

Integriertes Managementmodul II Benutzerhandbuch



Integriertes Managementmodul II Benutzerhandbuch

#### Dritte Ausgabe (Juli 2013)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs *IBM Integrated Management Module II, User's Guide,* IBM Teilenummer 47C9203, herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2013

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 Juli 2013

## Inhaltsverzeichnis

Tabellen	vii
Kapitel 1. Einführung         Funktionen von "IMM2 Basic Level", "IMM2 Stan- dard Level" und "IMM2 Advanced Level"         Gard Level" und "IMM2 Basic Level"         Funktionen von "IMM2 Advanced Level"         Funktionen von "IMM2 Advanced Level"         Funktionsverbesserungen beim IMM2         Upgrade für IMM2 durchführen         IMM2 zusammen mit dem erweiterten BladeCenter-	<b>1</b> . 2 . 3 . 3 . 3 . 3 . 4
Managementmodul verwenden	.4 4 .5
Kapitel 2. IMM2-Webschnittstelle öffnen	_
Zugriff auf die IMM2-Webschnittstelle. IMM2-Netzverbindung mit dem Konfigurations- dienstprogramm der Server-Firmware für IBM	. 7
System x einrichten	. 8
Am IMM2 anmelden	10
Beschreibungen der IMM2-Aktionen	11
Kapitel 3. Übersicht über die IMM2- Webbenutzerschnittstelle	17
Websitzungseinstellungen	17
Page Auto Refresh	17
Trespass Message	19
Abmelden	20
Registerkarte "Events" (Freignisse)	$\frac{21}{27}$
Event Log (Ereignisprotokoll)	27
Event Recipients (Ereignisempfänger).	30
Registerkarte "Service and Support"	32
Download Service Data (Servicedaten herunterla-	
den)	32
Registerkarte "Server Management" (Serververwal-	
$\operatorname{tung})  \cdot  \cdot  \cdot  \cdot  \cdot  \cdot  \cdot  \cdot  \cdot  $	33
Server Firmware (Server-Firmware)	34
Server Properties (Servereigenschaften)	39 44
Server Power Actions (Serverstromyersorgungs-	-1-1
aktionen)	49
Disks (Platten)	49
Memory (Speicher)	50
Processors (Prozessoren)	51
Server Timeouts (Serverzeitlimits)	52
PXE Network Boot (PXE-Netzboot)	52
Latest OS Failure Screen (Letzte Betriebssystem-	
Fehleranzeige)	53
Kegisterkarte "IMM Management" (IMM-Verwal- tung)	53

Kapitel 4. IMM2 konfigurieren	55
Serverzeitlimits festlegen	. 58
Datum und Uhrzeit für IMM2 einstellen Finstellungen für den seriellen Anschluss konfigu-	. 60
rieren	62
Benutzerkonten konfigurieren	. 02 63
Benutzerkonten	. 05
	. 64
Gruppenprome	. 66
Globale Anmeldeeinstellungen konfigurieren	. 6/
Allgemeine Einstellungen.	. 67
Einstellungen für die Kontensicherheitsrichtlinie	69
Netzprotokolle konfigurieren	. 72
Ethernet-Einstellungen konfigurieren	. 72
Einstellungen für SNMP-Alerts konfigurieren .	. 74
DNS konfigurieren	. 76
DDNS konfigurieren	. 77
SMTP konfigurieren	. 77
LDAP konfigurieren	. 78
Telnet konfigurieren	. 84
USB konfigurieren	. 84
Portzuordnungen konfigurieren	. 85
Sicherheitseinstellungen konfigurieren	. 86
HTTPS-Protokoll konfigurieren	. 87
CIM-over-HTTPS-Protokoll konfigurieren	88
Protokoll für IDAP-Client konfigurieren	. 00 89
Souro Shall Sorver konfigurieren	. 0) 01
Übersicht über SCI	. 71
	. 92
Handhabung von SSL-Zertifikaten.	. 92
Verwaltung von SSL-Zertifikaten	. 93
IMM-Konfiguration wiederherstellen und andern.	. 94
IMM2 erneut starten	. 94
IMM2 auf die werkseitigen Voreinstellungen zurück-	-
setzen	. 95
Aktivierungsschlüsselverwaltung	. 96
	~ 7
Kapitel 5. Serverstatus uberwachen	97
Systemstatus anzeigen	. 97
Systeminformationen anzeigen	. 99
Serverzustand anzeigen	100
Hardwarezustand anzeigen.	101
-	
Kapitel 6. IMM2-Tasks ausführen 1	05
Stromyarsorgungsstatus des Sarvars stauern	106
Remote Presence, und Fernsteuerungsfunktionen	107
MM2 Firmware und Java adar Actival Applet	107
Inniviz-Fillinwale und Java- odel ActiveA-Applet	100
aktualisieren.	100
Remote-Presence-Funktion aktivieren	109
Anzeigenerfassung per Fernsteuerung	109
Modi der Fernsteuerung im Video Viewer	110
Fernsteuerung des Videofarbmodus	110
Tastaturunterstützung per Fernsteuerung	111
Mausunterstützung per Fernsteuerung	113
Fernsteuerung der Stromversorgung	115
Leistungsstatistiken anzeigen	115
Remote Desktop Protocol starten	115

0 1	115
Ferner Datenträger	119
PXE-Netzboot einrichten	121
Server-Firmware aktualisieren	122
Systemereignisse verwalten	127
Freignisprotokoll verwalten	127
Benachrichtigung zu Systemereignissen	12/
Informationen für Service und Support erfassen	135
Daten der letzten Betriebssystem-Fehleranzeige	100 ar-
facen	136
Serverstromversorging verwalten	137
Stromuercorgung und gecomte Stromuercorg	107
dos Systems steuern	128
Altuell installierte Netzteile anzeigen	130
Stromyorsorgungskapagität angeigen	1 <del>4</del> 0 1 <i>1</i> 1
Varlaufenretakell zum Stremuschnungh	1 <del>4</del> 1
verlaufsprotokoli zum Stromverbrauch.	142
Kanital 7. Factures on Demond	140
Kapitel 7. Features on Demand	. 143
Aktivierungsschlüssel installieren	143
Aktivierungsschlüssel entfernen	146
Aktivierungsschlüssel exportieren	147
Kapitel 8. Befehlszeilenschnittstelle	149
IMM2 mit IPMI verwalten	149
IPMItool verwenden	149
Zugriff auf die Befehlszeilenschnittstelle	149
Anmeldung an der Befehlszeilensitzung	150
Seriell-zu-Telnet- oder -SSH-Umleitung konfigur	ie-
ren	150
Befehlssyntax	150
Merkmale und Einschränkungen	151
Alphabetische Befehlsliste	151
Alphabetische Befehlsliste	151
Alphabetische Befehlsliste	151 152 153 154
Alphabetische Befehlsliste	151 152 153 154 154
Alphabetische Befehlsliste	151 152 153 154 154 154
Alphabetische Befehlsliste	151 152 153 154 154 154 154
Alphabetische Befehlsliste	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155
Alphabetische Befehlsliste	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 159 159 159 160 160
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 159 159 160 eu- 161
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 159 160 161 161
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 159 160 161 161 161
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 159 160 161 162 162
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 159 160 161 162 162 162
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 159 160 161 162 162 162 162
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 160 161 162 162 162 162
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 160 161 162 162 162 162 163
Alphabetische Befehlsliste	151 152 153 154 154 154 154 154 154 155 155 156 158 159 159 160 161 162 162 162 163 163 165
Alphabetische Befehlsliste	<ul> <li>. 161</li> <li>. 152</li> <li>. 153</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 155</li> <li>. 155</li> <li>. 156</li> <li>. 158</li> <li>. 159</li> <li>. 159</li> <li>. 160</li> <li>. 161</li> <li>. 162</li> <li>. 163</li> <li>. 165</li> <li>. 166</li> </ul>
Alphabetische Befehlsliste	<ul> <li>. 161</li> <li>. 152</li> <li>. 153</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 155</li> <li>. 155</li> <li>. 156</li> <li>. 158</li> <li>. 159</li> <li>. 159</li> <li>. 160</li> <li>. 161</li> <li>. 162</li> <li>. 163</li> <li>. 165</li> <li>. 166</li> <li>. 169</li> </ul>
Alphabetische Befehlsliste	<ul> <li>. 161</li> <li>. 152</li> <li>. 153</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 154</li> <li>. 155</li> <li>. 155</li> <li>. 156</li> <li>. 158</li> <li>. 159</li> <li>. 159</li> <li>. 160</li> <li>. 161</li> <li>. 162</li> <li>. 163</li> <li>. 165</li> <li>. 166</li> <li>. 169</li> <li>. 170</li> </ul>

	Befehl	"dns" .										171
	Befehl	"ethtous	<b>)</b> "	•								173
	Befehl	"gprofile							•	•		173
	Befehl	"ifconfig'	'			•			•	•		174
	Befehl	"keycfg"				•	•		•	•		176
	Befehl	"ldap"				•			•	•	•	177
	Befehl	"ntp" .				•			•	•	•	179
	Befehl	"passwoi	dc	fg"					•	•	•	180
	Befehl	"ports"					•		•	•	•	181
	Befehl	"portcfg"					•		•	•		182
	Befehl	"restore"					•		•	•		183
	Befehl	"restored	efa	ult	s"							184
	Befehl	"set" .										184
	Befehl	"smtp"										184
	Befehl	"snmp"										185
	Befehl	"snmpale	erts	;"								187
	Befehl	"srcfg"										189
	Befehl	"sshcfg"										190
	Befehl	"ssl" .										191
	Befehl	"sslcfg"										192
	Befehl	"telnetcfg	5"									195
	Befehl	"thermal	ii ii									196
	Befehl	"timeout	s"									196
	Befehl	"usbeth"										197
	Befehl	"users"										197
IM	IM2-Ste	uerbefeh	le									202
	Befehl	"alertent	ries	5"								202
	Befehl	"batch"										205
	Befehl	"clearcfg"										206
	Befehl	"clock"										206
	Befehl	"identify										207
	Befehl	"info".										207
	Befehl	"resetsp"										208
	Befehl	"spreset"										208
		I										

### Anhang A. Hilfe und technische Unter-

stützung anfordern	209
Bevor Sie sich an den Kundendienst wenden.	. 209
Dokumentation verwenden.	. 210
Hilfe und Informationen über das World Wide Wel	b
anfordern	. 210
Vorgehensweise zum Senden von DSA-Daten an	
IBM	. 210
Personalisierte Unterstützungswebseite erstellen	211
Software-Service und -unterstützung	. 211
Hardware-Service und -unterstützung	. 211
IBM Produktservice in Taiwan	. 212
Anhang B. Bemerkungen	213
Anhang B. Bemerkungen	<b>213</b> . 213
Anhang B. Bemerkungen	<b>213</b> . 213 . 214
Anhang B. Bemerkungen	<b>213</b> . 213 . 214 . 215
Anhang B. Bemerkungen	<b>213</b> . 213 . 214 . 215 . 216
Anhang B. Bemerkungen	<b>213</b> . 213 . 214 . 215 . 216 . 217
Anhang B. Bemerkungen	<b>213</b> . 213 . 214 . 215 . 216 . 217 217
Anhang B. Bemerkungen	<b>213</b> . 213 . 214 . 215 . 216 . 217 217
Anhang B. Bemerkungen	<b>213</b> . 213 . 214 . 215 . 216 . 217 217 . 217
Anhang B. Bemerkungen	<b>213</b> 213 214 215 216 217 217 217

Avis de conformité à la réglementation	
d'Industrie Canada	. 217
Australia and New Zealand Class A statement	217
European Union EMC Directive conformance	
statement	. 217
Deutschland - Hinweis zur Klasse A	. 218
Japan VCCI Class A statement	. 219
Korea Communications Commission (KCC)	
statement	. 219

Russia Electromagnetic Interference (EMI) Class	
A statement	219
People's Republic of China Class A electronic	
emission statement	220
Taiwan Class A compliance statement	220
Index	221

## Tabellen

1.	IMM2-Aktionen	11
2.	Stromversorgungsstatus und Betriebsstatus des	
	Servers	24
3.	Werte für Sicherheitseinstellungsrichtlinie	69
4.	Berechtigungsbits	82
5.	Systemstatusbeschreibungen	98

6.	Stromversorgungsaktionen und Beschreibun-	
	gen	106
7.	ASU-Befehle	166
8.	Transaktionsbefehle	169
9.	Grenzwerte für Staubpartikel und Gase	216

## Kapitel 1. Einführung

Beim Serviceprozessor "Integrated Management Module II" (IMM2) handelt es sich um die zweite Generation des Serviceprozessors "Integrated Management Module" (IMM), bei dem die Serviceprozessor-Funktionalität sowie die Super E/A-, die Videocontroller- und die Remote-Presence-Funktion auf einem einzigen Chip auf der Systemplatine vereint sind. Wie schon das IMM bietet das IMM2 einige Verbesserungen gegenüber den kombinierten Funktionalitäten des Baseboard Management Controller (BMC) und des Remote Supervisor Adapter II, darunter die folgenden Funktionen:

- Auswahl zwischen einer dedizierten oder einer gemeinsam genutzten Ethernet-Verbindung für das Systemmanagement.
- Eine gemeinsame IP-Adresse für IPMI (Intelligent Platform Management Interface) und die Serviceprozessorschnittstelle. Diese Funktion ist nicht auf Blade-Servern von IBM<sup>®</sup> BladeCenter ausführbar.
- Embedded Dynamic System Analysis (DSA).
- Ferne Konfiguration mit dem Dienstprogramm f
  ür erweiterte Einstellungen (Advanced Settings Utility - ASU). Diese Funktion ist nicht auf Blade-Servern von IBM BladeCenter ausf
  ührbar.
- Die Möglichkeit für Anwendungen und Tools, zwischen Inband- oder Außerbandzugriff auf das IMM2 zu wählen. Auf Blade-Servern von IBM BladeCenter wird nur die Inbandverbindung zum IMM2 unterstützt.
- Erweiterte Remote-Presence-Funktion. Diese Funktion ist nicht auf Blade-Servern von IBM BladeCenter ausführbar.

#### Anmerkungen:

- Auf Blade-Servern von IBM BladeCenter und auf manchen System x-Servern ist kein dedizierter Systemmanagement-Netzanschluss verfügbar; für diese Server steht lediglich die Einstellung *shared* (gemeinsam genutzt) zur Verfügung.
- Bei Blade-Servern von IBM BladeCenter ist das erweiterte Managementmodul von IBM BladeCenter das primäre Managementmodul für Systemmanagementfunktionen und für KVM-Multiplexing (Keyboard/Video/Mouse - Tastatur/ Bildschirm/Maus).

Die IBM System x<sup>®</sup> Server-Firmware ist die IBM Implementierung der UEFI (Unified Extensible Firmware Interface). Es ersetzt bei Servern von IBM System x und in Blade-Servern von IBM BladeCenter das BIOS (Basic Input/Output System). Das BIOS war der Standardfirmwarecode, der die grundlegenden Hardwareoperationen, wie z. B. Interaktionen mit Diskettenlaufwerken, Festplattenlaufwerken und der Tastatur, steuerte. Die Server-Firmware von IBM System x bietet mehrere zusätzliche Funktionen, die im BIOS nicht zur Verfügung stehen, einschließlich Kompatibilität mit UEFI 2.3, iSCSI-Kompatibilität, Active Energy Manager-Technologie und erweiterter Zuverlässigkeits- und Servicekompetenzen. Das Konfigurationsdienstprogramm bietet Serverinformationen, Serverkonfiguration und Anpassungskompatibilität sowie die Möglichkeit, die Bootreihenfolge festzulegen.

#### Anmerkungen:

• In diesem Dokument wird die Server-Firmware von IBM System x oft als "Server-Firmware" und gelegentlich als "UEFI" bezeichnet.

- Die Server-Firmware von IBM System x ist mit Betriebssystemen ohne UEFI vollständig kompatibel.
- Weitere Informationen zur Verwendung der Server-Firmware von IBM System x finden Sie in der Dokumentation, die mit Ihrem IBM Server geliefert wurde.

In diesem Dokument wird erläutert, wie die Funktionen des IMM2 in einem IBM Server verwendet werden. Das IMM2 stellt mithilfe der Server-Firmware von IBM System x Systemverwaltungsfunktionen für System x, BladeCenter und IBM Flex System bereit.

Gehen Sie wie folgt vor, um zu prüfen, ob Firmwareaktualisierungen verfügbar sind.

Anmerkung: Beim ersten Zugriff auf das IBM Support Portal müssen Sie die Produktkategorie, die Produktfamilie und die Modellnummern Ihrer Speichersubsysteme auswählen. Wenn Sie das nächste Mal auf das IBM Support Portal zugreifen, werden die Produkte, die Sie beim ersten Mal ausgewählt haben, von der Website erneut geladen, sodass nur die Links für Ihre Produkte angezeigt werden. Um Ihre Produktliste zu ändern oder Elemente zu ihr hinzuzufügen, klicken Sie auf den Link Manage my product lists (Meine Produktlisten verwalten).

Die IBM Website wird in regelmäßigen Abständen aktualisiert. Die Vorgehensweisen zum Bestimmen der Firmware und der Dokumentation weicht möglicherweise geringfügig von den Beschreibungen im vorliegenden Dokument ab.

- 1. Wechseln Sie zu http://www.ibm.com/support/entry/portal.
- 2. Wählen Sie unter **Choose your products** (Produkt auswählen) die Option **Browse for a product** (Nach Produkt suchen) aus und erweitern Sie **Hardware**.
- Klicken Sie je nach Servertyp auf Systems > System x oder auf Systems > BladeCenter und wählen Sie das Feld für Ihre(n) Server aus.
- 4. Klicken Sie unter Choose your task (Task auswählen) auf Downloads.
- 5. Klicken Sie unter See your results (Ergebnisse anzeigen) auf View your page (Ihre Seite anzeigen).
- 6. Klicken Sie im Feld "Flashes & Alerts" auf den Link für den betreffenden Download oder klicken Sie auf **More results**, um weitere Links anzuzeigen.

# Funktionen von "IMM2 Basic Level", "IMM2 Standard Level" und "IMM2 Advanced Level"

Zusammen mit dem IMM2 werden die Funktionalitätsebenen "Basic Level", "Standard Level" und "Advanced Level" angeboten. Weitere Informationen zu der auf Ihrem IBM-Server installierten IMM2-Version finden Sie in der Dokumentation für Ihren Server. Alle Versionen bieten folgende Funktionen:

- · Fernzugriff und Fernverwaltung Ihres Servers rund um die Uhr
- Fernverwaltung unabhängig vom Status des verwalteten Servers
- Fernsteuerung der Hardware und der Betriebssysteme

Zusätzlich unterstützen die Versionen "Standard Level" und "Advanced Level" die webbasierte Verwaltung mit Standard-Web-Browsern.

**Anmerkung:** Manche Funktionen gelten möglicherweise nicht für IBM BladeCenter-Blade-Server.

Im Folgenden sind die allgemeinen Funktionen des IMM2 aufgeführt:

### Funktionen von "IMM2 Basic Level"

Im Folgenden sind die Funktionen vom Typ "IMM2 Basic Level" aufgeführt:

- IPMI 2.0 Interface (IPMI-2.0-Schnittstelle)
- Thermal Monitoring (Temperaturüberwachung)
- Fan Control (Lüftersteuerung)
- LED Management (Anzeigenverwaltung)
- Server Power/Reset Control (Steuerung von Einschalten/Zurücksetzen des Servers)
- Sensor Monitoring (Sensorüberwachung)
- IPMI Platform Event Trap Alerting (Trap-Alerts für IPMI-Plattformereignisse)
- IPMI Serial over LAN

#### Funktionen von "IMM2 Standard Level"

Im Folgenden finden sind die Funktionen von "IMM2 Standard Level" aufgeführt:

- Alle Funktionen von "IMM2 Basic Level"
- Webbasierte Verwaltung mithilfe von Standard-Web-Browsern
- SNMPv1- und SNMPv3-Schnittstellen
- Telnet- und SSH-Befehlszeilenschnittstelle (CLI)
- Zeitgesteuertes Ein-/Ausschalten und Neustarten des Servers
- Ereignisse in Klarschrift und Prüfprotokollaufzeichnung
- Anzeige des Systemzustands
- Betriebssystemladeprogramm- und Betriebssystem-Watchdogs
- LDAP-Authentifizierung und -Berechtigung
- Meldung von Alertausgaben in Form von SNMP-Trap, E-Mail, syslog und CIM
- NTP-Taktgebersynchronisation
- Serielle Konsolenumleitung über Telnet/SSH

#### Funktionen von "IMM2 Advanced Level"

Im Folgenden sind die Funktionen für "IMM2 Advanced Level" aufgeführt:

- Alle Funktionen von "IMM2 Basic Level" und "IMM2 Standard Level"
- Remote Presence-Java- und ActivX-Clients:
  - Remote Keyboard, Video, and Mouse Support (Unterstützung für ferne Tastatur, Anzeige und Maus)
  - Remote Media (Ferne Datenträger)
  - Remote Disk on Card (Ferne Kartendatenträger)
- Failure Screen Capture for Operating System hangs (Fehleranzeigenerfassung für Betriebssystemblockierungen)

#### Funktionsverbesserungen beim IMM2

Im Folgenden sind die im Vergleich zu den IMM-Funktionen verbesserten IMM2-Funktionen aufgeführt:

- Sicherheit (vertrauenswürdiger Serviceprozessor):
  - Sicheres Booten
  - Signierte Aktualisierungen
  - IMM2-Core-Root zur Überprüfung der Vertrauenswürdigkeit
  - TPM (Trusted Platform Module)

- Neues, bei IBM System x konsistentes Web-GUI-Design
- · Verbesserte Remote-Presence-Bildschirmauflösung und -Farbpalette
- Remote-Presence-Client von ActiveX
- Auf USB 2.0 aktualisierte Ethernet-over-USB-Schnittstelle
- Syslog-Alertausgabe
- Nach Konfigurationsänderungen kein Zurücksetzen des IMM2 erforderlich

#### Upgrade für IMM2 durchführen

Wenn Ihr IBM Server über die IMM2-Firmwarefunktion der Stufe "Basic Level" oder "Standard Level" verfügt, können Sie möglicherweise ein Upgrade für die IMM2-Funktionen auf Ihrem Server durchführen. Weitere Informationen zu den verfügbaren Upgradestufen und wie Sie sie bestellen können, finden Sie in Kapitel 7, "Features on Demand", auf Seite 143.

# IMM2 zusammen mit dem erweiterten BladeCenter-Managementmodul verwenden

Das erweiterte BladeCenter-Managementmodul ist die Systemmanagement-Standardschnittstelle für IBM BladeCenter-Produkte. Obwohl das IMM2 nun in einigen IBM Blade-Servern enthalten ist, bleibt das erweiterte Managementmodul das Managementmodul für Systemmanagementfunktionen und KVM-Multiplexing (Keyboard/Video/Mouse - Tastatur/Bildschirm/Maus) für IBM BladeCenter-Produkte einschließlich IBM Blade-Server.

Auf IBM BladeCenter-Blade-Servern gibt es keinen externen Netzzugriff auf das IMM2 und zur fernen Verwaltung von Blade-Servern von IBM BladeCenter muss das erweiterte Managementmodul verwendet werden. Das IMM2 ersetzt die Funktionalität des BMC und der cKVM-Erweiterungskarte (cKVM - Concurrent Keyboard, Video and Mouse) in früheren IBM Blade-Server-Produkten.

#### Voraussetzungen - Web-Browser und Betriebssystem

Für die IMM2-Webschnittstelle sind das Java<sup>™</sup>-Plug-in ab Version 1.5 (für die Remote-Presence-Funktion) und einer der folgenden Web-Browser erforderlich:

- Microsoft Internet Explorer Version 7 oder 8
- Mozilla Firefox ab Version 3.5

Wenn Sie neuere Microsoft Internet Explorer-Versionen verwenden, wird empfohlen, dass Sie die Kompatibilitätsansicht im Internet Explorer zum Anzeigen der IMM2-Webseiten verwenden. Die oben aufgelisteten Browser stellen die aktuell von der IMM2-Firmware unterstützen Browser dar. Die IMM2-Firmware kann in regelmäßigen Abständen erweitert werden, um Unterstützung für andere Browser bereitzustellen. Die Liste der Browser, die von der aktuell auf dem System ausgeführten IMM2-Firmwareversion unterstützt werden, finden Sie in der Liste "Supported Browsers" (Unterstützte Browser) auf der IMM2-Anmeldeseite. In der folgenden Abbildung ist die IMM2-Anmeldeanzeige dargestellt.

Integrated Management Module	
Note: To ensure security and avoid login conflicts, always end your session using the 'Log out' option in the upper right area of the web page. • Supported Browsers	
Learned Mannish. Property of DM Corp. 8: IDM Componence and dher(s) $(222,218)$ is a regulared trademark of the TBM Corporation in the United States, other countries, or both.	

Die folgenden Serverbetriebssysteme bieten USB-Unterstützung, die für die Remote-Presence-Funktion erforderlich ist:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux, Version 4.0 und 5.0
- SUSE Linux Version 10.0
- Novell NetWare 6.5

Im Zwischenspeicher Ihres Internet-Browsers werden Informationen zu Webseiten, die Sie besuchen, gespeichert, damit diese zukünftig schneller geladen werden können. Nach einer Flashaktualisierung der IMM2-Firmware verwendet Ihr Browser möglicherweise weiterhin die Informationen aus seinem Zwischenspeicher, anstatt sie aus dem IMM2 abzurufen. Nach Aktualisierung der IMM2-Firmware wird empfohlen, dass Sie den Browser-Zwischenspeicher leeren, um sicherzustellen, dass Webseiten, die durch IMM2 bereitgestellt werden, ordnungsgemäß angezeigt werden.

#### Bemerkungen in diesem Buch

In dieser Dokumentation werden die folgenden Bemerkungen verwendet:

- Anmerkung: Diese Bemerkungen enthalten wichtige Tipps, Anleitungen oder Ratschläge.
- Wichtig: Diese Bemerkungen enthalten Informationen oder Ratschläge, die Ihnen helfen, schwierige oder problematische Situationen 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.

## Kapitel 2. IMM2-Webschnittstelle öffnen und verwenden

Wichtig: Dieser Abschnitt gilt nicht für IBM BladeCenter und IBM Blade-Server. Obwohl das IMM2 in einigen IBM BladeCenter-Produkten und IBM Blade-Servern standardmäßig enthalten ist, bleibt das erweiterte IBM BladeCenter-Managementmodul das primäre Managementmodul für Systemmanagementfunktionen und KVM-Multiplexing (Keyboard/Video/Mouse - Tastatur/Bildschirm/Maus) für IBM BladeCenter-Produkte einschließlich IBM Blade-Server. Benutzer, die die IMM2-Einstellungen auf Blade-Servern konfigurieren möchten, sollten das Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility - ASU) auf dem Blade-Server zum Ausführen dieser Aktionen verwenden.

Das IMM2 kombiniert Serviceprozessorfunktionen, einen Videocontroller und eine Remote-Presence-Funktion (wenn ein optionaler Virtual Media Key installiert ist) in einem einzigen Chip. Für einen Fernzugriff auf das IMM2 mithilfe der IMM2-Webschnittstelle müssen Sie sich zuerst anmelden. In diesem Kapitel werden das Anmeldeverfahren und die Aktionen beschrieben, die Sie über die IMM2-Webschnittstelle ausführen können.

#### Zugriff auf die IMM2-Webschnittstelle

Das IMM2 unterstützt eine statische IPv4-Adressierung wie auch eine DHCP-IPv4-Adressierung. Die standardmäßig dem IMM2 zugewiesene statische IPv4-Adresse lautet 192.168.70.125. Das IMM2 ist anfangs so konfiguriert, dass es versucht, eine Adresse von einem DHCP-Server abzurufen. Ist dies nicht möglich, verwendet es die statische IPv4-Adresse.

Das IMM2 unterstützt auch IPv6, aber es verfügt standardmäßig nicht über eine festgelegte statische IPv6-IP-Adresse. Beim Erstzugriff auf das IMM2 in einer IPv6-Umgebung können Sie entweder die IPv4-IP-Adresse oder die lokale IPv6-Verbindungsadresse verwenden. Das IMM2 generiert eine eindeutige lokale IPv6-Verbindungsadresse, die in der IMM2-Webschnittstelle auf der Seite "Network Interfaces" (Netzschnittstellen) angezeigt wird. Die lokale IPv6-Verbindungsadresse weist dabei dasselbe Format auf, das im folgenden Beispiel dargestellt ist.

fe80::21a:64ff:fee6:4d5

Beim Zugriff auf das IMM2 sind die folgenden IPv6-Bedingungen als Standardwerte definiert:

- Die automatische IPv6-Adressenkonfiguration ist aktiviert.
- Die statische IPv6-IP-Adressenkonfiguration ist inaktiviert.
- DHCPv6 ist aktiviert.
- Die statusunabhängige automatische Konfiguration ist aktiviert.

Das IMM2 ermöglicht die Auswahl einer dedizierten Systemmanagement-Netzverbindung (falls vorhanden) oder einer Netzverbindung, die gemeinsam mit dem Server verwendet wird. Die Standardverbindung für in einem Gehäuserahmen installierte Server und Turmserver verwendet den dedizierten Systemmanagement-Netzanschluss. **Anmerkung:** Möglicherweise verfügt Ihr Server über keinen dedizierten Systemmanagement-Netzanschluss. Wenn auf Ihrer Hardware kein dedizierter Netzanschluss vorhanden ist, ist die Einstellung *shared* (freigegeben) die einzig verfügbare IMM2-Einstellung.

## IMM2-Netzverbindung mit dem Konfigurationsdienstprogramm der Server-Firmware für IBM System x einrichten

Nachdem Sie den Server gestartet haben, können Sie über das Konfigurationsdienstprogramm eine IMM2-Netzverbindung auswählen. Der Server mit der IMM2-Hardware muss mit einem DHCP-Server verbunden sein oder das Servernetz muss so konfiguriert sein, dass es die statische IP-Adresse des IMM2 verwendet. Gehen Sie wie folgt vor, um die IMM2-Netzverbindung über das Konfigurationsdienstprogramm herzustellen:

1. Schalten Sie den Server ein. Die Eingangsanzeige der Server-Firmware für IBM System x wird angezeigt.

**Anmerkung:** Der Netzschalter wird etwa 90 Sekunden nach dem Anschließen des Servers an die Wechselstromversorgung aktiviert.



- 2. Wenn die Aufforderung <F1> Setup (F1 für Konfiguration) angezeigt wird, drücken Sie die Taste F1. Wenn Sie sowohl ein Startkennwort als auch ein Administratorkennwort festgelegt haben, müssen Sie das Administratorkennwort eingeben, um auf das vollständige Menü des Konfigurationsdienstprogramms zugreifen zu können.
- **3**. Wählen Sie im Hauptmenü des Konfigurationsdienstprogramms **System Settings** (Systemeinstellungen) aus.
- 4. Wählen Sie in der nächsten Anzeige die Option **Integrated Management Module** aus.
- 5. Wählen Sie in der nächsten Anzeige die Option **Network Configuration** (Netzkonfiguration) aus.
- 6. Markieren Sie **DHCP Control**. Im Feld **DHCP Control** stehen drei IMM2-Netzverbindungen zur Auswahl:

- Static IP (Statisches IP)
- DHCP Enabled (DHCP aktiviert)
- DHCP with Failover (default) (DHCP mit Funktionsübernahme (Standard))

	Network Configuration	
Network Interface Port Burned-in NAC Address Hostname DHCP Control LP Address Submet Mask Default Gateway IP6 Local Link Address	<pre><dedicated> 00-1A-64-E6-11-AD DST110  Static IP DHCP Enabled DHCP with Failover <enabled> AD10::E664:1100:EAE5:11 27/64</enabled></dedicated></pre>	Set your DHCP Contro preferences.
Advanced IMM Ethernet Se	etup	
t∔=Move Highlight	4 <enter>=Complete Entry</enter>	Esc=Exit

- 7. Wählen Sie eine der Netzverbindungen aus.
- 8. Wenn Sie sich dafür entscheiden, eine statische IP-Adresse zu verwenden, müssen Sie die IP-Adresse, die Teilnetzmaske und das Standard-Gateway angeben.
- **9**. Sie können das Konfigurationsdienstprogramm auch dazu verwenden, eine dedizierte Netzverbindung (wenn Ihr Server einen dedizierten Netzanschluss hat) oder eine gemeinsam genutzte IMM2-Netzverbindung auszuwählen.

#### Anmerkungen:

- Möglicherweise verfügt Ihr Server über keinen dedizierten Systemmanagement-Netzanschluss. Wenn auf Ihrer Hardware kein dedizierter Netzanschluss vorhanden ist, ist die Einstellung *Shared* (Gemeinsam genutzt) die einzige verfügbare IMM2-Einstellung. Wählen Sie auf der Anzeige Network Configuration im Feld Network Interface Port (Netzschnittstellenport) Dedicated (dediziert) (falls zutreffend) oder Shared (gemeinsam genutzt) aus.
- Informationen dazu, wo sich auf Ihrem Server die vom IMM2 genutzten Ethernet-Anschlüsse befinden, finden Sie in der Dokumentation zum Server.
- 10. Blättern Sie abwärts und wählen Sie **Save Network Settings** (Netzeinstellungen speichern) aus.
- 11. Beenden Sie das Konfigurationsdienstprogramm.

#### Anmerkungen:

- Sie müssen etwa eine Minute warten, bis die Änderungen wirksam werden und die Server-Firmware wieder funktioniert.
- Sie können die IMM2-Netzverbindung auch über die IMM2-Webschnittstelle oder die Befehlszeilenschnittstelle konfigurieren. In der IMM2-Webschnittstelle werden die Netzverbindungen auf der Seite Network Protocol Properties (Netzprotokolleigenschaften) konfiguriert (Wählen Sie Network (Netz) im Menü IMM Management (IMM-Verwaltung) aus). In der IMM2-Befehlszeilenschnittstelle werden die Netzverbindungen mit mehreren Befehlen konfiguriert, je nach der Konfiguration Ihrer Installation.

#### Am IMM2 anmelden

Wichtig: Das IMM2 ist anfangs auf den Benutzernamen USERID und das Kennwort PASSWORD (mit einer Null anstelle des Buchstabens "O") eingestellt. Bei dieser Standard-Benutzereinstellung haben nur Administratoren Zugriff. Ändern Sie für größere Sicherheit diesen Benutzernamen und das zugehörige Kennwort bei der Erstkonfiguration.

Gehen Sie wie folgt vor, um über die IMM2-Webschnittstelle Zugriff auf das IMM2 zu erhalten:

- 1. Öffnen Sie einen Web-Browser. Geben Sie im Adress- oder URL-Feld die IP-Adresse oder den Hostnamen des IMM2 ein, mit dem Sie eine Verbindung herstellen möchten.
- 2. Geben Sie Ihren Benutzernamen und Ihr Kennwort in das Fenster "IMM2 Login" (Anmeldung am IMM2) ein. Wenn Sie das IMM2 zum ersten Mal verwenden, können Sie Ihren Benutzernamen und Ihr Kennwort von Ihrem Systemadministrator anfordern. Alle Anmeldeversuche werden im Ereignisprotokoll dokumentiert. Je nachdem, wie Ihr Systemadministrator die Benutzer-ID konfiguriert hat, müssen Sie möglicherweise ein neues Kennwort eingeben.

Das Fenster "Login" (Anmeldung) ist in der folgenden Abbildung dargestellt.



3. Klicken Sie auf **Log in** (Anmelden), um die Sitzung zu starten. Im Browser wird die Seite "System Status" (Systemstatus) geöffnet, wie in der folgenden Abbildung dargestellt. Auf dieser Seite erhalten Sie einen schnellen Überblick über den Serverstatus und eine Zusammenfassung des Serverzustands.



Beschreibungen der Aktionen, die Sie über die Registerkarten oben in der IMM2-Webschnittstelle ausführen können, finden Sie im Abschnitt "Beschreibungen der IMM2-Aktionen".

#### Beschreibungen der IMM2-Aktionen

Navigieren Sie zum Anfang des IMM2-Fensters, um mit dem IMM2 Aktivitäten durchzuführen. In der Titelleiste wird der angemeldete Benutzername angegeben. Über die Titelleiste können Sie **Settings** (Einstellungen) für die Aktualisierungsfrequenz der Statusanzeige sowie eine benutzerdefinierte Übergriffsnachricht konfigurieren und sich über die Option **Log out** (Abmeldung) von der Webschnittstelle des IMM2 abmelden. Unter der Titelleiste befinden sich Registerkarten, über die Sie Zugang zu unterschiedlichen in Tabelle 1 aufgeführten IMM2-Funktionen bekommen.



Tabelle 1. IMM2-Aktionen

Registerkarte	Auswahl	Beschreibung
System Status (Systemstatus)		Auf der Systemstatusseite können Sie Informationen zu Systemstatus, aktiven Systemereignissen und Hardwarezustand anzeigen. Sie bietet Quick Links zu den Systeminformationen, Serverstromversorgungsaktionen und Fernsteuerungsfunktionen der Registerkarte "Server Management" und ermöglicht es Ihnen, ein Bild von der Erfassung der letzten Anzeige bei einem Systemabsturz anzuzeigen. In den Abschnitten "Registerkarte "System Status"" auf Seite 21 und "Systemstatus anzeigen" auf Seite 97 finden Sie weitere Informationen.

Tabelle 1. IMM2-Aktionen (For
-------------------------------

Registerkarte	Auswahl	Beschreibung
Events (Ereignisse)	Event Log (Ereignisprotokoll)	Auf der Ereignisprotokollseite werden Einträge angezeigt, die derzeit im IMM2- Ereignisprotokoll gespeichert sind. Das Protokoll enthält eine Textbeschreibung von gemeldeten Systemereignissen, einschließlich Informationen über sämtliche Fernzugriffsversuche und Konfigurationsänderungen. Alle Ereignisse im Protokoll bekommen mithilfe der Datums- und Uhrzeiteinstellungen des IMM2 eine Zeitmarke. Manche Ereignisse lösen auch Alerts aus, wenn sie entsprechend konfi- guriert wurden. Sie können Ereignisse im Ereignisprotokoll sortieren und filtern und sie in eine Textdatei exportieren. Weitere Informationen finden Sie in den Ab- schnitten "Registerkarte "Events" (Ereignisse)" auf Seite 27 und "Ereignisprotokoll verwalten" auf Seite 127.
	Event Recipients (Er- eignis- empfänger)	Auf der Seite "Event Recipients" können Sie festlegen, wer bei Systemereignissen benachrichtigt werden soll. Sie können jeden Empfänger konfigurieren und Ein- stellungen verwalten, die für alle Ereignisempfänger gelten. Sie können außerdem ein Testereignis generieren, um zu überprüfen, ob die Benachrichtigungsfunktion funktioniert. Weitere Informationen finden Sie in den Abschnitten "Event Recipients (Ereignisempfänger)" auf Seite 30 und "Benachrichtigung zu Systemereignissen" auf Seite 129.
Service and Support (Service und Unter- stützung)	Download Service Data (Servicedaten herunterladen)	Die Seite "Download Service Data" erstellt eine komprimierte Datei mit Informatio- nen, die vom IBM Support dazu verwendet werden kann, Ihnen zu helfen. Weitere Informationen finden Sie in den Abschnitten "Download Service Data (Servicedaten herunterladen)" auf Seite 32 und "Informationen für Service und Support erfassen" auf Seite 135.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
Server Management (Serververwaltung)	Server Firmware (Server-Firmware)	Die Seite "Server Firmware" gibt Firmwareversionen an und ermöglicht es Ihnen, die IMM2-Firmware, Server-Firmware und DSA-Firmware zu aktualisieren. Weite- re Informationen finden Sie in den Abschnitten "Server Firmware (Server-Firmware)" auf Seite 34 und "Server-Firmware aktualisieren" auf Seite 122.
	Remote Control (Fern- steuerung)	Über die Seite "Remote Control" können Sie den Server auf Betriebssystemebene steuern. Sie bietet den Zugriff auf die Funktionalität für ferne Datenträger und fer- ne Konsolen. Sie können die Serverkonsole über Ihren Computer anzeigen und bedienen und eines der Plattenlaufwerke des Computers, z. B. das CD-ROM-Lauf- werk oder das Diskettenlaufwerk, an den Server anhängen. Wenn Sie einen Daten- träger angehängt haben, können Sie ihn für einen Neustart des Servers sowie für die Aktualisierung der Firmware auf dem Server verwenden. Das angehängte Laufwerk wird als an den Server angeschlossenes USB-Plattenlaufwerk angezeigt. Weitere Informationen finden Sie in den Abschnitten "Remote Control (Fernsteuerung)" auf Seite 39 und "Remote-Presence- und Fernsteuerungsfunktionen" auf Seite 107.
	Server Properties (Servereigen- schaften)	<ul> <li>Die Seite "Server Properties" ermöglicht den Zugriff auf unterschiedliche Eigenschaften, Statusbedingungen und Einstellungen Ihres Servers. Die folgenden Optionen sind von der Seite "Server Properties" verfügbar:</li> <li>Auf der Registerkarte "General Settings" werden Informationen angezeigt, die das System für Vorgänge sowie für Supportmitarbeiter kenntlich macht.</li> <li>Auf der Registerkarte "LEDs" wird der Status aller Systemanzeigen angezeigt. Über sie können Sie auch den Zustand der Positionsanzeige ändern.</li> <li>Auf der Registerkarte "Hardware Information" werden elementare Produktdaten (VPD - Vital Product Data) zum Server angezeigt. Das IMM2 erfasst Serverinformationen, Serverkomponentenangaben und Netzhardwareinformationen.</li> <li>Auf der Registerkarte "Environmentals" werden Informationen zur Spannung und Temperatur für den Server und seine Komponenten angezeigt.</li> <li>Auf der Registerkarte "Hardware Activity" wird ein Verlauf der Komponenten von durch den Kundendienst austauschbaren Funktionseinheiten (FRU - Field Replaceable Unit) angezeigt, die zum System hinzugefügt oder daraus entfernt worden sind.</li> <li>Weitere Informationen finden Sie im Abschnitt "Server Properties (Servereigenschaften)" auf Seite 44.</li> </ul>
	Server Power Actions (Serverstromver- sorgungsaktionen)	Über die Seite "Server Power Actions" kann die Stromversorgung des Servers voll- ständig ferngesteuert werden. Dies umfasst Aktionen zum Einschalten, Ausschal- ten und für den Neustart. Weitere Informationen finden Sie in den Abschnitten "Server Power Actions (Serverstromversorgungsaktionen)" auf Seite 49 und "Stromversorgungsstatus des Servers steuern" auf Seite 106.
	Disks (Platten)	Auf der Seite "Hard Disks" (Festplatten) wird der Status von Festplattenlaufwerken im Server angezeigt. Sie können auf den Namen eines Lauf- werks klicken, um aktive Ereignisse für das Festplattenlaufwerk anzuzeigen. Wei- tere Informationen finden Sie im Abschnitt "Disks (Platten)" auf Seite 49.
	Memory (Speicher)	Auf der Seite "Memory" werden die im System verfügbaren Speichermodule sowie deren Status, Typ und Kapazität angezeigt. Sie können auf einen Modulnamen kli- cken, um ein Ereignis und zusätzliche Hardwareinformationen für das Speichermodul anzuzeigen. Wenn Sie ein Dual Inline Memory Module (DIMM) entfernen oder ersetzen, muss der Server danach mindestens einmal eingeschaltet werden, um die korrekten Speicherdaten anzuzeigen. Weitere Informationen fin- den Sie im Abschnitt "Memory (Speicher)" auf Seite 50.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
Server Management (Serververwaltung) (Fortsetzung)	Processors (Prozesso- ren)	Auf der Seite für CPUs werden die Mikroprozessoren im System samt deren Sta- tus und Taktgeschwindigkeit angezeigt. Sie können auf den Namen eines Mikro- prozessors klicken, um Ereignisse und weitere Hardwareinformationen für den Mikroprozessor anzuzeigen. Weitere Informationen finden Sie im Abschnitt "Processors (Prozessoren)" auf Seite 51.
	Server Timeouts (Serverzeitlimits)	Über die Seite "Server Timeouts" können Sie zur Erkennung von und zum Wieder- herstellen nach aufgetretenen Blockierungen des Servers Startzeitlimits für den Server verwalten. Weitere Informationen finden Sie in den Abschnitten "Server Timeouts (Serverzeitlimits)" auf Seite 52 und "Serverzeitlimits festlegen" auf Seite 58.
	PXE Network Boot (PXE-Netzboot)	Auf der Seite "PXE Network Boot" können Sie die Startreihenfolge (Bootreihenfolge) des Host-Servers für den nächsten Neustart ändern, um einen PXE/DHCP-Netzwerkstart (Preboot Execution Environment/Dynamic Host Configuration Protocol) zu versuchen. Die Host-Startreihenfolge wird nur geän- dert, wenn für den Host kein privilegierter Zugriffsschutz (Privileged Access Protection, PAP) festgelegt ist. Weitere Informationen finden Sie in den Abschnit- ten "PXE Network Boot (PXE-Netzboot)" auf Seite 52 und "PXE-Netzboot einrichten" auf Seite 121.
	Latest OS Failure Screen (Letzte Be- triebssystem- Fehleranzeige)	Auf der Seite "Latest OS Failure Screen" wird (falls vorhanden) eine Anzeige des letzten Betriebssystemfehlers auf dem Server angezeigt. Damit Ihr IMM2 Anzeigen von Betriebssystemfehlern aufzeichnen kann, muss der Watchdog Ihres Betriebs- systems aktiviert sein. Weitere Informationen finden Sie in den Abschnitten "Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige)" auf Seite 53 und "Daten der letzten Betriebssystem-Fehleranzeige erfassen" auf Seite 136.
	Power Management (Stromverbrauchs- steuerung)	Über die Seite "Server Power Management" können Sie die Richtlinien zum Strom- verbrauch und die Hardware verwalten. Hier befindet sich auch das Verlaufsprotokoll zur Stromverbrauchsmenge des Servers. Weitere Informationen finden Sie im Abschnitt "Serverstromversorgung verwalten" auf Seite 137.
IMM Management (IMM-Verwaltung)	IMM Properties (IMM-Eigenschaften)	Die Seite "IMM Properties" ermöglicht den Zugriff auf unterschiedliche Eigen- schaften und Einstellungen Ihres IMM2. Die folgenden Optionen sind von der Sei- te "IMM Properties" verfügbar:
(Fortsetzung auf der nächsten Seite)		• Die Registerkarte "Firmware" enthält einen Link zum Abschnitt "Server Firmwa- re" des Bereichs "Server Management".
		• Auf der Registerkarte "IMM Date and Time Settings" können Sie die Einstellung für Datum und Uhrzeit beim IMM2 anzeigen und konfigurieren.
		<ul> <li>Auf der Registerkarte "Serial Port" werden die IMM2-Einstellungen f ür den seri- ellen Anschluss konfiguriert. Diese Einstellungen schlie ßen die von der Umleitungsfunktion des seriellen Anschlusses verwendete Baudrate des seriellen Anschlusses sowie die Schl üsselfolge zum Wechseln zwischen dem Modus zur seriellen Umleitung und dem CLI-Modus ein.</li> </ul>
		Weitere Informationen finden Sie in Kapitel 4, "IMM2 konfigurieren", auf Seite 55.
	Users (Benutzer)	Auf der Seite "Users" werden die Anmeldeprofile und die allgemeinen Anmeldeeinstellungen für das IMM2 konfiguriert. Sie können auch Benutzerkonten anzeigen, die derzeit am IMM2 angemeldet sind. Die globalen Anmeldeeinstellungen umfassen das Aktivieren der LDAP-Serverauthentifizierung (Lightweight Directory Access Protocol), das Festlegen des Inaktivitätszeitlimits für das Web und das Anpassen der Einstellungen für die Accountsicherheit. Weitere Informationen finden Sie im Abschnitt "Benutzerkonten konfigurieren" auf Seite 63.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung	
IMM Management (IMM-Verwaltung) (Fortsetzung)	Network (Netz)	<ul> <li>Die Seite "Network Protocol Properties" (Netzprotokolleigenschaften) ermöglicht den Zugriff auf Netzwerkeigenschaften, Statusangaben und Einstellungen Ihres IMM2:</li> <li>Auf der Registerkarte "Ethernet" können Sie verwalten, wie das IMM2 über Ethernet kommuniziert.</li> <li>Auf der Registerkarte "SNMP" werden die SNMPv1- und SNMPv3-Agenten konfiguriert.</li> <li>Auf der Registerkarte "DNS" werden die DNS-Server konfiguriert, mit denen das IMM2 interagiert.</li> <li>Auf der Registerkarte "DDNS" wird das Dynamic Domain Name System für das IMM2 aktiviert oder inaktiviert und konfiguriert.</li> <li>Auf der Registerkarte "SMTP" werden SMTP-Serverinformationen für Alerts konfiguriert, die per E-Mail gesendet werden.</li> <li>Auf der Registerkarte "LDAP" wird die Benutzerauthentifizierung für die Verwendung mit einem oder mehreren LDAP-Servern konfiguriert.</li> <li>Auf der Registerkarte "USB" wird die USB-Schnittselle für die In-band-Kommunikation zwischen dem Server und dem IMM2 gesteuert. Diese Einstellungen haben keine Auswirkungen auf die USB-Fernsteuerungsfunktionen (Tastatur, Maus und Massenspeicher).</li> <li>Auf der Registerkarte "Port Assignments" können Sie die Portnummern ändern, die von einigen Services auf dem IMM2 verwendet werden.</li> </ul>	
	Security (Sicherheit)	<ul> <li>Die Seite "IMM Security" ermöglicht den Zugriff auf Sicherheitseigenschaften, Statusangaben und Einstellungen Ihres IMM2:</li> <li>Auf der Registerkarte "HTTPS Server" können Sie den HTTPS-Server aktivieren oder inaktivieren und seine Zertifikate verwalten.</li> <li>Auf der Registerkarte "CIM Over HTTPS" können Sie CIM over HTTPS aktivie- ren oder inaktivieren und die zugehörigen Zertifikate verwalten.</li> <li>Auf der Registerkarte "LDAP Client" können Sie die LDAP-Sicherheit aktivieren oder inaktivieren und ihre Zertifikate verwalten.</li> <li>Auf der Registerkarte "SSH Server" können Sie den SSH-Server aktivieren oder inaktivieren und seine Zertifikate verwalten.</li> <li>Weitere Informationen finden Sie im Abschnitt "Sicherheitseinstellungen konfigurieren" auf Seite 86.</li> </ul>	
	IMM Configuration (IMM-Konfiguration)	Auf der Seite "IMM Configuration" wird eine Zusammenfassung der aktuellen Einstellungen für die IMM2-Konfiguration angezeigt. Weitere Informationen finden Sie im Abschnitt "IMM-Konfiguration wiederherstellen und ändern" auf Seite 94.	
	Restart IMM (IMM erneut starten)	Über die Seite "Restart IMM" können Sie das IMM2 zurücksetzen. Weitere Infor- mationen finden Sie im Abschnitt "IMM2 erneut starten" auf Seite 94.	
	Reset IMM to factory defaults (IMM auf werkseitige Voreinstellungen zu- rücksetzen)	Über die Seite "Reset IMM to factory defaults" können Sie die Konfiguration des IMM2 auf die werkseitigen Voreinstellungen zurücksetzen. Weitere Informationen finden Sie im Abschnitt "IMM2 auf die werkseitigen Voreinstellungen zurücksetzen" auf Seite 95. Achtung: Wenn Sie auf <b>Reset IMM to factory defaults</b> klicken, gehen alle Ände- rungen, die Sie am IMM2 vorgenommen haben, verloren.	
	Activation Key Ma- nagement (Aktivierungs- schlüssel- verwaltung)	Auf der Seite "Activation Key Management" können Sie Aktivierungsschlüssel für optionale FoD-Funktionen (Features on Demand) des IMM2 oder des Servers ver- walten. Weitere Informationen finden Sie im Abschnitt "Aktivierungsschlüsselverwaltung" auf Seite 96.	

## Kapitel 3. Übersicht über die IMM2-Webbenutzerschnittstelle

Dieses Kapitel enthält eine Übersicht der Funktionen der IMM2-Webbenutzerschnittstelle und ihre Verwendung.

Wichtig: Dieser Abschnitt gilt nicht für IBM BladeCenter und IBM Blade-Server. Obwohl das IMM2 in einigen IBM BladeCenter-Produkten und IBM Blade-Servern standardmäßig enthalten ist, bleibt das erweiterte IBM BladeCenter-Managementmodul das primäre Managementmodul für Systemmanagementfunktionen. Benutzer, die die IMM2-Einstellungen auf Blade-Servern konfigurieren möchten, sollten das Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility -ASU) auf dem Blade-Server zum Ausführen dieser Aktionen verwenden.

#### Websitzungseinstellungen

Dieser Abschnitt enthält Informationen zu den Einstellungen für die Hauptseite der Webschnittstellensitzung.

Auf der IMM2-Hauptseite werden Menüoptionen im oberen rechten Bereich der Webseite angezeigt. Mithilfe dieser Menüoptionen können Sie das Aktualisierungsverhalten der Webseite sowie die Nachricht, die einem Benutzer beim Eingeben des Berechtigungsnachweises zur Anmeldung angezeigt wird, konfigurieren. In der folgenden Abbildung werden die Menüoptionen im oberen rechten Bereich der Webseite dargestellt.



Klicken Sie auf die Menüoption **Settings** (Einstellungen). Die folgenden Menüoptionen werden angezeigt:



#### Page Auto Refresh

Verwenden Sie die Option **Page Auto Refresh** (Seite automatisch aktualisieren) unter der Menüoption "Settings" (Einstellungen) im oberen rechten Bereich der Websitzungsseite, um festzulegen, dass der Seiteninhalt alle 60 Sekunden automatisch aktualisiert wird. Um festzulegen, dass der Seiteninhalt alle 60 Sekunden aktualisiert wird, wählen Sie das Kontrollkästchen **Automatically refresh appropriate data...** (Entsprechende Daten automatisch aktualisieren) aus und klicken Sie auf **OK**. Um die automatische Aktualisierung der Seite zu inaktivieren, wählen Sie das Kontrollkästchen ab und klicken Sie auf **OK**. In der folgenden Abbildung ist das Fenster "Auto refresh settings" (Einstellungen für automatische Aktualisierung) dargestellt.

Auto refresh settings	х
ZAutomatically refresh appropriate data (e.g., health status) every 60 seconds.	
OK Cancel	

Manche IMM2-Webseiten werden automatisch aktualisiert, auch wenn das Kontrollkästchen zur automatischen Aktualisierung nicht ausgewählt ist. Folgende IMM2-Webseiten werden automatisch aktualisiert:

• System Status (Systemstatus):

Der Systemstatus und der Stromversorgungsstatus werden automatisch alle drei Sekunden aktualisiert.

• Server Power Actions (Serverstromversorgungsaktionen, auf der Registerkarte "Server Management" (Serververwaltung):

Der Stromversorgungsstatus wird automatisch alle drei Sekunden aktualisiert.

• **Remote Control** (Fernsteuerung, auf der Registerkarte "Server Management": Die Schaltflächen zur Option "Start remote control..." (Fernsteuerung starten) werden automatisch jede Sekunde aktualisiert. Die Tabelle "Session List" (Sitzungsliste) wird alle 60 Sekunden aktualisiert.

#### Anmerkungen:

- Wenn Sie über Ihren Web-Browser zu einer Webseite wechseln, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch durch das Inaktivitätszeitlimit beendet.
- Wenn Sie über die Seite mit den Optionen für die Fernsteuerung unter "Server Management" eine Anforderung an einen Fernsteuerungsbenutzer senden, läuft das Zeitlimit für Ihre Websitzung unabhängig davon, von welcher Webseite aus Sie navigieren, nicht ab, bis eine Antwort vom Fernsteuerungsbenutzer empfangen wird oder bis das Zeitlimit für den Fernsteuerungsbenutzer abläuft. Wenn die Verarbeitung der Anforderung durch den Fernsteuerungsbenutzer abgeschlossen wurde, wird die Funktion für das Inaktivitätszeitlimit wieder aktiv.

Anmerkung: Die vorherige Anmerkung gilt für alle Webseiten.

• Die IMM2-Firmware unterstützt bis zu sechs gleichzeitige Websitzungen. Um Sitzungen für andere Benutzer freizugeben, melden Sie sich von der Websitzung ab, wenn Sie fertig sind, anstatt darauf zu warten, dass Ihre Sitzung durch das Inaktivitätszeitlimit automatisch geschlossen wird. Wenn Sie den Browser verlassen, während Sie sich auf einer IMM2-Webseite befinden, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch aufgrund von Inaktivität geschlossen.

#### **Trespass Message**

Verwenden Sie die Option **Trespass Message** (Übertretungsnachricht) unter der Menüoption "Settings" (Einstellungen) im oberen rechten Bereich der Websitzungsseite, um eine Nachricht zu konfigurieren, die angezeigt werden soll, wenn sich ein Benutzer beim IMM2-Server anmeldet. Die folgende Anzeige erscheint, wenn Sie die Option "Trespass Message" auswählen. Geben Sie den Nachrichtentext, der dem Benutzer angezeigt werden soll, im vorgesehenen Feld ein und klicken Sie auf **OK**.

Trespass message	х
A trespass message is text that will be displayed to any user logging in through the web or CLI interface. You can enter any relevant warning or informational text here that you wish users to see.	
WARNING! This computer system and network is PRIVATE AND PROPRIETARY and m	
OK Cancel	

Der Nachrichtentext wird im Nachrichtenbereich der IMM2-Anmeldeseite angezeigt, wenn sich ein Benutzer anmeldet, wie in der folgenden Abbildung dargestellt.

-	User name:
_	
	Password:
	Inactive session timeout:
	No timeout 👻
	Message:
	WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users.
	Log
ote: To ensure	security and avoid login conflicts, always
the your account	web page

#### Abmelden

Um unbefugten Zugriff zu verhindern, melden Sie sich von der IMM2-Websitzung ab, wenn Sie Ihre Arbeit beendet haben, und schließen Sie alle anderen IMM2-Web-Browser-Fenster, die Sie möglicherweise geöffnet haben, manuell.

Um sich von der Websitzung abzumelden, klicken Sie oben rechts auf der Webseite auf Log out (Abmelden). Das Fenster "Login" (Anmeldung) wird angezeigt.

	User name:
=	Password:
	Inactive session timeout:
	No timeout 👻
	Message:
	WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users.
	Log In
Note: To opsure	security and avoid login conflicts, always
and your session ight area of the	ns using the "Log out" option in the upper e web page.

**Anmerkung:** Die IMM2-Firmware unterstützt bis zu sechs gleichzeitige Websitzungen. Um Sitzungen für andere Benutzer freizugeben, melden Sie sich von einer Websitzung ab, wenn Sie Ihre Arbeit beendet haben, anstatt darauf zu warten, dass die Sitzung nach dem Inaktivitätszeitlimit automatisch geschlossen wird. Wenn Sie das Browserfenster geöffnet lassen, während Sie eine IMM2-Webseite anzeigen, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch aufgrund von Inaktivität geschlossen.

### Registerkarte "System Status"

Dieser Abschnitt enthält Informationen zur Verwendung der Optionen auf der Registerkarte "System Status" (Systemstatus) in der IMM2-Webbenutzerschnittstelle.

Die Seite "System Status" wird angezeigt, wenn Sie sich bei der IMM2-Webbenutzerschnittstelle angemeldet haben oder wenn Sie auf die Registerkarte "System Status" klicken. Auf der Seite "System Status" können Sie den Systemstatus, aktive Systemereignisse und Informationen zum Hardwarezustand anzeigen. Die folgende Anzeige wird geöffnet, wenn Sie auf die Registerkarte "System Status" klicken oder sich bei der IMM2-Webschnittstelle anmelden.

IBM Integrated Managemen	nt Module II		USERID	Settings   Log out	IBM.
System Status Even	ts - Service and Suppo	nt • Server Management • IMM Management • Search			
IBM Flex System	x240 with 100	Gb			
The System Status and Health p	age provides an at-a-glanc	e overview of the operating status of the server in which this IMM resides. Common informa-	ition and actions are co-locat	ed on this one page.	
System Status Power: Off System state: System power System Information  Power	off/State unknown er Actions 💌 🛛 Remote (	Control Lutest: OS Falure Screen			
Active Events					
Severity   Source	Date	Message			
Hardware Health					
Component Type	Status				
Disks	Normal				
Processors	Normal				
Memory	Normal				
System	Normal				

Sie können auf das grüne Symbol (mit dem Häkchen) in der oberen linken Ecke der Seite klicken, um eine kurze Übersicht über den Serverstatus zu erhalten. Ein Häkchen gibt an, dass der Server sich im Normalbetrieb befindet.



Wenn ein roter Kreis oder ein gelbes Dreieck angezeigt wird, bedeutet dies, dass eine Fehler- oder Warnbedingung vorliegt, wie in der folgenden Abbildung dargestellt.



Das Symbol mit dem roten Kreis gibt an, dass auf dem Server eine Fehlerbedingung vorliegt. Das Symbol mit dem gelben Dreieck gibt an, dass eine Warnbedingung vorliegt. Wenn ein Symbol mit einem roten Kreis oder einem gelben Dreieck angezeigt wird, sind die Ereignisse, die der Bedingung zugeordnet sind, im Abschnitt "Active Events" (Aktive Ereignisse) auf der Seite "System Status" aufgeführt, wie in der folgenden Abbildung dargestellt.

Active Events	0		
Severity .	<ul> <li>Source</li> </ul>	Date	Message
🔕 Error	System	16 Jul 2012 01:00:28.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.
Error	System	16 Jul 2012 01:00:29.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.

Sie können zum IMM2-Server einen beschreibenden Namen hinzufügen, damit Sie die einzelnen IMM2-Server voneinander unterscheiden können. Um dem IMM2-Server einen beschreibenden Namen zuzuordnen, klicken Sie auf den Link Add System Descriptive Name... (Beschreibenden Systemnamen hinzufügen) unter dem Namen des Serverprodukts.



Wenn Sie auf den Link **Add System Descriptive Name...** (Beschreibenden Systemnamen einfügen) klicken, wird das folgende Fenster angezeigt, in dem Sie einen Namen eingeben können, der dem IMM2-Server zugeordnet wird. Sie können den beschreibenden Systemnamen jederzeit ändern.



Der Abschnitt **System Status** auf der Seite "System Status" enthält Informationen zum Stromversorgungsstatus und zum Betriebsstatus des Servers. Angezeigt wird der Serverstatus zum Zeitpunkt des Öffnens der Seite "System Status" (wie in der folgenden Abbildung dargestellt).

System Status			
Power:	On		
System state:	System running in UEFI		
System Information   Power Actions			

Der Server kann sich in einem der folgenden Status befinden:

Serverstatus	Beschreibung
System power off/state unknown (Stromver- sorgung des Systems ausgeschaltet/Status unbekannt)	Der Server ist ausgeschaltet.
System on/starting UEFI (System eingeschaltet/UEFI wird gestartet)	Der Server ist eingeschaltet, aber die UEFI wird noch nicht ausgeführt.
System running in UEFI (System wird in UEFI ausgeführt)	Der Server ist eingeschaltet und die UEFI wird ausgeführt.
System stopped in UEFI (System wurde in UEFI gestoppt)	Der Server ist eingeschaltet; die UEFI hat einen Fehler erkannt und ihre Ausführung wurde beendet.
Booting OS or in unsupported OS (Betriebs- system wird gebootet oder es wird ein nicht	Der Server kann sich aus einem der folgen- den Gründe in diesem Status befinden:
unterstütztes Betriebssystem gebootet)	<ul> <li>Das Ladeprogramm des Betriebssystems wurde gestartet, aber das Betriebssystem wird noch nicht ausgeführt.</li> </ul>
	• Die Ethernet-over-USB-Schnittstelle des IMM2 ist inaktiviert.
	• Das Betriebssystem hat die Treiber, die die Ethernet-over-USB-Schnittstelle unterstützen, nicht geladen.
OS booted (Betriebssystem gebootet)	Das Serverbetriebssystem wird ausgeführt.
Suspend to RAM (Aussetzen in RAM)	Der Server wurde in den Bereitschafts- oder Ruhemodus versetzt.

Tabelle 2. Stromversorgungsstatus und Betriebsstatus des Servers

Auf der Seite "System Status" werden außerdem die Registerkarten **System Information** (Systeminformationen), **Power Actions** (Stromversorgungsaktionen), **Remote Control** (Fernsteuerung) und **Latest OS Failure Screen** (Letzte Betriebssystem-Fehleranzeige) angezeigt.

System Information 🔻	Power Actions 🔻	Remote Control	Latest OS Failure Screen

Klicken Sie auf die Registerkarte **System Information**, um Informationen zum Server anzuzeigen.

ystem Information (	Quick View
lame	Value
lachine Name	System x3650 M4
lachine Type	7915
lodel	35Z
erial Number	06CNZ40
JUID	E596B684B75E11E0A0B0E41F13EB0F72
erver Power	On
erver State	System running in UEFI
otal hours powered-on	117
testart count	6
mbient Temperature	80.60 F / 27.00 C
inclosure Identify LED	Off Change
heck Log LED	Off

Klicken Sie auf die Registerkarte **Power Actions**, um die Aktionen anzuzeigen, die Sie zur vollständigen fernen Stromversorgungssteuerung des Servers über die Aktionen zum Einschalten, Ausschalten und Neustarten des Servers durchführen können. Details zur fernen Steuerung der Stromversorgung des Servers finden Sie unter "Stromversorgungsstatus des Servers steuern" auf Seite 106.

Klicken Sie auf die Registerkarte **Remote Control**, um Informationen zur Steuerung des Servers auf Betriebssystemebene zu erhalten. Unter "Remote-Presenceund Fernsteuerungsfunktionen" auf Seite 107 finden Sie Details zur Funktion "Remote Control".

Klicken Sie auf die Registerkarte **Latest OS Failure Screen**, um Informationen zum Erfassen der Daten der letzten Betriebssystem-Fehleranzeige zu erhalten. Details zur letzten Betriebssystem-Fehleranzeige finden Sie unter "Daten der letzten Betriebssystem-Fehleranzeige erfassen" auf Seite 136.

Im Abschnitt **Hardware Health** (Hardwarezustand) der Seite "System Status" befindet sich eine Tabelle mit einer Liste der überwachten Hardwarekomponenten und deren Status. In der Spalte "Component Type" (Komponententyp) der Tabelle wird möglicherweise der Zustand der Komponente mit dem kritischsten Zustand angezeigt. Ein Server kann z. B. über mehrere installierte Stromversorgungsmodule verfügen, die bis auf eines alle normal funktionieren. Der Status der Komponente "Power Modules" (Stromversorgungsmodule) wird dann aufgrund dieses einen Stromversorgungsmoduls als kritisch angezeigt (wie in der folgenden Abbildung dargestellt).

Hardware Health @			
Component Type	Status		
Cooling Devices	Normal		
Power Modules	🔇 Critical		
Disks	Normal		
Processors	Normal		
Mempry	🔽 Normal		
System	Normal		

Bei jedem Komponententyp handelt es sich um einen Link, auf den Sie klicken können, um ausführlichere Informationen zu erhalten. Wenn Sie auf den Komponententyp klicken, wird eine Tabelle angezeigt, in der die Status der einzelnen Komponenten aufgeführt sind (wie in der folgenden Abbildung dargestellt).

Memory Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: EV				
FRU Name	<ul> <li>Status</li> </ul>	Туре	Capacity (GB)	
DIMM 4	Normal	DDR3	4	
DIMM 9	Normal	DDR3	4	
DIMM 16	Normal	DDR3	4	
DIMM 21	Normal	DDR3	4	

Sie können auf eine Komponente in der Spalte "FRU Name" (Name der durch den Kundendienst austauschbaren Funktionseinheit) klicken, um zusätzliche Informationen zu dieser Komponente zu erhalten. Alle aktiven Ereignisse für die Komponente werden angezeigt.

Pr	Properties for DIMM 4		
	Events	Hardware Information	
There are no active events for this device			
Close			
Klicken Sie auf die Registerkarte **Hardware Information** (Hardwareinformationen), um ausführliche Informationen zur Komponente anzuzeigen.

Properties for DIMM 4	
Events Hardwa	re Information
Description PartNumber FRU Serial Number Manuf Date Type Size	DIMM 4 M393B5773CH0-YH9 8634E095 2211 DDR3 2 GB
Close	

### **Registerkarte** "Events" (Ereignisse)

Dieser Abschnitt enthält Informationen zur Verwendung der Optionen auf der Registerkarte "Events" in der IMM2-Webbenutzerschnittstelle.

Die Optionen auf der Registerkarte **Events** ermöglichen Ihnen die Verwaltung des Ereignisprotokollverlaufs (Event Log) und der Ereignisempfänger (Event Recipients) für E-Mail- und syslog-Benachrichtigungen. In der folgenden Abbildung sind die Optionen auf der Registerkarte "Events" auf der IMM2-Webseite dargestellt.

IBM Integrated Management Module II								
System Status	Events 🕶	Service and Support	•	Server Management 😽	IMM Management + 5			
	Event Log	1	Full	log history of all events				
System x3750 Add System Descriptive Nam	Event Red	cipients	Add	and modify E-Mail and fications	SysLog			

## Event Log (Ereignisprotokoll)

Wählen Sie auf der Registerkarte "Events" (Ereignisse) die Option **Event Log** (Ereignisprotokoll) aus, um die Seite "Event Log" anzuzeigen. Auf der Seite "Event Log" wird der Schweregrad der Ereignisse angezeigt, die vom IMM2 gemeldet wurden, und Informationen zu allen Fernzugriffversuchen sowie zu allen Konfigurationsänderungen. Alle Ereignisse im Protokoll weisen eine Zeitmarke auf, die die IMM2-Einstellung für Datum und Uhrzeit verwendet. Einige Ereignisse generieren außerdem Alerts, falls dies auf der Seite "Event Recipients" (Ereignisempfänger) so konfiguriert wurde. Sie können Ereignisse im Ereignisprotokoll sortieren und filtern. In der folgenden Abbildung ist ein Beispiel für die Seite "Event log" dargestellt.

	🕓 🦉 🔛	2.10 A.W.	Fiters: 🔕	🛕 🚺 💄 🛛 Time: 🔺 Date	HS + Search Events. Go
	Severity	Source	Date	Event ID	Message
•	0 of 51 items filtered		0 items selected	Clear filter Applied filters: Events ( Em	or Warning Information Audit ]
	💽 informational	System	31 1 2013 09:02:42.771 AM	Dx4000000e00000000	Remote Login Successful, Login ID: USERID from webguis at IP address 9.111.29.57.
	🚺 Informational	System	31 1 2013 09:01:00:297 AM	0x400000160000000	ENETICM.tep11 DHCP-HSTN-HM2-5cae8b4e83c5, DN-coil.bm.com, IP@=8 186,156,78, SN-255_255_255_255,128, GW@=9,186,156,1, DNS1@=9.0.148,50
	informational	System	31 1 2013 09:00:58.957 AM	0x4000001900000000	LAN: Ethernet()BM:ep2) interface is now active.
	informational	System	31 1 2013 09:00:55:004 AM	Dx4000001700000000	ENET[CNItep2] IP-Cfg:H5Name=INIt2-6cae8b4e83c6, IP@=169.254.95.118,NetMak=255.255.0.0, GW@=0.0.0.
	Informational	System	31 1 2013 09:00:53 403 AM	Dx400000370000000D	ENET[CM ep 1] IPv6-Linit.ocal HstName=IMM2-6caeBb4eB3c6, IP@=fe80:6eae 8bfffe4e B3c6, Pref=64,
	Informational	System	31 1 2013 09:00:51 592 AM	Dx4000001900000000	LAN: Ethernet(IBN:ep1) interface is now active.
	💽 Informational	System	31 1 2013 09:00:47 068 AM	0×4000000 100000000	Management Controller SN# 06KNKL9 Network Initialization Complete.
	Informational	S)stem	31 1 2013 09:00:02:874 AM	0x800801282101mm	Device Low Security Jmp has been added.
	Informational	Power	31 1 2013 09:00:02:304 AM	0x805f00091301fm	Host Power has been turned off.
	💽 Informational	System	31 1 2013 08:55:11.252 AM	0x4000001500000000	Management Controller SN# 05KNKL9 reset was initiated by user USERID.
	Informational	System	31 1 2013 08:47:59.118 AM	0x4000002300000000	Flash of SN# 05KNKL9 from (.1111.9.186.166.119) succeeded for user USERID .
	Informational	System	31 1 2013 08 43 15 666 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9 186 166 119.
	Informational	Sustam	21 1 2012 02:04:07 470 6M	0+4000000-00000000	Remote Login Successful, Login ID: USERID from

Um Ereignisse im Ereignisprotokoll zu sortieren und zu filtern, wählen Sie die entsprechende Spaltenüberschrift aus (wie in der folgenden Abbildung dargestellt).

	Seventy	Source	Dute	Event ID	Message
24	0 of 52 items litered		0 Rems selected	Clear The Appled Stars Events	[Error Warning Information Audit]
13	E Informational	System	31 Jan 2013 09:11:04.024 AM	0x4000000e00000000	Remote Login Successful, Login ID: USERID N. webguis at IP address 9.185.166.119.
Ш.	Informational	System	31 Jan 2013 09:02:42:771 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID to webguis at IP address 9.111.29.57.

Sie können mithilfe der Schaltfläche **Export** alle oder ausgewählte Ereignisse aus dem Ereignisprotokoll speichern. Um bestimmte Ereignisse auszuwählen, wählen Sie auf der Hauptseite von "Event Log" ein oder mehr Ereignisse aus und klicken Sie mit der linken Maustaste auf die Schaltfläche **Export** (Exportieren) (wie in der folgenden Abbildung dargestellt).

Event Log This page displays the contents of the IMM event log, and allows y entry first). For each log entry, the severity of the event is displayed									
Export Event Logs									
Severity Source Date									
	0 of 52 items filtered		2 items selecte						
	🚹 Informational	System	31 Jan 2013 09:1						
	🚹 Informational	System	31 Jan 2013 09:0						

Mit der Schaltfläche **Delete Events** (Ereignisse löschen) können Sie den Ereignistyp auswählen, den Sie löschen möchten (wie in der folgenden Abbildung dargestellt).

2	S 🕺 📾	100 100	Filter	r 🔕 🚹 🚺 🔮	Time: All Dates	+ Search Events Go
	Severity	Source	Date			Message
-	0 of 52 items filtered		Delete Events		x	g Information Audit ]
	1 Informational	System	3 Choose which even	its you wish to delete		Remote Login Successful. Login ID: USI webguis at IP address 9.186.166.119.
	👔 Informational	System	3 Platform Events			Remote Login Successful. Login ID: USE webguis at IP address 9.111.29.57.
	T Informational	System	OK Cancel 31 Jan 2013 05:01:00	T21.474 004000010000	00000	ENET[CIM:ep1] DHCP-HSTN=IMM2-6cae8b4e83c6, DN=cn.ibm.com, IP@=9.186.166.78, SN=255.255.255.128. GW@=9.186.166

Um den Typ der Ereignisprotokolleinträge auszuwählen, den Sie anzeigen möchten, klicken Sie auf die entsprechende Schaltfläche (wie in der folgenden Abbildung dargestellt).



Um nach bestimmten Ereignistypen oder Suchbegriffen zu suchen, geben Sie den betreffenden Ereignistyp oder den Suchbegriff im Feld **Search Events** (Ereignisse suchen) ein. Klicken Sie dann auf **Go** (Start) (wie in der folgenden Abbildung dargestellt).

2	🛃 🔻 🔛	X	Filters: 🚫	$\wedge$	Time:	All Dates	+ IENET	(Fq)
	Severity	Source	Date		Event ID		Message	
3	0 of 53 items filtered		0 items selected	2	Clear filter Applied filters: Ev	ents:[Error War	ning Information Audit]	
	1 Informational	System	1 Feb 2013 01:29:28.414 AM		0x4000000e00000000		Remote Login Succe webguis at IP addres	ssful. Login ID: USERID t s 9.186.166.119.

Um die Protokollprüfanzeige "Check Log LED" auszuschalten, wenn die Protokollprüfanzeige angeschaltet ist und die zugehörigen "Event Logs" (Ereignisprotokolle) ausgewählt wurden, klicken Sie auf die Schaltfläche **Check Log LED Status** (Status der Protokollprüfanzeige) (wie in der folgenden Abbildung dargestellt).

5		27	Filters: 🧐 🔔 🔟 🚢 Time: All Dates	- Search Eventa Go
	Severity	Source	Date - Event ID	Message
	0 of 55 items filtered		Change Check Log LED X	g Information Audit ]
	Informational	System	1 When this LED is lit, it indicates that an error has occurred. Read the event log to net more information about this event Turning off the Check Log LED.	ED Check Log state changed to Lit by USER
	📑 Informational	System	a cknowledges that you have read event log information but the error may still be present.	Remote Login Successful. Login ID: USERID webguis at IP address 9.186.166.119.
	🔝 Informational	System	Do you want to turn off the Check Log LED in your system?	Remote Login Successful. Login ID: USERID webguis at IP address 9.186.166.119.
	Informational	System	a	Remote Login Successful. Login ID: USERID webguis at IP address 9.186.166.119.

In der Symbolleiste "Event Log" (Ereignisprotokoll) können Sie auf jede beliebige Schaltfläche von **Filter Events** (Ereignisse filtern) klicken, um die Ereignisse auszuwählen, die angezeigt werden sollen. Um den Filter zu löschen und alle Ereignistypen anzuzeigen, klicken Sie auf den in der folgenden Abbildung dargestellten Link **Clear Filter** (Filter löschen).

2   🔄 🗏 🔛	X	Filters:	8		1	В	Time:	All Dates	÷	Search Events	Go
Severity	Source	Date		•	Event ID				Messag	je	
34 of 56 items filtered		0 items selected		C	ear filter	Applied filte	rs: Ever	nts: [ Error Warn	iing Audi	t]	

# Event Recipients (Ereignisempfänger)

Mit der Option **Events Recipients** (Ereignisempfänger) auf der Registerkarte "Events" (Ereignisse) können Sie E-Mail- und syslog-Benachrichtigungen hinzufügen und ändern.

IBM Integrated Manag	gement Mo	dule II			
System Status	Events 🗸	Service and Support	•	Server Management 👻	IMM Management 👻 Sea
	Event Log	9	Full	log history of all events	
System x3750 Add System Descriptive Nam	Event Re	cipients	Add	and modify E-Mail and fications	SysLog

Mithilfe der Option "Event Recipients" können Sie die Empfänger von Benachrichtigungen über Systemereignisse verwalten. Sie können die einzelnen Empfänger konfigurieren und die Einstellungen verwalten, die für alle Ereignisempfänger gelten. Sie können auch ein Testereignis generieren, um die Benachrichtigungsfunktion zu überprüfen.

Klicken Sie auf die Schaltfläche **Create** (Erstellen), um E-Mail- und syslog-Benachrichtigungen zu erstellen.



Wählen Sie die Option **Create E-mail Notification** (E-Mail-Benachrichtigung erstellen) aus, um eine Ziel-E-Mail-Adresse einzurichten und den Ereignistyp auszuwählen, für den Benachrichtigungen gesendet werden sollen. Außerdem können Sie auf **Advanced Settings** (Erweiterte Einstellungen) klicken, um die Startindexnummer auszuwählen. Um das Ereignisprotokoll in die E-Mail einzufügen, wählen Sie das Kontrollkästchen **Include the event log contents in the e-mail body** (Inhalt des Ereignisprotokolls in den Nachrichtentext der E-Mail einfügen) aus. In der folgenden Abbildung ist ein Beispiel für das Fenster "Create E-mail notification" dargestellt.

Create E-Mail Notificatio	on		×
Use this dialog to configu Note: To enable an E-ma Descriptive name: E-Mail address:	ure specified E-mail recipients to re <u>ceive</u> Cr il recipient, you need to go to the SMTP tai	tical, Attention or System notifications on Network Protocols/page to configure the	email server correctly.
Events to receive:			
Select all events			
Show sub-types	2 Critical	Z Attention	System
Include the event log	contents in the e-mail body		
Status: Enable this recipient Disable this recipient			
Advanced Settings			
OK Cancel			

Wählen Sie die Option **Create SysLog Notification** (SysLog-Benachrichtigung erstellen) aus, um einen Hostnamen und eine IP-Adresse für den SysLog-Collector einzurichten und den Ereignistyp auszuwählen, für den Benachrichtigungen gesendet werden sollen. Außerdem können Sie auf **Advanced Settings** (Erweiterte Einstellungen) klicken, um die Startindexnummer auszuwählen. Sie können außerdem den Port auswählen, den Sie für diesen Benachrichtigungstyp verwenden möchten. In der folgenden Abbildung ist ein Beispiel für das Fenster "Create SysLog Notification" dargestellt.

Create SysLog Notification			×
Use this dialog to configure specified SysLog server to Descriptive name:	Receive Critical, Attention or System notifi	cations.	
Events to receive:	Port		
Show sub-types	Attention	System	
Status: @ Enable this recipient O Disable this recipient			
Advanced Settings			
OK Cancel			

Wählen Sie die Schaltfläche **Generate Test Event** (Testereignis generieren) aus, um eine Test-E-Mail an das ausgewählte E-Mail-Ziel zu senden (wie in der folgenden Abbildung dargestellt).

Generate Test Event	x
Please first select the ev Close	nt notification that you wish to generate a test event for.

Wählen Sie die Schaltfläche **Global Settings** (Globale Einstellungen) aus, um einen Grenzwert für die Wiederholungsversuche für Ereignisbenachrichtigungen, die Verzögerung (in Minuten) zwischen den Ereignisbenachrichtigungseinträgen und die Verzögerung (in Minuten) zwischen den Benachrichtigungsversuchen festzulegen (wie in der folgenden Abbildung dargestellt).

Event Notification Global Settings	x
These settings will apply to all event notifications.	
Retry limit:	
Delay between entries (minutes): 0.5	
Delay between attempts (minutes): 0.5	
OK Cancel	

Wenn Sie ein Ziel für eine E-Mail- oder syslog-Benachrichtigung entfernen möchten, wählen Sie die Schaltfläche **Delete** (Löschen) aus. Das folgende Fenster wird geöffnet:

IBM Ir	ntegr Sys	ated Manag tem Status	ement Module II Events - Service and	Support 👻 Server Manage	ement 👻 IMM Manag	ement 👻 Sear
Ever This ta ame fo Create	nt F able le r that	ts you view a particular rec Generate Ti	nts summary list of all remote ipient est Event Global Se	e alert recipients. Use the lin	ks in the Name column	to configure in
	Nam	e	Notification Method	Events to Receive	Status	
0	Emai	il Subject	E-Mail	None	Enabled	
0	Emai	il2 Subject	E-Mail	None	Enabled	
		Confi	rm Event Notification	Deletion	x	
		() OK	Do you want to dele	te the notification 'Ema	il Subject' ?	

## **Registerkarte "Service and Support"**

Dieser Abschnitt enthält Informationen zur Verwendung der Optionen auf der Registerkarte "Service and Support" der IMM2-Webbenutzerschnittstelle.

## Download Service Data (Servicedaten herunterladen)

Verwenden Sie die Option **Download Service Data** (Servicedaten herunterladen) auf der Registerkarte "Service and Support" (Service und Unterstützung), um Informationen zu sammeln und eine komprimierte Datei über den Server zu erstellen, die Sie als Hilfestellung bei der Fehlerbestimmung an den IBM Support schicken können.

IBM Integrated Management Mo	dule II	
System Status Events 🗸	Service and Support $\star$	Server Management + IMM Management + Search
System x3750 M4	Download Service Da	ta Obtain a compressed file of relevant service data

Klicken Sie auf die Schaltfläche **Download Now** (Jetzt herunterladen), um die Informationen zu Service und Support herunterzuladen (siehe folgende Abbildung).



Der Prozess zum Sammeln der Daten beginnt. Der Prozess generiert in ein paar Minuten die Servicedaten, die Sie dann in einer Datei speichern können. In einem Fortschrittsfenster wird angezeigt, dass die Daten generiert werden.



Wenn der Prozess abgeschlossen ist, wird das folgende Fenster angezeigt, das Sie auffordert anzugeben, auf welcher Position die generierte Datei gespeichert werden soll.

IBM Integrated Managem	ent Module II
System Status Ev	ents   Service and Support  Server Management  IMM Management  Search
Download Servi Allows you to manually obtain Download Now Send Ser	Ce Data         ne service data for your system. Normally you would only do this at the request of IBM Support personnel.         ace Infor       Opening 7914A2A_06KNKL9_imm2_20130206_104046.tgz         You have chosen to open <sup>10</sup> 7914A2A_06KNKL9_imm2_20130206_104046.tgz          which is a: Gzip archive (1.0 MB)         from: https://9.186.166.78          What should Firefox do with this file?
	Open with Archive Manager (default)
	Save File
	Do this <u>a</u> utomatically for files like this from now on. Cancel OK

# Registerkarte "Server Management" (Serververwaltung)

Dieser Abschnitt enthält Informationen zu den Optionen auf der Registerkarte "Server Management" (Serververwaltung) auf der Homepage der IMM2-Webbenutzerschnittstelle.

Mithilfe der Optionen auf der Registerkarte "Server Management" können Sie Informationen zum Status und zur Steuerung der Server-Firmware, zum Fernsteuerungszugriff, zum Status und zur Steuerung der Servereigenschaften, zu Serverstromversorgungsaktionen, zu Kühleinheiten, zu Stromversorgungsmodulen, zu Datenträgern, zum Speicher, zu Prozessoren, zu Zeitlimitüberschreitungen auf dem Server, zum PXE-Netzboot und zur letzten Betriebssystem-Fehleranzeige anzeigen (wie in der folgenden Abbildung dargestellt).

System Status	Events + Service and Support +	Server Management + INM I	tanagement + Swarth	
Sustem v27E0		Server Firmware	View firmware levels and update firmware	
Add System Descriptive Name.	···	Remote Control	Allows you access into the operating system of your system	
The System Status and Health page provides an at-e-glance ove System Status lower: On		Server Properties	Various properties and settings related to your system	ormation and actions are co-located on this one page.
		Server Power Actions	Power actions such as power on, power off, and restart.	
		Cooling Devices	Cooling devices installed in your system	
System Information 💌 🕴	Power Actions * Remote Contro	Power Modules	Power modules installed in your system	
Active Events	ce Date	Disks	Hard disk drives installed directly in your system	
		Memory	RAM installed in your system	_
lardware Health Component Type	Status	Processors	Physical CPUs installed in your system	
Cooling Devices	Normal	Server Timeouts	Configure watchdogs, etc.	
Power Modules	Normal	PXE Network Boot	Settings for how your system performs	
Disks	Normal		Same control time and the	
Processors	Normal	Latest OS Failure Screen	Windows systems only. View an image of the most recent failure screen.	
lemory	Normal			-
System	Normal			

### Server Firmware (Server-Firmware)

Wählen Sie die Option **Server Firmware** (Server-Firmware) auf der Registerkarte "Server Management" (Serververwaltung) aus, um die auf dem Server installierten Firmwareversionen anzuzeigen und Firmwareaktualisierungen anzuwenden. In der folgenden Anzeige werden die Server-Firmwareversionen angezeigt. Sie können über diese Anzeige die DSA-, IMM2- und UEFI-Firmware aktualisieren.

IBM Integrated Manag	N Integrated Management Module II								
System Status	Events + Se	ervice and Support + 1	ierver Nanagement 👻 1414 A	anagement + [Search					
Server Firmware levels of Update Firmware	are In various serve	components, including t	he JMM tself.						
Firmware Type	Status	Version	Build	Release Date					
DS4	Active	9.24	DSYT44B	2012-08-10					
IVIN2									
INN2 (Primary)	Active	2.15	1AD039Q	2013-01-28					
IMM2 (Backup)	Inactive	3.00	1A00397	2013-01-30					
UEFI			0.75400.000	2040.00.00					
UEFI (Primary)	Active	1.20	D/E120CUS	2012-08-23					

Der aktuelle Status und die aktuellen Versionen der IMM2-, UEFI- und DSA-Firmware werden angezeigt, einschließlich der primären Versionen und der Sicherungsversionen. Der Status der Firmware wird in drei Kategorien angegeben:

- Active (aktiv): Die Firmware ist aktiv.
- Inactive (inaktiv): Die Firmware ist inaktiv.
- **Pending** (anstehend): Die Firmware befindet sich im Wartestatus vor der Aktivierung.

Achtung: Die Installation der falschen Firmware könnte eine Serverstörung verursachen. Bevor Sie eine Firmware- oder Einheitentreiberaktualisierung installieren, lesen Sie alle Readme- und Änderungsprotokolldateien, die mit der heruntergeladenen Aktualisierung bereitgestellt werden. Diese Dateien enthalten wichtige Informationen zur Aktualisierung und zur Installationsprozedur der Aktualisierung, einschließlich Informationen zu besonderen Prozeduren bei der Aktualisierung von einer frühen Firmware- oder Einheitentreiberversion auf die neueste Version.

Um die Firmware zu aktualisieren, wählen Sie die Schaltfläche **Update Firmware...** (Firmware aktualisieren) aus. Das Fenster "Update Server Firmware" (Server-Firmware aktualisieren) wird angezeigt. Sie können auf **Cancel** (Abbrechen) klicken und zum vorherigen Fenster von "Server Firmware" zurückkehren, oder auf die Schaltfläche **Select File...** (Datei auswählen) klicken, um die Firmwaredatei auszuwählen, die Sie für die Flashaktualisierung der Server-Firmware verwenden möchten.

**Anmerkung:** Lesen Sie die in der Eingabeaufforderung angezeigte Warnung, bevor Sie auf die Schaltfläche **Select File...** (Datei auswählen) klicken.

Select Firmware File	
Select the firmware file that you wish to use to flash the IMM/Server Firmware	
Please note that updating server firmware via this wizard is intended for recovery purposes only. It is strongly recommended that updates be performed using the IBM Updates/opress System Pack Installer, available as a download from the IBM web site.	
Select File Selected Flash File: ibm_fw_imm2_1aoo311.60_anyos_noarch.uxz	
	Select File Select File Select File

Wenn Sie auf die Schaltfläche **Select File...** klicken, wird das Fenster "File Upload" (Hochladen von Datei) angezeigt, in dem Sie nach der gewünschten Datei suchen können.

System Status	Update Server Firmwa								
	Choose Fernware File	Select Firmware File							
Server Firmw how the firmware levels Update Prinware	Upload and Verfy Additional Options	Select the formulare file that you wish to use to fash the DHV/Server Pinnware							
Firmware Type OSA IMM2 (Active) IMM2 (Primary)	Perform Pernware Plash	Please note that upd purposes only. It is Updates/press Systematics	lating server firmware via trongly recommended th en Pack Installer, availabli	this wizard is inter it updates be perfit as a download fit	nded for recovery formed using the IBM on the IBM web site.				
MM2 (Backup)			File Upload					2 ×	ā -
UEFI (Adlive)								1.1.1 Gal	1
UEFI (Primary)		Select File	Look in	System x37	50fw-updates	× 0	a 0. 0.		
	< Back Next > Fir	with Cancel	Ny Recert Documents Desktop My Documents						
			My Computer	File name:	bro.fwjmm2_1aos3	1-1.60_anyos_noar	huaz 🛩	Open	)

Klicken Sie, nachdem Sie zu der Datei navigiert sind, die Sie auswählen möchten, auf die Schaltfläche **Open** (Öffnen). Sie gelangen zurück zum Fenster "Update Server Firmware", in dem nun die ausgewählte Datei angezeigt wird (wie in der folgenden Abbildung dargestellt).



Klicken Sie auf die Schaltfläche **Next** > (Weiter), um den Upload- und Überprüfungsprozess für die ausgewählte Datei zu starten (wie in der folgenden Abbildung dargestellt). Eine Fortschrittsanzeige erscheint, während die Datei hochgeladen und überprüft wird.

Choose Firmware File	Upload and Verify							
Upload and Verify	The firmware file is being uploaded. You will have an opportunity to verify it is the correct file prior to the flashing procedure.							
Additional Options								
Perform Firmware Flash	Ste.	Upload and Verify Firmware File						
		15%						
		Uploading firmware file 'ibm fw imm2 1aco311.60 acvos poarch uv2'						

Ein Statusfenster wird angezeigt (wie in der folgenden Abbildung dargestellt), in dem Sie überprüfen können, ob es sich bei der ausgewählten zu aktualisierenden Datei um die richtige Datei handelt. Das Fenster enthält Informationen zum Typ der zu aktualisierenden Firmwaredatei, z. B. DSA, IMM2 oder UEFI. Wenn die Informationen richtig sind, klicken Sie auf die Schaltfläche **Next** >. Wenn Sie ausgewählte Optionen wieder abwählen möchten, klicken Sie auf die Schaltfläche **Schaltfläche Back** (Zurück).



Wenn Sie auf die Schaltfläche "Next >" klicken, wird eine Gruppe zusätzlicher Optionen angezeigt, wie in der folgenden Abbildung dargestellt.

Update Server Firmware							
Choose Firmware File	Additional Options Some firmware types have additional options that you can select.						
Additional Options							
Perform Firmware Flash	Action1: Update the primary bank (defat	ult action) *					
Reck (News) Epison	Cancel						
< Back [Next >] Finish	Cancel						

Im Dropdown-Menü neben Action 1 (Aktion 1, wie in der folgenden Abbildung dargestellt) können Sie die Aktion Update the primary bank (default action) (primäre Speichergruppe aktualisieren (Standardaktion)) oder die Aktion Update the backup bank (Sicherungsspeichergruppe aktualisieren) auswählen.

Update Server Firmwa	re		
Choose Firmware File	Additional Options Some firmware types haw	e additional options that you can select.	
Additional Options			
Perform Firmware Flash	Action1:	Update the primary bank (default action)	7
	Action2:	Update the primary bank (default action)	
		Update the backup bank	
< Back Next > Fir	aish Cancel		

Nachdem Sie eine Aktion ausgewählt haben, gelangen Sie zurück zum vorherigen Fenster. Hier können Sie durch Klicken auf das Kontrollkästchen Action 2 weitere Aktionen ausführen.

Nachdem die ausgewählte Aktion geladen wurde, werden die ausgewählte Aktion und ein neues Dropdown-Menü Action 2 (Aktion 2) angezeigt (wie in der folgenden Abbildung dargestellt).

Anmerkung: Um eine Aktion zu inaktivieren, klicken Sie auf das Kontrollkästchen neben der zugehörigen Aktion.

Update Server Firmware							
<ul> <li>Choose Firmware File</li> <li>Upload and Verify</li> </ul>	Additional Options Some firmware types have additional options that you can select.						
Additional Options							
Perform Firmware Flash	Action1:	Update the primary bank (default action) Update the backup bank	¥ ¥				
< Back Next > Finish	Cancel						

In der vorherigen Anzeige sehen Sie, dass für "Action 1" die primäre Speichergruppe zum Aktualisieren ausgewählt ist. Sie können auch auswählen, dass die Sicherungsspeichergruppe unter "Action 2" aktualisiert werden soll (wie im vorherigen Fenster dargestellt). Die primäre Speichergruppe und die Sicherungsspeichergruppe werden gleichzeitig aktualisiert, wenn Sie auf **Next** > klicken.

Anmerkung: "Action 1" muss sich von "Action 2" unterscheiden.

In einer Fortschrittsanzeige wird der Fortschritt der Firmwareaktualisierung angezeigt (wie in der folgenden Abbildung dargestellt).

Update Server Firmwa	vare							
Choose Firmware File	erform Firmware Flash •The firmware is being flashed now.							
Additional Options	Action 1 of 2: 'Update the primary bank (default action)'							
Perform Firmware Flash	Action 2 of 2: 'Update the backup bank'							
	27%							
< Back Next > Fir	inish Cancel							

Wenn die Firmwareaktualisierung erfolgreich abgeschlossen wurde, wird das folgende Fenster geöffnet. Wählen Sie die zugehörige Operation entsprechend den angezeigten Inhalten aus, um den Aktualisierungsprozess abzuschließen.



Wenn die primäre Firmwareaktualisierung nicht abgeschlossen wurde, wird das folgende Fenster geöffnet.

IBM Integrated Ma	anagement Me	odule II			USERID	Settings   Log out	IBM.
System Stat	tus Events <del>-</del>	Service and Support -	Server Management -	IMM Management - Search			
Server Firm	Ware	server components, includ	ing the IMM itself.				
Firmware Previous to take eff	update is succ are builds below imware will keep build name. ary IMM build has fect.	essful: require restart actions. Before the previous build and the tab i been updated to build 1AOO Schedule Restart A	the actions are taken, the le below still show the 19Q , and it must restart IMM colorns				
Lindata Eirmacara	1						
Update Firmware	Status	Version	Build	Release Date			
Update Firmware Firmware Type DSA	Status     Active	Version 9.24	Build DSYTA4B	Release Date 2012-08-10			
Update Firmware Firmware Type DSA IMM2	Status     Active	Version 9.24	Build DSYTA4B	Release Date 2012-08-10			
Update Firmware Firmware Type DSA IMM2 IMM2 (Primary)	Status     Active     Pendin	9.24 9.24 9 2.15	Build DSYTA4B 1A0039Q	Release Date 2012-08-10 2013-01-28			
Update Firmware Firmware Type DSA IMM2 IMM2 (Primary) IMM2 (Backup)	Status Active Pendin Inactive	9.24 9.24 9 2.15 9 2.15	Build DSYTA4B 1A0039Q 1A0039Q	Release Date 2012-08-10 2013-01-28 2013-01-28 2013-01-28			
Update Firmware Firmware Type DSA IMM2 IMM2 (Primary) IMM2 (Backup) UEFI	Status     Active     Pendin     Inactive	Version 9.24 1g 2.15 5 2.15	Build DSYTA4B 1A0039Q 1A0039Q	Release Date 2012-08-10 2013-01-28 2013-01-28			
Update Firmware Firmware Type DSA IMM2 IMM2 (Primary) IMM2 (Backup) UEFI UEFI (Primary)	Status Active Pendin Inactive Active	Version 9.24 92 2.15 2.15 1.20	Build DSYTA4B 1A0039Q 1A0039Q D7E120C95	Release Date 2012-08-10 2013-01-28 2013-01-28 2013-01-28 2013-01-28			

## **Remote Control (Fernsteuerung)**

Dieser Abschnitt enthält Informationen zur Fernsteuerungsfunktion.

Der ActiveX-Client und der Java-Client sind grafische ferne Konsolen, mit denen Sie über Fernzugriff die Anzeige des Video Viewer des Servers sehen und über Tastatur und Maus des Clients damit interagieren können.

#### Anmerkungen:

- Der ActiveX-Client ist nur zusammen mit dem Internet Explorer-Browser verfügbar.
- Zur Verwendung des Java-Clients ist das Java-Plug-in ab Version 1.5 erforderlich.
- Der Java-Client ist mit IBM Java ab Version 6 SR9 FP2 kompatibel.

Die Fernsteuerungsfunktion besteht aus zwei separaten Fenstern:

• Video Viewer (Videoanzeigefunktion)

Im Fenster "Video Viewer" wird eine ferne Konsole für die Verwaltung ferner Systeme verwendet. Bei einer fernen Konsole handelt es sich um eine interaktive Anzeige der grafischen Benutzeroberfläche (GUI) des Servers, die auf Ihrem Computer angezeigt wird. Sie sehen auf Ihrem Bildschirm genau das, was auf der Serverkonsole angezeigt wird, und Sie können die Konsole per Tastatur und Maus steuern.

• Virtual Media Session (Sitzung mit virtuellen Datenträgern)

Im Fenster "Virtual Media Session" werden alle Laufwerke auf dem Client angezeigt, die als ferne Laufwerke zugeordnet werden können. Außerdem können Sie ISO-Images und Imagedateien auf Disketten als virtuelle Laufwerke zuordnen. Jedes zugeordnete Laufwerk kann als schreibgeschützt gekennzeichnet werden. Die CD- und DVD-Laufwerke sowie die ISO-Images sind immer schreibgeschützt. Auf das Fenster "Virtual Media Session" wird über die Leiste des Menüs "Tools" (Werkzeuge) des Fensters "Video Viewer" zugegriffen.

#### Anmerkungen:

- Die Sitzung mit fernen Datenträgern kann immer nur von einem Client für Fernsteuerungssitzungen verwendet werden.
- Wenn der ActiveX-Client verwendet wird, wird ein übergeordnetes Fenster geöffnet. Dieses Fenster muss geöffnet bleiben, bis die ferne Sitzung abgeschlossen ist.

Gehen Sie wie folgt vor, um über Fernzugriff auf eine Serverkonsole zuzugreifen:

- 1. Melden Sie sich beim IMM2 an (weitere Informationen hierzu finden Sie unter "Am IMM2 anmelden" auf Seite 10).
- 2. Greifen Sie auf die Seite "Remote Control" (Fernsteuerung) zu, indem Sie eine der folgenden Menüoptionen auswählen:
  - Klicken Sie auf der Registerkarte "Server Management" auf Remote Control.
  - Klicken Sie auf der Seite "System Status" (Systemstatus) auf Remote Control....

Die Seite "Remote Control" wird geöffnet, wie in der folgenden Abbildung dargestellt.

System Status Events Service and Support Server Management MMM Management Centre  Centre  Centre  Control to server at the operating system level. A new window will appear that provides access to the Remote Disk and Remote Console functionality. The Rem Coulde for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Disk and Remote Console window, Tools' drop-down menu. (Note that the Remote Disk function does not, more) Cuice for Remote Control in single-user mode Cores of users to static remote session is achee. Remote Control Session in Progress Cuice active active active active active to disconnect one of the available sessions. Cuice for Name Active Sessions are currently consumed, you can send a request to disconnect one of the available sessions. Cuice for Name Active Sessions Cuice Acti	ІВМ	Integrated Manaç	jement Mo	dule II				USERID	Settings   Log out	IBM.
Remote Control         Allows you us control the server at the operating system level. A new window will appear that provides access to the Remote Disk and Remote Console functionality. The Rem         Cuide for Remote Disk and Remote Console window, "Tools" drop-down menu. (Note that the Remote Disk function does not, more         Cuide for Remote Disk and Remote Console         Use the ActiveX Client         Image: The Control         Image: The Control         Image: The Control image: Th	2	System Status	Events +	Service and Support -	Server Management	- IMM Management -	Search			
Use the ActiveX Client Use the Java Client Vour current browser. Java version (1.6.0.31) is supported for use with remote control.  Control for use version (1.6.0.31) is supported for use with remote control.  Allow others to request my remote session disconnect  Allow others to request my remote session disconnect  Start remote control in single-user mode) Core you exclusive access during the remote session.  Start remote control in multi-user mode) Advos other user is start remote session while your session is active.  Remote Control Session in Progress It all sessions are currently consumed, you can send a request to disconnect one of the available sessions.  Let remote control in advanced by the remote session is active.  Availability for Disconnection  It meout Va	Allow function Guide	note Cont s you to control the nality is launched for for Remote Disk ar	server at the om the Rem id Remote C	e operating system level. ote Console window, "Too Console	A new window will appea ols" drop-down menu. (No	r that provides access to de that the Remote Disk	the Remote Disk and Re function does not mor	mote Conse e	ole functionality. The I	Remote Disk
Use the Java Client  Use the Java Client  Use the Java Client  Concept disk and KVM data during transmission  Concept disk and KVM data during transmission  Allow others to request my remote session disconnect  Start remote control in single-user mode  Corres you excludee access during the remote session  Start remote control in single-user mode  Corres you excludee access during the remote session  Start remote control in single-user mode  To bus your session is active.  Remote Control Session in Progress  It all sessions are currently consumed, you can send a request to disconnect one of the available sessions.  Refreet User Name  Active Sessions  Availability for Disconnection  Timeout Va	Use	the ActiveX Clien	9		6					
Vour current browser. Java version (1.6.0.31) is supported for use with remote control.  Cherrypt disk and KVM data during transmission  Allow others to request my remote session disconnect  Start remote control in single-user mode  Cherrypt exclusive access during the remote session.  Start remote control in multi-user mode  Above other users to start remote sessions while your session is active.  Remote Control Session in Progress If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.  Vertex  Vertex  Availability for Disconnection  Timeout Va	© Use	the Java Client			R.					
	1	Your current brow	ser Java vers	ion (1.6.0.31) is supported to	or use with remote control.					
Start remote control in single-user model Gives you exclusive access during the remote session.         Start remote control in multi-user model Abors other users to start remote sessions while your session is active.         Remote Control Session in Progress         If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.         User Name       Active Sessions         Availability for Disconnection       Timeout Val	Allo	w others to reques	t my remote	session disconnect 🧟						
Carte sput addate access during the remote session.  Start remote control in multi-user mode Advess other users to start remote sessions whet your session is active.  Remote Control Session in Progress If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.  Refrest User Name  Active Sessions Availability for Disconnection Timeout Va	Start	remote control in	single-user	mode						
If all remote control in multi-user mode         Allows other users to start remote sessions with your session is active.         Remote Control Session in Progress         If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.         User Name       Active Sessions         Active Sessions       Availability for Disconnection	Gh	es you exclusive acce	is during the r	remote session.						
Advance offer User's to start remote sessions where your session is active.  Remote Control Session in Progress If all sessions are currently consumed, you can send a request to disconnectione of the available sessions.  Refress User Name Active Sessions Availability for Disconnection Timeout Va	Start	remote control in	multi-user n	node						
Remote Control Session in Progress     Refres       If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.     Refres       User Name     Active Sessions     Timeout Val	AR	ws other users to sta	t remote sess	sons while your session is act	bye.					
If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.           Refres           User Name         Active Sessions         Availability for Disconnection         Timeout Value	Rem	ote Control S	ession i	n Progress			k			
User Name Active Sessions Availability for Disconnection Timeout Va	If all se	ssions are currently	consumed,	you can send a request t	to disconnect one of the a	vailable sessions.			Re	fresh
21.5 2.5 2	User	Name		Active Sessions	5	Availal	bility for Disconnection		Timeou	rt Value
No active session is in progress.					No active s	ession is in progress.				

3. Sie können auf den Link **Guide for Remote Disk and Remote Console** (Anleitung für fernen Datenträger und ferne Konsole) klicken, um auf zusätzliche Informationen zuzugreifen. In der folgenden Abbildung ist das Fenster "Guide for Remote Disk and Remote Console" dargestellt.



- a. Klicken Sie auf **Close** (Schließen), um das Fenster "Guide for Remote Disk and Remote Console" zu verlassen.
- 4. Wählen Sie eine der folgenden Optionen der grafischen fernen Konsole aus:
  - Um den Internet Explorer als Browser zu verwenden, wählen Sie die Option **Use the ActiveX Client** (ActiveX-Client verwenden) aus.
  - Um den Java-Client zu verwenden, wählen Sie die Option Use the Java Client (Java-Client verwenden) aus, wie in der folgenden Abbildung dargestellt.

IBM	ntegrated Manaq	gement Mo	dule II			USEF	RID Settings	Log out	IBM.
2	System Status	Events +	Service and Support $\bullet$	Server Management +	IMM Management <del>-</del>	Search			
Ren Allow unction Guide	note Cont s you to control the ality is launched fr for Remote Disk ar	rol server at the om the Rem nd Remote C	e operating system level. A ote Console window, "Tool onsole	new window will appear t s" drop-down menu. (Note	hat provides access to that the Remote Disk f	the Remote Disk and Remote C unction does not more	Console function	nality. The R	emote Dis
Use	the ActiveX Clien	9							
i) Use	the Java Client 🖗		*						
10	Your current brow	vser Java vers	ion (1.6.0.31) is supported for	use with remote control.					
Allo	w others to reques	t my remote :	session disconnect						
Start	remote control in	single-user i	mode						
Giv	es you exclusive acce	ss during the r	emote session.						
Start	remote control in	multi-user m	lode						
Allo	ws other users to sta	rt remote sess	ions while your session is activ	e.					
Remo	ote Control S	ession ir	n Progress			k			
f all ses	isions are currently	consumed,	you can send a request to	disconnect one of the ava	illable sessions.			Ret	tresh
	4ame		Active Sessions		Availab	lity for Disconnection		Timeout	Value
Usern									

### Anmerkungen:

- Wenn Sie nicht den Internet Explorer-Browser verwenden, kann nur der Java-Client ausgewählt werden.
- Der ActiveX-Client und der Java-Client verfügen über dieselbe Funktionalität.

• Es wird eine Statuszeile angezeigt, der Sie entnehmen können, ob Ihr Client unterstützt wird.

Das folgende Fenster wird geöffnet. Darin werden Informationen angezeigt, die der Browser (z. B. der Firefox-Browser) zum Öffnen der Viewer-Datei verwendet.

Allows you to control the server at the operating s functionality is launched from the Remote Console	Opening viewer(192.168.5.36@443@0@135348798985 x Remote Console function hore
Guide for Remote Disk and Remote Console	You have chosen to open
Use the ActiveX Client	53487989897@0@1@1@jnlp@USERID@0@0@0@0
⊙ Use the Java Client ∅	which is a: JNLP file (3.0 KB) from: https://192.168.5.36
Your current browser Java version (1.6.0.31)	What should Firefox do with this file?
Encrypt disk and KVM data during transmission	Qpen with Browse Save Ele
Allow others to request my remote session disc	<ul> <li>Do this <u>a</u>utomatically for files like this from now on.</li> </ul>
Start remote control in single-user mode	
Gives you exclusive access during the remote session	Cancel
Start remote control in multi-user mode	

5. Nachdem der Browser die Viewer-Datei heruntergeladen und geöffnet hat, wird ein Bestätigungsfenster mit einer Warnung zur Überprüfung des Websitezertifikats angezeigt (wie in der folgenden Abbildung dargestellt). Klicken Sie auf **Yes**, um das Zertifikat zu akzeptieren.

viewer(192.168.5.3p@U Failed - 192.168.5.36	SERID@0@0@0@0) 04:56 PM		USERID	Settings   Log	a IBM.
viewer(192.168.5.3p@U 3.0 KB — 192.168.5.36	Warning - Security	×			
viewer(192.168.5.3p@U Failed — 192.168.5.36	verified. Do you want to continue?	•	pte Const	ale functionality 1	he Remote Disk
viewer(192.168.5.3p@U 3.0 KB – 192.168.5.36	Name: 192.168.5.36 Publisher: UNKNOWN			, and the second se	
Clear List	□ Always trust content from this publisher.				
Your ourrent browser Java version (1.6	The cartificate cannot be verified by a trusted	Yes No			
Encrypt disk and KVM data during transm	source.	More Information			
Start remote control in single-user mode	aisconnect ····				
Gives you exclusive access during the remote s Start remote control in multi-user mode	ession.				
Allows other users to start remote sessions wh	le your session is active.				

- 6. Um den Server über Fernzugriff zu steuern, wählen Sie eine der folgenden Menüoptionen aus:
  - Um während der Sitzung über exklusiven Fernzugriff zu verfügen, klicken Sie auf **Start remote control in single User mode** (Fernsteuerung im Einzelbenutzermodus starten).
  - Um zuzulassen, dass während Ihrer Sitzung auch andere Personen Zugriff auf die ferne Konsole haben, klicken Sie auf **Start remote control in multi user mode** (Fernsteuerung im Mehrbenutzermodus starten).

Anmerkung: Wenn vor dem Öffnen des Fensters "Video Viewer" das Kontrollkästchen Encrypt disk and KVM data during transmission (Datenträgerund KVM-Daten während der Übertragung verschlüsseln) ausgewählt wurde, werden die Datenträgerdaten während der Sitzung mit ADES verschlüsselt.

Das Fenster "Video Viewer" wird geöffnet (wie in der folgenden Abbildung dargestellt). Das Fenster bietet Zugriff auf die Funktion "Remote Console".



7. Schließen Sie die Fenster "Video Viewer" und das Fenster "Virtual Media Session", wenn Sie mit dem Verwenden der Funktion "Remote Control" fertig sind.

### Anmerkungen:

- Das Fenster "Video Viewer" schließt automatisch das Fenster "Virtual Media Session".
- Schließen Sie das Fenster "Virtual Media Session" *nicht*, wenn derzeit ein ferner Datenträger zugeordnet ist. Informationen zum Schließen und zum Trennen der Zuordnung eines fernen Datenträgers finden Sie im Abschnitt, Ferner Datenträger" auf Seite 119.
- Wenn beim Verwenden der Fernsteuerungsfunktion Probleme mit der Maus oder der Tastatur auftreten, finden Sie hierzu Hilfe auf der Seite "Remote Control" in der Webschnittstelle.
- Wenn Sie die ferne Konsole dazu verwenden, im Konfigurationsdienstprogramm Einstellungen des IMM2 zu ändern, kann es sein, dass der Server das IMM2 erneut startet. Die Verbindung zur fernen Konsole und die Anmeldesitzung werden abgebrochen. Nach einer kurzen Verzögerung können Sie sich mit einer neuen Sitzung erneut am IMM2 anmelden, die ferne Konsole erneut starten und das Konfigurationsdienstprogramm verlassen.

Wichtig: Das IMM2 verwendet ein Java-Applet oder ein ActiveX-Applet, um die Remote-Presence-Funktion auszuführen. Wenn das IMM2 auf die neueste Firmwareversion aktualisiert wird, werden auch das Java-Applet und das ActiveX-Applet auf die neueste Version aktualisiert. Java stellt zuvor verwendete Applets standardmäßig in den örtlichen Zwischenspeicher. Nach einer Flashaktualisierung der IMM2-Firmware ist das vom Server verwendete Java-Applet möglicherweise nicht auf dem neuesten Stand.

Um diesen Fehler zu beheben, inaktivieren Sie das Zwischenspeichern. Welche Methode verwendet wird, hängt von der Plattform und von der Java-Version ab. Die folgenden Schritte gelten für Oracle Java 1.5 unter Windows:

- Klicken Sie auf Start → Settings (Einstellungen) → Control Panel (Steuerkonsole).
- 2. Klicken Sie zweimal auf Java Plug-in 1.5. Das Fenster "Control Panel" des Java-Plug-in wird geöffnet.
- 3. Klicken Sie auf die Registerkarte Cache (Zwischenspeicher).
- 4. Wählen Sie eine der folgenden Optionen:

- Wählen Sie das Kontrollkästchen Enable Caching (Zwischenspeichern aktivieren) ab, damit die Java-Zwischenspeicherung immer inaktiviert ist.
- Klicken Sie auf Clear Caching (Zwischenspeichern abwählen). Wenn Sie diese Option wählen, müssen Sie nach jeder IMM2-Firmwareaktualisierung auf Clear Caching klicken.

Weitere Informationen zur Aktualisierung von IMM2-Firmware finden Sie im Abschnitt "Server-Firmware aktualisieren" auf Seite 122.

Weitere Informationen zum Verwenden der Fernsteuerungsfunktion finden Sie unter "Remote-Presence- und Fernsteuerungsfunktionen" auf Seite 107.

### Server Properties (Servereigenschaften)

Wenn Sie die Option **Server Properties** (Servereigenschaften) auf der Registerkarte "Server Management" auswählen, wird das folgende Fenster angezeigt. Mit dieser Option können Sie verschiedene Parameter zur Identifizierung des Systems festlegen. Dazu gehören ein beschreibender Name, ein Ansprechpartner, ein Standort usw. Die Informationen, die Sie in diese Felder eingeben, werden wirksam, wenn Sie auf **Apply** (Übernehmen) klicken. Wenn Sie die Informationen löschen möchten, die seit dem letzten Übernehmen von Änderungen eingegeben wurden, klicken Sie auf **Reset** (Zurücksetzen).

IBM Integrated Management Module II	USERID	Settings   Log out	IBM.
System Status Events • Service and Support • Server Management • 3MM Management • Search			
Server Properties Vinous properties, status and settings related to your system. (Root) Reset.			
General Settings LEDs Hardware Information Environmentals Hardware Activity			
General Settings			
Provide information which identifies this system to operations and support personnel.			
System descriptive name: 🖗			
Contact person: 🖗			
Location (ste, geographical coordinates, etc):			
Room ID: 10			
Rack (D): @			
Lowest unt of system: W			
U height of system: 0			

In der folgenden Abbildung können Sie die niedrigste Einheit des Systems (**Lowest unit of the system**) angeben. Für das Feld **Lowest unit of the system** ist eine Verbindung zum Managementmodul (z. B. Advanced Management Module oder CMM) erforderlich.

w megraceu wasagement wounte n	USERID Settings   Log out IB]
System Status Events + Service and Support + Server Management + IMM Management + Search	
rver Properties us properties, status and settings related to your system. of: Reset	
neral Settings LEDs Hardware Information Environmentals Hardware Activity	
eneral Settings	
wide information which identifies this system to operations and support personnel.	
tem descriptive name: 19	
ntact person: 🖗	
Re, geographical coordinates, etc): 🖗	
W t of systems () A · · ·	

Um die Systemanzeigen anzuzeigen, klicken Sie auf die Registerkarte LED. Das folgende Fenster wird geöffnet.

IBM Integrated N	Manageme	ent Module II		USERID Settings   Log out IBM.
System St	tatus Eve	nts - Service and Suppr	rt • Server Management • IMM Management • Starch	
Server Pro Various properties, s Apply Reset	perties	S ettings related to your syst	en.	
General Settings	LEDs	Hardware Information	Environmentals Hardware Activity	
LEDs.				
Check Log LED: Of	f	ange		
Name	<ul> <li>Color</li> </ul>	Status		
100bit Slot	YEROW	Vor		
Battery	Tesow	Vor		
Check Log	Greens	U Bank		
Chied Log	Nulleum	Con		
CRU	Vellow	Cor		
CPU1	Vellow	Cor		
CPU 2	Yellow	2 or		
CPU 3	Yellow	2 of		
CPU 4	Yellow	Corr		
CPU Tray Err	Vellow	?or		
DASD	Yellow	0 off		

Um Informationen zum System, zu Systemkomponenten und zur Netzhardware anzuzeigen, klicken Sie auf die Registerkarte **Hardware Information** (Hardware-Informationen). Wählen Sie die entsprechende Registerkarte auf der Registerkarte "Hardware Information" aus, um verschiedene Informationen zu elementaren Produktdaten anzuzeigen. Die Registerkarte **System Information** (Systeminformationen) bietet Informationen wie den Maschinennamen, die Seriennummer und das Modell. In der folgenden Abbildung ist das Fenster "System Information" dargestellt.

IBM Integrated Management	Module II						USERID	Settings   Log out	IBM.
System Status Event	<ul> <li>Service and Support</li> </ul>	t • Server Nanagement	- JMM Ma	nagement + 🤇	earch ( )				
erver Properties, arous properties, status and sett Apply Reset	ings related to your syste	m.							
General Settings LEDs	Hardware Information	Environmentals Hardwar	e Activity						
This section lists vital product da System Information System (	a (VPD) on a system, co component information	nponent and network basis Network Hardware							
Name	Value								
Machine Name	System x	1750 M4							
Machine Type	8722								
	1.00.0								
Model	AC1								
Model Serial Number	AC1 23D4895								
Nodel Serial Number UUID	AC1 23D4895 9AC5F5A	141D211E192CAE41F13D4	09AA						
Model Serial Number UUID Server Power	23D4895 8AC5F5A On	341D211E192CAE41F13D/	09AA						
Nodel Senal Number UUID Server Power Server State	AC1 23D4895 9AC5F5A On OS boote	841D211E192CAE41F13D/	0944						
Model Serial Number UUID Server Power Server State Total hours powered-on	AC1 23D4895 9AC5F5A On OS boote 5	841D211E182CAE41F13DA 1	09AA						
Nodel Senial Number UUID Server Power Server State Total hours powered-on Restart count	AC1 23D4895 9AC5F5A On OS boote 5	341D211E192CAE41F13DA 8	09AA						
Model Senial Number UUID Server Power Server State Total hours powered-on Restart count Ambient Temperature	AC1 23D4895 9AC5F5A On OS boote 5 7B.80 F //	941D211E192CAE41F13D/ 9 16.00 C	09AA						
Nodel Senial Number UUID Server Power Berver State Total hours powered-on Restart count Ambient Tamperature Enclosure Identify LED	AC1 23D4894 BAC5F5A On OS boote 5 78.80 F / Off Chan	941D211E192CAE41F13D4 8 16.00 C 6	09AA						

Der Status der Gehäuse-ID-Anzeige (**Enclosure Identify LED**) kann über das Fenster "System Information" angezeigt und geändert werden. Um die Einstellung für **Enclosure Identify LED** zu ändern, klicken Sie auf den Link **Change...** (Ändern). Das folgende Fenster wird geöffnet.

**Anmerkung:** Die Anzeige "Enclosure Identity" befindet sich an der Vorderseite des Diagnosefelds "Light Path Diagnostics".

Choose the desired state for the Enclosure Identify LED	
The Location LED is on the front of the Light Path panel. It is Identify in the LED table.	called
Note: The system might need to be powered on for the Locat to turn on or blink.	tion LED
Current state: Off	
Turn Off	
Turn On     Blink	

Wählen Sie die Registerkarte **System Component Information** (Informationen zu Systemkomponenten) aus, um Informationen zu Komponenten anzuzeigen. Zu den Informationen zu den Komponenten gehören der Name der FRU, die Seriennummer, die Hersteller-ID und das Herstellungsdatum. In der folgenden Abbildung sehen Sie die Informationen, die angezeigt werden, wenn Sie auf die Registerkarte **System Component Information** klicken.

-	ment Module II				USERID	Settings   Log out	IBM
System Status	Events - Service and	d Support - Server Mana	igement + IMM Management	Search			
erver Proper ious properties, status ar pply Reset	ties id settings related to you	ur system.					
eneral Settings LEI Hardware Info	Hardware Inform Drmation uct data (VPD) on a syst	tem, component and networ	Hardware Activity k basis.				
And Ware Info Hardware Info his section lists vital prod System Information	Dis Hardware Inform Distance of the second	tem, component and networ attory Network Hardware	Hardware Activity k basis.				
Antipation of the section lists vital prod System Information System Information System CPU 1	Hardware Inform Dermation uct data (VPD) on a syst stem Component Inform Serial Number Not Available	tem, component and networ attor: Network Hardware Manufacturer ID Intel(R) Corporation	Hardware Activity k basis. Manufacturer Date Not Available				
eneral Settings LEI Hardware Infe his section lists vital prod System Information Sy FRU Name CPU 1 DASD Backplane 1	Hardware Inform A A A A A A A A A A A A A A A A A A A	tem, component and networ attors Network Hardware Manufacturer ID Intel(R) Corporation USIS	Hardware Activity k basis. Manutacturer Date Not Available 1996-01				
Anter a settings LEI LEI LEI LEI LEI LEI LEI LEI	Ardware Inform Ardware Inform	aation Environmentals tem, component and networ aator: Network Hardware Manufacturer ID Intel(), corporation USIS Hynik Semiconductor	Hardware Activity k basis. Manufacturer Date Not Available 1996-01-01 2012-10-15				
An eneral Settings LEI LEI Hardware Info his section lists vital prod System Information FRU Name CPU 1 DASD Backplane 1 DIMM 1 Power Supply 1	Ardware Inform Ardware Information Ardware Inform Ardware I	tem, component and network attori Network Hardware Manufacturer ID Intel(R) Corporation USIS Hynix Semiconductor ACBE	Hardware Activity k basis. Manutacturer Date Not Available 1996-01-01 2921-210-15 1996-01-01				

Wählen Sie die Registerkarte **Network Hardware** (Netzhardware) aus, um Informationen zur Netzhardware anzuzeigen. Zu den Informationen zur Netzhardware gehören die Host-Ethernet-MAC-Adressnummer und -MAC-Adresse. In der folgenden Abbildung sehen Sie die Informationen, die angezeigt werden, wenn Sie auf die Registerkarte "Network Hardware" klicken.

IBM Integrated Management	Module II					USERID	Settings   Log out	IBM.
System Status Event	s      Service and Suppo	ort 👻 Server Man	agement 🗸 🛛 IMM Ma	nagement 🕶 🔄	arch	]		
Server Properties Various properties, status and setti Apply Reset	ings related to your system	m. <b>k</b>						
General Settings LEDs	Hardware Information	Environmentals	Hardware Activity					
Host Ethernet MAC Address 1	ta (VPD) on a system, co Component Information ( Number <u>MAC</u> .	Network Hardware Address	ITK DASIS.					
Host Ethernet MAC Address 2	5C:F3	FC:3C:13:D1						
Host Ethernet MAC Address 3	5C:F3	FC:3C:13:D2						
Host Ethernet MAC Address 4	5C:F3	FC:3C:13:D3						

Wählen Sie die Registerkarte **Environmentals** (Umgebungsdaten) auf der Seite "Server Properties" (Servereigenschaften) aus, um die Spannungs- und Temperaturwerte der Hardwarekomponenten im System anzuzeigen. Das folgende Fenster wird geöffnet. In der Spalte **Status** der Tabelle werden entweder der normale Betrieb oder Problembereiche im Server angezeigt.

System Sta	stus Events + S	ervice and Support +	Server Manageme	nt • IMM Manageme	nt +   Search. L .					
erver Prop rious properties, st hooly Reset	Derties atus and settings reli	ited to your system.								
Seneral Settings	LEDs Hardw	are Information En	vironmentals Hard	ware Activity						
Invironme	antals									
	entats									
is section displays	s the current voltage	and temperature rea	dings for various hard	ware components in th	is system. All voltage rea	adings are displayed in	Volta. All temperatu	ire readings are	displayed in degrees	
titerines at aregin	the prost ashering	an Isai assessin								
oltages										
Ehour Threshold	5.00									
S anone suscention										
Source	Value (Volts)	Status	Fatal Lower Threshold	Critical Lower Threshold	Non-critical Lower Threshold	Non-critical Upper Threshold	Critical Upper Threshold	Fatal Upper Threshold		
Source Planar 3.3V	Value (Volts) 3.39	Status	Fatal Lower Threshold N/A	Critical Lower Threshold 3.04	Non-critical Lower Threshold	Non-critical Upper Threshold	Critical Upper Threshold 3.55	Fatal Upper Threshold NIA	r	
Planar 3.3V Planar 5V	Value (Volts) 3.39 5.08	Status Status Normal Normal	Fatal Lower Threshold N/A N/A	Critical Lower Threshold 3.04 4.44	Non-critical Lower Threshold N/A N/A	Non-critical Upper Threshold N/A N/A	Critical Upper Threshold 3.56 5.53	Fatal Upper Threshold NIA NIA	r	
Planar 3.3V Planar 5V Planar 12V	Value (Volta) 3.39 5.08 12.26	Status  Normal  Normal  Normal  Normal	Fatal Lower Threshold N/A N/A N/A	Critical Lower Threshold 3.04 4.44 10.96	Non-critical Lower Threshold NUA NUA NUA	Non-critical Upper Threshold N/A N/A N/A	Critical Upper Threshold 3.56 5.53 13.23	Fatal Upper Threshold NIA NIA NIA	-	
Planar 3.3V Planar 5V Planar 5V Planar 12V Planar VBAT	Value (Volts) 3.39 5.08 12.26 3.20	Status Status Normal Stormal Normal Normal Normal	Fatal Lower Threshold N/A N/A N/A N/A	Critical Lower Threshold 3.04 4.44 10.96 2.00	Non-ontical Lower Threshold NIA NIA NIA 2.27	Non-critical Upper Threshold N/A N/A N/A N/A	Critical Upper Threshold 3.56 5.53 13.23 N/A	Fatal Upper Threshold NIA NIA NIA NIA		
Planar 3.3V Planar 3.3V Planar 5V Planar 12V Planar VBAT	Value (Volts) 3.39 5.08 12.26 3.20	Status Normal Normal Normal	Fatal Lower Threshold Na%, Na%, Pa%, Na%,	Critical Lower Threshold 3.04 4.44 10.96 2.00	Non-ontical Lower Threshold NA NA NA 2.27	Non-critical Upper Threshold N/A N/A N/A N/A	Critical Upper Threshold 3.56 5.53 13.23 N/A	Fatal Upper Threshold NIA NIA NIA NIA NIA		,
Planar 3.3V Planar 3.3V Planar 5V Planar 12V Planar VBAT	Value (Volts) 3.39 5.08 12.26 3.20	Status Normal Normal Normal	Fatal Lower Threahold NAA SalA SalA SalA SalA NAA	Critical Lower Threshold 3.04 4.44 10.96 2.00	Non-ortical Lower Threshold NUA NUA NUA 2.27	Non-critical Upper Threshold NA NA NA NA	Critical Upper Threshold 3.56 5.53 13.23 NIA	Fatal Upper Threshold NiA NiA NiA NiA NiA	r	
Planar 3.3V Planar 5V Planar 12V Planar VBAT	Value (Volts) 3.39 5.08 12.26 3.20	Status Normal Normal Normal	Fatal Lower Threshold NA NA NA NA	Critical Lower Threshold 3.04 4.44 10.96 2.00	Non-critical Lower Threshold NUA NUA NUA 2.27	Non-critical Upper Threshold NAA NAA NAA NAA	Critical Upper Threshold 3.56 5.53 13.23 NIA	Fatal Upper Threshold NiA NiA NiA NiA NiA	r	
Planar 3.3V Planar 5V Planar 12V Planar VBAT	Value (Volts) 3.39 5.08 12.26 3.20	Status Normal Normal Normal	Fatal Lower Threshold PalA PalA PalA PalA PalA	Critical Lower Threshold 3.04 4.44 10.96 2.00	Non-ortical Lower Threshold NUA NUA NUA 2.27	Non-critical Upper Threshold NA NA NA NA NA	Critical Upper Threshold 3.56 5.53 13.23 NIA	Fatal Upper Threshold NIA NIA NIA NIA NIA	r	
Planar 3.3V Planar 3.3V Planar 5V Planar 12V Planar VBAT Comperature 2 Show Threshold Source	Value (Volts) 3.39 5.06 12.26 3.20 S Value (* F)	Status Normal Normal Normal Normal Status	Fatal Lower Threahold SAA SAA SAA SAA SAA SAA Fatal Lower	Critical Lower	Non-critical Lower Threshold NUA NUA 2.27	Non-critical Upper Threshold NaA NaA NaA NaA NaA NaA	Critical Upper Threshold 3.55 5.53 13.23 NIA Critical Upper	Fatal Upper Threshold NiA NiA NiA NiA NiA Fatal Upper		2
Planar 3.3V Planar 3.3V Planar 5V Planar 12V Planar VBAT Planar VBAT Show Threshold Source	Value (Vofts) 3.39 5.08 12.26 3.20 S Value (*F)	Status Normal Normal Normal Normal Status	Fatal Lower Threahold NNA NNA NNA NNA NNA Fatal Lower Threahold	Critical Lower Threshold 3.04 4.44 10.96 2.00 Critical Lower Threshold	Non-ortical Lower Threshold NUA NUA NUA 2.27 Non-ortical Lower Threshold	Non-critical Upper Threshold NiA NiA NiA NiA NiA NiA NiA NiA NiA NiA	Critical Upper Threshold 3.55 5.53 13.23 NiA Critical Upper Threshold	Fatal Upper Threshold NUA NUA NUA NUA Fatal Upper Threshold		
Planar 3.3V Planar 3.3V Planar 5V Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar SV Planar 3.3V Planar 3.3V Planar 3.3V Planar 3.3V Planar 3.3V Planar 3.3V Planar 5V Planar 5V Plan	Value (Volta) 3.39 5.08 12.28 3.20 5 5 Value (* F) 78.80	Status Status Normal Normal Normal Status Status Normal	Fatal Lower Threahold Naik Naik Naik Naik Fatal Lower Threahold Naik	Critical Lower Threshold 3.34 4.44 10.96 2.00 Critical Lower Threshold NeA	Non-ortical Lower Threshold NA NA NA 227 Non-ortical Lower Threshold NA	Non-onfical Upper Threshold NA NA NA NA NA NA NA NA NA NA	Critical Upper Threshold 3.56 5.53 13.23 N/A Critical Upper Threshold 114.80	Fatal Upper Threshold NIA NIA NIA NIA NIA NIA Fatal Upper Threshold 122.00		
Planar 3.3V Planar 3.3V Planar 5V Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar VBAT Planar SV Planar 3.3V Planar 3.2V Planar 5V Planar 5V Pl	Value (Volts) 3.39 5.08 12.26 3.20 S Value (*F) 70.80 NIA	Status Status Normal Normal Status Normal Na Normal NA	Fatal Lower Threahold Nik Nik Nik Nik Fatal Lower Threahold Nik Nik	Critical Lower Threshold 3.04 4.44 10.96 2.00 Critical Lower Threshold Nik	Non-ortical Lower Threshold NA NA 2.27 Non-ortical Lower Threshold NA NA	Non-critical Upper Threshold NA NA NA NA NA NA Non-critical Upper Threshold 109.40 NA	Critical Upper Threshold 3.56 5.53 13.23 N/A Critical Upper Threshold 114.40 N/A	Fatal Upper Threshold NIA NIA NIA NIA Fatal Upper Threshold 122.00 NIA		

Die Registerkarte **Hardware Activity** (Hardware-Aktivität) auf der Seite "Servereigenschaften" enthält den Verlauf der zum System hinzugefügten oder vom System entfernten Hardware. In der folgenden Abbildung sehen Sie die Informationen, die angezeigt werden, wenn Sie auf die Registerkarte "Hardware Activity" klicken.

IBM Integrated Man	agement Module II					USERID	Settings   Log out	IBM
System Status	Events + Service and	d Support • Server Mana	igement + DHH Han	agement + (Search	1			
Server Prope Various properties, statur Apple (Reset	rties s and settings related to yo	our system.						
General Settings	LEDs Hardware Inform	mation Environmentals	Hardware Activity					
This table contains a his FRU Name	story of Field Replacable Ur Serial Number	nt (FRU) components whic Manufacturer ID CI CN	h have been added to Action	Time of Action				
on one-man read			Contraction of the second seco					
Power Supply 1	K10511BE086	Detta	BP Added	19 Jul 2012 00:12 AM				
Power Supply 1 Power Supply 2	K10511BE086 K10511BE00F	Delta Delta	Added	19 Jul 2012 00:12 AM 19 Jul 2012 00:12 AM				
Power Supply 1 Power Supply 2 SAS Backplane 1	K10511BE006 K10511BE00F Y011US15G98C	Delta Delta MOLX	Added BP Added	19 Jul 2012 09 12 AM 19 Jul 2012 09 12 AM 19 Jul 2012 09 12 AM				
Power Supply 1 Power Supply 2 SAS Backplane 1 CPU 1	K10511BE006 K10511BE00F Y011US15G9BC Not Available	Detta Detta MOLX Intel(R) Corporation	Added	19 Jul 2012 00 12 AM 19 Jul 2012 00 12 AM				
Fower Supply 1 Power Supply 2 SAS Backplane 1 CPU 1 CPU 2	K10511BE086 K10511BE00F V011US15G98C Not Available Not Available	Delta Delta MOLX Intel(R) Corporation Intel(R) Corporation	Added Added Added Added Added	19 Jul 2012 00:12 AM 19 Jul 2012 00:12 AM				
Power Supply 1 Power Supply 2 SAS Backplane 1 CPU 1 CPU 2 CPU 3	K105118E086 K105118E00F Y011US15G98C Not Available Not Available Not Available	Delta Delta MOLX Intel(R) Corporation Intel(R) Corporation Intel(R) Corporation	Added Added Added Added Added Added	19 Jul 2012 00 12 00 12 AM 19 Jul 2012 09 12 AM 19 Jul 2012 09 12 AM				

## Server Power Actions (Serverstromversorgungsaktionen)

Dieser Abschnitt enthält Informationen zur Option "Server Power Actions" (Serverstromversorgungsaktionen) auf der Registerkarte "Server Management" auf der Homepage der IMM2-Webschnittstelle.

Wählen Sie die Option **Server Power Actions** auf der Registerkarte "Server Management" aus, um eine Liste der Aktionen anzuzeigen, die Sie zum Steuern der Stromversorgung des Servers verwenden können. In der folgenden Abbildung ist ein Beispiel für das Fenster "Server Power Actions" dargestellt.

IBM Integrated Management Module II	USERID	Settings   Log out	IBM.
System Status Events • Service and Support • Server Management • DMM Management • Search			
Server Actions Current server power state: ON Actors Parent On Server al Specified Date and Time Parent Of Server al Specified Date and Time Parent Of Server tamondary			
Shat down OS and then Power OF Server Shat down OS and then Restart Server Restart the Server with Neo semiability Kernegit (MM) Scheduk Dally Workely Power and Informat Actions			

Sie können auswählen, dass der Server sofort oder zu einem geplanten Zeitpunkt eingeschaltet wird. Sie können auch auswählen, dass das Betriebssystem heruntergefahren und erneut gestartet wird. Weitere Informationen zum Steuern der Stromversorgung des Servers finden Sie unter "Stromversorgungsstatus des Servers steuern" auf Seite 106.

## **Disks (Platten)**

Wählen Sie die Option **Disks** (Platten) auf der Registerkarte "Server Management" (Serververwaltung) aus, um die Festplattenlaufwerke im System anzuzeigen. Die folgende Anzeige wird eingeblendet. Klicken Sie auf ein Festplattenlaufwerk, um die dem Festplattenlaufwerk zugeordneten Ereignisse anzuzeigen.

IBM Integrated M	anagement Mod	ule II					SERID	Settings   Log out	IBM.
System Stat	tus Events •	Service and Support +	Server Management +	IMM Management +	Starch				
Hard Disks Display hard disk driver FRU Name	s in the system. Gi Status	ck on a drive to see activ	ve events.						
Disk 0	Normal								
Disk 1	Normal								

# **Memory (Speicher)**

Wählen Sie auf der Registerkarte "Server Management" die Option **Memory** (Speicher) aus, um Informationen zu den im System installierten Speichermodulen anzuzeigen. Das folgende Fenster wird geöffnet. In der Tabelle wird jedes Speichermodul als Link angezeigt, auf den Sie klicken können, um ausführlichere Informationen zu dem betreffenden Speichermodul abzufragen. In der Tabelle werden außerdem der Status des DIMM, der DIMM-Typ und die DIMM-Kapazität angezeigt.

**Anmerkung:** Wenn Sie ein DIMM entfernen oder ersetzen, müssen Sie das System erneut starten, um die aktualisierten DIMM-Informationen zu den Änderungen anzuzeigen, die Sie an den System-DIMMs vorgenommen haben.

IBM Integrated Man	agement Module					USERID	Settings   Log out	IB
System Statu	s Events • Sen	vice and Support + Server I	Aanagement + IMM Management	• Search				
Homony								
Display the memory mod once after the removal	dules available on the replacement to show	e server. Clicking on a module of the correct DIMM information	Ssplays a Properties pop-up window n.	with 2 tabs: Events, HW Info. If	you remove or replace DBMMs,	the server	needs to be powered o	n at les
FRU Name +	Status	Type	Capacity (GB)					
DIMM 1	Normal	DDR3	8					
DIMM 2	Normal	DDR3	8					
DIMM 3	Normal	DOR3	8					
DIMM 4	Normal	DOR3	8					
DHMM 5	Normal	DOR3	8					
DIMM 6	Normal	DOR3	8					
DIMM 7	Normal	DOR3	8					
DIMM 8	Normal	DOR3	8					
DIMM 9	Normal	DOR3	0					
DIMM 10	Normal	DOR3	8					
DIMM 11	Normal	DOR3	8					
DIMM 12	Normal	DOR3	8					
DIMM 13	Normal	DDR3	4					
DIMM 14	Normal	DOR3	4					
DIMM 15	14ormal	DDR3	4					
DIMM 16	Normal	DOR3	4					
DIMM 17	Normal	DDR3	4					
DIMM 18	Normal	DOR3	4					
DIMM 19	Normal	DOR3	4					
DIMM 20	Normal	DOR3	4					
DIMM 21	Normal	DOR3	4					

Klicken Sie in der Tabelle auf den Link zu einem **DIMM**, um die aktiven Ereignisse und weitere Informationen zu der Komponente anzuzeigen (wie in der folgenden Abbildung dargestellt).

							-
System :	itatus Events • Sen	vice and Support + Server I	terapement +DMM Management +Starshill				1
Memory Deplay the memory	modules available on the	e serves. Clicking on a module i	inplays a Properties pop-up window with 2 table: Events	a, HW Info, If you remove or replace DDHHs, the server need	i to be powered a	n at least	
FRU Name	* Properties for	DIMM 3			x		
DIMAN 1							
DIMM 2		Manda an Information					
DIMM 3	There are a	riardware unormation					
DIMM 4	inere are n	o active events for this de	ice		-		
Dama 5	Close						
DIMM 6							
DIMM 7	_						
DIMM 8	_						
DHMM 0	_						
DIMM 10							
DIMM 11	_						
DIVM 12							
DIMM 13							
DIVM 14							
DRMM 15		10 M 10					
DIVIN 18	2 Kormal	DDR3	4				
DIMM 17	Piormal	DOR3	4				
DIMM 18	Normal	DDR3	4				
Davis 19	Normal	DDR3	4				
DIMM 20	formak 🖾	DORG	4				
Dillina 21	2 Normal	DOR3	4.				1

Klicken Sie auf die Registerkarte **Hardware Information**, um Details zu der betreffenden Komponente anzuzeigen, wie z. B. Beschreibung, Teilenummer, FRU-Seriennummer, Produktionsdatum (Woche/Jahr), Typ (z. B. DDR3) und Größe in Gigabyte (wie in der folgenden Abbildung dargestellt).

IBM Integrated M	anagement Module II						USERID			IBM.
System Sta	tux Erenta - Service and	Support + Server M	tanägement + 2414 Manaj	pement + 🕞						
Memory Display the memory in once after the remov	odules available on the server. a/replacement to show the co	Clicking on a module d nect 0944 informatio	isplays a Properties pop-up i N	window with 2	taba: Eventa, HW Info	3° you remove or replace (	DHMs, the serve	r needs to b	e powered o	in at least
FRU Name	Properties for DIMM							×		
DRM 1										
CRIM 2 CRIMI 3	Events Hardwa	are Information								
DIMM 4	Description	DEMM 3								
DIMITS	FRU Serial Number	18553028	-119							
DIVIN 6	Manuf Date	3611								
DIMM 7	Size	8 GB								
CHUIK B	1.000									
Dimit a	Close									
CHMM 10	-									
DIMM 11										
DIMM 12										
DIMM 13										
DIMM 14										
DMM 15		Sector 1 Mag								
DIMM 16	2 Normal	DOR3	4							
DIMM 17	liemoi 4	DDR3	4							
DIMM 18	2 Vormal	DORO	4							
DIMM 19	Ploimal	DOR3	4							
DIMM 20	Normal	DDR3	4							
Dillin 21	2 tormal	DORS	4							

# **Processors (Prozessoren)**

Wählen Sie die Option **Processors** (Prozessoren) auf der Registerkarte "Server Management" (Serververwaltung) aus, um Informationen zu den im System installierten Mikroprozessoren anzuzeigen. Das folgende Fenster wird geöffnet.

IBM Integrated Mar	nagement Me	odule II					USERID	Settings   Log out	IBM.
System Statu	n Events •	Service and Support $\star$	Server Management +	3	NN Management + Search c.	ł			
CPUs Display the processors a	available on the	server. Clicking on a CPU d	isplays a Properties pop-u	up w	endow with 2 tabs: Events, HW Info.				
CPU 1 Status	Normal	2.20							
CPU 2 Status	Normal	2.20							
CPU 3 Status	Normal	2.20							
CPU 4 Status	Normal	2.20							

Klicken Sie auf einen der **CPU**-Links in der Tabelle, um aktive Ereignisse sowie weitere Informationen zur Komponente anzuzeigen (wie in der folgenden Abbildung dargestellt).

18M Integrate	d Managemi	eet Module II	USERID Ser		IBM
System	Status Eve	nts + - Service and Support + - Service Management +			
CPUS Display the proces FRU Name	nors available Status	In the server. Colong on a CPU deplays a Properties pap-up window with 2 table. Events, HW Info. Disolution (dott) mai 2 20			
CPU 2 Status	Properties fi	or CPU 1 Status		ж	
CPU 3 Status					
CPU 4 Status	Events	Hardware Information			
	There are	no active events for this device			
(	Close				
<u> </u>					

Klicken Sie auf die Registerkarte **Hardware Information** (Hardwareinformationen), um Details zur Komponente, wie z. B. den Namen der FRU (Field-Replaceable Unit, durch den Kundendienst austauschbare Funktionseinheit) und die Hersteller-ID anzuzeigen (wie in der folgenden Abbildung dargestellt).

IBM Integrated Management Module II		
System Statum Events + Service and Support + Server Hanagement + 1994 Hanagement + Service		
CPUS Display the processors available on the server. Globing on a CPU displays a Properties pop-up window with 2 fabric Events, HW lafe. FRU Name		
CPU2 Shine Properties for CPU 1 Status	ж	
CPU 3 Status CPU 4 Status FRU Name CPU 1 Status Manufacturer ID Intel(R) Corporation		

## Server Timeouts (Serverzeitlimits)

Wählen Sie die Option **Server Timeouts** (Zeitlimits für den Server) auf der Registerkarte "Server Management" (Serververwaltung) aus, um Zeitlimits festzulegen, die sicherstellen, dass das System bei einer Firmwareaktualisierung oder beim Einschalten nicht auf unabsehbare Zeit hin blockiert wird. Sie können diese Funktion aktivieren, indem Sie die Werte für die Optionen festlegen.

**Anmerkung:** Bei Serverzeitlimits muss die Inband-USB-Schnittstelle (oder LAN over USB) aktiviert sein, damit Befehle verwendet werden können. Weitere Informationen zum Konfigurieren der USB-Schnittstelle finden Sie unter "USB konfigurieren" auf Seite 84.

In der folgenden Abbildung ist das Fenster "Server Timeouts" dargestellt.



Weitere Informationen zu Zeitlimits für Server finden Sie unter "Serverzeitlimits festlegen" auf Seite 58.

## PXE Network Boot (PXE-Netzboot)

Wählen Sie die Option **PXE Network Boot** (PXE-Netzboot) auf der Registerkarte "Server Management" (Serververwaltung) aus, um den Server so zu konfigurieren, dass beim nächsten Neustart des Servers versucht wird, einen PXE-Netzboot durchzuführen. Weitere Informationen zum Konfigurieren eines PXE-Netzboots finden Sie unter "PXE-Netzboot einrichten" auf Seite 121.

# Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige)

Wählen Sie auf der Registerkarte "Server Management" die Option Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige) aus, um die Daten zur neuesten Betriebssystem-Fehleranzeige, die vom IMM2 gespeichert wurde, anzuzeigen oder zu löschen. Das IMM2 speichert nur die Informationen zu den aktuellsten Fehlerereignissen und überschreibt die Daten früherer Betriebssystem-Fehleranzeigen, wenn ein neues Fehlerereignis auftritt.

In der folgenden Abbildung ist ein Beispiel für die Betriebssystem-Fehleranzeige dargestellt.



Weitere Informationen zur Option "Latest OS Failure Screen" finden Sie im Abschnitt "Daten der letzten Betriebssystem-Fehleranzeige erfassen" auf Seite 136.

## Registerkarte "IMM Management" (IMM-Verwaltung)

Dieser Abschnitt enthält Informationen zu den Optionen auf der Registerkarte "IMM Management" auf der Homepage der IMM2-Webbenutzerschnittstelle.

Die Optionen auf der Registerkarte "IMM Management" ermöglichen Ihnen das Anzeigen und Ändern der IMM2-Einstellungen. Eine Liste der Optionen und ausführliche Informationen zur Verwendung dieser Optionen zum Konfigurieren des IMM2 finden Sie in Kapitel 4, "IMM2 konfigurieren", auf Seite 55.

# Kapitel 4. IMM2 konfigurieren

Die Registerkarte "IMM Management" enthält Optionen zum Konfigurieren des IMM2. Verwenden Sie die Registerkarte "IMM Management", um Einstellungen des IMM2 anzuzeigen und zu ändern. Die folgenden Optionen sind auf der Registerkarte "IMM Management" aufgeführt (wie in der folgenden Abbildung dargestellt).

- IMM Properties (IMM-Eigenschaften)
- Users (Benutzer)
- Network (Netz)
- Security (Sicherheit)
- IMM Configuration (IMM-Konfiguration)
- Restart IMM (IMM erneut starten)
- Reset IMM to factory defaults (IMM auf werkseitige Voreinstellungen zur
  ücksetzen)
- Activation Key Management (Aktivierungsschlüsselverwaltung)

IBM Integrated Management Module II	Welcon	ne USERID Settings Log out			
System Status Events - Service and Support - Server Managem	ent 👻 IMM Management (h) Searc	ħ			
	IMM Properties	Various properties and settings related to the IMM			
System Descriptive Name:	Users	Create and modify user accounts that will have access to the IMM console			
System x3550 M4 change	Network	Network settings such as SNMP and LDAP used by the IMM Configure security protocols such as SSL and SSH			
System Status and Health	Security				
The System Status and Health page provides an at-a-glance overview of the operato- co-located on this one page.	ting sta IMM Configuration	View a summary of the current configuration settings.			
System Status @ ower: On System state: System running in UEFI	Restart IMM	Restart the IMM. Typically only needed when experiencing problems with the IMM			
System Information   Power Actions   Remote Control Latest OS	Reset IMM to factory defaults	Sets all current configuration settings back to default values			
Active Events	Activation Key Management	Add and remove activation keys for additional functionality			
Severity A Source Date Message	1				

Über die Seite "Integrated Management Module (IMM) Properties" (Eigenschaften des integrierten Managementmoduls (IMM)) können Sie die folgenden Funktionen ausführen:

- Zugriff auf die Server-Firmwareinformationen
- Datum und Uhrzeit festlegen:
  - Methode zur Einstellung der Uhrzeit des IMM2 auswählen: manuell oder NTP (Network Time Protocol)
  - Für Datum und Uhrzeit des IMM2 die manuelle Einstellungsmethode festlegen
  - Für NTP-Informationen NTP-Einstellungsmethode festlegen
  - Zeitzoneninformationen für das IMM2 festlegen
- Auf Informationen zum seriellen Anschluss des IMM2 zugreifen:
  - Seriellen Anschluss des IMM2 konfigurieren
  - Tastenkombinationen für die Befehlszeilenschnittstelle des IMM2 festlegen

Über die Seite "User Accounts" (Benutzerkonten) können Sie die folgenden Funktionen durchführen:

- IMM2-Benutzerkonten verwalten:
  - Benutzerkonto erstellen
  - Klicken Sie auf einen Benutzernamen, um Eigenschaften f
    ür diesen Benutzer zu bearbeiten:
    - Benutzernamen bearbeiten
    - Benutzerkennwort festlegen
    - SNMPv3-Einstellungen für den Benutzer konfigurieren
    - Öffentliche Secure Shell-Authentifizierungsschlüssel (SSH) für den Benutzer verwalten
  - Benutzerkonto löschen
- Allgemeine Anmeldeeinstellungen für Benutzer konfigurieren:
  - Benutzerauthentifizierungsverfahren festlegen
  - Inaktivitätszeitlimit für das Web festlegen
  - Für das IMM2 verfügbare Sicherheitsstufen für Benutzerkonten konfigurieren
- Benutzer anzeigen, die derzeit mit dem IMM2 verbunden sind

Auf der Seite "Network Protocol Properties" (Netzprotokolleigenschaften) können Sie die folgenden Funktionen ausführen:

- Ethernet-Einstellungen konfigurieren:
  - Ethernet-Einstellungen:
    - Hostname
    - Aktivierungs- und Adresseinstellungen von IPv4 und IPv6
  - Erweiterte Ethernet-Einstellungen:
    - Aktivierung von automatischer Vereinbarung
    - MAC-Adressenverwaltung
    - Größte zu übertragende Einheit festlegen
- SNMP-Einstellungen konfigurieren:
  - Aktivierung und Konfiguration von SNMPv1:
    - Kontaktinformationen festlegen
    - Aktivierung und Konfiguration von SNMP-Traps
    - Communityverwaltung
  - Aktivierung und Konfiguration von SNMPv3:
    - Kontaktinformationen festlegen
    - Konfiguration von Benutzerkonten
- DNS-Einstellungen konfigurieren:
  - Adressierungsvorgabe für DNS festlegen (IPv4 oder IPv6)
  - Aktivierung und Konfiguration zusätzlicher DNS-Serveradressierung
- DDNS-Einstellungen konfigurieren:
  - Aktivierung von Dynamic Domain Name System (DDNS)
  - Quelle für Domänennamen aussuchen (benutzerdefiniert oder DHCP-Server)
    - Benutzerdefinierten Domänennamen für benutzerdefinierte, manuell angegebene Quelle festlegen
    - Vom DHCP-Server angegebenen Domänennamen anzeigen
- SMTP-Einstellungen konfigurieren:

- IP-Adresse oder Hostnamen des SMTP-Servers festlegen
- SMTP-Server-Portnummer festlegen
- SMTP-Verbindung testen
- LDAP-Einstellungen konfigurieren:
  - Konfiguration für LDAP-Server festlegen (DNS oder vorkonfiguriert):
    - Bei DNS-definierter LDAP-Serverkonfiguration Suchdomäne festlegen:
      - Suchdomäne von Anmelde-ID extrahieren
      - Manuell definierte Suchdomäne und manuell definierter Servicename
      - Versuchen, Suchdomäne von Anmelde-ID zu extrahieren, dann manuell angegebene Suchdomäne und manuell angegebenen Servicenamen verwenden
    - Bei Verwendung eines vorkonfigurierten LDAP-Servers:
      - Hostnamen oder IP-Adresse für LDAP-Server festlegen
      - LDAP-Server-Portnummer festlegen
  - Definierten Namen für den Stammeintrag des LDAP-Servers festlegen
  - Suchattribut für Benutzer-ID festlegen
  - Bindungsmethode auswählen (anonym, mit konfigurierten Berechtigungsnachweisen, mit Berechtigungsnachweisen für Anmeldung):
    - Bei konfigurierten Berechtigungsnachweisen definierten Namen und Kennwort des Clients festlegen
  - Erweiterte rollenbasierte Sicherheit f
    ür Aktivierung von Active Directory-Benutzern:
    - Bei Inaktivierung:
      - Gruppenfilter festlegen
      - Gruppensuchattribut festlegen
      - Anmeldeberechtigungsattribut festlegen
    - Bei Aktivierung Zielnamen des Servers festlegen
- Telnet-Einstellungen konfigurieren:
  - Telnet-Zugriffsaktivierung
  - Maximale Anzahl an Telnet-Sitzungen festlegen
- USB-Einstellungen konfigurieren:
  - Aktivierung von Ethernet over USB
  - Aktivierung und Verwaltung der Weiterleitung von externem Ethernet-Port zu Ethernet-over-USB-Port
- Portzuordnungen konfigurieren:
  - Nummern offener Ports anzeigen
  - Von IMM2-Services verwendete Portnummern festlegen:
    - HTTP
    - HTTPS
    - Telnet-Befehlszeilenschnittstelle
    - SSH-Befehlszeilenschnittstelle
    - SNMP-Agent
    - SNMP Traps (SNMP-Traps)
    - Remote Control (Fernsteuerung)
    - CIM over HTTPS
    - CIM over HTTP

Über die Seite "Security" (Sicherheit) können Sie die folgenden Funktionen ausführen:

- HTTPS-Serveraktivierung und Zertifikatsverwaltung
- Aktivierung von CIM over HTTPS und Zertifikatsverwaltung
- LDAP-Sicherheitsoptionen und Zertifikatsverwaltung
- SSH-Serveraktivierung und Zertifikatsverwaltung

Über die Seite "IMM Configuration" können Sie die folgenden Funktionen ausführen:

- Zusammenfassung der IMM2-Konfiguration anzeigen
- IMM2-Konfiguration sichern oder wiederherstellen
- · Sicherungs- oder Wiederherstellungsstatus anzeigen
- IMM2-Konfiguration auf werkseitig vorgenommene Standardeinstellungen zurücksetzen
- Auf den Assistenten für die IMM2-Erstkonfiguration zugreifen

Über die Seite "Restart IMM" können Sie das IMM2 zurücksetzen.

Über die Seite "Reset IMM2 to factory defaults..." (IMM2 auf werkseitige Voreinstellungen zurücksetzen) können Sie die IMM2-Konfiguration auf die werkseitig vorgenommenen Standardeinstellungen zurücksetzen.

Über die Seite "Activation Key Management" (Aktivierungsschlüsselverwaltung) können Sie Aktivierungsschlüssel für optionale FoD-Funktionen (Features On Demand) des IMM2 und des Servers verwalten. Informationen zur FoD-Aktivierungsschlüsselverwaltung finden Sie unter Kapitel 7, "Features on Demand", auf Seite 143.

### Serverzeitlimits festlegen

Verwenden Sie die Option "Server Timeouts" (Serverzeitlimits) zum Festlegen von Zeitlimits, damit der Server während einer Firmwareaktualisierung oder beim Einschalten des Servers nicht unbegrenzt blockiert wird. Sie können diese Funktion aktivieren, indem Sie den Wert für diese Option einstellen, wie in der folgenden Abbildung dargestellt.

**Anmerkung:** Bei Serverzeitlimits muss die Inband-USB-Schnittstelle (oder LAN over USB) aktiviert sein, um Befehle zu verwenden. Weitere Informationen zur Aktivierung und Inaktivierung der USB-Schnittstelle finden Sie im Abschnitt "USB konfigurieren" auf Seite 84.

IBM Integrated Management Module II	USERID	Settings   Log out	IBM.
System Status Events + Service and Support + Server Nanagement + 30M Management + Search			
Server Timeouts Set traves to a many that backing firmware and powering on the server do not hang indefinitely. Similar backer Watchdog Enable Power off Deby Acolv Reset			

Gehen Sie wie folgt vor, um die Werte für das Serverzeitlimit festzulegen:

- 1. Melden Sie sich an dem IMM2 an, für das Sie die Serverzeitlimits festlegen möchten. (Siehe Abschnitt "Am IMM2 anmelden" auf Seite 10).
- 2. Klicken Sie auf Server Management (Serververwaltung) und wählen Sie anschließend Server Timeouts aus.

Sie können das IMM2 so einstellen, dass es automatisch auf die folgenden Ereignisse reagiert:

- Das Betriebssystem läuft in einer Endlosschleife
- Das Betriebssystem wird nicht geladen
- **3.** Aktivieren Sie die Serverzeitlimits, die den Ereignissen entsprechen, auf die das IMM2 automatisch reagieren soll. Eine Beschreibung der Auswahloptionen finden Sie unter "Server timeout selections" (Serverzeitlimitoptionen).
- 4. Klicken Sie auf Apply (Übernehmen).

**Anmerkung:** Die Schaltfläche **Reset** (Zurücksetzen) ermöglicht es Ihnen, alle Zeitlimitwerte gleichzeitig zu löschen.

### Serverzeitlimitoptionen

### Enable OS Watchdog (Betriebssystem-Watchdog aktivieren)

Verwenden Sie das Feld **Enable OS Watchdog**, um die Anzahl an Minuten zwischen Prüfungen des Betriebssystems durch das IMM2 anzugeben. Wenn das Betriebssystem auf eine dieser Prüfungen nicht reagiert, generiert das IMM2 einen Betriebssystem-Zeitlimitalert und startet den Server erneut. Nach dem Neustart des Servers ist der Betriebssystem-Watchdog inaktiviert, bis das Betriebssystem heruntergefahren und der Server ausund wieder eingeschaltet wird. Wählen Sie zum Festsetzen des Wertes für den Betriebssystem-Watchdog **Enable OS Watchdog** aus und wählen Sie ein Zeitintervall aus dem Menü aus. Wählen Sie zum Ausschalten dieses Watchdogs **Enable OS Watchdog** ab. Zum Aufzeichnen von Betriebssystem-Fehleranzeigen müssen Sie den Watchdog im Feld **Enable OS Watchdog** aktivieren.

#### Enable Loader Watchdog (Ladeprogramm-Watchdog aktivieren)

Verwenden Sie das Feld Enable Loader Watchdog, um anzugeben, wie viele Minuten das IMM2 zwischen der Fertigstellung des POST und dem Starten des Betriebssystems warten soll. Wenn diese Zeitspanne überschritten wird, generiert das IMM2 einen Ladeprogramm-Zeitlimitalert und startet den Server automatisch erneut. Nach dem Neustart des Servers wird das Ladeprogramm-Zeitlimit automatisch inaktiviert, bis das Betriebssystem heruntergefahren und der Server aus- und wieder eingeschaltet wird (oder bis das Betriebssystem startet und die Software erfolgreich geladen wird). Zum Festlegen des Wertes für das Ladeprogramm-Zeitlimit wählen Sie aus, wie lange das IMM2 auf die Fertigstellung des Betriebssystemstarts warten soll. Wählen Sie zum Ausschalten dieses Watchdogs Enable Loader Watchdog im Menü ab.

#### Enable Power Off Delay (Ausschaltverzögerung aktivieren)

Verwenden Sie das Feld **Enable Power Off Delay**, um anzugeben, wie viele Minuten das IMM2-Subsystem darauf warten soll, dass das Betriebssystem herunterfährt, bevor es die Stromversorgung des Systems abschaltet. Zum Festlegen des Wertes für die Ausschaltverzögerung wählen Sie aus, wie lange das IMM2 nach dem Ausschalten des Betriebssystems warten soll. Wählen Sie zum Ausschalten dieses Watchdogs **Enable Loader Watchdog** im Menü ab.

### Datum und Uhrzeit für IMM2 einstellen

**Anmerkung:** Die Einstellungen für Datum und Uhrzeit des IMM2 können auf einem IBM Flex System-Knoten nicht geändert werden.

Wählen Sie die Registerkarte **Date and Time** aus, um das Datum und die Uhrzeit für das IMM2 anzuzeigen oder zu ändern. Das IMM2 verwendet einen eigenen Taktgeber, um alle Ereignisse im Ereignisprotokoll zeitlich zu markieren. Bei Alerts, die per E-Mail und SNMP versendet werden, wird die Taktgebereinstellung zur zeitlichen Markierung verwendet. Zwecks größerer Benutzerfreundlichkeit für Administratoren, die über Fernzugriff Systeme in unterschiedlichen Zeitzonen verwalten, werden Abweichungen von der westeuropäischen Zeit und die Sommerzeit von den Zeiteinstellungen unterstützt. Sie können selbst dann über Fernzugriff auf das Ereignisprotokoll zugreifen, wenn der Server ausgeschaltet oder inaktiviert ist.

Die Datums- und Uhrzeiteinstellung des IMM2 wirkt sich nur auf den IMM2-Taktgeber und nicht auf den Servertaktgeber aus. Beim IMM2-Taktgeber und beim Servertaktgeber handelt es sich um separate, voneinander unabhängige Taktgeber, die auf unterschiedliche Uhrzeiten eingestellt werden können.

### Einstellung für Datum und Uhrzeit ändern (manueller Modus)

Gehen Sie wie folgt vor, um die Uhrzeit und das Datum manuell zu ändern:

- 1. Klicken Sie in der Liste Indicate how the IMM date and time should be set (Angeben, wie das IMM-Datum und die IMM-Uhrzeit festgelegt werden sollen) auf Set Date and Time Manually (Datum und Uhrzeit manuell festlegen).
- 2. Geben Sie im Feld Date den laufenden Monat, den Tag und das Jahr ein.
- **3**. Geben Sie im Feld **Time** (Zeit) in den entsprechenden Feldern die Zahlen ein, die der laufenden Stunde und Minute entsprechen.
  - Bei der Stunde muss eine Zahl zwischen 1 und 12 entsprechend einer 12-Stunden-Zeiteinteilung stehen.
  - Bei den Minuten müssen Zahlen zwischen 00 und 59 stehen.
  - Wählen Sie AM (vormittags) oder PM (nachmittags) aus.
- 4. Wählen Sie im Feld **GMT offset** (GMT-Abweichung) die Zahl aus, die die Abweichung von der westeuropäischen Zeit in Stunden angibt. Diese Zahl muss der Zeitzone entsprechen, in der sich der Server befindet.
- 5. Wählen Sie das Kontrollkästchen Automatically adjust for daylight saving time (DST) (Automatisch an Sommerzeit anpassen) aus oder wählen Sie es ab, um anzugeben, ob der IMM2-Taktgeber sich automatisch anpasst, wenn die Ortszeit zwischen Standardzeit und Sommerzeit wechselt.

In der folgenden Abbildung ist die Registerkarte "IMM Date and Time" beim manuellen Festlegen von Datum und Uhrzeit dargestellt.

ISM Inter	grated Managem	ent Module II					VSERU
2	ystem Status Ex	erts + Service	and Support + Serve	er Manapement = 1	901 Management. •	leach	
Integr Anna Pro Anna Pro	ated Mana refer and settings feast	agement related to the P	Module (IMN	N) Propertie	rs		
<b>Firmware</b>	Oute and Time	Serai Port					
Indicate 1 Set Date 2/ 7/ 7/ 8/	how the 34H Date and Time Hanualy te: 24/2012 ne: H3 AM	and Time should	be set. Occus a meth	od from the pull-down	n list and supply appr	aprate settings.	
GM +	T Offset: () 0:00 - Greenwich H	lean Time (Britan	, Ireland, Portugal, Rey	kpark (Iceland), West	tern Africa)		- (w)
	Automatically adjust	t for Daylight Sav	ergs Time (DST) 🖗				

### Einstellungen für Datum und Uhrzeit ändern (NTP-Servermodus)

Gehen Sie wie folgt vor, um den IMM2-Taktgeber mit dem Servertaktgeber zu synchronisieren:

- Klicken Sie in der Liste Indicate how the IMM date and time should be set (Angeben, wie das IMM-Datum und die -Uhrzeit festgelegt werden sollen) auf Synchronize with an NTP server (Mit einem NTP-Server synchronisieren).
- 2. Geben Sie im Feld **NTP server host name or IP address** (Hostname oder IP-Adresse des NTP-Servers) den Namen des NTP-Servers an, der für die Taktgebersynchronisation verwendet werden soll.
- **3**. Geben Sie im Feld **Synchronization frequency (in minutes)** (Synchronisationshäufigkeit (in Minuten)) das ungefähre Intervall zwischen den Synchronisationsanforderungen ein. Geben Sie einen Wert zwischen 3 und 1440 Minuten ein.
- 4. Wählen Sie das Kontrollkästchen **Synchronize when these settings are saved** (Beim Speichern dieser Einstellungen synchronisieren) aus, um eine sofortige Synchronisierung anzufordern, (wenn Sie auf **Apply** klicken) anstatt darauf zu warten, bis das Zeitintervall abgelaufen ist.
- 5. Wählen Sie im Feld **GMT offset** (GMT-Abweichung) die Zahl aus, die die Abweichung von der westeuropäischen Zeit in Stunden angibt, entsprechend der Zeitzone, in der sich der Server befindet.
- 6. Wählen Sie das Kontrollkästchen Automatically adjust for daylight saving time (DST) (Automatisch an Sommerzeit anpassen) aus oder wählen Sie es ab, um anzugeben, ob der IMM2-Taktgeber sich automatisch anpasst, wenn die Ortszeit zwischen Standardzeit und Sommerzeit wechselt.

In der folgenden Abbildung ist die Registerkarte "IMM Date and Time" beim Synchronisieren mit dem Servertaktgeber dargestellt.

ronize with an NTP server	*
Time: 2012/07/20 08:43 (NTP time)	
NTP server host name or IP addres	is (you can specify up to 4 addresses): 🕖
(not used)	
Synchronization frequency (minute 1,440	s) 💿
Synchronize when these setting	ps are saved 🎯
GMT Offset:	
+0:00 - Greenwich Mean Time (P	ritain, Treland, Portugal, Revklavik (Tceland), Western Africa)

## Einstellungen für den seriellen Anschluss konfigurieren

Wählen Sie die Option **Serial Port** (Serieller Anschluss) aus, um die Umleitung des seriellen Anschlusses des Hosts anzugeben. Das IMM2 stellt zwei serielle Anschlüsse bereit, die für serielle Umleitungen verwendet werden:

#### Serial port 1 (Serieller Anschluss 1) (COM1)

Der serielle Anschluss 1 (COM1) auf System x Servern wird für IPMI Serial over LAN (SOL) verwendet. COM1 kann nur über die IPMI-Schnittstelle konfiguriert werden.

#### Serial port 2 (Serieller Anschluss 2) (COM2)

Auf Blade-Servern wird der serielle Anschluss 2 (COM2) für SOL verwendet. Auf System x-Gehäuserahmenservern und IBM Flex System-Knoten wird COM2 für serielle Umleitungen über Telnet oder SSH verwendet. COM2 kann nicht über die IPMI-Schnittstelle konfiguriert werden. Auf in einem Gehäuse installierten Servern und auf Turmservern ist COM2 ein interner COM-Anschluss ohne die Möglichkeit eines externen Zugriffs.

Machen Sie in den folgenden Feldern die für die Umleitung des seriellen Anschlusses erforderlichen Angaben:

### Baud Rate (Baudrate)

Geben Sie in diesem Feld die Datenübertragungsgeschwindigkeit Ihrer seriellen Anschlussverbindung an. Um die Baudrate festzulegen, wählen Sie eine Datenübertragungsgeschwindigkeit zwischen 9600 und 115200 aus, die der Geschwindigkeit Ihrer seriellen Anschlussverbindung entspricht.

### Parity (Parität)

Geben Sie in diesem Feld die Paritätsbits Ihrer seriellen Anschlussverbindung an. Die verfügbaren Optionen lauten "None" (Keine), "Odd" (Ungerade) oder "Even" (Gerade).

#### Stop Bits (Stoppbits)

Geben Sie in diesem Feld die Anzahl der Stoppbits Ihrer seriellen Anschlussverbindung an. Die verfügbaren Optionen lauten "1" oder "2".

### CLI Mode (CLI-Modus)

Wählen Sie in diesem Feld die Option **CLI with IMM2 compatible keystroke sequences** (CLI mit IMM2-kompatiblen Tastenfolgen) oder, wenn Sie Ihre eigene Tastenkombination verwenden möchten, die Option
**CLI with user defined keystroke sequences** (CLI mit benutzerdefinierten Tastenfolgen) aus. Wenn Sie **CLI with user defined keystroke sequences** auswählen, müssen Sie die Tastenkombination im Feld **User-defined key sequence for 'Enter CLI'** (Benutzerdefinierte Tastenkombination für 'Enter CLI') definieren.

Nachdem die serielle Umleitung gestartet wurde, wird sie so lange fortgesetzt, bis Sie die Tastenkombination zum Beenden eingeben. Wenn die Tastenkombination zum Beenden eingegeben wird, wird die serielle Umleitung gestoppt und Sie wechseln in den Befehlsmodus in der Telnet- oder SSH-Sitzung zurück. Verwenden Sie das Feld **User-defined key sequence for 'Enter CLI'**, um die Tastenkombination zum Beenden anzugeben.

In der folgenden Abbildung ist die Registerkarte "Serial Port" dargestellt.

IBM	Integrated Ma	nagem	ent Mo	dule II					
<u>~</u>	System Statu	is Eve	ents 🗸	Service and	Support 🗸	Server Manage	ment 🗸	IMM Management +	Search
Inte Various Apply	properties and Reset	<b>Aana</b> settings	igen related	to the IMM	dule	(IMM) Pro	perti	ies	
Firmy	vare Date an	d Time	Seria	Port					
Serial Sei Baut	rial Port 2 ( Rate: 0	of the I	2)	Ŧ					
Parit	y:@ ne								
Stop 1	Bits: @								
	Mode: with user-define	ed keyst	roke se	quences	-				
User ^[(	-defined key see	quence	for 'Ent	er CLI' 🧶					

## Benutzerkonten konfigurieren

Wählen Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) die Option **Users** (Benutzer) aus, um Benutzerkonten für das IMM2 zu erstellen und zu ändern und um Gruppenprofile anzuzeigen. Die folgende Informationsnachricht wird angezeigt.

**Anmerkung:** In einem IBM Flex System-Knoten werden IMM2-Benutzerkonten vom CMM verwaltet.



# Benutzerkonten

Wählen Sie die Registerkarte **Users Accounts** (Benutzerkonten) aus, um Benutzerkonten zu erstellen, zu ändern und anzuzeigen, wie in der folgenden Abbildung dargestellt.

Anmerkung: Das IMM2-Subsystem wird mit einem Anmeldeprofil geliefert.

BM Int	tegrated N	lanagement Module I					USERID Setting
1	System St	atus Events <del>-</del> Servi	e and S	Support 👻 Server Manaj	pement +	IMM Management + Sewich	
ISET	ACCOL ad modify ar	unts nd view user accounts. U	ie 'Grou	ip Profiles' tab to create, i	modify and	view group profile for active directory user	s.
Jsers A	ccounts	Group Profiles					
Create create Create	r ACCO e, modify an ies for that	unts id view user accounts the user. Note: By default, the Global Login Settings.	e 3MM s	ave access to the IMM cor subsystem comes configur mently Logged in Users	nsole. To a ed with or Delete	dd a user profile, click "Create User" and co te login profile that all more	nfigure the profile details. Click a User Name to view or change
	User Nam	Access		Password Expiration		Active Sessions	
	USERID	Supervis	or	No Expiration		(Web-HTTPS)9.44.77.169	
	usemame	1 Supervis	or	No Expiration		(none)	

### Benutzer erstellen

Klicken Sie auf die Registerkarte **Create User...** (Benutzer erstellen), um ein neues Benutzerkonto zu erstellen. Füllen Sie die folgenden Felder aus: **User name** (Benutzername), **Password** (Kennwort) und **Confirm Password** (Kennwort bestätigen) (wie in der folgenden Abbildung dargestellt).

Create New Use	r	x
User Credentials	User Credentials	
Authority	Enter a user name and password.	
SNMPv3	User name: username1 Password: ••••••• Confirm password: ••••••• User name rules:	Password rules:
< Back Next >	<ul> <li>Must be 1-16 characters</li> <li>Cannot contain white space characters</li> <li>Can only contain the characters A-Z, a-Z, 0-9, '_' (underscore) and '.' (period)</li> <li>Must be different for each user</li> </ul>	<ul> <li>Passwords are not required</li> <li>Must be 0-20 characters</li> <li>Cannot contain white space characters</li> <li>Password and password confirm values must match</li> <li>Can only contain the characters A-Z, a-z, 0-9, ~`!@#\$%^&amp;*()-+={}[]:;"&lt;&gt;,?/</li> </ul>

### Benutzereigenschaften

Klicken Sie auf die Registerkarte **User Properties** (Benutzereigenschaften), um ein bestehendes Benutzerkonto zu ändern (wie in der folgenden Abbildung dargestellt).

Jser Properties			
User Credentials	Authority	SNMPv3	SSH Client Public Key
User name: USERID			
Password:			
Confirm password	:		
User name rules:			Password rules:
Cannot con	tain white sp	ace charact	ers Passwords are not required

### Benutzerberechtigung

Klicken Sie auf die Registerkarte **Authority** (Berechtigung), um die Benutzerberechtigung festzulegen. Die folgenden Benutzerberechtigungsstufen sind verfügbar:

#### Supervisor (Administrator)

Für den Benutzer gelten keine Einschränkungen.

#### Read only (Lesezugriff)

Der Benutzer verfügt nur über Lesezugriff und kann keine Aktionen ausführen, wie z. B. Dateiübertragungen, Einschalt- und Neustartaktionen sowie Remote-Presence-Funktionen.

#### Custom (Angepasst)

Das Profil für die Benutzerberechtigung kann durch Einstellungen für die Aktionen, die der Benutzer ausführen kann, angepasst werden.

### SNMP-Zugriffsberechtigungen

Klicken Sie auf die Registerkarte **SNMPv3**, um SNMP-Zugriff für das Konto festzulegen. Die folgenden Benutzerzugriffsoptionen sind verfügbar:

#### Authentication protocol (Authentifizierungsprotokoll)

Geben Sie entweder **HMAC-MD5** oder **HMAC-SHA** als Authentifizierungsprotokoll an. Dabei handelt es sich um die Algorithmen, die vom SN-MPv3-Sicherheitsmodell für die Authentifizierung verwendet werden. Wenn die Option **Authentication Protocol** nicht aktiviert ist, wird kein Authentifizierungsprotokoll verwendet.

#### Privacy protocol (Datenschutzprotokoll)

Die Datenübertragung zwischen dem SNMP-Client und dem Agenten kann mithilfe von Verschlüsselung geschützt werden. Folgende Methoden werden unterstützt: **DES** und **AES**. Das Datenschutzprotokoll ist nur dann gültig, wenn für das Authentifizierungsprotokoll entweder **HMAC-MD5** oder **HMAC-SHA** festgelegt wurde.

#### Privacy password (Datenschutzkennwort)

Geben Sie das Verschlüsselungskennwort in diesem Feld an.

#### Confirm privacy password (Datenschutzkennwort bestätigen)

Geben Sie das Verschlüsselungskennwort zum Bestätigen nochmals an.

#### Access type (Zugriffstyp)

Geben Sie als Zugriffstyp entweder **Get** (Abrufen) oder **Set** (Festlegen) an. SNMPv3-Benutzer mit dem Zugriffstyp **Get** können nur Abfrageoperationen ausführen. SNMPv3-Benutzer mit dem Zugriffstyp **Set** können Abfrageoperationen ausführen und Einstellungen ändern (z. B. das Kennwort für einen Benutzer festlegen).

#### Hostname/IP address for traps (Hostname/IP-Adresse für Traps)

Geben Sie das Trapziel für den Benutzer an. Das kann eine IP-Adresse oder ein Hostname sein. Mithilfe von Traps benachrichtigt der SNMP-Agent die Verwaltungsstation über Ereignisse (z. B. wenn die Temperatur eines Prozessors den Grenzwert überschreitet).

### Gruppenprofile

Wählen Sie die Registerkarte **Group Profiles** (Gruppenprofile) aus, um Gruppenprofile zu erstellen, zu ändern oder anzuzeigen (wie in der folgenden Abbildung dargestellt).

IBM I	ntegrated N	lanager	nent Mo	dule II												
2	System St	atus E	vents 🕶	Service and Support	t•	Server M	anagem	ent 🕶	IMM P	lanagem	ent +	Sea	ch. , ,			
Use Create	r Accou	unts	iser accou	ints. Use 'Group Prof	iles' tab	b to creat	te, mod	fy and	view gr	oup prof	lie for	active	directo	ry useri	L	
Gro Note: To use	These profile	files es will not	for A	while the LDAP clien	t is con	y infigured f	for both , reconfi	authen gure th	ntication ne LDAP	and aut	horizat	tion. of the	Netwo	ork Prot	ocols pag	e.
Crea	te Group	Delete														
	Group ID		R	ole												
	No	o Group P	rofiles Av	ailable.												

Klicken Sie auf **Create Group** (Gruppe erstellen), um eine neue Benutzergruppe zu erstellen. In der folgenden Abbildung ist das Fenster "Create Group Profile" (Gruppenprofil erstellen) dargestellt.

Create Group Profile	х
Group ID: 🖗	
Role:	
Supervisor Has no restrictions.	
Read-only 🕖 Has only read-only access, and cannot perform any save, modify, clear, or state affecting operations (e.g. restart IMM, restore defaults, upgrade the firmware, et	.c.)
Custom May or may not have any restrictions, depending on which custom authority level is assigned to the group.	
OK Cancel	

Geben Sie eine **Group ID** (Gruppen-ID) ein und wählen Sie die **Role** (Rolle) aus (Informationen zu Benutzerberechtigungsstufen finden Sie im Abschnitt "Benutzerberechtigung" auf Seite 65).

Um eine Gruppe zu löschen, klicken Sie auf **Delete** (Löschen). In der folgenden Abbildung ist das Fenster "Confirm Group Deletion" (Löschen von Gruppe bestätigen) dargestellt.

IBM Integrated Manage	ement Module II		
System Status	Events - Service and Support	Server Management      IMM Management      Search	
User Accounts			
Create and modify and view	user accounts. Use 'Group Profile	s' tab to create, modify and view group profile for active directory users.	
Users Accounts Group	Profiles		
Group Profiles	s for Active Direct	tory	
Note: These profiles will n	ot be used while the LDAP client i	is configured for both authentication and authorization.	
To use these group profile	s for authorization and LDAP for a	uthentication recontinue the LDAP Client section of the Natwork Proto	stole name
To use these group profile Create Group	s for authorization and LDAP for a	Confirm Group Deletion	vole nane )
To use these group profile Create Group Delet Group ID	s for authorization and LDAP for a	Confirm Group Deletion Do you want to delete the group 'groupProfile1'?	vrok nade N

# Globale Anmeldeeinstellungen konfigurieren

Auf der Registerkarte "Global login settings" (Globale Anmeldeeinstellungen) können Sie Anmeldeeinstellungen konfigurieren, die für alle Benutzer gelten.

## Allgemeine Einstellungen

Geben Sie auf der Registerkarte **General** (Allgemein) an, wie Benutzeranmeldeversuche authentifiziert werden und wie lange (in Minuten) das IMM2 wartet, bevor es die Verbindung einer inaktiven Websitzung trennt. Geben Sie im Feld **User authentication method** (Benutzerauthentifizierungsmethode) an, wie die Benutzer, die versuchen, sich anzumelden, authentifiziert werden sollen. Wählen Sie eine der folgenden Authentifizierungsmethoden aus:

- Local only (Nur lokal): Benutzer werden durch eine Suche nach dem lokalen Benutzerkonto authentifiziert, das auf dem IMM2 konfiguriert ist. Wenn keine Übereinstimmung für die Benutzer-ID und das Kennwort vorhanden ist, wird der Zugriff verweigert.
- LDAP only (Nur LDAP): Das IMM2 versucht, den Benutzer mithilfe eines LDAP-Servers zu authentifizieren. Bei dieser Authentifizierungsmethode werden die lokalen Benutzerkonten auf dem IMM2 *nicht* durchsucht.
- Local first, then LDAP (Zuerst lokal, dann LDAP): Zuerst wird eine lokale Authentifizierung versucht. Falls diese lokale Authentifizierung fehlschlägt, wird eine LDAP-Authentifizierung versucht.
- LDAP first, then Local (Zuerst LDAP, dann lokal): Zuerst wird die LDAP-Authentifizierung versucht. Falls die LDAP-Authentifizierung fehlschlägt, wird eine lokale Authentifizierung versucht.

#### Anmerkungen:

• Nur lokal verwaltete Konten werden für die IPMI- und SNMP-Schnittstellen freigegeben. Diese Schnittstellen unterstützen keine LDAP-Authentifizierung. • IPMI- und SNMP-Benutzer können sich mithilfe der lokal verwalteten Konten anmelden, wenn für das Feld **User authentication method** die Option **LDAP only** ausgewählt ist.

Geben Sie im Feld **Web inactivity session timeout** (Sitzungszeitlimit bei Webinaktivität) an, wie lange (in Minuten) das IMM2 wartet, bevor es die Verbindung einer inaktiven Websitzung trennt. Wählen Sie **No timeout** (Kein Zeitlimit) aus, um diese Funktion zu inaktivieren. Wählen Sie **User picks timeout** (Benutzer legt Zeitlimit fest) aus, wenn der Benutzer das Zeitlimitintervall während des Anmeldeprozesses festlegen soll.

Das Inaktivitätszeitlimit gilt nur für Webseiten, die *nicht* automatisch aktualisiert werden. Wenn ein Web-Browser fortlaufend Webseitenaktualisierungen anfordert, wenn ein Benutzer zu einer Webseite wechselt, die automatisch aktualisiert wird, wird die Sitzung dieses Benutzers nicht automatisch durch das Inaktivitätszeitlimit beendet. Benutzer können auswählen, ob der Inhalt der Webseiten automatisch alle 60 Sekunden aktualisiert werden soll. Weitere Informationen zur Einstellung für automatisches Aktualisieren finden Sie im Abschnitt "Page Auto Refresh" auf Seite 17.

Die Registerkarte "General" ist in der folgenden Abbildung dargestellt.

lobal Logi	Settings	3
Global	Login Settings	
General	Account Security Level	
User auth	entication method: 🥥	
Local Onl	/ *	
20 minute	15	
OK Canc	el	

Einige IMM2-Webseiten werden automatisch aktualisiert, auch wenn die Einstellung für automatisches Aktualisieren nicht ausgewählt wurde. Folgende IMM2-Webseiten werden automatisch aktualisiert:

- System Status: Der System- und der Stromversorgungsstatus werden automatisch alle drei Sekunden aktualisiert.
- Server Power Actions: (Serverstromversorgungsaktionen) Der Stromversorgungsstatus wird automatisch alle drei Sekunden aktualisiert.
- **Remote Control:** (Fernsteuerung) Die Schaltflächen zum Starten der Fernsteuerung werden automatisch einmal pro Sekunde aktualisiert. Die Tabelle "Session List" (Sitzungsliste) wird automatisch einmal pro Minute aktualisiert.

Die IMM2-Firmware unterstützt bis zu sechs gleichzeitige Websitzungen. Um Sitzungen für andere Benutzer freizugeben, sollten Sie sich von einer Websitzung abmelden, wenn Sie Ihre Arbeit beendet haben, anstatt sich darauf zu verlassen, dass die Sitzung nach dem Inaktivitätszeitlimit automatisch geschlossen wird.

**Anmerkung:** Wenn Sie das Browserfenster geöffnet lassen, während Sie eine IMM2-Webseite anzeigen, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch aufgrund von Inaktivität geschlossen.

# Einstellungen für die Kontensicherheitsrichtlinie

Klicken Sie auf die Registerkarte **Account Security Level** (Kontensicherheitsstufe), um die Einstellung für die Kontensicherheitsrichtlinie auszuwählen. Es gibt drei Stufen von Kontensicherheitsrichtlinieneinstellungen:

- Legacy Security Settings (Traditionelle Sicherheitseinstellungen)
- High Security Settings (Strenge Sicherheitseinstellungen)
- Custom Security Settings (Angepasste Sicherheitseinstellungen)

Die Registerkarte "Account Security Level" ist in der folgenden Abbildung dargestellt.

ilobal	Login Settings			
General	Account Security Level			
Custom S	Security Settings 🤜 🥝			ŕ
Pass	word required @			
Com	plex password required 🥝			
Pass	word expiration period (days) 🥝	0	*	
Minin	num password length 🥝	5	*	
Minin	num password reuse cycle 🧼	0	-	
Minin	num password change interval (hours) 🎱	0	+	
Maxi	mum number of login failures (times) 🎱	5	-	
Lock	out period after maximum login failures (minutes) @	2	-	
Minin	num different characters in passwords	0	*	
Facto	ry default 'USERID' account password must be changed on next login			
-				

Wählen Sie die gewünschte Stufe in der Elementliste aus. Bei den Stufen "Legacy Security Settings" und "High Security Settings" sind die Werte für die Richtlinieneinstellungen vordefiniert und können nicht geändert werden. Die Stufe "Custom Security Settings" ermöglicht Benutzern das Anpassen der Sicherheitsrichtlinien nach Bedarf.

In der folgenden Tabelle sind die Werte für alle Stufen der Sicherheitseinstellungen aufgeführt.

Tabelle 3. Werte für Sicherheitseinstellungsrichtlinie

Richtlinien-	Legacy Security	High Security	Custom Security
einstellung/-feld	Settings	Settings	Settings
Password required	Nein	Ja	Ja oder Nein

Richtlinien- einstellung/-feld	Legacy Security Settings	High Security Settings	Custom Security Settings
Complex password required	Nein	Ja	Ja oder Nein
Password expiration period (days)	Keine	90	0 - 365
Minimum password length	Keine	8	5 - 20
Minimum password reuse cycle	Keiner	5	0 - 5
Minimum password change interval (hours)	Keins	24	0 - 240
Maximum number of login failures (times)	5	5	0 - 10
Lockout period after maximum login failures (minutes)	2	60	0 - 240
Minimum different characters in passwords	Keins	2	0 - 19
Factory default 'USERID' account password must be changed on next login	Nein	Ja	Ja oder Nein
Force user to change password on first access	Nein	Ja	Ja oder Nein

Tabelle 3. Werte für Sicherheitseinstellungsrichtlinie (Forts.)

Im Folgenden werden die Felder für die Sicherheitseinstellungen beschrieben.

#### Password required (Kennwort erforderlich)

Dieses Feld gibt an, ob Anmelde-IDs ohne Kennwort erstellt werden können. Wenn das Kontrollkästchen **Password required** ausgewählt wird, muss für alle bereits vorhandenen Anmelde-IDs ohne Kennwort bei der nächsten Anmeldung des betreffenden Benutzers ein Kennwort definiert werden.

#### Complex password required (Komplexes Kennwort erforderlich)

Wenn komplexe Kennwörter erforderlich sind, gelten für das Kennwort die folgenden Regeln:

- Kennwörter müssen mindestens acht Zeichen lang sein.
- Kennwörter müssen mindestens drei Vorgaben aus den folgenden vier Kategorien erfüllen:
  - Mindestens ein alphabetisches Zeichen in Kleinbuchstaben.
  - Mindestens ein alphabetisches Zeichen in Großbuchstaben.
  - Mindestens ein numerisches Zeichen.
  - Mindestens ein Sonderzeichen.
- Leerzeichen sind nicht zulässig.

- In Kennwörtern dürfen maximal drei gleiche Zeichen aufeinanderfolgen (wie z. B. aaa).
- Kennwörter dürfen keine Wiederholung oder Umkehrung der zugeordneten Benutzer-ID sein.

Wenn keine komplexen Kennwörter erforderlich sind, gelten folgende Regeln für das Kennwort:

- Kennwörter müssen mindestens fünf Zeichen lang sein (oder die Anzahl an Zeichen, die im Feld Minimum password length angegeben wurde).
- Kennwörter dürfen keine Leerzeichen enthalten.
- Kennwörter müssen mindestens ein numerisches Zeichen enthalten.
- Das Feld für das Kennwort kann leer sein (nur wenn das Kontrollkästchen **Password Required** nicht ausgewählt ist).

#### Password expiration period (days) (Kennwortablaufdauer (Tage))

Dieses Feld gibt die maximale zulässige Gültigkeitsdauer des Kennworts an, bevor das Kennwort geändert werden muss. Es werden Werte von 0 bis 365 Tagen unterstützt. Der Standardwert für dieses Feld lautet 0 (inaktiviert).

#### Minimum password length (Mindestlänge des Kennworts)

Dieses Feld gibt die Mindestlänge des Kennworts an. Für dieses Feld werden 5 bis 20 Zeichen unterstützt. Wenn das Kontrollkästchen **Complex password required** ausgewählt wurde, muss die Mindestlänge des Kennworts mindestens acht Zeichen betragen.

#### Minimum password reuse cycle (Mindestwiederverwendungszyklus des Kenn-

worts) Dieses Feld gibt die Anzahl an vorherigen Kennwörtern an, die nicht wiederverwendet werden dürfen. Es können bis zu fünf vorherige Kennwörter verglichen werden. Wählen Sie 0 aus, um die Wiederverwendung aller vorherigen Kennwörter zuzulassen. Der Standardwert für dieses Feld lautet 0 (inaktiviert).

# Minimum password change interval (hours) (Mindeständerungsintervall für Kennwörter (Stunden))

Dieses Feld gibt an, wie lange ein Benutzer von einer Kennwortänderung bis zur nächsten warten muss. Es werden Werte von 0 bis 240 Stunden unterstützt. Der Standardwert für dieses Feld lautet 0 (inaktiviert).

#### Maximum number of login failures (times) (Maximale Anzahl an Anmeldefehlern (Anzahl))

Dieses Feld gibt die zulässige Anzahl an fehlgeschlagenen Anmeldeversuchen an, bevor der Benutzer für einen bestimmten Zeitraum gesperrt wird. Es werden Werte von 0 bis 10 unterstützt. Der Standardwert für dieses Feld lautet 0 (inaktiviert).

# Lockout period after maximum login failures (minutes) (Aussperrungszeit nach maximaler Anzahl an Anmeldefehlern (Minuten))

Dieses Feld gibt an, wie lange (in Minuten), das IMM2-Subsystem Fernanmeldungsversuche von allen Benutzern sperrt, nachdem mehr als fünf aufeinanderfolgende Anmeldefehler bei einem der Benutzer festgestellt wurden.

# Minimum different characters in passwords (Mindestunterschied an Zeichen in Kennwörtern)

Dieses Feld gibt die Mindestanzahl an Zeichen an, in denen sich das neue Kennwort von dem vorherigen Kennwort unterscheiden muss. Es werden Werte von 0 bis 19 unterstützt.

#### Factory default 'USERID' account password must be changed on next login (Werkseitige Voreinstellung des Kennworts für 'USERID' muss bei der nächsten Anmeldung geändert werden)

Diese Herstelleroption wird bereitgestellt, um das Zurücksetzen des Standardprofils USERID nach der ersten erfolgreichen Anmeldung zu ermöglichen. Wenn dieses Kontrollkästchen ausgewählt wurde, muss das Standardkennwort geändert werden, bevor das Konto verwendet werden kann. Für das neue Kennwort gelten alle aktiven Kennwortdurchsetzungsregeln.

# Force user to change password on first access (Benutzer zwingen, das Kennwort beim ersten Zugriff zu ändern)

Nachdem ein neuer Benutzer mit einem Standardkennwort konfiguriert wurde, erzwingt die Auswahl dieses Kontrollkästchens, dass der betreffende Benutzer sein Kennwort bei der ersten Anmeldung ändern muss.

### Netzprotokolle konfigurieren

Klicken Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) auf die Option **Network** (Netz), um die Netzeinstellungen anzuzeigen und festzulegen.

# Ethernet-Einstellungen konfigurieren

Klicken Sie auf die Registerkarte **Ethernet**, um die IMM2-Ethernet-Einstellungen anzuzeigen oder zu ändern (wie in der folgenden Abbildung dargestellt).

Sys	tem Status	Events +	Service and Se	upport + S	erver Manager	ment 👻 IMM	Manageme	nt + Search
Vetwork	k Proto	NMP and LD/	operties AP used by the	IMM				
ubbit we	Ser							

Gehen Sie wie folgt vor, um eine IPv4-Ethernet-Verbindung zu verwenden:

1. Wählen Sie die Option IPv4 aus. Wählen Sie nun das zugehörige Kontrollkästchen aus.

Anmerkung: Durch Inaktivieren der Ethernet-Schnittstelle können Sie den Zugriff auf das IMM2 vom externen Netz aus verhindern.

- 2. Wählen Sie in der Liste **Configure IP address settings** (Einstellungen für IP-Adressen konfigurieren) eine der folgenden Optionen aus:
  - Obtain an IP address from a DHCP server (IP-Adresse von einem DHCP-Server anfordern)
  - Use static IP address (Statische IP-Adresse verwenden)
- 3. Wenn das IMM2 standardmäßig eine statische IP-Adresse verwenden soll, falls keine Verbindung zu einem DHCP-Server hergestellt werden kann, wählen Sie das entsprechende Kontrollkästchen aus.
- 4. Geben Sie im Feld **Static address** (Statische Adresse) die IP-Adresse des IMM2 ein.

**Anmerkung:** Die IP-Adresse muss vier Ganzzahlen von 0 bis 255 enthalten, die durch Punkte voneinander getrennt sind. Sie darf keine Leerzeichen enthalten.

5. Geben Sie im Feld **Subnet mask** (Teilnetzmaske) die Teilnetzmaske ein, die vom IMM2 verwendet wird.

**Anmerkung:** Die Teilnetzmaske muss vier Ganzzahlen von 0 bis 255 ohne Leerzeichen oder aufeinanderfolgende Punkte enthalten, wobei die Ganzzahlen durch Punkte voneinander getrennt sind. Die Standardeinstellung ist 255.255.255.0.

6. Geben Sie im Feld **Default Gateway** (Standard-Gateway) Ihren Netz-Gateway-Router ein.

**Anmerkung:** Die Gateway-Adresse muss vier Ganzzahlen von 0 bis 255 ohne Leerzeichen oder aufeinanderfolgende Punkte enthalten, wobei die Ganzzahlen durch Punkte voneinander getrennt sind.

In der folgenden Abbildung ist die Registerkarte "Ethernet" dargestellt.

/6		
anod IDv4 addrocc int	ormation	
Address	ormation	
IMM2-e41f13d90631		
9.37.189.59		
255.255.240.0		
9.37.176.1		
raleigh.ibm.com		
9.0.128.50		
9.0.130.50		
0.0.0		
ddress settings		
from DHCP server		
dress		
ess from DHCP server		
192.168.70.125	0	
255.255.255.0	0	
	Image: second	r6         gned IPv4 address information         Address         IMM2-e41f13d90631         9.37.189.59         255.255.240.0         9.37.176.1         raleigh.bm.com         9.0.128.50         9.0.130.50         0.0.0.0         ddress settings         from DHCP server         dress         ses from DHCP server

### Erweiterte Ethernet-Einstellungen konfigurieren

Klicken Sie auf die Registerkarte Advanced Ethernet (Erweitertes Ethernet), um zusätzliche Ethernet-Einstellungen festzulegen. Wählen Sie in der Liste MAC selection (MAC-Auswahl) eine der folgenden Optionen aus:

- Used burned in MAC address (Herstellerkennung der MAC-Adresse verwenden)
  - Die Option "Burned-in MAC address" (Herstellerkennung der MAC-Adresse) ist eine eindeutige physische Adresse, die dem IMM2 vom Hersteller zugeordnet wurde. Die Adresse ist ein Anzeigefeld.
- Use locally administered MAC address (Lokal verwaltete MAC-Adresse verwenden)

Geben Sie im Feld **Maximum transmission unit** (Größte zu übertragende Einheit) die größte zu übertragende Einheit eines Datenpakets (in Byte) für Ihre Netzschnittstelle an. Der gültige Bereich für die größte zu übertragende Einheit reicht von 60 bis 1500. Der Standardwert für dieses Feld lautet 1500. In der folgenden Abbildung sind die Registerkarte "Advanced Ethernet" und die zugehörigen Felder dargestellt.

IRM Into	gratod Manaj	jamant Mar	iulo II						
<b>S</b>	System Status	Events 🕶	Service and Su	upport 🔹 S	erver Manager	nent 🔻 IMM	Manageme	nt 🔹 [Search	
Network se Apply	ork Proto Hing such as S Reset	DCOL Pro	perties Pused by the	тмм					
Ethernet	SNMP	DNS	DDNS	SMTP	LDAP	Teinet	USB	Port Assignments	
Etherr Settings Ethern Vise J Use J Burne Maxmur 1,500	et Advanced Autonegotiation cotton: rned-in MAC addre ed-in MAC addre	M communica Ethemet drass drass e4:1f:13: init (bytes)	d9:06:31 🖉	et –					

## Einstellungen für SNMP-Alerts konfigurieren

Gehen Sie wie folgt vor, um die SNMP-Einstellungen für das IMM2 zu konfigurieren.

1. Klicken Sie auf die Registerkarte **SNMP** (wie in der folgenden Abbildung dargestellt).

IBM Integrated Management Module II	USERID Settings   Log out IBM
System Status Events - Service and Support - Server Management - IMM Management - Server Management - IMM Management - Server - S	sarch
Network Protocol Properties Network setting such as SNMP and LDAP used by the IMM Apply Reset Ethernet SNMP DNS DDNS SMTP LDAP Teinet USB Port	Assignments
Simple Network Management Protocol (SNMP) Configure SNMP v1 and/or v3 agents. Enable SNMPv1 Agent Enable SNMPv3 Agent Enable SNMP Traps	

2. Wählen Sie das entsprechende Kontrollkästchen aus, um den SNMPv1-Agenten, den SNMPv3-Agenten oder SNMP-Traps zu aktivieren.

- **3.** Wenn Sie den SNMPv1-Agenten aktivieren, fahren Sie mit Schritt 4 fort. Wenn Sie den SNMPv3-Agenten aktivieren, fahren Sie mit Schritt 5 fort. Wenn Sie die SNMP-Traps aktivieren, fahren Sie mit Schritt 6 auf Seite 76 fort.
- 4. Füllen Sie die folgenden Felder aus, wenn Sie den SNMPv1-Agenten aktiviert haben:
  - a. Klicken Sie auf die Registerkarte **Contact** (Ansprechpartner). Geben Sie im Feld **Contact person** (Ansprechpartner) den Namen des Ansprechpartners ein. Geben Sie im Feld **Location** (Standort) den Standort (geografische Koordinaten) ein.
  - b. Klicken Sie auf die Registerkarte **Communities**, um eine Community zum Definieren der Verwaltungsbeziehungen zwischen SNMP-Agenten und SN-MP-Managern zu konfigurieren. Sie müssen mindestens eine Community definieren.

#### 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 dann zum Anfang der Seite und klicken Sie auf **Apply** (Übernehmen), um die korrigierten Informationen zu speichern.
- Sie müssen mindestens eine Community konfigurieren, um diesen SNMP-Agenten zu aktivieren.

Machen Sie in folgenden Feldern die erforderlichen Angaben:

- 1) Geben Sie im Feld **Community Name** (Community-Name) einen Namen oder eine Zeichenfolge zur Authentifizierung ein, um die Community zu benennen.
- 2) Wählen Sie im Feld Access Type (Zugriffstyp) einen Zugriffstyp aus.
  - Wählen Sie **Trap** aus, um allen Hosts in der Community das Empfangen von Traps zu ermöglichen.
  - Wählen Sie **Get** (Abrufen) aus, um allen Hosts in der Community das Empfangen von Traps und das Abfragen von MIB-Objekten (Management Information Base) zu ermöglichen.
  - Wählen Sie **Set** (Festlegen) aus, um allen Hosts in der Community das Empfangen von Traps sowie das Abfragen und Festlegen von MIB-Objekten (Management Information Base) zu ermöglichen.
- c. Geben Sie im Feld **Host Name** (Hostname) oder im Feld **IP Address** (IP-Adresse) den Hostnamen oder die IP-Adresse der einzelnen Community-Manager ein.
- d. Klicken Sie auf **Apply**, um die vorgenommenen Änderungen zu übernehmen.
- 5. Füllen Sie die folgenden Felder aus, wenn Sie den SNMPv3-Agenten aktiviert haben:
  - a. Klicken Sie auf die Registerkarte **Contact** (Ansprechpartner). Geben Sie im Feld **Contact person** (Ansprechpartner) den Namen des Ansprechpartners ein. Geben Sie im Feld **Location** (Standort) den Standort (geografische Koordinaten) ein.
  - b. Klicken Sie auf die Registerkarte **Users** (Benutzer), um die Liste der lokalen Benutzerkonten für die Konsole anzuzeigen.

**Anmerkung:** Es handelt sich um dieselbe Liste, die über die Option "Users" angezeigt wird. Sie müssen SNMPv3 für alle Benutzerkonten konfigurieren, für die ein SNMPv3-Zugriff erforderlich ist.

- Klicken Sie auf Apply, um die vorgenommenen Änderungen zu übernehmen.
- 6. Wenn Sie die SNMP-Traps aktivieren, konfigurieren Sie die Ereignisse, die auf der Registerkarte **Traps** gemeldet werden.

**Anmerkung:** Bei der Konfiguration von SNMP werden erforderliche Felder, die nicht vollständig sind oder falsche Werte enthalten, mit einem roten X hervorgehoben, das Sie dabei unterstützt, die erforderlichen Felder (richtig) auszufüllen.

In der folgenden Abbildung ist die Registerkarte "SNMP" bei der Konfiguration des SNMPv1-Agenten dargestellt.



### **DNS konfigurieren**

Klicken Sie auf die Registerkarte **DNS**, um die Einstellungen für das IMM2-DNS (Domain Name System) anzuzeigen oder zu ändern. Wenn Sie das Kontrollkästchen **Use additional DNS address servers** (Zusätzliche DNS-Adressserver verwenden) auswählen, können Sie die IP-Adressen von bis zu drei DNS-Servern in Ihrem Netz angeben. Jede IP-Adresse muss aus Ganzzahlen von 0 bis 255 bestehen, die voneinander durch Punkte getrennt sind (wie in der folgenden Abbildung dargestellt).



# **DDNS konfigurieren**

Klicken Sie auf die Registerkarte **DDNS**, um die Einstellungen für das IMM2-DDNS (Dynamic Domain Name System) anzuzeigen oder zu ändern. Wählen Sie das Kontrollkästchen **Enable DDNS** (DDNS aktivieren) aus, um DDNS zu aktivieren. Wenn DDNS aktiviert ist, benachrichtigt das IMM2 einen DNS-Server, wenn die aktive DNS-Konfiguration der konfigurierten Hostnamen, Adressen oder anderer im DNS gespeicherter Informationen in Echtzeit geändert werden sollen.

Wählen Sie eine Option aus der Elementliste aus, um anzugeben, wie der Domänenname des IMM2 ausgewählt werden soll (wie in der folgenden Abbildung dargestellt).



## SMTP konfigurieren

Klicken Sie auf die Registerkarte **SMTP**, um die SMTP-Einstellungen für das IMM2 anzuzeigen oder zu ändern. Füllen Sie die folgenden Felder aus, um SMTP-Einstellungen anzuzeigen oder zu ändern:

#### IP address or host name (IP-Adresse oder Hostname)

Geben Sie 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.

**Port** Geben Sie die Portnummer für den SMTP-Server ein. Der Standardwert ist 25.

#### Test connection (Verbindung testen)

Klicken Sie auf **Test Connection**, um eine Test-E-Mail zu senden und zu überprüfen, ob Ihre SMTP-Einstellungen richtig sind.

In der folgenden Abbildung ist die Registerkarte "SMTP" dargestellt.

IBM Integrated Manage	ment Module II						
System Status	Events   Service and	Support 🗸 Se	rver Managem	nent 👻 IMM	Managemen	t + Search	
Network Protoc Network setting such as SNM Apply Reset Ethemet SNMP	DNS DDNS	S IMM SMTP	LDAP	Tehet	USB	Port Assignments	
Simple Mail Trans Provide the information fo IP address or host name:	r an SMTP server. This w	<b>∖TP)</b> ∥ be used if you	configure ale	erts to be sent	: via E-Mail.		
0.0.0.0	25						
Test Connection							

# LDAP konfigurieren

Klicken Sie auf die Registerkarte LDAP, um die Einstellungen für den LDAP-Client für das IMM2 anzuzeigen oder zu ändern.

**Anmerkung:** In einem IBM Flex System-Knoten wird das IMM2 für den LDAP-Server konfiguriert, der auf dem CMM ausgeführt wird. Sie werden in einer Informationsnachricht darauf hingewiesen, dass die LDAP-Einstellungen nicht geändert werden können (wie in der folgenden Abbildung dargestellt).

i	The protocols listed below are preset to comply with required security policies.
	LDAP is pre-configured

Mithilfe eines LDAP-Servers kann das IMM2 einen Benutzer durch Abfragen oder Durchsuchen eines LDAP-Verzeichnisses auf einem LDAP-Server ohne Abfragen der lokalen Benutzerdatenbank authentifizieren. Anschließend kann das IMM2 jeden Benutzerzugriff über einen zentralen LDAP-Server authentifizieren. Sie können Berechtigungsstufen auf der Basis der Informationen auf dem LDAP-Server zuordnen. Sie können LDAP auch dazu verwenden, Benutzer und IMM2-Module Gruppen zuzuordnen und eine Gruppenauthentifizierung zusätzlich zu der normalen Benutzerauthentifizierung (Kennwortprüfung) durchzuführen. Ein IMM2 kann z. B. einer oder mehreren Gruppen zugehörig sein. In diesem Fall besteht der Benutzer die Gruppenauthentifizierung nur dann, wenn er zu mindestens einer der Gruppen gehört, die dem IMM2 zugeordnet sind.

In der folgenden Abbildung ist die Registerkarte "LDAP" dargestellt.

IBM Integrated Management Mo	dule II	USER
System Status Events •	Service and Support   Server Management   IMM Management   Search	
Network Protocol Pr Network setting such as SNMP and LD Apply Reset	Operties Prused by the IMM	
Ethernet SNMP DNS	DDNS SMTP LDAP Teinet US8 Port Assignments	
Lightweight Directory A The JMM contains a Version 2.2 Oper authentication can be discovered dy	:cess Protocol (LDAP) Client nLDAP clent that can be configured to provide user authentication through one or more LDAP servers. The LDAP server(s) to be us namcally or manually pre-configured. Use the pull-down list to select which of these two methods should be used.	ed for
Use LDAP Servers for: Authentication	and Authorization *	
Active Directory Settings:		
Enable enhanced role-based	ecurity for Active Directory Users	
Use Pre-configured LDAP servers	0	
Host name or IP address	Port 🖉	
0.0.0	389	
	389	
	389	
	963	
Miscallanaous Cattings		
Pliscellaneous Setungs		
Root distinguished name: 🤍		
UID search attribute:		
annocountraine.		
Anonymously +		
Group Filter		
Group Search Attribute 🖗 memberOf		
Login Permission Attribute 🧐		

Um einen vorkonfigurierten LDAP-Server zu verwenden, füllen Sie die folgenden Felder aus:

#### Elementliste "LDAP server configuration" (LDAP-Server-Konfiguration)

Wählen Sie **Use Pre-Configured LDAP Server** (Vorkonfigurierten LDAP-Server verwenden) in der Elementliste aus. Die Portnummer für die einzelnen Server ist optional. Wenn in diesem Feld keine Angaben gemacht werden, wird der Standardwert 389 für nicht sichere LDAP-Verbindungen verwendet. Für sichere Verbindungen lautet der Standardwert 636. Sie müssen mindestens einen LDAP-Server konfigurieren.

#### Root distinguished name (Definierter Name für den Stammeintrag)

Der definierte Name (DN) für den Stammeintrag der Verzeichnisstruktur des LDAP-Servers (z. B. dn=mycompany,dc=com). Dieser definierte Name wird als Basisobjekt für alle Suchvorgänge verwendet.

#### UID search attribute (UID-Suchattribut)

Wenn als Bindungsmethode **Anonymously** (Anonym) oder **With Configured Credentials** (Mit konfigurierten Berechtigungsnachweisen) festgelegt wurde, folgt der einleitenden Verbindung zum LDAP-Server eine Suchanforderung, die bestimmte Informationen zum Benutzer abruft, einschließlich des definierten Namens (DN), der Anmeldeberechtigungen und der Gruppenmitgliedschaft des Benutzers. Diese Suchanforderung muss den Attributnamen angeben, der für die Benutzer-IDs auf diesem Server steht. Dieser Attributname wird in diesem Feld konfiguriert. Auf Active Directory-Servern lautet der Attributname normalerweise **sAMAccountName**. Auf Novell eDirectory- und OpenLDAP-Servern lautet der Attributname **uid**. Wenn in diesem Feld keine Angaben gemacht werden, lautet der Standardwert **uid**.

#### **Binding method (Bindungsmethode)**

Bevor eine Suchanfrage oder eine Abfrage an den LDAP-Server gesendet werden kann, muss eine Bindeanforderung gesendet werden. Mit diesem Feld wird gesteuert, wie diese einleitende Verbindung zum LDAP-Server ausgeführt wird. Die folgenden Bindungsmethoden sind verfügbar:

- Anonymously (Anonym)
  - Mit dieser Methode wird eine Bindung ohne einen definierten Namen oder ein Kennwort hergestellt. Diese Methode sollte jedoch nicht verwendet werden, da die meisten Server so konfiguriert sind, dass sie Suchanforderungen für bestimmte Benutzersätze nicht zulassen.
- With Configured Credentials (Mit konfiguriertem Berechtigungsnachweis)
  - Mit dieser Methode wird eine Bindung mit einem konfigurierten definierten Namen und einem Kennwort hergestellt.
- With Login Credentials (Mit Berechtigungsnachweis für Anmeldung)
  - Mit dieser Methode wird eine Bindung mit dem Berechtigungsnachweis hergestellt, der beim Anmeldeprozess angegeben wird. Die Benutzer-ID kann als definierter Name, als vollständig qualifizierter Domänenname oder als eine Benutzer-ID angegeben werden, die mit der Angabe unter UID Search Attribute (UID-Suchattribut) übereinstimmt, die auf dem IMM2 konfiguriert wurde. Wenn die einleitende Verbindung erfolgreich hergestellt werden kann, wird eine Suche durchgeführt, um einen Eintrag auf dem LDAP-Server zu finden, der zu dem Benutzer gehört, der versucht, sich anzumelden. Falls erforderlich, wird ein zweiter Verbindungsversuch durchgeführt, diesmal mit dem definierten Benutzernamen, der aus dem LDAP-Datensatz des Benutzers abgerufen wurde, und dem Kennwort, das bei der Anmeldung eingegeben wurde. Schlägt dieser Versuch fehl, wird dem Benutzer der Zugriff verweigert. Der zweite Verbindungsversuch wird nur dann durchgeführt, wenn die Bindungsmethoden Anonymous oder With Configured Credentials verwendet werden.

#### Group Filter (Gruppenfilter)

Das Feld **Group Filter** (Gruppenfilter) wird für die Gruppenauthentifizierung verwendet. Nachdem der Berechtigungsnachweis des Benutzers erfolgreich überprüft wurde, wird versucht, die Gruppenauthentifizierung durchzuführen. Wenn die Gruppenauthentifizierung fehlschlägt, wird dem Benutzer die Anmeldung verweigert. Wenn der Gruppenfilter konfiguriert ist, gibt er an, zu welchen Gruppen der Serviceprozessor gehört. Das bedeutet, dass der Benutzer zu mindestens einer der konfigurierten Gruppen gehören muss, damit die Gruppenauthentifizierung erfolgreich durchgeführt werden kann. Wenn das Feld **Group Filter** leer ist, ist die Gruppenauthentifizierung automatisch erfolgreich. Wenn der Gruppenfilter konfiguriert wurde, 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.

Beim Abgleich muss die Groß-/Kleinschreibung beachtet werden. Der Filter ist auf 511 Zeichen begrenzt und kann aus einem oder aus mehreren Gruppennamen bestehen. Um mehrere Gruppennamen voneinander abzugrenzen, muss das Doppelpunktzeichen (:) verwendet werden. Vorangestellte und nachgestellte Leerzeichen werden nicht beachtet. Alle anderen Leerzeichen werden als Teil des Gruppennamens behandelt. Sie haben die Möglichkeit, auszuwählen, ob Platzhalterzeichen in Gruppennamen verwendet werden sollen oder nicht. Der Filter kann ein bestimmter Gruppenname (z. B. IMMWest), ein Stern (\*), der als Platzhalterzeichen für alle anderen Zeichen steht, oder ein Platzhalterzeichen mit einem Präfix (z. B. IMM\*) sein. Der Standardfilter lautet "IMM\*". Wenn die Sicherheitsrichtlinien in Ihrer Installation die Verwendung von Platzhalterzeichen untersagen, können Sie auswählen, dass keine Platzhalterzeichen zulässig sind. Das Platzhalterzeichen (\*) wird dann als normales Zeichen und nicht als Platzhalter behandelt. Ein Gruppenname kann als vollständiger definierter Name oder nur mithilfe des *cn*-Teils angegeben werden. Beispiel: Eine Gruppe mit dem definierten Namen

"cn=adminGroup,dc=mycompany,dc=com" kann mit dem tatsächlichen definierten Namen oder mit "adminGroup" angegeben werden.

verschachtelte Gruppenmitgliedschaften werden nur in Active Directory-Umgebungen unterstützt. Wenn ein Benutzer z. B. ein Mitglied von GroupA und GroupB ist und GroupA auch ein Mitglied von GroupC ist, ist der Benutzer (implizit) auch ein Mitglied von GroupC. Verschachtelte Suchprozesse werden nach dem Durchsuchen von 128 Gruppen gestoppt. Zuerst werden alle Gruppen einer Ebene durchsucht, bevor Gruppen einer tieferen Ebene durchsucht werden. Schleifen werden nicht erkannt.

#### Group Search Attribute (Attribut für die Gruppensuche)

In einer Active Directory- oder Novell eDirectory-Umgebung gibt das Feld **Group Search Attribute** den Attributnamen an, der die Gruppen bezeichnet, denen ein Benutzer angehört. In einer Active Directory-Umgebung lautet der Attributname **memberOf**. In einer eDirectory-Umgebung lautet der Attributname **groupMembership**. In einer OpenLDAP-Serverumgebung werden Benutzer normalerweise Gruppen zugeordnet, deren objectClass gleich "PosixGroup" ist. In diesem Kontext gibt dieses Feld den Attributnamen an, der die Mitglieder einer bestimmten PosixGroup bezeichnet. Dieser Attributname lautet **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 erfolgreich über einen LDAP-Server authentifiziert wird, müssen die Anmeldeberechtigungen für den Benutzer abgerufen werden. Um diese Anmeldeberechtigungen abzurufen, muss der an den Server gesendete Suchfilter den Attributnamen angeben, der den Anmeldeberechtigungen zugeordnet wurde. Das Feld **Login Permission Attribute** gibt den Attributnamen an. Wenn in diesem Feld keine Angaben gemacht werden, werden dem Benutzer standardmäßig Leseberechtigungen zugeordnet, vorausgesetzt, der Benutzer besteht die Benutzer- und die Gruppenauthentifizierung.

Der vom LDAP-Server zurückgegebene Attributwert sucht nach der Suchbegriffszeichenfolge "IBMRBSPermissions=". Auf diese Suchbegriffszeichenfolge muss unmittelbar danach eine Bitfolge (aus bis zu 12 aufeinanderfolgenden Nullen oder Einsen) folgen. Jedes Bit steht für eine Gruppe von Funktionen. Die Bits sind entsprechend ihren Positionen nummeriert. Das erste Bit (links) ist Bitposition 0, das letzte Bit (rechts) ist Bitposition 11. Der Wert 1 in einer Bitposition aktiviert die Funktion, die dieser Bitposition zugeordnet ist. Der Wert 0 in einer Bitposition inaktiviert die Funktion, die dieser Bitposition zugeordnet ist.

Ein gültiges Beispiel ist die Zeichenfolge "IBMRBSPermissions=01000000000". Der Suchbegriff "IBMRBSPermissions=" wird verwendet, damit er in einer beliebigen Position in diesem Feld platziert werden kann. So kann der LDAP-Administrator ein vorhandenes Attribut wiederverwenden und eine Erweiterung des LDAP-Schemas verhindern. Außerdem ermöglicht es die Verwendung des Attributs für seine ursprüngliche Bestimmung. Sie können die Suchbegriffszeichenfolge in eine beliebige Position in diesem Feld einfügen. Das verwendete Attribut lässt eine frei formatierte Zeichenfolge zu. Wenn das Attribut erfolgreich abgerufen werden kann, wird der Wert, der vom LDAP-Server zurückgegeben wird, entsprechend den Informationen in der folgenden Tabelle interpretiert.

Bit- position	Funktion	Erläuterung
0	Deny Always (Nie zulassen)	Die Authentifizierung eines Benutzers schlägt immer fehl. Diese Funktion kann verwendet werden, um einen oder mehrere bestimmte Benutzer, die einer bestimmten Gruppe zugeordnet sind, zu blockieren.
1	Supervisor Access (Administratorzugriff)	Einem Benutzer wird die Administratorberechtigung erteilt. Der Benutzer hat Schreib-/Lesezugriff auf jede Funktion. Wenn Sie dieses Bit ein- stellen, müssen Sie die anderen Bits nicht einzeln einstellen.
2	Read Only Access (Lesezugriff)	Ein Benutzer hat Lesezugriff und kann keine Wartungsarbeiten (beispielsweise Neustart, fern ausgeführte Aktionen oder Firmwareaktualisierungen) oder Änderungen (wie z. B. Funktionen zum Speichern, Löschen oder Wieder- herstellen) durchführen. Bitposition 2 und alle anderen Bits schließen sich gegenseitig aus, wobei Bitposition 2 die niedrigste Vorrangstellung hat. Wenn irgendein anderes Bit gesetzt ist, wird dieses Bit ignoriert.
3	Networking and Security (Netzbetrieb und Sicherheit)	Ein Benutzer kann die Konfiguration für "Security" (Sicherheit), "Network Protocols" (Netzprotokolle), "Network Interface" (Netzschnittstelle), "Port Assignments" (Portzuordnungen) und "Serial Port" (Serieller Anschluss) än- dern.
4	User Account Management (Benutzerkontenverwaltung)	Ein Benutzer kann andere Benutzer hinzufügen, ändern oder löschen und die "Global Login Settings" (Globale Anmeldungseinstellungen) im Fenster "Login Profiles" (Anmeldeprofile) än- dern.
5	Remote Console Access (Zugriff auf ferne Konsole)	Ein Benutzer kann auf die Remote- Server-Konsole zugreifen.
6	Remote Console and Remote Disk Access (Zugriff auf ferne Konsole und fernen Datenträger)	Ein Benutzer kann auf die Remote- Server-Konsole und die Funktionen für ferne Datenträger für den fernen Ser- ver zugreifen.
7	Remote Server Power/Restart Access (Zugriff auf Einschalten/Neustart des fernen Servers)	Der Benutzer kann auf die Einschalt- und Neustartfunktionen für den fernen Server zugreifen.

Tabelle 4. Berechtigungsbits

Bit- position	Funktion	Erläuterung
8	Basic Adapter Configuration (Basisadapterkonfiguration)	Ein Benutzer kann Konfigurationsparameter auf den Sei- ten "System Settings" (Systemeinstel- lungen) und "Alerts" ändern.
9	Ability to Clear Event Logs (Fähigkeit, Ereignisprotokolle zu löschen)	Ein Benutzer kann die Ereignisprotokolle löschen. <b>Anmerkung:</b> Alle Benutzer können die Ereignisprotokolle einsehen; um jedoch die Protokolle löschen zu kön- nen, muss der Benutzer diese Berechtigungsstufe haben.
10	Advanced Adapter Configuration (Er- weiterte Adapterkonfiguration)	Für Benutzer gelten keine Einschrän- kungen beim Konfigurieren des IMM2. Außerdem verfügt der Benutzer über einen Verwaltungszugriff auf das IMM2. Der Benutzer kann folgende erweiterte Funktionen ausführen: Firmwareaktualisierungen, PXE- Netzboot, werkseitige IMM2- Voreinstellungen wiederherstellen, die Adapterkonfiguration aus einer Konfigurationsdatei ändern und wie- derherstellen und das IMM2 erneut starten bzw. zurücksetzen.
11	Reserved (Reserviert)	Diese Bitposition ist für den künftigen Gebrauch reserviert. Wenn keines der Bits gesetzt ist, hat der Benutzer eine Leseberechtigung. Priorität haben die Anmeldeberechtigungen, die direkt aus dem Benutzersatz abgerufen wer- den.
		Wenn das Attribut für die Anmeldeberechtigung nicht im Datensatz des Benutzers enthalten ist, wird versucht, die Berechtigungen von den Gruppen abzurufen, zu denen der Benutzer gehört. Dies wird als Teil der Gruppenauthentifizierungsphase aus- geführt. Dem Benutzer wird das inklu- sive OR aller Bits für alle Gruppen zugewiesen.
		Das Bit für den Lesezugriff (Position 2) wird nur gesetzt, wenn alle anderen Bits auf null gesetzt werden. Wenn das Bit für "Deny Always" (Position 0) für eine der Gruppen gesetzt ist, wird dem Benutzer der Zugriff verweigert. Das Bit "Deny Always" (Position 0) hat vor allen anderen Bits Vorrang.

Tabelle 4. Berechtigungsbits (Forts.)

# Telnet konfigurieren

Wählen Sie die Registerkarte **Telnet** aus, um die Telnet-Einstellungen für das IMM2 anzuzeigen oder zu ändern. Füllen Sie die folgenden Felder aus, um Telnet-Einstellungen anzuzeigen oder zu ändern:

#### Allow telnet access (Telnet-Zugriff zulassen)

Wählen Sie das entsprechende Kontrollkästchen aus, wenn das IMM2 einen Telnet-Zugriff zulassen soll.

Allowed simultaneous connections (Zugelassene gleichzeitige Verbindungen) Wählen Sie mithilfe der Liste Allowed simultaneous connections die Anzahl an gleichzeitigen Telnet-Verbindungen aus, die zulässig sind.

In der folgenden Abbildung ist die Registerkarte "Telnet" dargestellt.



## **USB** konfigurieren

Wählen Sie die Registerkarte **USB** aus, um die IMM2-USB-Einstellungen für das IMM2 anzuzeigen oder zu ändern. Die USB-Inband-Schnittstelle (oder Schnittstelle "LAN over USB") wird für die Inbandkommunikation zum IMM2 verwendet. Klicken Sie auf das Kontrollkästchen **Enable Ethernet over USB** (Ethernet over USB aktivieren), um die IMM2-Schnittstelle "LAN over USB" zu aktivieren oder zu inaktivieren.

Wichtig: Wenn Sie die USB-Inband-Schnittstelle inaktivieren, können Sie keine Inband-Aktualisierung der IMM2-Firmware, der Server-Firmware und der DSA-Firmware mithilfe der Linux- oder Windows-Flashdienstprogramme durchführen. Wenn die USB-Inband-Schnittstelle inaktiviert ist, verwenden Sie die Option "Firmware Server" auf der Registerkarte "Server Management" zum Aktualisieren der Firmware. Wenn Sie die USB-Inband-Schnittstelle inaktivieren, inaktivieren Sie auch die Watchdog-Zeitlimitüberschreitungen, um zu verhindern, dass der Server unerwartet neu startet.

In der folgenden Abbildung ist die Registerkarte "USB" dargestellt.

thernet	SI	IMP	DNS D	DNS	SMTP	LDAP	Telnet	USB	
nivers ontrol the nass stora Enable E	al Se e USB i ge). Etherne	erial Bus nterface us et over USB	(USB) Se ed for in-band	ettings communicati	ion betwe	en the server	and the IMM.	This setti	
E	Add N	external Eth lapping	Remove	net over US	B port for	warding 🥯			
		External E	thernet port nu	mber	▲ Eth	nernet over US	B port numbe	r	
	0	0			0	0			
	0	0			0				
	0	0			0				
	0	0			0				
	0	0			0				
	0	0			0				
	0	0			0				
	0	0			0				
	0	3389			338	89			

Die Zuordnung von externen Ethernet-Portnummern zu Ethernet-over-USB-Portnummern können Sie durch Klicken auf das Kontrollkästchen **Enable external Ethernet to Ethernet over USB port forwarding** (Weiterleitung von externem Ethernet-Port zu Ethernet-over-USB-Port) steuern. Füllen Sie anschließend die Zuordnungsinformationen für die Ports aus, für die die Weiterleitung gelten soll.

# Portzuordnungen konfigurieren

Wählen Sie die Registerkarte **Port Assignments** (Portzuordnungen) aus, um die Portzuordnungen für das IMM2 anzuzeigen oder zu ändern. Füllen Sie die folgenden Felder aus, um Portzuordnungen anzuzeigen oder zu ändern:

**HTTP** Geben Sie in diesem Feld die Portnummer für den HTTP-Server des IMM2 an. Der Standardwert ist 80. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

#### HTTPS

Geben Sie in diesem Feld die Portnummer an, die für Webschnittstellen-HTTPS-SSL-Datenverkehr verwendet wird. Der Standardwert ist 443. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

#### Telnet CLI (Telnet-Befehlszeilenschnittstelle)

Geben Sie in diesem Feld die Portnummer für die traditionelle Befehlszeilenschnittstelle für die Anmeldung über den Telnet-Service an. Der Standardwert ist 23. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

#### SSH Legacy CLI (Traditionelle SSH-Befehlszeilenschnittstelle)

Geben Sie in diesem Feld die Portnummer an, die für die traditionelle Befehlszeilenschnittstelle für die Anmeldung über das SSH-Protokoll konfiguriert ist. Der Standardwert ist 22.

#### SNMP Agent (SNMP-Agent)

Geben Sie in diesem Feld die Portnummer für den SNMP-Agenten an, der auf dem IMM2 ausgeführt wird. Der Standardwert ist 161. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

#### SNMP Traps (SNMP-Traps)

Geben Sie in diesem Feld die Portnummer an, die für SNMP-Traps verwendet wird. Der Standardwert ist 162. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

#### **Remote Control (Fernsteuerung)**

Geben Sie in diesem Feld die Portnummer an, die die Fernsteuerungsfunktion für Anzeige und Interaktion mit der Serverkonsole verwendet. Der Standardwert lautet 3900 für in Gehäuse installierte Server und Turmserver.

#### CIM over HTTP

Geben Sie in diesem Feld die Portnummer für CIM over HTTP an. Der Standardwert ist 5988.

#### CIM over HTTPS

Geben Sie in diesem Feld die Portnummer für CIM over HTTPS an. Der Standardwert ist 5989.

In der folgenden Abbildung ist die Registerkarte "Port Assignments" dargestellt.

IBM Integrated	i Manage	ment Module II						USERID	Settings
System	Status I	Events     Service and	Support + S	ierver Manage	ement + DAD	I Manageme	nt + Search		
Network   Network setting st Apply Reset	Proto	col Propertie	S e 34M						
Ethernet 5	SNMP	DNS DONS	SMTP	LDAP	Teinet	USB	Port Assignments		
Currently open p HTTP HTTPS	80 443	3, 80, 115, 121, 161, 4	27, 443, 546,	623, 3389, 3	900, 5900, 59	88, 5989, 93	993		
Teinet CLI	443 23	0							
SSH CLI SNMP agent	22	0							
SNMP Traps	162	0							
Remote Control	3900	9							
CIM Over HTTP	5988	a							

## Sicherheitseinstellungen konfigurieren

Klicken Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) auf die Option **Security** (Sicherheit), um auf die Sicherheitseigenschaften, den Status und die Einstellungen für das IMM2 zuzugreifen und sie zu konfigurieren (wie in der folgenden Abbildung dargestellt).

Um Ihre Änderungen zu übernehmen, klicken Sie oben links im Fenster "IMM Security" auf die Schaltfläche **Apply** (Übernehmen). Um Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Reset Values** (Werte zurücksetzen).

IMM Management 👻 Search	h
IMM Properties	Various properties and settings related to the IMM
Users	Create and modify user accounts and group profiles that will have access to the IMM console
Network	Network settings such as SNMP and LDAP used by the IMM
Security	Configure security protocols such as SSL and SSH
IMM Configuration	View a summary of the current configuration settings.
Restart IMM	Restart the IMM. Typically only needed when experiencing problems with the IMM
Reset IMM to factory defaults	Sets all current configuration settings back to default values
Activation Key Management	Add and remove activation keys for additional functionality

# **HTTPS-Protokoll konfigurieren**

Klicken Sie auf die Registerkarte **HTTPS Server**, um die IMM2-Webschnittstelle so zu konfigurieren, dass sie das sicherere HTTPS-Protokoll und nicht das HTTP-Standardprotokoll verwendet.

#### Anmerkungen:

- Es kann nur ein Protokoll aktiviert sein.
- Das Aktivieren dieser Option erfordert eine zusätzliche Konfiguration der SSL-Zertifikate.
- Wenn Sie das Protokoll ändern, müssen Sie anschließend den IMM2-Web-Server erneut starten.

Weitere Informationen zu SSL finden Sie im Abschnitt "Übersicht über SSL" auf Seite 92. In der folgenden Abbildung ist die Registerkarte "HTTPS Server" dargestellt.

Configure securit	J <b>rity</b> y protocols such as H	TTPS and SSH.	. Manage secu	ity certificates.
Apply Reset	Values			
HTTPS Server	CIM Over HTTPS	LDAP Client	SSH Server	
Enable HTTI	PS server @			
HTTPS Server	certificate status: A si	igned certificate	e is installed. A	CSR has been generated.
HTTPS Server	certificate status: A s	igned certificate Actions	e is installed. A	CSR has been generated.
HTTPS Server	certificate status: A s	igned certificate Actions ed Certificate	e is installed. A	CSR has been generated.
HTTPS Server Generate a Nev Generate a Nev	certificate status: A si w Key and a Self-sign w Key and a Certificat	igned certificate Actions ed Certificate te Signing Requ	e is installed. A est (CSR)	CSR has been generated.
HTTPS Server Generate a Nev Generate a Nev Import a Signe	certificate status: A si w Key and a Self-sign w Key and a Certificat d Certificate	igned certificate Actions ed Certificate le Signing Requ	e is installed. A est (CSR)	CSR has been generated.
HTTPS Server Generate a New Generate a New Import a Signe Download Cert	certificate status: A si w Key and a Self-sign w Key and a Certificat d Certificate tificate	igned certificate Actions ed Certificate te Signing Requ	e is installed. A est (CSR)	CSR has been generated.

**Anmerkung:** Auf manchen Servern werden die IMM2-Sicherheitsstufen möglicherweise von einem anderen Managementsystem gesteuert. In diesen Umgebungen können Sie die oben genannten Aktionen in der IMM2-Webschnittstelle inaktivieren.

### Handhabung von HTTPS-Zertifikaten

Verwenden Sie die Optionen im Menü "Actions" für die Handhabung von HTTPS-Zertifikaten. Wenn eine Option inaktiviert ist, müssen Sie möglicherweise zuerst eine andere Aktion ausführen, um diese Option zu aktivieren. Während Sie mit HTTPS-Zertifikaten arbeiten, sollten Sie den HTTPS-Server inaktivieren. Weitere Informationen zur Handhabung von Zertifikaten finden Sie im Abschnitt "Handhabung von SSL-Zertifikaten" auf Seite 92.

**Anmerkung:** Nachdem Sie die Handhabung von Zertifikaten konfiguriert haben, müssen Sie das IMM2 erneut starten, damit Ihre Änderungen wirksam werden.

## **CIM-over-HTTPS-Protokoll konfigurieren**

Klicken Sie auf die Registerkarte **CIM over HTTPS**, um die IMM2-Webschnittstelle so zu konfigurieren, dass sie das sicherere CIM-over-HTTPS-Protokoll und nicht das CIM-over-HTTP-Standardprotokoll verwendet.

#### Anmerkungen:

- Es kann nur ein Protokoll aktiviert sein.
- Das Aktivieren dieser Option erfordert eine zusätzliche Konfiguration der SSL-Zertifikate.
- Wenn Sie das Protokoll ändern, müssen Sie anschließend den IMM2-Web-Server erneut starten.

Weitere Informationen zu SSL finden Sie im Abschnitt "Übersicht über SSL" auf Seite 92. In der folgenden Abbildung ist die Registerkarte "CIM over HTTPS" dargestellt.

onfigure security protocols such as H	ITTPS and SSH.	Manage securit	y certificates.
Apply Reset Values			
HTTPS Server CIM Over HTTPS	LDAP Client	SSH Server	
Enable CIM Over HTTPS			
Certificate Management @ Certificate status:A signed certificate	e is installed.		
Certificate Management @ Certificate status:A signed certificate	e is installed. Actions		
Certificate Management Certificate status:A signed certificate Generate a New Key and a Self-sign	e is installed. Actions ed Certificate		@
Certificate Management Certificate status:A signed certificate Generate a New Key and a Self-sign Generate a New Key and a Certificat	e is installed. Actions ed Certificate te Signing Reque	est (CSR)	e e
Certificate Management Certificate status: A signed certificate Generate a New Key and a Self-sign Generate a New Key and a Certificat Import a Signed Certificate	e is installed. Actions ed Certificate te Signing Reque	est (CSR)	9
Certificate Management Certificate status: A signed certificate Generate a New Key and a Self-sign Generate a New Key and a Certificat Import a Signed Certificate Download Certificate	e is installed. Actions ed Certificate te Signing Reque	est (CSR)	9

### Handhabung von CIM-over-HTTPS-Zertifikaten

Verwenden Sie die Optionen im Menü "Actions" für die Handhabung von CIMover-HTTPS-Zertifikaten. Wenn eine Option inaktiviert ist, müssen Sie möglicherweise zuerst eine andere Aktion ausführen, um diese Option zu aktivieren. Weitere Informationen zur Handhabung von Zertifikaten finden Sie im Abschnitt "Handhabung von SSL-Zertifikaten" auf Seite 92.

**Anmerkung:** Nachdem Sie die Handhabung von Zertifikaten konfiguriert haben, müssen Sie das IMM2 erneut starten, damit Ihre Änderungen wirksam werden.

# Protokoll für LDAP-Client konfigurieren

Klicken Sie auf die Option **LDAP Client**, um das sicherere LDAP-over-SSL-Protokoll anstatt des LDAP-Standardprotokolls zu verwenden.

**Anmerkung:** Das Aktivieren dieser Option erfordert eine zusätzliche Konfiguration der SSL-Zertifikate.

Weitere Informationen zu SSL finden Sie im Abschnitt "Übersicht über SSL" auf Seite 92. In der folgenden Abbildung ist die Registerkarte "LDAP Client" dargestellt.

onfigure security protocols such	h as HTTPS and SSH	. Manage security ce	rtificates.
Apply Reset Values			
HTTPS Server CIM Over HT	TPS LDAP Client	SSH Server	
LDAP security:			
LDAP security: @			
Disable secure LDAP			
Certificate Management	Ø		
Certificate Management Signed Certificate status:	No certificate is ins	talled.	
Certificate Management Signed Certificate status: Trusted certificates:	O certificate is ins <u>No trusted certificate</u>	italled. ates are installed	
Certificate Management Signed Certificate status: Trusted certificates:	No certificate is ins <u>No trusted certificate</u> Actions	talled. ates are installed	
Certificate Management Signed Certificate status: Trusted certificates: Generate a New Key and a Sel	No certificate is ins No trusted certificate Actions f-signed Certificate	talled. ates are installed	0
Certificate Management Signed Certificate status: Trusted certificates: Generate a New Key and a Self Generate a New Key and a Cer	No certificate is ins <u>No trusted certificate</u> <u>Actions</u> f-signed Certificate rtificate Signing Requ	talled. ates are installed est (CSR)	0
Certificate Management Signed Certificate status: Trusted certificates: Generate a New Key and a Self Generate a New Key and a Cer Import a Signed Certificate	No certificate is ins No trusted certificate Actions f-signed Certificate rtificate Signing Required	talled. ates are installed est (CSR)	0
Certificate Management Signed Certificate status: Trusted certificates: Generate a New Key and a Self Generate a New Key and a Cer Import a Signed Certificate Import a Trusted Certificate	No certificate is ins No trusted certificate Actions f-signed Certificate rtificate Signing Require	talled. ates are installed est (CSR)	0
Certificate Management Signed Certificate status: Trusted certificates: Generate a New Key and a Self Generate a New Key and a Cert Import a Signed Certificate Import a Trusted Certificate Download Certificate	No certificate is ins <u>No trusted certificate</u> <u>Actions</u> f-signed Certificate rtificate Signing Requi	talled. ates are installed est (CSR)	

### Handhabung von Zertifikaten für sicheren LDAP-Client

Verwenden Sie die Optionen im Menü "Actions" für die Handhabung von LDAPover-SSL-Zertifikaten. Wenn eine Option inaktiviert ist, müssen Sie möglicherweise zuerst eine andere Aktion ausführen, um diese Option zu aktivieren. Während Sie mit HTTPS-Zertifikaten arbeiten, sollten Sie den HTTPS-Server inaktivieren. Weitere Informationen zur Handhabung von Zertifikaten finden Sie im Abschnitt "Handhabung von SSL-Zertifikaten" auf Seite 92. Nachdem Sie das vertrauenswürdige Zertifikat (Trusted Certificate) installiert haben, können Sie LDAP over SSL aktivieren, wie in der folgenden Abbildung dargestellt.

#### Anmerkungen:

- Änderungen am IMM2 werden sofort wirksam.
- Ihr LDAP-Server muss SSL3 (Secure Socket Layer 3) oder TLS (Transport Layer Security) unterstützen, damit er kompatibel mit dem sicheren LDAP-Client des IMM2 ist.

MM Security onfigure security protocols suc Apply Reset Values	h as HTTPS and SSH.	Manage security certificate:	5.		
HTTPS Server CIM Over HT	TPS LDAP Client	SSH Server			
LDAP security:					
IDAD cocurtus Q				1	
Enable secure LDAP			- <		
Certificate Management Signed Certificate status: Trusted certificates:	A self-signed certificate	cate is installed. #1 is installed Download	Replace	Remove	
	Actions				
Generate a New Key and a Sel	f-signed Certificate		0		
Generate a New Key and a Certificate Signing Request (CSR)		est (CSR)	0		
Import a Signed Certificate			0		
Import a Trusted Certificate			0		
Download Certificate					
Download Certificate Signing	Request (CSR)				

# Secure Shell-Server konfigurieren

Klicken Sie auf die Registerkarte **SSH Server**, um die IMM2-Webschnittstelle so zu konfigurieren, dass sie das sicherere SSH-Protokoll und nicht das Telnet-Standardprotokoll verwendet.

#### Anmerkung:

- Für diese Option ist keine Zertifikatsverwaltung erforderlich.
- Das IMM2 erstellt anfangs einen SSH-Server-Schlüssel. Wenn Sie einen neuen SSH-Server-Schlüssel generieren möchten, klicken Sie im Menü "Actions" auf **Generate SSH Server Private Host Key** (Privaten SSH-Server-Host-Schlüssel generieren).
- Nachdem Sie diese Aktion abgeschlossen haben, müssen Sie das IMM2 erneut starten, damit Ihre Änderungen wirksam werden.

Die Registerkarte "SSH Server" ist in der folgenden Abbildung dargestellt.

Apply Reset	v protocols such as H Values	TTPS and SSH.	. Manage securit	y certificates.
HTTPS Server	CIM Over HTTPS	LDAP Client	SSH Server	
Enable SSH	Server			
💟 Enable SSH S	Server @			
Certificate M	anagement 🔍			
Key status: SSH	Server Key is installe	ed.		
		Actions		
Conorato SSH 9	erver Drivate Host K	ev		

# Übersicht über SSL

SSL ist ein Sicherheitsprotokoll, das eine geschützte Datenübertragung bereitstellt. SSL ermöglicht Client-/Serveranwendungen eine Datenübertragung, die gegen das Ausspionieren, das Manipulieren von Daten während der Übertragung und das Fälschen von Nachrichten geschützt ist. Sie können das IMM2 so konfigurieren, dass die SSL-Unterstützung für verschiedene Verbindungsmöglichkeiten, wie z. B. den sicheren Web-Server (HTTPS), die sichere LDAP-Verbindung (LDAPS), CIM over HTTPS oder den SSH-Server, verwendet wird. Sie können die SSL-Einstellungen mit der Option "Security" (Sicherheit) auf der Registerkarte "IMM Management" (IMM-Verwaltung) anzeigen oder ändern. Außerdem haben Sie auf dieser Seite die Möglichkeit, SSL zu aktivieren oder zu inaktivieren und die für SSL erforderlichen Zertifikate zu verwalten.

# Handhabung von SSL-Zertifikaten

Sie können SSL mit einem selbst signierten Zertifikat oder mit einem von einer unabhängigen Zertifizierungsstelle signierten Zertifikat verwenden. Ein selbst signiertes Zertifikat ist die einfachste Methode für die Verwendung von SSL, allerdings stellt es ein geringes Sicherheitsrisiko dar. Das Risiko besteht darin, dass der SSL-Client keine Möglichkeit hat, beim ersten Verbindungsversuch zwischen Client und Server die Identität des SSL-Servers zu prüfen. Beispielsweise besteht die Möglichkeit, dass ein anderer Anbieter die Identität des IMM2-Web-Servers vortäuschen und Daten zwischen dem tatsächlichen IMM2-Web-Server und dem Web-Browser des Benutzers abfangen könnte. Wenn das selbst signierte Zertifikat beim ersten Verbindungsaufbau zwischen dem Browser und dem IMM2 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 (CA) signiert ist. Klicken Sie auf **Generate a New Key and a Certificate Signing Request (CSR)** (Einen neuen Schlüssel und eine Zertifikatssignieranforderung (CSR) generieren) im Menü "Actions" (Aktionen), um ein signiertes Zertifikat zu erhalten. Senden Sie dann die Zertifikatssignieranforderung (CSR) an eine Zertifizierungsstelle (CA) und fordern Sie dort ein Endzertifikat an. Sobald Sie das Endzertifikat erhalten haben, klicken Sie auf **Import a Signed Certificate** (Ein signiertes Zertifikat importieren) im Menü "Actions", um es ins IMM2 zu importieren.

Die Aufgabe der Zertifizierungsstelle (CA) ist es, die Identität des IMM2 zu überprüfen. Ein Zertifikat enthält digitale Signaturen für die Zertifizierungsstelle (CA) und das IMM2. Wenn eine anerkannte Zertifizierungsstelle (CA) das Zertifikat ausstellt oder wenn das Zertifikat der Zertifizierungsstelle (CA) bereits in den Web-Browser importiert wurde, kann der Browser das Zertifikat validieren und den IMM2-Web-Server eindeutig identifizieren.

Das IMM2 erfordert ein Zertifikat für die Verwendung mit HTTPS-Servern, CIM over HTTPS und sicheren LDAP-Clients. Außerdem müssen für den sicheren LDAP-Client ebenfalls ein oder mehrere vertrauenswürdige Zertifikate importiert werden. Das vertrauenswürdige Zertifikat wird vom sicheren LDAP-Client verwendet, um den LDAP-Server sicher zu identifizieren. Das vertrauenswürdige Zertifikat ist das Zertifikat der Zertifizierungsstelle (CA), die das Zertifikat des LDAP-Servers signiert hat. Wenn der LDAP-Server selbst signierte Zertifikate verwendet, kann das vertrauenswürdige Zertifikat das Zertifikat des LDAP-Servers selbst sein. Sie müssen zusätzliche vertrauenswürdige Zertifikate importieren, wenn Sie in Ihrer Konfiguration mehrere LDAP-Server verwenden.

# Verwaltung von SSL-Zertifikaten

Wenn Sie IMM2-Zertifikate verwalten, erhalten Sie eine Liste mit Aktionen oder eine Teilliste (wie in der folgenden Abbildung dargestellt).

Actions	
Generate a New Key and a Self-signed Certificate	0
Generate a New Key and a Certificate Signing Request (CSR)	0
Import a Signed Certificate	0
Import a Trusted Certificate	0
Download Certificate	0
Download Certificate Signing Request (CSR)	0

Wenn derzeit ein Zertifikat installiert ist, können Sie die Aktion **Download Certificate** (Zertifikat herunterladen) im Menü "Actions" verwenden, um das derzeit installierte Zertifikat oder eine Zertifikatssignieranforderung herunterzuladen. Zertifikate, die abgeblendet sind, sind derzeit *nicht* installiert. Der sichere LDAP-Client erfordert, dass der Benutzer ein vertrauenswürdiges Zertifikat importiert. Klicken Sie auf **Import a Trusted Certificate** (Ein vertrauenswürdiges Zertifikat importieren) im Menü "Actions" (Aktionen). Klicken Sie nach Generierung einer Zertifikatssignieranforderung auf **Import a Signed Certificate** im Menü "Actions".

Wenn Sie eine der "Generate"-Aktionen ausführen, wird das Fenster "Generate New Key and Self-signed Certificate" (Neuen Schlüssel und selbst signiertes Zertifikat generieren) geöffnet (wie in der folgenden Abbildung dargestellt).

Required SSI	Certificate Data	۲
Country	US United States	7 0
State or Province	NY	G
City or Locality	New York	0
Organization Name	My Company	0
IMM Host Name	imm 1004	-
Optional SSL	. Certificate Data	
Optional SSL Contact Person	Certificate Data	0
Optional SSL Contact Person E-Mail address	Chris Manager cmanager@mycomp.com	
Optional SSL Contact Person E-Mail address Organizational Unit	Chris Manager cmanager@mycomp.com Sales	
Optional SSL Contact Person E-Mail address Organizational Unit Surname	Chris Manager cmanager@mycomp.com Sales	
Optional SSL Contact Person E-Mail address Organizational Unit Surname Given Name	Certificate Data Chris Manager cmanager@mycomp.com Sales	
Optional SSL Contact Person E-Mail address Organizational Unit Surname Given Name Initials	Certificate Data Chris Manager cmanager@mycomp.com Sales	

Das Fenster "Generate New Key and Self-signed Certificate" fordert Sie auf, die Pflicht- und Wahlfelder auszufüllen. Sie *müssen* die Pflichtfelder ausfüllen. Klicken Sie nach Angabe Ihrer Informationen auf **Ok**, um den Vorgang abzuschließen. Das Fenster "Certificate Generated" (Zertifikat generiert) wird geöffnet (wie in der folgenden Abbildung dargestellt).



# IMM-Konfiguration wiederherstellen und ändern

Wählen Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) die Option **IMM Configuration** (IMM-Konfiguration) aus, um folgende Aktionen ausführen zu können:

- Zusammenfassung der IMM2-Konfiguration anzeigen
- IMM2-Konfiguration sichern oder wiederherstellen
- Sicherungs- oder Wiederherstellungsstatus anzeigen
- IMM2-Konfiguration auf die werkseitig vorgenommenen Standardeinstellungen zurücksetzen
- Auf den Assistenten für die IMM2-Erstkonfiguration zugreifen

### IMM2 erneut starten

Wählen Sie die Option **Restart IMM** (IMM erneut starten) auf der Registerkarte "IMM Management" (IMM-Verwaltung) aus, um das IMM2 erneut zu starten. Nur Benutzer mit Administratorberechtigung können diese Funktion ausführen. Wenn Ethernet-Verbindungen vorübergehend unterbrochen wurden, müssen Sie sich am IMM2 anmelden, um auf die IMM2-Webschnittstelle zuzugreifen.

Gehen Sie wie folgt vor, um das IMM2 erneut zu starten:

- 1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt "Am IMM2 anmelden" auf Seite 10.
- 2. Klicken Sie auf die Registerkarte IMM Management und anschließend auf Restart IMM.
- **3**. Klicken Sie auf die Schaltfläche **OK** im Fenster "Confirm Restart" (Neustart bestätigen). Das IMM2 wird erneut gestartet.

In der folgenden Abbildung ist das Fenster "Confirm Restart" dargestellt.

Confi	Confirm Restart 2			
?>	Do you want to restart the IMM?			
	The IMM will be unavailable during the restart. When the restart is complete, you must log in to the IMM web console to access the IMM.	9		
ОК	Cancel			

Wenn Sie das IMM2 erneut starten, werden Ihre TCP/IP- oder Modemverbindungen unterbrochen.

In der folgenden Abbildung ist das Benachrichtigungsfenster dargestellt, das angezeigt wird, während das IMM2 erneut gestartet wird.



4. Melden Sie sich erneut an, um die IMM2-Schnittstelle zu verwenden (Anweisungen hierzu finden Sie im Abschnitt "Am IMM2 anmelden" auf Seite 10).

### IMM2 auf die werkseitigen Voreinstellungen zurücksetzen

Wählen Sie die Option **Reset IMM to factory defaults...** (IMM auf werkseitige Voreinstellungen zurücksetzen) aus der Registerkarte "IMM Management" (IMM-Verwaltung) aus, um das IMM2 auf die werkseitigen Voreinstellungen zurückzusetzen. Nur Benutzer mit Administratorberechtigung können diese Funktion ausführen. Wenn Ethernet-Verbindungen vorübergehend unterbrochen wurden, müssen Sie sich am IMM2 anmelden, um auf die IMM2-Webschnittstelle zuzugreifen.

Achtung: Wenn Sie die Option "Reset IMM to factory defaults" verwenden, gehen alle Änderungen, die Sie am IMM2 vorgenommen haben, verloren.

Gehen Sie wie folgt vor, um die werkseitigen Voreinstellungen des IMM2 wiederherzustellen:

- 1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt "Am IMM2 anmelden" auf Seite 10.
- Klicken Sie auf die Registerkarte IMM Management und anschließend auf IMM Reset to factory defaults....
- **3**. Klicken Sie auf die Schaltfläche **OK** im Fenster "Confirm Reset to factory defaults" (Zurücksetzen auf werkseitige Voreinstellungen bestätigen) (wie in der folgenden Abbildung dargestellt).



**Anmerkung:** Nach Abschluss der Konfiguration des IMM2 wird dieses erneut gestartet. Wenn es sich um einen lokalen Server handelt, wird Ihre TCP/IP-Verbindung unterbrochen und Sie müssen die Netzschnittstelle rekonfigurieren, um wieder eine funktionsfähige Verbindung herzustellen.

- 4. Melden Sie sich erneut am IMM2 an, um die IMM2-Webschnittstelle zu verwenden (Anweisungen hierzu finden Sie im Abschnitt "Am IMM2 anmelden" auf Seite 10).
- 5. Rekonfigurieren Sie die Netzschnittstelle, um wieder eine funktionsfähige Verbindung herzustellen.

# Aktivierungsschlüsselverwaltung

Klicken Sie auf der Registerkarte "IMM Management" (IMM-Verwaltung) auf die Option **Activation Key Management** (Aktivierungsschlüsselverwaltung), um die einzelnen Funktionen der Aktivierungsschlüssel für optionale FoD (Features on Demand) für das IMM2 und den Server zu verwalten. Weitere Informationen zur FoD-Aktivierungsschlüsselverwaltung finden Sie in Kapitel 7, "Features on Demand", auf Seite 143.

# Kapitel 5. Serverstatus überwachen

Dieses Kapitel enthält Informationen zum Anzeigen und Überwachen der Informationen zu dem Server, auf den Sie zugreifen.

### Systemstatus anzeigen

Die Seite "System Status" (Systemstatus) bietet eine Übersicht über den Betriebsstatus des IMM2-Servers. Auf dieser Seite werden Informationen zum Hardwarezustand des Servers und zu aktiven Ereignissen auf dem Server angezeigt.

**Anmerkung:** Wenn Sie über die Seite "System Status" auf eine andere Seite zugreifen, können Sie zur Seite "System Status" zurückkehren, indem Sie in den Menüoptionen oben auf der Seite auf **System Status** klicken.

Sie können zum IMM2 einen beschreibenden Namen hinzufügen, damit Sie die einzelnen IMM2-Module voneinander unterscheiden können. Klicken Sie unten auf den Link **Add System Descriptive Name...** (Beschreibenden Systemnamen hinzufügen) unter dem Serverproduktnamen, um einen Namen festzulegen, der dem IMM2 zugeordnet werden soll (wie in der folgenden Abbildung dargestellt).



Geben Sie im Fenster "Change System Descriptive Name" (Beschreibenden Systemnamen ändern) einen Namen an, der dem IMM2 zugeordnet werden soll (wie in der folgenden Abbildung dargestellt).

IBM Integrated N	lanagement Module II
System St	tus Events + Service and Support + Server Management + IMM Management + Search
System x36 Add System Descriptiv The System Status a	b 50 M4 e Name nd Health page provides an at-a-glance overview of the operating status of the server in which this IMM resides. Cor
Power: On-	Change System Descriptive Name X
System state: Sys	Edit the name of your system. This is a name used for descriptive purposes to help you identify your system.
System Information	Test Server System name must be specified
Active Events	OK Cancel

Sie können den beschreibenden Systemnamen ändern, indem Sie neben dem beschreibenden Systemnamen auf den Link **Rename...** (Umbenennen) klicken.

In der folgenden Abbildung ist der Link "Rename" dargestellt.

IBM Integrated Management Module II				
	System Status	Events 🗸	Service	
Sys Test S	tem x365( Server <sub>Renam</sub>	0 M4 •		

Auf der Seite "System Status" werden der Stromversorgungsstatus und der Betriebsstatus des Servers angezeigt. Angezeigt wird der Serverstatus zum Zeitpunkt des Öffnens der Seite "System Status".

In der folgenden Abbildung sind die Felder **Power** (Stromversorgung) und **System** state (Systemstatus) dargestellt.



Der Server kann sich in einem der Systemstatus befinden, die in der folgenden Tabelle aufgeführt sind.

Tabelle 5.	Systemstatusbeschreib	oungen
------------	-----------------------	--------

Status	Beschreibung
System power off/State unknown (Stromversorgung des Systems ausgeschaltet/Status unbekannt)	Der Server ist ausgeschaltet.
System on/starting UEFI (System eingeschaltet/UEFI wird gestartet)	Der Server ist eingeschaltet, aber die UEFI wird noch nicht ausgeführt.
System running in UEFI (System wird in UEFI ausgeführt)	Der Server ist eingeschaltet und die UEFI wird ausgeführt.
System stopped in UEFI (System wurde in UEFI gestoppt)	Der Server ist eingeschaltet; die UEFI hat einen Fehler erkannt und ihre Ausfüh- rung wurde beendet.
Status	Beschreibung
---	--
Booting OS or in unsupported OS (Be- triebssystem wird gebootet oder es wird ein nicht unterstütztes Betriebssystem	Der Server kann sich aus einem der fol- genden Gründe in diesem Status befin- den:
gebootet)	<ul> <li>Das Ladeprogramm des Betriebssys- tems wurde gestartet, aber das Be- triebssystem wird nicht ausgeführt.</li> </ul>
	• Die Ethernet-over-USB-Schnittstelle des IMM2 ist inaktiviert.
	• Das Betriebssystem hat die Treiber, die die Ethernet-over-USB-Schnittstelle unterstützen, nicht geladen.
OS booted (Betriebssystem gebootet)	Das Betriebssystem des Servers wird aus- geführt.
Suspend to RAM (Aussetzen in RAM)	Der Server wurde in den Bereitschafts- oder Ruhemodus versetzt.

Tabelle 5. Systemstatusbeschreibungen (Forts.)

Die folgenden Menüoptionen auf der Seite "System Status" bieten zusätzliche Serverinformationen und -aktionen, die auf dem Server ausgeführt werden können.

- System Information (Systeminformationen)
- · Power Actions (Stromversorgungsaktionen)
- Remote Control (Fernsteuerung, weitere Informationen hierzu finden Sie unter "Remote-Presence- und Fernsteuerungsfunktionen" auf Seite 107)
- Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige, weitere Informationen hierzu finden Sie unter "Daten der letzten Betriebssystem-Fehleranzeige erfassen" auf Seite 136)

## Systeminformationen anzeigen

Das Menü "System Information" (Systeminformationen) stellt eine Zusammenfassung allgemeiner Serverinformationen bereit. Klicken Sie auf die Registerkarte **System Information** auf der Seite "System Status", um die folgenden Informationen anzuzeigen:

- Machine name (Name der Maschine)
- Machine type (Maschinentyp)
- Model (Modell)
- Serial number (Seriennummer)
- Universally Unique Identifier (UUID)
- Server power (Serverstromversorgung)
- Server state (Serverstatus)
- Total hours powered on (Gesamtbetriebsdauer in Stunden)
- Restart count (Zähler für Neustart)
- Ambient temperature (Umgebungstemperatur)
- Enclosure identity LED (Gehäuse-ID-Anzeige)
- Check log LED (Protokollprüfanzeige)

In der folgenden Abbildung ist das Fenster "System Information" dargestellt.

Wetom Information (	
Machine Name	System x3650 M4
Machine Type	7915
Model	35Z
Serial Number	06CNZ40
UUID	E596B684B75E11E0A0B0E41F13EB0F72
Server Power	On
Server State	System running in UEFI
Total hours powered-on	117
Restart count	6
Ambient Temperature	80.60 F / 27.00 C
Enclosure Identify LED	Off Change
Check Log LED	Off

## Serverzustand anzeigen

Der Serverzustand wird unter der Titelleiste in der linken oberen Ecke der Seite "System Status" (Systemstatus) angezeigt und ist durch ein Symbol designiert. Ein grünes Häkchen gibt an, dass die Server-Hardware normal funktioniert. Bewegen Sie Ihren Cursor über das grüne Häkchen, um eine Kurzmeldung zum Serverzustand zu erhalten.

In der folgenden Abbildung ist ein Beispiel für einen Server, der normal funktioniert, dargestellt.



Ein gelbes Dreieck gibt an, dass eine Warnbedingung vorliegt. Ein roter Kreis gibt an, dass eine Fehlerbedingung vorliegt.

In der folgenden Abbildung ist ein Beispiel für einen Server mit aktiven Fehlerereignissen dargestellt.



Wenn ein Warnsymbol (gelbes Dreieck) oder ein Fehlersymbol (roter Kreis) angezeigt wird, klicken Sie auf das Symbol, um die entsprechenden Ereignisse im Abschnitt "Active Events" (Aktive Ereignisse) der Seite "System Status" anzuzeigen.

In der folgenden Abbildung ist ein Beispiel für den Abschnitt "Active Events" mit Fehlerbedingungen dargestellt.

Active Events	Active Events						
Severity 🔺	Source	Date	Message				
Strop	System	16 Jul 2012 01:00:28.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.				
🔕 Error	System	16 Jul 2012 01:00:29.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.				

## Hardwarezustand anzeigen

Im Abschnitt "Hardware Health" (Hardwarezustand) der Seite "System Status" (Systemstatus) sind die Server-Hardware-Komponenten aufgelistet. Hier wird der Allgemeinzustand jeder Komponente, die durch das IMM2 überwacht wird, angezeigt. Der angezeigte Allgemeinzustand einer Komponente entspricht möglicherweise dem kritischsten Status aller einzelnen Komponenten eines Komponententyps. Beispiel: Auf einem Server können mehrere Stromversorgungsmodule installiert sein und bis auf ein Stromversorgungsmodul funktionieren alle normal. Aufgrund des Stromversorgungsmoduls, das nicht fehlerfrei funktioniert, wird der Status der Komponente "Power Modules" (Stromversorgungsmodule) als kritisch angezeigt.

In der folgenden Abbildung ist der Abschnitt "Hardware Health" der Seite "System Status" dargestellt.

Hardware Health @	
Component Type	Status
Cooling Devices	Normal
Power Modules	🔕 Critical
Disks	Normal
Processors	Normal
Mempry	🔽 Normal
System	Normal

Jede Komponente wird als Link angezeigt, auf den Sie klicken können, um genauere Informationen zu erhalten. Wenn Sie einen Komponententyp (Component Type) auswählen, wird eine Tabelle angezeigt, in der alle Komponenten dieses Komponententyps aufgelistet sind.

In der folgenden Abbildung sind Komponenten für den Komponententyp "Memory" (Speicher) dargestellt.

Memory Display the memory m	nodules available on the	server. Clicking on a module	e displays a Properties pop-up window with 2 tal
FRU Name	<ul> <li>Status</li> </ul>	Туре	Capacity (GB)
DIMM 4	Normal	DDR3	4
DIMM 9	Normal	DDR3	4
DIMM 16	Normal	DDR3	4
DIMM 21	Normal	DDR3	4

Sie können auf einen einzelnen FRU-Link (Field Replaceable Unit) in der Tabelle klicken, um weitere Informationen zu dieser Komponente zu erhalten. Alle aktiven Ereignisse für die Komponente werden auf der Registerkarte "Events" (Ereignisse) angezeigt.

In der folgenden Abbildung ist die Registerkarte "Events" für DIMM 4 dargestellt.

Pr	operties fo	r DIMM 4	
	Events	Hardware Information	
	There are	no active events for this device	
	Close		

Falls vorhanden, sind für die Komponente auf der Registerkarte "Hardware Information" (Hardwareinformationen) möglicherweise weitere Informationen angegeben.

In der folgenden Abbildung ist die Registerkarte "Hardware Information" für DIMM 4 dargestellt.

Properties for DIMM 4	
Events Hardwa	ro Information
Description	
PartNumber	M393B5773CH0-YH9
FRU Serial Number	8634E095
Manuf Date	2211
Size	2 GB
Close	

# Kapitel 6. IMM2-Tasks ausführen

Verwenden Sie die Informationen in diesem Abschnitt und in Kapitel 3, "Übersicht über die IMM2-Webbenutzerschnittstelle", auf Seite 17, um die folgenden Tasks zur Steuerung des IMM2 auszuführen.

Auf der Registerkarte "System Status" (Systemstatus) können Sie folgende Tasks ausführen:

- Serverzustand anzeigen
- Serverinformationen anzeigen, z. B. Servername, Servertyp und Seriennummer
- · Serverstromversorgung und Neustartaktivitäten anzeigen
- Stromversorgungsstatus des Servers über Fernzugriff steuern
- Serverkonsole über Fernzugriff verwenden
- Eine Platte oder ein Plattenimage über Fernzugriff an den Server anhängen
- Aktive Ereignisse anzeigen
- · Hardwarezustand der Serverkomponenten anzeigen

**Anmerkung:** Die Seite "System Status" wird nach dem Anmelden am IMM2 angezeigt. Auf dieser Seite sind allgemeine Informationen und Aktionen zusammengestellt.

Auf der Registerkarte "Events" (Ereignisse) können Sie folgende Tasks ausführen:

- Ereignisprotokollverlauf verwalten
- Ereignisempfänger für E-Mail-Benachrichtigungen verwalten
- Ereignisempfänger für syslog-Benachrichtigungen verwalten

Auf der Registerkarte "Services and Support" (Services und Support) können Sie folgende Tasks ausführen:

Servicedaten für Ihren Server manuell abrufen

Auf der Registerkarte "Server Management" (Serververwaltung) können Sie Optionen zum Ausführen folgender Tasks auswählen:

- Mit der Option "Server Firmware" (Server-Firmware) können Sie Firmwareversionen der Serverkomponenten anzeigen und aktualisieren.
- Mit der Option "Remote Control" (Fernsteuerung) können Sie Ihre Serverkonsole über Fernzugriff anzeigen und mit ihr interagieren:
  - Stromversorgungsstatus des Servers über Fernzugriff steuern
  - Serverkonsole über Fernzugriff verwenden
  - CD-Laufwerk, DVD-Laufwerk, Diskettenlaufwerk, USB-Flashlaufwerk oder Plattenimage über Fernzugriff Ihrem Server zuordnen
- Mit der Option "Server Properties" (Servereigenschaften) können Sie Parameter festlegen, um das Ermitteln des Servers zu unterstützen.
- Mit der Option "Server Power Actions" (Serverstromversorgungsaktionen) können Sie den Server einschalten, ausschalten und erneut starten.
- Mit der Option "Disks" (Festplatten) können Sie die im Server installierten Festplattenlaufwerke und ihnen zugeordnete Ereignisse anzeigen.
- Mit der Option "Memory" (Speicher) können Sie Informationen zu im Server installierten Speichermodulen anzeigen.

- Mit der Option "Processor" (Prozessor) können Sie Informationen zu im Server installierten Mikroprozessoren anzeigen.
- Mit der Option "Server Timeouts" (Serverzeitlimits) können Sie Zeitlimits festlegen, damit der Server während einer Firmwareaktualisierung oder beim Einschalten des Servers nicht unbegrenzt blockiert wird.
- Mit der Option "PXE Network Boot" (PXE-Netzboot) können Sie Bootversuche der Server-Ausführungsumgebung vor dem Start einrichten.
- Mit der Option "Latest OS Failure Screen" (Letzte Betriebssystem-Fehleranzeige) können Sie die Daten aus der Fehleranzeige des Betriebssystems erfassen und speichern.
- Mit der Option "Power Management" können Sie den Systemstromverbrauch und die Netzteilkapazität anzeigen sowie Parameter für den Systemstromverbrauch festlegen.

## Stromversorgungsstatus des Servers steuern

Die Option "Power Actions" (Stromversorgungsaktionen) enthält eine Liste von Aktionen, mit der Sie die Serverstromversorgung steuern können (wie in der folgenden Abbildung dargestellt). Sie können den Server sofort oder zu einem geplanten Zeitpunkt einschalten. Sie können auch das Betriebssystem herunterfahren und anschließend erneut starten.

IBM Integrated Management Module II	USERID	Settings   Log out	IBM.
System Status Events • Service and Support • Server Management • IMM Management • Search			
Server Actions Corrent server power state: ON Actions Power On Server Immediately			
Power On Sarver at Specified Date and Time Power Off Sarver Immediately Shat down OS and then Neuro Off Sarver Shat down OS and then Retart Sarver Retart the Sarver Immediately			
Restart the Server with Non-maskable Intempt (HMI) Schedule Daily/Weekly Power and Restart Actions			

Gehen Sie wie folgt vor, um Aktionen zur Stromversorgung und zum Neustart des Servers auszuführen:

- 1. Führen Sie einen der folgenden Schritte aus, um auf das Menü "Power Actions" zuzugreifen:
  - Klicken Sie auf der Seite "System Status" auf die Registerkarte **Power Actions**.
  - Klicken Sie auf der Registerkarte "Server Management" auf Server Power Actions.
- 2. Wählen Sie die Serveraktion aus der Menüliste "Actions" aus.

Die folgende Tabelle enthält eine Beschreibung der Stromversorgungs- und Neustartaktionen, die auf dem Server ausgeführt werden können.

Tabelle 6. Stromversorgungsaktionen und Beschreibungen

Stromversorgungsaktion	Beschreibung
Power on server immediately (Server sofort einschalten)	Wählen Sie dieses Aktionselement aus, um den Server einzuschalten und das Betriebs- system zu booten.

Stromversorgungsaktion	Beschreibung			
Power on server at specified date and time (Server an einem bestimmten Datum und zu einer bestimmten Uhrzeit einschalten)	Wählen Sie dieses Aktionselement aus, um einen Zeitplan für den Server zu erstellen, sodass er automatisch an einem bestimmten Datum, zu einer bestimmten Uhrzeit einge- schaltet wird.			
Power off server immediately (Server sofort ausschalten)	Wählen Sie dieses Aktionselement aus, um den Server auszuschalten, ohne das Betriebs- system herunterzufahren.			
Shut down operating system and then pow- er off server (Betriebssystem herunterfahren und dann Server ausschalten) <sup>1</sup>	Wählen Sie dieses Aktionselement aus, um das Betriebssystem herunterzufahren und den Server anschließend auszuschalten.			
Shut down OS and then restart server (Be- triebssystem herunterfahren und Server an- schließend erneut starten) <sup>1</sup>	Wählen Sie dieses Aktionselement aus, um einen Warmstart des Betriebssystems durch- zuführen.			
Restart the server immediately (Server sofort erneut starten)	Wählen Sie dieses Aktionselement aus, um den Server sofort aus- und anschließend wieder einzuschalten, ohne das Betriebssys- tem herunterzufahren.			
Restart the server with non-maskable interrupt (NMI) (Server mit NMI erneut star- ten)	Wählen Sie dieses Aktionselement aus, um ein NMI für ein blockiertes System zu er- zwingen. Die Auswahl dieses Aktionselements ermöglicht es dem Plattformbetriebssystem, einen Hauptspeicherauszug zu erstellen, der für die Fehlerbehebung des blockierten Systems verwendet werden kann. Die IMM2-Firmwa- re verwendet den automatischen Warmstart der NMI-Einstellung von "UEFI F1" im Menü "Setup", um zu bestimmen, ob ein Warmstart nach dem NMI erforderlich ist.			
Schedule daily/weekly power and restart actions (Tägliche/Wöchentliche Aktionen zum Einschalten und erneuten Starten pla- nen)	Wählen Sie dieses Aktionselement aus, um tägliche oder wöchentliche Aktionen zum Einschalten und zum erneuten Starten für den Server zu planen.			
<ol> <li>Falls sich das Betriebssystem im Bildschirr befindet, wenn die Anforderung zum Her- möglicherweise keinen ordnungsgemäßen dann einen Kaltstart oder einen Systemabs Ausschaltverzögerungsintervalls durch, we noch ausgeführt wird.</li> </ol>	nschonermodus oder im gesperrten Modus unterfahren gesendet wird, kann das IMM2 Systemabschluss einleiten. Das IMM2 führt schluss nach Ablaufen des ährend das Betriebssystem möglicherweise			

Tabelle 6. Stromversorgungsaktionen und Beschreibungen (Forts.)

## **Remote-Presence- und Fernsteuerungsfunktionen**

Sie können die IMM2-Fernsteuerungsfunktion oder die Remote-Presence-Funktion in der IMM2-Webschnittstelle verwenden, um die Serverkonsole anzuzeigen und mit ihr zu interagieren. Sie können dem Server ein CD- oder DVD-Laufwerk, ein Diskettenlaufwerk, ein USB-Flashlaufwerk oder ein Plattenimage zuordnen, das sich auf Ihrem Computer befindet. Die Remote-Presence-Funktion ist mit den IMM2 Premium-Funktionen verfügbar und kann nur über die IMM2-Webschnittstelle verwendet werden. Sie müssen sich am IMM2 mit einer Benutzer-ID anmelden, die über Administratorzugriff verfügt, um die Fernsteuerungsfunktionen verwenden zu können. Weitere Informationen zum Durchführen eines Upgrades von IMM2 Basic oder IMM2 Standard auf IMM2 Premium finden Sie im Abschnitt "Upgrade für IMM2 durchführen" auf Seite 4. Informationen dazu, welche IMM2-Version auf Ihrem Server installiert ist, finden Sie in der mit dem Server gelieferten Dokumentation.

Verwenden Sie die Fernsteuerungsfunktionen, um folgende Aktionen auszuführen:

- Zeigen Sie, unabhängig vom Serverzustand, über Fernzugriff Videos mit einer Grafikauflösung von bis zu 1600 x 1200 bei 75 Hz an.
- Greifen Sie mithilfe der Tastatur und der Maus eines fernen Clients über Fernzugriff auf den Server zu.
- Ordnen Sie das CD- oder DVD-Laufwerk, das Diskettenlaufwerk und das USB-Flashlaufwerk einem fernen Client zu. Ordnen Sie ISO- und Diskettenimagedateien als virtuelle Laufwerke zu, die zur Verwendung durch den Server verfügbar sind.
- Laden Sie ein Diskettenimage in den IMM2-Speicher hoch und ordnen Sie es dem Server als virtuelles Laufwerk zu.

### IMM2-Firmware und Java- oder ActiveX-Applet aktualisieren

Dieser Abschnitt enthält Informationen zum Aktualisieren der Firmware sowie des Java- und des ActiveX-Applets.

Wichtig: Das IMM2 verwendet ein Java-Applet oder ein ActiveX-Applet, um die Remote-Presence-Funktion auszuführen. Wenn das IMM2 auf die neueste Firmwareversion aktualisiert wird, werden auch das Java-Applet und das ActiveX-Applet auf die neueste Version aktualisiert. Java stellt zuvor verwendete Applets standardmäßig in den örtlichen Zwischenspeicher. Nach einer Flashaktualisierung der IMM2-Firmware ist das vom Server verwendete Java-Applet möglicherweise nicht auf dem neuesten Stand.

Um diesen Fehler zu beheben, inaktivieren Sie das Zwischenspeichern. Welche Methode verwendet wird, hängt von der Plattform und von der Java-Version ab. Die folgenden Schritte gelten für Oracle Java 1.5 unter Windows:

- Klicken Sie auf Start → Settings (Einstellungen) → Control Panel (Steuerkonsole).
- Klicken Sie zweimal auf Java Plug-in 1.5. Das Fenster "Control Panel" des Java-Plug-in wird geöffnet.
- 3. Klicken Sie auf die Registerkarte Cache (Zwischenspeicher).
- 4. Wählen Sie eine der folgenden Optionen:
  - Wählen Sie das Kontrollkästchen Enable Caching (Zwischenspeichern aktivieren) ab, damit die Java-Zwischenspeicherung immer inaktiviert ist.
  - Klicken Sie auf Clear Caching (Zwischenspeichern abwählen). Wenn Sie diese Option auswählen, müssen Sie nach jeder IMM2-Firmwareaktualisierung auf Clear Caching klicken.

Weitere Informationen zur Aktualisierung von IMM2-Firmware finden Sie im Abschnitt "Server-Firmware aktualisieren" auf Seite 122.

## **Remote-Presence-Funktion aktivieren**

Die Remote-Presence-Funktion des IMM2 ist nur in IMM2 Premium verfügbar. Weitere Informationen zum Durchführen eines Upgrades von IMM Standard auf IMM Premium finden Sie im Abschnitt "Upgrade für IMM2 durchführen" auf Seite 4.

Nachdem Sie den Aktivierungsschlüssel für das IMM2 Premium-Upgrade gekauft und erhalten haben, installieren Sie ihn. Lesen Sie dazu "Aktivierungsschlüssel installieren" auf Seite 143.

# Anzeigenerfassung per Fernsteuerung

Die Anzeigenerfassungsfunktion im Fenster Video Viewer erfasst die Inhalte des Serverbildschirms. Gehen Sie wie folgt vor, um eine Bildschirmanzeige zu erfassen und zu speichern:

- 1. Klicken Sie im Fenster Video Viewer auf File (Datei).
- 2. Wählen Sie aus dem Menü Capture to File (in Datei speichern) aus.
- **3**. Wenn Sie dazu aufgefordert werden, geben Sie einen Namen für die Bilddatei ein und speichern Sie sie an dem Ort, den Sie auf dem lokalen Client auswählen.

**Anmerkung:** Der Java-Client speichert das Anzeigenerfassungsbild als eine Datei vom Typ JPG. Der ActiveX-Client speichert das Anzeigenerfassungsbild als eine Datei vom Typ BMP.

In der folgenden Abbildung ist das Fenster dargestellt, in dem Sie den Standort für die Bilddatei angeben und den Namen der Bilddatei eingeben können.

	0011110110110	1101010010	0101101010101010101	000110111	010110001	100101010	oon <b>IBM</b>	
00 00	Save	1	MM Sustem Lven	t Loa			a	
0x0001 0x0002	Save In:	My Documents	S	-	a ĉ		:52	
0x0003 0x0004 0x0005 0x0006 0x0007 0x0008 0x0009 0x0009 0x0000 0x0000	a Access Co Bluetooth Download My eBooks My Music My Picture File <u>Name</u> :	nnections Exchange Fold 3 5 5	C My Videos Snagit Catalo der Updater5	g			:s: 10	
0x000D 0x000E 100 11=Move	Files of <u>Type</u> :	*.jpg or *.jpe	g files		Save	Cancel	. <u> </u>	

## Modi der Fernsteuerung im Video Viewer

Um die Ansicht im Fenster "Video Viewer" zu ändern, klicken Sie auf **View** (Ansicht). Die folgenden Menüoptionen sind verfügbar:

#### Hide Status Bar (Statusleiste ausblenden)

Blendet die Statusleiste aus, die den Zustand der Tasten für den Großschreibmodus, die numerische Verriegelung und das Blättern anzeigt. Diese Option ist nur bei eingeblendeter Statusleiste verfügbar.

#### Show Status Bar (Statusleiste einblenden)

Blendet die Statusleiste ein, die den Zustand der Tasten für den Großschreibmodus, die numerische Verriegelung und das Blättern anzeigt. Diese Option ist nur bei ausgeblendeter Statusleiste verfügbar.

#### **Refresh (Aktualisieren)**

Der Video Viewer aktualisiert die Bildschirmanzeige mit den Videodaten vom Server.

#### Full Screen (Gesamtanzeige)

Der Video Viewer verwendet den gesamten Client-Desktop für die Videoanzeige. Diese Option ist nur dann verfügbar, wenn der Video Viewer nicht im Gesamtanzeigemodus ausgeführt wird.

#### Windowed (Fenstermodus)

Der Video Viewer wechselt vom Gesamtanzeigemodus in den Fenstermodus. Diese Option ist nur dann verfügbar, während der Video Viewer im Gesamtanzeigemodus ausgeführt wird.

#### Fit (Eingepasst)

Die Größe des Video Viewers wird so verändert, dass die Zielarbeitsoberfläche vollständig und ohne einen zusätzlichen Rand oder Schiebeleisten angezeigt wird. Der Client-Desktop muss groß genug sein, um das größenangepasste Fenster anzuzeigen.

### Fernsteuerung des Videofarbmodus

Wenn Ihre Verbindung zum fernen Server eine begrenzte Bandbreite hat, können Sie den Bandbreitenbedarf des Video Viewer verringern, indem Sie die Farbeinstellungen im Video Viewer-Fenster anpassen.

Anmerkung: Das IMM2 bietet eine Menüoption, die es ermöglicht, die Farbtiefe anzupassen, um bei geringer Bandbreite die übertragene Datenmenge zu verringern. Diese Menüoption ersetzt den Bandbreiten-Schieberegler der Schnittstelle beim Remote Supervisor Adapter II.

Gehen Sie wie folgt vor, um den Videofarbmodus zu ändern:

- 1. Klicken Sie im Fenster Video Viewer auf View (Ansicht).
- 2. Klicken Sie auf **Color Mode** (Farbmodus). Es sind zwei Farbmodusoptionen verfügbar (wie in der folgenden Abbildung dargestellt):
  - Farbe: 7-, 9-, 12-, 15- und 23-Bit
  - Grauskala: 16, 32, 64 und 128 Grautöne

Hide Status Bar Refresh Full Screen	01100011101101	01101101100011100110110001100001110110011001001100101			
Adapters an Integrated Processors Memory Devices and Power Operating N Legacy Supp System Sect Recovery Storage Network Driver Heal	Color Grayscale Grayscale Management Managem	7 bit 9 bit 12 bit 15 bit 23 bit	ystem Settings This option is only for older generation UEFI drivers to configure their corresponding device.		
14=Move H	lighlight mational Ever	<enter: nt(s) Det</enter: 	>=Select Entry Esc=Exit		

3. Wählen Sie die Einstellung für die Farbe oder die Graustufe aus.

# Tastaturunterstützung per Fernsteuerung

Das Betriebssystem auf dem Clientserver, den Sie verwenden, fängt bestimmte Tastenkombinationen ab, etwa "Strg + Alt + Entf" in Microsoft Windows, anstatt sie an den Blade-Server zu übertragen. Andere Tasten wie etwa F1 verursachen möglicherweise gleichzeitig eine Aktion auf dem Server und auf Ihrem Computer.

Gehen Sie wie folgt vor, um Tastenkombinationen zu verwenden, die den fernen Server und nicht den lokalen Client beeinflussen:

- 1. Klicken Sie im Fenster Video Viewer auf Macros.
- 2. Wählen Sie eine der vordefinierten Tastenkombinationen aus dem Menü oder wählen Sie **Soft Key** (Programmfunktionssymbol) aus, um eine benutzerdefinierte Tastenkombination auszuwählen oder hinzuzufügen (wie in der folgenden Abbildung dargestellt).

Alt-Tab Alt-ESC	1001101010010101010101000010101000	0101010101000110000010001000101010100000
Ctrl-ESC Alt-Space	System Configuration and Bo	ot Management
Alt-Enter		
Alt-Hyphen		This selection
Alt-F4		displays the basic
PrtScrn		details of the System.
Alt-PrtScrn		
F1		
Pause		
Tab		
Ctri-Enter 19	5	
Syskey Alt SysBog		
Alt J Shift PShift Esc		
Ctrl_Alt_Backspace		
Alt-F?	tings	
Ctrl-Alt-F?		, and the second se
Soft Koy		
T <sup>1</sup> =Move Highligh	t <enter>=Select Entry</enter>	<esc>=Exit Setup</esc>
900 · · ·		
000		
Carls		

Verwenden Sie die Menüoption **Macros** von Video Viewer, um spezielle Schaltflächen zu erstellen oder zu bearbeiten, mit deren Hilfe Tastatureingaben an den Server gesendet werden können.

Gehen Sie wie folgt vor, um spezielle Schaltflächen zu erstellen und zu bearbeiten:

- 1. Klicken Sie im Fenster "Video Viewer" auf Macros.
- 2. Wählen Sie **Soft Key** und dann **Add** (Hinzufügen) aus. Ein neues Fenster wird geöffnet.
- **3.** Klicken Sie auf **New**, um eine neue Tastenkombination hinzuzufügen, oder wählen Sie eine Tastenkombination und klicken Sie auf **Delete** (Löschen), um eine bestehende Tastenkombination zu entfernen.
- 4. Wenn Sie eine neue Kombination hinzufügen, geben Sie die Tastenkombination ein, die Sie in dem Fenster definieren möchten, das sich öffnet, nachdem **New** ausgewählt wurde, und klicken Sie dann auf **OK**.
- 5. Wenn Sie damit fertig sind, Tastenkombinationen zu definieren oder zu entfernen, klicken Sie auf **OK**.

### Unterstützung für internationale Tastatur

Der Video Viewer verwendet plattformspezifischen nativen Code, um Tastaturereignisse abzufangen und direkt auf die Daten zur physischen Taste zuzugreifen. Der Client erkennt die Ereignisse der physischen Tasten und übergibt sie an den Server. Der Server erkennt dieselbe physische Tastatureingabe, die der Client festgestellt hat, und unterstützt alle Standardtastaturbelegungen. Die einzige Einschränkung dabei ist, dass das Ziel und der Client dieselbe Tastaturbelegung verwenden. Wenn ein ferner Benutzer eine andere Tastaturbelegung als der Server verwendet, kann der Benutzer die Serverbelegung umschalten, während der ferne Zugriff erfolgt, und anschließend wieder zurückschalten.

## Tastaturdurchgriffsmodus

Der Tastaturdurchgriffsmodus inaktiviert die Behandlung der meisten Sondertastenkombinationen auf dem Client, sodass sie direkt an den Server übergeben werden können. Dies bietet eine Alternative zur Verwendung der Makros.

Einige Betriebssysteme definieren bestimmte Tastatureingaben als außerhalb der Steuerung einer Anwendung, sodass das Verhalten des Durchgriffsmechanismus unabhängig vom Server ausgeführt wird. Beispiel: In einer Linux-Sitzung bewirkt die Tastenkombination Strg+Alt+F2 einen Wechsel zur virtuellen Konsole 2. Es gibt keinen Mechanismus zum Abfangen dieser Tastenfolge und daher auch keine Möglichkeit für den Client, diese Tastatureingaben direkt an das Ziel zu übergeben. Die einzige Option in diesem Fall ist die Verwendung der Tastaturmakros, die für diese Zweck definiert wurden.

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

- 1. Klicken Sie im Fenster "Video Viewer" auf Tools.
- 2. Wählen Sie aus dem Menü Session Options (Sitzungsoptionen) aus.
- 3. Wenn sich das Fenster "Session Options" öffnet, klicken Sie auf die Registerkarte **General** (Allgemein).
- 4. Wählen Sie das Kontrollkästchen **Pass all keystrokes to target** (Alle Tastatureingaben an Ziel übergeben) aus, um den Tastaturdurchgriffsmodus zu aktivieren oder zu inaktivieren.
- 5. Klicken Sie auf OK, um die Auswahl zu speichern.

## Mausunterstützung per Fernsteuerung

Im Fenster "Video Viewer" haben Sie verschiedene Möglichkeiten der Maussteuerung, einschließlich absolute Maussteuerung, relative Maussteuerung und Einzelcursormodus.

#### Absolute und relative Maussteuerung

Gehen Sie wie folgt vor, um auf die absoluten und relativen Optionen zum Steuern der Maus zuzugreifen:

- 1. Klicken Sie im Fenster "Remote Control" (Fernsteuerung) auf Tools.
- 2. Wählen Sie aus dem Menü Session Options (Sitzungsoptionen) aus.
- **3**. Wenn sich das Fenster "Session Options" öffnet, klicken Sie auf die Registerkarte **Mouse** (Maus) (wie in der folgenden Abbildung dargestellt).

	IMM System Event Log	
0x0001_Sus	Session Options	4:21:52
0x0002 Sys	General Mouse Browser	
0x0003 Sys	Single Cursor	dress: 10
0x0004 Sys	Single Cursor	1B
0x0005 Sys	Termination Key: F12	4
UXUUUB Sys		-le nt
AxAAA8 Sus	Mouse Mode	12
0x0009 Sus	Absolute	
0x000A Sys		
0x000B Sys	Unclubre	
0x000C Sys	Relative (default Linux acceleration)	
Ux000D Sys		
UXUUUL SYS	OK Apply Cancel	
0.00000 A.		
î↓=Move Hig	yhlight Esc=Exit	

- 4. Wählen Sie einen der folgenden Mausmodi aus:
  - Absolute: (Absolut)

Der Client sendet Mauspositionsnachrichten an den Server, die immer relativ zum Ursprung (oberer linker Bereich) des Anzeigebereichs sind.

• Relative: (Relativ)

Der Client sendet die Mausposition als relative Position im Hinblick auf die vorherige Position.

• **Relative (default Linux acceleration):** (Relativ (Linux-Standardbeschleunigung))

Der Client wendet einen Beschleunigungsfaktor an, um die Maus besser auf Linux-Ziele abzustimmen. Die Beschleunigungseinstellungen wurden ausgewählt, um die Kompatibilität mit Linux-Distributionen zu maximieren.

### Einzelcursormodus

Manche Betriebssysteme richten die lokalen und fernen Cursor nicht aneinander aus, was zu Abweichungen zwischen den lokalen und fernen Mauszeigern führt. Beim Einzelcursormodus wird der lokale Client ausgeblendet, während die Maus sich innerhalb des Video Viewer-Fensters befindet. Bei aktiviertem Einzelcursormodus sehen Sie nur den fernen Cursor. Um den Einzelcursormodus zu aktivieren, klicken Sie im Video Viewer-Fenster auf **Tools > Single Cursor** (Tools, Einzelcursor).

**Anmerkung:** Wenn der Video Viewer im Einzelcursormodus läuft, können Sie die Maus nicht verwenden, um in ein anderes Fenster zu wechseln oder außerhalb des KVM-Clientfensters auf etwas zu klicken, da es keinen lokalen Cursor gibt.

Drücken Sie zum Inaktivieren des Einzelcursormodus die dafür festgelegte Beendigungstaste. Klicken Sie zum Anzeigen der festgelegten Beendigungstaste (Termination Key) oder um eine andere Beendigungstaste festzulegen auf **Tools > Session Options > Mouse** (Tools, Sitzungsoptionen, Maus).

## Fernsteuerung der Stromversorgung

Vom Fenster "Video Viewer" können Sie Serverbefehle für Stromversorgung und Neustart versenden, ohne zum Web-Browser zurückzukehren. Gehen Sie wie folgt vor, um die Stromversorgung des Servers über den Video Viewer zu steuern:

- 1. Klicken Sie im Fenster "Video Viewer" auf Tools.
- 2. Klicken Sie auf Power. Wählen Sie einen der folgenden Befehle aus:

On Schaltet die Stromversorgung des Servers ein.

Off Schaltet die Stromversorgung des Servers aus.

#### **Reboot (Warmstart)**

Startet den Server erneut.

#### Cycle (Aus- und wieder einschalten)

Schaltet die Stromversorgung des Servers erst aus, dann wieder ein.

## Leistungsstatistiken anzeigen

Um die Leistungsstatistik des Video Viewers im Fenster "Video Viewer" anzuzeigen, klicken Sie auf **Tools** und dann auf **Stats**. Die folgenden Informationen werden angezeigt:

#### Frame Rate (Vollbildrate)

Ein gleitender Durchschnittswert der Anzahl an Bildern, die pro Sekunde durch den Client entschlüsselt wird.

#### Bandwidth (Bandbreite)

Ein gleitender Durchschnittswert der Gesamtzahl an Kilobytes pro Sekunde, die der Client empfängt.

#### **Compression (Komprimierung)**

Ein gleitender Durchschnittswert der Bandbreitenverkleinerung aufgrund von Videokomprimierung. Dieser Wert wird häufig mit "100.0%" angegeben. Er wird auf ein Zehntel Prozent gerundet.

#### Packet Rate (Paketübertragungsrate)

Ein gleitender Durchschnittswert der Anzahl an Videopaketen, die pro Sekunde empfangen wird.

## **Remote Desktop Protocol starten**

Wenn der Windows-basierte RDP-Client (Remote Desktop Protocol) installiert ist, können Sie einen RDP-Client anstelle des KVM-Clients verwenden. Der ferne Server muss so konfiguriert sein, dass er RDP-Verbindungen empfangen kann.

## Beschreibung der Funktion "Anklopfen"

Wenn alle verfügbaren Fernsteuerungssitzungen besetzt sind (eine Option im Einzelbenutzermodus oder vier Optionen im Mehrbenutzermodus), hat ein anderer Webbenutzer die Möglichkeit, eine Anforderung zum Trennen der Verbindung an einen Fernsteuerungsbenutzer zu senden, der die Funktion "Anklopfen" aktiviert hat, falls dieser Benutzer nicht bereits eine Anforderung zum Trennen der Verbindung von einem anderen Webbenutzer erhalten hat.

Wenn der Fernsteuerungsbenutzer, der die Funktion "Anklopfen" aktiviert hat, die Anforderung akzeptiert oder nicht innerhalb des Zeitlimits auf die Anforderung antwortet, wird die Fernsteuerungssitzung beendet und für den Webbenutzer reserviert, der diese Anforderung gesendet hat. Wenn der Webbenutzer, der die Anforderung zum Trennen der Verbindung gesendet hat, nicht innerhalb von fünf Minuten eine Java- oder ActiveX-Fernsteuerungssitzung mit der reservierten Fernsteuerungssitzung startet, erlischt die Reservierung der Fernsteuerungssitzung für diesen Webbenutzer.

Gehen Sie wie folgt vor, um die Funktion "Anklopfen" zu aktivieren:

- 1. Öffnen Sie die Seite "Remote Control" (Fernsteuerung) über eine der folgenden Menüoptionen:
  - Klicken Sie auf der Registerkarte "Server Management" auf Remote Control.
  - Klicken Sie auf der Seite "System Status" auf Remote Control....
- 2. Wählen Sie das Kontrollkästchen Allow others to request my remote session disconnect (Anforderungen zum Trennen der Verbindung meiner fernen Sitzung durch andere Benutzer zulassen) aus.

Anmerkung: Für die Verwendung der Fernsteuerungsfunktion muss mindestens ein weiterer Benutzer vorhanden sein, der das Kontrollkästchen Allow others to request my remote session disconnect ausgewählt hat.

- **3**. Wählen Sie im Feld **No response time interval** (Zeitintervall, in dem keine Antwort erfolgt) ein Zeitintervall aus.
- 4. Starten Sie die Fernsteuerungssitzung, indem Sie den Benutzermodus auswählen. Wählen Sie einen der folgenden Modi aus:
  - Start remote control in single-user mode (Fernsteuerung im Einzelbenutzermodus starten)
  - Start remote control in multi-user mode (Fernsteuerung im Mehrbenutzermodus starten)

Anmerkung: Die Funktion "Anklopfen" wird automatisch aktiviert.

In der folgenden Abbildung sind die Felder dargestellt, die in Schritt 2 bis 4 beschrieben wurden.

No response	e time interval: 🥮	1 hour	-
Start remote co	ontrol in single-use	r mode	
Gives you exclu	usive access during the	e remote session.	

Gehen Sie wie folgt vor, um eine ferne Sitzung anzufordern:

1. Klicken Sie auf **Refresh** (Aktualisieren), um die Fernsteuerungssitzung anzuzeigen, die derzeit aktiv ist.

In der folgenden Abbildung ist das Fenster "Remote Control Session in Progress" (Aktive Fernsteuerungssitzung) dargestellt.

	Remote Control Session in Progress						
	If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.						
I	User Name	Active Sessions	Availability for Disconnection	Timeout Value			
I	USERID	192.168.5.11	Request to connect	1 hour			

Im Feld **Availability for Disconnection** (Verfügbarkeit für das Trennen der Verbindung) wird eine der folgenden Antworten angezeigt:

- **Request to connect** (Verbindung ist angefordert): Dieser Text wird angezeigt, wenn der Fernsteuerungsbenutzer die Funktion "Anklopfen" aktiviert hat und derzeit keine Anforderung zum Trennen der Verbindung von einem anderen Webbenutzer erhalten hat. Der aktuelle Webbenutzer hat keine Anforderung zum Trennen der Verbindung an den Fernsteuerungsbenutzer gesendet.
- Waiting for response (Warten auf Antwort): Dieser Text wird angezeigt, wenn der Fernsteuerungsbenutzer die Anforderung zum Trennen der Verbindung des aktuellen Webbenutzers verarbeitet. Der aktuelle Webbenutzer kann eine Anforderung zum Abbrechen an den Fernsteuerungsbenutzer senden, indem er auf die Schaltfläche **Cancel** (Abbrechen) klickt.
- Other request is pending (Andere Anforderung ist anstehend): Dieser Text wird in einer der folgenden Situationen angezeigt:
  - Der Fernsteuerungsbenutzer verarbeitet die Anforderung zum Trennen der Verbindung eines anderen Webbenutzers.
  - Der Fernsteuerungsbenutzer hat die Funktion "Anklopfen" aktiviert und der aktuelle Webbenutzer wartet auf die Antwort auf die Anforderung zum Trennen der Verbindung, die von einem anderen Fernsteuerungsbenutzer gesendet wurde.
- Not available (Nicht verfügbar): Dieser Text wird in einer der folgenden Situationen angezeigt:
  - Es sind nicht alle Fernsteuerungssitzungen besetzt. Ob der Fernsteuerungsbenutzer die Funktion "Anklopfen" aktiviert hat oder nicht, hat keine Auswirkungen auf diese Situation.
  - Alle Fernsteuerungssitzungen sind besetzt und der Fernsteuerungsbenutzer hat die Funktion "Anklopfen" nicht aktiviert.
  - Diese Fernsteuerungsverbindung ist fünf Minuten lang für einen anderen Benutzer reserviert.
- 2. Klicken Sie auf **Request to connect**, um eine Anforderung zum Trennen der Verbindung an den Fernsteuerungsbenutzer zu senden.

In der folgenden Abbildung ist das Fenster dargestellt, das angezeigt wird, wenn die Anforderung erfolgreich gesendet wurde.

Sendrequest	X
Your request has been sent su Please wait for the response fro	ocessfully. om the remote user.
Close	

Wenn der Fernsteuerungsbenutzer die Anforderung zum Trennen der Verbindung akzeptiert, muss der Webbenutzer die Fernsteuerungssitzung innerhalb von fünf Minuten starten. Wenn der Webbenutzer die Sitzung nicht innerhalb von fünf Minuten startet, ist die Sitzung nicht mehr reserviert.

In den folgenden Abbildungen sind die Informationen dargestellt, die angezeigt werden, wenn die Anforderung zum Trennen der Verbindung akzeptiert wird.

In der folgenden Abbildung wird die Anforderung zum Trennen der Verbindung im reservierten Zustand dargestellt.



In der folgenden Abbildung wird die Anforderung zum Trennen der Verbindung im nicht reservierten Zustand dargestellt.

Request is accepted		х
The request to disconnect r If no response within 0 sec control session will be disal	emote session has be ond, the option to sta bled.	een accepted art a remote
Start Remote Control Now	Cancel	

Wenn der Fernsteuerungsbenutzer die Anforderung zum Trennen der Verbindung zurückweist, erhält der Benutzer, der die Anforderung zum Trennen der Verbindung gesendet hat, eine Benachrichtigung, dass die Anforderung zurückgewiesen wurde (wie in der folgenden Abbildung dargestellt).

Reque	stis denied	×
Clos	Your request to disconnect the remote session has been denied.	

Wenn der Webbenutzer versucht, sich vom IMM2 abzumelden, bevor er eine Nachricht zu seiner Anforderung erhalten hat, erhält der Webbenutzer eine Nachricht (wie in der folgenden Abbildung dargestellt).



Nachdem der Fernsteuerungsbenutzer die Anforderung erhalten hat, muss er in dem ausgewählten Zeitintervall entscheiden, ob er die ferne Sitzung freigibt, bevor er die Fernsteuerungssitzung startet. Das Fenster "Request to End Remote Session" (Anforderung zur Beendigung der fernen Sitzung) wird angezeigt, um den Fernsteuerungsbenutzer an die verbleibende Zeit zu erinnern.

Das Fenster "Request to End Remote Session" ist in der folgenden Abbildung dargestellt.



Wenn der Fernsteuerungsbenutzer **Accept, end my session now** (Akzeptieren, meine Sitzung jetzt beenden) auswählt, wird die Anzeigefunktion für die ferne Sitzung automatisch geschlossen. Wenn der Fernsteuerungsbenutzer **Deny** (Zurückweisen) auswählt, behält der Fernsteuerungsbenutzer die ferne Sitzung. Nachdem die Anforderung zur Beendigung der fernen Sitzung (Request to End Remote Session) beendet wird, wird die ferne Sitzung automatisch freigegeben und das folgende Fenster wird geöffnet.

	Timeout of Remote Session	×
i	A request to end your session has timed out waiting for your response. Your remote session has ended automatically	
	OK	

# Ferner Datenträger

Über das Fenster "Virtual Media Session" können Sie dem Server ein CD- oder DVD-Laufwerk, ein Diskettenlaufwerk oder ein USB-Flashlaufwerk zuordnen oder Sie können ein Plattenimage auf Ihrem Computer angeben, das der Server verwenden kann. Sie können das Laufwerk für verschiedene Funktionen verwenden, z. B. zum erneuten Starten (Booten) des Servers, zum Installieren neuer Software auf dem Server und zum Installieren oder Aktualisieren des Betriebssystems auf dem Server. Sie haben Zugriff auf den fernen Datenträger. Die Laufwerk und Plattenimages werden auf dem Server als USB-Laufwerke angezeigt.

### Anmerkungen:

- Die folgenden Serverbetriebssysteme verfügen über USB-Unterstützung. Bei der Funktionalität für ferne Datenträger ist USB-Unterstützung erforderlich.
  - Microsoft Windows-Server 2003: Web, Std, Ent, DC (SP2, R2, SBS)
  - Microsoft Windows-Server 2008 SP2: Std, SBS, EBS
  - Microsoft Windows-Server 2008 R2
  - SUSE Linux Enterprise-Server von Version 10 SP3: x86\_64
  - SUSE Linux Enterprise Server von Version 11: x86,\_64
  - Red Hat Enterprise Linux Enterprise-Server von Version 3.7: x86, x86\_64
  - Red Hat Enterprise Linux Enterprise-Server von Version 4.8: x86, x86\_64
  - Red Hat Enterprise Linux Enterprise-Server von Version 5.5: x86, x86\_64
  - Red Hat Enterprise Linux Enterprise-Server von Version 6.0: x86, x86\_64
  - ESX 4.5: 4.0 U1
- Für den Client-Server ist das Plug-in Java 1.5 oder eine aktuellere Version erforderlich.
- Der Client-Server muss über einen Mikroprozessor vom Typ Intel Pentium III (oder neuer) mit 700 MHz oder mehr (oder über einen funktional entsprechenden Mikroprozessor) verfügen.

## Zugriff auf die Fernsteuerung

Gehen Sie wie folgt vor, um eine Fernsteuerungssitzung zu starten und auf einen fernen Datenträger zuzugreifen:

- 1. Klicken Sie im Fenster "Video Viewer" auf Tools.
- 2. Klicken Sie auf Launch Virtual Media (virtuellen Datenträger starten). Das Fenster "Video Viewer" wird geöffnet.

Anmerkung: Wenn vor dem Öffnen des Fensters "Video Viewer" das Kontrollkästchen Encrypt disk and KVM data during transmission (Disketten- und KVM-Daten während der Übertragung verschlüsseln) ausgewählt wurde, werden die Daten auf dem Datenträger mit ADES verschlüsselt.

Das Fenster "Virtual Media Session" ist von dem Fenster "Video Viewer" getrennt. Im Fenster "Virtual Media Session" sind alle Laufwerke auf dem Client aufgelistet, die als ferne Laufwerke zugeordnet werden können. Im Fenster "Virtual Media Session" können Sie außerdem ISO-Image- und Diskettenimage-Dateien als virtuelle Laufwerke zuordnen. Jedes zugeordnete Laufwerk kann als schreibgeschützt gekennzeichnet werden. Die CD- und DVD-Laufwerke sowie die ISO-Images sind immer schreibgeschützt.

#### Laufwerkzuordnung festlegen und aufheben

Wählen Sie zum Zuordnen eines Laufwerks das Kontrollkästchen **Select** (Auswählen) neben dem Laufwerk aus, das Sie zuordnen möchten.

**Anmerkung:** Ein CD- oder DVD-Laufwerk muss Datenträger enthalten, bevor es zugeordnet wird. Wenn das Laufwerk leer ist, werden Sie aufgefordert, eine CD oder eine DVD in das Laufwerk einzulegen.

Klicken Sie auf die Schaltfläche **Mount Selected** (Auswahl anhängen), um das ausgewählte Laufwerk bzw. die ausgewählten Laufwerke anzuhängen oder und zuzuordnen.Wenn Sie auf **Add Image** (Bild hinzufügen) klicken, können Diskettenund ISO-Imagedateien zur Liste verfügbarer Laufwerke hinzugefügt werden. Wenn die Disketten- oder ISO-Imagedatei im Fenster "Virtual Media Session" angeführt wird, kann sie genau wie die anderen Laufwerke zugeordnet werden.Klicken Sie zum Aufheben der Laufwerkzuordnung auf die Schaltfläche **Unmount All** (Alle abhängen). Bevor die Laufwerkzuordnungen aufgehoben werden, müssen Sie Ihren Wunsch bestätigen, dass die Laufwerkzuordnungen aufgehoben werden sollen.

**Anmerkung:** Nachdem Sie bestätigt haben, dass die Laufwerkzuordnungen aufgehoben werden sollen, werden sämtliche Laufwerke abgehängt. Sie können Laufwerke nicht einzeln abhängen.

Sobald ein Bild zur Liste hinzugefügt und das Kontrollkästchen **Map** (Zuordnung) ausgewählt wurde (vorausgesetzt, das Bild eignet sich zum Hochladen auf den IMM2-Speicher für die RDOC-Funktion), öffnet sich ein Fenster mit der Option, das Bild auf den Server zu übertragen. Wenn Sie **Yes** auswählen, geben Sie einen Namen für das Bild ein.

**Anmerkung:** Geben Sie keine Sonderzeichen wie etwa ein Et-Zeichen (&) oder Leerzeichen im Namen ein.

Durch das Hochladen eines Bildes kann die Festplatte an den Server angehängt bleiben, sodass Sie später Zugriff auf die Festplatte haben, auch nachdem die IMM2-Webschnittstellensitzung beendet wurde. Auf dem IMM2 können mehrere Bilder gespeichert werden; der insgesamt beanspruchte Speicherplatz darf jedoch 50 Mb nicht überschreiten. Um die Imagedatei aus dem Speicher herunterzuladen, wählen Sie deren Namen im Fenster "RDOC Setup" (RDOC-Konfiguration) aus und klicken Sie auf **Delete** (Löschen).

#### Fernsteuerung beenden

Schließen Sie die Fenster "Video Viewer" und "Virtual Media Session", wenn Sie die Verwendung der Fernsteuerungsfunktion beendet haben.

## **PXE-Netzboot einrichten**

Verwenden Sie die Option "PXE Network Boot" (PXE-Netzboot), um Bootversuche der Server-Ausführungsumgebung vor dem Start einzurichten. Führen Sie die folgenden Schritte aus, um Ihren Server für den Versuch eines PXE-Netzboots (Preboot Execution Environment) beim nächsten Serverneustart einzurichten.

- 1. Melden Sie sich am IMM2 an. Weitere Informationen finden Sie im Abschnitt "Am IMM2 anmelden" auf Seite 10.
- 2. Klicken Sie auf Server Management (Serververwaltung) und wählen Sie anschließend PXE Network Boot aus.

Das folgende Fenster wird geöffnet.



3. Wählen Sie aus den Optionen von "Actions" (Aktionen) die Option Attempt PXE Network Boot at next server restart (Bei nächstem Serverneustart PXE-Netzboot versuchen) aus. Das folgende Fenster wird geöffnet.



Wenn Sie die Auswahl zurücknehmen möchten, klicken Sie auf **CancelPxeBoot** (PXE-Boot abbrechen). Das folgende Fenster zum Bestätigen des Abbruchs (Confirm Cancel) wird geöffnet.



## Server-Firmware aktualisieren

In der Option "Server Firmware" werden die Firmwareversionen angezeigt und Sie können hier die DSA-, IMM2- und UEFI-Firmware aktualisieren. Die aktuellen Versionen der IMM2-, UEFI- und DSA-Firmware werden angezeigt. Dies umfasst die Versionstypen "Active" (Aktiv), "Primary" (Primär) und "Backup" (Sicherungskopie).

In der folgenden Abbildung ist die Seite "Server Firmware" dargestellt.

IBM Integrated Ma	anagement Modul	- 11			USERID Settings	Log ou
System Sta	tus Events • Se	rvice and Support 🔹 🕴	Server Nanagement 👻 IMM M	lanagement + Search		
Server Firm	IWARE vels on various server	components, including t	the IMM Itself.			
Firmware Tipe	+ Status	Version	Build	Release Date		
DSA	Active	9.24	DSYT44B	2012-08-10		
10012						
	Active	2.15	1AD0390	2013-01-28		
INVI2 (Primary)						
INN2 (Primary) INN2 (Backup)	Inactive	3.00	1A0039T	2013-01-30		
IWW2 (Primary) IWW2 (Backup) UEFI	Inactive	3.00	1A0039T	2013-01-30		
IMN2 (Primary) IMN2 (Backup) UEFI UEFI (Primary)	Active	3.00	140039T D7E120CUB	2013-01-30 2012-08-23		

Der aktuelle Status und die aktuellen Versionen der IMM2-, UEFI- und DSA-Firmware werden angezeigt, einschließlich der primären Versionen und der Sicherungsversionen. Der Status der Firmware wird in drei Kategorien angegeben:

- Active (aktiv): Die Firmware ist aktiv.
- Inactive (inaktiv): Die Firmware ist inaktiv.
- **Pending** (anstehend): Die Firmware befindet sich im Wartestatus vor der Aktivierung.

Achtung: Die Installation der falschen Firmware könnte eine Serverstörung verursachen. Bevor Sie eine Firmware- oder Einheitentreiberaktualisierung installieren, lesen Sie alle Readme- und Änderungsprotokolldateien, die mit der heruntergeladenen Aktualisierung bereitgestellt werden. Diese Dateien enthalten wichtige Informationen zur Aktualisierung und zur Installationsprozedur der Aktualisierung, einschließlich Informationen zu besonderen Prozeduren bei der Aktualisierung von einer frühen Firmware- oder Einheitentreiberversion auf die neueste Version.

Gehen Sie wie folgt vor, um die Server-Firmware zu aktualisieren:

- 1. Klicken Sie in der Menüliste "Server Management" auf Server Firmware.
- Klicken Sie auf Update Firmware (Firmware aktualisieren). Das Fenster "Update Server Firmware" (Server-Firmware aktualisieren) wird geöffnet (wie in der folgenden Abbildung dargestellt).



- 3. Lesen Sie den Warnhinweis, bevor Sie mit dem nächsten Schritt fortfahren.
- 4. Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie auf **Cancel** (Abbrechen) und kehren Sie zum vorherigen Fenster "Server Firmware" zurück.
  - Klicken Sie auf **Select File...** (Datei auswählen), um die gewünschte Firmwaredatei zum Durchführen eines Flash-Updates der Server-Firmware auszuwählen.

**Anmerkung:** Alle anderen Optionen sind beim ersten Öffnen des Fensters "Update Server Firmware" abgeblendet.

Wenn Sie auf **Select File...** klicken, wird das Fenster "File Upload" (Hochladen von Datei) geöffnet (wie in der folgenden Abbildung dargestellt). In diesem Fenster können Sie nach der gewünschten Datei suchen.

System Status	Update Server Firmw	erver Firmware						
Server Firmw	Choose Firmware File Upload and Vierfy	Select Firmware File Select the firmware file that you w	Select Firmware File Select the firmware file that you wish to use to fash the DM/Server Firmware					
Update Firmware Firmware Type DSA MISIZ (Active)	Additional Options Perform Fernisare Flash	Please note that upd purposes only. It is a Updates/press Syste	ating server firmware via trongly recommended tha m Pack Installer, available	this wizard is intended for re t updates be performed usin as a download from the 254	covery g the IBM ( web site.			
MM2 (Primary) MM2 (Backup)			File Upload				28	
UEFI (Adiva) UEFI (Primary) UEFI (Bachup)			Select File	Look in My Recert Documents	System x37504w.upd	ifes -1.60_anyos_noa	rðhuxz	
	< Back Next > Fi	nish Cancel	My Documents					
			(1)	Fienane: brife	.jmn2_1aos31-1	50_anyos_noarch.uxz M	Open	

 Navigieren Sie zu der Datei, die Sie auswählen möchten, und klicken Sie auf Open (Öffnen). Sie kehren zum Fenster "Update Server Firmware" zurück. Die ausgewählte Datei wird angezeigt (wie in der folgenden Abbildung dargestellt).

Update Server Firmw	are
Choose Firmware File	Select Firmware File
Upload and Verify	Select the firmware file that you wish to use to flash the DMM/Server Firmware
Additional Options	
Perform Firmware Flash	Please note that updating server firmware via this wizard is intended for recovery purposes only. It is strongly recommended that updates be performed using the IBM Updates/Qress System Pack Installer, available as a download from the IBM web site.
	Selected Flash File: ibm_fw_imm2_1aoo311.60_anyos_noarch.uxz
< Back Next > F	inish Cancel

6. Klicken Sie auf **Next** > (Weiter), um die ausgewählte Datei hochzuladen und zu prüfen. Eine Fortschrittsanzeige wird angezeigt, während die Datei hochgeladen und geprüft wird (wie in der folgenden Abbildung dargestellt).



Sie können dieses Statusfenster anzeigen, um zu prüfen, ob Sie die richtige Datei zur Aktualisierung ausgewählt haben. Das Statusfenster enthält Informationen zum Dateityp der Firmware, die aktualisiert wird, wie DSA, IMM oder UEFI.

Nachdem die Firmwaredatei erfolgreich hochgeladen und geprüft wurde, erscheint ein Fenster mit der Meldung, dass das Hochladen erfolgreich war (Successful upload) (wie in der folgenden Abbildung dargestellt).



 Klicken Sie auf Next >, wenn die Informationen richtig sind. Klicken Sie auf < Back (Zurück), wenn Sie Ihre Auswahl ändern möchten.

Wenn Sie auf **Next** > klicken, wird eine Gruppe zusätzlicher Optionen angezeigt (wie in der folgenden Abbildung dargestellt).

Update Server Firmware	8		
Choose Firmware File	Additional Options Some firmware types have	3 e additional options that you can select.	
Additional Options			
Perform Firmware Flash	Action1:	Update the primary bank (default action)	* *
Park (Managara) Colo	k.		

8. Im Dropdown-Menü neben dem Feld Action 1 (Aktion 1) können Sie die Aktion Update the primary bank (default action) (primäre Speichergruppe aktualisieren (Standardaktion)) oder die Aktion Update the backup bank (Sicherungsspeichergruppe aktualisieren) auswählen (wie in der folgenden Abbildung dargestellt).

Update Server Firmware							
Choose Firmware File	Additional Options Some firmware types have additional options that you can select.						
Additional Options							
Perform Firmware Flash	Action1:	Undate the primary bank (default action)					
	Action2:	Update the primary bank (default action)					
		Update the backup bank					
<back next=""> Finish</back>	Cancel						

Nachdem Sie eine Aktion ausgewählt haben, kehren Sie zur vorherigen Anzeige zurück. Die angeforderte Zusatzaktion wird angezeigt.

Nachdem die ausgewählte Aktion geladen wurde, werden diese Aktion und ein neues Dropdown-Menü **Action 2** (Aktion 2) angezeigt (wie in der folgenden Abbildung dargestellt).

**Anmerkung:** Um eine Aktion zu inaktivieren und die Auswahl zusätzlicher Optionen erneut zu starten, klicken Sie auf das Kontrollkästchen neben der zugehörigen Aktion.

Update Server Firmware								
<ul> <li>Choose Firmware File</li> <li>Upload and Verify</li> </ul>	Additional Options Some firmware types have additional options that you can select.							
Additional Options								
Perform Firmware Flash	Action1:	Update the primary bank (default action) Update the backup bank	×					
		k						
< Back Next > Finis	Cancel							

In der vorherigen Anzeige sehen Sie, dass für "Action 1" die primäre Speichergruppe zum Aktualisieren ausgewählt ist. Sie können auch auswählen, dass die Sicherungsspeichergruppe unter "Action 2" aktualisiert werden soll (wie in der vorherigen Abbildung dargestellt). Die primäre Speichergruppe und die Sicherungsspeichergruppe werden gleichzeitig aktualisiert, wenn Sie auf **Next** > klicken.

Anmerkung: "Action 1" muss sich von "Action 2" unterscheiden.

Eine Fortschrittsanzeige zeigt den Fortschritt der Aktualisierung der primären Speichergruppe und der Sicherungsspeicherguppe an (wie in der folgenden Abbildung dargestellt).

Update Server Firmwa	are						
Choose Firmware File	Perform Firmware Flash >The firmware is being flashed now.						
Additional Options	Action 1 of 2: 'Update the primary bank (default action)'						
Perform Firmware Flash	Action 2 of 2: "Update the backup bank"						
	27%						
< Back Next > Fir	inish Cancel						

Wenn die Firmwareaktualisierung erfolgreich abgeschlossen wurde, wird das folgende Fenster geöffnet. Wählen Sie die zugehörige Operation entsprechend den angezeigten Inhalten aus, um den Aktualisierungsprozess abzuschließen.

Update Server Firmware	
Choose Firmware File	Perform Firmware Flash >The firmware is being flashed now.
Additional Options	
Perform Firmware Flash	
	Firmware update success. The firmware update procedure completed successfully. Click Finish to close this wizard. If the update included a flash of the IMM primary partition, it will also be necessary to Restart the IMM for the IMM update to take effect. If the update included a flash of the UEFI firmware it will also be necessary to Restart the OS for the update to take effect.
	Restart OS Restart IMM
< Back Next> Finish	Cancel

Wenn die primäre Firmwareaktualisierung nicht abgeschlossen wurde, wird das folgende Fenster geöffnet, wenn die Anzeige "Server Firmware" aufgerufen wird.

IBM Integrated Ma	anage	ment Modul	e II			USERID	Settings   Log out	IBM.
System Sta	tus	Events + S	ervice and Support +	Server Management +	IMM Management - Search			
Server Firm	NWa vels on	re various serve	r components, includir	ng the IMM itself.				
Firmward The firm pending to previous The prim to take et	e upda ware bu trmwar build na ary IMM flect.	te is successfu ids below requi e will keep the p ime. I build has been	II: re restart actions. Before revious build and the tabl updated to build 1AOO3	the actions are taken, the e below still show the 90 , and it must restart IMM				
Restart OS	R	estart IMM	Schedule Restart Ac	tions				
Restart OS	R	estart IMM	Schedule Restart Ac	tions Build	Release Date			
Restart OS Update Firmware Firmware Type DSA	(R	Status Active	Schedule Restart Ac Version 9.24	tions Build DSYTA4B	Release Date 2012-08-10			
Restart OS Update Firmware Firmware Type DSA IMM2	R	Status Active	Schedule Restart Ac Version 9.24	Build DSYTA4B	Release Date 2012-08-10		-	
Restart OS Update Firmware Firmware Type DSA IMM2 IMM2 (Primary)	R	Status Active Pending	Schedule Restart Ac Version 9.24 2.15	Build DSYTA4B 1A0039Q	Release Date 2012-08-10 2013-01-28			
Restart OS Update Firmware Firmware Type DSA IMM2 IMM2 IMM2 (Primary) IMM2 (Backup)	(R	Status Active Pending Inactive	Schedule Restart Ac 9.24 2.15 2.15	Build DSYTA4B 1A0039Q 1A0039Q	Release Date 2012-08-10 2013-01-28 2013-01-28			
Restart OS Firmware Type DSA MM2 IMM2 (Primary) IMM2 (Backup) UEFI	R	Status Active Pending Inactive	Version 9.24 2.15 2.15	Build DSYTA4B 1A0039Q 1A0039Q	Release Date 2012-08-10 2013-01-28 2013-01-28			
Restart OS Update Firmware Type DSA IMM2 IMM2 (Primary) IMM2 (Backup) UEFI UEFI UEFI (Primary)	R	Status Active Pending Inactive Active	Schedule Restart Act 9.24 2.15 2.15 1.20	Build DSYTA4B 1A0039Q D7E12009	Release Date 2012-08-10 2013-01-28 2013-01-28 2013-01-28			

# Systemereignisse verwalten

Das Menü "Events" (Ereignisse) ermöglicht es Ihnen, den Verlauf des Ereignisprotokolls (Event Log) und die Ereignisempfänger (Event Recipients) für E-Mail- und syslog-Benachrichtigungen zu verwalten.

## Ereignisprotokoll verwalten

Klicken Sie auf die Option **Event Log** (Ereignisprotokoll), um das Fenster "Event Log" anzuzeigen. Das Fenster "Event Log" beinhaltet eine Beschreibung der Ereignisse, die durch das IMM2 gemeldet werden, und Informationen zu allen Fernzugriffsversuchen und Konfigurationsänderungen. Alle Ereignisse im Protokoll besitzen eine Zeitmarke, die die Datums- und Uhrzeiteinstellungen des IMM2 verwendet. Einige Ereignisse generieren Alerts, falls sie im Fenster "Event Recipients" (Ereignisempfänger) entsprechend konfiguriert wurden. Im Ereignisprotokoll können Sie Ereignisse auch sortieren und filtern.

Klicken Sie auf die Option Event Log. Das folgende Fenster wird geöffnet.

IBM Integrated Management Module II							
System Status	Events 🕶	Service and Support + Server Management + IMM Management +					
	Event Log	Full log history of all events					
System x3750 Add System Descriptive Nam	Event Red	cipients Add and modify E-Mail and SysLog notifications					

Nach Auswahl der Option "Event Log" wird das folgende Fenster geöffnet.

1 🔜 💌 📓		Fiters: 🔕	🛕 🚺 🛔 Time: Al Dates	Search Events: . Go
Severity	Source	Date	Event ID	Message
0 of 51 items filte	red	0 items selected	Clear filter Applied filters: Events ( Erro	r Warning Information Audit ]
information:	al System	31 1 2013 09:02:42.771 AM	0x4000000e00000000	Remote Login Successful, Login ID: USERID from webguis at IP address 9.111.29.57.
Information:	al System	31 1 2013 09:01:00.297 AM	0x400000160000000	ENET[CM.ep1] DHCP.HSTN-NMM2-5cae8b4e83c6, DN=on.ibm.com, IP@=9.186.166.78, SN+255 255 128, GW@=9.186.166.1, DNS1@=9.0.148.50.
III Information:	al System	31 1 2013 09:00:58.957 AM	0x4000001900000000	LAN: Ethernet(IBM:ep2) interface is now active.
information:	al System	31 1 2013 0R 00:55 004 AM	0x4000001700000000	ENET[CIM4p2] IP-CfgH8tName=INN2-6cae8b4e83c6. IP@=169.254.95.118.NetIIsk=255.255.0.0. GW@=0.0.0.0.
Information:	al System	31 1 2013 09:00:53 403 AM	Dx4000003700000000	ENET[CM.ep1] IPv6-Linit_ocal HstName=IMM2-5cae8b4e83c5, IP@=te80:5eae8bfffe4e83c5,Pret=64.
Information:	al System	31 1 2013 09:00:51 592 AM	0x4000001900000000	LAN: Ethernet(IBM:ep1) interface is now active.
information:	al System	31 1 2013 09:00:47.068 AM	0x4000000100000000	Management Controller SN# 05KNKL9 Network Initialization Complete
Information:	al System	31 1 2013 09:00:02.874 AM	0x800801282101mm	Device Low Security Jmp has been added.
Information:	al Power	31 1 2013 09:00:02:304 AM	0x805f00091301fm	Host Power has been turned off.
Information:	al System	31 1 2013 08:55:11.252 AM	0x4000001500000000	Management Controller SN# 05KNKL9 reset was initiated by user USERID.
Information:	al System	31 1 2013 08:47:59.118 AM	0x4000002300000000	Flash of SN# D5kNKL9 from (: 107.9.186.166.119) succeeded for user USERID .
Information.	al System	31 1 2013 08 43 15 666 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.185 156 119.
The information	al Guetana	24 4 2042 02 04 07 470 444	0-1000000-00000000	Remote Login Successful, Login ID: USERID from

Um Ereignisse im Ereignisprotokoll zu sortieren und zu filtern, wählen Sie die entsprechende Spaltenüberschrift aus (wie in der folgenden Abbildung dargestellt).



Sie können mithilfe der Schaltfläche **Export** alle oder ausgewählte Ereignisse aus dem Ereignisprotokoll speichern. Um bestimmte Ereignisse auszuwählen, wählen Sie auf der Hauptseite von "Event Log" ein oder mehr Ereignisse aus und klicken Sie mit der linken Maustaste auf die Schaltfläche **Export** (Exportieren) (wie in der folgenden Abbildung dargestellt).

Event Log This page displays the contents of the IMM event log, and allows y entry first). For each log entry, the severity of the event is displayed Export Event Logs								
	Severity Source Date							
	0 of 52 items filtered		2 items selecte					
	🚹 Informational	System	31 Jan 2013 09:1					
	🚹 Informational	System	31 Jan 2013 09:0					

Klicken Sie auf **Delete Events** (Ereignisse löschen), um auszuwählen, welche Ereignistypen Sie löschen möchten. Sie müssen die Kategorie der Ereignisse, die Sie löschen möchten, auswählen.

In der folgenden Abbildung ist das Fenster "Delete Events" dargestellt.

2   🖼 🦉 🖩	A MP	Filte	ers; 🔕 🛕 🚺 🔮	Time: All Dates	✓ Search Events Go
Severity	Source	Date			Message
0 of 52 items filter	red	Delete Events		х	g Information Audit ]
Informationa	al System	3 Choose which ev	ents you wish to delete		Remote Login Successful, Login ID: US webguis at IP address 9 186.166.119.
🖸 👔 Informationa	al System	3 Platform Events	15		Remote Login Successful. Login ID: US webguis at IP address 9.111.29.57.
Informations	al System	OK Cancel	0.131.40% 0040000010000	00000	ENET[CIM:ep1] DHCP-HSTN=IMM2-6cae8b4e83c6, DN=cn.ibm.com, IP@=9.186.166.78, SN=255.255.255.128, GW/@=9.186.164

Um den Typ der Ereignisprotokolleinträge auszuwählen, die Sie anzeigen möchten, klicken Sie auf die entsprechende Schaltfläche (wie in der folgenden Abbildung dargestellt).

Refresh Events	Warning Events	Audit Events	
a i 🔁 🖉 🔛 🖿	Filters: 🔞 🛕	Time:	All Dates - Search Events Go
Visible Columns	Error Events	Information Events	Date ranges to show

Um nach bestimmten Ereignistypen oder Suchbegriffen zu suchen, geben Sie den betreffenden Ereignistyp oder den Suchbegriff im Feld **Search Events** (Ereignisse suchen) ein. Klicken Sie dann auf **Go** (Start) (wie in der folgenden Abbildung dargestellt).

2	🔜 🧏 🔛	XIII AM	Filters: 🔞			Time: All Dates	- IE	NET M
	Severity	Source	Date	-	Event ID		Message	
*	0 of 53 items filtered		0 items selected	2	Clear filter Appli	ed filters: Events:[Error V	Warning Informatio	on Audit]
	11 Informational	System	1 Feb 2013 01:29:28.414 AM		0x4000000e000	00000	Remote Log webguis at l	gin Successful. Login ID: USERID IP address 9.186.166.119.

# Benachrichtigung zu Systemereignissen

Wählen Sie die Option **Event Recipients** (Ereignisempfänger) aus, um E-Mail- und syslog-Benachrichtigungen hinzuzufügen und zu ändern.

In der folgenden Abbildung ist die Auswahl der Option "Event Recipients" dargestellt.

IBM Integrated Management Module II									
System Status	Events 👻	Service and Support	Ŧ	Server Management 👻	IMM Management + Sea				
	Event Log		Full	log history of all events					
System x3750 Add System Descriptive Nam	Event Recipients		Add	SysLog					

Mithilfe der Option "Event Recipients" können Sie die Empfänger von Benachrichtigungen über Systemereignisse verwalten. Sie können die einzelnen Empfänger konfigurieren und die Einstellungen verwalten, die auf alle Ereignisempfänger angewendet werden. Sie können außerdem ein Testereignis erstellen, um zu überprüfen, ob die Benachrichtigungsfunktion funktioniert. In der folgenden Abbildung ist die Seite "Event Recipients" dargestellt.



In der folgenden Abbildung sind weitere Informationen dargestellt, die angezeigt werden, wenn Sie auf den Link **more** (mehr) auf der Seite "Event Recipients" klicken.



### E-Mail- und syslog-Benachrichtigungen erstellen

Wählen Sie die Registerkarte **Create** (Erstellen) aus, um E-Mail- und syslog-Benachrichtigungen zu erstellen.

In der folgenden Abbildung sind die verfügbaren Optionen im Menü "Create" dargestellt.

IBM Integrated Manageme	nt Module II			
System Status Ever	nts 👻 Service and Si	upport 👻 Server Manage	ment 👻 IMM Man	agement - Search
Event Recipients This table lets you view a sum labeled with the configured nam Create V Generate Test E	mary list of all remote a re for that particular re vent Global Set	alert recipients. Use the link cipient more tings	is in the Name colu	mn to configure individual alert recip
Create E-mail Notification	tification Method	Events to Receive	Status	
Create SysLog Notification				

Mit der Option **Create E-mail Notification** (E-Mail-Benachrichtigung erstellen) können Sie eine Empfangs-E-Mail-Adresse einrichten und die Ereignistypen auswählen, über die Sie benachrichtigt werden möchten. Außerdem können Sie auf **Advanced Settings** (Erweiterte Einstellungen) klicken, um die Startindexzahl auszuwählen. Um das Ereignisprotokoll in die E-Mail einzufügen, wählen Sie das Kontrollkästchen **Include the event log contents in the e-mail body** (Ereignisprotokollinhalte in den E-Mail-Text einfügen) aus. In der folgenden Abbildung ist die Anzeige "Create E-mail Notification" dargestellt.

Create E-Mail Notificatio	on			×
Use this dialog to configu Note: To enable an E-ma Descriptive name: E-Mail address:	ure specified E-mail recipier il recipient, you need to go	its to re <u>ceive Critical, Attention or Syste</u> m noti to the SMTP tab on Network Protocols page t	ications o configure the email server correctly.	
Events to receive: Select all events Show sub-types	2 Critical	<b>₩</b> Attention	✓ System	
Include the event log	contents in the e-mail body	(		
Enable this recipient     Disable this recipient				
OK Cancel				

In der folgenden Abbildung sind die Optionen des Teilfensters "Advanced Settings" dargestellt.

Create	E-Ma	il Notification			
Use this Note: To Descrip E-Mail a	dialo enat tive r	g to configure specified E-mail recipie le an E-mail recipient, you need to go name:	Its to receive Critical, Attention or System notification to the SMTP tab on Network Protocols page to con	ons figure the email server correctly.	
Events t	2	e: ents			
> Sh	4	types Critical	Z Attention	System	
Inclu	6 7	vent log contents in the e-mail body			
Status: Enat Disal	8 9 10	ecipient recipient	k		
	11	ettings			
Specif	12	dex number in the command line int	erface for this alert recipient		
OK	Can	cel			

Mit der Option **Create Syslog Notification** (syslog-Benachrichtigung erstellen) können Sie den Hostnamen und die IP-Adresse des syslog-Collectors einrichten und die Ereignistypen auswählen, über die Sie benachrichtigt werden möchten. Sie können auf **Advanced Settings** klicken, um die Startindexzahl auszuwählen. Sie können außerdem den Port auswählen, den Sie für diesen Benachrichtigungstyp verwenden möchten.

In der folgenden Abbildung ist die Anzeige "Create Syslog Notification" dargestellt.

Create SysLog Notification			×
Use this dialog to configure specified SysLog server to	receive Critical, Attention or System notifi	cations.	
.Descriptive name:			
Host name or IP address of the SysLog collector:	Port:		
Events to receive:			
Show sub-types	Z Attention	🔽 System	
Status: © Enable this recipient Disable this recipient			
Advanced Settings			
OK Cancel			

In der folgenden Abbildung sind die Optionen des Teilfensters "Advanced Settings" dargestellt.

### Testereignisse generieren

Verwenden Sie die Registerkarte **Generate Test Event...** (Testereignis generieren), um eine Test-E-Mail an eine bestimmte E-Mail-Adresse zu senden. Klicken Sie nach Auswahl der Ereignisbenachrichtigung auf **OK**, um ein Testereignis zu generieren. Das Testereignis mit dem Hinweis, dass es sich um einen Test handelt, wird an den Empfänger gesendet.

In der folgenden Abbildung ist das Fenster "Generate Test Event" dargestellt.

IBM	Integrated Ma	magement Module II								USERID	Settings	Log 6
2	System Stat	tus Events + Service and Si	upport 🔹 Server Hanage	roent 🐖 DHM Mar	nagement •	t + (See	A.222	1				
Ve This release	nt Recip table lets you vi with the confo	Dients ew a summary list of all remote : gured name for that particular re ite Test Event	alert recipients. Use the lini opientmore tings	is in the Name colu	umn to conf	infigure ind	lvidual alert rec	ipients. You can	define up to 12 i	nique recipient	s. Each link f	lor an aler
	Name	Notification Method	Events to Receive	Status								
	Target User	E-Mall	None	Enabled								
	(	Generate Test Event										×
		This will generate a	test event and will be	broadcast to th	the recipie	iient 'Targ	get User' indi	cating that it	is just a test.	Do you wish	to procee	d7

### Wiederholungslimit für Benachrichtigungen festlegen

Verwenden Sie die Registerkarte **Global Settings...** (Globale Einstellungen), um ein Wiederholungslimit für die Ereignisbenachrichtigungen festzulegen. Bestimmen Sie das Verzögerungsintervall zwischen den Ereignisbenachrichtigungen (in Minuten) und zwischen den Versuchen (in Minuten).

In der folgenden Abbildung sind die Einstellungen für die Option "Retry limit" (Wiederholungslimit) dargestellt.



In der folgenden Abbildung sind die Einstellungen für die Option "Delay between entries (minutes)" (Verzögerung zwischen Einträgen (Minuten)) dargestellt.

Event	Event Notification Global Settings	
Thes	e settings will apply to all event notifications.	
Retry	limit: 🎯	
Delay	between entries (minutes): 🧼	
0.5	etween attempts (minutes): 🤍	
0.5		
1	ancel	
1.5		
2		
2.5		
3		
3.5		
4		

In der folgenden Abbildung sind die Einstellungen für die Option "Delay between attempts (minutes)" (Verzögerung zwischen Versuchen (Minuten)) dargestellt.

Event Notification Global Settings	х
These settings will apply to all event notifications.	
Retry limit:	
Delay between entries (minutes): 0.5 👻	
Delay between attempts (minutes): 0.5	
0 ancel	
0.5	
1.5	
2	
2.5	
3	
3.5	
4	

## E-Mail- oder syslog-Benachrichtigungen löschen

Verwenden Sie die Registerkarte **Delete** (Löschen), um ein E-Mail- oder syslog-Benachrichtigungsziel zu löschen.

In der folgenden Abbildung ist das Fenster "Confirm Event Notification Deletion" (Löschen der Ereignisbenachrichtigung bestätigen) dargestellt.

IBM Integrated Manag	ement Module II Events - Service and Si	upport 👻 Server Manage	ment 👻 IMM Manager	nent 👻 Sear
Event Recipie This table lets you view a name for that particular rec Create	nts summary list of all remote a ipient more est Event Global Set	alert recipients. Use the lini	is in the Name column t	o configure in
Name	Notification Method	Events to Receive	Status	
Email Subject	E-Mail	None	Enabled	
Email2 Subject	E-Mail	None	Enabled	
Confi	rm Event Notification [	Deletion	x	
3	Do you want to delet	e the notification 'Ema	il Subject' ?	
OK	Cancel			
Committee of the second s				
# Informationen für Service und Support erfassen

Klicken Sie auf die Option **Download Service Data** (Servicedaten herunterladen) im Menü "Service and Support" (Service und Support), um Informationen zum Server zu erfassen. Diese kann der IBM Support verwenden, um Sie bei der Lösung Ihres Problems zu unterstützen.

In der folgenden Abbildung ist das Menü "Service and Support" dargestellt.

IBM Integrated Management Module II							
System Status Events 🗸	Service and Support $\bullet$	Server Management + IMM Management + Search					
System x3750 M4	Download Service Da	ta Obtain a compressed file of relevant service data					

Klicken Sie auf die Schaltfläche **Download Now** (Jetzt herunterladen), wenn Sie die Daten für Service und Support herunterladen möchten.

In der folgenden Abbildung ist das Fenster "Download Service Data" (Servicedaten herunterladen) dargestellt.

IBM Integrated Management Module II							
	System Status	Events 🗸	Service and Support $\star$	Server Management 👻	IMM Management 🗸	Search	
Dow Allows yo personne Downk	nload Ser ou to manually obt el. pad Now Send	vice D tain the serv Service Info	ata ice data for your system. I rmation	Normally you would only d	o this at the request o	f IBM Support	

Der Erfassungsprozess der Daten für Service und Support wird gestartet. Dieser Prozess dauert ein paar Minuten; es werden die Servicedaten zum Speichern in einer Datei generiert.

Das folgende Fortschrittsfenster wird angezeigt, während die Servicedaten generiert werden.



Nachdem der Prozess beendet wurde, werden Sie dazu aufgefordert, den Speicherort für die Datei anzugeben. Ein Beispiel dafür finden Sie in der folgenden Abbildung.



### Daten der letzten Betriebssystem-Fehleranzeige erfassen

Verwenden Sie die Option "Latest OS Failure Screen" (Letzte Betriebssystem-Fehleranzeige), um die Daten der Betriebssystem-Fehleranzeige zu erfassen und zu speichern. Das IMM2 speichert nur die Informationen zu den aktuellsten Fehlerereignissen und überschreibt die Daten früherer Betriebssystem-Fehleranzeigen, wenn ein neues Fehlerereignis auftritt. Die Funktion "OS Watchdog" (Betriebssystem-Watchdog) muss aktiviert sein, damit Sie die Betriebssystem-Fehleranzeige erfassen können. Wenn ein Ereignis eintritt, durch das die Ausführung des Betriebssystems gestoppt wird, wird die Funktion "OS Watchdog" ausgelöst. Die Erfassung der Betriebssystem-Fehleranzeige ist nur mit der IMM2-Funktion "Advanced Level" verfügbar. Informationen zur Funktionalitätsstufe des IMM2, das in Ihrem Server installiert ist, finden Sie in der Dokumentation zum Server.

Um ein Bild einer Betriebssystem-Fehleranzeige über Fernzugriff anzuzeigen, wählen Sie eine der folgenden Menüoptionen aus:

- Latest OS Failure Screen auf der Registerkarte "Server Management"
- Registerkarte Latest OS Failure Screen auf der Seite "System Status"

**Anmerkung:** Wenn eine Betriebssystem-Fehleranzeige nicht erfasst wurde, wird die Registerkarte "Latest OS Failure Screen" auf der Seite "System Status" abgeblendet angezeigt und kann nicht ausgewählt werden.

In der folgenden Abbildung ist die Betriebssystem-Fehleranzeige dargestellt.



#### Serverstromversorgung verwalten

Verwenden Sie die Registerkarte "Power Management", um die folgenden Tasks auszuführen:

- Zeigen Sie Informationen zu installierten Netzteilen an.
- Steuern Sie, wie die "Leistung" der Stromversorgung verwaltet wird.
- Steuern Sie die gesamte Stromversorgung des Systems.
- Zeigen Sie Informationen zu installierten Netzteilen und der aktuellen Stromversorgungskapazität an.
- Zeigen Sie das Verlaufsprotokoll zur Stromverbrauchsmenge an.

Wählen Sie die Option **Power Management** (Stromverbrauchssteuerung) unter der Registerkarte "Server Management" (Serververwaltung) aus, um Informationen zur Stromverbrauchssteuerung anzuzeigen und Funktionen zur Stromverbrauchssteuerung auszuführen (wie in der folgenden Abbildung dargestellt).

Server Management -	IMM Management - Search
Server Firmware	View firmware levels and update firmware
Remote Control	Allows you access into the operating system of your system
Server Properties	Various properties and settings related to your system
Server Power Actions	Power actions such as power on, power off, and restart
Cooling Devices	Cooling devices installed in your system
Power Modules	Power modules installed in your system
Disks	Hard disk drives installed directly in your system
Memory	RAM installed in your system
Processors	Physical CPUs installed in your system
Server Timeouts	Configure watchdogs, etc.
PXE Network Boot	Settings for how your system performs boot from PXE server
Latest OS Failure Screen	Windows systems only. View an image of the most recent failure screen.
Power Management	Power devices, policies, and consumption

# Stromversorgung und gesamte Stromversorgung des Systems steuern

Klicken Sie auf die Registerkarte **Policies** (Richtlinien), um zu steuern, wie die Stromversorgung verwaltet wird. Außerdem können Sie optional die gesamte Stromversorgung des Systems über "Active Energy Manager" steuern, indem Sie eine Begrenzungsrichtlinie festlegen (wie in der folgenden Abbildung dargestellt).

**Anmerkung:** Die Registerkarte **Policies** ist in einem IBM Flex System-Knoten nicht verfügbar.



Um die Richtlinie auszuwählen, die Sie zum Schützen Ihres Servers bei Ausfall eines Stromversorgungsmoduls verwenden möchten, klicken Sie im Fenster "Power Policies" (Stromversorgungsrichtlinien) auf die Schaltfläche **Change** (Ändern) von "Current Policy" (Aktuelle Richtlinie) für die Option "Redundant with Throttling" (Redundant mit Leistungsdrosselung).

**Anmerkung:** Durch Auswahl einer Stromversorgungsrichtlinie können Sie einen Kompromiss zwischen Redundanz und verfügbarer Leistung finden.

Die Auswahlmöglichkeiten für die Stromversorgungsrichtlinie sind:

#### Redundant without Throttling (Redundant ohne Leistungsdrosselung)

Das Booten des Servers ist zulässig, wenn garantiert ist, dass der Server den Ausfall eines Netzteils übersteht und ohne Leistungsdrosselung in Betrieb bleiben kann.

#### Redundant with Throttling (Redundant mit Leistungsdrosselung)

Das Booten des Servers ist zulässig, wenn garantiert ist, dass der Server den Ausfall eines Netzteils übersteht, aber möglicherweise ist eine Leistungsdrosselung des Servers notwendig, damit er in Betrieb bleibt.

#### Non-Redundant (Nicht redundant)

Das Booten des Servers ist zulässig, wenn garantiert ist, dass der Server ohne Leistungsdrosselung in Betrieb bleibt und beide Stromversorgungsmodule betriebsbereit sind. Die Leistung des Servers wird gedrosselt, wenn der Versuch, den Betrieb eines Netzteils aufrechtzuerhalten, fehlschlägt; es gibt jedoch keine Garantie dafür.

Das folgende Fenster wird geöffnet, wenn Sie die Schaltfläche **Change** für die Option "Redundant with Throttling" auswählen.

Power Policies			
	Power Supply Failure Limit <sup>1</sup>	Maximum Power Limit (Watts)	Estimated Usage <sup>††</sup>
Redundant without Throttling			
System will be allowed to boot only if it is guaranteed to survive the loss of a power supply and continue to run without throttling.	1	550	100%
© Redundant with Throttling			
System will be allowed to boot only if it is guaranteed to survive the loss of a poper supply, though it may need to throttle to continue running.	1	660	83%
Non-Redundant			
System will be allowed to boot provided that it is guaranteed to stay up and running without throtting and both power supplies operational. The system will throttle if a power supply fails in an attempt to stay up and running, but there is no guarantee.	0	1045	52%
<sup>†</sup> This is the maximum number of power supplies that can fail while still guaranteeing the operation of the selecte	d policy.		
<sup>11</sup> The estimated usage is based on the maximum power limit allowed in this policy and the current aggregated p	ower in use of all	components in t	he chassis.
Ok Cancel			

Über "Active Energy Manager" können Sie einen Grenzwert für den zulässigen Gesamtnetzstromverbrauch des Servers festlegen. Um einen Grenzwert für den Stromverbrauch des Servers festzulegen, klicken Sie im Fenster "Power Policies" auf die Schaltfläche **Change** von "Current Policy" für die Option "Power Limiting/ Capping Policy" (Netzstrombegrenzung/Begrenzungsrichtlinie). Das Fenster "Change Power Capping Policy" (Netzstrombegrenzungsrichtlinie ändern) wird geöffnet (wie in der folgenden Abbildung dargestellt).



Wählen Sie die Schaltfläche **Power Capping** (Netzstrombegrenzung) aus und verschieben Sie die Schiebereglermarke auf die gewünschte Wattleistung. Der Pfeil rechts unter der Schiebereglermarke zeigt die minimale Einstellung an, die durch "Active Energy Manager" garantiert werden kann. Der Pfeil links unter der Schiebereglermarke zeigt den maximalen Stromverbrauch des Systems in den letzten 24 Stunden an. Diese beiden Pfeile stellen einen Richtwert für das Festlegen eines Grenzwerts für die Netzstrombegrenzung dar.

#### Aktuell installierte Netzteile anzeigen

Klicken Sie auf die Registerkarte **Power Modules** (Stromversorgungsmodule), um Informationen zu aktuell installierten Netzteilen anzuzeigen (wie in der folgenden Abbildung dargestellt).

Server Manage pow	Power I	Aanagement	t	
Policies	Power Modul	Power Allocation	Power History	
Display po with 3 tabs	wer modules in t Events, HW Info	S ne system with status ar , and Errors.	nd power ratings. Clicking	a module displays a Properties pop-up window
Name	<ul> <li>Stat</li> </ul>	21	Rated Power (Watts)	
Name Power Sy	stem Sta	lormal	Rated Power (Watts) N/A	_
Name Power Sy Power 1	stem Sta	lormal	Rated Power (Watts) N/A 550	_

Der Name jedes Stromversorgungsmoduls im Server wird zusammen mit dem Status und der Belastbarkeit der einzelnen Netzteile angezeigt. Um weitere Informationen zu einem Stromversorgungsmodul anzuzeigen, klicken Sie auf den Namen eines Stromversorgungsmoduls. Das Fenster "Properties" (Eigenschaften) wird geöffnet. Es enthält drei Registerkarten für das ausgewählte Modul: Events (Ereignisse), HW Info (Hardware-Info) und Errors (Fehler).

### Stromversorgungskapazität anzeigen

Klicken Sie auf die Registerkarte **Power Allocation** (Netzstromzuordnung), um anzuzeigen, wie viel der Stromversorgungskapazität verwendet wird, und um den aktuellen Gleichstromverbrauch des Servers anzuzeigen (wie in der folgenden Abbildung dargestellt).



# Verlaufsprotokoll zum Stromverbrauch

Klicken Sie auf die Registerkarte **Power History** (Verlaufsprotokoll zum Stromverbrauch), um für einen ausgewählten Zeitraum anzuzeigen, wie viel Strom vom System verbraucht wird. Über die Registerkarte **Chart** (Diagramm) können Sie den Zeitraum auswählen. Außerdem haben Sie auch die Möglichkeit, den Wechseloder Gleichstrom anzuzeigen. Der durchschnittliche, maximale und minimale Stromverbrauch wird angezeigt (wie in der folgenden Abbildung dargestellt).

ower	HIS	tory														
	-															
Chart		Table														
The cha	rt below	shows th	e DC po	wer consump	stion history. Y	ou can ch	heck the a	verage,	maximu	m, and r	ninimu	n DC p	ower for	the sys	lem.	
Previou	is hour		DC -	Refresh												
	** T															-
	38	-					-									-
	32					-			-	-		-	-			-
(A)	28															-
vatt	24															-
r (v	29															-
We.	16															-
2	12															-
	-															-
	4															-
	0+															-
	23.5	4 11.17	11.19	11.22 11.2	11.27 11.	29 11.3	2 11.34	11.37	11,39	11-43	11.44	11.58	12:02	12.04	12:07	1
Dominio I.		5 D					rage	ager sears								
Poling	CONT VIA	5 Data Pi	Denes-													
Note: Ba	used or	the pollin	interva	and the tree	nd period sele	cted, if th	e total nur	mber of	data poi	nts retur	ned car	not be	clearly o	Sisplaye	d due to	1
settion	enis chi	ur, some o	nata poer	is may be on	used and the	se pend	ous peove	en mos	e aspaj	rea may	not ma	C) 218 (	,na55/5	pound	nierval	

# Kapitel 7. Features on Demand

Mit der Funktion "Features on Demand" (FoD) von IMM2 können Sie optionale Server- und Systemmanagementfunktionen installieren und verwalten.

Für Ihren Server gibt es mehrere Stufen von IMM2-Firmwarefunktionalitäten und -Funktionen. Die Stufen der auf Ihrem Server installierten IMM2-Firmwarefunktionen variieren je nach Hardwaretyp. Informationen dazu, welche Arten von IMM2-Hardware und -Funktionen in Ihrem Server installiert sind, finden Sie in der Dokumentation im Lieferumfang Ihres Servers.

Sie können die IMM2-Funktionen aktualisieren, indem Sie einen FoD-Aktivierungsschlüssel erwerben und installieren. Zusätzliche ausführliche Informationen zu FoD finden Sie im *Features on Demand User's Guide* unter http://www.ibm.com/ systems/x/fod/.

**Anmerkung:** Auf Servern mit IMM2-Grundstufenfunktionalität ist das IBM Integrated Management Module Standard Upgrade vor dem Installieren der Funktionalität des IBM Integrated Management Module Advanced Upgrade erforderlich.

Um einen FoD-Aktivierungsschlüssel anzufordern, kontaktieren Sie Ihren IBM Ansprechpartner oder Ihren IBM Geschäftspartner oder rufen Sie die folgende Seite auf: http://www.ibm.com/systems/x/fod/.

Verwenden Sie die IMM2-Webschnittstelle oder die IMM2-Befehlszeilenschnittstelle, um manuell einen FoD-Aktivierungsschlüssel zu installieren, mit dem Sie eine optionale Funktion verwenden können, die Sie erworben haben. Beachten Sie Folgendes, bevor Sie einen Schlüssel aktivieren:

- Der FoD-Aktivierungsschlüssel muss sich auf dem System befinden, das Sie verwenden, um sich am IMM2 anzumelden.
- Sie müssen die FoD-Option angefordert und deren Berechtigungscode per Post oder E-Mail erhalten haben.

Informationen zur Verwaltung eines FoD-Aktivierungsschlüssels mithilfe der IMM2-Webschnittstelle finden Sie unter "Aktivierungsschlüssel installieren", "Aktivierungsschlüssel entfernen" auf Seite 146 oder "Aktivierungsschlüssel exportieren" auf Seite 147. Informationen zur Verwaltung eines FoD-Aktivierungsschlüssels mithilfe der IMM2-Befehlszeilenschnittstelle finden Sie unter "Befehl "keycfg"" auf Seite 176.

#### Aktivierungsschlüssel installieren

Sie können einen FoD-Aktivierungsschlüssel installieren, um eine Zusatzfunktion zu Ihrem Server hinzuzufügen.

Gehen Sie wie folgt vor, um einen FoD-Aktivierungsschlüssel zu installieren:

- 1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt "Am IMM2 anmelden" auf Seite 10.
- Klicken Sie in der IMM2-Webschnittstelle auf die Registerkarte IMM Management (IMM-Verwaltung). Klicken Sie anschließend auf Activation Key Management (Aktivierungsschlüsselverwaltung).

				USERID	Settings	Log out	IBM.
anage	ement <del>+</del>	IMM Management <del>+</del>	Search				
	IMM Prop	perties	Various properties and IMM	settings related	d to the		
	Users		Create and modify user profiles that will have a	r accounts and ccess to the IM	group M console		
ope	Network		Network settings such a by the IMM	as SNMP and I	_DAP used	ins are	co-located o
	Security		Configure security prote SSH				
	IMM Con	figuration	View a summary of the settings.	current config	uration		
est O	Restart I	MM	Restart the IMM. Typica experiencing problems				
N	Reset IM	M to factory defaults	Sets all current configu default values				
	Activatio	on Key Management	Add and remove activa functionality				

**3**. Klicken Sie auf der Seite "Activation Key Management" auf **Add...** (Hinzufügen).

IBM Integrated Management Module II							
	System Status	Events 🗸	Service and Support $ extsf{v}$	Server			
Activ	vation Key ove and export ac Delete Exp Descriptor Type	y Mana ctivation keys port	agement s for additional functionalit ature Description	y.			

4. Klicken Sie im Fenster "Add Activation Key" (Aktivierungsschlüssel hinzufügen) auf Select File... (Datei auswählen). Wählen Sie nun die Aktivierungsschlüsseldatei aus, die Sie im Fenster "File Upload" (Hochladen von Datei) hinzufügen möchten, und klicken Sie auf Open, um die Datei hinzuzufügen, oder klicken Sie auf Cancel, um die Installation zu stoppen. Um das Hinzufügen des Schlüssels fertigzustellen, klicken Sie im Fenster "Add Activation Key" auf OK oder klicken Sie auf Cancel, um die Installation zu stoppen.



Das Fenster "Success" (Erfolg) gibt an, dass der Aktivierungsschlüssel installiert wurde.



#### Anmerkung:

• Wenn der Aktivierungsschlüssel nicht gültig ist, wird das folgende Fehlernachrichtenfenster angezeigt.



• Wenn Sie versuchen, den Aktivierungsschlüssel auf einem Maschinentyp zu installieren, der die FoD-Funktion nicht unterstützt, wird das folgende Fehlernachrichtenfenster angezeigt.

Error	х
Error Code:Invalid Machine Type in License key	
Close	

5. Klicken Sie auf **OK**, um das Fenster "Success" zu schließen.

Der ausgewählte Aktivierungsschlüssel wird zum Server hinzugefügt und erscheint auf der Seite "Activation Key Management".

Activa	Activation Key Management							
Add, remove	Add, remove and export activation keys for additional functionality.							
Add	Add Delete Export							
De	escriptor Type	Feature Description	Unique IDs	Constraints				
. 1		IBM Integrated Management Module Advanced Upgrade	791406KNKL9	No Constraints				

### Aktivierungsschlüssel entfernen

Sie können einen FoD-Aktivierungsschlüssel entfernen, um eine Zusatzfunktion auf Ihrem Server zu löschen.

Gehen Sie wie folgt vor, um einen FoD-Aktivierungsschlüssel zu entfernen:

- 1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt "Am IMM2 anmelden" auf Seite 10.
- Klicken Sie in der IMM2-Webschnittstelle auf die Registerkarte IMM Management (IMM-Verwaltung). Klicken Sie anschließend auf Activation Key Management (Aktivierungsschlüsselverwaltung).

			USERID	Settings	Log out	IBM.
ement 🗸	IMM Management <del>+</del>	Search				
IMM Prop	perties	Various properties and IMM	settings related	d to the		
Users		Create and modify use profiles that will have a	r accounts and ccess to the IM	group M console		
Network		Network settings such a by the IMM	as SNMP and I	LDAP used	ins are (	co-located o
Security		Configure security prot SSH				
IMM Con	figuration	View a summary of the settings.	current config	uration		
Restart I	MM	Restart the IMM. Typica experiencing problems				
Reset IM	M to factory defaults	Sets all current configu default values				
Activatio	n Key Managernent	Add and remove activa functionality	tion keys for a	ditional		
	ement 🗸 IMM Prop Users Network Security IMM Con Restart II Reset IM	IMM Management    IMM Properties   Users   Users   Network   Security   IMM Configuration   Restart IMM   Reset IMM to factory defaults   Activation Key Management	IMM Management <	IMM Management        Search         IMM Properties       Various properties and settings related IMM         Users       Create and modify user accounts and profiles that will have access to the IM         Network       Network settings such as SNMP and I by the IMM         Security       Configure security protocols such as SSH         IMM Configuration       View a summary of the current config settings.         Restart IMM       Restart the IMM. Typically only neede experiencing problems with the IMM         Reset IMM to factory defaults       Sets all current configuration settings default values         Activation Key Management       Add and remove activation keys for an functionality	USERID       Settings         ement -       IMM Management -       Search         IMM Properties       Various properties and settings related to the IMM         Users       Create and modify user accounts and group profiles that will have access to the IMM console         Network       Network settings such as SNMP and LDAP used by the IMM         Security       Configure security protocols such as SSL and SSH         IMM Configuration       View a summary of the current configuration settings.         Restart IMM       Restart the IMM. Typically only needed when experiencing problems with the IMM         Reset IMM to factory defaults       Sets all current configuration settings back to default values         Activation Key Management       Add and remove activation keys for additional functionality	USERID       Settings       Log out         ement < IMM Management < Search

3. Wählen Sie auf der Seite "Activation Key Management" den Aktivierungsschlüssel aus, den Sie entfernen möchten. Klicken Sie anschließend auf **Delete** (Löschen).

Activation Key Management Add, remove and export activation keys for additional functionality. Add Delete Export						
Descriptor Type 🔺	Feature Description	Unique IDs				
1	IBM Integrated Management Module Advanced Upgrade	791406KNKL9				

4. Klicken Sie im Fenster "Confirm Activation Key Deletion" (Löschen des Aktivierungsschlüssels bestätigen) auf **OK**, um das Löschen des Aktivierungsschlüssels zu bestätigen, oder klicken Sie auf **Cancel**, um die Schlüsseldatei zu behalten.



Der ausgewählte Aktivierungsschlüssel wird vom Server entfernt und nicht mehr auf der Seite "Activation Key Management" angezeigt.

IBM Integrated Management Module II							
System Status	Events 🗸	Service and Support $ extsf{-}$	Server				
ation Key re and export ac Delete Exp escriptor Type	y Mana ctivation keys port	agement s for additional functionality ature Description	у.				
	System Status Ation Key ve and export at Delete Exp escriptor Type	System Status Events - Ation Key Mana ve and export activation keys Delete Export escriptor Type - Fea	System Status Events - Service and Support - ation Key Management ve and export activation keys for additional functionality Delete Export escriptor Type - Feature Description				

# Aktivierungsschlüssel exportieren

Sie können einen FoD-Aktivierungsschlüssel exportieren, um eine Zusatzfunktion vom Server zu exportieren.

Gehen Sie wie folgt vor, um einen FoD-Aktivierungsschlüssel zu exportieren:

- 1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt "Am IMM2 anmelden" auf Seite 10.
- Klicken Sie in der IMM2-Webschnittstelle auf die Registerkarte IMM Management (IMM-Verwaltung). Klicken Sie anschließend auf Activation Key Management (Aktivierungsschlüsselverwaltung).

				USERID	Settings	Log out	IBM.
nage	ement 🗸	IMM Management 🗸	Search				
	IMM Prop	perties	Various properties and IMM	settings relate	d to the		
	Users		Create and modify user profiles that will have a	r accounts and ccess to the IM	group M console		
ope	Network		Network settings such a by the IMM	as SNMP and	LDAP used	ins are (	co-located or
	Security		Configure security prote SSH	ocols such as §	SSL and		
	IMM Con	figuration	View a summary of the settings.	current config	uration		
st O	Restart I	MM	Restart the IMM. Typica experiencing problems	ally only neede with the IMM	d when		
N	Reset IM	M to factory defaults	Sets all current configu default values	ration settings	back to		
	Activatio	n Key Management	Add and remove activa functionality	tion keys for a	Iditional		

**3**. Wählen Sie auf der Seite "Activation Key Management" den Aktivierungsschlüssel aus, den Sie exportieren möchten. Klicken Sie anschließend auf **Export** (Exportieren).

Activation Key Management Add, remove and export activation keys for additional functionality. Add Delete Expret					
Descriptor Type 🔺 Feature Description Unique IDs					
IBM Integrated Management Module Advanced     791406KNKL9					

- 4. Klicken Sie im Fenster "Confirm Activation Key Export" (Export des Aktivierungsschlüssels bestätigen) auf **OK**, um das Exportieren des Aktivierungsschlüssels zu bestätigen, oder klicken Sie auf **Cancel** (Abbrechen), um das Exportieren des Schlüssels abzubrechen.
- 5. Wählen Sie das Speicherverzeichnis für die Datei aus. Der ausgewählte Aktivierungsschlüssel wird vom Server exportiert.

# Kapitel 8. Befehlszeilenschnittstelle

Verwenden Sie die IMM2-Befehlszeilenschnittstelle (CLI) für den Zugriff auf das IMM2, ohne die Webschnittstelle verwenden zu müssen. Diese Schnittstelle stellt einen Teil der Managementfunktionen bereit, die von der Webschnittstelle bereitgestellt werden.

Sie können über eine Telnet- oder eine SSH-Sitzung auf die Befehlszeilenschnittstelle zugreifen. Bevor Sie CLI-Befehle absetzen können, müssen Sie durch das IMM2 authentifiziert werden.

# IMM2 mit IPMI verwalten

Anfangs ist beim IMM2 die Benutzer-ID 1 auf den Benutzernamen "USERID" und das Kennwort "PASSW0RD" (mit einer Null anstelle des Buchstabens "O") eingestellt. Dieser Benutzer hat Administratorzugriff.

Wichtig: Ändern Sie für größere Sicherheit diesen Benutzernamen und das zugehörige Kennwort bei der Erstkonfiguration.

Das IMM2 bietet außerdem die folgenden IPMI-Funktionen (Intelligent Peripheral Management Interface) zur Verwaltung ferner Server:

#### Befehlszeilenschnittstellen

Die Befehlszeilenschnittstelle gewährt durch das IPMI 2.0-Protokoll direkten Zugriff auf Serververwaltungsfunktionen. Sie können IPMItool verwenden, um Befehle zum Steuern der Stromversorgung am Server, zum Anzeigen von Serverinformationen und zum Identifizieren des Servers auszugeben. Weitere Informationen zu IPMItool finden Sie im Abschnitt "IPMItool verwenden".

#### Serial over LAN

Verwenden Sie zum Verwalten von Servern von einem fernen Standort aus IPMItool, um eine SOL-Verbindung (Serial over LAN) herzustellen. Weitere Informationen zu IPMItool finden Sie im Abschnitt "IPMItool verwenden".

#### **IPMItool verwenden**

IPMItool bietet diverse Tools, die Sie zum Verwalten und Konfigurieren eines IP-MI-Systems verwenden können. Sie können IPMItool intern oder extern verwenden, um das IMM2 zu verwalten und zu konfigurieren.

Gehen Sie für weitere Informationen zu IPMItool oder zum Herunterladen von IP-MItool auf http://sourceforge.net/.

### Zugriff auf die Befehlszeilenschnittstelle

Um auf die Befehlszeilenschnittstelle zuzugreifen, starten Sie eine Telnet- oder SSH-Sitzung mit der IP-Adresse des IMM2 (weitere Informationen hierzu finden Sie im Abschnitt "Seriell-zu-Telnet- oder -SSH-Umleitung konfigurieren" auf Seite 150).

#### Anmeldung an der Befehlszeilensitzung

Gehen Sie wie folgt vor, um sich an der Befehlszeile anzumelden:

- 1. Stellen Sie eine Verbindung mit dem IMM2 her.
- 2. Wenn Sie nach dem Benutzernamen gefragt werden, geben Sie die Benutzer-ID ein.
- **3.** Wenn Sie nach dem Kennwort gefragt werden, geben Sie das Kennwort ein, das Sie zur Anmeldung am IMM2 verwenden.

Sie werden an der Befehlszeile angemeldet. Die Befehlszeilenaufforderung lautet system>. Die Befehlszeilensitzung wird aufrechterhalten, bis Sie in der Befehlszeile exit (Verlassen) eingeben. Dann werden Sie abgemeldet und die Sitzung wird beendet.

#### Seriell-zu-Telnet- oder -SSH-Umleitung konfigurieren

Die Seriell-zu-Telnet- oder -SSH-Umleitung ermöglicht es einem Systemadministrator, das IMM2 als seriellen Terminal-Server zu verwenden. Auf einen seriellen Serveranschluss kann ein Zugriff von eine Telnet- oder SSH-Verbindung aus erfolgen, wenn die serielle Umleitung aktiviert ist.

#### Anmerkungen:

- Das IMM2 ermöglicht maximal zwei geöffnete Telnet-Sitzungen gleichzeitig. Über die beiden Telnet-Sitzungen kann unabhängig voneinander ein Zugriff auf die seriellen Anschlüsse erfolgen, sodass mehrere Benutzer einen umgeleiteten seriellen Anschluss gleichzeitig anzeigen können.
- 2. Mit dem Befehl **console 1** für die Befehlszeilenschnittstelle wird eine Sitzung für serielle Umleitung mit dem COM-Anschluss gestartet.

#### Beispielsitzung

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125... username: USERID (Press Enter.)
password: ******** (Press Enter.)
system> console 1 (Press Enter.)
```

Der gesamte Datenverkehr von COM2 wird nur zur Telnet-Sitzung umgeleitet. Der gesamte Datenverkehr von der Telnet- oder SSH-Sitzung wird zu COM2 umgeleitet.

ESC (

Geben Sie die Tastenkombination zum Beenden ein, um zur Befehlszeilenschnittstelle zurückzukehren. In diesem Beispiel drücken Sie die Taste "Esc" und geben dann eine linke Klammer ein. Die Eingabeaufforderung der Befehlszeilenschnittstelle erscheint und gibt an, dass Sie zur Befehlszeilenschnittstelle des IMM2 zurückgekehrt sind.

```
system>
```

#### Befehlssyntax

Lesen Sie die folgenden Richtlinien, bevor Sie die Befehle verwenden:

- Jeder Befehl weist das folgende Format auf: Befehl [Argumente] [-Optionen]
- In der Befehlssyntax muss die Groß-/Kleinschreibung beachtet werden.
- Der Befehlsname wird in Kleinbuchstaben angegeben.

- Alle Argumente müssen direkt auf den Befehl folgen. Die Optionen wiederum folgen direkt auf die Argumente.
- Vor jeder Option steht ein Bindestrich (-). Eine Option kann als Kurzoption (ein einzelner Buchstabe) oder als Langoption (mehrere Buchstaben) angegeben werden.
- Wenn eine Option ein Argument aufweist, ist dieses Argument obligatorisch. Beispiel:

ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0

Dabei ist **ifconfig** der Befehl, "eth0" ist ein Argument und "-i", "-g" und "-s" sind Optionen. In diesem Beispiel weisen alle drei Optionen Argumente auf.

• Eckige Klammern geben an, dass ein Argument oder eine Option optional ist. Dabei sind die eckigen Klammern nicht Teil des Befehls, den Sie eingeben.

#### Merkmale und Einschränkungen

Die Befehlszeilenschnittstelle weist folgende Merkmale und Einschränkungen auf:

 Mehrere gleichzeitige Befehlszeilenschnittstellensitzungen sind mit verschiedenen Zugriffsmethoden (Telnet oder SSH) zulässig. Es können höchstens zwei Telnet-Befehlszeilensitzungen gleichzeitig aktiv sein.

**Anmerkung:** Die Anzahl der Telnet-Sitzung ist konfigurierbar. Gültige Werte sind 0, 1 und 2. Der Wert 0 bedeutet, dass die Telnet-Schnittstelle inaktiviert ist.

- Es ist ein Befehl pro Zeile zulässig (maximal 160 Zeichen, einschließlich Leerzeichen).
- Für lange Befehle gibt es kein Fortsetzungszeichen. Die einzige Editierfunktion ist die Rückschritttaste, mit der Sie das zuvor eingegebene Zeichen löschen können.
- Sie können die Aufwärts- und die Abwärtspfeiltaste verwenden, um durch die letzten acht Befehle zu blättern. Mit dem Befehl **history** können Sie eine Liste der letzten acht Befehle anzeigen, die sie anschließend als Direktaufruf zum Ausführen eines Befehls verwenden können, wie im folgenden Beispiel dargestellt:

```
system> history
0 ifconfig eth0
1 readlog
2 readlog
3 readlog
4 history
system> !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-1 00:00:00:00:00:00
svstem>
```

- In der Befehlszeilenschnittstelle liegt der Ausgabepuffergrenzwert bei 2 KB. Es gibt keine Pufferung. Die Ausgabe eines einzelnen Befehls darf 2048 Zeichen nicht überschreiten. Dieser Grenzwert gilt nicht im Modus für serielle Umleitung (die Daten werden bei der seriellen Umleitung gepuffert).
- Die Ausgabe eines Befehls erscheint in der Anzeige, nachdem die Ausführung des Befehls beendet ist. Dadurch ist es für Befehle unmöglich, den Echtzeitaus-

führungsstatus zu melden. Beispiel: Im ausführlichen Modus des Befehls flashing wird der Vorgang des Blinkens nicht in Echtzeit angezeigt. Er wird erst angezeigt, nachdem die Befehlsausführung beendet ist.

• Der Befehlsausführungsstatus wird durch einfache Textnachrichten angegeben, wie im folgenden Beispiel dargestellt:

```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```

- In der Befehlssyntax muss die Groß-/Kleinschreibung beachtet werden.
- Zwischen einer Option und dem zugehörigen Argument muss mindestens ein Leerzeichen stehen. Im Beispiel ifconfig eth0 -i192.168.70.133 ist die Befehlssyntax falsch. Die richtige Syntax lautet ifconfig eth0 -i 192.168.70.133.
- Alle Befehle verfügen über die Optionen -h, -help und ?, mit denen Hilfe zur Syntax angezeigt werden kann. Alle der folgenden Beispiele haben dasselbe Ergebnis:

```
system> power -h
system> power -help
system> power ?
```

 Einige der Befehle, die in den folgenden Abschnitten beschrieben werden, sind möglicherweise für Ihre Systemkonfiguration nicht verfügbar. Um eine Liste der von Ihrer Konfiguration unterstützten Befehle anzuzeigen, verwenden Sie die Hilfsoption oder die Option "?", wie in den folgenden Beispielen dargestellt: system> help

```
system> ?
```

#### Alphabetische Befehlsliste

Die vollständige Liste aller Befehle der IMM2-Befehlszeilenschnittstelle in alphabetischer Reihenfolge lautet wie folgt:

- "Befehl "accseccfg"" auf Seite 163
- "Befehl "alertcfg"" auf Seite 165
- "Befehl "alertentries"" auf Seite 202
- "Befehl "asu"" auf Seite 166
- "Befehl "backup"" auf Seite 169
- "Befehl "batch"" auf Seite 205
- "Befehl "clearcfg"" auf Seite 206
- "Befehl "clearlog"" auf Seite 154
- "Befehl "clock"" auf Seite 206
- "Befehl "console"" auf Seite 162
- "Befehl "dhcpinfo"" auf Seite 170
- "Befehl "dns"" auf Seite 171
- "Befehl "ethtousb"" auf Seite 173
- "Befehl "exit"" auf Seite 154
- "Befehl "fans"" auf Seite 155
- "Befehl "ffdc"" auf Seite 155
- "Befehl "gprofile"" auf Seite 173
- "Befehl "help"" auf Seite 154
- "Befehl "history"" auf Seite 154

- "Befehl "identify"" auf Seite 207
- "Befehl "ifconfig"" auf Seite 174
- "Befehl "info"" auf Seite 207
- "Befehl "keycfg"" auf Seite 176
- "Befehl "ldap"" auf Seite 177
- "Befehl "led"" auf Seite 156
- "Befehl "ntp"" auf Seite 179
- "Befehl "passwordcfg"" auf Seite 180
- "Befehl "ports"" auf Seite 181
- "Befehl "portcfg"" auf Seite 182
- "Befehl "power"" auf Seite 161
- "Befehl "pxeboot"" auf Seite 162
- "Befehl "readlog"" auf Seite 158
- "Befehl "reset"" auf Seite 162
- "Befehl "resetsp"" auf Seite 208
- "Befehl "restore"" auf Seite 183
- "Befehl "restoredefaults"" auf Seite 184
- "Befehl "set"" auf Seite 184
- "Befehl "show"" auf Seite 159
- "Befehl "smtp"" auf Seite 184
- "Befehl "snmp"" auf Seite 185
- "Befehl "snmpalerts"" auf Seite 187
- "Befehl "spreset"" auf Seite 208
- "Befehl "srcfg"" auf Seite 189
- "Befehl "sshcfg"" auf Seite 190
- "Befehl "ssl"" auf Seite 191
- "Befehl "sslcfg"" auf Seite 192
- "Befehl "syshealth"" auf Seite 159
- "Befehl "telnetcfg"" auf Seite 195
- "Befehl "temps"" auf Seite 159
- "Befehl "thermal"" auf Seite 196
- "Befehl "timeouts"" auf Seite 196
- "Befehl "usbeth"" auf Seite 197
- "Befehl "users"" auf Seite 197
- "Befehl "volts"" auf Seite 160
- "Befehl "vpd"" auf Seite 160

#### Dienstprogrammbefehle

Folgende Dienstprogrammbefehle sind verfügbar:

- "Befehl "exit"" auf Seite 154
- "Befehl "help"" auf Seite 154
- "Befehl "history"" auf Seite 154

# Befehl "exit"

Mit dem Befehl **exit** können Sie sich abmelden und die Sitzung der Befehlszeilenschnittstelle beenden.

# Befehl "help"

Mit dem Befehl **help** können Sie eine Liste aller Befehle und eine Kurzbeschreibung zu den einzelnen Befehlen anzeigen. Sie können auch ? an der Eingabeaufforderung eingeben.

### **Befehl** "history"

Mit dem Befehl **history** können Sie eine indexierte Protokollliste der letzten acht Befehle anzeigen, die ausgegeben wurden. Die Indizes können dann als Direktaufrufe (mit davor stehendem !) verwendet werden, um die Befehle aus dieser Protokollliste erneut auszugeben.

#### Beispiel:

```
system> history
0 ifconfig eth0
1 readlog
2 readlog
3 readlog
4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-1 00:00:00:00:00:00
system>
```

# Überwachungsbefehle

Folgende Überwachungsbefehle sind verfügbar:

- "Befehl "clearlog""
- "Befehl "fans"" auf Seite 155
- "Befehl "ffdc"" auf Seite 155
- "Befehl "led"" auf Seite 156
- "Befehl "readlog"" auf Seite 158
- "Befehl "show"" auf Seite 159
- "Befehl "syshealth"" auf Seite 159
- "Befehl "temps"" auf Seite 159
- "Befehl "volts"" auf Seite 160
- "Befehl "vpd"" auf Seite 160

# Befehl "clearlog"

Mit dem Befehl **clearlog** können Sie das Ereignisprotokoll des IMM2 löschen. Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung zu Löschen von Ereignisprotokollen verfügen.

# Befehl "fans"

Mit dem Befehl **fans** können Sie die Geschwindigkeit der einzelnen Serverlüfter anzeigen.

Beispiel:

system> **fans** fan1 75% fan2 80% fan3 90% system>

### Befehl "ffdc"

Verwenden Sie den Befehl **ffdc** (first failure data capture, Erfassung von Fehlerdaten beim ersten Auftreten), um Servicedaten zu generieren und an den IBM Support zu übertragen.

Die folgende Liste enthält Befehle, die zusammen mit dem Befehl **ffdc** verwendet werden können:

- generate erstellt eine neue Servicedatendatei
- status überprüft den Status der Servicedatendatei
- copy kopiert die vorhandenen Servicedaten
- delete löscht die vorhandenen Servicedaten

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-t	Typennummer	1 (Prozessorspeicherauszug) und 4 (Servicedaten). Der Standardwert ist 1.
-f <sup>1</sup>	Name der fernen Datei oder des SFTP- Zielverzeichnisses.	Verwenden Sie für SFTP den vollständigen Pfad oder einen abschließenden Schrägstrich (/) für den Verzeichnisnamen (~/ oder /tmp/). Der Standardwert ist der vom System generierte Name.
ip 1	Adresse des TFTP/ SFTP-Servers.	
-pn <sup>1</sup>	Portnummer des TFTP/SFTP-Servers.	Der Standardwert ist 69/22.
-u <sup>1</sup>	Benutzername für den SFTP-Server.	
-pw <sup>1</sup>	Kennwort für den SFTP-Server.	
1. Zusätzl	iches Argument für die B	efehle <b>generate</b> und <b>copy</b>

Syntax:

ffdc [Optionen]
Option:
 -t 1 oder 4
 -f -ip IP-Adresse
 -pn Portnummer
 -u Benutzername
 -pw Kennwort

Beispiel:

system> ffdc generate Generating ffdc... system> ffdc status Type 1 ffdc: in progress system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/ Waiting for ffdc.... Copying ffdc... ok system> ffdc status Type 1 ffdc: completed 8737AC1\_DSY0123\_imm2\_120317-153327.tgz

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_imm2_120926-105320.tgz
system>
```

### Befehl "led"

Verwenden Sie den Befehl **led**, um den Zustand von Anzeigen anzuzeigen und festzulegen.

- Wird der Befehl **led** ohne Optionen ausgeführt, so wird der Status von Anzeigen im Bedienfeld angezeigt.
- Die Befehlsoption led -d muss gemeinsam mit der Befehlsoption led -identify on angewendet werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-1	Den Status aller Anzei- gen auf dem System und dessen Unterkomponenten abrufen	
-chklog	Anzeige für Prüfprotokoll aus- schalten	off
-identify	Zustand der Gehäusebestimmungs- anzeige ändern	off, on, blink
-d	Identifikationsanzeige für einen angegebenen Zeitraum einschalten	Zeitraum (Sekunden)

Syntax: led [Optionen] Option: -1 -chklog off -identify Zustand -d Zeit

Beispiel:			
system> led			
Fault	Off		
Identify	On Blue		
Chklog	Off		
Power	Off		
systems lad -1			
label	location	State	Color
Batterv	Planar	Off	
BMC Heartbeat	Planar	Blink	Green
BRD	Lightpath Card	Off	
Channel A	Planar	Off	
Channel B	Planar	Off	
Channel C	Planar	Off	
Channel D	Planar	Off	
Channel E	Planar	011	
	Front Panel	UTT	
	Lightpath Card	UTT Off	
	Dlanan	011 Off	
	Planar	0ff	
DASD	Lightpath Card	Off	
DIMM	Lightpath Card	Off	
DIMM 1	Planar	Off	
DIMM 10	Planar	Off	
DIMM 11	Planar	Off	
DIMM 12	Planar	Off	
DIMM 13	Planar	Off	
DIMM 14	Planar	Off	
DIMM 15	Planar	011	
DIMM 16	Planar	011	
	Planan	011 Off	
	Planan	011 Off	
DIMM 5	Planar	0ff	
DIMM 6	Planar	Off	
DIMM 7	Planar	Off	
DIMM 8	Planar	Off	
DIMM 9	Planar	Off	
FAN	Lightpath Card	Off	
FAN 1	Planar	Off	
FAN 2	Planar	011	
FAN 3	Planar	011	
Fault Idontify	Front Panel (+)	UTT On	Dluc
	Lightpath Card		Dine
LOG	Lightpath Card	Off	
NMI	Lightpath Card	Off	
OVER SPEC	Lightpath Card	Off	
PCI 1	FRŬ	Off	
PCI 2	FRU	Off	
PCI 3	FRU	Off	
PCI 4	FRU	Off	
Planar	Planar	Off	
Power	Front Panel (+)	011	
r5 DATD	Lightpath Card		
Riser 1	Planar	Off	
Riser 2	Planar	Off	
SAS ERR	FRU	Off	
SAS MISSING	Planar	Off	
SP	Lightpath Card	Off	
TEMP	Lightpath Card	Off	
VRM	Lightpath Card	Off	
system>			

### Befehl "readlog"

Mit dem Befehl **readlog** können Sie jeweils fünf IMM2-Ereignisprotokolleinträge anzeigen. Die Einträge werden in der Reihenfolge vom aktuellsten bis zum ältesten Eintrag angezeigt.

**readlog** zeigt die ersten fünf Einträge im Ereignisprotokoll an, angefangen mit dem aktuellsten Eintrag (bei seiner ersten Ausführung), und dann die nächsten fünf für jeden nachfolgenden Aufruf.

**readlog -a** zeigt alle Einträge im Ereignisprotokoll an, angefangen mit dem aktuellsten Eintrag.

**readlog -f** setzt den Zähler zurück und zeigt die ersten fünf Einträge im Ereignisprotokoll an, angefangen mit dem aktuellsten Eintrag.

**readlog -date** *date* zeigt Ereignisprotokolleinträge für das angegebene Datum im Format mm/tt/jj an. Es kann sich um eine Liste handeln, in der die einzelnen Datumsangaben durch ein Pipe-Zeichen (1) voneinander getrennt sind.

**readlog** -sev *severity* zeigt Ereignisprotokolleinträge des angegebenen Schweregrades an (E, W, I). Es kann sich um eine Liste handeln, in der die einzelnen Schweregrade durch ein Pipe-Zeichen (1) voneinander getrennt sind.

**readlog -i** *ip\_address* legt die IPv4- oder die IPv6-IP-Adresse des TFTP- oder SFTP-Servers fest, auf dem das Ereignisprotokoll gespeichert wird. Die Befehlsoptionen -i und -l werden gemeinsam verwendet, um den Standort anzugeben.

**readlog -1** *filename* legt den Dateinamen der Ereignisprotokolldatei fest. Die Befehlsoptionen -i und -1 werden gemeinsam verwendet, um den Standort anzugeben.

**readlog -pn** *port\_number* zeigt die Portnummer des TFTP- oder SFTP-Servers an oder legt sie fest (Standard: 69/22).

readlog -u username gibt den Benutzernamen für den SFTP-Server an.

readlog -pw password gibt das Kennwort für den SFTP-Server an.

#### Syntax:

```
readlog [Optionen]
Option:
   -a -f -date Datum
   -sev Schweregrad
   -i IP-Adresse
   -l Dateiname
   -pn Portnummer
   -u Benutzername
   -pw Kennwort
```

Beispiel:

```
system> readlog -f
1 I SERVPROC 12/18/03 10:18:58 Remote Login Successful.
Login ID:''USERID' CLI authenticated from 192.168.70.231 (Telnet).'
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.
Login ID: ''USERID' from web browser at IP@=192.168.70.231'
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
4 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
5 system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
```

```
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

#### Befehl "show"

Mit dem Befehl show können Sie einfache Einstellungen des IMM2 anzeigen.

- Mit dem Befehl show werden über den Befehl set festgelegte Werte angezeigt.
- Einstellungen sind wie in einer Verzeichnisbaumstruktur angeordnet. Verwenden Sie die Befehlsoption **show -r**, um die vollständige Verzeichnisstruktur anzuzeigen.
- Manche dieser Einstellungen, etwa Umgebungsvariablen, werden vom CLI verwendet.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
value	Anzuzeigender Pfadwert oder Einstellungswert	
-r	Einstellungen rekursiv anzeigen	

Syntax:

```
show [Optionen]
Option:
value
-r
```

### Befehl "syshealth"

Mit dem Befehl **syshealth** können Sie eine Zusammenfassung des Serverzustands anzeigen. Es werden der Stromversorgungsstatus, der Systemstatus, der Zähler für den Neustart und der Status der IMM2-Software angezeigt.

Beispiel:

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

### Befehl "temps"

Mit dem Befehl **temps** können Sie alle Temperaturwerte und Temperaturschwellenwerte anzeigen. Dieselben Temperaturwerte werden auch in der Webschnittstelle angezeigt.

Beispiel: system> temps Temperatures are displayed in degrees Fahrenheit/Celsius WR W T SS HS ------CPU1 65/18 72/22 80/27 85/29 90/32

CPU2	58/14	72/22	80/27	85/29	90/32
DASD1	66/19	73/23	82/28	88/31	92/33
Amb	59/15	70/21	83/28	90/32	95/35
system	>				

#### Anmerkungen:

1. Die Ausgabe weist die folgenden Spaltenüberschriften auf:

WR: Warnungzurücksetzung

W: Warnung

T: Temperatur (aktueller Wert)

SS: Normaler Systemabschluss

- HS: Erzwungener Systemabschluss
- 2. Alle Temperaturwerte sind in Grad Fahrenheit/Grad Celsius angegeben.

#### Befehl "volts"

Mit dem Befehl **volts** können Sie alle Spannungswerte und Spannungsschwellenwerte anzeigen. Dieselben Spannungswerte werden auch in der Webschnittstelle angezeigt.

#### Beispiel:

system	VOI	15							
	HSL	SSL	WL	WRL	V	WRH	WH	SSH	HSH
5v 3.3v 12v -5v -3.3v VRM1 VRM2	5.02 3.35 12.25 -5.10 -3.35	4.00 2.80 11.10 -5.85 -4.10	4.15 2.95 11.30 -5.65 -3.95	4.50 3.05 11.50 -5.40 -3.65	4.60 3.10 11.85 -5.20 -3.50 3.45 5.45	5.25 3.50 12.15 -4.85 -3.10	5.50 3.65 12.25 -4.65 -2.95	5.75 3.70 12.40 -4.40 -2.80	6.00 3.85 12.65 -4.20 -2.70
5,5000									

Anmerkung: Die Ausgabe weist die folgenden Spaltenüberschriften auf:

HSL: Erzwungener Systemabschluss (Unterspannung)

SSL: Normaler Systemabschluss (Unterspannung)

WL: Warnung (Unterspannung)

WRL: Warnungszurücksetzung (Unterspannung)

V: Spannung (aktueller Wert)

WRH: Warnungszurücksetzung (Überspannung)

WH: Warnung (Überspannung)

SSH: Normaler Systemabschluss (Überspannung)

HSH: Erzwungener Systemabschluss (Überspannung)

# Befehl "vpd"

Mit dem Befehl **vpd** können Sie elementare Produktdaten für das System (sys), das IMM2 (imm), das Server-BIOS (uefi), Dynamic System Analysis Preboot des Servers (dsa), die Server-Firmware (fw) und die Serverkomponenten (comp) anzeigen. Dieselben Informationen werden auch in der Webschnittstelle angezeigt.

Syntax:

vpd [Optionen]
Option:
 -sys

-imm -uefi -dsa -fw -comp

Verwenden Sie den Befehl "vpd", um elementare Produktdaten für verschiedene Komponenten des Servers anzuzeigen.

Option	Beschreibung		
-sys	zeigt elementare Produktdaten für das System an		
-imm	zeigt elementare Produktdaten für den IMM2-Controller an		
-uefi	zeigt elementare Produktdaten für das BIOS an		
-dsa	zeigt elementare Produktdaten für die Diagnose an		
-fw	zeigt elementare Produktdaten für die Systemfirmware an		
-comp	zeigt elementare Produktdaten für die Systemkomponenten an		

```
Beispiel:
```

system> Type	<b>vpd -dsa</b> Version	Build	ReleaseDate
DSA system>	9,25	DSYTA5A	2012/07/31

### Steuerbefehle für Serverstromversorgung und -neustart

Folgende Befehle für Serverstromversorgung und -neustart sind verfügbar:

- "Befehl "power""
- "Befehl "pxeboot"" auf Seite 162
- "Befehl "reset"" auf Seite 162

## Befehl "power"

Mit dem Befehl **power** können Sie die Stromversorgung des Servers steuern. Um die Befehle vom Typ **power** ausgeben zu können, müssen Sie über eine Zugriffsberechtigung für Stromversorgung und Neustarts verfügen.

power on - Die Serverstromversorgung wird eingeschaltet.

**power off** - Die Serverstromversorgung wird ausgeschaltet. Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.

**power state** - Zeigt den Serverstromversorgungszustand (on oder off) und den aktuellen Zustand des Servers an.

**power cycle** - Schaltet die Serverstromversorgung zunächst aus und dann wieder ein. Mit der Option -s wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.

Syntax:

```
power on
power off [-s]
power state
power cycle [-s]
```

## Befehl "pxeboot"

Mit dem Befehl **pxeboot** können Sie die Bedingung für die Ausführungsumgebung vor dem Starten (Preboot eXecution Environment - PXE) anzeigen und einstellen.

Wird **pxeboot** ohne Optionen ausgeführt, so wird auf die aktuelle PXE-Einstellung zurückgegriffen. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-en	Legt die PXE-Bedin- gung für den nächsten Systemwiederanlauf fest	enabled, disabled

Syntax:

```
pxeboot [Optionen]
Option:
    -en Zustand
```

Beispiel:

system> pxeboot
-en disabled
system>

#### Befehl "reset"

Mit dem Befehl **reset** können Sie den Server erneut starten. Um diesen Befehl ausgeben zu können, müssen Sie über eine Zugriffsberechtigung für Stromversorgung und Neustarts verfügen. Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server erneut gestartet wird.

Syntax: reset [Option] Option: -s

#### Befehl zur seriellen Umleitung

Es gibt einen Befehl zur seriellen Umleitung: den "Befehl "console"".

#### Befehl "console"

Mit dem Befehl **console** können Sie eine Konsolensitzung mit serieller Umleitung zum designierten seriellen Anschluss des IMM2 starten.

Syntax:

console 1

### Konfigurationsbefehle

Folgende Konfigurationsbefehle sind verfügbar:

- "Befehl "accseccfg"" auf Seite 163
- "Befehl "alertcfg"" auf Seite 165
- "Befehl "asu"" auf Seite 166
- "Befehl "backup"" auf Seite 169

- "Befehl "dhcpinfo"" auf Seite 170
- "Befehl "dns"" auf Seite 171
- "Befehl "ethtousb"" auf Seite 173
- "Befehl "gprofile"" auf Seite 173
- "Befehl "ifconfig"" auf Seite 174
- "Befehl "keycfg"" auf Seite 176
- "Befehl "ldap"" auf Seite 177
- "Befehl "ntp"" auf Seite 179
- "Befehl "passwordcfg"" auf Seite 180
- "Befehl "ports"" auf Seite 181
- "Befehl "portcfg"" auf Seite 182
- "Befehl "restore"" auf Seite 183
- "Befehl "restoredefaults"" auf Seite 184
- "Befehl "set"" auf Seite 184
- "Befehl "smtp"" auf Seite 184
- "Befehl "snmp"" auf Seite 185
- "Befehl "snmpalerts"" auf Seite 187
- "Befehl "srcfg"" auf Seite 189
- "Befehl "sshcfg"" auf Seite 190
- "Befehl "ssl"" auf Seite 191
- "Befehl "sslcfg"" auf Seite 192
- "Befehl "telnetcfg"" auf Seite 195
- "Befehl "thermal"" auf Seite 196
- "Befehl "timeouts"" auf Seite 196
- "Befehl "usbeth"" auf Seite 197
- "Befehl "users"" auf Seite 197

# Befehl "accseccfg"

Mit dem Befehl **accseccfg** können Sie Kontosicherheitseinstellungen anzeigen und konfigurieren.

Wird der Befehl **accseccfg** ohne Optionen ausgeführt, so werden alle Informationen zur Kontensicherheit angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-legacy	Legt für die Accountsicherheit eine vordefinierte Gruppe von traditionellen Standardwerten fest.	
-high	Legt für die Accountsicherheit eine vordefinierte Gruppe von hohen Standardwerten fest.	
-custom	Stellt Kontosicherheit auf benutzerdefinierte Werte ein	

Option	Beschreibung	Werte
-am	Legt Benutzerauthen- tifizierungsverfahren fest	local, ldap, localldap, ldaplocal
-lp	Aussperrungszeit nach erreichter Höchstzahl an Anmeldefehlern (Minuten)	0, 1, 2, 5, 10, 15, 20, 30, 60, 120, 180 oder 240 Minuten. Der Standardwert beträgt 60, wenn "High Security" (hohes Sicherheitsniveau) aktiviert ist, und 2, wenn "Legacy Security" (traditionelle Sicherheit) aktiviert ist. Bei einem Wert von 0 wird diese Funktion inaktiviert.
-pe	Zeitraum bis Verfalls- datum des Kennworts (Tage)	0 bis 365 Tage
-pr	Kennwort erforderlich	on, off
-pc	Regeln zur Kennwortkomplexität	on, off
-pd	Mindestanzahl unter- schiedlicher Zeichen für ein Kennwort	0 bis 19 Zeichen
-pl	Kennwortlänge	1 bis 20 Zeichen
-ci	Mindestintervall für Kennwortänderung (Stunden)	0 bis 240 Stunden
-lf	Maximale Anzahl an Anmeldefehlern	0 bis 10
-chgdft	Standardkennwort nach erster Anmel- dung ändern	on, off
-chgnew	Neues Benutzerkennwort nach erster Anmel- dung ändern	on, off
-rc	Wiederverwendungs- zyklus für Kennwort	0 bis 5
-wt	Sitzungszeitlimit bei Webinaktivität (Minu- ten)	1, 5, 10, 15, 20, keine Angabe oder 'user'

Syntax:

accseccfg [Optionen] Option: -legacy -high -custom -am Authentifizierungsmethode -lp Lockout-Zeitraum -pe Zeitraum -pr Zustand -pc Zustand -pd Anzahl an Zeichen -pl Anzahl an Zeichen -ci Mindestintervall -lf Anzahl an Fehlern

```
-chgdft Zustand
  -chgnew Zustand
  -rc Wiederverwendungszyklus
  -wt Zeitlimit
Beispiel:
system> accseccfg
-legacy
-am local
-1p 2
-pe 0
-pr off
-pd 1
-p1 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

# Befehl "alertcfg"

Mit dem Befehl **alertcfg** können Sie die Parameter für allgemeine ferne Alerts des IMM2 anzeigen und konfigurieren.

Wird der Befehl **alertcfg** ohne Optionen ausgeführt, so werden alle Parameter für allgemeine ferne Alerts angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-dr	Legt fest, wie viel Zeit zwischen Wieder- holungsversuchen lie- gen soll, bevor das IMM2 erneut einen Alert sendet	Minutenangaben von "0" bis "4.0" (für 4,0 Minuten), in Inkrementen von einer halben Minute
-da	Legt fest, wie viel Zeit vergehen soll, bevor das IMM2 einen Alert an den nächsten Emp- fänger auf der Liste sendet	Minutenangaben von "0" bis "4.0" (für 4,0 Minuten), in Inkrementen von einer halben Minute
-rl	Legt fest, wie oft das IMM2 zusätzlich ver- sucht, einen Alert zu senden, wenn vorheri- ge Versuche nicht er- folgreich waren	0 bis 8

Syntax:

alertcfg [Optionen] Optionen: -rl Begrenzung\_für\_Neuversuche

- -dr Verzögerung\_vor\_Neuversuch
- -da Agentenverzögerung

Beispiel:

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

# Befehl "asu"

Befehle des Dienstprogramms für erweiterte Einstellungen werden verwendet, um UEFI-Einstellungen festzulegen. Das Hostsystem muss erneut gestartet werden, damit Änderungen an UEFI-Einstellungen wirksam werden.

Die folgende Tabelle enthält eine Untermenge von Befehlen, die zusammen mit dem Befehl **asu** verwendet werden können.

Befehl	Beschreibung	Wert
delete	Verwenden Sie diesen Befehl, um eine Instanz oder einen Datensatz einer Einstellung zu löschen. Bei der Einstel- lung muss es sich um eine Instanz handeln, für die das Löschen zulässig ist, z. B. "iSCSI.AttemptName.1".	Einstellung_Instanz
help	Verwenden Sie diesen Befehl, um Hilfetext zu einer oder mehreren Einstellungen an- zuzeigen.	Einstellung
set	<ul> <li>Verwenden Sie diesen Befehl, um den Wert einer Einstel- lung zu ändern. Legen Sie als UEFI-Einstellung den Eingabewert fest.</li> <li>Anmerkungen:</li> <li>Legen Sie ein oder mehre- re Paare aus Einstellung und Wert fest.</li> </ul>	Einstellung Wert
	<ul> <li>Die Einstellung kann Platzhalterzeichen enthal- ten, wenn sie für eine ein- zelne Einstellung gilt.</li> <li>Der Wert muss in Anfüh- rungszeichen gesetzt wer-</li> </ul>	
	den, wenn er Leerzeichen enthält.	
	Sortierlistenwerte werden durch das Gleichheitszei- chen (=) getrennt. Beispiel: set B*.Bootorder "CD/ DVD Rom=Hard Disk 0=PXE Network."	

Tabelle 7. ASU-Befehle

Befehl	Beschreibung	Wert
showgroups	Verwenden Sie diesen Befehl, um die verfügbaren Einstellungsgruppen anzu- zeigen. Dieser Befehl zeigt die Namen der bekannten Gruppen an. Gruppennamen können je nach den installier- ten Einheiten variieren.	Einstellung
show	Verwenden Sie diesen Befehl, um den aktuellen Wert einer oder mehrerer Einstellungen anzuzeigen.	Einstellung
showvalues	<ul> <li>Verwenden Sie diesen Befehl, um alle möglichen Werte für eine oder mehrere Einstellun- gen anzuzeigen.</li> <li>Anmerkungen:</li> <li>Dieser Befehl zeigt Infor- mationen zu den zulässi- gen Werten für die Einstellung an.</li> <li>Die minimale und maxi- male Anzahl der für diese Einstellung zulässigen Ins- tanzen werden angezeigt.</li> <li>Der Standardwert wird angezeigt, falls er verfüg- bar ist.</li> <li>Der Standardwert steht zwischen einer öffnenden und einer schließenden spitzen Klammer (&lt; und &gt;).</li> <li>Die Textwerte zeigen die minimale und die maxima- le Länge sowie den regulä- ren Ausdruck.</li> </ul>	Einstellung

Tabelle 7. ASU-Befehle (Forts.)

#### Anmerkungen:

- In der Befehlssyntax ist *Einstellung* der Name einer Einstellung, die Sie anzeigen oder ändern möchten, und *Wert* ist der Wert, den Sie für die Einstellung festlegen.
- Für *Einstellung* können mehrere Werte angegeben werden, außer bei Verwendung des Befehls **set**.
- Der Wert für *Einstellung* kann Platzhalterzeichen enthalten, z. B. einen Stern (\*) oder ein Fragezeichen (?).

• Bei *Einstellung* kann es sich um eine Gruppe, einen Einstellungsnamen oder den Wert **all** (alles) handeln.

In der folgenden Liste sind einige Beispiele für die Befehlssyntax für den Befehl **asu** dargestellt:

• Um alle Befehlsoptionen für den Befehl "asu" anzuzeigen, geben Sie asu --help ein.

- Um die ausführliche Hilfe für alle Befehle anzuzeigen, geben Sie asu -v --help ein.
- Um die ausführliche Hilfe zu einem Befehl anzuzeigen, geben Sie asu -v set --help ein.
- Um einen Wert zu ändern, geben Sie asu set Wert der Einstellung ein.
- Um den aktuellen Wert anzuzeigen, geben Sie asu show Einstellung ein.
- Um Einstellungen im Langformat anzuzeigen, geben Sie asu show -1 -b all ein.
- Um alle möglichen Werte für eine Einstellung anzuzeigen, geben Sie asu showvalues *Einstellung* an.

Beispiel für den Befehl show values:

```
system> asu showvalues S*.POST*
```

```
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
```

SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-b <sup>1</sup>	Im Batchformat anzeigen.	
help <sup>3</sup>	Befehlssyntax und -optio- nen anzeigen. Die Option "help" wird vor den Be- fehl gesetzt, wie z. B. <b>asu</b> <b>help show</b> .	
help <sup>3</sup>	Hilfe zum Befehl anzeigen. Die Option "help" wird hinter den Befehl gesetzt, z. B. <b>asu showhelp</b> .	
-11	Name der Einstellung im Langformat (Konfigurationsgruppe ein- schließen).	
-m <sup>1</sup>	Name der Einstellung im Mischformat (Konfigurations-ID verwen- den).	
-v <sup>2</sup>	Ausführliche Ausgabe.	
1 Die Optionen !	' h" " 1" und " m" worden nur	zusamman mit dam Bafahl aharu yaruan

1. Die Optionen "-b", "-l" und "-m" werden nur zusammen mit dem Befehl **show** verwendet.

2. Die Option "-v" wird nur zwischen asu und dem Befehl verwendet.

3. Die Option "--help" kann zusammen mit jedem Befehl verwendet werden.

Syntax:

```
asu [Optionen] command
[cmd-Optionen]
Optionen:
    -v ausführliche Ausgabe
    --help Haupthilfetext anzeigen
cmd-Optionen:
    --help Hilfe zum Befehl
```

Anmerkung: Weitere Befehlsoptionen finden Sie bei den einzelnen Befehlen.

Verwenden Sie die asu-Transaktionsbefehle, um mehrere UEFI-Einstellungen festzulegen und um Batchmodusbefehle zu erstellen und auszuführen. Verwenden Sie die Befehle **tropen** und **trset**, um eine Transaktionsdatei, die mehrere Einstellungen enthält, anzuwenden. Eine Transaktion mit einer angegebenen ID wird mit dem Befehl **tropen** geöffnet. Einstellungen werden mithilfe des Befehls **trset** zur Gruppe hinzugefügt. Die abgeschlossene Transaktion wird mithilfe des Befehls **trcommit** festgeschrieben. Wenn Sie mit der Transaktion fertig sind, kann diese mithilfe des Befehls **trrm** gelöscht werden.

**Anmerkung:** Die Operation zum Wiederherstellen der UEFI-Einstellungen erstellt eine Transaktion mit einer ID unter Verwendung einer willkürlichen dreistelligen Zahl.

Die folgende Tabelle enthält Transaktionsbefehle, die zusammen mit dem Befehl **asu** verwendet werden können.

Befehl	Beschreibung	Wert
tropen ID	Dieser Befehl erstellt eine neue Transaktionsdatei mit mehreren festzulegenden Einstellungen.	<i>ID</i> ist die ID- Zeichenfolge aus 1-3 al- phanumerischen Zeichen.
trset ID	Dieser Befehl fügt eine oder mehrere Einstellungen oder Wertepaare zu einer Transaktion hinzu.	<i>ID</i> ist die ID- Zeichenfolge aus 1-3 al- phanumerischen Zeichen.
trlist ID	Dieser Befehl zeigt zuerst die Inhalte der Transaktionsdatei an. Dies kann hilfreich sein, wenn die Transaktionsdatei in der CLI-Shell erstellt wird.	<i>ID</i> ist die ID- Zeichenfolge aus 1-3 al- phanumerischen Zeichen.
trcommit ID	Dieser Befehl schreibt die Inhalte der Transaktionsdatei fest und führt sie aus. Die Ergeb- nisse der Ausführung sowie eventuelle Fehler wer- den angezeigt.	<i>ID</i> ist die ID- Zeichenfolge aus 1-3 al- phanumerischen Zeichen.
trrm ID	Dieser Befehl entfernt die Transaktionsdatei, nach- dem sie festgeschrieben wurde.	<i>ID</i> ist die ID- Zeichenfolge aus 1-3 al- phanumerischen Zeichen.

Tabelle 8. Transaktionsbefehle

Beispiel für das Erstellen mehrerer UEFI-Einstellungen:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

### Befehl "backup"

Mit dem Befehl **backup** können Sie eine Sicherungsdatei mit den aktuellen Systemsicherheitseinstellungen erstellen.

Option	Beschreibung	Werte
-f	Name der Sicherungsdatei	Gültiger Dateiname
-рр	Kennwort oder Verschlüsselungstext, mithilfe dessen Kenn- wörter innerhalb der Sicherungsdatei ver- schlüsselt sind	Gültiges Passwort oder durch Anführungszeichen be- grenzter Verschlüsselungstext
-ip	IP-Adresse des TFTP-/ SFTP-Servers	Gültige IP-Adresse
-pn	Portnummer des TFTP-/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP- Server	Gültiges Kennwort
-fd	Dateiname für die XML-Beschreibung von CLI- Sicherungsbefehlen	Gültiger Dateiname

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

#### Syntax:

```
backup [Optionen]
Option:
    -f Dateiname
    -pp Kennwort
    -ip IP-Adresse
    -pn Portnummer
    -u Benutzername
    -pw Kennwort
    -fd Dateiname
```

#### Beispiel:

```
system> backup -f imm-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

# Befehl "dhcpinfo"

Mit dem Befehl **dhcpinfo** können Sie die durch den DHCP-Server zugeordnete IP-Konfiguration für eth0 anzeigen, wenn die Schnittstelle automatisch durch einen DHCP-Server konfiguriert wird. Mit dem Befehl **ifconfig** können Sie DHCP aktivieren oder inaktivieren.

Syntax: dhcpinfo eth0

Beispiel:

system> dhcpinfo eth0

```
-server : 192.168.70.29
-n : IMM2A-00096B9E003A
-i : 192.168.70.202
```
```
: 192.168.70.29
-g
- S
      : 255.255.255.0
-d
       : linux-sp.raleigh.ibm.com
-dns1 : 192.168.70.29
-dns2 : 0.0.0.0
-dns3 : 0.0.0.0
-i6
     : 0::0
-d6
      : *
-dns61 : 0::0
-dns62 : 0::0
-dns63 : 0::0
system>
```

In der folgenden Tabelle wird die Ausgabe dieses Beispiels beschrieben.

Option	Beschreibung
-server	DHCP-Server, der die Konfiguration zugeordnet hat
-n	Zugeordneter Hostname
-i	Zugeordnete IPv4-Adresse
-g	Zugeordnete Gateway-Adresse
-s	Zugeordnete Teilnetzmaske
-d	Zugeordneter Domänenname
-dns1	Primäre IP-Adresse des IPv4-DNS-Servers
-dns2	Sekundäre IPv4-DNS-IP-Adresse
-dns3	Tertiäre IP-Adresse des IPv4-DNS-Servers
-i6	IPv6-Adresse
-d6	IPv6-Domänenname
-dns61	Primäre IP-Adresse des IPv6-DNS-Servers
-dns62	Sekundäre IPv6-DNS-IP-Adresse
-dns63	Tertiäre IP-Adresse des IPv6-DNS-Servers

### Befehl "dns"

Mit dem Befehl **dns** können Sie die DNS-Konfiguration des IMM2 anzeigen und einstellen.

Wird der Befehl **dns** ohne Optionen ausgeführt, so werden alle Informationen zur DNS-Konfiguration angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-state	DNS-Zustand	on, off
-ddns	DDNS-Zustand	enabled, disabled
-i1	Primäre IP-Adresse des IPv4-DNS-Servers	IP-Adresse im IP-Adressformat mit Trennzeichen.
-i2	Sekundäre IPv4-DNS- IP-Adresse	IP-Adresse im IP-Adressformat mit Trennzeichen.
-i3	Tertiäre IP-Adresse des IPv4-DNS-Servers	IP-Adresse im IP-Adressformat mit Trennzeichen.
-i61	Primäre IP-Adresse des IPv6-DNS-Servers	IP-Adresse im IPv6-Format.

Option	Beschreibung	Werte
-i62	Sekundäre IPv6-DNS- IP-Adresse	IP-Adresse im IPv6-Format.
-i63	Tertiäre IP-Adresse des IPv6-DNS-Servers	IP-Adresse im IPv6-Format.
-p	IPv4-/IPv6-Priorität	ipv4, ipv6

dns [Optionen]
Option:
 -state Zustand
 -i1 Erste\_IPv4-IP-Adresse
 -i2 Zweite\_IPv4-IP-Adresse
 -i3 Dritte\_IPv4-IP-Adresse
 -i61 Erste\_IPv6-IP-Adresse
 -i62 Zweite\_IPv6-IP-Adresse
 -i63 Dritte\_IPv6-IP-Adresse
 -p Priorität

**Anmerkung:** Im folgenden Beispiel ist eine IMM2-Konfiguration mit aktiviertem DNS dargestellt.

#### Beispiel:

```
system> dns
-state : enabled
     : 192.168.70.202
-i1
-i2
       : 192.168.70.208
-i3
       : 192.168.70.212
-i61
     : fe80::21a:64ff:fee6:4d5
-i62
     : fe80::21a:64ff:fee6:4d6
-i63
       : fe80::21a:64ff:fee6:4d7
-ddns : enabled
-ddn
       : ibm.com
-ddncur : ibm.com
-dnsrc : dhcp
      : ipv6
-p
```

system>

In der folgenden Tabelle wird die Ausgabe dieses Beispiels beschrieben.

Option	Beschreibung
-state	Zustand des DNS (on oder off)
-i1	Primäre IP-Adresse des IPv4-DNS-Servers
-i2	Sekundäre IPv4-DNS-IP-Adresse
-i3	Tertiäre IP-Adresse des IPv4-DNS-Servers
-i61	Primäre IP-Adresse des IPv6-DNS-Servers
-i62	Sekundäre IPv6-DNS-IP-Adresse
-i63	Tertiäre IP-Adresse des IPv6-DNS-Servers
-ddns	Zustand des DDNS (enabled oder disabled)
-dnsrc	Bevorzugter DDNS-Domänenname (dhcp oder manual)
-ddn	Manuell angegebenes DDN
-ddncur	Aktuelles DDN (Lesezugriff)

Option	Beschreibung
-р	Bevorzugte DNS-Server (ipv4 oder ipv6)

# Befehl "ethtousb"

Mit dem Befehl **ethtousb** können Sie die Portzuordnung für Ethernet zu Ethernet over USB anzeigen und konfigurieren.

Mit diesem Befehl können Sie für Ethernet over USB eine externe Ethernet-Portnummer einer anderen Portnummer zuordnen.

Wird der Befehl **ethtousb** ohne Optionen ausgeführt, so werden Informationen zu Ethernet über USB angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-en	Zustand von Ethernet über USB	enabled, disabled
-mx	Portzuordnung für Index <i>x</i> konfigurieren	Durch einen Doppelpunkt (:) getrenntes Portpaar in der Form <i>port1:port2</i>
		<ul> <li>die Portindexnummer <i>x</i> wird in der Befehlsoption als Ganzzahl zwischen 1 und 10 angegeben.</li> </ul>
		• Bei <i>port1</i> des Portpaares handelt es sich um die ex- terne Ethernet-Portnummer.
		<ul> <li>Bei <i>port2</i> des Portpaares handelt es sich um die Ethernet-over-USB-Portnummer.</li> </ul>
-rm	Portzuordnung für angegebenen Index	1 bis 10
entfern	entfernen	Über den Befehl <b>ethtousb</b> ohne Optionen werden Portzuordnungsindizes angezeigt.

Syntax:

ethtousb [Optionen] Option: -en Zustand -mx Portpaar -rm Zuordnungsindex

Beispiel:

```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
  -en enabled
  -m1 100:200
  -m2 101:201
system> ethtousb -rm 1
system>
```

# Befehl "gprofile"

Mit dem Befehl **gprofile** können Sie Gruppenprofile für das IMM2 anzeigen und konfigurieren.

Option	Beschreibung	Werte
-clear	Löscht eine Gruppe	enabled, disabled
-n	Der Name der Gruppe	Zeichenfolge mit bis zu 63 Zeichen für <i>Gruppenname</i> . Der <i>Gruppenname</i> muss ein- deutig sein.
-a	Rollenbasierte Berechtigungsstufe	supervisor, operator, rbs <rollenliste>: nsc   am   rca   rcvma   pr   bc   cel   ac Die Rollenlistenwerte werden in einer Lis- te, in der die einzelnen Werte durch Pipe- Zeichen voneinander getrennt sind, angegeben.</rollenliste>
-h	Zeigt die Befehlssyntax und die Optionen an	

```
gprofile [1 - 16
Bereichsnummer_des_Gruppenprofils] [options]
Optionen:
-clear Status
-n Gruppenname
-a Berechtigungsebene:
    -nsc Netzbetrieb und Sicherheit
    -am Benutzerkontenverwaltung
    -rca Zugriff auf ferne Konsole
    -rcvma Zugriff auf ferne Konsole und fernen Datenträger
    -pr Zugriff auf ferne Konsole und fernen Datenträger
    -pr Zugriff auf Einschalten/Neustart eines fernen Servers
    -bc Allgemeine Adapterkonfiguration
    -cel Fähigkeit zum Löschen von Ereignisprotokollen
    -ac Erweiterte Adapterkonfiguration
```

## Befehl "ifconfig"

Mit dem Befehl **ifconfig** können Sie die Ethernet-Schnittstelle konfigurieren. Geben Sie ifconfig eth0 ein, um die aktuelle Ethernet-Schnittstellenkonfiguration anzuzeigen. Um die Konfiguration der Ethernet-Schnittstelle zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Schnittstellenkonfiguration ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

Option	Beschreibung	Werte
-state	Schnittstellenstatus	disabled, enabled
-C	Konfigurationsmethode	dhcp, static, dthens ("dthens" entspricht der Option <b>Try dhcp server, if it fails</b> <b>use static config</b> (Nach DHCP-Server suchen. Falls das fehlschlägt, statische Konfiguration verwenden) in der Webschnittstelle)
-i	Statische IP-Adresse	Adresse im gültigen Format
-g	Gateway-Adresse	Adresse im gültigen Format
-s	Teilnetzmaske	Adresse im gültigen Format

Option	Beschreibung	Werte
-n	Hostname	Zeichenfolge von bis zu 63 Zeichen. Die Zeichenfolge kann Buchstaben, Ziffern, Punkte, Unterstriche und Bindestriche enthalten.
-r	Übertragungs- geschwindigkeit	10, 100, auto
-d	Duplexmodus	full, half, auto
-m	MTU	Numerisch zwischen 60 und 1500
-1	LAA	MAC-Adressenformat. Multicastadressen sind nicht zulässig (das erste Byte muss gerade sein).
-dn	Domänenname	Domänenname im gültigen Format
-auto	Einstellung für automatische Vereinbarung, die bestimmt, ob die Netzeinstellungen für die Übertragungs- geschwindigkeit und den Duplexmodus konfigurierbar sind.	true, false
-nic	NIC-Zugriff	shared, dedicated
-address_table	Tabelle der automatisch ge- nerierten IPv6-Adressen und ihre Präfixlängen <b>Anmerkung:</b> Diese Option wird nur dann angezeigt, wenn IPv6 und die statusunabhängige automati- sche Konfiguration aktiviert sind.	Dieser Wert ist schreibgeschützt und nicht konfigurierbar.
-ipv6	IPv6-Status	disabled, enabled
-lla	Lokale Verbindungsadresse Anmerkung: Die lokale Verbindungsadresse wird nur angezeigt, wenn IPv6 aktiviert ist.	Die lokale Linkadresse wird vom IMM2 bestimmt. Dieser Wert ist schreibgeschützt und nicht konfigurierbar.
-ipv6static	Statischer IPv6-Status	disabled, enabled
-i6	Statische IP-Adresse	Statische IP-Adresse für Ethernet-Kanal 0 im IPv6-Format
-p6	Länge des Adresspräfix	Numerisch zwischen 1 und 128
-g6	Gateway oder Standardroute	IP-Adresse für das Gateway oder die Standardroute für Ethernet-Kanal 0 im IPv6-Format.
-dhcp6	DHCPv6-Status	disabled, enabled
-sa6	Statusunabhängiger IPv6- Status mit automatischer Konfiguration	disabled, enabled

ifconfig eth0 [Optionen]
Optionen:
 -state Schnittstellenstatus

```
-c Konfigurationsmethode
-i Statische IPv4-IP-Adresse
-g IPv4-Gateway-Adresse
-s Teilnetzmaske
-n Hostname

    -r Übertragungsgeschwindigkeit

-d Duplexmodus
-m MTU
-1 Lokal_verwalteter MAC
-dn Domänenname
-auto Zustand
-nic Zustand
-address table
-ipv6 Zustand
-ipv6static Zustand
-sa6 Zustand
-i6 Statische IPv6-IP-Adresse
-g6 IPv6-Gateway-Adresse
-p6 Länge
```

Beispiel:

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-1 00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
Diese Konfigurationsänderungen werden nach der nächsten Zurücksetzung des IMM2 aktiv.
system>
```

**Anmerkung:** Die Option **-b** in der Anzeige von "ifconfig" steht für die Herstellerkennung der MAC-Adresse. Die Herstellerkennung der MAC-Adresse ist schreibgeschützt und nicht konfigurierbar.

## Befehl "keycfg"

Verwenden Sie den Befehl **keycfg**, um Aktivierungsschlüssel anzuzeigen, hinzuzufügen oder zu löschen. Über diese Schlüssel wird der Zugriff auf optionale FoD-Funktionen (Features on Demand) des IMM2 gesteuert.

- Wird **keycfg** ohne Optionen ausgeführt, so wird die Liste installierter Aktivierungsschlüssel angezeigt. Die angezeigten Schlüsselinformationen umfassen eine Indexzahl für jeden Aktivierungsschlüssel, den Aktivierungsschlüsseltyp, das Datum, bis zu dem der Schlüssel gültig ist, die Anzahl verbleibender Verwendungen, den Schlüsselstatus und eine Beschreibung des Schlüssels.
- Durch Dateiübertragung neue Aktivierungsschlüssel hinzufügen.
- Löschen Sie alte Schlüssel, indem Sie die Zahl des Schlüssels oder den Schlüsseltyp angeben. Beim Löschen von Schlüsseln nach Typ wird nur der erste Schlüssel eines bestimmten Typs gelöscht.

Option	Beschreibung	Werte
-add	Aktivierungsschlüssel hinzufügen	Werte für die Befehlsoptionen -ip, -pn, -u, -pw und -f.

Option	Beschreibung	Werte
-ip	IP-Adresse des TFTP- Servers mit hinzuzufü- gendem Aktivierungsschlüssel	Gültige IP-Adresse für TFTP-Server.
-pn	Portnummer für TFTP-/SFTP-Server mit hinzuzufügendem Aktivierungsschlüssel	Gültige Portnummer für TFTP-/SFTP-Server (Standard 69/22).
-u	Benutzername für SFTP-Server mit hin- zuzufügendem Aktivierungsschlüssel	Gültiger Benutzername für SFTP-Server
-pw	Kennwort für SFTP- Server mit hinzuzufü- gendem Aktivierungsschlüssel	Gültiges Kennwort für SFTP-Server
-f	Dateiname für hinzu- zufügenden Aktivierungsschlüssel	Gültiger Dateiname für Aktivierungsschlüsseldatei.
-del	Aktivierungsschlüssel nach Indexzahl lö- schen	Gültige Indexzahl für Aktivierungsschlüssel aus <b>keycfg-</b> Liste.
-deltype	Aktivierungsschlüssel nach Schlüsseltyp lö- schen	Gültiger Wert für Schlüsseltyp.

```
keycfg [Optionen]
Option:
   -add   -ip IP-Adresse
   -pn Portnummer
   -u Benutzername
   -pw Kennwort
   -f Dateiname
   -del Schlüsselindex
   -deltype Schlüsseltyp
```

Beispiel:

system> keycfg
ID Type Valid Uses Status Description
1 4 10/10/2010 5 "valid" "IMM remote presence"
2 3 10/20/2010 2 "valid" "IMM feature"
system>

# Befehl "Idap"

Mit dem Befehl **ldap** können Sie die Konfigurationsparameter des LDAP-Protokolls anzeigen und konfigurieren.

Option	Beschreibung	Werte
-a	Benutzerauthentifi- zierungsverfahren	"local only", "LDAP only", "local first then LDAP", "LDAP first then local"

Option	Beschreibung	Werte
-aom	Modus nur für Authentifizierung	enabled, disabled
-b	Bindungsmethode	"anonymous", "bind with ClientDN and password", "bind with Login Credential"
-С	Definierter Name des Clients	Zeichenfolge mit bis zu 127 Zeichen für Definierter_Name_des_Clients
-d	Suchdomäne	Zeichenfolge mit bis zu 63 Zeichen für Suchdomäne
-f	Gruppenfilter	Zeichenfolge mit bis zu 127 Zeichen für Gruppenfilter
-fn	Gesamtstrukturname	Für aktive Verzeichnisumgebungen. Zeichenfolge mit bis zu 127 Zeichen.
-g	Gruppensuchattribut	Zeichenfolge mit bis zu 63 Zeichen für <i>Gruppensuchattribut</i>
-1	Anmeldeberechti- gungsattribut	Zeichenfolge mit bis zu 63 Zeichen für Zeichenfolge
-р	Clientkennwort	Zeichenfolge mit bis zu 15 Zeichen für Clientkennwort
-pc	Clientkennwort bestä- tigen	Zeichenfolge mit bis zu 15 Zeichen für Bestätigungskennwort
		Befehlssyntax: ldap -p <i>Clientkennwort</i> -pc <i>Bestätigungskennwort</i>
		Diese Option ist erforderlich, wenn Sie das Clientkennwort ändern. Sie vergleicht das Argument <i>Bestätigungskennwort</i> mit dem Argument <i>Clientkennwort.</i> Der Befehl schlägt fehl, wenn die bei- den Argumente nicht miteinander übereinstimmen.
-r	Definierter Name des Stammeintrags (DN)	Zeichenfolge mit bis zu 127 Zeichen für definierter_Rootname
-rbs	Erweiterte rollenbasierte Sicher- heit für Active Directory-Benutzer	enabled, disabled
-s1ip	Hostname/IP-Adresse von Server 1	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Ad- resse für <i>Hostname/IP-Adresse</i>
-s2ip	Hostname/IP-Adresse von Server 2	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Ad- resse für <i>Hostname/IP-Adresse</i>
-s3ip	Hostname/IP-Adresse von Server 3	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Ad- resse für <i>Hostname/IP-Adresse</i>
-s4ip	Hostname/IP-Adresse von Server 4	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Ad- resse für <i>Hostname/IP-Adresse</i>
-s1pn	Portnummer von Ser- ver 1	Eine numerische Portnummer mit bis zu 5 Ziffern für <i>Portnummer</i>
-s2pn	Portnummer von Ser- ver 2	Eine numerische Portnummer mit bis zu 5 Ziffern für <i>Portnummer</i>
-s3pn	Portnummer von Ser- ver 3	Eine numerische Portnummer mit bis zu 5 Ziffern für <i>Portnummer</i>
-s4pn	Portnummer von Ser- ver 4	Eine numerische Portnummer mit bis zu 5 Ziffern für <i>Portnummer</i>

Option	Beschreibung	Werte
-t	Zielname des Servers	Wenn die Option "-rbs" aktiviert ist, gibt dieses Feld einen Zielnamen an, der mithilfe des Snap-in-Tools für die rollenbasierte Sicherheit auf dem Active Directory- Server einer oder mehreren Rollen zugeordnet werden kann.
-u	UID-Suchattribut	Zeichenfolge mit bis zu 63 Zeichen für Suchattribut
-V	LDAP-Serveradresse über DNS abrufen	off, on
-h	Zeigt die Befehlssyntax und die Optionen an	

ldap [Optionen] Optionen: -a loc |ldap |locld |ldloc -aom enable/disabled -b anon client login -c Definierter\_Name\_des\_Clients -d Suchdomäne -f Gruppenfilter -fn Gesamtstrukturname -g Gruppensuchattribut -1 Zeichenfolge -p Clientkennwort -pc Bestätigungskennwort -r definierter Rootname -rbs enable/disabled -slip Hostname/IP-Adresse -s2ip Hostname/IP-Adresse -s3ip Hostname/IP-Adresse -s4ip Hostname/IP-Adresse -s1pn Portnummer -s2pn Portnummer -s3pn Portnummer -s4pn Portnummer -t Name -u Suchattribut -v off on -h

## Befehl "ntp"

Mit dem Befehl **ntp** können Sie das Network Time Protocol (NTP) anzeigen und konfigurieren.

Option	Beschreibung	Werte
-en	Aktiviert oder inaktiviert das Network Time Protocol.	enabled, disabled
-i <sup>1</sup>	Name oder IP-Adresse des Network Time Protocol- Servers. Hierbei handelt es sich um die Indexnummer des Network Time Protocol-Servers.	Der Name des NTP-Servers, der für die Taktgebersynchronisation verwendet wer- den soll.Die Reichweite der Indexnummer des NTP-Servers reicht von -i1 bis -i4.

Option	Beschreibung	Werte
-f	Die Häufigkeit (in Minu- ten), mit der der IMM2- Taktgeber mit dem Network Time Protocol- Server synchronisiert wird	3 - 1440 Minuten
-synch	Fordert eine sofortige Syn- chronisation mit dem Network Time Protocol- Server an	Mit diesem Parameter werden keine Werte verwendet.
1i entspricht i1.		

ntp [Optionen] Optionen: -en Zustand -i Hostname/IP-Adresse -f Häufigkeit -synch

Beispiel:

system> ntp
-en: disabled
-f: 3 minutes
-i: not set

## Befehl "passwordcfg"

Mit dem Befehl **passwordcfg** können Sie die Kennwortparameter anzeigen und konfigurieren.

Option	Beschreibung	
-legacy	Legt für die Accountsicherheit eine vordefinierte Gruppe von traditionellen Standardwerten fest.	
-high	Legt für die Accountsicherheit eine vordefinierte Gruppe von hohen Standardwerten fest.	
-exp	Maximale Gültigkeitsdauer des Kennworts (0 - 365 Tage). Der Wert "0" bedeu- tet, dass das Kennwort nie abläuft.	
-cnt	Anzahl der vorherigen Kennwörter, die nicht erneut verwendet werden dür- fen.	
-nul	Lässt Konten ohne Kennwort zu (yes   no)	
-h	Zeigt die Befehlssyntax und die Optionen an	

Syntax:

```
passwordcfg [Optionen]
Optionen: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

Beispiel:

```
system> passwordcfg
Security Level: Legacy
system> passwordcfg -exp 365
ok
system> passwordcfg -nul yes
ok
system> passwordcfg -cnt 5
ok
system> passwordcfg
Security Level: Customize
-exp: 365
-cnt: 5
-nul: allowed
```

## Befehl "ports"

Mit dem Befehl ports können Sie IMM2-Ports anzeigen und konfigurieren.

Wird der Befehl **ports** ohne Optionen ausgeführt, so werden Informationen für alle IMM2-Ports angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-open	Offene Ports anzeigen	
-reset	Ports auf Standardeinstellungen zurücksetzen	
-httpp	HTTP-Portnummer	Standardportnummer: 80
-httpsp	HTTPS-Portnummer	Standardportnummer: 443
-telnetp	Traditionelle Telnet- CLI-Portnummer	Standardportnummer: 23
-sshp	Traditionelle SSH-CLI- Portnummer	Standardportnummer: 22
-snmpap	SNMP-Agenten- Portnummer	Standardportnummer: 161
-snmptp	SNMP-Traps- Portnummer	Standardportnummer: 162
-rpp	Remote-Presence- Portnummer	Standardportnummer: 3900
-cimhp	CIM-over-HTTP- Portnummer	Standardportnummer: 5988
-cimhsp	CIM-over-HTTPS- Portnummer	Standardportnummer: 5989

### Syntax:

ports [Optionen]

Option:

-open

-reset

-httpp Portnummer

-httpsp Portnummer

-telnetp Portnummer

-sshp Portnummer -snmpap Portnummer

```
-snmptp Portnummer

-rpp Portnummer

-cimhp Portnummer

-cimhsp Portnummer

Beispiel:

System> Ports

-httpp 80

-httpsp 443

-rpp 3900
```

```
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-telnetp 23
-cimhp 5988
-cimhsp 5989
system>
```

## Befehl "portcfg"

Mit dem Befehl **portcfg** können Sie das IMM2 für die Funktion zur seriellen Umleitung konfigurieren.

Das IMM2 muss so konfiguriert sein, dass es mit den Servereinstellungen für interne serielle Anschlüsse übereinstimmt. Um die Konfiguration des seriellen Anschlusses zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Konfiguration des seriellen Anschlusses ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

**Anmerkung:** Der externe serielle Anschluss des Servers kann vom IMM2 nur für die IPMI-Funktion verwendet werden. Die Befehlszeilenschnittstelle wird durch den seriellen Anschluss nicht unterstützt. Die Optionen **serred** und **cliauth**, die in der Befehlszeilenschnittstelle von Remote Supervisor Adapter II vorhanden waren, werden nicht unterstützt.

Wird der Befehl **portcfg** ohne Optionen ausgeführt, so wird die Konfiguration des seriellen Anschlusses angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-b	Baudrate	9600, 19200, 38400, 57600, 115200
-р	Parität	none, odd, even
-S	Bits stoppen	1, 2
-climode	CLI-Modus	0, 1, 2
		Dabei gilt:
		• 0 = none: Die Befehlszeilenschnittstelle wird inak- tiviert
		<ul> <li>1 = cliems: Die Befehlszeilenschnittstelle wird mit EMS-kompatiblen Tastenfolgen aktiviert</li> </ul>
		<ul> <li>2 = cliuser: Die Befehlszeilenschnittstelle wird mit benutzerdefinierten Tastenfolgen aktiviert</li> </ul>

Anmerkung: Die Anzahl an Datenbits (8) ist in der Hardware festgelegt und kann nicht geändert werden.

```
Syntax:
portcfg [Optionen]
Optionen:
  -b Baudrate
  -p Parität
  -s Bits stoppen
  -climode Modus
Beispiel:
system> portcfg
-b : 57600
-climode : 2 (CLI mit benutzerdefinierter Tastenfolge)
-p : even
       : 1
-s
system> portcfg -b 38400
ok
system>
```

# Befehl "restore"

Mit dem Befehl **restore** können Sie Systemeinstellungen aus einer Sicherungsdatei wiederherstellen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-f	Name der Sicherungsdatei	Gültiger Dateiname
-pp	Kennwort oder Verschlüsselungstext, mithilfe dessen Kenn- wörter innerhalb der Sicherungsdatei ver- schlüsselt sind	Gültiges Passwort oder durch Anführungszeichen be- grenzter Verschlüsselungstext
-ip	IP-Adresse des TFTP-/ SFTP-Servers	Gültige IP-Adresse
-pn	Portnummer des TFTP-/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP- Server	Gültiges Kennwort

Syntax:

```
restore [Optionen]
Option:
-f Dateiname
-pp Kennwort
-ip IP-Adresse
-pn Portnummer
-u Benutzername
-pw Kennwort
```

Beispiel: system> restore -f imm-back.cli -pp xxxxxx -ip 192.168.70.200 ok system>

## Befehl "restoredefaults"

Mit dem Befehl **restoredefaults** können Sie alle IMM2-Einstellungen auf die werkseitige Voreinstellung zurücksetzen.

- Für den Befehl restoredefaults gibt es keine Optionen.
- · Sie werden aufgefordert, den Befehl zu bestätigen, bevor dieser verarbeitet wird.

Syntax:

restoredefaults

Beispiel:

system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result. You will need to reconfigure the IMM network interface to restore connectivity. After the IMM configuration is cleared, the IMM will be restarted.

```
Proceed? (y/n)
Y
```

Restoring defaults...

### Befehl "set"

Mit dem Befehl set können Sie Einstellungen des IMM2 ändern.

- Manche Einstellungen des IMM2 können einfach durch den Befehl set geändert werden.
- Manche dieser Einstellungen, etwa Umgebungsvariablen, werden vom CLI verwendet.
- Mit dem Befehl show können Sie über den Befehl set festgelegte Werte anzeigen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
value	Wert für angegebenen Pfad oder angegebene Einstellung festlegen	Entsprechender Wert für angegebenen Pfad oder ange- gebene Einstellung.
value	Wert für angegebenen Pfad oder angegebene Einstellung festlegen	Entsprechender Wert für angegebenen Pfad oder an gebene Einstellung.

Syntax:

set [Optionen]
Option:
 value

### Befehl "smtp"

Mit dem Befehl **smtp** können Sie Einstellungen für die SMTP-Schnittstelle anzeigen und konfigurieren.

Wird der Befehl **smtp** ohne Optionen ausgeführt, so werden alle Informationen zur SMTP-Schnittstelle angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-auth	Authentifizierungs- support für SMTP	enabled, disabled

Option	Beschreibung	Werte
-authepw	verschlüsseltes Kenn- wort für die SMTP- Authentifizierung	Gültige Kennwort-Zeichenkette
-authmd	SMTP-Authentifi- zierungsverfahren	CRAM-MD5, LOGIN
-authn	Benutzername zur SMTP- Authentifizierung	Zeichenkette (auf 256 Zeichen begrenzt).
-authpw	SMTP-Authentifi- zierungskennwort	Zeichenkette (auf 256 Zeichen begrenzt).
-pn	SMTP-Portnummer	Gültige Portnummer.
-S	IP-Adresse oder Hostname des SMTP- Servers	Gültige IP-Adresse oder gültiger Hostname (auf 63 Zeichen begrenzt).

```
smtp [Optionen]
Option:
    -auth enabled|disabled
    -authepw Kennwort
    -authmd CRAM-MD5|LOGIN
    -authn Benutzername
    -authpw Kennwort
    -s IP-Adresse_oder_Hostname
    -pn Portnummer
```

Beispiel:

```
system> smtp
-s test.com
-pn 25
system>
```

# Befehl "snmp"

Mit dem Befehl **snmp** können Sie die SNMP-Schnittstelleninformationen anzeigen und konfigurieren.

Wird der Befehl **snmp** ohne Optionen ausgeführt, so werden alle Informationen zur SNMP-Schnittstelle angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-a	SNMPv1-Agent	on, off <b>Anmerkung:</b> Folgende Kriterien müssen zur Aktivie- rung des SNMPv1-Agenten erfüllt sein:
		• Über die Befehlsoption "-cn" angegebener Ansprech- partner für das IMM2.
		<ul> <li>Über die Befehlsoption "-l" angegebener Standort des IMM2.</li> </ul>
		<ul> <li>Mindestens ein über eine der "-cx"-Befehlsoptionen angegebener SNMP-Community-Name.</li> </ul>
		<ul> <li>Mindestens eine g ültige IP-Adresse wird  über eine der "-cxiy"-Befehlsoptionen f ür jede SNMP- Community angegeben.</li> </ul>

Option	Beschreibung	Werte
-a3	SNMPv3-Agent	<ul> <li>on, off</li> <li>Anmerkung: Folgende Kriterien müssen zum Aktivieren des SNMPv3-Agenten erfüllt sein:</li> <li>Über die Befehlsoption "-cn" angegebener Ansprechpartner für das IMM2.</li> </ul>
		<ul> <li>Über die Befehlsoption "-l" angegebener Standort des IMM2.</li> </ul>
-t	SNMP-Traps	on, off
-1	IMM2-Standort	Zeichenkette (auf 47 Zeichen begrenzt). Anmerkung:
		• Argumente mit Leerzeichen müssen in Anführungs- zeichen gesetzt werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig.
		• Löschen Sie beim IMM2-Standort den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa "".
-cn	Ansprechpartner für IMM2	Zeichenkette (auf 47 Zeichen begrenzt). Anmerkung:
		• Argumente mit Leerzeichen müssen in Anführungs- zeichen gesetzt werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig.
		• Löschen Sie beim IMM2-Ansprechpartner den In- halt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa "".
-c <i>x</i>	Name von SNMP- Community <i>x</i>	Zeichenkette (auf 15 Zeichen begrenzt). Anmerkung:
		• <i>x</i> wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Communitynummer anzuzeigen.
		• Argumente mit Leerzeichen müssen in Anführungs- zeichen gesetzt werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig.
		• Löschen Sie bei einem SNMP-Community-Namen den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument an- geben, etwa "".
-cxiy	IP-Adresse oder Hostname <i>y</i> von SNMP-Community <i>x</i>	Gültige IP-Adresse oder gültiger Hostname (auf 63 Zeichen begrenzt). <b>Anmerkung:</b>
		• <i>x</i> wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Communitynummer anzuzeigen.
		• <i>y</i> wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Nummer der IP-Adresse oder des Hostnamens anzuzeigen.
		• Eine IP-Adresse oder ein Hostname darf nur Punk- te, Unterstriche, Minuszeichen, Buchstaben und Zif- fern enthalten. Eingebettete Leerzeichen oder aufeinanderfolgende Punkte sind nicht zulässig.
		<ul> <li>Löschen Sie den Inhalt bei der IP-Adresse oder beim Hostnamen einer SNMP-Community, indem Sie kein Argument angeben.</li> </ul>

Option	Beschreibung	Werte
-ca <i>x</i>	Zugriffstyp bei SNMPv3-Community x	get, set, trap <b>Anmerkung:</b> <i>x</i> wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Communitynummer anzuzeigen.

snmp [Optionen] Option: -a Zustand -a3 Zustand -t Zustand -1 Standort -cn Name\_des\_Ansprechpartners -c1 Name von SNMP-Community 1 -c2 Name\_von\_SNMP-Community\_2 -c3 Name\_von\_SNMP-Community\_3 -cli1 IP-Adresse\_oder\_Hostname\_1\_von\_Community\_1 -c1i2 IP-Adresse\_oder\_Hostname\_2\_von\_Community\_1 -cli3 IP-Adresse\_oder\_Hostname\_3\_von\_Community\_1 -c2i1 IP-Adresse\_oder\_Hostname\_1\_von\_Community\_2 -c2i2 IP-Adresse\_oder\_Hostname\_2\_von\_Community\_2 -c2i3 IP-Adresse\_oder\_Hostname\_3\_von\_Community\_2 -c3i1 IP-Adresse\_oder\_Hostname\_1\_von\_Community\_3 -c3i2 IP-Adresse oder Hostname 2 von Community 3 -c3i3 IP-Adresse\_oder\_Hostname\_3\_von\_Community\_3 -cal Zugriffstyp\_von\_Community\_1 -ca2 Zugriffstyp\_von\_Community\_2 -ca3 Zugriffstyp von Community 3

Beispiel:

```
system> snmp
-a Enabled
-a3 Enabled
-t Enabled
-1 RTC,NC
-cn Snmp Test
-c1 public
-c1i1 192.44.146.244
-c1i2 192.44.146.181
-c1i3 192.44.143.16
-cal set
-ch1 specific
-c2 private
-c2i1 192.42.236.4
-c2i2
-c2i3
-ca2 get
-ch2 specific
-c3
-c3i1
-c3i2
-c3i3
-ca3 get
-ch3 ipv4only
system>
```

### Befehl "snmpalerts"

Mit dem Befehl snmpalerts können Sie über SNMP Alerts verwalten.

Wird **snmpalerts** ohne Optionen ausgeführt, so werden alle SNMP-Alerteinstellungen angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-status	SNMP-Alertstatus	on, off
-crt	Legt kritische Ereignis- se fest, die Alerts sen- den	<ul> <li>all, none, custom:te   vo   po   di   fa   cp   me   in   re   ot</li> <li>Benutzerdefinierte Einstellungen für kritische Alerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit</li> <li>Werten in der Form snmpalerts -crt custom:te   vo an- gegeben; benutzerdefinierte Werte sind: <ul> <li>te: kritischer Temperaturschwellenwert überschritten</li> <li>vo: kritischer Spannungsschwellenwert überschritten</li> <li>po: kritischer Netzausfall</li> <li>di: Fehler beim Festplattenlaufwerk</li> <li>fa: Lüfterfehler</li> <li>cp: Mikroprozessorfehler</li> <li>in: Hardwareinkompatibilität</li> <li>re: Stromversorgungsredundanzfehler</li> <li>ot: alle anderen kritischen Ereignisse</li> </ul> </li> </ul>
-crten	Alerts bei kritischen Ereignissen senden	enabled, disabled
-wrn	Legt Warnungsereignisse fest, die Alerts senden	all, none, custom:rp   te   vo   po   fa   cp   me   ot Benutzerdefinierte Einstellungen für Warnungsalerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form <b>snmpalerts -wrn custom:rp</b>   <b>te</b> angegeben; benutzerdefinierte Werte sind: • rp: Warnung bei Stromversorgungsredundanz • te: Warnungstemperaturschwellenwert überschritten • vo: Warnungsspannungsschwellenwert überschritten • po: Warnungsnetzschwellenwert überschritten • fa: unkritischer Lüfterfehler • cp: Mikroprozessor in beeinträchtigtem Zustand • me: Speicherwarnung • ot: alle anderen Warnungsereignisse
-wrnen	Alerts bei Warnungsereignissen senden	enabled, disabled

Option	Beschreibung	Werte
-sys	Legt Routineereignisse fest, die Alerts senden	<ul> <li>all, none, custom:lo tio ot po bf til pf el ne</li> <li>Benutzerdefinierte Einstellungen für Routinealerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form snmpalerts -sys custom:lo tio angegeben; benutzerdefinierte Werte sind: <ul> <li>lo: erfolgreiche Fernanmeldung</li> <li>tio: Zeitlimit des Betriebssystems</li> <li>ot: alle anderen Informations- und Systemereignisse</li> <li>po: Stromversorgung des Systems ein/aus</li> <li>bf: Bootfehler des Betriebssystems</li> <li>til: Watchdog-Zeitlimitüberschreitung des Betriebssystemladeprogramms</li> <li>pf: vorhergesagter Fehler (PFA - Predictive Failure Analysis)</li> <li>el: Ereignisprotokoll zu 75% voll</li> </ul> </li> </ul>
-sysen	Alerts bei Routineereignissen senden	enabled, disabled

```
snmpalerts [Optionen]
Optionen:
-status Status
-crt Ereignistyp
-crten Zustand
-wrn Ereignistyp
-wrnen Zustand
-sys Ereignistyp
-sysen Zustand
```

## Befehl "srcfg"

Verwenden Sie den Befehl **srcfg**, um die Tastenkombination für den Zugang zur Befehlszeilenschnittstelle vom Modus für serielle Umleitung anzugeben. Um die Konfiguration der seriellen Umleitung zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Konfiguration der seriellen Umleitung ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Networking and Security Configuration" (Konfiguration von Adapternetzbetrieb und -sicherheit) verfügen.

Anmerkung: Die IMM2-Hardware sieht keine Pass-Through-Fähigkeit zwischen seriellen Anschlüssen vor. Daher werden die Optionen -passthru und entercliseq, die in der Befehlszeilenschnittstelle des Remote Supervisor Adapter II vorhanden sind, nicht unterstützt.

Wird der Befehl **srcfg** ohne Optionen ausgeführt, so wird die aktuelle Tastenfolge für die serielle Umleitung angezeigt. In der folgenden Tabelle sind die Argumente für die Befehlsoption srcfg -entercliseq aufgelistet.

Option	Beschreibung	Werte
-entercliseq	Beschreibung Tastenfolge für Befehlszeilen- schnittstelle ein- geben	Werte Benutzerdefinierte Tastenfolge für den Zugang zur Befehlszeilenschnittstelle. Anmerkung: Diese Sequenz muss mindestens ein Zeichen und darf höchstens 15 Zeichen enthalten. Das Winkelzeichen (^) hat in dieser Sequenz eine spezielle Bedeutung. Es steht bei Tastatureingaben, die 'Strg'-Sequenzen zugeordnet sind (beispielsweise ^[ für die Abbruchtaste und ^M für einen
		Zeilenumbruch), für 'Strg'. Jedes Auftreten von '^' wird als Teil einer 'Strg'-Sequenz interpretiert. Eine vollständige Liste mit 'Strg'-Sequenzen finden Sie in der ASCII-Konvertierungstabelle. Der Standardwert für dieses Feld ist ^[(, d. h. die Abbruchtaste gefolgt von einer (.

srcfg [Optionen]
Optionen:
-entercliseq entercli\_keyseq

Beispiel:

system> srcfg
-entercliseq ^[Q
system>

## Befehl "sshcfg"

Mit dem Befehl sshcfg können Sie die SSH-Parameter anzeigen und konfigurieren.

Wird der Befehl **sshcfg** ohne Optionen ausgeführt, so werden alle SSH-Parameter angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-cstatus	Zustand von SSH-CLI	enabled, disabled
-hk gen	Privaten Schlüssel für SSH-Server generieren	
-hk rsa	Öffentlichen Schlüssel von Server-RSA anzei- gen	

Syntax:

```
sshcfg [Optionen]
Option:
    -cstatus Zustand
    -hk gen
    -hk rsa
```

Beispiel:

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

### Befehl "ssl"

Mit dem Befehl ssl können Sie die SSL-Parameter anzeigen und konfigurieren.

**Anmerkung:** Bevor Sie einen SSL-Client aktivieren können, muss ein Clientzertifikat installiert werden.

Wird der Befehl **ssl** ohne Optionen ausgeführt, so werden SSL-Parameter angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-ce	Aktiviert oder inakti- viert einen SSL-Client	on, off
-se	Aktiviert oder inakti- viert einen SSL-Server	on, off
-cime	Aktiviert oder inakti- viert CIM over HTTPS auf dem SSL-Server	on, off

#### Syntax:

portcfg [Optionen] Optionen: -ce Zustand -se Zustand -cime Zustand

Parameter: Die folgenden Parameter erscheinen in der Optionsstatusanzeige für den Befehl **ssl** und werden nur über die Befehlszeilenschnittstelle ausgegeben:

#### Server secure transport enable (Sichere Serverübertragung aktivieren) Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt

werden.

#### Server Web/CMD key status (Server-Web/CMD-Schlüsselstatus)

Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

### SSL server CSR key status (CSR-Schlüssel für SSL-Server)

Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

### SSL Client LDAP key status (LDAP-Schlüssel für SSL-Client)

Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed Private Key and Auto-gen self-signed cert installed Private Key and Self-signed cert installed Private Key stored, CSR available for download

### SSL Client CSR key status (CSR-Schlüssel für SSL-Client)

Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

### Befehl "sslcfg"

Verwenden Sie den Befehl **sslcfg**, um SSL für das IMM2 anzuzeigen und zu konfigurieren und um Zertifikate zu verwalten.

Wird der Befehl **sslcfg** ohne Optionen ausgeführt, so werden alle Informationen zur SSL-Konfiguration angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-server	SSL-Serverstatus	enabled, disabled Anmerkung: Der SSL-Server kann nur bei Vorliegen eines gültigen Zertifikats aktiviert werden.
-client	SSL-Clientstatus	enabled, disabled <b>Anmerkung:</b> Der SSL-Client kann nur bei Vorliegen eines gültigen Server- oder Clientzertifikats aktiviert werden.
-cim	CIM-over-HTTPS-Sta- tus	enabled, disabled Anmerkung: CIM over HTTPS kann nur bei Vorliegen eines gültigen Server- oder Clientzertifikats aktiviert werden.
-cert	Selbst signiertes Zerti- fikat generieren	<ul> <li>server, client, sysdir</li> <li>Anmerkung:</li> <li>Werte für die Befehlsoptionen -c, -sp, -cl, -on und -hn sind bei der Erstellung eines selbst signierten Zertifikats erforderlich.</li> <li>Werte für die Befehlsoptionen -cp, -ea, -ou, -s, -gn, -in und -dq sind bei der Erstellung eines selbst sig- nierten Zertifikats optional.</li> </ul>
-csr	Zertifikatssignier- anforderung generieren	<ul> <li>server, client, sysdir</li> <li>Anmerkung:</li> <li>Werte für die Befehlsoptionen -c, -sp, -cl, -on und -hn sind bei der Erstellung einer Zertifikatssignieranforderung erforderlich.</li> <li>Werte für die Befehlsoptionen -cp, -ea, -ou, -s, -gn, -in, -dq, -cpwd und -un sind bei der Erstellung ei- ner Zertifikatssignieranforderung optional.</li> </ul>

Option	Beschreibung	Werte
-i	IP-Adresse für TFTP-/ SFTP-Server	Gültige IP-Adresse Anmerkung: Beim Hochladen eines Zertifikats und beim Herunterladen eines Zertifikats oder einer Zertifikatssignieranforderung muss eine IP-Adresse für den TFTP- oder SFTP-Server angegeben werden.
-pn	Portnummer des TFTP-/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP- Server	Gültiges Kennwort
-1	Dateiname des Zertifi- kats	Gültiger Dateiname Anmerkung: Beim Herunterladen oder Hochladen eines Zertifikats oder einer Zertifikatssignieranforderung ist ein Dateiname erfor- derlich. Wenn beim Herunterladen kein Dateiname angegeben wird, wird der Standardname für die Datei verwendet und angezeigt.
-dnld	Zertifikatsdatei herun- terladen	Bei dieser Option sind keine Argumente erforderlich; es müssen jedoch Werte für die Befehlsoptionen -cert oder -csr angegeben werden (abhängig davon, welcher Zertifikatstyp heruntergeladen wird). Bei dieser Opti- on sind keine Argumente erforderlich; es müssen je- doch Werte für die Befehlsoption -i und die (optionale) Befehlsoption -I angegeben werden.
-upld	Importiert Zertifikatsdatei	Bei dieser Option sind keine Argumente erforderlich, es müssen jedoch Werte für die Befehlsoptionen <b>-cert</b> , <b>-i</b> und <b>-l</b> angegeben werden.
-tcx	Vertrauenswürdiges Zertifikat <i>x</i> für SSL- Client	import, download, remove <b>Anmerkung:</b> Die vertrauenswürdige Zertifikatsnummer <i>x</i> wird in der Befehlsoption als Ganzzahl zwischen 1 und 3 angegeben.
-C	Land	Landescode (2 Buchstaben) Anmerkung: Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-sp	Land oder Bundesland	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) <b>Anmerkung:</b> Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cl	Ort oder Standort	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 50 Zeichen) <b>Anmerkung:</b> Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-on	Name des Unterneh- mens	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) <b>Anmerkung:</b> Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.

Option	Beschreibung	Werte
-hn	IMM2-Hostname	Zeichenkette (höchstens 60 Zeichen) Anmerkung: Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cp	Ansprechpartner	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) <b>Anmerkung:</b> Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-ea	E-Mail-Adresse des Ansprechpartners	Gültige E-Mail-Adresse (höchstens 60 Zeichen) Anmerkung: Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-ou	Organisationseinheit	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) <b>Anmerkung:</b> Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-5	Nachname	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) <b>Anmerkung:</b> Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-gn	Vorname	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) <b>Anmerkung:</b> Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-in	Initialen	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 20 Zeichen) <b>Anmerkung:</b> Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-dq	Qualifikationsmerkmal des Domänennamens	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) <b>Anmerkung:</b> Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cpwd	Kennwort abfragen	Zeichenkette (mindestens 6 Zeichen, höchstens 30 Zei- chen) Anmerkung: Optional bei der Erstellung einer Zertifikatssignieranforderung.
-un	Unstrukturierter Name	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) <b>Anmerkung:</b> Optional bei der Erstellung einer Zertifikatssignieranforderung.

sslcfg [Optionen]
Option:
 -server Zustand
 -client Zustand
 -cim Zustand
 -cert Zertifikatstyp

```
-csr Zertifikatstyp
-i IP-Adresse
-pn Portnummer
-u Benutzername
-pw Kennwort
-1 Dateiname
-dnld
-upld
-tcx Maßnahme
-c Landescode
-sp Land oder Bundesland
-cl Ort_oder_Standort
-on Name des Unternehmens
-hn IMM-Hostname
-cp Ansprechpartner
-ea E-Mail-Adresse
-ou Organisationseinheit
-s Nachname
-gn Vorname
-in Initialen
-dq Qualifikationsmerkmal des Domänennamens
-cpwd Kennwort abfragen
-un Unstrukturierter_Name
```

Beispiel:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
A self-signed certificate is installed
SSL Client Certificate status:
A self-signed certificate is installed
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
system>
```

## Befehl "telnetcfg"

Mit dem Befehl **telnetcfg** können Sie Telnet-Einstellungen anzeigen und konfigurieren.

Wird der Befehl **telnetcfg** ohne Optionen ausgeführt, so wird der Telnet-Zustand angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-en	Telnet-Zustand	disabled (inaktiviert), 1, 2 <b>Anmerkung:</b> Wenn Telnet nicht inaktiviert wird, ist es für entweder einen oder zwei Benutzer aktiviert.

Syntax: telnetcfg [Optionen] Option: -en Zustand

Beispiel:

system> telnetcfg
-en 1
system>

### Befehl "thermal"

Verwenden Sie den Befehl **thermal**, um die Richtlinie für den Temperaturmodus des Hostsystems anzuzeigen und zu konfigurieren.

Wird der Befehl **thermal** ohne Optionen ausgeführt, so wird die Richtlinie für den Temperaturmodus angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-mode	Auswahl des Temperaturmodus	normal, performance

Syntax:

thermal [Optionen]
Option:
 -mode Temperaturmodus

Beispiel:

system> thermal
-mode normal
system>

### Befehl "timeouts"

Mit dem Befehl **timeouts** können Sie die Zeitlimitwerte anzeigen oder ändern. Um die Zeitlimitwerte anzuzeigen, geben Sie timeouts ein. Um die Zeitlimitwerte zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um Zeitlimitwerte ändern zu können, müssen Sie mindestens über die Berechtigung "Adapter Configuration" (Adapterkonfiguration) verfügen.

In der folgenden Tabelle sind die Argumente für die Zeitlimitwerte aufgelistet. Diese Werte entsprechen den abgestuften Pulldownoptionsskalen für Serverzeitlimits in der Webschnittstelle.

Option	Zeitlimit	Einheiten	Werte
-f	Ausschaltverzögerung	Minuten	disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-1	Zeitlimit für das Ladeprogramm	Minuten	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
-0	Zeitlimit für das Betriebs- system	Minuten	disabled, 2.5, 3, 3.5, 4

Syntax:

timeouts [Optionen]
Optionen:
-f Watchdogoption\_für\_Ausschaltverzögerung
-o Option\_für\_Betriebssystem-Watchdog
-1 Option\_für\_Ladeprogramm-Watchdog

Beispiel:

```
system> timeouts
-o disabled
-1 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-1 3.5
```

### Befehl "usbeth"

Mit dem Befehl **usbeth** können Sie die Inbandschnittstelle "LAN over USB" aktivieren oder inaktivieren.

Syntax:

```
usbeth [Optionen]
Optionen:
-en <enabled|disabled>
```

Beispiel:

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

### Befehl "users"

Mit dem Befehl **users** können Sie auf alle Benutzerkonten und auf die zugehörigen Berechtigungsstufen zugreifen. Mit dem Befehl **users** können Sie außerdem neue Benutzerkonten erstellen und bereits vorhandene Konten ändern.

Wenn Sie den Befehl **users** ohne Optionen ausführen, werden eine Liste der Benutzer und bestimmte grundlegende Benutzerinformationen angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-Benutzer- index	Indexnummer des Benutzerkontos	1 bis 12 einschließlich oder all für alle Benutzer.
-n	Name des Benutzerkontos	Eindeutige Zeichenfolge, die nur Zahlen, Buchstaben, Punkte und Unterstriche enthält. Mindestens vier Zei- chen; höchstens 16 Zeichen.
-р	Kennwort des Benutzerkontos	Zeichenfolge, die mindestens ein alphabetisches und ein nicht alphabetisches Zeichen enthält. Mindestens sechs Zeichen; höchstens 20 Zeichen. Mit null Zeichen wird ein Konto ohne Kennwort erstellt. Der Benutzer muss das Kennwort bei der ersten Anmeldung festle- gen.

Option	Beschreibung	Werte
-a	Benutzerberechti- gungsstufe	super, ro, custom
	Sungootale	Dabei gilt:
		• super (Supervisor)
		• ro (Lesezugriff)
		<ul> <li>custom wird gefolgt von einem Doppelpunkt und einer Liste mit Werten, die durch Pipes voneinan- der getrennt sind, wie im folgenden Format: custom:am rca. Diese Werte können in beliebiger Kombination verwendet werden.</li> </ul>
		am (Benutzerkontenverwaltungszugriff)
		rca (Zugriff auf ferne Konsole)
		rcvma (Zugriff auf ferne Konsole und virtuelle Datenträger)
		pr (Zugriff auf Einschalten/Neustart eines fer- nen Servers)
		cel (Berechtigung zum Löschen von Ereignisprotokollen)
		bc (Adapterkonfiguration - Allgemein)
		nsc (Adapterkonfiguration - Netz und Sicher- heit)
		rcvma (Adapterkonfiguration - Erweitert)
-ep	Verschlüsselungs- kennwort (für Sicherung/ Wiederherstellung)	Gültiges Kennwort
-clear	Angegebenes Benutzerkonto entfer- nen	Die Indexnummer des zu entfernenden Benutzerkontos muss im folgenden Format angegeben werden:
-curr	Benutzer anzeigen	
-sauth	SNMPv3-Authenti- fizierungsprotokoll	HMAC-MD5, HMAC-SHA, none
-spriv	SNMPv3- Datenschutzprotokoll	CBC-DES, AES, none
-spw	SNMPv3- Datenschutzkennwort	Gültiges Kennwort
-sepw	SNMPv3- Datenschutzkennwort (verschlüsselt)	Gültiges Kennwort
-sacc	SNMPv3-Zugriffstyp	get, set
-strap	SNMPv3-Trap- Hostname	Gültiger Hostname

Option	Beschreibung	Werte
-pk	Öffentlichen SSH- Schlüssel für Benutzer anzeigen	<ul> <li>Indexnummer des Benutzerkontos.</li> <li>Anmerkung:</li> <li>Es werden jeder dem Benutzer zugeordnete SSH-Schlüssel und die jeweilige Schlüsselindexnummer angezeigt.</li> <li>Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option -pk nach dem Benutzerindex (Option -Benutzerindex) im folgenden Format verwendet werden: users -2 -pk.</li> <li>Alle Schlüssel weisen das OpenSSH-Format auf.</li> </ul>
-e	Vollständigen SSH- Schlüssel im OpenSSH-Format an- zeigen (Option für öffentliche SSH-Schlüssel)	Diese Option kann nur ohne Argumente verwendet werden. Sie muss ohne die anderen Optionen vom Typ users -pk verwendet werden. <b>Anmerkung:</b> Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option -pk nach dem Benutzerindex (Option <i>-Benutzerindex</i> ) im fol- genden Format verwendet werden: users -2 -pk -e.
-remove	Öffentlichen SSH- Schlüssel für Benutzer entfernen ( <i>Option für öffentliche</i> <i>SSH-Schlüssel</i> )	Die Indexnummer des öffentlichen Schlüssels, der entfernt werden soll, muss für einen bestimmten Schlüssel mit - <i>Schlüsselindex</i> oder für alle dem Be- nutzer zugeordneten Schlüssel mit -all angegeben werden. <b>Anmerkung:</b> Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option -pk nach dem Benutzerindex (Option - <i>Benutzerindex</i> ) im fol- genden Format verwendet werden: users -2 -pk -remove -1.
-add	Öffentlichen SSH- Schlüssel für Benutzer hinzufügen (Option für öffentliche SSH-Schlüssel)	<ul> <li>Durch Anführungszeichen begrenzter Schlüssel im OpenSSH-Format</li> <li>Anmerkung:</li> <li>Die Option -add muss ohne die anderen Befehlsoptionen vom Typ users -pk verwendet werden.</li> <li>Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option -pk nach dem Benutzerindex (Option -Benutzerindex) im folgen- den Format verwendet werden: users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyL0CiIaN0y400ICEKCqjKEhrYymtAoVtfKApv Y39GpnSGC/qcLGWLM4cmirKL5kxHN0qIcwbT1NPceoKH j46X7E+mq1fWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR9803/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTB13SAtMu cUsTkYj1Xcqex10Qz4+N50R6MbNcwlsx+mTEAvvcpJhug a70UNPGhLJM16k7jeJiQ8Xd2p Xb0ZQ=="</li> </ul>

Option	Beschreibung	Werte
-upld	Öffentlichen SSH- Schlüssel hochladen (Option für öffentliche SSH-Schlüssel)	<ul> <li>Die Optionen -i und -l sind für die Angabe der Schlüsselposition erforderlich.</li> <li>Anmerkung:</li> <li>Die Option -upld muss ohne die anderen Befehlsoptionen vom Typ users -pk verwendet werden (mit Ausnahme der Optionen -i und -l).</li> <li>Um einen Schlüssel durch einen neuen Schlüssel zu ersetzen, müssen Sie einen -Schlüsselindex ange- ben. Wenn Sie einen Schlüssel zum Ende der Liste der aktuellen Schlüssel hinzufügen möchten, geben Sie keinen Schlüsselindex an.</li> <li>Wenn Sie die Optionen für öffentliche SSH-Schlüs- sel verwenden, muss die Option -pk nach dem Benutzerindex (Option -Benutzerindex) im folgen- den Format verwendet werden: users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key.</li> </ul>
-dnld	Angegebenen öffentli- chen SSH-Schlüssel herunterladen (Option für öffentliche SSH-Schlüssel)	<ul> <li>Der -Schlüsselindex zum Herunterladen des betreffenden Schlüssels und die Optionen -i und -l zum Angeben der Speicherposition für den Download (auf einem anderen Computer als auf dem, auf dem ein TFTP-Server ausgeführt wird) sind erforderlich.</li> <li>Anmerkung:</li> <li>Die Option -dnld muss ohne die anderen Befehlsoptionen vom Typ users -pk verwendet werden (mit Ausnahme von -i, -l und -Schlüsselindex).</li> <li>Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option -pk nach dem Benutzerindex (Option -Benutzerindex) im folgenden Format verwendet werden: users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -1 file.key.</li> </ul>
-i	IP-Adresse des TFTP/ SFTP-Server zum Hoch- oder Herunter- laden einer Schlüsseldatei (Option für öffentliche SSH-Schlüssel)	Gültige IP-Adresse Anmerkung: Die Option -i ist für die Befehlsoptionen users -pk -upld und users -pk -dnld erforderlich.
-pn	Portnummer des TFTP/SFTP-Servers (Option für öffentliche SSH-Schlüssel)	Gültige Portnummer (Standard 69/22) Anmerkung: Ein optionaler Parameter für die Befehlsoptionen users -pk -upld und users -pk -dnld.
-u	Benutzername für SFTP-Server (Option für öffentliche SSH-Schlüssel)	Gültiger Benutzername Anmerkung: Ein optionaler Parameter für die Befehlsoptionen users -pk -upld und users -pk -dnld.
-pw	Kennwort für SFTP- Server (Option für öffentliche SSH-Schlüssel)	Gültiges Kennwort Anmerkung: Ein optionaler Parameter für die Befehlsoptionen users -pk -upld und users -pk -dnld.

Option	Beschreibung	Werte
-1	Dateiname zum Hoch- oder Herunterladen einer Schlüsseldatei über TFTP oder SFTP ( <i>Option für öffentliche</i> <i>SSH-Schlüssel</i> )	Gültiger Dateiname Anmerkung: Die Option -1 ist für die Befehlsoptionen users -pk -up1d und users -pk -dn1d erforderlich.
-af	Verbindungen vom Host akzeptieren (Option für öffentliche SSH-Schlüssel)	Eine durch Kommas getrennte Liste von Hostnamen und IP-Adressen, begrenzt auf 511 Zeichen. Gültige Zeichen: alphanumerisch, Komma, Stern, Fragezei- chen, Ausrufezeichen, Punkt, Bindestrich, Doppel- punkt und Prozentzeichen.
-cm	Kommentar (Option für öffentliche SSH-Schlüssel)	Eine durch Anführungszeichen begrenzte Zeichenfolge von bis zu 255 Zeichen. <b>Anmerkung:</b> Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option -pk nach dem Benutzerindex (Option <i>-Benutzerindex</i> ) im fol- genden Format verwendet werden: users -2 -pk -cm "This is my comment.".

```
users [Optionen]
 Optionen:
   -Benutzerindex
  -n Benutzername
  -p Kennwort
  -a Berechtigungsstufe
  -ep Verschlüsselungskennwort
  -clear
  -curr
  -sauth Protokoll
   -spriv Protokoll
   -spw Kennwort
  -sepw Kennwort
  -sacc Zustand
  -strap Hostname
users -pk [Optionen]
 Optionen:
   -e
   -remove Index
   -add Schlüssel
  -upld
  -dnld
  -i IP-Adresse
  -pn Portnummer
  -u Benutzername
  -pw Kennwort
   -1 Dateiname
   -af Liste
   -cm Kommentar
```

Beispiel:

system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration

```
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSWORD -a custom:am|rca|ce1|nsc|ac
ok
system> users
1. USERID Read/Write
Password Expires: no expiration
2. test Read/Write
Password Expires: no expiration
3. test2 Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest custom:am rca cel nsc ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>
```

### IMM2-Steuerbefehle

Die Steuerbefehle für das IMM2 lauten wie folgt:

- "Befehl "alertentries""
- "Befehl "batch"" auf Seite 205
- "Befehl "clearcfg"" auf Seite 206
- "Befehl "clock"" auf Seite 206
- "Befehl "identify"" auf Seite 207
- "Befehl "info"" auf Seite 207
- "Befehl "resetsp"" auf Seite 208
- "Befehl "spreset"" auf Seite 208

### **Befehl** "alertentries"

Mit dem Befehl alertentries können Sie Alertempfänger verwalten.

- Wird **alertentries** ohne Optionen ausgeführt, so werden alle Alerteintragseinstellungen angezeigt.
- Beim Befehl **alertentries -number -test** wird ein Testalert an die angegebene Empfängerindexnummer generiert.
- Beim Befehl **alertentries -number** (wobei für 'number' eine Zahl zwischen 0 und 12 steht) werden Alerteintragseinstellungen für die angegebene Empfängerindexnummer angezeigt oder es wird Ihnen ermöglicht, die Alerteinstellungen für diesen Empfänger zu ändern.

Option	Beschreibung	Werte
-number	Indexnummer des Alertempfängers, der angezeigt, hinzuge- fügt, geändert oder gelöscht werden soll	1 bis 12

Option	Beschreibung	Werte
-status	Alertempfängerstatus	on, off
-type	Alerttyp	email, syslog
-log	Ereignisprotokoll in Alert-E-Mail einschlie- ßen	on, off
-n	Alertempfängername	Zeichenkette
-е	E-Mail-Adresse des Alertempfängers	Gültige E-Mail-Adresse
-ip	Syslog-IP-Adresse oder Hostname	Gültige IP-Adresse oder gültiger Hostname
-pn	Syslog-Portnummer	Gültige Portnummer
-del	Angegebene Empfängerindex- nummer löschen	
-test	Generiert einen Testalert an die ange- gebene Empfänger- indexnummer	
-crt	Legt kritische Ereignis- se fest, die Alerts sen- den	<ul> <li>all, none, custom:te   vo   po   di   fa   cp   me   in   re   ot</li> <li>Benutzerdefinierte Einstellungen für kritische Alerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit</li> <li>Werten in der Form alertentries -crt custom:te   vo an- gegeben; benutzerdefinierte Werte sind:</li> <li>te: kritischer Temperaturschwellenwert überschritten</li> <li>vo: kritischer Spannungsschwellenwert überschrit- ten</li> <li>po: kritischer Netzausfall</li> <li>di: Fehler beim Festplattenlaufwerk</li> <li>fa: Lüfterfehler</li> <li>cp: Mikroprozessorfehler</li> <li>me: Speicherfehler</li> <li>in: Hardwareinkompatibilität</li> <li>re: Stromversorgungsredundanzfehler</li> <li>ot: alle anderen kritischen Ereignisse</li> </ul>
-crten	Alerts bei kritischen Ereignissen senden	enabled, disabled

Option	Beschreibung	Werte
-wrn	Legt Warnungsereignisse fest, die Alerts senden	all, none, custom:rp   te   vo   po   fa   cp   me   ot
		Benutzerdefinierte Einstellungen für Warnungsalerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form <b>alertentries -wrn custom:rp</b>   <b>te</b> angegeben; benutzerdefinierte Werte sind:
		• rp: Warnung bei Stromversorgungsredundanz
		• te: Warnungstemperaturschwellenwert überschritten
		• vo: Warnungsspannungsschwellenwert überschritten
		• po: Warnungsnetzschwellenwert überschritten
		• fa: unkritischer Lüfterfehler
		• cp: Mikroprozessor in beeinträchtigtem Zustand
		me: Speicherwarnung
		ot: alle anderen Warnungsereignisse
-wrnen	Alerts bei Warnungsereignissen senden	enabled, disabled
-sys	Legt Routineereignisse fest_die Alerts senden	all, none, custom:lo   tio   ot   po   bf   til   pf   el   ne
	lest, die Alerts senden	Benutzerdefinierte Einstellungen für Routinealerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form <b>alertentries -sys custom:lo</b>   <b>tio</b> angegeben; benutzerdefinierte Werte sind:
		<ul> <li>lo: erfolgreiche Fernanmeldung</li> </ul>
		• tio: Zeitlimit des Betriebssystems
		• ot: alle anderen Informations- und Systemereignisse
		• po: Stromversorgung des Systems ein/aus
		• bf: Bootfehler des Betriebssystems
		<ul> <li>til: Watchdog-Zeitlimitüberschreitung des Betriebssystemladeprogramms</li> </ul>
		<ul> <li>pf: vorhergesagter Fehler (PFA - Predictive Failure Analysis)</li> </ul>
		• el: Ereignisprotokoll zu 75% voll
		• ne: Netzänderung
-sysen	Alerts bei Routineereignissen senden	enabled, disabled

```
alertentries [Optionen]
Optionen:
    -number Empfängernummer
        -status Status
        -type Alerttyp
        -log Protokollzustand_einschließen
        -n Empfängername
        -e E-Mail-Adresse
        -ip IP-Adresse_oder_Hostname
        -pn Portnummer
        -del
        -test
```

```
-crt Ereignistyp
      -crten Zustand
      -wrn Ereignistyp
      -wrnen Zustand
      -sys Ereignistyp
      -sysen Zustand
Beispiel:
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

## Befehl "batch"

Mit dem Befehl **batch** können Sie einen oder mehrere in einer Datei enthaltene CLI-Befehle ausführen.

- Kommentarzeilen in der Batchdatei beginnen mit einem #.
- Beim Ausführen einer Batchdatei werden fehlgeschlagene Befehle zusammen mit einem Fehlerrückgabecode zurückgeleitet.
- Batchdateibefehle, die nicht erkannte Befehlsoptionen enthalten, generieren möglicherweise Warnungen.

Option	Beschreibung	Werte
-f	Name der Batchdatei	Gültiger Dateiname
-ip	IP-Adresse des TFTP-/ SFTP-Servers	Gültige IP-Adresse
-pn	Portnummer des TFTP-/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP- Server	Gültiges Kennwort

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Syntax:

```
batch [Optionen]
Option:
    -f Dateiname
    -ip IP-Adresse
    -pn Portnummer
    -u Benutzername
    -pw Kennwort
```

### Beispiel:

```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg -client -dnld -ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

# Befehl "clearcfg"

Mit dem Befehl **clearcfg** können Sie die IMM2-Konfiguration auf die werkseitigen Voreinstellungen zurücksetzen. Sie müssen mindestens über die Berechtigung "Advanced Adapter Configuration" (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können. Nachdem die Konfiguration des IMM2 gelöscht wurde, wird das IMM2 erneut gestartet.

### Befehl "clock"

Mit dem Befehl **clock** können Sie das aktuelle Datum und die aktuelle Uhrzeit entsprechend der IMM2-Uhr und der GMT-Abweichung anzeigen. Sie können das Datum, die Uhrzeit, die GMT-Abweichung und die Sommerzeiteinstellungen festlegen.

Beachten Sie Folgendes:

- Für eine GMT-Abweichung von +2, -7, -6, -5, -4 oder -3 sind besondere Einstellungen für die Sommerzeit erforderlich:
  - Für +2 gibt es folgende Optionen für die Sommerzeit: off, ee (Eastern Europe), mik (Minsk), tky (Turkey), bei (Beirut), amm (Amman), jem (Jerusalem).
  - Für -7 gibt es folgende Sommerzeiteinstellungen: off, mtn (Mountain), maz (Mazatlan).
  - Für -6 gibt es folgende Sommerzeiteinstellungen: off, mex (Mexico), cna (Central North America).
  - Für -5 gibt es folgende Sommerzeiteinstellungen: off, cub (Cuba), ena (Eastern North America).
  - Für -4 gibt es folgende Sommerzeiteinstellungen: off, asu (Asuncion), cui (Cuiaba), san (Santiago), cat (Canada - Atlantic).
  - Für -3 gibt es folgende Sommerzeiteinstellungen: off, gtb (Godthab), moo (Montevideo), bre (Brazil - East).
- Das Jahr muss von 2000 bis einschließlich 2089 angegeben werden.
- Monat, Datum, Stunden, Minuten und Sekunden können als Einzelzifferwerte angegeben werden (z. B. 9:50:25 anstatt 09:50:25).
- Die GMT-Abweisung kann im Format +2:00, +2 oder 2 (f
  ür positive Abweichungen) und im Format -5:00 oder -5 (f
  ür negative Abweichungen) angegeben werden.

Syntax:
clock [Optionen] Optionen: -d mm/tt/jjjj -t hh:mm:ss -g gmt offset -dst on/off/special case

Beispiel:

system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2011
ok
system> clock
12/31/2011 13:15:30 GMT-5:00 dst on

### Befehl "identify"

Mit dem Befehl **identify** können Sie die Gehäusekennzeichnungsanzeige einschalten, ausschalten oder blinken lassen. Die Option -d kann zusammen mit -s verwendet werden, um die Anzeige nur für eine bestimmte Anzahl an Sekunden einzuschalten, die mit dem Parameter -d angegeben werden. Nachdem die Anzahl an Sekunden verstrichen ist, wird die Anzeige ausgeschaltet.

```
Syntax:
```

```
identify [Optionen]
Optionen:
-s on/off/blink
-d Sekunden
Beispiel:
```

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

## Befehl "info"

Mit dem Befehl **info** können Sie die Informationen zum IMM2 anzeigen und konfigurieren.

Wird der Befehl **info** ohne Optionen ausgeführt, so werden alle Standort- und Kontaktinformationen zum IMM2 angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-name	Name des IMM2	Zeichenkette
-contact	Name des Ansprech- partners für das IMM2	Zeichenkette
-location	IMM2-Standort	Zeichenkette
-room <sup>1</sup>	Raum-ID des IMM2	Zeichenkette
-rack <sup>1</sup>	Gehäuserahmen-ID des IMM2	Zeichenkette
-rup <sup>1</sup>	Position des IMM2 im Gehäuserahmen	Zeichenkette
-ruh	Höhe der Gehäuserahmeneinheit	Read only (Lesezugriff)

Option	Beschreibung	Werte	
-bbay	Standort der Bladeposition	Read only (Lesezugriff)	
1. Der Wert lautet "read only" und kann nicht zurückgesetzt werden, wenn sich das IMM2 auf einem IBM Flex System-Knoten befindet.			

Syntax:

```
info [Optionen]
Option:
    -name IMM-Name
    -contact Name_des_Ansprechpartners
    -location IMM-Standort
    -room Raum-ID
    -rack Gehäuserahmen-ID
    -rup Position_der_Gehäuserahmeneinheit
    -ruh Höhe_der_Gehäuserahmeneinheit
    -bbay Bladeposition
```

### Befehl "resetsp"

Mit dem Befehl **resetsp** können Sie das IMM2 erneut starten. Sie müssen mindestens über die Berechtigung "Advanced Adapter Configuration" (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können.

### Befehl "spreset"

Mit dem Befehl **spreset** können Sie das IMM2 erneut starten. Sie müssen mindestens über die Berechtigung "Advanced Adapter Configuration" (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können.

## Anhang A. Hilfe und technische Unterstützung anfordern

Wenn Sie Hilfe, Service oder technische Unterstützung benötigen oder einfach nur Informationen zu IBM-Produkten erhalten möchten, finden Sie bei IBM eine Vielzahl von hilfreichen Quellen.

Verwenden Sie diese Informationen, um zusätzliche Informationen zu IBM und IBM Produkten zu erhalten, um herauszufinden, was Sie bei Problemen mit Ihrem IBM System oder Ihrer Zusatzeinrichtung tun können und an wen Sie sich wenden können, wenn Sie Service benötigen.

### Bevor Sie sich an den Kundendienst wenden

Stellen Sie sicher, bevor Sie sich an den Kundendienst wenden, dass Sie die folgenden Schritte durchgeführt haben, um zu versuchen, das Problem selbst zu beheben.

Wenn Sie denken, dass Sie den IBM Herstellerservice für Ihr IBM Produkt in Anspruch nehmen müssen, können die IBM Kundendiensttechniker Sie besser unterstützen, wenn Sie sich vor Ihrem Anruf beim Kundendienst vorbereiten.

- Überprüfen Sie alle Kabel und vergewissern Sie sich, dass diese angeschlossen sind.
- Prüfen Sie an den Netzschaltern, ob das System und die Zusatzeinrichtungen eingeschaltet sind.
- Überprüfen Sie, ob aktualisierte Software, Firmware und Einheitentreiber für das Betriebssystem Ihres IBM Produkts vorhanden sind. In den Bedingungen des freiwilligen IBM Herstellerservices steht, dass Sie als Eigentümer des Produkts dafür verantwortlich sind, die Software und Firmware für das Produkt zu warten und zu aktualisieren (es sei denn, dies ist durch einen zusätzlichen Wartungsvertrag abgedeckt). Der IBM Kundendiensttechniker wird Sie dazu auffordern, ein Upgrade für Ihre Software und Firmware durchzuführen, wenn in einem Software-Upgrade eine dokumentierte Lösung für das Problem vorhanden ist.
- 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.
- Rufen Sie die folgende Seite auf http://www.ibm.com/supportportal, um nach Informationen zu suchen, die Ihnen bei der Fehlerbehebung helfen können.
- Stellen Sie für den IBM Support folgende Informationen zusammen. Mithilfe dieser Daten findet der IBM Support schnell eine Lösung für Ihr Problem und kann sicherstellen, dass Sie genau die Servicestufe erhalten, die Sie vertraglich vereinbart haben.
  - Hardware- und Softwarewartungsvertragsnummern, falls vorhanden
  - Maschinentypnummer (vierstellige IBM Maschinenkennung)
  - Modellnummer
  - Seriennummer
  - Aktuelle UEFI- und Firmwareversionen des Systems
  - Andere relevante Informationen wie z. B. Fehlernachrichten und -protokolle

 Rufen Sie die folgende Seite auf http://www.ibm.com/support/entry/portal/ Open\_service\_request, um eine ESR (Electronic Service Request - elektronische Serviceanforderung) zu senden. Wenn Sie eine ESR senden, beginnt der Lösungsfindungsprozess für Ihr Problem, da die relevanten Informationen dem IBM Support schnell und effizient zur Verfügung gestellt werden. IBM Kundendiensttechniker können mit der Fehlerbehebung beginnen, sobald Sie eine ESR ausgefüllt und übergeben haben.

Viele Fehler können ohne Hilfe von außen anhand der IBM Hinweise zur Fehlerbehebung in der Onlinehilfefunktion oder in der Dokumentation, die im Lieferumfang Ihres IBM Produkts enthalten ist, behoben werden. In der Begleitdokumentation der IBM Systeme sind auch die Diagnosetests beschrieben, die Sie ausführen können. Im Lieferumfang der meisten Systeme, Betriebssysteme und Programme sind eine Dokumentation zu Fehlerbehebungsprozeduren sowie Erläuterungen zu Fehlernachrichten und Fehlercodes enthalten. Wenn Sie einen Softwarefehler vermuten, finden Sie weitere Informationen dazu in der Dokumentation zum Betriebssystem oder zum 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 der Systemdokumentation. Über die Fehlerbehebungsinformationen oder die Diagnoseprogramme erfahren Sie möglicherweise, dass Sie zusätzliche oder aktuelle Einheitentreiber oder andere Software benötigen. IBM verwaltet Seiten im World Wide Web, über die Sie nach den neuesten technischen Informationen suchen und Einheitentreiber und Aktualisierungen herunterladen können. Für den Zugriff auf diese Seiten rufen Sie http://www.ibm.com/ supportportal auf.

#### Hilfe und Informationen über das World Wide Web anfordern

Aktuelle Informationen zu IBM Produkten und zur Unterstützung sind im World Wide Web verfügbar.

Im World Wide Web finden Sie aktuelle Informationen zu IBM Systemen, Zusatzeinrichtungen, Services und Unterstützung unter http://www.ibm.com/ supportportal. 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

Senden Sie Ihre Diagnosedaten über das IBM Enhanced Customer Data Repository (ECuRep) an IBM.

Lesen Sie vor dem Senden von Diagnosedaten an IBM die Nutzungsbedingungen unter http://www.ibm.com/de/support/ecurep/terms.html.

Sie können eine der folgenden Methoden zum Senden von Diagnosedaten an IBM verwenden:

- 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

### Personalisierte Unterstützungswebseite erstellen

Durch die gezielte Angabe von IBM Produkten, an denen Sie interessiert sind, können Sie eine personalisierte Unterstützungswebseite erstellen.

Wenn Sie eine personalisierte Unterstützungswebseite erstellen möchten, rufen Sie folgende Adresse auf http://www.ibm.com/support/mynotifications. Über diese personalisierte 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 bei Problemen mit der Nutzung, der Konfiguration und der Software von IBM Produkten.

Für weitere Informationen zur Support Line und zu anderen IBM Services rufen Sie http://www.ibm.com/services auf. Telefonnummern für Unterstützung finden Sie, wenn Sie http://www.ibm.com/planetwide aufrufen. In den Vereinigten Staaten oder in Kanada können Sie die folgende Nummer anrufen: 1-800-IBM-SERV (1-800-426-7378).

### Hardware-Service und -unterstützung

Hardware-Service können Sie über den IBM Reseller oder den IBM Kundendienst erhalten.

Um nach einem Reseller zu suchen, der durch IBM zur Bereitstellung von Herstellerservice autorisiert wurde, rufen Sie http://www.ibm.com/partnerworld auf und klicken Sie rechts auf der Seite auf **Business Partner suchen**. Telefonnummern für technische Unterstützung von IBM finden Sie, wenn Sie http://www.ibm.com/ planetwide aufrufen. In den Vereinigten Staaten oder in Kanada können Sie die folgende Nummer anrufen: 1-800-IBM-SERV (1-800-426-7378).

In den USA und in Kanada ist Hardware-Service und -unterstützung jederzeit rund um die Uhr erhältlich. In Großbritannien sind diese Serviceleistungen von Montag bis Freitag von 9 bis 18 Uhr verfügbar.

### **IBM Produktservice in Taiwan**

Wenden Sie sich mithilfe dieser Informationen an den IBM Produktservice in Taiwan.



Kontaktinformationen für den IBM Produktservice in Taiwan:

IBM Taiwan Corporation 3F, No 7, Song Ren Rd. Taipei, Taiwan Telefon: 0800-016-888

## Anhang B. 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. Die auf diesen Websites verfügbaren Informationen beziehen sich nicht auf die für dieses IBM Produkt bereitgestellten Informationen. 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 International Business Machines Corporation. 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 ihrer Tochtergesellschaften in den USA und/oder 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 Hinweise

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 die Abkürzung MB für 1.000.000 Bytes und GB für 1.000.000 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 hat eine Halbleitereinheit eine maximale Anzahl von Schreibzyklen, die darauf ausgeführt werden können. Diese wird in "TBW" (total bytes written - Gesamtzahl der geschriebenen Bytes) angegeben. Hat eine Einheit dieses Limit überschritten, antwortet sie möglicherweise nicht mehr auf vom System generierte Befehle oder kann nicht mehr beschrieben werden. IBM ist nicht für den Austausch einer Einheit verantwortlich, die ihre maximale Anzahl garantierter Programmierungs-/Löschzyklen überschritten hat, welche in den offiziellen, veröffentlichten Spezifikationen dieser Einheit dokumentiert ist.

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 9. Grenzwerte für Staubpartikel und Gas
---

Verunreinigung	Grenzwerte
Staubpartikel	• Die Raumluft muss kontinuierlich mit einem Wirkungsgrad von 40 % gegenüber atmosphärischem Staub (MERV 9) nach ASHRAE-Norm 52.2 <sup>1</sup> 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 <sup>2</sup> .
	<ul> <li>Im Raum dürfen keine elektrisch leitenden Verunreinigungen wie Zink-Whisker vorhanden sein.</li> </ul>
Gase	• Kupfer: Klasse G1 gemäß ANSI/ISA 71.04-1985 <sup>3</sup>
	• Silber: Korrosionsrate von weniger als 300 Å in 30 Tagen
<sup>1</sup> ASHRAE 52.2-20 <i>Efficiency by Partic</i> Conditioning Eng	108 - Method of Testing General Ventilation Air-Cleaning Devices for Removal le Size. Atlanta: American Society of Heating, Refrigerating and Air- ineers, Inc.
<sup>2</sup> Die relative hygr relative Feuchtigk Ionen leiten zu kö	roskopische Feuchtigkeit der Verunreinigung durch Staubpartikel ist die eit, bei der der Staub genug Wasser absorbiert, um nass zu werden und mnen.
3 ANICI /ICA 71.04	

<sup>3</sup> 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, wenden Sie sich schriftlich 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.

#### Vorschriften 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. Wenden Sie sich bei Fragen an einen IBM Ansprechpartner oder IBM Reseller.

#### 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, Deutschland Telefon: +49 7032 15 2941 E-Mail: 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 von 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 Postanschrift: 71137 Ehningen 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

中华人民共和国"A类"警告声明

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** 



## Index

## Α

Absolute Maussteuerung 113 Active Directory-Benutzer LDAP 57, 197 Active Energy Manager Registerkarte "Policies" 138 ActiveX-Applet aktualisieren 108 Advanced Level-Funktionen 3 Aktivierungsschlüssel entfernen 146, 176 exportieren 147 installieren 143, 176 verwalten 58, 176 Aktualisieren ActiveX-Applet 108 Java-Applet 108 Aktuelle anzeigen Benutzer 56, 197 Alphabetische Befehlsliste 152 Anmeldeberechtigungsattribut LDAP 57, 177 Anmeldung, global Einstellungen 67 Anmeldung am IMM2 10 Ansichtsmodi in Fernsteuerung 110 Ansprechpartner für SNMPv1 festlegen 56, 185 Ansprechpartner für SNMPv3 festlegen 56, 185 Anzeigen Hardwarezustand 101 Systemstatus 97 Systemzustand 100 Arbeiten mit Ereignissen im Ereignisprotokoll 27 Ausführen IMM2-Tasks 105 Australia Class A statement 217 Automatische Vereinbarung festlegen 56, 174

## B

Baseboard Management Controller (BMC) 1 Basic Level-Funktionen 3 Befehl "accseccfg" 163 Befehl "alertcfg" 165 Befehl "alertentries" 202 Befehl "asu" 166 Befehl "backup" 170 Befehl "batch" 205 Befehl "clearcfg" 206 Befehl "clearlog" 154 Befehl "clock" 206 Befehl "console" 162 Befehl "dhcpinfo" 170 Befehl "dns" 171 Befehl "ethtousb" 173

Befehl "exit" 154 Befehl "fans" 155 Befehl "ffdc" 155 Befehl "gprofile" 173 Befehl "help" 154 Befehl "history" 154 Befehl "identify" 207 Befehl "ifconfig" 174 Befehl "info" 207 Befehl "keycfg" 176 Befehl "ldap" 177 Befehl "led" 156 Befehl "ntp" 179 Befehl "passwordcfg" 180 Befehl "portcfg" 182 Befehl "ports" 181 Befehl "power" 161 Befehl "pxeboot" 162 Befehl "readlog" 158 Befehl "reset" 162 Befehl "resetsp" 208 Befehl "restore" 183 Befehl "restoredefaults" 184 Befehl "set" 184 Befehl "show" 159 Befehl "smtp" 184 Befehl "snmp" 185 Befehl "snmpalerts" 188 Befehl "spreset" 208 Befehl "srcfg" 189 Befehl "sshcfg" 190 Befehl "ssl" 191 Befehl "sslcfg" 192 Befehl "syshealth" 159 Befehl "telnetcfg" 195 Befehl "temps" 159 Befehl "thermal" 196 Befehl "timeouts" 196 Befehl "usbeth" 197 Befehl "users" 197 Befehl "volts" 160 Befehl "vpd" 160 Befehl zur seriellen Umleitung 162 Befehle accseccfg 163 alertcfg 165 alertentries 202 asu 166 backup 170 batch 205 clearcfg 206 clearlog 154 clock 206 console 162 dhcpinfo 170 dns 171 ethtousb 173 exit 154 fans 155 ffdc 155 gprofile 173

Befehle (Forts.) help 154 history 154 identify 207 ifconfig 174 info 207 keycfg 176 ldap 177 led 156 ntp 179 passwordcfg 180 portcfg 182 ports 181 power 161 pxeboot 162 readlog 158 reset 162 resetsp 208 restore 183 restoredefaults 184 set 184 show 159 smtp 184 snmp 185 snmpalerts 188 spreset 208 srcfg 189 sshcfg 190 ssl 191 sslcfg 192 syshealth 159 telnetcfg 195 temps 159 thermal 196 timeouts 196 usbeth 197 users 197 volts 160 vpd 160 Befehle, alphabetische Liste 152 Befehle, Typen Dienstprogramm 153 IMM2-Steuerung 202 Konfiguration 162 serielle Umleitung 162 Serverstromversorgung und Neustart 161 Überwachung 154 Befehlszeilenschnittstelle (CLI - command-line interface) Anmeldung 150 Befehlssyntax 150 Beschreibung 149 Merkmale und Einschränkungen 151 Zugriff 149 Bemerkungen 213 elektromagnetische Verträglichkeit 217 FCC, Class A 217 Bemerkungen und Hinweise 5

Benutzer aktuelle anzeigen 56, 197 Kennwort 56, 197 löschen 56, 197 SNMPv3-Einstellungen 56, 197 SSH-Schlüssel 56, 197 verwalten 56, 197 Benutzerauthentifizierungsverfahren festlegen 56, 163 Benutzerdefinierte Unterstützungswebseite 211 Benutzerkonten konfigurieren 63 Benutzerkonto erstellen 56, 197 Gruppenprofil 66 Verwaltung 64 Betriebssystem, Voraussetzungen 4 Bindungsmethode LDAP-Server 57, 177 BIOS (Basic Input/Output System) 1 Blade-Server 1, 4, 7 BladeCenter 1, 4, 7 Booten, über Fernzugriff 119 Browservoraussetzungen 4

## С

Canada Class A electronic emission statement 217 China Class A electronic emission statement 220 CIM-over-HTTP-Port festlegen 57, 181 CIM over HTTPS Sicherheit 58, 191, 192 Zertifikatsverwaltung 58, 191, 192 CIM-over-HTTPS-Port festlegen 57, 181 Class A electronic emission notice 217

## D

Daten der Betriebssystem-Fehleranzeige erfassen 136 Daten für Service und Support erfassen 135 herunterladen 135 Daten für Service und Support erfassen 135 Datenträger, fern 119 Datum festlegen 55, 206 Datum und Uhrzeit, IMM2 einstellen 60 DDNS benutzerdefinierter Domänenname 56, 171 konfigurieren 56, 171 Quelle für Domänennamen 56, 171 verwalten 56, 171 vom DHCP-Server angegebener Domänenname 56, 171 Definierter Name, Client LDAP-Server 57, 177

Definierter Name, Stammeintrag LDAP-Server 57, 177 Definierter Name des Clients LDAP-Server 57, 177 Definierter Name für den Stammeintrag LDAP-Server 57, 177 Deutschland, Hinweis zur Klasse A 218 Dienstprogramm für erweiterte Einstellungen 1 Dienstprogrammbefehle 153 DNS IPv4-Adressierung 56, 171 IPv6-Adressierung 56, 171 konfigurieren 56, 171 LDAP-Server 57, 177 Serveradressierung 56, 171 Dokumentation Format 216 verwenden 210 Domänenname, benutzerdefiniert DDNS 56, 171 Domänenname, vom DHCP-Server angegeben DDNS 56, 171 Download Service Data Option, Übersicht 32 DSA, Senden von Daten an IBM 210

Ε

E-Mail-Empfänger konfigurieren 30 Einstellen Datum und Uhrzeit für IMM2 60 Einstellungen Anmeldung, global 67 Registerkarte "Account Security Level" 69 Registerkarte "General" 67 CIM over HTTPS 88 DDNS 77 DNS 76 erweitert 72 Ethernet 72 für die Websitzung 17 HTTPS 87 LDAP 78 Portzuordnungen 85 Protokoll für LDAP-Client 89 Sicherheit 86 SMTP 77 SNMP-Alert 74 SSH-Server 91 Telnet 84 USB 84 Einzelcursormodus 114 Electronic emission Class A notice 217 Entfernen Aktivierungsschlüssel 146, 176 Ereignis Protokoll 127 Ereignisbenachrichtigung 30 Ereignisempfänger 30 verwalten 127 Ereignisprotokoll 27 verwalten 127

Ereignisse Empfänger 129 Erfassung der Betriebssystemanzeige 109 Erfassung der Systemabsturzanzeige 109 Erneut starten IMM 208 IMM2 58 Erstellen Benutzerkonto 56, 197 E-Mail-Benachrichtigung 129 syslog-Benachrichtigung 129 Erstellen einer personalisierten Unterstützungswebseite 211 Erweiterte rollenbasierte Sicherheit LDAP 57, 197 Erweitertes Managementmodul 1, 4, 7 Ethernet konfigurieren 56, 174 Ethernet, erweitert Einstellungen 72 Ethernet over USB konfigurieren 57, 173 Portweiterleitung 57, 173 European Union EMC Directive conformance statement 218 Exportieren Aktivierungsschlüssel 147

## F

FCC Class A notice 217 Features on Demand 143 Funktion entfernen 146, 176 Funktion exportieren 147 Funktion installieren 143, 176 verwalten 58, 176 Ferner Datenträger 119, 120 Fernsteuerung absolute Maussteuerung 113 Anzeigenerfassung 109 beenden 121 Befehle für Stromversorgung und Neustart 115 Einzelcursormodus 114 Leistungsstatistiken 115 Mausunterstützung 113 relative Maussteuerung 113 relative Maussteuerung für Linux (Linux-Standardbeschleunigung) 113 Tastaturdurchgriffsmodus 113 Tastaturunterstützung 111 Unterstützung für internationale Tastatur 112 Video Viewer 107, 110 Virtual Media Session 107, 119 zugreifen 120 Fernsteuerung, Fenster Video Viewer 39 Virtual Media Session 39 Fernsteuerung der Stromversorgung 115 Fernsteuerungsfunktion 39, 107 Fernsteuerungsport festlegen 57, 181 Fernzugriff 2

Festlegen Ansprechpartner für SNMPv1 56, 185 Ansprechpartner für SNMPv3 56, 185 automatische Vereinbarung 56, 174 Benutzerauthentifizierungsverfahren 56, 163 CIM-over-HTTP-Port 57, 181 CIM-over-HTTPS-Port 57, 181 Datum 55, 206 Fernsteuerungsport 57, 181 größte zu übertragende Einheit 56, 174 Hostname 56, 174 HTTP-Port 57, 181 HTTPS-Port 57, 181 Inaktivitätszeitlimit für das Web 56, 163 LDAP-Server-Port 57, 177 MTU 56, 174 SNMP-Agenten-Port 57, 181 SNMP-Traps-Port 57, 181 SSH-CLI-Port 57, 181 Tastenkombination für Befehlszeilenschnittstelle 55, 182 Telnet-CLI-Port 57, 181 Uhrzeit 55, 206 Firmware des Servers anzeigen 160 Server anzeigen 55 Firmware, Server aktualisieren 122 Firmware aktualisieren 108 Firmwaredaten anzeigen Server 55, 160 FoD 143 Funktion entfernen 146, 176 Funktion exportieren 147 Funktion installieren 143, 176 verwalten 58, 176 Funktion Anklopfen 115 Funktion "Anklopfen" aktivieren 115 Benutzermodus Einzelbenutzer 115 Mehrbenutzer 115 Ferne Sitzung anfordern 115 Funktion entfernen Features on Demand 146, 176 FoD 146, 176 Funktion exportieren Features on Demand 147 FoD 147 Funktion installieren Features on Demand 143, 176 FoD 143, 176

## G

Gase, Verunreinigung 215 Globale Anmeldeeinstellungen Registerkarte "Account Security Level" 69 Registerkarte "General" 67 Größte zu übertragende Einheit festlegen 56, 174 Gruppe löschen aktivieren, inaktivieren 173 Gruppenfilter LDAP 57, 177 Gruppenprofil Verwaltung 66 Gruppensuchattribut LDAP 57, 177

## Η

Handhabung von Zertifikaten CIM over HTTPS 88 sicherer LDAP-Client 89 Hardwarezustand 101 Hilfe im World Wide Web 210 Quellen 209 Senden von Diagnosedaten an IBM 210 Hinweise, wichtige 214 Hostname festlegen 56, 174 LDAP-Server 57, 177 SMTP-Server 57, 184 HTTP-Port festlegen 57, 181 HTTPS-Port festlegen 57, 181 HTTPS-Server Sicherheit 58, 191, 192 Zertifikatsverwaltung 58, 191, 192

## 

IBM Blade-Server 1, 4, 7 IBM BladeCenter 1, 4, 7 IBM Produktservice in Taiwan 212 IMM erneut starten 208 Konfiguration wiederherstellen 183 Konfiguration zurücksetzen 184 konfigurieren 58 spreset 208 Standardkonfiguration 184 zurücksetzen 208 **IMM-Verwaltung** Aktivierungsschlüsselverwaltung 96 Benutzer Gruppenprofile 66 Konten 64 Benutzerkonten konfigurieren 63 IMM-Eigenschaften Einstellungen für den seriellen Anschluss 62 **IMM-Konfiguration** IMM-Konfiguration wiederherstellen und ändern 94 IMM2 erneut starten 94 Netzprotokoll konfigurieren 72 Sicherheitseinstellungen 86 IMM2 Aktionsbeschreibungen 11 Aktivierungsschlüsselverwaltung 96

IMM2 (Forts.) Beschreibung 1 erneut starten 58, 94 Funktionen 2 IMM2 Advanced Level 2 IMM2 Basic Level 2 IMM2 Standard Level 2 Konfiguration anzeigen 58 Konfiguration sichern 58 Konfiguration wiederherstellen 58 Konfiguration zurücksetzen 58 Konfigurationsansicht 58 Konfigurationsassistent 58 Konfigurationsoptionen 55 Konfigurationssicherung 58 Konfigurationswiederherstellung 58, 183 Netzverbindung 8 neue Funktionen 1 serielle Umleitung 150 Sicherungsstatus anzeigen 58 Sicherungsstatusansicht 58 Standardkonfiguration 58 Übersicht über die Webbenutzerschnittstelle 17 Webschnittstelle 7 Wiederherstellungsstatus anzeigen 58 Wiederherstellungsstatusansicht 58 zurücksetzen 58, 95 IMM2-Funktionen 2 Advanced Level 3 Basic Level 3 IMM2-FunktionenFunktionen von Standard Level Standard Level 3 IMM2 konfigurieren Optionen bei der Konfiguration das IMM2 55 IMM2-Steuerbefehle 202 IMM2-Tasks 105 IMM2-Verwaltung **IMM-Eigenschaften** Datum und Uhrzeit 60 IMM2 zurücksetzen 95 IMM2-Webbenutzerschnittstelle Registerkarte "Events' Übersicht über die Optionen 27 Registerkarte "Service and Support" Übersicht über Optionen 32 Registerkarte "System Status" Übersicht 21 Übersicht 17 IMM2-Websitzung abmelden 20 Inaktivitätszeitlimit für das Web festlegen 56, 163 Information Center 210 Installieren Aktivierungsschlüssel 143, 176 Installierte Netzteile Registerkarte "Power Modules" 140 Stromverbrauchssteuerung 140 **IP-Adresse** IPv4 7 IPv6 7 konfigurieren 7

IP-Adresse (*Forts.*) LDAP-Server 57, 177 SMTP-Server 57, 184 IP-Adresse, statischer Standard 8 IPMI ferne Serververwaltung 149 IPMItool 149 IPv4 konfigurieren 56, 174 IPv4-Adressierung DNS 56, 171 IPv6 7 konfigurieren 56, 174 IPv6-Adressierung DNS 56, 171

## J

Japan Class A electronic emission statement 219 Java 4, 119 Java-Applet aktualisieren 108

## K

Kennwort Benutzer 56, 197 LDAP-Server 57, 177 Konfiguration anzeigen IMM2 58 Konfiguration sichern IMM2 58 Konfiguration wiederherstellen IMM2 58, 183 Konfiguration zurücksetzen IMM 184 IMM2 58 Konfigurationsansicht IMM2 58 Konfigurationsassistent IMM2 58 Konfigurationsbefehle 162 Konfigurationssicherung IMM2 58 Konfigurationswiederherstellung IMM2 58, 183 Konfigurationszusammenfassung anzeigen 11 Konfigurieren Alertempfänger 30 CIM-over-HTTPS-Protokoll 88 DDNS 56, 171 DDNS-Einstellungen 77 DNS 56, 171 DNS-Einstellungen 76 Einstellungen für SNMP-Alerts 74 Ethernet 56, 174 Ethernet-Einstellungen 72 Ethernet over USB 57, 173 globale Anmeldeeinstellungen 67 HTTPS-Protokoll 87 IMM2 58 IPv4 56, 174 IPv6 56, 174 LDAP 57, 177

Konfigurieren (Forts.) LDAP-Einstellungen 78 LDAP-Server 57, 177 Netzprotokolle 72 Ports 57, 181 Portzuordnungen 85 Protokoll für LDAP-Client 89 Seriell-zu-SSH-Umleitung 150 Seriell-zu-Telnet-Umleitung 150 serieller Anschluss 55, 62, 182 Sicherheit 58 Sicherheitseinstellungen 86 Sicherheitsstufen für Benutzerkonten 56, 163 SMTP 56, 184 SMTP-Einstellungen 77 SNMPv1 56, 185 SNMPv1-Traps 56, 185 SNMPv3-Benutzerkonten 56, 197 SSH-Server 91 Telnet 195 Telnet-Einstellungen 57, 84 USB 57, 173 USB-Einstellungen 84 Korea Class A electronic emission statement 219

### L

Laufwerke zuordnen 120 Zuordnung aufheben 120 Laufwerke zuordnen 120 Laufwerkzuordnung aufheben 120 LDAP Active Directory-Benutzer 57, 197 Anmeldeberechtigungsattribut 57, 177 erweiterte rollenbasierte Sicherheit 197 Erweiterte rollenbasierte Sicherheit 57 Gruppenfilter 57, 177 Gruppensuchattribut 57, 177 konfigurieren 57, 177 Rollenabhängige Sicherheit, erweitert 57 rollenbasierte Sicherheit, erweitert 197 Sicherheit 58, 191, 192 Zertifikatsverwaltung 58, 191, 192 Zielname des Servers 57, 177 LDAP-Server Bindungsmethode 57, 177 definierter Name des Clients 177 Definierter Name des Clients 57 definierter Name für den Stammeintrag 177 Definierter Name für den Stammeintrag 57 DNS 57, 177 Hostname 57, 177 IP-Adresse 57, 177 Kennwort 57, 177 konfigurieren 57, 177 Portnummer 57, 177 Suchdomäne 57, 177

LDAP-Server (Forts.) UID-Suchattribut 57, 177 vorkonfiguriert 57, 177 LDAP-Server-Port festlegen 57, 177 Löschen Benutzer 56, 197 E-Mail-Benachrichtigung 129 syslog-Benachrichtigung 129

### Μ

MAC-Adresse verwalten 56, 174 Marken 213 Maussteuerung absolute 113 relative 113 relative mit Linux-Standardbeschleunigung 113 Mausunterstützung in Fernsteuerung 113 Mausunterstützung per Fernsteuerung 113 Maximale Anzahl an Sitzungen Telnet 57, 195 Menü "Events" 127 MTU festlegen 56, 174

## Ν

Netzprotokolleigenschaften DDNS 77 DNS 76 Einstellungen für SNMP-Alerts 74 Ethernet-Einstellungen 72 LDAP 78 Portzuordnungen 85 SMTP 77 Telnet 84 USB 84 Netzverbindung 8 IP-Adresse, statischer Standard 8 statische IP-Adresse, Standard 8 statische Standard-IP-Adresse 8 New Zealand Class A statement 217

## 0

Offene Ports anzeigen 57, 181 Onlineveröffentlichungen Informationen zu Dokumentationsaktualisierungen 1 Informationen zu Fehlercodes 1 Informationen zu Firmwareaktualisierungen 1 Option "Disks" auf der Registerkarte "Server Management" 49 Option "Latest OS Failure Screen" auf der Registerkarte "Server Management" 53 Option "Memory" auf der Registerkarte "Server Management" 50

Option "Page Auto Refresh" 17 Option "Power Management" auf der Registerkarte "Server Management' Stromverbrauch 137 Stromversorgungseinheiten 137 Stromversorgungsrichtlinien 137 Option "Processors" auf der Registerkarte "Server Management" 51 Option "PXE Network Boot" auf der Registerkarte "Server Management" 52 Option "Server Firmware" auf der Registerkarte "Server Management" 34 Option "Server Power Actions" auf der Registerkarte "Server Management" 49 Option "Server Properties" auf der Registerkarte "Server Management" 44 Option "Server Timeouts" auf der Registerkarte "Server Management" 52 Option "Trespass Message" 19 Optionen Registerkarte "IMM Management" 53 Optionen auf Registerkarte "Server Management" 33

### Ρ

People's Republic of China Class A electronic emission statement 220 Portnummer LDAP-Server 57, 177 SMTP-Server 57, 184 Portnummern festlegen 57, 181 Portnummern festlegen 57, 181 Ports konfigurieren 57, 181 Nummern festlegen 57, 181 offene anzeigen 57, 181 Portweiterleitung Ethernet over USB 57, 173 Produktservice, IBM Taiwan 212 PXE Boot Agent 11 PXE-Netzboot einrichten 121

## Q

Quelle für Domänennamen DDNS 56, 171

## R

Registerkarte "Events" Protokoll 27 Übersicht 27 Registerkarte "IMM Management" 53 Registerkarte "Power Allocation" Stromverbrauchssteuerung 141 Registerkarte "Power Allocation" (Forts.) Stromversorgung 141 Registerkarte "Server Management" 33 Registerkarte "Service and Support" Übersicht 32 Registerkarte "System Status" Übersicht 21 Relative Maussteuerung 113 Relative Maussteuerung für Linux (Linux-Standardbeschleunigung) 113 Remote Desktop Protocol (RDP) Start 115 Remote-Presence-Funktion 107 aktivieren 109 Remote Supervisor Adapter II 1 Rollenabhängige Sicherheit, erweitert LDAP 57 Rollenbasierte Sicherheit, erweitert LDAP 197 Rollenbasierte Stufen operator 173 rbs 173 supervisor 173 Russia Class A electronic emission statement 219

## S

Seite "System Status", Übersicht 21 Senden von Diagnosedaten an IBM 210 Serial over LAN 149 Seriell-zu-SSH-Umleitung 150 Seriell-zu-Telnet-Umleitung 150 Serieller Anschluss konfigurieren 55, 62, 182 Server-Firmware aktualisieren 122 Server-Firmware für IBM System x Beschreibung 1 Konfigurationsdienstprogramm 8 Server Management Option "Disks" 49 Option "Latest OS Failure Screen" 53 Option "Memory" 50 Option "Processors" 51 Option "PXE Network Boot" 52 Option "Server Firmware" 34 Option "Server Power Actions" 49 Option "Server Properties" 44 Option "Server Timeouts" 52 Server Properties Registerkarte "Environmentals" 44 Registerkarte "General Settings" 44 Registerkarte "Hardware Activity" 44 Registerkarte "Hardware Information" Registerkarte "Network Hardware" 44 Registerkarte "System Component Information" 44 Registerkarte "System Information" 44 Registerkarte "LED" 44 Serveradressierung DNS 56, 171 Serverstatus überwachen 97 Serverstatus überwachen 97

Serverstromversorgung steuern 106 Serverstromversorgung und Neustart Befehle 161 Serverwaltung Daten der Betriebssystem-Fehleranzeige 136 PXE-Netzboot 121 Server-Firmware 122 Serverzeitlimits, festlegen 58 Serverzeitlimit Optionen 58 Serverzeitlimits festlegen 58 Service und Unterstützung bevor Sie sich an den Kundendienst wenden 209 Hardware 211 Software 211 Sicherheit CIM over HTTPS 58, 191, 192 CIM-over-HTTPS-Protokoll 88 Handhabung von SSL-Zertifikaten 92 HTTPS-Protokoll 87 HTTPS-Server 58, 191, 192 konfigurieren 58 LDAP 58, 191, 192 LDAP-Client 89 SSH-Server 58, 91, 190 Übersicht über SSL 92 Verwaltung von SSL-Zertifikaten 93 Sicherheitsstufen für Benutzerkonten konfigurieren 56, 163 Sicherungsstatus anzeigen IMM 58 Sicherungsstatusansicht IMM2 58 Sitzungen, maximale Anzahl Telnet 57, 195 SMTP IP-Adresse des Servers 57, 184 konfigurieren 56, 184 Server-Hostname 57, 184 Server-Portnummer 57, 184 testen 57 SNMP-Agenten-Port festlegen 57, 181 SNMP-Traps-Port festlegen 57, 181 SNMPv1 konfigurieren 56, 185 SNMPv1-Communitys verwalten 56, 185 SNMPv1-Traps konfigurieren 56, 185 SNMPv3-Benutzerkonten konfigurieren 56, 197 SNMPv3-Einstellungen Benutzer 56, 197 SSH-CLI-Port festlegen 57, 181 SSH-Schlüssel Benutzer 56, 197 SSH-Server Sicherheit 58, 190 Zertifikatsverwaltung 58, 190 SSI Handhabung von Zertifikaten 92

SSL (Forts.) Zertifikatsverwaltung 93 Standardkonfiguration IMM 184 IMM2 58 Startreihenfolge ändern 11 Startreihenfolge des Host-Servers ändern 11 Statische IP-Adresse, Standard 8 Statische Standard-IP-Adresse 8 Staubpartikel, Verunreinigung 215 Stromverbrauchssteuerung Active Energy Manager 138 Registerkarte "Chart" 142 Registerkarte "Policies" 138 Registerkarte "Power Allocation" 141 Registerkarte "Power History" 142 Registerkarte "Power Modules" 140 Stromversorgung Kapazität 141 Stromversorgungsaktionen 106 Stromversorgungsstatus steuern des Servers 106 Suchdomäne LDAP-Server 57, 177 Systemereignis Benachrichtigung 129 Benachrichtigung wiederholen 129 Systemereignisbenachrichtigung 30 Systeminformationen 99 anzeigen 99 Systemstatus 97 Systemzustand 100

## T

Taiwan Class A electronic emission statement 220 Tastaturdurchgriffsmodus in Fernsteuerung 113 Tastaturunterstützung in Fernsteuerung 111 Tastenkombination für Befehlszeilenschnittstelle festlegen 55, 182 Telefonnummern 211 Telefonnummern für Hardware-Service und -unterstützung 211 Telefonnummern für Software-Service und -unterstützung 211 Telnet konfigurieren 195 maximale Anzahl an Sitzungen 57, 195 zugreifen 57 Zugriff 195 Telnet-CLI-Port festlegen 57, 181 Telnet-Einstellungen konfigurieren 57 Testen SMTP 57 Testereignisse generieren 129 Tools IPMItool 149

# U

Übersicht Download Service Data 32 SSL 92 Überwachungsbefehle 154 Uhrzeit festlegen 55, 206 UID-Suchattribut LDAP-Server 57, 177 United States FCC Class A notice 217 Unterstützung erhalten 209 Unterstützung für internationale Tastatur in Fernsteuerung 112 Unterstützungswebseite, benutzerdefiniert 211 USB konfigurieren 57, 173

#### V

Verunreinigung, Staubpartikel und Gase 215 Verwalten Aktivierungsschlüssel 58, 176 Benutzer 56, 197 DDNS 56, 171 Features on Demand 58, 176 FoD 58, 176 MAC-Adresse 56, 174 SNMPv1-Communitys 56, 185 Verwenden ActiveX-Client 39 Java-Client 39 Video Viewer absolute Maussteuerung 113 Ansichtsmodi 110 Anzeigenerfassung 109 beenden 121 Befehle für Stromversorgung und Neustart 115 Einzelcursormodus 114 Leistungsstatistiken 115 Mausunterstützung 113 relative Maussteuerung 113 relative Maussteuerung für Linux (Linux-Standardbeschleunigung) 113 Tastaturdurchgriffsmodus 113 Unterstützung für internationale Tastatur 112 Videofarbmodus 110, 111 Videofarbmodus in Fernsteuerung 110 Virtual Light Path 11 Virtual Media Session beenden 121 ferner Datenträger 119 Laufwerkzuordnung aufheben 120 Laufwerkzuordnung festlegen 120 Start 120 Von der IMM2-Sitzung abmelden 20 Voraussetzungen Betriebssystem 4 Web-Browser 4 Voraussetzungen, Web-Browser 4 Vorkonfiguriert LDAP-Server 57, 177 Vorschriften zur Telekommunikation 217

## W

Webschnittstelle Anmeldung an der Webschnittstelle 10
Webschnittstelle öffnen und verwenden 7
Websitzungseinstellungen 17
Wichtige Hinweise 214
Wiederherstellungsstatus anzeigen IMM2 58
Wiederherstellungsstatusansicht IMM2 58

## Ζ

Zertifikatsverwaltung CIM over HTTPS 58, 191, 192 HTTPS-Server 58, 191, 192 LDAP 58, 191, 192 SSH-Server 58, 190 Zielname, Server LDAP 57, 177 Zielname des Servers LDAP 57, 177 Zugängliche Dokumentation 216 Zugreifen Fernsteuerung 120 Telnet 57 Zugriff Telnet 195 Zurücksetzen IMM 208 IMM2 58



Teilenummer: 47C9125

(1P) P/N: 47C9125

