы хотите записать запланированные операции для самой НМС выберите **Управление НМС** и перейдите к шагу 3.
2. Выберите управляемую систему и разделы, для которых необходимо записать сведения о конфигурации НМС.
3. В списке задач выберите **Запланировать операции**. Будут показаны все запланированные операции для выбранного целевого объекта.
4. Выберите **Сортировать > По объекту**.
5. Последовательно выберите каждый объект и запишите следующие сведения:
 - Имя объекта
 - Запланированная дата
 - Время выполнения (в 24-часовом формате)
 - Повторяющийся (если указано значение Да, выполните следующие действия):
 - a. Выберите **Вид > Сведения о расписании**.
 - b. Запишите информацию об интервале.
 - c. Закройте окно запланированных операций.
 - d. Повторите эти действия для каждой запланированной операции.
6. Закройте окно Настроить запланированные операции.
7. Перейдите к “Шаг 6. Запись состояния удаленной команды”.

Шаг 6. Запись состояния удаленной команды:

Для регистрации состояния удаленной команды выполните следующее:

1. В области навигации выберите **Управление НМС**.
2. В списке задач выберите **Удаленное выполнение команд**.
3. Запишите состояния переключателя **Разрешить удаленное выполнение команд по протоколу ssh**.
4. Нажмите **Отмена**.
5. Перейдите к “Шаг 7. Сохранение данных модернизации” на стр. 118.

Шаг 7. Сохранение данных модернизации:

Текущую конфигурацию НМС можно сохранить в выделенном разделе диска НМС или на локальном носителе. Данные об обновлении необходимо сохранять непосредственно перед переходом к следующему выпуску программного обеспечения НМС. Такой подход позволяет восстановить параметры конфигурации НМС после обновления.

Примечание: Сохранить можно только одну резервную копию. Каждый раз при сохранении данных обновления предыдущие данные удаляются.

Для того чтобы сохранить данные обновления, выполните следующее:

1. В области навигации выберите **Управление НМС**.
2. В области содержимого в разделе Операции выберите **Сохранить данные модернизации**. Откроется мастер сохранения данных обновления.
3. Выберите носитель для сохранения данных обновления. Если выбран съемный носитель, то установите его. Нажмите кнопку **Далее**.
4. Нажмите кнопку **Закончить**.
5. Дождитесь завершения задачи. Если задача Сохранить данные обновления не будет выполнена, обратитесь на следующий уровень поддержки.

Примечание: Если задача сохранения данных обновления не будет выполнена, процесс обновления следует приостановить.

6. Нажмите кнопку **ОК**.
7. Перейдите к “Шаг 8. Модернизация программного обеспечения НМС”.

Шаг 8. Модернизация программного обеспечения НМС:

Для модернизации программного обеспечения НМС перезапустите систему, установив в дисковод DVD съемный носитель.

1. Вставьте установочный диск продукта НМС в дисковод DVD.
2. В меню навигации выберите **Управление НМС**.
3. В области содержимого выберите **Завершить работу или перезапустить НМС**.
4. Проследите за тем, чтобы был выбран пункт **Перезапустить НМС**.
5. Нажмите кнопку **ОК**. В ходе перезапуска НМС в окне прокручивается системная информация.
6. Выберите **Обновить** и нажмите кнопку **Далее**.
7. Можно выполнить следующие действия:
 - Если данные обновления были сохранены при выполнении предыдущей задачи, перейдите к следующему шагу.
 - Если данные обновления не были сохранены, перед продолжением их следует сохранить.
8. Выберите **Обновить с носителя** и нажмите кнопку **Далее**.
9. Подтвердите параметры и нажмите кнопку **Готово**.
10. Следуйте инструкциям.

Примечание:

- Если экран станет пустым, для просмотра информации нажмите пробел.
 - Установка первого DVD может занять приблизительно 20 минут.
11. В приглашении входа в систему введите ИД пользователя и пароль. Установка кода НМС завершена.
 12. Перейдите к “Шаг 9. Проверка правильности установки модернизации машинного кода НМС”.

Шаг 9. Проверка правильности установки модернизации машинного кода НМС:

Для проверки правильности установки обновления НМС выполните следующее:

1. В области навигации выберите **Обновления**. В рабочей области под заголовком Уровень кода НМС отображается версия НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
2. Убедитесь, что версия и выпуск совпадают с версией установленного обновления.
3. Если показана другая версия кода, повторите операцию с другим диском DVD. Если ошибка возникнет снова, обратитесь на следующий уровень поддержки.

Обновление НМС из удаленного расположения с помощью образов сетевого обновления

Инструкции по обновлению программного обеспечения НМС из удаленного расположения с помощью образов сетевого обновления.

Инструкции по обновлению программного обеспечения НМС из удаленного расположения с помощью образов сетевого обновления. Приведены инструкции по обновлению НМС уровня V6R1.2 или более высокого, включая все уровни НМС V7.

1. С компьютера или сервера, подключенного к Internet, перейдите на веб-сайт Консоль аппаратного обеспечения (<http://www14.software.ibm.com/webapp/set2/sas/f/netinstall/v7770network.html>)
2. Загрузите подходящие сетевые образы НМС V7 и сохраните их на сервере FTP. Эти файлы нельзя загрузить непосредственно в НМС. Файлы образов необходимо загрузить на сервер, принимающий запросы FTP.
3. Загрузите следующие файлы:
 - img2a
 - img3a
 - base.img
 - disk1.img
 - hmcnetworkfiles.sum
4. Сохраните данные обновления в НМС. Выполните следующие строки команды для сохранения данных обновления:
 - Для сохранения данных на диске DVD и жестком диске выполните следующие команды:
`mount /media/cdrom`
`saveupgdata -r diskdvd`
 - Для сохранения данных на жестком диске выполните следующую команду:
`saveupgdata -r disk`
5. Скопируйте файлы обновления в загрузочный раздел диска НМС. Выполните команду **getupgfiles** для копирования файлов.
 Пример: `getupgfiles -h <сервер ftp> -u <ИД пользователя> -d <удаленный каталог>`
 Где,
 - **сервер ftp** - это имя хоста или IP-адрес сервера FTP, содержащий сетевые образы НМС.
 - **ИД пользователя** - это допустимый ИД пользователя на сервере FTP. Если пароль не указан в аргументе `--passwd`, то он будет запрошен.
 - **удаленный каталог** - это каталог на сервере FTP, в котором сохранены сетевые образы НМС.
6. Перезагрузите НМС, чтобы обновить код, скопированный в раздел загрузочного диска. Выполните команду `chhmc -c altdiskboot -s enable --mode upgrade` для перезапуска НМС.
7. Перезагрузите НМС и начните обновление. Выполните команду `hmcshutdown -r -t now` для запуска процедуры обновления.

Настройка НМС с помощью интерфейса НМС Enhanced+

Рассматриваются настройка сетевых соединений, настройка НМС, действия после настройки и обновление НМС с помощью интерфейса НМС Enhanced+.

Примечание: Процедуры и функции интерфейса HMC Enhanced + Tech Preview (предварительная версия), который выступал как опция, предоставленная с HMC версии 8.20, не отличаются от интерфейса HMC Enhanced+, предоставляемого с HMC версии 8.30. В документации называется только HMC Enhanced+, но данные материалы относятся также и к интерфейсу HMC Enhanced + Tech Preview (предварительная версия).

Выбор параметров сети в HMC

Знакомит с параметрами сети, которые можно использовать в HMC.

Сетевые соединения HMC

Для соединения HMC с управляемыми системами можно использовать разные типы сетевых соединений. Дополнительная информация о настройке HMC для подключения к сети приведена в разделе “Настройка HMC” на стр. 91. Дополнительная информация об использовании HMC в сети приведена в следующем разделе:

Типы сетевых соединений HMC:

Знакомит с использованием функций дистанционного управления HMC и служебных функций при помощи сети.

HMC поддерживает следующие типы логических связей:

Соединение HMC с управляемой системой

Используется для выполнения большинства функций управления аппаратными средствами; в нем HMC выдает запросы функции управления через служебный процессор управляемой системы. Другое название соединения между HMC и служебным процессором: *сеть обслуживания*. Оно требуется для работы с управляемой системой.

Соединение HMC с логическим разделом

Используется для получения информации, связанной с платформой (события при ошибках аппаратных средств, реестр аппаратных средств), от операционных систем, работающих в логических разделах, а также для координации определенных действий платформы (динамический LPAR, оперативный ремонт) с указанными операционными системами. Для работы с функциями обслуживания и извещений об ошибках используется именно этот тип соединения.

HMC к BMC

Примечание: Соединение с контроллером управления базовой платой (BMC) применимо только к HMC модели 7063-CR1.

Применяется для выполнения задач обслуживания. Соединение BMC используется для настройки и обслуживания встроенного программного обеспечения HMC в системе. Это соединение требуется для доступа к BMC в HMC.

Соединение HMC с удаленными пользователями

Обеспечивает удаленный доступ к функциям HMC. Удаленные пользователи могут получить доступ к HMC следующим образом:

- С помощью веб-браузера для удаленного доступа ко всем функциям графического пользовательского интерфейса HMC.
- С помощью протокола SSH для доступа к функциям командной строки HMC.

Соединение HMC со службой сопровождения и поддержки

Используется для обмена данными, такими как отчеты об ошибках аппаратных средств, реестровые данные и обновления микрокодов, с обслуживающей системой. С его помощью можно также осуществлять автоматические вызовы сервисного центра.

HMC может поддерживать до четырех отдельных физических интерфейсов Ethernet, в зависимости от модели. Автономная версия HMC поддерживает три физических интерфейса HMC, используя один встроенный адаптер Ethernet и один или два встраиваемых адаптера. Каждый из указанных интерфейсов используется следующим образом:

- Один или несколько сетевых интерфейсов могут использоваться только для связи между НМС и управляемой системой; это означает, что в такой сети могут присутствовать только НМС и служебные процессоры управляемых систем. Несмотря на то, что сетевые интерфейсы для связи со служебными процессорами зашифрованы по протоколу Secure Sockets Layer (SSL) и защищены паролем, выделенная сеть обеспечивает более высокую степень защиты таких интерфейсов.
- Интерфейс открытой сети используется обычно для сетевых соединений между НМС и логическими разделами управляемых систем, обеспечивая связь между НМС и логическими разделами. Кроме того, интерфейс открытой сети обеспечивает удаленное управление НМС.
- При необходимости можно настроить третий интерфейс для подключения к логическим разделам и удаленного управления НМС. Третий интерфейс можно также использовать для отдельного соединения НМС с разными группами логических разделов. Например, можно создать отдельный сегмент локальной сети для задач администрирования, не связанный с общей локальной сетью, в которой выполняются деловые задачи. По этой сети администраторы смогут обращаться к НМС и другим управляемым компонентам. Иногда логические разделы размещаются в отдельных защищенных сегментах сети, возможно - за брандмауэром, и иногда требуются отдельные соединения НМС с этими сегментами сети.

Требования к веб-браузерам для НМС

Консоль аппаратного обеспечения (НМС) версии 8.7.0 поддерживается Google Chrome версии 57, Microsoft Internet Explorer (IE) версии 11.0, Mozilla Firefox версий 45 и 52 Extended Support Release (ESR), а также Safari версии 10.1.

Если браузер настроен для использования прокси-сервера, то в список исключений следует добавить локальные IP-адреса. За дополнительной информацией о списке исключений обратитесь к администратору сети. Если для подключения к НМС требуется использовать прокси-сервер, то включите переключатель Использовать HTTP 1.1 через прокси-соединения на вкладке Дополнительно в окне Свойства обозревателя.

Для работы Расширенного интерфейса управления системой (ASMI) при удаленном подключении к НМС необходимо включить cookie для текущего сеанса. В коде `asm.proxu` сохраняется информация о сеансе, которая используется в дальнейшем. Выполните инструкции по включению cookie сеансов.

Включение cookie сеансов в Internet Explorer.

1. Выберите Сервис, затем выберите Свойства обозревателя.
2. Выберите Конфиденциальность и нажмите кнопку Дополнительно
3. Убедитесь, что переключатель Всегда разрешать сеансовые cookie включен. Если он выключен, то включите переключатели Перекрыть автоматическую обработку файлов cookie и Всегда разрешать сеансовые cookie.
4. Включите переключатель Запрашивать в списках Основные cookie и Сторонние cookie.
5. Нажмите кнопку ОК.

Включение cookie сеансов в Firefox.

1. Выберите Инструменты, затем выберите Настройки.
2. Выберите Cookie
3. Включите переключатель Разрешить сайтам задавать cookie.
4. Выберите Исключения и добавьте НМС.
5. Нажмите кнопку ОК.

Частные и открытые сети в среде НМС:

НМС может быть настроена на открытые и частные сети. Частная сеть позволяет пользоваться избранным диапазоном немаршрутизируемых IP-адресов. *Общая*, или "открытая" сеть представляет собой сетевое соединение между НМС и любыми логическими разделами, а также другими системами обычной сети.

Частные сети

Из устройств в частной сети с НМС имеются только сама НМС и каждая из управляемых систем, к которым она подключена. НМС подключена к FSP (гибкому служебному процессору) каждой управляемой системы.

В большинстве систем FSP обеспечивает два порта Ethernet с метками **НМС1** и **НМС2**. Поэтому подключаться можно к двум НМС.

В некоторых системах предусмотрена такая возможность, как наличие двух FSP. В этой ситуации второй FSP выступает в роли "избыточного" резервного сервера. Основные требования установки системы с двумя FSP мало чем отличаются от требований к системе без второго FSP. НМС должна быть подключена к каждому FSP, поэтому при наличии дополнительного FSP или нескольких управляемых систем потребуются дополнительные аппаратные средства (например, коммутатор или концентратор LAN).

Примечание: Каждый порт FSP управляемой системы должен быть подключен только к одной НМС.

Общие сети

Открытая сеть может быть соединена с брандмауэром или маршрутизатором для подключения к Internet. Подключение к Internet позволяет НМС "обратиться к сервисный центр" в случае аппаратных сбоев, требующих отправки сообщений.

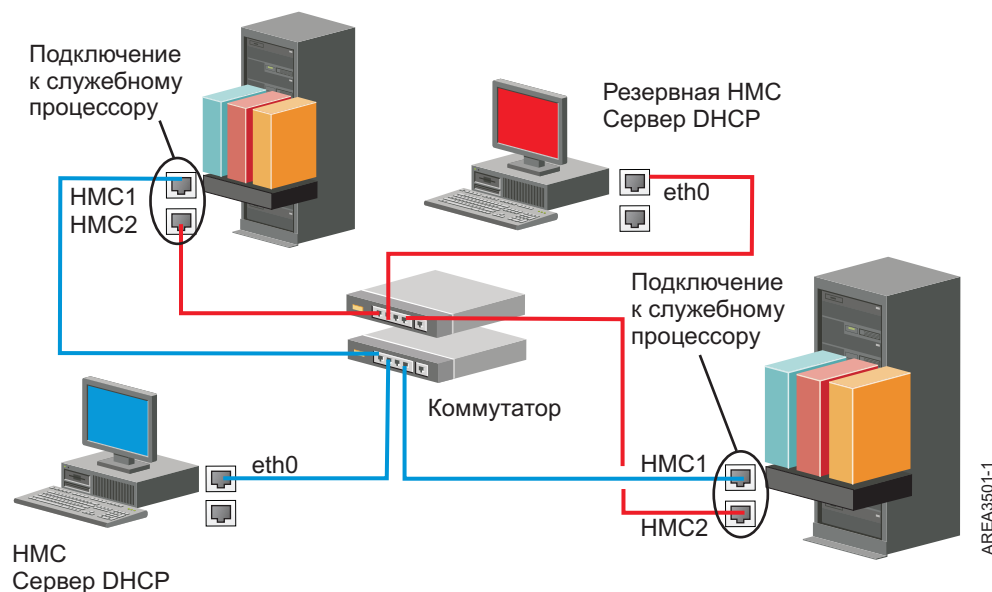
НМС предоставляет собственный брандмауэр на каждом из своих сетевых интерфейсов. Основной брандмауэр настраивается автоматически при запуске мастера пошаговой настройки НМС, но по окончании начальной установки и настройки НМС необходимо настроить брандмауэра, задав собственные параметры с учетом своих требований.

НМС в качестве сервера DHCP:

Данную НМС можно использовать в качестве сервера DHCP.

Примечание: При использовании IPv6 поиск необходимо выполнить вручную. Для IPv6 нет автоматической процедуры поиска.

Дополнительная информация о настройке НМС в качестве сервера DHCP приведена в разделе "Настройка НМС в качестве сервера DHCP" на стр. 99.

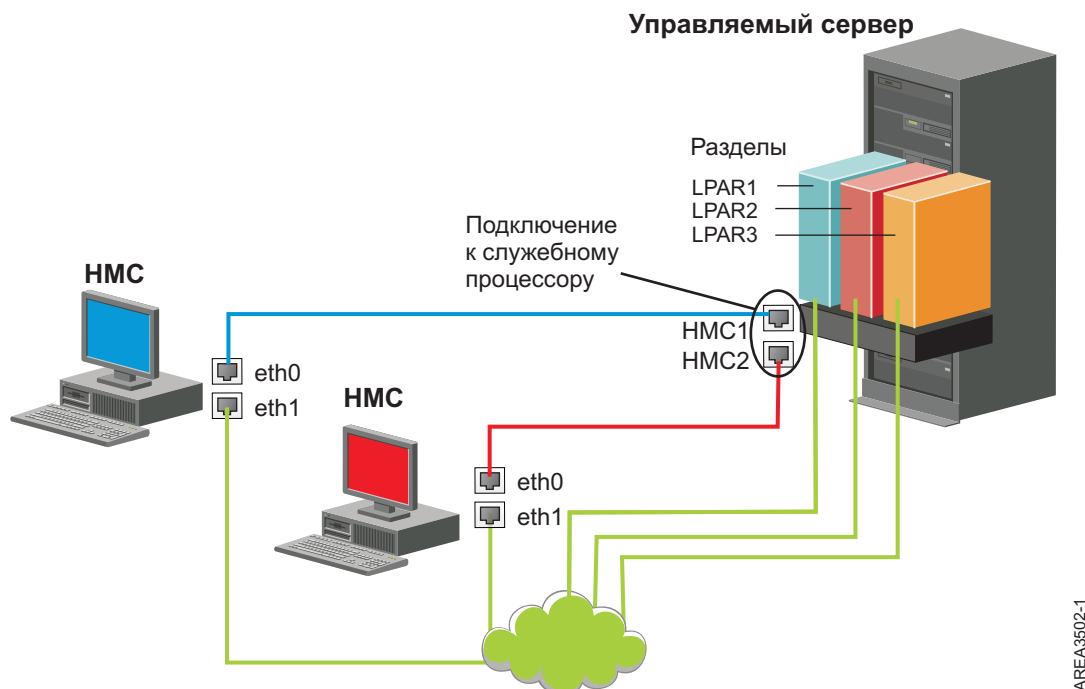


На рисунке показана среда дополнительной HMC с двумя управляемыми системами. Первая HMC подключена к первому порту на каждом FSP, дополнительная HMC - ко второму порту на каждой HMC. Каждая HMC настроена в качестве сервера DHCP с использованием отдельного диапазона IP-адресов. Соединения выполняются в разных частных сетях. Исходя из этого, важно, чтобы каждый порт был подключен только к одной HMC.

Каждый порт FSP управляемой системы, подключенный к HMC, требует уникального IP-адреса. С этой целью воспользуйтесь встроенной функцией сервера DHCP консоли HMC. После обнаружения процессором FSP активной сетевой ссылки, он выдает оповещающий запрос для нахождения сервера DHCP. Если настройка выполнена правильно, HMC в ответ на этот запрос назначает один из выбранных диапазонов адресов.

При наличии нескольких FSP требуется отдельный коммутатор или концентратор LAN для подключения HMC к частной сети FSP. В альтернативном варианте этот частный сегмент может существовать в виде нескольких портов в частной *виртуальной LAN* (VLAN) на более крупном управляемом переключателе. При наличии нескольких частных сетей VLAN они должны быть изолированными друг от друга, и между ними не должно быть перекрестного трафика.

В среде с несколькими HMC необходимо, кроме того, подключить каждый HMC к логическим разделам и к остальным HMC в одной и той же открытой сети.



На рисунке представлены две консоли HMC, подключенные к одному управляемому серверу в частной сети и к трем логическим разделам в открытой сети. Для того чтобы пользоваться тремя сетевыми интерфейсами, можно предусмотреть дополнительный адаптер Ethernet для HMC. Эту третью сеть можно использовать в качестве сети управления или можно подключить ее к серверу управления CSM (Cluster Systems Manager).

Дополнительная информация о настройке HMC в качестве сервера DHCP приведена в разделе “Настройка HMC в качестве сервера DHCP” на стр. 99.

Выбор способа соединения для сервисного сервера:

Дополнительные сведения об опциях соединения при работе с сервисным центром.

HMC можно настроить для передачи сервисной информации по аппаратному обеспечению в компанию IBM через Internet-соединение на основе LAN или соединение по телефонной линии через модем.

Примечание: Виртуальная частная сеть Internet (VPN) и соединение по телефонной линии через модем доступны только в HMC версии 8.2.0 и более ранних версий.

При настройке Internet-соединения на базе LAN обмен данными можно организовать двумя способами. В первом варианте используется стандартный протокол защищенных сокетов (SSL). Связь по протоколу SSL можно разрешить для подключения к Internet через сервер Proxy. SSL-соединение с большей вероятностью будет соответствовать корпоративным рекомендациям по обеспечению защиты. Во втором - соединение VPN.

Примечание: Если для открытого сетевого соединения интерфейса используется только Internet Protocol Version 6 (IPv6), нельзя использовать Internet VPN для соединения со службой поддержки. Дополнительная информация о применяемых протоколах приведена в разделе “Выбор протокола соединения с Интернетом” на стр. 80.

К преимуществам использования Internet-соединения можно отнести:

- Более высокая скорость передачи данных
- Более низкие расходы пользователя (например, затраты на выделенную телефонную линию)

- Более высокая надежность

При любом способе соединения действуют следующие характеристики защиты:

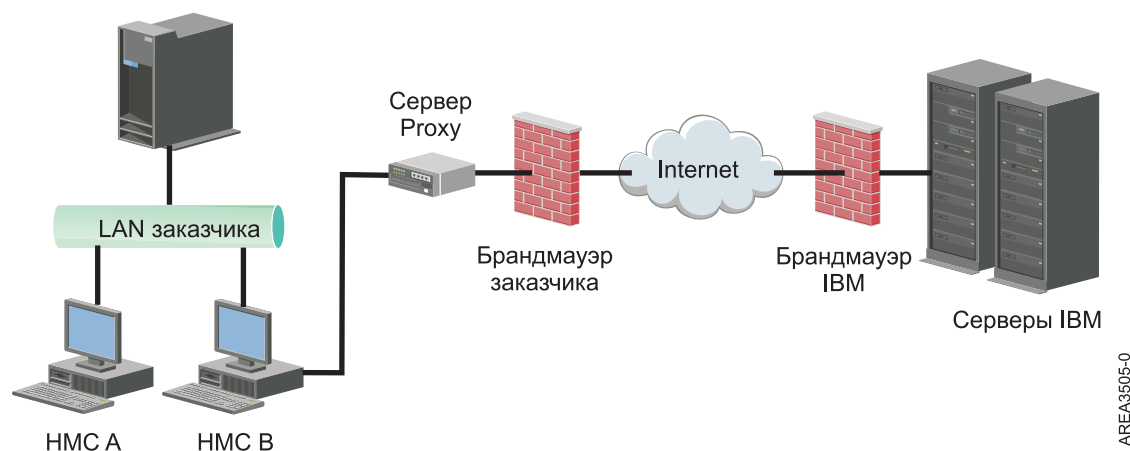
- Запросы Remote Support Facility всегда инициируются с НМС к IBM. Соединение для приема данных никогда не инициируется с системы сервисной поддержки IBM.
- Все данные, передаваемые между НМС и системой сервисной поддержки IBM, шифруются с помощью высококачественного шифрования. В зависимости от выбранного способа соединения, шифрование выполняется с помощью SSL или безопасного закрытия содержания по протоколу IPSec (ESP).
- При инициализации зашифрованного соединения НМС идентифицирует целевую систему как систему сервисной поддержки IBM.

Данные, отправляемые в систему сервисной поддержки IBM, состоят исключительно из сведений о неполадках аппаратных средств и данных конфигурации. Данные о прикладных программах и пользовательские данные в компанию IBM не передаются.

Использование непрямого Internet-соединения через прокси-сервер

Если по требованиям установки НМС должна находиться в частной сети, то соединение с Интернетом может выполняться через SSL прокси-сервер, используемый для направления запросов в Интернет. Еще одно потенциальное преимущество использования SSL прокси-сервера состоит в том, что прокси-сервер может поддерживать средства регистрации и контроля.

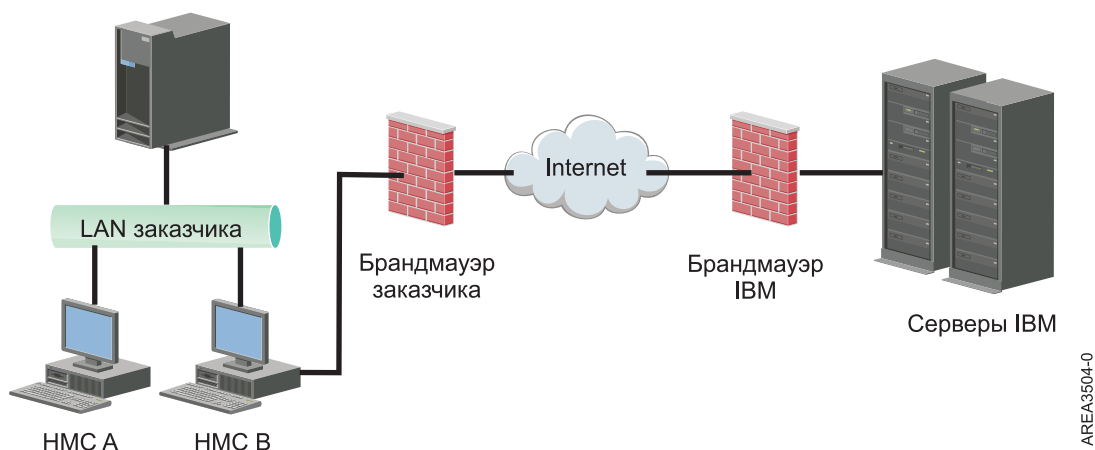
Для пересылки SSL сокетов сервер Proxy должен поддерживать основные функции заголовка сервера Proxy (как описано в RFC 2616) и метод CONNECT. По желанию можно настроить базовую идентификацию прокси (RFC 2617), чтобы НМС выполняла идентификацию перед пересылкой данных через прокси-сервер.



Для успешного обмена данными с НМС сервер Proxy клиента должен допускать соединение с портом 443. Можно настроить прокси-сервер таким образом, чтобы ограничить конкретные IP-адреса, с которыми НМС может устанавливать соединение. Список IP-адресов приведен в разделе “Списки адресов Internet SSL” на стр. 80.

Использование прямого SSL-соединения с Internet

Если можно устанавливать соединение НМС с Internet, и внешний брандмауэр можно настроить для передачи установленных исходящих пакетов TCP получателям, описанным в “Списки адресов Internet SSL” на стр. 80, то можно использовать прямое соединение с Internet.



Использование Internet SSL для соединения с удаленным сервисным центром:

Вся передача данных обрабатывается через сокеты TCP, инициированные HMC: в процессе передачи используется скоростной SSL для шифрования передаваемых данных. TCP/IP адреса получателей публикуются (см. “Списки адресов Internet SSL” на стр. 80), что позволяет настраивать внешние брандмауэры для разрешения таких соединений.

Примечание: Для всей передачи данных используется стандартный порт HTTPS 443.

HMC можно включать для соединения с Internet напрямую или для непрямого соединения с Internet через клиентский прокси-сервер. Выбор подходящего решения зависит от защиты и требований к сетевому взаимодействию конкретной организации. HMC, настроенная для работы с соединениями Internet SSL, использует (прямо или через SSL прокси-сервер) следующие адреса.

Выбор протокола соединения с Интернетом:

Определите версию IP-адреса, используемую при соединении HMC с Internet-провайдером.

Большинство пользователей для связи с Internet-провайдером используют Internet Protocol Version 4 (IPv4). Для доступа к Internet адреса IPv4 имеют формат, состоящий из четырех байтов адреса IPv4, разделенных точками (например 9.60.12.123). Также можно использовать Internet Protocol Version 6 (IPv6). IPv6 часто используется администраторами сети для обеспечения уникального пространства адресов. Если вы не уверены в том, какой протокол используется в вашей системе, обратитесь к сетевому администратору. Дополнительная информация об использовании каждой версии приведена в “Установка IPv4-адреса” на стр. 99 и “Установка IPv6-адреса” на стр. 100.

Списки адресов Internet SSL:

Описываются адреса HMC, используемые при соединении с Internet по протоколу SSL.

Для связи с сервисным центром IBM HMC, настроенная для работы с соединениями Internet SSL, использует следующие адреса IPv4.

Следующие адреса IPv4 используются для всех регионов:

- 129.42.26.224
- 129.42.42.224
- 129.42.50.224
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216

- 170.225.15.41

Следующие адреса IPv4 используются для Северной и Южной Америк:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

Следующие адреса IPv4 используются для всех регионов, за исключением Северной и Южной Америк:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

Примечание: При настройке брандмауэра, который должен разрешать соединение НМС с указанными серверами, требуются только IP-адреса, специфические для географического региона.

Для связи с сервисным центром IBM HMC, настроенная для работы с соединениями Internet SSL, использует следующие адреса IPv6:

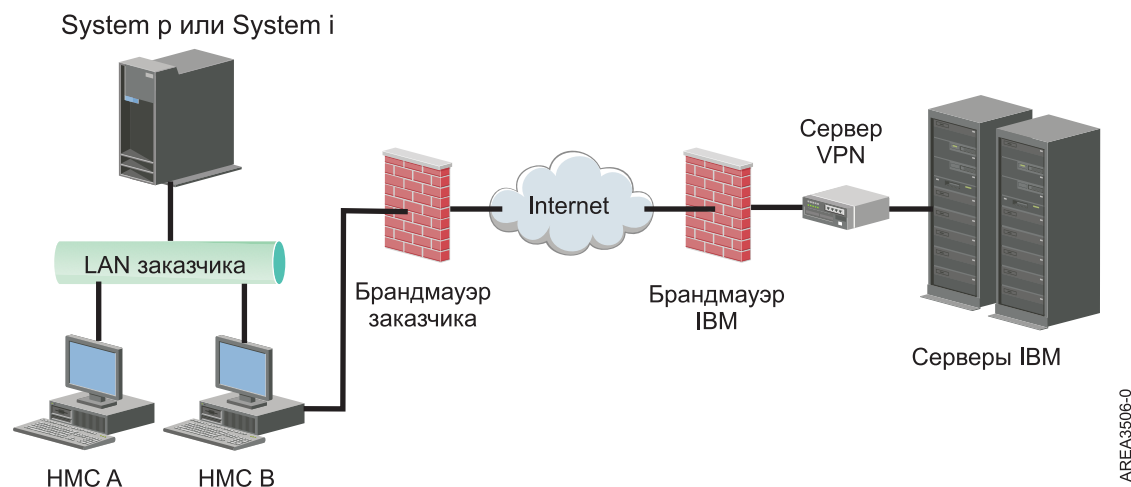
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

Использование виртуальной частной сети для соединения с сервисным центром:

Виртуальная частная сеть (VPN) обеспечивает защиту соединения с удаленным сервисным центром.

Примечание: Соединение этого типа доступно только в НМС версии 8.2.0 и более ранних версий.

VPN обеспечивает конфиденциальность отдельной сети по общедоступным соединениям путем применения шифрования и других способов защиты данных в физически разделенных сетевых соединениях стандартных частных сетей. Кроме использования для передачи исходящих сообщений, соединение VPN можно также настраивать по мере необходимости для поддержки запросов к сервисной службе.



Соединение с Интернетом обеспечивает администратор системы. При необходимости брандмауэр можно настроить таким образом, чтобы ограничить IP-адреса, к которым может подключаться НМС. При

необходимости настройки брандмауэра для ограничения IP-адресов обратитесь к “Список адресов серверов VPN” на стр. 81, где приведен список возможных адресов.

Дополнительная информация о соединении с Internet с использованием VPN на основе LAN приведена в разделе “Настройка типов сетей НМС” на стр. 94.

Список адресов серверов VPN:

Приведен список серверов, используемых НМС, когда НМС настроена для работы по соединению с Internet VPN.

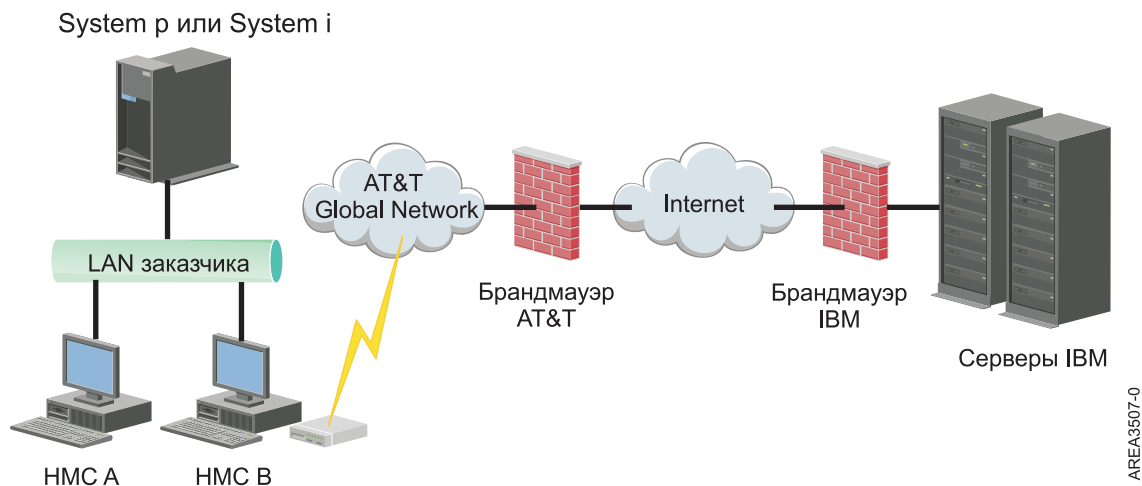
Если НМС настроена для работы по соединению с Internet VPN, она использует следующие серверы. Для всех соединений используются ESP и UDP на порте 500 и порте 4500 в случае использования брандмауэра преобразования сетевых адресов (NAT).

- 129.42.160.16 IBM VPN Server
- 207.25.252.196 IBM VPN Server

Использование телефона и модемов для соединения с удаленным сервисным центром:

При использовании модема для соединения с удаленным сервисным центром необходимо иметь выделенную аналоговую линию. НМС использует модем для соединения по телефонным линиям с глобальной сетью и для соединения со службой поддержки IBM.

Примечание: Соединение этого типа доступно только в НМС версии 8.2.0 и более ранних версий.



Дополнительная информация о соединении с удаленным сервисным центром с помощью телефона и модема приведена в разделе “Настройка типов сетей НМС” на стр. 94.

Использование нескольких серверов вызова сервисного центра:

Приведены необходимые сведения для использования нескольких серверов вызова сервисного центра.

Во избежание единственной точки сбоя настройте НМС для использования нескольких серверов вызова сервисного центра. Каждое сервисное событие будет обрабатываться первым доступным сервером. Если

произойдет сбой соединения или передачи с этого сервера, то попытка отправки сервисного запроса будет повторяться со следующих доступных серверов до тех пор, пока она не будет успешно завершена или пока не произойдет сбой на всех серверах.

Сообщение о неполадке отправляется подключенной НМС, которая была распознана при анализе неполадок как главная консоль анализа для данной управляемой системы. Главная консоль также отправляет копию отчета о неполадке вспомогательным НМС. Вспомогательная НМС должна быть распознана в сети главной НМС. Вспомогательная НМС распознается главной НМС как дополнительный сервер вызова сервисного центра, если:

- Главная НМС настроена для использования "обнаруженных" серверов вызова сервисного центра, и сервер либо находится в той же подсети, что и главная НМС, либо управляет той же системой
- Сервер вызова сервисного центра был вручную добавлен в список консолей серверов, доступных для осуществления исходящих соединений

Подготовка к настройке НМС

Пользуясь этим разделом, соберите обязательные параметры конфигурации, которые понадобятся для выполнения шагов настройки.

Для того чтобы настроить НМС, ознакомьтесь со связанными концепциями, спланируйте варианты решения и подготовьте необходимую информацию.

В этом разделе приведена информация, необходимая для подключения НМС к следующим устройствам и системам:

- Служебные процессоры управляемых систем
- Логические разделы управляемых систем
- Удаленные рабочие станции
- Служба поддержки IBM для реализации функций “вызова сервисного центра”.

Примечание: Существуют дополнительные сведения о соединениях и защите. Дополнительная информация приведена в документе **ESA for HMC Connectivity Security for IBM POWER6, POWER7 and POWER8 Processor-Based Systems and IBM Storage Systems DS8000** : IBM Electronic Service Agent (<http://www-01.ibm.com/support/esa/security.htm>).

Для подготовки конфигурации НМС выполните следующие действия:

1. Приобретите и установите самый новый уровень версии НМС, который вы хотите установить.
2. Определите физическое расположение НМС по отношению к управляемым серверам. Если расстояние между НМС и управляемой системой превышает 7,5 метров, то необходимо настроить доступ к НМС через веб-браузер.
3. Определите серверы, которые должны работать под управлением НМС.
4. Определите, будет ли для управления серверами использоваться частная или открытая сеть. В частной сети следует использовать сервер DHCP, если не применяется конфигурация Cluster Systems Management (CSM). CSM не поддерживает IPv6. Для доступа к CSM нужно иметь две сети. Дополнительная информация о CSM приведена в соответствующей документации. Дополнительная информация об открытых и частных сетях приведена в разделе “Частные и открытые сети в среде НМС” на стр. 75.
5. В открытой сети адрес FSP следует указать вручную с помощью меню расширенного интерфейса управления системой (ASMI). Рекомендуется использовать частную сеть без возможности маршрутизации.
6. Если у вас две НМС, назначьте главную и вспомогательную НМС. Главная НМС должна находиться физически ближе к компьютеру и быть настроена для вызова сервисного центра.
7. Определите сетевые параметры, которые потребуются настроить для подключения НМС к удаленным системам, логическим разделам и сетевым устройствам.
8. Определите способ вызова сервисного центра. Можно выбрать исходящее соединение Secure Socket Layer (SSL), модем или соединение виртуальной частной сети (VPN).

9. Определите пользователей НМС, пароли пользователей, а также выполняемые ими роли. Пароли должны быть указаны для пользователей hscroot и hscpe.
10. Подготовьте следующую информацию об организации:
 - Имя компании
 - Имя администратора
 - Электронный адрес
 - Номера телефонов
 - Номера факсов
 - Адрес помещения, в котором предполагается установить НМС
11. Если планируется уведомлять операторов или администраторов об отправке информации в сервисный центр IBM, то укажите сервер SMTP и электронные адреса.
12. Необходимо задать следующие пароли:
 - Пароль доступа для идентификации НМС при обращении к FSP.
 - Пароль ASMI для **администратора**.
 - Пароль ASMI для **обычных** пользователей.

Укажите пароли при первом подключении НМС к новому серверу. В случае применения резервной или второй консоли НМС необходимо получить пароль пользователя НМС и указать его при первом подключении к FSP управляемого сервера.

После завершения подготовительной процедуры перейдите к разделу “Форма настройки НМС перед установкой” на стр. 84.

Форма настройки НМС перед установкой

В этой справочной таблице приведена информация, необходимая для подготовки к установке.

Параметры сети

Интерфейс LAN: Выберите доступные адаптеры (например, eth0, eth1), с помощью которых НМС будет соединяться с управляемыми системами, логическими разделами, сервисным центром и/или удаленными пользователями. Дополнительная информация приведена в разделе “Сетевые соединения НМС” на стр. 73. Соединение с НМС может устанавливаться в частной или открытой сети.

Пропускная способность и дуплексный режим адаптера Ethernet

Введите требуемую пропускную способность и дуплексный режим адаптера Ethernet. Параметр автоматическое определение определяет оптимальный параметр для данных аппаратных средств. Стандартное значение = Автоматическое определение Пропускная способность задает пропускную способность в дуплексном режиме адаптера Ethernet. Выберите автоматическое определение, если не требуется указывать конкретную пропускную способность. Любое устройство, подключенное к FSP (коммутаторы/НМС) должно работать в режиме Автоматически (быстродействие) / Автоматически (дуплексный), поскольку это режим FSP по умолчанию, который нельзя изменить.

Таблица 34. Пропускная способность и дуплексный режим адаптера Ethernet

	eth0	eth1	eth2	eth3
Выберите пропускную способность и дуплексный режим				
Пропускная способность (Автоматическое определение, 10/100/1000 дуплексный/ полудуплексный)				

Дополнительная информация об открытых и частных сетях приведена в разделе “Частные и открытые сети в среде НМС” на стр. 75.

Таблица 35. Частные и открытые сети

	eth0	eth1	eth2	eth3
Для каждого адаптера укажите Частная или Открытая сеть				

Протокол динамической настройки хостов (DHCP) является автоматическим способом динамической настройки клиента. Данную НМС можно определить как сервер DHCP. Для первой или единственной НМС в частной сети разрешите НМС в качестве сервера DHCP. Как только это будет сделано, НМС автоматически настроит и найдет управляемые системы.

Для адаптеров Ethernet, заданных как частные сети, заполните следующую таблицу:

Таблица 36. Частные сети

	eth0	eth1
Определить эту НМС как сервер DHCP? (да/нет)		
Если "да," запишите диапазон IP-адресов, который необходимо использовать.		

В случае применения НМС 7063-CR1 необходимо подключить порт **IPMI** Ethernet к сети, чтобы обеспечить доступ к контроллеру управления платформой (BMC) в НМС. Дополнительная информация приведена в разделе “Настройка связи BMC” на стр. 146. Заполните следующую таблицу для соединения BMC.

Таблица 37. Соединение BMC

	IPMI
Вы хотите настроить это соединение в режиме DHCP? (да/нет)	
Если "нет", введите указанные статические адреса ниже:	
IP-адрес:	
Маска подсети:	
Шлюз:	

Для адаптеров Ethernet, заданных как *открытые* сети, заполните следующие таблицы. Более подробная информация о различных версиях протокола IP приведена в разделе “Выбор протокола соединения с Интернетом” на стр. 80.

Применение IPv6

Если вы используете IPv6, обсудите с администратором сети то, как необходимо получать IP-адреса. Затем заполните следующие таблицы:

Таблица 38. Применение IPv6

	eth0	eth1	eth2	eth3
Используете ли вы статически присвоенный IP-адрес? Если "да", укажите его здесь.				

Таблица 39. Применение IPv6

	eth0	eth1	eth2	eth3
Получаете ли вы IP-адреса от сервера DHCP? (Да/Нет)				

Таблица 40. Применение IPv6

	eth0	eth1	eth2	eth3
Получаете ли вы IP-адреса от маршрутизатора IPv6?				

Дополнительная информация о настройке адресов IPv6 приведена в разделе “Установка IPv6-адреса” на стр. 100. Дополнительная информация об использовании только адресов IPv6 приведена в разделе “Использование только адресов IPv6” на стр. 100.

Применение IPv4

Заполните следующие таблицы для адаптеров Ethernet, заданных как открытые сети с использованием IPv4.

Таблица 41. Применение IPv4

	eth0	eth1	eth2	eth3
Получать IP-адреса автоматически? (да/нет)				
Если "нет", введите указанный адрес ниже:				
Адрес интерфейса TCP/IP:				
Маска сети интерфейса TCP/IP:				
Параметры брандмауэра:				
Настроить параметры брандмауэра НМС? (да/нет)				
Если "да", перечислите приложения и IP-адреса, которые должны пропускаться через брандмауэр:				

Информация о TCP/IP

Уникальный адрес TCP/IP требуется для каждого узла, как для элемента поддержки (SE), так и для консоли аппаратного обеспечения (НМС). Заданная маска сети используется для создания уникального адреса (по умолчанию) для локальной частной LAN. Если узлы будут связаны в более крупную сеть с устанавливаемым адресом TCP/IP, можно указать адрес TCP/IP. Стандартное значение генерируется системой.

Параметры брандмауэра

Параметры брандмауэра НМС создают защитный барьер, который разрешает или запрещает доступ к конкретным сетевым приложениям на НМС. Эти параметры управления можно устанавливать для каждого физического интерфейса сети отдельно; таким образом можно регулировать, через какую НМС будет предоставляться доступ к сетевым приложениям в каждой сети.

Если хотя бы один адаптер настроен как адаптер открытой сети, то для разрешения доступа к LAN с НМС потребуется следующая дополнительная информация:

Таблица 42. Информация о локальном хосте

Информация о локальном хосте	
Имя хоста НМС:	
Имя домена:	
Описание НМС:	
Информация о шлюзе	
Адрес шлюза: (nnn.nnn.nnn.nnn)	
Устройство шлюза:	
Разрешение DNS	
Использовать DNS? (да/нет)	
Если “да”, укажите очередность обращения к серверам DNS ниже:	
1.	
2.	
Порядок просмотра доменных суффиксов:	
1.	
2.	

Информация о локальном хосте

Для того чтобы идентифицировать консоль аппаратного обеспечения (НМС) для сети, введите имя хоста и имя домена НМС. Введите полное имя хоста, кроме случаев, когда в сети используются только короткие имена. Пример имени домена: name.yourcompany.com

Информация о шлюзе

Для определения стандартного шлюза введите адрес TCP/IP, который будет использоваться для маршрутизации IP-пакетов. Адрес шлюза сообщает каждому компьютеру или сетевому устройству, когда пересылать данные, если целевая станция и отправитель находятся в разных подсетях.

Включение DNS

Система имен доменов (DNS) служит стандартным соглашением об именах для поиска компьютеров, использующих IP-протокол. Определив серверы DNS, можно вместо IP-адресов использовать имена хостов для идентификации серверов и консолей аппаратного обеспечения (НМС).

Очередность обращения к серверам DNS

Введите IP-адреса серверов DNS, которые нужно будет искать для преобразования имен хостов и IP-адресов. Очередность обращения доступна только тогда, когда DNS включен.

Порядок просмотра доменных суффиксов

Введите используемые доменные суффиксы. НМС использует доменные суффиксы, которые добавляются к неполным именам для обращений к DNS. Суффиксы просматриваются в порядке их следования в списке. Порядок просмотра доступен только тогда, когда DNS включен.

Уведомление по электронной почте

Введите информацию для контактов по электронной почте, если желательно получать извещения по email при неполадках аппаратных средств локальной системы.

Таблица 43. Уведомление по электронной почте

Поля	
Адреса электронной почты:	
Сервер SMTP:	
Порт:	
Уведомлять об ошибках:	
Только события при неполадках для сервисного центра	
События при всех неполадках	

Сервер SMTP

Введите адрес SMTP-сервера, который будет использоваться для отправки электронного сообщения. Пример имени сервера SMTP - relay.us.ibm.com.

SMTP - это протокол для отправки электронной почты. При использовании SMTP клиент отправляет сообщение и обменивается данными с сервером SMTP по протоколу SMTP.

Если вам не известен адрес SMTP сервера или нет уверенности в его правильности, обратитесь к администратору сети.

Порт Введите номер порта сервера, который нужно оповещать о системном событии, или воспользуйтесь стандартным портом.

Электронный адрес

Введите настроенные электронные адреса для отправки сообщений о системных событиях.

- **Только события при неполадках для сервисного центра** выбирают только для получения извещения при наступлении событий, создающих сервисную функцию.
- **События при всех неполадках** выбирают для получения извещения при наступлении любых событий.

Сервисная контактная информация

Таблица 44. Сервисная контактная информация

Сервисная контактная информация	
Имя компании	
Имя администратора	
Электронный адрес	
Номер телефона	
Другой номер телефона	
Номер факса	
Другой номер факса	
Адрес местонахождения	
Адрес местонахождения 2	
Город или населенный пункт	

Таблица 44. Сервисная контактная информация (продолжение)

Сервисная контактная информация	
Состояние	
Почтовый индекс	
Страна или регион	
Местонахождение НМС (если совпадает с вышеуказанным адресом администратора, укажите “то же”):	
Адрес местонахождения	
Адрес местонахождения 2	
Город или населенный пункт	
Состояние	
Почтовый индекс	
Страна или регион	

Связь с сервисным центром и доступ

Выберите тип соединения для контактов с сервисным центром. Описание указанных методов, включая требования к характеристикам защиты и конфигурации, приведено в разделе “Выбор способа соединения для сервисного сервера” на стр. 77.

Таблица 45. Тип соединения

Тип соединения	
	Secure Sockets Layer (SSL) через Internet
	Соединение по телефонной линии с локальной НМС
	Виртуальная частная сеть (VPN) через Internet

Secure Sockets Layer (SSL) через Internet:

При наличии существующего Internet-соединения с НМС им можно пользоваться для связи с сервисным центром. С сервисным центром можно связываться напрямую с использованием зашифрованного Secure Sockets Layer (SSL) по существующему Internet соединению. Если требуется настроить использование зашифрованного SSL с использованием непрямого соединения через SSL Проxy, выберите **Использовать SSL Proxy**.

Таблица 46. Secure Sockets Layer (SSL) через Internet

Secure Sockets Layer (SSL) через Internet	
Использовать SSL? (да/нет)	
Если "да", введите информацию ниже:	
Адрес:	
Порт:	
Идентифицировать с SSL Proxy?	
Если "да", введите информацию ниже:	
Пользователь:	
Пароль:	

Используемый протокол соединения с Internet

Более подробная информация о различных протоколах IP приведена в разделе “Выбор протокола соединения с Интернетом” на стр. 80.

___ IPv4

___ IPv6

___ IPv4 и IPv6

Соединение по телефонной линии с локальной НМС

Введите информацию телефонного соединения для настройки локального модема. Укажите номера телефонов для связи с сервисным центром. При соединении телефонные номера будут набираться в порядке их следования в списке.

Таблица 47. Соединение по телефонной линии с локальной НМС

Поля	
Префикс телефонного номера:	
Тональный:	
Импульсный:	
Дождаться гудка?	
Включить громкую связь?	

Виртуальная частная сеть (VPN)

При наличии существующего Internet-соединения с НМС им можно пользоваться для связи с сервисным центром. С сервисным центром можно связываться напрямую через виртуальную частную сеть (VPN) с использованием существующего Internet соединения.

Примечание: При выборе виртуальной частной сети (VPN) через Internet никакие другие параметры выбирать не нужно.

Серверы сервисного центра

Определите, какие НМС необходимо настроить в качестве серверов для вызова сервисного центра и службы поддержки. Дополнительная информация об использовании нескольких серверов вызова сервисного центра приведена в разделе “Использование нескольких серверов вызова сервисного центра” на стр. 82.

___ Эту НМС

___ Другую НМС

Если вы выбрали **Другую НМС**, перечислите другие НМС, настроенные как серверы вызова сервисного центра:

Таблица 48. Другие НМС, настроенные как серверы вызова сервисного центра

Список имен хостов или IP-адресов НМС, настроенных как серверы вызова сервисного центра

Дополнительные преимущества поддержки

Мои системы и премиальный поиск

Таблица 49. Дополнительные преимущества поддержки

Поля	
Укажите свой ИД в IBM	
Укажите свой ИД в IBM	

Для получения доступа к ценной персонализированной вспомогательной информации в разделах Мои системы и Премиальный поиск веб-сайта Electronic Services пользователи должны зарегистрировать ID IBM в данной системе. При отсутствии ИД IBM зарегистрироваться для его получения можно на: www.ibm.com/account/profile.

Примечание: IBM предоставляет персонализированные веб-функции, в которых используется информация, собранная приложением IBM Electronic Service Agent. Для того чтобы иметь возможность пользоваться этими функциями, необходимо вначале зарегистрироваться на веб-сайте регистрации в IBM по адресу <http://www.ibm.com/account/profile>.

Для предоставления пользователям права на использование информации Electronic Service Agent с целью персонализации веб-функций введите ID IBM, зарегистрированный на веб-сайте регистрации IBM. Для ознакомления с ценной информацией поддержки, доступной для клиентов, зарегистрировавших ИД IBM в своих системах, перейдите к разделу <http://www.ibm.com/support/electronic.systems>.

Настройка НМС

Рассмотрена настройка сетевых соединений, защиты, служебных приложений и некоторых параметров для пользователей.

В зависимости от предполагаемого уровня настройки конфигурации НМС, можно воспользоваться несколькими вариантами настройки НМС, выбирая из них наиболее подходящий для своих задач. Инструментальное средство Мастер пошаговой настройки из НМС позволяет легко и быстро выполнить настройку НМС. Мастер предоставляет возможность выбрать быстрое прохождение, при этом быстро создается рекомендуемая среда НМС. Кроме того, в нем предусмотрена возможность подробного ознакомления с доступными параметрами. Настройку можно также выполнить без помощи мастера в соответствии с инструкциями из раздела Настройка НМС с помощью меню НМС.

Перед выполнением настройки получите обязательную информацию о конфигурации, которая потребуется для успешного выполнения шагов. Список обязательной информации приведен в разделе “Подготовка к настройке НМС” на стр. 82. По завершении подготовки выполните инструкции из раздела “Форма настройки НМС перед установкой” на стр. 84 и вернитесь к этому разделу.

Настройка НМС с помощью быстрого выполнения мастера пошаговой настройки

В большинстве случаев НМС можно настроить для эффективной работы с помощью многочисленных стандартных параметров. Для того чтобы быстро и эффективно подготовить НМС к работе, воспользуйтесь данной справочной таблицей быстрого выполнения. После выполнения этих действий НМС будет настроена в качестве сервера протокола динамической настройки хостов (DHCP) частной (подключенной напрямую) сети.

Запуск НМС и выполнение шагов мастера пошаговой настройки:

Войдите в интерфейс НМС и настройте свою НМС с помощью мастера пошаговой настройки.

Примечание: В случае новой установки убедитесь, что управляемая система не подключена к источнику питания. Для консоли НМС, монтируемой в стойке, данное требование означает, что единственным устройством, подключаемым к шине распределения питания (PDB) до подключения источника питания, является НМС. Если речь идет о второй НМС, подключенной к той же управляемой системе, то управляемая система может быть подключена к источнику питания.

1. Включите НМС, нажав кнопку питания.
2. Дождитесь, пока НМС автоматически выберет стандартный язык и желательную локаль по истечении 30 секунд.
3. Примите условия лицензионных соглашений на Консоль аппаратного обеспечения. Если условия лицензионных соглашений на Консоль аппаратного обеспечения не будут приняты, выполнить настройку НМС не удастся.
4. Выберите **Войти и запустить веб-приложение Консоль аппаратного обеспечения**.
5. Войдите в НМС:

Примечание: Введите пароль, если его изменил системный администратор (**hmcadmin**).

- ИД: hscroot
- Пароль: abc123

Откроется мастер пошаговой настройки.

6. Нажмите **ОК** в окне входа в пошаговую настройку.

Примечание: Если после запуска НМС Мастер пошаговой настройки не показан, выберите **Мастер пошаговой настройки** в области навигации начальной страницы НМС.

7. Выполните шаги, предлагаемые мастером пошаговой настройки, в соответствии с заполненной перед установкой справочной таблицей. Для продолжения нажмите **Да** и выполните шаги, описанные в мастере Соединений и вызова сервисного центра.
8. В окне Обзор нажмите кнопку **Закончить**.
9. Подсоедините к управляемой системе перекрестный кабель Ethernet.
10. В области навигации НМС выберите **Управление службами**.
11. В области содержимого выберите **Предоставить пользователю права доступа**. Откроется окно Предоставление пользователю прав доступа.
12. Введите свой ИД IBM в поле и нажмите **ОК**.

Проверка конфигурации:

В окне Состояние отследите текущее состояние разных выбранных вами параметров конфигурации. Для некоторых параметров в течение нескольких минут может отражаться состояние Ожидание. Выберите **Просмотреть протокол** и просмотрите сообщения о состоянии по каждой задаче. Мастер пошаговой настройки можно закрыть в любой момент - для этого нужно нажать кнопку **Закрыть**. При этом запущенные задачи будут продолжать выполнение. НМС настроена.

Настройка НМС с помощью меню НМС

В этом разделе приведен полный список всех задач настройки НМС, направляющих пользователя в процессе настройки НМС. Выберите данный пункт, если Мастер пошаговой настройки не будет использован.

Для вступления в силу параметров конфигурации необходимо будет перезапустить НМС, поэтому имеет смысл распечатать данную таблицу, чтобы пользоваться ею при настройке НМС.

В данном документе имеются ссылки на задачи, не вошедшие в данный PDF. Для получения доступа к дополнительным материалам поддержки можно обратиться к разделу **Дополнительные ресурсы** на начальных страницах НМС.

Предварительные требования

Перед тем, как приступить к настройке НМС с помощью меню НМС, выполните подготовительные действия, описанные в разделе “Подготовка к настройке НМС” на стр. 82.

Таблица 50. Задачи настройки НМС вручную и источники связанной информации

Задача	Где искать связанную информацию
1. Запустите НМС.	“Запуск НМС” на стр. 93
2. Задайте дату и время.	
3. Измените стандартные пароли.	
4. Создайте дополнительных пользователей и вернитесь к этой справочной таблице.	
5. Настройте сетевые соединения.	“Настройка типов сетей НМС” на стр. 94
6. При использовании открытой сети и фиксированных IP-адресов установите идентификационную информацию.	
7. При использовании открытой сети и фиксированных IP-адресов настройте запись маршрутизации как стандартный шлюз.	“Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 101
8. При использовании открытой сети и фиксированных IP-адресов настройте службы имен доменов.	“Настройка служб имен доменов” на стр. 101
9. При использовании фиксированных IP-адресов и включении DNS настройте доменные суффиксы.	“Настройка доменных суффиксов” на стр. 102
10. Настройте сервер для соединения со службой поддержки IBM и вернитесь к данной справочной таблице после выполнения этого шага.	“Настройка НМС для связи с сервисным центром и службой поддержки” на стр. 103
11. Настройте Администратор событий для вызова сервисного центра.	“Настройка Администратора событий для вызова сервисного центра” на стр. 108
12. Подключите управляемую систему к источнику питания.	
13. Укажите пароли для управляемой системы, а также пароли ASMI (общий и администратора).	“Задание паролей для управляемой системы” на стр. 109
14. Задайте дату и время управляемой системы с помощью ASMI.	
15. Запустите управляемую систему и вернитесь к этой справочной таблице.	
16. Убедитесь, что в управляемой системе создан один логический раздел.	
17. Необязательно: Добавьте другую управляемую систему и вернитесь к этой справочной таблице.	
18. Необязательно: При установке нового сервера с НМС настройте логические разделы и установите операционную систему.	
19. Если вы не устанавливаете новый сервер, то выполните задачи заключительного этапа настройки для дополнительной настройки конфигурации.	“Действия после настройки” на стр. 110

Запуск НМС:

Войдите в НМС и выберите рабочий язык для интерфейса. Для первого входа в НМС воспользуйтесь стандартными ИД hscroot и паролем abc123.

Для запуска НМС выполните следующие действия:

1. Включите НМС, нажав кнопку питания.
2. Если предпочитаемым языком является английский, перейдите к шагу 4.
Если предпочтение отдается другому языку, введите номер **2** после предложения изменить локаль.

Примечание: Для ответа на предложение пользователю дается 30 секунд.

3. Выберите необходимую локаль в окне Выбор локали и нажмите кнопку **ОК**. Локаль определяет язык, который используется интерфейсом НМС.
4. Войдите в НМС, используя приведенный ниже стандартный ИД и пароль пользователя:

Имя пользователя: hscroot

Пароль: abc123

На странице входа в систему можно просмотреть состояние систем, разделов и серверов виртуального ввода-вывода. Кроме того, можно просмотреть индикаторы Внимание и обслуживаемые события. На странице входа в систему доступны ссылки на различные социальные сети и сайт IBM developerWorks с дополнительной информацией о функциях НМС.

Примечание: В НМС версии 8.6.0.1 можно выбрать следующие варианты входа в систему:

Вход в систему: НМС Classic или НМС Enhanced+

Для продолжения выберите интерфейс НМС Enhanced+. Интерфейс НМС Classic предоставляет доступ ко всем стандартным функциям НМС, а интерфейс НМС Enhanced+ предлагает графические представления систем, разделов и серверов виртуального ввода-вывода, а также упрощенную навигацию.

НМС Classic

Отображает стандартный графический пользовательский интерфейс без расширенных функций PowerVM.

НМС Enhanced+

Показывает новое представление полностью переработанного интерфейса управления НМС, который обеспечивает интуитивную рабочую среду интерфейса с графическими представлениями систем, разделов и серверов виртуального ввода-вывода, а также упрощенной навигацией.

Примечание: Если НМС работает в качестве сервера DHCP, то она применяет пароль по умолчанию при первом подключении к служебному процессору.

5. Выберите **Войти**.

Изменение даты и времени:

Работающие от батарей часы хранят дату и время НМС. Иногда необходимо восстановить дату и время консоли, например, в случае замены батарей или при физическом перемещении системы в другой часовой пояс. Знакомит с процедурой изменения даты и времени для НМС.

При смене информации о дате и времени внесенные изменения не отразятся на системах и логических разделах под управлением НМС.

Для изменения даты и времени НМС выполните следующие действия:

1. Проверьте, входите ли вы в группу пользователей с одной из ролей:
 - Главный администратор
 - Сотрудник сервисного представительства
 - Оператор
 - Наблюдатель



2. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
3. На панели содержимого выберите **Изменить дату и время**.
4. При выборе пункта **UTC** в поле **Часы** значение времени будет настроено автоматически как сезонное время выбранного часового пояса. Введите дату, время и часовой пояс и нажмите **ОК**.

Настройка типов сетей НМС:

Настройка НМС для взаимодействия с управляемой системой, логическими разделами, удаленными пользователями и службой поддержки.

Настройка НМС для подключения к управляемой системе по открытой сети:

Процедура настройки НМС для подключения к управляемой системе по открытой сети.

Для того чтобы настроить НМС для подключения к управляемой системе по открытой сети, выполните следующие действия:

Таблица 51. Настройка НМС для подключения к управляемой системе по открытой сети

Задача	Где искать связанную информацию
1. Выберите интерфейс управляемой системы. Рекомендуемый интерфейс: eth0 .	“Форма настройки НМС перед установкой” на стр. 84
2. Выберите порты Ethernet для НМС.	“Идентификация порта Ethernet, определяемого как eth0” на стр. 97
3. Настройте адаптер Ethernet. Для этого выполните следующие задачи:	
a. Укажите пропускную способность.	“Установка пропускной способности” на стр. 98
b. Выберите тип открытой сети.	“Выбор типа сети (частная, открытая)” на стр. 99
c. Укажите статические адреса.	“Установка IPv4-адреса” на стр. 99
d. Укажите брандмауэр.	“Изменение параметров брандмауэра НМС” на стр. 100
e. Настройте шлюз по умолчанию.	“Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 101
f. Настройте DNS.	“Настройка служб имен доменов” на стр. 101
4. Настройте дополнительные адаптеры (если они установлены).	
5. Проверьте соединение между управляемым сервером и НМС.	“Проверка соединения между НМС и управляемой системой” на стр. 110

Настройка НМС для подключения к управляемой системе по частной сети:

Процедура настройки НМС для подключения к управляемой системе по частной сети.

Для того чтобы настроить НМС для подключения к управляемой системе по частной сети, выполните следующие действия:

Таблица 52. Настройка НМС для подключения к управляемой системе по частной сети

Задача	Где искать связанную информацию
1. Выберите интерфейс управляемой системы.	“Форма настройки НМС перед установкой” на стр. 84

Таблица 52. Настройка НМС для подключения к управляемой системе по частной сети (продолжение)

Задача	Где искать связанную информацию
2. Выберите порты Ethernet для НМС.	“Идентификация порта Ethernet, определяемого как eth0” на стр. 97
3. Настройте НМС в качестве сервера DHCP.	“Настройка НМС в качестве сервера DHCP” на стр. 99
4. Проверьте соединение между управляемым сервером и НМС.	“Проверка соединения между НМС и управляемой системой” на стр. 110

Настройка НМС для подключения к логическим разделам по открытой сети:

Для того чтобы настроить НМС для подключения к логическим разделам по открытой сети, выполните следующие действия:

Таблица 53. Настройка НМС для подключения к логическим разделам по открытой сети

Задача	Где искать связанную информацию
1. Выберите интерфейс управляемой системы.	“Форма настройки НМС перед установкой” на стр. 84
2. Выберите порты Ethernet для НМС.	“Идентификация порта Ethernet, определяемого как eth0” на стр. 97
3. Настройте адаптер Ethernet. Для этого выполните следующие задачи:	
a. Укажите пропускную способность.	“Установка пропускной способности” на стр. 98
b. Выберите тип открытой сети.	“Выбор типа сети (частная, открытая)” на стр. 99
c. Укажите статические адреса.	“Установка IPv4-адреса” на стр. 99
d. Укажите брандмауэр.	“Изменение параметров брандмауэра НМС” на стр. 100
e. Настройте шлюз по умолчанию.	“Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 101
f. Настройте DNS.	“Настройка служб имен доменов” на стр. 101
4. Настройте дополнительные адаптеры (если они установлены).	
5. Проверьте соединение между управляемым сервером и НМС.	“Проверка соединения между НМС и управляемой системой” на стр. 110

Настройка НМС для подключения к удаленным пользователям по открытой сети:

Для того чтобы настроить НМС для подключения к удаленным пользователям по открытой сети, выполните следующие действия:

Таблица 54. Настройка НМС для подключения к удаленным пользователям по открытой сети

Задача	Где искать связанную информацию
1. Выберите интерфейс управляемой системы.	“Форма настройки НМС перед установкой” на стр. 84
2. Выберите порты Ethernet для НМС.	“Идентификация порта Ethernet, определяемого как eth0” на стр. 97
3. Настройте адаптер Ethernet. Для этого выполните следующие задачи:	
a. Укажите пропускную способность.	“Установка пропускной способности” на стр. 98
b. Выберите тип открытой сети.	“Выбор типа сети (частная, открытая)” на стр. 99
c. Укажите статические адреса.	“Установка IPv4-адреса” на стр. 99
d. Укажите брандмауэр.	“Изменение параметров брандмауэра НМС” на стр. 100

Таблица 54. Настройка НМС для подключения к удаленным пользователям по открытой сети (продолжение)

Задача	Где искать связанную информацию
e. Настройте шлюз по умолчанию.	“Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 101
f. Настройте DNS.	“Настройка служб имен доменов” на стр. 101
g. Настройте суффиксы.	“Настройка доменных суффиксов” на стр. 102
4. Настройте дополнительные адаптеры (если они установлены).	

Настройка параметров сервера НМС для вызова сервисного центра:

Для настройки параметров сервера НМС для вызова сервисного центра и отправки сообщений о неполадках выполните следующие шаги:

Таблица 55. Настройка параметров сервера НМС для вызова сервисного центра

Задача	Где искать связанную информацию
1. Убедитесь, что у вас есть все необходимые сведения о клиенте	“Форма настройки НМС перед установкой” на стр. 84
2. Настройте НМС для отправки сообщений об ошибках или выберите существующий сервер для вызова сервисного центра	“Настройка локальной консоли для отправки сервисному центру сообщений об ошибках” на стр. 104 “Выбор из существующих серверов вызова сервисного центра для соединения со службой поддержки для данной НМС” на стр. 107
3. Убедитесь, что конфигурация вызова сервисного центра функционирует	“Проверка работоспособности соединения с сервисным центром и службой поддержки” на стр. 107
4. Предоставьте пользователям права доступа для просмотра собранных системных данных	“Предоставление пользователям права доступа для просмотра собранных системных данных” на стр. 107
5. Запланируйте передачу системных данных	“Передача служебной информации” на стр. 108

Идентификация порта Ethernet, определяемого как eth0:

Ethernet должна подключаться к управляемому серверу через порт Ethernet, определяемый как eth0 на вашем НМС.

Если в гнездах PCI НМС не установлены дополнительные адаптеры Ethernet, то основной встроенный порт Ethernet НМС всегда определяет как eth0 или eth1 при использовании НМС в качестве сервера DHCP для управляемых систем.

Если дополнительные адаптеры Ethernet в гнездах PCI установлены, то определение порта как eth0 будет зависеть от расположения и типа установленных адаптеров Ethernet.

Примечание: Существуют общие правила, которые в случае некоторых конфигураций могут не выполняться.

В следующей таблице описаны правила размещения адаптеров Ethernet для разных типов НМС.

Таблица 56. Типы НМС и соответствующие правила размещения Ethernet

Тип НМС	Правила размещения Ethernet
Смонтированные в стойке НМС с двумя встроенными портами Ethernet	НМС поддерживает только один дополнительный адаптер Ethernet. - Если дополнительный адаптер Ethernet установлен, то этот порт определяется как eth0. В этом случае первичный встроенный порт Ethernet определяется как eth1, а вторичный встроенный порт Ethernet - как eth2. - В случае двухпортового адаптера Ethernet в качестве порта eth0 обычно определяется порт с обозначением Act/Link A. Порт с обозначением Act/link B будет определен как eth1. Тогда первичный встроенный порт Ethernet определяется как eth2, а вторичный встроенный порт Ethernet - как eth3. - Если же адаптеры не установлены, то основной встроенный порт Ethernet определяется как eth0.
Автономные модели с одним встроенным портом Ethernet	Рассмотренные определения будут зависеть от типа устанавливаемого адаптера Ethernet: - Если установлен только один адаптер Ethernet, то он будет определяться как eth0. - Для двухпортового адаптера Ethernet в качестве порта eth0 будет определен порт с обозначением Act/link A. Порт с обозначением Act/link B будет определен как eth1. При этом основной встроенный порт Ethernet определяется как eth2. - Если ни один адаптер не установлен, то встроенный порт Ethernet определяется как eth0. - Установка нескольких адаптеров Ethernet рассматривается в разделе “Определение имени интерфейса для адаптера Ethernet” на стр. 98.

Определение имени интерфейса для адаптера Ethernet:

При настройке НМС в качестве сервера DHCP этот сервер сможет работать только с соединителями сетевой интерфейсной платы (NIC), которые НМС идентифицирует как eth0 и eth1. Также необходимо выбрать соединитель NIC для подключения кабеля Ethernet. Обратитесь к соответствующей информации по выбору соединителей NIC, которые НМС идентифицирует как eth0 и eth1.

Для того чтобы определить имя, присваиваемое НМС адаптеру Ethernet, выполните следующее:

1. Откройте терминал ограниченной оболочки. Выберите пункт **Управление НМС > Откройте Терминал ограниченной оболочки**.
2. Введите в командную строку следующее: `tail -f /var/log/messages`. Протокол сообщений смещается соответственно новым событиям.
3. Подключите кабель Ethernet. Если кабель уже подключен, отсоедините его, подождите 5 секунд и снова подключите. При подключении кабеля ограниченная оболочка перейдет на вывод некоторого сообщения. Следующий пример записи означает, что этот порт Ethernet идентифицируется как eth0: `Aug 28 12:41:20 termite kernel: e1000: eth0: e1000_watchdog: NIC Link is Up 100.`
4. Выполните эту процедуру для всех остальных портов Ethernet и запишите результаты.
5. Для остановки команды **tail** нажмите Ctrl+C.

Установка пропускной способности:

Знакомит с процессом установки пропускной способности и дуплексного режима адаптера Ethernet.

Стандартным параметром адаптера НМС является **Автоматическое определение**. Если адаптер подключен к коммутатору LAN, то необходимо настроить параметры портов коммутатора. Для настройки пропускной способности и дуплексного режима выполните следующие действия:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. В разделе информации о локальной сети выберите **Автоматическое обнаружение** или укажите пропускную способность и дуплексный режим.
6. Нажмите кнопку **ОК**.

Выбор типа сети (частная, открытая):

Частная сеть обслуживания состоит из НМС и управляемых систем. Частная сеть обслуживания ограничивается консолями и системами, которыми они управляют. Это сеть, отдельная от сети компании. *Открытая сеть* состоит из частной сети обслуживания и сети компании. Кроме консолей и управляемых систем, в открытую сеть могут входить конечные точки сети, и сеть может охватывать несколько подсетей и сетевых устройств.

Для выбора частной или общей сети выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Щелкните на вкладке **Сетевой адаптер**.
6. В разделе Информация о локальной сети выберите **Частная** или **Открытая**.
7. Нажмите кнопку **ОК**.

Настройка НМС в качестве сервера DHCP:

Протокол динамической настройки хостов (DHCP) является автоматическим способом динамической настройки клиента.

Для настройки НМС в качестве сервера DHCP выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**. Откроется окно Настройка параметров сети.
3. Выберите нужный адаптер LAN и нажмите на **Сведения**.
4. Выберите **Частная** и укажите тип сети.

5. В разделе Сервер DHCP включите переключатель **Разрешить сервер DHCP**, чтобы разрешить НМС в качестве сервера DHCP.

Примечание: НМС можно настроить в качестве сервера DHCP только в частной сети. При использовании открытой сети выбрать опцию **Разрешить DHCP** невозможно.

6. Введите диапазон адресов сервера DHCP.
7. Нажмите кнопку **ОК**.

Если НМС настроена в качестве сервера DHCP в частной сети, необходимо проверить правильность настройки частной сети НМС DHCP. Информация о соединении НМС с частной сетью приведена в разделе “Выбор типа сети (частная, открытая)” на стр. 99.

Дополнительные сведения содержатся в разделе “НМС в качестве сервера DHCP” на стр. 75.

Настройка связи ВМС:

Можно настроить или просмотреть сетевые параметры ВМС для консоли управления.

Примечание: Эта задача относится только к 7063-CR1. Это соединение необходимо для подключения к контроллеру управления платформой (ВМС) в НМС.

Для настройки соединения ВМС выполните следующие действия:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети ВМС/IPMI**.
3. Выберите режим соединения (**DHCP** или **Статический**).
Если выбран режим **Статический**, то укажите следующие адреса:
 - **IP-адрес**
 - **Маска подсети**
 - **Шлюз**
4. Нажмите кнопку **ОК**.

Сетевое соединение ВМС можно также настроить с помощью интерфейса загрузчика ядра Petitboot. Дополнительная информация приведена в разделе Настройка IP-адреса встроенного программного обеспечения.

Установка IPv4-адреса:

Знакомит с процессом установки IPv4-адреса на НМС.



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Выберите вкладку **Основные параметры**.
6. Выберите адрес IPv4.

7. Если выбран пункт Указать IP-адрес, введите адрес интерфейса TCP/IP и маску сети интерфейса TCP/IP.
8. Нажмите кнопку **ОК**.

Установка IPv6-адреса:

Описан процесс установки IPv6-адреса на НМС.



1. В области навигации щелкните на значке **Управление НМС консоли**, затем выберите **Параметры**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Выберите вкладку **Параметры IPv6**.
6. Выберите опцию автонастройка или добавьте постоянный IP адрес.
7. При добавлении IP адреса, введите адрес IPv6 и длину префикс, а затем нажмите **ОК**.
8. Нажмите кнопку **ОК**.

Использование только адресов IPv6:

Настройка НМС для использования только адресов IPv6.



1. В области навигации щелкните на значке **Управление НМС консоли**, затем выберите **Параметры**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Выберите **Без адресов IPv4**.
6. Выберите вкладку **Параметры IPv6**.
7. Выберите **Использовать DHCPv6 для настройки параметров IP** или добавьте постоянные IP адреса. Затем нажмите **ОК**.

Для того чтобы изменения вступили в силу необходимо перезагрузить НМС.

Изменение параметров брандмауэра НМС:

В открытой сети брандмауэр обычно используется для управления внешним доступом к сети компании. В НМС также имеется брандмауэр на каждом Ethernet адаптере. Для удаленного управления НМС или предоставления удаленного доступа другим пользователям измените параметры брандмауэра адаптера Ethernet на консоли НМС, подключенной к вашей открытой сети.

Для настройки брандмауэра выполните следующие действия:



1. В области навигации щелкните на значке **Управление НМС консоли**, затем выберите **Параметры**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.

4. Выберите нужный адаптер LAN и нажмите на **Сведения**.
5. Выберите вкладку **Брандмауэр**.
6. С помощью одного из приведенных ниже методов можно разрешить любой IP-адрес, использующий конкретные приложения через брандмауэр, или можно указать один или несколько IP-адресов:
 - Разрешить любой IP-адрес, использующий конкретное приложение через брандмауэр:
 - a. В верхнем окне выделите приложение.
 - b. Выберите **Разрешить входящие**. Приложение появится в нижнем окне - это говорит о том, что приложение выбрано.
 - Укажите IP-адреса, разрешенные через брандмауэр:
 - a. В верхнем окне выделите приложение.
 - b. Выберите **Разрешить входящие по IP-адресу**.
 - c. В окне Разрешенные хосты введите IP-адрес и маску сети.
 - d. Выберите **Добавить** и нажмите кнопку **ОК**.
7. Нажмите кнопку **ОК**.

Включение доступа через удаленную оболочку с ограничениями:

При настройке брандмауэра можно включить доступ через удаленную оболочку с ограничениями.

Для включения доступа через удаленную оболочку с ограничениями выполните следующие действия:

1. В области навигации выберите **Управление НМС**.
2. Выберите **Удаленное выполнение команд**.
3. Выберите **Разрешить удаленное выполнение команд по протоколу ssh** и нажмите кнопку **ОК**.

Доступ через удаленную оболочку с ограничениями включен.

Включение удаленного доступа с помощью веб-браузера:

Можно настроить удаленный доступ к НМС с помощью веб-браузера.

Для включения удаленного доступа с помощью веб-браузера выполните следующие действия:

1. В области навигации выберите **Управление НМС**.
2. Выберите **Удаленная работа**.
3. Выберите **Включить** и нажмите кнопку **ОК**.

Удаленный доступ включен.

Настройка записи маршрутизации в качестве стандартного шлюза:

Знакомит с настройкой записи маршрутизации в качестве стандартного шлюза. Эта задача доступна только для открытой сети.

Для настройки записи маршрутизации в качестве стандартного шлюза выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**. Откроется окно Настройка параметров сети.
3. Выберите вкладку **Маршрутизация**.

4. В области Информация о шлюзе по умолчанию введите адрес и устройства шлюза записи маршрутизации в качестве стандартного шлюза.
5. Нажмите кнопку **ОК**.

Настройка служб имен доменов:

При установке открытой сети настройте службы имен доменов.

При установке открытой сети настройте службы имен доменов. Система имен доменов (DNS) - это распределенная база данных для управления именами хостов и их соответствующими адресами протокола IP (IP-адресами). Для настройки служб имен доменов необходимо включить DNS и указать порядок просмотра доменных суффиксов.



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**. Откроется окно Изменение параметров сети.
3. Выберите вкладку **Службы имен**.
4. Для включения DNS выберите **DNS включено**.
5. Укажите порядок просмотра серверов DNS и доменных суффиксов и нажмите кнопку **Добавить**.
6. Нажмите кнопку **ОК**.

Настройка доменных суффиксов:

Список доменных суффиксов служит для поиска IP-адреса, начиная с первой записи списка.

Доменный суффикс - это строка после имени хоста, которая помогает находить его IP-адрес. Например, имя хоста мое_имя может быть не найдено. Но если в таблице доменных суффиксов присутствует строка myloc.mysompany.com, то сервер попытается найти также myname.mloc.mysompany.com.

Для настройки записи доменного суффикса выполните следующие действия:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**. Откроется окно Настройка параметров сети.
3. Выберите вкладку **Службы имен**.
4. Введите строку в качестве записи доменного суффикса.
5. Выберите **Добавить**, и запись будет добавлена в список.

Настройка НМС для использования удаленной идентификации с помощью LDAP:

Консоль аппаратного обеспечения (НМС) можно настроить для использования удаленной идентификации с помощью LDAP (Упрощенный протокол доступа к каталогам).

Когда пользователь входит в НМС, сначала идентификация осуществляется путем сравнения с локальным файлом пароля. Если локальный файл пароля не обнаружен, НМС может связаться с удаленным сервером LDAP для идентификации. Для использования удаленной идентификации с помощью LDAP необходимо настроить НМС.

Примечание: Прежде чем настраивать НМС для использования удаленной идентификации с помощью LDAP, необходимо убедиться, что существует рабочее сетевое соединение между НМС и серверами LDAP. Дополнительная информация о настройке сетевых соединений НМС приведена в разделе “Настройка типов сетей НМС” на стр. 94.

Для настройки идентификации LDAP в НМС выполните следующие действия:



1. В области навигации щелкните на значке **Пользователи и защита**, затем выберите **Защита систем и консоли**.
2. На панели содержимого выберите **Управление LDAP**. Откроется окно Описание сервера LDAP.
3. Выберите **Включить LDAP**.
4. Укажите сервер LDAP, который будет использоваться при идентификации.
5. Определите атрибут LDAP, используемый для идентификации пользователя. Значение по умолчанию - **uid**, но можно использовать собственное.
6. Определите для сервера LDAP дерево отличительного имени, также известное как база поиска.
7. Нажмите кнопку **ОК**.
8. Если пользователь желает использовать идентификацию с помощью LDAP, он должен настроить свой профайл для использования удаленной идентификации LDAP вместо локальной идентификации.

Настройка НМС для использования Центров рассылки ключей (KDC) для удаленной идентификации Kerberos:

НМС можно настроить для использования Центров рассылки ключей для удаленной идентификации Kerberos

Когда пользователь входит в НМС, сначала идентификация осуществляется путем сравнения с локальным файлом пароля. Если локальный файл пароля не обнаружен, НМС может связаться с удаленным сервером Kerberos для идентификации. Для использования удаленной идентификации Kerberos необходимо настроить НМС.

Примечание: Прежде чем настраивать НМС для использования Центров рассылки ключей для удаленной идентификации Kerberos, необходимо убедиться, что существует рабочее сетевое соединение между НМС и Центрами рассылки ключей. Дополнительная информация о настройке сетевых соединений НМС приведена в разделе “Настройка типов сетей НМС” на стр. 94.

Для настройки НМС выполните следующие действия:

1. Включите службу Протокола сетевого времени (NTP) в НМС и задайте синхронизацию времени серверов НМС и KDC с одним и тем же сервером NTP. Для того чтобы включить службу NTP в НМС выполните следующее:



- a. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
 - b. На панели содержимого выберите **Изменить дату и время**.
 - c. Выберите вкладку **Конфигурация NTP**.
 - d. Выберите **Включить службу NTP** в данной НМС.
 - e. Нажмите кнопку **ОК**.
2. Настройте каждый профайл удаленного пользователя НМС для использования удаленной идентификации Kerberos, а не локальной идентификации.

3. Необязательно: можно импортировать файл служебных ключей в НМС. В файле служебных ключей содержится субъект хоста, идентифицирующий НМС для сервера KDC. Файлы служебных ключей также известны как *keytab*. Для того чтобы импортировать файл служебных ключей в НМС, выполните следующие действия:



- a. В области навигации щелкните на значке **Пользователи и защита**, затем выберите **Защита систем и консоли**.
 - b. На панели содержимого выберите **Управление KDC**.
 - c. Выберите **Действия > Импортировать служебный ключ**. Откроется окно Импорта служебного ключа.
 - d. Введите расположение файла служебного ключа.
 - e. Нажмите кнопку **ОК**.
4. Добавьте новый сервер KDC в НМС. Для этого выполните следующие действия:



- a. В области навигации щелкните на значке **Пользователи и защита**, затем выберите **Защита систем и консоли**.
- b. На панели содержимого выберите **Управление KDC**.
- c. Выберите **Действия > Добавить сервер KDC**. Откроется окно Импорта служебного ключа.
- d. Введите область и имя хоста или IP-адрес сервера KDC.
- e. Нажмите кнопку **ОК**.

Настройка локальной консоли для отправки сервисному центру сообщений об ошибках:

Настройте НМС таким образом, чтобы она могла отправлять сервисному центру сообщения об ошибках с помощью соединений LAN.

Настройка НМС для соединения со службой поддержки с помощью мастера настройки вызова сервисного центра:

Настройте НМС в качестве сервера вызова сервисного центра с помощью мастера.

В этой процедуре описывается, как настроить НМС в качестве сервисного сервера с помощью прямых (на основе LAN) и косвенных (на основе протокола SSL) соединений с Internet.

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Администратор сети проверил, что соединение разрешено. Дополнительные сведения содержатся в разделе “Подготовка к настройке НМС” на стр. 82.
- При настройке поддержки Internet через прокси-сервер также необходимы:
 - IP-адрес и порт прокси-сервера
 - Идентификационные данные сервера Proxu
- Применяется адаптер **eth1** (адаптер, применяемый для подключения к открытой сети). Дополнительные сведения содержатся в разделе “Выбор параметров сети в НМС” на стр. 73.
- Кабель Ethernet физически соединяет НМС с LAN.

Для настройки НМС в качестве сервера вызова сервисного центра с помощью мастера выполните следующие действия:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Мастер настройки вызова сервисного центра**. Откроется мастер соединений и вызова сервисного центра Call-Home. Для настройки вызова сервисного центра Call-Home следуйте инструкциям мастера установки.

Настройка локальной консоли для отправки сервисному центру сообщений об ошибках:

Настройте HMC таким образом, чтобы она могла отправлять сервисному центру сообщения об ошибках с помощью соединений LAN.

Примечание: Виртуальная частная сеть Internet (VPN) и соединение по телефонной линии через модем доступны только в HMC версии 8.2.0 и более ранних версий.

Настройка HMC для связи со службой поддержки через Internet и SSL на основе LAN:

Описывается, как настроить HMC в качестве сервисного сервера с помощью прямых (на основе LAN) и косвенных (на основе протокола SSL) соединений с Internet.

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Администратор сети проверил, что соединение разрешено. Дополнительные сведения содержатся в разделе “Подготовка к настройке HMC” на стр. 82.
- Контактная информация клиента задана. Для проверки нужно воспользоваться интерфейсом HMC и выбрать **Обслуживание > Управление службами > Управление информацией о клиентах**.
- При настройке поддержки Internet через сервер Proxu также необходимы:
 - IP-адрес и порт прокси-сервера
 - Идентификационные данные сервера Proxu
- Необходим по крайней мере один настроенный открытый сетевой интерфейс. Дополнительные сведения содержатся в разделе “Частные и открытые сети в среде HMC” на стр. 75.
- Кабель Ethernet физически соединяет HMC с LAN.

Для настройки HMC в качестве сервисного сервера с помощью Интернета на основе LAN и SSL выполните следующие действия:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
2. В разделе Соединение выберите **Управление исходящими соединениями**. Откроется окно Консоли сервера вызова сервисного центра.
3. Выберите **Настроить**.
4. В окне Параметры исходящих соединений отметьте **Разрешить использование локальной системы в качестве сервисного сервера**.
5. Примите условия соглашения.
6. В окне Параметры исходящих соединений выберите страницу **Интернет**.
7. Поставьте отметку в окне **Разрешить существующие соединения с Internet для обслуживания**.
8. При использовании SSL прокси-сервера поставьте отметку в окне **Использовать SSL прокси-сервер**.
9. Если используется SSL прокси-сервер, введите его адрес и порт. Такую информацию можно получить у администратора системы.

10. Если отмечено окно **Использовать SSL прокси-сервер**, и прокси-сервер требует идентификации по идентификатору и паролю пользователя, поставьте отметку в окне **Идентификация на SSL прокси-сервере**. Введите идентификатор и пароль пользователя. Информацию об ИД и пароле пользователя получите у администратора системы.
11. Выберите **Протокол связи с Internet**, который необходимо использовать.
12. На странице **Интернет** выберите **Проверить**.
13. В окне Тестирование Internet нажмите кнопку **Запустить**.
14. Убедитесь, что проверка была успешно выполнена.
15. В окне Тестирование Internet нажмите кнопку **Завершить**.
16. В окне Параметры исходящих соединений нажмите **ОК**.

Связь со службой поддержки с помощью телефона и модемов:

Описывается, как настроить НМС в качестве сервисного сервера с помощью доступа к службе поддержки IBM через модем.

Примечание: Виртуальная частная сеть Internet (VPN) и соединение по телефонной линии через модем доступны только в НМС версии 8.2.0 и более ранних версий.

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Имеется выделенная аналоговая телефонная линия.
- Имеется информация, необходимая для настройки модема. Дополнительные сведения содержатся в разделе “Подготовка к настройке НМС” на стр. 82.
- Контактная информация клиента задана. Для проверки можно воспользоваться интерфейсом НМС и выбрать **Обслуживание > Управление службами > Управление информацией о клиентах**.
- Убедитесь в наличии следующей информации:
 - Тип аналоговой линии - тональная или импульсная. Большинство линий являются тональными, однако пока еще сохраняются некоторые более старые линии ротационного или импульсного типа.
 - Если при поднятии трубки в линию выдается непрерывный гудок. Большинство телефонов работают с гудком, однако некоторые - без гудка.
 - Если при наборе необходима строка префиксов. Строка префиксов - это номер или последовательность номеров для выхода во внешнюю линию.

Для настройки НМС в качестве сервисного сервера с помощью доступа к службе поддержки IBM через модем выполните следующие действия:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
2. В разделе Соединение выберите **Управление исходящими соединениями**.
3. Нажмите **Настройка**.
4. В окне Параметры исходящих соединений включите переключатель **Разрешить использование локальной системы в качестве сервисного сервера**.
5. Примите условия соглашения.
6. В окне Параметры исходящих соединений выберите вкладку **Локальный модем**.
7. На странице Локальный модем включите переключатель **Разрешить набор номера через локальный модем для обслуживания**.
8. На странице Локальный модем включите переключатель **Конфигурация модема**.

9. В окне Настройка параметров модема выберите **Тип набора - тональный или импульсный**. Если при поднятии трубки в линию выдается непрерывный гудок, включите переключатель **Дождаться гудка**. Введите необходимую строку префиксов набора для выхода во внешнюю линию.
10. Нажмите кнопку **ОК**.
11. На странице Локальный модем нажмите кнопку **Добавить**.
12. Выберите номер из списка.
13. Для местных номеров удалите код области из поля **Номер телефона**.
14. На панели Добавление телефонного номера нажмите кнопку **Добавить**.
15. На панели Настройка параметров модема выберите **Проверка**.
16. На панели Проверка номера телефона нажмите кнопку **Запустить**.
17. Убедитесь, что проверка была успешно выполнена.
18. В окне Проверка номера телефона нажмите кнопку **Завершить**.
19. Можно настроить до пяти телефонных номеров. Рекомендуется настроить, по крайней мере, два телефонных номера (основной и резервный). Попытки соединения с номерами будут выполняться в той же очередности, что и настройка. Для того чтобы добавить номера в список вызываемых номеров, повторите шаги данной процедуры.
20. В окне Параметры исходящих соединений нажмите **ОК**.

Подключение к службе поддержки с помощью VPN на основе LAN:

Настройка сервисного сервера с помощью VPN

Примечание: Виртуальная частная сеть Internet (VPN) и соединение по телефонной линии через модем доступны только в НМС версии 8.2.0 и более ранних версий.

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Администратор сети проверил, что соединение разрешено. Дополнительные сведения содержатся в разделе “Подготовка к настройке НМС” на стр. 82.
- Применяется адаптер **eth1** (адаптер, применяемый для подключения к открытой сети). Дополнительные сведения содержатся в разделе “Выбор параметров сети в НМС” на стр. 73.
- Кабель Ethernet физически соединяет НМС с LAN.
- Контактная информация клиента задана. Для проверки можно выбрать **Обслуживание > Управление службами > Управление информацией о клиентах** в интерфейсе НМС.

Для того чтобы настроить сервисный сервер с помощью VPN, выполните следующие действия:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
2. В разделе Соединение выберите **Управление исходящими соединениями**.
3. Нажмите **Настройка**.
4. В окне Параметры исходящих соединений включите переключатель **Разрешить использование локальной системы в качестве сервисного сервера**.
5. Примите условия соглашения.
6. В окне Параметры исходящих соединений выберите вкладку **Internet**.
7. На странице Интернет через VPN выберите **Разрешить обслуживание по VPN через существующее соединение с Интернетом**.
8. На странице Интернет через VPN включите переключатель **Проверить**.
9. В окне Тестирование Internet VPN нажмите кнопку **Запустить**.

10. Убедитесь, что проверка была успешно выполнена.
11. В окне Тестирование Internet VPN нажмите кнопку **Завершить**.
12. В окне Параметры исходящих соединений нажмите **ОК**.

Выбор из существующих серверов вызова сервисного центра для соединения со службой поддержки для данной НМС:

Выберите из существующих серверов вызова сервисного центра НМС, которые были распознаны, или "обнаружены," данной НМС для отправки отчета об ошибках.

Обнаруженные НМС - это НМС, которые подключены как серверы вызова сервисного центра и либо находятся в той же подсети, либо управляют той же системой, что и данная НМС.

Для того чтобы выбрать обнаруженную НМС для вызова сервисного центра при возникновении ошибок данной НМС, выполните следующее:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Управление исходящими соединениями**. Откроется окно Консоли сервера вызова сервисного центра.
3. Включите переключатель **Использовать обнаруженные консоли сервера вызова сервисного центра**. В НМС будет показан IP-адрес или имя хоста НМС, настроенных для вызова сервисного центра.
4. Нажмите кнопку **ОК**.

Также можно вручную добавить существующие серверы вызова сервисного центра НМС, которые находятся в другой подсети. Выберите IP-адрес или имя хоста НМС, настроенной для вызова сервисного центра и нажмите **Добавить**. Затем нажмите **ОК**.

Проверка работоспособности соединения с сервисным центром и службой поддержки:

Отправка тестовой неполадки для проверки работоспособности соединения с сервисным центром и службой поддержки

Для проверки работоспособности конфигурации вызова сервисного центра выполните следующие действия:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Создать событие**.
3. Выберите **Проверка автоматического создания отчета о неполадках** и введите комментарий.
4. Выберите **Запросить обслуживание**. Дождитесь отправки запроса.
5. В окне Службное управление выберите **Управление событиями**.
6. Выберите **Все сообщенные неполадки**.
7. Проверьте, выбрано ли событие РМН и присвоен ли номер неполадке, о которой Вы сообщили.
8. Выберите это событие и нажмите кнопку **Заккрыть**.
9. В окне Заккрыть введите свое имя и краткое замечание.

Предоставление пользователям права доступа для просмотра собранных системных данных:

Для просмотра данных о системе необходимо предоставить пользователям права доступа.

Прежде чем предоставить пользователям права доступа для просмотра собранных системных данных, необходимо получить ИД IBM. Более подробная информация о получении ИД IBM приведена в разделе “Форма настройки НМС перед установкой” на стр. 84.

Для предоставления пользователям прав доступа для просмотра собранных системных данных выполните следующие действия:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Предоставить пользователю права доступа**.
3. Введите свой ИД IBM.
4. Нажмите кнопку **ОК**.

Передача сервисных данных:

Сведения можно передавать в сервисный центр немедленно или запланировать их регулярную пересылку.

IBM предоставляет персонализированные веб-функции, в которых используется информация, собранная приложением IBM Electronic Service Agent. Для того чтобы иметь возможность пользоваться этими функциями, необходимо вначале зарегистрироваться на веб-сайте регистрации в IBM по адресу <http://www.ibm.com/account/profile>. Для предоставления пользователям права пользования информацией Electronic Service Agent с целью персонализации веб-функций обратитесь к разделу “Предоставление пользователям права доступа для просмотра собранных системных данных” на стр. 107. Более подробная информация о преимуществах регистрации ИД IBM для систем приведена в разделе <http://www.ibm.com/support/electronic>.

Примечание: Как только НМС установлена и настроена, необходимо предоставить информацию для официального сервисного центра.

Для передачи служебной информации выполните следующие действия:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Передать сервисные данные**.
3. Выполните задачи в окне Передача сервисных данных и нажмите **ОК**.

Планирование служебной информации:

Можно запланировать время передачи служебной информации для использования ее в целях выявления неполадок.

Примечание: Как только НМС установлена и настроена, необходимо предоставить информацию для официального сервисного центра.

Для планирования служебной информации выполните следующие действия:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.

2. На панели содержимого выберите **Планирование служебной информации**.
3. На панели содержимого перейдите на вкладку **Планирование и отправка данных**, чтобы запланировать служебную информацию.

Примечание: Кроме того, на следующих вкладках можно выбрать данные для отправки и настроить соединения FTP:

- **Планирование и отправка данных:** информацию о производительности можно отправить в сервисный центр немедленно или запланировать отправку по расписанию.
 - **Отправить отчеты о неполадках:** выберите данные и их назначение.
 - **Настроить соединение FTP:** укажите параметры для загрузки служебной информации по FTP.
4. Выберите типы служебной информации для регулярной или немедленной отправки.
 - **Данные рабочего теста (Пульс) -- всегда включено:** отправьте протокол событий неполадок.
 - **Служебная информация аппаратного обеспечения (VPD):** отправка данных реестра аппаратного обеспечения (VPD) для всех управляемых систем, подключенных к этой НМС.
 - **Служебная информация программного обеспечения:** отправка VPD для программного обеспечения, работающего в разделах.
 - **Информация об управлении производительностью:** сбор и отправка информации об управлении производительностью.
 - **Обновить информацию о ключе доступа:** проверка и обновление информации о ключе доступа.
 5. Выберите интервал (в днях) и время повторяющихся передач. Для немедленной отправки информации нажмите кнопку **Отправить немедленно**.
 6. Нажмите кнопку **ОК**.

Дополнительная информация о планировании служебной информации приведена в электронной справке.

Настройка Администратора событий для вызова сервисного центра:

Рассмотрена настройка задачи Администратор событий для вызова сервисного центра. Эта задача позволяет отслеживать и утверждать данные, передаваемые из НМС в IBM.

Режим Администратор событий для вызова сервисного центра включается и выключается с помощью интерфейса командной строки НМС. Включение задачи Администратор событий для вызова сервисного центра предусматривает выключение автоматического вызова сервисного центра. Для того чтобы запретить вызов сервисного центра без подтверждения, необходимо включить режим Администратор событий для вызова сервисного центра на всех НМС в среде.

Для включения или выключения задачи Администратор событий для вызова сервисного центра выполните следующую команду:

```
chhmc -c emch
```

```
-s {enable | disable}
```

```
[--callhome {enable | disable}]
```

```
[--help]
```

Примечание: Включение задачи Администратор событий для вызова сервисного центра блокирует события вызова сервисного центра до их утверждения для задачи вызова сервисного центра. При выключении задачи Администратор событий для вызова сервисного центра не происходит автоматического включения функции вызова сервисного центра. Такая конфигурация позволяет избежать непреднамеренной передачи данных в IBM. Для задания требуемой конфигурации предусмотрены следующие опции командной строки:

- Включить задачу Администратор событий для вызова сервисного центра: **chhmc -c emch -s enable**

- Выключить задачу Администратор событий для вызова сервисного центра и повторно включить автоматический вызов сервисного центра: **chhmc -c emch -s disable --callhome enable**
- Выключить задачу Администратор событий для вызова сервисного центра без повторного включения автоматического вызова сервисного центра: **chhmc -c emch -s disable --callhome disable**

Убедитесь, что НМС может обмениваться данными с другими НМС, развернутыми в этой среде. В ходе регистрации НМС администратор событий для вызова сервисного центра выполняет проверку связи.

НМС можно зарегистрировать с помощью администратора событий для вызова сервисного центра. После регистрации НМС администратор событий запрашивает в зарегистрированной НМС события, ожидающие вызова сервисного центра IBM. администратор событий отображает данные, отправляемые в IBM, и утверждает события. После утверждения администратор событий разрешает зарегистрированной НМС продолжить операцию вызова сервисного центра.

Задачу Администратор событий для вызова сервисного центра можно запустить из любой НМС или из нескольких НМС. Для регистрации консоли управления в задаче Администратор событий для вызова сервисного центра выполните следующие действия:



1. В области навигации щелкните на значке **Обслуживание**, а затем выберите **Администратор событий для вызова сервисного центра**.
2. На панели **Администратор событий для вызова сервисного центра** выберите **Управление консолями**.
3. В окне **Управление зарегистрированными консолями** выберите **Добавить консоль** для ввода информации для регистрации консоли управления в Администраторе событий для вызова сервисного центра.
4. Нажмите кнопку **ОК**, чтобы сохранить изменения в списке зарегистрированных консолей управления.

Примечание: Администратор событий для вызова сервисного центра может работать, когда режим администратора событий выключен. Вы сможете зарегистрировать НМС и просмотреть события, однако администратор событий не будет управлять отправкой событий в сервисный центр.

Задание паролей для управляемой системы:

Вам необходимо задать пароли как для своего сервера, так и для расширенного интерфейса управления системой (ASM). Использование интерфейса НМС для задания этих паролей описывается далее.

При получении сообщения Ожидание идентификации НМС предлагает пользователю установить пароли для управляемой системы.

Если сообщение Ожидание идентификации не получено, выполните следующие шаги, чтобы установить пароли для управляемой системы.

Обновление пароля сервера:

Для обновления пароля своего сервера выполните следующее:

1. В области навигации выберите управляемую систему и щелкните на значке **Пользователи и защита**



, затем выберите **Пользователи и роли**.

2. Нажмите кнопку **Изменить пароль**. Откроется окно Обновление пароля.
3. Введите требуемую информацию и нажмите **ОК**.

Обновление общего пароля расширенного управления системой (ASM):

Примечание: Пароль по умолчанию для ИД обычного пользователя - `general`, для ИД администратора - `admin`.

Для обновления общего пароля ASM выполните следующее:

1. Выберите управляемую систему в области навигации НМС.
2. В области задач выберите **Операции**.
3. Выберите **Расширенное управление системой (ASM)**. Откроется окно Запуск интерфейса ASM.
4. Выберите IP-адрес служебного процессора и нажмите **ОК**. Откроется интерфейс ASM.
5. На начальной странице ASM1 укажите свой ИД пользователя и пароль и нажмите **Войти в систему**.
6. В области навигации разверните **Профиль входа в систему**.
7. Выберите **Изменить пароль**.
8. Укажите необходимую информацию и нажмите **Продолжить**.

Восстановление пароля администратора расширенного управления системой (ASM):
Для сброса пароля администратора обратитесь в официальный сервисный центр.

Проверка соединения между НМС и управляемой системой:

Этот параметр позволяет проверить правильность соединения с сетью.

Проверку соединения с сетью могут выполнять пользователи со следующими ролями:

- Главный администратор
- Сотрудник сервисного представительства

Для проверки соединения между НМС и управляемой системой выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Параметры консоли**.
2. На панели содержимого выберите **Тест сетевого подключения**.
3. Во вкладке Отправить пробный пакет введите имя хоста или IP-адрес любой системы, с которой нужно установить соединение. Для проверки открытой сети введите имя шлюза. Нажмите кнопку **Проверить связь**.

Проверка связи недоступна, если еще не созданы логические разделы. Для этого можно воспользоваться НМС. Дополнительная информация приведена в разделе Создание логических разделов.

Для того чтобы разобраться, как можно использовать НМС в сети, обратитесь к разделу “Сетевые соединения НМС” на стр. 73.

Дополнительная информация о настройке НМС для соединения с сетью приведена в разделе “Настройка НМС с помощью меню НМС” на стр. 92.

Действия после настройки

После установки и настройки НМС можно создать резервную копию данных НМС.

Резервное копирование наиболее важных данных НМС

Резервную копию важной информации о консоли можно сохранить на флэш-памяти USB, DVD-диске, в удаленной системе или на сервере FTP.

С помощью НМС можно выполнять резервное копирование всех важных данных, например:

- Файлы пользовательских параметров
- Информация пользователей
- Файлы конфигурации платформы НМС
- Файлы протокола НМС
- Обновления НМС через Установку исправлений

Функция резервного копирования сохраняет данные НМС, содержащиеся на жестком диске НМС на следующие носители:

- DVD диск
- флэш-память USB
- Удаленная система, вмонтированная в файловую систему НМС (например, NFS)
- Удаленный сайт с помощью FTP

Резервная копия НМС создается после внесения изменений в НМС или в информацию, связанную с логическими разделами.

Примечание: Прежде чем сохранять данные на съемном носителе, его следует отформатировать. Для форматирования носителя выберите **Управление НМС > Управление консолью > Форматировать носитель** и выполните инструкции.

Резервное копирование НМС могут выполнять пользователи со следующими ролями:

- Главный администратор
- Оператор
- Сотрудник сервисного представительства

Для резервного копирования важнейших данных НМС выполните следующие действия:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
2. На панели содержимого выберите **Резервное копирование данных консоли управления**.
3. Выберите параметры архивации. Резервную копию можно сохранить на носителе в локальной системе, в смонтированной удаленной системе, или можно переслать данные резервной копии на удаленный сайт.
4. Для выполнения этой задачи следуйте инструкциям на экране.

Создание полной резервной копии жесткого диска НМС в удаленной системе

С помощью консоли НМС можно выполнять резервное копирование всего жесткого диска НМС в удаленную систему.

Для этого в удаленной системе должна быть настроена сетевая файловая система (NFS) или защищенная оболочка (ssh), и эта сеть должна быть доступной из НМС. Для выполнения указанной задачи необходимо завершить выполнение и перезагрузить НМС. Эти задачи следует выполнять только с помощью НМС.

Резервное копирование жесткого диска НМС в удаленную систему могут выполнять пользователи со следующими ролями:

- Главный администратор
- Оператор
- Сотрудник сервисного представительства

Для резервного копирования жесткого диска НМС в удаленную систему выполните следующие действия:

1. Запишите номер интерфейса (eth0, eth1 и т. д.), MAC-адрес и IP-адрес каждого сетевого адаптера НМС. Для этого выберите **Управление НМС > Параметры консоли > Изменить параметры сети > Адаптеры LAN**.
2. Завершите работу и отключите питание НМС.
3. Подключите питание консоли НМС, вставив НМС съемный диск восстановления в дисковод DVD. При запуске интерфейса НМС с настроенного сервера загрузки из сети проследите за тем, чтобы в качестве сетевого интерфейса было выбрано одно из устройств, предусмотренных в последовательности запуска. Для просмотра списка загрузочных устройств нажмите F12 после включения питания НМС и выберите требуемый сетевой интерфейс для загрузки.
4. Выберите опцию резервного копирования и нажмите **Далее**.
5. Выберите сетевой интерфейс для обмена данными с удаленным сервером. Если для запуска НМС устанавливается связь с сервером загрузки из сети, и на тот же сервер будет выполняться резервное копирование данных, используйте стандартные параметры. Затем нажмите **Далее** и перейдите к шагу 7. Если стандартные параметры не выбраны, перейдите к следующему шагу.

Примечание: Номер интерфейса (eth0, eth1) может не совпадать с номером, записанным при выполнении шага 1. Для идентификации необходимого интерфейса можно использовать указанный MAC-адрес. Дополнительные сведения содержатся в разделе “Идентификация порта Ethernet, определяемого как eth0” на стр. 97.

6. В этом случае необходимо выбрать сетевой протокол для выбранного интерфейса. Для этого можно получить IP-адрес с сервера DHCP своей сети или назначить статический IP-адрес выбранному сетевому интерфейсу. Выберите нужное и нажмите кнопку **Далее**.
7. Если стандартные параметры не были выбраны, введите IP-адрес или имя хоста удаленного сервера. Резервный файл будет создан с помощью утилиты сжатия gzip и команды **tar**. В поле **Файл на удаленном хосте** укажите файл с расширением .tgz. Если были выбраны стандартные сетевые параметры, в сетевой загрузочной конфигурации нужно использовать настройку каталогов. Такая информация отображается в поле **Файл на удаленном хосте**. После ввода всей обязательной информации нажмите кнопку **Далее**.
8. Выберите требуемый способ переноса данных из НМС на удаленный сервер. Если данные будут зашифрованы, на удаленном хосте должен быть запущен сервер Secure Shell (SSH). При переносе данных без шифрования на удаленном хосте должен быть запущен сетевой файловый сервер (NFS), и должен быть экспортирован каталог, куда будет выполняться резервное копирование данных, для предоставления доступа для записи. Выберите нужное и нажмите кнопку **Далее**.
9. При выборе переноса данных с шифрованием необходимо ввести идентификатор и пароль пользователя удаленного сервера.
10. Проверьте правильность введенной информации и нажмите кнопку **Закончить**. По завершении резервного копирования будет отображен интерфейс НМС.

Если при включении питания НМС была нажата кнопка F1, и последовательность загрузки была изменена, необходимо перегрузить НМС и вновь изменить параметры. При изменении последовательности загрузки проследите за тем, чтобы жесткий диск был указан перед сетевым интерфейсом.

Обновление, модернизация и миграция машинного кода НМС

Для НМС периодически выходят обновления, позволяющие добавить новые возможности и улучшить существующие. В этом разделе приведено различий операций обновления, модернизации и миграции машинного кода НМС. Кроме того, рассмотрены процедуры обновления, модернизации и миграции машинного кода НМС.

После завершения каждой задачи выполняется перезагрузка НМС без остановки разделов.

Обновление кода НМС

Применение пакета обслуживания для текущего уровня НМС.

Не требуется выполнять задачу **Сохранить данные модернизации**.

Модернизация кода НМС

Замена программного обеспечения НМС новым выпуском или уровнем исправления.

Требуется загрузка с носителя восстановления.

Миграция кода НМС

Перемещение данных НМС из одной версии НМС в другую.

Миграция является частным случаем модернизации.

Определение версии и выпуска машинного кода НМС

Информация о том, как определить версию и выпуск машинного кода НМС.

Набор доступных функций, включая оперативное обслуживание встроенного программного обеспечения сервера, а также расширения для модернизации до нового выпуска, определяется уровнем машинного кода НМС.

Для просмотра версии и выпуска машинного кода НМС выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере НМС, включая: версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.

Получение и применение обновлений машинного кода для НМС через Internet-соединение

Знакомит с получением обновлений машинного кода для НМС при наличии соединения с Internet.

Для получения обновлений машинного кода для НМС выполните шаги 1 - 5.

Шаг 1. Убедитесь в наличии соединения с Internet:

Для того чтобы загрузить на НМС или сервер обновления с системы или веб-сайта службы поддержки, необходимо иметь одну из возможностей:

- SSL-соединение с или без SSL proxy
- Internet VPN

Для того чтобы убедиться в наличии соединения с Internet, выполните следующее:



1. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Управление исходящими соединениями**.
3. Откройте вкладку, соответствующую типу исходящего соединения, выбранному для НМС (Internet VPN или SSL-соединение).

Примечание: Если соединение со службой поддержки отсутствует, настройте его перед продолжением выполнения этого сценария. Инструкции по настройке соединения со службой поддержки приведены в разделе Настройка сервера для связи с сервисным центром IBM.

4. Нажмите кнопку **Проверить**.

5. Убедитесь, что проверка была успешно выполнена. Если проверка не была пройдена, устраните неполадку соединения перед продолжением выполнения этой процедуры. Кроме того, можно получить обновление на DVD.
6. Перейдите к “Шаг 2. Просмотр текущего уровня машинного кода НМС”.

Шаг 2. Просмотр текущего уровня машинного кода НМС:

Для просмотра текущего уровня машинного кода НМС выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере НМС, включая: версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Перейдите к “Шаг 3. Просмотр доступных уровней машинного кода НМС”.

Шаг 3. Просмотр доступных уровней машинного кода НМС:

Для просмотра доступных уровней машинного кода НМС выполните следующее:

1. С компьютера или сервера, подключенного к Internet, перейдите на веб-сайт <http://www.ibm.com/eserver/support/fixes>.
2. Выберите нужное семейство серверов в списке Product.
3. Выберите **Hardware Management Console** в списке Product or fix type.
4. Нажмите кнопку **Продолжить**. Будет показан консоли аппаратного обеспечения.
5. Прокрутите список до нужного уровня версии НМС и для просмотра доступных уровней.

Примечание: При необходимости обратитесь в службу поддержки.

6. Перейдите к “Шаг 4. Применение обновления машинного кода НМС”.

Шаг 4. Применение обновления машинного кода НМС:

Для применения обновления машинного кода НМС выполните следующее:

1. Перед установкой обновлений для машинного кода НМС следует создать резервную копию важнейшей информации о консоли на НМС. Соответствующие инструкции приведены в разделе “Резервное копирование наиболее важных данных НМС” на стр. 110. Затем перейдите к следующему шагу.



2. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
3. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**. Откроется окно Установка исправления.
4. Следуйте инструкциям по установке обновления.
5. Для того чтобы обновления вступили в силу, завершите работу и перезапустите НМС.
6. Выберите **Войти и запустить веб-приложение Консоль аппаратного обеспечения**.
7. Войдите в интерфейс НМС.

Шаг 5. Проверка правильности установки обновления машинного кода НМС:

Для проверки правильности установки обновления машинного кода НМС выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере НМС, включая: версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Убедитесь, что версия и выпуск совпадают с версией установленного обновления.
5. Если показана другая версия кода, выполните следующие действия:
 - a. Выберите сетевое соединение в НМС.
 - b. Повторно обновите встроенное программное обеспечение, используя другое хранилище.
 - c. Если ошибка возникнет снова, обратитесь на следующий уровень поддержки.

Получение и применение обновлений машинного кода для НМС на DVD или через сервер FTP

Знакомит с получением обновлений машинного кода на DVD или через сервер FTP.

Для получения обновлений машинного кода НМС выполните шаги 1 - 5.

Шаг 1. Просмотр текущего уровня машинного кода НМС:

Для просмотра текущего уровня машинного кода НМС выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере НМС, включая: версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Перейдите к “Шаг 2. Просмотр доступных уровней машинного кода НМС”.

Шаг 2. Просмотр доступных уровней машинного кода НМС:

Для просмотра доступных уровней машинного кода НМС выполните следующее:

1. На компьютере или сервере с подключением к Интернету откройте веб-страницу консоли программного обеспечения <http://www-933.ibm.com/support/fixcentral/>.
2. Прокрутите список до нужного уровня версии НМС и для просмотра доступных уровней.

Примечание: При необходимости обратитесь в службу поддержки IBM .

3. Перейдите к “Шаг 3. Получение обновления машинного кода НМС”.

Шаг 3. Получение обновления машинного кода НМС:

Для получения обновления машинного кода НМС выполните следующее:

Обновление машинного кода НМС можно заказать на веб-сайте Fix Central или в службе поддержки. Кроме того, его можно загрузить на сервер FTP.

Заказ обновления машинного кода НМС через веб-сайт Fix Central

1. На компьютере или сервере с подключением к Интернету откройте веб-страницу консоли программного обеспечения <http://www-933.ibm.com/support/fixcentral/>.
2. В продуктах, поддерживаемых НМС, выберите последний уровень НМС.

3. Прокрутите страницу вниз до области File name(s) / Package area и найдите обновление, которое требуется заказать.
4. В столбце Заказ выберите **Перейти**.
5. Щелкните на ссылке **Continue** для получения идентификатора IBM.
6. Для того чтобы отправить заказ, следуйте инструкциям, появляющимся на экране.

Загрузка обновления машинного кода НМС на съемные носители

1. На компьютере или сервере с подключением к Интернету откройте веб-страницу консоли программного обеспечения <http://www-933.ibm.com/support/fixcentral/>.
2. В продуктах, поддерживаемых НМС, выберите последний уровень НМС.
3. Прокрутите страницу вниз до области Имя (имена) файла / Пакетная область и найдите обновление, которое требуется загрузить.
4. Выберите обновление, которое требуется загрузить.
5. Примите условия лицензионного соглашения и сохраните обновление на съемном носителе.

По окончании перейдите к “Шаг 4. Применение обновления машинного кода НМС”.

Шаг 4. Применение обновления машинного кода НМС:

Для применения обновления машинного кода НМС выполните следующее:

1. Перед установкой обновлений для машинного кода НМС создайте резервную копию данных НМС. Дополнительная информация приведена в разделе “Резервное копирование наиболее важных данных НМС” на стр. 110
2. Если вы получили или создали обновление на DVD-RAM, вставьте его в дисковод DVD на консоли НМС. Если вы получили или создали обновление на накопителе USB, то установите его.
3. Перед установкой обновлений для машинного кода НМС следует создать резервную копию важнейшей информации о консоли на НМС. Соответствующие инструкции приведены в разделе “Резервное копирование наиболее важных данных НМС” на стр. 110. Затем перейдите к следующему шагу.



4. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
5. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**. Откроется окно Установка исправления.
6. Следуйте инструкциям по установке обновления.
7. Для того чтобы обновления вступили в силу, завершите работу, перезапустите и вновь войдите на НМС.
8. Перейдите к “Шаг 5. Проверка правильности установки обновления машинного кода НМС”.

Шаг 5. Проверка правильности установки обновления машинного кода НМС:

Для проверки правильности установки обновления машинного кода НМС выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере НМС, включая: версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Убедитесь, что версия и выпуск совпадают с версией установленного обновления.
5. Если показана другая версия кода, выполните следующие действия:

- a. Повторно обновите машинный код. Если для выполнения этой процедуры был создан диск DVD, замените его.
- b. Если ошибка возникнет снова, обратитесь на следующий уровень поддержки.

Модернизация программного обеспечения НМС

Знакомит с модернизацией программного обеспечения на НМС до следующего выпуска с сохранением данных конфигурации НМС.

Для обновления машинного кода в НМС выполните шаги 1 - 9.

Шаг 1. Получение модернизации:

Обновление машинного кода НМС можно заказать на веб-сайте Fix Central.

Для того чтобы получить обновление с веб-сайта Fix Central, выполните следующие действия:

1. На компьютере или сервере с подключением к Интернету откройте веб-страницу консоли программного обеспечения <http://www-933.ibm.com/support/fixcentral/>.
2. Нажмите кнопку **Продолжить**. Будет показан консоли аппаратного обеспечения.
3. Найдите версию НМС, которую вы хотите обновить.
4. Найдите раздел загрузки и заказа.

Примечание: Если у вас нет доступа к Internet, закажите обновление на DVD в службе сопровождения и поддержки IBM.

5. Для того чтобы отправить заказ, следуйте инструкциям, появляющимся на экране.
6. Получив обновление, перейдите к шагу “Шаг 2. Просмотр текущего уровня машинного кода НМС”.

Шаг 2. Просмотр текущего уровня машинного кода НМС:

Для определения текущего уровня машинного кода НМС выполните следующие действия:



1. В области навигации щелкните на значке **Управление НМС** , затем выберите **Управление консолью**. В области навигации выберите **Обновления**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере НМС, включая: версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Перейдите к “Шаг 3. Создание резервной копии данных профайла управляемой системы”.

Шаг 3. Создание резервной копии данных профайла управляемой системы:

Для того чтобы скопировать данные профайлов управляемой системы, выполните следующее:

1. области навигации выберите **Управление системами**.
2. Выберите **Серверы**.
3. Выберите сервер, который должен иметь состояние *Рабочий* или *Резервный*.
4. В разделе Задачи выберите **Настройка > Управление данными о разделах > Резервное копирование**.
5. Введите и запишите имя файла с резервной копией.
6. Нажмите кнопку **ОК**.
7. Повторите шаги для каждой управляемой системы.
8. Перейдите к “Шаг 4. Резервное копирование данных НМС”.

Шаг 4. Резервное копирование данных НМС:

Перед установкой новой версии программного обеспечения НМС следует выполнить резервное копирование данных НМС; это позволит восстановить предыдущие версии программного обеспечения в случае ошибок в процессе модернизации ПО. После успешной установки новой версии программного обеспечения НМС сохраненную информацию применять не следует.

Примечание: Для сохранения данных консоли на съемном носителе необходимо предварительно подготовить соответствующий носитель.

Для резервного копирования данных НМС выполните следующее:

1. Если резервную копию предполагается создать на съемном носителе, отформатируйте носитель:
 - a. Вставьте носитель в накопитель.



- b. В области навигации щелкните на значке **Обслуживание**, затем выберите **Управление обслуживанием**.
 - c. На панели содержимого выберите **Форматирование носителя**.
 - d. Выберите тип носителя.
 - e. Выберите тип форматирования.
 - f. Нажмите кнопку **ОК**.



2. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
3. На панели содержимого выберите **Резервное копирование данных консоли управления**. Откроется окно резервного копирования данных консоли управления.
4. Выберите параметры архивации. Резервную копию можно сохранить на носителе в локальной системе, в удаленной системе, смонтированной в файловой системе НМС, (например, NFS) или отправить на удаленный сервер FTP.
 - Для создания резервной копии на носителе выберите **Сохранить на носителе в локальной системе** и следуйте показанным инструкциям.
 - Для создания резервной копии в смонтированной удаленной системе выберите **Сохранить в смонтированной удаленной системе** и следуйте показанным инструкциям.
 - Для создания резервной копии на сервере FTP выберите **Отправить резервную копию важнейших данных на удаленный сервер** и следуйте показанным инструкциям.
5. Перейдите к “Шаг 5. Запись информации о текущей конфигурации НМС”.

Шаг 5. Запись информации о текущей конфигурации НМС:

Перед обновлением версии программного обеспечения НМС в качестве меры предосторожности следует записать информацию о конфигурации НМС.

Для регистрации существующей конфигурации НМС выполните следующее:

1. Для просмотра запланированных операций для управляемой системы или ее логических разделов откройте **Управление НМС > Управление консолью**. Если требуется записать запланированные операции для самой НМС, выберите **Управление НМС > Управление консолью**, затем перейдите к шагу 3.
2. Выберите управляемую систему и разделы, для которых необходимо записать сведения о конфигурации НМС.
3. В списке задач выберите **Запланировать операции**. Будут показаны все запланированные операции для выбранного целевого объекта.
4. Выберите **Сортировать > По объекту**.
5. Последовательно выберите каждый объект и запишите следующие сведения:

- Имя объекта
- Запланированная дата
- Время выполнения (в 24-часовом формате)
- Повторяющийся (если указано значение Да, выполните следующие действия):
 - a. Выберите **Вид > Сведения о расписании**.
 - b. Запишите информацию об интервале.
 - c. Закройте окно запланированных операций.
 - d. Повторите эти действия для каждой запланированной операции.
- 6. Закройте окно Настроить запланированные операции.
- 7. Перейдите к “Шаг 6. Запись состояния удаленной команды”.

Шаг 6. Запись состояния удаленной команды:

Для регистрации состояния удаленной команды выполните следующее:

1. В области навигации выберите **Управление НМС**.
2. В списке задач выберите **Удаленное выполнение команд**.
3. Запишите состояние переключателя **Разрешить удаленное выполнение команд по протоколу ssh**.
4. Нажмите **Отмена**.
5. Перейдите к “Шаг 7. Сохранение данных модернизации”.

Шаг 7. Сохранение данных модернизации:

Текущую конфигурацию НМС можно сохранить в выделенном разделе диска НМС или на локальном носителе. Данные об обновлении необходимо сохранять непосредственно перед переходом к следующему выпуску программного обеспечения НМС. Такой подход позволяет восстановить параметры конфигурации НМС после обновления.

Примечание: Сохранить можно только одну резервную копию. Каждый раз при сохранении данных обновления предыдущие данные удаляются.

Для того чтобы сохранить данные обновления, выполните следующее:



1. В области навигации щелкните на значке **Управление НМС** , затем выберите **Управление консолью**.
2. На панели содержимого выберите **Сохранить данные обновления**. Откроется мастер сохранения данных обновления.
3. Выберите носитель для сохранения данных обновления. Если выбран съемный носитель, то установите его. Нажмите кнопку **Далее**.
4. Нажмите кнопку **Закончить**.
5. Дождитесь завершения задачи. Если задача Сохранить данные обновления не будет выполнена, обратитесь на следующий уровень поддержки.

Примечание: Если задача сохранения данных обновления не будет выполнена, процесс обновления следует приостановить.

6. Нажмите кнопку **ОК**.
7. Перейдите к “Шаг 8. Модернизация программного обеспечения НМС”.

Шаг 8. Модернизация программного обеспечения НМС:

Для модернизации программного обеспечения НМС перезапустите систему, установив в дисковод DVD съемный носитель.

1. Вставьте установочный диск продукта НМС в дисковод DVD.



2. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
3. На панели содержимого выберите **Выключение или перезапуск консоли управления**.
4. Проследите за тем, чтобы был выбран пункт **Перезапустить НМС**.
5. Нажмите кнопку **ОК**. В ходе перезапуска НМС в окне прокручивается системная информация.
6. Выберите **Обновить** и нажмите кнопку **Далее**.
7. Выберите один из вариантов:
 - Если данные обновления были сохранены при выполнении предыдущей задачи, перейдите к следующему шагу.
 - Если данные обновления не были сохранены, перед продолжением их следует сохранить.
8. Выберите **Обновить с носителя** и нажмите кнопку **Далее**.
9. Подтвердите параметры и нажмите кнопку **Готово**.
10. Следуйте инструкциям.

Примечание:

- Если экран станет пустым, для просмотра информации нажмите пробел.
 - Установка первого DVD может занять приблизительно 20 минут.
11. В приглашении входа в систему введите ИД пользователя и пароль. Установка кода НМС завершена.
 12. Перейдите к “Шаг 9. Проверка правильности установки модернизации машинного кода НМС”.

Шаг 9. Проверка правильности установки модернизации машинного кода НМС:

Для проверки правильности установки обновления НМС выполните следующее:



1. В области навигации щелкните на значке **Управление НМС**, затем выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере НМС, включая: версию НМС, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Убедитесь, что версия и выпуск совпадают с версией установленного обновления.
5. Если показана другая версия кода, повторите операцию с другим диском DVD. Если ошибка возникнет снова, обратитесь на следующий уровень поддержки.

Обновление НМС из удаленного расположения с помощью образов сетевого обновления

Инструкции по обновлению программного обеспечения НМС из удаленного расположения с помощью образов сетевого обновления.

Инструкции по обновлению программного обеспечения НМС из удаленного расположения с помощью образов сетевого обновления. Приведены инструкции по обновлению НМС уровня V6R1.2 или более высокого, включая все уровни НМС V7.

1. С компьютера или сервера, подключенного к Internet, перейдите на веб-сайт Консоль аппаратного обеспечения (<http://www14.software.ibm.com/webapp/set2/sas/f/netinstall/v7770network.html>)

2. Загрузите подходящие сетевые образы НМС V7 и сохраните их на сервере FTP. Эти файлы нельзя загрузить непосредственно в НМС. Файлы образов необходимо загрузить на сервер, принимающий запросы FTP.
3. Загрузите следующие файлы:
 - `img2a`
 - `img3a`
 - `base.img`
 - `disk1.img`
 - `hmcnetworkfiles.sum`
4. Сохраните данные обновления в НМС. Выполните следующие строки команды для сохранения данных обновления:
 - Для сохранения данных на диске DVD и жестком диске выполните следующие команды:
`mount /media/cdrom`
`saveupgdata -r diskdvd`
 - Для сохранения данных на жестком диске выполните следующую команду:
`saveupgdata -r disk`
5. Скопируйте файлы обновления в загрузочный раздел диска НМС. Выполните команду **`getupgfiles`** для копирования файлов.
Пример: **`getupgfiles -h <сервер ftp> -u <ИД пользователя> -d <удаленный каталог>`**
Где,
 - **сервер ftp** - это имя хоста или IP-адрес сервера FTP, содержащий сетевые образы НМС.
 - **ИД пользователя** - это допустимый ИД пользователя на сервере FTP. Если пароль не указан в аргументе `--passwd`, то он будет запрошен.
 - **удаленный каталог** - это каталог на сервере FTP, в котором сохранены сетевые образы НМС.
6. Перезагрузите НМС, чтобы обновить код, скопированный в раздел загрузочного диска. Выполните команду **`chhmc -c altdiskboot -s enable --mode upgrade`** для перезапуска НМС.
7. Перезагрузите НМС и начните обновление. Выполните команду **`hmcshutdown -r -t now`** для запуска процедуры обновления.

Расположения портов НМС

Расположения компонентов можно найти с помощью кодов расположений. Диаграммы расположений портов НМС помогают сопоставить код расположения с положением порта НМС на сервере.

Расположения портов НМС модели 8247-21L, 8247-22L, 8284-21A или 8284-22A

С помощью этой диаграммы можно найти порты НМС в системе 8247-21L, 8247-22L, 8284-21A или 8284-22A.

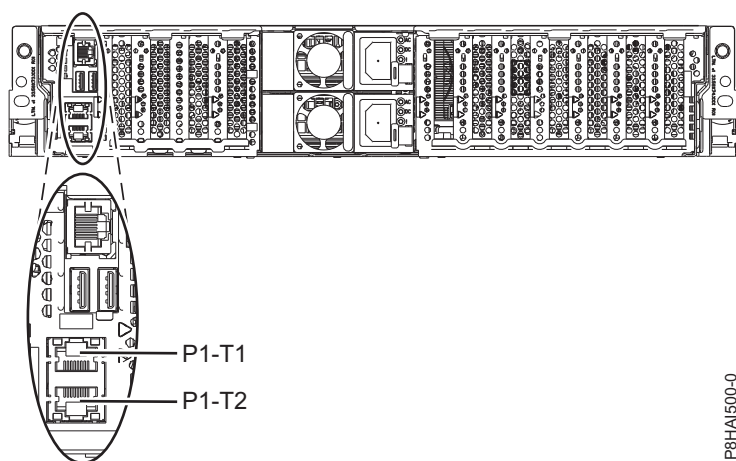


Рисунок 85. Расположения портов НМС 8247-21L, 8247-22L, 8284-21A или 8284-22A

Таблица 57. Расположения портов НМС 8247-21L, 8247-22L, 8284-21A или 8284-22A

Порт	Код физического расположения	Индикатор идентификации
Порт НМС 1	Un-P1-T1	Нет
Порт НМС 2	Un-P1-T2	Нет
Дополнительная информация о расположениях портов НМС в системе 8247-21L, 8247-22L, 8284-21A или 8284-22A приведена в разделе Расположение компонента и коды расположений для 8247-21L, 8247-22L или 8284-22A .		

Расположения портов НМС модели 8247-42L, 8286-41A и 8286-42A

С помощью этой диаграммы можно найти порты НМС в системе 8247-42L, 8286-41A или 8286-42A.

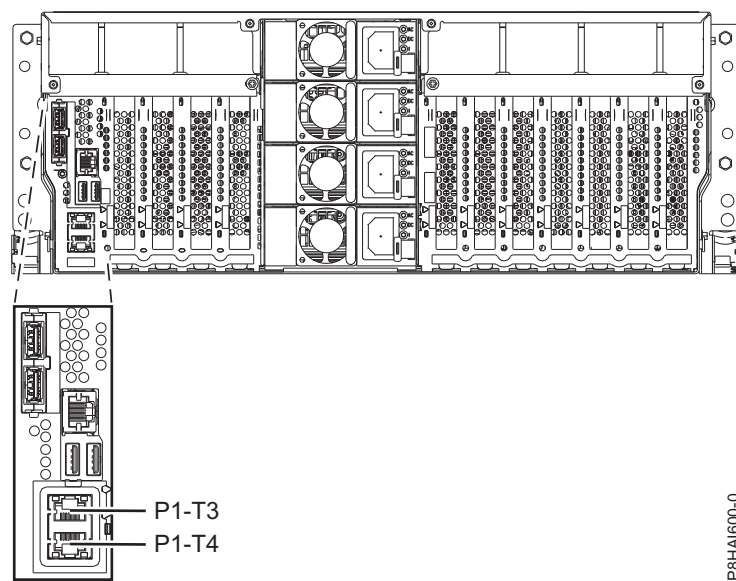


Рисунок 86. Стойка - расположения портов НМС 8247-42L, 8286-41A и 8286-42A

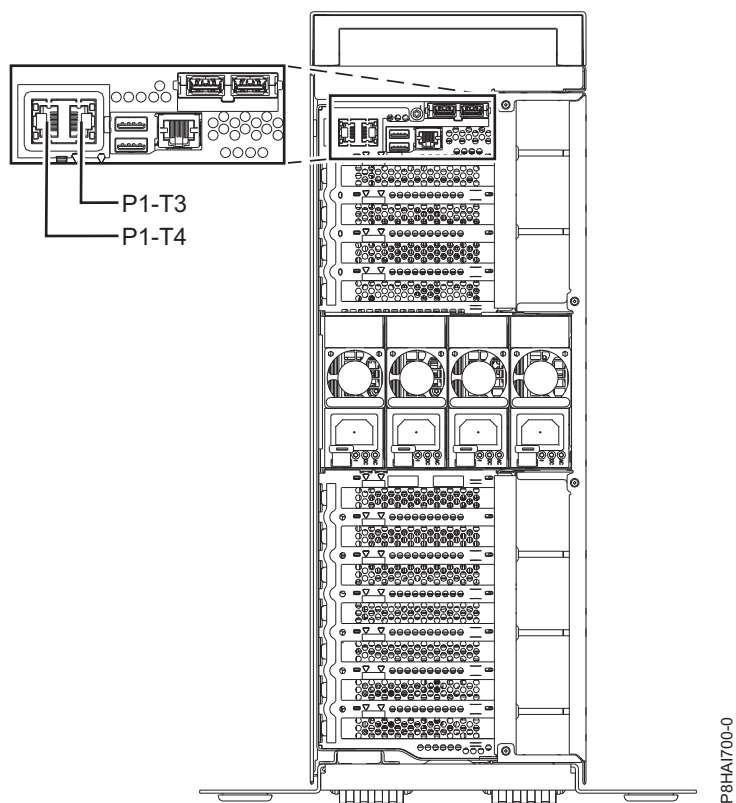


Рисунок 87. Расположения портов НМС для 8286-41А в виде системного блока

Таблица 58. Расположения портов НМС 8247-42L, 8286-41А и 8286-42А

Порт	Код физического расположения	Индикатор идентификации
Порт НМС 1	Un-P1-T3	Нет
Порт НМС 2	Un-P1-T4	Нет
Дополнительная информация о расположении портов НМС в системе 8247-42L, 8286-41А или 8286-42А приведена в разделе Расположение компонента и коды расположений для 8247-42L, 8286-41А и 8286-42А.		

Расположения портов НМС модели 9080-МНЕ, 9080-ММЕ,9119-МНЕ и 9119-ММЕ

С помощью этой диаграммы и таблицы можно найти порты НМС в системе 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ.

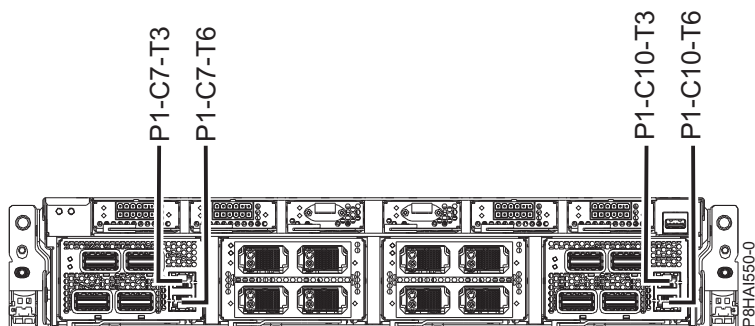


Рисунок 88. Расположения портов НМС 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ

Таблица 59. Расположения портов НМС 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ

Порт	Код физического расположения	Индикатор идентификации
Карта служебного процессора 1 - порт НМС 1	Un-P1-C7-T3	Нет
Карта служебного процессора 1 - порт НМС 2	Un-P1-C7-T6	Нет
Карта служебного процессора 2 - порт НМС 1	Un-P1-C10-T3	Нет
Карта служебного процессора 2 - порт НМС 2	Un-P1-C10-T6	Нет
Дополнительная информация о расположении портов НМС в системах 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ приведена в разделе Расположение компонента и коды расположений для 9080-МНЕ, 9080-ММЕ, 9119-МНЕ и 9119-ММЕ.		

Расположения портов НМС модели 8408-44Е и 8408-Е8Е

С помощью этой диаграммы и таблицы можно найти порты НМС в системе 8408-44Е или 8408-Е8Е.

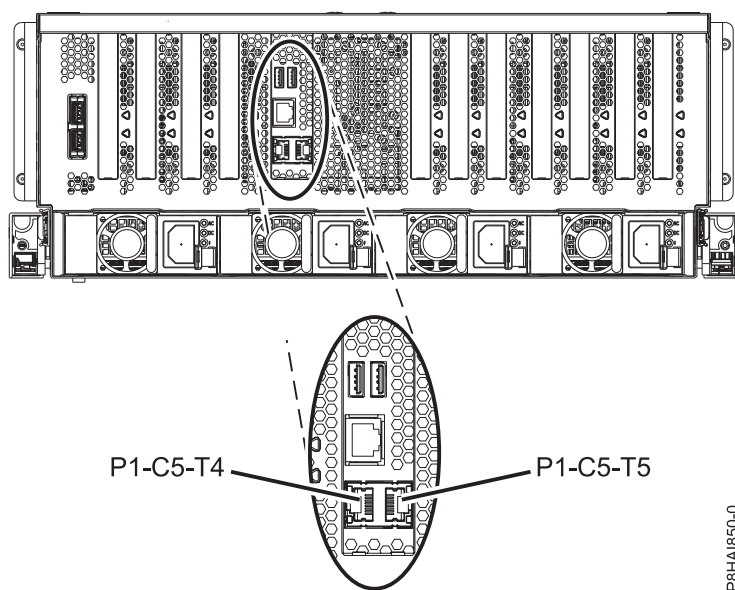


Рисунок 89. Расположения портов НМС 8408-44Е и 8408-Е8Е

Таблица 60. Расположения портов НМС 8408-44Е и 8408-Е8Е

Порт	Код физического расположения	Индикатор идентификации
Порт НМС 1	Un-P1-C5-T4	Нет
Порт НМС 2	Un-P1-C5-T5	Нет
Дополнительная информация о расположении портов НМС в системах 8408-44Е и 8408-Е8Е приведена в разделе Расположение компонента и коды расположений для 8404-44Е и 8408-Е8Е.		

Примечания

Данная информация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предоставлять продукты и услуги, обсуждаемые в данном документе, в других странах. Информацию о продуктах и услугах, распространяемых в вашей стране, можно получить в местном представительстве IBM. Ссылки на продукты, программы или услуги фирмы IBM не означают, что можно использовать только указанные продукты, программы или услуги фирмы IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако ответственность за оценку и проверку работоспособности любого продукта, программы или услуги, полученной от другого поставщика, лежит на пользователе.

IBM могут принадлежать рассматриваемые заявки на патенты или патенты на информацию, упомянутую в данном документе. Получение настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий направляйте в письменной форме по следующему адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ ДАННУЮ ПУБЛИКАЦИЮ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ) ПРЕДПОЛАГАЕМЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ АВТОРСКИХ ПРАВ, РЫНОЧНОЙ ПРИГОДНОСТИ ИЛИ СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ. В некоторых странах для ряда сделок не допускается отказ от явных или предполагаемых гарантий; в таком случае данное положение к вам не относится.

В данной публикации могут встретиться технические неточности и типографские опечатки. В приведенную информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления вносить улучшения и изменения в продукты и программы, описанные в настоящей публикации.

Любые ссылки в этой публикации на веб-сайты других фирм предоставлены только для удобства и не служат никоим образом в качестве поддержки этих веб-сайтов. Материалы, размещенные на этих веб-сайтах, не являются частью материалов для настоящего продукта IBM и ответственность за их применение лежит на пользователе.

IBM оставляет за собой право использовать или распространять любую предоставленную вами информацию любым способом по своему усмотрению без каких-либо обязательств перед вами.

Данные о производительности и примеры клиентов приведены исключительно иллюстративных целях. Фактические показатели производительности могут отличаться в зависимости от конкретной конфигурации и условий эксплуатации.

Информация о продуктах, выпущенных сторонними компаниями, была получена от поставщиков этих продуктов, из опубликованных документах или других общедоступных источников. IBM не тестировала подобные продукты и не может подтвердить точность сведений о производительности, совместимости и других заявленных характеристиках. Вопросы о функциях продуктов других фирм должны быть направлены поставщикам этих продуктов.

Заявления о будущих действиях или намерениях IBM могут быть изменены или аннулированы без предупреждения и должны рассматриваться исключительно как заявления о предполагаемых целях.

Все указанные цены являются рекомендуемыми розничными ценами IBM, эти цены текущие и могут быть изменены без соответствующего уведомления. Цены поставщиков могут от них отличаться.

Данная информация предназначена исключительно для целей планирования. Она может быть изменена до того, как будут выпущены описанные в ней продукты.

Эта информация содержит примеры данных и отчетов, применяемых в повседневной работе. Для большего правдоподобия эти примеры снабжены именами и фамилиями, названиями фирм, торговых марок и продуктов. Все эти имена являются вымышленными и любое сходство с настоящими лицами или предприятиями полностью случайно.

В электронной версии настоящей информации могут отсутствовать фотографии и цветные изображения.

Запрещается полностью или частично воспроизводить содержащиеся в этом документе рисунки и спецификации без письменного разрешения IBM.

Эта информация подготовлена IBM для использования с указанными компьютерами. IBM не утверждает, что данная публикация пригодна для каких-либо иных целей.

Компьютерные системы IBM содержат механизмы, разработанные для снижения вероятности невыевленного повреждения или потери данных. Однако этот риск не может быть исключен полностью. Пользователи, сталкивающиеся с незапланированными остановками, неполадками систем, нестабильностью или отключениями питания или отказами компонентов, должны убеждаться в надежности выполняемых операций и сохранения или передачи данных системой во время или перед отключением или отказом. Кроме того, пользователи должны учредить процедуры по обеспечению независимой проверки данных перед применением к этим данным критичных или сомнительных операций. Пользователям следует регулярно заходить на веб-сайты поддержки IBM изготовителя получения обновленной информации или исправлений, относящихся к системе и связанному программному обеспечению.

Заявление о сертификации

Этот продукт может быть не сертифицирован в вашей стране для подключения любыми средствами к интерфейсам общедоступных телекоммуникационных сетей. Может потребоваться дополнительная сертификация перед установкой такого подключения. Обратитесь к представителю IBM или посреднику по любым вопросам.

Специальные возможности серверов IBM Power Systems

Специальные возможности облегчают работу с информационными технологиями пользователям с физическими ограничениями, например с ограниченной подвижностью или плохим зрением.

Обзор

Серверы IBM Power Systems предлагают следующие специальные возможности:

- Работа только с клавиатурой
- Операции, выполняемые с помощью программы чтения с экрана

Серверы IBM Power Systems используют последний стандарт W3C WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) для обеспечения соответствия требованиям раздела 508 (США) (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) и Web Content Accessibility

Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Для поддержки специальных возможностей требуется последний выпуск программы чтения с экрана и последняя версия веб-браузера из числа поддерживаемых серверами IBM Power Systems.

Документация по серверам IBM Power Systems в справочной системе IBM Knowledge Center поддерживает специальные возможности. Функции специальных возможностей IBM Knowledge Center описаны в разделе Специальные возможности справочной системы IBM Knowledge Center (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Навигация с помощью клавиатуры

В данном продукте применяются стандартные клавиши навигации.

Информация об интерфейсе

В пользовательских интерфейсах серверов IBM Power Systems отсутствует информация, которая мигает с частотой 2 - 55 раз в секунду.

В пользовательском веб-интерфейсе серверов IBM Power Systems для вывода информации и взаимодействия с пользователем применяются таблицы CSS. Приложение обеспечивает поддержку пользователей с ограниченным зрением, используя параметры экрана системы, в том числе режим высокой контрастности. Размер шрифта можно изменить с помощью параметров устройства или веб-браузера.

В пользовательском веб-интерфейсе серверов IBM Power Systems применяются навигационные ориентиры WAI-ARIA, позволяющие быстро перемещаться между функциональными областями приложения.

Программное обеспечение других поставщиков

Серверы IBM Power Systems могут включать другое программное обеспечение, не входящее в лицензионное соглашение IBM. IBM не гарантирует совместимость с этими продуктами. О возможности использования этих продуктов консультируйтесь с поставщиком.

Связанная информация для специальных возможностей

В дополнение к стандартным веб-сайтам службы поддержки IBM оказывает информационные услуги по вопросам поддержки и приобретения через службу телетайпа для глухих и плохо слышащих заказчиков:

Служба телетайпа
800-IBM-3383 (800-426-3383)
(Северная Америка)

Дополнительная информация о стратегии IBM в отношении специальных возможностей приведена на веб-странице IBM Accessibility (www.ibm.com/able).

Замечания о правилах работы с личными данными

Продукты IBM Software, включающие решения Программа как услуга, (“Предложения программ”) могут использовать cookie или другие технологии сбора информации об использовании продукта для помощи в усовершенствовании интерфейса конечного пользователя, для организации взаимодействия с конечным пользователем или для других целей. В большинстве случаев Предложения программ не собирают персональную информацию. Некоторые из наших предложений программ могут помочь вам в сборе персональной информации. Если данное предложение программ использует cookie для сбора персональной информации, ниже приведены сведения об использовании cookie в данном предложении.

В зависимости от развернутых конфигураций, данное Предложение программ может использовать сеансовые cookie, собирающие имя и IP-адрес для каждого пользователя с целью управления сеансом. Эти cookie можно отключить, но их отключение приведет к потере функциональности, которые они обеспечивают.

Если развернутые конфигурации данного Предложения программ предоставляют вам как клиенту возможность сбора персональной информации от конечных пользователей с помощью cookie и других технологий, необходимо проконсультироваться с юристом о законах, применимых к сбору таких данных, включая требования о замечаниях и согласии.

Дополнительная информация об использовании для этих целей различных технологий, включая cookie, приведена в документе Заявление IBM о конфиденциальности по адресу <http://www.ibm.com/privacy>, а также в документе Заявление IBM о конфиденциальности в Интернете по адресу <http://www.ibm.com/privacy/details> и в разделах “Cookie, Web Beacon и другие технологии” и “Заявление IBM о конфиденциальности в отношении программных продуктов и программного обеспечения, предоставляемого в качестве услуги (SaaS)” на странице <http://www.ibm.com/software/info/product-privacy>.

Товарные знаки

IBM, эмблема IBM и [ibm.com](http://www.ibm.com) являются зарегистрированными товарными знаками корпорации International Business Machines во многих странах мира. Имена других продуктов и услуг могут быть товарными знаками IBM и других компаний. Текущий список товарных знаков IBM приведен на следующем веб-сайте: Информация об авторских правах и товарных знаках (www.ibm.com/legal/copytrade.shtml).

Linux является зарегистрированным товарным знаком Линуса Торвальдса (Linus Torvalds) в США и/или других странах.

Microsoft и Windows являются торговыми марками Microsoft в США и/или других странах.

Замечания об уровне электронного излучения

При подключении монитора к оборудованию следует использовать требуемый кабель монитора и устройства подавления помех, поставляемые вместе с монитором.

Информация о классе A

Следующие заявления об оборудовании класса A относятся к серверам IBM с процессорами POWER8 и их компонентам, если в описании компонента не указано, что он относится к классу B электромагнитной совместимости (EMC).

Заявление о соответствии требованиям Федеральной комиссии по связи (FCC)

Примечание: Данное оборудование было протестировано на соответствие требованиям, предъявляемым к цифровым устройствам класса A в соответствии с частью 15 спецификаций FCC, и было признано соответствующим всем предъявляемым требованиям. Эти требования обеспечивают защиту от вредного излучения при работе оборудования в нежилых помещениях. Это оборудование генерирует, использует и излучает радиоволны. Если оборудование установлено не в соответствии с прилагаемым руководством, то оно может приводить к возникновению радиопомех. При эксплуатации данного оборудования в жилых помещениях весьма вероятно возникновение помех, влияние которых в этом случае заказчик должен устранить самостоятельно.

Для того чтобы данное оборудование соответствовало ограничениям на излучение, установленным FCC, необходимо пользоваться только правильно экранированными и заземленными кабелями и соединителями. IBM не несет ответственности за любые помехи в радио- и телевизионном сигнале, вызванные применением кабелей и разъемов, отличных от рекомендуемых, или внесением несанкционированных изменений или

модификаций в это оборудование. В случае несанкционированного изменения или модификации пользователю может быть запрещено работать с оборудованием.

Данное устройство соответствует части 15 спецификаций FCC. Оно удовлетворяет следующим условиям: (1) устройство не вызывает опасные помехи и (2) устройство может работать в условиях внешних помех, в том числе таких, которые могут повлиять на его работу.

Соответствие стандартам для Канады

CAN ICES-3 (A)/NMB-3(A)

Соответствие стандартам Европейского Сообщества

Данное изделие соответствует защитным требованиям Директивы ЕС 2014/30/EU по электромагнитной совместимости с учетом законов государств-членов ЕС. Компания IBM не несет ответственности за любое несоответствие требованиям защиты в результате нереконмендованного изменения продукта, включая использование дополнительных плат других изготовителей.

Адрес Европейского сообщества:
IBM Deutschland GmbH
Technical Regulations, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Телефон: +49 800 225 5426
Электронная почта: halloibm@de.ibm.com

Предупреждение: Это устройство класса А. В домашних условиях данный продукт может вызвать электромагнитные помехи, которые могут потребовать от пользователя принять соответствующие меры.

Заявление о соответствии требованиям VCCI - Япония

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Ниже приведен сокращенный вариант положения о соответствии данного изделия нормам VCCI, принятым в Японии (полный вариант положения на японском языке приведен выше):

Это устройство класса А соответствует стандартам организации VCCI. При установке в жилых помещениях оно может вызывать радиопомехи. В этом случае пользователь должен самостоятельно предпринять необходимые меры.

Заявление Японской ассоциации электронной промышленности и информационных технологий

Описание заявления Japan JIS C 61000-3-2 о соответствии мощности устройств.

(一社) 電子情報技術産業会 高調波電流抑制対策実施
要領に基づく定格入力電力地 : See Knowledge Center

Описание заявления Японской ассоциации электронной промышленности и информационных технологий (JEITA) для устройств с током не более 20 А на фазу.

高周波電流規格 JIS C 61000-3-2 適合品

Описание заявления JEITA для устройств с током более 20 А на фазу.

高周波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 6（単相、P F C回路付）
- 換算係数 : 0

Описание заявления JEITA для устройств с током более 20 А на фазу, три фазы.

高周波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5（3相、P F C回路付）
- 換算係数 : 0

Соответствие нормам ограничения электромагнитных помех - Китайская Народная Республика

声 明

此为 A 级产品,在生活环境中,该产品可能会造成无线电干扰。在这种情况下,可能需要用户对其干扰采取切实可行的措施。

Заявление: Это устройство класса А. При установке в жилых помещениях оно может привести к возникновению радиопомех. В этом случае пользователь должен самостоятельно предпринять необходимые меры.

Соответствие нормам ограничения электромагнитных помех - Тайвань

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Ниже приведен сокращенный вариант положения о соответствии данного изделия нормам электромагнитного излучения, принятым на Тайване (полный вариант положения приведен выше).

Внимание: Это устройство класса А. При установке в жилых помещениях оно может привести к возникновению радиопомех. В этом случае пользователь должен самостоятельно предпринять необходимые меры.

Контактная информация IBM, Тайвань

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Заявление об электромагнитных помехах (EMI) - Республика Корея

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

Соглашение для Германии

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 / EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 / EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Телефон: +49 (0) 800 225 5426
Электронная почта: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 / EN 55032 Klasse A.

Соответствие нормам ограничения электромагнитных помех - Россия

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

Информация о классе В

Следующие заявления об оборудовании класса В относятся к компонентам с электромагнитной совместимостью (EMC) класса В в описании установки компонента.

Заявление о соответствии требованиям Федеральной комиссии по связи (FCC)

Данное оборудование было протестировано на соответствие требованиям, предъявляемым к цифровым устройствам класса В в соответствии с частью 15 спецификаций FCC, и было признано соответствующим всем предъявляемым требованиям. Эти требования обеспечивают защиту от вредного излучения при работе оборудования в жилых помещениях.

Это оборудование генерирует, использует и может излучать энергию частоты радиоволн, и оно может вызвать помехи в системах радиосвязи, если установлено и используется не в соответствии с инструкциями. Однако, нет гарантии, что помехи не возникнут в определенных установках.

Если это оборудование вызывает помехи в радио и телевизионном приеме, что может быть определено включением и выключением этого оборудования, пользователь может попытаться исправить ситуацию одной или несколькими из следующих мер:

- Изменить ориентацию или расположение принимающей антенны.
- Увеличить расстояние между оборудованием и приемником.
- Подключить оборудование к розетки из другого контура сети, чем тот, к которому подключен приемник.
- Для получения справки обратитесь к официальному дилеру IBM или в сервисное представительство.

Для того чтобы данное оборудование соответствовало ограничениям на излучение, установленным FCC, необходимо пользоваться только правильно экранированными и заземленными кабелями и соединителями. Нужные модели кабелей и соединителей можно приобрести у официальных дилеров IBM. IBM не несет ответственности за теле- и радиопомехи, вызванные несанкционированным изменением или модификацией этого оборудования. В случае несанкционированного изменения или модификации пользователь может потерять право работать с оборудованием.

Это устройство соответствует стандартам части 15 Правил FCC. Работа устройства подчиняется следующим двум ограничениям: (1) устройство не создает помехи; (2) устройство воспринимает любые помехи, включая те, которые могут вызвать нарушения в его работе.

Заявление о соответствии производственным нормам Канады

CAN ICES-3 (B)/NMB-3(B)

Заявление о соответствии директивам Европейского сообщества (ЕС)

Данное изделие соответствует защитным требованиям Директивы ЕС 2014/30/EU по электромагнитной совместимости с учетом законов государств-членов ЕС. Компания IBM не несет ответственности за любое несоответствие требованиям защиты в результате нереконмендованного изменения продукта, включая использование дополнительных плат других изготовителей.

Контактные данные для Европейского Сообщества:

IBM Deutschland GmbH

Technical Regulations, Abteilung M456

IBM-Allee 1, 71139 Ehningen, Germany

Телефон: +49 800 225 5426

email: halloibm@de.ibm.com

Соответствие стандартам VCCI в Японии

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCI-B

Заявление Японской ассоциации электронной промышленности и информационных технологий

Описание заявления Japan JIS C 61000-3-2 о соответствии мощности устройств.

**(一社) 電子情報技術産業会 高調波電流抑制対策実施
要領に基づく定格入力電力地：See Knowledge Center**

Описание заявления Японской ассоциации электронной промышленности и информационных технологий (JEITA) для устройств с током не более 20 А на фазу.

高周波電流規格 JIS C 61000-3-2 適合品

Описание заявления JEITA для устройств с током более 20 А на фазу.

高周波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 6（単相、P F C回路付）
- 換算係数 : 0

Описание заявления JEITA для устройств с током более 20 А на фазу, три фазы.

高周波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5（3相、P F C回路付）
- 換算係数 : 0

Контактная информация IBM, Тайвань

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Соответствие стандартам для Германии

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022/ EN 55032 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse B

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Телефон: +49 (0) 800 225 5426
Электронная почта: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022/ EN 55032 Klasse B.

Положения и условия

Разрешение на использование этих публикаций предоставляется в соответствии со следующими условиями.

Применимость: Данные условия и соглашения дополняют любые условия использования, опубликованные на веб-сайте IBM.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать эти публикации в рамках своей организации при условии сохранения информации об авторских правах. Эти публикации, а также любую их часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

Права: Относительно самих публикаций и упоминаемых в них информации, данных, программного обеспечения и иной интеллектуальной собственности не предоставляются никакие явные или подразумеваемые разрешения, лицензии и права, за исключением явно указанных в этом разрешении.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в случае, если, по мнению IBM, использование этих публикаций может принести ущерб его интересам или если будет установлено, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА СОДЕРЖАНИЕ ЭТИХ ПУБЛИКАЦИЙ. ПУБЛИКАЦИИ ПРЕДОСТАВЛЯЮТСЯ НА УСЛОВИЯХ "КАК ЕСТЬ" БЕЗ КАКИХ БЫ ТО НИ БЫЛО ГАРАНТИЙ, И В ЧАСТНОСТИ БЕЗ ПРЕДПОЛАГАЕМЫХ ГАРАНТИЙ КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ РЕШЕНИЯ КАКИХ БЫ ТО НИ БЫЛО ЗАДАЧ.



Напечатано в Дании