Erweitertes BladeCenter-Managementmodul
Erweitertes BladeCenter T-Managementmodul

Benutzerhandbuch

Erweitertes BladeCenter-Managementmodul
Erweitertes BladeCenter T-Managementmodul

Benutzerhandbuch

Hinweis

Lesen Sie vor Verwendung dieser Informationen und des darin beschriebenen Produkts die allgemeinen Informationen im Abschnitt „Hilfe und technische Unterstützung anfordern", auf Seite 221, den Abschnitt „Bemerkungen" auf Seite 225 und das Dokument mit den Informationen zum Herstellerservice sowie die Broschüre mit Sicherheitshinweisen und das Benutzerhandbuch mit Hinweisen zur Wiederverwertbarkeit auf der IBM Dokumentations-CD.

Siebenundzwanzigste Ausgabe (April 2013)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM BladeCenter Advanced Management Module, BladeCenter T Advanced Management Module, User's Guide,
IBM Teilenummer 00V9999,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
TSC Germany
Kst. 2877
April 2013

Inhaltsverzeichnis

Kapitel 1. Das BladeCenter-Managementmodul

Dieses *Benutzerhandbuch zum Managementmodul* enthält Informationen zum Konfigurieren des Managementmoduls und zum Verwalten der Komponenten, die in einer IBM® BladeCenter-Einheit installiert sind. Informationen zum Konfigurieren anderer Managementmodule als dem erweiterten Managementmodul finden Sie in einem separaten Dokument.

Zwar weisen alle Managementmodultypen ähnliche Funktionen auf, ihre physischen Attribute können sich jedoch voneinander unterscheiden. Informationen zu Steuerelementen und Anzeigen sowie zur Installation, Verkabelung und Konfiguration von Managementmodulen finden Sie im *Installationshandbuch* Ihres Managementmoduls.

Alle IBM BladeCenter-Einheiten werden in diesem Dokument als BladeCenter-Einheit bezeichnet. Alle Managementmodule werden in diesem Dokument als Managementmodul bezeichnet. Sofern nicht anders angegeben, können alle Befehle auf allen Typen von Managementmodulen und BladeCenter-Einheiten ausgeführt werden.

- Befehle mit der Bezeichnung „(nur BladeCenter H)" können auf allen Typen von BladeCenter H-Einheiten ausgeführt werden (BladeCenter H und BladeCenter HT).
- Befehle mit der Bezeichnung „(nur BladeCenter T)" können auf allen Typen von BladeCenter T-Einheiten ausgeführt werden (BladeCenter T und BladeCenter HT).

Das Managementmodul stellt Systemverwaltungsfunktionen und KVM-Multiplexing (Keyboard, Video, Mouse - Tastatur, Bildschirm, Maus) für alle Blade-Server in der BladeCenter-Einheit bereit, die KVM unterstützen. Es steuert die externen Verbindungen mit Tastatur, Maus und Bildschirm zur Verwendung über eine lokale Konsole und eine Ethernet-Fernverwaltungsverbindung mit 10/100 Mb/s.

Jede BladeCenter-Einheit beinhaltet mindestens ein Managementmodul. Einige BladeCenter-Einheiten unterstützen die Installation eines zweiten sogenannten Bereitschaftsmanagementmoduls. Nur eines der Managementmodule in einer BladeCenter-Einheit kann jeweils die BladeCenter-Einheit steuern. Bei diesem Managementmodul handelt es sich dann um das primäre Managementmodul. Wenn ein Bereitschaftsmanagementmodul installiert ist, wird es erst dann zur Steuerung der BladeCenter-Einheit herangezogen, wenn das primäre Managementmodul ausfällt und die Steuerung entweder manuell oder automatisch dem Bereitschaftsmanagementmodul übergeben wird, damit es als primäres Managementmodul fungieren kann.

Wenn in einer BladeCenter-Einheit zwei Managementmodule installiert sind, müssen sie vom selben Typ sein. Das erweiterte Managementmodul ist für eine Installation in derselben BladeCenter-Einheit mit anderen Managementmodultypen nicht kompatibel. Bevor die Steuerung vom primären zum Bereitschaftsmanagementmodul umgeschaltet werden kann, müssen die beiden Managementmodule dieselben Firmwareversionen aufweisen und in einigen Fällen auch dieselbe IP-Adresse. Die Firmwareversion muss redundante Managementmodule unterstützen, um die Umstellung der Steuerung vom primären (aktiven) Managementmodul zum Bereit-

schaftsmanagementmodul zu ermöglichen. Die aktuelle Firmwareversion für das Managementmodul ist unter der folgenden Adresse verfügbar: http://www.ibm.com/systems/support/.

Anmerkung: Nach einer Funktionsübernahme können Sie möglicherweise für die Dauer von fünf Minuten keine Netzverbindung zum Managementmodul herstellen.

Der Serviceprozessor im Managementmodul führt zu allen Serviceprozessoren in den einzelnen Blade-Servern eine Datenübertragung durch, um bestimmte Funktionen zu unterstützen, wie beispielsweise Einschaltanforderungen, Fehler- und Ereignisberichte, KVM-Anforderungen und Anforderungen zur Verwendung des gemeinsam genutzten BladeCenter-Laufwerkschlittens (Laufwerk für austauschbare Datenträger und USB-Anschlüsse).

Anmerkung: Das erweiterte Managementmodul verfügt über zwei USB-Anschlüsse. Wenn Sie eine USB-Speichereinheit in einem der Anschlüsse installieren, können die Blade-Server in der BladeCenter-Einheit diese Speichereinheit ebenfalls verwenden. Folgende Regeln legen fest, welcher Blade-Server die USB-Speichereinheit erkennt:

1. Bei BladeCenter- und BladeCenter T-Einheiten wird die USB-Speichereinheit an den Blade-Server angehängt, der der Eigner der KVM ist.
2. Bei BladeCenter H- oder HT-Einheiten wird die USB-Speichereinheit an den Blade-Server angehängt, der der Eigner des Laufwerkschlittens ist.

Sie konfigurieren die BladeCenter-Komponenten mithilfe des Managementmoduls und legen dabei Parameter oder Werte, wie zum Beispiel IP-Adressen, fest. Das Managementmodul führt zu allen Komponenten in der BladeCenter-Einheit eine Datenübertragung durch, erkennt, ob sie vorhanden sind, berichtet über ihren Status und sendet bei bestimmten Fehlerbedingungen Alerts, falls erforderlich.

Anmerkung: Die Anzeigen und Seiten in den Beispielen in diesem Dokument können von den Anzeigen und Seiten, die auf Ihrem Bildschirm angezeigt werden, geringfügig abweichen. Der Inhalt hängt vom Typ der BladeCenter-Einheit, die Sie verwenden, sowie von den Firmwareversionen und den installierten Zusatzeinrichtungen ab.

Referenzliteratur

Referenzliteratur für das *Benutzerhandbuch zum BladeCenter-Managementmodul* ist auf der Dokumentations-CD und unter http://www.ibm.com/systems/support/ verfügbar.

Neben diesem *Benutzerhandbuch* befinden sich möglicherweise die folgenden Dokumente im PDF-Format (Portable Document Format) auf der Dokumentations-CD, die mit dem BladeCenter-Managementmodul geliefert wird. Je nach BladeCenter-Produkt kann die Dokumentations-CD auch zusätzliche Dokumente enthalten. Die aktuellen Versionen aller BladeCenter-Dokumente finden Sie unter der Adresse http://www.ibm.com/systems/support/.

- *Sicherheitsinformationen*

  Dieses Dokument enthält Übersetzungen der Hinweise vom Typ "Vorsicht" und "Gefahr". Jeder Hinweis vom Typ "Vorsicht" und "Gefahr" in der vorliegenden Dokumentation ist mit einer Nummer versehen, mit der Sie den entsprechenden Hinweis in Ihrer Sprache in der Broschüre mit Sicherheitshinweisen auffinden können.

- *Installationshandbuch zum Managementmodul*

  Jedes Managementmodul verfügt über ein spezielles *Installationshandbuch*, das Anweisungen für das Installieren des Managementmoduls in einer BladeCenter-Einheit und für das Erstellen der Erstkonfiguration enthält. Dieses Dokument umfasst auch die Informationen zu Sicherheit und Herstellerservice, die speziell für dieses Managementmodul gelten.

- *Referenzhandbuch zur Befehlszeilenschnittstelle des erweiterten BladeCenter-Managementmoduls*

  In diesem Dokument wird die Verwendung der Befehlszeilenschnittstelle des Managementmoduls für den direkten Zugriff auf BladeCenter-Verwaltungsfunktionen erklärt. Dieser Zugriff stellt eine Alternative zur Verwendung der webbasierten Benutzerschnittstelle dar. Die Befehlszeilenschnittstelle ermöglicht auch den Zugriff auf die Textkonsolen-Eingabeaufforderung auf jedem Blade-Server über eine SOL-Verbindung (Serial over LAN).

- *Nachrichtenhandbuch zum erweiterten BladeCenter-Managementmodul*

  Dieses Dokument enthält zusätzliche Informationen zu Ereignisbenachrichtigungen des erweiterten Managementmoduls, zu Nachrichten im Ereignisprotokoll des erweiterten Managementmoduls und zu den Schritten, die Sie zur Behebung von Fehlern an einem BladeCenter-Gehäuse durchführen können.

- *Installations- und Benutzerhandbuch zu IBMSMASH Proxy*

  Dieses Dokument enthält einen Überblick über die Entstehung, Merkmale und Komponenten des SMASH-CLP-Standards (SMAHS - Systems Management Architecture for Server Hardware, CLP - Command-Line Protocol) und dessen Beziehung zum IBM SMASH-Produkt. Außerdem bietet dieses Dokument einen detaillierten Überblick über SMASH Proxy und SMASH Embedded, einschließlich Konfiguration, Funktionalität, Barrierefreiheit, Merkmale und Komponenten.
- *SOL-Installationshandbuch zu IBMBladeCenter*

  In diesem Dokument wird die Aktualisierung und Konfiguration der BladeCenter-Komponenten für den SOL-Betrieb (Serial over LAN) beschrieben. Die SOL-Verbindung ermöglicht einen Zugriff auf die Textkonsolen-Eingabeaufforderung auf jedem Blade-Server und sorgt dafür, dass die Blade-Server von einem fernen Standort aus verwaltet werden können.

Lesen Sie neben der Dokumentation in dieser Bibliothek das *Planungs- und Installationshandbuch zu IBM BladeCenter* für Ihre BladeCenter-Einheit. Darin finden Sie Informationen, die Ihnen bei der Vorbereitung der Systeminstallation und -konfiguration helfen. Dieses Dokument ist unter der folgenden Adresse verfügbar: http://www.ibm.com/systems/support/.

IBM Redbooks werden von der IBM International Technical Support Organization (ITSO) entwickelt und veröffentlicht. Die ITSO entwickelt Kenntnisse, technisches Know-how und Materialien und stellt diese für IBM Techniker, Geschäftspartner, Kunden und den allgemeinen Markt bereit. Sie finden die veröffentlichten IBM Redbooks für Ihr BladeCenter unter der Adresse http://www.redbooks.ibm.com/portals/bladecenter.

Lizenzschlüssel für Funktionen, die Sie für Ihre BladeCenter-Einheit erworben haben, erhalten Sie unter der Adresse http://licensing.datacentertech.net.

Bemerkungen und Hinweise in diesem Dokument

Durch die Bemerkungen und Hinweise in diesem Dokument sollen bestimme Informationen besonders hervorgehoben werden.

Die Hinweise vom Typ "Vorsicht" und "Gefahr" in diesem Dokument finden Sie auch in der mehrsprachigen *Broschüre mit Sicherheitshinweisen* auf der Dokumentations-CD zu IBM BladeCenter. Die Hinweise sind nummeriert, um ein rasches Auffinden der entsprechenden Hinweise in der Broschüre mit Sicherheitshinweisen zu ermöglichen.

In diesem Dokument finden Sie die folgenden Bemerkungen und Hinweise:

- **Anmerkung:** Diese Bemerkungen enthalten wichtige Tipps, Anleitungen oder Ratschläge.
- **Wichtig:** Diese Bemerkungen enthalten Informationen oder Ratschläge, die Ihnen helfen können, mögliche Schwierigkeiten oder Fehler zu vermeiden.
- **Achtung:** Diese Bemerkungen weisen auf die Gefahr der Beschädigung von Programmen, Einheiten oder Daten hin. Eine Bemerkung vom Typ "Achtung" befindet sich direkt vor der Anweisung oder der Beschreibung der Situation, die diese Beschädigung bewirken könnte.
- **Vorsicht:** Diese Hinweise weisen auf Situationen hin, von denen eine Gefährdung für Sie ausgehen könnte. Ein Hinweis vom Typ "Vorsicht" befindet sich direkt vor der Beschreibung eines potenziell gefährlichen Prozedurschritts oder einer potenziell gefährlichen Situation.
- **Gefahr:** Diese Hinweise weisen auf eine extreme Gefährdung des Benutzers hin. Ein Hinweis vom Typ "Gefahr" befindet sich direkt vor der Beschreibung eines Prozedurschritts oder einer Situation, die tödliche oder schwere Verletzungen zur Folge haben können.

Kapitel 2. Webschnittstelle des Managementmoduls verwenden

In den folgenden Abschnitten werden die Verfahren beschrieben, mit denen Sie eine Verbindung zur Webschnittstelle des Managementmoduls herstellen und diese Webschnittstelle starten, konfigurieren und verwenden.

- „Verbindung zum Managementmodul herstellen"
- „Webschnittstelle des Managementmoduls starten" auf Seite 13
- „Managementmodul konfigurieren" auf Seite 16
- „Kommunikation mit der IBM Systems Director-Software" auf Seite 26
- „Erweiterte Funktionen" auf Seite 27
- „E/A-Modul konfigurieren" auf Seite 95

Eine ausführliche Beschreibung zu Struktur und Inhalt der Webschnittstelle des Managementmoduls finden Sie in Kapitel 3, „Überblick über die Webschnittstelle des Managementmoduls", auf Seite 99. Sie können Funktionen der Webschnittstelle auch ausführen, indem Sie die Befehlszeilenschnittstelle des Managementmoduls und den SMASH-CLP-Standard verwenden. Informationen und Anweisungen dazu finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des BladeCenter-Managementmoduls* und im *Installations- und Benutzerhandbuch zu IBM SMASH Proxy*.

Verbindung zum Managementmodul herstellen

Sie können über einen angegebenen Web-Browser auf das Managementmodul zugreifen und es verwalten.

Zum Konfigurieren und Verwalten der Betriebsfunktionen der BladeCenter-Einheit ist eine ferne Konsolenverbindung zum Managementmodul erforderlich. Alle Managementmodultypen unterstützen Verbindungen über den Anschluss für Fernverwaltung und die ferne Konsole (Ethernet). Das erweiterte Managementmodul unterstützt außerdem Verbindungen nur durch die Befehlszeilenschnittstelle über den seriellen Managementanschluss.

Sie können die BladeCenter-Einheit und die Blade-Server, die KVM unterstützen, mithilfe der grafischen Benutzerschnittstelle verwalten, die von der Webschnittstelle des Managementmoduls bereitgestellt wird, oder mithilfe der Befehlszeilenschnittstelle, auf die Sie durch Telnet zugreifen. Sie können auch über einen SSH-Server (Secure Shell) oder den seriellen Anschluss des erweiterten Managementmoduls auf die Befehlszeilenschnittstelle zugreifen. Alle Verwaltungsverbindungen zu Blade-Servern, die KVM nicht unterstützen, erfolgen über die Befehlszeilenschnittstelle (nur Text) des Managementmoduls.

Sie können die Erstkonfiguration des Managementmoduls ausführen, nachdem Sie es an Ihr Netz angeschlossen haben. Aufgrund einiger Anforderungen in den Standardeinstellungen des Managementmoduls ist es jedoch möglicherweise einfacher, diese Konfiguration mithilfe einer temporären Verbindung vorzunehmen.

Dieser Abschnitt enthält die folgenden Informationen:

- „Überblick über die Verbindungen des Managementmoduls"
- „Verkabelung des Managementmoduls" auf Seite 10
- „Erstmalig eine Verbindung zum Managementmodul herstellen" auf Seite 11

Nachdem die Erstverkabelung und -konfiguration abgeschlossen ist, können Sie über einen Standard-Web-Browser zum Managementmodul navigieren. Weitere Informationen finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13.

Überblick über die Verbindungen des Managementmoduls

Der Zugriff auf die Webschnittstelle des Managementmoduls erfolgt über ein Netz oder einen Computer, der direkt mit dem Managementmodul verbunden ist.

Um eine ferne Konsole mit der Webschnittstelle des Managementmoduls zu verbinden, benötigen Sie folgende Geräte und Informationen:

- Einen Computer mit Web-Browser-Funktionalität. Sie können einen Notebook-Computer verwenden, um Verbindungen an mehreren Standorten zu ermöglichen.
- Die MAC-Adresse des Managementmoduls (Medium Access Control), die sich auf dem Etikett am Managementmodul befindet, wenn Sie die IP-Adresse des Managementmoduls auf einem DHCP-Server nachschlagen müssen.
- Für Netzverbindungen zum Managementmodul benötigen Sie folgende Geräte:
  - Ein handelsübliches Ethernet-Kabel
  - Einen lokalen Ethernet-Netzanschluss (Einrichtungsverbindung)
- Für Direktverbindungen zwischen einem Computer und dem Anschluss für Fernverwaltung und ferne Konsole (Ethernet) des Managementmoduls können Sie entweder ein handelsübliches Ethernet-Kabel oder ein gekreuztes Ethernet-Kabel verwenden.

Durch Verbindungen über den seriellen Anschluss des erweiterten Managementmoduls können Sie nur auf die Befehlszeilenschnittstelle des Managementmoduls zugreifen. Informationen zum Zugreifen auf die Befehlszeilenschnittstelle des Managementmoduls finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des erweiterten BladeCenter-Managementmoduls*.

Hardwarevoraussetzungen

Die Komponenten des Client-Computers müssen mindestens die folgenden Leistungsstufen aufweisen, um die Fernsteuerungsfunktion verwenden zu können, die den KVM-Zugriff (über Tastatur, Bildschirm und Maus) auf einen Blade-Server ermöglicht:

- Mikroprozessor: Intel Pentium III oder höher mit 700 MHz oder mehr (oder einen anderen, funktional entsprechenden Mikroprozessor)
- Speicher: 256 MB Arbeitsspeicher
- Video: 16 MB RADEON 7500 ATI Mobility-Videochipsatz oder einen funktional entsprechenden Chipsatz (AGP 4X mit 16 MB Bildspeicher)

Die folgende Tabelle listet die einzigen für Blade-Server angegebenen Kombinationen aus Bildschirmauflösung und Bildwiederholfrequenzen für die mit KVM ausgestatteten Blade-Server auf, die bei allen Systemkonfigurationen unterstützt werden. Sofern nicht anders angegeben, gelten diese Einstellungen für alle Managementmodultypen.

Auflösung	**Bildwiederholfrequenz**
640 x 480	60 Hz
640 x 480	72 Hz
640 x 480	75 Hz
640 x 480	85 Hz
800 x 600	60 Hz
800 x 600	72 Hz
800 x 600	75 Hz
800 x 600	85 Hz
1024 x 768	60 Hz
1024 x 768	70 Hz
1024 x 768	75 Hz

Softwarevoraussetzungen

Das Managementmodul unterstützt die folgenden Web-Browser für den (Client-) Fernzugriff:

- Microsoft Internet Explorer 6.0 oder höher (mit installiertem aktuellen Service-Pack)
- Mozilla Firefox Version 1.07 oder höher

Anmerkung: Die Webschnittstelle des E/A-Moduls wird nur von Mozilla Firefox Version 1.07 oder höher unterstützt.

Die ferne Konsole (Fernsteuerung) wird von Java™ Runtime Environment (JRE) Version 6.0 mit Update 10 oder höher unterstützt. JRE ist unter der Adresse http://www.java.com/ verfügbar. Das Plug-in für Java Virtual Machine (JVM) ist Bestandteil von JRE. Die auf einem Client-Computer installierten JRE- und JVM-Versionen müssen übereinstimmen: Stellen Sie sicher, dass keine anderen JRE- oder JVM-Versionen installiert sind.

Im Folgenden sind die Mindestversionen der Serverbetriebssysteme mit USB-Unterstützung aufgelistet. Diese Unterstützung ist für die Fernsteuerungsfunktion erforderlich:

- Microsoft Windows Server 2003
- Microsoft Windows 2000 mit Service-Pack 4
- Red Hat Enterprise Linux Version 3, Update 8
- SUSE Enterprise Linux Version 9
- VMware Version 3.0.1

Die Webschnittstelle des Managementmoduls unterstützt keine Sprachen mit Doppelbytezeichensatz.

Verkabelung des Managementmoduls

Sie können das Managementmodul mit einem Netz oder direkt mit einem Client-Computer verbinden.

Informationen und Anweisungen zur Verkabelung finden Sie im *Installationshandbuch* zu Ihrem Managementmodul. Informationen zum Verbinden einer fernen Konsole mit dem Managementmodul sowie zur Verwendung der Befehlszeilenschnittstelle des erweiterten Managementmoduls für die Konfiguration der BladeCenter-Einheit finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des erweiterten BladeCenter-Managementmoduls*.

Nach der Verkabelung des Managementmoduls finden Sie Informationen zur Erstkonfiguration im Abschnitt „Erstmalig eine Verbindung zum Managementmodul herstellen" auf Seite 11.

Netzverbindung

Mithilfe eines Ethernet-Kabels können Sie das Managementmodul an ein Netz anschließen.

Schließen Sie das eine Ende eines Ethernet-Kabels der Kategorie 5 oder höher an den (Ethernet-) Anschluss für die Fernverwaltung und ferne Konsole des Managementmoduls an. Schließen Sie das andere Ende des Ethernet-Kabels an das Netz der Einrichtung an.

Direktverbindung

Mithilfe eines Ethernet-Kabels können Sie einen Client-Computer direkt mit dem Managementmodul verbinden.

Verbinden Sie das eine Ende eines Ethernet-Kabels der Kategorie 5 (oder höher) oder eines gekreuzten Ethernet-Kabels der Kategorie 5 (oder höher) mit dem Anschluss für Fernverwaltung und ferne Konsole (Ethernet) des Managementmoduls. Verbinden Sie das andere Kabelende mit dem Ethernet-Anschluss des Client-Computers.

Anmerkung: Das erweiterte Managementmodul kann Auto-MDI(X) (Media Dependent Interface) ausführen, sodass keine gekreuzten Kabel oder Anschlüsse mit gekreuzter Buchsenbelegung (MDIX) erforderlich sind. Möglicherweise müssen Sie für die Verbindung mit dem erweiterten Managementmodul ein gekreuztes Kabel verwenden, wenn die Netzschnittstellenkarte im Client-Computer sehr alt ist.

Erstmalig eine Verbindung zum Managementmodul herstellen

Verbinden Sie eine ferne Konsole mit dem Managementmodul, um die Erstkonfiguration der BladeCenter-Einheit durchzuführen.

Anmerkung: Das erweiterte Managementmodul verfügt in der Standardeinstellung nicht über eine festgelegte statische IPv6-IP-Adresse. Beim Erstzugriff auf das erweiterte Managementmodul in einer IPv6-Umgebung können Benutzer entweder die IPv4-IP-Adresse oder die lokale IPv6-Verbindungsadresse verwenden. Informationen zur Bestimmung der IPv6-Adresse, die für den Erstzugriff auf ein erweitertes Managementmodul verwendet werden kann, finden Sie im Abschnitt „IPv6-Adressierung für die erstmalige Verbindung" auf Seite 12.

Das Managementmodul verfügt über die folgenden Standardnetzeinstellungen:

- "IPv4 IP address" (IPv4-IP-Adresse): 192.168.70.125 (primäres und sekundäres Managementmodul)
- "IPv4 Subnet" (IPv4-Teilnetz): 255.255.255.0
- "User ID" (Benutzer-ID): USERID (Großbuchstaben)
- "Password" (Kennwort): PASSW0RD (Achten Sie darauf, dass in "PASSW0RD" kein O, sondern eine Null (0) steht)

Standardmäßig ist das Managementmodul so konfiguriert, dass es erst auf DHCP antwortet, bevor es seine statische IP-Adresse verwendet.

Der Client-Computer, den Sie mit dem Managementmodul verbinden, muss so konfiguriert sein, dass er sich im selben Teilnetz befindet wie das BladeCenter-Managementmodul. Die IP-Adresse des Managementmoduls muss sich ebenfalls in derselben lokalen Domäne befinden wie der Client-Computer. Wenn Sie einen Client-Computer zum ersten Mal mit dem Managementmodul verbinden, müssen Sie die Internetprotokolleigenschaften auf dem Client-Computer ändern.

Nachdem Sie das Ethernet-Kabel des Managementmoduls mit dem Client-Computer verbunden haben, gehen Sie wie folgt vor:

1. Bei IPv4-Verbindungen müssen Sie sicherstellen, dass das Teilnetz des Client-Computers denselben Wert aufweist wie das Standardteilnetz des Managementmoduls (wie oben aufgeführt).
2. Öffnen Sie auf dem Client-Computer einen Web-Browser und steuern Sie ihn zur Standard-IP-Adresse des Managementmoduls (wie oben aufgeführt).
3. Geben Sie den Standardbenutzernamen (USERID) und das Standardkennwort (PASSW0RD) ein, um die ferne Sitzung zu starten.
4. Folgen Sie den Anweisungen auf dem Bildschirm. Vergewissern Sie sich, dass für die Websitzung der gewünschte Zeitlimitwert eingestellt ist.

Nachdem Sie einen Client-Computer zum ersten Mal mit dem Managementmodul verbunden haben, führen Sie die Erstkonfiguration der BladeCenter-Einheit durch (siehe „Managementmodul konfigurieren" auf Seite 16).

IPv6-Adressierung für die erstmalige Verbindung

Wenn Sie die IPv6-Adressierung verwenden, ist die einzige Möglichkeit, eine erstmalige Verbindung zum erweiterten Managementmodul herzustellen, die Verwendung der lokalen IPv6-Verbindungsadresse.

Die lokale Verbindungsadresse ist eine eindeutige IPv6-Adresse für das erweiterte Managementmodul, die anhand seiner MAC-Adresse automatisch generiert wird. Diese Adresse hat folgendes Format: `FE80::3BA7:94FF:FE07:CBD0`.

Die lokale Verbindungsadresse für das erweiterte Managementmodul kann mithilfe der folgenden Möglichkeiten bestimmt werden:

- Bei manchen erweiterten Managementmodulen befindet sich die lokale Verbindungsadresse auf einem Etikett am erweiterten Managementmodul selbst.
- Wenn Sie sich mithilfe der IPv4-Adressierung an der Befehlszeilenschnittstelle des Managementmoduls anmelden können, können Sie die lokale Verbindungsadresse mit dem Befehl `ifconfig` anzeigen (Informationen hierzu finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des erweiterten BladeCenter-Managementmoduls*.
- Wenn Sie sich mithilfe der IPv4-Adressierung an der Webschnittstelle des Managementmoduls anmelden können, können Sie die lokale Verbindungsadresse im primären Managementmodul, im Abschnitt "IPv6" der Seite **MM Control → Network Interfaces** (MM-Steuerung → Netzschnittstellen) anzeigen (Informationen hierzu finden Sie im Abschnitt „Network Interfaces (Netzschnittstellen)" auf Seite 188).

Wenn das erweiterte Managementmodul kein Etikett mit der lokalen Verbindungsadresse aufweist und Sie nicht über IPv4 auf das erweiterte Managementmodul zugreifen können, gehen Sie wie folgt vor, um die lokale Verbindungsadresse zu berechnen:

1. Schreiben Sie die MAC-Adresse des erweiterten Managementmoduls auf. Sie befindet sich auf einem Etikett am Managementmodul, unter dem IP-Grundstellungsknopf. Auf dem Etikett steht MM*xxxxxxxxxxxx*, wobei *xxxxxxxxxxxx* die MAC-Adresse darstellt. Beispiel:

   `39-A7-94-07-CB-D0`
2. Teilen Sie die MAC-Adresse in zwei Teile und fügen Sie in der Mitte die Zeichenfolge "FF-FE" ein. Beispiel:

   `39-A7-94-`**`FF-FE`**`-07-CB-D0`
3. Wandeln Sie die beiden Hexadezimalziffern am linken Ende der Zeichenfolge in binäre Ziffern um. Beispiel:
   - **`39`**`-A7-94-FF-FE-07-CB-D0`
   - **`00111001`**`-A7-94-FF-FE-07-CB-D0`
4. Kehren Sie den Wert des siebten Bits der Binärzeichenfolge um. Beispiel:
   - `00111`**`0`**`1-A7-94-FF-FE-07-CB-D0`
   - `00111`**`1`**`1-A7-94-FF-FE-07-CB-D0`
5. Wandeln Sie die Binärziffern am linken Ende der Zeichenfolge wieder in Hexadezimalziffern um. Beispiel:
   - **`00111011`**`-A7-94-FF-FE-07-CB-D0`
   - **`3B`**`-A7-94-FF-FE-07-CB-D0`
6. Kombinieren Sie die Hexadezimalziffernpaare in vier Zifferngruppen. Beispiel:
   - `3B-A7-94-FF-FE-07-CB-D0`
   - `3BA7-94FF-FE07-CBD0`

7. Ersetzen Sie die Trennstriche (-) durch Doppelpunkte (:). Beispiel:
   - 3BA7-94FF-FE07-CBD0
   - 3BA7:94FF:FE07:CBD0
8. Fügen Sie am linken Ende der Zeichenfolge die Zeichen "FE80::" hinzu. Beispiel:

   FE80::3BA7:94FF:FE07:CBD0

Für die MAC-Adresse 39-A7-94-07-CB-D0 lautet die entsprechende lokale Verbindungsadresse, die für den ersten IPv6-Zugriff verwendet wird, wie folgt: FE80::3BA7:94FF:FE07:CBD0.

Webschnittstelle des Managementmoduls starten

Verwenden Sie einen der angegebenen Web-Browser, um eine Webschnittstellensitzung für das Managementmodul zu starten.

Das Managementmodul unterstützt die folgenden Web-Browser für den (Client-) Fernzugriff:

- Microsoft Internet Explorer 6.0 oder höher (mit installiertem aktuellen Service-Pack)
- Mozilla Firefox Version 1.07 oder höher

Anmerkung: Die Webschnittstelle des E/A-Moduls wird nur von Mozilla Firefox Version 1.07 oder höher unterstützt.

Gehen Sie wie folgt vor, um die Webschnittstelle des Managementmoduls zu starten:

1. Öffnen Sie einen Web-Browser. Geben Sie im Adress- oder URL-Feld die IP-Adresse oder den Hostnamen für die Fernverbindung des Managementmoduls ein. (Weitere Details finden Sie im *Installationshandbuch* zu Ihrem Managementmodul.)

   Anmerkung: Die werkseitig definierte statische IPv4-IP-Adresse lautet 192.168.70.125, die standardmäßige IPv4-Teilnetzadresse lautet 255.255.255.0 und der Standardhostname lautet MM*xxxxxxxxxxx*, wobei *xxxxxxxxxxx* für die Herstellerkennung der MAC-Adresse steht. Die MAC-Adresse befindet sich auf einem Etikett am Managementmodul, das unter dem IP-Grundstellungsknopf angebracht ist. Informationen zum Bestimmen der IPv6-Adresse, die für den ersten Zugriff auf das erweiterte Managementmodul verwendet wird, finden Sie im Abschnitt „IPv6-Adressierung für die erstmalige Verbindung” auf Seite 12 .

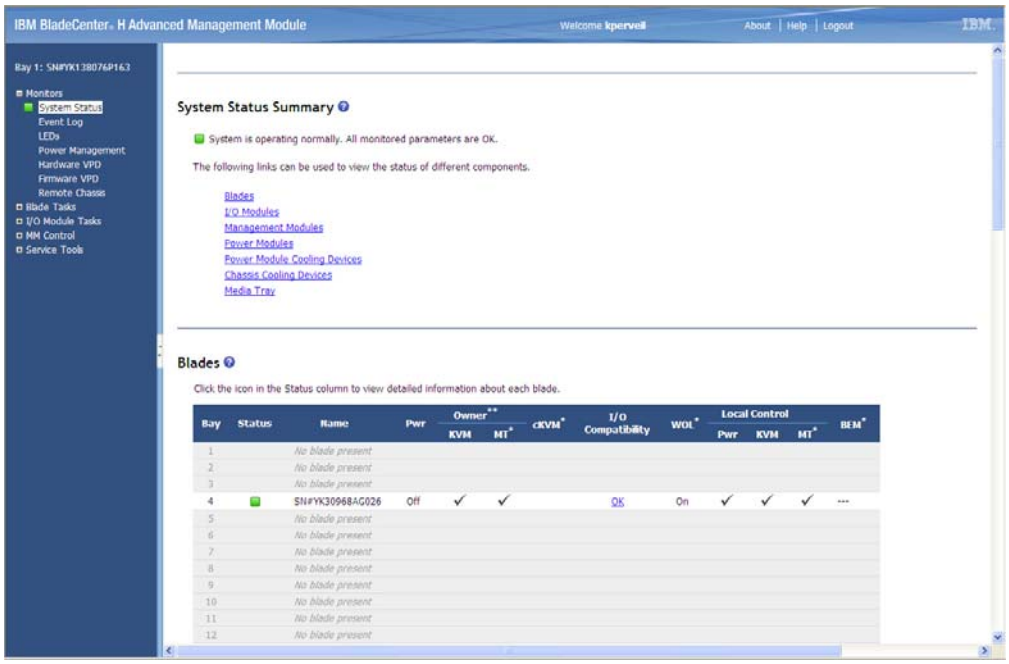
   Die Seite "Enter Network Password" (Netzkennwort eingeben) wird geöffnet.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Wenn Sie sich zum ersten Mal am Managementmodul anmelden, erhalten Sie Ihren Benutzernamen und Ihr Kennwort vom Systemadministrator. Alle Anmeldeversuche werden im Ereignisprotokoll dokumentiert.

   Anmerkung: Die Benutzer-ID und das Kennwort, die werkseitig für das Managementmodul vordefiniert sind, lauten wie folgt:
   - Benutzer-ID: USERID (nur Großbuchstaben)
   - Kennwort: PASSW0RD (beachten Sie die Null anstelle eines "O" in PASSW0RD)

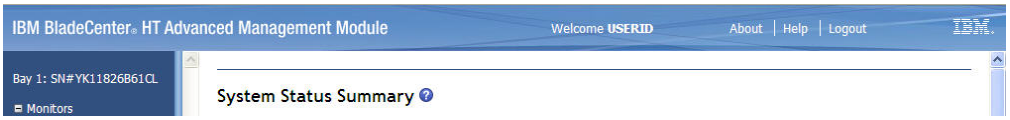
3. Befolgen Sie die Anweisungen auf dem Bildschirm. Stellen Sie sicher, dass Sie den gewünschten Zeitlimitwert für Ihre Websitzung festlegen. Wenn Sie das Kontrollkästchen **Use automatic refresh** (Automatische Aktualisierung verwenden) auswählen, können die Daten einiger Seiten automatisch aktualisiert werden.

Anmerkung: Wenn Sie das Managementmodul nach einer Firmwareaktualisierung zum ersten Mal starten, wird eine Seite mit Informationen zu lizenzierten Funktionen angezeigt, die aktiv sind. Informationen zu aktiven und inaktiven lizenzierten Funktionen finden Sie auf der Seite, die Sie über **MM Control → Licensed Features** (MM-Steuerung → Lizenzierte Funktionen) aufrufen (Informationen dazu finden Sie im Abschnitt „License Manager (Lizenzmanager)" auf Seite 205).

Die Webschnittstellenseite des BladeCenter-Managementmoduls wird geöffnet. Der Inhalt dieser Seite und aller anderen Webschnittstellenseiten hängt vom Typ der verwendeten BladeCenter-Einheit und von den installierten Firmwareversionen und Zusatzeinrichtungen ab. Ausführliche Informationen zur Webschnittstelle des Managementmoduls finden Sie in Kapitel 3, „Überblick über die Webschnittstelle des Managementmoduls", auf Seite 99.

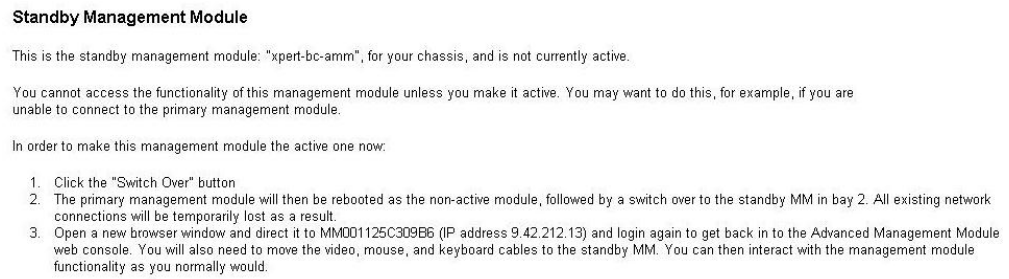


Oben auf der Webschnittstellenseite des Managementmoduls wird der Typ des Managementmoduls angezeigt, an dem Sie angemeldet sind. In den folgenden Abbildungen sind die Managementmodultypen für ein Managementmodul und für ein erweitertes Managementmodul dargestellt. Informationen zum Konfigurieren von Managementmodulen, bei denen es sich nicht um erweiterte Managementmodule handelt, finden Sie in einem separaten Dokument.



Oben auf der Webschnittstellenseite des Managementmoduls werden die Anmelde-ID des aktuellen Benutzers sowie der Standort und die Identität des aktiven (primären) Managementmoduls angezeigt. Im ersten Beispiel für ein Managementmodul, bei dem es sich nicht um ein erweitertes Managementmodul handelt, wird links oben auf der Seite die Anmelde-ID "USER1" angezeigt. Außerdem wird angegeben, dass das primäre Managementmodul mit der Identität "SN#01" in der Managementmodulposition 1 installiert ist. Im zweiten Beispiel für ein erweitertes Managementmodul wird oben in der Mitte der Seite die Anmelde-ID "USERID" angezeigt. Außerdem wird oben links auf der Seite angegeben, dass das primäre erweiterte Managementmodul mit der Identität "SN#YK11826B61CL" in der Managementmodulposition 1 installiert ist.

Bei erweiterten Managementmodulen können Sie eine Webschnittstellensitzung für das Bereitschaftsmanagementmodul starten, wenn die Netzschnittstelle für das Bereitschaftsmanagementmodul konfiguriert wurde. Die Bereitschaftsschnittstelle stellt keine Funktionen bereit, außer der Initialisierung einer Funktionsübernahme vom primären Managementmodul.



Managementmodul konfigurieren

Sie konfigurieren das primäre (aktive) Managementmodul. Die Konfiguration des Bereitschaftsmanagementmoduls, sofern vorhanden, wird so synchronisiert, dass sie mit der Konfiguration des primären Managementmoduls übereinstimmt. Diese Synchronisation kann bis zu 45 Minuten dauern.

Bei erweiterten Managementmodulen können Sie die Netzkonfiguration des Bereitschaftsmanagementmoduls als Teil der Funktionsübernahme manuell festlegen und den Zugang dazu ermöglichen, wenn bei der automatisierten Funktionsübernahme ein Fehler auftritt. Die Konfigurationsdaten in dieser Dokumentation beziehen sich auf das primäre Managementmodul, das möglicherweise das einzige Managementmodul in der BladeCenter-Einheit darstellt.

Wenn das von Ihnen installierte Managementmodul ein Ersatz für das einzige Managementmodul in der BladeCenter-Einheit ist und Sie die Konfigurationsdatei vor dem Austausch des Managementmoduls gespeichert haben, können Sie die gespeicherte Konfigurationsdatei über die Webschnittstelle des Managementmoduls auf das Austauschmanagementmodul anwenden. Informationen zur Anwendung einer gespeicherten Konfigurationsdatei finden Sie im Abschnitt „Konfiguration des Managementmoduls wiederherstellen und ändern" auf Seite 77.

Die BladeCenter-Einheit erkennt automatisch die installierten Module und BladeServer und speichert die elementaren Produktdaten (Vital Product Data, VPD). Beim Starten der BladeCenter-Einheit konfiguriert das Managementmodul automatisch den Anschluss für Fernverwaltung des Managementmoduls, sodass Sie die BladeCenter-Komponenten konfigurieren und verwalten können. Die BladeCenter-Komponenten werden per Fernzugriff über die Webschnittstelle des Managementmoduls, die Befehlszeilenschnittstelle des Managementmoduls oder über SNMP (Simple Network Management Protocol) konfiguriert und verwaltet.

Anmerkung: Es gibt zwei Möglichkeiten, die E/A-Module zu konfigurieren: über die Webschnittstelle des Managementmoduls oder über einen externen Anschluss für E/A-Module, der durch das Managementmodul über eine Telnet-Schnittstelle oder einen Web-Browser aktiviert wird. Weitere Informationen finden Sie in der Dokumentation zum betreffenden E/A-Modul.

Damit das aktive Managementmodul mit Netzressourcen und mit den E/A-Modulen in der BladeCenter-Einheit kommunizieren kann, müssen Sie die IP-Adressen für die folgenden internen und externen Anschlüsse konfigurieren:

- Den externen Ethernet-Anschluss (Fernverwaltung) (Ethernet 0) des Managementmoduls (siehe „Network Interfaces (Netzschnittstellen)" auf Seite 188). Mithilfe der automatischen Erstkonfiguration des Managementmoduls kann die Netzverwaltungsstation eine Verbindung zum Managementmodul herstellen, um den Anschluss vollständig zu konfigurieren und die restlichen Einstellungen für die BladeCenter-Einheit zu konfigurieren.
- Den internen Ethernet-Anschluss (Ethernet 1) des Managementmoduls zur Datenübertragung mit den E/A-Modulen (siehe „Network Interfaces (Netzschnittstellen)" auf Seite 188). Die internen Ethernet-Anschlüsse des erweiterten Managementmoduls können nicht manuell konfiguriert werden.
- Den Managementanschluss am jeweiligen E/A-Modul, der die Datenübertragung mit dem Managementmodul bereitstellt. Dieser Anschluss wird durch die Konfiguration der IP-Adresse für das E/A-Modul konfiguriert (siehe „Configuration (Konfiguration)" auf Seite 163).

Anmerkung: Einige Typen von E/A-Modulen, wie zum Beispiel Durchgriffsmodule, besitzen keinen Managementanschluss.

Informationen dazu, was zusätzlich im E/A-Modul konfiguriert werden muss, finden Sie in der Dokumentation zum betreffenden E/A-Modul.

Anmerkung: Konfigurieren Sie den Blade-Server und das erweiterte Managementmodul so, dass sie nicht demselben IP-Teilnetz angehören. Das erweiterte Managementmodul sollte sich in einem IP-Teilnetz für Managementdatenverkehr befinden.

Für die Datenübertragung mit Blade-Servern zur Ausführung bestimmter Funktionen, wie beispielsweise die Implementierung eines Betriebssystems oder von Anwendungsprogrammen über ein Netz, müssen Sie außerdem mindestens einen externen (Inband-) Anschluss an einem Ethernet-Switchmodul in der E/A-Modulposition 1 oder 2 konfigurieren.

Anmerkung: Wenn in der E/A-Modulposition 1 oder 2 ein Durchgriffsmodul (anstelle eines Ethernet-E/A-Moduls) installiert ist, müssen Sie den Netzswitch konfigurieren, mit dem das Durchgriffsmodul verbunden ist. Entsprechende Anweisungen finden Sie in der Dokumentation zum Netzswitch.

Managementmodul für den Fernzugriff konfigurieren

Bei IPv4 können Sie das Managementmodul so konfigurieren, dass es für den Fernzugriff DHCP (Dynamic Host Configuration Protocol) oder statische IP-Adressen verwendet. Bei IPv6 können Sie das Managementmodul so konfigurieren, dass es für den Fernzugriff DHCPv6 (Dynamic Host Configuration Protocol), statische IP-Adressen und eine statusunabhängige automatische Konfiguration verwendet.

Nachdem Sie das aktive Managementmodul mit dem Netz verbunden haben, wird die Verbindung über den Ethernet-Anschluss mithilfe einer der folgenden Vorgehensweisen konfiguriert:

- Bei IPv4:
  - Wenn Sie über einen zugänglichen, aktiven und konfigurierten DHCP-Server (Dynamic Host Configuration Protocol) im Netz verfügen, werden die IP-Adresse, die Gateway-Adresse, die Teilnetzmaske und die IP-Adressen (IPv4) des DNS-Servers automatisch festgelegt. Als Hostname wird standardmäßig die MAC-Adresse des Managementmoduls festgelegt; der Domänenserver kann sie nicht ändern.
  - Wenn der DHCP-Server nicht innerhalb von 2 Minuten, nachdem der Anschluss verbunden wurde, antwortet, verwendet das Managementmodul die werkseitig voreingestellte statische IP-Adresse sowie die Standard-Teilnetzadresse.

  Wichtig: Sie können erst dann mithilfe der werkseitig voreingestellten Konfiguration eine Verbindung zum Managementmodul herstellen, nachdem dieser Zeitraum verstrichen ist.
- Bei IPv6:
  - Wenn im Netz ein zugänglicher und aktiver IPv6-Router zur Verfügung steht, generiert das erweiterte Managementmodul statusunabhängige automatisch konfigurierte Adressen für die Ethernet-Anschlüsse.
  - Wenn im Netz ein zugänglicher, aktiver und konfigurierter DHCPv6-Server zur Verfügung steht, empfängt das erweiterte Managementmodul außerdem eine DHCPv6 zugewiesene IP-Konfiguration.

– Die lokale IPv6-Verbindungsadresse steht stets zur Verfügung, wenn IPv6 aktiviert ist. In Abschnitt „IPv6-Adressierung für die erstmalige Verbindung" auf Seite 12 erhalten Sie Informationen zur Bestimmung der lokalen Verbindungsadresse.

Jede dieser Aktionen aktiviert die Ethernet-Verbindung auf dem aktiven Managementmodul.

Stellen Sie sicher, dass sich der Client-Computer im selben Teilnetz befindet wie das Managementmodul. Verwenden Sie dann Ihren Web-Browser, um die Verbindung zum Managementmodul herzustellen (weitere Informationen finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13). Geben Sie im Adressen- oder URL-Feld des Browsers die IP-Adresse ein, die das Managementmodul verwendet:

- Wenn die IP-Adresse von einem DHCP-Server zugewiesen wurde, erhalten Sie die IP-Adresse von Ihren Netzadministrator.
- Die werkseitig voreingestellte statische IPv4-IP-Adresse ist 192.168.70.125, die IPv4-Standardteilnetzadresse lautet 255.255.255.0 und der Standardhostname ist *xxxxxxxxxxxx*. Dabei gibt *xxxxxxxxxxxx* die Herstellerkennung der MAC-Adresse an. Die MAC-Adresse befindet sich auf einem Etikett am Managementmodul, unterhalb des IP-Grundstellungsknopfs. Informationen zur Bestimmung der IPv6-Adresse für den erstmaligen Zugriff auf ein erweitertes Managementmodul finden Sie im Abschnitt „IPv6-Adressierung für die erstmalige Verbindung" auf Seite 12.

Anmerkung: Wenn die IP-Konfiguration vom DHCP-Server zugewiesen wurde, kann der Netzadministrator die MAC-Adresse der Netzschnittstelle des Managementmoduls verwenden, um herauszufinden, welche IP-Adresse und welcher Hostname zugewiesen wurden.

Ethernet-Anschluss des Managementmoduls konfigurieren

Sie können mithilfe der Webschnittstelle den externen Ethernet-Anschluss des Managementmoduls und den internen Ethernet-Managementanschluss der einzelnen E/A-Module konfigurieren.

Anmerkung: Konfigurieren Sie den Blade-Server und das erweiterte Managementmodul so, dass sie nicht demselben IP-Teilnetz angehören. Das erweiterte Managementmodul sollte sich in einem IP-Teilnetz für Managementdatenverkehr befinden.

Gehen Sie wie folgt vor, um den externen Ethernet-Anschluss des Managementmoduls zu konfigurieren:

1. Klicken Sie im Navigationsfenster unter **MM Control** (MM-Steuerung) auf **Network Interfaces** (Netzschnittstellen).

   Achtung: Wenn IPv6 aktiviert wurde, und Sie es inaktivieren oder die Firmware des erweiterten Managementmoduls auf eine Stufe aktualisieren, die keine IPv6-Adressierung unterstützt, geht die gesamte IPv6-Konnektivität verloren. Services und Schnittstellen, die für IPv6 konfiguriert wurden, funktionieren möglicherweise nicht mehr ordnungsgemäß und müssen rekonfiguriert werden.

2. Aktivieren oder inaktivieren Sie im Abschnitt **External Network Interface (eth0)** (Externe Netzschnittstelle (eth0)) die IPv6-Adressierung mithilfe des Kontrollkästchens **IPv6 Enabled** (IPv6 aktiviert). Die IPv4-Adressierung ist immer aktiviert und IPv6 ist standardmäßig aktiviert. Wenn die IPv6-Adressierung für die BladeCenter-Einheit inaktiviert wird, wird ein weiteres Kontrollkästchen angezeigt, mit dessen Hilfe die Anzeige von Informationen zu IPv6 unterdrückt werden kann. Sie müssen auf **Save** (Speichern) klicken, um die Änderungen zu übernehmen.

   Anmerkung: Wenn IPv6 aktiviert ist, muss mindestens eine der Konfigurationsmethoden von IPv6 (IPv6 statisch, DHCPv6 oder statusunabhängige automatische Konfiguration) ebenfalls aktiviert und konfiguriert werden.

3. Konfigurieren Sie die externe Ethernet-Schnittstelle (eth0) für IPv4 und IPv6 im Abschnitt **Primary Management Module** (Primäres Managementmodul).

   Anmerkung: Für die Datenübertragung von E/A-Modulen zu einer Fernverwaltungsstation, zum Beispiel zu einem Verwaltungsserver, der IBM Systems Director Server ausführt, über den externen Ethernet-Anschluss des Managementmoduls müssen sich die interne Netzschnittstelle des E/A-Moduls und die internen und externen Schnittstellen des Managementmoduls im selben Teilnetz befinden.

   a. Die folgenden Konfigurationseinstellungen gelten sowohl für die IPv4- als auch für die IPv6-Adressierung:
      - Feld **Host name** (Hostname): (Optional) Dies ist der IP-Hostname, den Sie für das Managementmodul verwenden möchten (mit maximal 63 Zeichen und den folgenden Standards für Hostnamen).
      - Feld **Domain name** (Domänenname): Der Domänenname des Managementmoduls, der in Verbindung mit einem dynamischen Domänennamensserver (DDNS) verwendet wird.

- Kontrollkästchen **Register this interface with DNS** (Diese Schnittstelle bei DNS registrieren): Wenn dieses Kontrollkästchen aktiviert ist, werden die konfigurierten DNS-Server (siehe „Network Protocols (Netzprotokolle)" auf Seite 192) auch als DDNS-Server betrachtet und die Informationen zu den Domänennamen werden an diese gesendet.

b. Für die IPv4-Adressierung gelten die folgenden Konfigurationseinstellungen:
   - **DHCP**: Wählen Sie eine der folgenden Auswahlmöglichkeiten aus:
     - **Enabled: Obtain IP config. from DHCP server** (Aktiviert: IP-Konfiguration vom DHCP-Server beziehen)
     - **Disabled: Use static IP configuration** (Inaktiviert: Statische IP-Konfiguration verwenden)
     - **Try DHCP server. If it fails, use static IP config.** (DHCP-Server versuchen. Bei Fehlschlagen statische IP-Konfig. verwenden.) (Die Standardeinstellung. Das Zeitlimit für DHCP läuft nach 2 Minuten ab.)

     Anmerkung: Ist für die DHCP-Einstellung des Managementmoduls die Option **Try DHCP server. If it fails, use static IP config.** (DHCP-Server versuchen. Bei Fehlschlagen statische IP-Konfig. verwenden.) ausgewählt, verwendet das Managementmodul die statische IP-Adresse, wenn der DHCP-Server beim Starten des Managementmoduls nicht verfügbar ist. In diesem Fall ist die IP-Adresse möglicherweise nicht erreichbar, wenn mehrere Managementmodule mit derselben statischen IP-Adresse gestartet wurden.
   - **IPv4 Static IP configuration** (Statische IPv4-IP-Konfiguration): Konfigurieren Sie diese Informationen nur, wenn DHCP inaktiviert ist.
     - **IP address** (IP-Adresse): Die IPv4-IP-Adresse des Managementmoduls muss aus vier Ganzzahlen von 0 bis 255 bestehen, die durch Punkte getrennt sind, und darf keine Leerzeichen oder aufeinanderfolgenden Punkte enthalten. Die Standardeinstellung ist 192.168.70.125.
     - **Subnet mask** (Teilnetzmaske): Die Teilnetzmaske muss aus vier Ganzzahlen von 0 bis 255 bestehen, die durch Punkte getrennt sind, und darf keine Leerzeichen enthalten. Die Standardeinstellung ist 255.255.255.0
     - **Gateway address** (Gateway-Adresse): Die IP-Adresse des Netzgatewayrouters muss aus vier Ganzzahlen von 0 bis 255 bestehen, die durch Punkte getrennt sind, und darf keine Leerzeichen enthalten. Diese Adresse muss von der IP-Adresse und der Teilnetzmaske, die oben angegeben wurden, erreichbar sein.
   - Klicken Sie auf **IP Configuration Assigned by DHCP Server** (IP-Konfiguration von DHCP-Server zugewiesen), um die vom DHCP-Server zugewiesene IP-Konfiguration anzuzeigen. (Diese Option steht nur zur Verfügung, wenn DHCP aktiviert ist.)

c. Die folgenden Konfigurationseinstellungen gelten für die IPv6-Adressierung. Sie werden nur angezeigt, wenn IPv6 aktiviert ist oder wenn IPv6 inaktiviert ist und die Anzeige der IPv6-Einstellungen nicht unterdrückt wurde.

   Anmerkung: Bei IPv6 können die DHCPv6-Konfiguration und die statische IPv6-Konfiguration gleichzeitig aktiviert werden, jeweils mit ihrer eigenen Adresse. Hosts wie das erweiterte Managementmodul können mehrere IPv6-Adressen besitzen.

   - **Link-local address** (Lokale Verbindungsadresse): (schreibgeschützt) Eine eindeutige IPv6-Adresse für das erweiterte Managementmodul, die anhand der MAC-Adresse automatisch generiert wird.
   - **IPv6 Static IP configuration** (Statische IPv6-IP-Konfiguration): Die statische IPv6-IP-Konfiguration ist standardmäßig inaktiviert.

     Anmerkung: Für das erweiterte Managementmodul ist standardmäßig keine statische IPv6-Adresse festgelegt. Für den ersten Zugang können Benutzer entweder die Standard-IPv4-Adresse oder die lokale IPv6-Verbindungsadresse verwenden.

     – **IP address** (IP-Adresse): Die IPv6-IP-Adresse des Managementmoduls muss aus 16 hexadezimalen Bytes bestehen, die paarweise angeordnet und durch Doppelpunkte getrennt sind, wie im folgenden Format: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A
     – **Address prefix length (1-128)** (Adresspräfixlänge (1 - 128): Die Länge des Präfixes für die IPv6-Adresse. Die Länge des Adresspräfixes kann für das erweiterte Bereitschaftsmanagementmodul nicht konfiguriert werden. Es wird derselbe Wert verwendet wie beim primären erweiterten Managementmodul.
     – **Default route** (Standardroute): Die IP-Adresse Ihres Netzgatewayrouters muss aus 16 hexadezimalen Bytes bestehen, die paarweise angeordnet und durch Doppelpunkte getrennt sind, wie im folgenden Format: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A. Die Standardroute kann für das erweiterte Bereitschaftsmanagementmodul nicht konfiguriert werden. Es wird derselbe Wert verwendet wie beim primären erweiterten Managementmodul.

   - **DHCPv6**: Wählen Sie eine der folgenden Auswahlmöglichkeiten aus:
     – **Enabled: Obtain IP configuration from DHCP server** (Aktiviert: IP-Konfiguration vom DHCP-Server erhalten) (Dies ist die Standardeinstellung)
     – **Disabled: Not obtain IP configuration from DHCP server** (Inaktiviert: IP-Konfiguration nicht von DHCP-Server anfordern)
   - **Stateless Auto-configuration** (Statusunabhängige automatische Konfiguration): Die automatische Konfiguration von Adressen basiert auf dem Empfang von Routermitteilungen. Diese Mitteilungen enthalten statusunabhängige Adresspräfixe. Die statusunabhängige automatische Konfiguration ist standardmäßig aktiviert.

4. Konfigurieren Sie den internen Ethernet-Managementanschluss auf jedem E/A-Modul in der BladeCenter-Einheit.

   Anmerkung:
   - Einige Typen von E/A-Modulen, wie zum Beispiel die Durchgriffsmodule, besitzen keinen Managementanschluss.
   - Einige E/A-Module unterstützen keine IPv6-Adressierung.

   a. Klicken Sie im Navigationsfenster unter **I/O Module Tasks** (E/A-Modul-Tasks) auf **Configuration** (Konfiguration).
   b. Klicken Sie auf **Bay 1** (Position 1).
   c. Geben Sie in den Feldern **New Static IP address** (Neue statische IP-Adresse) die IP-Konfiguration an, die für diese Schnittstelle verwendet werden soll. Bei IPv4 muss dieselbe Teilnetzmaske verwendet werden wie in der internen Netzschnittstelle (eth1).
   d. Klicken Sie auf **Advanced Configuration** (Erweiterte Konfiguration).
   e. Aktivieren Sie im Abschnitt **Advanced Setup** (Erweiterte Konfiguration) die externe Verwaltung über alle Anschlüsse.
   f. Klicken Sie im Navigationsfenster unter **I/O Module Tasks** (E/A-Modul-Tasks) auf **Admin/Power/Restart** (Admin/Einschalten/Erneut starten).
   g. Wählen Sie im Abschnitt **I/O Module Advanced Setup** (E/A-Modul, Erweiterte Konfiguration) **I/O module 1** (E/A-Modul 1) aus und aktivieren Sie dann die externen Anschlüsse. (Externe Anschlüsse sind standardmäßig inaktiviert.)

   Anmerkung: In der Ersteinstellung der Firmware des E/A-Moduls sind folgende Benutzer-ID und folgendes Benutzerkennwort definiert:
   - User ID (Benutzer-ID): USERID (Großbuchstaben)
   - Password (Kennwort): PASSW0RD (Achten Sie darauf, dass in PASSW0RD kein O, sondern eine Null (0) steht.)

5. Wiederholen Sie Schritt 3 für alle E/A-Module in der BladeCenter-Einheit.

Für die Datenübertragung mit Blade-Servern zur Ausführung bestimmter Funktionen, wie beispielsweise die Implementierung eines Betriebssystems oder von Anwendungsprogrammen, müssen Sie außerdem mindestens einen externen (Inband-) Anschluss an einem Ethernet-E/A-Modul konfigurieren.

Konfigurationsassistent verwenden

Sie können den Konfigurationsassistenten des erweiterten Managementmoduls verwenden, um das erweiterte Managementmodul zu konfigurieren.

Der Konfigurationsassistent wird automatisch gestartet, wenn Sie zum ersten Mal auf die Webschnittstelle eines neuen erweiterten Managementmoduls zugreifen. Der Konfigurationsassistent wird auch automatisch gestartet, wenn Sie zum ersten Mal auf die Webschnittstelle eines erweiterten Managementmoduls zugreifen, das auf die werkseitig vorgenommenen Standardeinstellungen zurückgesetzt wurde.

Um den Konfigurationsassistenten zu verwenden, klicken Sie im Navigationsfenster unter **Configuration Mgmt** (Konfigurationsverwaltung) auf **Configuration Wizard** (Konfigurationsassistent). Sie müssen über die Rolle "Supervisor" (Administrator, Befehlsberechtigung) verfügen, um den Konfigurationsassistenten zu nutzen. Der Konfigurationsassistent unterstützt Konfigurationspfade vom Typ **Express** (Express) und **Custom** (Benutzerdefiniert).

- Bei der Option **Express** (Express) werden einige allgemeine Einstellungen vorausgewählt.
- Bei der Option **Custom** (Benutzerdefiniert) werden Sie aufgefordert, die benötigten Konfigurationsdaten für die einzelnen Komponenten einzugeben.

Nachdem Sie den Konfigurationspfad ausgewählt haben, werden auf der Seite **Getting Started** (Erste Schritte) die Informationen zusammengefasst, die Sie zum Abschließen des Konfigurationsprozesses benötigen. Klicken Sie auf **View Configuration Worksheet** (Arbeitsblatt zur Konfiguration anzeigen), um ein praktisches Formular zur Erfassung dieser Informationen anzuzeigen und auszudrucken.

Nachdem Sie diese Informationen zusammengestellt haben, geben Sie sie auf den Assistentenseiten ein, um die grundlegende Konfiguration des Managementmoduls abzuschließen. Wenn Sie eine gespeicherte Konfiguration für das Managementmodul importieren oder wenn Sie eine Konfiguration wiederherstellen, die auf der Rückwandplatine der BladeCenter-Einheit gespeichert ist, finden Sie die entsprechenden Optionen auf der Seite **Import Configuration** (Konfiguration importieren) des Konfigurationsassistenten. Importierte oder wiederhergestellte Konfigurationen erfordern keine zusätzliche Informationseingabe.

Die Fertigstellungsseite enthält drei Optionsfelder und eine Schaltfläche **Finish** (Beenden). Folgende Optionsfelder stehen zur Auswahl:

- **Restart Management Module now to ensure all changes are applied** (Managementmodul jetzt erneut starten, um die Anwendung aller Änderungen sicherzustellen)
- **Allow me to update my Management Module Firmware now** (Aktualisierung der Firmware für das Managementmodul jetzt zulassen)
- **Do none of the above** (Keine der zuvor genannten Funktionen ausführen)

Blade-Server-Verwaltungsnetz konfigurieren

Sie können mithilfe der Webschnittstelle das Verwaltungsnetz für einen Blade-Server konfigurieren.

Gehen Sie wie folgt vor, um das Verwaltungsnetz für einen Blade-Server zu konfigurieren:

1. Klicken Sie im Navigationsfenster unter **Blade Tasks** (Blade-Tasks) auf **Configuration** (Konfiguration).

   Anmerkung:
   - Informationen zum Aktivieren oder Inaktivieren der IPv6-Adressierung für Ihre BladeCenter-Einheit finden Sie im Abschnitt „Ethernet-Anschluss des Managementmoduls konfigurieren" auf Seite 19.
   - Wenn ein Blade-Server die IPv6-Adressierung unterstützt und IPv6 aktiviert ist, werden die Konfigurationsfelder für die IPv4- und die IPv6-Konfiguration beide angezeigt. Wenn ein Blade-Server keine IPv6-Adressierung unterstützt oder wenn die IPv6-Adressierung inaktiviert ist und Sie ausgewählt haben, in diesem Fall die IPv6-Felder zu verbergen, werden nur die Konfigurationsfelder für die IPv4-Konfiguration angezeigt.
   - Wenn die IPv6-Adressierung aktiviert ist und ein Blade-Server die IPv6-Adressierung unterstützt, muss mindestens eine IPv6-Konfigurationsmethode konfiguriert werden.
2. Wählen Sie die Registerkarte **Management Network** (Verwaltungsnetz) aus.
3. Klicken Sie im Abschnitt **Interface Management** (Schnittstellenverwaltung) im Feld **Name** (Name) auf den Link für den Blade-Server, den Sie konfigurieren möchten.
4. Wählen Sie die Registerkarte für die zu konfigurierende Verwaltungsschnittstelle **eth0** oder **eth1** aus.
5. Konfigurieren Sie die Einstellungen für IPv4 und IPv6 im Abschnitt **General Settings** (Allgemeine Einstellungen):
   - **Enable/Disable NIC** (NIC aktivieren/inaktivieren (Network Interface Card, Netzschnittstellenkarte)): Aktiviert oder inaktiviert diese Verwaltungsnetzschnittstelle. Wenn die Schnittstelle inaktiviert ist, werden alle anderen Konfigurationselemente ignoriert.
   - **Enable/Disable IPv6** (IPv6 aktivieren/inaktivieren): Aktiviert oder inaktiviert die IPv6-Adressierung für diese Verwaltungsnetzschnittstelle.
   - **VLAN ID** (VLAN-ID): (Optional) Die VLAN-ID für diese Verwaltungsnetzschnittstelle.
   - **Route traffic through** (Datenverkehr leiten über): (Optional) Die Einheit, die diese Verwaltungsnetzschnittstelle für die Datenfernverarbeitung nutzt.
   - **Mac address** (read only) (MAC-Adresse (schreibgeschützt)): Die MAC-Adresse dieser Netzschnittstelle für den Blade-Systemmanagementprozessor (BSMP) des Blade-Servers.

6. Einstellungen im Abschnitt **IPv4** konfigurieren:
   - **DHCP**: Wählen Sie eine der folgenden Optionen aus:
     - **Enabled: Obtain IP config. from DHCP server** (Aktiviert: IP-Konfiguration vom DHCP-Server beziehen)
     - **Disabled: Use static IP configuration** (Inaktiviert: Statische IP-Konfiguration verwenden)
     - **Try DHCP server. If it fails, use static IP config.** (DHCP-Server versuchen. Bei Fehlschlagen statische IP-Konfig. verwenden.) (Die Standardeinstellung. Das Zeitlimit für DHCP läuft nach 2 Minuten ab.)

     Anmerkung: Wenn für die DHCP-Einstellung die Option **Try DHCP server. If it fails, use static IP config.** (DHCP-Server versuchen. Bei Fehlschlag statische IP-Konfiguration verwenden.) ausgewählt ist, verwendet die Verwaltungsnetzschnittstelle die statische IP-Adresse, wenn der DHCP-Server beim Systemstart nicht verfügbar ist. In diesem Fall ist die IP-Adresse möglicherweise nicht erreichbar, wenn mehrere Einheiten mit derselben statischen IP-Adresse gestartet wurden.
   - **IP address** (IP-Adresse): Die IPv4-IP-Adresse der Verwaltungsnetzschnittstelle muss aus vier Ganzzahlen von 0 bis 255 bestehen, die durch Punkte getrennt sind, und darf keine Leerzeichen oder aufeinanderfolgenden Punkte enthalten.
   - **Subnet mask** (Teilnetzmaske): Die Teilnetzmaske muss aus vier Ganzzahlen von 0 bis 255 bestehen, die durch Punkte getrennt sind, und darf keine Leerzeichen enthalten.
   - **Gateway address** (Gateway-Adresse): Die IP-Adresse des Netzgatewayrouters muss aus vier Ganzzahlen von 0 bis 255 bestehen, die durch Punkte getrennt sind, und darf keine Leerzeichen enthalten. Diese Adresse muss von der IP-Adresse und der Teilnetzmaske, die oben angegeben wurden, erreichbar sein.
7. Einstellungen im Abschnitt **IPv6** konfigurieren:
   - **Static IP configuration** (Statische IP-Konfiguration): Aktivieren oder inaktivieren Sie die statische IPv6-Adressierung für die Verwaltungsnetzschnittstelle. Die statische IPv6-IP-Konfiguration ist standardmäßig inaktiviert.
   - **IP address** (IP-Adresse): Die IPv6-IP-Adresse der Verwaltungsnetzschnittstelle muss aus 16 hexadezimalen Bytes bestehen, die paarweise angeordnet und durch Doppelpunkte getrennt sind, wie im folgenden Format: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A.
   - **Prefix length** (Präfixlänge): Die Länge des Präfixes für die IPv6-Adresse kann zwischen einschließlich 1 und 128 Zeichen liegen.
   - **Default route** (Standardroute): Die IP-Adresse Ihres Netzgatewayrouters muss aus 16 hexadezimalen Bytes bestehen, die paarweise angeordnet und durch Doppelpunkte getrennt sind, wie im folgenden Format: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A.
   - **Link-local address** (Lokale Verbindungsadresse): (schreibgeschützt) Eine eindeutige IPv6-Adresse für die Verwaltungsnetzschnittstelle, die anhand der MAC-Adresse automatisch generiert wird.

- **DHCPv6**: Wählen Sie eine der folgenden Optionen aus:
  - **Enabled** (Aktiviert): IP-Konfiguration vom DHCP-Server erhalten (Standardeinstellung).
  - **Disabled** (Inaktiviert): IP-Konfiguration nicht vom DHCP-Server erhalten
- **Stateless Auto-configuration** (Statusunabhängige automatische Konfiguration): Aktivieren oder inaktivieren Sie die statusunabhängige automatische Konfiguration für die Verwaltungsnetzschnittstelle. Die automatische Konfiguration von Adressen basiert auf dem Empfang von Routermitteilungen. Diese Mitteilungen enthalten statusunabhängige Adresspräfixe. Die statusunabhängige automatische Konfiguration ist standardmäßig aktiviert.

8. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).

Wenn die Konfiguration des Verwaltungsnetzes für den Blade-Server geändert wird, dauert es möglicherweise einige Minuten, bevor das erweiterte Managementmodul die neuen Werte anzeigen kann.

Kommunikation mit der IBM Systems Director-Software

IBM Systems Director ist eine Basis für die Plattformverwaltung, mit der die Verwaltung physischer und virtueller Systeme in einer heterogenen Umgebung optimiert wird. IBM Systems Director unterstützt mithilfe von Industriestandards mehrere Betriebssysteme und Virtualisierungstechnologien für x86-Plattformen von IBM und anderen Anbietern.

Bei dem Programm IBM Systems Director handelt es sich um ein Systemmanagementprodukt, das mit einigen BladeCenter-Einheiten ausgeliefert wird. Die IBM Systems Director-Software kommuniziert mit der BladeCenter-Einheit über den Ethernet-Anschluss am aktiven Managementmodul. Weitere Informationen zu IBM Systems Director finden Sie in der Dokumentation auf der *IBM Systems Director-CD*, die mit dem Server ausgeliefert wird und auf der Webseite zu IBM xSeries® Systemmanagement unter http://www.ibm.com/systems/management/. Hier finden Sie eine Übersicht über IBM Systemmanagement und IBM Systems Director. Auf dieser Seite wird darüber hinaus auch angegeben, welche Version von IBM Director für die Verwaltung redundanter Managementmodule mindestens erforderlich ist.

Damit Sie die Empfänger der fernen Alerts für IBM Director over LAN konfigurieren können, muss es sich beim Empfänger der fernen Alerts um einen IBM Systems Director-fähigen Server handeln.

Um mit der BladeCenter-Einheit kommunizieren zu können, benötigt die IBM Systems Director-Software ein verwaltetes Objekt (auf der Seite "Group Contents" (Gruppeninhalte) des Hauptfensters der IBM Systems Director-Managementkonsole), das die BladeCenter-Einheit repräsentiert. Wenn die IP-Adresse des BladeCenter-Managementmoduls bekannt ist, kann der Netzadministrator ein verwaltetes IBM Systems Director-Objekt für die Einheit erstellen. Wenn die IP-Adresse nicht bekannt ist, kann die IBM Systems Director-Software die BladeCenter-Einheit automatisch erkennen (Out-of-band, mithilfe des Ethernet-Anschlusses am BladeCenter-Managementmodul) und ein verwaltetes Objekt für die Einheit erstellen.

Damit die IBM Systems Director-Software die BladeCenter-Einheit erkennen kann, muss Ihr Netz von Anfang an eine funktionsfähige Verbindung zwischen dem IBM Systems Director-Server und dem Ethernet-Anschluss des BladeCenter-Managementmoduls bereitstellen.

Um eine funktionsfähige Verbindung herzustellen, versucht das Managementmodul mithilfe von DHCP, die IP-Startadresse für den Ethernet-Anschluss abzurufen. Wenn die DHCP-Anforderung fehlschlägt, verwendet das Managementmodul nach 2 Minuten die ihm zugewiesene statische IP-Adresse. Daher muss sich der DHCP-Server (sofern er verwendet wird) im Management-LAN für Ihre BladeCenter-Einheit befinden.

Anmerkungen:

1. Alle Managementmodule sind mit derselben statischen IP-Adresse vorkonfiguriert. Sie können die Webschnittstelle des Managementmoduls verwenden, um den einzelnen BladeCenter-Einheiten eine neue statische IP-Adresse zuzuweisen. Wenn DHCP nicht verwendet wird und Sie den einzelnen BladeCenter-Einheiten keine neue statische IP-Adresse zuweisen, bevor Sie versuchen, mit der IBM Systems Director-Software zu kommunizieren, kann immer jeweils nur eine BladeCenter-Einheit im Netz zur Erkennung hinzugefügt werden. Wenn mehrere Einheiten ohne eindeutige IP-Adresszuweisung für die einzelnen BladeCenter-Einheiten zum Netz hinzugefügt werden, führt dies zu IP-Adresskonflikten.
2. Für die Kommunikation zwischen einem E/A-Modul und einer Fernverwaltungsstation, wie z. B. einem Verwaltungsserver, auf dem IBM Systems Director Server ausgeführt wird, über den externen Ethernet-Anschluss des Managementmoduls müssen sich die interne Netzschnittstelle des E/A-Moduls und die interne und externe Schnittstelle des Managementmoduls im gleichen Teilnetz befinden.

Erweiterte Funktionen

Die folgenden Themen enthalten Anweisungen zum Ausführen einiger Funktionen, die von der Webschnittstelle des Managementmoduls unterstützt werden.

- „Netz- und Sicherheitskonfiguration" auf Seite 28
- „Wake on LAN konfigurieren" auf Seite 72
- „Konfigurationsdatei verwenden" auf Seite 75
- „Funktion für ferne Konsole verwenden" auf Seite 80
- „Funktion für ferne Datenträger verwenden" auf Seite 81
- „Automatische Erkennung des Verwaltungskanals verwenden" auf Seite 83
- „IBM Service Advisor" auf Seite 86

Eine ausführliche Beschreibung der Webschnittstelle des Managementmoduls finden Sie in Kapitel 3, „Überblick über die Webschnittstelle des Managementmoduls", auf Seite 99.

Netz- und Sicherheitskonfiguration

Die folgenden Themen beschreiben die Konfiguration der Parameter zu Netzbetrieb und Sicherheit des Managementmoduls für verschiedene Standardprotokolle.

- SNMP und DNS (siehe „SNMP (Simple Network Management Protocol) konfigurieren")
- SMTP (siehe „SMTP (Simple Mail Transfer Protocol) konfigurieren" auf Seite 32)
- SSL und LDAP (siehe „LDAP konfigurieren" auf Seite 32)
- Sicherer Web-Server und sichere LDAP-Verbindung (siehe „Sicherer Web-Server und sichere LDAP-Verbindung" auf Seite 52)
- SSH (siehe „SSH-Server konfigurieren (Secure Shell)" auf Seite 64)
- SMASH (siehe „SMASH aktivieren" auf Seite 69)
- Syslog (siehe „Syslog aktivieren" auf Seite 70)
- TFTP unter Linux (siehe „Linux-TFTP-Server konfigurieren" auf Seite 72)

SNMP (Simple Network Management Protocol) konfigurieren

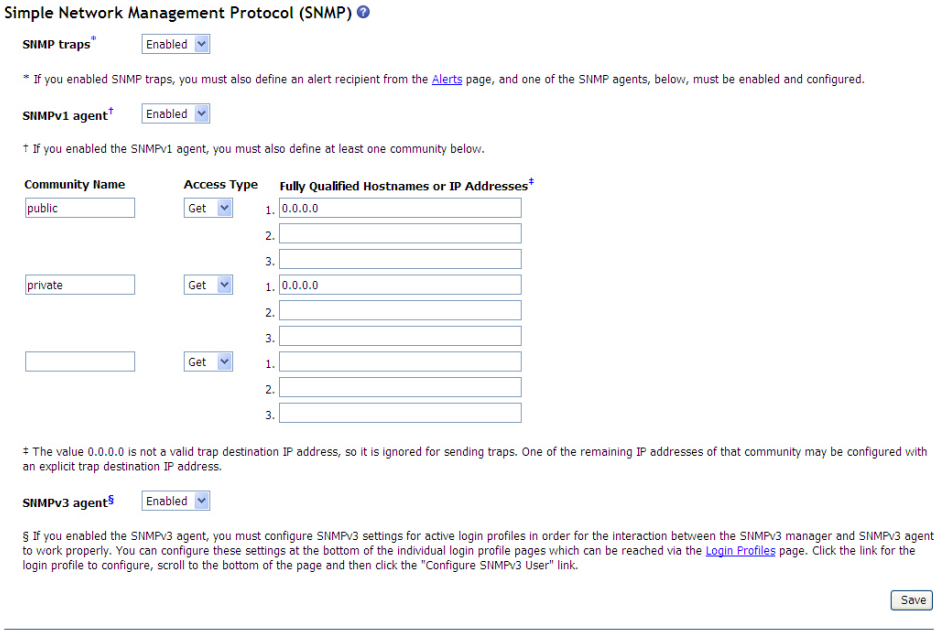
Sie können über eine Abfrage des SNMP-Agenten die sysgroup-Informationen erfassen und konfigurierte SNMP-Alerts an die konfigurierten Hostnamen oder IP-Adressen senden.

Anmerkung: Wenn Sie vorhaben, SNMP-Traps (Simple Network Management Protocol) im Managementmodul zu konfigurieren, müssen Sie die Management Information Base (MIB) auf Ihrem SNMP-Manager installieren und kompilieren. Die MIB unterstützt SNMP-Traps. Die MIB ist im Aktualisierungspaket der Firmware des Managementmoduls enthalten, das Sie von der folgenden Adresse heruntergeladen haben: http://www.ibm.com/systems/support/.

Gehen Sie wie folgt vor, um SNMP zu konfigurieren:

1. Melden Sie sich an dem Managementmodul an, in dem Sie SNMP konfigurieren möchten. Weitere Informationen finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **MM Control → General Settings** (MM-Steuerung → Allgemeine Einstellungen). Geben Sie auf der Informationsseite des Managementmoduls, die nun angezeigt wird, die folgenden Daten ein:
   - **Name** (Name): Der Name, den Sie zur Identifizierung des Managementmoduls verwenden möchten. Der Name wird in E-Mail- und SNMP-Alertbenachrichtigungen angeführt, um die Quelle des Alerts anzugeben. Wenn in einer BladeCenter-Einheit mehrere Managementmodule installiert sind, kann jedem Managementmodul ein eindeutiger Name gegeben werden.
   - **Contact** (Ansprechpartner): Der Name und die Rufnummer der Person, die als Ansprechpartner zur Verfügung steht, wenn ein Fehler an der BladeCenter-Einheit auftritt.
   - **Location** (Position): Hinreichend ausführliche Angaben, um die BladeCenter-Einheit zu Wartungs- oder anderen Zwecken rasch lokalisieren zu können.
3. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).

4. Klicken Sie im Navigationsfenster auf **MM Control → Network Protocols** (MM-Steuerung → Netzprotokolle) und klicken Sie dann auf den Link **Simple Network Management Protocol (SNMP)**. Eine ähnliche Seite wie in der folgenden Abbildung wird angezeigt.



5. Wählen Sie in den entsprechenden Feldern des SNMP-Agenten sowie im Feld **SNMP traps** (SNMP-Traps) die Option **Enabled** (Aktiviert) aus, um Alerts an die SNMP-Communitys und -Benutzer in Ihrem Netz weiterzuleiten. Folgende Kriterien müssen erfüllt sein, damit Sie einen SNMP-Agenten aktivieren können:
   - Auf der Seite "General Settings" (Allgemeine Einstellungen) müssen Systemkontakte angegeben sein.
   - Auf der Seite "General Settings" (Allgemeine Einstellungen) muss die Systemadresse angegeben sein.
   - Bei SNMPv1 muss mindestens ein Community-Name angegeben werden, wobei für jeden Community-Namen ein Zugriffstyp festgelegt werden muss:
     - **Get** (Abrufen): Alle Hosts in der Community können MIB-Objekte abfragen und Traps empfangen.
     - **Set** (Festlegen): Alle Hosts in der Community können MIB-Objekte abfragen und festlegen sowie Traps empfangen.
     - **Trap**: Alle Hosts in der Community können Traps empfangen.
   - Für jede Community muss mindestens eine gültige IP-Adresse oder ein gültiger Hostname (wenn DNS aktiviert ist) angegeben werden.
   - Bei SNMPv3 müssen alle SNMPv3-Benutzer konfiguriert werden.

   Anmerkung: Alertempfänger mit der Benachrichtigungsmethode SNMP erhalten Alerts nur, wenn sowohl der SNMP-Agent als auch die SNMP-Traps aktiviert sind.

6. Wenn Sie den SNMPv1-Agenten aktivieren, führen Sie die unten beschriebenen Schritte aus, um eine Community zu konfigurieren, die die administrative Beziehung zwischen SNMP-Agenten und SNMP-Managern definiert. Andernfalls fahren Sie mit Schritt 7 fort. Sie müssen mindestens eine SNMPv1-Community definieren. Jede Community-Definition enthält folgende Parameter:
   - Community name (Community-Name)
   - Host name or IP address (Hostname oder IP-Adresse)

   Wenn einer dieser Parameter nicht korrekt ist, kann der SNMP-Verwaltungszugriff nicht garantiert werden.

   Anmerkungen:
   - Wenn ein Fenster mit einer Fehlernachricht angezeigt wird, nehmen Sie in den Feldern, die im Fehlerfenster aufgeführt sind, die notwendigen Korrekturen vor. Blättern Sie anschließend zum Seitenende und klicken Sie auf **Save** (Speichern), um die korrigierten Daten zu speichern. Sie müssen mindestens eine Community konfigurieren, um den SNMP-Agenten zu aktivieren.
   - Sie können in der ersten Position der ersten Community eine IP-Adresse mit Platzhalterzeichen festlegen (0.0.0.0 für IPv4 oder 0::0 für IPv6), wobei für den Zugriffstyp der Wert "SET" (Festlegen) ausgewählt ist. Diese Community-Adresse unterstützt GET- und SET-Operationen (Operationen zum Abrufen und zum Festlegen) von allen IP-Adressen. Die verbleibenden acht Community-Adressen aktivieren spezifische IP-Adressen oder Hostadressen, um einen Empfänger für Traps anzugeben.

   a. Geben Sie im Feld **Community Name** (Community-Name) einen Namen oder eine Zeichenfolge zur Authentifizierung ein, um die Community zu benennen.
   b. Wählen Sie den **Access Type** (Zugriffstyp) für die Community aus.
   c. Geben Sie im entsprechenden Feld **Host Name** (Hostname) oder **IP Address** (IP-Adresse) den Hostnamen oder die IP-Adresse der einzelnen Community-Manager ein.
7. Führen Sie je nach Verfügbarkeit von DNS-Servern einen der folgenden Schritte aus:
   - Wenn in Ihrem Netz kein DNS-Server zur Verfügung steht, blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).
   - Wenn ein DNS-Server in Ihrem Netz zur Verfügung steht, blättern Sie weiter zum Abschnitt **Domain Name System (DNS)**. Eine ähnliche Seite wie in der folgenden Abbildung wird angezeigt.

8. Wenn mindestens ein DNS-Server in Ihrem Netz zur Verfügung steht, wählen Sie im Feld **DNS** die Option **Enabled** (Aktiviert) aus. Das Feld **DNS** gibt an, ob Sie in Ihrem Netz einen DNS-Server verwenden, um Hostnamen in IP-Adressen zu übersetzen.

9. (Optional) Wenn sowohl DNS als auch IPv6-Adressierung aktiviert sind, können Sie im Feld **Preferred DNS Servers** (Bevorzugte DNS-Server) angeben, welche IP-Adressen zuerst verwendet werden sollen, wenn für die DNS-Server sowohl IPv6- als auch IPv4-IP-Adressen angegeben werden (die Standardeinstellung lautet IPv6).
10. (Optional) Wenn Sie DNS aktiviert haben, aktivieren Sie das Kontrollkästchen **Send DDNS updates to these servers** (DDNS-Aktualisierungen an diese Server senden), um DNS-Informationen an die DDNS-Server (Dynamic Domain Name System) zu senden.
11. (Optional) Wenn Sie DNS aktiviert haben, geben Sie in den Feldern **DNS server IP address** (DNS-Server-IP-Adresse) die IP-Adressen von bis zu drei DNS-Servern, jeweils für IPv4 und IPv6, in Ihrem Netz an.
12. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).
13. Wenn Sie den SNMPv3-Agenten aktivieren, führen Sie die unten beschriebenen Schritte aus, um das SNMPv3-Profil für die einzelnen SNMPv3-Benutzer zu konfigurieren. Andernfalls ist die Konfiguration abgeschlossen.
    a. Klicken Sie auf den Link **Login Profiles** (Anmeldeprofile) im Abschnitt "Simple Network Management Protocol (SNMP)" oder klicken Sie im Navigationsfenster auf **MM Control → Login Profiles** (MM-Steuerung → Anmeldeprofile).
    b. Wählen Sie den Benutzer aus, der konfiguriert werden soll, und klicken Sie dann auf den Link **Configure SNMPv3 User** (SNMPv3-Benutzer konfigurieren) unten auf der Seite des Anmeldeprofils. Eine ähnliche Seite wie in der folgenden Abbildung wird angezeigt.

    c. Geben Sie die Daten zur SNMPv3-Konfiguration für diesen Benutzer an und klicken Sie auf **Save** (Speichern).

       Anmerkung: Wenn die Sicherheitseinstellungen Kennwörter verlangen, kann für das SNMPv3-Authentifizierungsprotokoll nicht der Wert "None" (Keine) angegeben werden, wenn der Benutzer über den Zugriffstyp GET oder SET (Abrufen oder Festlegen) verfügt. Dies bedeutet, dass, wenn Kennwörter erforderlich sind, ein Benutzer nur dann SNMP-Traps empfangen kann, wenn das SNMPv3-Authentifizierungsprotokoll den Wert "None" (Keine) aufweist.
    d. Wiederholen Sie die Schritte 13b und 13c für jeden SNMPv3-Benutzer.

SMTP (Simple Mail Transfer Protocol) konfigurieren

Sie können einen SMTP-Server (Simple Mail Transfer Protocol) so konfigurieren, dass beim Auftreten von Ereignissen im Managementmodul E-Mail-Benachrichtigungen gesendet werden.

Gehen Sie wie folgt vor, um die IP-Adresse oder den Hostnamen des SMTP-Servers (Simple Mail Transfer Protocol) anzugeben.

Anmerkung: Wenn Sie einen SMTP-Server für Alertbenachrichtigungen per E-Mail einrichten möchten, stellen Sie sicher, dass der Name im Feld **Name** (Name) im Abschnitt **MM Information** (MM-Informationen) der Seite **MM Control → General Settings** (MM-Steuerung → Allgemeine Einstellungen) gültig ist, wenn er als Teil einer E-Mail-Adresse verwendet wird (z. B. darf der Name keine Leerzeichen enthalten).

1. Melden Sie sich an dem Managementmodul an, in dem Sie SMTP (Simple Mail Transfer Protocol) konfigurieren möchten. Weitere Informationen finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **MM Control → Network Protocols** (MM-Steuerung → Netzprotokolle) und blättern Sie nach unten zum Abschnitt **Simple Mail Transfer Protocol (SMTP)**.

3. Geben Sie im Feld **SMTP server host name or IP address** (Hostname oder IP-Adresse des SMTP-Servers) den Hostnamen des SMTP-Servers ein. Geben Sie in diesem Feld die IP-Adresse oder, wenn DNS aktiviert und konfiguriert ist, den Hostnamen des SMTP-Servers ein.
4. Blättern Sie weiter zum Seitenende und klicken Sie auf **Save** (Speichern).

LDAP konfigurieren

Sie können LDAP (Lightweight Directory Access Protocol) konfigurieren, um Managementmodulbenutzer authentifizieren zu können.

Das erweiterte Managementmodul unterstützt sowohl die lokale als auch die ferne Benutzerauthentifizierung. Für die lokale Authentifizierung werden die Daten verwendet, die auf der Seite **MM Control → Login Profiles** (MM-Steuerung → Anmeldeprofile) angegeben werden, um Benutzer zu authentifizieren. Mithilfe eines LDAP-Servers kann ein Managementmodul einen Benutzer durch Abfragen oder Durchsuchen eines LDAP-Verzeichnisses auf einem fernen LDAP-Server ohne Abfragen der lokalen Benutzerdatenbank authentifizieren.

Wenn Sie eine Form der fernen Authentifizierung verwenden, können Sie auswählen, ob die Berechtigungen für die einzelnen erfolgreich authentifizierten Benutzer entweder lokal oder auf der Grundlage von Daten erteilt werden, die auf dem für die ferne Authentifizierung verwendeten LDAP-Server gespeichert sind. Die Berechtigungen, die für einen Benutzer erteilt werden, geben die Aktionen an, die der jeweilige Benutzer ausführen kann, während er am erweiterten Managementmodul angemeldet ist.

Die drei fernen Authentifizierungsmethoden werden in den folgenden Themen beschrieben:

- „Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen”
- „Rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory” auf Seite 37
- „Traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP” auf Seite 41

Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen:

Mithilfe von Active Directory können Sie die ferne LDAP-Authentifizierung mit lokaler Erteilung von Benutzerberechtigungen für Benutzer konfigurieren.

Anmerkung: Die Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen kann nur bei BladeCenter-Einheiten in einer Active Directory-Umgebung angewendet werden.

Wenn die Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen verwendet wird, werden die Active Directory-Server nur zum Authentifizieren von Benutzern, also zum Überprüfen der Berechtigungsnachweise für Benutzer, verwendet. Auf dem Active Directory-Server werden keine Berechtigungsdaten für einen bestimmten Benutzer gespeichert. Die im erweiterten Managementmodul gespeicherten Gruppenprofile müssen mit Berechtigungsdaten konfiguriert werden.

Die zum Konfigurieren der Gruppenprofile verwendeten Berechtigungsdaten können durch Abrufen von Daten zur Mitgliedschaft für einen Benutzer vom Active Directory-Server angefordert werden. Diese Daten zur Mitgliedschaft enthalten eine Liste der Gruppen, denen ein Benutzer angehört (verschachtelte Gruppen werden unterstützt). Die auf dem Active Directory-Server angegebenen Gruppen werden mit den auf dem erweiterten Managementmodul lokal konfigurierten Gruppennamen verglichen. Für jede übereinstimmende Gruppe werden dem Benutzer Berechtigungen für die jeweilige Gruppe zugewiesen. Das heißt, für jeden Gruppennamen, der auf dem erweiterten Managementmodul lokal konfiguriert ist, gibt es ein entsprechendes Berechtigungsprofil, das auch für die jeweilige Gruppe konfiguriert ist.

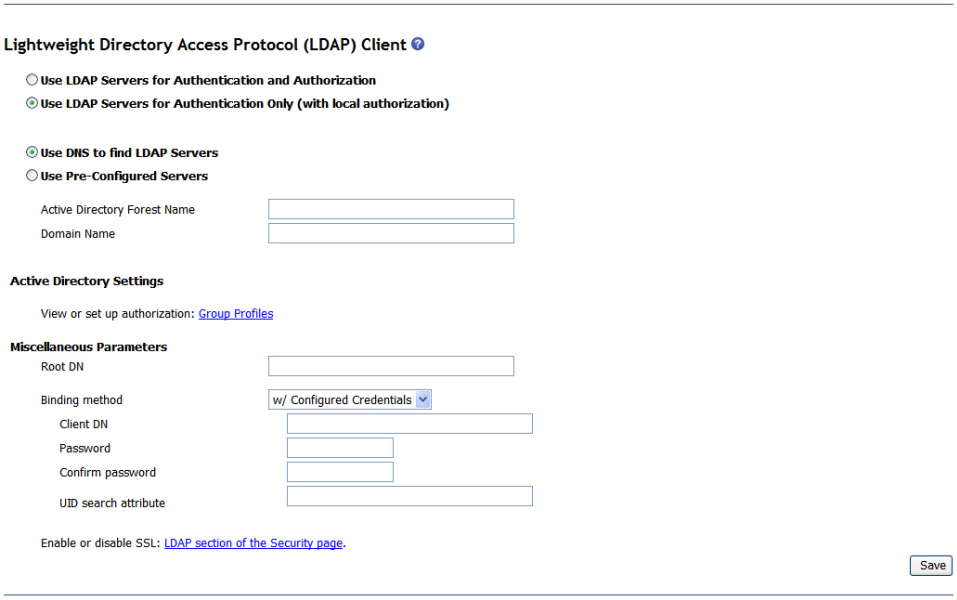
Das erweiterte Managementmodul unterstützt bis zu 16 lokal konfigurierte Gruppennamen. Jeder Gruppenname darf aus maximal 63 Zeichen bestehen. Eines der folgenden Attribute muss als Gruppenname konfiguriert werden, um mit den von den Active Directory-Servern abgerufenen Daten zur Gruppenmitgliedschaft abgeglichen werden zu können:

- Definierter Name
- Das Attribut "cn"
- Das Attribut "name"
- Das Attribut "sAMAccountName"

Gehen Sie wie folgt vor, um die Active Directory-Authentifizierung mit lokaler Erteilung von Berechtigungen für das erweiterte Managementmodul zu konfigurieren:

1. Klicken Sie im Navigationsfenster auf **MM Control → Network Protocols** (MM-Steuerung → Netzprotokolle).
2. Blättern Sie abwärts bis zum Abschnitt **Lightweight Directory Access Protocol (LDAP) Client** (LDAP-Client (Lightweight Directory Access Protocol)).

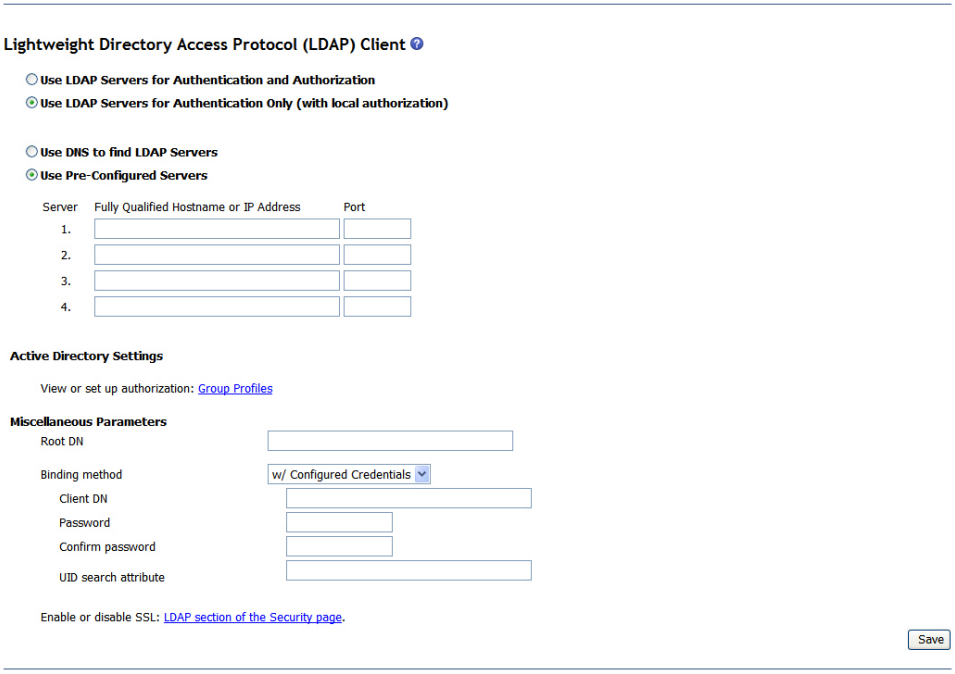
3. Wählen Sie **Use LDAP Servers for Authentication Only (with local authorization)** (Nur LDAP-Server für Authentifizierung verwenden (mit lokaler Erteilung von Berechtigungen)) aus.
4. Die für die Authentifizierung zu verwendenden Domänencontroller können entweder manuell konfiguriert oder mithilfe von DNS SVR-Datensätzen dynamisch ermittelt werden.
   - Wählen Sie **Use DNS to find LDAP Servers** (DNS für die Suche nach LDAP-Servern verwenden) aus, damit die Domänencontroller anhand von DNS SVR-Datensätzen dynamisch ermittelt werden (siehe Schritt 5).
   - Wählen Sie **Use Pre-Configured LDAP Servers** (Vorkonfigurierte LDAP-Server verwenden; Standardeinstellung) aus, um die Domänencontroller manuell zu konfigurieren (siehe Schritt 6).
5. Wenn Sie DNS zum dynamischen Ermitteln von Domänencontrollern verwenden, konfigurieren Sie zunächst die folgenden Einstellungen. Fahren Sie anschließend mit Schritt 7 auf Seite 35 fort.



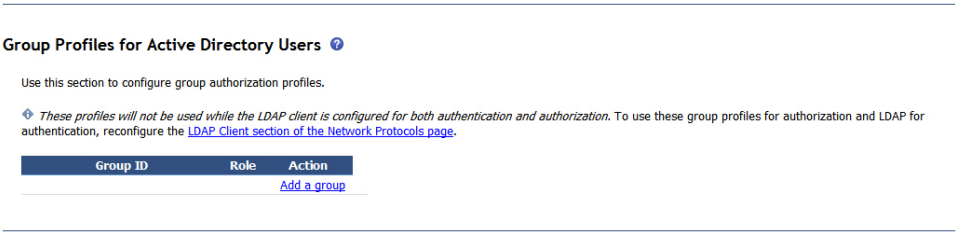
Domain Name (Domänenname)
Der vollständig qualifizierte Domänenname des Domänencontrollers. Der Domänenname wird zum Suchen nach dem Domänencontroller benötigt.

Active Directory Forest Name (Name der Active Directory-Gesamtstruktur)
Dieser optionale Parameter wird zum Ermitteln globaler Kataloge (GC, Global Catalog) verwendet. Globale Kataloge werden für Benutzer benötigt, die universellen Gruppen in mehreren Domänen angehören. In Umgebungen, in denen eine domänenübergreifende Gruppenzugehörigkeit nicht zulässig ist, muss dieses Feld nicht ausgefüllt werden.

6. Wenn Sie die Domänencontroller und globalen Kataloge manuell konfigurieren, konfigurieren Sie zunächst die Felder **LDAP Server Host Name or IP Address** (Hostname oder IP-Adresse des LDAP-Servers) und **Port** (Anschluss). Fahren Sie anschließend mit Schritt 7 auf Seite 35 fort. Mit einer IP-Adresse oder einem vollständig qualifizierten Hostnamen können bis zu vier Domänencontroller konfiguriert werden. Server für globale Kataloge werden anhand der Anschlussnummer 3268 oder 3269 identifiziert: Eine andere Anschlussnummer gibt an, dass ein Domänencontroller konfiguriert wurde.



7. Wenn Sie Gruppenberechtigungsprofile verwenden, zeigen Sie diese an oder konfigurieren Sie sie, indem Sie auf **Group Profiles** (Gruppenprofile) klicken. Kehren Sie anschließend zur Seite **MM Control → Network Protocols** (MM-Steuerung → Netzprotokolle) zurück und blättern Sie abwärts bis zum Abschnitt **Lightweight Directory Access Protocol (LDAP) Client** (LDAP-Client (Lightweight Directory Access Protocol)).



8. Konfigurieren Sie die folgenden **sonstigen Parameter**:

Root DN (Definierter Name des Stammelements)

Dieser optionale Parameter wird verwendet, um den Basis-DN des Active Directory-Servers zu konfigurieren (z. B. dn=companyABC,dn=com). Dieses Feld wird in der Regel nicht ausgefüllt, obwohl es bei der Fehlerbehebung durchaus hilfreich sein kann.

Das erweiterte Managementmodul sucht mithilfe der Root-DSE-Abfrage nach dem Basis-DN des Active Directory-Servers, mit dem es kommuniziert. Dieser Basis-DN wird dann für nachfolgende Suchvorgänge verwendet. Der Basis-DN wird von den über die Root-DSE-Abfrage abgerufenen Attributen `defaultNamingContext` und `rootDomaintNamingContext` abgeleitet. Wenn der Basis-DN mithilfe des Felds **Root DN** (Definierter Name des Stammelements) festgelegt wird, werden die Attribute `defaultNamingContext` und `rootDomaintNamingContext` überschrieben.

Binding Method (Bindungsmethode)

Wählen Sie bei einleitenden Verbindungen mit dem Server des Domänencontrollers eine der folgenden Optionen aus:

w/ Configured Credentials (Mit konfiguriertem Berechtigungsnachweis): Geben Sie für den Client den definierten Namen (**Client DN**) und das Kennwort (**Password**) an, die für die einleitende Verbindung verwendet werden sollen. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden. Wenn die Verbindung erfolgreich hergestellt werden kann, wird nach einem Benutzersatz gesucht, der mit dem im Feld **Client DN** (Definierter Name des Clients) eingegebenen Namen übereinstimmt. Bei der Suche wird in der Regel nach allgemeinen Attributen gesucht, die möglicherweise mit der bei der Anmeldung eingegebenen Benutzer-ID übereinstimmen. Zu diesen Attributen zählen die Attribute `displayName`, `sAMAccountName` und `userPrincipalName`. Wenn das Feld **UID search attribute** (Suchattribut für Benutzer-ID) konfiguriert wird, bezieht sich die Suche darüber hinaus auch auf dieses Attribut.

Wenn die Suche erfolgreich ist, wird versucht, eine zweite Verbindung, diesmal mit dem definierten Benutzernamen (über die Suche abgerufen) und dem bei der Anmeldung angegebenen Kennwort, herzustellen. Wenn die zweite Verbindung hergestellt werden kann, verläuft die Authentifizierung erfolgreich und die Daten zur Gruppenzugehörigkeit für den Benutzer werden abgerufen und mit den auf dem erweiterten Managementmodul konfigurierten Gruppen abgeglichen. Die übereinstimmenden Gruppen definieren die Berechtigungen, die dem Benutzer zugewiesen werden.

w/ Login Credentials (Mit Berechtigungsnachweis für die Anmeldung): Die einleitende Verbindung mit dem Server des Domänencontrollers wird mithilfe des bei der Anmeldung angegebenen Berechtigungsnachweises hergestellt. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden. Wenn die Verbindung erfolgreich hergestellt werden kann, wird nach dem Benutzersatz gesucht. Sobald dieser gefunden ist, werden die Daten zur Gruppenzugehörigkeit für den Benutzer abgerufen und mit den auf dem erweiterten Managementmodul konfigurierten Gruppen abgeglichen. Die übereinstimmenden Gruppen definieren die Berechtigungen, die dem Benutzer zugewiesen werden.

9. Um SSL (Secure Sockets Layer) zwischen dem erweiterten Managementmodul und dem Active Directory-Server zu aktivieren oder inaktivieren, klicken Sie auf **LDAP section of the security page** (LDAP-Abschnitt der Sicherheitsseite).

Rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory:

Mithilfe von Active Directory können Sie die ferne Authentifizierung und Erteilung von Berechtigungen mittels LDAP für Benutzer konfigurieren.

Anmerkung:

- Die rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory kann nur bei BladeCenter-Einheiten in einer Active Directory-Umgebung angewendet werden.
- Für die rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory ist das Snap-in für die erweiterte rollenabhängige Sicherheit erforderlich.

Für die rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory werden auf einem Active Directory-Server gespeicherte Konfigurationsdaten verwendet, um einen Benutzer zu authentifizieren und diesem Benutzer anschließend Berechtigungen zuzuweisen.

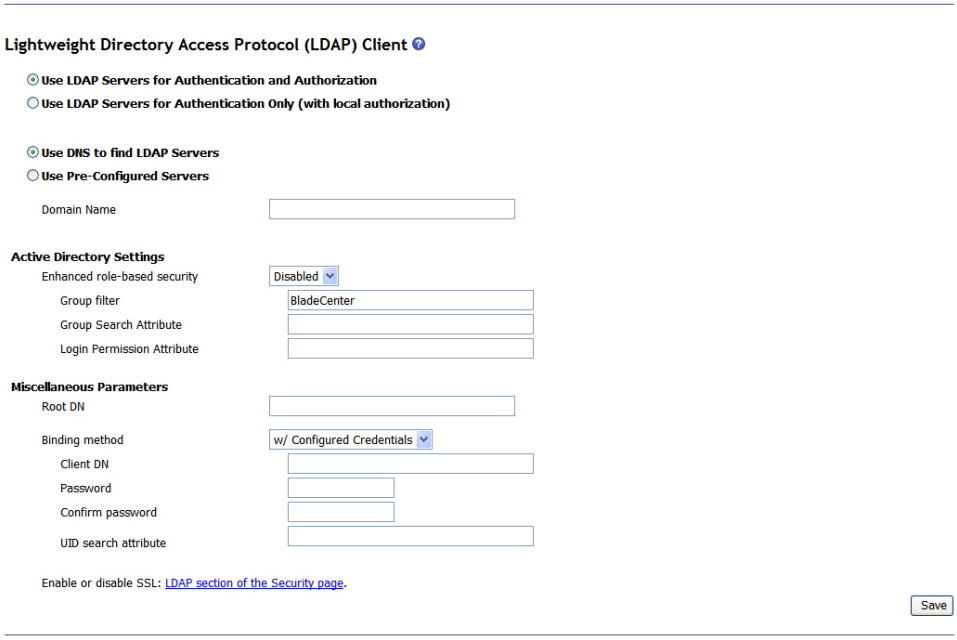
Verwenden Sie vor dem Aktivieren der rollenabhängigen Authentifizierung und Erteilung von Berechtigungen mittels Active Directory das Snap-in für die erweiterte rollenabhängige Sicherheit, um die Konfigurationsdaten auf dem Active Directory-Server zu speichern, der Benutzern Berechtigungen zuweist. Dieses Snap-in kann auf jedem Microsoft Windows-Client ausgeführt und von der Website http://www.ibm.com/systems/support/ heruntergeladen werden.

- Mithilfe des Snap-ins für die erweiterte rollenabhängige Sicherheit können Sie auf einem Active Directory-Server Rollen konfigurieren und diese Rollen Benutzern, Gruppen und erweiterten Managementmodulen zuweisen. Informationen und Anweisungen hierzu finden Sie in der Dokumentation zum Snap-in für die erweiterte rollenabhängige Sicherheit.
- Rollen geben die Benutzern und Gruppen zugewiesenen Berechtigungen sowie die Befehlsziele, wie z. B. das erweiterte Managementmodul oder einen Blade-Server, an, denen eine Rolle zugeordnet ist. Bevor die rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory aktiviert werden kann, müssen auf dem Active Directory-Server Rollen konfiguriert werden.
- Der im Feld **AMM Target Name** (Zielname des erweiterten Managementmoduls) konfigurierte optionale Name gibt ein bestimmtes erweitertes Managementmodul an und kann mithilfe des Snap-ins für die rollenabhängige Sicherheit auf dem Active Directory-Server einer oder mehreren Rollen zugewiesen werden. Hierzu müssen verwaltete Ziele erstellt, diesen bestimmte Namen und anschließend die entsprechenden Rollen zugewiesen werden. Ein konfigurierter **Zielname des erweiterten Managementmoduls** kann bestimmte Rollen für Benutzer und erweiterte Managementmodule (Ziele) definieren, die derselben Rolle angehören. Wenn sich ein Benutzer beim erweiterten Managementmodul anmeldet und er mittels Active Directory authentifiziert wird, werden die Rollen für diesen Benutzer aus dem Verzeichnis abgerufen. Die Berechtigungen, die dem Benutzer zugewiesen werden, werden aus den Rollen extrahiert, die über ein Ziel als Mitglied mit einem Namen verfügen, der dem des hier konfigurierten erweiterten Managementmoduls entspricht, oder die über ein Ziel verfügen, das einem beliebigen erweiterten Managementmodul entspricht. Einem erweiterten Managementmodul kann ein eindeutiger Name zugewiesen werden. Es ist aber auch möglich, dass mehrere erweiterte Managementmodule denselben Zielnamen verwenden. Wenn mehreren erweiterten Managementmodulen derselbe

Zielname zugewiesen wird, werden die erweiterten Managementmodule dadurch zusammengefasst und sie werden derselben Rolle zugeordnet.

Gehen Sie wie folgt vor, um die rollenabhängige Authentifizierung und Erteilung von Berechtigungen mittels Active Directory für das erweiterte Managementmodul zu konfigurieren:

1. Klicken Sie im Navigationsfenster auf **MM Control → Network Protocols** (MM-Steuerung → Netzprotokolle).
2. Blättern Sie abwärts bis zum Abschnitt **Lightweight Directory Access Protocol (LDAP) Client** (LDAP-Client (Lightweight Directory Access Protocol)).
3. Wählen Sie **Use LDAP Servers for Authentication and Authorization** (LDAP-Server für Authentifizierung und Erteilung von Berechtigungen verwenden) aus.
4. Legen Sie für **Enhanced role-based security** (Erweiterte rollenabhängige Sicherheit) die Option **Enabled** (Aktiviert) fest.
5. Die für die Authentifizierung zu verwendenden Domänencontroller können entweder manuell konfiguriert oder mithilfe von DNS SVR-Datensätzen dynamisch ermittelt werden.
   - Wählen Sie **Use DNS to find LDAP Servers** (DNS für die Suche nach LDAP-Servern verwenden) aus, damit die Domänencontroller anhand von DNS SVR-Datensätzen dynamisch ermittelt werden (siehe Schritt 6).
   - Wählen Sie **Use Pre-Configured LDAP Servers** (Vorkonfigurierte LDAP-Server verwenden; Standardeinstellung) aus, um die Domänencontroller manuell zu konfigurieren (siehe Schritt 7 auf Seite 39).
6. Wenn Sie DNS zum dynamischen Ermitteln von Domänencontrollern verwenden, konfigurieren Sie zunächst den Domänennamen des Domänencontrollers. Fahren Sie anschließend mit Schritt 8 auf Seite 39 fort.

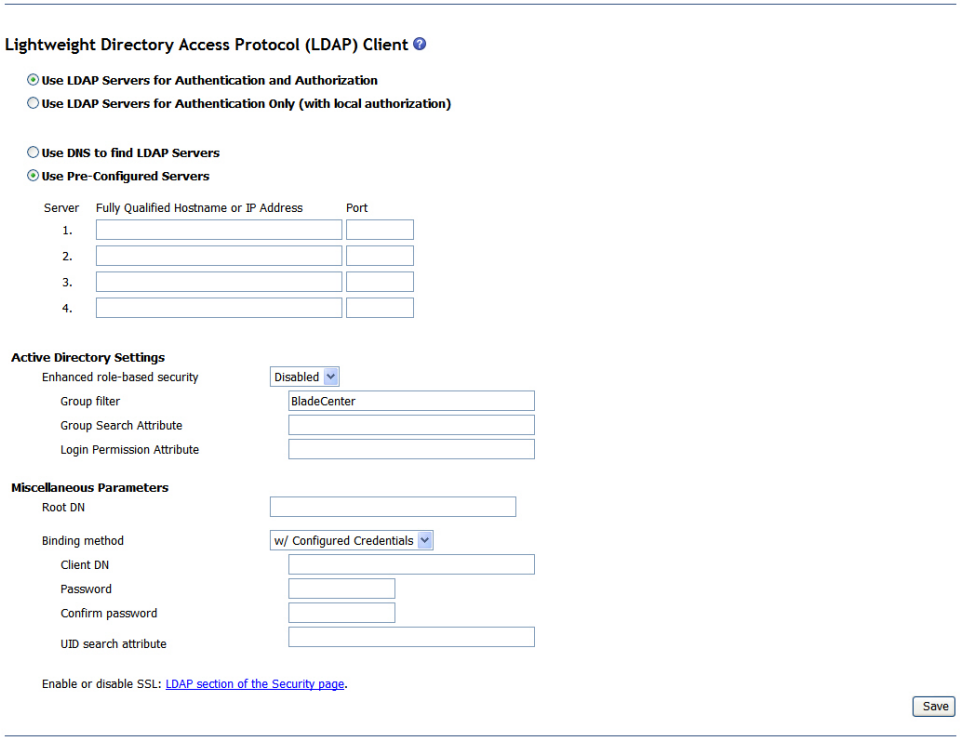


Domain Name (Domänenname)

Der vollständig qualifizierte Domänenname des Domänencontrollers. Der Domänenname wird zum Suchen nach dem Domänencontroller benötigt.

Active Directory Forest Name (Name der Active Directory-Gesamtstruktur)
Bei der rollenabhängigen Authentifizierung und Erteilung von Berechtigungen mittels Active Directory werden die globalen Kataloge nicht verwendet. Füllen Sie dieses Feld daher nicht aus.

7. Wenn Sie die Domänencontroller manuell konfigurieren, konfigurieren Sie zunächst das Feld **LDAP Server Host Name or IP Address** (Hostname oder IP-Adresse des LDAP-Servers). Fahren Sie anschließend mit Schritt 8 fort. Mit einer IP-Adresse oder einem vollständig qualifizierten Hostnamen können bis zu vier Domänencontroller konfiguriert werden.



8. Konfigurieren Sie die folgenden **sonstigen Parameter**:

Root DN (Definierter Name des Stammelements)
Dieser optionale Parameter wird verwendet, um den Basis-DN des Active Directory-Servers zu konfigurieren (z. B. dn=companyABC,dn=com). Dieses Feld wird in der Regel nicht ausgefüllt, obwohl es bei der Fehlerbehebung durchaus hilfreich sein kann.

Das erweiterte Managementmodul sucht mithilfe der Root-DSE-Abfrage nach dem Basis-DN des Active Directory-Servers, mit dem es kommuniziert. Dieser Basis-DN wird dann für nachfolgende Suchvorgänge verwendet. Der Basis-DN wird von den über die Root-DSE-Abfrage abgerufenen Attributen `defaultNamingContext` und `rootDomaintNamingContext` abgeleitet. Wenn der Basis-DN mithilfe des Felds **Root DN** (Definierter Name des Stammelements) festgelegt wird, werden die Attribute `defaultNamingContext` und `rootDomaintNamingContext` überschrieben.

Binding Method (Bindungsmethode)
Wählen Sie bei einleitenden Verbindungen mit dem Server des Domänencontrollers eine der folgenden Optionen aus:

w/ Configured Credentials (Mit konfiguriertem Berechtigungsnachweis): Geben Sie für den Client den definierten Namen (**Client DN**) und das Kennwort (**Password**) an, die für die einleitende Verbindung verwendet werden sollen. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden. Wenn die Verbindung erfolgreich hergestellt werden kann, wird nach einem Benutzersatz gesucht, der mit dem im Feld **Client DN** (Definierter Name des Clients) eingegebenen Namen übereinstimmt. Bei der Suche wird in der Regel nach allgemeinen Attributen gesucht, die möglicherweise mit der bei der Anmeldung eingegebenen Benutzer-ID übereinstimmen. Zu diesen Attributen zählen die Attribute `displayName`, `sAMAccountName` und `userPrincipalName`. Wenn das Feld **UID search attribute** (Suchattribut für Benutzer-ID) konfiguriert wird, bezieht sich die Suche darüber hinaus auch auf dieses Attribut.

Wenn die Suche erfolgreich ist, wird versucht, eine zweite Verbindung, diesmal mit dem definierten Benutzernamen (über die Suche abgerufen) und dem bei der Anmeldung angegebenen Kennwort, herzustellen. Wenn die zweite Verbindung hergestellt werden kann, verläuft die Authentifizierung erfolgreich und die Daten zur Gruppenzugehörigkeit für den Benutzer werden abgerufen und mit den auf dem erweiterten Managementmodul konfigurierten Gruppen abgeglichen. Die übereinstimmenden Gruppen definieren die Berechtigungen, die dem Benutzer zugewiesen werden.

w/ Login Credentials (Mit Berechtigungsnachweis für die Anmeldung): Die einleitende Verbindung mit dem Server des Domänencontrollers wird mithilfe des bei der Anmeldung angegebenen Berechtigungsnachweises hergestellt. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden. Wenn die Verbindung erfolgreich hergestellt werden kann, wird nach dem Benutzersatz gesucht. Sobald dieser gefunden ist, werden die Daten zur Gruppenzugehörigkeit für den Benutzer abgerufen und mit den auf dem erweiterten Managementmodul konfigurierten Gruppen abgeglichen. Die übereinstimmenden Gruppen definieren die Berechtigungen, die dem Benutzer zugewiesen werden.

9. Um SSL (Secure Sockets Layer) zwischen dem erweiterten Managementmodul und dem Active Directory-Server zu aktivieren oder inaktivieren, klicken Sie auf **LDAP section of the security page** (LDAP-Abschnitt der Sicherheitsseite).

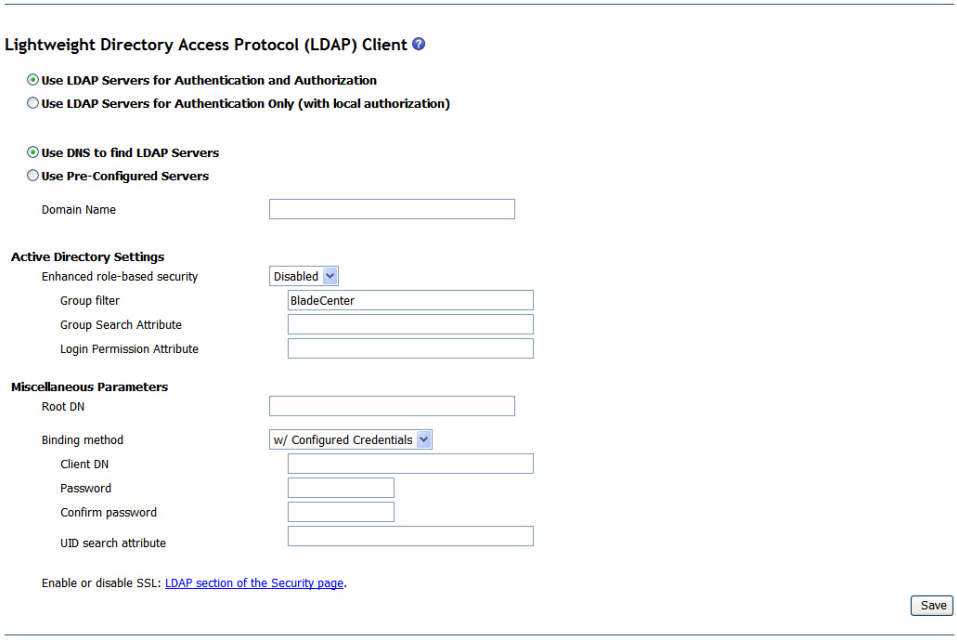
Traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP:

Sie können LDAP-Suchattribute für ein erweitertes Managementmodul konfigurieren, auf dem die erweiterte rollenabhängige Sicherheit für Active Directory-Benutzer inaktiviert ist.

Die traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP war das in erweiterten Managementmodulen ursprünglich implementierte Modell. Es unterstützt Active Directory-, Novell eDirectory- und OpenLDAP-Umgebungen und verwendet auf einem LDAP-Server gespeicherte Konfigurationsdaten, um Benutzern Berechtigungen zuzuweisen. Es wird verwendet, um Benutzer über einen LDAP-Server zu authentifizieren und um Benutzern über einen LDAP-Server Berechtigungen zu erteilen.

Gehen Sie wie folgt vor, um die traditionelle Authentifizierung und Erteilung von Berechtigungen mittels LDAP zu konfigurieren:

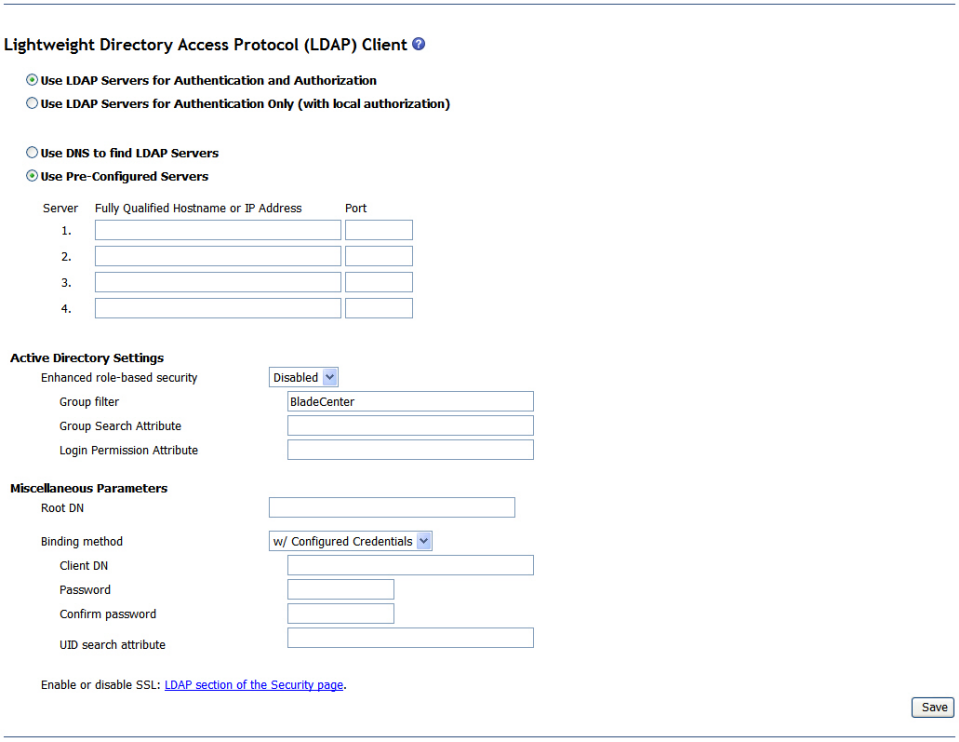
1. Klicken Sie im Navigationsfenster auf **MM Control → Network Protocols** (MM-Steuerung → Netzprotokolle).
2. Wählen Sie **Use LDAP Servers for Authentication and Authorization** (LDAP-Server für Authentifizierung und Erteilung von Berechtigungen verwenden) aus.
3. Legen Sie für **Enhanced role-based security** (Erweiterte rollenabhängige Sicherheit) die Option **Disabled** (Inaktiviert) fest.
4. Die für die Authentifizierung zu verwendenden LDAP-Server können entweder manuell konfiguriert oder mithilfe von DNS SVR-Datensätzen dynamisch ermittelt werden.
   - Wählen Sie **Use DNS to find LDAP Servers** (DNS für die Suche nach LDAP-Servern verwenden) aus, damit die LDAP-Server anhand von DNS SVR-Datensätzen dynamisch ermittelt werden (siehe Schritt 5).
   - Wählen Sie **Use Pre-Configured LDAP Servers** (Vorkonfigurierte LDAP-Server verwenden; Standardeinstellung) aus, um die LDAP-Server manuell zu konfigurieren (siehe Schritt 6 auf Seite 42).
5. Wenn Sie DNS zum dynamischen Ermitteln von LDAP-Servern verwenden, konfigurieren Sie zunächst den Domänennamen des LDAP-Servers. Fahren Sie anschließend mit Schritt 7 auf Seite 43 fort.



Domain Name (Domänenname)
Der vollständig qualifizierte Domänenname des LDAP-Servers. Der Domänenname wird zum Suchen nach dem LDAP-Server benötigt.

Active Directory Forest Name (Name der Active Directory-Gesamtstruktur)
Bei der rollenabhängigen Authentifizierung und Erteilung von Berechtigungen mittels Active Directory werden die globalen Kataloge nicht verwendet. Füllen Sie dieses Feld daher nicht aus.

6. Wenn Sie die LDAP-Server manuell konfigurieren, konfigurieren Sie zunächst das Feld **LDAP Server Host Name or IP Address** (Hostname oder IP-Adresse des LDAP-Servers). Fahren Sie anschließend mit Schritt 7 auf Seite 43 fort. Mit einer IP-Adresse oder einem vollständig qualifizierten Hostnamen können bis zu vier LDAP-Server konfiguriert werden.



7. Konfigurieren Sie die folgenden **sonstigen Parameter**:

Root DN (Definierter Name des Stammelements)

Dieser optionale Parameter wird verwendet, um den Basis-DN des Active Directory-Servers zu konfigurieren (z. B. dn=companyABC,dn=com). Dieses Feld wird in der Regel nicht ausgefüllt, obwohl es bei der Fehlerbehebung durchaus hilfreich sein kann.

Das erweiterte Managementmodul sucht mithilfe der Root-DSE-Abfrage nach dem Basis-DN des Active Directory-Servers, mit dem es kommuniziert. Dieser Basis-DN wird dann für nachfolgende Suchvorgänge verwendet. Der Basis-DN wird von den über die Root-DSE-Abfrage abgerufenen Attributen `defaultNamingContext` und `rootDomaintNamingContext` abgeleitet. Wenn der Basis-DN mithilfe des Felds **Root DN** (Definierter Name des Stammelements) festgelegt wird, werden die Attribute `defaultNamingContext` und `rootDomaintNamingContext` überschrieben.

Binding Method (Bindungsmethode)

Wählen Sie bei einleitenden Verbindungen mit dem Server des Domänencontrollers eine der folgenden Optionen aus:

w/ Configured Credentials (Mit konfiguriertem Berechtigungsnachweis): Geben Sie für den Client den definierten Namen (**Client DN**) und das Kennwort (**Password**) an, die für die einleitende Verbindung verwendet werden sollen. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden. Wenn die Verbindung erfolgreich hergestellt werden kann, wird nach einem Benutzersatz gesucht, der mit dem im Feld **Client DN** (Definierter Name des Clients) eingegebenen Namen übereinstimmt. Bei der Suche wird in der Regel nach allgemeinen Attributen gesucht, die möglicherweise mit der bei der Anmeldung eingegebenen Benutzer-ID übereinstimmen. Zu diesen Attributen zählen die Attribute `displayName`, `sAMAccountName` und `userPrincipalName`. Wenn das Feld **UID search attribute** (Suchattribut für Benutzer-ID) konfiguriert wird, bezieht sich die Suche darüber hinaus auch auf dieses Attribut.

Wenn die Suche erfolgreich ist, wird versucht, eine zweite Verbindung, diesmal mit dem definierten Benutzernamen (über die Suche abgerufen) und dem bei der Anmeldung angegebenen Kennwort, herzustellen. Wenn die zweite Verbindung hergestellt werden kann, verläuft die Authentifizierung erfolgreich und die Daten zur Gruppenzugehörigkeit für den Benutzer werden abgerufen und mit den auf dem erweiterten Managementmodul konfigurierten Gruppen abgeglichen. Die übereinstimmenden Gruppen definieren die Berechtigungen, die dem Benutzer zugewiesen werden.

w/ Login Credentials (Mit Berechtigungsnachweis für die Anmeldung): Die einleitende Verbindung mit dem Server des Domänencontrollers wird mithilfe des bei der Anmeldung angegebenen Berechtigungsnachweises hergestellt. Wenn diese Verbindung nicht hergestellt werden kann, kann auch der Authentifizierungsprozess nicht durchgeführt werden. Wenn die Verbindung erfolgreich hergestellt werden kann, wird nach dem Benutzersatz gesucht. Sobald dieser gefunden ist, werden die Daten zur Gruppenzugehörigkeit für den Benutzer abgerufen und mit den auf dem erweiterten Managementmodul konfigurierten Gruppen abgeglichen. Die übereinstimmenden Gruppen definieren die Berechtigungen, die dem Benutzer zugewiesen werden.

8. Konfigurieren Sie die folgenden **Active Directory-Einstellungen**:

Group Filter (Gruppenfilter)

Das Feld **Group Filter** (Gruppenfilter) wird für die Gruppenauthentifizierung verwendet. Hier werden die Gruppen angegeben, denen das erweiterte Managementmodul angehört. Wenn das Feld **Group Filter** (Gruppenfilter) leer ist, ist die Gruppenauthentifizierung inaktiviert. Wenn die Gruppenauthentifizierung aktiviert ist, wird sie nach der Benutzerauthentifizierung ausgeführt. Dabei wird versucht, mindestens eine Gruppe in der Liste zu finden, die mit einer Gruppe übereinstimmt, der der Benutzer angehört. Wenn es keine Übereinstimmung gibt, schlägt die Authentifizierung des Benutzers fehl und der Zugriff wird verweigert. Wenn mindestens eine Übereinstimmung vorhanden ist, ist die Gruppenauthentifizierung erfolgreich. Bei allen während der Authentifizierung durchgeführten Vergleichen wird die Groß-/Kleinschreibung beachtet.

Wenn die Gruppenauthentifizierung inaktiviert ist, müssen Benutzersätze das Berechtigungsattribut enthalten, andernfalls wird der Zugriff verweigert. (Informationen hierzu finden Sie im Abschnitt Attribut für die Anmeldeberechtigung). Dem Benutzer werden die Berechtigungen zugewiesen, die mit der Gruppe verknüpft sind, die dem Gruppenfilter entspricht. Die mit einer Gruppe verknüpften Berechtigungen werden durch Abrufen des Attributs für die Anmeldeberechtigung aus dem Gruppendatensatz gesucht.

Der Gruppenfilter ist auf 511 Zeichen begrenzt und kann mehrere Gruppennamen enthalten. Die Gruppennamen *müssen* mit einem Doppelpunkt (:) voneinander getrennt werden. Vorangestellte und nachgestellte Leerzeichen werden nicht beachtet. Alle anderen Leerzeichen werden als Teil des Gruppennamens behandelt. Ein Stern (*) als Platzhalterzeichen wird nicht als Platzhalter erkannt. Das Platzhalterkonzept wird aus Sicherheitsgründen nicht mehr angewendet. Ein Gruppenname kann als vollständiger Domänenname oder nur mithilfe des Unternehmensnamens angegeben werden. Eine Gruppe mit dem Domänennamen "cn=adminGroup,dc=mycompany,dc=com" kann beispielsweise mit dem eigentlichen Domänennamen oder mithilfe von "adminGroup" angegeben werden.

Group Search Attribute (Attribut für die Gruppensuche)
Dieses Feld wird vom Suchalgorithmus für die Suche nach Gruppenzugehörigkeitsdaten für einen bestimmten Benutzer verwendet. Wenn der Gruppenfiltername konfiguriert wurde, muss die Liste der Gruppen, denen der Benutzer angehört, vom LDAP-Server abgerufen werden. Diese ist zum Ausführen der Gruppenauthentifizierung erforderlich. Um diese Liste abzurufen, muss der an den Server gesendete Suchfilter den Attributnamen angeben, der Gruppen zugeordnet wurde. Dieser Attributname wird in diesem Feld angegeben.

In einer Active Directory- oder Novell eDirectory-Umgebung gibt das Attribut für die Gruppensuche den Attributnamen an, der die Gruppen bezeichnet, denen ein Benutzer angehört. Bei Active Directory ist dies in der Regel `memberOf` und bei Novell eDirectory `groupMembership`. In einer OpenLDAP-Serverumgebung werden Benutzer in der Regel Gruppen zugewiesen, deren `objectClass` "PosixGroup" entspricht. In diesem Kontext gibt dieser Parameter den Attributnamen an, der die Mitglieder einer bestimmten "PosixGroup" bezeichnet, meist `memberUid`.

Wenn in diesem Feld keine Angaben gemacht werden, wird für den Attributnamen im Filter standardmäßig `memberOf` verwendet.

Login Permission Attribute (Attribut für die Anmeldeberechtigung)
Wenn ein Benutzer über den LDAP-Server erfolgreich authentifiziert wurde, müssen die Anmeldeberechtigungen für den Benutzer abgerufen werden. Um diese Berechtigungen abzurufen, muss der an den Server gesendete Suchfilter den Attributnamen angeben, der Anmeldeberechtigungen zugeordnet wurde. Dieser Attributname wird in diesem Feld angegeben.

Dieses Feld muss ausgefüllt werden, andernfalls ist es nicht möglich, die Benutzerberechtigungen abzurufen. Ohne bestätigte Berechtigungen schlägt der Anmeldeversuch fehl. In diesem Punkt unterscheidet sich diese Version von früheren Versionen, bei denen einem Benutzer Zugriff mit Standardleseberechtigungen gewährt wurde, wenn dessen Berechtigungen nicht bestätigt werden konnten.

In dem vom LDAP-Server zurückgegebenen Attributwert wird nach der Suchbegriffszeichenfolge „IBMRBSPermissions=" gesucht. Diesem Suchbegriff folgt unmittelbar eine Bitfolge bestehend aus 64 aufeinanderfolgenden Nullen oder Einsen. Dabei stellt jedes Bit eine bestimmte Gruppe Funktionen dar. Die Bits sind entsprechend ihrer Position durchnummeriert, wobei das Bit ganz links der Bitposition 0 entspricht. Der Wert 1 an einer Position aktiviert die entsprechende Funktion. Der Wert 0 inaktiviert diese Funktion. Die Zeichenfolge „IBMRBSPermissions=010000000000" ist ein Beispiel für ein gültiges Attribut.

Mithilfe des Suchbegriffs „IBMRBSPermissions=" kann dieser an einer beliebigen Stelle im Attributfeld eingefügt werden. So kann der LDAP-Administrator ein vorhandenes Attribut wiederverwenden und eine Erweiterung des LDAP-Schemas verhindern. Darüber hinaus kann das Attribut auf diese Weise auch für seinen ursprünglichen Zweck verwendet werden. Die Suchbegriffszeichenfolge kann an einer beliebigen Stelle hinzugefügt werden. Das verwendete Attribut muss eine frei formatierte Zeichenfolge zulassen.

Anmerkung: Um die Konfiguration von Benutzern bei Verwendung einer Microsoft Windows-Plattform zu erleichtern, können Sie das Snap-in für die rollenabhängige Sicherheit verwenden. Sie erhalten es unter http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5069735&brandind=5000008. Mithilfe des Snap-ins können Sie auf einem Active Directory-Server Rollen konfigurieren und diese Rollen Benutzern, Gruppen und erweiterten Managementmodulen zuweisen.

Die Berechtigungsbits werden wie folgt interpretiert:

- Deny Always (Nicht zulassen, Bitposition 0): Wenn dieses Bit gesetzt ist, schlägt die Authentifizierung des Benutzers immer fehl. Diese Funktion kann verwendet werden, um einen oder mehrere bestimmte Benutzer, die einer bestimmten Gruppe zugeordnet sind, zu blockieren.
- Supervisor Access (Administratorzugriff, Bitposition 1): Wenn dieses Bit gesetzt ist, sind dem Benutzer Administratorberechtigungen zugewiesen, mit denen der Benutzer alle Seiten anzeigen, Änderungen an beliebigen Feldern vornehmen und alle von der Schnittstelle bereitgestellten Aktionen zulassen kann. Wenn dieses Bit gesetzt ist, müssen die anderen Bits, die einen bestimmten Funktionszugriff definieren, nicht einzeln gesetzt werden. Dieser Benutzer ist der einzige Benutzer, der die Konfiguration des erweiterten Managementmoduls auf der BladeCenter-Einheit sichern oder die gesicherte Konfiguration eines erweiterten Managementmoduls wiederherstellen kann.
- Read Only Access (Lesezugriff, Bitposition 2): Wenn dieses Bit gesetzt ist, hat der Benutzer nur Lesezugriff und kann keine Wartungsarbeiten (z. B. Neustart, fern ausgeführte Aktionen und Firmwareaktualisierungen) durchführen und keine Änderungen (mithilfe der Funktionen zum Speichern, Löschen oder Wiederherstellen) vornehmen. Das Bit für den Lesezugriff und alle anderen Bits schließen sich gegenseitig aus, wobei Bitposition 2 die niedrigste Vorrangstellung einnimmt. Das bedeutet, dass dieses Bit ignoriert wird, wenn ein anderes Bit gesetzt ist.
- Networking and Security (Netzbetrieb und Sicherheit, Bitposition 3): Wenn dieses Bit gesetzt ist, kann der Benutzer die Einstellungen auf den Seiten **Security** (Sicherheit), **Network Protocols** (Netzprotokolle)

und **Network Interface** (Netzschnittstelle) unter **MM Control** (MM-Steuerung) ändern. Wenn dieses Bit gesetzt ist, kann der Benutzer auch die IP-Konfigurationsparameter für E/A-Module auf der Seite **I/O Module Tasks → Management** (E/A-Modul-Tasks → Management) ändern.

- User Account Management (Benutzerkontenverwaltung, Bitposition 4): Wenn dieses Bit gesetzt ist, kann der Benutzer andere Benutzer hinzufügen, ändern und löschen und die globalen Anmeldungseinstellungen auf der Seite **Login Profiles** (Anmeldeprofile) ändern.
- Blade Server Remote Console Access (Zugriff auf ferne Blade-Server-Konsole, Bitposition 5): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf eine ferne Blade-Server-Videokonsole mit Tastatur- und Maussteuerung.
- Blade Server Remote Console and Virtual Media Access (Zugriff auf ferne Blade-Server-Konsole und virtuelle Datenträger, Bitposition 6): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf eine ferne Blade-Server-Videokonsole mit Tastatur- und Maussteuerung sowie auf die Funktionen für virtuelle Datenträger für diesen fernen Blade-Server.
- Blade Server and I/O Module Power/Restart Access (Zugriff für Einschalten/Neustart von Blade-Server und E/A-Modul, Bitposition 7): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf die Einschalt- und Neustartfunktionen für die Blade-Server und E/A-Module. Diese Funktionen sind auf der Seite **Blade Tasks → Power/Restart** (Blade-Tasks → Einschalten/Neustart) sowie auf der Seite **I/O Module Tasks → Power/Restart** (E/A-Modul-Tasks → Einschalten/Neustart) verfügbar.
- Basic Configuration (Allgemeine Konfiguration, Bitposition 8): Wenn dieses Bit gesetzt ist, kann der Benutzer allgemeine Konfigurationsparameter für das Managementmodul und für Blade-Server ändern. Diese Parameter befinden sich auf den Seiten **General Settings** (Allgemeine Einstellungen) und **Alarme** unter **MM Control** (MM-Steuerung) und auf der Seite **Configuration** (Konfiguration) unter **Blade Tasks** (Blade-Tasks).
- Ability to Clear Event Logs (Fähigkeit zum Löschen von Ereignisprotokollen (Bitposition 9): Wenn dieses Bit gesetzt ist, kann der Benutzer die Ereignisprotokolle löschen. Alle Benutzer können die Ereignisprotokolle anzeigen. Zum Löschen der Ereignisprotokolle ist jedoch diese Berechtigung erforderlich.
- Advanced Adapter Configuration (Erweiterte Adapterkonfiguration, Bitposition 10): Wenn dieses Bit gesetzt ist, gelten für den Benutzer keine Einschränkungen bei der Konfiguration von Managementmodul, Blade-Servern, E/A-Modulen und von elementaren Produktdaten. Zudem hat der Benutzer Verwaltungszugriff. Das bedeutet, dass dieser Benutzer darüber hinaus auch die folgenden erweiterten Funktionen ausführen kann: Firmware-Upgrades auf Managementmodulen oder Blade-Servern, Wiederherstellung von werkseitigen Voreinstellungen des Managementmoduls, Änderung und Wiederherstellung der Managementmodulkonfiguration von einer Konfigurationsdatei und Neustart oder Zurücksetzung des Managementmoduls.
- Version Number (Versionsnummer, Bitpositionen 11 bis 15): Die Versionsnummer 00000 gibt an, dass das Benutzerberechtigungsschema verwendet wird, bei dem die Bitpositionen 0 bis 10 gesetzt werden.

Die Versionsnummer 00001 gibt an, dass das rollenabhängige Benutzerberechtigungsschema verwendet wird, bei dem die Bitpositionen 16 bis 55 gesetzt werden. Bei allen anderen Versionsnummern wird das Benutzerberechtigungsschema verwendet, bei dem die Bitpositionen 0 bis 10 gesetzt werden.

- Deny Always Role (Nicht zulassen, Bitposition 16): Wenn dieses Bit gesetzt ist, schlägt die Authentifizierung des Benutzers immer fehl. Diese Funktion kann verwendet werden, um einen oder mehrere bestimmte Benutzer, die einer bestimmten Gruppe zugeordnet sind, zu blockieren.
- Supervisor Role (Administratorrolle, Bitposition 17): Wenn dieses Bit gesetzt ist, gelten für den Benutzer keine Einschränkungen. Der Benutzer hat Schreib-/Lesezugriff auf alle Seiten und Felder für alle Einheiten. Wenn dieses Bit gesetzt ist, müssen keine weiteren Berechtigungsstufen festgelegt werden, die über die Bits 18 bis 55 gesteuert werden.
- Operator Role (Bedienerrolle, Bitposition 18): Wenn dieses Bit gesetzt ist, hat der Benutzer Lesezugriff. Dieser Benutzer kann Wartungsarbeiten ausführen (z. B. Neustart, fern ausgeführte Aktionen, Firmwareaktualisierungen). Er kann jedoch keine Änderungen an Einstellungen (mithilfe der Funktionen zum Speichern, Löschen oder Wiederherstellen) vornehmen. Das Bit für den Lesezugriff und alle anderen Bits schließen sich gegenseitig aus, wobei das Bit für den Lesezugriff die niedrigste Vorrangstellung einnimmt. Das bedeutet, dass Bit 18 ignoriert wird, wenn ein anderes Bit gesetzt ist.
- Chassis Operator Role (Gehäusebedienerrolle, Bitposition 19): Wenn dieses Bit gesetzt ist, kann der Benutzer Status und Eigenschaften von BladeCenter-Einheiten (Managementmodul, Gebläse, Mittelplatine, Stromversorgungsmodul, Laufwerkschlitten) durchsuchen und die Managementmodulkonfiguration sichern. Dieser Benutzer kann auch die Konfiguration des erweiterten Managementmoduls in einer Datei sichern.
- Chassis User Account Management Role (Gehäusebenutzerkontenverwaltung, Bitposition 20): Wenn dieses Bit gesetzt ist, kann der Benutzer auf der Seite **MM Control → Login Profiles** (MM-Steuerung → Anmeldeprofile) Benutzer hinzufügen, ändern und löschen. Um die globalen Anmeldungseinstellungen ändern zu können, ist die Gehäusekonfigurationsrolle erforderlich. Dieser Benutzer kann auch die Konfiguration des erweiterten Managementmoduls in einer Datei sichern.
- Chassis Log Account Management Role (Gehäuseanmeldungskontenverwaltung, Bitposition 21): Wenn dieses Bit gesetzt ist, kann der Benutzer die Ereignisprotokolle löschen oder die Richtlinieneinstellungen für das Ereignisprotokoll ändern. Alle Benutzer können die Ereignisprotokolle anzeigen. Zum Löschen der Protokolle oder zum Ändern der Richtlinieneinstellungen für das Ereignisprotokoll (das Feld oben auf der Ereignisprotokollseite) ist jedoch diese Rolle erforderlich. Dieser Benutzer kann auch die Konfiguration des erweiterten Managementmoduls in einer Datei sichern.
- Chassis Configuration Role (Gehäusekonfigurationsrolle, Bitposition 22): Wenn dieses Bit gesetzt ist, kann der Benutzer mit Ausnahme von Benutzerprofilen und Ereignisprotokolleinstellungen alle Konfigurationsparameter für die BladeCenter-Einheit ändern und speichern (z. B. allgemeine Managementmoduleinstellungen, Portzuord-

nungen des Managementmoduls, Netzschnittstellen des Managementmoduls, Netzprotokolle des Managementmoduls und Managementmodulsicherheit). Dieser Benutzer kann auch die SOL-Konfiguration auf der Webseite für die SOL-Konfiguration ändern. Zudem kann er die globalen Anmeldungseinstellungen ändern und die Konfiguration des erweiterten Managementmoduls in einer Datei sichern. Darüber hinaus kann dieser Benutzer die werkseitigen Voreinstellungen der Konfiguration des Managementmoduls wiederherstellen, sofern er auch über die Berechtigung zur Gehäuseverwaltung verfügt.

- Chassis Administration Role (Gehäuseverwaltungsrolle, Bitposition 23): Wenn dieses Bit gesetzt ist, kann der Benutzer Firmwareaktualisierungen für das Managementmodul durchführen, den Status der Anzeigen der BladeCenter-Einheit ändern und das Managementmodul erneut starten. Der Benutzer kann zudem auch die werkseitigen Voreinstellungen der Konfiguration des Managementmoduls wiederherstellen, sofern er auch über die Berechtigung zur Gehäusekonfiguration verfügt.
- Blade Operator Role (Bladebedienerrolle, Bitposition 24): Wenn dieses Bit gesetzt ist, kann der Benutzer Informationen zum Blade lesen, jedoch nicht ändern.
- Blade Remote Presence Role (Blade-Remote-Presence-Rolle, Bitposition 25): Wenn dieses Bit gesetzt ist, kann der Benutzer auf die Fernsteuerungswebseite und die auf dieser Seite bereitgestellten Funktionen zugreifen: ferne Konsole (KVM) und ferner Datenträger. Zudem kann dieser Benutzer den Konsolbefehl der Befehlszeilenschnittstelle ausgeben, um eine SOL-Sitzung auf einem Blade-Server zu starten.
- Blade Configuration Role (Bladekonfigurationsrolle, Bitposition 26): Wenn dieses Bit gesetzt ist, kann der Benutzer mit Ausnahme der Parameter auf der Webseite für die SOL-Konfiguration alle Blade-Server-Konfigurationsparameter ändern und speichern (z. B. Blade-Server-Namen und Richtlinieneinstellungen für den Blade-Server) und er kann auf der Webseite für den SOL-Status SOL für einzelne Blade-Server aktivieren oder inaktivieren.
- Blade Administration Role (Blade-Verwaltungsrolle, Bitposition 27): Wenn dieses Bit gesetzt ist, kann der Benutzer Blade-Server einschalten, ausschalten und erneut starten, Standby-Blade-Server aktivieren, Firmwareaktualisierungen durchführen und den Status von Blade-Server-Anzeigen ändern.
- Switch Operator Role (Switch-Bedienerrolle, Bitposition 28): Wenn dieses Bit gesetzt ist, kann der Benutzer den Status und die Eigenschaften von E/A-Modulen durchsuchen und E/A-Module mit Ping überprüfen.
- Switch Configuration Role (Switch-Konfigurationsrolle, Bitposition 29): Wenn dieses Bit gesetzt ist, kann der Benutzer die IP-Adresse von E/A-Modulen konfigurieren, die externe Verwaltung für alle Anschlüsse aktivieren und inaktivieren und die neue IP-Konfiguration bei allen Zurücksetzungen beibehalten. Der Benutzer kann zudem auch die werkseitigen Voreinstellungen wiederherstellen und eine Telnet- oder Websitzung mit einem E/A-Modul starten, sofern er auch über die Berechtigung zur Switch-Verwaltung verfügt.
- Switch Administration Role (Switch-Verwaltungsrolle, Bitposition 30): Wenn dieses Bit gesetzt ist, kann der Benutzer E/A-Module einschalten, ausschalten und mit unterschiedlichen Diagnosestufen erneut

starten, die Firmware von Pass-through-E/A-Modulen aktualisieren, Fast-POST aktivieren und inaktivieren und externe Anschlüsse aktivieren und inaktivieren. Der Benutzer kann zudem auch die werkseitigen Voreinstellungen wiederherstellen und eine Telnet- oder Websitzung mit einem E/A-Modul starten, sofern er auch über die Berechtigung zur Switch-Konfiguration verfügt.

- Blade 1 Scope (Geltungsbereich Blade 1, Bitposition 31): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 1.
- Blade 2 Scope (Geltungsbereich Blade 2, Bitposition 32): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 2.
- Blade 3 Scope (Geltungsbereich Blade 3, Bitposition 33): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 3.
- Blade 4 Scope (Geltungsbereich Blade 4, Bitposition 34): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 4.
- Blade 5 Scope (Geltungsbereich Blade 5, Bitposition 35): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 5.
- Blade 6 Scope (Geltungsbereich Blade 6, Bitposition 36): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 6.
- Blade 7 Scope (Geltungsbereich Blade 7, Bitposition 37): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 7.
- Blade 8 Scope (Geltungsbereich Blade 8, Bitposition 38): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 8.
- Blade 9 Scope (Geltungsbereich Blade 9, Bitposition 39): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 9.
- Blade 10 Scope (Geltungsbereich Blade 10, Bitposition 40): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 10.
- Blade 11 Scope (Geltungsbereich Blade 11, Bitposition 41): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 11.
- Blade 12 Scope (Geltungsbereich Blade 12, Bitposition 42): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 12.
- Blade 13 Scope (Geltungsbereich Blade 13, Bitposition 43): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 13.
- Blade 14 Scope (Geltungsbereich Blade 14, Bitposition 44): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf den Blade-Server in Position 14.
- Chassis Scope (Geltungsbereich Gehäuse, Bitposition 45): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf die BladeCenter-Einheit und das Managementmodul.

- I/O Module 1 Scope (Geltungsbereich E/A-Modul 1, Bitposition 46): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 1.
- I/O Module 2 Scope (Geltungsbereich E/A-Modul 2, Bitposition 47): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 2.
- I/O Module 3 Scope (Geltungsbereich E/A-Modul 3, Bitposition 48): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 3.
- I/O Module 4 Scope (Geltungsbereich E/A-Modul 4, Bitposition 49): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 4.
- I/O Module 5 Scope (Geltungsbereich E/A-Modul 5, Bitposition 50): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 5.
- I/O Module 6 Scope (Geltungsbereich E/A-Modul 6, Bitposition 51): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 6.
- I/O Module 7 Scope (Geltungsbereich E/A-Modul 7, Bitposition 52): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 7.
- I/O Module 8 Scope (Geltungsbereich E/A-Modul 8, Bitposition 53): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 8.
- I/O Module 9 Scope (Geltungsbereich E/A-Modul 9, Bitposition 54): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 9.
- I/O Module 10 Scope (Geltungsbereich E/A-Modul 10, Bitposition 55): Wenn dieses Bit gesetzt ist, hat der Benutzer Zugriff auf E/A-Modul 10.
- Reserved (Reserviert, Bitposition 56 bis 63): reserviert für künftige Verwendung.

Wenn kein Bit gesetzt ist, wird die Standardeinstellung auf "deny always (read-only)" (Nicht zulassen (schreibgeschützt)) für den Benutzer festgelegt.

Direkt aus dem Benutzersatz abgerufene Anmeldeberechtigungen erhalten Priorität. Wenn der Benutzer nicht über das Anmeldeberechtigungsattribut im Benutzersatz verfügt, wird versucht, die Berechtigung von den Gruppen abzurufen, denen der Benutzer angehört. Dies geschieht während der Gruppenauthentifizierungsphase. Dem Benutzer wird das inklusive ODER aller Bits aller Gruppen zugeordnet. Das Bit "Deny Always" (Nicht zulassen) wird, wie bereits erwähnt, nur gesetzt, wenn alle anderen Bits null sind. Wenn das Bit "Deny Always" (Nicht zulassen) für eine Gruppe gesetzt ist, wird dem Benutzer der Zugriff verweigert. Das Bit "Deny Always" (Nicht zulassen) hat Vorrang vor allen anderen Bits.

Wichtig: Wenn Sie einem Benutzer die Möglichkeit geben, allgemeine Parameter sowie Netzbetriebs- und Sicherheitsparameter für die Adapterkonfiguration ändern zu können, sollten Sie diesem Benutzer auch die Möglichkeit geben, das Managementmodul erneut zu starten. Wenn der Benutzer das Managementmodul nicht erneut starten kann, werden vom Benutzer vorgenommene Änderungen, die einen Neustart erfordern, nicht wirksam.

9. Um SSL (Secure Sockets Layer) zwischen dem erweiterten Managementmodul und dem Active Directory-Server zu aktivieren oder inaktivieren, klicken Sie auf **LDAP section of the security page** (LDAP-Abschnitt der Sicherheitsseite).

Sicherer Web-Server und sichere LDAP-Verbindung

Mithilfe von SSL (Secure Sockets Layer) können Sie einen sicheren Web-Server und eine sichere LDAP-Verbindung für das Managementmodul konfigurieren.

SSL ist ein Sicherheitsprotokoll, das eine geschützte Datenübertragung bereitstellt. SSL ermöglicht Anwendungen eine Datenübertragung, die gegen das Ausspionieren, das Manipulieren von Daten während der Übertragung und das Fälschen von Nachrichten geschützt ist.

Sie können das Managementmodul so konfigurieren, dass die SSL-Unterstützung für zwei Verbindungsmöglichkeiten verwendet wird: den sicheren Web-Server (HTTPS) und die sichere LDAP-Verbindung (LDAPS). Das Managementmodul übernimmt je nach Verbindungstyp die Rolle des SSL-Clients oder des SSL-Servers. Die folgende Tabelle zeigt, dass das Managementmodul für sichere Web-Server-Verbindungen als SSL-Server agiert. Das Managementmodul agiert als SSL-Client für sichere LDAP-Verbindungen.

Tabelle 1. Managementmodul, Unterstützung von SSL-Verbindungen

Verbindungstyp	SSL-Client	SSL-Server
Sicherer Web-Server (HTTPS)	Web-Browser des Benutzers (zum Beispiel Microsoft Internet Explorer)	Web-Server des Managementmoduls
Sichere LDAP-Verbindung (LDAPS)	LDAP-Client des Managementmoduls	Ein LDAP-Server

Sie können die SSL-Einstellungen auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit) anzeigen oder ändern. Sie können SSL aktivieren oder inaktivieren und die für SSL erforderlichen Zertifikate verwalten. Änderungen in den SSL-Servereinstellungen werden für das erweiterte Managementmodul sofort wirksam; Sie müssen das erweiterte Managementmodul nicht erneut starten.

Sicherheit konfigurieren:

Verwenden Sie das in diesem Abschnitt beschriebene Verfahren, um die Sicherheit für den Web-Server des Managementmoduls sowie für die Verbindung zwischen dem Managementmodul und einem LDAP-Server zu konfigurieren.

Wenn Sie mit der Verwendung von SSL-Zertifikaten nicht vertraut sind, lesen Sie die Informationen im Abschnitt „Überblick über SSL-Zertifikate" auf Seite 54.

Der Inhalt der Sicherheits-Webseite ist kontextabhängig. Welche Optionen auf der Seite verfügbar sind, ändert sich, wenn Zertifikate oder Zertifikatssignieranforderungen erstellt werden, wenn Zertifikate importiert oder entfernt werden und wenn SSL für den Client oder Server aktiviert oder inaktiviert wird.

Führen Sie die folgenden allgemeinen Tasks aus, um die Sicherheit für das Managementmodul zu konfigurieren:

1. Konfigurieren Sie die SSL-Serverzertifikate für den sicheren Web-Server:
   a. Inaktivieren Sie den SSL-Server. Verwenden Sie hierzu den Abschnitt **SSL Server Configuration for Web Server** (Konfiguration des SSL-Servers für den Web-Server) auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit).
   b. Generieren oder importieren Sie ein Zertifikat. Verwenden Sie hierzu den Abschnitt **SSL Server Certificate Management** (Verwaltung von SSL-Serverzertifikaten) auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit). (Informationen hierzu finden Sie im Abschnitt „Verwaltung von SSL-Serverzertifikaten" auf Seite 55.)
   c. Aktivieren Sie den SSL-Server. Verwenden Sie hierzu den Abschnitt **SSL Server Configuration for Web Server** (Konfiguration des SSL-Servers für den Web-Server) auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit).(Informationen hierzu finden Sie im Abschnitt „SSL für den sicheren Web-Server aktivieren" auf Seite 61.)
2. Konfigurieren Sie die SSL-Clientzertifikate für sichere LDAP-Verbindungen:

   Anmerkung: Die Verwaltung von SSL-Clientzertifikaten ist optional. Sie können den SSL-Client für LDAP auch generieren ohne ein selbst signiertes Zertifikat zu erstellen oder ein signiertes Zertifikat in den Client zu importieren.
   a. Inaktivieren Sie den SSL-Client. Verwenden Sie hierzu den Abschnitt **SSL Client Configuration for LDAP Client** (Konfiguration des SSL-Clients für den LDAP-Client) auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit).
   b. Generieren oder importieren Sie ein Zertifikat. Verwenden Sie hierzu den Abschnitt **SSL Client Certificate Management** (Verwaltung von SSL-Clientzertifikaten) auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit). (Informationen hierzu finden Sie im Abschnitt „Verwaltung von SSL-Clientzertifikaten" auf Seite 61.)
   c. Importieren Sie ein oder mehrere vertrauenswürdige Zertifikate. Verwenden Sie hierzu den Abschnitt **SSL Client Trusted Certificate Management** (Verwaltung von vertrauenswürdigen SSL-Clientzertifikaten) auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit). (Informationen hierzu finden Sie im Abschnitt „Verwaltung von vertrauenswürdigen SSL-Clientzertifikaten" auf Seite 62.)
   d. Aktivieren Sie den SSL-Client. Verwenden Sie hierzu den Abschnitt **SSL Client Configuration for LDAP Client** (Konfiguration des SSL-Clients für den

LDAP-Client) auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit).(Informationen hierzu finden Sie im Abschnitt „SSL für den LDAP-Client aktivieren" auf Seite 63.)

Anmerkungen:

- Änderungen an der SSL-Clientkonfiguration werden ohne Neustart des Managementmoduls sofort wirksam.
- Beim erweiterten Managementmodul ist für die folgenden Konfigurationsänderungen an SSH, SMASH und Secure SMASH kein Neustart des erweiterten Managementmoduls mehr erforderlich:
  - Aktivieren/Inaktivieren von SSH oder Secure SMASH
  - Generieren neuer SSH-Hostschlüssel
  - Ändern der Portnummer für SSH oder Secure SMASH
  - Installieren, Löschen oder Ändern von öffentlichen SSH-Schlüsseln, die für die Authentifizierung verwendet werden

Überblick über SSL-Zertifikate:

Sie können SSL entweder mit einem selbst signierten Zertifikat oder mit einem von einer Zertifizierungsstelle signierten Zertifikat verwenden.

Die Verwendung eines selbst signierten Zertifikats ist die einfachste Methode, SSL zu verwenden, sie birgt jedoch ein geringes Sicherheitsrisiko: Der SSL-Client hat keine Möglichkeit, die Identität des SSL-Servers zu überprüfen, wenn zum ersten Mal ein Verbindungsversuch zwischen dem Client und dem Server erfolgt. Ein anderer Anbieter kann die Identität des Servers vortäuschen und Daten zwischen dem Managementmodul und dem Web-Browser abfangen. Wenn das selbst signierte Zertifikat beim ersten Verbindungsaufbau zwischen dem Browser und dem Managementmodul in den Zertifikatsspeicher des Browsers importiert wird, sind alle künftigen Datenübertragungen für diesen Browser sicher (vorausgesetzt, dass bei der ersten Verbindung kein Angriff erfolgt ist).

Mehr Sicherheit erhalten Sie, wenn Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert ist. Um ein signiertes Zertifikat zu erhalten, verwenden Sie die Seite zur Verwaltung von SSL-Zertifikaten, um eine Unterzeichnungsanforderung für ein SSL-Zertifikat zu erstellen. Senden Sie dann die Unterzeichnungsanforderung für das SSL-Zertifikat an eine Zertifizierungsstelle und vereinbaren Sie die Zustellung eines Zertifikats. Sobald Sie das Zertifikat erhalten haben, wird es über den Link **Import a Signed Certificate** (Signiertes Zertifikat importieren) in das Managementmodul importiert und Sie können SSL aktivieren.

Die Aufgabe der Zertifizierungsstelle ist es, die Identität des Managementmoduls zu überprüfen. Ein Zertifikat enthält digitale Signaturen für die Zertifizierungsstelle und das Managementmodul. Wenn eine anerkannte Zertifizierungsstelle das Zertifikat ausstellt oder wenn das Zertifikat der Zertifizierungsstelle bereits in den Web-Browser importiert wurde, kann der Browser das Zertifikat validieren und den Web-Server des Managementmoduls positiv identifizieren.

Das Managementmodul benötigt ein Zertifikat für den sicheren Web-Server und eines für den sicheren LDAP-Client. Der sichere LDAP-Client benötigt ebenfalls ein oder mehrere vertrauenswürdige Zertifikate. Das vertrauenswürdige Zertifikat wird vom sicheren LDAP-Client verwendet, um den LDAP-Server sicher zu identifizieren. Das vertrauenswürdige Zertifikat ist das Zertifikat der Zertifizierungsstelle, die das Zertifikat des LDAP-Servers signiert hat. Wenn der LDAP-Server selbst signierte Zertifikate verwendet, kann das vertrauenswürdige Zertifikat das Zertifi-

kat des LDAP-Servers selbst sein. Sie können zusätzliche vertrauenswürdige Zertifikate importieren, wenn Sie in Ihrer Konfiguration mehrere LDAP-Server verwenden.

Verwaltung von SSL-Serverzertifikaten:

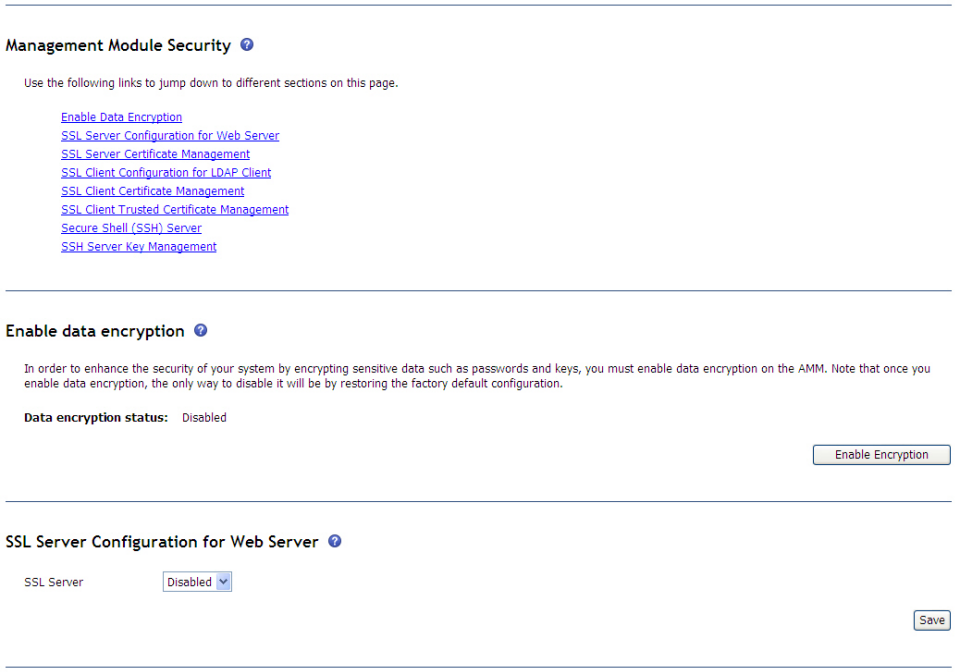
Der SSL-Server erfordert, dass ein gültiges Zertifikat und ein entsprechender privater Chiffrierschlüssel installiert werden, bevor SSL aktiviert wird.

Es stehen zwei Methoden zur Verfügung, um den privaten Schlüssel und das erforderliche Zertifikat zu generieren: Die Verwendung eines selbst signierten Zertifikats und die Verwendung eines von einer Zertifizierungsstelle signierten Zertifikats-.Weitere Informationen zur Verwendung eines selbst signierten Zertifikats für den SSL-Server finden Sie im Abschnitt „Selbst signiertes Zertifikat erstellen". Informationen zur Verwendung eines von einer Zertifizierungsstelle signierten Zertifikats für den SSL-Server finden Sie im Abschnitt „Zertifikatssignieranforderung erstellen" auf Seite 57.

Selbst signiertes Zertifikat erstellen:

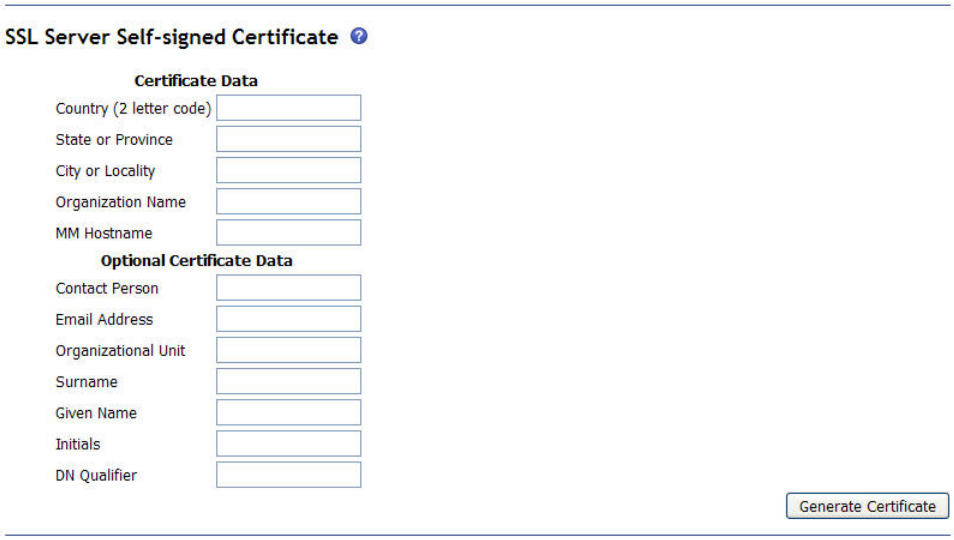
Gehen Sie wie folgt vor, um einen neuen privaten Chiffrierschlüssel und ein selbst signiertes Zertifikat für das Managementmodul zu erstellen:

1. Klicken Sie im Navigationsfenster auf **MM Control → Security** (MM-Steuerung → Sicherheit). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



2. Stellen Sie sicher, dass im Abschnitt **SSL Server Configuration for Web Server** (Konfiguration des SSL-Servers für den Web-Server) der SSL-Server inaktiviert ist. Wenn er nicht inaktiviert ist, wählen Sie im Feld **SSL Server** (SSL-Server) die Option **Disabled** (Inaktiviert) aus und klicken Sie anschließend auf **Save** (Speichern).

3. Wählen Sie im Abschnitt **SSL Server Certificate Management** (Verwaltung von SSL-Serverzertifikaten) die Option **Generate a New Key and a Self-signed Certificate** (Neuen Schlüssel und selbst signiertes Zertifikat erstellen) aus. Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.

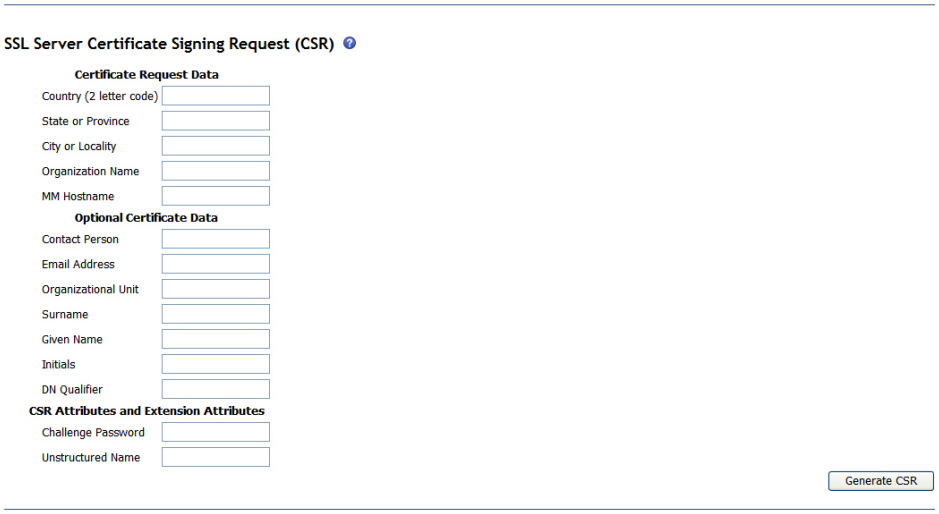


4. Geben Sie die Informationen in die erforderlichen und optionalen Felder zu Ihrer Konfiguration ein. Eine Beschreibung der Felder finden Sie unter Erforderliche Zertifikatsdaten. Nachdem Sie die erforderlichen Informationen eingegeben haben, klicken Sie auf **Generate Certificate** (Zertifikat erstellen). Ihre neuen Chiffrierschlüssel und das Zertifikat werden erstellt. Dieser Vorgang kann einige Minuten dauern. Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt. Hier wird angezeigt, dass ein selbst signiertes Zertifikat erstellt wurde.

Zertifikatssignieranforderung erstellen:

Gehen Sie wie folgt vor, um einen neuen privaten Chiffrierschlüssel und eine Zertifikatssignieranforderung zu erstellen:

1. Klicken Sie im Navigationsfenster auf **MM Control → Security** (MM-Steuerung → Sicherheit).
2. Stellen Sie sicher, dass im Abschnitt **SSL Server Configuration for Web Server** (Konfiguration des SSL-Servers für den Web-Server) der SSL-Server inaktiviert ist. Wenn er nicht inaktiviert ist, wählen Sie im Feld **SSL Server** (SSL-Server) die Option **Disabled** (Inaktiviert) aus und klicken Sie anschließend auf **Save** (Speichern).
3. Wählen Sie im Abschnitt **SSL Server Certificate Management** (Verwaltung von SSL-Serverzertifikaten) die Option **Generate a New Key and a Certificate Signing Request** (Neuen Schlüssel und Zertifikatssignieranforderung erstellen) aus. Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



4. Geben Sie die Informationen in die erforderlichen und optionalen Felder zu Ihrer Konfiguration ein. Die Felder sind dieselben wie bei einem selbst signierten Zertifikat. Daneben gibt es auch einige zusätzliche Felder. In den folgenden Abschnitten werden die einzelnen allgemeinen Felder beschrieben.
   - **Erforderliche Zertifikatsdaten**

     Die folgenden Benutzereingabefelder sind erforderlich, um ein selbst signiertes Zertifikat oder eine Zertifikatssignieranforderung zu erstellen:

     Country (Land)
     Geben Sie in diesem Feld das Land an, in dem sich das Managementmodul befindet. Dieses Feld muss den aus 2 Zeichen bestehenden Landescode enthalten.

     State or Province (Bundesland)
     Geben Sie in diesem Feld das Bundesland an, in dem sich das Managementmodul befindet. Dieses Feld ist auf maximal 30 Zeichen begrenzt.

     City or Locality (Ort oder Standort)
     Geben Sie in diesem Feld den Ort oder Standort an, an dem sich das Managementmodul befindet. Dieses Feld ist auf maximal 50 Zeichen begrenzt.

Organization Name (Name des Unternehmens)
Geben Sie in diesem Feld das Unternehmen an, in dem das Managementmodul verwendet wird. Wenn diese Informationen zum Erstellen einer Zertifikatssignieranforderung verwendet werden, kann die ausstellende Zertifizierungsstelle überprüfen, ob das Unternehmen, das das Zertifikat anfordert, berechtigt ist, Eigentumsrecht am angegebenen Unternehmensnamen zu beanspruchen. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

MM Host Name (Hostname des Managementmoduls)
Geben Sie in diesem Feld den Hostnamen des Managementmoduls an, der im Adressfeld des Web-Browsers angezeigt wird.

Achten Sie darauf, dass der Wert, den Sie im Feld **MM host name** (Hostname des Managementmoduls) eingeben, exakt mit dem Hostnamen übereinstimmt, den der Web-Browser kennt. Der Browser vergleicht den Hostnamen in der aufgelösten Webadresse mit dem Namen im Zertifikat. Um Zertifikatwarnungen vom Browser zu vermeiden, muss der in diesem Feld angegebene Wert mit dem Hostnamen übereinstimmen, der vom Browser zum Herstellen einer Verbindung mit dem Managementmodul verwendet wird. Beispiel: Wenn die Webadresse im Adressfeld "http://mm11.xyz.com/private/main.ssi" lautet, muss der im Feld **MM Host Name** (Hostname des Managementmoduls) angegebene Wert "mm11.xyz.com" lauten. Wenn die Webadresse "http://mm11/private/main.ssi" lautet, muss der verwendete Wert "mm11" lauten. Wenn die Webadresse "http://192.168.70.2/private/main.ssi" lautet, muss der verwendete Wert "192.168.70.2" lauten.

Dieses Zertifikatattribut wird im Allgemeinen als "allgemeiner Name" bezeichnet.

Dieses Feld ist auf maximal 60 Zeichen begrenzt.

- **Optionale Zertifikatsdaten**

  Die folgenden Benutzereingabefelder sind beim Erstellen eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung optional:

  Contact Person (Ansprechpartner)
  Geben Sie in diesem Feld den Namen des Ansprechpartners an, der für das Managementmodul verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

  Email Address (E-Mail-Adresse)
  Geben Sie in diesem Feld die E-Mail-Adresse des Ansprechpartners an, der für das Managementmodul verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

  Organizational Unit (Organisationseinheit)
  Geben Sie in diesem Feld die Einheit innerhalb des Unternehmens an, in der das Managementmodul verwendet wird. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

  Surname (Nachname)
  Geben Sie in diesem Feld zusätzliche Informationen an, wie etwa den Nachnamen der Person, die für das Managementmodul verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

  Given Name (Vorname)
  Geben Sie in diesem Feld zusätzliche Informationen an, wie etwa

den Vornamen der Person, die für das Managementmodul verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Initials (Initialen)
Geben Sie in diesem Feld zusätzliche Informationen an, wie etwa die Initialen der Person, die für das Managementmodul verantwortlich ist. Dieses Feld ist auf maximal 20 Zeichen begrenzt.

DN Qualifier (Qualifikationsmerkmal des definierten Namens)
Geben Sie in diesem Feld zusätzliche Informationen an, wie etwa das Qualifikationsmerkmal des definierten Namens für das Managementmodul. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Years Valid (Gültigkeitsdauer in Jahren)
Dieses Feld wird nur für einen SSL-Server angezeigt. Für einen SSL-Client wird es nicht angezeigt.

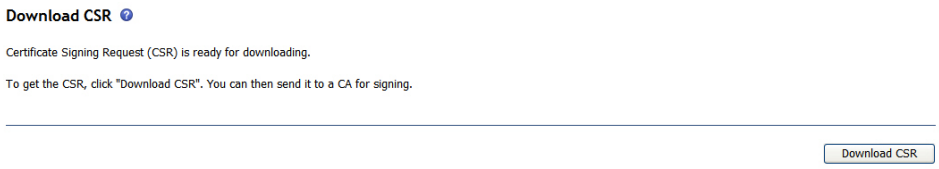
- **Attribute der Zertifikatssignieranforderung**

  Die folgenden Felder sind optional, es sei denn, sie werden von der ausgewählten Zertifizierungsstelle benötigt:

  Challenge Password (Kennwort abfragen)
  Verwenden Sie dieses Feld, um der Zertifikatssignieranforderung ein Kennwort zuzuweisen. Dieses Feld ist auf maximal 30 Zeichen begrenzt.

  Unstructured Name (Unstrukturierter Name)
  Geben Sie in diesem Feld zusätzliche Informationen an, wie etwa einen unstrukturierten Namen, der dem Managementmodul zugewiesen ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

5. Nachdem Sie die erforderlichen Informationen eingegeben haben, klicken Sie auf **Generate CSR** (Zertifikatssignieranforderung erstellen). Die neuen Chiffrierschlüssel und die Zertifikatssignieranforderung werden erstellt. Dieser Vorgang kann einige Minuten dauern. Eine Seite ähnlich der in der folgenden Abbildung wird nach Abschluss des Vorgangs angezeigt.



6. Klicken Sie auf **Download CSR** (Zertifikatssignieranforderung herunterladen) und dann auf **Save** (Speichern), um die Datei auf Ihrem Computer zu speichern. Beim Erstellen der Zertifikatssignieranforderung wird eine Datei im Format DER erstellt. Wenn Ihre Zertifizierungsstelle die Daten in einem anderen Format, wie z. B. PEM, erwartet, können Sie die Datei mit einem Tool wie OpenSSL (http://www.openssl.org) konvertieren. Wenn Sie von Ihrer Zertifizierungsstelle aufgefordert werden, den Inhalt der Datei mit der Zertifikatssignieranforderung in eine Webseite zu kopieren, wird in der Regel eine Datei im PEM-Format erwartet.

Der Befehl zum Konvertieren einer Zertifikatssignieranforderung mittels OpenSSL von DER in PEM lautet ähnlich wie der folgende Befehl:

```
openssl req -in csr.der -inform DER -out csr.pem -outform PEM
```

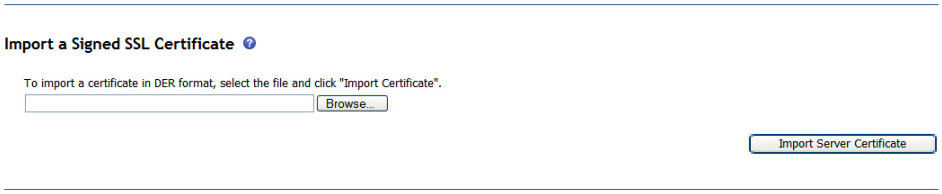
7. Senden Sie die Zertifikatssignieranforderung an Ihre Zertifizierungsstelle. Wenn die Zertifizierungsstelle Ihr signiertes Zertifikat zurückgibt, müssen Sie das Zertifikat möglicherweise in das DER-Format konvertieren. (Wenn Sie das Zertifikat als Text in einer E-Mail oder Webseite erhalten, weist sie vermutlich das Format PEM auf.) Sie können das Format mithilfe eines Tools, das von Ihrer Zertifizierungsstelle bereitgestellt wird, oder mithilfe eines Tools wie OpenSSL (http://www.openssl.org) ändern. Der Befehl zum Konvertieren eines Zertifikats von PEM in DER lautet ähnlich wie der folgende Befehl:

   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   Nachdem Sie das signierte Zertifikat von der Zertifizierungsstelle erhalten haben, fahren Sie mit Schritt 8 fort.

8. Klicken Sie im Navigationsfenster auf **MM Control → Security** (MM-Steuerung → Sicherheit). Blättern Sie abwärts bis zum Abschnitt **SSL Server Certificate Management** (Verwaltung von SSL-Serverzertifikaten), der ähnlich aussieht wie die Seite in der folgenden Abbildung.

9. Wählen Sie **Import a Signed Certificate** (Signiertes Zertifikat importieren) aus. Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



10. Klicken Sie auf **Browse** (Durchsuchen).
11. Klicken Sie auf die gewünschte Zertifikatsdatei und dann auf **Open** (Öffnen). Der Dateiname (mit Angabe des vollständigen Pfades) wird in dem Feld neben der Schaltfläche **Browse** (Durchsuchen) angezeigt.
12. Klicken Sie auf **Import Server Certificate** (Serverzertifikat importieren), um den Vorgang zu starten. Während die Datei zum Speicher des Managementmoduls übertragen wird, wird eine Statusanzeige angezeigt. Zeigen Sie diese Seite solange an, bis die Übertragung abgeschlossen ist.

SSL für den sicheren Web-Server aktivieren:

Sie können SSL (Secure Sockets Layer) für den sicheren Web-Server des Managementmoduls aktivieren.

Anmerkung: Damit SSL aktiviert werden kann, muss ein gültiges SSL-Zertifikat installiert werden.

Gehen Sie wie folgt vor, um den sicheren Web-Server zu aktivieren:

1. Klicken Sie im Navigationsfenster auf **MM Control → Security** (MM-Steuerung → Sicherheit). Die Seite, die angezeigt wird, ist der in der folgenden Abbildung ähnlich und zeigt, dass ein gültiges SSL-Serverzertifikat installiert wurde. Wenn der Status des SSL-Serverzertifikats nicht angibt, dass ein gültiges SSL-Zertifikat installiert wurde, finden Sie Informationen im Abschnitt „Verwaltung von SSL-Serverzertifikaten" auf Seite 55.

2. Blättern Sie abwärts bis zum Abschnitt "SSL Server Configuration for Web Server" (Konfiguration des SSL-Servers für den Web-Server) und wählen Sie im Feld **SSL Server** (SSL-Server) die Option **Enabled** (Aktiviert) aus. Klicken Sie anschließend auf **Save** (Speichern). Der ausgewählte Wert wird nach dem nächsten Neustart des Managementmoduls wirksam.

Verwaltung von SSL-Clientzertifikaten:

Der SSL-Client erfordert, dass ein gültiges Zertifikat und ein entsprechender privater Chiffrierschlüssel installiert werden, bevor SSL aktiviert wird.

Es stehen zwei Methoden zur Verfügung, um den privaten Schlüssel und das erforderliche Zertifikat zu generieren: Die Verwendung eines selbst signierten Zertifikats und die Verwendung eines von einer Zertifizierungsstelle signierten Zertifikats.

Anmerkung: Die Verwaltung von SSL-Clientzertifikaten ist optional. Sie können den SSL-Client für LDAP auch aktivieren, ohne ein selbst signiertes Zertifikat zu erstellen oder ein signiertes Zertifikat in den Client zu importieren.

Die Vorgehensweise zum Erstellen des privaten Chiffrierschlüssels und Zertifikats für den SSL-Client ist dieselbe wie beim SSL-Server, nur dass Sie nicht den Abschnitt **SSL Server Certificate Management** (Verwaltung von SSL-Serverzertifikaten) auf der Sicherheitswebseite verwenden, sondern den Abschnitt **SSL Client Certificate Management** (Verwaltung von SSL-Clientzertifikaten). Weitere Informationen zur Verwendung eines selbst signierten Zertifikats für den SSL-Client finden Sie im Abschnitt „Selbst signiertes Zertifikat erstellen" auf Seite 55. Informationen zur Verwendung eines von einer Zertifizierungsstelle signierten Zertifikats für den SSL-Client finden Sie im Abschnitt „Zertifikatssignieranforderung erstellen" auf Seite 57.

Verwaltung von vertrauenswürdigen SSL-Clientzertifikaten:

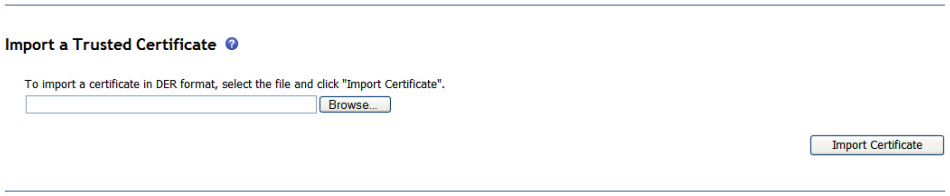
Der sichere SSL-Client (LDAP-Client) verwendet vertrauenswürdige Zertifikate, um den LDAP-Server positiv zu identifizieren.

Ein vertrauenswürdiges Zertifikat kann das Zertifikat der Zertifizierungsstelle sein, die das Zertifikat des LDAP-Servers signiert hat, oder es kann das Zertifikat des LDAP-Servers selbst sein. Bevor der SSL-Client aktiviert wird, muss mindestens ein Zertifikat in das Managementmodul importiert werden. Sie können bis zu drei vertrauenswürdige Zertifikate importieren.

Gehen Sie wie folgt vor, um ein vertrauenswürdiges Zertifikat zu importieren:

1. Wählen Sie im Navigationsfenster die Option **MM Control → Security** (MM-Steuerung → Sicherheit) aus.
2. Stellen Sie im Abschnitt "SSL Client Configuration for LDAP Client" (SSL-Clientkonfiguration für LDAP-Client) sicher, dass der SSL-Client inaktiviert ist. Wenn er nicht inaktiviert ist, wählen Sie im Feld **SSL Client** (SSL-Client) die Option **Disabled** (Inaktiviert) aus und klicken Sie anschließend auf **Save** (Speichern).
3. Blättern Sie weiter zum Abschnitt **SSL Client Trusted Certificate Management** (Verwaltung von vertrauenswürdigen SSL-Clientzertifikaten). Eine ähnliche Seite wie in der folgenden Abbildung wird angezeigt.

4. Klicken Sie neben einem der Felder **Trusted Certificate** (Vertrauenswürdiges Zertifikat) auf **Import** (Importieren). Eine ähnliche Seite wie in der folgenden Abbildung wird angezeigt.



5. Klicken Sie auf **Browse** (Durchsuchen).
6. Wählen Sie die gewünschte Zertifikatsdatei aus und klicken Sie auf **Open** (Öffnen). Der Dateiname (mit Angabe des vollständigen Pfads) wird in dem Feld neben der Schaltfläche **Browse** (Durchsuchen) angezeigt.
7. Zum Starten des Importprozesses klicken Sie auf **Import Certificate** (Zertifikat importieren). Während die Datei zum Speicher des Managementmoduls übertragen wird, wird eine Statusanzeige angezeigt. Schließen Sie diese Seite erst, wenn die Übertragung abgeschlossen ist.

Der Abschnitt zur Verwaltung von vertrauenswürdigen SSL-Clientzertifikaten auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit) sieht nun ähnlich aus wie in der folgenden Abbildung.

Nun steht die Schaltfläche **Remove** (Entfernen) der Option für das vertrauenswürdige Zertifikat 1 zur Verfügung. Wenn Sie ein vertrauenswürdiges Zertifikat entfernen möchten, klicken Sie auf die entsprechende Schaltfläche **Remove** (Entfernen).

Sie können weitere vertrauenswürdige Zertifikate importieren, indem Sie die Schaltflächen **Import** (Importieren) für die vertrauenswürdigen Zertifikate 2 und 3 verwenden.

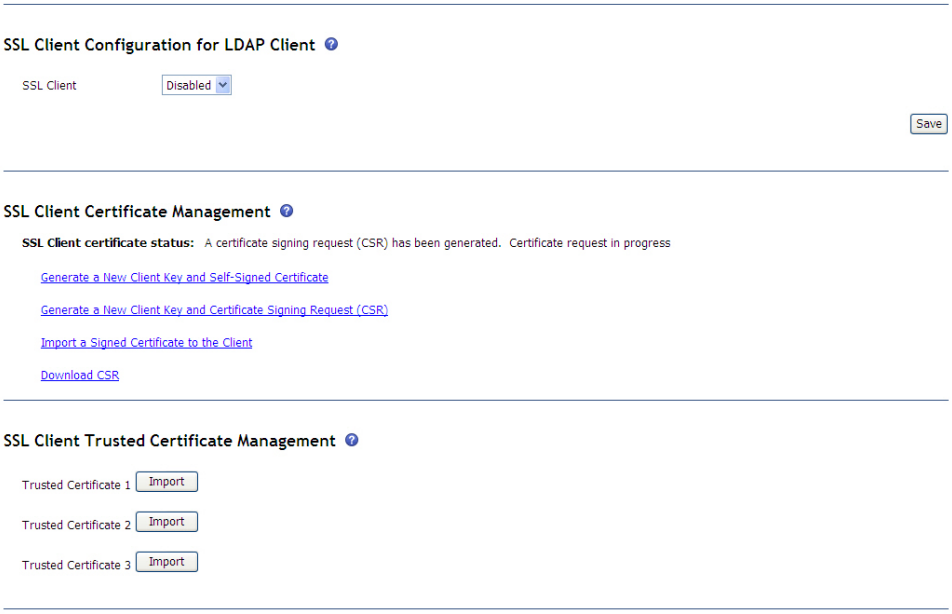
SSL für den LDAP-Client aktivieren:

Sie können SSL für den LDAP-Client des Managementmoduls aktivieren oder inaktivieren.

Verwenden Sie den Abschnitt "SSL Client Configuration for LDAP Client" (Konfiguration des SSL-Clients für den LDAP-Client) der Seite "Security" (Sicherheit), um SSL für den LDAP-Client zu aktivieren oder zu inaktivieren. Um SSL aktivieren zu können, müssen Sie ein gültiges SSL-Clientzertifikat und mindestens ein vertrauenswürdiges Zertifikat installieren.

Gehen Sie wie folgt vor, um SSL für den Client zu aktivieren:

1. Klicken Sie im Navigationsfenster auf **MM Control → Security** (MM-Steuerung → Sicherheit) und blättern Sie abwärts bis zum Abschnitt **SSL Client Configuration for LDAP Client** (Konfiguration des SSL-Clients für den LDAP-Client). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



Auf der Seite **MM Control → Security** (MM-Steuerung → Sicherheit) werden ein installiertes SSL-Clientzertifikat und das vertrauenswürdige Zertifikat 1 einer Zertifizierungsstelle angezeigt.

2. Wählen Sie auf der Seite **SSL Client Configuration for LDAP Client** (Konfiguration des SSL-Clients für den LDAP-Client) im Feld **SSL Client** (SSL-Client) die Option **Enabled** (Aktiviert) aus.
3. Klicken Sie auf **Save** (Speichern). Der ausgewählte Wert wird sofort wirksam.

SSH-Server konfigurieren (Secure Shell)

SSH (Secure Shell) ermöglicht den sicheren Zugriff auf die Befehlszeilenschnittstelle und die SOL-Umleitungsfunktionen (Serial Over LAN, Textkonsole) des Managementmoduls.

SSH-Benutzer werden über die Authentifizierung über öffentliche Schlüssel oder über die Kennwortauthentifizierung authentifiziert. Die Authentifizierung über öffentliche Schlüssel wird nur vom erweiterten Managementmodul unterstützt. SSH ist auf dem erweiterten Managementmodul standardmäßig aktiviert und es wird automatisch ein Hostschlüssel für SSH generiert.

Bei der Kennwortauthentifizierung wird das Kennwort nach dem Einrichten eines Verschlüsselungskanal gesendet. Bei der Kombination aus Anmelde-ID und Kennwort kann es sich um eine der 12 lokal oder auf einem LDAP-Server gespeicherten Kombinationen handeln.

SSH-Hostschlüssel erstellen:

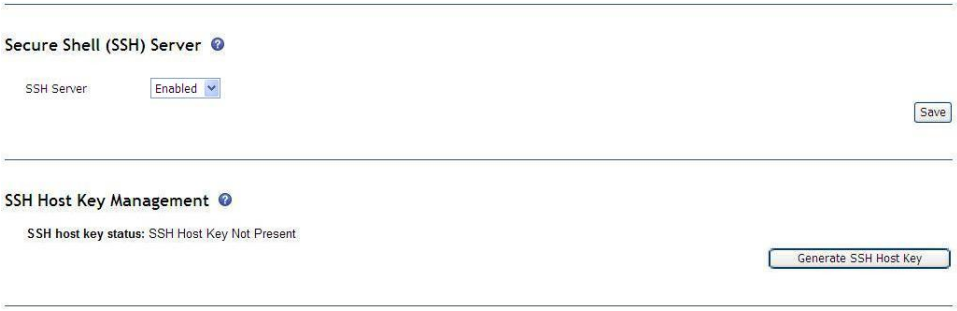
Sie können einen SSH-Hostschlüssel (Secure Shell) erstellen, um die Identität des SSH-Servers gegenüber dem Client zu authentifizieren.

Beim erweiterten Managementmodul werden die Hostschlüssel automatisch erstellt, wenn beim Aktivieren des SSH-Servers oder beim Aktivieren von Secure SMASH keine Hostschlüssel vorhanden sind. Der SSH-Server kann erst nach Abschluss der Schlüsselerstellung verwendet werden. Dieser Vorgang kann zwischen 3 und 5 Minuten in Anspruch nehmen. Im Ereignisprotokoll werden der Start und der Abschluss der Schlüsselerstellung aufgezeichnet.

Wenn Sie einen neuen Hostschlüssel anfordern, werden für den Zugriff auf das Managementmodul ein RSA-Schlüssel und ein DSA-Schlüssel erstellt. Damit der private Teil des SSH-Hostschlüssels geschützt bleibt, wird dieser während der Sicherung und Wiederherstellung der Konfiguration nicht gesichert.

Gehen Sie wie folgt vor, um einen neuen SSH-Hostschlüssel zu erstellen:

1. Klicken Sie im Navigationsfenster auf **MM Control → Security** (MM-Steuerung → Sicherheit).
2. Blättern Sie abwärts bis zum Abschnitt **Secure Shell (SSH) Server/SSH Host Key Management** (SSH-Server (Secure Shell)/Verwaltung von SSH-Hostschlüsseln). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



3. Klicken Sie auf **Generate SSH Host Key** (SSH-Hostschlüssel erstellen).

Der Prozess der Schlüsselerstellung wird im Hintergrund gestartet. Den Fortschritt des Prozesses der Schlüsselerstellung können Sie anhand des Ereignisprotokolls überprüfen. Wenn der SSH-Server aktiviert ist, wird er nach dem Erstellen des Hostschlüssels automatisch mit dem neuen Schlüssel neu gestartet.

SSH-Server aktivieren:

SSH ist auf dem erweiterten Managementmodul standardmäßig aktiviert und es wird automatisch ein Hostschlüssel für SSH generiert.

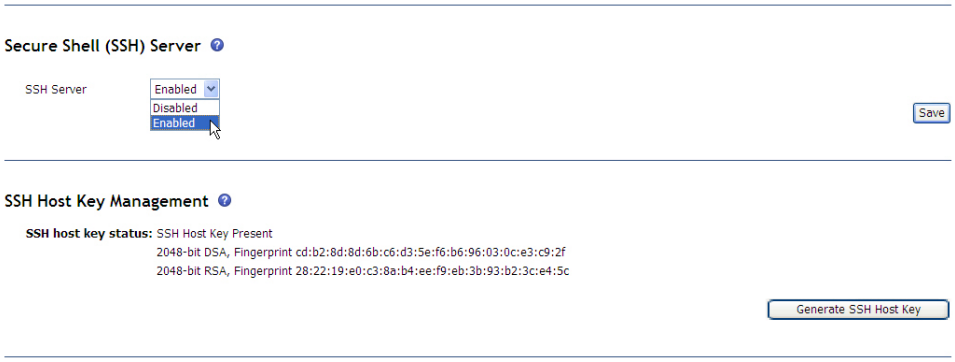
Der Wert, der auf der Seite angezeigt wird ("Enabled" (Aktiviert) oder "Disabled" (Inaktiviert)), ist der zuletzt ausgewählte Wert und der Wert, der beim Neustart des Managementmoduls verwendet wird. Beim erweiterten Managementmodul werden diese Änderungen sofort wirksam.

Anmerkungen:

- Der SSH-Server kann nur aktiviert werden, wenn ein gültiger SSH-Hostschlüssel installiert ist.
- Beim erweiterten Managementmodul sind die SSH- und Secure-SMASH-Schnittstellen standardmäßig aktiviert.
- Beim erweiterten Managementmodul kann der SSH-Server auch über SNMP oder über die Befehlszeilenschnittstelle des Managementmoduls aktiviert oder inaktiviert werden. Weitere Informationen finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des erweiterten BladeCenter-Managementmoduls*.

Gehen Sie wie folgt vor, um den SSH-Server zu aktivieren:

1. Klicken Sie im Navigationsfenster auf **Security** (Sicherheit).
2. Blättern Sie abwärts bis zum Abschnitt **Secure Shell (SSH) Server** (SSH-Server (Secure Shell)). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



3. Klicken Sie im Feld **SSH Server** (SSH-Server) auf **Enabled** (Aktiviert).
4. Klicken Sie im Navigationsfenster auf **Restart ASM** (ASM erneut starten), um das Managementmodul erneut zu starten.

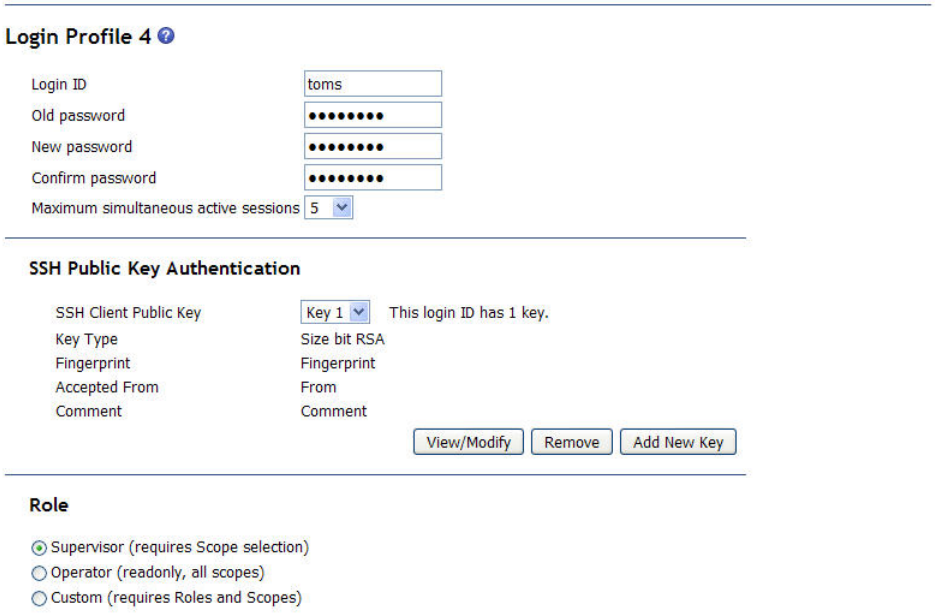
Öffentlichen SSH-Schlüssel zuordnen:

Sie können die Authentifizierung über einen öffentlichen SSH-Schlüssel verwenden, um auf SSH oder Secure SMASH zuzugreifen, ohne ein Kennwort zu benutzen.

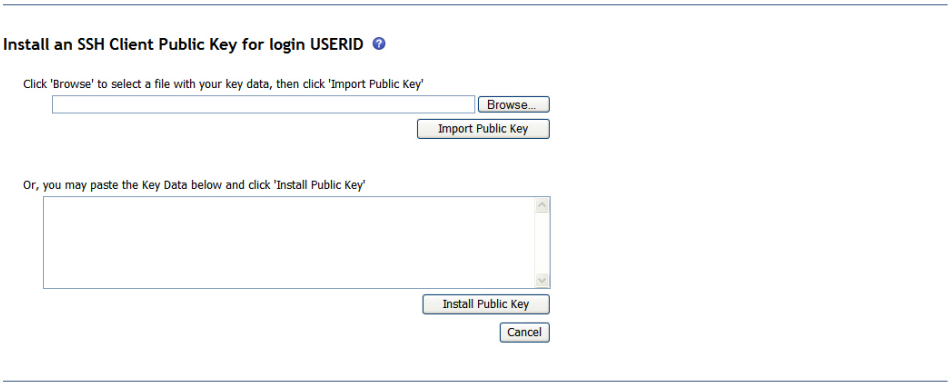
Sie können pro Anmeldeprofil bis zu vier private SSH-Schlüssel importieren. Dabei gilt für das erweiterte Managementmodulsystem die Obergrenze von 12 Schlüsseln.

Die öffentlichen Schlüssel werden den angegebenen Benutzern zugeordnet. Gehen Sie wie folgt vor, um einen öffentlichen Schlüssel zuzuordnen:

1. Klicken Sie im Navigationsfenster auf **MM Control → Login profiles** (MM-Steuerung → Anmeldeprofile). Wenn die Anmelde-ID nicht angezeigt wird, müssen Sie eine Anmelde-ID und ein Kennwort eingeben, das Kennwort bestätigen und diese Angaben speichern. Fahren Sie dann mit Schritt 2 fort.
2. Wählen Sie die Anmelde-ID aus, die Sie verwenden möchten. Eine ähnliche Seite wie in der folgenden Abbildung wird angezeigt.



3. Um dem ausgewählten Benutzer einen neuen öffentlichen Schlüssel zuzuordnen, klicken Sie auf **Add New Key** (Neuen Schlüssel hinzufügen). Eine ähnliche Seite wie in der folgenden Abbildung wird angezeigt.



4. Wenn Sie über Ihr Verzeichnissystem auf den öffentlichen Schlüssel zugreifen können, klicken Sie auf **Browse** (Durchsuchen), um die Datei zu suchen, die verwendet werden soll. Klicken Sie anschließend auf **Import Public Key** (Öffentlichen Schlüssel importieren).
5. Wenn sich die Daten zum öffentlichen Schlüssel in einem geöffneten Dokument befinden, kopieren Sie die Daten und fügen Sie sie in das angegebene Feld ein. Klicken Sie dann auf **Install Public Key** (Öffentlichen Schlüssel installieren).

Weitere Informationen zum Anzeigen, Ändern und Löschen von öffentlichen Schlüsseln finden Sie im Abschnitt „Login Profiles (Anmeldeprofile)" auf Seite 172.

Secure Shell-Server verwenden:

Verwenden Sie den Secure Shell-Server des Managementmoduls, um eine sichere Verbindung zu einer Befehlszeilenschnittstelle (Command-Line Interface, CLI) zu öffnen.

Folgende SSH-Clients stehen zur Verfügung. Es wurden einige SSH-Clients getestet, die Unterstützung oder Nichtunterstützung eines bestimmten SSH-Clients ist jedoch nicht enthalten.

- SSH-Clients, die im Lieferumfang von Betriebssystemen wie beispielsweise Linux, AIX und UNIX enthalten sind (siehe die Dokumentation Ihres Betriebssystems).
- Der SSH-Client von cygwin (weitere Informationen finden Sie unter http://www.cygwin.com)

Wenn Sie einen auf openSSH basierenden SSH-Client verwenden, wie zum Beispiel den Client, der im Lieferumfang von Red Hat Linux, Version 7.3, enthalten ist, um eine interaktive Secure Shell-Befehlszeilensitzung mit einem Managementmodul mit der Netzadresse 192.168.70.2 zu starten, geben Sie einen Befehl ähnlich dem folgenden Beispiel ein:

```
ssh -x -l USERID 192.168.70.2
```

Dabei gibt `-x` an, dass keine X Window System-Weiterleitung erfolgt und `-l` gibt an, dass die Sitzung die Anmelde-ID "USERID" verwenden soll.

Das erweiterte Managementmodul unterstützt nicht-interaktive Secure Shell-Sitzungen. Diese Unterstützung ist äußerst nützlich in Verbindung mit der Authentifizierung über öffentliche Schlüssel. Verwenden Sie diese Funktionalität, um einen einzelnen CLI-Befehl auszugeben, indem Sie den Befehl an das Ende des SSH-Befehls anhängen. Um beispielsweise eine Liste der gegenwärtigen Benutzer des erweiterten Managementmoduls abzurufen, geben Sie Folgendes ein:

```
ssh -l USERID 192.168.70.2 users -T mm[1] -curr
```

Wenn der CLI-Befehl ein Sonderzeichen erfordert, wie beispielsweise ein Anführungszeichen, stellen Sie diesem Zeichen eine Escapezeichenfolge voran, sodass es von der Befehlsshell Ihres Clientsystems ordnungsgemäß verarbeitet wird. Wenn Sie zum Beispiel eine Warnmeldung bei Überschreitung einrichten möchten, geben Sie einen ähnlichen Befehl wie den folgenden ein:

```
ssh -l USERID 192.168.70.2 trespass -T mm[1] -tw \"New  WARNING\"
```

Der Prozess zum Starten einer Serial-over-LAN- Umleitungssitzung über Texteingabe an einen Blade-Server ist ähnlich, aber in diesem Fall ist es wichtig anzugeben, dass die Secure Shell-Serversitzung ein Pseudoterminal (PTY) verwenden muss, um die richtige Ausgabeformatierung und die Behandlung der Tastenanschläge

richtig einzustellen. Im folgenden Beispiel, das eine Serial-over-LAN-Sitzung auf dem Blade-Server in Position 2 startet, gibt die Option `-t` für den SSH-Client an, dass ein Pseudoterminal zugeordnet werden sollte:

```
ssh -t -l USERID 192.168.70.1 console -T blade[2]
```

SMASH aktivieren

Sie können das erweiterte Managementmodul für die Verwendung des Befehlszeilenprotokolls SMASH CLP (System Management Architecture for Server Hardware Command Line Protocol) konfigurieren.

Über die Seite "Network Protocols" (Netzprotokolle) können Sie die Befehlszeilenprotokolle SMASH bzw. Secure SMASH aktivieren oder inaktivieren. Diese Änderungen werden sofort wirksam.

Anmerkungen:

- Um die SMASH-Schnittstelle verwenden zu können, müssen Sie eine Anmelde-ID verwenden, die auf der Seite "Login Profiles" (Anmeldeprofile) definiert wurde. Mittels LDAP authentifizierte Benutzer haben keinen Zugriff auf die SMASH-Schnittstellen.
- Die Secure-SMASH-Schnittstelle ist standardmäßig aktiviert.
- Wenn kein SSH-Hostschlüssel vorhanden und das Befehlszeilenprotokoll Secure SMASH aktiviert ist, wird der SSH-Hostschlüssel automatisch erstellt. Das Erstellen des SSH-Hostschlüssels kann bis zu 5 Minuten in Anspruch nehmen. Die Schlüsselerstellung wird im Ereignisprotokoll aufgezeichnet.
- Weitere Informationen erhalten Sie im Installations- und Benutzerhandbuch *IBM SMASH Proxy Installation and User's Guide*.

Gehen Sie wie folgt vor, um das Befehlszeilenprotokoll SMASH zu aktivieren:

1. Klicken Sie im Navigationsfenster auf **Network Protocols** (Netzprotokolle).
2. Blättern Sie abwärts bis zum Abschnitt **SMASH Command Line Protocol (CLP)** (Befehlszeilenprotokoll SMASH). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.

3. Um das Befehlszeilenprotokoll SMASH über Telnet zu aktivieren, klicken Sie im Feld **SMASH CLP** (SMASH CLP) auf **Enabled** (Aktiviert). Der ausgewählte Wert ("Enabled" (Aktiviert) bzw. "Disabled" (Inaktiviert)) wird sofort wirksam.
4. Um das Befehlszeilenprotokoll Secure SMASH über SSH zu aktivieren, klicken Sie im Feld **Secure SMASH CLP** (Secure SMASH CLP) auf **Enabled** (Aktiviert). Der ausgewählte Wert ("Enabled" (Aktiviert) bzw. "Disabled" (Inaktiviert)) wird sofort wirksam.
5. Klicken Sie auf **Save** (Speichern).

SMASH verwenden:

Sie können das Befehlszeilenprotokoll SMASH CLP (System Management Architecture for Server Hardware Command Line Protocol) für die Kommunikation mit dem erweiterten Managementmodul verwenden. Weitere Informationen erhalten Sie im Installations- und Benutzerhandbuch *Installations- und Benutzerhandbuch zu IBM SMASH Proxy*.

Zum Starten einer interaktiven SMASH CLP-Sitzung mithilfe eines SSH-Clients wie beispielsweise ein OpenSSH-Client mit einem erweiterten Managementmodul mit der Netzadresse 192.168.70.2 geben Sie einen ähnlichen Befehl wie den folgenden ein:

```
ssh -p 50022 -l USERID 192.168.70.2
```

Dabei gibt `-p 50022` den TCP-Anschluss 50022 an, die Standardportnummer für Secure SMASH auf dem erweiterten Managementmodul, und `-l USERID` gibt eine der 12 Anmelde-IDs des lokalen Kontos an.

Das erweiterte Managementmodul unterstützt nicht-interaktive Secure SMASH-Sitzungen. Diese Unterstützung ist äußerst nützlich in Verbindung mit der Authentifizierung über öffentliche Schlüssel. Verwenden Sie diese Funktionalität, um einen einzelnen SMASH CLP-Befehl auszugeben. Beim Starten einer nicht-interaktiven SMASH-Sitzung ist es wichtig anzugeben, dass der Secure SMASH-Server ein Pseudoterminal (PTY) verwenden soll. Wenn kein Pseudoterminal für die Sitzung angegeben wird, wird die Fehlermeldung `Input Redirection not Supported` (Eingabeumleitung wird nicht unterstützt) angezeigt. Um beispielsweise eine Liste der mit SMASH adressierbaren Entitäten abzurufen, geben Sie einen ähnlichen Befehl wie den folgenden ein:

```
ssh -t -p 50022 -l USERID 192.168.70.2 show /modular1
```

Dabei gibt `-t` an, dass für die Sitzung ein Pseudoterminal erforderlich ist, und `show /modular1` ist der SMASH-Befehl, der auf dem erweiterten Managementmodul ausgeführt werden soll.

Wenn Sie einen Telnet-Client verwenden, um eine interaktive SMASH-CLP-Sitzung zu starten, müssen Sie die richtige TCP-Anschlussnummer angeben. In der Standardeinstellung hat der dem SMASH -Protokoll zugewiesene Anschluss die Nummer 50023.

Syslog aktivieren

Wählen Sie **MM Control → Network Protocols** (MM-Steuerung → Netzprotokolle) aus, um das Syslog-Protokoll zu aktivieren oder zu inaktivieren.

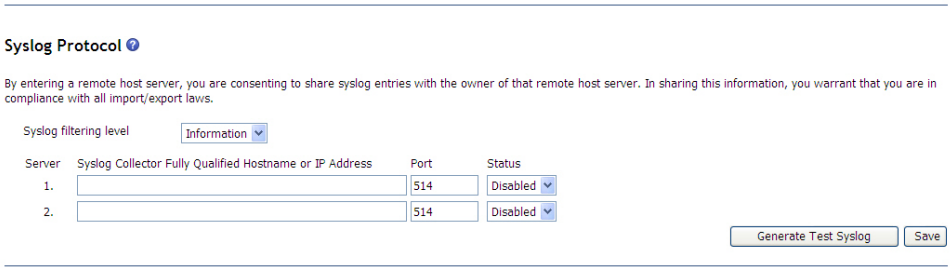
Das Syslog-Protokoll stellt eine Methode für das erweiterte Managementmodul bereit, mit der Ereignisprotokollnachrichten gemäß RFC 3164 über das Netz an bis zu zwei Syslog-Collectors gesendet werden können. Diese Methode ist hilfreich, da im Ereignisprotokoll des erweiterten Managementmoduls nur eine begrenzte Anzahl von Nachrichten gespeichert werden kann, sodass die ältesten Nachrichten überschrieben werden, sobald das Protokoll voll ist. Durch die Konfiguration der Syslog-Collectors vermeiden Sie also den Verlust von Ereignisnachrichten. Der Syslog-Service des erweiterten Managementmoduls ist standardmäßig inaktiviert. Sie können die Syslog-Collectors aktivieren und konfigurieren, indem Sie ihre IP-Adressen, Hostnamen und Portnummern angeben. (Die Standardportnummer lautet 514.)

Das erweiterte Managementmodul bietet zudem die Möglichkeit, die übertragenen Protokollnachrichten für alle Ziele nach der Mindestbewertung hinsichtlich der Wertigkeit zu filtern.

Anmerkung: Beim erweiterten Managementmodul werden diese Änderungen sofort wirksam.

Gehen Sie wie folgt vor, um das Syslog-Protokoll zu aktivieren:

1. Klicken Sie im Navigationsfenster auf **Network Protocols** (Netzprotokolle).
2. Blättern Sie abwärts bis zum Abschnitt **Syslog Protocol** (Syslog-Protokoll). Eine Seite ähnlich der in der folgenden Abbildung wird angezeigt.



3. Verwenden Sie das Feld **Syslog filtering level** (Syslog-Filtergrad), um festzulegen, welche Einträge im Ereignisprotokoll je nach Bewertungsstufe des Ereignisses an den fernen Syslog-Collector weitergeleitet werden.
   - **Error** (Fehler): Einträge im Ereignisprotokoll mit der Bewertungsstufe "Error" (Fehler) werden an den fernen Syslog-Collector weitergeleitet.
   - **Warning** (Warnung): Einträge im Ereignisprotokoll mit der Bewertungsstufe "Error" (Fehler) oder "Warning" (Warnung) werden an den fernen Syslog-Collector weitergeleitet.
   - **Information** (Information): Alle Einträge im Ereignisprotokoll werden an den Syslog-Collector weitergeleitet.
4. Verwenden Sie die Felder **Syslog Collector Host Name or IP Address** (Hostname oder IP-Adresse des Syslog-Collectors), um die IP-Adresse oder, wenn DNS aktiviert und konfiguriert ist, den Hostnamen des Syslog-Collectors anzugeben. Sie können bis zu zwei Syslog-Collectors angeben.
5. Verwenden Sie das Feld **Port** (Port), um die Nummer des Zielports anzugeben, an dem die Ereignisprotokolle des erweiterten Managementmoduls auf dem Syslog-Collector empfangen werden.
6. Wählen Sie im Feld **Status** (Status) die Option **Enabled** (Aktiviert) oder **Disabled** (Inaktiviert) aus, um anzugeben, ob die Ereignisprotokolle des Managementmoduls an den Syslog-Collector gesendet werden sollen.

Klicken Sie auf **Generate Test Syslog** (Test-Syslog erstellen), um ein Syslog-Testpaket zu erstellen, mit dem überprüft wird, ob die Syslog-Collector-Informationen ordnungsgemäß konfiguriert wurden.

Linux-TFTP-Server konfigurieren

Sie müssen die Konfiguration von Linux-basierten TFTP-Servern ändern, damit bestimmte automatisierte Funktionen, wie z. B. Service Advisor, unterstützt werden.

Damit automatisch eine Servicedatendatei mithilfe von TFTP auf einen angegebenen Server übertragen werden kann, wenn ein Call-Home-Ereignis erkannt wird, muss die TFTP-Konfigurationsdatei so geändert werden, dass sie auch die Option zum Erstellen von Dateien auf dem TFTP-Server enthält. Gehen Sie wie folgt vor:

1. Öffnen Sie die TFTP-Konfigurationsdatei im Verzeichnis "/etc/xinet.d".
2. Fügen Sie die Option "-c" zum Argument "server_args" hinzu.
3. Speichern und schließen Sie die Datei.
4. Starten Sie den TFTP-Server mit dem Befehl `/etc/rc.d/init.d/xinetd restart` erneut.

Im folgenden Beispiel ist eine Konfigurationsdatei "/etc/xinetd.d/tftp" dargestellt, bei der die Option "-c" zum Serverargument hinzugefügt wurde:

Geänderte Inhalte von "/etc/xinetd.d/tftp"

```
service tftp
{
socket_type             = dgram
protocol                = udp
wait                    = yes
user                    = root
server                  = /usr/sbin/in.tftpd
server_args             = -c -s /tftpboot
disable                 = no
per_source              = 11
cps                     = 100 2
flags                   = IPv4
}
```

Wake on LAN konfigurieren

Sie können mithilfe des Managementmoduls Wake on LAN für Blade-Server konfigurieren, die diese Funktion unterstützen. Weitere Informationen dazu finden Sie in der Dokumentation zu Ihrem Blade-Server.

Anmerkung: Diese Funktion ist nicht bei allen Blade-Server-Modellen verfügbar. Weitere Informationen dazu finden Sie in der Dokumentation zu Ihrem Blade-Server.

Gehen Sie wie folgt vor, um die Funktion Wake on LAN in der BladeCenter-Einheit zu konfigurieren:

1. Notieren Sie die jeweiligen MAC-Adressen der integrierten Ethernet-Controller in den einzelnen Blade-Servern. Sie finden diese Angaben mithilfe einer der folgenden Möglichkeiten. Die MAC-Adressen sind erforderlich, um ein fernes System so zu konfigurieren, dass es die Blade-Server über die Funktion Wake on LAN einschaltet: Das ferne System gibt den Wake on LAN-Befehl aus (einen Aktivierungspaket-Frame), indem es ihn an eine MAC-Adresse sendet.
   - Die MAC-Adressen der Blade-Server gehören zu den elementaren Produktdaten (VPD), die das Managementmodul für alle installierten Blade-Server verwaltet. (Wechseln Sie zum Abschnitt **Monitors → Hardware VPD** (Monitore → Elementare Hardware-Produktdaten) in der Webschnittstelle des Managementmoduls und zeigen Sie den Abschnitt mit dem Blade-Server-Hardwarebestand an. Klicken Sie auf den Modulnamen eines bestimmten Blade-Servers, um auf die Seite mit den elementaren Produktdaten des Blade-Servers zuzugreifen. Wählen Sie auf dieser Seite oben die Registerkarte **Ports** (Anschlüsse) aus, um die Daten zur MAC-Adresse anzuzeigen.
   - Die MAC-Adresse befindet sich auch auf dem Barcodeetikett an der Unterseite des Blade-Server-Gehäuses. Jeder Blade-Server besitzt außerdem möglicherweise ein loses Etikett, auf dem die MAC-Adressen gedruckt sind.
   - Bei einigen Blade-Server-Typen können Sie die MAC-Adresse auch mithilfe des Konfigurationsdienstprogramms des Blade-Servers lesen (**Devices and I/O Ports → System MAC Addresses** (Einheiten und E/A-Anschlüsse → System-MAC-Adressen)).
2. Stellen Sie sicher, dass die Funktion Wake on LAN im BladeCenter-Managementmodul aktiviert ist (**Blade Tasks → Power/Restart** (Blade-Tasks → Einschalten/Neu starten) und **Blade Tasks → Configuration** (Blade-Tasks → Konfiguration) in der Webschnittstelle des Managementmoduls).
3. Vergewissern Sie sich, dass die externen Anschlüsse der Ethernet-Switchmodule oder der Durchgriffsmodule in den E/A-Modulpositionen 1 und 2 aktiviert sind (**I/O Module Tasks → Admin/Power/Restart → I/O Module Advanced Setup** (E/A-Modul-Tasks → Admin/Einschalten/Neu starten → E/A-Modul, Erweiterte Konfiguration) in der Webschnittstelle des Managementmoduls). Wenn die externen Anschlüsse nicht aktiviert sind, können die Blade-Server in der BladeCenter-Einheit nicht mit dem externen Netz kommunizieren.

Wake on LAN-Konfiguration überprüfen

Gehen Sie wie folgt vor, um zu überprüfen, ob die Funktion Wake on LAN richtig konfiguriert wurde und ordnungsgemäß funktioniert:

1. Starten Sie das Betriebssystem des Blade-Servers.
2. Versuchen Sie, den fernen Computer, der den Wake on LAN-Befehl (Aktivierungspaket-Frame) ausgeben soll, mit Ping zu überprüfen. Ein erfolgreich zurückgegebenes Ping-Signal dient zur Überprüfung der Netzkonnektivität.
3. Stellen Sie sicher, dass der Blade-Server der aktuelle Eigentümer der Tastatur, des Bildschirms und der Maus ist.
4. Schalten Sie den Blade-Server aus, legen Sie eine bootfähige Diskette in ein über USB angehängtes Diskettenlaufwerk ein und starten Sie dann den Blade-Server erneut.
5. Wenn die Eingabeaufforderung "A:\" angezeigt wird, schalten Sie den Blade-Server am Netzschalter aus.
6. Geben Sie vom fernen Computer aus den Wake on LAN-Befehl (Aktivierungspaket-Frame) aus. Wenn die Wake on LAN-Funktion richtig konfiguriert wurde und ordnungsgemäß funktioniert, wird der Blade-Server aktiviert. Diese Methode ist sehr nützlich, um festzustellen, ob im Betriebssystem ein Fehler in der Blade-Server- oder BladeCenter-Konfiguration oder bei einem Einheitentreiber aufgetreten ist.

Linux-spezifische Konfiguration

Gehen Sie wie folgt vor, um die Funktion Wake on LAN für Red Hat oder SUSE Linux zu konfigurieren:

1. Geben Sie den folgenden Befehl ein:
   ```
   insmod bcm5700.o enable_wol=1,1
   ```
   Der Parameter `enable_wol=1,1` weist den Einheitentreiber an, die Funktion Wake on LAN für beide Broadcom-Controller in einem einzelnen Blade-Server zu aktivieren. Da es zwei Broadcom-Controller gibt, müssen Sie für jeden eine 1 angeben.
2. Kompilieren Sie den Einheitentreiber für Ihr Linux-Image erneut. Beispielsweise ist nicht garantiert, dass ein Einheitentreiber, der in Red Hat Linux kompiliert wurde, auch bei SUSE Linux funktioniert. Informationen zum Kompilieren von Einheitentreibern finden Sie in der Dokumentation Ihres Betriebssystems. Für das Kompilieren der Broadcom-Einheitentreiber in Red Hat Linux reicht die Standardinstallation nicht aus, da nicht alle für eine erfolgreiche Kompilierung erforderlichen Dateien enthalten sind. Eine benutzerdefinierte Installation von Red Hat Linux, in der die Pakete für Software- und Kernelentwicklung ausgewählt sind, enthält die Dateien, die für die erfolgreiche Kompilierung von Einheitentreibern erforderlich sind.

Konfigurationsdatei verwenden

Mithilfe einer Konfigurationsdatei können Sie die Konfiguration des Managementmoduls sichern und wiederherstellen.

Verfahren zum Sichern und Wiederherstellen der Konfiguration des Managementmoduls finden Sie in den folgenden Abschnitten.

- „Konfiguration des Managementmoduls sichern"
- „Konfiguration des Managementmoduls wiederherstellen und ändern" auf Seite 77

Anmerkung: Wenn über die Webschnittstelle keine Datenübertragung mehr mit einem Austauschmanagementmodul möglich ist, hat es möglicherweise eine andere IP-Adresse als das Managementmodul, das entfernt wurde. Mit dem IP-Grundstellungsknopf können Sie die werkseitige Voreinstellung für die IP-Adressen des Managementmoduls wiederherstellen. Greifen Sie dann über die werkseitig voreingestellte IP-Adresse auf das Managementmodul zu (die werkseitig voreingestellten IP-Adressen und Anweisungen zur Verwendung des IP-Grundstellungsknopfs finden Sie im *Installationshandbuch* Ihres Managementmoduls) und konfigurieren Sie das Managementmodul oder laden Sie die gespeicherte Konfigurationsdatei.

Konfiguration des Managementmoduls sichern

Wenn Sie die Konfiguration des Managementmoduls in einer Konfigurationsdatei in der BladeCenter-Einheit sichern, können Sie die Konfiguration des Managementmoduls wiederherstellen, wenn sie versehentlich geändert oder beschädigt wurde.

Bei allen Managementmodultypen kann die Konfiguration des Managementmoduls in einer Datei gesichert werden. Beim erweiterten Managementmodul können Sie die Konfiguration des Managementmoduls zudem in der Rückwandplatine der BladeCenter-Einheit sichern. Für die Sicherung der Managementmodulkonfiguration sind spezielle Benutzerberechtigungen erforderlich. (Informationen hierzu finden Sie im Abschnitt „Webschnittstellenseiten und Benutzerrollen" auf Seite 100.)

Sie können eine Kopie der aktuellen Konfiguration des Managementmoduls auf den Client-Computer herunterladen, auf dem die Webschnittstelle des Managementmoduls ausgeführt wird. Verwenden Sie diese Sicherungskopie, um die Konfiguration des Managementmoduls wiederherzustellen, wenn sie versehentlich geändert oder beschädigt wurde. Verwenden Sie sie als Basis, die Sie ändern können, um mehrere Managementmodule mit ähnlicher Konfiguration zu konfigurieren.

Konfiguration eines erweiterten Managementmoduls sichern:

Sie können die Konfiguration für ein erweitertes Managementmodul sichern.

Gehen Sie wie folgt vor, um die aktuelle Konfiguration zu sichern:

1. Melden Sie sich bei dem Managementmodul an, dessen aktuelle Konfiguration gesichert werden soll. Weitere Informationen hierzu finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **MM Control → Configuration Mgmt** (MM-Steuerung → Konfigurationsverwaltung).
3. Wählen Sie die Art der Sicherung aus, die durchgeführt werden soll:
   - **Backup Configuration to File** (Konfiguration in Datei sichern)
   - **Save Configuration to Chassis** (Konfiguration in Gehäuse speichern)

   Anmerkungen:
   - Wenn für die BladeCenter-Einheit die Datenverschlüsselung aktiviert ist, müssen Sie für die Konfigurationsdatei ein Kennwort eingeben. Dieses Kennwort muss beim Wiederherstellen der Konfigurationsdatei eingegeben werden.
   - Konfigurationsdateien, die von BladeCenter-Einheiten gespeichert werden, bei denen die Datenverschlüsselung aktiviert ist, können nur mit Firmwareversionen des erweiterten Managementmoduls verwendet werden, die die Datenverschlüsselung unterstützen.
   - Wenn für die BladeCenter-Einheit die Datenverschlüsselung aktiviert ist und die UUID (Universally Unique Identifier) der BladeCenter-Einheit geändert wird, werden in der BladeCenter-Einheit gesicherte Konfigurationsdaten ungültig: Sie müssen die Konfiguration nach dem Ändern der UUID daher erneut sichern.

   a. Um die Konfiguration in der BladeCenter-Einheit zu speichern, klicken Sie auf **Save** (Speichern). Wenn Sie die Konfiguration für andere BladeCenter-Einheiten als BladeCenter H-Einheiten sichern, klicken Sie auf **Save (compressed format)** (Speichern (komprimiertes Format)), um die Konfiguration in einem komprimierten Format zu speichern, das weniger Speicherplatz belegt. (Bei BladeCenter H-Einheiten wird die Konfiguration automatisch in einem komprimierten Format gespeichert.)
   b. Um die Konfiguration in einer Datei zu sichern, klicken Sie im Abschnitt **Backup Configuration to File** (Konfiguration in Datei sichern) auf **View the current configuration summary** (Aktuelle Konfigurationszusammenfassung anzeigen) und gehen Sie wie folgt vor.

      Anmerkung: Die Sicherheitseinstellungen für die Datenverschlüsselung auf der Seite "Security" (Sicherheit) werden nicht gesichert.

      1) Überprüfen Sie die Einstellungen und klicken Sie dann auf **Close** (Schließen).
      2) Um die Konfiguration zu sichern, klicken Sie auf **Backup** (Sichern).
      3) Geben Sie einen Namen für die Sicherung ein, wählen Sie den Speicherort für die Datei aus und klicken Sie auf **Save** (Speichern).
         - Klicken Sie in Mozilla Firefox auf **Save to Disk** (Auf Datenträger speichern) und dann auf **OK**.
         - Klicken Sie in Microsoft Internet Explorer auf **Datei auf Datenträger speichern** und dann auf **OK**.

Konfiguration des Managementmoduls wiederherstellen und ändern

Sie können eine Standardkonfiguration oder eine gespeicherte Konfiguration vollständig wiederherstellen oder Sie können Schlüsselfelder in der gespeicherten Konfiguration ändern, bevor Sie die Konfiguration für das Managementmodul wiederherstellen.

Änderungen an der Konfigurationsdatei vor ihrer Wiederherstellung helfen Ihnen dabei, mehrere Managementmodule mit ähnlichen Konfigurationen einzurichten. Sie können schnell Parameter festlegen, die eindeutige Werte erfordern, wie z. B. Namen und IP-Adressen, ohne dass Sie allgemeine, gemeinsam genutzte Informationen eingeben müssen. Mit dem erweiterten Managementmodul können Sie auch eine Konfiguration wiederherstellen, die zuvor auf der Rückwandplatine der BladeCenter-Einheit gespeichert wurde. Die Wiederherstellung der Konfiguration des Managementmoduls erfordert spezielle Benutzerberechtigungen (Informationen dazu finden Sie im Abschnitt „Webschnittstellenseiten und Benutzerrollen" auf Seite 100).

Konfiguration eines Managementmoduls wiederherstellen:

Sie können Ihre aktuelle Konfiguration wiederherstellen oder ändern, indem Sie eine gespeicherte Konfiguration für das Managementmodul verwenden.

Gehen Sie wie folgt vor:

1. Melden Sie sich an dem Managementmodul an, dessen Konfiguration Sie wiederherstellen möchten. Weitere Informationen hierzu finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13.
2. Bestimmen Sie die Art der Wiederherstellung, die Sie durchführen möchten: **Restore Defaults** (Standardwerte wiederherstellen) oder **Restore Configuration from File** (Konfiguration aus Datei wiederherstellen).
   a. Zum Wiederherstellen der Standardkonfiguration klicken Sie im Navigationsfenster auf **MM Control → Restore Defaults** (MM-Steuerung → Standardwerte wiederherstellen) und dann auf **Restore Defaults** (Standardwerte wiederherstellen).
   b. Zum Wiederherstellen der Konfiguration aus einer Datei klicken Sie im Navigationsfenster auf **MM Control → Configuration File** (MM-Steuerung → Konfigurationsdatei) und gehen Sie dann wie folgt vor:
      1) Klicken Sie im Abschnitt **Restore MM Configuration** (MM-Konfiguration wiederherstellen) auf **Browse** (Durchsuchen).
      2) Klicken Sie auf die gewünschte Konfigurationsdatei und dann auf **Open** (Öffnen). Die Datei wird (einschließlich des vollständigen Pfads) im Feld neben **Browse** (Durchsuchen) angezeigt.
      3) Wenn Sie keine Änderungen an der Konfigurationsdatei vornehmen möchten, klicken Sie auf **Restore** (Wiederherstellen). Ein neues Fenster mit den Konfigurationsdaten für das Managementmodul wird geöffnet. Vergewissern Sie sich, dass es sich um die Konfiguration handelt, die Sie wiederherstellen möchten. Handelt es sich nicht um die richtige Konfiguration, klicken Sie auf **Cancel** (Abbrechen). Um die Konfigurationsdatei zu ändern, bevor sie wiederhergestellt wird, klicken Sie auf **Modify and Restore** (Ändern und wiederherstellen).

Dadurch wird ein Fester mit einer bearbeitbaren Konfigurationszusammenfassung geöffnet. Zu Beginn werden nur die Felder angezeigt, die Sie ändern können. Um zwischen dieser Ansicht und der vollständigen Ansicht der Konfigurationszusammenfassung zu wechseln, klicken Sie oben oder unten im Fenster auf **Toggle View** (Ansicht umschalten).

Anmerkung: Wenn Sie auf **Restore** (Wiederherstellen) oder **Modify and Restore** (Ändern und wiederherstellen) klicken, wird möglicherweise ein Alertfenster geöffnet, falls die Konfigurationsdatei, die Sie wiederherstellen möchten, mit einem Managementmodul mit älterer Firmware (und daher weniger Funktionalität) erstellt wurde. Diese Alertnachricht enthält eine Liste mit Systemverwaltungsfunktionen, die Sie nach beendeter Wiederherstellung konfigurieren müssen. Einige Funktionen erfordern Konfigurationen in mehr als einem Fenster.

4) Um die Wiederherstellung dieser Datei für das Managementmodul fortzusetzen, klicken Sie auf **Restore Configuration** (Konfiguration wiederherstellen). Die Aktualisierung der Firmware auf dem Managementmodul kann in einer Statusanzeige verfolgt werden. In einem Bestätigungsfenster wird angegeben, ob die Aktualisierung erfolgreich war.

Anmerkung: Die Sicherheitseinstellungen auf der Seite "Security" (Sicherheit) werden bei der Wiederherstellungsoperation nicht wiederhergestellt. Informationen zum Ändern von Sicherheitseinstellungen finden Sie im Abschnitt „Sicherer Web-Server und sichere LDAP-Verbindung" auf Seite 52.

3. Nachdem Sie eine Bestätigung erhalten haben, dass der Wiederherstellungsprozess abgeschlossen wurde, klicken Sie im Navigationsfenster auf **MM Control → Restart MM** (MM-Steuerung → MM-Neustart). Klicken Sie anschließend auf **Restart** (Neustart).
4. Klicken Sie auf **OK** (OK), um zu bestätigen, dass Sie das Managementmodul erneut starten möchten.
5. Klicken Sie auf **OK** (OK), um das Browserfenster zu schließen.
6. Um sich erneut am Managementmodul anzumelden, starten Sie den Browser und führen Sie den Anmeldeprozess durch.

Konfiguration eines erweiterten Managementmoduls wiederherstellen:

Sie können eine gespeicherte Konfiguration für ein erweitertes Managementmodul wiederherstellen.

Gehen Sie wie folgt vor, um Ihre aktuelle Konfiguration wiederherzustellen oder zu ändern. Sie können die Konfiguration eines erweiterten Managementmoduls nur wiederherstellen, wenn die Konfiguration zuvor auf der BladeCenter-Einheit oder auf einem externen Datenträger gespeichert wurde, wie im Abschnitt „Konfiguration eines erweiterten Managementmoduls sichern" auf Seite 75 beschrieben.

1. Melden Sie sich an dem Managementmodul an, dessen Konfiguration Sie wiederherstellen möchten. Weitere Informationen hierzu finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **MM Control → Configuration Mgmt** (MM-Steuerung → Konfigurationsverwaltung).
3. Wählen Sie die Art der Wiederherstellung aus, die Sie durchführen möchten: **Restore Defaults** (Standardwerte wiederherstellen), **Restore Configuration from File** (Konfiguration aus Datei wiederherstellen) oder **Restore Configuration from Chassis** (Konfiguration aus Gehäuse wiederherstellen).
   a. Zum Wiederherstellen der Standardkonfiguration klicken Sie auf eine der folgenden Optionen:
      - **Restore Defaults** (Standardwerte wiederherstellen): Die werkseitigen Voreinstellungen für das Managementmodul werden wiederhergestellt.
      - **Restore Defaults Preserve Logs** (Standardwerte wiederherstellen, Protokolle erhalten): Die werkseitigen Voreinstellungen für das Managementmodul werden wiederhergestellt, aber der Inhalt des Ereignisprotokolls des Managementmoduls bleibt erhalten.

      Die Aktualisierung der Firmware auf dem Managementmodul kann in einer Statusanzeige verfolgt werden. In einem Bestätigungsfenster wird angegeben, ob die Aktualisierung erfolgreich war.
   b. Wenn Sie die Konfiguration aus einer Datei wiederherstellen, klicken Sie im Abschnitt **Restore Configuration from File** (Konfiguration aus Datei wiederherstellen) auf **Browse** (Durchsuchen) und gehen Sie wie folgt vor.

      Anmerkung: Wenn die Konfigurationsdatei von einer BladeCenter-Einheit mit aktivierter Datenverschlüsselung gespeichert wurde, müssen Sie dasselbe Kennwort eingeben, das auch zum Speichern der Datei verwendet wurde.

      1) Klicken Sie auf die gewünschte Konfigurationsdatei und dann auf **Open** (Öffnen). Die Datei wird (einschließlich des vollständigen Pfads) im Feld neben **Browse** (Durchsuchen) angezeigt.
      2) Um die Konfigurationsdatei zu ändern, bevor sie wiederhergestellt wird, klicken Sie auf **Modify and Restore** (Ändern und wiederherstellen). Dadurch wird ein Fester mit einer bearbeitbaren Konfigurationszusammenfassung geöffnet. Zu Beginn werden nur die Felder angezeigt, die Sie ändern können. Um zwischen dieser Ansicht und der vollständigen Ansicht der Konfigurationszusammenfassung zu wechseln, klicken Sie oben oder unten im Fenster auf **Toggle View** (Ansicht umschalten).
      3) Zum Wiederherstellen dieser Datei für das Managementmodul klicken Sie auf **Restore Configuration** (Konfiguration wiederherstellen). Die Aktualisierung des Managementmoduls kann in einer Statusanzeige verfolgt werden. In einem Bestätigungsfenster wird angegeben, ob die Aktualisierung erfolgreich war.

         Anmerkung: Die Sicherheitseinstellungen auf der Seite "Security" (Sicherheit) werden bei der Wiederherstellungsoperation nicht wiederher-

gestellt. Informationen zum Ändern von Sicherheitseinstellungen finden Sie im Abschnitt „Sicherer Web-Server und sichere LDAP-Verbindung" auf Seite 52.

Die Aktualisierung der Firmware auf dem Managementmodul kann in einer Statusanzeige verfolgt werden. In einem Bestätigungsfenster wird angegeben, ob die Aktualisierung erfolgreich war.

c. Zum Wiederherstellen der Konfiguration aus der BladeCenter-Einheit klicken Sie auf **Restore** (Wiederherstellen) und dann auf **OK** (OK). Die Aktualisierung des Managementmoduls kann in einer Statusanzeige verfolgt werden. In einem Bestätigungsfenster wird angegeben, ob die Aktualisierung erfolgreich war.

4. Nachdem Sie eine Bestätigung erhalten haben, dass der Wiederherstellungsprozess abgeschlossen wurde, klicken Sie im Navigationsfenster auf **MM Control → Restart MM** (MM-Steuerung → MM-Neustart). Klicken Sie anschließend auf **Restart** (Neustart).
5. Klicken Sie auf **OK** (OK), um zu bestätigen, dass Sie das Managementmodul erneut starten möchten.
6. Klicken Sie auf **OK** (OK), um das Browserfenster zu schließen.
7. Um sich erneut am Managementmodul anzumelden, starten Sie den Browser und führen Sie den Anmeldeprozess durch.

Funktion für ferne Konsole verwenden

Das Managementmodul unterstützt die Fernsteuerung von Blade-Servern, als ob diese von der lokalen Konsole aus gesteuert werden.

Mit der fernen Konsole können Sie über Fernzugriff auf die Bildschirmkonsole eines Blade-Servers zugreifen, einschließlich Tastatur- und Maussteuerung. Dazu verwenden Sie ein Fenster einer eigenständigen Java-Anwendung, das geöffnet wird, wenn Sie auf der Seite **Blade Tasks → Remote Control** (Blade-Tasks → Fernsteuerung) auf **Start Remote Control** (Fernsteuerung starten) klicken. Dieses separate Browserfenster enthält sowohl die Fernsteuerungsfunktion als auch die Funktion für ferne Datenträger (Informationen hierzu finden Sie im Abschnitt „Funktion für ferne Datenträger verwenden" auf Seite 81).

Während einer Sitzung an einer fernen Konsole können die Tastatur, der Bildschirm und die Maus, die in einer BladeCenter-Einheit gemeinsam genutzt werden, immer nur jeweils einem Blade-Server zugeordnet werden. Mit der fernen Konsole können Sie dynamisch auswählen, welcher Blade-Server die gemeinsam genutzten Ressourcen der BladeCenter-Einheit steuert, darunter Laufwerkschlitten, ferner Datenträger und Tastatur/Bildschirm/Maus (die Optionen hängen vom Typ Ihrer BladeCenter-Einheit ab). Sitzungen an der fernen Konsole werden beendet, indem das Fenster der fernen Konsole geschlossen wird.

Bei der fernen Konsole handelt es sich um ein Java-2-Applet, das das Plug-in für Java Runtime Environment (JRE) erfordert. Wenn das JRE-Plug-in nicht installiert ist und Sie mit dem Internet verbunden sind, werden Sie aufgefordert, das Plug-in zu installieren. Andernfalls müssen Sie das JRE-Plug-in anfordern und installieren, bevor Sie die ferne Konsole verwenden können.

Die ferne Konsole wird von JRE Version 6.0, Update 10 oder höher unterstützt.

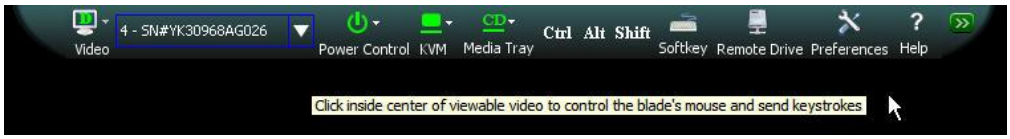
Die ferne Konsole unterstützt die folgenden Standard-VESA-Bildschirmmodi:

- 640 x 480 - 60 Hz, 72 Hz, 75 Hz, 85 Hz

- 800 x 600 - 60 Hz, 72 Hz, 75 Hz, 85 Hz
- 1024 x 768 - 60 Hz, 70 Hz, 75 Hz

Alle Standard-DOS-VGA-Modi werden unterstützt.

Das Betriebssystem Ihres fernen Konsolsystems fängt bestimmte Tastenkombinationen ab, wie z. B. "Strg + Alt + Entf" in Microsoft Windows, anstatt sie an den Blade-Server zu übertragen. Sie können diese abgefangenen Tastenkombinationen übertragen, indem Sie die Symbolleiste oben im Fenster der fernen Konsole verwenden.



Funktion für ferne Datenträger verwenden

Das Managementmodul kann ferne Massenspeichereinheiten verwenden.

Über das Fenster "Remote Control" (Fernsteuerung) (Informationen dazu finden Sie im Abschnitt „Remote Control (Fernsteuerung)" auf Seite 142) können Sie ein optisches Laufwerk, Diskettenlaufwerk oder USB-Laufwerk, das sich auf dem fernen Client-Computer befindet, an einen Blade-Server anhängen oder es diesem zuweisen. Mit diesem Fenster können Sie auch ein Datenträgerimage oder CD-(ISO-)Image auf dem fernen System angeben, das der Blade-Server verwenden soll, oder Sie können Dateien in den lokalen Speicher eines erweiterten Managementmoduls hochladen.

Sie können den fernen Datenträger für verschiedene Funktionen verwenden, z. B. zum Aktualisieren der Blade-Server-Firmware, zum Installieren neuer Software auf dem Blade-Server und zum Installieren oder Aktualisieren des Betriebssystems auf dem Blade-Server. Nachdem Sie den fernen Datenträger zugewiesen haben, können Sie mit der Funktion der fernen Konsole darauf zugreifen. Der ferne Datenträger wird als USB-Laufwerk auf dem Blade-Server angezeigt.

Ihr Betriebssystem muss USB unterstützen, damit Sie die Funktion für ferne Datenträger verwenden können. Im Folgenden sind die Mindestversionen der Serverbetriebssysteme mit USB-Unterstützung aufgelistet. :

- Microsoft Windows Server 2003
- Microsoft Windows 2000 mit Service-Pack 4
- Red Hat Enterprise Linux Version 3, Update 8
- SUSE Enterprise Linux Version 9
- VMware Version 3.0.1

Außerdem müssen Microsoft Windows 2000 oder höher und das Plug-in für Java Virtual Machine (JVM) Version 6.0, Update 10 oder höher auf dem (fernen) Clientsystem installiert sein. Zudem muss das Clientsystem über einen Mikroprozessor vom Typ Intel Pentium III oder höher mit 700 MHz oder mehr (oder über einen funktional entsprechenden Mikroprozessor) verfügen. Mithilfe der Fernsteuerung können maximal 15 ferne Datenträger angehängt werden. Dazu zählen USB-Einheiten, die an das erweiterte Managementmodul angeschlossen sind, sowie alle von anderen Benutzern angehängten Datenträger.

Datenträgerlaufwerk oder -image anhängen

Sie können mithilfe des Managementmoduls ein Datenträgerlaufwerk oder -image auf einem fernen System an einen Blade-Server anhängen.

Gehen Sie wie folgt vor, um ein Datenträgerlaufwerk oder -image auf einem fernen System an einen Blade-Server anzuhängen:

1. Starten Sie die Webschnittstelle des Managementmoduls (Informationen hierzu finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13).
2. Klicken Sie im Navigationsfenster auf **Blade Tasks → Remote Control** (Blade-Tasks → Fernsteuerung).
3. Klicken Sie im Abschnitt **Start Remote Control** (Fernsteuerung starten) auf **Start Remote Control** (Fernsteuerung starten).

   Anmerkung: USB-Memory-Key-Images weisen das Dateisuffix `.uki` auf. Verwenden Sie zum Erstellen einer Imagedatei für ein USB-Flash-Key-Laufwerk ein Binärkopiertool und stellen Sie sicher, dass die Imagedatei das Dateisuffix `.uki` aufweist.
4. Wählen Sie im Abschnitt **Remote Disk** (Ferner Datenträger) den Blade-Server aus, dem die Steuerung des Laufwerkschlittens zugeordnet wird.
5. Wählen Sie im Abschnitt **Remote Disk** (Ferner Datenträger) die Ressourcen für das Anhängen auf der linken Seite der Auswahl für ferne Datenträgerlaufwerke (unter **Available Resources** (Verfügbare Ressourcen)) aus. Klicken Sie anschließend auf **>>**, um die Auswahl zu beenden und die Ressourcen auf die rechte Seite der Auswahl für ferne Datenträgerlaufwerke (unter **Selected Resources** (Ausgewählte Ressourcen)) zu verschieben. Zum Abwählen von Elementen wählen Sie diese auf der rechten Seite der Auswahl für ferne Datenträgerlaufwerke aus und klicken dann auf **<<**.

   Sie können ein kleines Datenträgerimage direkt in den Flashspeicher des erweiterten Managementmoduls (permanent) hochladen, indem Sie in der Liste **Available Resources** (Verfügbare Ressourcen) die Option **Upload image to AMM** (Image auf erweitertes Managementmodul hochladen) auswählen. Der Speicher des erweiterten Managementmoduls wird auch von anderen Managementmodulfunktionen verwendet, sodass der verfügbare Speicherplatz variieren kann.

   Wenn Sie das Image im Managementmodul speichern, kann das Image an den Blade-Server angehängt bleiben, sodass Sie auch nach Beendigung der Webschnittstellensitzung darauf zugreifen können. Angehängte Laufwerke, die nicht im Managementmodul gespeichert sind, werden beim Schließen des Fernsteuerungsfensters abgehängt.
6. Klicken Sie auf **Write Protect** (Schreibschutz), damit keine Daten auf die angehängten Laufwerke geschrieben werden können.
7. Wählen Sie in der Auswahl für ferne Datenträgerlaufwerke (unter **Selected Resources** (Ausgewählte Ressourcen)) mindestens ein Laufwerk oder Image zum Anhängen aus. Klicken Sie anschließend auf **Mount Drive** (Laufwerk anhängen). Bei einem erweiterten Managementmodul, das die Funktion für gleichzeitige KVM-Nutzung (cKVM - concurrent KVM) verwendet, können Sie den herkömmlichen Betrieb (Funktion "Chassis Media Tray Owner" (Eigentümer für Gehäuselaufwerkschlitten)) auswählen oder in der Liste **Mount remote media to** (Fernen Datenträger anhängen an) einen der Blade-Server mit gleichzeitiger KVM-Nutzung auswählen. Das angehängte Laufwerk oder Datenträgerimage funktioniert wie eine an den Blade-Server angeschlossene USB-Einheit.

Datenträgerlaufwerk oder Datenträgerimage abhängen

Sie können mithilfe des Managementmoduls ein Datenträgerlaufwerk oder Datenträgerimage von einem Blade-Server abhängen.

Wenn Sie ein Laufwerk oder Datenträgerimage nicht mehr verwenden, gehen Sie wie folgt vor, um das Laufwerk oder Datenträgerimage zu beenden und abzuhängen:

1. Führen Sie alle Prozeduren durch, die bei Ihrem Betriebssystem erforderlich sind, um ein fernes Laufwerk oder Image zu beenden und abzuhängen. Informationen und Anweisungen hierzu finden Sie in der Dokumentation zu Ihrem Betriebssystem. Führen Sie beim Microsoft Windows-Betriebssystem eine der folgenden Prozeduren aus, um ein Laufwerk oder Datenträgerimage zu beenden und abzuhängen:
   - Wenn in der Windows-Taskleiste ein Symbol für das Entfernen oder Auswerfen von Hardware angezeigt wird, gehen Sie wie folgt vor:
     a. Klicken Sie doppelt auf das Symbol für das Entfernen oder Auswerfen von Hardware.
     b. Wählen Sie **USB Mass Storage Device** (USB-Massenspeichergerät) aus und klicken Sie auf **Stop** (Beenden).
     c. Klicken Sie auf **Close** (Schließen).
   - Wenn in der Windows-Taskleiste kein Symbol für das Entfernen oder Auswerfen von Hardware angezeigt wird, gehen Sie wie folgt vor:
     a. Klicken Sie in der Microsoft Windows-Systemsteuerung auf **Add/Remove Hardware** (Hardware hinzufügen/entfernen) und anschließend auf **Next** (Weiter).
     b. Wählen Sie **Uninstall/Unplug a device** (Gerät deinstallieren/entfernen) aus und klicken Sie anschließend auf **Next** (Weiter).
     c. Klicken Sie auf **Unplug/Eject a device** (Gerät entfernen/auswerfen) und anschließend auf **Next** (Weiter).
2. Klicken Sie im Fenster "Remote Control" (Fernsteuerung) der Webschnittstelle des Managementmoduls im Abschnitt **Remote Disk** (Ferner Datenträger) auf **Unmount Drive** (Laufwerk abhängen).

Automatische Erkennung des Verwaltungskanals verwenden

Sie können die automatische Erkennung des Verwaltungskanals (Management Channel Auto-Discovery - MCAD) verwenden, um die Datenübertragungen der BladeCenter-Verwaltungskanäle für MCAD-fähige Blade-Server weiterzuleiten.

Anmerkung: Die Funktion zur automatischen Erkennung des Verwaltungskanals ist standardmäßig inaktiviert. Informationen zum Aktivieren dieser Funktion finden Sie im Abschnitt „Automatische Erkennung des Verwaltungskanals aktivieren" auf Seite 84.

Durch die automatische Erkennung des Verwaltungskanals (Management Channel Auto-Discovery - MCAD) kann ein Blade-Server einen Übertragungskanal auswählen, der für den Verwaltungsdatenverkehr in der BladeCenter-Einheit verwendet wird, und der Blade-Server kann einen alternativen Kanal bestimmen, falls der aktuelle Kanal nicht mehr verfügbar ist. Der Blade-Server kann die Standard-Netzschnittstellenkarte auf seiner Systemplatine, eine andere Netzschnittstellenkarte auf der Systemplatine oder einen Port oder eine Erweiterungskarte als Pfad für den Verwaltungsdatenverkehr auswählen. Die Vorgänge zur automatischen Erkennung des Verwaltungskanals auf dem Blade-Server werden vom Bladesystem-Manage-

mentprozessor (BSMP) oder von einem MCAD-fähigen Serviceprozessor gesteuert. Der mithilfe von MCAD weitergeleitete Verwaltungsdatenverkehr umfasst die folgenden Datenübertragungen:

- SOL (Serial over LAN)
- cKVM (concurrent KVM - gleichzeitige KVM-Nutzung)
- FTP/TFTP
- Telnet
- BSMP-Servicedaten und -Image-Flashing
- Internes Gehäusenetz (Chassis Internal Network - CIN)
- Andere IP-Datenübertragungen zwischen dem erweiterten Managementmodul und dem Blade-Server, die über das interne BladeCenter-Verwaltungsnetz stattfinden

Beim MCAD-Betrieb bestimmt der Blade-Server, wann der nächstbeste Übertragungskanal für den Verwaltungsdatenverkehr ausgewählt werden kann, und sendet diese Information an das erweiterte Managementmodul.

Das erweiterte Managementmodul berechnet eine Liste der Übertragungskanalkandidaten. Diese Liste basiert auf den verfügbaren Kanälen auf dem Blade-Server, die der BSMP oder Serviceprozessor gemeldet hat (abhängig von der im Blade-Server installierten Hardware), und auf den in der BladeCenter-Einheit installierten E/A-Modulen. Das erweiterte Managementmodul gruppiert und priorisiert alle Ports in der Kandidatenliste anhand der Übertragungsgeschwindigkeit und sendet die Liste an den Blade-Server zurück.

Der Blade-Server bestimmt aufgrund der aktuellen Bedingungen des Verwaltungsdatenverkehrs, wann der nächstbeste Kanal ausgewählt wird und welcher Kanal ausgewählt wird. Das erweiterte Managementmodul reagiert auf Verwaltungspakete, die es vom Blade-Server empfängt, und leitet den Verwaltungsdatenverkehr an den neuen Netzpfad.

Das erweiterte Managementmodul meldet, welches E/A-Modul derzeit von den einzelnen Blade-Servern für den Verwaltungsdatenverkehr verwendet wird, und es meldet den Status des Pfades für den Verwaltungsdatenverkehr. In BladeCenter-Einheiten, die Blade-Server ohne MCAD-Unterstützung enthalten, werden die betreffenden Blades automatisch erkannt und der Verwaltungsdatenverkehr dieser Blades wird mit der Standardmethode ohne MCAD weitergeleitet.

Automatische Erkennung des Verwaltungskanals aktivieren

In diesem Abschnitt wird beschrieben, wie die automatische Erkennung des Verwaltungskanals (Management Channel Auto-Discovery, MCAD) aktiviert bzw. inaktiviert wird.

Auf der Blade-Konfigurationsseite (siehe „Configuration (Konfiguration)" auf Seite 149) können Sie MCAD aktivieren oder inaktivieren. In der Standardeinstellung ist die MCAD-Funktion inaktiviert.

Anmerkung: Die Aktivierung von MCAD ist nur bei MCAD-fähigen Blade-Servern verfügbar.

Gehen Sie wie folgt vor, um MCAD zu aktivieren oder zu inaktivieren:

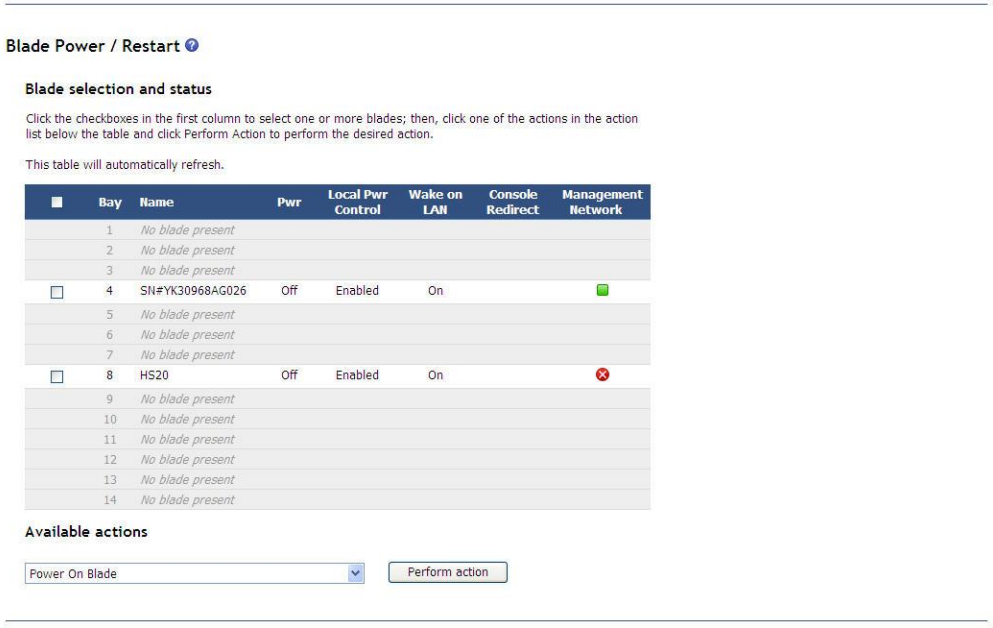
1. Klicken Sie im Navigationsfenster auf **Blade Tasks → Configuration** (Blade-Tasks → Konfiguration).
2. Wählen Sie die Registerkarte **Management Network** (Verwaltungsnetz) aus. Eine ähnliche Seite wie in der folgenden Abbildung wird angezeigt.

3. Wählen Sie im Feld **Enable management network auto-discovery** (Automatische Erkennung des Verwaltungsnetzes aktivieren) die Option **Enabled** (Aktiviert) oder **Disabled** (Inaktiviert) aus, um anzugeben, ob der Übertragungskanal für Verwaltungsdaten vom iBMC (Baseboard-Management-Controller) des Blade-Servers gesteuert werden soll.

Status der automatischen Erkennung des Verwaltungskanals anzeigen

Sie können den Status der automatischen Erkennung des Verwaltungskanals (Management Channel Auto-Discovery, MCAD) für sämtliche Blade-Server anzeigen.

Klicken Sie auf **Blade Tasks → Blade Power / Restart** (Blade-Tasks → Blade Einschalten/Neustart), um den Status der Verwaltungsnetzverbindung für den Blade-Server anzuzeigen.



Der Verwaltungsnetzstatus wird in der Spalte **Management Network** (Verwaltungsnetz) angezeigt und verfügt über die folgenden Status:

- - Dieses Symbol zeigt an, dass der Verwaltungspfad zwischen dem Blade-Server und dem erweiterten Managementmodul betriebsbereit ist.
- - Dieses Symbol zeigt an, dass der Verwaltungspfad zwischen dem Blade-Server und dem erweiterten Managementmodul nicht betriebsbereit ist.

- Wenn kein Symbol angezeigt wird, bedeutet dies, dass der Blade-Server die Anzeige von detaillierten Statusinformationen zum Verwaltungsnetz nicht unterstützt.

Klicken Sie auf ein Symbol zum Verwaltungsnetzstatus, um die detaillierten Statusinformationen zum Verwaltungsnetz für einen Blade-Server anzuzeigen, ähnlich den Informationen, die in der folgenden Abbildung dargestellt sind.

IBM Service Advisor

BladeCenter Service Advisor kann automatisch Hardware-Serviceinformationen an IBM senden.

Anmerkung: Service Advisor kann täglich rund um die Uhr Alerts senden, Ihr Service-Provider wird jedoch entsprechend der mit Ihnen getroffenen Vereinbarungen antworten. Bei Fragen wenden Sie sich bitte an Ihren Service-Provider.

Die folgenden Abschnitte enthalten Anweisungen zum Konfigurieren, Testen und Warten von Service Advisor.

- „Service Advisor konfigurieren" auf Seite 87
- „Service Advisor verwenden" auf Seite 90
- „Verbindungssicherheit für Service Advisor" auf Seite 92

Ausführliche Beschreibungen der Service Advisor-Webschnittstelle finden Sie in Kapitel 3, „Service Advisor" auf Seite 214.

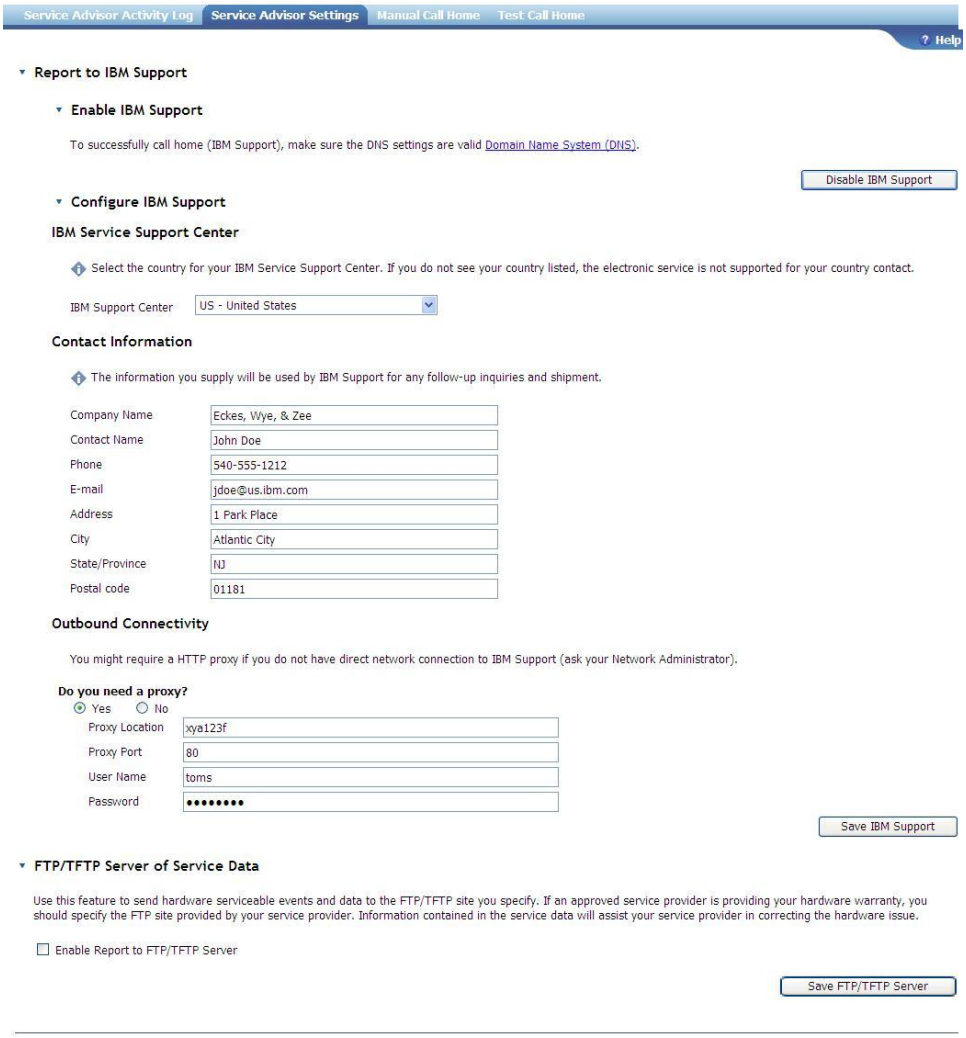
Service Advisor konfigurieren

Sie können den BladeCenter Service Advisor so konfigurieren, dass er Wartungsinformationen zu Hardware und Firmware automatisch an IBM sendet.

Gehen Sie wie folgt vor, um den BladeCenter Service Advisor zu konfigurieren:

1. Melden Sie sich an dem Managementmodul an, auf dem Sie den Service Advisor aktivieren möchten. Weitere Informationen hierzu finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Service Tools → Service Advisor** (Service-Tools → Service Advisor). Wenn Sie diese Option zum ersten Mal auswählen oder wenn die Firmware des Managementmoduls auf die Standardwerte zurückgesetzt wurde, müssen Sie die Lizenzvereinbarung anzeigen und akzeptieren.
   a. Klicken Sie auf **View terms and conditions** (Bedingungen anzeigen), um die Service Advisor-Vereinbarung anzuzeigen.
   b. Klicken Sie auf der Seite mit den Bedingungen auf **I accept the agreement** (Ich akzeptiere die Vereinbarung), um die Seite zu schließen.

   Anmerkungen:
   - Die Call-Home-Funktion ist standardmäßig inaktiviert und stellt nur eine Verbindung zur IBM Unterstützung her, wenn sie aktiviert wurde.
   - Die Call-Home-Funktion überträgt Daten, die das Inventar und den Status der BladeCenter-Einheit enthalten. Informationen zum Herunterladen dieser Daten in eine lokale Datei finden Sie im Abschnitt „AMM Service Data (Servicedaten des erweiterten Managementmoduls)" auf Seite 208.
   - Die Servicedaten in einem Bericht der Call-Home-Funktion werden für Fehlerbehebungszwecke verwendet. Dabei gelten die Bedingungen, die vor dem Aktivieren von Service Advisor akzeptiert wurden. Der Link **View Terms and Conditions** (Bedingungen anzeigen) befindet sich auf der Hauptseite von **Service Advisor**.
   - Die Informationen im Bericht der Call-Home-Funktion enthalten keine Kundendaten von den Servern oder E/A-Modulen.
3. Klicken Sie auf die Registerkarte **Service Advisor Settings** (Service Advisor-Einstellungen), um die Kontaktinformationen zu definieren. Es wird eine Seite angezeigt, die ähnlich wie in der folgenden Abbildung aussieht. Die Felder in dieser Abbildung enthalten Mustereinträge.



4. Klicken Sie auf **Enable IBM Support** (IBM Unterstützung aktivieren). Nun werden auf der Seite "Service Advisor Activity Log" (Service Advisor-Aktivitätenprotokoll) zwei zusätzliche Registerkarten angezeigt: **Manual Call Home** (Manuelle Call-Home-Funktion) und **Test Call Home** (Call-Home-Funktion testen).
5. Klicken Sie auf die Registerkarte **Service Advisor Settings** (Service Advisor-Einstellungen) und füllen Sie die Felder mit den Kontaktinformationen aus.

   IBM Service Support Center (IBM Service Support Center)
   Wählen Sie in dieser Dropdown-Liste das Land für Ihr IBM Service Support Center aus. Ist Ihr Land nicht in der Liste aufgeführt, wird der elektronische Service für Ihr Land nicht unterstützt.

   Company Name (Name des Unternehmens)
   Geben Sie in diesem Feld das Unternehmen an, in dem das Managementmodul verwendet wird. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

   Contact Name (Name des Ansprechpartners)
   Geben Sie in diesem Feld die Person an, die für das Managementmodul verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.

Phone (Telefon)
Geben Sie in diesem Feld die Telefonnummer des Ansprechpartners an.

E-mail (E-Mail)
Geben Sie in diesem Feld die E-Mail-Adresse der Person an, die für das Managementmodul verantwortlich ist.

Address (Adresse)
Geben Sie in diesem Feld die Straße und Hausnummer des Unternehmens an, in dem das Managementmodul verwendet wird.

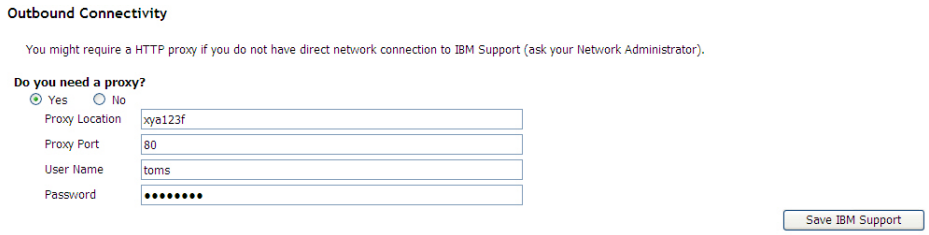
City (Ort)
Geben Sie in diesem Feld den Ort des Unternehmens an, in dem das Managementmodul verwendet wird.

State/Province (Bundesland)
Geben Sie in diesem Feld das Bundesland an, in dem sich das Managementmodul befindet. Dieses Feld ist auf maximal 30 Zeichen begrenzt.

Postal code (Postleitzahl)
Geben Sie in diesem Feld die Postleitzahl an.

Outbound connectivity (Ausgehende Verbindung)
Geben Sie in diesem Abschnitt mithilfe des Optionsfelds an, ob Sie einen Proxy verwenden müssen oder nicht.

6. Klicken Sie auf **Save** (Speichern). Die Seite für Service Advisor wird angezeigt.
7. Wenn Ihre BladeCenter-Einheit einen HTTP-Proxy verwenden muss, füllen Sie die Felder "Proxy Location" (Proxy-Standort), "Proxy Port" (Proxy-Port), "User Name" (Benutzername) und "Password" (Kennwort) aus.



Anmerkungen:

- Der Proxy-Server sorgt dafür, dass das erweiterte Managementmodul die Call-Home-Funktion auch hinter bestimmten Firewalls nutzen kann.
- Der Proxy-Server muss Verbindungen zu Port 443 und Port 80 unterstützen.
- Alle Datenübertragungen zur IBM Unterstützung erfolgen über TCP-Sockets, die vom erweiterten Managementmodul eingeleitet werden. Außerdem wird SSL bei allen Datenübertragungen verwendet, um die gesendeten und empfangenen Daten zu verschlüsseln.

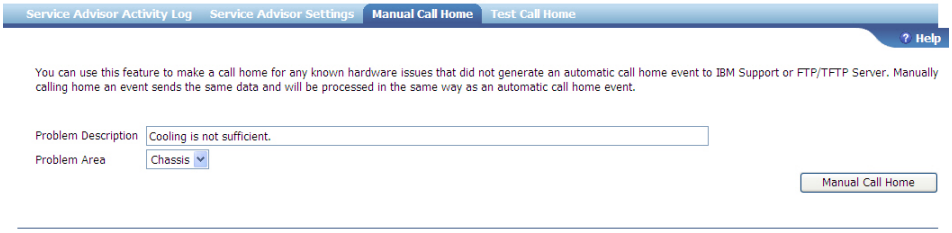
8. Wählen Sie **Enable Report to FTP/TFTP Server** (Bericht an FTP-/TFTP-Server aktivieren) aus, um wartungsfähige Hardware-Ereignisse und -Daten an die angegebene FTP-/TFTP-Site zu senden. Wenn diese Funktion aktiviert ist, füllen Sie die zusätzlichen Konfigurationsfelder aus, die nun angezeigt werden. Klicken Sie anschließend auf **Save FTP/TFTP Server** (FTP-/TFTP-Server speichern).

Service Advisor verwenden

Nach dem Konfigurieren des BladeCenter Service Advisor können Sie das Aktivitätenprotokoll anzeigen oder eine Testnachricht generieren.

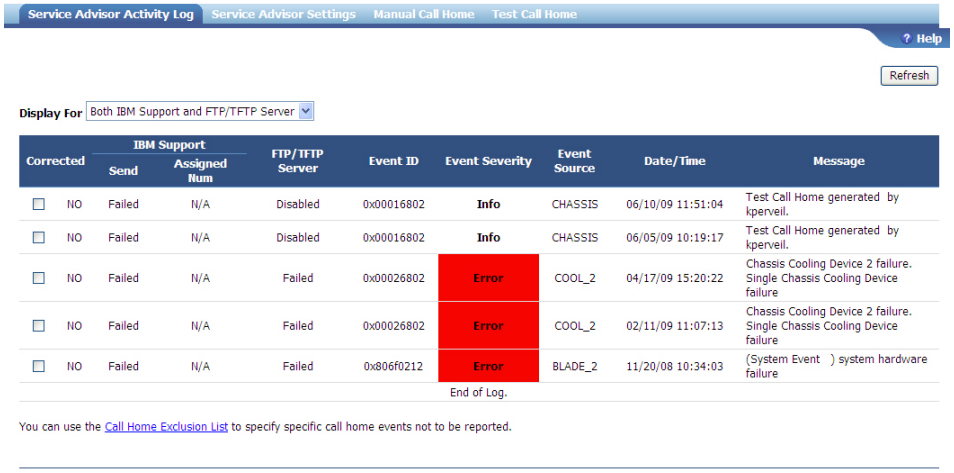
Gehen Sie wie folgt vor, um einen Hardwarefehlerbericht zu Ihrer BladeCenter-Einheit oder zu einem der darin installierten Blade-Server zu erstellen.

1. Melden Sie sich an dem Managementmodul an, auf dem Sie den Service Advisor aktivieren möchten. Weitere Informationen hierzu finden Sie im Abschnitt „Webschnittstelle des Managementmoduls starten" auf Seite 13.
2. Klicken Sie im Navigationsfenster auf **Service Tools → Service Advisor** (Service-Tools → Service Advisor).
3. Klicken Sie auf die Registerkarte **Manual Call Home** (Manuelle Call-Home-Funktion). Es wird eine Seite angezeigt, die ähnlich wie in der folgenden Abbildung aussieht.



4. Gehen Sie wie folgt vor.
   a. Wählen Sie den Problembereich in der Dropdown-Liste aus.
   b. Geben Sie die Fehlerbeschreibung ein.
   c. Klicken Sie auf **Manual Call Home** (Manuelle Call-Home-Funktion).

   Anmerkung: Wenn Sie Servicedaten per E-Mail senden möchten, verwenden Sie die Funktion **Manually Email Service Information** (Serviceinformationen manuell per E-Mail senden), die in den Verwaltungsoptionen des Ereignisprotokolls verfügbar ist. Siehe „Event Log (Ereignisprotokoll)" auf Seite 115.
5. Zum Generieren einer Testnachricht klicken Sie auf die Registerkarte **Test Call Home** (Call-Home-Funktion testen) und auf die Schaltfläche **Test Call Home** (Call-Home-Funktion testen). Durch das Testen der Call-Home-Funktion wird sichergestellt, dass Fehler vom erweiterten Managementmodul erfolgreich an IBM gesendet werden können. Wenn Sie auf **Test Call Home** (Call-Home-Funktion testen) klicken, wird das **Service Advisor-Aktivitätenprotokoll** aufgerufen. Klicken Sie im Aktivitätenprotokoll auf die Schaltfläche **Refresh** (Aktualisieren), bis in der Spalte mit dem Sendeergebnis im Aktivitätenprotokoll angegeben wird, ob das Senden erfolgreich war oder fehlgeschlagen ist. War das Senden erfolgreich, wird eine Servicenummer bzw. Ticketnummer zugewiesen. Das bei IBM geöffnete Ticket wird als Testticket gekennzeichnet. Für ein Testticket muss die IBM Unterstützung keine Aktion durchführen, sodass der Vorgang geschlossen wird. Wenn das Testen der Call-Home-Funktion fehlschlägt, finden Sie im Abschnitt „Verbindungssicherheit für Service Advisor" auf Seite 92 weitere Informationen.
6. Zum Anzeigen des Aktivitätenprotokolls klicken Sie auf die Registerkarte **Service Advisor Activity Log** (Service Advisor-Aktivitätenprotokoll).



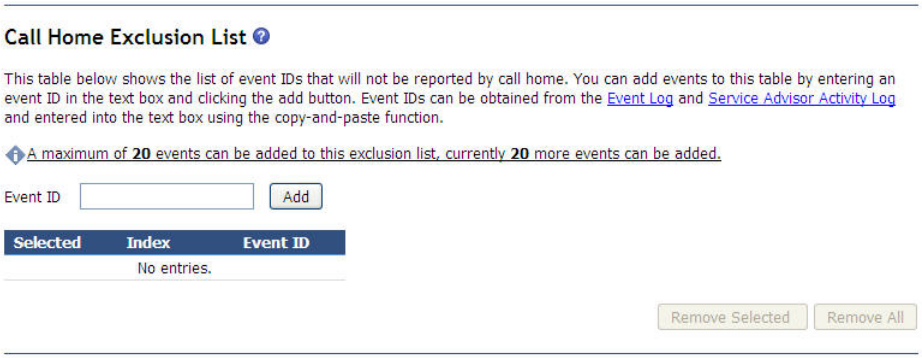
Anmerkung:

- Im Aktivitätenprotokoll werden die 5 neuesten Call-Home-Ereignisse angezeigt, darunter auch die Ereignisse, die sich auf Tests der Call-Home-Funktion und auf die manuelle Call-Home-Funktion beziehen.
- Das Sendeergebnis kann "Success" (Erfolgreich), "Pending" (Ausstehend) oder "Failed" (Fehlgeschlagen) lauten.
  - Success (Erfolgreich) - Die gesendeten Daten wurden erfolgreich bei IBM empfangen. Im Feld mit der zugewiesenen Servicenummer wird eine Problemticketnummer angezeigt.
  - Pending (Ausstehend) - Der Call-Home-Vorgang wird gerade ausgeführt.
  - Failed (Fehlgeschlagen) - Das Senden ist fehlgeschlagen. Wenn die Call-Home-Funktion fehlschlägt, wenden Sie sich an den zuständigen IBM Ansprechpartner, um das Hardware-Service-Ereignis zu melden. Fehlgeschlagene Call-Home-Ereignisse werden nicht erneut versucht.

7. Aktivieren Sie nach der Behebung jedes Ereignisses das Kontrollkästchen **Corrected** (Behoben), damit Sie noch nicht behobene Ereignisse schneller erkennen.

   Anmerkung: Wenn das Kontrollkästchen **Corrected** (Behoben) für ein Ereignis nicht aktiviert ist, wird ein Auftreten desselben Ereignisses erst wieder mit der Call-Home-Funktion gesendet, wenn seit dem ersten Auftreten des Ereignisses fünf Tage vergangen sind.
8. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die neuesten Informationen anzuzeigen. Die zugewiesene Servicenummer kann bei der Kommunikation mit IBM als Referenz für das Call-Home-Ereignis verwendet werden.

   Anmerkung: Informationen zum Herunterladen der Servicedaten, einschließlich des Serviceprotokolls, finden Sie im Abschnitt „AMM Service Data (Servicedaten des erweiterten Managementmoduls)” auf Seite 208.
9. Damit ein bestimmtes Ereignis nicht in den Bericht an IBM aufgenommen wird, klicken Sie auf den Link "Call Home Exclusion List" (Call-Home-Ausschlussliste).



Anmerkungen:

- Bevor Sie die Funktion der Call-Home-Ausschlussliste nutzen, wenden Sie sich an die IBM Unterstützung.
- Eine Liste der Call-Home-Nachrichten des Service Advisor finden Sie im *Nachrichtenhandbuch zum Service Advisor des erweiterten IBM BladeCenter-Managementmoduls*.

10. Geben Sie im Feld "Event ID" (Ereignis-ID) die hexadezimale Ereignis-ID ein.
11. Klicken Sie auf **Add** (Hinzufügen).

Verbindungssicherheit für Service Advisor

In diesem Abschnitt werden die Daten, die zwischen dem erweiterten Managementmodul und dem IBM Service Center übertragen werden, sowie die Methode für diese Datenübertragung beschrieben. Diese Beschreibung ist auf die Konfiguration und Verwendung der Call-Home-Funktion (Service Advisor) auf dem erweiterten Managementmodul für die automatische Fehlermeldung beschränkt.

Das erweiterte Managementmodul kann so konfiguriert werden, dass Serviceinformationsdaten an IBM zurückgesendet werden. Die Call-Home-Funktion ist standardmäßig inaktiviert. Service Advisor erfordert eine Reihe von Parametern und Kontaktinformationen, um die Call-Home-Funktion zu aktivieren.

Service Advisor stellt nur eine Verbindung zu IBM her, wenn die Meldung von Fehlern aktiviert wurde und ein Fehler aufgetreten ist. Die Daten werden in einer Servicedaten-Erfassungsdatei übertragen, die Inventar- und Statusinformationen enthält. Informationen zum Speichern und Anzeigen einer Servicedaten-Erfassungsdatei finden Sie im Abschnitt „AMM Service Data (Servicedaten des erweiterten Managementmoduls)” auf Seite 208.

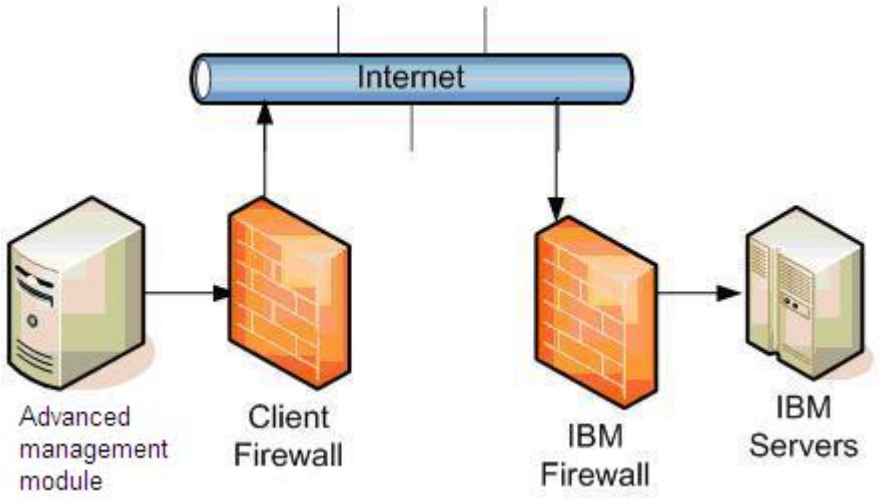
Bei der Servicedaten-Erfassungsdatei handelt es sich um eine Datei im Format "tgz" (gzip-komprimiertes tar-Archiv), die Sie mit gängigen Dienstprogrammen entpacken können. Die Kategorien der erfassten Daten sind immer dieselben, doch die folgenden Details zu den Daten können variieren:

- Firmwareversionen können sich ändern.
- Installierte Komponenten können sich ändern.
- Wenn die Protokolle voll sind, werden ältere Informationen durch neuere Ereignisse überschrieben.
- Das genaue Format und der genaue Inhalt der erfassten und gemeldeten Daten können sich ändern.

Anmerkung: Die an IBM gesendeten Informationen oder Debugdaten enthalten keine Kundendaten von den Blade-Servern oder E/A-Modulen.

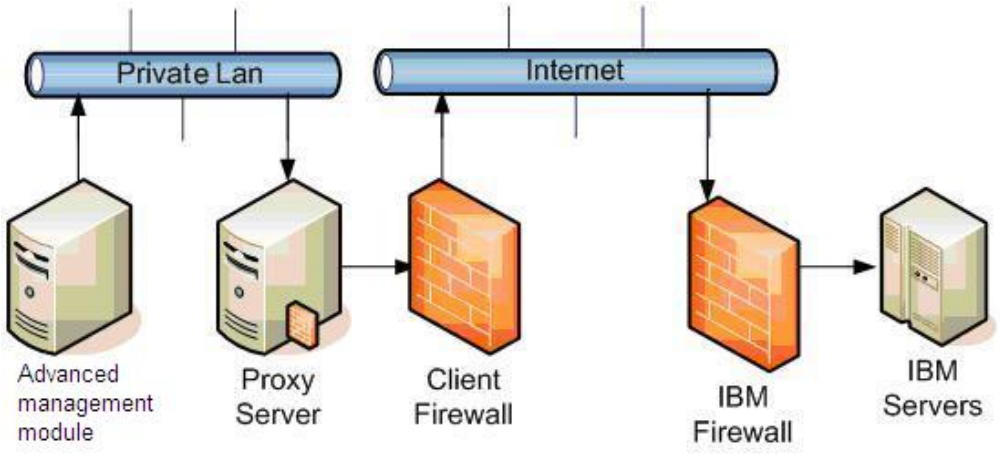
Wenn Service Advisor aktiviert ist, verwendet das erweiterte Managementmodul eine vom Kunden bereitgestellte Internetverbindung, um eine Verbindung zur IBM Unterstützung herzustellen. Alle Datenübertragungen erfolgen über TCP-Sockets, die immer vom erweiterten Managementmodul eingeleitet werden. Außerdem wird SSL bei allen Datenübertragungen verwendet, um die gesendeten und empfangenen Daten zu verschlüsseln. Das erweiterte Managementmodul kann so konfiguriert werden, dass es eine Internetverbindung über einen vom Kunden konfigurierten Proxy-Server herstellt.

Im folgenden Diagramm ist dargestellt, wie das erweiterte Managementmodul eine Verbindung zu IBM ohne Proxy-Server herstellt.



In dieser Konfiguration stellt das erweiterte Managementmodul eine Verbindung her, indem die Standardroute der vom Kunden bereitgestellten Internetverbindung verwendet wird. Für eine erfolgreiche Datenübertragung des erweiterten Managementmoduls muss Ihre externe Firewall so konfiguriert sein, dass etablierte TCP-Pakete ungehindert über Port 443 (HTTPS) übertragen werden dürfen.

Im folgenden Diagramm ist dargestellt, wie das erweiterte Managementmodul eine Verbindung zu IBM über einen Proxy-Server herstellt.



Zur Weiterleitung von SSL-Sockets muss der Proxy-Server die grundlegenden Proxy-Header-Funktionen (wie in RFC 2616 zum Hypertext Transfer Protocol 1.1 beschrieben; siehe http://www.ietf.org/rfc/rfc2616.txt) und die Verbindungsmethode unterstützen. Die grundlegende Proxy-Authentifizierung (RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication"; siehe http://www.ietf.org/rfc/rfc2617.txt) kann so konfiguriert werden, dass das erweiterte Managementmodul authentifiziert wird, bevor es versucht, Sockets über den Proxy-Server weiterzuleiten.

Für eine erfolgreiche Datenübertragung des erweiterten Managementmoduls muss der Proxy-Server des Kunden die Verbindungen zu Port 443 und Port 80 zulassen. Mithilfe des Proxy-Servers können auch die einzelnen IP-Adressen begrenzt werden, zu denen das erweiterte Managementmodul eine Verbindung herstellen darf.

Wenn das erweiterte Managementmodul mit aktiviertem Service Advisor einen Fehler bei sich selbst oder einer BladeCenter-Komponente erkennt, wird über die Call-Home-Funktion ein Fehlerbericht an IBM gesendet. Alle Informationen in diesem Bericht werden vorübergehend gespeichert. Nach beendeter Übertragung stellt das erweiterte Managementmodul keine Statusinformationen zum geöffneten Call-Home-Vorgang mehr bereit. Die IBM Unterstützung meldet sich bei Ihnen, um eine zusätzliche Fehlerbestimmung durchzuführen und eine Lösung zu ermitteln. Support Engineers, die aktiv an einem Fehler arbeiten, können die Daten für Fehlerbehebungszwecke auslagern und nach beendeter Arbeit löschen.

Wenn das erweiterte Managementmodul aktiviert ist, verwendet es einige oder alle der folgenden IPv4-IP-Adressen. Sowohl HTTP (Port 80) als auch HTTPS (Port 443) sind erforderlich.

Anmerkung: Änderungen dieser IP-Adressen sind vorbehalten.

- www6.software.ibm.com, 207.25.253.41
- www.ecurep.ibm.com, 192.109.81.20
- download2.boulder.ibm.com, 207.25.253.8
- download3.boulder.ibm.com, 207.25.253.76
- www-945.ibm.com, 129.42.26.224
- www-945.ibm.com, 129.42.34.224
- www-945.ibm.com, 129.42.42.224
- eccgw01.boulder.ibm.com, 207.25.252.197
- eccgw02.rochester.ibm.com, 129.42.160.51
- testcase.boulder.ibm.com, 207.25.253.31

Um die Verbindung des erweiterten Managementmoduls zu IBM zu überprüfen, rufen Sie in Ihrem Browser eine der oben aufgelisteten Adressen auf. Bei erfolgreicher Verbindungsherstellung wird eine IBM Webseite angezeigt. Beachten Sie, dass die mit "eccgw" beginnenden Adressen nicht durchsucht werden können.

E/A-Modul konfigurieren

Sie können ein BladeCenter-E/A-Modul mithilfe der Schnittstelle des Managementmoduls konfigurieren.

Anmerkung:

- Die Seiten zur Konfiguration des E/A-Moduls sind je nach Typ des E/A-Moduls unterschiedlich. Auf den einzelnen Seiten werden nur die Einstellungen angezeigt, die auf das installierte E/A-Modul angewendet werden. Aus diesem Grund gelten möglicherweise nicht alle im Folgenden beschriebenen Schritte für Ihr E/A-Modul.
- Die IPv6-Adressierung wird nicht von allen E/A-Modulen unterstützt.
- Die Webschnittstelle des E/A-Moduls wird nur von Microsoft Internet Explorer Version 8 oder höher und von Mozilla Firefox Version 1.07 oder höher unterstützt.

Der Großteil der E/A-Modulkonfiguration wird über die von den einzelnen E/A-Modulen bereitgestellte Managementschnittstelle durchgeführt. Bevor Sie über einen Web-Browser auf diese Managementumgebung zugreifen können, müssen die Kommunikationsparameter einiger E/A-Module über die Webschnittstelle oder über die Befehlszeilenschnittstelle des Managementmoduls festgelegt werden.

In diesem Abschnitt finden Sie Anweisungen zum Konfigurieren der Kommunikationsparameter des E/A-Moduls mithilfe der Webschnittstelle des Managementmoduls. Spezielle Konfigurationsinformationen finden Sie im *Installationshandbuch* zu Ihrem E/A-Modul. Anweisungen zum Konfigurieren des E/A-Moduls mithilfe der Befehlszeilenschnittstelle des Managementmoduls finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des BladeCenter-Managementmoduls*.

Gehen Sie wie folgt vor, um das E/A-Modul mithilfe der Webschnittstelle des Managementmoduls für die externe Kommunikation zu konfigurieren:

1. Melden Sie sich beim Managementmodul an, wie im Abschnitt „Verbindung zum Managementmodul herstellen” auf Seite 7 beschrieben. Das Managementmodul-Fenster wird geöffnet.
2. Klicken Sie im Menü **I/O Module Tasks** (E/A-Modul, Tasks) auf **Configuration** (Konfiguration).
3. Klicken Sie im Abschnitt **I/O Module Configuration** (Konfiguration des E/A-Moduls) auf die Positionsnummer, die der Position des zu konfigurierenden E/A-Moduls entspricht. Die entsprechende Positionsnummer wird unten im Fenster zusammen mit anderen Informationen zum E/A-Modul angezeigt, wie etwa der IP-Adresse. Die Informationen zum E/A-Modul sind in zwei Bereiche unterteilt: "Current IP Configuration" (Aktuelle IP-Konfiguration) und "New Static IP Configuration" (Neue statische IP-Konfiguration).
4. Geben Sie im Feld **IP address** (IP-Adresse) im Abschnitt **New Static IP Configuration** (Neue statische IP-Konfiguration) die neue IP-Adresse des E/A-Moduls ein. Klicken Sie dann auf **Save** (Speichern). Es gibt zwei Möglichkeiten, die IP-Adresse für das Gigabit Ethernet-Switchmodul zu konfigurieren:
   - IP-Standardadresse verwenden
   - Eine gültige eindeutige IP-Adresse vom Systemadministrator anfordern

   Anmerkung: Bei IPv4 muss sich die IP-Adresse des E/A-Moduls im gleichen Teilnetz wie das Managementmodul befinden. Das Managementmodul prüft nicht, ob die IP-Adresse gültig ist.

5. Klicken Sie auf **Advanced Management** (Erweiterte Verwaltung) und stellen Sie sicher, dass die folgenden Switchmodul-Funktionen aktiviert sind:
   - Externe Anschlüsse
   - Externe Verwaltung für alle Anschlüsse
   - Neue IP-Konfiguration bei allen Zurücksetzungen beibehalten

   Die Standardeinstellung für diese Funktionen ist **Disabled** (Inaktiviert). Wenn diese Funktionen nicht bereits aktiviert wurden, ändern Sie die Einstellung in **Enabled** (Aktiviert), und klicken Sie dann auf **Save** (Speichern).

   Anmerkung: Weitere Informationen zum Aktivieren der externen Verwaltung für alle Anschlüsse finden Sie im *Installations- und Benutzerhandbuch* zu Ihrer BladeCenter-Einheit.
6. Bei E/A-Modulen, die die NAT-Tabelle (Network Address Translation, Netzadressumsetzung) unterstützen, klicken Sie auf **Network Protocol Configuration** (Netzprotokollkonfiguration). Die erste Spalte der NAT-Tabelle enthält Links, die Sie zum Konfigurieren der Protokollwerte verwenden können. Die maximale Anzahl an Protokollen beträgt 10. Fünf Protokolle sind vordefiniert. Das erste Protokoll ist beispielsweise immer HTTP (Hypertext Transfer Protocol) und das zweite immer Telnet.

   Sie können die Netzprotokolleinstellungen auf dieser Seite der Schnittstelle des Managementmoduls aktivieren oder ändern, indem Sie auf eine der folgenden Schaltflächen klicken:
   - Um alle Werte in der NAT-Tabelle zu aktivieren, klicken Sie auf **Activate** (Aktivieren).
   - Um alle Werte in der NAT-Tabelle sofort auf die Standardwerte zurückzusetzen, klicken Sie auf **Reset to defaults** (Auf Standard zurücksetzen).

Sie können nun eine Webschnittstellen-, Telnet- oder SSH-Sitzung (Secure Shell) mit dem E/A-Modul starten, um weitere Konfigurationsschritte durchzuführen. Informationen hierzu finden Sie in der Dokumentation zu Ihrem E/A-Modul.

Unterstützung für NEBS-Modus

BladeCenter T- und BladeCenter HT-Einheiten unterstützen den NEBS-Modus (Network Equipment-Building System).

Wenn Sie eine BladeCenter T- oder BladeCenter HT-Einheit in einer NEBS-Umgebung (für die Telekommunikation) betreiben, müssen Sie den NEBS-Modus aktivieren. Rufen Sie dazu die Seite **Monitors → Power Management** (Monitore → Stromverbrauchssteuerung) auf und wählen Sie im Abschnitt **BladeCenter Chassis Configuration Setting** (Konfigurationseinstellung für BladeCenter-Gehäuse) das Kontrollkästchen **Network Equipment-Building System (NEBS) mode** (NEBS-Modus (Network Equipment-Building System)) aus (weitere Informationen finden Sie im Abschnitt „Power Management (Stromverbrauchssteuerung)" auf Seite 123).

In einer NEBS-Umgebung wird die Drehzahl der Lüfter in einer BladeCenter-Einheit nicht so schnell höher geschaltet, um auf potenzielle Wärmeereignisse zu reagieren, wie in einer Nicht-NEBS-Umgebung. Um den geräuscharmen Modus für die BladeCenter-Einheit zu aktivieren, durch den der Stromverbrauch des BladeServers so reduziert wird, dass ein bestimmter Geräuschpegel nicht überschritten wird, müssen Sie den NEBS-Modus inaktivieren.

Luftfilterverwaltung für BladeCenter HT- und BladeCenter T-Einheiten

Die BladeCenter HT- und BladeCenter T-Einheiten stellen Alarme und Erinnerungen zum Zustand des Luftfilters bereit.

Die Luftfilter in den BladeCenter HT- und BladeCenter T-Einheiten müssen regelmäßig gewechselt werden. Je nach Typ der BladeCenter-Einheit werden die Luftfilteralarme und -erinnerungen möglicherweise automatisch gelöscht.

Erkennung verschmutzter Filter

BladeCenter T- und BladeCenter HT-Einheiten warnen Sie, wenn der Luftfilter verschmutzt ist.

Das erweiterte Managementmodul generiert je nach dem Grad der Verschmutzung in der Anzeige der Frontblende einen Luftfilteralarm (geringfügig, schwerwiegend oder kritisch). Diese Alarmanzeigen können auf der Seite **Monitors → System Status** (Monitore → Systemstatus) sowie im Ereignisprotokoll des Managementmoduls angezeigt werden. (Weitere Informationen hierzu finden Sie in den Abschnitten „System Status (Systemstatus)" auf Seite 105 und „Event Log (Ereignisprotokoll)" auf Seite 115.)

Bei der BladeCenter HT-Einheit müssen Sie Luftfilteralarme nicht manuell verwalten, da der Filter in dieser BladeCenter-Einheit automatisch erkannt und die Erkennung verschmutzter Filter bei der Installation der Frontblende aktiviert wird. Wenn die Frontblende entfernt wird, wird die Erkennung verschmutzter Filter automatisch inaktiviert und es wird kein Alarm für verschmutzte Filter generiert. Der Alarm für verschmutzte Filter wird automatisch zurückgesetzt, wenn die Frontblende erneut an der BladeCenter HT-Einheit installiert wird.

Bei der BladeCenter T-Einheit müssen Sie die Konfigurationseinstellungen für verschmutzte Filter manuell verwalten, da diese Einheit nicht erkennen kann, wenn die Frontblende installiert oder entfernt wird. Die Erkennung verschmutzter Filter wird im Rahmen der Konfiguration von Erinnerungen für Luftfilter auf der Seite **MM Control → Alerts** (MM-Steuerung → Alarme) im Abschnitt **Passive Air Filter Reminder** (Erinnerung für Luftfilteraustausch) aktiviert, inaktiviert oder zurückgesetzt. (Weitere Informationen hierzu finden Sie im Abschnitt „Alerts" auf Seite 181.) Alarme für einen verschmutzten Filter müssen in den Abschnitten **Major Alarms** (Alarme für schwerwiegende Systemfehler) oder **Minor Alarms** (Alarme für geringfügige Systemfehler) der Seite **Monitors → System Status** (Monitore → Systemstatus) manuell gelöscht werden. (Weitere Informationen und Anweisungen finden Sie im Abschnitt „BladeCenter T- und BladeCenter HT-Alarmverwaltung" auf Seite 106.)

Erinnerung für Luftfilteraustausch

BladeCenter T- und BladeCenter HT-Einheiten erinnern Sie alle sechs Monate daran, den Luftfilter zu wechseln.

In einer BladeCenter T- oder BladeCenter HT-Einheit wird alle sechs Monate eine Serviceerinnerung zum Wechseln des Luftfilters generiert. Diese Erinnerungen werden als Informationsnachrichten im Ereignisprotokoll des Managementmoduls angezeigt. (Informationen zur Verwendung des Ereignisprotokolls finden Sie im Abschnitt „Event Log (Ereignisprotokoll)" auf Seite 115.)

Die BladeCenter HT-Einheit generiert automatisch ein Ereignis, um Sie daran zu erinnern, den Luftfilter zu wechseln, wenn sechs Monate verstrichen sind, seit das erweiterte Managementmodul erkannt hat, dass Sie die Frontblende entfernt und anschließend installiert haben. Die BladeCenter HT-Einheit erkennt und reagiert automatisch auf die folgenden Bedingungen im Zusammenhang mit der Luftfilterverwaltung:

Einsetzen
Die Zeitpläne für den sechsmonatigen Service und die Erkennung verschmutzter Filter beginnen, wenn die Frontblende in der BladeCenter HT-Einheit installiert wird.

Entfernen
Wenn die Frontblende von der BladeCenter HT-Einheit entfernt wurde, stehen keine Filterverwaltungsservices zur Verfügung.

Die BladeCenter T-Einheit stellt in der Benutzerschnittstelle des erweiterten Managementmoduls Steuerelemente bereit, mit deren Hilfe Sie das Serviceintervall zurücksetzen können, da diese BladeCenter-Einheit Aktivitäten an der Frontblende nicht erkennt. Sechs Monate nach dem Zurücksetzen des Serviceintervalls in der Benutzerschnittstelle des erweiterten Managementmoduls wird eine Erinnerung zum Wechseln des Luftfilters in der Frontblende angezeigt.

Die BladeCenter T-Einheit stellt die folgenden Optionen für die Luftfilterverwaltung im Abschnitt **Passive Air Filter Reminder** (Erinnerung für Luftfilteraustausch) der Seite **MM Control → Alerts** (MM-Steuerung → Alarme) bereit (weitere Informationen finden Sie im Abschnitt „Alerts" auf Seite 181):

- **Disable** (Inaktivieren): Services für die Luftfilterverwaltung werden inaktiviert (es werden keine Luftfilteralarme oder -ereignisse generiert).
- **Enable** (Aktivieren): Der Zeitplan für die Erinnerung an den Service nach sechs Monaten und die Erkennung verschmutzter Filter werden aktiviert.
- **Restart** (Neustart): Services für die Luftfilterverwaltung werden zurückgesetzt (der Zeitplan für die Erinnerung an den Service nach sechs Monaten wird so festgelegt, dass nach sechs Monaten eine Erinnerung für Luftfilter generiert wird).

Kapitel 3. Überblick über die Webschnittstelle des Managementmoduls

Die folgenden Abschnitte enthalten Informationen zu Struktur und Inhalt der Webschnittstelle des Managementmoduls für alle Typen von Managementmodulen:

- Funktionen der Webschnittstelle des Managementmoduls, auf die Benutzer abhängig von ihren zugewiesenen Rollen oder Berechtigungsstufen zugreifen können (siehe Abschnitt „Webschnittstellenseiten und Benutzerrollen" auf Seite 100)
- Beschreibungen der Seiten der Webschnittstelle des Managementmoduls (siehe Abschnitt „Optionen der Webschnittstelle des Managementmoduls" auf Seite 105)

In Kapitel 2, „Webschnittstelle des Managementmoduls verwenden", auf Seite 7 finden Sie Informationen zur Verwendung der Webschnittstelle des Managementmoduls, um ausgewählte Funktionen durchzuführen.

Die webbasierte Benutzerschnittstelle kommuniziert mit dem Verwaltungs- und Konfigurationsprogramm der Firmware, die mit dem Managementmodul geliefert wird. Mit diesem Programm können Sie die folgenden Tasks ausführen:

- Anmelde-IDs und Anmeldekennwörter definieren.
- Sicherheitseinstellungen konfigurieren, wie z. B. Datenverschlüsselung und Benutzerkontosicherheit.
- Empfänger von Alertbenachrichtigungen für bestimmte Ereignisse auswählen.
- Den Status der BladeCenter-Einheit, Blade-Server und anderen BladeCenter-Komponenten überwachen.
- Andere BladeCenter-Einheiten im Netz ermitteln und den Zugriff auf diese Einheiten über die Webschnittstelle ihrer Managementmodule ermöglichen.
- Die BladeCenter-Einheit, Blade-Server und anderen BladeCenter-Komponenten steuern.
- Auf die E/A-Module zugreifen, um sie zu konfigurieren.
- Die Startreihenfolge in einem Blade-Server ändern.
- Datum und Uhrzeit einstellen.
- Eine ferne Konsole für die Blade-Server verwenden.
- Das Eigentumsrecht für Tastatur, Bildschirm und Maus ändern.
- Das Eigentumsrecht für Laufwerke für austauschbare Datenträger und USB-Anschlüsse ändern. (Die Laufwerke für austauschbare Datenträger in der BladeCenter-Einheit werden vom Betriebssystem des Blade-Servers als USB-Einheiten betrachtet.)
- Die Farbe festlegen, die die Alarmanzeige für kritische Systemfehler (Critical - CRT) und die Alarmanzeige für schwere Systemfehler (Major - MJR) annehmen, wenn sie aktiv sind (nur bei BladeCenter T-Einheiten).

Sie können die Webschnittstelle des Managementmoduls, SNMP, SMASH und die Befehlszeilenschnittstelle des Managementmoduls auch verwenden, um einige der Konfigurationseinstellungen des Blade-Servers anzuzeigen. Weitere Informationen finden Sie in diesem Kapitel und in der Dokumentation zur Verwaltungsmethode, die Sie verwenden.

Webschnittstellenseiten und Benutzerrollen

Der Zugriff auf die verschiedenen Seiten der Webschnittstelle des Managementmoduls erfordert unterschiedliche Benutzerberechtigungen.

Einige Felder und Optionen auf den Webschnittstellenseiten des Managementmoduls können nur von Benutzern geändert oder ausgeführt werden, denen Rollen mit der erforderlichen Berechtigungsstufe für diese Seiten zugewiesen wurden. Benutzer mit der Rolle "Supervisor" (Administrator, Befehlsberechtigung) für eine Seite können Informationen ändern und alle Tasks auf der Seite ausführen. Das Anzeigen von Informationen erfordert keine bestimmte Befehlsberechtigung. Den Benutzern kann jedoch ein beschränkter Lesezugriff auf bestimmte Einheiten in der BladeCenter-Einheit zugewiesen werden. Dabei gilt Folgendes:

- Benutzer mit der Bedienerrolle können alle Informationen anzeigen.
- Benutzer mit der angepassten Rolle des Gehäusebedieners können Informationen zu den allgemeinen Komponenten der BladeCenter-Einheit anzeigen.
- Benutzer mit der angepassten Rolle des Bladebedieners können Informationen zu den Blade-Servern anzeigen.
- Benutzer mit der angepassten Rolle des E/A-Modul-(Switch-)Bedieners können Informationen zu den E/A-Modulen anzeigen.

In Tabelle 2 auf Seite 101 sind die Webschnittstellenseiten des Managementmoduls und die Rollen (Befehlsberechtigungsstufen) aufgelistet, die zum Ändern von Informationen auf diesen Seiten erforderlich sind. Die in dieser Tabelle aufgeführten Seiten und Rollen gelten nur für das Ändern der Informationen auf einer Seite oder für das Ausführen einer Task, die auf einer Seite angegeben wird. Das Anzeigen der Informationen auf einer Seite erfordert keine bestimmte Rolle oder Befehlsberechtigung. In jeder Tabellenzeile sind die gültigen Benutzerrollen (Befehlsberechtigungen) angegeben, mit denen ein Benutzer die Informationen ändern oder eine Task auf dieser Seite ausführen kann. So ist in Tabelle 2 auf Seite 101 beispielsweise angegeben, dass Benutzer zum Ausführen von Tasks auf der Seite **Blade Tasks → Power/Restart** (Blade-Tasks → Einschalten/Neustart) die Rolle "Supervisor" (Administrator) oder "Blade Administration" (Bladeverwaltung) benötigen.

Wichtig: Stellen Sie nach der Aktualisierung der Firmware des Managementmoduls sicher, dass die Rollen der einzelnen Benutzer korrekt festgelegt sind, da sich diese Definitionen möglicherweise je nach Firmwareversion unterscheiden.

Tabelle 2. Beziehungen der Benutzerrollen

Seite	Erforderliche Rolle zum Ändern von Informationen oder zum Ausführen von Tasks										
	Supervisor (Administrator)	**Chassis User Account Management (Gehäusebenutzerkontenverwaltung)**	**Blade Server Remote Presence (Blade-Server-Remote-Presence)**	**Chassis Operator (Gehäusebediener)**	**Chassis Administration (Gehäuseverwaltung)**	**Blade Administration (Bladeverwaltung)**	**I/O Module Administration (E/A-Modulverwaltung)**	**Chassis Log Administration (Gehäuseprotokollverwaltung)**	**Chassis Configuration (Gehäusekonfiguration)**	**Blade Configuration (Bladekonfiguration)**	**I/O Module Configuration (E/A-Modulkonfiguration)**
Monitors (Monitore)											
System Status (Systemstatus)	•	•	•	•	•	•	•	•	•	•	•
Event Log (Ereignisprotokoll) (anzeigen)	•	•	•	•	•	•	•	•	•	•	•
Event Log (Ereignisprotokoll) (Inhalt löschen oder Protokollrichtlinie festlegen)	•							•			
LEDs (Anzeigen)	•	•	•		•	•	•	•	•	•	•
Power Management (Stromverbrauchssteuerung)	•	•	•		•	•	•	•	•	•	•
Hardware VPD (Elementare Hardware-Produktdaten)	•	•	•		•	•	•	•	•	•	•
Firmware VPD (Elementare Firmware-Produktdaten)	•	•	•		•	•	•	•	•	•	•
Remote Chassis (Ferne Gehäuse)	•			•	•						
Blade Tasks (Blade-Tasks)											
Power/Restart (Einschalten/ Neustart)	•					•					
Remote Control (Fernsteuerung) (ferne Konsole)	•		•								
Firmware Update (Firmwareaktualisierung)	•					•					

Tabelle 2. Beziehungen der Benutzerrollen (Forts.)

Seite	Erforderliche Rolle zum Ändern von Informationen oder zum Ausführen von Tasks										
	Supervisor (Administrator)	**Chassis User Account Management (Gehäusebenutzerkontenverwaltung)**	**Blade Server Remote Presence (Blade-Server-Remote-Presence)**	**Chassis Operator (Gehäusebediener)**	**Chassis Administration (Gehäuseverwaltung)**	**Blade Administration (Bladeverwaltung)**	**I/O Module Administration (E/A-Modulverwaltung)**	**Chassis Log Administration (Gehäuseprotokollverwaltung)**	**Chassis Configuration (Gehäusekonfiguration)**	**Blade Configuration (Bladekonfiguration)**	**I/O Module Configuration (E/A-Modulkonfiguration)**
Configuration (Konfiguration)	•									•	
Advanced Configuration (Erweiterte Konfiguration) (Bladepositionsdaten)	•										
Serial Over LAN (Serial over LAN)	•								•	•	
Open Fabric Manager (Open Fabric Manager)	•										
I/O Module Tasks (E/A-Modul-Tasks)											
Admin/Power/Restart (Administration/Einschalten/ Neustart)	•						•				
Configuration (Konfiguration) (siehe Anmerkung 1)	•										•
Firmware Update (Firmwareaktualisierung)	•						•				
Storage Tasks (Speicher-Tasks)											
Configuration (Konfiguration)	•								•		
MM Control (MM-Steuerung)											
General Settings (Allgemeine Einstellungen)	•								•		
„Login Profiles (Anmeldeprofile)" auf Seite 172 (Kontosicherheitsverwaltung)	•	•									

Tabelle 2. Beziehungen der Benutzerrollen (Forts.)

Seite	Erforderliche Rolle zum Ändern von Informationen oder zum Ausführen von Tasks										
	Supervisor (Administrator)	**Chassis User Account Management (Gehäusebenutzerkontenverwaltung)**	**Blade Server Remote Presence (Blade-Server-Remote-Presence)**	**Chassis Operator (Gehäusebediener)**	**Chassis Administration (Gehäuseverwaltung)**	**Blade Administration (Bladeverwaltung)**	**I/O Module Administration (E/A-Modulverwaltung)**	**Chassis Log Administration (Gehäuseprotokollverwaltung)**	**Chassis Configuration (Gehäusekonfiguration)**	**Blade Configuration (Bladekonfiguration)**	**I/O Module Configuration (E/A-Modulkonfiguration)**
„Alerts" auf Seite 181 (siehe Anmerkung 2)	•								•		
Serial Port (Serieller Anschluss)	•								•		
Port Assignments (Portzuordnungen)	•								•		
Network Interfaces (Netzschnittstellen)	•								•		
Network Protocols (Netzprotokolle)	•								•		
Chassis Internal Network (Internes Gehäusenetz)	•										
Security (Sicherheit)	•								•		
Configuration Mgmt (Konfigurationsverwaltung) (Konfiguration in Datei sichern)	•	•		•	•			•	•		
Configuration Mgmt (Konfigurationsverwaltung) (Konfiguration in BladeCenter-Einheit speichern)	•										
Configuration Mgmt (Konfigurationsverwaltung) (wiederherstellen)	•										

Tabelle 2. Beziehungen der Benutzerrollen (Forts.)

Seite	Erforderliche Rolle zum Ändern von Informationen oder zum Ausführen von Tasks										
	Supervisor (Administrator)	**Chassis User Account Management (Gehäusebenutzerkontenverwaltung)**	**Blade Server Remote Presence (Blade-Server-Remote-Presence)**	**Chassis Operator (Gehäusebediener)**	**Chassis Administration (Gehäuseverwaltung)**	**Blade Administration (Bladeverwaltung)**	**I/O Module Administration (E/A-Modulverwaltung)**	**Chassis Log Administration (Gehäuseprotokollverwaltung)**	**Chassis Configuration (Gehäusekonfiguration)**	**Blade Configuration (Bladekonfiguration)**	**I/O Module Configuration (E/A-Modulkonfiguration)**
Configuration Mgmt (Konfigurationsverwaltung) (Konfigurationsassistent)	•										
File Management (Dateiverwaltung)	•				•	•	•		•	•	•
Firmware Update (Firmwareaktualisierung)	•				•						
Restart MM (MM-Neustart)	•				•						
„License Manager (Lizenzmanager)" auf Seite 205	•				•						
Service Tools (Service-Tools)											
AMM Service Data (Servicedaten des erweiterten Managementmoduls) (nur anzeigen)											
Blade Service Data (Blade-Servicedaten) (nicht für alle Blade-Server)	•										
AMM Status (Status der erweiterten Managementmodule) (nur anzeigen)											
Service Advisor (Service Advisor) (siehe Anmerkung 4)	•								•		
„Scalable Complex (Skalierbarer Komplex)" auf Seite 215	•									•	

Anmerkungen:

1. Das Absetzen von Pingsignalen an ein E/A-Modul (Link **Advanced Management** (Erweiterte Verwaltung) auf der Seite **I/O Module Tasks → Configuration** (E/A-Modul-Tasks → Konfiguration)) erfordert die Rolle "I/O Module Administration" (E/A-Modulverwaltung), "I/O Module Configuration" (E/A-Modulkonfiguration) oder "I/O Module Operator" (E/A-Modulbediener).
2. Beim BladeCenter T-Managementmodul erfordert das Zurücksetzen der Filtererkennung unter **MM Control → Alerts** (MM-Steuerung → Alerts) die Rolle "Supervisor" (Administrator) oder "Chassis Administration" (Gehäuseverwaltung).
3. Die Seite **MM Control → Restore Defaults** (MM-Steuerung → Standardwerte wiederherstellen) erfordert sowohl die Rolle "Chassis Administration" (Gehäuseverwaltung) als auch die Rolle "Chassis Configuration" (Gehäusekonfiguration).
4. Das Ausführen der Service Advisor-Optionen **Manual Call Home** (Manuelle Call-Home-Funktion) oder **Test Call Home** (Call-Home-Funktion testen) erfordert die Rolle "Chassis Configuration" (Gehäusekonfiguration), "Chassis Administration" (Gehäuseverwaltung), "Blade Configuration" (Bladekonfiguration), "Blade Administration" (Bladeverwaltung), "I/O Module Configuration" (E/A-Modulkonfiguration) oder "I/O Module Administration" (E/A-Modulverwaltung).

Optionen der Webschnittstelle des Managementmoduls

Führen Sie das Verwaltungs- und Konfigurationsprogramm über die Webschnittstelle des Managementmoduls aus, um die BladeCenter-Einstellungen auszuwählen, die Sie anzeigen oder ändern möchten.

Das Navigationsfenster (auf der linken Seite in der Webschnittstelle des Managementmoduls) enthält Navigationslinks, mit denen Sie Ihre BladeCenter-Einheit verwalten und den Status der Komponenten (Module und Blade-Server) überprüfen können. Die Links im Navigationsfenster werden in den folgenden Abschnitten beschrieben.

Für die Webschnittstelle des Managementmoduls steht eine Onlinehilfe zur Verfügung. Klicken Sie auf das Hilfesymbol neben einer Abschnittsüberschrift, um weitere Informationen zu diesem Thema anzuzeigen. Beim erweiterten Managementmodul werden die Webschnittstellenseiten nach jeder Aktualisierung mit Zeitmarken für Datum und Uhrzeit versehen.

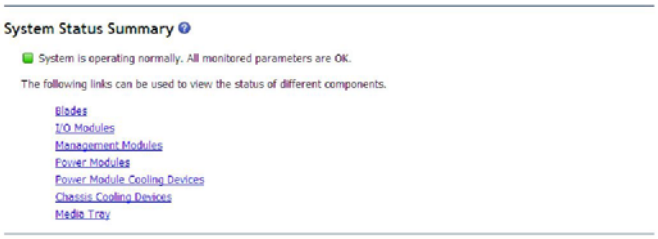
Monitors (Monitore)

Wählen Sie die Optionen unter **Monitors** (Monitore) aus, um den Status, die Einstellungen und andere Informationen zu Komponenten in Ihrer BladeCenter-Einheit anzuzeigen.

System Status (Systemstatus)

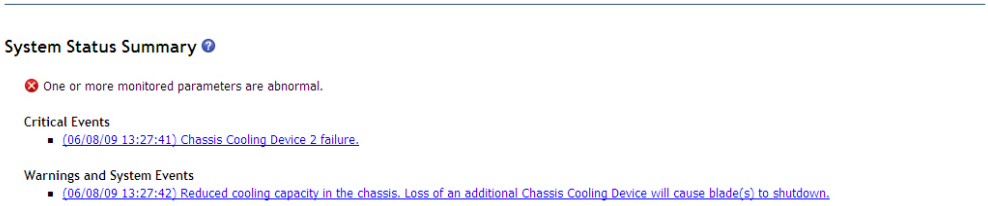
Wählen Sie **Monitors → System Status** (Monitore → Systemstatus) aus, um den allgemeinen Systemstatus, eine Liste der ausstehenden Ereignisse, die sofortige Aufmerksamkeit erfordern, und den allgemeinen Status der einzelnen Blade-Server und anderen Komponenten in der BladeCenter-Einheit anzuzeigen.

Die folgende Seite wird angezeigt.



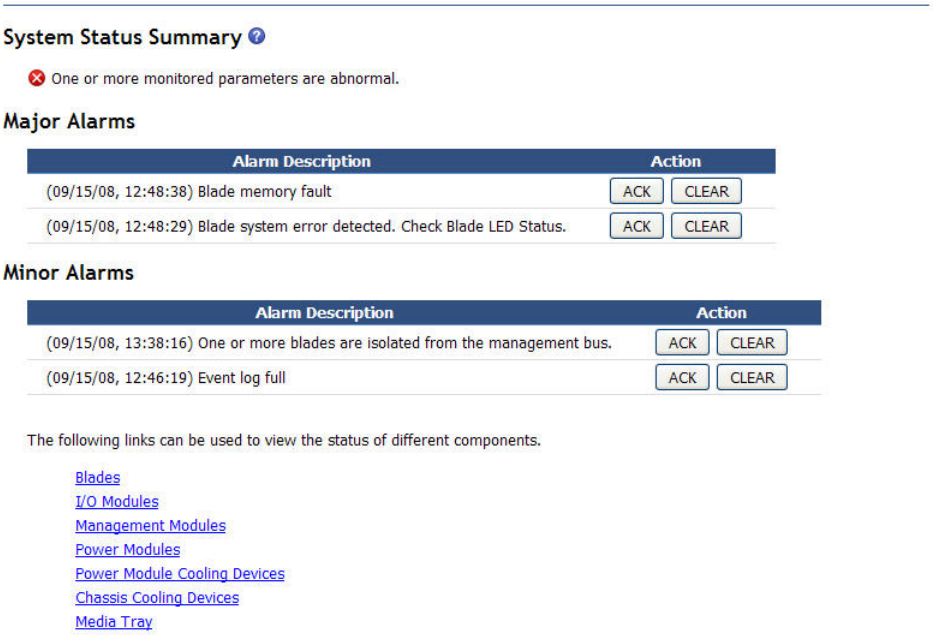
Anmerkung: Die BladeCenter S-Einheit enthält einen Link **Storage Module** (Speichermodul) für den Speichermodulstatus.

Wenn eine abnormale Systembedingung erkannt wird, erscheint diese in der Zusammenfassung zum Systemstatus. Dabei werden auch das Datum und die Uhrzeit für das Auftreten der Bedingung sowie ein Link auf zusätzliche Informationen angezeigt. Wenn Sie auf einen Ereignislink klicken, werden ausführliche Ereignisinformationen und empfohlene Maßnahmen angezeigt. (Eine vollständige Liste aller nicht einheitenspezifischen Ereignisse und empfohlenen Maßnahmen, die nach der Ereignis-ID geordnet sind, finden Sie im *Nachrichtenhandbuch zum erweiterten BladeCenter-Managementmodul*. Einheitenspezifische Ereignisinformationen finden Sie in der Dokumentation zur Einheit.) In der folgenden Abbildung ist die Zusammenfassung zum Systemstatus mit einem abnormalen Ereignis dargestellt.



BladeCenter T- und BladeCenter HT-Alarmverwaltung:

Wählen Sie diese Seite aus, um Alarme für die BladeCenter T- und BladeCenter HT-Einheiten zu verwalten.



Bei den BladeCenter T- und BladeCenter HT-Einheiten werden auf der Seite "System Status Summary" (Zusammenfassung des Systemstatus) aktive Alarmbedingungen angezeigt, die nach Alarmtyp gruppiert sind (kritisch, schwerwiegend oder geringfügig). Bei einem Alarm der Kategorie "Critical" (Kritisch), "Major" (Schwerwiegend) oder "Minor" (Geringfügig) leuchtet die entsprechende Anzeige der Alarmstufe an der BladeCenter T- oder BladeCenter HT-Einheit auf. Durch Bestätigen eines Alarms wird er aus der Liste "Critical", "Major" bzw. "Minor" in die Liste der bestätigten Alarme verschoben und die Anzeige hört auf zu leuchten. Durch Löschen eines Alarms wird er aus allen Alarmlisten entfernt und die Anzeige hört auf zu leuchten. Durch Bestätigen oder Löschen eines Alarms wird die Anzeige nur ausgeschaltet, wenn keine anderen Alarme derselben Stufe vorliegen, die aktiv sind und die Anzeige weiter leuchten lassen.

Neben den einzelnen Alarmbeschreibungen in der Liste der aktiven Alarme befinden sich jeweils die beiden Aktionsschaltflächen **ACK** (Bestätigen) und **CLEAR** (Löschen). Klicken Sie auf **ACK** (Bestätigen), um die Anzeige zum jeweiligen Alarm auszuschalten und den Alarm in die Liste der bestätigten Alarme zu verschieben. Klicken Sie auf **CLEAR** (Löschen), um die Anzeige zum jeweiligen Alarm auszuschalten und den Alarm aus allen Alarmlisten zu entfernen. Nachdem ein Alarm in die Liste der bestätigten Alarme verschoben wurde, können Sie ihn aus allen Alarmlisten entfernen. Klicken Sie hierzu auf die Aktionsschaltfläche **CLEAR** (Löschen) rechts neben der Beschreibung des bestätigten Alarms.

BladeCenter-Einheit, detaillierter Komponentenstatus:

Wählen Sie **Monitors → System Status** (Monitore → Systemstatus) aus, um detaillierte Informationen zum Komponentenstatus anzuzeigen.

Die Seite zum Systemstatus zeigt die folgenden detaillierten Statusinformationen für BladeCenter-Komponenten an.

Die folgende Abbildung zeigt eine Blade-Server-Statusseite für das erweiterte Managementmodul.

Wenn Sie auf **Blade servers** (Blade-Server) klicken, werden die folgenden Informationen angezeigt:

- **Bay:** (Position) Die Position mit der niedrigsten Nummer, die der Blade-Server belegt.
- **Status:** (Status) Ein Symbol, das anzeigt, ob der Status des Blade-Servers "good" (Gut) , "warning" (Warnung) oder "critical" (Kritisch) lautet. Klicken Sie auf das Symbol, um ausführlichere Statusinformationen zu erhalten.
- **Name:** (Name) Der Name des Blade-Servers nach der erfolgreich abgeschlossenen Initialisierung. Ehe der Blade-Server diesen Status erreicht, zeigt er möglicherweise eine der folgenden Textzeichenfolgen an:
  - **Discovery** (Erkennung): Der Blade-Server wird noch initialisiert
  - **Comm Error** (Fehler bei Datenübertragung): Der Blade-Server hat bei der Datenübertragung mit dem erweiterten Managementmodul einen Fehler festgestellt
  - **Kernel Mode** (Kernelmodus): Bei der Initialisierung des Blade-Servers ist ein Fehler aufgetreten. Er befindet sich in einem reduzierten Funktionsstatus.
- **Pwr:** (Stromversorgung) Der Stromversorgungsstatus (ein oder aus) des Blade-Servers.

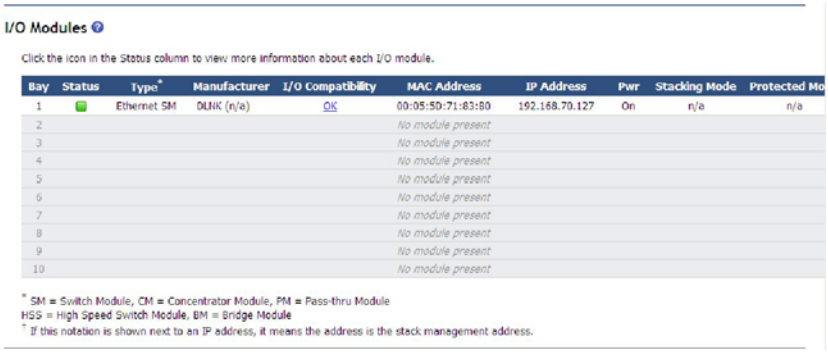
- **Owner** (Eigner): Ein Hinweis darauf, ob der aktuelle Blade-Server die folgenden BladeCenter-Ressourcen steuert:
  - **KVM:** (Keyboard, Video, Mouse) Tastatur, Bildschirm und Maus
  - **MT:** (Media Tray, Laufwerkschlitten) Der Laufwerkschlitten, der die Laufwerke für austauschbare Datenträger und die USB-Anschlüsse enthält

  Anmerkung: Das erweiterte Managementmodul verfügt über zwei USB-Anschlüsse. Wenn Sie an einen dieser Anschlüsse eine USB-Speichereinheit anschließen, kann diese auch von den Blade-Servern in der BladeCenter-Einheit verwendet werden. Folgende Regeln legen fest, welcher Blade-Server die USB-Speichereinheit erkennt:

  1. Bei BladeCenter-Einheiten wird die USB-Speichereinheit an den Blade-Server angehängt, der der Eigner von Tastatur, Bildschirm und Maus ist.
  2. Bei BladeCenter H- oder HT-Einheiten wird die USB-Speichereinheit an den Blade-Server angehängt, der der Eigner des Laufwerkschlittens ist.
  3. Die Managementmodule für die BladeCenter T-Einheit besitzen keine USB-Anschlüsse.
- **cKVM** (concurrent KVM): Zeigt an, ob eine Erweiterungskarte einer konkurrierenden KVM (Tastatur, Bildschirm und Maus) im Blade-Server installiert ist.
- **I/O Compatibility** (E/A-Kompatibilität): Der Kompatibilitätsstatus des Blade-Servers. Jeder Status stellt einen Link zu ausführlichen Kompatibilitätsinformationen für den Blade-Server dar.
- **WOL**: Ein Hinweis, ob die Wake on LAN-Funktion für den Blade-Server gegenwärtig aktiviert ist. Die Funktion Wake on LAN ist im Blade-Server-BIOS standardmäßig aktiviert und kann nicht inaktiviert werden. Das BladeCenter-Managementmodul stellt einen zentralen Steuerungspunkt für die Wake on LAN-Funktion bereit, der es ermöglicht, die Einstellungen für die gesamte BladeCenter-Einheit oder für einen einzigen Blade-Server zu steuern. Die Wake on LAN-Einstellungen im Managementmodul überschreiben die Einstellungen im Blade-Server-BIOS. Weitere Informationen erhalten Sie im Abschnitt „Einschalten/Neustart" auf Seite 141.

  Anmerkung: Wenn ein Blade-Server die Wake on LAN-Funktion nicht unterstützt, wird in diesem Feld `n/a` angezeigt.
- **Local Control** (Lokale Steuerung): Ein Hinweis darauf, ob die folgenden Optionen aktiviert sind:
  - Local power control (Lokale Stromversorgungssteuerung)
  - Local keyboard, video, and mouse switching (Lokale Übergabe der KVM-Steuerung (Tastatur, Bildschirm und Maus))
  - Local removable-media drive and USB port switching (Lokale Übergabe der Steuerung des Laufwerks für austauschbare Datenträger und des USB-Anschlusses)
- **BEM**: Ein Hinweis darauf, ob sich eine Erweiterungseinheit, wie beispielsweise eine SCSI-Erweiterungseinheit oder eine PCI-E/A-Erweiterungseinheit, in der Bladeposition befindet.

Die folgende Abbildung zeigt eine E/A-Modul-Statusseite für das erweiterte Managementmodul.



Wenn Sie auf **I/O Modules** (E/A-Module) klicken, werden die folgenden Informationen angezeigt. Die Anzahl der E/A-Modulpositionen hängt jeweils vom Typ der BladeCenter-Einheit ab.

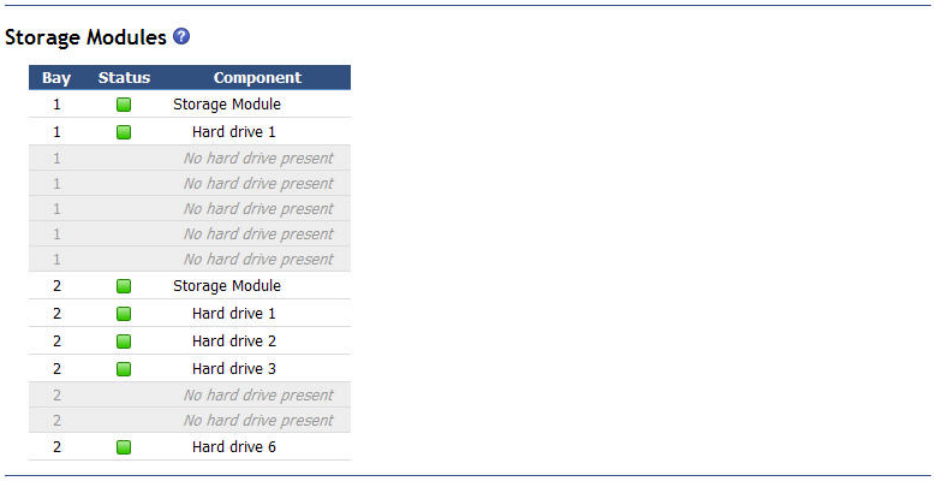
- **Bay** (Position): Die Nummer der Position des E/A-Moduls.
- **Status** (Status): Ein Symbol, das den Status "good" (Gut) , "warning" (Warnung) oder "critical" (Kritisch) für das E/A-Modul angibt. Klicken Sie auf dieses Symbol, um detaillierte Informationen zur Kompatibilität des E/A-Moduls anzuzeigen.
- **Type** (Typ): Der Typ des E/A-Moduls in der Position, zum Beispiel ein Ethernet-E/A-Modul, ein Fibre-Channel-E/A-Modul oder ein Durchgriffsmodul.
- **Manufacturer** (Hersteller): Der Hersteller des E/A-Moduls.
- **I/O Compatibility** (E/A-Kompatibilität): Der Kompatibilitätsstatus des E/A-Moduls. Jeder Status stellt einen Link zu ausführlichen Kompatibilitätsinformationen für das E/A-Modul dar.Bei einigen E/A-Modulen werden beim Klicken auf den Statuslink detaillierte Statusinformationen für die E/A-Modul-Anschlüsse angezeigt.
- **MAC Address** (MAC-Adresse): Die MAC-Adresse (Medium Access Control) des E/A-Moduls.

  Anmerkung: Einige Typen von E/A-Modulen, wie zum Beispiel Durchgriffsmodule, besitzen keine MAC- oder IP-Adresse.

  Anmerkungen:
  - Einige Typen von E/A-Modulen, wie zum Beispiel Durchgriffsmodule, besitzen keine MAC- oder IP-Adresse.
  - Das RAID-SAS-Modul, verfügbar im BladeCenter S, erfordert zwei MAC-Adressen und zwei IP-Adressen und zeigt diese an.
- **IP Address** (IP-Adresse): Die IP-Adresse des E/A-Moduls.
- **Pwr** (Stromversorgung): Der Stromversorgungsstatus (ein oder aus) des E/A-Moduls.
- **Stacking Mode** (Stapelmodus): Der Status des Stapelmodus des E/A-Moduls.

- **Protected Mode** (Schutzmodus): Der aktuelle Status des geschützten Modus des E/A-Moduls.
  - **n/a**: Die Schutzmodusfunktion ist im E/A-Modul nicht vorhanden.
  - **Disabled** (Inaktiviert): Die Schutzmodusfunktion ist im E/A-Modul vorhanden, wurde im E/A-Modul oder im erweiterten Managementmodul jedoch nicht aktiviert.
  - **Pending** (Anstehend): Der Schutzmodus wurde im erweiterten Managementmodul aktiviert, aber noch nicht im E/A-Modul.
  - **Active** (Aktiv): Der Schutzmodus ist sowohl im E/A-Modul als auch im erweiterten Managementmodul aktiv.
  - **Attention** (Achtung): Der Schutzmodus ist im E/A-Modul, aber nicht im erweiterten Managementmodul aktiviert.
- **POST Status** (POST-Status (Power-On Self Test, Selbsttest beim Einschalten)): Textdaten zum Status des E/A-Moduls.

In der BladeCenter S-Einheit stellt das erweiterte Managementmodul einen Link zur Seite **Storage Modules** (Speichermodule) bereit, auf der folgende Informationen angezeigt werden.



- **Bay** (Position): Die Positionsnummer des jeweiligen installierten Speichermoduls.
- **Status** (Status): Ein Symbol, das den Status "good" (Gut) , "warning" (Warnung) oder "critical" (Kritisch) des Speichermoduls angibt.
- **Component** (Komponente): Der Typ der Komponente, die sich in diesem Speichermodul befindet.

Wenn Sie auf **Management Modules** (Managementmodule) klicken, werden die folgenden Informationen angezeigt:

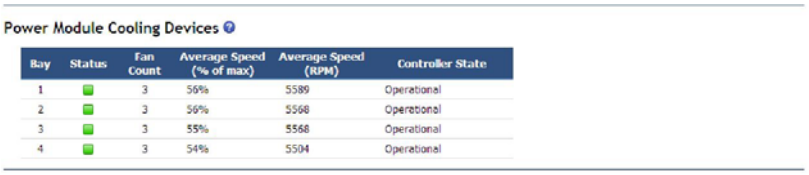
- **Bay** (Position): Die Nummer der Position, die das Managementmodul belegt.
- **Status** (Status): Ein Symbol, das den Status "good" (Gut) , "warning" (Warnung) oder "critical" (Kritisch) des Managementmoduls anzeigt. Klicken Sie auf das Statussymbol, um detailliertere Statusinformationen anzuzeigen, wie zum Beispiel Ergebnisse des Selbsttests, Spannungshöhen des Netzteils, die Innentemperatur der BladeCenter-Einheit und eine Liste der gegenwärtig an der BladeCenter-Einheit angemeldeten Benutzer. Beim erweiterten Managementmodul zeigt der detaillierte Status außerdem eine Liste der Benutzer an, die am Managementmodul angemeldet sind, sowie ihre Zugriffsinformationen. Für jeden Benutzer, der zum Zeitpunkt der Erstellung dieser Seite am erweiterten Managementmodul angemeldet ist, wird die Schaltfläche **Terminate** (Beenden) angezeigt. Wenn ein Benutzer nicht über eine Systemadministratorberechtigung verfügt, wird die Schaltfläche nur für die Sitzung dieses Benutzers aktiviert.
- **IP Address** (IP-Adresse): Wenn Sie auf **View** (Anzeigen) klicken, werden die IP-Adressinformationen für die Fernverwaltung und Konsolenverbindung (externer Ethernet-Anschluss) auf dem Managementmodul angezeigt.
- **Primary** (Primär): Ein Hinweis darauf, welches Managementmodul das primäre oder aktive Managementmodul ist.

Wenn Sie auf **Power Modules** (Stromversorgungsmodule) klicken, werden die folgenden Informationen angezeigt:

- **Bay** (Position): Die Nummer der Position, die das Stromversorgungsmodul belegt.
- **Status** (Status): Ein Symbol, das den Status "good" (Gut) , "warning" (Warnung) oder "critical" (Kritisch) des Stromversorgungsmoduls anzeigt.
- **Details** (Details): Textdaten zum Status des Stromversorgungsmoduls.

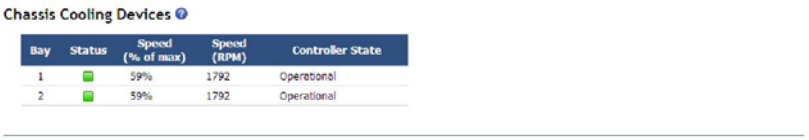
Anmerkung: Wenn in einer BladeCenter S-Einheit ein erweitertes Managementmodul installiert ist, wird in einer Zeile unter der Tabelle der Stromversorgungsmodule angezeigt, ob die BladeCenter-Einheit an eine Stromquelle mit 110 oder mit 220 Volt Wechselstrom angeschlossen ist.

Wenn Sie auf **Power Module Cooling Devices** (Kühleinheiten der Stromversorgungsmodule) (einige BladeCenter-Einheiten unterstützen diese Komponenten) klicken, werden die folgenden Informationen angezeigt:



- **Bay** (Position): Die Nummer der Stromversorgungsmodulposition, in der sich die Kühleinheit des Stromversorgungsmoduls befindet.
- **Status** (Status): Ein Symbol, das den Status "good" (Gut) , "warning" (Warnung) oder "critical" (Kritisch) der Kühleinheit des Stromversorgungsmoduls anzeigt.
- **Fan Count** (Lüfteranzahl): Die Anzahl der betriebsbereiten Lüfter in der Kühleinheit des Stromversorgungsmoduls.
- **Average Speed (% of max)** (Durchschnittliche Geschwindigkeit (% von max)): Die gegenwärtige Geschwindigkeit der Kühleinheit des Stromversorgungsmoduls als Prozentsatz der maximalen Anzahl Umdrehungen pro Minute. Die Geschwindigkeit der Kühleinheit des Stromversorgungsmoduls variiert abhängig von der thermischen Last. Der Eintrag `Offline` zeigt an, dass die Kühleinheit des Stromversorgungsmoduls nicht betriebsbereit ist.
- **Average Speed (RPM)** (Durchschnittliche Geschwindigkeit (Umdrehungen pro Minute)): Die gegenwärtige Geschwindigkeit der Kühleinheit des Stromversorgungsmoduls in Umdrehungen pro Minute. Die gegenwärtige Geschwindigkeit der Kühleinheit des Stromversorgungsmoduls variiert abhängig von der thermischen Last.
- **Controller State** (Controllerstatus): Der Status des Geschwindigkeitscontrollers der Kühleinheit des Stromversorgungsmoduls: "operational" (betriebsbereit), "flashing" (Flash-Speicher-Vorgang) (Firmware wird aktualisiert), "not present" (nicht vorhanden) oder "communication error" (Übertragungsfehler).

Wenn Sie auf **Chassis Cooling Devices** (Gehäusekühleinheiten) klicken, werden die folgenden Informationen angezeigt:



- **Bay** (Position): Die Nummer der Position, in der sich das Kühleinheitenmodul der BladeCenter-Einheit befindet.
- **Status** (Status): Ein Symbol, das den Status "good" (Gut) , "warning" (Warnung) oder "critical" (Kritisch) der Kühleinheit der BladeCenter-Einheit anzeigt.
- **Speed (% of max)**: (Geschwindigkeit (% von max)): Die gegenwärtige Geschwindigkeit des Kühleinheitenmoduls der BladeCenter-Einheit als Prozentsatz der maximalen Anzahl Umdrehungen pro Minute. Die Geschwindigkeit der Kühleinheit der BladeCenter-Einheit variiert abhängig von der thermischen Last. Der Eintrag `Offline` zeigt an, dass die Kühleinheit der BladeCenter-Einheit nicht betriebsbereit ist.

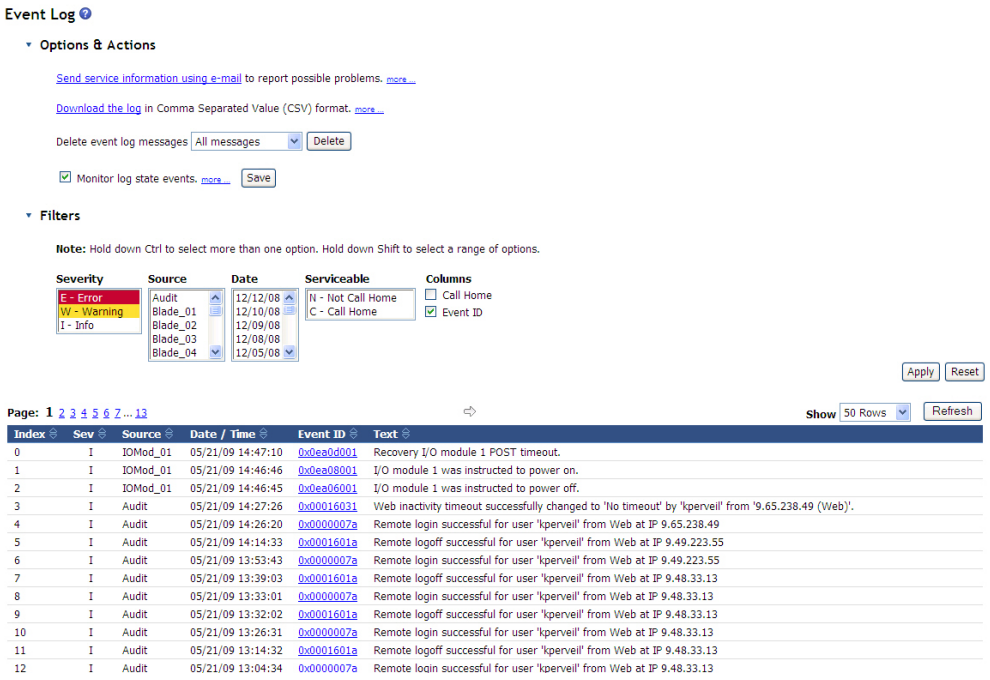
- **Speed (RPM)** (Geschwindigkeit (Umdrehungen pro Minute)) (nur bei in einer BladeCenter H-Einheit installierten erweiterten Managementmodulen): Die gegenwärtige Geschwindigkeit des Kühleinheitenmoduls der BladeCenter-Einheit in Umdrehungen pro Minute. Die Geschwindigkeit der Kühleinheit der BladeCenter-Einheit variiert abhängig von der thermischen Last.
- **Controller State** (Controllerstatus) (nur bei in einer BladeCenter H-Einheit installierten erweiterten Managementmodulen): Der Status des Geschwindigkeitscontrollers des Gebläses: "operational" (betriebsbereit), "flashing" (Flash-Speicher-Vorgang) (Firmware wird aktualisiert), "not present" (nicht vorhanden) oder "communication error" (Übertragungsfehler).

Wenn Sie auf **Media Tray** (Laufwerkschlitten) klicken, werden folgende Informationen angezeigt (der Temperaturstatus des Laufwerkschlittens ist nicht bei allen Typen von BladeCenter-Einheiten verfügbar):

- **Temp (C°)** (Temperatur (C°)): Die Umgebungstemperatur des Laufwerkschlittens, der vom Temperatursensor an der Vorderseite angegeben wird.
- **Warning** (Warnung): Der Schwellenwert für die Umgebungstemperatur des Laufwerkschlittens, bei dessen Erreichen ein Warnungsereignis in das Ereignisprotokoll eingetragen wird.
- **Warning Reset** (Warnung zurücksetzen): Schwellenwert für die Umgebungstemperatur des Laufwerkschlittens. Wenn die Temperatur den Warnungsschwellenwert überschreitet und anschließend unter den Schwellenwert für das Zurücksetzen der Warnung zurückfällt, wird das Warnungsereignis zur Temperatur gelöscht. In das Ereignisprotokoll wird ein Hinweis darauf eingetragen, dass die Temperaturwarnung wieder gelöscht wurde.
- **Hysteresis** (Hysterese) (nur bei in einer BladeCenter T-Einheit installierten erweiterten Managementmodulen): Die Differenz zwischen den Schwellenwerten für die Temperaturwarnung und das Zurücksetzen der Temperaturwarnung.

Event Log (Ereignisprotokoll)

Wählen Sie die Option **Monitors → Event Log** (Monitore → Ereignisprotokoll) aus, um die Einträge anzuzeigen, die derzeit im Ereignisprotokoll des Managementmoduls gespeichert sind.



Die Seite "Event log" (Ereignisprotokoll) enthält Einträge für die Systemereignisse, die von der BladeCenter-Einheit und den installierten Komponenten erkannt werden, sowie für die Prüfereignisse, die von den Benutzern erstellt werden. Die Seite "Event log" (Ereignisprotokoll) zeigt zuerst die neuesten Einträge an. Informationen zu jedem versuchten Fernzugriff und zu allen Änderungen der Konfigurationseinstellungen für das erweiterte Managementmodul werden im Prüfprotokoll aufgezeichnet. Das Managementmodul sendet die entsprechenden Alerts aus, wenn es entsprechend konfiguriert wurde. Das Ereignisprotokoll verfügt über eine festgelegte Kapazität. Wenn das Protokoll vollständig beschrieben ist, werden die ältesten Einträge durch die neuen Einträge überschrieben. Bei BladeCenter T- oder BladeCenter HT-Einheiten leuchtet die MNR-Anzeige (Minor Alarm, geringfügiger Alarm) der entsprechenden BladeCenter T- oder BladeCenter HT-Einheit auf, wenn das Protokoll vollständig beschrieben ist. Wenn das Managementmodul den Status des Ereignisprotokolls nicht überwachen soll, inaktivieren Sie das Kontrollkästchen **Monitor log state events** (Protokoll-Statusereignisse überwachen) oben auf der Seite "Event log" (Ereignisprotokoll).

Auf der Seite "Event log" (Ereignisprotokoll) können Sie Einträge sortieren und filtern und die Anzeige von Ereignis-IDs, die einen Link zu den jeweiligen Ereignisdaten enthalten, unterdrücken. Wenn Sie auf eine Ereignis-ID klicken, werden die ausführlichen Ereignisdaten sowie gegebenenfalls empfohlene Aktionen angezeigt. Weitere Informationen finden Sie in der Hilfe zum Ereignisprotokoll. Eine vollständige Liste aller Ereignisse, die nicht einheitenspezifisch sind, und der empfohlenen Aktionen, sortiert nach Ereignis-ID, finden Sie im *Nachrichtenhandbuch zum erweiterten BladeCenter-Managementmodul*. Informationen zu einheitenspezifischen Ereignissen finden Sie in der Dokumentation der jeweiligen Einheit.

Folgende Quellen können Ereignisse generieren, die im Ereignisprotokoll aufgezeichnet werden:

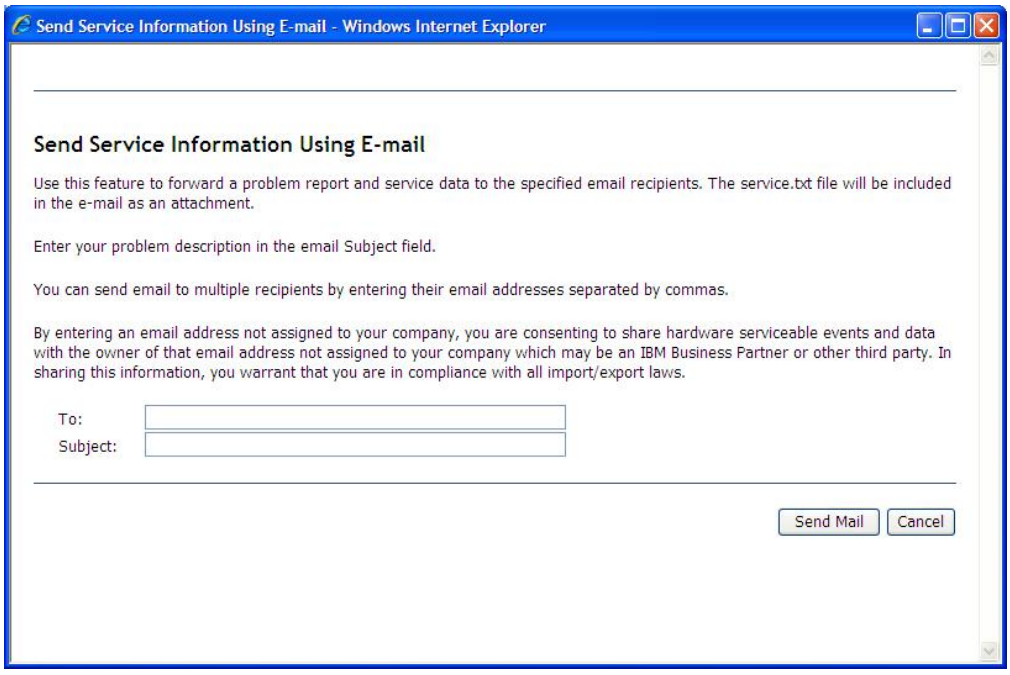
- BladeCenter-Einheit (SERVPROC)
- Blade-Einheit nach Positionsnummer (Blade_*xx*)
- Bedieneraktionen (Prüfereignis)
- Speichermodul nach Positionsnummer (Stor_*xx*)
- E/A-Modul nach Positionsnummer (IOMod_*xx*)
- Kühleinheit nach Nummer (Cool_*xx*)
- Stromversorgungsmodul nach Nummer (Power_*xx*)

Anmerkungen:

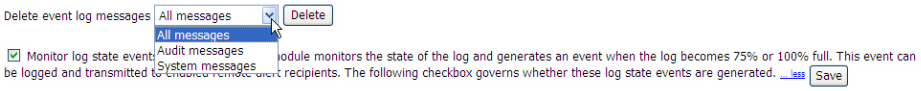
- *xx* in einer Ereignisquelle verweist auf die Positionsnummer der berichtenden Einheit.
- Ereignisse, die in der Blade Center T-Einheit einen Alarm auslösen, senden Alerts an das erweiterte Managementmodul. Einem Alert wird jeweils die Sicherheitseinstufung "Error" (Fehler), "Warning" (Warnung) und "Information" (Information) zugeordnet. Kritische und schwerwiegende Ereignisse werden als Fehler in das Protokoll eingetragen, geringfügige Ereignisse als Warnungen.

Aktivieren Sie das Kontrollkästchen **Call Home** (Call-Home) , um anzuzeigen, welche Ereignisse wartungsfähig sind. Wartungsfähige Ereignisse werden in der Regel durch Hardware- oder Firmwareprobleme ausgelöst. Wenn Sie die Funktion "Service Manager" (Service-Manager) aktiviert haben (siehe „Service Advisor konfigurieren” auf Seite 87), werden diese Ereignisse automatisch gemeldet.

Sie können auch auf den Link **Send service information using e-mail** (Serviceinformationen per E-Mail senden) klicken, um eine Momentaufnahme des Ereignisprotokolls an eine angegebene E-Mail-Adresse zu senden. Bei dieser Option wird ein Dialogfenster angezeigt, ähnlich dem in der folgenden Abbildung, in dem Sie die E-Mail-Adresse und den Zweck der Datenübertragung angeben können. Der SMTP-Server muss für die Verwendung dieser Funktion konfiguriert sein (Informationen hierzu finden Sie unter „Network Protocols (Netzprotokolle)” auf Seite 192). Klicken Sie auf den Link **Download the log** (Protokoll herunterladen), um eine Kopie des Ereignisprotokolls im CSV-Format (durch Kommas getrennte Werte) herunterzuladen.



Sie können Nachrichten aus dem Ereignisprotokoll löschen, indem Sie die zu löschenden Nachrichten auswählen und dann oben auf der Seite auf **Delete** (Löschen) klicken. Sie können auch auf **Save** (Speichern) klicken, um das kombinierte Ereignisprotokoll als Textdatei zu speichern.



LEDs (Anzeigen)

Wählen Sie die Option **Monitors → LEDs** (Monitore → Anzeigen) aus, um das Verhalten der Anzeigen für Telekommunikationseinheiten und andere BladeCenter-Einheiten zu verwalten.

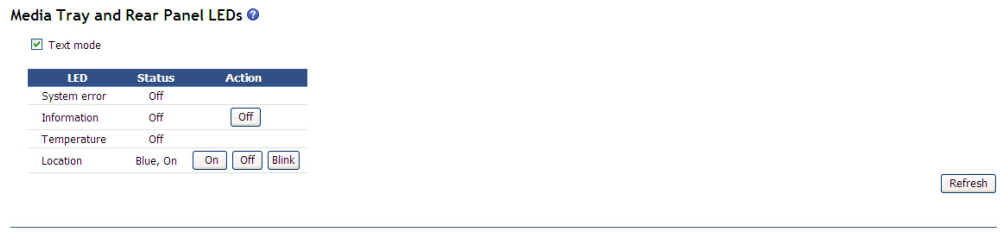
Anzeigen der BladeCenter-Einheit:

Wählen Sie **Monitors → LEDs** (Monitore → Anzeigen) aus, um das Verhalten der Anzeigen für die BladeCenter-Einheit zu verwalten.

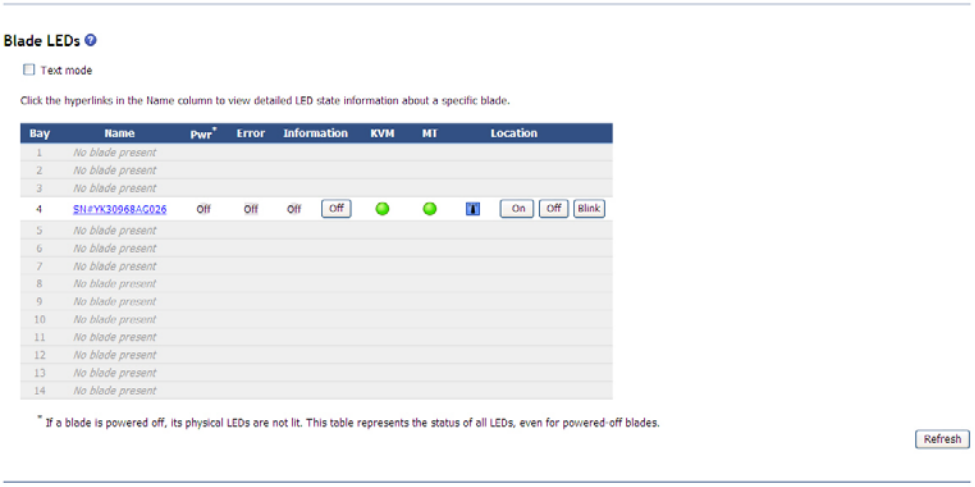
Anmerkung: Die BladeCenter S-Einheit enthält nach dem Link für die E/A-Modulanzeigen einen Link **Storage LEDs** (Speicheranzeigen).

Wählen Sie **LEDs** (Anzeigen) aus, um den Status der Anzeigen auf der BladeCenter-System-LED-Anzeige und auf dem Blade-Server-Bedienfeld anzuzeigen. Mit dieser Option können Sie auch die Informationsanzeige ausschalten und die Positionsanzeige auf der BladeCenter-Einheit und auf den Blade-Servern einschalten, ausschalten oder blinken lassen. Wenn Sie **Text Mode** (Textmodus) auswählen, wird der Einheitenstatus ohne grafische Symbole angegeben.

Die folgenden Informationen werden angezeigt. (Die Beispiele für Laufwerkschlittenanzeigen sind sowohl mit Symbolen als auch im Textmodus dargestellt.)



- **Media Tray LEDs** (Laufwerkschlittenanzeigen): Der Status der folgenden Anzeigen auf der BladeCenter-System-LED-Anzeige. Sie können den Status der Informations- und Positionsanzeigen ändern.
  - Systemfehler
  - Information
  - Temperaturüberschreitung
  - Position



- **Blade LEDs** (Bladeanzeigen): Der Status der folgenden Anzeigen auf dem Blade-Server-Bedienfeld. Sie können den Status der Informations- und Positionsanzeigen ändern.
  - Betrieb
  - Fehler
  - Information
  - Tastatur-, Bildschirm- und Mausauswahl
  - Datenträgerauswahl (optisches Laufwerk, Diskettenlaufwerk, USB-Anschluss)
  - Position

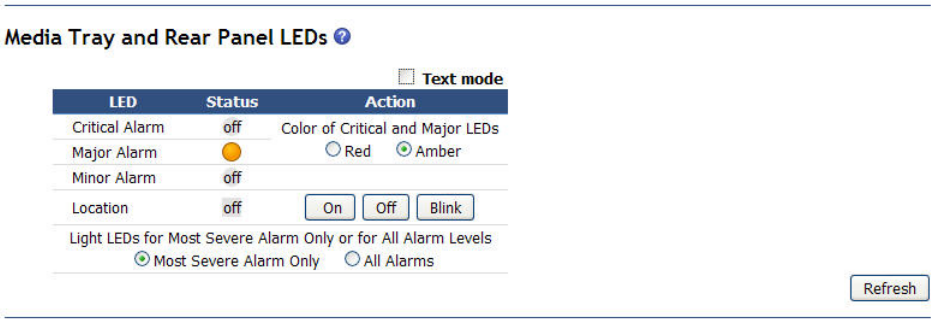
  Klicken Sie beim erweiterten Managementmodul auf den Namen des Blade-Servers, um den Status der Light Path Diagnostics-Anzeigen für den Blade-Server anzuzeigen. (Die aufgeführten Anzeigen hängen vom Typ des Blade-Servers ab.) In der folgenden Abbildung ist ein Beispiel für die Light Path Diagnostics-Anzeigen dargestellt, die auf der Seite **Blade LED Details** (Details zu Bladeanzeigen) aufgeführt werden.

- **I/O-Module LEDs** (E/A-Modulanzeigen): Der Status der Anzeigen auf einigen E/A-Modulen. Bei manchen E/A-Modulen werden möglicherweise auch simulierte E/A-Modulanzeigen unterstützt. Diese basieren auf den Statusinformationen des E/A-Moduls, wie z. B. dem Portverbindungsstatus. Informationen hierzu finden Sie im Abschnitt zur Option **I/O Module Tasks → Configuration** (E/A-Modul-Tasks → Konfiguration). Der Status simulierter Anzeigen wird aus Statusbedingungen abgeleitet und gibt nicht den Status einer tatsächlichen Anzeige an.
- **Storage Unit LEDs** (Anzeigen von Speichereinheiten): (nur BladeCenter S-Einheit) Der Status der Speichereinheiten.

- **Power module cooling devices LEDs** (Anzeigen der Kühleinheiten für Stromversorgungsmodule) (nur erweiterte Managementmodule, die in einer BladeCenter H-Einheit installiert sind): Der Status der Fehleranzeige auf jedem Lüftersatz für Stromversorgungsmodule.
- **Chassis cooling devices LEDs** (Anzeigen der Gehäusekühleinheiten) (nur erweiterte Managementmodule, die in einer BladeCenter H-Einheit installiert sind): Der Status der Fehleranzeige auf jeder Kühleinheit der BladeCenter-Einheit.

BladeCenter T- und BladeCenter HT-Alarmverwaltung:

Wählen Sie **Monitors → LEDs** (Monitore → Anzeigen) aus, um für die BladeCenter T- und BladeCenter HT-Einheiten Alarme anzuzeigen und zu verwalten.



Wählen Sie **LEDs** (Anzeigen) aus, um den Status der Anzeigen auf der BladeCenter T- oder BladeCenter HT-Systemstatusseite und der Bedienfeldanzeigen des Blade-Servers anzuzeigen. Mithilfe dieser Option können Sie auch die Positionsanzeige an der BladeCenter-Einheit und den Blade-Servern einschalten, ausschalten oder auf blinkend schalten oder festlegen, wie die Anzeigen auf Alarme reagieren sollen.

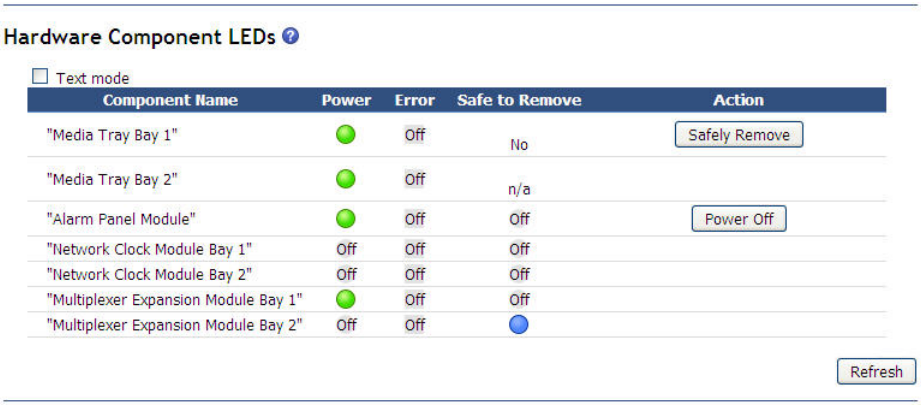
Die folgenden Informationen werden angezeigt:

- **Media Tray and Rear Panel LEDs** (Laufwerkschlitten- und Rückwandanzeigen): Hier wird der Status der folgenden Anzeigen in der BladeCenter T- oder BladeCenter HT-Systemstatusanzeige festgelegt und angezeigt:
  - Critical Alarm (Alarm für kritischen Systemfehler, CRT LED)
  - Major Alarm (Alarm für schwerwiegenden Systemfehler, MJR LED)
  - Minor Alarm (Alarm für geringfügigen Systemfehler, MNR LED)
  - Position

  Sie können den Status der Positionsanzeige ändern und für die Alarmanzeigen für kritische oder schwerwiegende Systemfehler die Farbe für aktive Anzeigen auswählen (rot oder bernsteinfarben). Diese Farbauswahl wird auf die Anzeigen an der Vorderseite und Rückseite der BladeCenter T- oder BladeCenter HT-Einheit und auf die Anzeigengruppe angewendet, die auf dieser Seite dargestellt werden. Sie können zudem auch festlegen, ob das Managementmodul für alle auftretenden Alarmstufen (kritisch, schwerwiegend oder geringfügig) Anzeigen aufleuchten lässt oder ob das Modul nur die Anzeige aufleuchten lässt, die der Alarmstufe für die schwerwiegendsten Systemfehler entspricht. Bernsteinfarben ist die Standardfarbe der Alarmanzeigen für kritische und schwerwiegende Systemfehler. Darüber hinaus wird für das Managementmodul festgelegt, dass es standardmäßig die Anzeigen für alle auftretenden Alarmstufen (kritisch, schwerwiegend oder geringfügig) aufleuchten lässt.
- **Set Alarm Panel LEDs** (Systemstatusanzeigen festlegen): Sie können den Status der Anzeigen an der Vorderseite und Rückseite der BladeCenter T- oder BladeCenter HT-Einheit mithilfe der Alarmdatenbank des Managementmoduls festlegen. Um eine benutzerdefinierte Festlegung zu ermöglichen, können zur Alarmdatenbank Alarme hinzugefügt werden. Um einen Alarm hinzuzufügen, wählen Sie den Schweregrad des Alarms aus, durch den bestimmt wird, welche Anzeige durch den Alarm angesteuert wird, und geben Sie eine Alarmbeschreibung ein.

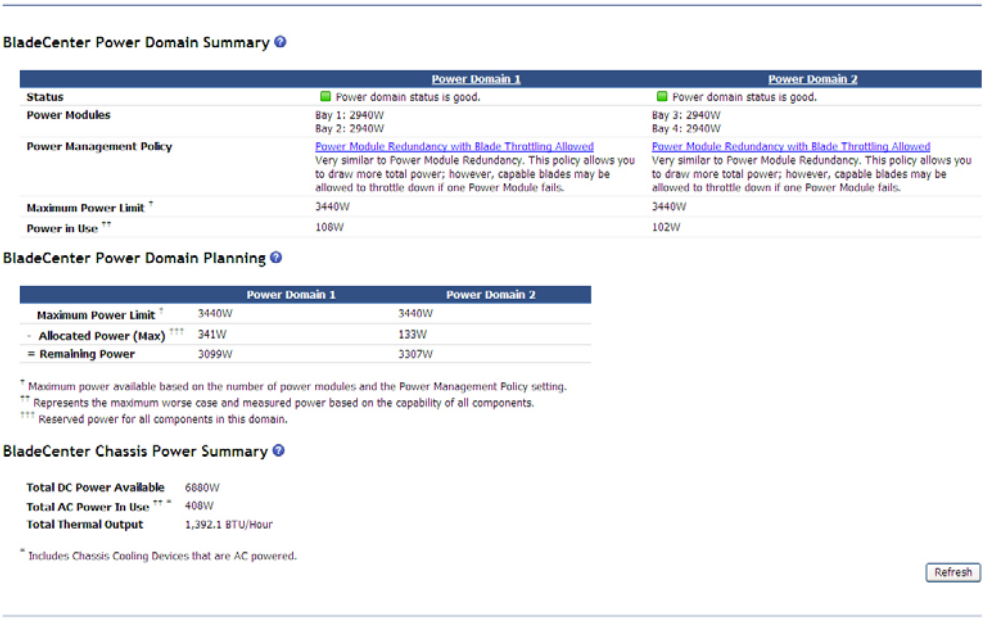
Dabei darf die Beschreibung nicht leer bleiben. Klicken Sie anschließend auf **Set** (Festlegen). Nach dem Hinzufügen eines Alarms zur Datenbank können Sie den Alarm und die zugehörige Anzeige über die Seite "System Status" (Systemstatus) mithilfe der Schaltflächen "ACK" (Bestätigen) und "CLEAR" (Löschen) verwalten. (Informationen hierzu finden Sie im Abschnitt „System Status (Systemstatus)" auf Seite 105.)

- **Blade LEDs** (Blade-Anzeigen): Der Status der folgenden Anzeigen im Anzeigenfeld des Blade-Servers. Sie können den Status der Informations- und der Positionsanzeige ändern.
  - Stromversorgung
  - Fehler
  - Informationen
  - Auswahl von Tastatur, Bildschirm und Maus
  - Datenträgerauswahl (optisches Laufwerk und USB-Anschluss)
  - Position
- **I/O-Module LEDs** (Anzeigen an E/A-Modulen): Der Status der Anzeigen an einigen E/A-Modulen.
- **Hardware Component LEDs** (Anzeigen der Hardwarekomponenten): Der Status der Anzeigen an einigen BladeCenter-Hardwarekomponenten. Einige Komponenten enthalten die Anzeige "FRU bereit zum Entfernen". Der Status dieser Anzeige wird in der Spalte "Safe to Remove" (Kann sicher entfernt werden) angezeigt. Bei BladeCenter HT-Gehäusen können Sie in den Laufwerkschlitten CompactFlash-Karten anschließen, um die Kapazität des lokalen Speichers im erweiterten Managementmodul zu erweitern. Auf diese Weise können Sie mithilfe der Funktion für ferne Datenträger größere ISO-/Imagedateien hochladen. Um die Integrität des Dateisystems auf CompactFlash-Karten sicherzustellen, bereiten Sie den Laufwerkschlitten auf das Entfernen vor. Klicken Sie hierzu zunächst auf die Schaltfläche **Safely Remove** (Sicher entfernen). Sobald für **Safe to Remove** (Kann sicher entfernt werden) **Yes** (Ja) angezeigt wird, können Sie den Laufwerkschlitten entfernen. Wenn der Laufwerkschlitten den Status "Safe to Remove" (Kann sicher entfernt werden) aufweist und Sie sich anders entscheiden, können Sie auf die Schaltfläche **Re-Enable** (Erneut aktivieren) klicken, um das Dateisystem erneut auf die CompactFlash-Karten zu laden.



Power Management (Stromverbrauchssteuerung)

Wählen Sie **Monitors → Power Management** (Monitore → Stromverbrauchssteuerung) aus, um die Stromversorgungsinformationen auf Basis des vorausberechneten Stromverbrauchs für jede Stromversorgungsdomäne anzuzeigen und um die Stromverbrauchssteuerung für die BladeCenter-Einheit zu konfigurieren.



In den meisten BladeCenter-Einheiten gibt es zwei Stromversorgungsdomänen.

Anmerkung: Die BladeCenter S-Einheit weist nur eine Stromversorgungsdomäne auf. Bei einer BladeCenter S-Einheit wird in der Tabelle auf der Seite **Power Management** (Stromverbrauchssteuerung) nur eine Stromversorgungsdomäne angezeigt. Außerdem enthält die Tabelle eine zusätzliche Zeile mit der Angabe, ob die Einheit mit 110 V Wechselstrom oder 220 V Wechselstrom versorgt wird.

Klicken Sie auf **Power Domain 1 details** (Details zu Stromversorgungsdomäne 1) oder auf **Power Domain 2 details** (Details zu Stromversorgungsdomäne 2), um eine Liste der BladeCenter-Komponenten in jeder Stromversorgungsdomäne anzuzeigen (Informationen hierzu finden Sie im Abschnitt „Ausführliche Informationen zur Stromversorgung" auf Seite 127). Über die Richtlinieneinstellungen für die Stromverbrauchssteuerung wird festgelegt, wie die BladeCenter-Einheit in jeder Stromversorgungsdomäne reagiert, wenn eine Stromquelle oder ein Stromversorgungsmodul ausfällt. Die Kombination, die sich aus der BladeCenter-Konfiguration, den Richtlinieneinstellungen für die Stromverbrauchssteuerung und dem verfügbaren Strom ergibt, führt möglicherweise dazu, dass die Leistungsstufe von Blade-Servern reduziert (gedrosselt) wird oder dass Blade-Server nicht eingeschaltet werden.

In den Abschnitten **BladeCenter Power Domain Summary** (Zusammenfassung für BladeCenter-Stromversorgungsdomänen), **BladeCenter Power Domain Planning** (Planung für BladeCenter-Stromversorgungsdomänen) und **BladeCenter Chassis Power Summary** (Zusammenfassung für BladeCenter-Gehäusestromversorgung) werden die folgenden Informationen zum Stromversorgungsstatus angezeigt:

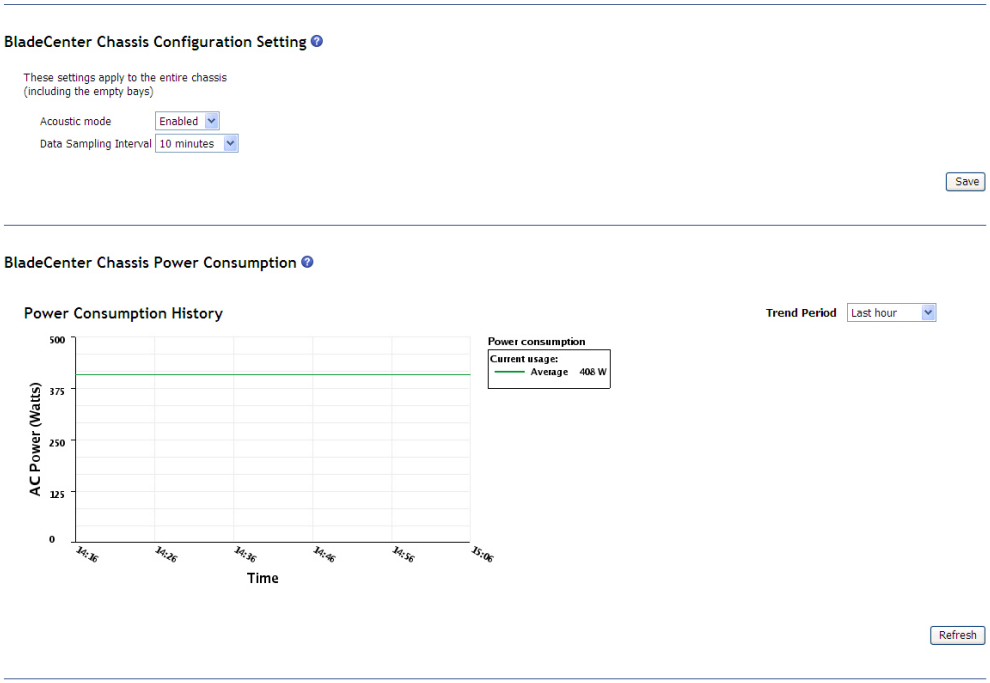
- **Status** (Status): Dieses Feld enthält ein farbcodiertes Symbol, das den Status der Stromversorgungsdomänen angibt, sowie eine kurze Statusbeschreibung mit allen ausstehenden Problemen, die den Stromverbrauch oder die Redundanz in den einzelnen Stromversorgungsdomänen betreffen.
- **Power Modules** (Stromversorgungsmodule): In diesem Feld sind die Stromversorgungsmodule in jeder Stromversorgungsdomäne mit ihrer jeweiligen Nennkapazität in Watt aufgelistet.
- **Power-Management Policy** (Richtlinie für Stromverbrauchssteuerung): In diesem Feld wird die Richtlinie für die Stromverbrauchssteuerung angezeigt, die für jede Stromversorgungsdomäne festgelegt wurde. In dieser Richtlinie ist definiert, wie die Stromversorgungsdomäne auf Bedingungen reagiert, die möglicherweise zu einem Verlust der Redundanz führen. Diese Einstellung wird auf der Seite **Blade Tasks → Configuration** (Blade-Tasks → Konfiguration) konfiguriert (Informationen hierzu finden Sie im Abschnitt „Configuration (Konfiguration)" auf Seite 149).
- **Maximum Power Limit** (Maximaler Strom): In diesem Feld wird die Strommenge in Watt angezeigt, die in jeder Stromversorgungsdomäne zur Verfügung steht. Das erweiterte Managementmodul berechnet die Gesamtstrommenge anhand der Nennkapazitäten der Stromversorgungsmodule, die in einer Stromversorgungsdomäne installiert sind, und anhand der Richtlinie für die Stromverbrauchssteuerung dieser Stromversorgungsdomäne.
- **Power in Use** (Verwendeter Strom): In diesem Feld wird die Strommenge in Watt angezeigt, die derzeit in den einzelnen Stromversorgungsdomänen genutzt wird. In der Regel verbraucht ein Modul weniger Strom als die maximale zugeordnete Strommenge. Aus diesem Grund liegt der tatsächliche Gesamtstromverbrauch des Gehäuses möglicherweise unter der in diesem Feld angezeigten Menge.
- **Allocated Power (Max)** (Zugeordnete Strommenge (Max)): In diesem Feld wird die Gesamtstrommenge in Watt angezeigt, die für die in einer Stromversorgungsdomäne installierten Komponenten reserviert ist. Dieser Wert enthält möglicherweise die Stromversorgung von Komponenten, die derzeit nicht in der BladeCenter-Einheit installiert sind, wie z. B. die E/A-Module. Für diese Komponenten ist Strom reserviert, weil das Managementmodul den Strom für einige Komponenten, die normalerweise für den Betrieb einer BladeCenter-Einheit erforderlich sind, im Voraus zuweist. Die reservierte Gesamtstrommenge enthält möglicherweise auch Strom für Komponenten, die in der BladeCenter-Einheit installiert sind, die sich im Bereitschaftsstatus befinden und die nicht eingeschaltet sind. Diese Komponenten werden in die Gesamtmenge aufgenommen, damit die übrige (nicht zugeordnete) Strommenge in der Stromversorgungsdomäne genau berechnet werden kann.

  Anmerkung: Bei der zugeordneten maximalen Strommenge für Module wird vom ungünstigsten Stromverbrauch ausgegangen, den das Modul aufweisen kann. Die verwendete Strommenge entspricht bei einigen Modulen, darunter E/A-Module, die Mittelplatine und das Managementmodul, der maximalen zugeordneten Strommenge, wenn das Modul eingeschaltet ist. In der Regel verbraucht ein Modul weniger Strom als die maximale zugeordnete Strommenge.

Daher liegt der tatsächliche Gesamtstromverbrauch des Gehäuses möglicherweise unter der Menge, die im Feld **Power in Use** (Verwendeter Strom) angezeigt wird.

- **Remaining Power** (Verbleibender Strom): In diesem Feld wird die nicht zugeordnete (übrige) Strommenge einer Stromversorgungsdomäne in Watt angezeigt. Mithilfe dieses Werts bestimmt das Managementmodul, ob ein neu installiertes Modul eingeschaltet werden soll. Die verbleibende Strommenge wird anhand der Gesamtstrommenge und der reservierten Strommenge für jede Stromversorgungsdomäne berechnet.
- **Total DC Power Available** (Gesamter verfügbarer Gleichstrom): In diesem Feld wird die Gesamtmenge an Gleichstrom angezeigt, die für die gesamte BladeCenter-Einheit zur Verfügung steht. Dabei handelt es sich um die Summe der Nennwerte für beide Stromversorgungsdomänen.
- **Total AC Power In Use** (Gesamter verwendeter Wechselstrom): In diesem Feld wird die gesamte Wechselstrommenge angezeigt, die derzeit von allen Modulen in der BladeCenter-Einheit verbraucht wird. Bei BladeCenter H-Einheiten wird auch die von den Lüftern verbrauchte Strommenge einberechnet.
- **Total Thermal Output** (Gesamte Wärmeabgabe): In diesem Feld wird die Wärmeabgabe (-last) der BladeCenter-Einheit in BTU/h angezeigt. Der Wert wird anhand der gesamten verwendeten Wechselstrommenge berechnet.

Auf dieser Seite können Sie auch die Reaktion der BladeCenter-Einheit auf Temperaturüberschreitungen konfigurieren, das Stichprobenintervall für Stromversorgungsdaten festlegen und eine Grafik zum Stromverbrauch der BladeCenter-Einheit anzeigen. Außerdem können Sie den NEBS-Betriebsmodus für BladeCenter T- und BladeCenter HT-Einheiten aktivieren oder inaktivieren.

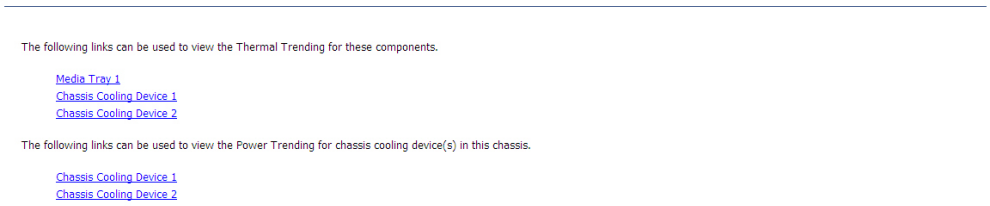


Im Abschnitt **BladeCenter Chassis Configuration Setting** (Konfigurationseinstellung für BladeCenter-Gehäuse) legen Sie fest, wie das Managementmodul reagiert, wenn eine Temperaturüberschreitung (ein Wärmeereignis) auf einem Blade-Server eintritt. Als Reaktion auf Wärmeereignisse werden die folgenden Optionen des geräuscharmen Modus unterstützt:

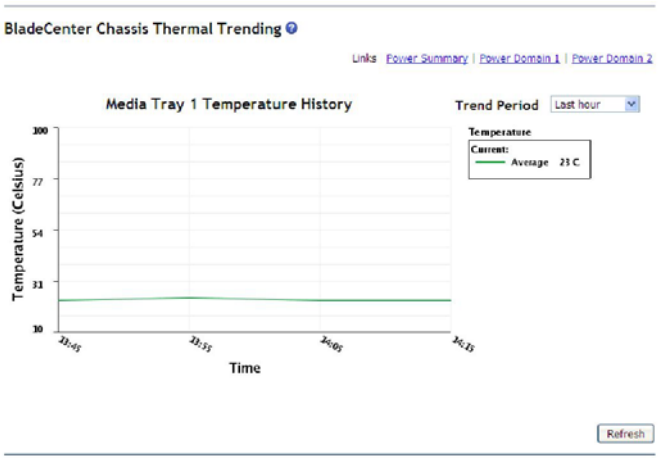
- **Network Equipment-Building System (NEBS) mode** (NEBS-Modus (Network Equipment-Building System)) (nur BladeCenter T- und BladeCenter HT-Einheiten): Mit diesem Kontrollkästchen können Sie den NEBS-Modus aktivieren oder inaktivieren (weitere Informationen dazu finden Sie im Abschnitt „Unterstützung für NEBS-Modus" auf Seite 96).
- **Acoustic mode** (Geräuscharmer Modus):
  - **Disabled** (Inaktiviert) (Standardeinstellung): Die Lüftergeschwindigkeit wird nach Bedarf erhöht, um für zusätzliche Kühlung zu sorgen.
  - **Enabled** (Aktiviert): Der Stromverbrauch der Blade-Server wird reduziert (die Blade-Server werden gedrosselt), um einen bestimmten Geräuschpegel nicht zu überschreiten. Diese Option betrifft nur die BladeCenter-Komponenten, die eine Stromregulierung unterstützen.

    Anmerkung: Um den geräuscharmen Modus für BladeCenter T- und BladeCenter HT-Einheiten zu aktivieren, müssen Sie den NEBS-Modus inaktivieren.
- **Data Sampling Interval** (Datenerhebungsintervall): Dieser Wert legt fest, wie häufig die Stromversorgungsdaten für die Trendermittlung zusammengestellt werden.

Klicken Sie auf die Links unten auf der Seite, um die Wärmetrendinformationen für einzelne BladeCenter-Komponenten anzuzeigen. Die überwachten und aufgelisteten Komponenten hängen vom Typ der BladeCenter-Einheit ab.



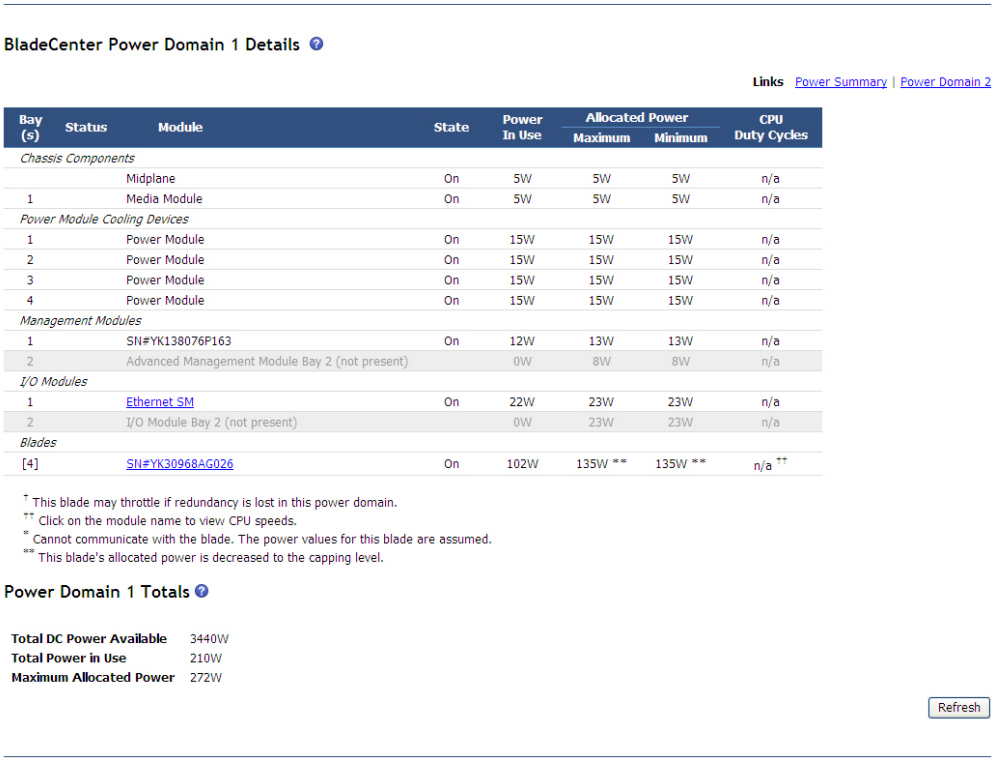
In der folgenden Abbildung sind beispielhaft die Informationen zur Laufwerkschlittentemperatur dargestellt.



Ausführliche Informationen zur Stromversorgung:

Wählen Sie **Monitors → Power Management → Power Domain Summary** (Monitore → Stromverbrauchssteuerung → Zusammenfassung der Stromversorgungsdomäne) aus, um ausführliche Informationen zum Stromversorgungsstatus für die einzelnen überwachten BladeCenter-Komponenten anzuzeigen.

Die BladeCenter-Komponenten, die Teil einer Stromversorgungsdomäne sind, sind nach Typ gruppiert. Es werden die Informationen zur Stromversorgungsdomäne 1 angezeigt. Für jede Stromversorgungsdomäne in Ihrer BladeCenter-Einheit wird eine eigene Statusseite angezeigt. Auf dieser Seite können Sie darüber hinaus auch konfigurieren, wie die Stromversorgungsdomäne auf den Verlust von Stromversorgungsredundanz reagieren soll, und eine Abbildung zum Stromverbrauch für die Stromversorgungsdomäne anzeigen (ähnlich der Abbildung zum Stromverbrauch der BladeCenter-Einheit). Siehe „Power Management (Stromverbrauchssteuerung)" auf Seite 123.



BladeCenter Power Domain 1 Details

Links Power Summary | Power Domain 2

Bay (s)	Status	Module	State	Power In Use	Allocated Power		CPU Duty Cycles
					Maximum	Minimum	
Chassis Components							
		Midplane	On	5W	5W	5W	n/a
1		Media Module	On	5W	5W	5W	n/a
Power Module Cooling Devices							
1		Power Module	On	15W	15W	15W	n/a
2		Power Module	On	15W	15W	15W	n/a
3		Power Module	On	15W	15W	15W	n/a
4		Power Module	On	15W	15W	15W	n/a
Management Modules							
1		SN#YK138076P163	On	12W	13W	13W	n/a
2		Advanced Management Module Bay 2 (not present)		0W	8W	8W	n/a
I/O Modules							
1		Ethernet SM	On	22W	23W	23W	n/a
2		I/O Module Bay 2 (not present)		0W	23W	23W	n/a
Blades							
[4]		SN#YK30968AG026	On	102W	135W **	135W **	n/a ††

† This blade may throttle if redundancy is lost in this power domain.
†† Click on the module name to view CPU speeds.
* Cannot communicate with the blade. The power values for this blade are assumed.
** This blade's allocated power is decreased to the capping level.

Power Domain 1 Totals

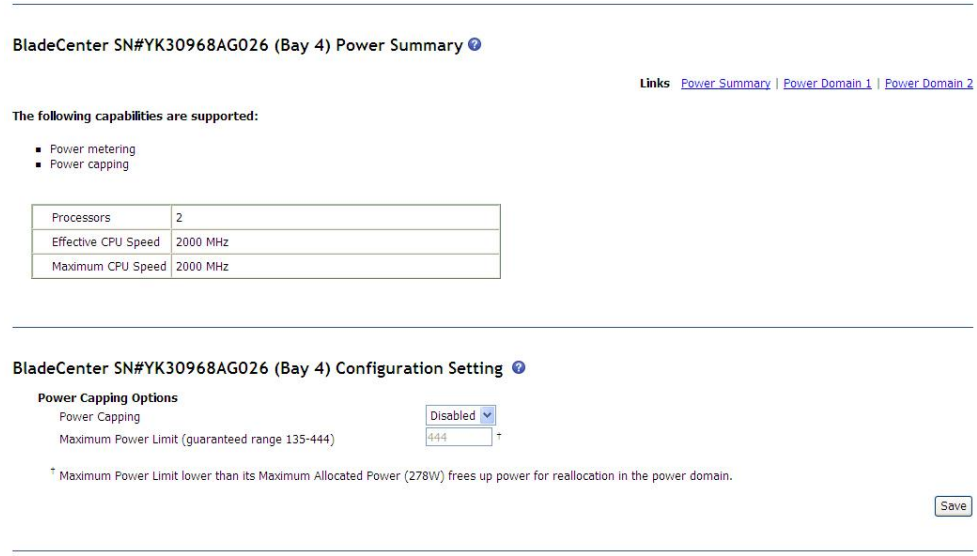
Total DC Power Available	3440W
Total Power in Use	210W
Maximum Allocated Power	272W

Refresh

Die folgenden Informationen werden für Komponenten angezeigt, die in einer Stromversorgungsdomäne installiert sind:

- **Bay** (Position): In diesem Feld werden ggf. die Positionen angezeigt, die von einer BladeCenter-Komponente belegt werden. Hier wird zudem angezeigt, ob ein Blade-Server im Falle des Verlusts der Stromversorgungsredundanz seinen Stromverbrauch reduzieren (regulieren) kann.
- **Status** (Status): In diesem Feld wird ein Symbol angezeigt, das für die Komponente ausstehende Ereignisse der Stromverbrauchssteuerung anzeigt. Das Symbol gibt an, dass ein Blade-Server nicht eingeschaltet werden kann, weil in der Stromversorgungsdomäne nicht genügend Reststrom zu dessen Unterstützung vorhanden ist. Das Symbol gibt an, dass ein Blade-Server derzeit seinen Stromverbrauch reduziert (reguliert), um die redundante Stromversorgung in einer Stromversorgungsdomäne aufrecht zu erhalten.
- **Module** (Modul): In diesem Feld wird die Beschreibung der Komponente angezeigt. Einige BladeCenter-Komponenten stellen zusätzliche Informationen zur Stromversorgung bereit. Bei der Beschreibung der einzelnen Komponenten handelt es sich um einen Link. Wenn Sie auf diesen klicken, wird eine Abbildung mit weiteren ausführlichen Informationen zur Stromversorgung für die Komponente angezeigt. In der Abbildung können Sie die Art der Stromversorgungsinformationen auswählen, die angezeigt werden sollen: durchschnittliche, maximale oder minimale Stromversorgung. Klicken Sie bei Blade-Servern auf den Modulnamen, um Informationen zur Leistung des Mikroprozessors anzuzeigen.

Bei Blade-Servern mit Funktionen zur Konfiguration der Stromversorgung zeigt das Managementmodul Felder an, mit deren Hilfe Sie die Begrenzungsfunktion für die Stromversorgung aktivieren oder inaktivieren und die maximale Stromversorgungskapazität für Blade-Server festlegen können. Diese Felder werden nur bei Blade-Servern angezeigt, die diese erweiterten Funktionen unterstützen.



Das erweiterte Managementmodul zeigt Informationen zur zugeordneten Stromversorgung sowie zum Begrenzungsbereich der Stromversorgung für einzelne Blade-Server an.

- Die zugeordnete maximale Stromversorgung ist ein typischer Maximalwert der Stromversorgung für verschiedene Konfigurationen. Er wird vom erweiterten Managementmodul verwendet, um zu ermitteln, ob ein Blade-Server in das Stromversorgungsbudget der Domäne passt. Wenn das Stromversorgungsbudget genügend Reserven für die Unterstützung des Blade-Servers aufweist, schaltet das Managementmodul den Blade-Server ein.
- Die maximale Stromversorgung im Begrenzungsbereich der Stromversorgung gibt die Stromversorgung auf dem Typenschild für den Blade-Server an. Dieser Wert ist nicht derselbe wie der Wert für die zugeordnete maximale Stromversorgung.

Der Wert für die Begrenzung der maximalen Stromversorgung kann für einzelne Blade-Server festgelegt werden. Bei diesem Wert, der in Watt angegeben wird,

handelt es sich um den Stromversorgungswert, auf den ein Blade-Server durch die Stromverbrauchssteuerung des erweiterten Managementmoduls begrenzt wird. Der Wert für die Begrenzung der maximalen Stromversorgung gilt für alle Ein- und Ausschaltvorgänge bei Blade-Servern.

Einige Server-Blades wie die JS12- und JS22-Blades unterstützen eine Funktion zur eingeschränkten Begrenzung der Stromversorgung. Wenn diese Funktion unterstützt wird, werden auf der Webseite der Bereich und der garantierte Bereich angezeigt.

- Der **Bereich** wird als eingeschränkter Minimal- und Maximalwert für die Begrenzung angezeigt.
- Der **garantierte Bereich** wird als Minimal- und Maximalwert für die Begrenzung angezeigt. Bei früheren Releases der Firmware des erweiterten Managementmoduls wurde dies als der Begrenzungsbereich bezeichnet.

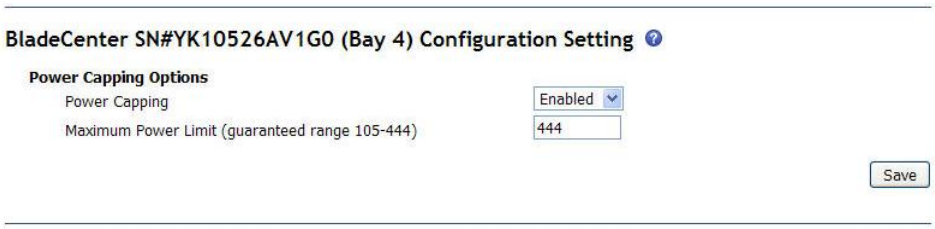
Einige Server-Blades wie die JS12- und JS22-Blades unterstützen die dynamische Energiesparfunktion Dynamic Power Saver. Hierbei handelt es sich um einen Energiesparmodus, mit dessen Hilfe der Blade-Server seine Betriebsspannung und Frequenz gezielt ändern kann, um den Stromverbrauch zu reduzieren. Ausführliche Informationen hierzu finden Sie in der Dokumentation zum Server. Die folgenden Bedingungen gelten für diese Funktion.

- Die Einstellung **Dynamic Power Saver** (Dynamische Energiesparfunktion) wird nur angezeigt, wenn der Blade-Server eingeschaltet ist.
- Der **garantierte Bereich** wird als Minimal- und Maximalwert für die Begrenzung angezeigt. Bei früheren Releases der Firmware des erweiterten Managementmoduls wurde dies als der Begrenzungsbereich bezeichnet.
- Die beiden Funktionen **Static Low Power Saver** (Statische Energiesparfunktion) und **Dynamic Power Saver** (Dynamische Energiesparfunktion) können nicht gleichzeitig aktiviert werden.
- Das Kontrollkästchen **Favor Performance over Power** (Leistung vor Stromversorgung) ist nur aktiv, wenn die Funktion **Dynamic Power Saver** (Dynamische Energiesparfunktion) ausgewählt wurde.

Einige Blade-Server unterstützen die dynamische Energiesparfunktion.

Anmerkung: Der Blade-Server muss eingeschaltet sein, damit die Optionen der Begrenzungsfunktion für die Stromversorgung verfügbar sind. Wenn ein Blade-Server aus einer BladeCenter-Einheit entfernt wird oder wenn die BladeCenter-Einheit ausgeschaltet wird, geht die Einstellung für die Begrenzung der maximalen Stromversorgung verloren.

Der durchschnittliche Stromverbrauch bei einem Blade-Server erreicht oder überschreitet den Grenzwert für die Begrenzung der minimalen Stromversorgung nicht regelmäßig. Beim Grenzwert für die Begrenzung der minimalen Stromversorgung handelt es sich um einen Wert, der unter allen Betriebsbedingungen garantiert werden kann. Der Gesamtstromverbrauch bei einem Blade-Server hängt von Bedingungen ab, die sich sowohl auf die Hardwarekonfiguration als auch auf die Anwendungen, die auf dem Blade-Server ausgeführt werden, beziehen können.



- **State** (Status): In diesem Feld wird der Stromversorgungsstatus des Moduls angezeigt (On (Ein) oder Standby (Standby)).
- **Power in Use** (Genutzte Stromversorgung): In diesem Feld wird die dem Modul zugeordnete Stromversorgungskapazität in Watt angezeigt. In der Regel nutzt ein Modul weniger als die maximal zugeordnete Stromversorgung. Daher kann der tatsächliche Gesamtstromverbrauch der BladeCenter-Einheit geringer sein als die in diesem Feld angezeigte Kapazität.
- **Maximum Allocated Power** (Maximal zugeordnete Stromversorgung): In diesem Feld wird die maximale Stromversorgungskapazität, die eine Komponente erfordert, in Watt angezeigt. Die maximal zugeordnete Stromversorgung für Module ist die Kapazität, die das Modul im ungünstigsten Fall nutzen kann, wobei der Wert für die genutzte Stromversorgung bei einigen Modulen wie bei E/A-Modulen, bei der Mittelplatine und beim Managementmodul beim Einschalten der maximal zugeordneten Stromversorgung entspricht. In der Regel nutzt ein Modul weniger als die maximal zugeordnete Stromversorgung. Daher kann der tatsächliche Gesamtstromverbrauch der BladeCenter-Einheit geringer sein als die im Feld **Power in Use** (Genutzte Stromversorgung) angezeigte Kapazität.
- **Minimum Allocated Power** (Mindestens zugeordnete Stromversorgung): In diesem Feld wird die minimale Stromversorgungskapazität, die ein Blade-Server, der auf niedrigster Leistungsstufe betrieben wird (vollständig gedrosselt), erfordert, in Watt angezeigt.
- **CPU Duty Cycles** (CPU-Arbeitszyklen): Dieses Feld bezieht sich nur auf Blade-Server. Hier wird der Arbeitszyklus der einzelnen Mikroprozessoren in einem Blade-Server als Prozentsatz des Vollbetriebs angezeigt. Die Arbeitszyklen der Mikroprozessoren werden durch Kommas voneinander getrennt. Für Blade-Server, die Arbeitszyklen nicht unterstützen oder dokumentieren, wird `n/a` (nicht zutreffend) angezeigt. Ein Arbeitszyklus ist das Verhältnis zwischen der tatsächlichen Prozessorzeit und der insgesamt verfügbaren Prozessorzeit in Prozent. Klicken Sie bei Blade-Servern auf den Modulnamen, um Informationen zur Leistung des Mikroprozessors anzuzeigen.
- **DOMAIN TOTALS** (DOMÄNE GESAMT): In diesen Feldern wird die Gesamtstromversorgung angezeigt, die allen Komponenten in der Stromversorgungsdomäne zugeordnet ist.

In diesem Abschnitt können Sie Einstellungen für die Richtlinie zur Stromverbrauchssteuerung konfigurieren. Die Einstellungen in diesem Abschnitt gelten für die gesamte BladeCenter-Einheit sowie für die leeren Bladepositionen. Damit Sie die Einstellungen für die Richtlinie zur Stromverbrauchssteuerung konfigurieren können, müssen Sie auf die BladeCenter-Einheit zugreifen können und Ihnen muss die Rolle für die Gehäusekonfiguration oder die Rolle des Systemadministrators zugewiesen sein. Die Einstellungen werden auf jede Stromversorgungsdomäne einzeln angewendet. Um eine korrekte Meldung von Stromversorgungsinformationen sicherzustellen, müssen die Firmware des Managementmoduls, die Firmware des Blade-Server-BIOS und die BSMP-Firmware (Blade Systems Management Processor) auf dem neuesten Stand sein.

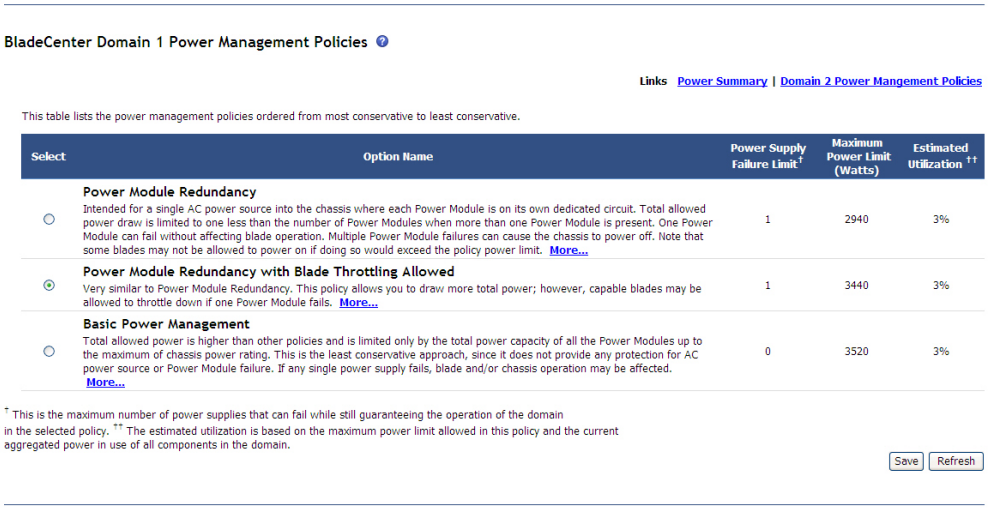
Die Regulierung eines Blade-Servers bewirkt, dass der Stromverbrauch eines Blade-Servers durch vorübergehende Reduzierung der Mikroprozessorleistung gesenkt wird. Das erweiterte Managementmodul und die Blade-Server nutzen in bestimmten Mikroprozessoren integrierte Technologien der Stromverbrauchssteuerung, um die Blade-Server zu regulieren und so einen geringeren Stromverbrauch zu erzielen.

Mithilfe von Regulierungsrichtlinien können Sie mehr von der Gesamtstromversorgung der BladeCenter-Einheit nutzen, sodass Sie mehr Blade-Server einschalten

können, als dies andernfalls möglich wäre. Blade-Server müssen möglicherweise auf einen geringeren Stromverbrauch reguliert werden, wenn ein Stromversorgungsmodul die BladeCenter-Einheit nicht betriebsbereit halten kann.

Beachten Sie den Unterschied zwischen einer *Netzstromquelle* und einem *Netzstromkreis*. Bei einer Netzstromquelle wird Strom von einer einzelnen Netzstation wie einem öffentlichen Energieversorgungsunternehmen, einem Generator vor Ort oder einer unterbrechungsfreien Stromversorgung bezogen. Bei einem Netzstromkreis stammt der Strom von einer Netzstromquelle und wird durch einen Trennschalter begrenzt. Die Nutzung dualer Netzstromquellen bedeutet, dass der Strom von mehreren Netzstationen bezogen wird. Auch wenn die meisten Serverinstallationen diese elektrische Konfiguration nicht aufweisen, sind einige Richtlinien für die Verwendung mit dualen Netzstromquellen vorgesehen. Unabhängig von der Anzahl der vorhandenen Netzstromquellen muss sich in Ihrer BladeCenter-Einheit für jedes Stromversorgungsmodul ein dedizierter Netzstromkreis befinden.

Der Name für die für die einzelnen Stromversorgungsdomänen geltenden Richtlinie ist ein Live-Link. Klicken Sie auf einen Link, um eine ausführlichere Erläuterung zur Richtlinie anzuzeigen und um die Richtlinie zu ändern.



BladeCenter Domain 1 Power Management Policies

Links Power Summary | Domain 2 Power Mangement Policies

This table lists the power management policies ordered from most conservative to least conservative.

Select	Option Name	Power Supply Failure Limit†	Maximum Power Limit (Watts)	Estimated Utilization ††
○	**Power Module Redundancy** Intended for a single AC power source into the chassis where each Power Module is on its own dedicated circuit. Total allowed power draw is limited to one less than the number of Power Modules when more than one Power Module is present. One Power Module can fail without affecting blade operation. Multiple Power Module failures can cause the chassis to power off. Note that some blades may not be allowed to power on if doing so would exceed the policy power limit. More...	1	2940	3%
◉	**Power Module Redundancy with Blade Throttling Allowed** Very similar to Power Module Redundancy. This policy allows you to draw more total power; however, capable blades may be allowed to throttle down if one Power Module fails. More...	1	3440	3%
○	**Basic Power Management** Total allowed power is higher than other policies and is limited only by the total power capacity of all the Power Modules up to the maximum of chassis power rating. This is the least conservative approach, since it does not provide any protection for AC power source or Power Module failure. If any single power supply fails, blade and/or chassis operation may be affected. More...	0	3520	3%

† This is the maximum number of power supplies that can fail while still guaranteeing the operation of the domain in the selected policy. †† The estimated utilization is based on the maximum power limit allowed in this policy and the current aggregated power in use of all components in the domain.

Save Refresh

Die folgenden Richtlinien zur Stromverbrauchssteuerung gelten für die BladeCenter-Einheiten E, H, T, HT und S:

- **Basic Power Management** (Allgemeine Stromverbrauchssteuerung; Standardeinstellung): Diese Richtlinie gilt, wenn die BladeCenter-Einheit der empfohlenen Konfiguration für die anderen Stromversorgungsrichtlinien nicht entspricht. Blade-Server werden eingeschaltet, vorausgesetzt, die genutzte Stromversorgung ist geringer oder gleich dem Grenzwert für die maximale Stromversorgung für diese Richtlinie. Der Wert für die insgesamt verfügbare Stromversorgung ist für diese Richtlinie größer als für andere Richtlinien und wird durch die Kapazität aller Stromversorgungsmodule bis zur maximalen Einstufung der Stromversorgungsdomäne der BladeCenter-Einheit begrenzt. Die Einstufung der Stromversorgungsdomäne der BladeCenter-Einheit kann geringer sein als die Gesamtsumme der Kapazität aller Stromversorgungsmodule. Dies ist die am wenigsten konservative Richtlinie für die Stromverbrauchssteuerung der BladeCenter-Einheit.

  Anmerkung: Wenn ein Stromversorgungsmodul ausfällt, können regulierungsfähige Mikroprozessoren in Blade-Servern den Stromverbrauch in der Stromversorgungsdomäne durch Regulierung reduzieren. Stromversorgungsredundanz ist

nicht garantiert und kann zu einem vollständigen Stromausfall in der Domäne führen, wenn die derzeitige Stromversorgung die Kapazität des verbleibenden Stromversorgungsmoduls übersteigt.

- **Power-Module Redundancy** (Redundante Stromversorgungsmodule): Diese Richtlinie gilt, wenn in der BladeCenter-Einheit eine einzelne Netzstromquelle genutzt wird, wobei sich jedes Stromversorgungsmodul in einem eigenen dedizierten Netzstromkreis befindet. Der Grenzwert für die innerhalb der Stromversorgungsdomäne maximal zugeordnete Stromversorgung entspricht der Anzahl der Stromversorgungsmodule minus eins, wenn mehr als ein Stromversorgungsmodul installiert ist. So kann ein Stromversorgungsmodul ausfallen, ohne dass der Betrieb von Blade-Servern beeinträchtigt wird. Wenn mehrere Stromversorgungsmodule ausfallen, kann dies zur Folge haben, dass alle Komponenten in der Stromversorgungsdomäne ausgeschaltet werden. Blade-Server werden nur eingeschaltet, wenn sie ungedrosselt betrieben werden können, auch wenn ein Stromversorgungsmodul ausfällt. Die Anzahl der Blade-Server, die eingeschaltet werden können, wird durch die Gesamtstromversorgung bestimmt, die von der Gesamtzahl der Stromversorgungsmodule minus eins maximal bereitgestellt werden kann. Wenn ein Stromversorgungsmodul ausfällt, werden alle eingeschalteten Blade-Server mit ungedrosselter Leistungsstufe weiter betrieben. Wenn zwei oder mehr Stromversorgungsmodule ausfallen, werden die Komponenten in der Stromversorgungsdomäne möglicherweise ausgeschaltet.
- **Power Module Redundancy with Blade Throttling Allowed** (Redundante Stromversorgungsmodule mit Blade-Regulierung): Diese Richtlinie gilt, wenn in der BladeCenter-Einheit eine einzelne Netzstromquelle genutzt wird, wobei sich jedes Stromversorgungsmodul in einem eigenen dedizierten Netzstromkreis befindet. Der Grenzwert für die innerhalb der Stromversorgungsdomäne maximal zugeordnete Stromversorgung entspricht der Anzahl der Stromversorgungsmodule minus eins, wenn mehr als ein Stromversorgungsmodul installiert ist. Der Ausfall eines Stromversorgungsmoduls kann dazu führen, dass Blade-Server gedrosselt werden, die Stromversorgungsdomäne bleibt jedoch betriebsbereit. Wenn mehrere Stromversorgungsmodule ausfallen, kann dies zur Folge haben, dass alle Komponenten in der Stromversorgungsdomäne ausgeschaltet werden. Mithilfe dieser Richtlinie können die Komponenten insgesamt mehr Strom ziehen als durch die Richtlinie für redundante Stromversorgungsmodule unterstützt wird. Mit dieser Richtlinie ist es ggf. möglich, Blade-Server einzuschalten, die mit einer restriktiveren Richtlinie nicht eingeschaltet werden könnten. Die Richtlinie hat jedoch möglicherweise den Nebeneffekt, dass Blade-Server den Stromverbrauch drosseln müssen, wenn ein Stromversorgungsmodul ausfällt, damit die Stromversorgungsdomäne betriebsbereit bleibt. Die Regulierung eines Blade-Servers bewirkt, dass der Stromverbrauch eines Blade-Servers durch vorübergehende Reduzierung der Mikroprozessorleistung gesenkt wird. Das Managementmodul und die Blade-Server nutzen in bestimmten Mikroprozessoren integrierte Technologien der Stromverbrauchssteuerung, um die Blade-Server zu regulieren und so einen geringeren Stromverbrauch zu erzielen. Nicht alle Blade-Server sind regulierungsfähig. Blade-Server können eingeschaltet werden, vorausgesetzt, die genutzte Stromversorgung ist geringer oder gleich dem Grenzwert für die maximale Stromversorgung für diese Richtlinie. Wenn ein Stromversorgungsmodul ausfällt, können regulierungsfähige Prozessoren in Blade-Servern den Stromverbrauch durch Regulierung auf einen Wert kleiner oder gleich der angegebenen Kapazität der Stromversorgungsmodule reduzieren. Blade-Server werden in einigen Konfigurationen in gedrosseltem Zustand eingeschaltet. Wenn die Stromversorgungsredundanz wiederhergestellt wird, kehren die Mikroprozessoren der Blade-Server wieder zur ungedrosselten Leistungsstufe zurück.

Die BladeCenter-S-Einheit unterstützt zwei weitere Optionen für Richtlinien zur Stromverbrauchssteuerung:

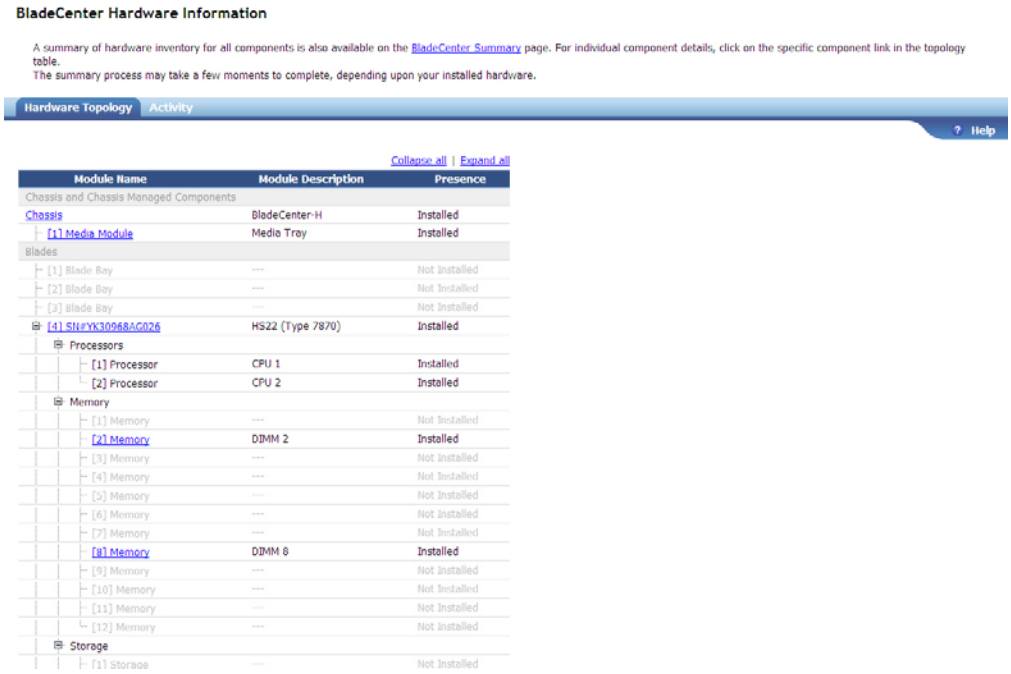
- **AC Power Source Redundancy** (Redundante Netzstromquellen): Diese Richtlinie gilt, wenn in der BladeCenter-Einheit zwei Netzstromquellen genutzt werden. Der Grenzwert für die innerhalb der Stromversorgungsdomäne maximal zugeordnete Stromversorgung entspricht der maximalen Kapazität von zwei Stromversorgungsmodulen. Hierbei handelt es sich um die konservativste Richtlinie, die empfohlen wird, wenn alle vier Stromversorgungsmodule installiert sind. Wenn die BladeCenter-Einheit ordnungsgemäß mit zwei Netzstromquellen verdrahtet ist, kann eine Netzstromquelle ausfallen, ohne dass der Blade-Server-Betrieb beeinträchtigt wird. Einige Blade-Server können möglicherweise nicht eingeschaltet werden, wenn dadurch der Grenzwert für die maximale Stromversorgung dieser Richtlinie überschritten würde.
- **AC Power Source Redundancy with Blade Throttling Allowed** (Redundante Netzstromquellen mit Blade-Regulierung): Diese Richtlinie gilt, wenn in der BladeCenter-Einheit zwei Netzstromquellen genutzt werden. Der Grenzwert für die innerhalb der Stromversorgungsdomäne maximal zugeordnete Stromversorgung entspricht der maximalen Kapazität von zwei Stromversorgungsmodulen. Hierbei handelt es sich um eine konservative Richtlinie für die Verwendung, wenn alle vier Stromversorgungsmodule installiert sind. Wenn die BladeCenter-Einheit ordnungsgemäß mit zwei Netzstromquellen verdrahtet ist, kann der Ausfall einer Netzstromquelle dazu führen, dass einige Blade-Server gedrosselt werden. Die BladeCenter-Einheit bleibt jedoch betriebsbereit. Einige Blade-Server können möglicherweise nicht eingeschaltet werden, wenn dadurch der Grenzwert für die maximale Stromversorgung dieser Richtlinie überschritten würde. Mithilfe dieser Richtlinie können die Komponenten insgesamt mehr Strom von der BladeCenter-Einheit ziehen als durch die Richtlinie **Redundante Netzstromquellen** unterstützt wird, sodass Sie Blade-Server einschalten können, die Sie andernfalls möglicherweise nicht einschalten könnten. Die Richtlinie hat jedoch möglicherweise den Nebeneffekt, dass einige Blade-Server den Stromverbrauch reduzieren müssen, wenn eine Netzstromquelle ausfällt, damit die BladeCenter-Einheit betriebsbereit gehalten werden kann. Die Regulierung eines Blade-Servers bewirkt, dass der Stromverbrauch eines Blade-Servers durch vorübergehende Reduzierung der Mikroprozessorleistung gesenkt wird. Das Managementmodul und die Blade-Server nutzen in bestimmten Prozessoren integrierte Technologien der Stromverbrauchssteuerung, um die Blade-Server zu regulieren und so einen geringeren Stromverbrauch zu erzielen. Nicht alle Blade-Server sind regulierungsfähig.

Hardware VPD (Elementare Hardware-Produktdaten)

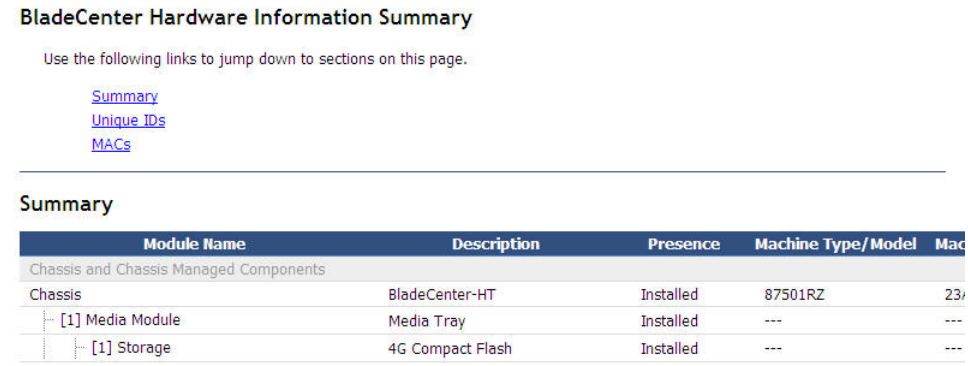
Wählen Sie **Monitors → Hardware VPD** (Monitore → Elementare Hardware-Produktdaten) aus, um die elementaren Hardware-Produktdaten der BladeCenter-Einheit anzuzeigen.

Die folgende Abbildung zeigt die Seite "Hardware VPD" (Elementare Hardware-Produktdaten) eines erweiterten Managementmoduls. Beim Öffnen der Seite wird die Registerkarte **Hardware Topology** (Hardwaretopologie) angezeigt.

Anmerkung: Diese Seite kann außerdem Funktionen anzeigen, die nur für die BladeCenter S-Einheit gelten, wie zum Beispiel die integrierten Speichermodule, das Direct Serial Attach-Modul und das optionale RAID-SAS-Modul.



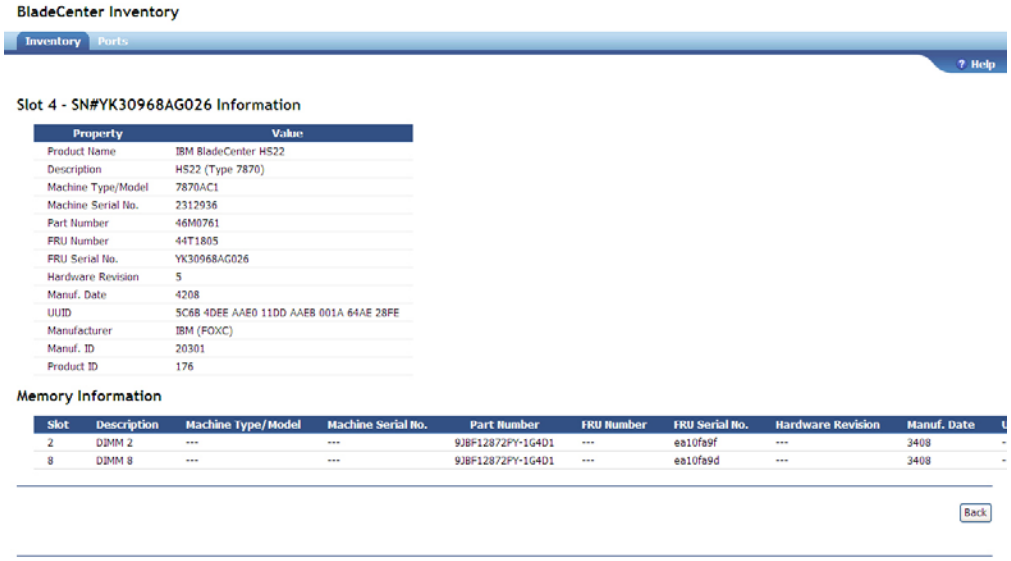
Wählen Sie den Link zur BladeCenter-Zusammenfassung aus, um eine Seite mit der Zusammenfassung der elementaren Hardware-Produktdaten anzuzeigen.



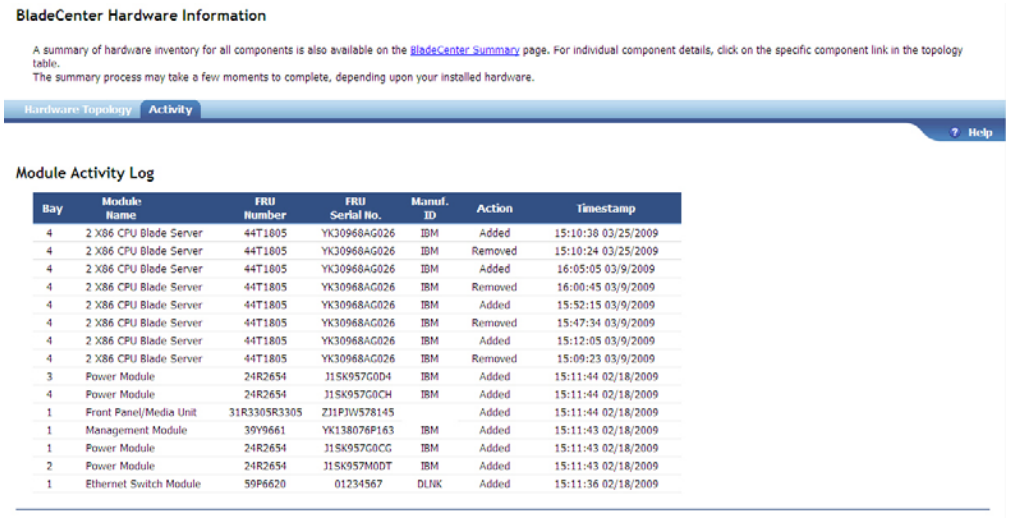
Wählen Sie die Option **Monitors → Hardware VPD** (Monitore → Elementare Hardware-Produktdaten) aus, um die elementaren Produktdaten für die BladeCenter-Einheit anzuzeigen. Wenn die BladeCenter-Einheit gestartet wird, erfasst das Ma-

nagementmodul die elementaren Produktdaten und speichert sie im nicht flüchtigen Speicher. Anschließend modifiziert das Managementmodul die gespeicherten elementaren Produktdaten, wenn Komponenten zur BladeCenter-Einheit hinzugefügt oder daraus entfernt werden. Welche elementaren Hardware-Produktdaten erfasst und gespeichert werden, hängt vom Typ der BladeCenter-Einheit ab.

Klicken Sie auf einen **Module Name** (Modulnamen), um eine Seite mit zusätzlichen Bestandsdaten und Anschlussinformationen anzuzeigen. Hierzu können der Maschinentyp oder die Modellnummer, die Seriennummer und die UUID-MAC-Adresse (Universally Unique Identifier) gehören.



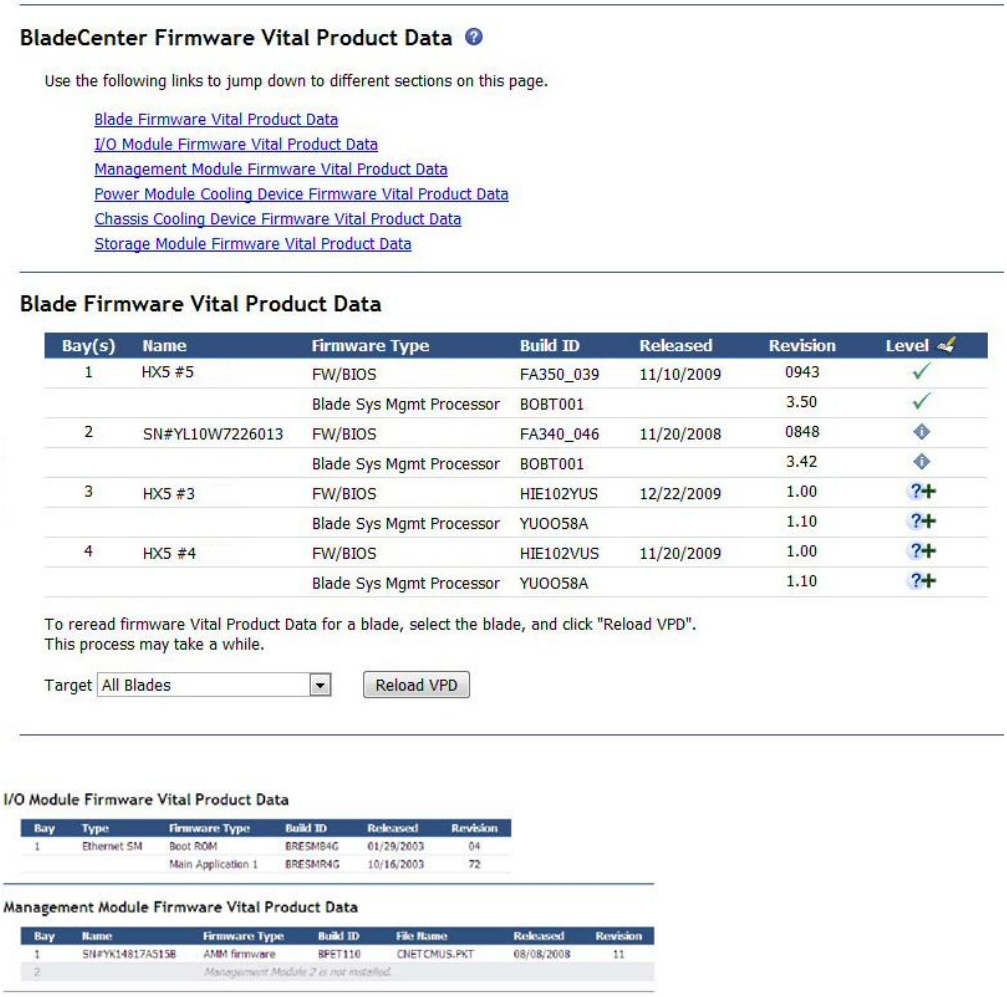
Klicken Sie auf die Registerkarte **Activity** (Aktivität), um das Protokoll der Module anzuzeigen, die in der BladeCenter-Einheit installiert oder daraus entfernt wurden.



Firmware VPD (Elementare Firmware-Produktdaten)

Wählen Sie **Monitors → Firmware VPD** (Monitore → Elementare Firmware-Produktdaten) aus, um die elementaren Firmware-Produktdaten für die BladeCenter-Einheit anzuzeigen.

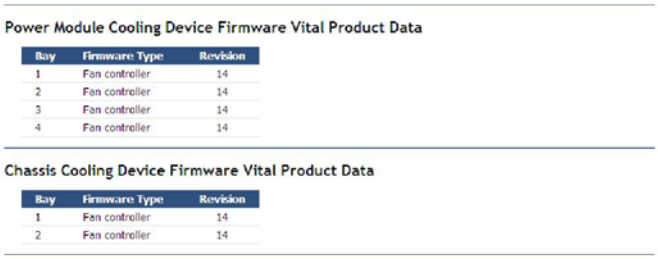
Die folgende Abbildung zeigt die Seite "Firmware Vital Product Data" (Elementare Firmware-Produktdaten) für ein erweitertes Managementmodul an.



Anmerkung: Das Managementmodul muss erneut gestartet werden, bevor es ein neu heruntergeladenes Firmware-Image verwenden kann. Diese Seite zeigt in mehreren Zeilen die elementaren Produktdaten zu den aktuellen und den anstehenden Software-Downloads an.

Klicken Sie auf **Firmware Vital Product Data** (Elementare Firmware-Produktdaten), um die elementaren Firmware-Produktdaten in allen Blade-Servern, E/A-Modulen und Managementmodulen in der BladeCenter-Einheit anzuzeigen. Welche elementaren Firmware-Produktdaten aufgezeichnet und gespeichert werden, variiert abhängig vom Typ der BladeCenter-Einheit.

- In einigen BladeCenter-Einheiten, in denen ein erweitertes Managementmodul installiert ist, können Sie auch die elementaren Firmware-Produktdaten für die Kühleinheit des Gehäuses und die Kühleinheit des Netzteils anzeigen.



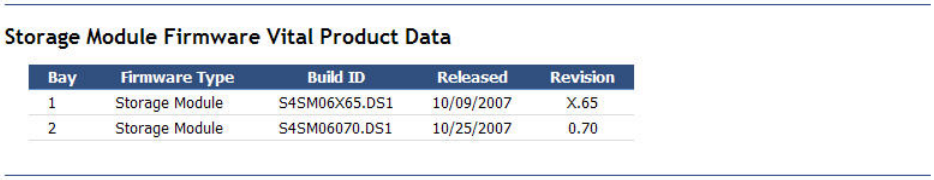
Power Module Cooling Device Firmware Vital Product Data

Bay	Firmware Type	Revision
1	Fan controller	14
2	Fan controller	14
3	Fan controller	14
4	Fan controller	14

Chassis Cooling Device Firmware Vital Product Data

Bay	Firmware Type	Revision
1	Fan controller	14
2	Fan controller	14

- Wenn ein erweitertes Managementmodul in einer BladeCenter S-Einheit installiert ist, können Sie außerdem die elementaren Produktdaten für die Firmware des Speichermoduls anzeigen.



Storage Module Firmware Vital Product Data

Bay	Firmware Type	Build ID	Released	Revision
1	Storage Module	S4SM06X65.DS1	10/09/2007	X.65
2	Storage Module	S4SM06070.DS1	10/25/2007	0.70

Die elementaren Firmware-Produktdaten enthalten Informationen zum Firmwaretyp und Versionsinformationen, wie zum Beispiel die Build-ID, das Releasedatum und die Überarbeitungsnummer. Die elementaren Produktdaten variieren abhängig vom Typ der BladeCenter-Komponente; die elementaren Firmware-Produktdaten für das Managementmodul können zum Beispiel auch die Dateinamen der Firmwarekomponenten enthalten. (Nach der Auswahl der Option **Firmware Vital Product Data** (Elementare Firmware-Produktdaten) dauert es bis zu 30 Sekunden, bis die Informationen aktualisiert und angezeigt werden.)

Bei Blade-Servern vergleicht der Versionsstatus die Buildstufe der Firmware für alle Blade-Server in einer BladeCenter-Einheit und die Buildstufen in der Liste der optionalen Blade-Firmware. Dabei wird einer der folgenden Hinweise angezeigt:

- Wenn die Angabe des Versionsstatus für einen Blade-Server leer ist, wird die Firmware dieses Blade-Servers nicht überprüft.
- Das Symbol  zeigt an, dass die gleichen Blade-Server über dieselbe Firmwareversion verfügen oder dass die Firmware auf dem Blade-Server mit den in der Liste der Blade-Firmware spezifizierten Anforderungen übereinstimmt. Klicken Sie auf das Symbol, um die Liste der Blade-Firmware anzuzeigen und zu bearbeiten.
- Das Symbol  zeigt an, dass gleiche Blade-Server unterschiedliche (abweichende) Firmwareversionen aufweisen oder dass die Firmware auf dem Blade-Server nicht mit den in der Liste der Blade-Firmware spezifizierten Anforderungen übereinstimmt. Klicken Sie auf das Symbol, um die Firmware des Blade-Servers zu aktualisieren.
- Das Symbol  zeigt einen einzelnen Blade-Server an (es ist nur ein Blade-Server dieses Typs in der BladeCenter-Einheit installiert) und gibt an, dass in der Liste der Blade-Firmware keine Anforderungen für diesen Blade-Servertyp spezifiziert sind. Klicken Sie auf das Symbol, um die Liste der Blade-Firmware zu bearbeiten, in der automatisch ein neuer Eintrag für den Blade-Servertyp erstellt wird. Nachdem die Informationen zur Firmware für den Blade-Server eingegeben wurden, muss die Konfiguration gespeichert werden, damit die Änderungen wirksam werden.

Klicken Sie auf das Symbol  oben in der Spalte "Level" (Version), um in der Liste der Blade-Firmware Build-ID-Stufen anzuzeigen, zu bearbeiten, herunterzuladen oder hochzuladen.

Die Liste der elementaren Firmware-Produktdaten der Blade-Server wird anfänglich anhand der in der BladeCenter-Einheit erkannten Komponenten erstellt und in der Liste der Blade-Firmware auf der Seite "Blade Firmware Management" (Verwaltung der Blade-Firmware) angezeigt.

Auf der Seite "Blade Firmware Management" (Blade-Firmwareverwaltung) können Sie auf der Registerkarte "Blade Firmware List" (Liste der Blade-Firmware) die elementaren Produktdaten zur Blade-Server-Firmware bearbeiten. Durch Klicken auf **Rebuild List** (Liste neu erstellen) können Sie die BladeCenter-Einheit durchsuchen und anhand der erkannten Komponenten eine Liste der elementaren Produktdaten zur Blade-Server-Firmware erstellen. Die Liste enthält nur zu den Blade-Servern Informationen, auf deren elementare Produktdaten das erweiterte Managementmodul uneingeschränkt zugreifen kann. Alle Blade-Server, deren elementare Produktdaten nicht verfügbar oder fehlerhaft sind, werden ignoriert und nicht in die Liste aufgenommen. Diese Liste kann anschließend manuell geändert werden, um verschiedene Anforderungen anzugeben. Sie müssen sicherstellen, dass in den Feldern "Manufacturer" (Hersteller), "Machine type" (Maschinentyp), "Firmware type" (Firmwaretyp) und "Build ID" (Build-ID) die entsprechenden Angaben gemacht werden.

Mithilfe der Registerkarten "Export List" (Liste exportieren) und "Import List" (Liste importieren) können Sie die elementaren Firmware-Produktdaten des Blade-Servers, wie sie auf der Registerkarte "Blade Firmware List" (Liste der Blade-Firmware) dargestellt sind, in einer Datei speichern oder von einer Datei laden. Der Dateiname der Datei mit den elementaren Firmware-Produktdaten des Blade-Servers wird automatisch in folgendem Format generiert: *ammName*`_YYYYMMDD_hhmmss_buildids`. Dabei gilt:

- Der *ammName* gibt den Namen des erweiterten Managementmoduls an.
- Der Eintrag *YYYYMMDD* gibt das Datum des Exports der elementaren Produktdaten zur Blade-Server-Firmware im Format Jahr-Monat-Tag an.
- Der Eintrag *hhmmss* gibt die Uhrzeit des Exports der elementaren Produktdaten zur Blade-Server-Firmware im Format Stunde-Minute-Sekunde (24-Stunden-Format) an.

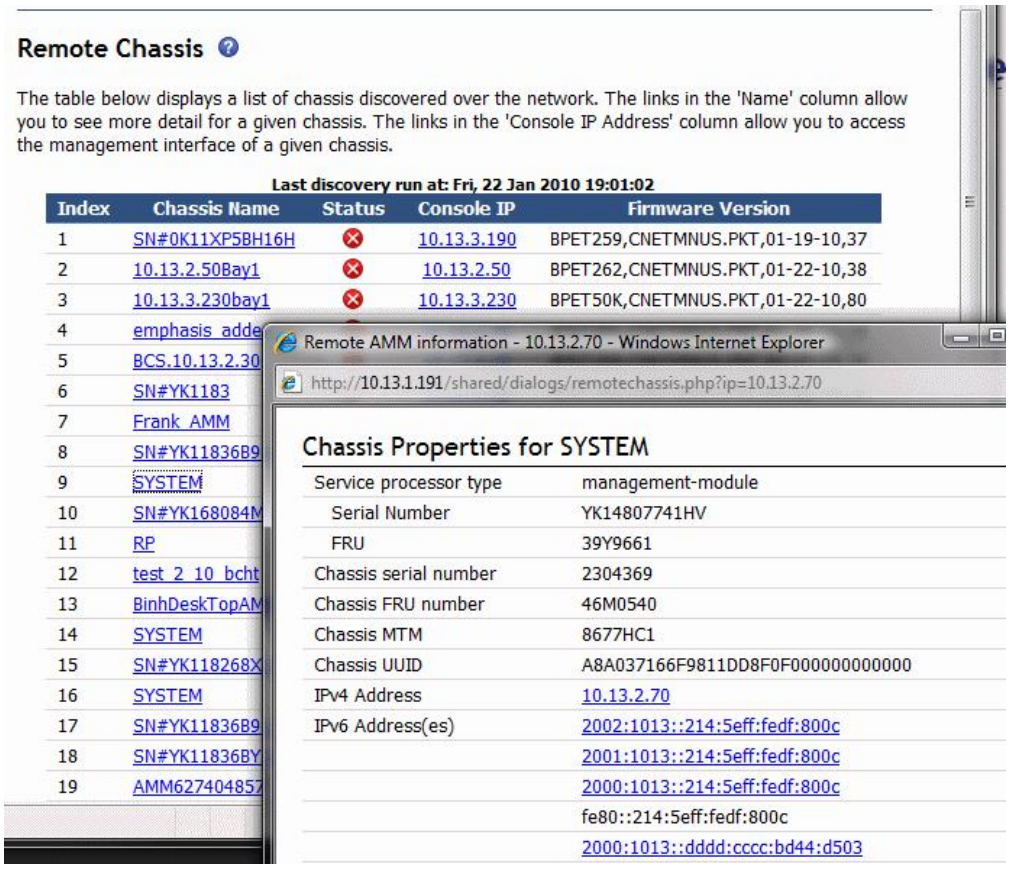
Wenn ein optionales erweitertes Bereitschaftsmanagementmodul installiert ist, spiegelt das aktive erweiterte Managementmodul die Daten und die Firmwareaktualisierungen auf das Bereitschaftsmanagementmodul. Die elementaren Firmware-Produktdaten für das aktive erweiterte Managementmodul und das erweiterte Bereitschaftsmanagementmodul werden auf dieser Seite angezeigt. Wenn das aktive erweiterte Managementmodul erkennt, dass das erweiterte Bereitschaftsmanagementmodul eine andere Firmwareversion aufweist, versucht es, die Firmware des erweiterten Bereitschaftsmanagementmoduls zu derselben Version zu aktualisieren. Die elementaren Firmware-Produktdaten sollten für beide, das aktive erweiterte Managementmodul und das erweiterte Bereitschaftsmanagementmodul, identisch sein, es sei denn, es wird gerade dieser Vorgang ausgeführt.

Anmerkung: Die BladeCenter S-Einheit verfügt über ein erweitertes Managementmodul und unterstützt kein zusätzliches erweitertes Bereitschaftsmanagementmodul.

Klicken Sie auf **Reload VPD** (elementare Produktdaten erneut laden), um die elementaren Firmware-Produktdaten für einen ausgewählten Blade-Server oder für alle Blade-Server in der BladeCenter-Einheit zu aktualisieren.

Remote Chassis (Ferne Gehäuse)

Wählen Sie **Monitors → Remote Chassis** (Monitore → Ferne Gehäuse) aus, um eine Liste aller im Netz gefundenen BladeCenter-Einheiten anzuzeigen.



Auf der Seite **Remote Chassis** (Ferne Gehäuse) wird das Service Location Protocol (SLP) verwendet, um Informationen zu allen BladeCenter-Einheiten im Netz zu ermitteln und anzuzeigen. Die Informationen zur BladeCenter-Einheit umfassen Name, Status, IP-Adresse des Managementmoduls und Firmwareversion des Managementmoduls. Klicken Sie auf den Namen der BladeCenter-Einheit, um eine Detailsicht mit den Eigenschaften dieser BladeCenter-Einheit anzuzeigen. Klicken Sie auf die IP-Adresse der Konsole der BladeCenter-Einheit, um eine Webschnittstellensitzung für diese BladeCenter-Einheit zu starten. Sie müssen SLP auf der Seite "Network Protocols" (Netzprotokolle) (Informationen dazu finden Sie im Abschnitt „Network Protocols (Netzprotokolle)" auf Seite 192) aktivieren, damit die Liste auf der Seite "Remote Chassis" (Ferne Gehäuse) ausgefüllt werden kann.

Klicken Sie auf **Discover** (Ermitteln), um eine sofortige Netzsuche zu erzwingen und dadurch die Liste mit den fernen BladeCenter-Einheiten erneut auszufüllen.

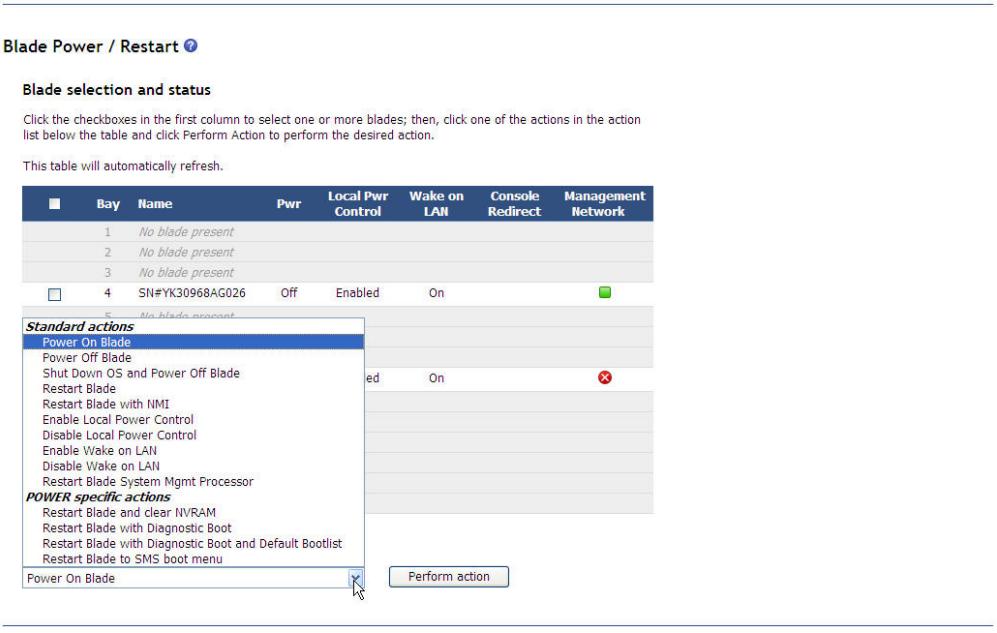
Klicken Sie auf **Clear** (Löschen), um den Inhalt der Liste mit den fernen BladeCenter-Einheiten zu löschen. Die Liste wird erst erneut ausgefüllt, wenn Sie auf **Discover** (Ermitteln) klicken.

Blade Tasks (Blade-Tasks)

Wählen Sie die **Blade Tasks**-Optionen (Blade-Tasks) aus, um die Einstellungen oder Konfigurationen der Blade-Server in der BladeCenter-Einheit anzuzeigen und zu ändern.

Einschalten/Neustart

Wählen Sie **Blade Tasks → Power/Restart** (Blade-Tasks → Einschalten/Neustart) aus, um einzelne Blade-Server ein- und auszuschalten oder neu zu starten.



Wählen Sie **Power/Restart** (Einschalten/Neustart) aus, um die folgenden Aktionen auf einem Blade-Server in der BladeCenter-Einheit durchzuführen.

- Ein- oder Ausschalten des ausgewählten Blade-Servers (den Stromversorgungsstatus aktivieren oder inaktivieren).
- Herunterfahren des Betriebssystems und Ausschalten des Blade-Servers.
- Erneutes Starten des Blade-Servers mit oder ohne NMI (Non-Maskable Interrupt).
- Aktivieren oder Inaktivieren der lokalen Stromversorgungssteuerung. Wenn die lokale Stromversorgungssteuerung aktiviert ist, kann ein lokaler Benutzer den Blade-Server ein- oder ausschalten, indem er den Netzschalter am Blade-Server drückt.
- Aktivieren oder Inaktivieren der Wake on LAN-Funktion.
- Erneutes Starten des Blade-Servers oder des Serviceprozessors im Blade-Server.
- Überprüfen, welche Blade-Server derzeit über eine ferne Konsole gesteuert werden (angezeigt durch ein X in der Spalte "Console Redirect" (Konsolenumleitung)).

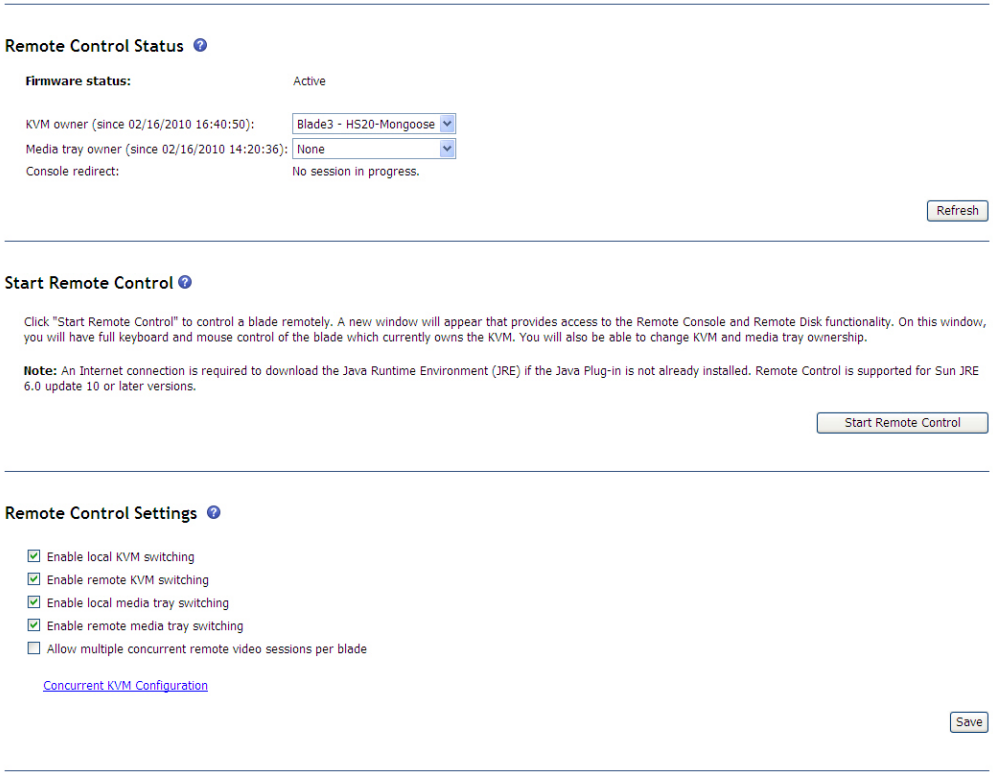
Die folgenden Vorgänge können auf einigen POWER-basierten Blade-Servern ausgeführt werden.

- Erneutes Starten des ausgewählten Blade-Servers und Öffnen des Menüs für die Systemverwaltungsfunktion.
- Erneutes Starten des ausgewählten Blade-Servers und Löschen des NVRAM.
- Erneutes Starten des ausgewählten Blade-Servers und Ausführen des Diagnoseprogramms.
- Erneutes Starten des ausgewählten Blade-Servers und Ausführen des Diagnoseprogramms mithilfe der für den Blade-Server konfigurierten Standardstartreihenfolge.

Remote Control (Fernsteuerung)

Wählen Sie **Blade Tasks → Remote Control** (Blade-Tasks → Fernsteuerung) aus, um die lokale KVM- und Laufwerkschlittensteuerung bestimmten Blade-Servern zuzuordnen oder um einen Blade-Server über eine ferne Konsole im Netz zu bedienen.

In der folgenden Abbildung ist die Seite "Remote Control" (Fernsteuerung) für ein erweitertes Managementmodul dargestellt.



Um die lokale KVM- oder Laufwerkschlittensteuerung einem anderen Blade-Server zuzuordnen, wählen Sie den Blade-Server aus der Liste **KVM owner** (KVM-Eigner) oder aus der Liste **Media tray owner** (Laufwerkschlitteneigner) aus und klicken Sie auf **Refresh** (Aktualisieren).

Klicken Sie auf **Start Remote Control** (Fernsteuerung starten), um eine ferne Konsole einzurichten. Die ferne Konsole startet in einem eigenständigen Java-Anwendungsfenster. (Weitere Informationen hierzu finden Sie im Abschnitt „Funktion für ferne Konsole verwenden” auf Seite 80.)

An einer fernen Konsole können Sie den Blade-Server so steuern, als würden Sie eine lokale Konsole bedienen, d. h. Sie können den Blade-Server neu starten und den POST-Prozess anzeigen und Sie verfügen über die vollständige Steuerung von Tastatur und Maus. Dabei bezieht sich die Tastaturunterstützung der fernen Konsole auf alle Tasten. Für Tasten, die möglicherweise eine spezielle Bedeutung für den Blade-Server haben, werden Symbole angezeigt. Beispiel: Um den Befehl Strg+S an den Blade-Server zu übertragen, klicken Sie auf das Symbol **Ctrl** (Strg) im Videobereich und drücken Sie dann die Taste **S** auf der Tastatur.

Verwenden Sie die ferne Konsole, um die folgenden Tasks auszuführen:

- Den Blade-Server anzeigen und wechseln, der derzeit Tastatur, Bildschirm und Maus (Keyboard, Video und Mouse, KVM) sowie den Laufwerkschlitten in der BladeCenter-Einheit steuert. Weitere Informationen zum Wechsel der KVM- und Laufwerkschlittensteuerung finden Sie im *Installations- und Benutzerhandbuch* zu Ihrem Blade-Server.

Anmerkungen:

- Das Betriebssystem auf dem Blade-Server muss USB unterstützen, damit der Blade-Server die Tastatur und die Maus erkennen kann, auch wenn Tastatur und Maus über einen PS/2-Anschluss verfügen.
- Wenn das Betriebssystem auf dem Blade-Server den USB-Massenspeicher nicht unterstützt, ist die Funktion für ferne Datenträger nicht verfügbar.
- Wenn Sie auf dem Blade-Server ein unterstütztes Microsoft Windows-Betriebssystem installieren, das jedoch nicht der aktuelle KVM-Eigner ist, tritt bei der Übergabe der KVM-Steuerung an den Blade-Server eine Verzögerung von bis zu 1 Minute auf. Alle nachfolgenden Steuerungsübergaben erfolgen im üblichen Zeitrahmen für die Übergabe der KVM-Steuerung (bis zu 20 Sekunden).
- Die Laufwerke im Laufwerkschlitten auswählen und auf diese zugreifen.
- Ein Laufwerk oder Image auf einem Blade-Server über das System bereitstellen, das als ferne Konsole dient. Das bereitgestellte Laufwerk oder Image wird als eine an den Blade-Server angeschlossene USB-Einheit angezeigt. Informationen und Anweisungen finden Sie im Abschnitt „Funktion für ferne Datenträger verwenden” auf Seite 81.
- Die Details von allen derzeit aktiven Fernsteuerungssitzungen anzeigen (Benutzer-ID, IP-Adresse des Clients, Startzeit).
- Die lokale Übergabe der KVM-Steuerung für Blade-Server aktivieren oder inaktivieren, bis sie explizit wieder aktiviert wird. Auf diese Weise wird verhindert, dass ein lokaler Benutzer die Steuerung der Konsole an einen anderen Blade-Server übergibt, während Sie Fernsteuerungstasks ausführen. Benutzer mit Zugriff auf die BladeCenter-Einheit können mithilfe des KVM-Auswahlknopfs (Keyboard/Video/Mouse, Tastatur/Bildschirm/Maus) an einem Blade-Server den KVM-Eigner wechseln. Wenn Sie den lokalen Zugriff nicht inaktivieren, können diese auch mithilfe einer direkt an das Managementmodul angeschlossenen Tastatur die KVM-Steuerung zwischen Blade-Servern übertragen.

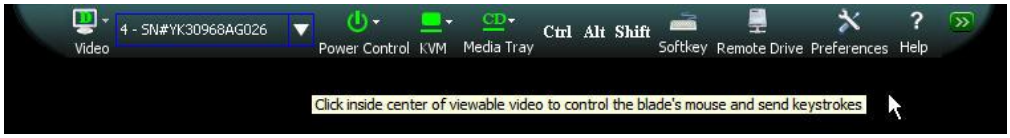
  Wenn ein lokaler Benutzer feststellt, dass auf das Drücken des KVM-Auswahlknopfs keine Reaktion folgt, wurde die lokale Steuerung möglicherweise von einem fernen Benutzer am Blade-Server mithilfe des Managementmoduls inaktiviert.
- Die lokale Übergabe der Laufwerkschlittensteuerung für alle Blade-Server aktivieren oder inaktivieren, bis sie explizit wieder aktiviert werden. Auf diese Weise wird verhindert, dass lokale Benutzer die Steuerung des Laufwerkschlittens an einen anderen Blade-Server übergeben, während Sie eine Task ausführen. Der Laufwerkschlitten wird immer jeweils nur von einem Blade-Server genutzt.

Es werden die folgenden Funktionen unterstützt:

- Die ferne Übergabe der Laufwerkschlittensteuerung für alle Blade-Server aktivieren oder inaktivieren, bis sie explizit wieder aktiviert werden.
- Die ferne Übergabe der KVM-Steuerung für alle Blade-Server aktivieren oder inaktivieren, bis diese Funktion explizit wieder aktiviert wird.
- Aktivieren oder Inaktivieren mehrerer gleichzeitiger Videositzungen. Wenn die Sitzungen aktiviert wurden, kann das Video über die ferne Konsole von bis zu

vier Benutzern gleichzeitig auf einem Blade-Server angezeigt werden. Wenn nicht, kann es nur von einem Benutzer angezeigt werden.

In der folgenden Abbildung ist eine Fernsteuerungssitzung für ein erweitertes Managementmodul dargestellt.



Beim erweiterten Managementmodul sind die Videosteuerelemente der fernen Konsole in eine Taskleiste oben auf dem Bildschirm integriert.

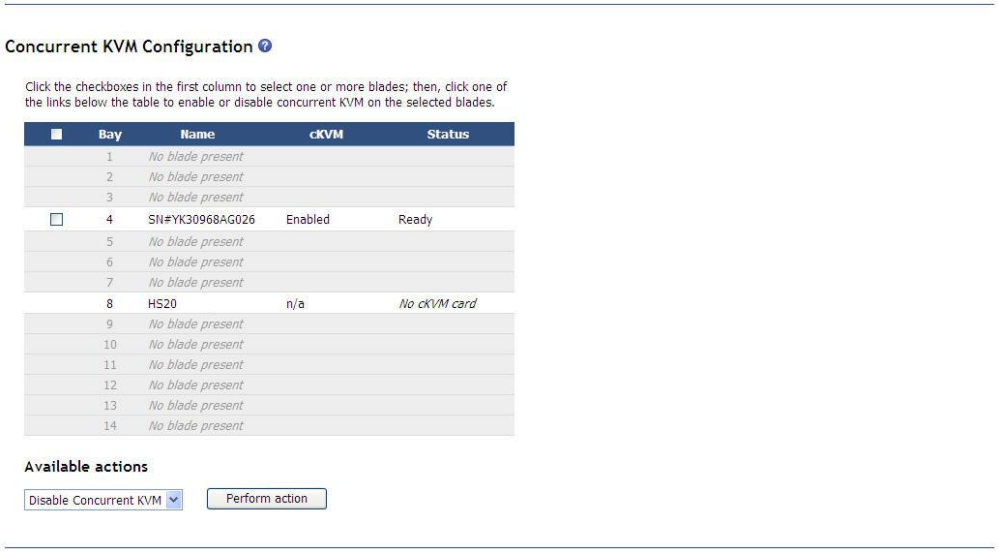
- Verwenden Sie das Symbol **Video** (Video), um die horizontale Position der Anzeige neu aufzubauen, zu kalibrieren oder anzupassen.
  - Wählen Sie **Toggle Full Screen** (Vollbildmodus ein-/ausschalten) aus, um zwischen der Anzeige der fernen Sitzung in einem Fenster mit anpassbarer Größe und einer Ansicht zu wechseln, die den gesamten Bildschirm belegt. Diese Funktion ist nur bei der Anzeige eines gleichzeitigen Video-Blade-Servers verfügbar.
  - Wählen Sie **Repaint** (Neu aufbauen) aus, um die Anzeige der fernen Konsole zu aktualisieren und Artefakte zu bereinigen.
  - Wählen Sie **Calibrate** (Kalibrieren) aus (kann bei cKVM-Blade-Server-Sitzungen nicht angewendet werden), um eine Videokalibrierungssequenz auszuführen, mit der die Leistung der fernen Videositzung optimiert wird. Kalibrieren Sie eine Sitzung, wenn sich die angezeigten Farben erheblich von den erwarteten Farben unterscheiden.
  - Wählen Sie **Horizontal Adjust** (Horizontale Anpassung) aus, um die Anzeige zu zentrieren.
  - Wählen Sie **Screenshot** (Screenshot) aus, um die aktuelle Videoanzeige zu erfassen und in einem der unterstützten Bildformate im lokalen Festplattenlaufwerk zu speichern. Diese Funktion ist nur bei der Anzeige eines gleichzeitigen Video-Blade-Servers verfügbar.

  Anmerkung: Diese Vorgänge können bei cKVM-Video nicht ausgeführt werden.
- Wählen Sie über die Dropdown-Liste **Server Blade** (Blade-Server) den zu steuernden Blade-Server aus.
- Verwenden Sie das Symbol **Power Control** (Stromversorgungssteuerung), um den ausgewählten Blade-Server auszuschalten, neu zu starten, das Betriebssystem zu beenden und auszuschalten oder mit einem NMI neu zu starten.
- Verwenden Sie das Symbol **KVM** (KVM), um die lokale KVM-Steuerung einem ausgewählten Blade-Server zuzuweisen.
- Verwenden Sie das Symbol **Media Tray** (Laufwerkschlitten), um die lokale Laufwerkschlittensteuerung einem ausgewählten Blade-Server zuzuweisen.
- Verwenden Sie die Schaltflächen **Sticky Key** (Gedrückte Taste), um Ihre nächste Tastenkombination mit der Strg-, Alt- oder Umschalttaste zu ändern.
- Verwenden Sie das Symbol **Softkey** (Programmfunktionssymbol), um benutzerdefinierte Tastenkombinationen zu definieren oder zu verwenden.
- Verwenden Sie das Symbol **Remote Drive** (Fernes Laufwerk), um das Fenster "Remote Drive" (Fernes Laufwerk) zu öffnen, das zum Bereitstellen von virtuellen Datenträgern und zum Aufheben der Bereitstellung verwendet wird. Siehe „Datenträgerlaufwerk oder -image anhängen” auf Seite 82.

- Verwenden Sie das Symbol **Preferences** (Vorgaben), um Vorgaben für Fernsteuerungssitzungen und KVM-Vorgaben festzulegen und benutzerdefinierte Tastensymbole für häufig verwendete Tastenkombinationen zu erstellen. Sie können auch die Mauserfassungsfunktion inaktivieren oder aktivieren, sodass Sie mit der lokalen Computermaus je nach Bildschirmposition entweder die ferne Sitzung oder den lokalen Computer steuern können. Wenn die Mauserfassung inaktiviert ist, haben Sie darüber hinaus auch die Möglichkeit, die lokale Maus zu aktivieren oder inaktivieren.

Der Zeitlimitwert für eine Fernsteuerungssitzung entspricht dem Zeitlimitwert, den Sie bei Ihrer Anmeldung für die Sitzung für die Webschnittstelle des Managementmoduls festgelegt haben.

Klicken Sie auf **Concurrent KVM Configuration** (cKVM-Konfiguration), um den cKVM-Status (concurrent KVM, gleichzeitige KVM-Steuerung) und die Einstellungen für die einzelnen Blade-Server anzuzeigen und zu konfigurieren. Für die Verwendung der cKVM-Funktion sind optionale Hardware und ein cKVM-fähiger Blade-Server erforderlich. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Blade-Server.



Wenn cKVM verwendet wird, können mehrere Fernsteuerungssitzungen auf mehrere Blade-Server gleichzeitig zugreifen. Bei üblichen Sitzungen über die ferne Konsole (ohne cKVM) wird pro Blade-Server jeweils immer nur eine Sitzung über die ferne Konsole aktiviert. Wenn in den "Remote Control Settings" (Einstellungen für die Fernsteuerung) mehrere ferne Videositzungen gleichzeitig aktiviert sind, kann das Video über die ferne Konsole von bis zu vier Benutzern gleichzeitig auf einem Blade-Server angezeigt werden. Wenn nicht, kann es nur von einem Benutzer angezeigt werden. Wenn die maximale Anzahl an aktiven Fernsteuerungssitzungen erreicht wird, müssen Sie eine der aktuellen Sitzungen beenden, um eine neue zu starten.

Firmware Update (Firmwareaktualisierung)

Wählen Sie **Blade Tasks → Firmware Update** (Blade-Tasks → Firmwareaktualisierung) aus, um einige Firmwaretypen auf einem Blade-Server zu aktualisieren.

Wichtig:

- Einige Clusterlösungen erfordern bestimmte Codeversionen oder koordinierte Codeaktualisierungen. Wenn die Einheit Teil einer Clusterlösung ist, überprüfen Sie, ob die aktuelle Codeversion für die Clusterlösung unterstützt wird, bevor Sie den Code aktualisieren.
- Alle Blade-Server in einem skalierbaren Komplex müssen dieselbe Firmware-Version aufweisen. Informationen zum Durchführen einer koordinierten Firmwareaktualisierung für mehrere Blade-Server finden Sie im Abschnitt „Firmware Multi-flash (Firmware-Multiflash)" auf Seite 148.

Verwenden Sie diese Seite, um die Firmware auf einem bestimmten Blade-Server zu aktualisieren. Derzeit kann die Blade-Server-Firmware des BSMPs (Blade System Management Processor, Blade-Systemmanagementprozessor) oder des Serviceprozessors auf den meisten Blade-Server-Typen mithilfe dieser Seite aktualisiert werden. Die Aktualisierung der Blade-Server-Firmware des BIOS oder der UEFI (Unified Extensible Firmware Interface, vereinheitlichte erweiterbare Firmware-Schnittstelle) wird für einige Blade-Server-Typen auch von dieser Seite unterstützt. Diese Seite unterstützt jedoch die Aktualisierung der Blade-Server-Firmware des BIOS für die meisten Blade-Server oder die Aktualisierung der Firmware für Diagnose, Netzadapter oder cKVM-Adapter nicht. Ausführliche Informationen und Anweisungen zum Aktualisieren der Firmware finden Sie in der Dokumentation zu Ihrer Firmwareaktualisierung.

Wählen Sie den Ziel-Blade-Server und die für die Aktualisierung zu verwendende Firmwaredatei aus und klicken Sie auf **Update** (Aktualisieren). Wenn mehr als ein Blade-Server in der BladeCenter-Einheit installiert ist, der eine Multiflash-Firmwareaktualisierung unterstützt, können mehrere Blades vom selben Typ ausgewählt werden. (Weitere Informationen hierzu finden Sie im Abschnitt „Firmware Multiflash (Firmware-Multiflash)" auf Seite 148.) Wenn für Ihre BladeCenter-Einheit skalierbare Komplexe aktiviert wurden, werden alle Blade-Server, die sich in dem Komplex mit dem ausgewählten Blade-Server befinden, automatisch ausgewählt. Wenn Sie für einen Blade-Server im skalierbaren Komplex die Auswahl aufheben, wird die Auswahl für alle Blade-Server in diesem Komplex aufgehoben. Wenn skalierbare Komplexe für Ihre BladeCenter-Einheit inaktiviert wurden, können Sie die Kontrollkästchen für mehrere multiflashfähige Blade-Server vom selben Typ aktivieren und inaktivieren, um eine gleichzeitige Firmwareaktualisierung durchzuführen.

Die Firmwaredateien erhalten Sie unter http://www.ibm.com/systems/support/.

Mithilfe der Methode "Remote File" (Ferne Datei) können Sie die vollständig qualifizierte Adresse der Firmware-Paketdatei zum Aktualisieren der BSMP-Firmware angeben. Die vollständig qualifizierte Adresse enthält ein vom erweiterten Managementmodul unterstütztes Protokoll, einen Doppelpunkt und zwei Schrägstriche (//), den Benutzernamen und das Kennwort (durch einen Doppelpunkt voneinander getrennt) zur Anmeldeauthentifizierung, ein @-Zeichen, den Hostnamen oder die IP-Adresse, eine optionale Portnummer und den vollständigen Pfadnamen.

Anmerkung: Wenn die Portnummer angegeben wird, muss diese durch einen Doppelpunkt vom Hostnamen (oder der IP-Adresse) getrennt werden.

Das vollständige Format sieht wie folgt aus: *Protokoll*://*Benutzername*:*Kennwort*@*Hostname*:*Port*/*Pfad*/*Dateiname*

Das erweiterte Managementmodul unterstützt die folgenden Protokolle:

- tftp
- ftp
- ftps
- http
- https

Beispiel für eine vollständig qualifizierte Adresse:

```
ftp://USERID:PASSW0RD@192.168.0.2:30045/tmp/CNETCMUS.pkt
```

In diesem Beispiel wird das FTP-Protokoll für die Übertragung der Paketdatei verwendet, der Benutzername lautet `USERID`, das Kennwort `PASSW0RD`, die IP-Adresse des Hosts (IPv4) `192.168.0.2`, die Portnummer `30045` und `/tmp` ist der vollständige Pfadname der Paketdatei `CNETCMUS.pkt`.

Bei einigen Protokollen muss weder Benutzername, noch Kennwort oder Portnummer angegeben werden, sodass die Mindestvoraussetzung für eine vollständig qualifizierte Adresse wie folgt aussehen kann:

Protokoll://*Hostname*/*Pfad*/*Dateiname*

Gehen Sie wie folgt vor, um die Firmware des erweiterten Managementmoduls mithilfe einer fernen Datei zu aktualisieren:

1. Aktivieren Sie das Kontrollkästchen **Remote File** (Ferne Datei).
2. Geben Sie in das Textfeld eine vollständig qualifizierte Adresse ein.
3. Klicken Sie entweder auf die Schaltfläche **Update** (Aktualisieren) oder auf die Schaltfläche **Update and Reboot** (Aktualisieren und einen Warmstart durchführen).

Anmerkung: Wenn Sie anstelle einer IP-Adresse einen Hostnamen verwenden, um eine ferne Datei anzugeben, stellen Sie sicher, dass DNS aktiviert ist.

Firmware Multi-flash (Firmware-Multiflash):

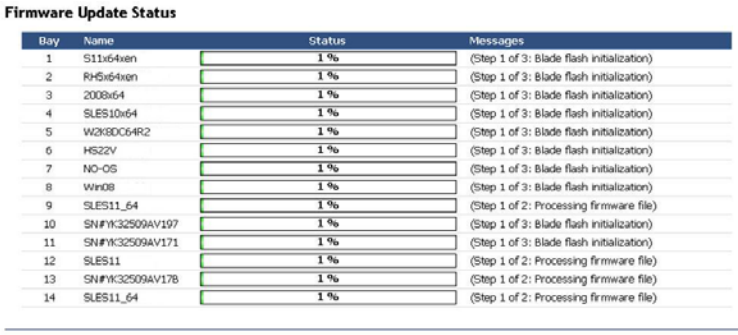
Bei einer bestimmten Firmware-Version und einem bestimmten Blade-Servertyp können Sie mithilfe des erweiterten Managementmoduls mehrere Blade-Server auswählen und deren Firmware gleichzeitig aktualisieren.

Anmerkung:

- Die Firmware-Multiflash-Funktion und die Seite "Firmware Update Status" (Status der Firmwareaktualisierung) sind nur verfügbar, wenn Blade-Server, die diese Funktion unterstützen, in der BladeCenter-Einheit installiert sind.
- Wenn sich in einem Blade-Server Firmwaretypen befinden, die aktualisiert werden müssen, müssen die Aktualisierungen einzeln durchgeführt werden.

Nach der Auswahl von Servern für die Multiflash-Aktualisierung wählen Sie die Firmwaredatei aus, die auf den ausgewählten Blade-Servern aktualisiert werden soll. Anschließend wird jeder Blade-Server in einem separaten Prozess aktualisiert.

In der folgenden Abbildung ist die Seite mit dem Multiflash-Status für koordinierte Blade-Server-Firmwareaktualisierungen dargestellt.



Anmerkung: Während einer Multiflash-Aktualisierung überprüft das erweiterte Managementmodul nicht, ob ein Blade-Server für die Aktualisierung verfügbar ist, bevor es versucht, die zugehörige Firmware zu aktualisieren. Bei Blade-Servern, die für die Aktualisierung nicht bereit sind, tritt bei der Aktualisierung ein Fehler auf.

Auf der Seite "Firmware Update Status" (Status der Firmwareaktualisierung) wird der Fortschritt für die einzelnen Blade-Server, die aktualisiert werden, angezeigt. Wenn bei einem Blade-Server bei der Aktualisierung ein Fehler auftritt, erstellt das erweiterte Managementmodul einen Ereignisprotokolleintrag, der das Problem beschreibt: Sie sollten keinen weiteren Versuch unternehmen, die Firmware zu aktualisieren, bis Sie diese Einträge geprüft haben. Wenn die ausgewählte Firmwaredatei mit keinem ausgewählten Blade-Server kompatibel ist oder nur mit einigen ausgewählten Blade-Servern nicht kompatibel ist, werden die Fehler für jeden Blade-Server, bei dem ein Fehler aufgetreten ist, als separates Ereignis angezeigt.

Configuration (Konfiguration)

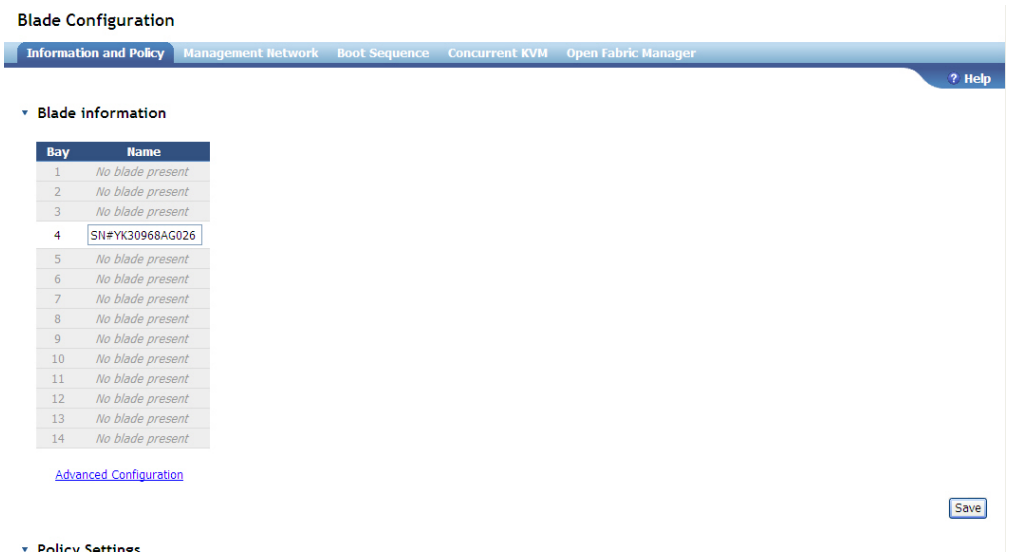
Wählen Sie **Blade Tasks → Configuration** (Blade-Tasks → Konfiguration) aus, um Konfigurationseinstellungen für den Blade-Server anzuzeigen und zu ändern.

In der folgenden Abbildung sind die Blade-Server-Konfigurationsoptionen für ein erweitertes Managementmodul dargestellt.

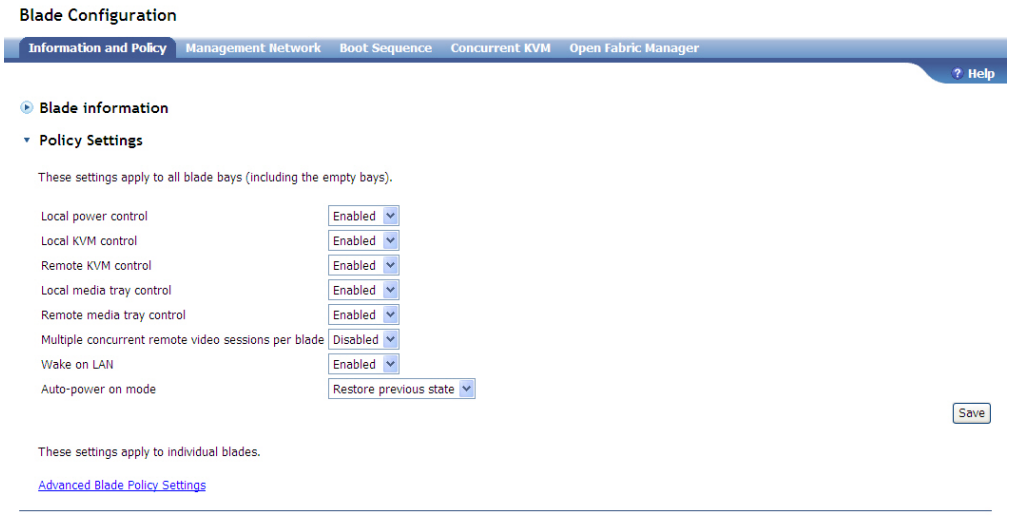
Anmerkung: Open Fabric Manager ist keine Standardkomponente des erweiterten Managementmoduls, sondern wird gesondert verkauft und dokumentiert. Ausführlichere Informationen hierzu finden Sie in der Dokumentation zum *BladeCenter Open Fabric Manager*. Informationen zum Kauf der Open Fabric Manager-Komponente finden Sie im Abschnitt „License Manager (Lizenzmanager)" auf Seite 205.

Klicken Sie auf **Blade Information** (Informationen zum Blade), um die folgenden Tasks auszuführen:

- Positionen und Namen von installierten Blade-Servern anzeigen
- Die Seite „Erweiterte Konfiguration" auf Seite 156 (Erweiterte Konfiguration) aufrufen, um Bladepositionsdaten anzuzeigen und zu bearbeiten



Klicken Sie auf **Policy Settings** (Richtlinieneinstellungen), um die folgenden Elemente auf allen Blade-Servern in der BladeCenter-Einheit zu aktivieren oder zu inaktivieren:



- **Local power, KVM, and media tray control** (Lokale Stromversorgungssteuerung, KVM-Steuerung und Laufwerkschlittensteuerung): Diese Felder zeigen die globale Richtlinieneinstellung für alle Bladepositionen an. Wenn **Enabled** (Aktiviert) ausgewählt wird, ist diese Funktion für alle Positionen aktiviert. Wenn **Disabled** (Inaktiviert) ausgewählt wird, ist diese Funktion für alle Positionen inaktiviert. Der Wert **Not set** (Nicht festgelegt) gibt an, dass keine globale Richtlinie festgelegt wurde. Bei einigen Positionen ist die Funktion möglicherweise aktiviert, bei anderen dagegen inaktiviert.
- **Remote KVM and media tray control** (Ferne KVM-Steuerung und Laufwerkschlittensteuerung): Diese Felder zeigen die globale Richtlinieneinstellung für alle Bladepositionen an. Wenn **Enabled** (Aktiviert) ausgewählt wird, ist diese Funktion für alle Positionen im Fernsteuerungsapplet aktiviert. Wenn **Disabled** (Inaktiviert) ausgewählt wird, ist diese Funktion für alle Positionen im Fernsteuerungsapplet inaktiviert. Der Wert **Not set** (Nicht festgelegt) gibt an, dass keine globale Richtlinie festgelegt wurde. (Bei einigen Positionen ist die Funktion möglicherweise aktiviert, bei anderen dagegen inaktiviert.) Wenn die Funktion für die Datenträger- oder KVM-Fernsteuerung inaktiviert ist, ist das zugehörige Feld ebenfalls inaktiviert. Sie können die Datenträgerfernsteuerung aktivieren. Wechseln Sie hierzu auf die Seite **MM Control → Network Protocols → Remote Control** (MM-Steuerung → Netzprotokolle → Fernsteuerung).
- **Multiple concurrent remote video sessions per blade** (Mehrere gleichzeitige Fernvideositzungen pro Blade): Dieses Feld zeigt die globale Richtlinieneinstellung dafür an, ob mehrere gleichzeitige Fernvideositzungen auf den einzelnen Blade-Servern unterstützt werden. Wenn **Enabled** (Aktiviert) ausgewählt wird, können bis zu vier Benutzer gleichzeitig mithilfe des Applets für ferne Konsolen den Bildschirminhalt des Blade-Servers anzeigen. Wenn **Disabled** (Inaktiviert) ausgewählt wird, wird auf den einzelnen Blade-Servern nur eine Fernvideositzung unterstützt. Der Wert **Not set** (Nicht festgelegt) gibt an, dass diese globale Richtlinie nicht initialisiert wurde und jeweils nur eine Fernvideositzung pro Blade-Server unterstützt wird.
- **Wake on LAN** (Wake on LAN): Dieses Feld zeigt die globale Richtlinieneinstellung für die Funktion "Wake on LAN" für alle Bladepositionen an. Wenn **Enabled** (Aktiviert) ausgewählt wird, ist "Wake on LAN" für alle Positionen aktiviert. Wenn **Disabled** (Inaktiviert) ausgewählt wird, ist "Wake on LAN" für alle Positionen inaktiviert. Der Wert **Not set** (Nicht festgelegt) gibt an, dass keine globale Richtlinie festgelegt wurde. Bei einigen Positionen ist "Wake on LAN" möglicherweise aktiviert, bei anderen dagegen inaktiviert. Nicht alle Blade-Server-Typen

unterstützen die Funktion "Wake on LAN". Die BIOS-Standardeinstellung für "Wake on LAN" für Blade-Server, die diese Funktion unterstützen, ist **Enabled** (Aktiviert).

- **Auto-power on mode** (Modus für automatisches Einschalten): Dieses Feld zeigt die globale Richtlinieneinstellung für automatisches Einschalten für alle Bladepositionen an. Wenn **Auto power** (Automatisches Einschalten) ausgewählt wird, werden alle Blade-Server unabhängig vom vorherigen Stromversorgungsstatus entsprechend der Einschaltberechtigung automatisch eingeschaltet, wenn an die BladeCenter-Einheit Spannung angelegt wird. Wenn **Manual power** (Manuelles Einschalten) ausgewählt wird, bleiben alle Blade-Server beim Anlegen einer Spannung an die BladeCenter-Einheit so lange ausgeschaltet, bis sie vom Benutzer eingeschaltet werden. Wenn **Restore previous state** (Vorherigen Status wiederherstellen; Standardeinstellung) ausgewählt wird, versucht das erweiterte Managementmodul beim Anlegen einer Spannung an die BladeCenter-Einheit, alle zuvor eingeschalteten Blade-Server einzuschalten.

  Anmerkung:

  – Wenn die Hardwarekonfiguration der BladeCenter-Einheit seit dem letzten bekannten Stromversorgungsstatus geändert wurde, wird kein Blade-Server eingeschaltet.

  – Änderungen an den Richtlinieneinstellungen für automatisches Einschalten werden erst nach einem Neustart der BladeCenter-Einheit wirksam.

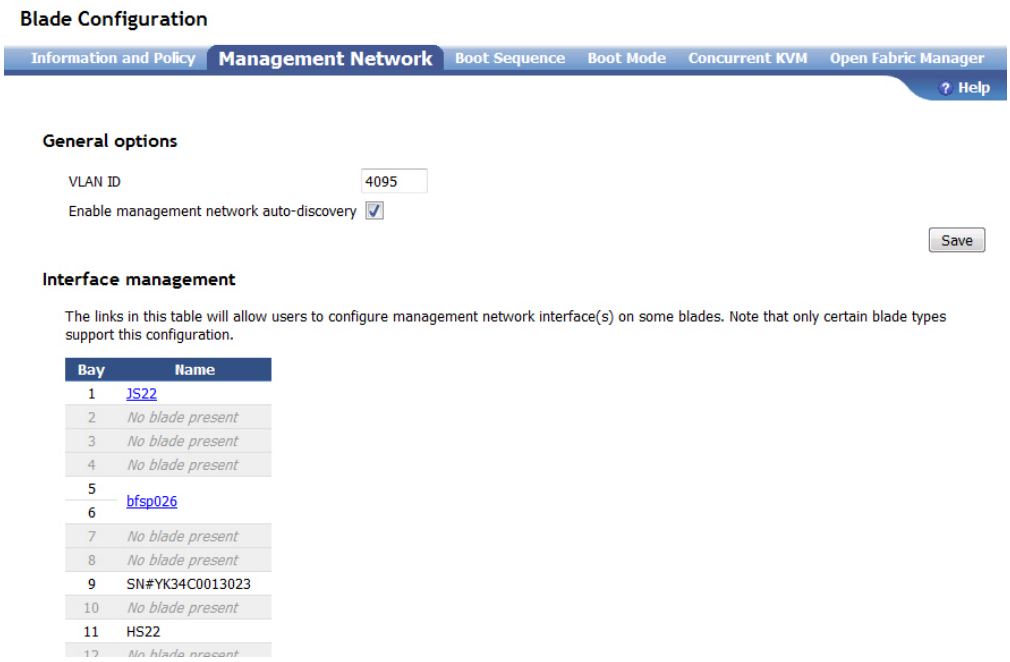
- Klicken Sie auf **Advanced Blade Policy Settings** (Erweiterte Blade-Richtlinieneinstellungen), um die Seite aufzurufen, auf der Sie die Ethernet-Schnittstelle an den Serviceprozessoren der Blade-Server inaktivieren oder aktivieren können. Für die Installation einiger Linux-Betriebssysteme über ein Netz muss bei einigen Serviceprozessoren die Ethernet-zu-USB-Schnittstelle inaktiviert sein. Erweiterte Blade-Richtlinieneinstellungen werden nicht von allen Blade-Servern unterstützt.

Klicken Sie auf **Management Network Configuration** (Verwaltungsnetzkonfiguration), um die VLAN-ID für das interne Verwaltungsnetz zu konfigurieren, die für die Kommunikation zwischen dem erweiterten Managementmodul und den BSMPs der Blade-Server verwendet wird. Wenn **Enable management network auto discovery** (Automatische Erkennung des Verwaltungsnetzes aktivieren) ausgewählt wird, können alle MCAD-fähigen (Management Channel Auto Discovery, Automatische Erkennung des Verwaltungskanals) Blade-Server und das erweiterte Managementmodul bestimmen, welcher Übertragungskanal basierend auf den in einem Blade-Server installierten Erweiterungskarten und den in der BladeCenter-Einheit installierten E/A-Modulen verwendet werden soll.

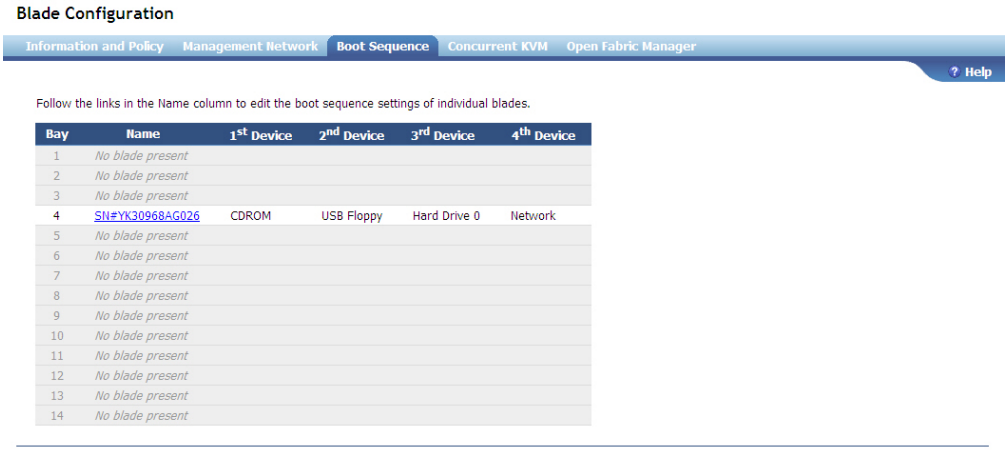
Der Kommunikationspfad erhält automatisch eine höhere Priorität für Hochgeschwindigkeits-E/A-Module. Die automatische Erkennung des Verwaltungskanals wird vom BSMP oder von einem MCAD-fähigen Serviceprozessor gesteuert. Der Pfad für die Übertragung von Kommunikationsdaten kann vom Benutzer nicht manuell festgelegt werden. Weitere Informationen zur MCAD-Konfiguration finden Sie im Abschnitt „Automatische Erkennung des Verwaltungskanals verwenden" auf Seite 83, im *BladeCenter SOL-Installationshandbuch* sowie in der Dokumentation zu Ihrem Blade-Server.

Für jeden Blade-Server, der die manuelle Konfiguration seiner Verwaltungsnetzschnittstelle ermöglicht, wird im Abschnitt "Interface Management" (Schnittstellenverwaltung) ein Link angezeigt. Wenn Sie auf diesen Link klicken, wird ein Bildschirm angezeigt, auf dem Sie die Netzkonfiguration für den Serviceprozessor im Blade-Server einrichten können. Weitere Informationen zum manuellen Konfigurieren des Verwaltungsnetzes eines Blade-Servers finden Sie im Abschnitt „Blade-Server-Verwaltungsnetz konfigurieren" auf Seite 24 sowie in der Dokumentation zu Ihrem Blade-Server.

Anmerkung: Diese Funktion wird nicht von allen Blade-Servern unterstützt.



Klicken Sie auf **Boot Sequence** (Startreihenfolge), um die Startreihenfolge für einen oder mehrere Blade-Server anzuzeigen oder zu definieren. Mit der Startreihenfolge werden für die Bootsatzquellen für einen Blade-Server Prioritäten festgelegt.



Für Ihre BladeCenter-Einheit und Ihre Blade-Server stehen die folgenden Startreihenfolgen zur Verfügung. Für einige Blade-Server-Typen sind möglicherweise weitere Booteinheiten verfügbar.

- **Hard disk drives** (Festplattenlaufwerke, 0 bis 4). Die Auswahl von Festplattenlaufwerken hängt von den in Ihrem Blade-Server installierten Festplattenlaufwerken ab.
- **CD-ROM** (CD-ROM, optisches Laufwerk).
- **Diskette drive** (Diskettenlaufwerk, einige BladeCenter-Einheitentypen)
- **Network - PXE** (Netz - PXE). Wenn "Network - PXE" ausgewählt wird, wird beim nächsten Einschalten oder Neustarten des Blade-Servers versucht, einen PXE/DHCP-Netzstart durchzuführen.
- **USB modular flash drive** (Modulares USB-Flashlaufwerk)

  Anmerkungen: Das erweiterte Managementmodul ist mit zwei USB-Anschlüssen ausgestattet. Wenn Sie eine USB-Speichereinheit mit einem USB-Anschluss verbinden, kann diese auch von Blade-Servern in der BladeCenter-Einheit genutzt werden. Es gelten folgende Regeln für die Bestimmung des Blade-Servers, der die USB-Speichereinheit erkennen soll:

  – Für die BladeCenter-Einheit gilt: Die USB-Speichereinheit wird für den Blade-Server bereitgestellt, der das Eigentumsrecht für die KVM hat.

  – Für die BladeCenter H- oder HT-Einheit gilt: Die USB-Speichereinheit wird für den Blade-Server bereitgestellt, der das Eigentumsrecht für den Laufwerkschlitten hat.

  – Das erweiterte Managementmodul für die BladeCenter T-Einheit hat keine externen USB-Anschlüsse.

  – Damit das optische Laufwerk oder das Diskettenlaufwerk (einige BladeCenter-Einheitentypen) als Bootsatzquelle für einen Blade-Server verwendet werden kann, muss der Blade-Server als Eigner des optischen Laufwerks, des Diskettenlaufwerks (wenn dies für Ihre BladeCenter-Einheit unterstützt wird) und des USB-Anschlusses festgelegt sein. Sie legen das Eigentumsrecht fest, indem Sie entweder den CD/Diskette/USB-Auswahlknopf am Blade-Server drücken oder die Option **Remote Control** (Fernsteuerung) verwenden, die im Abschnitt „Remote Control (Fernsteuerung)” auf Seite 142 beschrieben wird.

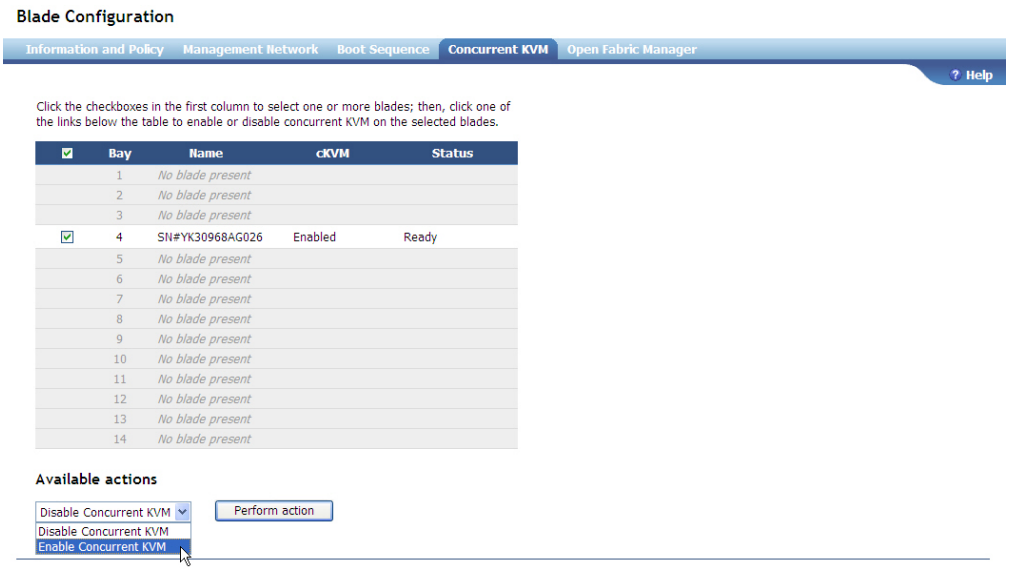
  – Einige Blade-Server unterstützen den Systemstart über ein Diskettenlaufwerk nicht.

- iSCSI boot devices (iSCSI-Booteinheiten). Wählen Sie **iSCSI Critical** (iSCSI kritisch) aus, um zu erzwingen, dass der Blade-Server nach einer iSCSI-Booteinheit sucht, bis er eine findet.

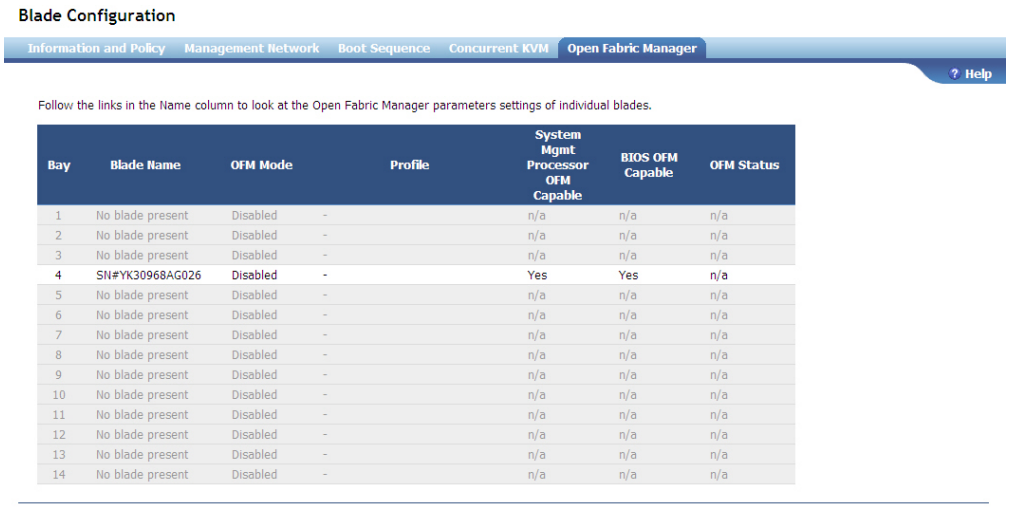
Klicken Sie auf **Boot Mode** (Bootmodus), um die BIOS- oder Systemfirmwarekopie auszuwählen, die beim Booten des Blade-Servers verwendet werden soll. Sie können eine primäre (temporäre) Kopie oder eine sekundäre (permanente) Kopie auswählen. Sie sollten von einer temporären Kopie aus starten, da diese in der Regel die aktuellen Erweiterungen und Aktualisierungen enthält. Zur permanenten Kopie sollten Sie nur wechseln, wenn das Booten von der temporären Kopie aus nicht mehr möglich ist. Änderungen an der Bootmoduseinstellung werden erst nach dem nächsten Neustart des Blade-Servers wirksam.

Anmerkung: Diese Funktion wird nicht von allen Blade-Servern unterstützt.

Klicken Sie auf **Concurrent KVM Configuration** (Gleichzeitige KVM-Konfiguration), um eine Liste mit Positionen, Blade-Servern und dem zugehörigen cKVM-Status anzuzeigen. Klicken Sie auf die Kontrollkästchen in der ersten Spalte, um einen oder mehrere Blade-Server auszuwählen. Klicken Sie anschließend auf einen der Links unterhalb der Tabelle, um eine Konfiguration für die gleichzeitige KVM-Steuerung auf den ausgewählten Blade-Servern zu aktivieren oder inaktivieren.

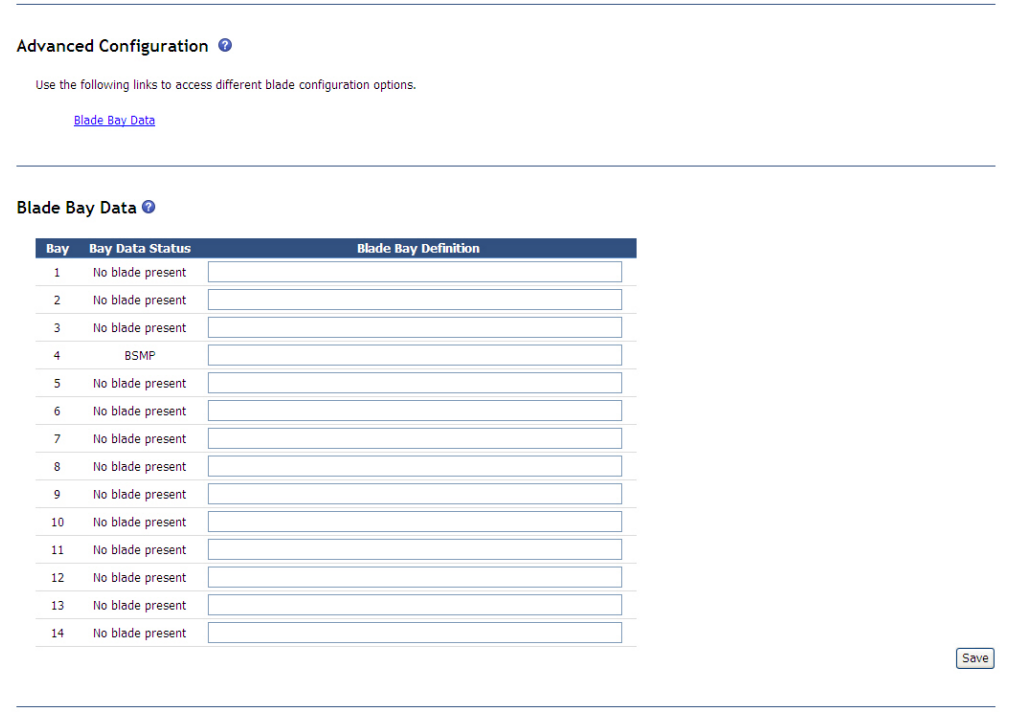


Wenn Ihre BladeCenter-Einheit die optionale Open Fabric Manager-Komponente verwendet, klicken Sie auf **Open Fabric Manager** (Open Fabric Manager), um eine Liste mit Positionen, Blade-Servern und den zugehörigen Open Fabric Manager-Parametern anzuzeigen. Klicken Sie anschließend auf einen der Links, um ausführliche Informationen zu den einzelnen Blade-Servern anzuzeigen.



Erweiterte Konfiguration:

Wählen Sie **Blade Tasks → Configuration → Advanced Configuration** (Blade-Tasks → Konfiguration → Erweiterte Konfiguration) aus, um Bladepositionsdaten anzuzeigen und zu bearbeiten.



Klicken Sie auf der Seite "Blade Information" (Informationen zum Blade) auf **Advanced Configuration** (Erweiterte Konfiguration), um Bladepositionsdaten anzuzeigen und zu bearbeiten.

Die Bladepositionsdaten sind im NVRAM (nicht flüchtiger Arbeitsspeicher) des erweiterten Managementmoduls gespeichert und der Bladeposition der BladeCenter-Einheit zugeordnet. Wenn Sie einen Blade-Server an eine neue oder andere Position

versetzen, erhält der Blade-Server die Bladepositionsdaten der neuen Position. Alle vorherigen Bladepositionsdaten im Blade-Server werden überschrieben.

Mithilfe von Bladepositionsdaten kann das Betriebssystem des Blade-Servers zur Unterstützung der eigenen Konfiguration bei der Initialisierung positionsspezifische Daten lesen. Diese Daten können Informationen dazu enthalten, welche Gerätetreiber oder Softwareoptionen geladen werden sollen und ob der Blade-Server eine übergeordnete Einheit oder Mitglied in einem System mit hoher Verfügbarkeit ist. Zudem können diese Daten die Gehäusenummer, die IP-Adresse und die für die Codelast zu verwendende PXE (Preboot eXecution Environment) beinhalten.

Sie können bis zu 60 alphanumerische Zeichen in das Feld **Blade Bay Definition** (Bladepositionsdefinition) eingeben, um Bladepositionsdaten zu definieren. Klicken Sie auf **Save** (Speichern), wenn Sie eine oder mehrere Definitionen von Bladepositionsdaten konfiguriert haben. Es kann möglicherweise einige Minuten dauern, bis das erweiterte Managementmodul diese Felder aktualisiert hat.

Das Betriebssystem des Blade-Servers kann Bladepositionsdaten entweder direkt aus dem BSMP des Blade-Servers oder über die Blade-Server-BIOS-SMBIOS-Struktur (System Management BIOS) lesen. Das Betriebssystem des Blade-Servers kann hierzu eine oder beide Methoden verwenden. Beide Methoden haben Vor- und Nachteile:

- Bladepositionsdaten sind über den BSMP sofort nach dem Speichern im Managementmodul verfügbar. Damit der Blade-Server IPMI-Befehle an den BSMP ausgeben kann, müssen jedoch mehr Gerätetreiber und Code auf dem Blade-Server ausgeführt werden.
- Das Betriebssystem kann mit weniger ausführbarem Code während der Initialisierung früher auf SMBIOS-Daten zugreifen. Das BIOS muss jedoch jedes Mal erneut ausgeführt werden, wenn Bladepositionsdaten im Managementmodul definiert oder geändert werden. Sie müssen den Blade-Server ausschalten, einschalten und erneut starten oder den Blade-Server entfernen und erneut installieren, um die aktuellen Bladepositionsdaten in der BIOS-SMBIOS-Datenstruktur zu speichern.

In der Spalte **Bay Data Status** (Status der Positionsdaten) wird der aktuelle Support und Status des Blade-Servers angegeben. Es werden die folgenden Statuswerte definiert:

Blade not present (Blade nicht vorhanden)
In der Position ist kein Blade-Server installiert.

Unsupported (Nicht unterstützt)
Die BSMP-Firmware des Blade-Servers unterstützt keine Funktionen für Bladepositionsdaten. Möglicherweise können Sie für die BSMP-Firmware ein Upgrade auf eine Version durchführen, die Bladepositionsdaten unterstützt.

BSMP
Der BSMP des Blade-Servers unterstützt Bladepositionsdaten, aber das BIOS hat die aktuelle Definition der Bladepositionsdaten nicht gelesen. Hierbei handelt es sich um einen Betriebszustand. Das Betriebssystem des Blade-Servers kann Bladepositionsdaten aus dem BSMP lesen. Wenn das Blade-Server-BIOS die Bladepositionsdaten nicht gelesen hat, muss es neu gestartet werden oder die Version der BIOS-Firmware muss auf eine Version aktualisiert werden, die Bladepositionsdaten unterstützt.

Supported (Unterstützt)
Der Blade-Server unterstützt Bladepositionsdaten vollständig. Die aktuelle Definition der Bladepositionsdaten ist sowohl im BSMP als auch in der BIOS-SM-BIOS-Struktur gespeichert.

Discovering (Erkennung)
Das erweiterte Managementmodul erkennt einen Blade-Server.

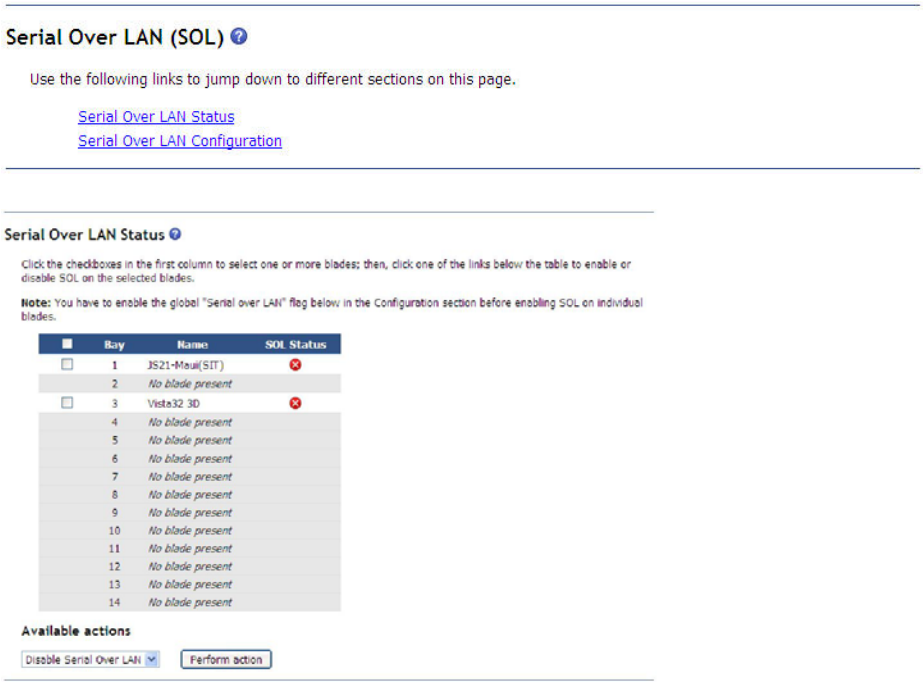
Anmerkung: Sie können Bladepositionsdaten definieren, auch wenn der Blade-Server keine Bladepositionsdaten unterstützt oder nicht installiert ist.

Für Schreiboperationen für Bladepositionsdaten sind Berechtigungen für die Blade-Konfiguration erforderlich. Wenn Sie keine Berechtigung zum Ändern dieser Felder haben, sind diese Felder nicht verfügbar.

Informationen und Anweisungen zur Verwendung der Befehlszeilenschnittstelle des Managementmoduls für diese Tasks finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des BladeCenter-Managementmoduls*.

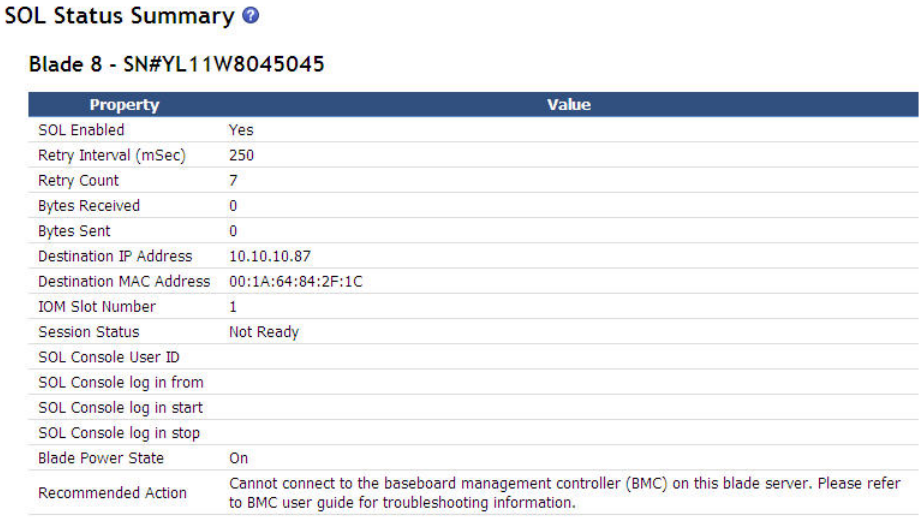
Serial Over LAN (Serial Over LAN)

Wählen Sie **Blade Tasks → Serial Over LAN** (Blade-Tasks → Serial Over LAN) aus, um den SOL-Status (Serial Over LAN) zu überwachen und SOL zu aktivieren oder inaktivieren.



Wählen Sie **Serial Over LAN** (Serial Over LAN) für die einzelnen Blade-Server und global für die BladeCenter-Einheit aus. Die globale Aktivierung oder Inaktivierung von SOL hat keine Auswirkungen auf den SOL-Sitzungsstatus der einzelnen Blade-Server. SOL muss sowohl global für die BladeCenter-Einheit als auch einzeln für die jeweiligen Blade-Server aktiviert werden, auf denen eine SOL-Sitzung gestartet werden soll. SOL ist standardmäßig global und auf den Blade-Servern aktiviert.

Klicken Sie auf das Symbol **SOL Status** (SOL-Status) für einen Blade-Server, um eine ausführliche Zusammenfassung des Status des Blade-Servers sowie empfohlene Aktionen anzuzeigen.



SOL Status Summary

Blade 8 - SN#YL11W8045045

Property	Value
SOL Enabled	Yes
Retry Interval (mSec)	250
Retry Count	7
Bytes Received	0
Bytes Sent	0
Destination IP Address	10.10.10.87
Destination MAC Address	00:1A:64:84:2F:1C
IOM Slot Number	1
Session Status	Not Ready
SOL Console User ID	
SOL Console log in from	
SOL Console log in start	
SOL Console log in stop	
Blade Power State	On
Recommended Action	Cannot connect to the baseboard management controller (BMC) on this blade server. Please refer to BMC user guide for troubleshooting information.

Klicken Sie auf den Link **SOL Status Summary** (SOL-Statuszusammenfassung), um die Informationen der Statuszusammenfassung für alle vom erweiterten Managementmodul verwalteten Blade-Server anzuzeigen.

Serial Over LAN Configuration

The SOL VLAN ID field can be configured on the Blade Configuration page.

Serial over LAN: Enabled

SOL VLAN ID: 4095

Transport Parameters

Accumulate timeout (in msec): 150

Send threshold (in bytes): 250

Retry count: 7

Retry interval (in msec): 250

User Defined Keystroke Sequences

'Enter CLI' key sequence: ^[(

'Reset blade' key sequence: ^[R^[r^[R

Save

Wählen Sie diese Option auch aus, um die globalen SOL-Einstellungen anzuzeigen und zu ändern, die von allen Blade-Servern in der BladeCenter-Einheit verwendet werden, und um SOL global für die BladeCenter-Einheit zu aktivieren oder inaktivieren.

Anmerkung: Beim erweiterten Managementmodul wird die von SOL verwendete **VLAN-ID** auf der Seite **Blade Tasks → Configuration** (Blade-Tasks → Konfiguration) festgelegt. Über diese Seite können Sie darüber hinaus auch die automatische Erkennung des Verwaltungskanals aktivieren, mit deren Hilfe SOL über ein in der BladeCenter-Einheit installiertes E/A-Modul kommunizieren kann. Informationen hierzu finden Sie im Abschnitt „Configuration (Konfiguration)” auf Seite 149.

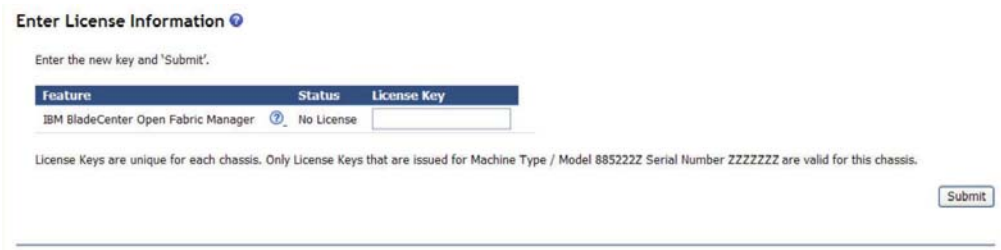
Mithilfe der Befehlszeilenschnittstelle des Managementmoduls können Sie SOL-Sitzungen starten und ausführen. Weitere Informationen hierzu finden Sie im *Refe-*

renzhandbuch zur Befehlszeilenschnittstelle des erweiterten BladeCenter-Managementmoduls und im *Serial Over LAN-Installationshandbuch*.

Open Fabric Manager (Open Fabric Manager)

Wählen Sie **Blade Tasks → Open Fabric Manager** (Blade-Tasks → Open Fabric Manager) aus, um Schnittstellen und Hardwareadapter zu verwalten.

Diese Task befindet sich in der Navigationsleiste unter **Blade Tasks** (Blade-Tasks) für erweiterte Managementmodule, die mit dieser Funktion ausgestattet sind. Wenn diese Funktion nicht aktiviert ist, wird eine Seite angezeigt, auf der Sie, wie in der folgenden Abbildung dargestellt, den Lizenzschlüssel für Ihre BladeCenter-Einheit eingeben können, sofern Sie bereits über einen Lizenzschlüssel verfügen.



Wenn die Funktion aktiviert ist, wird die Seite zur Konfiguration von Open Fabric Manager wie in der folgenden Abbildung angezeigt.

Anmerkung: Open Fabric Manager ist keine Standardkomponente des Managementmoduls, sondern erfordert einen Lizenzschlüssel, der gegen Aufpreis erhältlich ist. Lizenzschlüssel für Komponenten, die Sie für Ihre BladeCenter-Einheit erworben haben, erhalten Sie auf der Website http://licensing.datacentertech.net. Diese Website enthält eine Übersicht über den Vorgang der BladeCenter-Lizenzierung. Nachdem Sie den Lizenzschlüssel erhalten haben, müssen Sie ihn auf dem erweiterten Managementmodul installieren. (Informationen hierzu finden Sie im Abschnitt „License Manager (Lizenzmanager)" auf Seite 205.) Ausführlichere Informationen finden Sie in der Dokumentation zum *BladeCenter Open Fabric Manager*.

Verwenden Sie den Open Fabric Manager, um die Adressierung für Hardwareadapter zu aktivieren und festzulegen. Hierzu zählen die MAC-Adressen von Netzschnittstellenkarten sowie die weltweiten Knotennamen (WWNN, World Wide Node Name) und die weltweiten Portnamen (WWPN, World-Wide Port Name) von FC-Hostbusadaptern (Fibre Channel). Mithilfe dieser Funktion können Sie in den einzelnen BladeCenter-Einheiten virtuelle Adressen für Bladepositionen zuweisen. Wenn ein Blade-Server in eine Bladeposition eingesetzt wird und Open Fabric

Manager für diese Bladeposition aktiviert ist, wird die Open Fabric Manager-Konfiguration automatisch dem Blade-Server zugewiesen und der Blade-Server beginnt automatisch, diese Adressen zu verwenden. Sie können bis zu vier Arten von Adressen auswählen: Ethernet, Fibre Channel, SAS und virtuelle Netzschnittstellenkarte. Zudem können Sie die maximale Anzahl Offsets (0 bis 3) angeben, die unterstützt werden sollen, wenn Blade-Server mit mehrfacher Breite in der BladeCenter-Einheit installiert werden.

Sie können den Open Fabric Manager für bis zu 100 BladeCenter-Einheiten konfigurieren.

I/O Module Tasks (E/A-Modul-Tasks)

Wählen Sie die Option **I/O Module Tasks** (E/A-Modul-Tasks) aus, um die E/A-Module der Netzschnittstelle in der BladeCenter-Einheit zu verwalten.

Zur Option "I/O Module Tasks" (E/A-Modul-Tasks) gehören folgende Seiten:

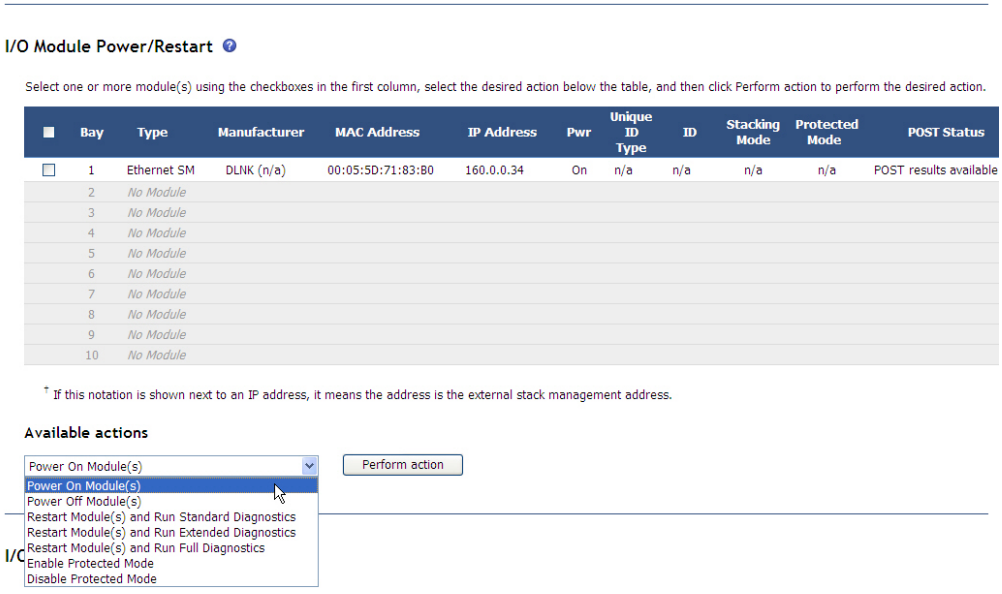
- „Admin/Power/Restart (Administration/Einschalten/Neustart)"
- „Configuration (Konfiguration)" auf Seite 163
- „Firmware Update (Firmwareaktualisierung)" auf Seite 167

Anmerkung: Einige Optionen sind nicht bei allen E/A-Modulen verfügbar.

Admin/Power/Restart (Administration/Einschalten/Neustart)

Wählen Sie die Option **I/O Module Tasks → Admin/Power/Restart** (E/A-Modul-Tasks → Administration/Einschalten/Neustart) aus, um den Stromversorgungsstatus der E/A-Module anzuzeigen und zu verwalten.

Die folgende Abbildung zeigt die Einstellungen für Stromversorgung und Neustart der E/A-Module für ein erweitertes Managementmodul.



Wählen Sie **Admin/Power/Restart** (Administration/Einschalten/Neustart) aus, um den Stromversorgungsstatus der E/A-Module anzuzeigen und folgende Aktionen auszuführen:

- Ein E/A-Modul ein- oder ausschalten
- Ein E/A-Modul erneut starten
- Den geschützten Modus für ein E/A-Modul aktivieren oder inaktivieren, das diese Funktion unterstützt. Wenn der geschützte Modus für ein E/A-Modul aktiviert ist, können die Einstellungen für dieses E/A-Modul nicht durch das Managementmodul konfiguriert werden. Sämtliche Einstellungen des E/A-Moduls müssen über die vom E/A-Modul bereitgestellte Verwaltungsschnittstelle konfiguriert werden. Wenn Sie den geschützten Modus durch das Managementmodul aktiviert oder inaktiviert haben, müssen Sie diese Funktion auch durch die Verwaltungskonsole des E/A-Moduls aktivieren oder inaktivieren und das E/A-Modul erneut starten. Das E/A-Modul bleibt im Status des geschützten Modus, der in der Verwaltungskonsole des E/A-Moduls festgelegt wurde, auch wenn es erneut gestartet oder in eine andere BladeCenter-Einheit versetzt wird. Weitere Informationen dazu finden Sie in der Dokumentation zu Ihrem E/A-Modul.

Anmerkung: Die BladeCenter S-Einheit unterstützt das RAID-SAS-Modul (RAID serial-attached SCSI, SAS), eine Einheit mit zwei Subsystemen: einem SAS-Switch und einem RAID-Controller. Wenn diese Einheit installiert ist, wird die Seite "Power/Restart" des E/A-Moduls wie folgt geändert:

- Die Spalten **MAC Address** (MAC-Adresse) und **IP Address** (IP-Adresse) zeigen die MAC-Adressen und die IP-Adressen der beiden Subsysteme an.
- Die Spalte **Pwr** (Stromversorgung) unterstützt eine dritte Statusnachricht: "Shutdown in Progress" (Systemabschluss wird ausgeführt). Dieser Status kann auftreten, wenn eine Aufforderung zum Ausschalten an das E/A-Modul gesendet wird, das zusätzliche Zeit benötigt, um noch anstehende Operationen abzuschließen und einen ordnungsgemäßen Systemabschluss durchzuführen. Zum Beispiel muss ein SAS-Controllermodul vor dem Ausschalten möglicherweise die noch anstehenden E/A-Operationen aus dem Datencache löschen, um die Datenintegrität sicherzustellen.
- Die Spalte **ID** (ID) zeigt die Kennungen der elementaren Produktdaten für beide Subsysteme an.
  - Das SAS-Switch-Subsystem weist eine Netzschnittstellenkarte (Network Interface Card, NIC) auf, die über eine direkte Ethernet-Verbindung zum erweiterten Managementmodul verfügt. Das obere Kennungsetikett mit der IP-Adresse, das mit "S" endet, ist die IP-Adresse des SAS-Switch-Subsystems.
  - Das RAID-Controller-Subsystem verfügt über eine Netzschnittstellenkarte und über eine indirekte Ethernet-Verbindung zum erweiterten Managementmodul durch das E/A-Modul in Position 1. Das untere Kennungsetikett, das mit "R" endet, ist das Etikett des RAID-Controller-Subsystems.

Bei jedem E/A-Modul können die folgenden Funktionen aktiviert oder inaktiviert werden:

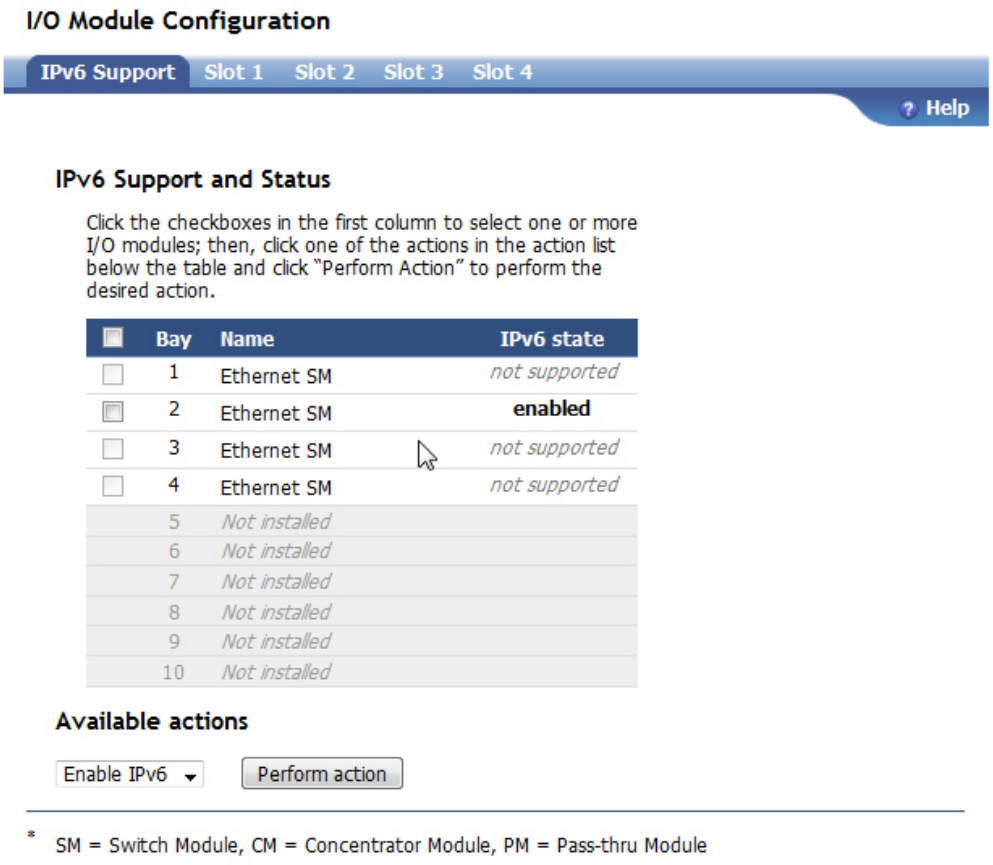
- Fast POST (Schneller Selbsttest beim Einschalten)
- External ports (Externe Anschlüsse)

Configuration (Konfiguration)

Wählen Sie die Option **I/O Module Tasks → Configuration** (E/A-Modul-Tasks → Konfiguration) aus, um die IP-Konfiguration der E/A-Module anzuzeigen oder zu ändern.

Anmerkung:

- Der Inhalt der Konfigurationsseiten der E/A-Module hängt vom jeweiligen Typ des E/A-Moduls ab. Auf den einzelnen Seiten werden nur die Einstellungen des jeweils installierten E/A-Moduls angezeigt. Einige E/A-Module verfügen über zusätzliche einheitenspezifische untergeordnete Seiten, die ausführlichere Informationen und Konfigurationsoptionen bereitstellen. Einheitenspezifische Informationen finden Sie in der Dokumentation zum betreffenden E/A-Modul.
- Die IPv6-Adressierung wird nicht von allen E/A-Modulen unterstützt.

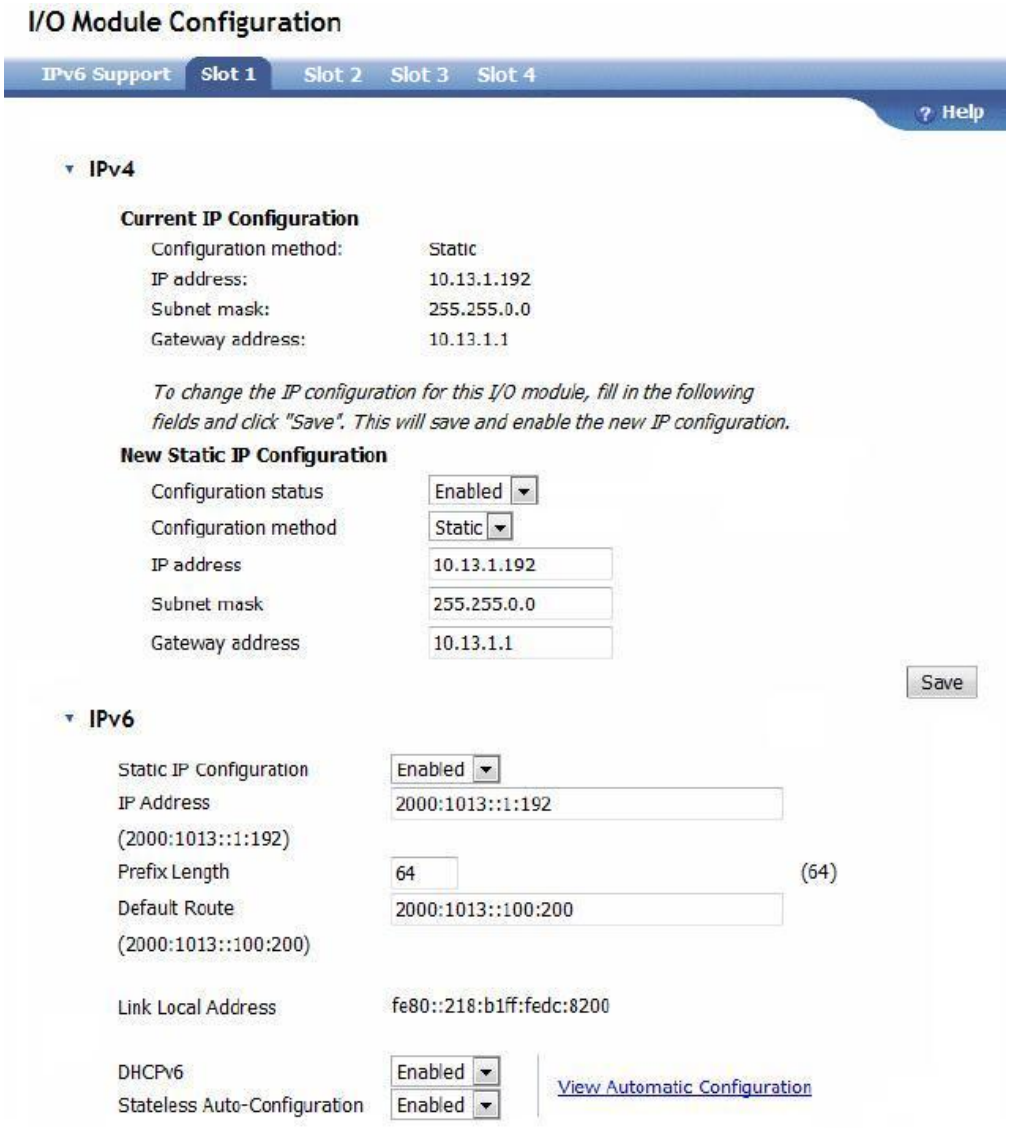


Die Konfigurationsseite des E/A-Moduls zeigt zunächst die Registerkarte zur IPv6-Unterstützung an. Hier können Sie den Status der IPv6-Unterstützung für die einzelnen E/A-Module anzeigen und ändern.

Für jedes E/A-Modul befindet sich oben auf der Konfigurationsseite für E/A-Module eine Registerkarte, die angibt, in welcher Position (Öffnung) es installiert ist. Wählen Sie eine Registerkarte aus, wenn Sie die Daten der einzelnen E/A-Module

anzeigen und ändern möchten. Auf dieser Seite können Sie auch die statische IPv4- und IPv6-Adressierung für das E/A-Modul aktivieren oder inaktivieren.

Anmerkung: Wenn sich in der ausgewählten Position das RAID-SAS-Modul befindet, können Sie ebenfalls diese Registerkarte auswählen, um die IP-Adresse, die Teilnetzmaske, die Gateway-Adresse und die VLAN-ID des RAID-Controller-Subsystems anzuzeigen und zu ändern. Diese Funktion wird von der BladeCenter S-Einheit unterstützt.



Wenn Sie die Webschnittstelle des Managementmoduls verwenden, um eine E/A-Modul-Konfiguration zu aktualisieren, schreibt die Firmware des Managementmoduls die Einstellungen für das E/A-Modul nur in den NVRAM (nicht flüchtiger Arbeitsspeicher) des Managementmoduls. Die Einstellungen werden nicht in den NVRAM des E/A-Moduls geschrieben.

Falls das E/A-Modul neu gestartet wird, wenn das Managementmodul die IP-Adresse des E/A-Moduls im NVRAM nicht anwenden kann, verwendet das E/A-Modul die in seinem NVRAM gespeicherte IP-Adresse. Stimmen die beiden IP-Adressen nicht überein, können Sie das E/A-Modul möglicherweise nicht mehr verwalten. Unter den folgenden Bedingungen kann das Managementmodul die in seinem NVRAM gespeicherte IP-Adresse des E/A-Moduls nicht verwenden:

- Das Managementmodul wird neu gestartet.
- Beim Managementmodul ist ein Fehler aufgetreten.
- Das Managementmodul wurde aus der BladeCenter-Einheit entfernt.

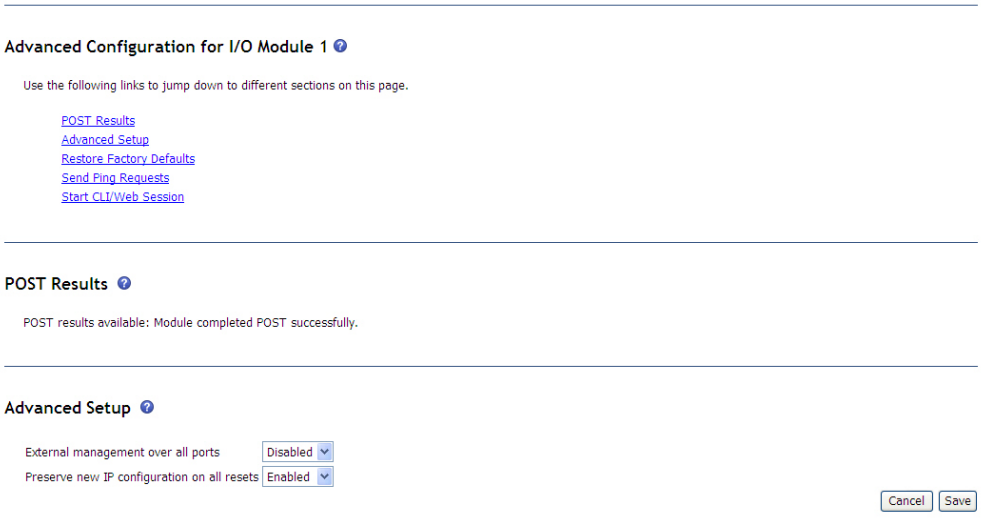
Sie müssen sich über die Telnet-Schnittstelle am E/A-Modul anmelden, die IP-Adresse ändern, sodass sie mit der dem Managementmodul zugewiesenen IP-Adresse übereinstimmt und dann die Einstellungen für das E/A-Modul in der Telnet-Sitzung speichern (**Basic Setup → Save Changes** (Basiskonfiguration → Änderungen speichern)).

Für die Datenübertragung von E/A-Modulen zu einer Fernverwaltungsstation über den externen Ethernet-Anschluss des Managementmoduls müssen sich die interne Netzschnittstelle des E/A-Moduls und die internen und externen Schnittstellen des Managementmoduls im selben Teilnetz befinden.

Wählen Sie die Option **Advanced Configuration** (Erweiterte Konfiguration) aus, um die Ergebnisse des Selbsttests beim Einschalten anzuzeigen, erweiterte Konfigurationstasks auszuführen, die werkseitigen Voreinstellungen für ein E/A-Modul wiederherzustellen, ein Ping-Signal an ein E/A-Modul zu senden oder eine CLI-/Web-Sitzung (Command Line Interface, Befehlszeilenschnittstelle) über Telnet zu starten.

Anmerkung: Bei einer CLI-Verbindung zu einem E/A-Modul muss der Browser für die Verwendung der Telnet-Anwendung auf Ihrem Host konfiguriert sein. Das erweiterte Managementmodul beinhaltet kein Telnet-Applet.

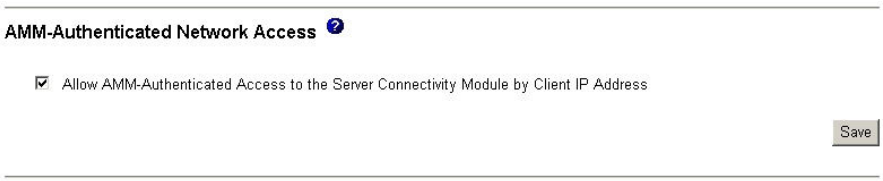
Wenn im System das RAID-SAS-Modul enthalten ist, können Sie mithilfe dieser Seite Ping-Signale senden oder eine CLI-Sitzung (Telnet) mit dem RAID-Subsystem herstellen. Diese Funktion wird von der BladeCenter S-Einheit unterstützt.



Anmerkungen:

- In der werkseitigen Voreinstellung der Firmware des E/A-Moduls sind folgende Benutzer-ID und folgendes Benutzerkennwort definiert:
  - User ID (Benutzer-ID): USERID (Großbuchstaben)
  - "Password" (Kennwort): PASSW0RD (Achten Sie darauf, dass in "PASSW0RD" eine Null (0), nicht der Buchstabe "O" steht)
- Wenn Ihr E/A-Modul sichere Websitzungen und eine NAT-Tabelle (Network Address Translation, Netzadressumsetzung) unterstützt, müssen diese in der NAT-Tabelle auf der Seite **Network Protocol Configuration** (Konfiguration des Netzprotokolls) konfiguriert werden.

Wählen Sie die Option **Network Protocol Configuration** (Konfiguration des Netzprotokolls) aus, um das Netzprotokoll für ein E/A-Modul, das NAT-Tabellen unterstützt, zu konfigurieren. Klicken Sie auf **Activate** (Aktivieren), um die Änderungen zu übernehmen.



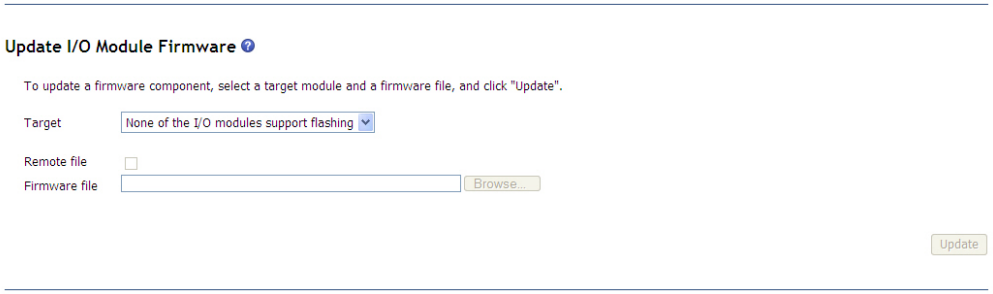
Wenn die Option **AMM-Authenticated Network Access** (Vom erweiterten Managementmodul authentifizierter Netzzugriff) aktiviert ist, können Benutzer erst dann eine Verbindung zu einem Server-Konnektivitätsmodul herstellen, nachdem das erweiterte Managementmodul die Anmeldung an der Webschnittstellensitzung von diesem Client authentifiziert hat. Der Zugriff von diesem Client wird nur inaktiviert, wenn der Benutzer sich abmeldet oder das Zeitlimit für die Webschnittstellensitzung abläuft. Mithilfe dieser Funktion kann der Verwaltungszugriff auf das Server-Konnektivitätsmodul auf die Benutzer beschränkt werden, die über die Administratorberechtigung für das erweiterte Managementmodul verfügen.

Wenn das E/A-Modul anzeigt, dass es eine sichere Webschnittstelle über SSL unterstützt, kann das erweiterte Managementmodul eine SSL-Sitzung mit dem E/A-Modul starten.

Weitere Informationen zur allgemeinen Konfiguration von E/A-Modulen finden Sie im *Installations- und Benutzerhandbuch* Ihrer BladeCenter-Einheit sowie im Abschnitt „E/A-Modul konfigurieren" auf Seite 95. Ausführliche Informationen zur Konfiguration und Verwaltung der Firmware für das E/A-Modul finden Sie in der Dokumentation zum E/A-Modul. Die Dokumentation zu einigen E/A-Modulen ist auf der IBM *Dokumentations*-CD für Ihre BladeCenter-Einheit enthalten.

Firmware Update (Firmwareaktualisierung)

Wählen Sie die Option **I/O Module Tasks → Firmware** (E/A-Modul-Tasks → Firmware) **Update** (Aktualisierung) aus, um die Firmware des E/A-Moduls zu aktualisieren.



Wichtig: Einige Clusterlösungen erfordern bestimmte Codeversionen oder koordinierte Code-Aktualisierungen. Wenn die Einheit zu einer Clusterlösung gehört, überprüfen Sie, ob die aktuelle Codestufe für die Clusterlösung unterstützt wird, bevor Sie den Code aktualisieren.

Anmerkung: Firmwareaktualisierungen sind nur für einige Typen von E/A-Modulen verfügbar.

Wählen Sie die Option **Firmware Update** (Firmwareaktualisierung) aus, um die Firmware des E/A-Moduls zu aktualisieren. Wählen Sie das betreffende E/A-Modul und die Firmwaredatei für die Aktualisierung aus und klicken Sie dann auf **Update** (Aktualisieren). Sie erhalten die Firmwaredateien unter der folgenden Adressehttp://www.ibm.com/systems/support/.

Mithilfe der Methode "Remote File" (Ferne Datei) können Sie die vollständig qualifizierte Adresse der Firmware-Paketdatei für die Aktualisierung der E/A-Firmware angeben. Die vollständig qualifizierte Adresse enthält ein Protokoll, das vom erweiterten Managementmodul unterstützt wird, gefolgt von einem Doppelpunkt und zwei Schrägstrichen (//), den Benutzernamen und das Kennwort, getrennt durch einen Doppelpunkt zur Authentifizierung bei der Anmeldung, ein At-Zeichen (@), gefolgt von dem Hostnamen oder von der IP-Adresse, eine optionale Anschlussnummer und den vollständigen Pfadnamen der Datei.

Anmerkung: Wenn die Anschlussnummer angegeben wird, muss sie durch einen Doppelpunkt vom Hostnamen (oder der IP-Adresse) getrennt werden.

Das vollständige Format lautet wie folgt: *Protokoll*://
Benutzername:*Kennwort*@*Hostname*:*Anschluss*/*Pfad*/*Dateiname*

Das erweiterte Managementmodul unterstützt die folgenden Protokolle:

- TFTP
- FTP
- FTPS
- HTTP
- HTTPS

Eine vollständig qualifizierte Adresse könnte zum Beispiel wie folgt aussehen:

```
ftp://USERID:PASSW0RD@192.168.0.2:30045/tmp/CNETCMUS.pkt
```

In diesem Beispiel wird das FTP-Protokoll für die Übertragung der Paketdatei verwendet, der Benutzername lautet `USERID`, das Kennwort ist `PASSW0RD`, die IP-Adresse des Hosts (IPv4) lautet `192.168.0.2`, die Anschlussnummer ist `30045` und `/tmp` ist der vollständige Pfadname der Paketdatei mit dem Namen `CNETCMUS.pkt`.

Bei manchen Protokollen müssen Benutzername, Kennwort und Anschlussnummer nicht angegeben werden. Die Mindestvoraussetzungen für eine vollständige Adresse können daher wie folgt aussehen:

Protokoll://*Hostname*/*Pfad*/*Dateiname*

Gehen Sie wie folgt vor, um die Firmware eines erweiterten Managementmoduls mithilfe einer fernen Datei zu aktualisieren:

1. Aktivieren Sie das Kontrollkästchen **Remote File** (Ferne Datei).
2. Geben Sie im Textfeld eine vollständig qualifizierte Adresse ein.
3. Klicken Sie auf die Schaltfläche **Update** (Aktualisieren) oder auf die Schaltfläche **Update and Reboot** (Aktualisieren und erneut starten).

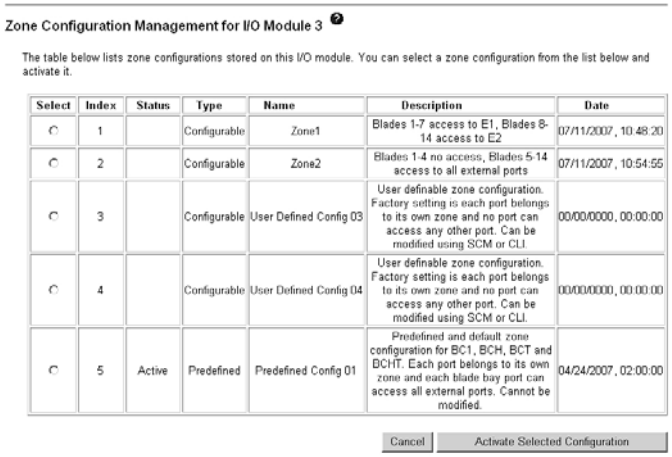
Anmerkung: Wenn Sie anstelle einer IP-Adresse einen Hostnamen verwenden, um eine ferne Datei anzugeben, stellen Sie sicher, dass DNS aktiviert ist.

Storage Tasks (Speicher-Tasks)

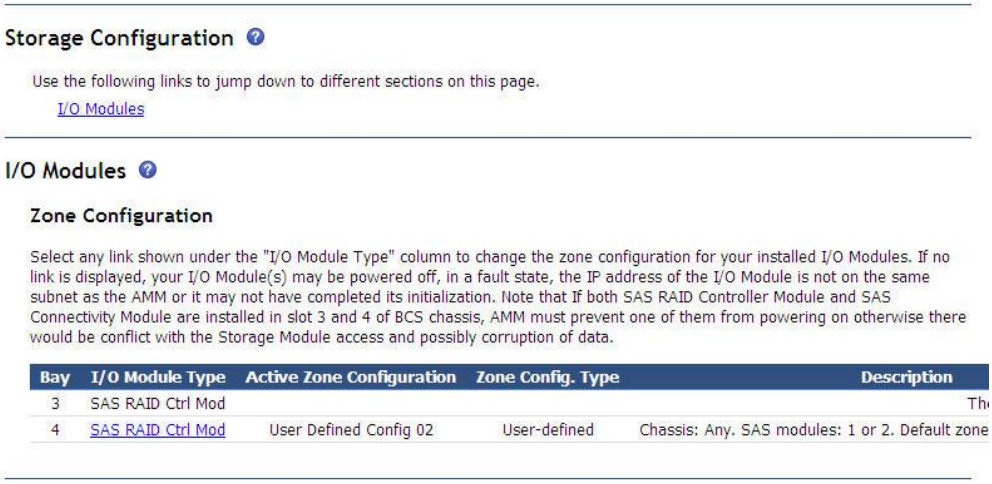
Die Seiten unter **Storage Tasks** (Speicher-Tasks) werden nur angezeigt, wenn das erweiterte Managementmodul in einer BladeCenter-Einheit installiert ist, in der auch Speicherkomponenten oder bestimmte Arten von E/A-Modulen installiert sind.

Wählen Sie im Abschnitt **Storage Configuration** (Speicherkonfiguration) eine Komponente aus, um ihre Speicherkonfigurationseinstellungen anzuzeigen und zu ändern. Diese Einstellungen sind nur verfügbar, wenn eine Speichereinheit in der BladeCenter-Einheit installiert ist. Wenn keine Speicherkomponenten installiert sind, wird der Abschnitt **Storage Configuration** (Speicherkonfiguration) nicht angezeigt.

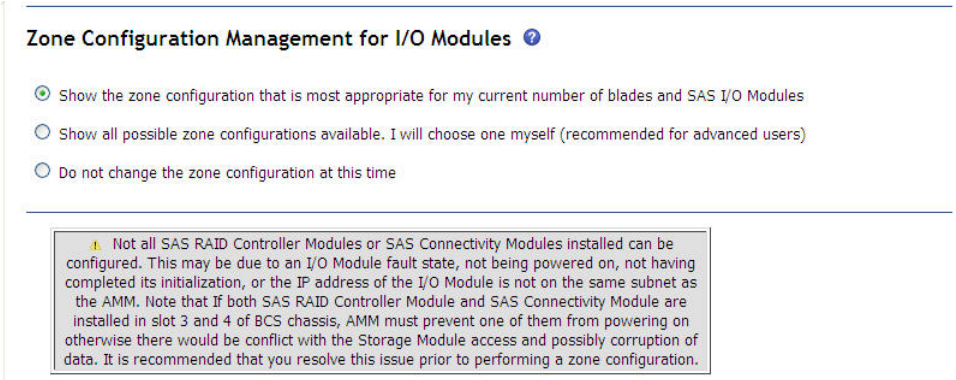
In der folgenden Abbildung ist ein Beispiel für die verfügbaren Speicherkonfigurationseinstellungen eines SAS-Konnektivitätsmoduls dargestellt. Ausführliche Informationen und Anweisungen zum Konfigurieren der Einheit finden Sie in der Dokumentation zu Ihrer Speichereinheit.

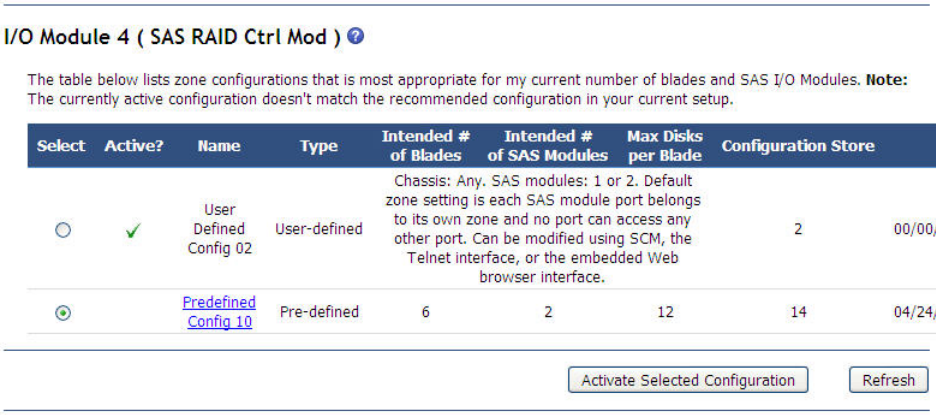


In der folgenden Abbildung ist ein Beispiel für die Speicherkonfigurationseinstellungen einer BladeCenter S-Einheit dargestellt.



Zum Ändern der Zonenkonfiguration für ein installiertes E/A-Modul klicken Sie auf seinen Link. Dadurch wird die Seite geöffnet, auf der Sie die Konfiguration von E/A-Modulen und die optionale SAS-RAID-Funktion verwalten können.





Wenn sowohl Speichermodule mit RAID als auch Speichermodule ohne RAID installiert sind, kann jeweils nur ein Modul eingeschaltet werden, um seine Zonenkonfiguration verwalten zu lassen. Wenn mehrere SAS-Module installiert und beide in Betrieb sind, stellen Sie sicher, dass die Standardeinstellung verwendet wird, um dieselbe Zonenkonfiguration auf jedes SAS-Modul anzuwenden. Zum Anwenden unterschiedlicher Zonenkonfigurationen verwenden Sie die Tabelle für separate Zonenkonfigurationen für die SAS-Module.

MM Control (MM-Steuerung)

Mit den Optionen unter **MM Control** (MM-Steuerung) können Sie die Einstellungen oder die Konfiguration des Managementmoduls, an dem Sie angemeldet sind (primäres Managementmodul), über die Webschnittstellensitzung des Managementmoduls anzeigen und ändern.

Wenn Ihre BladeCenter-Einheit über ein Bereitschaftsmanagementmodul verfügt, werden die Konfigurationseinstellungen des primären Managementmoduls automatisch auf das zweite Managementmodul übertragen. Diese Übertragung kann bis zu 45 Minuten dauern.

Die Konfiguration des Managementmoduls umfasst die folgenden Elemente:

- Name des Managementmoduls
- Bis zu 12 Anmeldeprofile für die Anmeldung am Managementmodul
- Ports, die das Managementmodul verwendet
- Handhabung von Alerts
- Übertragungseinstellungen für den seriellen Anschluss des erweiterten Managementmoduls
- Die Ethernet-Verbindungen des Managementmoduls für die ferne Konsole und die Datenübertragung zu den E/A-Modulen
- Einstellungen für die folgenden Protokolle:
  - FTP (File Transfer Protocol)
  - LDAP (Lightweight Directory Access Protocol)
  - NTP (Network Time Protocol)
  - SSH (Secure Shell)
  - SLP (Service Location Protocol) für Server
  - SMTP (Simple Mail Transfer Protocol)
  - SNMP (Simple Network Management Protocol)
  - SMASH CLP (Command Line Protocol)
  - Syslog-Protokoll
  - TCP-Befehlsmodusprotokoll
  - Telnet-Protokoll

  - TFTP (Trivial File Transfer Protocol)
- Einstellungen für SSL- (Secure Sockets Layer) und SSH-Sicherheit (Secure Shell)
- Sicherheitseinstellungen, wie z. B. Datenverschlüsselung und Kontosicherheit

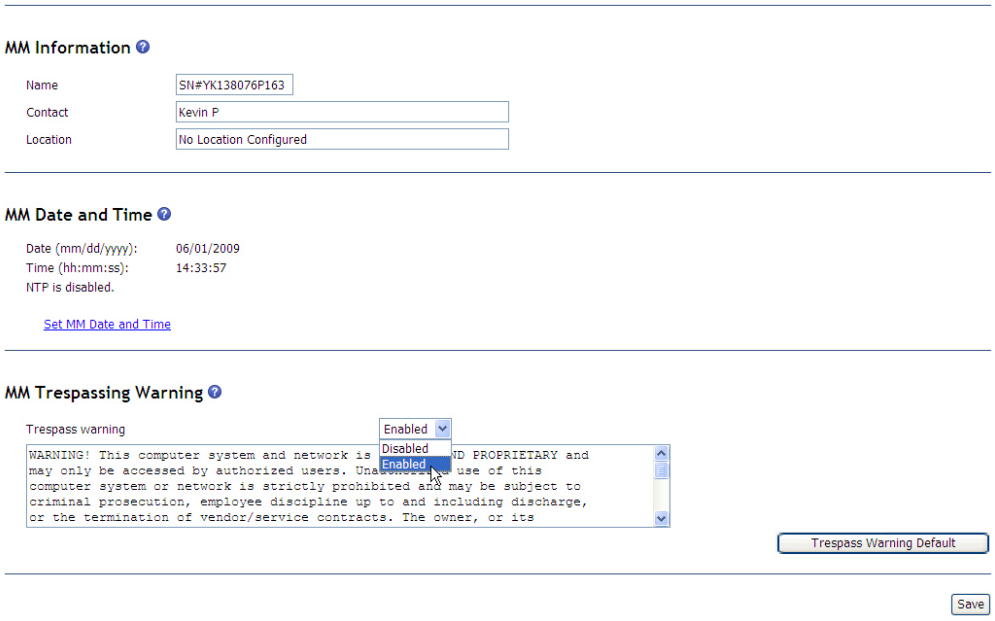
Dazu gehört auch die Ausführung folgender Tasks:
- Sicherung und Wiederherstellung der Konfiguration des Managementmoduls
- Aktualisierung der Firmware des Managementmoduls
- Wiederherstellung der Standardkonfiguration
- Neustart des Managementmoduls
- Umschalten vom primären, derzeit aktiven Managementmodul auf das Bereitschaftsmanagementmodul (bei BladeCenter-Einheiten, die redundante Managementmodule unterstützen)

Anmerkung: Bei BladeCenter-Einheiten mit einem Bereitschaftsmanagementmodul wird die Steuerung nach einem Ausfall des primären Managementmoduls automatisch auf das Bereitschaftsmanagementmodul umgeschaltet.

General Settings (Allgemeine Einstellungen)

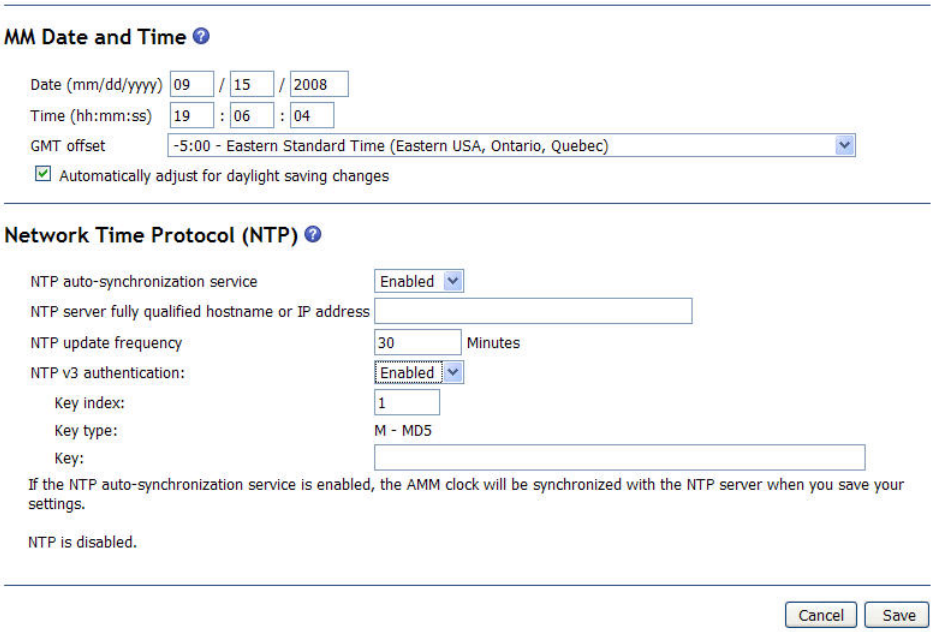
Wählen Sie **MM Control → General Settings** (MM-Steuerung → Allgemeine Einstellungen) aus, um ausführlichere Informationen einzugeben, wie zum Beispiel Uhrzeit, Datum und Standort.

Die folgende Abbildung zeigt die Seite "General Settings" eines erweiterten Managementmoduls.



Wählen Sie die Option **General Settings** (Allgemeine Einstellungen) aus, um die folgenden Einstellungen anzuzeigen oder zu ändern:

- Den Namen des Managementmoduls
- Den Namen des Ansprechpartners, der für das Managementmodul verantwortlich ist
- Den physischen Standort des Managementmoduls
- Die Taktgebereinstellungen im Managementmodul, beispielsweise die NTP-Einstellungen (Network Time Protocol) für das erweiterte Managementmodul. Über die NTP-Einstellungen können Sie eine automatische Synchronisation vornehmen, die IP-Adresse des NTP-Servers und die Aktualisierungsfrequenz festlegen sowie angeben, wie oft das Managementmodul eine Verbindung herstellt.



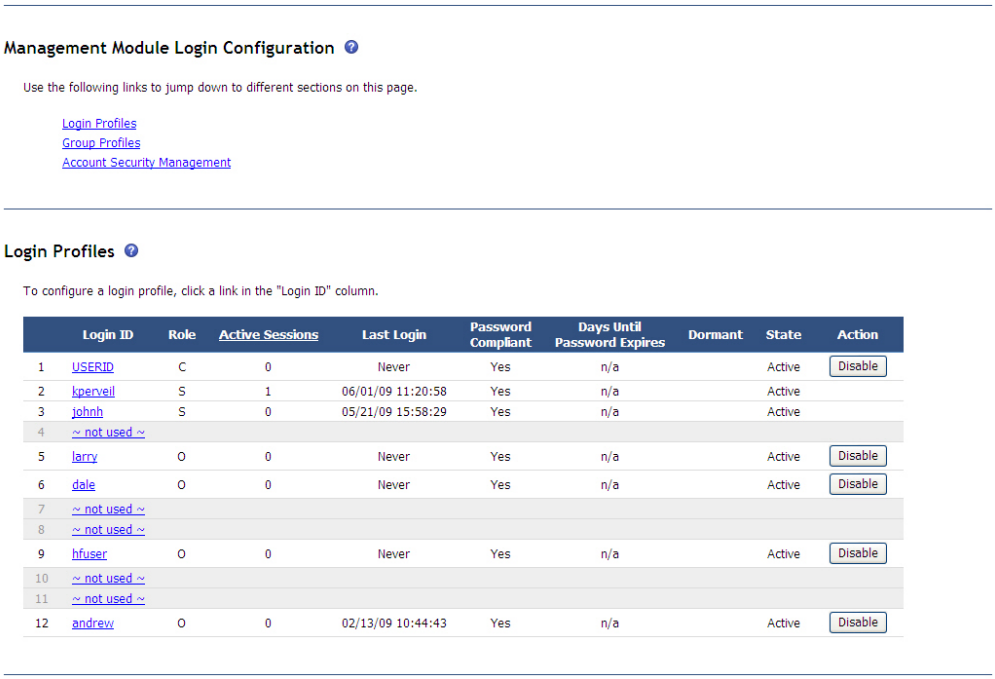
- Aktivieren oder inaktivieren Sie die Überschreitungswarnung und ändern Sie den Text der Warnung. Wenn die Warnung aktiviert ist, wird den Benutzern jedes Mal, wenn sie sich am Managementmodul anmelden, diese Nachricht angezeigt.

Einige der allgemeinen Einstellungen werden während der SNMP- und SMTP-Konfiguration verwendet. Weitere Informationen hierzu finden Sie in den Abschnitten „SNMP (Simple Network Management Protocol) konfigurieren" auf Seite 28 und „SMTP (Simple Mail Transfer Protocol) konfigurieren" auf Seite 32.

Login Profiles (Anmeldeprofile)

Wählen Sie die Option **MM Control → Login Profiles** (MM-Steuerung → Anmeldeprofile) aus, um Benutzernamen und Berechtigungen zu verwalten.

Die folgende Abbildung zeigt die Seite "Login Profiles Settings" (Anmeldeprofile, Einstellungen) für ein erweitertes Managementmodul.



Management Module Login Configuration

Use the following links to jump down to different sections on this page.

Login Profiles
Group Profiles
Account Security Management

Login Profiles

To configure a login profile, click a link in the "Login ID" column.

	Login ID	Role	Active Sessions	Last Login	Password Compliant	Days Until Password Expires	Dormant	State	Action
1	USERID	C	0	Never	Yes	n/a		Active	Disable
2	kperveil	S	1	06/01/09 11:20:58	Yes	n/a		Active	
3	johnh	S	0	05/21/09 15:58:29	Yes	n/a		Active	
4	~ not used ~								
5	larry	O	0	Never	Yes	n/a		Active	Disable
6	dale	O	0	Never	Yes	n/a		Active	Disable
7	~ not used ~								
8	~ not used ~								
9	hfuser	O	0	Never	Yes	n/a		Active	Disable
10	~ not used ~								
11	~ not used ~								
12	andrew	O	0	02/13/09 10:44:43	Yes	n/a		Active	Disable

Sie können bis zu 12 Anmeldeprofile für das Managementmodul konfigurieren. Wählen Sie **Login Profiles** (Anmeldeprofile) aus, um Informationen zu den einzelnen Anmeldeprofilen anzuzeigen. Alle Typen von Managementmodulen zeigen die Anmelde-ID und die Berechtigungsklasse oder die Zugriffsebene an, die den einzelnen Benutzern zugeordnet sind: "Supervisor" (S) (Administrator), "Operator" (O) (Bediener) oder "Custom" (C) (Benutzerdefiniert).

Bei erweiterten Managementmodulen werden außerdem die folgenden Informationen angezeigt:

- Die derzeit am Managementmodul angemeldeten Benutzer.
  - Klicken Sie auf die Spaltenüberschrift **Active Sessions** (Aktive Sitzungen), um detaillierte Informationen zu allen angemeldeten Benutzern anzuzeigen oder um die Sitzung eines angemeldeten Benutzers zu beenden.
  - Klicken Sie auf die **Login ID** (Anmelde-ID) eines Benutzers, um ein Kennwort zu ändern und die maximale Anzahl von Sitzungen festzulegen, die der Benutzer gleichzeitig öffnen kann.
- Das Datum und die Uhrzeit, zu der sich die einzelnen Benutzer zuletzt angemeldet haben.
- Hinweise darauf, ob das Benutzerkennwort mit der aktuellen Kennwortrichtlinie, die für die BladeCenter-Einheit festgelegt wurde, übereinstimmt.
- Die Anzahl der verbleibenden Tage, bevor das Benutzerkennwort abläuft.
- Ein Hinweis darauf, ob ein Benutzerprofil derzeit ruht (ob es für einen bestimmten Zeitraum, der im Zeitraum für den Inaktivitätsalert festgelegt ist, nicht verwendet wurde). Der Benutzer muss sich anmelden, um den Ruhezustand zu beenden.
- Der Status der einzelnen Benutzerprofile: Aktiv oder inaktiviert. Sie können die Profile "Operator" (Bediener) und "Custom" (Benutzerdefiniert) über eine Schaltfläche in der Spalte **Action** (Aktion) manuell aktivieren oder inaktivieren.

Klicken Sie auf eine Anmelde-ID, um bestimmte Einstellungen für ein Anmeldeprofil zu konfigurieren. Sie können auch die Einstellungen konfigurieren, die für alle Anmeldeprofile gelten. Bei erweiterten Managementmodulen werden diese Einstellungen im Bereich **Account Security Management** (Kontosicherheitsmanagement) konfiguriert. Klicken Sie auf die Anmelde-ID eines nicht verwendeten Profils, um ein Profil für einen neuen Benutzer zu konfigurieren.

Geben Sie bei jedem Benutzerprofil die folgenden Werte an:

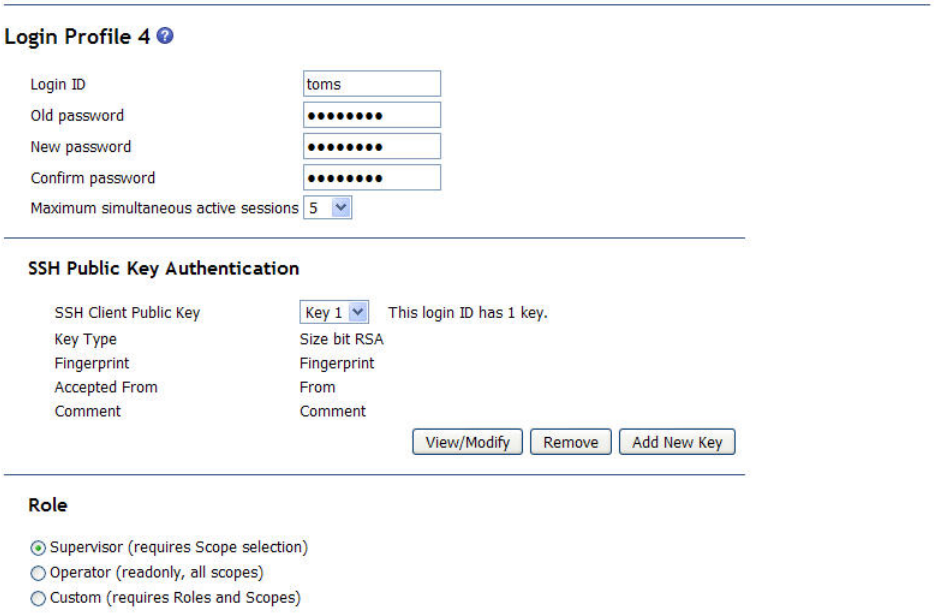
- Anmelde-ID
- Kennwort (erfordert Bestätigung)
- Berechtigungsklasse oder Berechtigungsebene (Standardeinstellung ist "Operator" (Bediener) oder "Read-Only" (Lesezugriff))

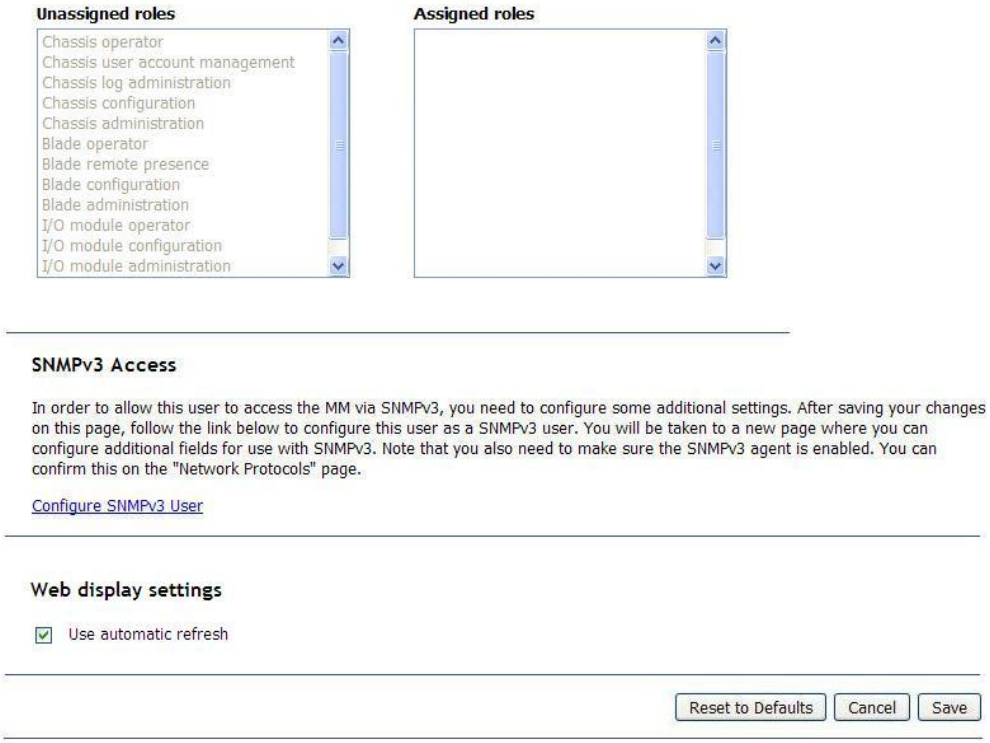
  Diese Einstellung legt die Befehlsbereiche fest, auf die ein Benutzer entsprechend seinen Zugriffsbefugnissen zugreifen kann. Berechtigungsklassen oder Berechtigungsebenen können sich abhängig vom Typ der verwendeten BladeCenter-Einheit und der jeweils installierten Firmware des Managementmoduls voneinander unterscheiden.
- Zugriffsbefugnisse

  Legt fest, in welchen Bereichen die für einen Benutzer definierte Berechtigungsklasse oder Benutzerberechtigung Gültigkeit besitzt.

Wichtig: Die Definitionen von Berechtigungsklassen oder Benutzerberechtigungen können sich je nach Firmware voneinander unterscheiden. Stellen Sie sicher, dass nach der Aktualisierung der Firmware des Managementmoduls für alle Benutzer die korrekten Berechtigungsklassen oder Berechtigungsebenen für Befehle festgelegt wurden.

Die folgende Abbildung zeigt die Einstellung der Benutzerprofile.



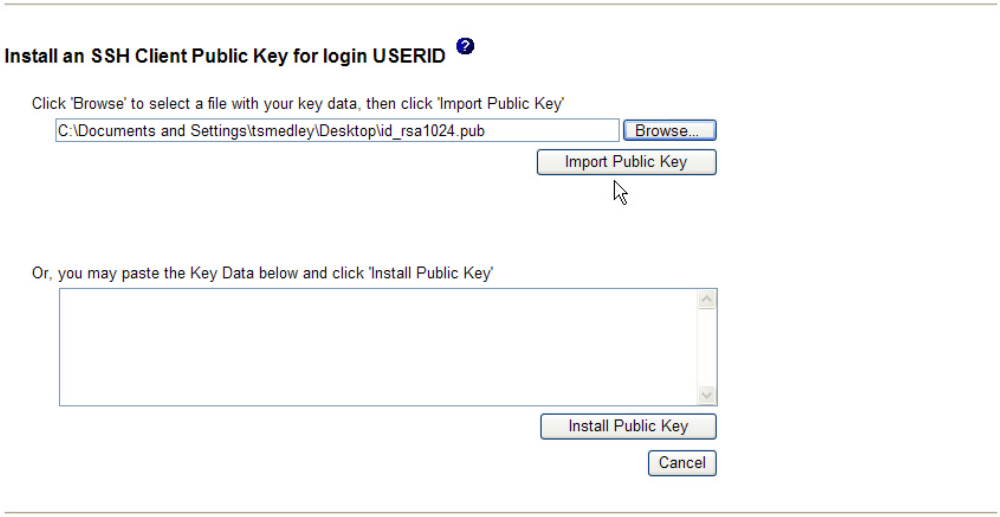


Klicken Sie auf **Configure SNMPv3 User** (SNMPv3-Benutzer konfigurieren), um eine zusätzliche Benutzerkonfiguration durchzuführen, die für SNMPv3 erforderlich ist (Anweisungen hierzu finden Sie im Abschnitt „SNMP (Simple Network Management Protocol) konfigurieren" auf Seite 28). Wenn in einem Benutzerprofil die automatische Aktualisierung für **Web display settings** (Web-Anzeigeeinstellungen) aktiviert ist, werden alle Webseiten der Benutzerschnittstelle des erweiterten Managementmoduls, die über die Fähigkeit zur automatischen Aktualisierung verfügen, während der Websitzungen für den betreffenden Benutzer automatisch aktualisiert. Wenn die automatische Aktualisierung inaktiviert ist, erfolgt für diesen Benutzer keine automatische Aktualisierung von Websitzungen.

Im Abschnitt "SSH Public Key Authentication" (Authentifizierung über öffentlichen SSH-Schlüssel) der Seite "Login Profile" (Anmeldeprofil) können Sie die öffentlichen SSH-Schlüssel des Benutzers hinzufügen, entfernen, anzeigen oder ändern. Beim Aufrufen der Seite "Login Profile" (Anmeldeprofil) auf dem erweiterten Managementmodul wird eine Zusammenfassung der Schlüsselinformationen für den ersten Schlüssel angezeigt (sofern vorhanden), der für das Anmeldeprofil installiert wurde. Sind mehrere Schlüssel für das Anmeldeprofil installiert, wählen Sie den Schlüssel aus, den Sie anzeigen, ändern oder aus der Liste entfernen möchten.

Wenn keine Schlüssel für dieses Anmeldeprofil installiert wurden, wird nur die Schaltfläche **Add New Key** (Neuen Schlüssel hinzufügen) angezeigt.

Auf der nächsten Seite können Sie einen öffentlichen Schlüssel importieren oder die Schlüsseldaten einfügen und einen öffentlichen Schlüssel installieren.



Das erweiterte Managementmodul akzeptiert öffentliche SSH-Schlüssel, die als öffentliche OpenSSH-Schlüssel formatiert sind. Schlüssel, die mit dem OpenSSH-Programm "ssh-keygen" erstellt wurden, sind zulässig. Die Länge des Schlüssels kann bis zu 4096 Bit betragen. Die Schlüsseltypen "ssh-rsa" und "ssh-dss" werden akzeptiert. In der Regel enthält der Schlüssel keine Zeilenumbruch- oder Zeilenvorschubzeichen. Diese sind jedoch zulässig, wenn die Schlüsseldaten mithilfe der Funktion "Paste" (Einfügen) in das Feld **Key Data** (Schlüsseldaten) eingefügt werden. Schlüssel im RFC4716-Format können nicht über die Webschnittstelle importiert werden. Verwenden Sie für den Import von Schlüsseln im RFC4716-Format die Befehlszeilenschnittstelle. Das akzeptierte Schlüsselformat kann bis zu vier Felder aufweisen, wie in folgendem Beispiel:

```
< Accepted From specification > < key type > < key data > < comment >
```

Die Parameter `< Accepted From specification >` (Akzeptiert von) und `<comment>` (Kommentar) sind optional. Zum Trennen der einzelnen Felder können Leerzeichen verwendet werden.

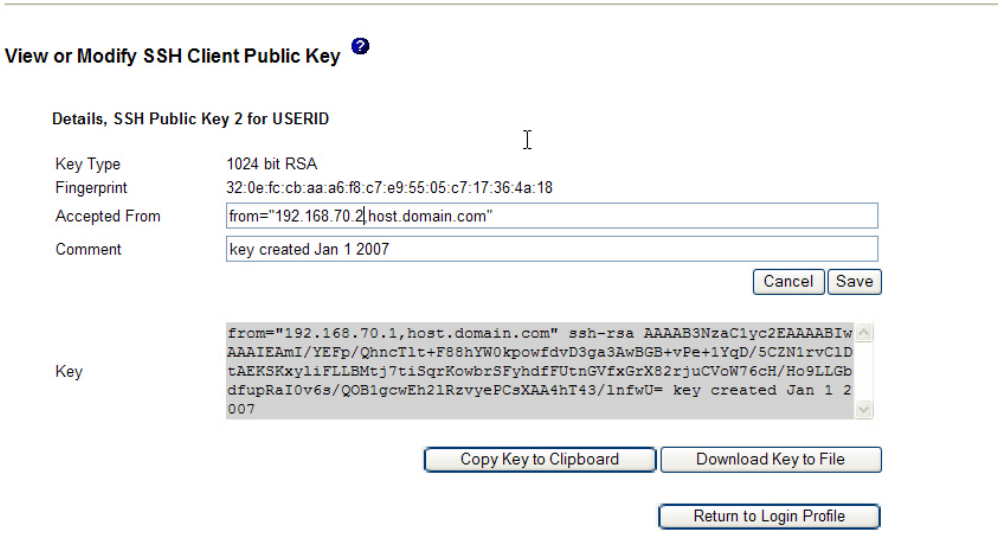
<Accepted From specification> (Die Spezifikation "Akzeptiert von")
Wird dieser Parameter nicht verwendet, wird der öffentliche SSH-Schlüssel von allen Hosts akzeptiert. Wird dieser Parameter verwendet, gibt er die Gruppe von fernen IP-Adressen und Hostnamen an, die diesen öffentlichen SSH-Schlüssel für die Authentifizierung über dieses Anmeldeprofil verwenden können. Die Spezifikation "Accepted From" (Akzeptiert von) hat folgendes Format `from=`*`pattern-list`*.

<key type> (Schlüsseltyp)
Der Schlüsseltyp muss entweder "ssh-rsa" oder "ssh-dss" sein.

<key data> (Schlüsseldaten)
Die Schlüsseldaten bestehen aus anzeigbaren Textzeichen. Leerzeichen, wie beispielsweise Leerschritte, Tabulatorzeichen oder Zeilenvorschub werden nicht unterstützt.

<comment> (Kommentar)
Dieser Parameter kann Textdaten zum Schlüssel enthalten. Mithilfe dieser Informationen können Sie die verschiedenen installierten Schlüssel verfolgen. Das Kommentarfeld wird im Authentifizierungsprozess nicht verwendet.

Wenn der Benutzer über einen öffentlichen Schlüssel verfügt, klicken Sie auf **View/ Modify** (Anzeigen/Ändern), um den ausgewählten Schlüssel anzuzeigen oder zu exportieren. Auf dieser Seite können Sie auch die Einträge in den Feldern "Accepted From" (Akzeptiert von) und "Comment" (Kommentar) für den ausgewählten Schlüssel ändern.



Die Felder auf dieser Seite haben folgende Funktionen:

Key Type (Schlüsseltyp)
Dieses Feld zeigt die Anzahl der Bits im Schlüssel und den Schlüsseltyp (DSA oder RSA) an.

Fingerprint (Fingerabdruck)
Dieses Feld zeigt einen 128-Bit-MD5-Fingerabdruck des installierten Schlüssels an.

Accepted From (Akzeptiert von)
Wenn dieses Feld leer ist, wird der öffentliche SSH-Schlüssel von allen Hosts akzeptiert. Ist dieses Feld nicht leer, wird hier die Gruppe von fernen IP-Adressen und Hostnamen angegeben, die den öffentlichen SSH-Schlüssel für die Authentifizierung verwenden können.

Comment (Kommentar)
Dieses Feld kann Textdaten zum Schlüssel enthalten. Mithilfe dieser Informationen kann der Administrator die verschiedenen installierten Schlüssel verfolgen. Das Kommentarfeld wird im Authentifizierungsprozess nicht verwendet.

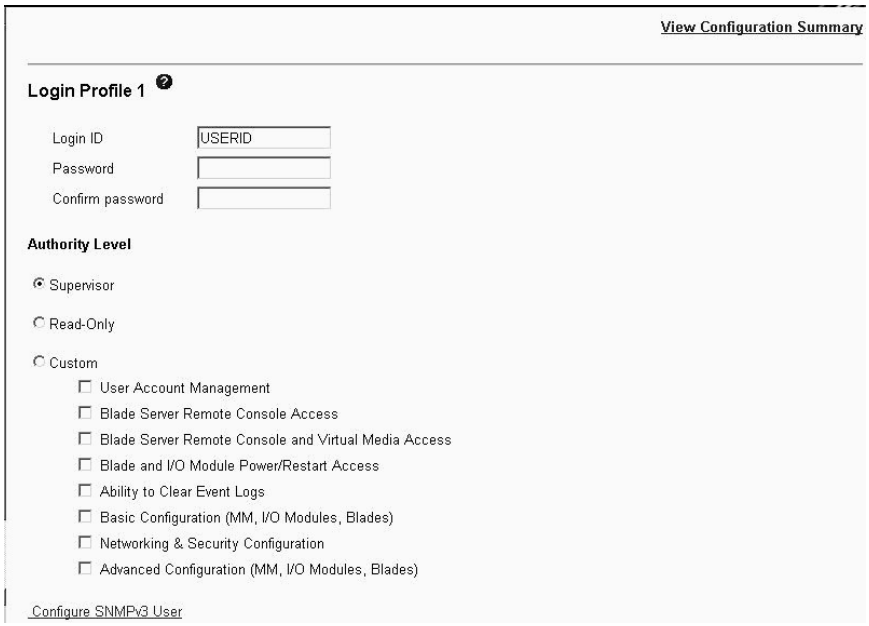
Sie können den Eintrag im Feld "Accepted From" (Akzeptiert von) auf dieser Seite aktualisieren, indem Sie die neue Spezifikation in das Feld eingeben und auf **Save** (Speichern) klicken. Die Spezifikation "Accepted From" (Akzeptiert von) hat folgendes Format:

`from=`*`pattern-list`*

Dabei steht "pattern-list" für eine durch Kommas getrennte Liste von Hostnamen und IP-Adressen.

Sämtliche Hostnamen und IP-Adressen können Platzhalterzeichen enthalten * (Stern) oder ? (Fragezeichen). Dabei steht der Stern für eine beliebige Zeichenfolge und das Fragezeichen für ein beliebiges einzelnes Zeichen. Wenn vor dem Hostnamen oder der IP-Adresse ein ! (Ausrufezeichen) steht, wird der Schlüssel von dem Host mit diesem Hostnamen oder dieser IP-Adresse nicht akzeptiert. Auf dem Managementmodul muss DNS aktiviert sein, wenn in der Spezifikation "Accepted From" (Akzeptiert von) Hostnamen verwendet werden. Der Zweck der Spezifikation "Accepted From" (Akzeptiert von) ist eine höhere Sicherheit: Die Authentifizierung über öffentlichen Schlüssel selbst vertraut nicht dem Netz, den Namensservern oder anderen Elementen, sondern ausschließlich dem Schlüssel). Wenn jedoch ein Eindringling den zu einem öffentlichen Schlüssel gehörenden privaten Schlüssel stiehlt, kann er sich mit diesem Schlüssel von einem beliebigen Standort weltweit aus anmelden. Diese zusätzliche Option erschwert die Verwendung eines gestohlenen Schlüssels. Zusätzlich zum Schlüssel müssten außerdem auf den Namensserver oder den Router oder auf beide ebenfalls Angriffe ausgeführt werden.

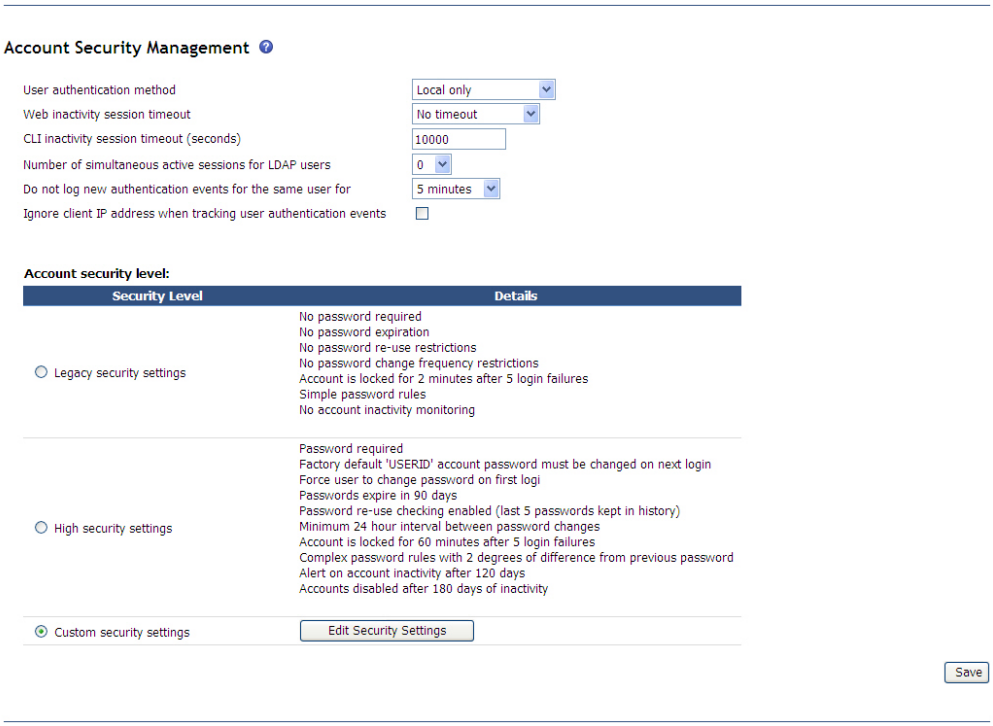
Die folgende Abbildung zeigt die Einstellungen der Benutzerprofile für ältere Firmwareversionen des Managementmoduls.



Es stehen verschiedene Benutzerrollen (Berechtigungsebenen) zur Verfügung und jede davon erteilt einem Benutzer den Schreib- und Lesezugriff auf verschiedene Bereiche der Funktionen des Managementmoduls und der BladeCenter-Komponenten. Benutzer mit Bedienerberechtigung verfügen nur über den Lesezugriff und können die Funktionen des Managementmoduls lediglich anzeigen. Über die Rolle "Custom" (Benutzerdefiniert) können einem Benutzer mehrere Rollen zugewiesen werden und Benutzer mit der Rolle "Supervisor" (Administrator) verfügen über den Schreib- und Ausführungszugriff für alle Funktionen innerhalb der ihnen zugewiesenen Bereiche.

Achtung: Wenn Sie die Standardeinstellung des Anmeldeprofils auf dem Managementmodul ändern, sollten Sie sicherstellen, dass Sie die Angaben zu Ihrer Anmelde-ID und Ihrem Kennwort an einem sicheren Platz aufbewahren. Wenn Sie die Anmelde-ID und das Kennwort für das Managementmodul vergessen haben, müssen Sie sich an den Service wenden.

Die folgende Abbildung zeigt den Bereich **Account Security Management** (Kontosicherheitsmanagement) für das erweiterte Managementmodul.



Sie können die folgenden Einstellungen ändern:

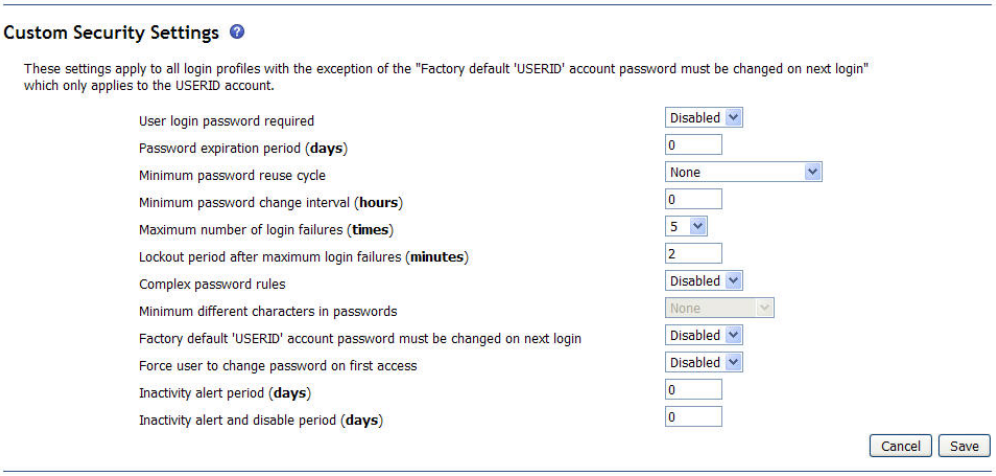
- Die Benutzerauthentifizierungsmethode (lokal, LDAP oder beide).
- Das Zeitlimit bei inaktiver Sitzung beim Zugriff über die Webschnittstelle und über die Befehlszeilenschnittstelle.
- Die Anzahl der simultanen aktiven Sitzungen für LDAP-Benutzer. Dieser Wert gilt für alle LDAP-Benutzer und gibt an, wie viele Sitzungen ein LDAP-Benutzer gleichzeitig öffnen kann. Der Mindestwert ist 1, der Maximalwert ist 20. Der Wert 0 bedeutet, dass für das Anmeldeprofil des Benutzers keine Sitzungsbegrenzung vorliegt.
- Ob neue Authentifizierungsereignisse für denselben Benutzer für ein angegebenes Intervall protokolliert werden sollen. Einige Scripts, die auf das Managementmodul zugreifen, können eine Vielzahl von Aktivitäten zur Benutzeranmeldung und -abmeldung generieren, die das Ereignisprotokoll des Managementmoduls mit An- und Abmeldeereignissen füllen können. In diesem Feld können Sie die Protokollierung von einigen oder allen dieser An- und Abmeldeereignisse unterdrücken. Wählen Sie **Log all** (Alle protokollieren) aus, um alle An- und Abmeldeereignisse eines Benutzers zu protokollieren. Wählen Sie **Log none** (Keine protokollieren) aus, um das Protokollieren dieser Ereignisse zu beenden. Mithilfe der anderen Optionen können Sie den Zeitraum festlegen, für den ein Benutzer inaktiv sein muss, bevor ein neuer Protokolleintrag zum Ereignisprotokoll hinzugefügt wird. Wenn Sie zum Beispiel **5 minutes** (5 Minuten)

auswählen und ein SNMP-Script über einen Benutzer verfügt, der sich jede Minute am Managementmodul anmeldet, wird nur die erste Anmeldung protokolliert. Dies ist eine globale Einstellung, die für alle Zugriffsmethoden und alle Benutzer gilt.

- Ob die Client-IP-Adresse bei der Verfolgung von Benutzerauthentifizierungsereignissen ignoriert werden soll. Dieses Kontrollkästchen ist nicht verfügbar, wenn die Option **Log all** (Alle protokollieren) oder **Log none** (Keine protokollieren) aktiviert ist. Andernfalls steht dieses Kontrollkästchen zur Verfügung und Sie können damit angeben, ob eine zweite Anmeldung desselben Benutzers von einem anderen Client aus als neue Anmeldeaktivität betrachtet werden soll. Wenn das Kontrollkästchen aktiviert ist, wird die zweite Anmeldung nicht als neue Aktivität betrachtet, andernfalls wird sie als neue Aktivität betrachtet. Wenn zum Beispiel die Option **5 minutes** (5 Minuten) im Feld **Do not log new authentication events for the same user** (Keine neuen Authentifizierungsereignisse für denselben Benutzer protokollieren) ausgewählt ist, dieses Kontrollkästchen aktiviert ist und ein Script über einen Benutzer verfügt, der sich alle 3 Minuten von zwei unterschiedlichen Clients aus am erweiterten Managementmodul anmeldet, wird nur die erste Anmeldung protokolliert. Im selben Szenario wird jedoch, wenn dieses Kontrollkästchen nicht ausgewählt ist, jede Benutzeranmeldung protokolliert, weil der Benutzer alle 6 Minuten von jeder Client-IP-Adresse auf das erweiterte Managementmodul zugreift. Dies ist eine globale Einstellung, die für alle Zugriffsmethoden und alle Benutzer gilt.
- Die Kontosicherheitsstufe, die für alle Benutzerprofile gilt. Es stehen zwei Optionen mit voreingestellten Werten zur Verfügung, sowie eine Option mit benutzerdefinierten Einstellungen, die eine Änderung der einzelnen Werte ermöglicht.
- Die minimalen Intervalle für eine Kennwortänderung. Hierbei handelt es sich um eine Sicherheitsfunktion, die begrenzt, wie oft Benutzer ihre Kennwörter ändern.

  Anmerkung: Wenn die Kontosicherheitseinstellungen Kennwörter erfordern, wird für jeden Benutzer, bei dem keine SNMPv3-Zugriffseinstellungen für die Verwendung von Kennwörtern konfiguriert wurden, ein Eintrag im Ereignisprotokoll erzeugt.

Die folgende Abbildung zeigt die **Custom Security Settings** (Benutzerdefinierte Sicherheitseinstellungen) für das erweiterte Managementmodul.

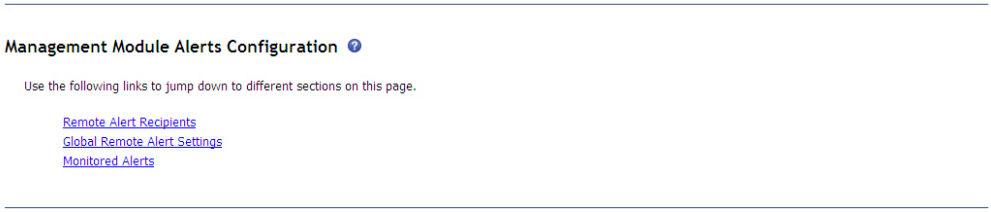


Anmerkung: Die Einstellung **Minimum password change interval** (Mindestintervall für Kennwortänderungen) ist eine Sicherheitsfunktion, die begrenzt, wie oft Benutzer ihre Kennwörter ändern. Mithilfe dieser Einstellung kann ein Benutzer daran gehindert werden, seine Kennwörter innerhalb kurzer Zeit häufig zu ändern und anschließend ein altes Kennwort zu verwenden.

Klicken Sie auf **View Configuration Summary** (Konfigurationszusammenfassung anzeigen), um die Konfigurationseinstellungen für alle BladeCenter-Benutzer und -Komponenten anzuzeigen.

Alerts

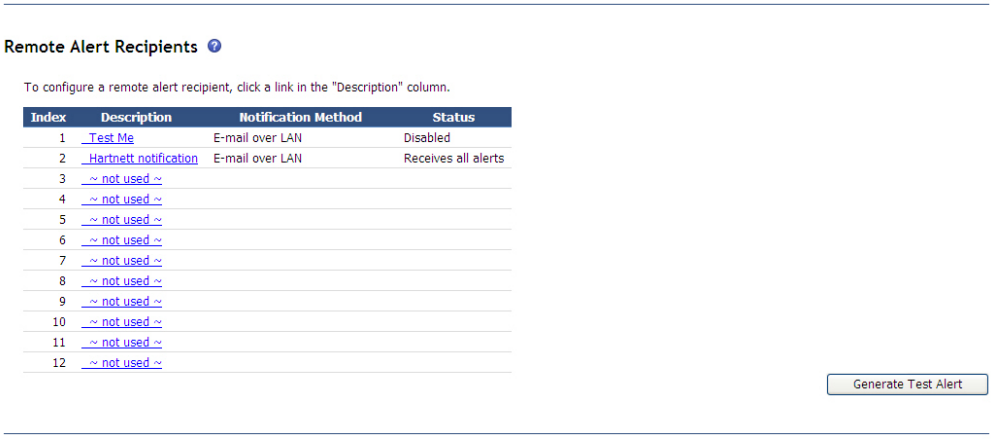
Wählen Sie die Option **MM Control → Alerts** (MM-Steuerung → Alerts) aus, um den Prozess zur Benachrichtigung von fernen Benutzern in Bezug auf bestimmte Ereignisse im BladeCenter-System zu verwalten.



Auf der Seite **MM Control → Alerts** (MM-Steuerung → Alerts) können Sie die folgenden Tasks ausführen:

- Empfänger der fernen Alerts definieren
- Globale Alert-Einstellungen definieren
- Überwachte Alerts definieren
- (Nur bei BladeCenter S- und BladeCenter T-Einheiten) Erinnerungen für Luftfilteraustausch verwalten

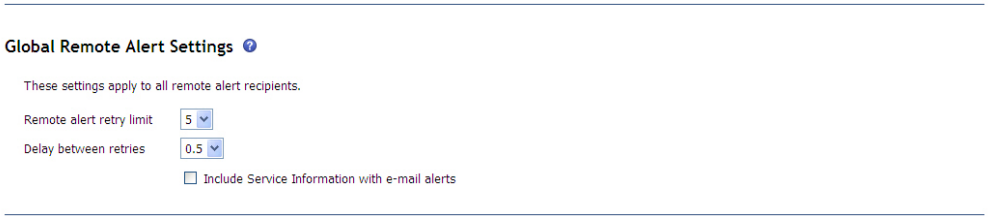
Wählen Sie **Remote Alert Recipients** (Empfänger der fernen Alerts) aus, um eine Liste aller Benutzer anzuzeigen, die bei Systemereignissen benachrichtigt werden müssen. Klicken Sie auf einen Benutzernamen, um eine zweite Seite anzuzeigen, in der Sie angeben können, welche Ereignisbenachrichtigungen gesendet werden, wie sie gesendet werden (SNMP, E-Mail oder IBM Systems Director), wohin sie gesendet werden (E-Mail-Adresse) und ob der Empfänger derzeit in der Lage ist, Benachrichtigungen zu empfangen. Klicken Sie auf **Generate Test Alert** (Testalerts generieren), um sicherzustellen, dass die Empfänger der fernen Alerts die Alerts wirklich erhalten.



Anmerkungen:

- IBM Systems Director (früher bekannt unter der Bezeichnung Netfinity Director oder IBM Director) ist ein Produkt zur Systemverwaltung, das im Lieferumfang der BladeCenter-Einheit enthalten ist. Wenn Sie den Empfänger der fernen Alerts für IBM Systems Director über ein LAN konfigurieren möchten, muss der Empfänger der fernen Alerts ein Server sein, der IBM Systems Director ausführen kann.
- IBM Systems Director empfängt alle Alerts vom erweiterten Managementmodul, auch wenn auf der Webseite unter **Monitored Alerts** (Überwachte Alerts) keine Alerts ausgewählt sind.
- Ein Empfänger, der die (umfassende) Benachrichtigungsmethode von IBM Systems Director verwendet, empfängt alle Alerts, die vom erweiterten Managementmodul generiert werden, unabhängig davon, ob der entsprechende Alerttyp aktiviert ist.

Wählen Sie **Global Remote Alert Settings** (Globale Einstellungen für ferne Alerts) aus, um anzugeben, wie oft das System versucht, einen Alert zu senden, wie lange die Wartezeit zwischen den Wiederholungen ist und ob die Serviceinformationen in die E-Mail-Alerts integriert werden sollen.

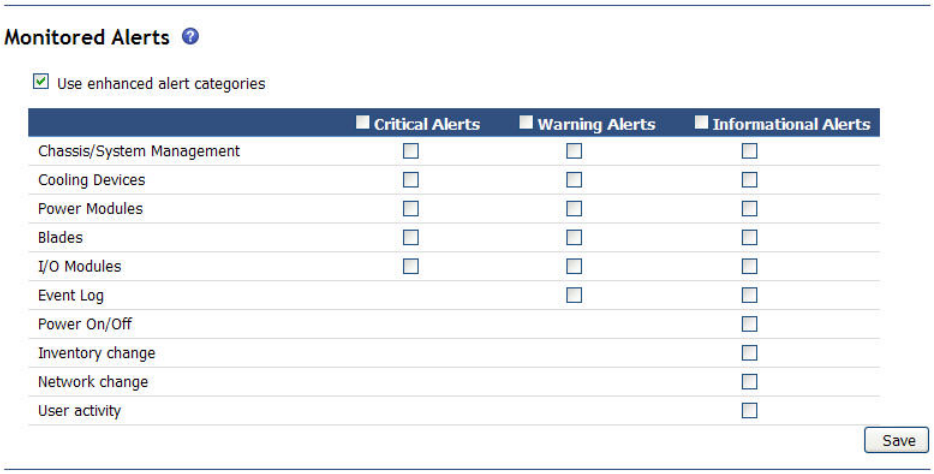


Wählen Sie die Option **Monitored Alerts** (Überwachte Alerts) aus, um anzugeben, welche Ereignisse (aus der Liste der kritischen Alerts, Warnungen und Systemalerts) überwacht werden, und um andere Parameter festzulegen. Die spezifischen Alerts, die Sie auswählen, gelten für alle konfigurierten Alertempfänger. Wenn der Alert ein behebbares Ereignis betrifft, wird ein Informationsalert derselben Kategorie gesendet, um darauf hinzuweisen, dass eine Wiederherstellung erfolgt ist.

Anmerkung: Die alten (traditionellen) Alertkategorien wurden durch neu definierte, erweiterte Alertkategorien ersetzt. Wenn das Kontrollkästchen **Use enhanced alert categories** (Erweiterte Alertkategorien verwenden) auf der Seite "Monitored

Alerts" (Überwachte Alerts) nicht aktiviert ist, behandelt das erweiterte Managementmodul Traps und Alerts auf dieselbe Weise wie vorher. Die Einstellungen können jedoch nicht mehr geändert werden. Wenn dieses Kontrollkästchen aktiviert ist, werden die derzeit festgelegten alten Kategorien in die neuen Kategorien überführt. Die Alertüberwachung sollte ebenfalls zur Verwendung der erweiterten Alertkategorien übergehen. Wenn dieses Kontrollkästchen einmal aktiviert wurde und die Migration der Alertkategorien erfolgt ist, wird das Kontrollkästchen **Use enhanced alert categories** (Erweiterte Alertkategorien verwenden) nicht mehr angezeigt. Sie können nicht mehr zu den alten (traditionellen) Kategorien zurückkehren.

Die folgende Abbildung zeigt die Seite "Monitored Alerts" (Überwachte Alerts) für ein erweitertes Managementmodul.



Die folgende Tabelle zeigt die Zuordnung der traditionellen zu den erweiterten Alertkategorien.

Tabelle 3. Traditionelle und erweiterte Alertkategorien

Traditionelle Alertkategorien	**Erweiterte Alertkategorien**
Temperatur	Blade-Server, E/A-Module und Gehäuse-/Systemverwaltung, falls zutreffend
Spannung	Blade-Server, E/A-Module und Gehäuse-/Systemverwaltung, falls zutreffend
Festplattenlaufwerk	Blade-Server
Fehler am Spannungsreglermodul	Blade-Server
Mehrere Gehäusekühleinheiten ausgefallen (Gebläse)	Kühleinheiten
Eine Gehäusekühleinheit ausgefallen (Gebläse)	Kühleinheiten
Netzausfall	Stromversorgungsmodule
Einschalten	Ein-/Ausschalten
Ausschalten	Ein-/Ausschalten
Mehrere E/A-Module ausgefallen	E/A-Module
Ungültige Konfiguration	E/A-Module

Tabelle 3. Traditionelle und erweiterte Alertkategorien (Forts.)

Traditionelle Alertkategorien	Erweiterte Alertkategorien
Fehler bei Übergabe der KVM-/ Laufwerkschlittensteuerung	Gehäuse-/Systemverwaltung
Blade-Drosselung	Gehäuse-/Systemverwaltung
Stromverbrauchssteuerung	Gehäuse-/Systemverwaltung
Ereignisprotokoll zu 100% beschrieben	Ereignisprotokoll
Ereignisprotokoll zu 75% beschrieben	Ereignisprotokoll
PFA	An betreffende Warnung weitergeleitet
Ausfall des redundanten Moduls	An betreffende Warnung weitergeleitet
Bestand	Bestandsänderung
Fernanmeldung	Benutzeraktivität
Netzänderung	Netzänderung

Im Abschnitt **Passive Air Filter Reminder** (Erinnerungen für Luftfilteraustausch) können Sie die Luftfilter für BladeCenter S- und BladeCenter T-Einheiten verwalten. Erinnerungen für den Luftfilteraustausch für die BladeCenter-Einheit werden automatisch verarbeitet. Weitere Informationen zu Erinnerungen für Luftfilteraustausch bei BladeCenter T- und BladeCenter HT-Einheiten finden Sie im Abschnitt „Erinnerung für Luftfilteraustausch" auf Seite 97.

Zum Einstellen von regelmäßigen Erinnerungen daran, dass der Luftfilter einer BladeCenter S-Einheit gewechselt werden muss, aktivieren Sie das Kontrollkästchen **Remind me to change this filter in** (An Filteraustausch erinnern) und wählen Sie ein Zeitintervall für die Erinnerungen aus. Die folgende Abbildung zeigt den Abschnitt **Passive Air Filter Reminder** (Erinnerungen für Luftfilteraustausch) für BladeCenter S-Einheiten.

Bei BladeCenter T-Einheiten ist das Erinnerungsintervall für den Austausch des Luftfilters auf sechs Monate festgelegt. Es kann nicht geändert werden. Sie können eine der folgenden Optionen zur Filterverwaltung auswählen:

- **Disable** (Inaktivieren): Die Services zur Luftfilterverwaltung werden abgeschaltet (es werden keine Alarmmeldungen oder Ereignisse für Filter generiert).
- **Enable** (Aktivieren): Das sechsmonatige Intervall für die Serviceerinnerung und die Erkennung fehlerhafter Filter sind eingeschaltet (nur bei BladeCenter T- und BladeCenter HT-Einheiten).
- **Restart** (Neustart): Die Services zur Luftfilterverwaltung werden zurückgesetzt (der Zeitplan für die Serviceerinnerungen wird so festgelegt, dass nach Ablauf des angegebenen Intervalls eine Erinnerung für den Luftfilteraustausch generiert wird).

Serial Port (Serieller Anschluss)

Wählen Sie **MM Control → Serial Port** (MM-Steuerung → Serieller Anschluss) aus, um Übertragungseinstellungen für den seriellen Anschluss des erweiterten Managementmoduls zu konfigurieren.

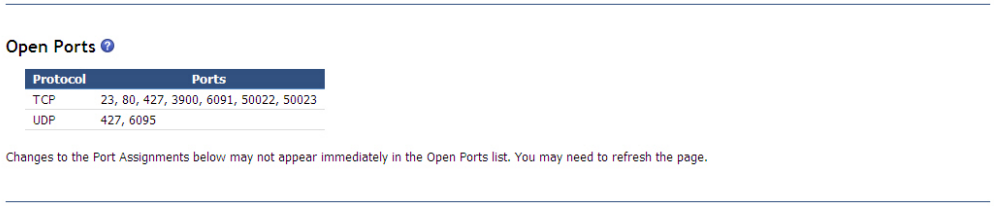
Sie können die Einstellungen des seriellen Anschlusses für die Baudrate, Fehlerprüfungsparität und Anzahl an Stoppbits konfigurieren. Verbindungen, die über den seriellen Anschluss des erweiterten Managementmoduls hergestellt werden, können nur auf die Befehlszeilenschnittstelle des Managementmoduls und auf die SOL-Funktion (Serial over LAN) zugreifen. Weitere Informationen zur Verwendung des seriellen Anschlusses finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des erweiterten BladeCenter-Managementmoduls*.

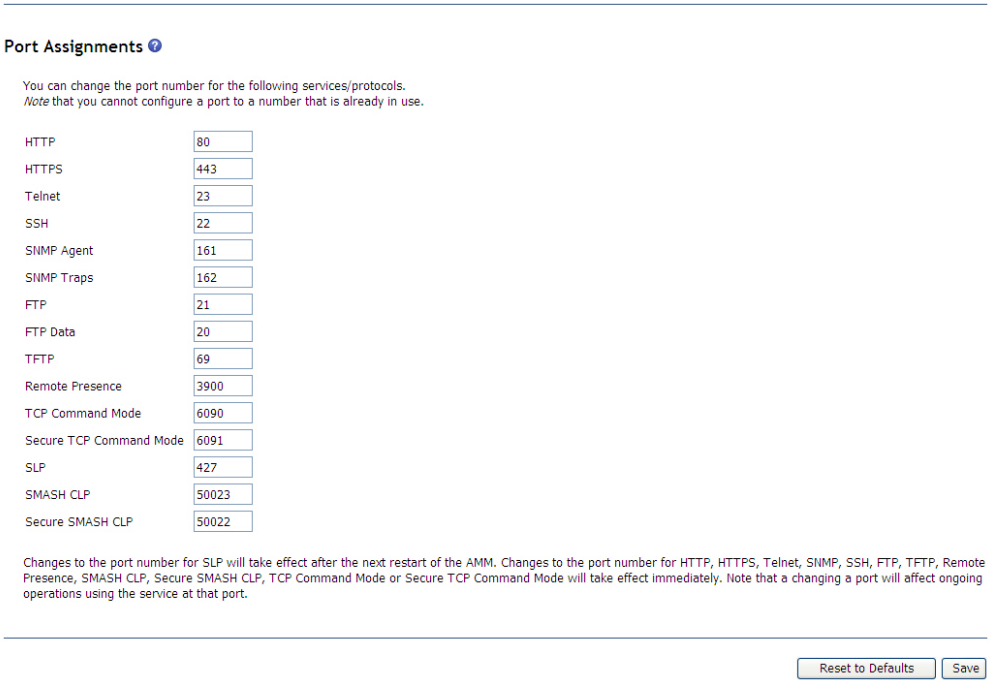
Klicken Sie auf **View Configuration Summary** (Konfigurationszusammenfassung anzeigen), um die Konfigurationseinstellungen für alle BladeCenter-Benutzer und -Komponenten anzuzeigen.

Port Assignments (Portzuordnungen)

Wählen Sie **MM Control → Port Assignments** (MM-Steuerung → Portzuordnungen) aus, um E/A-Ports zu verschiedenen Protokollen zuzuordnen.

In der folgenden Abbildung sind Portzuordnungseinstellungen eines erweiterten Managementmoduls dargestellt.





Wählen Sie **Port Assignments** (Portzuordnungen) aus, um einige der Ports zu konfigurieren, die das Managementmodul verwendet. Die Ports, die auf der Seite "Port Assignments" (Portzuordnungen) für das Managementmodul konfiguriert werden können, sind in Tabelle 4 aufgelistet. Die fest zugeordneten Ports, die das Managementmodul verwendet, sind in Tabelle 5 auf Seite 187 aufgeführt. Einige Ports können nur mit bestimmten Managementmodultypen geändert werden.

Klicken Sie auf **View Configuration Summary** (Konfigurationszusammenfassung anzeigen), um die Konfigurationseinstellungen für alle BladeCenter-Benutzer und -Komponenten anzuzeigen.

Tabelle 4. Vom Benutzer konfigurierbare Ports des Managementmoduls

Portname	Standard-portnummer	Zweck
HTTP	80	HTTP-Verbindung des Web-Servers über UDP
HTTPS	443	SSL-Verbindung über TCP
Telnet	23	Telnet-Verbindung über Befehlszeilenschnittstelle
SSH	22	SSH-Verbindung (Secure Shell) über Befehlszeilenschnittstelle
SNMP-Agent	161	get-/set-SNMP-Befehle über UDP
SNMP-Traps	162	SNMP-Alarmnachrichten über UDP
FTP	21	Empfangsport des FTP-Servers des Managementmoduls
FTP-Daten	20	Datenport des FTP-Servers des Managementmoduls
TFTP	69	TFTP-Server des Managementmoduls
Remote Presence	3900	Ferne Vorgänge für Datenträger, Speicher und KVM
SLP	427	UDP-SLP-Verbindung (SLP - Service Location Protocol)

Tabelle 4. Vom Benutzer konfigurierbare Ports des Managementmoduls (Forts.)

Portname	Standard-portnummer	Zweck
TCP-Befehlsmodus	6090	IBM Systems Director-Befehle über TCP/IP **Anmerkung:** IBM Systems Director kann das erweiterte Managementmodul möglicherweise nicht über den TCP-Befehlsmodus finden, wenn diese Portnummer geändert wurde.
Secure TCP-Befehlsmodus	6091	IBM Systems Director-Befehle über TCP/IP **Anmerkung:** IBM Systems Director kann das erweiterte Managementmodul möglicherweise nicht über den Secure TCP-Befehlsmodus finden, wenn diese Portnummer geändert wurde.
SMASH-Befehlszeilen-prozessor	50023	SMASH-Befehlszeilenprotokoll des Managementmoduls über Telnet
Secure SMASH-Befehlszeilen-prozessor	50022	Secure SMASH-Befehlszeilenprotokoll des Managementmoduls über SSH

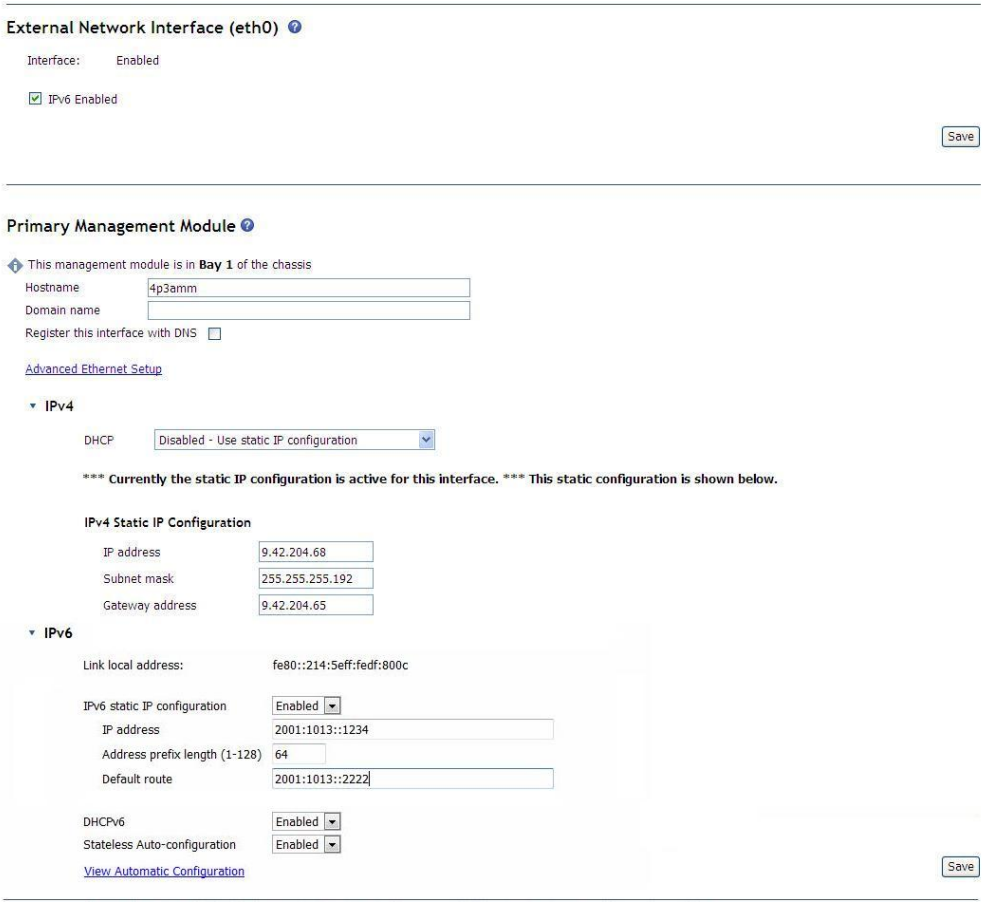
Tabelle 5. Fest zugeordnete Ports des Managementmoduls

Portnummer (fest zugeordnet)	Zweck
25	TCP-E-Mail-Alerts
53	UDP-DNS-Auflösung (DNS - Domain Name Server)
68	DHCP-Clientverbindung über UDP
13991	IBM Systems Director-Alerts über UDP

Network Interfaces (Netzschnittstellen)

Wählen Sie **MM Control → Network Interfaces** (MM-Steuerung → Netzschnittstellen) aus, um den Netzzugriff zu konfigurieren.

In der folgenden Abbildung ist die Seite "Network Interfaces" (Netzschnittstellen) eines erweiterten Managementmoduls dargestellt.



Achtung: Wenn IPv6 aktiviert wurde, führt das Inaktivieren von IPv6 oder das Aktualisieren der Firmware des erweiterten Managementmoduls auf eine Version, die keine IPv6-Adressierung unterstützt, zum Verlust der gesamten IPv6-Konnektivität. Services und Schnittstellen, die für den IPv6-Betrieb konfiguriert sind, funktionieren möglicherweise nicht ordnungsgemäß und Sie müssen diese Services und Schnittstellen neu konfigurieren.

Wählen Sie **Network Interfaces** (Netzschnittstellen) aus, um die Ethernet-Schnittstellen des Managementmoduls zu konfigurieren. Beim erweiterten Managementmodul können Sie nur die externe Ethernet-Schnittstelle konfigurieren, die für die Datenübertragung zur Fernverwaltung und fernen Konsole verwendet wird. Die interne Ethernet-Schnittstelle des erweiterten Managementmoduls weist keine vom Benutzer konfigurierbaren Einstellungen auf.

Das erweiterte Managementmodul unterstützt sowohl die IPv4- als auch die IPv6-Adressierung. Die IPv4-Adressierung ist immer aktiviert und IPv6 ist standardmäßig aktiviert. Wenn im Abschnitt **External Network Interface (eth0)** (Externe Netzschnittstelle (eth0)) das Kontrollkästchen **IPv6 Enabled** (IPv6 aktiviert) nicht

ausgewählt ist, wurde die IPv6-Adressierung für die BladeCenter-Einheit inaktiviert und es wird ein zusätzliches Kontrollkästchen angezeigt, mit dem Sie die Anzeige von IPv6-Informationen ausschalten können. Sie müssen auf **Save** (Speichern) klicken, damit Änderungen wirksam werden. Der Status der internen Ethernet-Verbindung (eth1) für das primäre Managementmodul lautet "Enabled" (Aktiviert) und kann nicht geändert werden.

Anmerkung: Wenn IPv6 aktiviert ist, muss auch mindestens eine der IPv6-Konfigurationsmethoden (IPv6 statisch, DHCPv6 oder statusunabhängige automatische Konfiguration) aktiviert und konfiguriert sein.

Für die Datenübertragung des E/A-Moduls zu einer Fernverwaltungsstation über den externen Ethernet-Anschluss des Managementmoduls müssen sich die interne Netzschnittstelle des E/A-Moduls und die internen und externen Schnittstellen des Managementmoduls im selben Teilnetz befinden.

Im Abschnitt **Primary Management Module** (Primäres Managementmodul) werden Informationen zur Schnittstelle angezeigt, die für den Anschluss für Fernverwaltung und ferne Konsole des primären Managementmoduls verwendet wird.

Anmerkung: Wenn Ihre BladeCenter-Einheit redundante Managementmodule unterstützt und Sie diese Funktion verwenden und dabei dieselbe externe IP-Adresse für beide Managementmodule festlegen möchten, inaktivieren Sie DHCP und DHCPv6; konfigurieren und verwenden Sie stattdessen eine statische IP-Adresse. Diese Maßnahme muss bei Bedarf sowohl für IPv4 als auch für IPv6 durchgeführt werden. (Die IP-Konfigurationsdaten werden automatisch an das Bereitschaftsmanagementmodul übertragen, wenn dieses benötigt wird.)

- Die folgenden Bereiche des Abschnitts **Primary Management Module** (Primäres Managementmodul) beziehen sich sowohl auf die IPv4- als auch auf die IPv6-Adressierung:
  - Feld **Hostname** (Hostname): (Optional) Hierbei handelt es sich um den IP-Hostnamen, den Sie für das Managementmodul verwenden möchten (maximal 63 Zeichen gemäß den Standards für Hostnamen).
  - Feld **Domain name** (Domänenname): Der Domänenname des Managementmoduls, der in Verbindung mit einem DDNS-Server (Dynamic Domain Name System) verwendet wird.
  - Kontrollkästchen **Register this interface with DNS** (Diese Schnittstelle bei DNS registrieren): Ist dieses Kontrollkästchen aktiviert, werden die konfigurierten DNS-Server (Informationen hierzu finden Sie im Abschnitt „Network Protocols (Netzprotokolle)" auf Seite 192) auch als DDNS-Server betrachtet und erhalten Angaben zu Domänennamen.

  Klicken Sie auf **Advanced Ethernet Setup** (Erweiterte Ethernet-Konfiguration), um die Übertragungsgeschwindigkeit, den Duplexmodus, die größte zu übertragende Einheit (MTU) und die lokal verwaltete MAC-Adresse für diese Schnittstelle anzuzeigen und zu konfigurieren. Das Feld mit der Herstellerkennung der MAC-Adresse für die externe Schnittstelle ist schreibgeschützt.

  Beim erweiterten Managementmodul können Sie die Funktionsübernahme durch eine physische oder logische Uplink-Verbindung aktivieren oder inaktivieren. Dazu verwenden Sie die Felder **Failover on loss of physical network link** (Funktionsübernahme bei Verlust der physischen Netzverbindung) und **Failover on loss of logical network link** (Funktionsübernahme bei Verlust der logischen Netzverbindung). Wenn die externe Netzschnittstelle des primären Managementmoduls ausfällt, erzwingen die Funktionen für Uplink-Verbindungen eine Funktionsübernahme durch das Bereitschaftsmanagementmodul, falls installiert, nach-

dem die festgelegte Verzögerung für die Netzfunktionsübernahme verstrichen ist. Bei einem erweiterten Managementmodul können Sie auch die IP-Adresse angeben, die das Managementmodul verwendet, um den Status seiner logischen Netzverbindung zu überprüfen. Die IP-Adresse sollte für eine zuverlässige Einheit gelten, die sich im selben physischen LAN wie das erweiterte Managementmodul befindet. Wurde keine IP-Adresse angegeben, verwendet das erweiterte Managementmodul die IP-Adresse des Gateways des erweiterten Managementmoduls, falls diese konfiguriert wurde. Das erweiterte Managementmodul kann auch passiv für eine Routing-Multicastadresse empfangsbereit sein, um zu bestimmen, ob das Netz aktiv ist.

- Die folgenden Bereiche des Abschnitts **External Network Interface (eth0)** (Externe Netzschnittstelle (eth0)) beziehen sich auf die IPv4-Adressierung:
  - **DHCP** (DHCP): Wählen Sie eine der folgenden Optionen aus:
    - **Enabled: Obtain IP config. from DHCP server** (Aktiviert: IP-Konfig. von DHCP-Server anfordern)
    - **Disabled: Use static IP configuration** (Inaktiviert: Statische IP-Konfiguration verwenden)
    - **Try DHCP server. If it fails, use static IP config.** (DHCP-Server versuchen. Bei Fehlschlagen statische IP-Konfig. verwenden.) (Dies ist die Standardeinstellung; das DHCP-Zeitlimit läuft nach zwei Minuten ab.)

    Anmerkung: Ist für die DHCP-Einstellung des Managementmoduls die Option **Try DHCP server. If it fails, use static IP config.** (DHCP-Server versuchen. Bei Fehlschlagen statische IP-Konfig. verwenden.) ausgewählt, verwendet das Managementmodul die statische IP-Adresse, wenn der DHCP-Server beim Starten des Managementmoduls nicht verfügbar ist. In diesem Fall ist die IP-Adresse möglicherweise nicht erreichbar, falls mehrere Managementmodule mit derselben statischen IP-Adresse gestartet wurden.
  - **IPv4 Static IP configuration** (Statische IPv4-IP-Konfiguration): Konfigurieren Sie diese Informationen nur, wenn DHCP inaktiviert ist.
    - **IP address** (IP-Adresse): Die IPv4-IP-Adresse des Managementmoduls muss aus vier Ganzzahlen von 0 bis 255 bestehen, die durch Punkte getrennt sind, und sie darf keine Leerzeichen oder aufeinanderfolgenden Punkte enthalten. Die Standardeinstellung lautet 192.168.70.125.
    - **Subnet mask** (Teilnetzmaske): Die Teilnetzmaske muss aus vier Ganzzahlen von 0 bis 255 bestehen, die durch Punkte getrennt sind, und sie darf keine Leerzeichen enthalten. Die Standardeinstellung lautet 255.255.255.0.
    - **Gateway address** (Gateway-Adresse): Die IP-Adresse des Netz-Gateway-Routers muss aus vier Ganzzahlen von 0 bis 255 bestehen, die durch Punkte getrennt sind, und sie darf keine Leerzeichen enthalten. Diese Adresse muss über die IP-Adresse und Teilnetzmaske erreichbar sein, die oben angegeben wurden.
  - Klicken Sie auf **IP Configuration Assigned by DHCP Server** (Von DHCP-Server zugewiesene IP-Konfiguration), um die IP-Konfiguration anzuzeigen, die vom DHCP-Server zugewiesen wurde. (Diese Option ist nur verfügbar, wenn DHCP aktiviert ist.)
- Die folgenden Bereiche des Abschnitts **External Network Interface (eth0)** (Externe Netzschnittstelle (eth0)) beziehen sich auf die IPv6-Adressierung:

  Anmerkung: Bei IPv6 können die statische DHCPv6- und IPv6-Konfiguration gleichzeitig aktiviert werden, jeweils mit eigener Adresse. Hosts wie z. B. das erweiterte Managementmodul können mehrere IPv6-Adressen aufweisen.

– **Link-local address** (Lokale Verbindungsadresse): (schreibgeschützt) Eine eindeutige IPv6-Adresse für das erweiterte Managementmodul, die automatisch auf Basis der MAC-Adresse generiert wird (zusätzliche Informationen finden Sie im Abschnitt „IPv6-Adressierung für die erstmalige Verbindung" auf Seite 12).
– **IPv6 Static IP configuration** (Statische IPv6-IP-Konfiguration): Die statische IPv6-IP-Konfiguration ist standardmäßig inaktiviert.

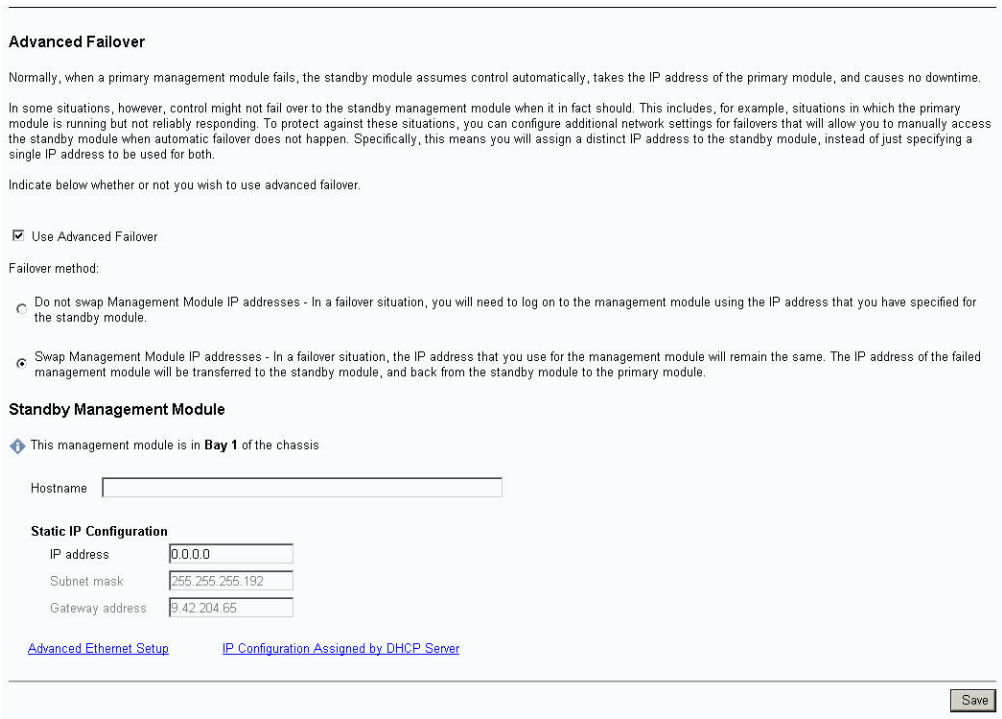
  Anmerkung: Das erweiterte Managementmodul weist standardmäßig keine fest zugeordnete statische IPv6-Adresse auf. Für den Erstzugriff können Benutzer die Adresse der lokalen IPv4- oder IPv6-Verbindung verwenden.

  - **IP address** (IP-Adresse): Die IPv6-IP-Adresse des Managementmoduls muss aus 16 hexadezimalen Bytes bestehen, die durch 2-Byte-Begrenzungen unterteilt und durch Doppelpunkte getrennt sind. Dies ergibt folgendes Format: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A.
  - **Address prefix length (1-128)** (Länge des Adresspräfix (1-128)): Die Präfixlänge der IPv6-Adresse. Die Länge des Adresspräfix ist beim erweiterten Bereitschaftsmanagementmodul nicht konfigurierbar; es wird derselbe Wert wie für das primäre erweiterte Managementmodul verwendet.
  - **Default route** (Standardroute): Die IP-Adresse des Netz-Gateway-Routers muss aus 16 hexadezimalen Bytes bestehen, die durch 2-Byte-Begrenzungen unterteilt und durch Doppelpunkte getrennt sind. Dies ergibt folgendes Format: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A. Die Standardroute ist beim erweiterten Bereitschaftsmanagementmodul nicht konfigurierbar; es wird derselbe Wert wie für das primäre erweiterte Managementmodul verwendet.

– **DHCPv6**: Wählen Sie eine der folgenden Optionen aus:
  - **Enabled: Obtain IP configuration from DHCP server** (Aktiviert: IP-Konfiguration von DHCP-Server anfordern) (Standardeinstellung)
  - **Disabled: Not obtain IP configuration from DHCP server** (Inaktiviert: IP-Konfiguration nicht von DHCP-Server anfordern)
– **Stateless Auto-configuration** (Statusunabhängige automatische Konfiguration): Die automatische Konfiguration von Adressen basiert auf dem Empfang von Routermitteilungsnachrichten. Diese Nachrichten beinhalten statusunabhängige Adresspräfixe. Die statusunabhängige automatische Konfiguration ist standardmäßig aktiviert.

Klicken Sie auf **View Automatic Configuration** (Automatische Konfiguration anzeigen), um die DHCPv6-Informationen und die Adressen der statusunabhängigen automatischen Konfiguration anzuzeigen, die dem primären erweiterten Managementmodul zugewiesen wurden. Alle Felder sind schreibgeschützt.

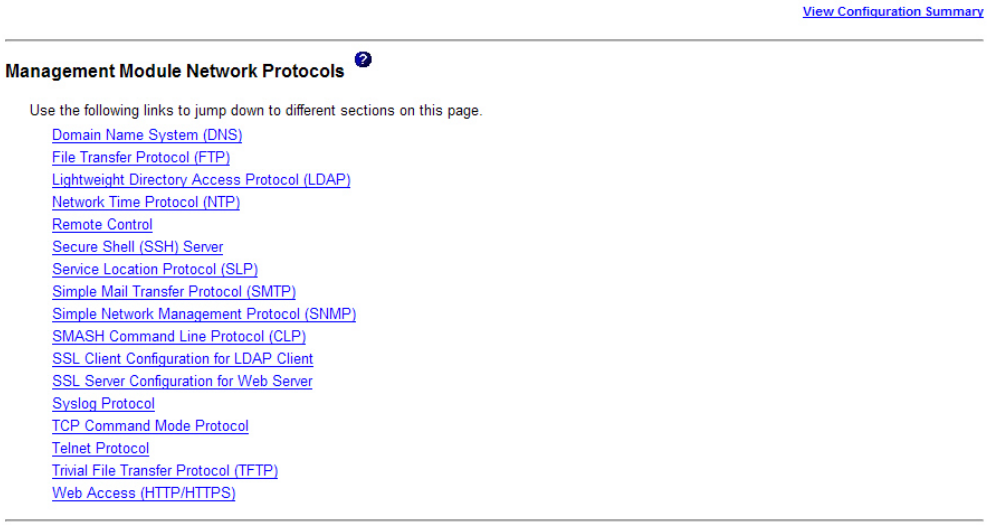
Im Abschnitt **Advanced Failover** (Erweiterte Funktionsübernahme) wird festgelegt, wie sich das Managementmodul verhält, wenn für die Funktionsübernahme auf das Bereitschaftsmanagementmodul umgeschaltet wird. Außerdem werden Informationen zur Schnittstelle angezeigt, die für den Anschluss für Fernverwaltung und ferne Konsole des Bereitschaftsmanagementmoduls verwendet wird, ähnlich wie in den Abschnitten **External Network Interface (eth0)** (Externe Netzschnittstelle (eth0)) und **Primary Management Module** (Primäres Managementmodul) für das primäre Managementmodul.



Network Protocols (Netzprotokolle)

Wählen Sie **MM Control → Network Protocols** (MM-Steuerung → Netzprotokolle) aus, um die Einstellungen für Standardnetzprotokolle anzuzeigen oder zu ändern.

In der folgenden Abbildung sind Netzprotokolleinstellungen eines erweiterten Managementmoduls dargestellt.



Klicken Sie auf **View Configuration Summary** (Konfigurationszusammenfassung anzeigen), um die Konfigurationseinstellungen für alle BladeCenter-Benutzer und -Komponenten anzuzeigen.

Wählen Sie **Network Protocols** (Netzprotokolle) aus, um die Einstellungen für SNMP, DNS, SMTP, LDAP und SLP anzuzeigen oder zu ändern. Sie können die

Zeitlimitintervalle für die Telnet- und TCP-Schnittstellen aktivieren oder inaktivieren und festlegen. Bei einem erweiterten Managementmodul können Sie auch die FTP-, TFTP-, Syslog- und SMASH-Einstellungen konfigurieren und die einzelnen Verwaltungsschnittstellen (Webschnittstelle des Managementmoduls, Befehlszeilenschnittstelle, TCP und SNMP) aktivieren oder inaktivieren.

SLP stellt einen Broadcast-basierten Mechanismus bereit, um den Status von erweiterten Managementmodulen im Netz abzufragen. Ein erweitertes Managementmodul verwendet die Ergebnisse dieser Abfragen, um den Status von fernen BladeCenter-Einheiten anzuzeigen.

Das Syslog-Protokoll stellt eine Methode für das erweiterte Managementmodul bereit, mit der Ereignisprotokollnachrichten über das Netz an einen oder zwei Syslog-Collectors gesendet werden können. Dies ist eine hilfreiche Funktion, weil das Ereignisprotokoll des erweiterten Managementmoduls eine begrenzte Kapazität aufweist, sodass die ältesten Nachrichten überschrieben werden, sobald das Protokoll voll ist. Durch die Konfiguration der Syslog-Collectors vermeiden Sie den Verlust von Ereignisnachrichten. Weitere Informationen zum Konfigurieren der Syslog-Funktion und zum Generieren von Testnachrichten finden Sie im Abschnitt „Syslog aktivieren" auf Seite 70.

Anmerkung: Bei einem erweiterten Managementmodul können die Telnet-Schnittstelle und der SMASH-Befehlszeilenprozessor auch über SNMP und die Befehlszeilenschnittstelle des Managementmoduls aktiviert oder inaktiviert werden. Weitere Informationen finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des erweiterten BladeCenter-Managementmoduls* oder im *Installations- und Benutzerhandbuch zu IBM SMASH Proxy*.

Einige Netzprotokolleinstellungen werden bei der SNMP-, SMTP- und LDAP-Konfiguration verwendet. Weitere Informationen dazu finden Sie in den Abschnitten „SNMP (Simple Network Management Protocol) konfigurieren" auf Seite 28, „SMTP (Simple Mail Transfer Protocol) konfigurieren" auf Seite 32 und „LDAP konfigurieren" auf Seite 32.

Chassis Internal Network (Internes Gehäusenetz)

Wählen Sie **MM Control → Chassis Int Network** (MM-Steuerung → Internes Gehäusenetz) aus, um die internen Verbindungen zwischen den Blade-Server-Anschlüssen und einem internen Managementanschluss für erweiterte Managementmodule zu verwalten.

Das interne Gehäusenetz (Chassis Internal Network - CIN) stellt die internen Verbindungen zwischen Blade-Server-Anschlüssen und dem Managementanschluss für

das interne erweiterte Managementmodul bereit. So können Sie über eine WEB-, CLI- oder SNMP-Sitzung von einem Blade-Server aus auf das Managementmodul zugreifen.

Der Übertragungsweg ist bidirektional, sodass das erweiterte Managementmodul auch die Services auf dem Blade-Server verwenden kann, wie beispielsweise LDAP, SMTP, DNS und NTP (Network Time Protocol).

Auf der Seite **Chassis Internal Network (CIN) Status** (Status des internen Gehäusenetzes) können Sie den Status der bereits vorhandenen Elemente des internen Gehäusenetzes anzeigen.


Chassis Internal Network (CIN) Status

Seq No	CIN VLAN ID	CIN IP Address	CIN MAC	Status
1	4094	0.0.0.0		Operational
2	4090	2000:1013::1:192	00:00:00:00:00:00	Not Operational

* = learned address

CIN VLAN ID (VLAN-ID des internen Gehäusenetzes)
Die VLAN-ID (Virtual LAN), die das interne Gehäusenetz unterstützt.

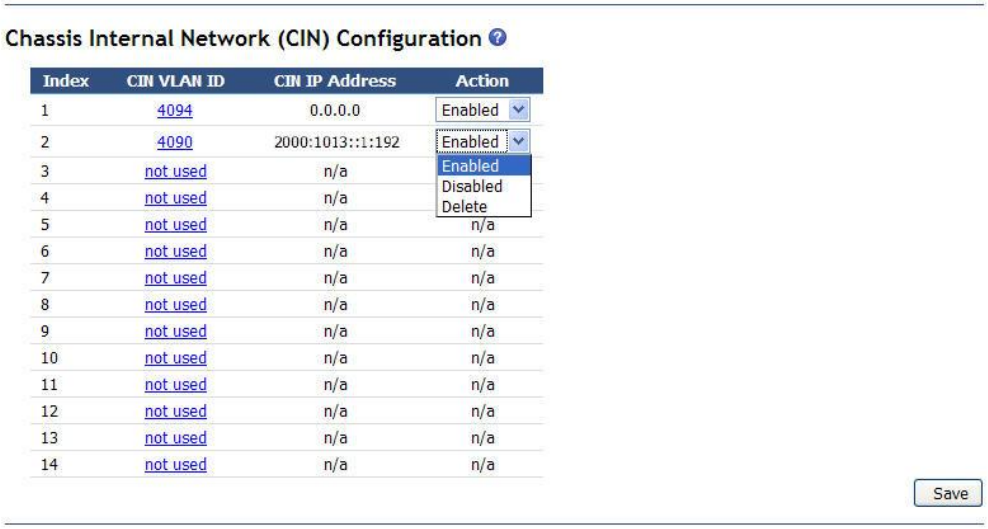
CIN IP Address (IP-Adresse des internen Gehäusenetzes)
Die IP-Adresse für die Datenübertragung des internen Gehäusenetzes. Ein Stern (*) nach der Adresse zeigt an, dass die Adresse dynamisch zugewiesen wurde und nicht explizit durch den Benutzer konfiguriert wird.

CIN MAC (MAC des internen Gehäusenetzes)
Die zur IP-Adresse gehörende MAC-Adresse.

Status (Status)
Der Verbindungsstatus des internen Gehäusenetzes. Der Status kann folgende Werte aufweisen:

- **Operational** (Betriebsbereit): Das erweiterte Managementmodul kann die IP-Adresse des internen Gehäusenetzes mit Ping überprüfen.
- **Not Operational** (Nicht betriebsbereit): Das erweiterte Managementmodul kann die IP-Adresse des internen Gehäusenetzes nicht mit Ping überprüfen. Stellen Sie sicher, dass der Blade-Server und das E/A-Modul ordnungsgemäß konfiguriert sind und dass ihre Konfigurationen mit dem erweiterten Managementmodul kompatibel sind. Die Verbindung des internen Gehäusenetzes weist den Status "Not Operational" (Nicht betriebsbereit) auf, wenn eine der folgenden Bedingungen vorliegt:
  - Für das Betriebssystem des Blade-Servers muss eine IP-Hostroute definiert sein.
  - Für die E/A-Module ist bereits ein VLAN definiert, das den Anschluss für den Blade-Server und das erweiterte Managementmodul enthält.
- **Disabled** (Inaktiviert): Die Konfiguration des internen Gehäusenetzes wurde von einem Administrator des erweiterten Managementmoduls inaktiviert.

Damit das Managementmodul vom Blade-Server aus gefunden wird, müssen Sie auf der Seite **Chassis Internal Network (CIN) Configuration** (Konfiguration des internen Gehäusenetzes) mindestens eine VLAN-ID für das interne Gehäusenetz (CIN VID) zuweisen.



Jeder Schnittstelle des internen Gehäusenetzes zum erweiterten Managementmodul ist eine Indexnummer, eine ID, eine IP-Adresse und ein Aktionswert zugewiesen.

CIN Index (Index des internen Gehäusenetzes)
Dies ist ein Index von 1 bis 14, um die Konfiguration des internen Gehäusenetzes zu identifizieren.

CIN VLAN ID (VLAN-ID des internen Gehäusenetzes)
Dies kann eine Zahl von 3 bis 4094 sein. Diese VLAN-IDs müssen sich von der ID für SOL/cKVM unterscheiden. Der Wert **~not used~** (nicht verwendet) gibt an, dass dieser Konfigurationseintrag nicht definiert wurde. Klicken Sie auf eine VLAN-ID, um den Eintrag festzulegen.

CIN IP Address (IP-Adresse des internen Gehäusenetzes)
Hierbei handelt es sich um die IP-Adresse, die für die Datenübertragung im internen Gehäusenetz aktiviert ist. Ein Wert von 0.0.0.0 (IPv4) oder 0::0 (IPv6) gibt an, dass im internen Gehäusenetz alle IP-Adressen zur Datenübertragung verwendet werden können. In diesem Fall überwacht das erweiterte Managementmodul die VLAN-ID des internen Gehäusenetzes und lernt die IP-Adressen dynamisch. Um die Adressen zu beschränken, definieren Sie die IP-Adressen einzeln. Die Einträge zum internen Gehäusenetz dürfen keine übereinstimmenden IP-Adressen aufweisen, ausgenommen die Adressen 0.0.0.0 (IPv4) oder 0::0 (IPv6). Es werden mehrere Einträge zum internen Gehäusenetz mit der IP-Adresse 0.0.0.0 (IPv4) oder 0::0 (IPv6) unterstützt, vorausgesetzt, dass sich die VLAN-IDs voneinander unterscheiden. Die IP-Adresse eines Eintrags zum internen Gehäusenetz darf kein Multicasting unterstützen und nicht mit der IP-Adresse des erweiterten Managementmoduls übereinstimmen.

Action (Aktion)
In diesem Menü können Sie eine vorhandene Konfiguration des internen Gehäusenetzes aktivieren, inaktivieren oder löschen.

Anmerkung: Sie können das interne Gehäusenetz global aktivieren oder inaktivieren. Wenn das interne Gehäusenetz inaktiviert ist, sind sämtliche Funktionen des internen Gehäusenetzes inaktiviert, auch wenn die Indexeinträge 1 bis 14 konfiguriert sind.

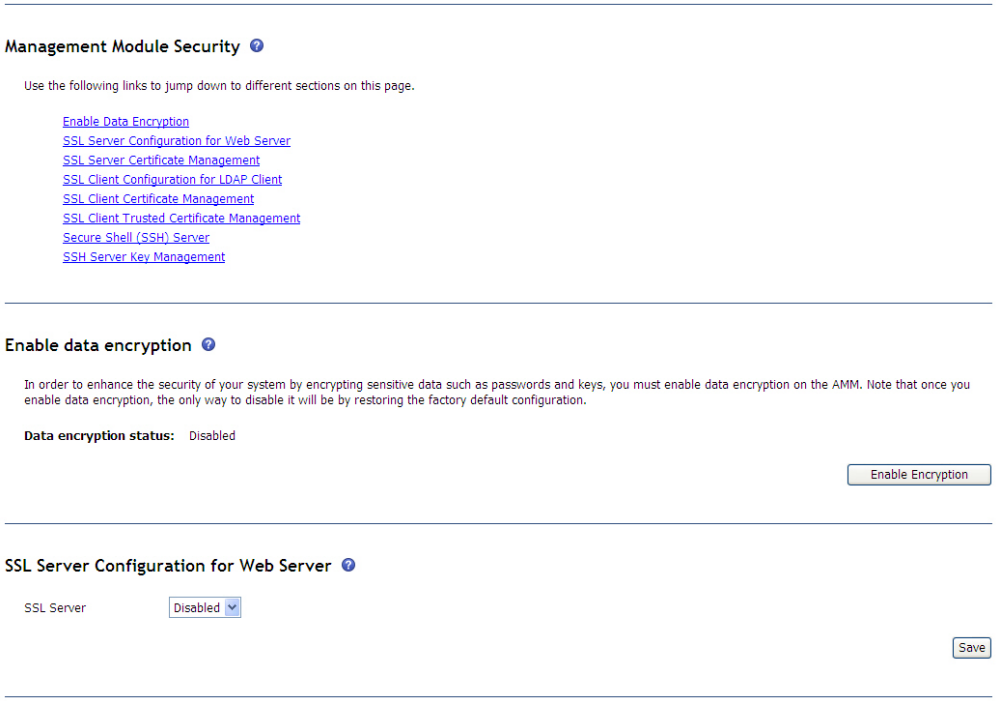
Wenn Sie eine neue VLAN-Konfiguration für das interne Gehäusenetz erstellen möchten, klicken Sie auf einen der Einträge mit dem Wert **~not used~** (nicht verwendet). Daraufhin wird die Seite **Chassis Internal Network (CIN) Entry Definition** (Internes Gehäusenetz, Eintragsdefinition) angezeigt.

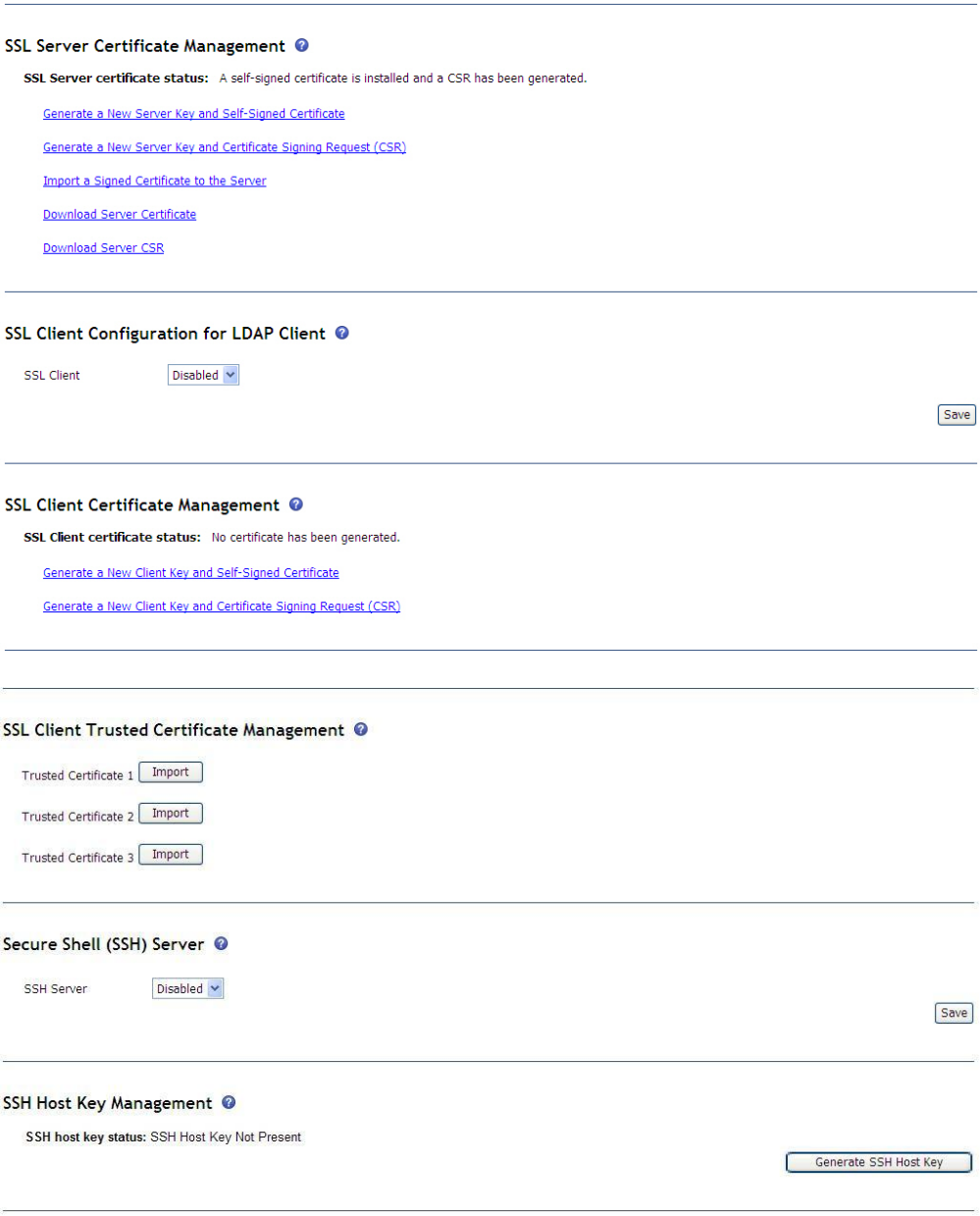
Geben Sie die VLAN-ID und die IP-Adresse ein und klicken Sie dann auf **Save** (Speichern), um die Konfiguration zu den vorhandenen VLAN-Konfigurationen des internen Gehäusenetzes hinzuzufügen, oder klicken Sie auf **Cancel** (Abbrechen), um zur vorherigen Seite zurückzukehren.

Security (Sicherheit)

Wählen Sie **MM Control → Security** (MM-Steuerung → Sicherheit) aus, um Sicherheitseinstellungen anzuzeigen und zu verwalten.

In den folgenden Abbildungen sind Beispiele für Sicherheitseinstellungen eines erweiterten Managementmoduls dargestellt.



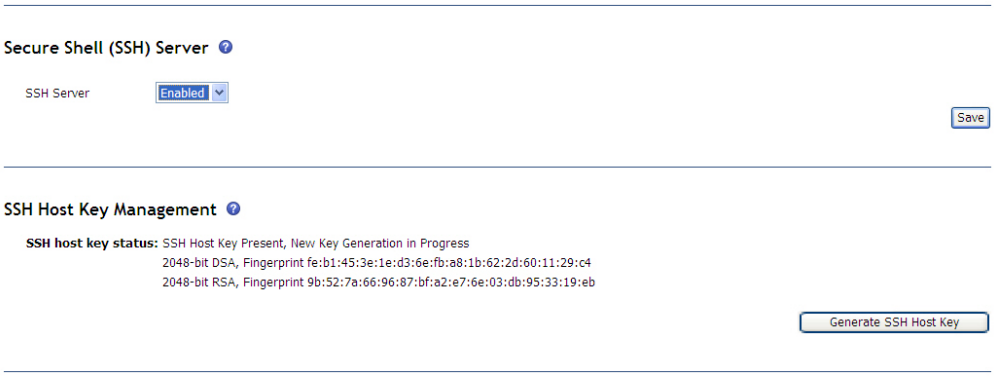


Wählen Sie **Security** (Sicherheit) aus, um die SSL-Einstellungen (Secure Sockets Layer) für den Web-Server und LDAP-Client und die SSH-Servereinstellungen (Secure Shell) anzuzeigen oder zu ändern. Sie können SSL aktivieren oder inaktivieren (Standardeinstellung) und zwischen selbst signierten Zertifikaten und von einer Zertifizierungsstelle bereitgestellten Zertifikaten auswählen. Sie können auch SSH aktivieren (Standardeinstellung) oder inaktivieren und den SSH-Serverschlüssel generieren und verwalten. Bei einem erweiterten Managementmodul können Sie zudem die Datenverschlüsselung für sensible Daten, wie z. B. Kennwörter und Schlüssel, aktivieren oder inaktivieren. Wenn die Datenverschlüsselung aktiviert ist, kann sie nur inaktiviert werden, indem das Managementmodul auf die werkseitig voreingestellte Konfiguration zurückgesetzt wird. Wenn die Datenverschlüsselung aktiviert ist und eine Firmwareaktualisierung für das Managementmodul installiert wird, die keine Datenverschlüsselung unterstützt, werden alle Konfigurationseinstellungen des Managementmoduls auf die Werte der werkseitigen Voreinstellung zurückgesetzt.

Anmerkungen:

- Bei einem erweiterten Managementmodul können Sie SSH auch über SNMP und die Befehlszeilenschnittstelle des Managementmoduls aktivieren oder inaktivieren. Weitere Informationen finden Sie im *Referenzhandbuch zur Befehlszeilenschnittstelle des erweiterten BladeCenter-Managementmoduls*.
- Bei einem erweiterten Managementmodul können installierte öffentliche SSH-Schlüssel verwendet werden, um eine Authentifizierung ohne Kennwörter zu ermöglichen. Es können bis zu 12 öffentliche Schlüssel für den Benutzerzugriff installiert werden.
- Ein erweitertes Managementmodul generiert automatisch SSH-Hostschlüssel, wenn keine Hostschlüssel installiert sind und entweder SSH oder Secure SMASH aktiviert ist.

In der folgenden Abbildung ist die Konfigurationsseite für Secure Shell eines erweiterten Managementmoduls dargestellt.

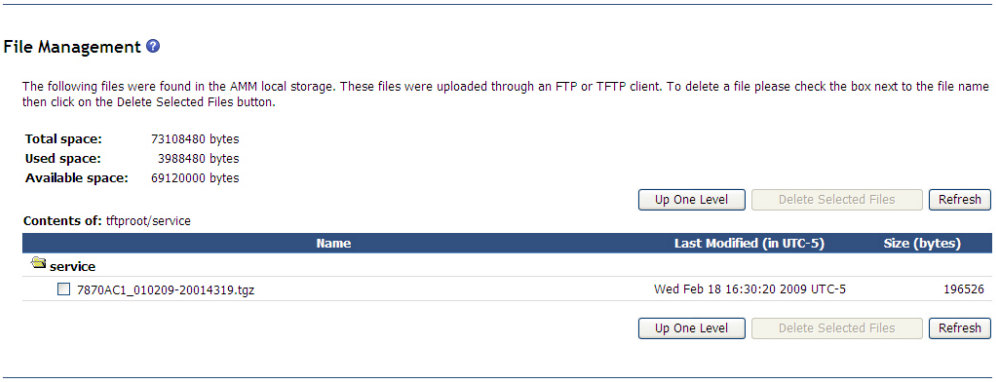


Einige Sicherheitseinstellungen werden bei der SSL-, LDAP- und SSH-Konfiguration verwendet. Weitere Informationen dazu finden Sie in den Abschnitten „Sicherer Web-Server und sichere LDAP-Verbindung" auf Seite 52 und „SSH-Server konfigurieren (Secure Shell)" auf Seite 64.

File Management (Dateiverwaltung)

Wählen Sie **MM Control → File Management** (MM-Steuerung → Dateiverwaltung) aus, um die Inhalte des lokalen Speicherbereichs auf dem erweiterten Managementmodul anzuzeigen und zu verwalten.

Die folgende Abbildung zeigt die Seite "File Management" (Dateiverwaltung) für erweiterte Managementmodule.



Die Option **File Management** (Dateiverwaltung) zeigt eine Liste von Dateien und den verfügbaren Speicherplatz im Dateisystem des erweiterten Managementmoduls an. Sie können die im erweiterten Managementmodul gespeicherten Dateien löschen. Die Seite zeigt bis zu zwei Dateiverzeichnisebenen und ihren Inhalt an. Jedes hier angezeigte Verzeichnis wird durch ein Symbol für einen geöffneten Ordner dargestellt. Wenn unterhalb der angezeigten Ebenen weitere Unterverzeichnisse vorhanden sind, werden die Verzeichnisnamen der nächsten Ebene als Web-Links angezeigt, die durch Symbole für geschlossene Ordner dargestellt werden. Klicken Sie auf den Link eines Verzeichnisnamens, um die beiden nächsten Verzeichnisebenen anzuzeigen. Es gibt keine Beschränkung der Verzeichnistiefe. Mithilfe der Schaltfläche "Zurück" des Web-Browsers können Sie jeweils zwei Verzeichnisebenen in der Verzeichnisstruktur zurücknavigieren. Sie können aber auch im Navigationsfenster auf **File Management** (Dateiverwaltung) klicken, um direkt zur obersten Ebene der Verzeichnisstruktur des erweiterten Managementmoduls zu wechseln.

Das Hochladen von Dateien in den lokalen Speicherbereich des erweiterten Managementmoduls erfolgt über FTP oder TFTP oder mithilfe der Funktion "Remote Disk" (Ferner Datenträger) des erweiterten Managementmoduls (Informationen und Anweisungen hierzu finden Sie im Abschnitt „Funktion für ferne Datenträger verwenden” auf Seite 81). FTP- und TFTP-Server im erweiterten Managementmodul werden auf der Seite "MM Control" > "Network Protocols" (MM-Steuerung, Netzprotokolle) aktiviert (siehe „Network Protocols (Netzprotokolle)” auf Seite 192).

Wenn Sie eine Datei löschen möchten, wählen Sie sie aus und klicken Sie anschließend auf **Delete Selected Files** (Ausgewählte Dateien löschen). Klicken Sie dann auf **Refresh** (Aktualisieren), um die Anzeige zu aktualisieren.

Anmerkung:

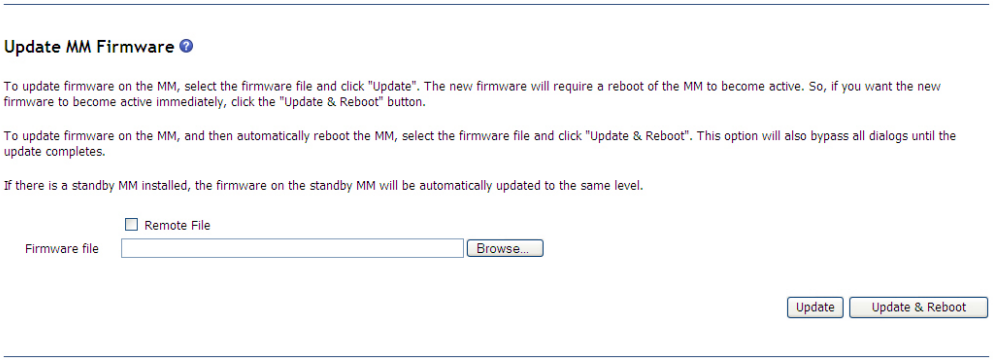
- Benutzer müssen über die Berechtigung "Supervisor" (Administrator), "Chassis Administrator" (Gehäuseadministrator), "Chassis Configuration" (Gehäusekonfiguration), "Blade Administration" (Blade-Administration), "Blade Configuration" (Blade-Konfiguration), "I/O Module Administration" (E/A-Modul-Administration) der "I/O Module Configuration" (E/A-Modul-Konfiguration) verfügen, um eine Datei zu löschen.
- Verzeichnisse können nicht gelöscht werden.

Firmware Update (Firmwareaktualisierung)

Wählen Sie die Option **MM Control → Firmware Update** (MM-Steuerung → Firmwareaktualisierung) aus, um die Firmware des Managementmoduls zu aktualisieren.

Wichtig: Einige Clusterlösungen erfordern bestimmte Codeversionen oder koordinierte Code-Aktualisierungen. Wenn die Einheit zu einer Clusterlösung gehört, überprüfen Sie, ob die aktuelle Codestufe für die Clusterlösung unterstützt wird, bevor Sie den Code aktualisieren.

Die folgende Abbildung zeigt die Seite "Management Module Firmware Update" (Aktualisierung der Firmware des Managementmoduls) für das erweiterte Managementmodul.



Wenn ein Bereitschaftsmanagementmodul installiert ist, wird die Firmwareaktualisierung automatisch für beide Managementmodule ausgeführt. Klicken Sie auf **Browse** (Durchsuchen), um die gewünschte Firmwaredatei zu finden, und klicken Sie dann auf **Update** (Aktualisieren).

Die Firmware des Managementmoduls befindet sich in verschiedenen separaten Dateien, die unabhängig voneinander installiert werden. Sie müssen sämtliche Dateien zur Firmwareaktualisierung installieren. Sie erhalten die Firmwaredateien unter der folgenden Adressehttp://www.ibm.com/systems/support/.

Mithilfe der Methode "Remote File" (Ferne Datei) können Sie die vollständig qualifizierte Adresse der Firmware-Paketdatei für die Aktualisierung der Firmware des erweiterten Managementmoduls angeben. Die vollständig qualifizierte Adresse enthält ein Protokoll, das vom erweiterten Managementmodul unterstützt wird, gefolgt von einem Doppelpunkt und zwei Schrägstrichen (//), den Benutzernamen und das Kennwort, getrennt durch einen Doppelpunkt, zur Authentifizierung bei der Anmeldung, ein At-Zeichen (@), gefolgt von dem Hostnamen oder der IP-Adresse, eine optionale Anschlussnummer und den vollständigen Pfadnamen der Datei.

Anmerkung: Wenn die Anschlussnummer angegeben wird, muss sie durch einen Doppelpunkt vom Hostnamen (oder der IP-Adresse) getrennt werden.

Das vollständige Format der Adresse lautet:

Protokoll://*Benutzername*:*Kennwort*@*Hostname*:*Anschluss*/*Pfad*/*Dateiname*

Derzeit akzeptiert und versteht das erweiterte Managementmodul die folgenden Protokolle:

- TFTP
- FTP
- FTPS
- HTTP
- HTTPS

Eine vollständig qualifizierte Adresse sieht zum Beispiel wie folgt aus:
`ftp://USERID:PASSW0RD@192.168.0.2:30045/tmp/CNETCMUS.pkt`

In diesem Beispiel wird das FTP-Protokoll für die Übertragung der Paketdatei verwendet, der Benutzername lautet `USERID`, das Kennwort ist `PASSW0RD`, die IP-Adresse des Hosts (IPv4) lautet `192.168.0.2`, die Anschlussnummer ist `30045` und `/tmp` ist der vollständige Pfadname der Paketdatei mit dem Namen `CNETCMUS.pkt`.

Bei manchen Protokollen müssen Benutzername, Kennwort und Anschlussnummer nicht angegeben werden. Die Mindestvoraussetzungen für eine vollständige Adresse können daher wie folgt aussehen:

Protokoll://*Hostname*/*Pfad*/*Dateiname*

Gehen Sie wie folgt vor, um die Firmware des erweiterten Managementmoduls mithilfe einer fernen Datei zu aktualisieren:

1. Aktivieren Sie das Kontrollkästchen **Remote File** (Ferne Datei).
2. Geben Sie im Textfeld eine vollständig qualifizierte Adresse ein.
3. Klicken Sie auf die Schaltfläche **Update** (Aktualisieren) oder auf die Schaltfläche **Update and Reboot** (Aktualisieren und erneut starten).Wenn Sie die Schaltfläche **Update and Reboot** (Aktualisieren und erneut starten) verwenden, werden die Bestätigungsfenster umgangen und das erweiterte Managementmodul wird automatisch erneut gestartet, wenn das Flash-Update abgeschlossen ist.

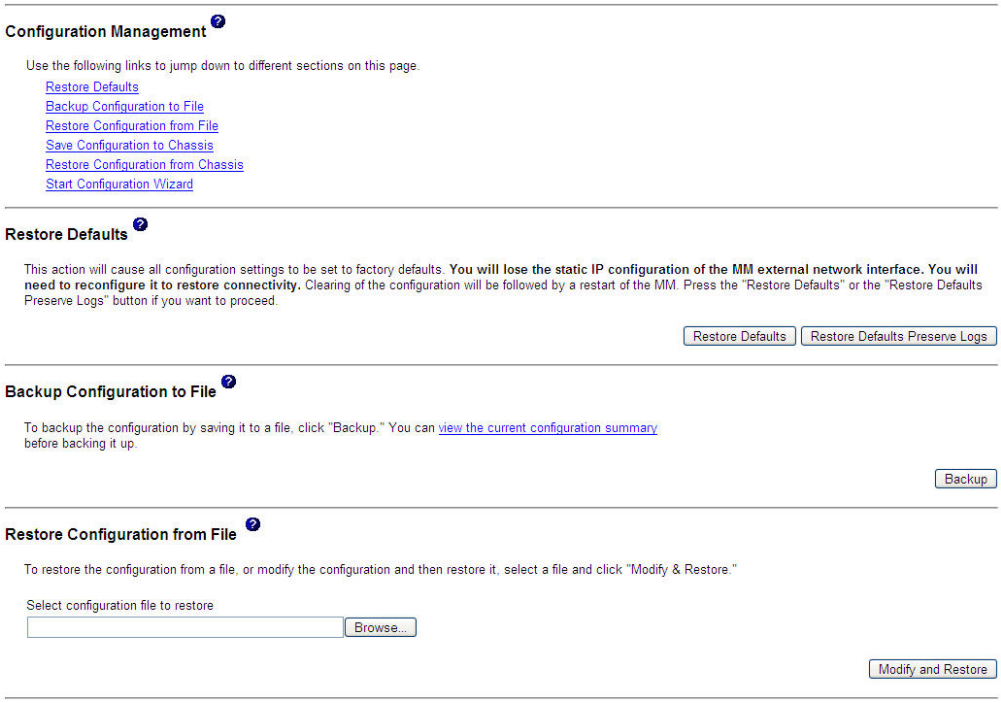
Anmerkung: Wenn Sie anstelle einer IP-Adresse einen Hostnamen verwenden, um eine ferne Datei anzugeben, stellen Sie sicher, dass DNS aktiviert ist.

Wichtig: Stellen Sie sicher, dass nach der Aktualisierung der Firmware des Managementmoduls für alle Benutzer die korrekten Berechtigungsklassen oder Berechtigungsebenen für Befehle festgelegt werden, da sich diese Festlegungen bei unterschiedlichen Firmwareversionen möglicherweise unterscheiden.

Wenn in einer BladeCenter-Einheit, die vorher nur über ein Managementmodul verfügte, ein Bereitschaftsmanagementmodul installiert wird, wird die Firmware für das neue Managementmodul mit der Firmwareversion des primären (bereits installierten) Managementmoduls aktualisiert. Diese Aktualisierung erfolgt während der Installation des Bereitschaftsmanagementmoduls. Es spielt keine Rolle, ob das neue Managementmodul bereits eine neuere Firmwareversion aufweist: die Firmwareversion des primären Managementmoduls hat Vorrang. Es kann bis zu 45 Minuten dauern, bis die Firmware im Bereitschaftsmanagementmodul aktualisiert und die Konfiguration für das Managementmodul übertragen ist.

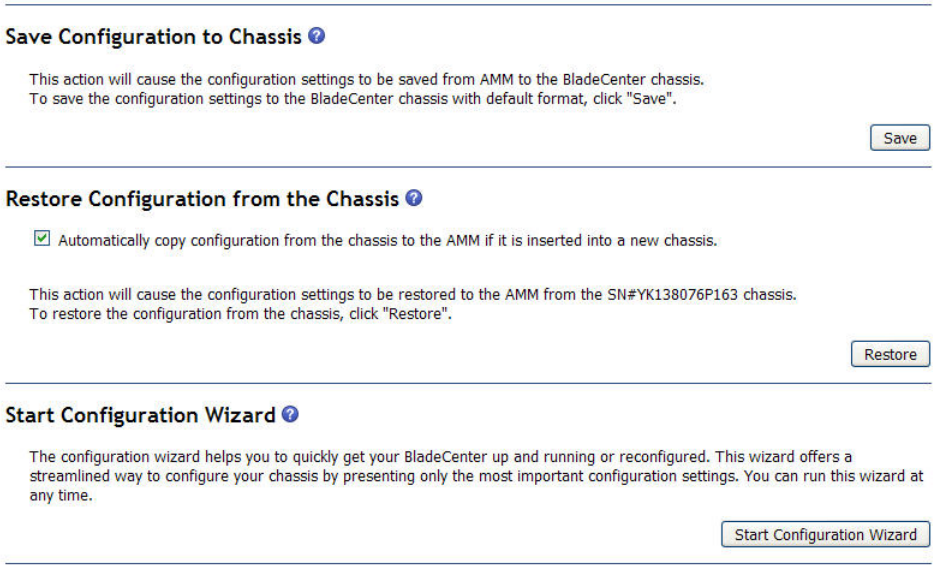
Configuration Mgmt (Konfigurationsverwaltung)

Wählen Sie **MM Control → Configuration Mgmt** (MM-Steuerung → Konfigurationsverwaltung) aus, um die Konfiguration des Managementmoduls zu sichern oder wiederherzustellen. Auf dieser Seite können Sie außerdem den Konfigurationsassistenten starten.

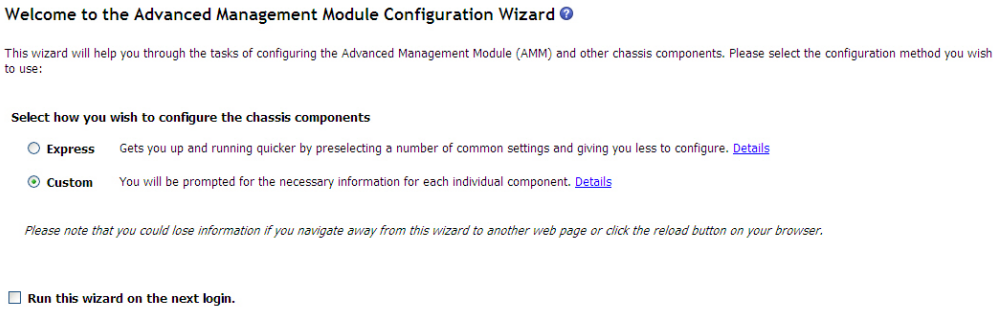


Das erweiterte Managementmodul stellt verschiedene Optionen für die Sicherung und Wiederherstellung bereit, einschließlich der Verwendung einer komprimierten Konfigurationsdatei für BladeCenter-Einheiten (ausgenommen BladeCenter H-Einheiten). (In BladeCenter H-Einheiten werden Sicherungen automatisch komprimiert.) Wenn Sie die Standardwerte wiederherstellen, können Sie auswählen, ob das Ereignisprotokoll des Managementmoduls gespeichert oder gelöscht werden soll. Entsprechende Anweisungen finden Sie im Abschnitt „Konfigurationsdatei verwenden” auf Seite 75.

Sie können Konfigurationsdateien auch auf der lokalen BladeCenter-Einheit (Gehäuse) speichern und sie von dieser Position wieder abrufen.



Klicken Sie auf den Link **Start Configuration Wizard** (Konfigurationsassistenten starten), um eine Installationsanleitung für das erweiterte Managementmodul aufzurufen. Der Konfigurationsassistent bietet Optionen für eine Expresskonfiguration und eine benutzerdefinierte Konfiguration.

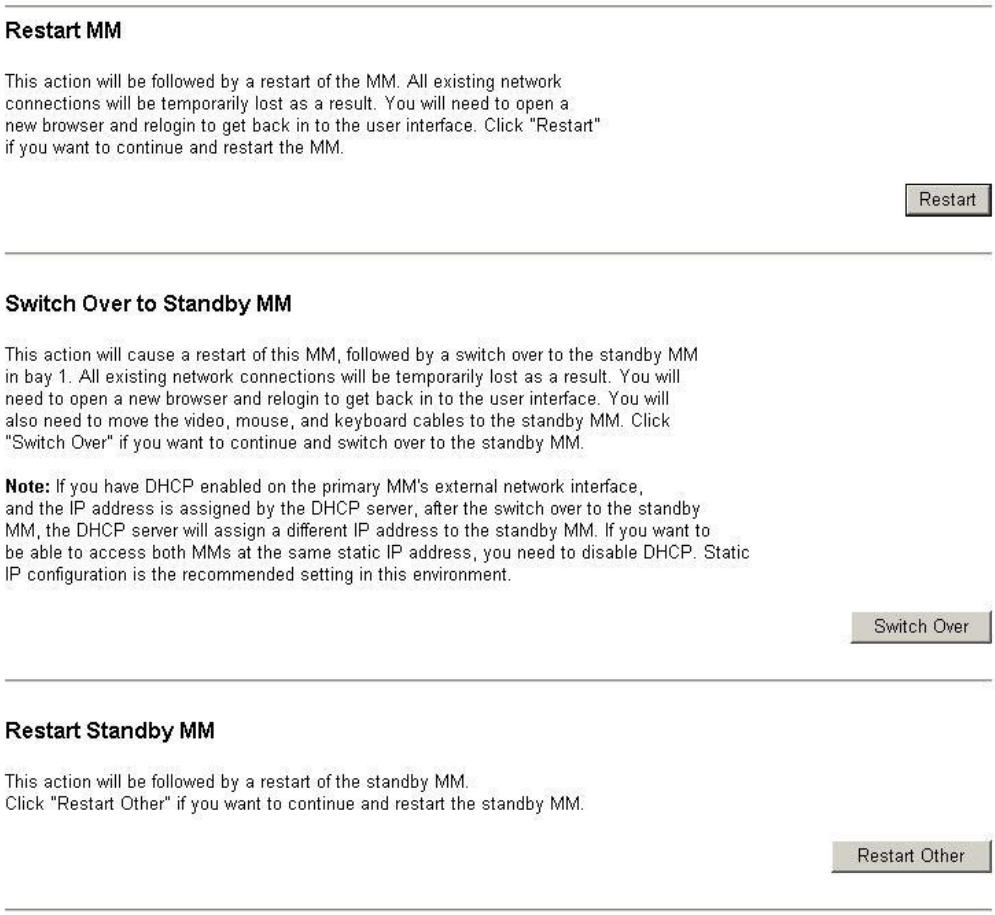


Der Konfigurationsassistent fasst die Informationen der anderen Seiten des erweiterten Managementmoduls in einem strukturierten Ablauf zusammen, der den Konfigurationsprozess vereinfacht. Informationen zur Verwendung des Konfigurationsassistenten finden Sie im Abschnitt „Konfigurationsassistent verwenden” auf Seite 23.

Restart MM (MM-Neustart)

Wählen Sie **MM Control → Restart MM** (MM-Steuerung → MM-Neustart) aus, um entweder das Managementmodul erneut zu starten oder die Steuerung auf ein alternatives Managementmodul in der BladeCenter-Einheit umzuschalten.

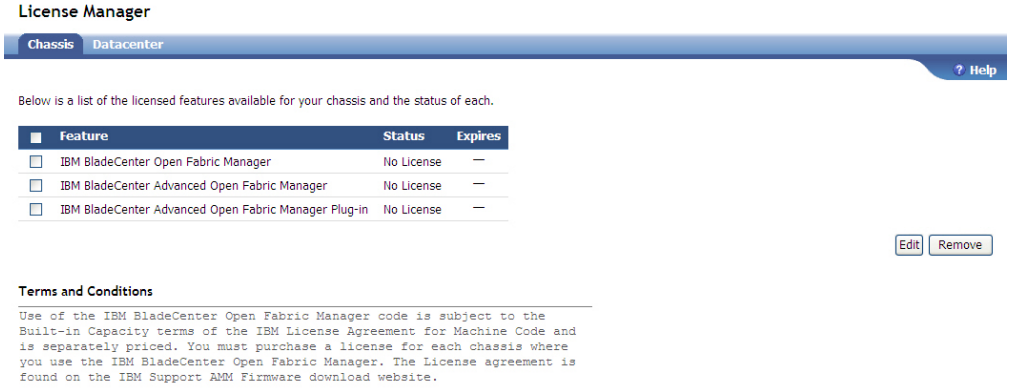
In der folgenden Abbildung ist die Seite "Restart MM" (MM-Neustart) eines erweiterten Managementmoduls dargestellt.



Wählen Sie **Restart MM** (MM-Neustart) aus, um das primäre Managementmodul erneut zu starten (zurückzusetzen). Wenn ein zweites Managementmodul installiert ist, können Sie mit dieser Option die Steuerung auf das Bereitschaftsmanagement-modul umschalten. Bei einem erweiterten Managementmodul können Sie auch das Bereitschaftsmanagementmodul erneut starten.

License Manager (Lizenzmanager)

Wählen Sie **MM Control → License Manager** (MM-Steuerung → Lizenzmanager) aus, um die Funktionen des erweiterten Managementmoduls zu verwalten, für die eine Lizenz erforderlich ist.



Die Option "License Manager" (Lizenzmanager) wird verwendet, um die Lizenzinformationen für einzelne BladeCenter-Einheiten oder für eine beliebige Anzahl von BladeCenter-Einheiten in einem Rechenzentrum zu verwalten. Sobald ein gültiger Lizenzschlüssel für die Funktion installiert wurde, können Sie die mit Extrakosten verbundenen Funktionen, wie beispielsweise Open Fabric Manager, in Ihrer BladeCenter-Einheit verwenden. Weitere Informationen zum Erhalt von Lizenzschlüsseln für die von Ihnen erworbenen Funktionen finden Sie unter der folgenden Adresse: http://licensing.datacentertech.net.

Lizenzschlüssel werden im erweiterten Managementmodul gespeichert und sind nur gültig, wenn das erweiterte Managementmodul in einer BladeCenter-Einheit installiert ist, die den richtigen Maschinentyp und die richtige Modell- und Seriennummer aufweist. Wenn Sie in der BladeCenter-Einheit ein neues erweitertes Managementmodul installieren oder die Konfiguration des erweiterten Managementmoduls auf ihre Standardwerte zurücksetzen, müssen Sie die Lizenzschlüssel erneut installieren. Bei BladeCenter-Einheiten mit primären und redundanten erweiterten Managementmodulen werden die Lizenzschlüssel, die im primären erweiterten Managementmodul gespeichert sind, im redundanten erweiterten Managementmodul gesichert. Bei diesen BladeCenter-Einheiten werden die Lizenzschlüssel beibehalten, wenn ein erweitertes Managementmodul ausgetauscht wird.

Auf der Seite "License Manager" (Lizenzmanager) wird die Registerkarte "Chassis" (Gehäuse) angezeigt, die den Status der lizenzierten Funktionen anzeigt, die im erweiterten Managementmodul für diese BladeCenter-Einheit installiert sind. Angezeigt werden die Namen der einzelnen Funktionen, die Anzahl der Tage bis zum Ablaufen der Lizenz und eine der folgenden Statusanzeigen für jede Funktion:

No License (Keine Lizenz)
: Die Funktion ist nicht verfügbar. Es wurden keine Daten zur Lizenzberechtigung eingegeben.

Active (Aktiv)
: Die lizenzierte Funktion ist verfügbar. Die Lizenz ist mit den korrekten Parametern installiert.

Chassis Serial Mismatch (Keine Übereinstimmung mit der Seriennummer des Gehäuses)
Die Funktion ist nicht verfügbar. Der im erweiterten Managementmodul gespeicherte Lizenzschlüssel stimmt nicht mit der Seriennummer der BladeCenter-Einheit überein.

Chassis Type Mismatch (Keine Übereinstimmung mit dem Gehäusetyp)
Die Funktion ist nicht verfügbar. Der auf der Seite "Enter License Information" (Lizenzinformationen eingeben) eingegebene Lizenzschlüssel ist nicht mit dem Typ der BladeCenter-Einheit kompatibel.

Expired (Abgelaufen)
Die Funktion ist nicht verfügbar. Die Testlizenz ist abgelaufen und nicht mehr aktiv.

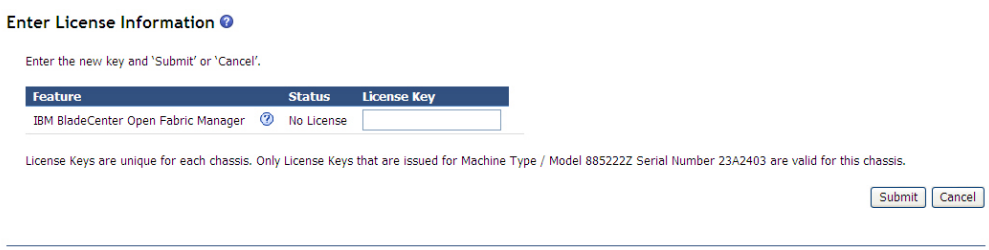
Für die BladeCenter-Funktionen stehen die folgenden Lizenztypen zur Verfügung:

Permanent (Permanent)
Dies ist der Standard-Lizenztyp für gekaufte Funktionen. Er weist kein Ablaufdatum auf.

60 Day Trial (60-Tage-Test)
Dieser Lizenztyp erlaubt die Verwendung einer Funktion für die Dauer von 60 Tagen beginnend mit dem Tag, an dem der Testlizenzschlüssel auf dem erweiterten Managementmodul installiert wurde.

Transitional (Übergang)
Die Generierung dieses Lizenztyps erfolgt automatisch für Benutzer von Basic Open Fabric Manager, die ihre Firmware für das erweiterte Managementmodul auf eine Version aktualisieren, die eine Überprüfung der Lizenzberechtigung implementiert. Mithilfe der Übergangslizenz können diese Benutzer den Basic Open Fabric Manager ohne Unterbrechung weiterhin verwenden. Wenn Sie eine Übergangslizenz besitzen, rufen Sie die folgende Adresse auf, um eine permanente Lizenz für Ihre BladeCenter-Einheit zu erhalten: http://licensing.datacentertech.net. Auf dieser Website werden permanente Lizenzen gesichert, um die Lizenzschlüssel bei Verlust oder im Falle eines Hardwarefehlers zu schützen. Rufen die Adresse http://licensing.datacentertech.net auf, um nach Lizenzen für Rechenzentren zu suchen, die über mehrere BladeCenter-Einheiten verfügen.

Wenn Sie die Lizenzinformationen für eine Funktion ändern möchten, wählen Sie sie aus und klicken Sie dann auf **Edit** (Bearbeiten). Wenn Sie eine Funktion auswählen und auf **Remove** (Entfernen) klicken, wird eine lizenzierte Funktion inaktiviert. Die folgende Seite wird angezeigt, wenn Sie eine Funktion bearbeiten.

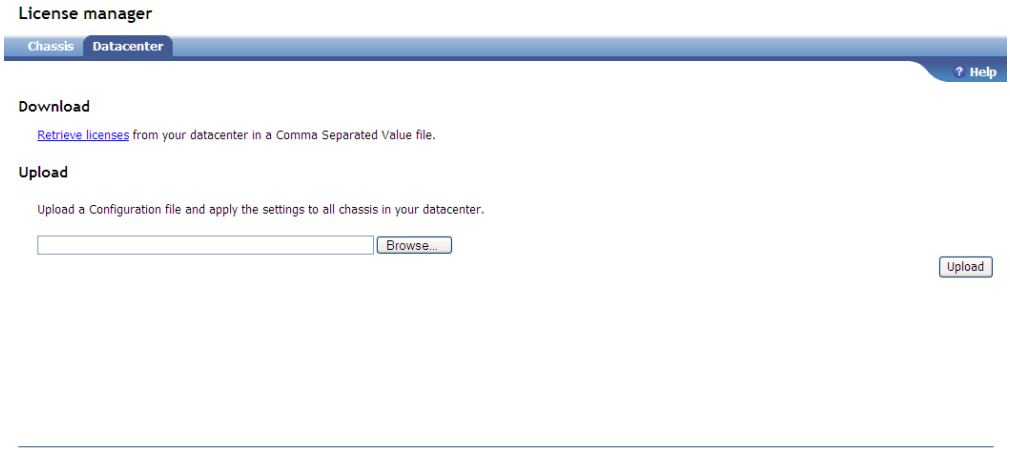


Zur Aktivierung von Funktionslizenzen müssen die folgenden Informationen eingegeben werden:

Lizenzschlüssel

Eine siebenstellige alphanumerische Zeichenfolge in Kleinschreibung, die für die Kombination aus Funktion, Gehäuse und Lizenztyp eindeutig ist. Lizenzschlüssel erhalten Sie auf der Lizenzierungs-Website unter der folgenden Adresse: http://licensing.datacentertech.net.

Auf der Registerkarte "Datacenter" (Rechenzentrum) können Sie eine Konfigurationsdatei mit den Lizenzinformationen für Ihr Rechenzentrum abrufen und herunterladen oder hochladen. Beide Vorgänge sind notwendig, um die Lizenzen in der Umgebung eines Rechenzentrums mit mehreren BladeCenter-Einheiten zu implementieren und zu verwalten.



Beim Downloadvorgang werden alle Managementmodule in einem Rechenzentrum lokalisiert. Dabei wird eine Lizenzdatei mit Hardware- und Lizenzinformationen für alle BladeCenter-Einheiten, die von den einzelnen Managementmodulen gemeldet werden, erzeugt. Diese Datei kann auf die folgende Lizenzierungs-Website hochgeladen werden: http://licensing.datacentertech.net, um den Datensatz mit den Lizenzinformationen für das Rechenzentrum zu erstellen oder zu aktualisieren. Auf der Seite „Network Protocols (Netzprotokolle)" auf Seite 192 in jedem Managementmodul im Rechenzentrum muss SLP (Service Location Protocol) aktiviert sein, damit diese Datenabfrage durchgeführt werden kann. Auf der Seite „Port Assignments (Portzuordnungen)" auf Seite 185 muss außerdem das TCP-Befehlsmodusprotokoll aktiviert sein und der Benutzername und das Kennwort für die laufende Anmeldesitzung müssen für alle erkannten Managementmodule gelten, damit ihr Lizenzstatus erfasst werden kann.

Beim Upload-Vorgang wird die angegebene Lizenzdatei akzeptiert und die darin enthaltenen Lizenzschlüssel werden auf den in der Datei aufgeführten Managementmodulen implementiert. Die Download- und Upload-Vorgänge beschleunigen die Datenabfrage und die Implementierung der Lizenzen und vermeiden die mit der manuellen Dateneingabe verbundenen Fehler.

Service Tools (Service-Tools)

Wählen Sie bei einem erweiterten Managementmodul die Seiten unter **Service Tools** (Service-Tools) aus, um auf Informationen zuzugreifen, die einem Techniker bei der Wartung der BladeCenter-Einheit helfen können.

Zu den Optionen unter "Service Tools" (Service-Tools) zählen:

- „AMM Service Data (Servicedaten des erweiterten Managementmoduls)"
- „Blade Service Data (Blade-Servicedaten)" auf Seite 209
- „AMM Status (Status der erweiterten Managementmodule)" auf Seite 211
- „Service Advisor" auf Seite 214

AMM Service Data (Servicedaten des erweiterten Managementmoduls)

Wählen Sie **Service Tools → AMM Service Data** (Service-Tools → Servicedaten des erweiterten Managementmoduls) aus, um Informationen aus der Servicedaten-Erfassungsdatei anzuzeigen oder herunterzuladen.

Anmerkungen:

- Wenn Sie die Service Advisor-Funktion aktiviert haben, wird diese Servicedaten-Erfassungsdatei automatisch an IBM gesendet, sobald ein wartungsfähiges Ereignis eintritt. Weitere Informationen dazu finden Sie im Abschnitt „IBM Service Advisor" auf Seite 86.
- Klicken Sie zum Senden dieser Servicedaten-Erfassungsdatei an IBM auf **Manually Email Service Information** (Serviceinformationen manuell per E-Mail senden).
- Bei BladeCenter S-Einheiten mit installiertem RAID-SAS-Modul werden auf dieser Seite die elementaren Produktdaten für die Einheit zur Notstromversorgung aufgelistet.

Klicken Sie auf **Save Service Data** (Servicedaten speichern), um diese Servicedaten-Erfassungsdatei auf Ihrem System zu speichern.

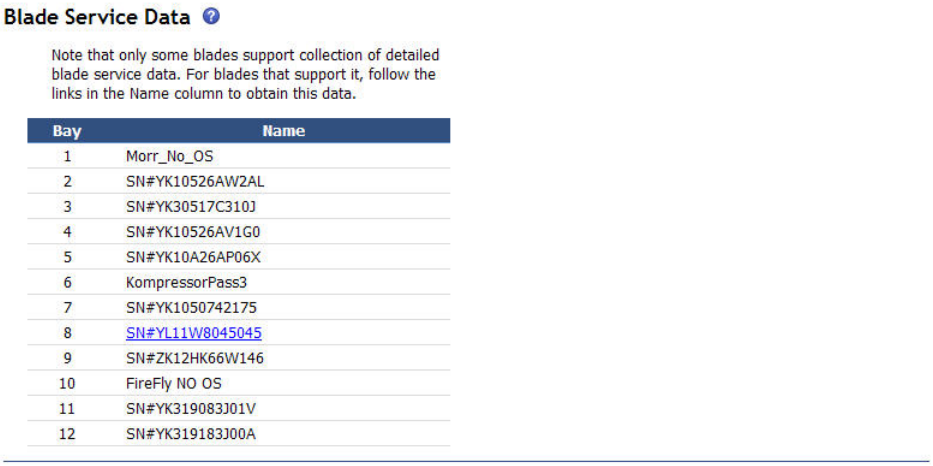
Der Dateiname der Servicedaten-Erfassungsdatei wird automatisch generiert und weist das Format *NameEMM_JJJJMMTT_hhmmss*.tgz auf. Dabei gilt:

- *NameEMM* steht für den Namen des erweiterten Managementmoduls.
- *JJJJMMTT* steht für das Datum der Servicedatenerfassung im Format "Jahr-Monat-Tag".
- *hhmmss* steht für die Uhrzeit der Servicedatenerfassung im 24-Stunden-Format "Stunde-Minute-Sekunde".
- Die Erweiterung ".tgz" bedeutet, dass es sich um eine gzip-komprimierte tar-Archivdatei handelt, die Sie mit gängigen Dienstprogrammen entpacken können.

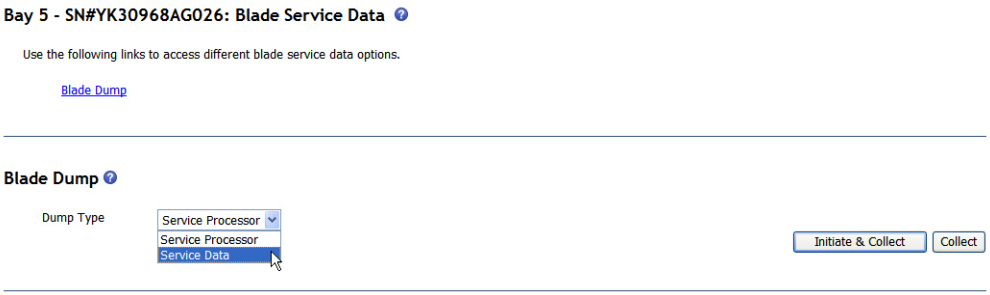
Blade Service Data (Blade-Servicedaten)

Wählen Sie **Service Tools → Blade Service Data** (Service-Tools → Blade-Servicedaten) aus, um eine Tabelle mit allen Blade-Servern in der BladeCenter-Einheit anzuzeigen. Die Seite "Blade Service Data" (Blade-Servicedaten) ist nur verfügbar, wenn sich in der BladeCenter-Einheit mindestens ein Blade-Server befindet, der die Erfassung von Blade-Servicedaten unterstützt.

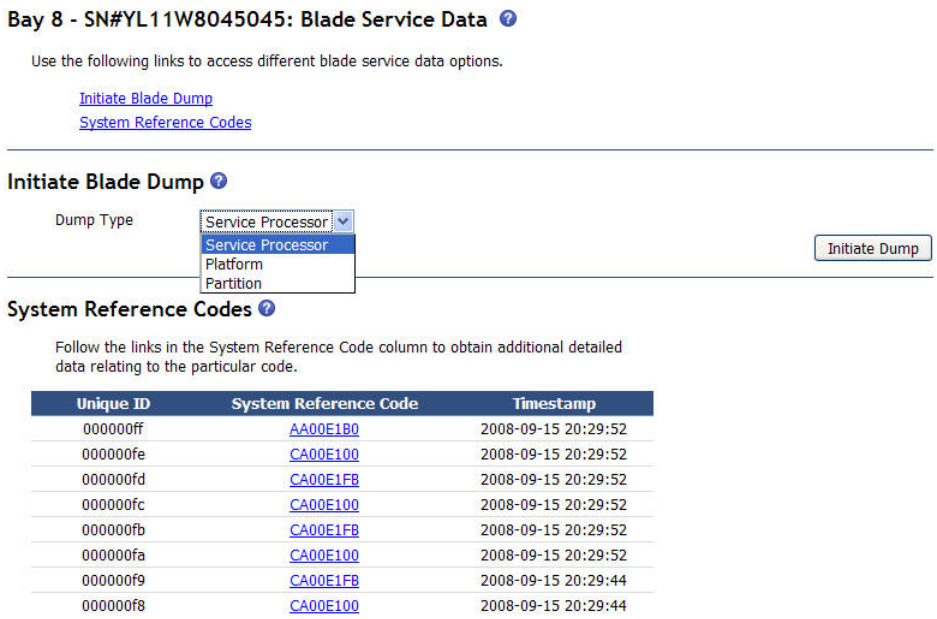
Für jeden Blade-Server, der die Erfassung detaillierter Blade-Server-Servicedaten unterstützt, gibt es in der Spalte **Name** (Name) einen Link. Klicken Sie auf den Link, um die Servicedaten für diesen Blade-Server zu verwalten. Diese Links werden nur angezeigt, wenn sich in der BladeCenter-Einheit mindestens ein Blade-Server befindet, der die Erfassung von Blade-Server-Servicedaten unterstützt.



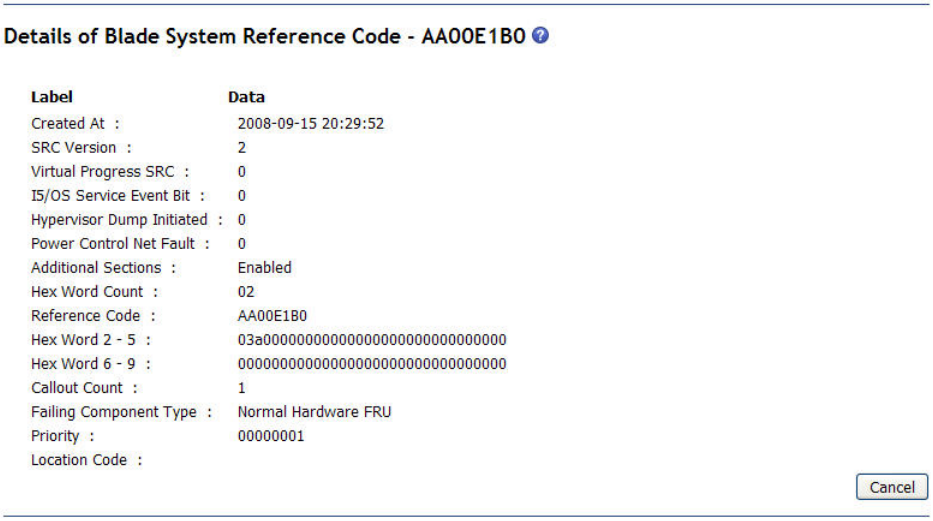
Wählen Sie mithilfe des Menüs im Abschnitt **Initiate Blade Dump** (Blade-Speicherauszug einleiten) die Art des Speicherauszugs aus, den Sie für die Blade-Server-Servicedaten generieren möchten. Klicken Sie anschließend auf **Initiate & Collect** (Einleiten & Erfassen), um einen Speicherauszug für die Blade-Server-Servicedaten zu erstellen und anzuzeigen, oder klicken Sie auf **Collect** (Erfassen), um die Daten anzuzeigen, die während des letzten Speicherauszugs erfasst wurden. Die verfügbaren Arten von Servicedaten hängen vom jeweiligen Blade-Server-Typ ab. Durch neue Speicherauszüge werden vorhandene Speicherauszugsdaten überschrieben und die Speicherauszüge können von den Unterstützungsmitarbeitern zur Fehlerdiagnose verwendet werden. Möglicherweise bewirkt der Speicherauszug, dass zugeordnete Datensätze mit Systemreferenzcodes generiert werden.



Im Abschnitt **System Reference Codes** (Systemreferenzcodes) wird eine Tabelle mit den 32 neuesten Systemreferenzcodes für einen Blade-Server angezeigt. In dieser Schnittstelle ist angegeben, ob ausführliche Daten für einen bestimmten Systemreferenzcode verfügbar sind.



Zum Anzeigen der Details zu einem Systemreferenzcode klicken Sie auf den jeweiligen Link. Eine Seite mit den Details zum ausgewählten Systemreferenzcode wird angezeigt.



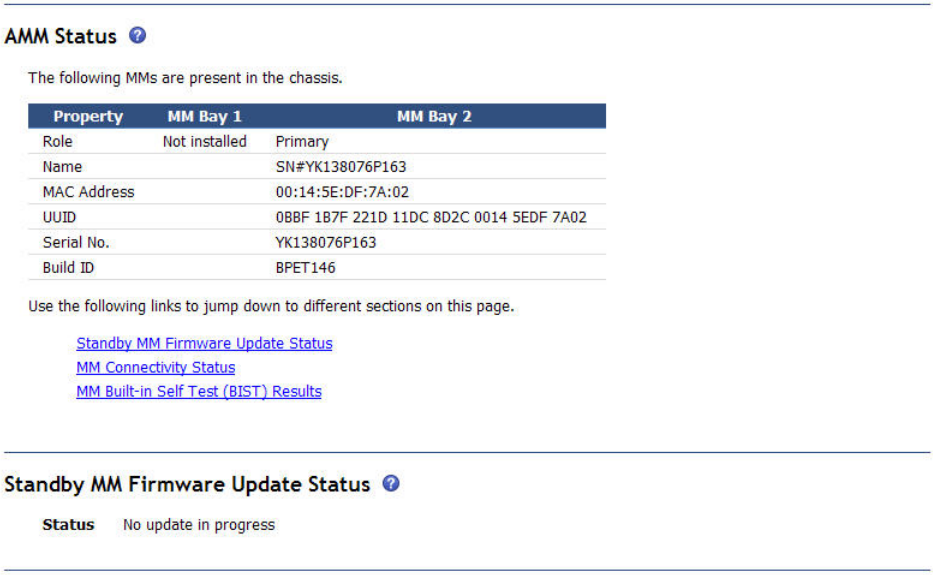
Die Informationen auf dieser Seite können von den Unterstützungsmitarbeitern zur Fehlerdiagnose verwendet werden. Hilfreiche Informationen zum Interpretieren der Codes und Detaildaten finden Sie im *Fehlerbestimmungs- und Servicehandbuch*.

Anmerkung: Manche Blade-Server unterstützen keine Systemreferenzcodes.

AMM Status (Status der erweiterten Managementmodule)

Wählen Sie **Service Tools → AMM Status** (Service-Tools → Status der erweiterten Managementmodule) aus, um Informationen anzuzeigen, mit denen die in der BladeCenter-Einheit installierten erweiterten Managementmodule eindeutig identifiziert werden können.

Klicken Sie auf **Standby MM Firmware Update Status** (Status der Firmwareaktualisierung des Bereitschaftsmanagementmoduls), um den Fortschritt einer Firmwareaktualisierung für das erweiterte Bereitschaftsmanagementmodul anzuzeigen. Klicken Sie auf **MM Connectivity Status** (MM-Verbindungsstatus), um den Status der Verbindungen von Managementmodulen anzuzeigen. Klicken Sie auf **MM Built-in Self Test (BIST) Results** (Ergebnisse der integrierten MM-Selbsttests), um die Ergebnisse der Selbsttests für Managementmodule anzuzeigen.



Im Abschnitt **Standby MM Firmware Update Status** (Status der Firmwareaktualisierung des Bereitschaftsmanagementmoduls) werden der Status der Firmwareaktualisierung, die Versionen der Firmware-Images, der Fertigstellungsprozentsatz und die geschätzte Zeit bis zum Abschluss der Firmwareaktualisierung für das Bereitschaftsmanagementmodul angezeigt.

Anmerkung: Die BladeCenter S-Einheit unterstützt kein zweites (Bereitschafts-) Managementmodul. Daher wird diese Kategorie nicht in der Benutzerschnittstelle des Managementmoduls für die BladeCenter S-Einheit angezeigt.

Im Abschnitt **MM Connectivity Status** (MM-Verbindungsstatus) wird der Status der Verbindungen zwischen den Managementmodulen und anderen BladeCenter-Komponenten angezeigt. Der Status von Verbindungen zum primären Managementmodul wird in regelmäßigen Abständen aktualisiert. Wenn ein Bereitschaftsmanagementmodul installiert ist, werden für seinen Verbindungsstatus die Daten angezeigt, die erfasst wurden, als das Managementmodul zum letzten Mal als primäres Managementmodul verwendet wurde. Wenn das Managementmodul noch nie als primäres Managementmodul eingesetzt wurde, sind keine Statusdaten dazu verfügbar. Das Feld **Last Update** (Letzte Aktualisierung) wird angezeigt, nachdem die Statusinformationen für jedes Managementmodul erfasst wurden.

Anmerkung: Bei der Version des erweiterten Managementmoduls für die BladeCenter S-Einheit werden auch Verbindungsinformationen für die Speichermodule angezeigt.

MM Connectivity Status

Status:
Last update: 6/01/2009 15:37

Module	MM Bay 1 (Primary)	MM Bay 2 (Empty)
Blade 1	Not Installed	
Blade 2	Not Installed	
Blade 3	Not Installed	
Blade 4	Communicating	
Blade 5	Not Installed	
Blade 6	Not Installed	
Blade 7	Not Installed	
Blade 8	Not Installed	
Blade 9	Not Installed	
Blade 10	Not Installed	
Blade 11	Not Installed	
Blade 12	Not Installed	
Blade 13	Not Installed	
Blade 14	Not Installed	
I/O Module 1	Communicating	
I/O Module 2	Not Installed	
I/O Module 3	Not Installed	
I/O Module 4	Not Installed	
I/O Module 5	Not Installed	
I/O Module 6	Not Installed	
I/O Module 7	Not Installed	
I/O Module 8	Not Installed	
I/O Module 9	Not Installed	
I/O Module 10	Not Installed	
Media Tray	Communicating	
Power Module 1	Communicating	
Power Module 2	Communicating	
Power Module 3	Communicating	
Power Module 4	Communicating	
Power Module Cooling Device 1	Communicating	

Im Abschnitt **MM Built-in Self Test (BIST) Results** (Ergebnisse der integrierten MM-Selbsttests) werden die Ergebnisse der integrierten Selbsttests für die Managementmodule angezeigt.Die Testergebnisse werden sowohl für das primäre Managementmodul als auch für das Bereitschaftsmanagementmodul aktualisiert. Das Feld **Last Update** (Letzte Aktualisierung) wird angezeigt, nachdem die Testergebnisse für jedes Managementmodul erfasst wurden.

MM BIST Results

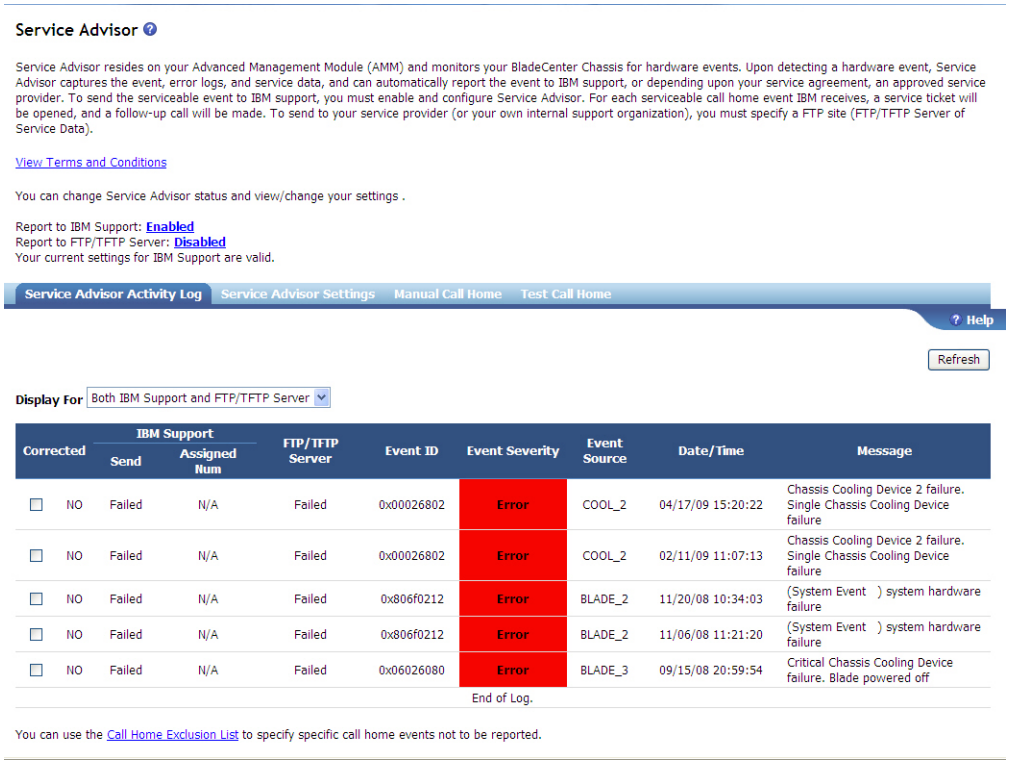
Status:
Last update: 6/01/2009 15:37

Function	MM Bay 1 (Primary)	MM Bay 2 (Empty)
Blade Management Bus 1	Passed	
Blade Management Bus 2	Passed	
Real-time Clock	Passed	
Local Management Bus	Passed	
Primary File System	Passed	
Backup File System	Passed	
Boot Loader	Passed	
Ethernet Port (eth0)	Passed	
External Management Bus	Passed	
Internal Ethernet Switch	Passed	
Video Capture	Passed	
USB Keyboard/Mouse Emulation	Passed	
USB Mass Storage Emulation	Passed	
USB Keyboard/Mouse Firmware	Passed	
USB Mass Storage Firmware	Passed	
Primary Core	Passed	
Backup Core	Passed	
Internal I/O Expander	Passed	
Remote Control Firmware	Passed	
Physical Network Link	Passed	
Logical Network Link	Passed	

Refresh

Service Advisor

Wählen Sie **Service Tools → Service Advisor** (Service-Tools → Service Advisor) aus, um den BladeCenter Service Advisor so zu konfigurieren, dass er Informationen zur Wartungsfähigkeit von Hardware und Firmware automatisch an IBM sendet.



Service Advisor

Service Advisor resides on your Advanced Management Module (AMM) and monitors your BladeCenter Chassis for hardware events. Upon detecting a hardware event, Service Advisor captures the event, error logs, and service data, and can automatically report the event to IBM support, or depending upon your service agreement, an approved service provider. To send the serviceable event to IBM support, you must enable and configure Service Advisor. For each serviceable call home event IBM receives, a service ticket will be opened, and a follow-up call will be made. To send to your service provider (or your own internal support organization), you must specify a FTP site (FTP/TFTP Server of Service Data).

View Terms and Conditions

You can change Service Advisor status and view/change your settings .

Report to IBM Support: Enabled
Report to FTP/TFTP Server: Disabled
Your current settings for IBM Support are valid.

Service Advisor Activity Log | Service Advisor Settings | Manual Call Home | Test Call Home

Help

Refresh

Display For: Both IBM Support and FTP/TFTP Server

Corrected	IBM Support: Send	IBM Support: Assigned Num	FTP/TFTP Server	Event ID	Event Severity	Event Source	Date/Time	Message
NO	Failed	N/A	Failed	0x00026802	Error	COOL_2	04/17/09 15:20:22	Chassis Cooling Device 2 failure. Single Chassis Cooling Device failure
NO	Failed	N/A	Failed	0x00026802	Error	COOL_2	02/11/09 11:07:13	Chassis Cooling Device 2 failure. Single Chassis Cooling Device failure
NO	Failed	N/A	Failed	0x806f0212	Error	BLADE_2	11/20/08 10:34:03	(System Event) system hardware failure
NO	Failed	N/A	Failed	0x806f0212	Error	BLADE_2	11/06/08 11:21:20	(System Event) system hardware failure
NO	Failed	N/A	Failed	0x06026080	Error	BLADE_3	09/15/08 20:59:54	Critical Chassis Cooling Device failure. Blade powered off

End of Log.

You can use the Call Home Exclusion List to specify specific call home events not to be reported.

Anmerkung: Obwohl Service Advisor in der Lage ist, Alerts rund um die Uhr an sieben Tagen der Woche zu senden, reagiert Ihr Service-Provider gemäß der mit Ihnen getroffenen Vereinbarung. Bei Fragen wenden Sie sich bitte an Ihren Service-Provider. Informationen zu den Bedingungen des Herstellerservice und zum Anfordern von Service und Unterstützung finden Sie im Dokument mit den Informationen zu Herstellerservice und Unterstützung für Ihre BladeCenter-Einheit. Aktuelle Informationen zu Ihrer BladeCenter-Einheit finden Sie unter der Adresse http://www.ibm.com/bladecenter/.

Auf der Registerkarte **Service Advisor Activity Log** (Service Advisor-Aktivitätenprotokoll) werden alle Ereignisse angezeigt, die gemeldet werden können. Klicken Sie auf den Link **Call Home Exclusion List** (Call-Home-Ausschlussliste), um die Ereignisse auszuwählen, die nicht gemeldet werden sollen (wenden Sie sich an Ihren zuständigen IBM Ansprechpartner, bevor Sie diese Funktion verwenden). Auf der Registerkarte **Service Advisor Settings** (Service Advisor-Einstellungen) können Sie die Kontaktinformationen und Konfigurationsdaten für Service Advisor definieren. Auf den Registerkarten **Manual Call Home** (Manuelle Call-Home-Funktion) und **Test Call Home** (Call-Home-Funktion testen) können Sie Testnachrichten generieren. Wenn Sie den BladeCenter Service Advisor zum ersten Mal konfigurieren oder wenn die Firmware des Managementmoduls auf die Standardwerte zurückgesetzt wurde, müssen Sie eine Lizenzvereinbarung anzeigen und akzeptieren, die Kontaktinformationen definieren und die Service Advisor-Funktion aktivieren. Weitere Informationen und Anweisungen finden Sie im Abschnitt „IBM Service Advisor" auf Seite 86.

Anmerkung: Wenn Sie einen Linux-TFTP-Server verwenden, um Informationen zur Wartungsfähigkeit von Hardware und Firmware an IBM zu senden, müssen Sie die TFTP-Konfigurationsdatei ändern. Siehe „Linux-TFTP-Server konfigurieren" auf Seite 72.

Scalable Complex (Skalierbarer Komplex)

Wählen Sie bei einem erweiterten Managementmodul die Optionen unter **Scalable Complex** (Skalierbarer Komplex) aus, um die skalierbaren Komplexe in der BladeCenter-Einheit anzuzeigen und zu verwalten.

Anmerkung:

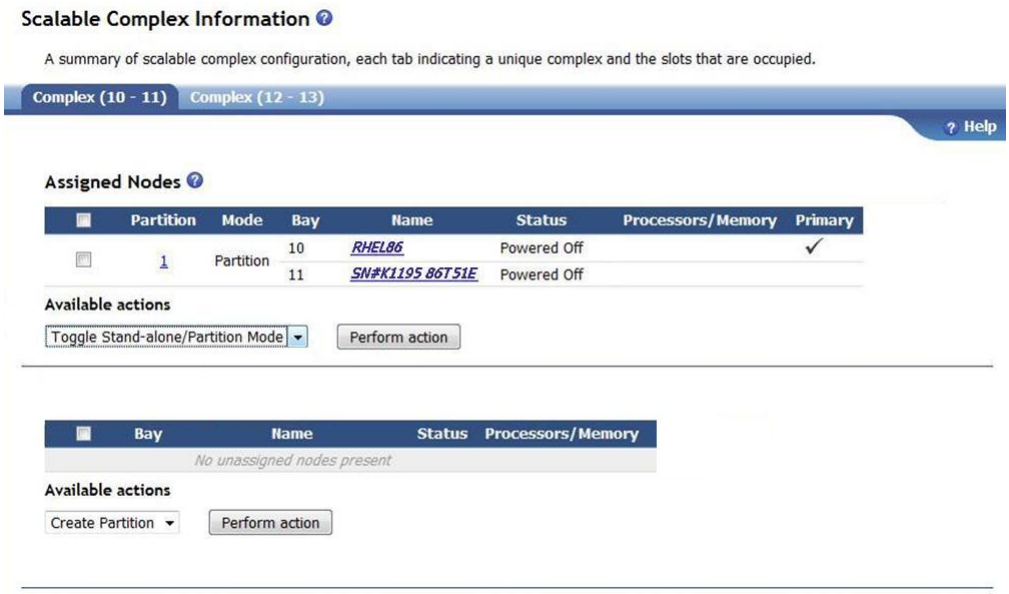
- Diese Seiten sind nur verfügbar, wenn ein Blade-Server mit Unterstützung für skalierbare Komplexe in der BladeCenter-Einheit installiert ist. Wenn keine Blade-Server installiert sind, die diese Funktion unterstützen, wird der Abschnitt "Scalable Complex" (Skalierbarer Komplex) nicht angezeigt.
- Alle Blade-Server in einem skalierbaren Komplex müssen dieselbe Firmwareversion aufweisen. Die koordinierte Aktualisierung der Firmware für alle Blade-Server in einem skalierbaren Komplex wird vom erweiterten Managementmodul unterstützt (zusätzliche Informationen finden Sie im Abschnitt „Firmware Update (Firmwareaktualisierung)" auf Seite 146).

Mithilfe eines skalierbaren Komplexes können Blade-Server, die als "Knoten" bezeichnet werden, in logischen Gruppen zusammengefasst werden, den sogenannten "Partitionen". Blade-Server in einer Partition verhalten sich wie ein einziges System und können Ressourcen gemeinsam nutzen. Einzelne Blade-Server können als Standalone-Partition mit nur einem Knoten konfiguriert werden, damit sie diese Konfiguration beibehalten, wenn sie in einer anderen BladeCenter-Einheit installiert werden.

Configuration (Konfiguration)

Wählen Sie **Scalable Complex → Configuration** (Skalierbarer Komplex → Konfiguration) aus, um die Einstellungen für skalierbare Blade-Server-Komplexe anzuzeigen und zu ändern.

In der folgenden Abbildung sind die verfügbaren Aktionen für zugeordnete Knoten in einem skalierbaren Komplex dargestellt. Beim Öffnen der Seite wird die Registerkarte für den ersten skalierbaren Komplex angezeigt. Sind weitere skalierbare Komplexe verfügbar, können Sie auf die einzelnen Registerkarten klicken, um die Informationen zu jedem Komplex anzuzeigen und zu ändern.



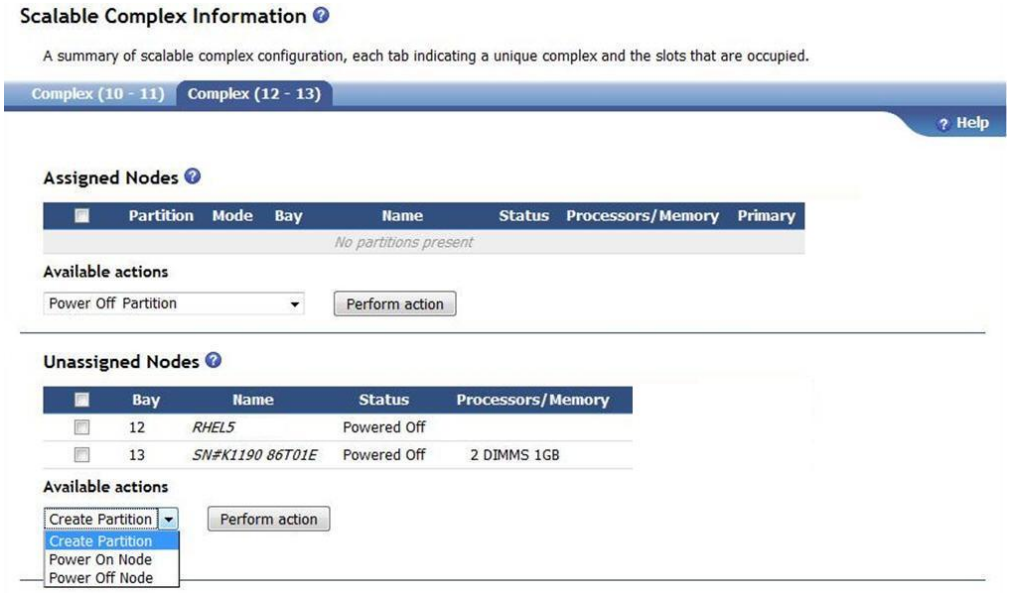
In einem skalierbaren Komplex handelt es sich bei jedem Knoten um einen Blade-Server. Die Blade-Server-Knoten können in Partitionen gruppiert werden, die als ein einziges System funktionieren und gemeinsame Ressourcen nutzen. Der Name jedes Knotens stellt einen Link dar, der auf ausführliche Informationen zu dem Blade-Server verweist, für den der Knoten steht.

Sie können die folgenden Aktionen, die unter **Available actions** (Verfügbare Aktionen) aufgeführt sind, auf eine ausgewählte Partition und deren Blade-Server-Knoten anwenden, indem Sie auf **Perform action** (Aktion durchführen) klicken. Wählen Sie mithilfe des Kontrollkästchens mindestens eine Partition in einem Komplex aus.

- Power off partition (Partition ausschalten).
- Power on partition (Partition einschalten).
- Power cycle partition (Partition aus- und wieder einschalten): Ist die Partition ausgeschaltet, wird sie eingeschaltet. Ist die Partition eingeschaltet, wird sie aus- und dann wieder eingeschaltet.
- Remove partition (Partition entfernen): Alle Blade-Server-Knoten in der Partition werden wieder in den nicht zugeordneten Status versetzt.
- Toggle stand-alone/partition mode (Standalone-/Partitionsmodus umschalten): Eine Partition, für die der Standalone-Modus festgelegt wurde, wird als ein einziges Blade-Server-System betrieben. Einzelne Blade-Server, die als Standalone-Partition konfiguriert wurden, verhalten sich einheitlich, wenn sie in einer anderen BladeCenter-Einheit installiert werden.

Anmerkung: Eine Partition muss vor dem Entfernen ausgeschaltet werden.

In der folgenden Abbildung sind die verfügbaren Aktionen für nicht zugeordnete Knoten in einem skalierbaren Komplex dargestellt.



Sie können die folgenden Aktionen, die unter **Available actions** (Verfügbare Aktionen) aufgeführt sind, auf einen ausgewählten Blade-Server-Knoten anwenden, indem Sie auf **Perform action** (Aktion durchführen) klicken. Wählen Sie mithilfe des Kontrollkästchens mindestens einen Knoten in einem Komplex aus.

- Power off node (Knoten ausschalten): Die ausgewählten Knoten werden ausgeschaltet.
- Power on node (Knoten einschalten): Die ausgewählten Knoten werden eingeschaltet.
- Cycle node (Knoten aus- und wieder einschalten): Sind die ausgewählten Knoten ausgeschaltet, werden sie eingeschaltet. Sind die ausgewählten Knoten eingeschaltet, werden sie aus- und dann wieder eingeschaltet.
- Create partition (Partition erstellen): Alle ausgewählten Blade-Server-Knoten werden in einer Partition gruppiert.

Anmerkung:

- Zum Erstellen einer Partition müssen alle Knoten, die darin gruppiert werden, ausgeschaltet sein.
- Das Erstellen einer Partition mit Blade-Server-Knoten, die für die optionale BOFM-Funktion (Blade Open Fabric Manager) aktiviert wurden, führt möglicherweise zum Verlust von Ports, die für Open Fabric Manager konfiguriert wurden.

Kapitel 4. Fehlerbehebung

Dieser Abschnitt enthält grundlegende Informationen zur Fehlerbehebung, die Sie bei der Lösung von häufig auftretenden Problemen unterstützen sollen.

Wenn Sie ein Problem nicht mithilfe der Informationen in diesem Abschnitt bestimmen und lösen können, finden Sie Informationen unter „Hilfe und technische Unterstützung anfordern", auf Seite 221.

Häufig auftretende Probleme

Dieser Abschnitt enthält Beschreibungen von häufig auftretenden Problemen, zu denen es bei der Verwendung des erweiterten Managementmoduls kommen kann.

Tabelle 6. Häufig auftretende Probleme

Fehlersymptom	Maßnahme
Für das erweiterte Managementmodul mit der FRU-Teilenummer 44X3058 kann nur ein Upgrade auf die Firmwareversion BPET62C (oder höher) durchgeführt werden. **Anmerkungen:** • Sie können kein Firmwareupgrade für eine ältere Version als BPET62C, wie z. B. BPET54V, durchführen. • Wenn die FRU 44X3058 als sekundäres erweitertes Managementmodul installiert ist und das primäre erweiterte Managementmodul eine ältere Firmwareversion als BPET62C aufweist, übernimmt die FRU 44X3058 nicht die ältere Firmwareversion des primären Moduls. Kommt es zu einer nachfolgenden Funktionsübernahme, bei der die FRU 44X3058 als primäres Modul arbeitet, wird für das System eine Aktualisierung auf die neuere Firmwareversion durchgeführt.	Aktualisieren Sie die Firmware. Wählen Sie **Monitors** > **Firmware VPD** (**Monitore** > **Elementare Firmware-Produktdaten**) und **Management Module Firmware Vital Product Data** > **Build ID** (**Elementare Firmware-Produktdaten des Managementmoduls** > **Build-ID**) aus, um die Firmwareversion des erweiterten Managementmoduls für die BladeCenter-Einheit anzuzeigen. Weitere Informationen dazu finden Sie im Abschnitt „Firmware VPD (Elementare Firmware-Produktdaten)" auf Seite 137.

Anhang. Hilfe und technische Unterstützung anfordern

Wenn Sie Hilfe, Serviceleistungen oder technische Unterstützung benötigen oder einfach nur Informationen zu IBM Produkten erhalten möchten, finden Sie bei IBM eine Vielzahl von hilfreichen Quellen.

In diesem Abschnitt finden Sie Informationen dazu, wo Sie ausführlichere Informationen zu IBM und zu IBM Produkten finden, was Sie bei Problemen mit dem IBM System oder der Zusatzeinrichtung tun können, und an wen Sie sich wenden können, wenn Sie Serviceleistungen benötigen.

Bevor Sie anrufen

Bevor Sie anrufen, sollten Sie die folgenden Schritte durchführen und versuchen, das Problem selbst zu beheben.

Wenn Sie denken, dass Sie den IBM Herstellerservice für Ihr IBM Produkt benötigen, sollten Sie sich vorbereiten, bevor Sie sich an den Kundendienst wenden, damit Ihnen die IBM Kundendiensttechniker besser helfen können.

- Überprüfen Sie alle Kabel, um sicherzustellen, dass sie angeschlossen sind.
- Überprüfen Sie die Netzschalter, um sicherzustellen, dass das System und alle Zusatzeinrichtungen eingeschaltet sind.
- Überprüfen Sie, ob aktualisierte Software, Firmware und Einheitentreiber für das Betriebssystem Ihres IBM Produkts vorhanden sind. In den Bedingungen des IBM Herstellerservice ist festgelegt, dass Sie als Eigner des IBM Produkts für die Wartung und Aktualisierung der gesamten Software und Firmware für das Produkt verantwortlich sind (es sei denn, dies ist durch einen zusätzlichen Wartungsvertrag abgedeckt). Der zuständige IBM Kundendiensttechniker wird Sie bitten, ein Upgrade für Ihre Software und Firmware durchzuführen, wenn ein Softwareupgrade eine dokumentierte Lösung für das Problem enthält.
- Wenn Sie neue Hardware oder Software in Ihrer Umgebung installiert haben, überprüfen Sie unter http://www.ibm.com/systems/info/x86servers/serverproven/compat/us, ob die Hardware und Software von Ihrem IBM Produkt unterstützt werden.
- Informationen zur Fehlerbehebung finden Sie unter http://www.ibm.com/supportportal.
- Halten Sie folgende Informationen für die IBM Unterstützung bereit. Anhand dieser Daten kann die IBM Unterstützung einen Fehler schnell beheben und sicherstellen, dass Sie Ihren vertraglich vereinbarten Service erhalten.
  - Nummern von Hardware- und Softwarewartungsverträgen, falls zutreffend
  - Maschinentypnummer (vierstellige IBM Geräte-ID)
  - Modellnummer
  - Seriennummer
  - Aktuelle UEFI- und Firmwareversionen des Systems
  - Weitere relevante Informationen wie Fehlernachrichten und Protokolle
- Rufen Sie die Seite http://www.ibm.com/support/entry/portal/Open_service_request auf, um eine ESR (Electronic Service Request) zu senden. Wenn Sie eine ESR senden, beginnt der Lösungsfindungsprozess für Ihr Problem, indem die relevanten Informationen der IBM Unterstützung schnell und ef-

fizient zur Verfügung gestellt werden. Die IBM Kundendiensttechniker können mit der Lösungssuche beginnen, sobald Sie eine ESR ausgefüllt und gesendet haben.

Sie können viele Probleme ohne Unterstützung beheben, indem Sie die Prozeduren zur Fehlerbehebung durchführen, die IBM in der Onlinehilfefunktion oder in der Dokumentation beschreibt, die mit Ihrem IBM Produkt geliefert werden. Die Dokumentation zu IBM Systemen enthält zudem Beschreibungen von Diagnosetests, die Sie durchführen können. Im Lieferumfang der meisten Systeme, Betriebssysteme und Programme ist Dokumentation enthalten, die Prozeduren zur Fehlerbehebung und Erläuterungen zu Fehlernachrichten und -codes umfasst. Wenn Sie ein Softwareproblem vermuten, finden Sie Informationen in der Dokumentation zum Betriebssystem oder Programm.

Dokumentation verwenden

Informationen zu Ihrem IBM System und, falls vorhanden, zu vorinstallierter Software sowie zu Zusatzeinrichtungen finden Sie in der mit dem Produkt gelieferten Dokumentation. Zu dieser Dokumentation können gedruckte Dokumente, Onlinedokumente, Readme-Dateien und Hilfedateien gehören.

Anweisungen zur Verwendung der Diagnoseprogramme finden Sie in den Fehlerbehebungsinformationen in Ihrer Systemdokumentation. Über die Fehlerbehebungsinformationen oder die Diagnoseprogramme erfahren Sie möglicherweise, dass Sie zusätzliche oder aktuelle Einheitentreiber oder andere Software benötigen. IBM verwaltet Homepages im World Wide Web, über die Sie die neuesten technischen Informationen suchen und Einheitentreiber und Aktualisierungen herunterladen können. Auf diese Seiten können Sie unter folgender Adresse zugreifen: http://www.ibm.com/supportportal.

Über das World Wide Web Hilfe und Informationen anfordern

Aktuelle Informationen zu IBM Produkten und Unterstützung finden Sie im World Wide Web.

Im World Wide Web finden Sie unter http://www.ibm.com/supportportal aktuelle Informationen zu IBM Systemen, Zusatzeinrichtungen, Services und Unterstützung. Informationen zu IBM System x finden Sie unter http://www.ibm.com/systems/x. Informationen zu IBM BladeCenter finden Sie unter http://www.ibm.com/systems/bladecenter. Informationen zu IBM IntelliStation finden Sie unter http://www.ibm.com/systems/intellistation.

Vorgehensweise zum Senden von DSA-Daten an IBM

Verwenden Sie das IBM Enhanced Customer Data Repository, um Diagnosedaten an IBM zu senden.

Lesen Sie vor dem Senden von Diagnosedaten an IBM die Nutzungsbedingungen unter http://www.ibm.com/de/support/ecurep/terms.html.

Diagnosedaten können Sie mit einer der folgenden Methoden an IBM senden:

- **Standardupload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standardupload mit der Seriennummer des Systems:** http://www.ecurep.ibm.com/app/upload_hw

- **Sicherer Upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Sicherer Upload mit der Seriennummer des Systems:** https://www.ecurep.ibm.com/app/upload_hw

Individuell gestaltete Unterstützungswebseite erstellen

Sie können eine individuell gestaltete Unterstützungswebseite erstellen, indem Sie IBM Produkte angeben, die Sie interessieren.

Wenn Sie eine individuell gestaltete Unterstützungswebseite erstellen möchten, rufen Sie folgende Adresse auf: http://www.ibm.com/support/mynotifications. Über diese individuell gestaltete Seite können Sie wöchentliche E-Mail-Benachrichtigungen zu neuen technischen Dokumenten abonnieren, nach Informationen und Downloads suchen und auf verschiedene Verwaltungsservices zugreifen.

Software-Service und -unterstützung

Über die IBM Support Line erhalten Sie gegen eine Gebühr telefonische Unterstützung zur Verwendung und zur Konfiguration Ihrer IBM Produkte sowie bei Softwareproblemen mit Ihren IBM Produkten.

Informationen dazu, welche Produkte von der Support Line in Ihrem Land oder in Ihrer Region unterstützt werden, finden Sie unter http://www.ibm.com/services/supline/products.

Weitere Informationen zur Support Line und zu weiteren IBM Services finden Sie unter http://www.ibm.com/services. Eine Liste der Unterstützungstelefonnummern finden Sie unter http://www.ibm.com/planetwide. In den USA und Kanada können Sie unter 1-800-IBM-SERV (1-800-426-7378) anrufen.

Hardware-Service und -unterstützung

Hardware-Service können Sie vom IBM Kundendienst oder von Ihrem IBM Reseller erhalten.

Reseller, die von IBM zum Erbringen des Herstellerservice berechtigt sind, finden Sie unter http://www.ibm.com/partnerworld. Klicken Sie dort auf der rechten Seite auf **Find Business Partners**. Telefonnummern für den IBM Support finden Sie unter http://www.ibm.com/planetwide. In den USA und Kanada können Sie uns unter 1-800-IBM-SERV (1-800-426-7378) anrufen.

In den USA und in Kanada sind der Hardware-Service und die Unterstützung rund um die Uhr an allen sieben Wochentagen verfügbar. In Großbritannien sind diese Serviceleistungen von Montag bis Freitag von 9.00 bis 18.00 Uhr verfügbar.

IBM Produktservice in Taiwan

Anhand dieser Informationen können Sie sich an den IBM Produktservice in Taiwan wenden.

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

Kontaktinformationen für den IBM Produktservice in Taiwan:

IBM Taiwan Corporation3F, No 7, Song Ren Rd.Taipei, Taiwan
Telefon: 0800-016-888

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für die in diesem Handbuch beschriebenen Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Dokumentation ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes 2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Marken

IBM, das IBM Logo und ibm.com sind eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein.

Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite http://www.ibm.com/legal/us/en/copytrade.shtml.

Adobe und PostScript sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Cell Broadband Engine wird unter Lizenz verwendet und ist eine Marke der Sony Computer Entertainment, Inc. in den USA und/oder anderen Ländern.

Intel, Intel Xeon, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder deren Tochtergesellschaften in den USA und anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows und Windows NT sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Wichtige Anmerkungen

Die Prozessorgeschwindigkeit bezieht sich auf die interne Taktgeschwindigkeit des Mikroprozessors. Das Leistungsverhalten der Anwendung ist außerdem von anderen Faktoren abhängig.

Die Geschwindigkeit von CD- oder DVD-Laufwerken wird als die variable Lesegeschwindigkeit angegeben. Die tatsächlichen Geschwindigkeiten können davon abweichen und liegen oft unter diesem Höchstwert.

Bei Angaben in Bezug auf Hauptspeicher, realen/virtuellen Speicher oder Kanalvolumen steht die Abkürzung KB für 1.024 Bytes, MB für 1.048.576 Bytes und GB für 1.073.741.824 Bytes.

Bei Angaben zur Kapazität von Festplattenlaufwerken oder zu Übertragungsgeschwindigkeiten steht MB für 1.000.000 Bytes und GB für 1.000.000.000 Bytes. Die gesamte für den Benutzer verfügbare Speicherkapazität kann je nach Betriebsumgebung variieren.

Die maximale Kapazität von internen Festplattenlaufwerken geht vom Austausch aller Standardfestplattenlaufwerke und der Belegung aller Festplattenlaufwerkpositionen mit den größten derzeit unterstützten Laufwerken aus, die IBM zur Verfügung stellt.

Zum Erreichen der maximalen Speicherkapazität muss der Standardspeicher möglicherweise durch ein optionales Speichermodul ersetzt werden.

Jede Halbleiterspeicherzelle verfügt über eine intrinsische, endliche Zahl von Schreibzyklen, welche die Zelle ausführen kann. Daher kann eine Solid-State-Einheit nur eine begrenzte Anzahl an Schreibzyklen durchlaufen. Diese ist in „Total Bytes Written" (TBW) angegeben. Eine Einheit, bei der diese Grenze überschritten wurde, reagiert möglicherweise nicht mehr auf vom System generierte Befehle oder kann nicht mehr für Schreibvorgänge verwendet werden.

IBM ist nicht für den Austausch einer Einheit verantwortlich, deren maximale Anzahl zugesicherter Programmierungs-/Löschzyklen überschritten wurde, wie in der offiziell veröffentlichten Spezifikation für diese Einheit dokumentiert.

IBM enthält sich jeder Äußerung in Bezug auf ServerProven-Produkte und -Services anderer Unternehmen und übernimmt für diese keinerlei Gewährleistung. Dies gilt unter anderem für die Gewährleistung der Gebrauchstauglichkeit und der Eignung für einen bestimmten Zweck. Für den Vertrieb dieser Produkte sowie entsprechende Gewährleistungen sind ausschließlich die entsprechenden Fremdanbieter zuständig.

IBM übernimmt keine Verantwortung oder Gewährleistungen bezüglich der Produkte anderer Hersteller. Eine eventuelle Unterstützung für Produkte anderer Hersteller erfolgt durch Drittanbieter, nicht durch IBM.

Manche Software unterscheidet sich möglicherweise von der im Einzelhandel erhältlichen Version (falls verfügbar) und enthält möglicherweise keine Benutzerhandbücher bzw. nicht alle Programmfunktionen.

Verunreinigung durch Staubpartikel

Achtung: Staubpartikel in der Luft (beispielsweise Metallsplitter oder andere Teilchen) und reaktionsfreudige Gase, die alleine oder in Kombination mit anderen Umgebungsfaktoren, wie Luftfeuchtigkeit oder Temperatur, auftreten, können für die in diesem Dokument beschriebene Einheit ein Risiko darstellen.

Zu den Risiken, die aufgrund einer vermehrten Staubbelastung oder einer erhöhten Konzentration gefährlicher Gase bestehen, zählen Beschädigungen, die zu einer Störung oder sogar zum Totalausfall der Einheit führen. Durch die in dieser Spezifikation festgelegten Grenzwerte für Staubpartikel und Gase sollen solche Beschädigungen vermieden werden. Diese Grenzwerte sind nicht als unveränderliche Grenzwerte zu betrachten oder zu verwenden, da viele andere Faktoren, wie z. B. die Temperatur oder der Feuchtigkeitsgehalt der Luft, die Auswirkungen von Staubpartikeln oder korrosionsfördernden Stoffen in der Umgebung sowie die Verbreitung gasförmiger Verunreinigungen beeinflussen können. Sollte ein bestimmter Grenzwert in diesem Dokument fehlen, müssen Sie versuchen, die Verunreinigung durch Staubpartikel und Gase so gering zu halten, dass die Gesundheit und die Sicherheit der beteiligten Personen dadurch nicht gefährdet sind. Wenn IBM feststellt, dass die Einheit aufgrund einer erhöhten Konzentration von Staubpartikeln oder Gasen in Ihrer Umgebung beschädigt wurde, kann IBM die Reparatur oder den Austausch von Einheiten oder Teilen unter der Bedingung durchführen, dass geeignete Maßnahmen zur Minimierung solcher Verunreinigungen in der Umgebung der Einheit ergriffen werden. Die Durchführung dieser Maßnahmen obliegt dem Kunden.

Tabelle 7. Grenzwerte für Staubpartikel und Gase

Verunreinigung	Grenzwerte
Staubpartikel	• Die Raumluft muss kontinuierlich mit einem Wirkungsgrad von 40 % gegenüber atmosphärischem Staub (MERV 9) nach ASHRAE-Norm 52.2[1] gefiltert werden. • Die Luft in einem Rechenzentrum muss mit einem Wirkungsgrad von mindestens 99,97 % mit HEPA-Filtern (HEPA - High Efficiency Particulate Air) gefiltert werden, die gemäß MIL-STD-282 getestet wurden. • Die relative hygroskopische Feuchtigkeit muss bei Verunreinigung durch Staubpartikel mehr als 60 % betragen[2]. • Im Raum dürfen keine elektrisch leitenden Verunreinigungen wie Zink-Whisker vorhanden sein.
Gase	• Kupfer: Klasse G1 gemäß ANSI/ISA 71.04-1985[3] • Silber: Korrosionsrate von weniger als 300 Å in 30 Tagen

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] Die relative hygroskopische Feuchtigkeit der Verunreinigung durch Staubpartikel ist die relative Feuchtigkeit, bei der der Staub genug Wasser absorbiert, um nass zu werden und Ionen leiten zu können.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Dokumentationsformat

Die Veröffentlichungen für dieses Produkt liegen im PDF-Format vor und entsprechen den handelsüblichen Zugriffsstandards. Falls beim Verwenden der PDF-Dateien Probleme auftreten und Sie ein webbasiertes Format oder ein zugängliches PDF-Dokument für eine Veröffentlichung anfordern möchten, senden Sie eine E-Mail an folgende Adresse:

Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

Geben Sie in der Anforderung die Teilenummer und den Titel der Veröffentlichung an.

Werden an IBM Informationen eingesandt, gewährt der Einsender IBM ein nicht ausschließliches Recht zur beliebigen Verwendung oder Verteilung dieser Informationen, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Hinweis zur Telekommunikation

Möglicherweise ist dieses Produkt in Ihrem Land nicht für den Anschluss an Schnittstellen von öffentlichen Telekommunikationsnetzen zertifiziert. Vor der Herstellung einer solchen Verbindung ist eine entsprechende Zertifizierung ggf. gesetzlich vorgeschrieben. Bei Fragen wenden Sie sich bitte an einen IBM Ansprechpartner oder Vertriebspartner.

Hinweise zur elektromagnetischen Verträglichkeit

Wenn Sie einen Bildschirm an das Gerät anschließen, müssen Sie das dazugehörige Bildschirmkabel und jede Störschutzeinheit, die im Lieferumfang des Bildschirms enthalten ist, verwenden.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Deutschland - Hinweis zur Klasse A

Deutschsprachiger EU-Hinweis: Hinweis für Geräte der Klasse A, EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 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 IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: „Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen 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 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) 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
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Deutschland
Telefon: +49 7032 15 2941
E-Mail: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Class A statement

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

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Korea Communications Commission (KCC) statement

이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для
снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

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。

Taiwan Class A compliance statement

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。

Index

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

Teilenummer: 00Y8002

(1P) P/N: 00Y8002