



Integriertes Managementmodul II
Benutzerhandbuch





Integriertes Managementmodul II
Benutzerhandbuch

Fünfte Ausgabe (Mai 2014)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Integrated Managementmodul II, User's Guide,
IBM Teilenummer 00FH349,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2014

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
Mai 2014

Inhaltsverzeichnis

Tabellen	vii
-----------------	------------

Kapitel 1. Einführung **1**

Funktionen von "IMM2 Basic Level", "IMM2 Standard Level" und "IMM2 Advanced Level"	2
Funktionen von "IMM2 Basic Level"	3
Funktionen von "IMM2 Standard Level"	3
Funktionen von "IMM2 Advanced Level"	3
Funktionsverbesserungen beim IMM2	3
Upgrade für IMM2 durchführen	4
IMM2 zusammen mit dem erweiterten BladeCenter-Managementmodul verwenden	4
Voraussetzungen für Web-Browser und Betriebssystem	4
Bemerkungen in diesem Buch	7

Kapitel 2. IMM2-Webschnittstelle öffnen und verwenden **9**

Zugriff auf die IMM2-Webschnittstelle	9
IMM2-Netzverbindung mit dem Konfigurationsdienstprogramm der Server-Firmware für IBM System x einrichten	10
Am IMM2 anmelden	12
Beschreibungen der IMM2-Aktionen	13

Kapitel 3. Übersicht über die IMM2-Webbenutzerschnittstelle **21**

Websitzungseinstellungen	21
Page Auto Refresh	21
Trespass Message	23
Abmelden	24
Registerkarte "System Status"	25
Registerkarte "Events" (Ereignisse)	32
Event Log (Ereignisprotokoll)	32
Event Recipients (Ereignisempfänger)	35
Registerkarte "Service and Support"	37
Option "Problems"	37
Option "Settings"	40
Firewalls und Proxy-Server vorbereiten	43
Option "Download Service Data"	44
Registerkarte "Server Management"	45
Server Firmware (Server-Firmware)	46
Remote Control (Fernsteuerung)	51
Server Properties (Servereigenschaften)	56
Server Power Actions (Serverstromversorgungsaktionen)	61
Cooling Devices (Kühlungseinheiten)	61
Power Modules (Stromversorgungsmodule)	62
Option "Local Storage"	64
Memory (Speicher)	64
Processors (Prozessoren)	66
Adapter	67
Server Timeouts (Serverzeitlimits)	67
PXE Network Boot (PXE-Netzboot)	68

Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige)	68
Stromverbrauchssteuerung	69
Skalierbarer Komplex	69
Registerkarte "IMM Management" (IMM-Verwaltung)	70

Kapitel 4. IMM2 konfigurieren **71**

Serverzeitlimits festlegen	74
Einstellungen für die automatisierte Hochstufung der IMM2-Firmware ändern	76
Datum und Uhrzeit für IMM2 einstellen	77
Einstellungen für den seriellen Anschluss konfigurieren	79
Benutzerkonten konfigurieren	80
Benutzerkonten	81
Gruppenprofile	84
Globale Anmeldeeinstellungen konfigurieren	85
Allgemeine Einstellungen	85
Einstellungen für die Kontensicherheitsrichtlinie	87
Netzprotokolle konfigurieren	90
Ethernet-Einstellungen konfigurieren	91
Einstellungen für SNMP-Alerts konfigurieren	93
DNS konfigurieren	95
DDNS konfigurieren	96
SMTP konfigurieren	96
LDAP konfigurieren	97
Telnet konfigurieren	103
USB konfigurieren	103
Portzuordnungen konfigurieren	104
Sicherheitseinstellungen konfigurieren	105
HTTPS-Protokoll konfigurieren	106
CIM-over-HTTPS-Protokoll konfigurieren	107
Protokoll für LDAP-Client konfigurieren	108
Secure Shell-Server konfigurieren	110
Übersicht über SSL	111
Handhabung von SSL-Zertifikaten	111
Verwaltung von SSL-Zertifikaten	112
Verschlüsselungsverwaltung konfigurieren	113
IMM-Konfiguration wiederherstellen und ändern	115
IMM2 erneut starten	116
IMM2 auf die werkseitigen Voreinstellungen zurücksetzen	117
Aktivierungsschlüsselverwaltung	118

Kapitel 5. Serverstatus überwachen **119**

Systemstatus anzeigen	119
Systeminformationen anzeigen	121
Serverzustand anzeigen	122
Hardwarezustand anzeigen	123

Kapitel 6. IMM2-Tasks ausführen . . . **127**

Stromversorgungsstatus des Servers steuern	128
Remote-Presence- und Fernsteuerungsfunktionen	130

IMM2-Firmware und Java- oder ActiveX-Applet aktualisieren.	130
Remote-Presence-Funktion aktivieren	131
Anzeigenerfassung per Fernsteuerung	131
Modi der Fernsteuerung im Video Viewer.	132
Fernsteuerung des Videofarbmodus	133
Tastaturunterstützung per Fernsteuerung	133
Mausunterstützung per Fernsteuerung	135
Fernsteuerung der Stromversorgung.	137
Leistungsstatistiken anzeigen	137
Remote Desktop Protocol starten	137
Beschreibung der Funktion "Anklopfen"	137
Ferner Datenträger	141
PXE-Netzboot einrichten	143
Server-Firmware aktualisieren.	144
Systemereignisse verwalten.	149
Ereignisprotokoll verwalten	149
Benachrichtigung zu Systemereignissen.	151
Informationen für Service und Support erfassen	157
Daten der letzten Betriebssystem-Fehleranzeige er- fassen	158
Serverstromversorgung verwalten	159
Stromversorgung und gesamte Stromversorgung des Systems steuern	159
Aktuell installierte Netzteile anzeigen	164
Stromversorgungskapazität anzeigen	165
Verlaufsprotokoll zum Stromverbrauch.	165
Skalierbaren Komplex verwalten	166
Partition erstellen	167
Modus zum Ändern einer Partition	169
Modus zum Löschen einer Partition.	170
Partitionsfehler	171
Konfiguration des lokalen Speichers anzeigen	171
Informationen zu physischen Ressourcen anzei- gen.	172
Adapterinformationen anzeigen	177

Kapitel 7. Features on Demand. . . . 179

Aktivierungsschlüssel installieren.	179
Aktivierungsschlüssel entfernen	182
Aktivierungsschlüssel exportieren	183

Kapitel 8. Befehlszeilenschnittstelle 185

IMM2 mit IPMI verwalten	185
IPMItool verwenden	185
Zugriff auf die Befehlszeilenschnittstelle	186
Anmeldung an der Befehlszeilenschnittstelle	186
Seriell-zu-Telnet- oder -SSH-Umleitung konfigurie- ren	186
Befehlssyntax	187
Merkmale und Einschränkungen	187
Alphabetische Befehlsliste	188
Dienstprogrammbeefhle	190
Befehl "exit".	190
Befehl "help"	190
Befehl "history".	190
Überwachungsbefehle	191
Befehl "adapter"	191
Befehl "clearlog"	193
Befehl "fans".	193

Befehl "ffdc".	193
Befehl "led"	194
Befehl "readlog"	196
Befehl "storage".	197
Befehl "syshealth"	201
Befehl "temps"	201
Befehl "volts"	202
Befehl "vpd".	202
Steuerbefehle für Serverstromversorgung und -neu- start	203
Befehl "fuelg"	203
Befehl "power"	204
Befehl "pxeboot"	207
Befehl "reset"	207
Befehl zur seriellen Umleitung	208
Befehl "console"	208
Konfigurationsbefehle	208
Befehl "accseccfg"	209
Befehl "alertcfg"	211
Befehl "asu"	211
Befehl "autopromo"	215
Befehl "backup"	216
Befehl "cryptomode"	217
Befehl "dhcpcfg"	218
Befehl "dns"	219
Befehl "eththousb"	220
Befehl "gprofile"	221
Befehl "ifconfig"	222
Befehl "keycfg"	225
Befehl "ldap"	226
Befehl "ntp"	228
Befehl "passwordcfg"	228
Befehl "ports"	229
Befehl "portcfg".	230
Befehl "portcontrol"	231
Befehl "restore".	232
Befehl "restoredefaults"	232
Befehl "scale"	233
Befehl "set"	243
Befehl "smtp"	243
Befehl "snmp"	244
Befehl "snmpalerts"	247
Befehl "srcfg"	248
Befehl "sshcfcg"	249
Befehl "ssl"	250
Befehl "sslcfcg"	251
Befehl "telnetcfg"	254
Befehl "tls"	254
Befehl "thermal"	255
Befehl "timeouts"	255
Befehl "usbeth"	256
Befehl "users"	256
IMM2-Steuerbefehle	260
Befehl "alertentries"	260
Befehl "batch"	263
Befehl "clearcfg"	264
Befehl "clock"	264
Befehl "identify"	265
Befehl "info".	265
Befehl "resetsp".	266
Befehl "spreset".	266

Service Advisor-Befehle	266
Befehl "autoftp".	266
Befehl "chconfig".	267
Befehl "chlog".	269
Befehl "chmanual".	269
Befehl "events".	270
Befehl "sdemail".	270

Anhang A. Hilfe und technische Unterstützung anfordern 273

Bevor Sie sich an den Kundendienst wenden.	273
Dokumentation verwenden.	274
Hilfe und Informationen über das World Wide Web anfordern.	274
Vorgehensweise zum Senden von DSA-Daten an IBM	274
Personalisierte Unterstützungswebseite erstellen	275
Software-Service und -unterstützung	275
Hardware-Service und -unterstützung	275
IBM Produktservice in Taiwan.	276

Anhang B. Bemerkungen 277

Marken	277
Wichtige Hinweise	278

Verunreinigung durch Staubpartikel	279
Dokumentationsformat	280
Gesetzliche Bestimmungen zur Telekommunikation	281
Hinweise zur elektromagnetischen Verträglichkeit	281
Federal Communications Commission (FCC) statement.	281
Industry Canada Class A emission compliance statement.	281
Avis de conformité à la réglementation d'Industrie Canada	281
Australia and New Zealand Class A statement	281
European Union EMC Directive conformance statement.	282
Deutschland - Hinweis zur Klasse A	282
Japan VCCI Class A statement.	283
Korea Communications Commission (KCC) statement.	283
Russia Electromagnetic Interference (EMI) Class A statement	284
People's Republic of China Class A electronic emission statement	284
Taiwan Class A compliance statement	284

Index 285

Tabellen

1. IMM2-Aktionen	14	7. Stromversorgungsaktionen und Beschreibungen	129
2. Stromversorgungsstatus und Betriebsstatus des Servers	28	8. Partitionsfehlerbedingungen	171
3. Erforderliche Internetverbindungen	44	9. Befehle vom Typ "power"	204
4. Werte für Sicherheitseinstellungsrichtlinie	88	10. ASU-Befehle	212
5. Berechtigungsbits	101	11. Transaktionsbefehle	215
6. Systemstatusbeschreibungen	120	12. Grenzwerte für Staubpartikel und Gase	280

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 des Servers 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® BladeCenter ausführbar.
- Embedded Dynamic System Analysis (DSA).
- Ferne Konfiguration mit dem Dienstprogramm für erweiterte Einstellungen (Advanced Settings Utility - ASU). Diese Funktion ist nicht auf Blade-Servern von IBM BladeCenter ausführbar.
- 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® Server-Firmware ist die IBM Implementierung der UEFI (Unified Extensible Firmware Interface). Sie 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**.
3. 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 Funktionalitätsversionen "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 Funktionen von "IMM2 Basic Level" aufgeführt:

Funktionen von "IMM2 Basic Level"

Im Folgenden sind die Funktionen von "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 Alertaussagen 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 von "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 -Farbtiefe
- Remote-Presence-Client von ActiveX
- Auf USB 2.0 aktualisierte Ethernet-über-USB-Schnittstelle
- Syslog-Alertausgabe
- Nach Konfigurationsänderungen kein Zurücksetzen des IMM2 erforderlich

Upgrade für IMM2 durchführen

Wenn Ihr IBM Server über die IMM2-Firmwarefunktionalitätsversion "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 179.

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.

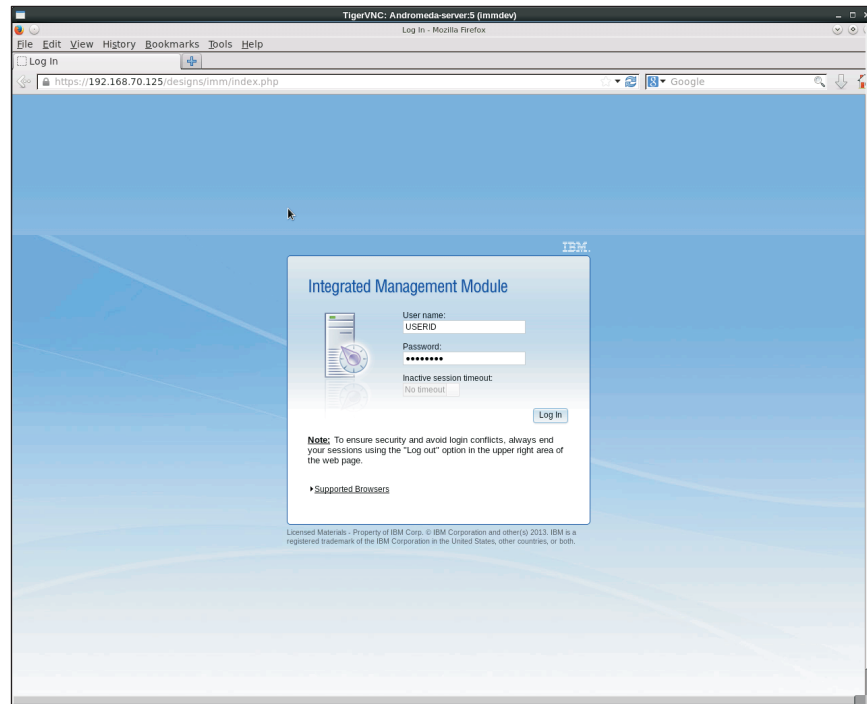
Auf IBM BladeCenter-Blade-Servern gibt es keinen externen Netzzugriff auf das IMM2 und zur fernen Verwaltung von Blade-Servern von IBM BladeCenter muss das erweiterte Managementmodul verwendet werden. Das IMM2 ersetzt die Funktionalität des BMC und der cKVM-Erweiterungskarte (cKVM - Concurrent Keyboard,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

Voraussetzungen für Web-Browser und Betriebssystem

Für die IMM2-Webschnittstelle sind das Java™-Plug-in ab Version 1.7 (für die Remote-Presence-Funktion) und einer der folgenden Web-Browser erforderlich:

- Microsoft Internet Explorer, Versionen 8 bis 10
- Mozilla Firefox, Versionen 3.6 bis 20
- Chrome, Versionen 13 bis 26

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. In der folgenden Abbildung ist die IMM2-Anmeldeanzeige dargestellt.



Je nachdem, welche Version der Firmware auf dem IMM2 verwendet wird, kann sich die Web-Browser-Unterstützung von den in diesem Abschnitt aufgeführten Browsern unterscheiden. Wenn Sie die Liste unterstützter Browser für die Firmware anzeigen möchten, die derzeit auf dem IMM2 verwendet wird, klicken Sie auf der IMM-Anmeldeseite auf die Menüliste **Supported Browsers** (wie in der folgenden Abbildung dargestellt).

Integrated Management Module



User name:

Password:

Inactive session timeout:
20 minutes ▼

Log In

Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

▼Supported Browsers

The Firefox browser is recommended for JAWs users.
The IMM2 web interface works with these browsers:

- Internet Explorer 8-10
- Firefox 3.6-20
- Chrome 13-26

The IMM2 Remote Control function works with these client operating systems:

- SLES11
- RHEL5, RHEL6
- Windows XP
- Windows Vista
- Windows 2008
- Windows 7, 8
- Windows 2012

Für eine höhere Sicherheit werden bei der Verwendung von HTTPS nur noch hohe Verschlüsselungsgrade unterstützt. Bei der Verwendung von HTTPS muss die Kombination aus Ihrem Clientbetriebssystem und Ihrem Browser eine der folgenden Cipher-Suites unterstützen:

- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA
- DHE-RSA-CAMELLIA256-SHA
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- DHE-RSA-SEED-SHA
- DHE-RSA-CAMELLIA128-SHA
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA

- CAMELLIA256-SHA
- CAMELLIA128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- SEED-SHA
- RC4-SHA

Die Fernbedienungsfunktion des IMM2 funktioniert mit den folgenden Clientbetriebssystemen:

- SUSE Linux Enterprise Server 11 (SLES11)
- Red Hat Enterprise Linux Enterprise 5 (RHEL5)
- Red Hat Enterprise Linux Enterprise 6 (RHEL6)
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 2008
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 2012

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.

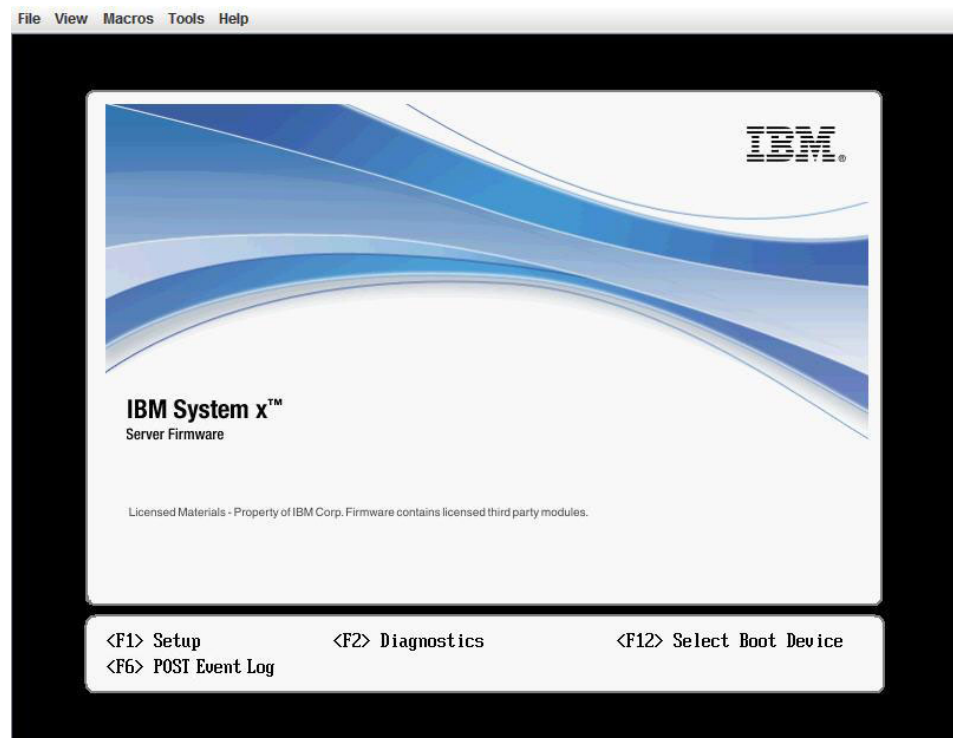
Anmerkung: Möglicherweise verfügt Ihr Server über keinen dedizierten Systemmanagement-Netzanschluss. Wenn auf Ihrer Hardware kein dedizierter Netzanschluss vorhanden ist, ist die Einstellung *shared* (freigegeben) die einzig verfügbare IMM2-Einstellung.

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:

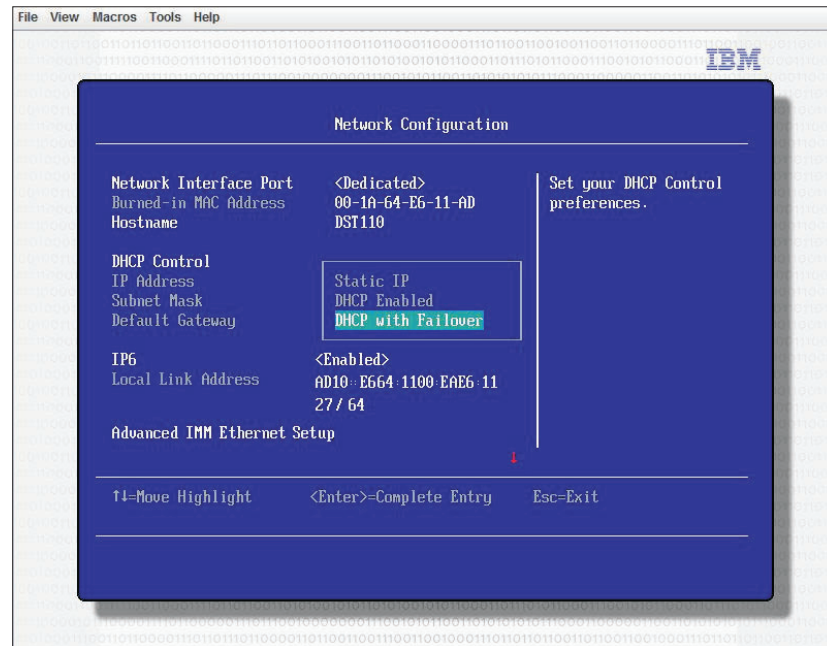
1. Schalten Sie den Server ein. Die Eingangsanzeige der Server-Firmware für IBM System x wird angezeigt.

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 (DHCP mit Funktionsübernahme; dies ist die Standardeinstellung)



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 Netzananschluss hat) oder eine gemeinsam genutzte IMM2-Netzverbindung auszuwählen.

Anmerkungen:

- Möglicherweise verfügt Ihr Server über keinen dedizierten Systemmanagement-Netzananschluss. Wenn auf Ihrer Hardware kein dedizierter Netzananschluss vorhanden ist, ist die Einstellung *Shared* (Gemeinsam genutzt) die einzige verfügbare IMM2-Einstellung. Wählen Sie in 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.

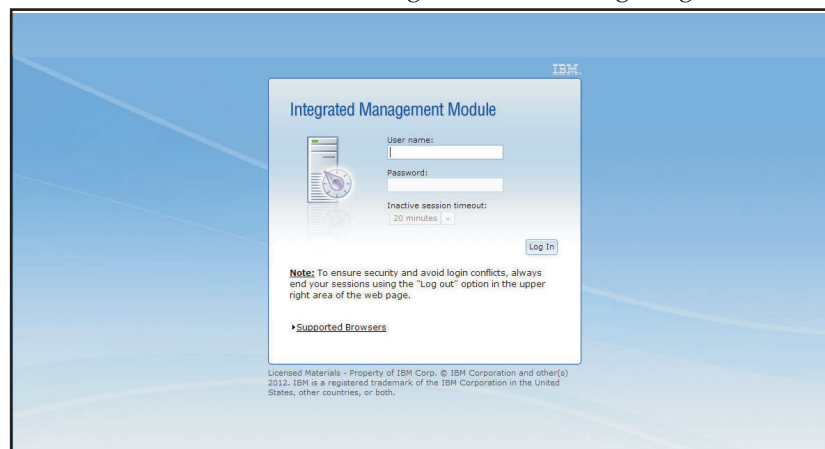
Am IMM2 anmelden

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 IMM2-Anmeldefenster 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 Anmeldefenster ist in der folgenden Abbildung dargestellt.

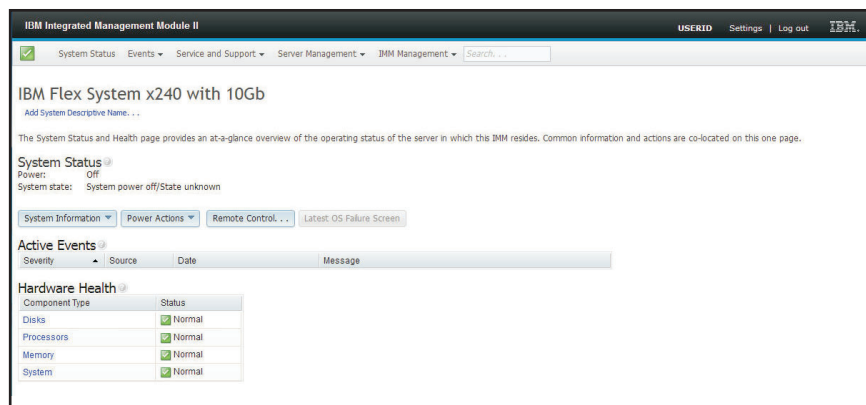


3. Klicken Sie auf **Log in** (Anmelden), um die Sitzung zu starten. Im Browser wird die Seite "System Status" (Systemstatus) geöffnet, wie in der folgenden Abbildung dargestellt. Auf dieser Seite erhalten Sie einen schnellen Überblick über den Serverstatus und eine Zusammenfassung des Serverzustands.

Anmerkung: Wenn Sie das Betriebssystem booten, während Sie sich auf der grafischen Benutzeroberfläche des IMM2 befinden, und die Nachricht „Booting OS or in unsupported OS“ (Betriebssystem wird gebootet oder es wird ein nicht unterstütztes Betriebssystem gebootet) unter **System Status** → **System State** (Systemstatus > Systemzustand) angezeigt wird, inaktivieren Sie die Firewall von Windows 2008 oder geben Sie den folgenden Befehl in die Konsole von Windows 2008 ein. Dies kann sich auch auf Funktionen zur Erfassung von Systemabsturzanzeigen auswirken.

```
netsh firewall set icmpsetting type=8 mode=ENABLE
```

Standardmäßig wird das icmp-Paket durch die Windows-Firewall geblockt. Daraufhin wechselt die grafische Benutzeroberfläche des IMM2 in den Status „OS booted“ (Betriebssystem gebootet), nachdem Sie die Einstellung wie oben angezeigt sowohl auf der Web- als auch auf der Befehlszeilenschnittstelle geändert haben.



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 trespass-Nachricht konfigurieren und sich über die Option **Log out** (Abmeldung) von der Webschnittstelle des IMM2 abmelden, wie in der folgenden Abbildung dargestellt. Unter der Titelleiste befinden sich Registerkarten, über die Sie Zugang zu unterschiedlichen in Tabelle 1 auf Seite 14 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 25 und „Systemstatus anzeigen“ auf Seite 119 finden Sie weitere Informationen.
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 konfiguriert wurden. Sie können Ereignisse im Ereignisprotokoll sortieren und filtern und sie in eine Textdatei exportieren. Weitere Informationen finden Sie in den Abschnitten „Registerkarte "Events" (Ereignisse)“ auf Seite 32 und „Ereignisprotokoll verwalten“ auf Seite 149.
	Event Recipients (Ereignisempfänger)	Auf der Seite "Event Recipients" können Sie festlegen, wer bei Systemereignissen benachrichtigt werden soll. Sie können jeden Empfänger konfigurieren und Einstellungen 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 35 und „Benachrichtigung zu Systemereignissen“ auf Seite 151.
Service and Support (Service und Unterstützung)	Problems (Fehler)	Auf der Seite "Problems" können Sie aktuelle nicht behobene Fehler anzeigen, die vom Support Center behoben werden können. Sie können außerdem den Status jedes Fehlers im Bezug auf dessen Auflösung anzeigen. Weitere Informationen finden Sie im Abschnitt „Option "Problems"“ auf Seite 37.
	Settings (Einstellungen)	Über die Seite "Settings" wird Ihr Server für die Überwachung von und Berichterstellung zu Serviceereignissen konfiguriert. Weitere Informationen finden Sie im Abschnitt „Option "Settings"“ auf Seite 40.
	Download Service Data (Servicedaten herunterladen)	Die Seite "Download Service Data" erstellt eine komprimierte Datei mit Informationen, die vom IBM Support dazu verwendet werden kann, Ihnen zu helfen. Weitere Informationen finden Sie in den Abschnitten „Option "Download Service Data"“ auf Seite 44 und „Informationen für Service und Support erfassen“ auf Seite 157.

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. Weitere Informationen finden Sie in den Abschnitten „Server Firmware (Server-Firmware)“ auf Seite 46 und „Server-Firmware aktualisieren“ auf Seite 144.
	Remote Control (Fernsteuerung)	Über die Seite "Remote Control" können Sie den Server auf Betriebssystemebene steuern. Sie bietet den Zugriff auf die Funktionalität für ferne Datenträger und ferne Konsolen. Sie können die Serverkonsole über Ihren Computer anzeigen und bedienen und eines der Plattenlaufwerke des Computers, z. B. das CD-ROM-Laufwerk oder das Diskettenlaufwerk, an den Server anhängen. Wenn Sie einen Datenträger 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 51 und „Remote-Presence- und Fernsteuerungsfunktionen“ auf Seite 130.
	Server Properties (Servereigenschaften)	Die Seite "Server Properties" ermöglicht den Zugriff auf unterschiedliche Eigenschaften, Statusbedingungen und Einstellungen Ihres Servers. Die folgenden Optionen sind auf der Seite "Server Properties" verfügbar: • Auf der Registerkarte "General Settings" werden Informationen angezeigt, die das System für Vorgänge sowie für Supportmitarbeiter kenntlich macht. • Auf der Registerkarte "LEDs" wird der Status aller Systemanzeigen angezeigt. Über sie können Sie auch den Zustand der Positionsanzeige ändern. • Auf der Registerkarte "Hardware Information" werden elementare Produktdaten (VPD - Vital Product Data) zum Server angezeigt. Das IMM2 erfasst Serverinformationen, Serverkomponentenangaben und Netzhardwareinformationen. • Auf der Registerkarte "Environmentals" werden Informationen zur Spannung und Temperatur für den Server und seine Komponenten angezeigt. • 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. Weitere Informationen finden Sie im Abschnitt „Server Properties (Servereigenschaften)“ auf Seite 56.
	Server Power Actions (Serverstromversorgungsaktionen)	Über die Seite "Server Power Actions" kann die Stromversorgung des Servers vollständig ferngesteuert werden. Dies umfasst Aktionen zum Einschalten, Ausschalten und für den Neustart. Weitere Informationen finden Sie in den Abschnitten „Server Power Actions (Serverstromversorgungsaktionen)“ auf Seite 61 und „Stromversorgungsstatus des Servers steuern“ auf Seite 128.
	Cooling Devices (Kühleinheiten)	Auf der Seite "Cooling Devices" werden aktuelle Geschwindigkeiten und Status für Lüfter im Server angezeigt. Weitere Informationen finden Sie im Abschnitt „Cooling Devices (Kühlungseinheiten)“ auf Seite 61.
	Power Modules (Stromversorgungsmodule)	Auf der Seite "Power Modules" werden Stromversorgungsmodule im System samt Status und Belastbarkeit angezeigt. Weitere Informationen finden Sie im Abschnitt „Power Modules (Stromversorgungsmodule)“ auf Seite 62.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
Server Management (Serververwaltung) (Fortsetzung)	Memory (Speicher)	Auf der Seite "Memory" werden die im System verfügbaren Speichermodule sowie deren Status, Typ und Kapazität angezeigt. Sie können auf einen Modulnamen klicken, 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 finden Sie im Abschnitt „Memory (Speicher)“ auf Seite 64.
	Local Storage (Lokaler Speicher)	Auf der Seite "Local Storage" wird die physische Struktur und die Speicherkonfiguration einer Speichereinheit angezeigt. Weitere Informationen finden Sie in den Abschnitten „Option "Local Storage"“ auf Seite 64 und „Konfiguration des lokalen Speichers anzeigen“ auf Seite 171.
	Processors (Prozessoren)	Auf der Seite für CPUs werden die Mikroprozessoren im System samt deren Status und Taktgeschwindigkeit angezeigt. Sie können auf den Namen eines Mikroprozessors klicken, um Ereignisse und weitere Hardwareinformationen für den Mikroprozessor anzuzeigen. Weitere Informationen finden Sie im Abschnitt „Processors (Prozessoren)“ auf Seite 66.
	Adapters (Adapter)	Auf der Seite "Adapters" werden die Hardware, die Firmware und Netzadapterinformationen zu im Server installierten Adaptern angezeigt. Weitere Informationen finden Sie in den Abschnitten „Adapter“ auf Seite 67 und „Adapterinformationen anzeigen“ auf Seite 177.
	Server Timeouts (Serverzeitlimits)	Über die Seite "Server Timeouts" können Sie zur Erkennung von und zum Wiederherstellen nach aufgetretenen Blockierungen des Servers Startzeitlimits für den Server verwalten. Weitere Informationen finden Sie in den Abschnitten „Server Timeouts (Serverzeitlimits)“ auf Seite 67 und „Serverzeitlimits festlegen“ auf Seite 74.
	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 geändert, wenn für den Host kein privilegierter Zugriffsschutz (Privileged Access Protection, PAP) festgelegt ist. Weitere Informationen finden Sie in den Abschnitten „PXE Network Boot (PXE-Netzboot)“ auf Seite 68 und „PXE-Netzboot einrichten“ auf Seite 143.
	Latest OS Failure Screen (Letzte Betriebssystem-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 Betriebssystems aktiviert sein. Weitere Informationen finden Sie in den Abschnitten „Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige)“ auf Seite 68 und „Daten der letzten Betriebssystem-Fehleranzeige erfassen“ auf Seite 158.
	Power Management (Stromverbrauchssteuerung)	Über die Seite "Server Power Management" können Sie die Richtlinien zum Stromverbrauch und die Hardware verwalten. Hier befindet sich auch das Verlaufsprotokoll zur Stromverbrauchsmenge des Servers. Weitere Informationen finden Sie in den Abschnitten „Stromverbrauchssteuerung“ auf Seite 69 und „Serverstromversorgung verwalten“ auf Seite 159.
	Scalable Complex (Skalierbarer Komplex)	Die Seite "Scalable Complex" ermöglicht Ihnen das Anzeigen und Verwalten eines skalierbaren Komplexes. Weitere Informationen finden Sie in den Abschnitten „Skalierbarer Komplex“ auf Seite 69 und „Skalierbaren Komplex verwalten“ auf Seite 166.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
IMM Management (IMM-Verwaltung) (Fortsetzung auf der nächsten Seite)	IMM Properties (IMM-Eigenschaften)	Die Seite "IMM Properties" ermöglicht den Zugriff auf unterschiedliche Eigenschaften und Einstellungen Ihres IMM2. Die folgenden Optionen sind auf der Seite "IMM Properties" verfügbar: • Die Registerkarte "Firmware" enthält einen Link zum Abschnitt "Server Firmware" des Bereichs "Server Management". Über diese Registerkarte können Sie außerdem die automatisierte Hochstufung der Sicherungsfirmware für das IMM2 aktivieren. • Auf der Registerkarte "IMM Date and Time Settings" können Sie die Einstellung für Datum und Uhrzeit beim IMM2 anzeigen und konfigurieren. • Auf der Registerkarte "Serial Port" werden die IMM2-Einstellungen für den seriellen Anschluss konfiguriert. Diese Einstellungen schließen die von der Umleitungsfunktion des seriellen Anschlusses verwendete Baudrate des seriellen Anschlusses sowie die Schlüsselfolge zum Wechseln zwischen dem Modus zur seriellen Umleitung und dem CLI-Modus ein. Weitere Informationen finden Sie in Kapitel 4, „IMM2 konfigurieren“, auf Seite 71.
	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 80.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
IMM Management (IMM-Verwaltung) (Fortsetzung auf der nächsten Seite)	Network (Netz)	Die Seite "Network Protocol Properties" (Netzprotokolleigenschaften) ermöglicht den Zugriff auf Netzwerkeigenschaften, Statusangaben und Einstellungen Ihres IMM2: • Auf der Registerkarte "Ethernet" können Sie verwalten, wie das IMM2 über Ethernet kommuniziert. • Auf der Registerkarte "SNMP" werden die SNMPv1- und SNMPv3-Agenten konfiguriert. • Auf der Registerkarte "DNS" werden die DNS-Server konfiguriert, mit denen das IMM2 interagiert. • Auf der Registerkarte "DDNS" wird das Dynamic Domain Name System für das IMM2 aktiviert oder inaktiviert und konfiguriert. • Auf der Registerkarte "SMTP" werden SMTP-Serverinformationen für Alerts konfiguriert, die per E-Mail gesendet werden. • Auf der Registerkarte "LDAP" wird die Benutzerauthentifizierung für die Verwendung mit einem oder mehreren LDAP-Servern konfiguriert. • Auf der Registerkarte "Telnet" wird der Telnet-Zugriff auf das IMM2 verwaltet. • Über die Registerkarte "USB" wird die USB-Schnittstelle 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). • Auf der Registerkarte "Port Assignments" können Sie die Portnummern ändern, die von einigen Services auf dem IMM2 verwendet werden. Weitere Informationen finden Sie im Abschnitt „Netzprotokolle konfigurieren“ auf Seite 90.
	Security (Sicherheit)	Die Seite "IMM Security" ermöglicht den Zugriff auf Sicherheitseigenschaften, Statusangaben und Einstellungen Ihres IMM2: • Auf der Registerkarte "HTTPS Server" können Sie den HTTPS-Server aktivieren oder inaktivieren und seine Zertifikate verwalten. • Auf der Registerkarte "CIM Over HTTPS" können Sie CIM over HTTPS aktivieren oder inaktivieren und die zugehörigen Zertifikate verwalten. • Auf der Registerkarte "LDAP Client" können Sie die LDAP-Sicherheit aktivieren oder inaktivieren und ihre Zertifikate verwalten. • Auf der Registerkarte "SSH Server" können Sie den SSH-Server aktivieren oder inaktivieren und seine Zertifikate verwalten. • Die Registerkarte "Cryptography Management" (Verschlüsselungsverwaltung) ermöglicht es Ihnen, die IMM2-Firmware so zu konfigurieren, dass sie den Anforderungen für SP 800-131A entspricht. Weitere Informationen finden Sie im Abschnitt „Sicherheitseinstellungen konfigurieren“ auf Seite 105.
	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 115.

Tabelle 1. IMM2-Aktionen (Forts.)

Registerkarte	Auswahl	Beschreibung
IMM Management (IMM-Verwaltung) (Fortsetzung)	Restart IMM (IMM erneut starten)	Über die Seite "Restart IMM" können Sie das IMM2 zurücksetzen. Weitere Informationen finden Sie im Abschnitt „IMM2 erneut starten“ auf Seite 116.
	Reset IMM to factory defaults... (IMM auf werkseitige Voreinstellungen zurücksetzen)	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 117. Achtung: Wenn Sie auf Reset IMM to factory defaults... klicken, gehen alle Änderungen, die Sie am IMM2 vorgenommen haben, verloren.
	Activation Key Management (Aktivierungs- schlüsselver- waltung)	Auf der Seite "Activation Key Management" können Sie Aktivierungsschlüssel für optionale FoD-Funktionen (Features on Demand) des IMM2 oder des Servers verwalten. Weitere Informationen finden Sie im Abschnitt „Aktivierungsschlüsselverwaltung“ auf Seite 118.

Kapitel 3. Übersicht über die IMM2-Webbenutzerschnittstelle

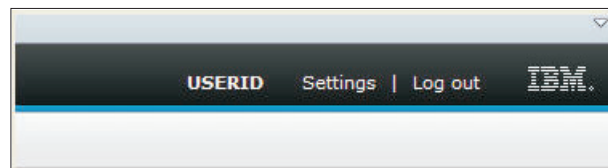
Dieses Kapitel enthält eine Übersicht der Funktionen der IMM2-Webbenutzerschnittstelle und ihre Verwendung.

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.

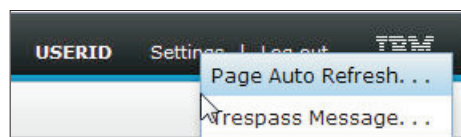
Websitzungseinstellungen

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.

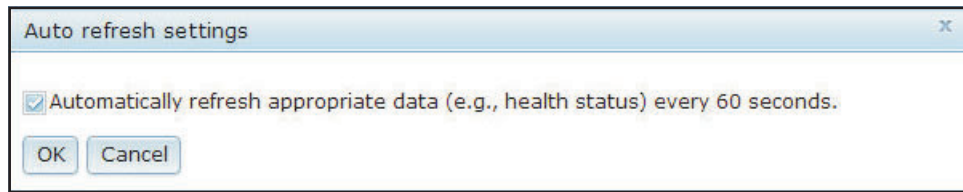


Klicken Sie auf die Menüoption **Settings** (Einstellungen). Die folgenden Menüoptionen werden angezeigt:



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.



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:

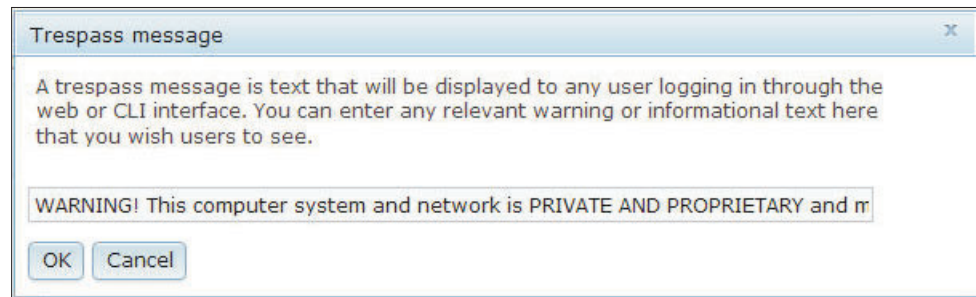
- Wenn Sie über Ihren Web-Browser zu einer Webseite wechseln, die automatisch aktualisiert wird, wird Ihre Websitzung möglicherweise nicht automatisch durch das Inaktivitätszeitlimit beendet.
- Wenn Sie über die Seite mit den Optionen für die Fernsteuerung unter "Server Management" eine Anforderung an 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.

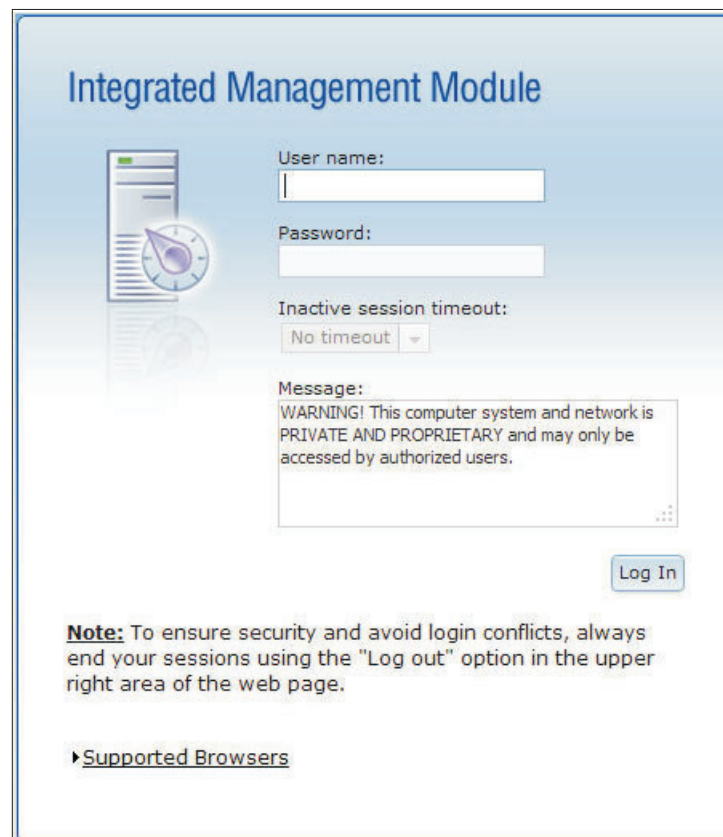
Trespass Message

Verwenden Sie die Option **Trespass Message** 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**.



The screenshot shows a dialog box titled "Trespass message" with a close button (X) in the top right corner. Inside the dialog, there is a text area containing the message: "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." Below this text area is a text input field containing the text: "WARNING! This computer system and network is PRIVATE AND PROPRIETARY and m". At the bottom of the dialog are two buttons: "OK" and "Cancel".

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

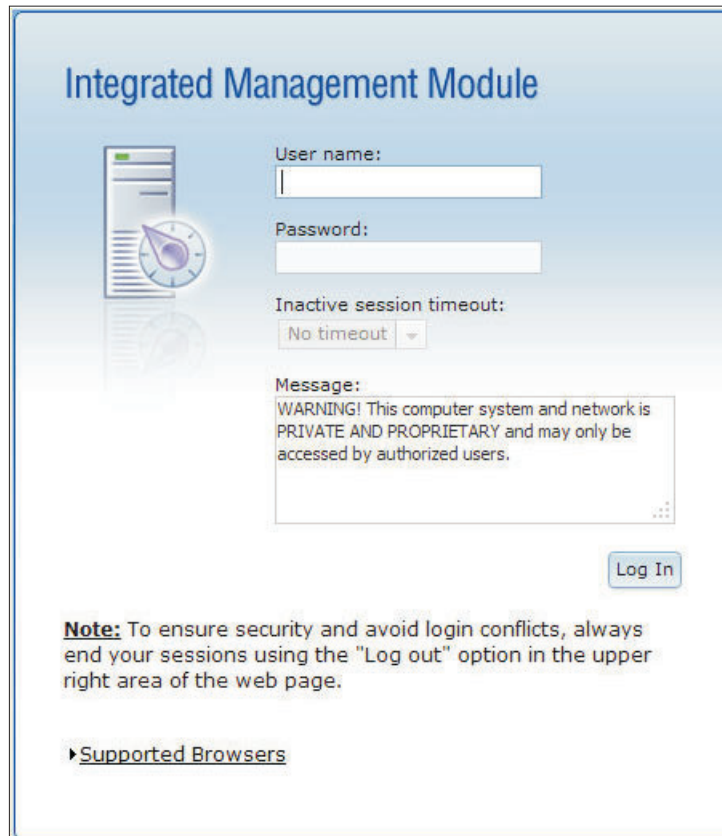


The screenshot shows the "Integrated Management Module" login page. On the left is a logo featuring a computer monitor and a clock. To the right of the logo are the login fields: "User name:" with a text input field, "Password:" with a text input field, and "Inactive session timeout:" with a dropdown menu showing "No timeout". Below these fields is a "Message:" section with a text area displaying the warning: "WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users." To the right of the message text area is a "Log In" button. At the bottom of the page, there is a "Note:" stating: "To ensure security and avoid login conflicts, always end your sessions using the 'Log out' option in the upper right area of the web page." Below the note is a link: "Supported Browsers".

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 Anmeldefenster wird angezeigt.



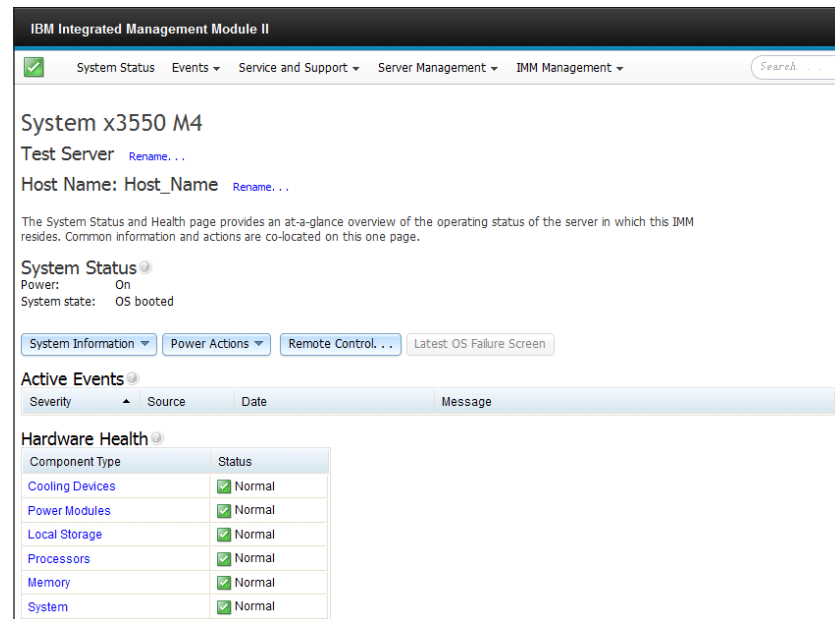
The screenshot shows the login interface for the Integrated Management Module. It features a blue header with the title "Integrated Management Module". On the left is a graphic of a server rack with a clock icon. The login form includes fields for "User name:" and "Password:", followed by an "Inactive session timeout:" dropdown menu set to "No timeout". A "Message:" box contains a warning: "WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users." A "Log In" button is located to the right of the message box. Below the login fields is a "Note:" stating: "To ensure security and avoid login conflicts, always end your sessions using the 'Log out' option in the upper right area of the web page." At the bottom, there is a link for "Supported Browsers".

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 möglicherweise nicht automatisch aufgrund von Inaktivität geschlossen.

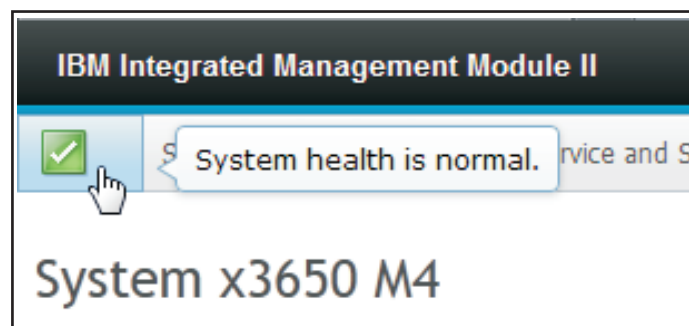
Registerkarte "System Status"

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

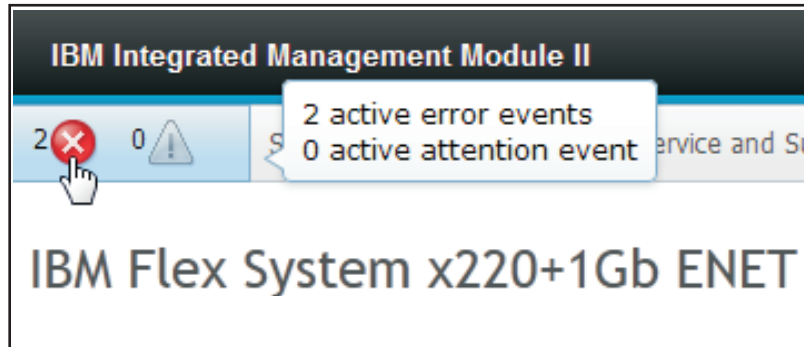
Die Seite "System Status" wird angezeigt, wenn Sie sich bei der IMM2-Webbenutzerschnittstelle angemeldet haben oder wenn Sie auf die Registerkarte **System Status** klicken. Auf der Seite "System Status" können Sie den Systemstatus, aktive Systemereignisse und Informationen zum Hardwarezustand anzeigen.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



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.



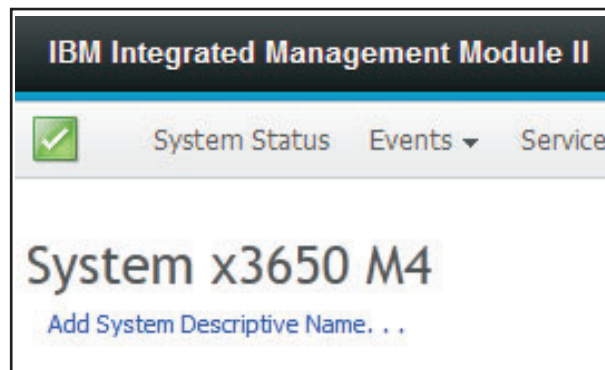
Wenn ein roter Kreis oder ein gelbes Dreieck angezeigt wird, bedeutet dies, dass eine Fehler- oder Warnbedingung vorliegt, wie in der folgenden Abbildung dargestellt.



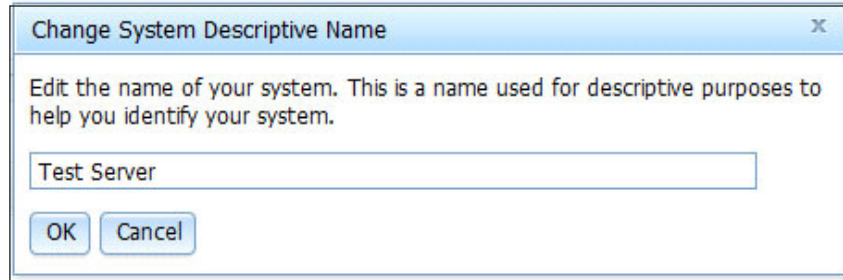
Das Symbol mit dem roten Kreis gibt an, dass auf dem Server eine Fehlerbedingung vorliegt. Das Symbol mit dem gelben Dreieck gibt an, dass eine Warnbedingung vorliegt. Wenn ein Symbol mit einem roten Kreis oder einem gelben Dreieck angezeigt wird, sind die Ereignisse, die der Bedingung zugeordnet sind,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

Active Events			
Severity	Source	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.



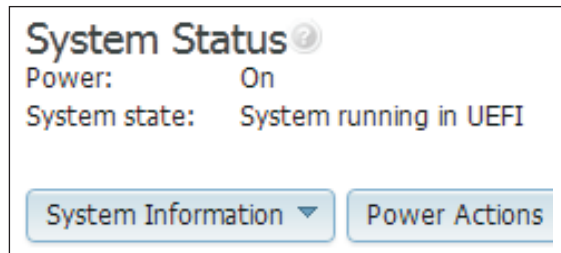
Wenn Sie auf den Link **Add System Descriptive Name...** (Beschreibenden Systemnamen einfügen) klicken, wird das folgende Fenster angezeigt, in dem Sie einen Namen eingeben können, der dem IMM2-Server zugeordnet wird. Sie können den beschreibenden Systemnamen jederzeit ändern.



A dialog box titled "Change System Descriptive Name" with a close button (X) in the top right corner. The text inside reads: "Edit the name of your system. This is a name used for descriptive purposes to help you identify your system." Below the text is a text input field containing the text "Test Server". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Wenn Sie auf den Link **Rename...** (Umbenennen) neben dem Hostnamen klicken, wird die Seite "Network Protocol Properties" (Netzprotokolleigenschaften) geöffnet. Sie können die Seite "Network Protocol Properties" verwenden, um den Hostnamen auf der Registerkarte **Ethernet** zu konfigurieren. Weitere Informationen finden Sie im Abschnitt „Netzprotokolle konfigurieren“ auf Seite 90.

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).



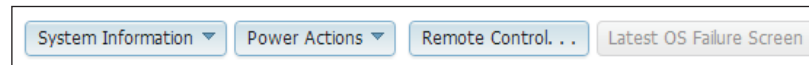
A panel titled "System Status" with a help icon (question mark in a circle) to the right of the title. Below the title, it displays "Power: On" and "System state: System running in UEFI". At the bottom, there are two buttons: "System Information" with a dropdown arrow and "Power Actions".

Der Server kann sich in einem der Status befinden, die in der folgenden Tabelle aufgeführt sind:

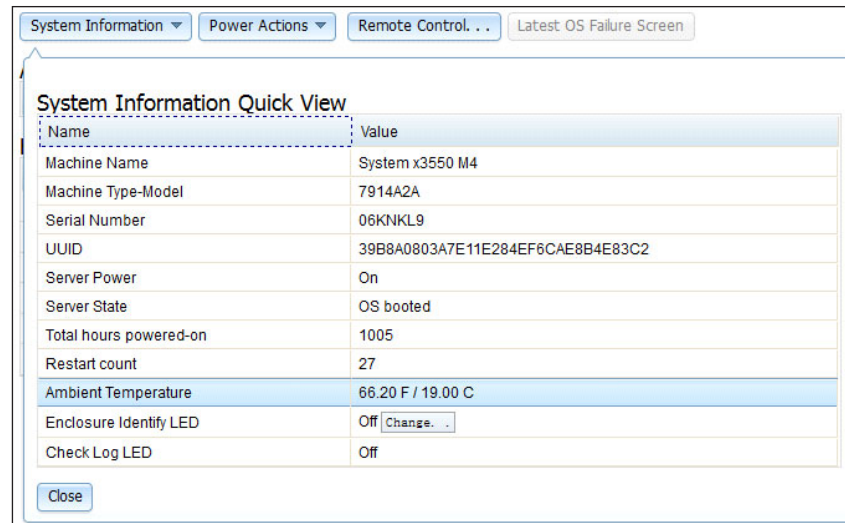
Tabelle 2. Stromversorgungsstatus und Betriebsstatus des Servers

Serverstatus	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 Ausführung wurde beendet.
Bootting OS or in unsupported OS (Betriebssystem wird gebootet oder es wird ein nicht unterstütztes Betriebssystem gebootet)	Der Server kann sich aus einem der folgenden Gründe in diesem Status befinden: • Das Ladeprogramm des Betriebssystems wurde gestartet, aber das Betriebssystem wird noch nicht ausgeführt. • Die Ethernet-über-USB-Schnittstelle des IMM2 ist inaktiviert. • Das Betriebssystem hat die Treiber, die die Ethernet-über-USB-Schnittstelle unterstützen, nicht geladen. • Möglicherweise wird auf dem System eine Firewall ausgeführt, wodurch die Kommunikation mit dem IMM2 blockiert wird.
OS booted (Betriebssystem gebootet)	Das Serverbetriebssystem wird ausgeführt.
Suspend to RAM (Aussetzen in RAM)	Der Server wurde in den Bereitschafts- oder Ruhemodus versetzt.

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.



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



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 128.

Klicken Sie auf die Registerkarte **Remote Control**, um Informationen zur Steuerung des Servers auf Betriebssystemebene zu erhalten. Unter „Remote-Presence- und Fernsteuerungsfunktionen“ auf Seite 130 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 158.

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 Status 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
Local Storage	 Normal
Processors	 Normal
Memory	 Normal
System	 Normal

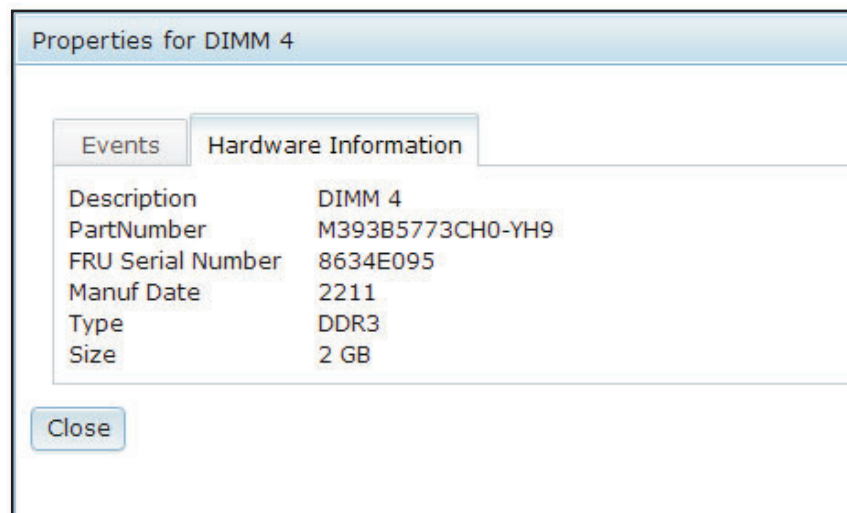
Bei jedem Komponententyp handelt es sich um einen Link, auf den Sie klicken können, um ausführlichere Informationen zu erhalten. Wenn Sie auf einen Komponententyp klicken, wird eine Tabelle angezeigt, in der die Status der einzelnen Komponenten aufgeführt sind (wie in der folgenden Abbildung dargestellt).

Memory			
Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Eve			
FRU Name	Status	Type	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.



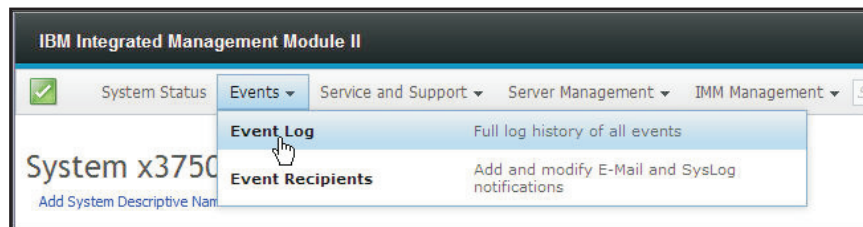
Klicken Sie auf die Registerkarte **Hardware Information** (Hardwareinformationen), um ausführliche Informationen zur Komponente anzuzeigen.



Registerkarte "Events" (Ereignisse)

Dieser Abschnitt enthält Informationen zur Verwendung der Optionen auf der Registerkarte **Events** (Ereignisse) 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.

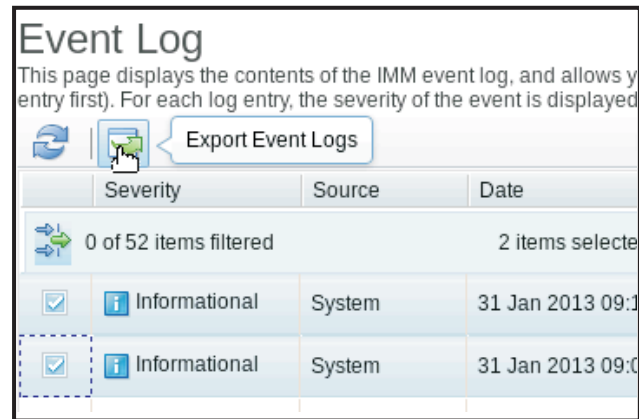


Event Log (Ereignisprotokoll)

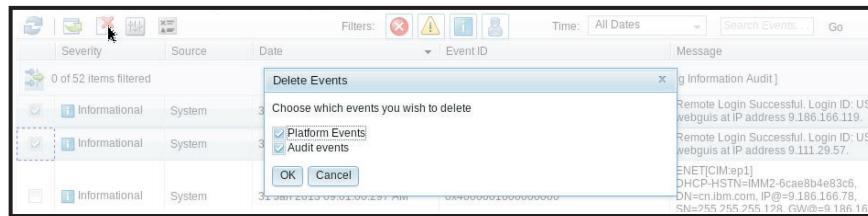
Wählen Sie auf der Registerkarte **Events** (Ereignisse) die Option **Event Log** (Ereignisprotokoll) aus, um die Seite "Event Log" anzuzeigen. Auf der Seite "Event Log" wird der Schweregrad der Ereignisse angezeigt, die vom IMM2 gemeldet wurden, und Informationen zu allen Fernzugriffsversuchen sowie 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.

Severity	Source	Date	Event ID	Message
Informational	System	31 1 2013 09:02:42.771 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webgus at IP address 9.111.20.57.
Informational	System	31 1 2013 09:01:00.297 AM	0x4000001600000000	ENETICIM.ep1 DHCP+HSTN=IMM2-6cae8b4e83c5, DN=cn.ibm.com, IP=@=9.186.166.78, SN=255.255.255.128, GW=@=9.186.166.1, DNS1=@=9.0.148.50.
Informational	System	31 1 2013 09:00:58.957 AM	0x4000001900000000	LAN: Ethernet[IMM2] interface is now active.
Informational	System	31 1 2013 09:00:55.004 AM	0x4000001700000000	ENETICIM.ep2 IP-Cfg.HstName=IMM2-6cae8b4e83c5, IP=@=189.254.95.119, NetMask=255.255.0.0, GW=@=0.0.0.0.
Informational	System	31 1 2013 09:00:53.403 AM	0x4000003700000000	ENETICIM.ep1 IPv6-LinkLocal.HstName=IMM2-6cae8b4e83c5, IP=@fe80: 6ae8:80ff:fe4e:83c5: Prefix54.
Informational	System	31 1 2013 09:00:51.592 AM	0x4000001900000000	LAN: Ethernet[IMM2] interface is now active.
Informational	System	31 1 2013 09:00:47.068 AM	0x4000001000000000	Management Controller SN# 06K9KL9 Network Initialization Complete.
Informational	System	31 1 2013 09:00:02.874 AM	0x800801282101fff	Device Low Security Jmp has been added.
Informational	Power	31 1 2013 09:00:02.304 AM	0x806800091301fff	Host Power has been turned off.
Informational	System	31 1 2013 08:55:11.252 AM	0x4000001500000000	Management Controller SN# 06K9KL9 reset was initiated by user USERID.
Informational	System	31 1 2013 08:47:59.118 AM	0x4000002300000000	Flash of SN# 06K9KL9 from (IMM2) 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 webgus at IP address 9.186.166.119.
Informational	System	31 1 2013 08:43:15.666 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webgus at IP address 9.111.20.57.

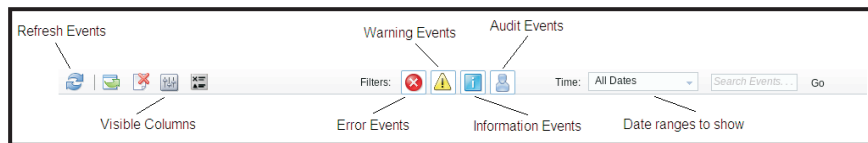
Um Ereignisse im Ereignisprotokoll zu sortieren und zu filtern, wählen Sie die entsprechende Spaltenüberschrift aus. Sie können mithilfe der Schaltfläche **Export** alle oder ausgewählte Ereignisse aus dem Ereignisprotokoll speichern. Um bestimmte Ereignisse auszuwählen, wählen Sie auf der Hauptseite 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).



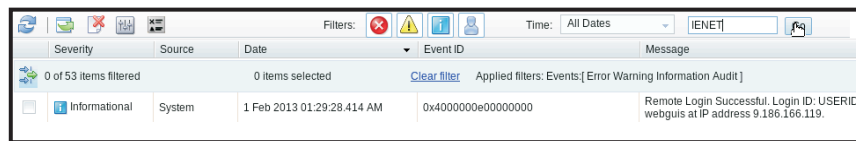
Mit der Schaltfläche **Delete Events** (Ereignisse löschen) können Sie den Ereignistyp auswählen, den Sie löschen möchten (wie in der folgenden Abbildung dargestellt).



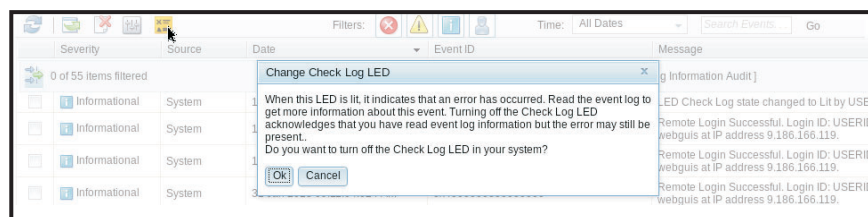
Um den Typ der Ereignisprotokolleinträge auszuwählen, den Sie anzeigen möchten, klicken Sie auf die entsprechende Schaltfläche (wie in der folgenden Abbildung dargestellt).



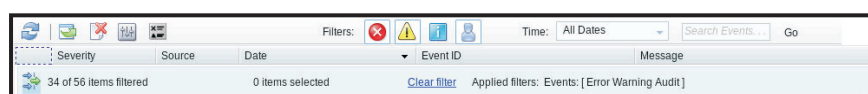
Um nach bestimmten Ereignistypen oder Suchbegriffen zu suchen, geben Sie den betreffenden Ereignistyp oder den Suchbegriff im Feld **Search Events** (Ereignisse suchen) ein. Klicken Sie dann auf **Go** (Start) (wie in der folgenden Abbildung dargestellt).



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).

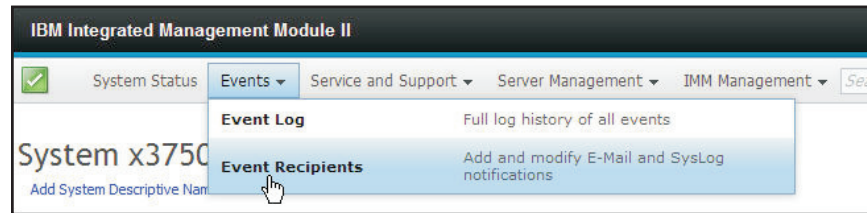


In der Symbolleiste "Event Log" (Ereignisprotokoll) können Sie auf jede beliebige Schaltfläche von **Filter Events** (Ereignisse filtern) klicken, um die Ereignisse auszuwählen, die angezeigt werden sollen. Um den Filter zu löschen und alle Ereignistypen anzuzeigen, klicken Sie auf den in der folgenden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



Event Recipients (Ereignisempfänger)

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

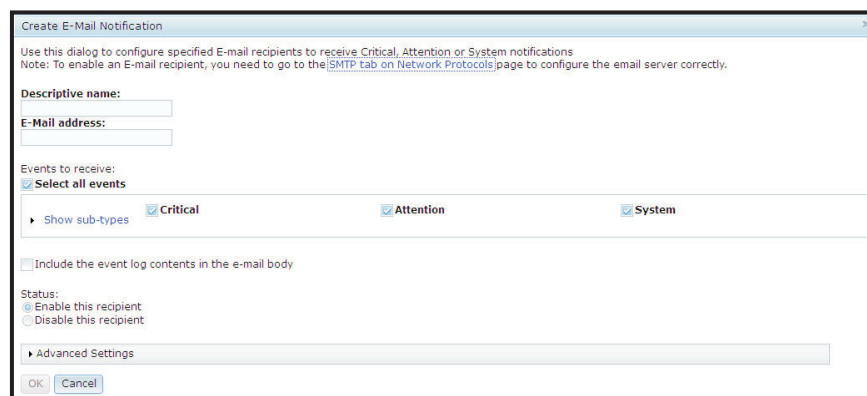


Mithilfe der Option **Event Recipients** (Ereignisempfänger) können Sie die Empfänger von Benachrichtigungen über Systemereignisse verwalten. Sie können die einzelnen Empfänger konfigurieren und die Einstellungen verwalten, die für alle Ereignisempfänger gelten. Sie können auch ein Testereignis generieren,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

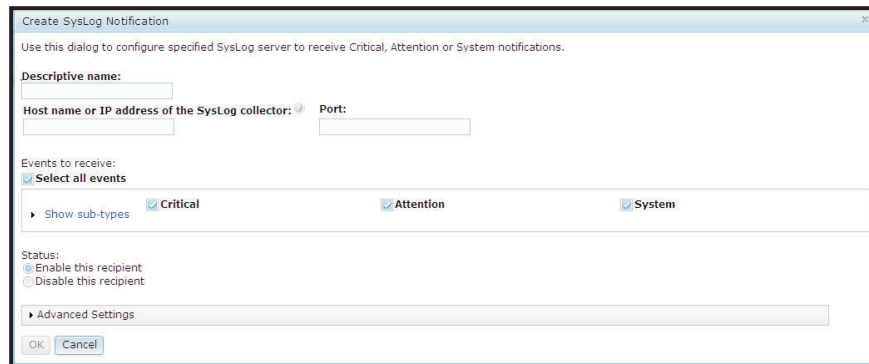
Klicken Sie auf die Schaltfläche **Create** (Erstellen), um E-Mail- und syslog-Benachrichtigungen zu erstellen. In der folgenden Abbildung ist das Fenster "Event Recipients" dargestellt.



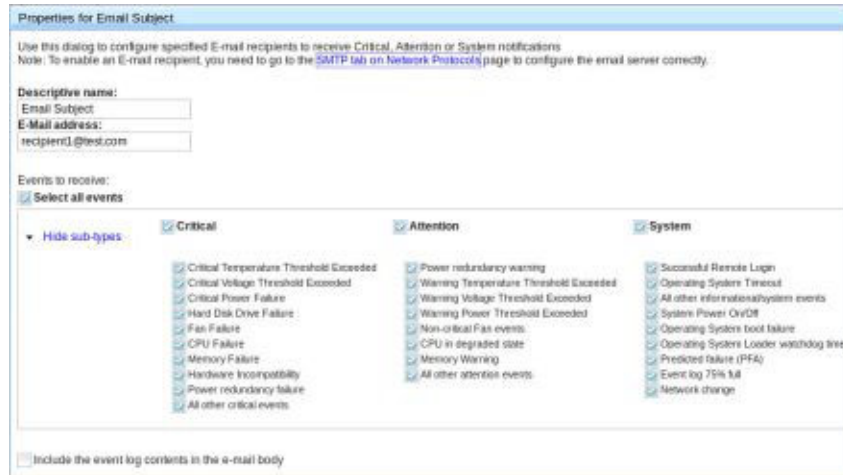
Wählen Sie die Option **Create E-mail Notification** (E-Mail-Benachrichtigung erstellen) aus, um eine Ziel-E-Mail-Adresse einzurichten und den Ereignistyp auszuwählen, für den Benachrichtigungen gesendet werden sollen. Außerdem können Sie auf **Advanced Settings** (Erweiterte Einstellungen) klicken, 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 das Fenster "Create E-mail notification" dargestellt.



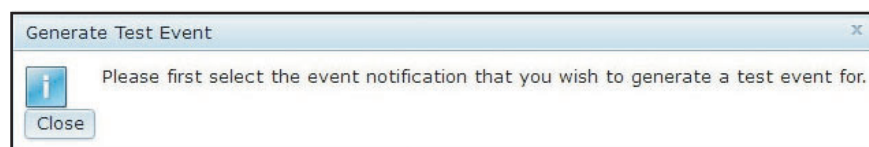
Wählen Sie die Option **Create SysLog Notification** (SysLog-Benachrichtigung erstellen) aus, um einen Hostnamen und eine IP-Adresse für den SysLog-Collector einzurichten und den Ereignistyp auszuwählen, für den Benachrichtigungen gesendet werden sollen. Außerdem können Sie auf **Advanced Settings** (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 das Fenster "Create SysLog Notification" dargestellt.



Um ein *vorhandenes* E-Mail-Benachrichtigungs- oder Systembenachrichtigungsziel zu konfigurieren, klicken Sie auf den Zielnamen. Beim Folgenden handelt es sich um eine Darstellung des Fensters "Properties for Email Subject" (Eigenschaften für E-Mail-Betreff), das zum Konfigurieren vorhandener E-Mail-Benachrichtigungs- und Systembenachrichtigungsziele verwendet wird.

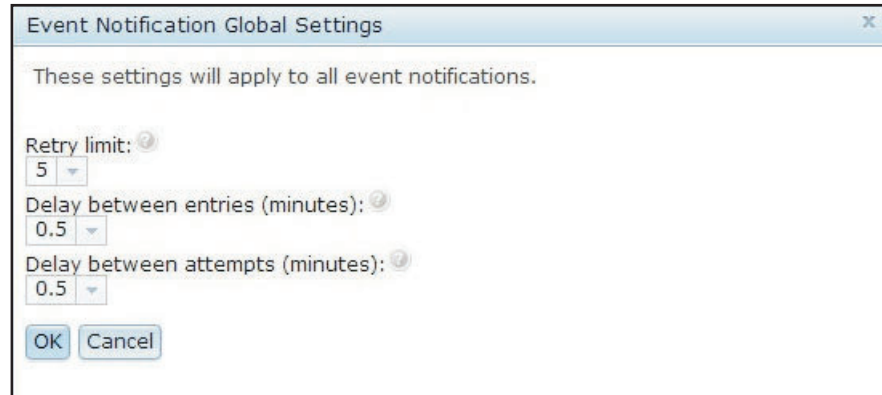


Wählen Sie die Schaltfläche **Generate Test Event** (Testereignis generieren) aus, um eine Test-E-Mail an das ausgewählte E-Mail-Ziel zu senden (wie in der folgenden Abbildung dargestellt).



Wählen Sie die Schaltfläche **Global Settings** (Globale Einstellungen) aus, um einen Grenzwert für die Wiederholungsversuche für Ereignisbenachrichtigungen, die Ver-

zögerung (in Minuten) zwischen den Ereignisbenachrichtigungseinträgen und die Verzögerung (in Minuten) zwischen den Benachrichtigungsversuchen festzulegen (wie in der folgenden Abbildung dargestellt).



Event Notification Global Settings

These settings will apply to all event notifications.

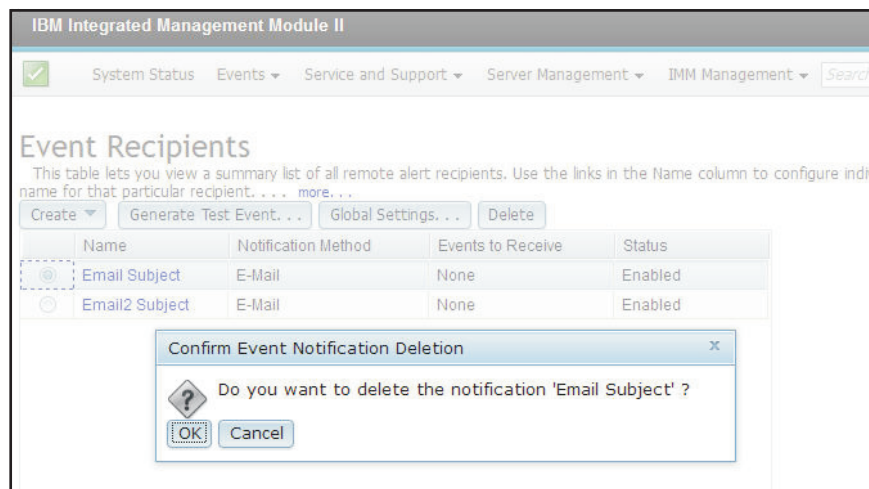
Retry limit: 5

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 Integrated Management Module II

System Status Events Service and Support Server Management IMM Management Search

Event Recipients

This table lets you view a summary list of all remote alert recipients. Use the links in the Name column to configure individual recipients. ... more...

Create Generate Test Event... Global Settings... Delete

Name	Notification Method	Events to Receive	Status
Email Subject	E-Mail	None	Enabled
Email2 Subject	E-Mail	None	Enabled

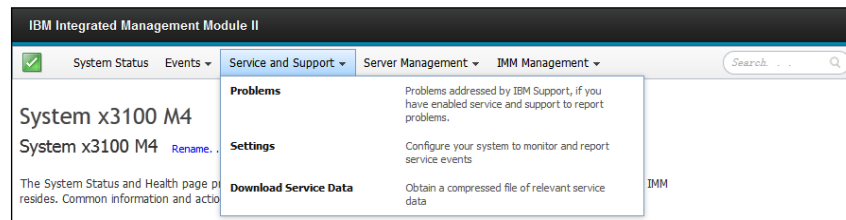
Confirm Event Notification Deletion

Do you want to delete the notification 'Email Subject' ?

OK Cancel

Registerkarte "Service and Support"

Dieser Abschnitt enthält Informationen zur Verwendung der Optionen auf der Registerkarte **Service and Support** der IMM2-Webbenutzerschnittstelle (wie in der folgenden Abbildung dargestellt).



IBM Integrated Management Module II

System Status Events Service and Support Server Management IMM Management Search

System x3100 M4

System x3100 M4 Rename...

The System Status and Health page resides. Common information and actions.

Problems Problems addressed by IBM Support, if you have enabled service and support to report problems.

Settings Configure your system to monitor and report service events.

Download Service Data Obtain a compressed file of relevant service data.

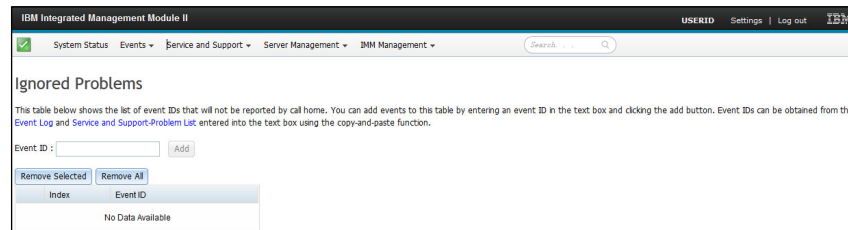
IMM

Option "Problems"

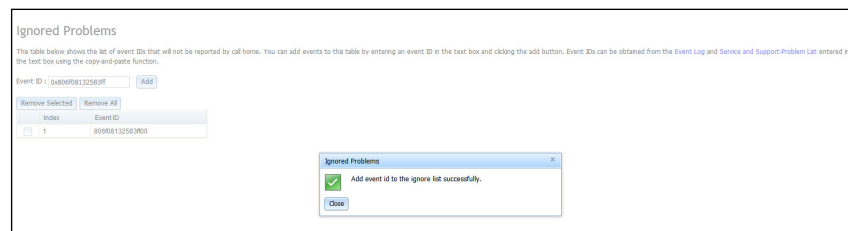
Wählen Sie die Option **Problems** (Probleme) auf der Registerkarte **Service and Support** (Service und Unterstützung) aus, um eine Liste mit nicht behobenen Prob-

Klicken Sie auf die Registerkarte **Ignore Problems**, um die Liste mit Ereignis-IDs anzuzeigen, die nicht durch die Funktion *call home* gemeldet werden sollen. Sie können Ereignis-IDs zu dieser Liste hinzufügen, indem Sie sie in das Feld **Event ID** eingeben und auf die Schaltfläche **Add** (Hinzufügen) klicken (wie in der folgenden Abbildung dargestellt).

Anmerkung: Ereignis-IDs können aus dem Ereignisprotokoll oder aus der Spalte "Event ID" in der Liste mit Service- und Support-Problemen abgerufen werden. Fügen Sie die Ereignis-ID mithilfe der Funktion zum Kopieren und Einfügen in das Textfeld ein.



Nach der Eingabe einer gültigen Ereignis-ID und dem Klicken auf die Schaltfläche **Add** (Hinzufügen) wird ein Bestätigungsfenster angezeigt, das angibt, dass die Ereignis-ID erfolgreich hinzugefügt wurde.

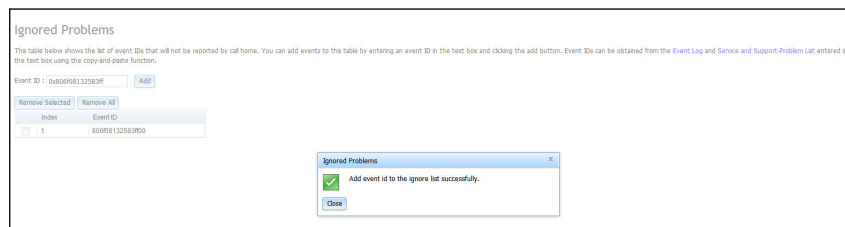


Gehen Sie wie folgt vor, um eine Ereignis-ID aus der Liste "Ignored Problems" (Ignorierte Probleme) zu entfernen:

1. Wählen Sie das Kontrollkästchen **Index** der Ereignis-ID aus, die Sie entfernen möchten.

Anmerkung: Um mehrere Ereignis-IDs zu entfernen, wählen Sie alle zutreffenden **Index**-Kontrollkästchen aus.

2. Klicken Sie auf die Schaltfläche **Remove Selected** (Ausgewählte entfernen) (wie in der folgenden Abbildung dargestellt).



Das ausgewählte Ereignis wird gelöscht und ein Bestätigungsfenster wird angezeigt.



Um alle Ereignis-IDs aus der Liste zu entfernen, wählen Sie die Schaltfläche **Remove All** (Alle entfernen) aus. Das folgende Fenster wird angezeigt.



Klicken Sie auf die Registerkarte **Open Service Request** (Serviceanforderung öffnen), um manuell eine Serviceanforderung zu öffnen, indem Sie den Problembe-
reich angeben und eine Textbeschreibung des Problems eingeben.

Klicken Sie auf die Registerkarte **Open Test Request** (Testanforderung öffnen), um eine Testanforderung vom Typ *call home* (IBM Support anfordern) zu generieren, um die richtige Konfiguration dieser Funktion zu beschleunigen oder um zu über-
prüfen, ob diese ordnungsgemäß funktioniert.

Klicken Sie auf die Registerkarte **Refresh** (Aktualisieren), um die Liste mit Proble-
men mit dem aktuellen Status zu aktualisieren (wie in der folgenden Abbildung dargestellt).

⚠ Service and Support is not yet enabled.

Display for: Both IBM Support and File Transfer Server

Corrected	Message	Severity	Problem Status	Ticket Number	File Transfer Server	Event Date	Event ID
☐ No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	11 Nov 2013, 09:43:54.000 PM	0x806f08132583fff
☐ No	Fault in slot One of PCs on system System x3750 M4.	Error	Disabled	N/A	Disabled	11 Nov 2013, 08:41:25.000 PM	0x806f002125820900
☐ No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	11 Nov 2013, 08:37:50.000 PM	0x806f08132583fff
☐ Yes	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	28 Oct 2013, 08:28:12.000 PM	0x806f08132583fff
☐ No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	23 Oct 2013, 07:47:31.000 PM	0x806f08132583fff

Option "Settings"

Wählen Sie die Option **Settings** (Einstellungen) auf der Registerkarte **Service and Support** (Service und Unterstützung) aus, um Service- und Support-Einstellungen anzuzeigen, hinzuzufügen oder zu ändern (wie in der folgenden Abbildung dargestellt).

Anmerkungen:

- Damit der IBM Support erfolgreich angefordert werden kann, stellen Sie sicher, dass die DNS-Einstellungen (Domain Name System) gültig sind.
- Die Informationen zum Service Center sowie die Kontaktinformationen sind zum Aktivieren des IBM Support erforderlich.
- Damit der Dateübertragungsserver aktiviert werden kann, müssen die Serverinformationen richtig angegeben werden.

IBM Integrated Management Module II USERID Settings Log out

System Status Events Service and Support Server Management IMM Management

Service and Support - Settings

Use this page to view or change current service and support settings. To successfully call home (IBM support), make sure DNS settings are valid. The service center and contact information is required to enable IBM support. To enable file transfer server, to input the server information correctly.

... more ...

Service and Support is not yet enabled.

IBM Support File Transfer Server HTTP Proxy

Enable IBM Support

To successfully call home (IBM support), make sure DNS settings are valid. The service center and contact information is required to enable IBM support.

☐ **Enable IBM Support.** Automatically send the service information to IBM.

IBM Service Center

Country code:

Contact Information

The information here will be used by IBM Support for any follow-up inquiries and shipment.

Primary Contact

Company name:

Contact name:

Telephone number: Extension:

Alternate Contact (Optional)

Contact name:

Telephone number: Extension:

Contact Email address:

Gehen Sie wie folgt vor (wie in der folgenden Abbildung dargestellt), um es dem Serviceprozessor zu ermöglichen, automatisch Serviceinformationen an IBM zu senden:

1. Klicken Sie auf die Registerkarte **IBM Support**.
2. Klicken Sie auf das Kontrollkästchen **Enable IBM Support** (IBM Support aktivieren).
3. Wählen Sie aus der Liste **IBM Service Center** die Position Ihres IBM Service Center aus.
4. Geben Sie die Informationen zu Ihrem primären Ansprechpartner in die folgenden Felder ein:
 - Name des Unternehmens
 - Name des Ansprechpartners
 - Telefonnummer
 - Durchwahl (falls zutreffend)
 - E-Mail-Adresse des Ansprechpartners
 - Adresse
 - Stadt
 - Staat/Bundesland
 - Postleitzahl
5. Klicken Sie auf die Schaltfläche **Apply IBM Support Settings** (IBM Support-Einstellungen übernehmen).

Gehen Sie wie folgt vor (wie in der folgenden Abbildung dargestellt), um es dem Serviceprozessor zu ermöglichen, Ereignisse und Daten zu wartungsfähiger Hardware an die angegebene File Transfer Server-Site (Dateiübertragungsserver) zu senden:

1. Klicken Sie auf die Registerkarte **File Transfer Server**.
2. Wählen Sie das Kontrollkästchen **Enable File Transfer Server** (Dateiübertragungsserver aktivieren) aus.
3. Klicken Sie auf die Schaltfläche **Apply File Transfer Server Settings** (Dateiübertragungsservereinstellungen übernehmen).

Gehen Sie wie folgt vor (wie in der folgenden Abbildung dargestellt), um die Methode festzulegen, mit der eine Verbindung zum Internet hergestellt werden soll:

1. Klicken Sie auf die Registerkarte **HTTP Proxy**.
2. Klicken Sie auf eine der folgenden Methoden für den Internetzugriff:
 - Der Verwaltungsserver kann ohne einen Proxy-Server auf das Internet zugreifen.

- Der Verwaltungsserver benötigt für den Internetzugriff einen Proxy-Server

IBM Support | File Transfer Server | **HTTP Proxy**

Select the method to connect internet

☒ The management server can access the Internet without a proxy server

☐ The management server will require a proxy server to access the Internet

Apply Reset

- Gehen Sie wie folgt vor (wie in der folgenden Abbildung dargestellt), wenn ein Proxy-Server für den Internetzugriff erforderlich ist; fahren Sie andernfalls mit Schritt 4 fort.
 - Geben Sie in das Feld **IP address or host name** (IP-Adresse oder Hostname) die IP-Adresse oder den Hostnamen für den Proxy-Server ein.
 - Geben Sie in das Feld **Port** den Port für den Proxy-Server ein.

Anmerkung: Das Kontrollkästchen **Use authentication** (Authentifizierung verwenden) ist optional.

IBM Support | File Transfer Server | **HTTP Proxy**

Select the method to connect internet

☐ The management server can access the Internet without a proxy server

☒ The management server will require a proxy server to access the Internet

IP address or host name: Port:

☒ Use authentication

User name:

Password:

Apply Reset

- Klicken Sie auf die Schaltfläche **Apply** (Übernehmen).

Firewalls und Proxy-Server vorbereiten

Sie müssen die Firewalls und den Proxy-Server konfigurieren, wenn in Ihrem Netz Firewalls enthalten sind oder wenn der Verwaltungsserver einen Proxy-Server für den Zugriff auf das Internet verwenden muss.

Gehen Sie wie folgt vor, um die Firewalls und Proxy-Server in Ihrem Netz zu konfigurieren:

- Bestimmen Sie, welche Ports Sie in Ihrer Systemmanagementumgebung verwenden werden, und stellen Sie sicher, dass diese Ports offen sind, bevor Sie mit der Installation beginnen. Sie müssen z. B. sicherstellen, dass die Listener-Ports offen sind.
- Stellen Sie sicher, dass Internetverbindungen zu den folgenden Internetadressen vorhanden sind.

Anmerkung: IP-Adressen können sich ändern, stellen Sie deshalb sicher, dass Sie DNS-Namen verwenden, sofern es möglich ist.

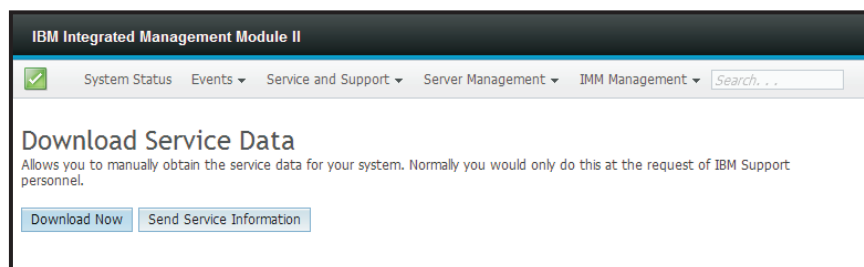
Tabelle 3. Erforderliche Internetverbindungen

Hostname	IP-Adresse	Port	Beschreibung
eccgw01.boulder.ibm.com	207.25.252.197	443	ECC-Transaktionsgateway (Electronic Customer Care)
eccgw02.rochester.ibm.com	129.42.160.51	443	ECC-Transaktionsgateway
www.ecurep.ibm.com	192.109.81.20	443	Hochladen von Dateien für Status- und Problemmeldungen
www6.software.ibm.com	170.225.15.41	443	Hochladen von Dateien für Status- und Problemmeldungen. Proxy-Server für testcase.boulder.ibm.com
www-945.ibm.com	129.42.26.224	443	Server für Problemmeldungen v4
	129.42.34.224	443	Server für Problemmeldungen v4
	129.42.42.224	443	Server für Problemmeldungen v4
www.ibm.com	129.42.56.216	80, 443	Download Service-Provider-Datei (CCF)
	129.42.58.216	80, 443	Download Service-Provider-Datei (CCF)
	129.42.60.216	80, 443	Download Service-Provider-Datei (CCF)
www-03.ibm.com	204.146.30.17	80, 443	Download Service-Provider-Datei (CCF)

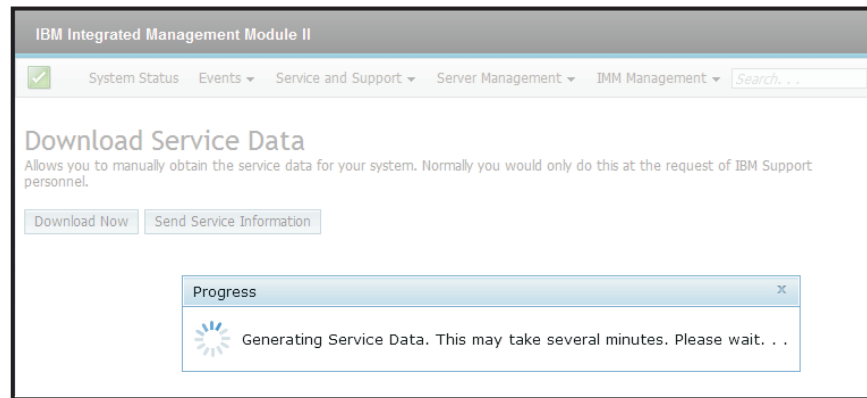
Option "Download Service Data"

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. Diese Datei können Sie als Hilfestellung bei der Fehlerbestimmung an den IBM Support schicken.

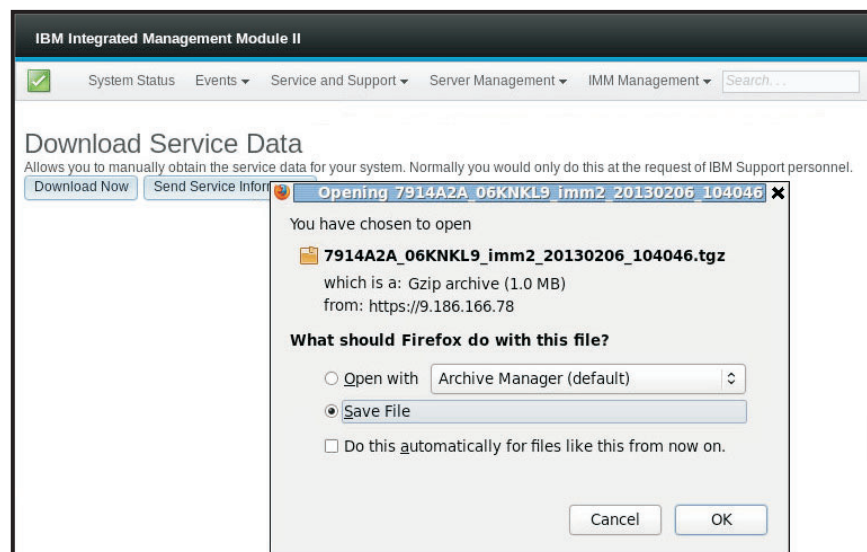
Klicken Sie auf die Schaltfläche **Download Now** (Jetzt herunterladen), um die Informationen zu Service und Support herunterzuladen (siehe folgende Abbildung).



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, an welcher Position die generierte Datei gespeichert werden soll.



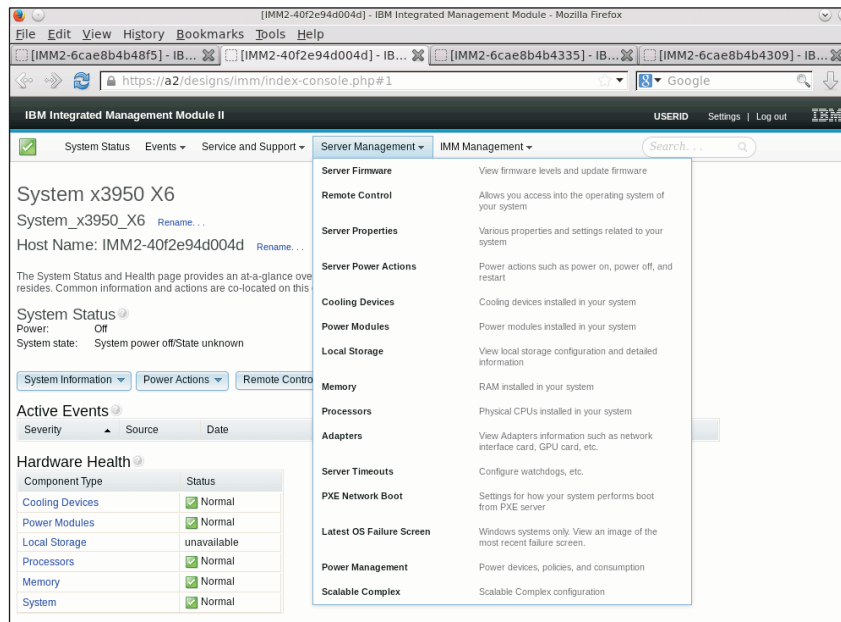
Registerkarte "Server Management"

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 lokalen Speichereinheiten, zum Speicher, zu Prozessoren, zu Adaptern, zu Zeitlimitüberschreitungen auf dem Server, zum PXE-Netzboot, zur letzten Betriebssystem-Fehleranzeige, zur Stromverbrauchssteuerung und zum skalierbaren Komplex anzeigen oder Tasks für diese Elemente ausführen (wie in der folgenden Abbildung dargestellt).

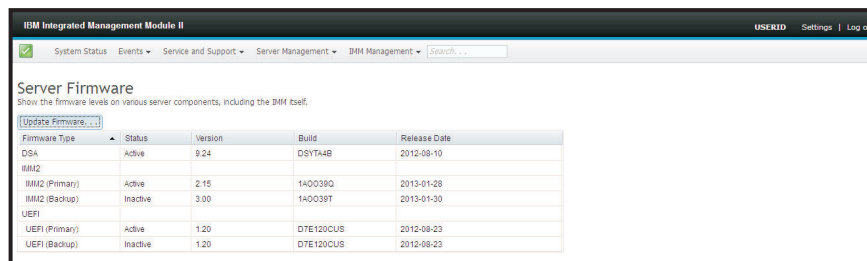
Wichtig: Einige Optionen sind möglicherweise auf Ihrem Server nicht verfügbar. Die Optionen, die auf der Registerkarte "Server Management" angezeigt werden,

richten sich danach, auf welcher Serverplattform das IMM2 gespeichert ist und welche Adapter auf dem Server installiert sind.



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.



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:

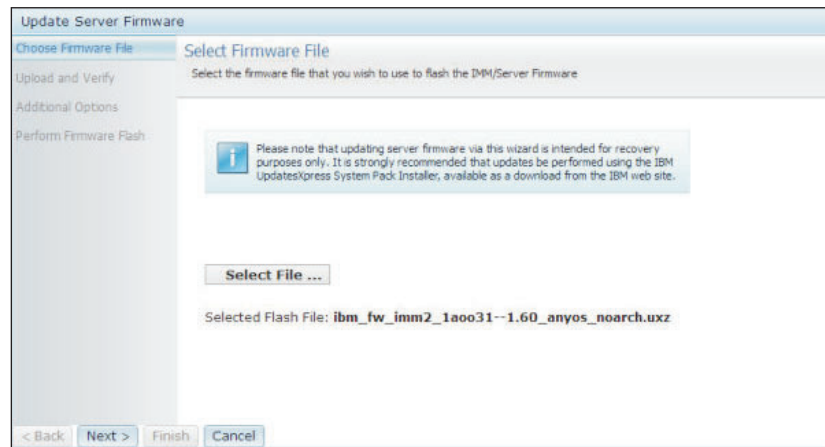
- **Active** (aktiv): Die Firmware ist aktiv.
- **Inactive** (inaktiv): Die Firmware ist inaktiv.
- **Pending** (anstehend): Die Firmware befindet sich im Wartestatus vor der Aktivierung.

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,

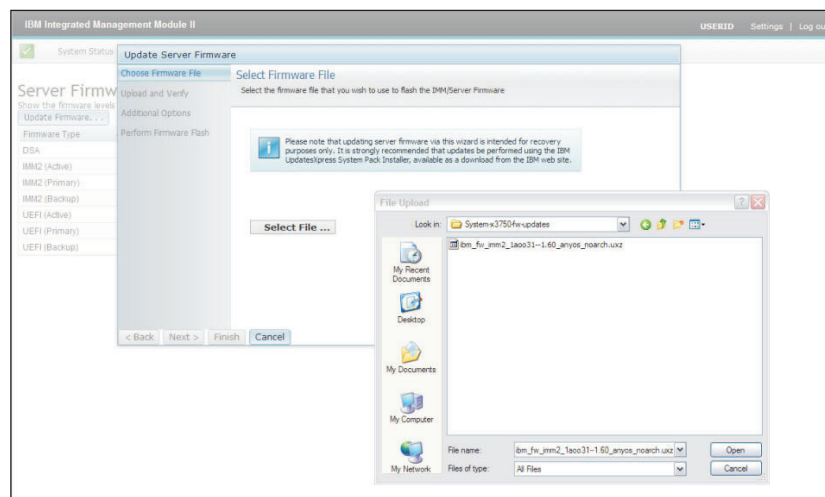
einschließlich Informationen zu besonderen Prozeduren bei der Aktualisierung von einer frühen Firmware- oder Einheitentreiberversion auf die neueste Version.

Um die Firmware zu aktualisieren, wählen Sie die Schaltfläche **Update Firmware...** (Firmware aktualisieren) aus. Das Fenster "Update Server Firmware" (Server-Firmware aktualisieren) wird angezeigt (wie in der folgenden Abbildung dargestellt). 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.

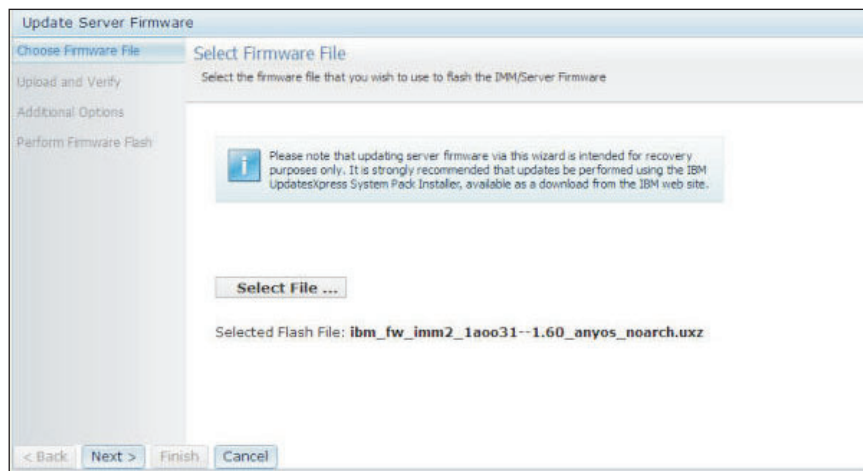
Anmerkung: Lesen Sie die in der Eingabeaufforderung angezeigte Warnung, bevor Sie auf die Schaltfläche **Select File...** (Datei auswählen) klicken.



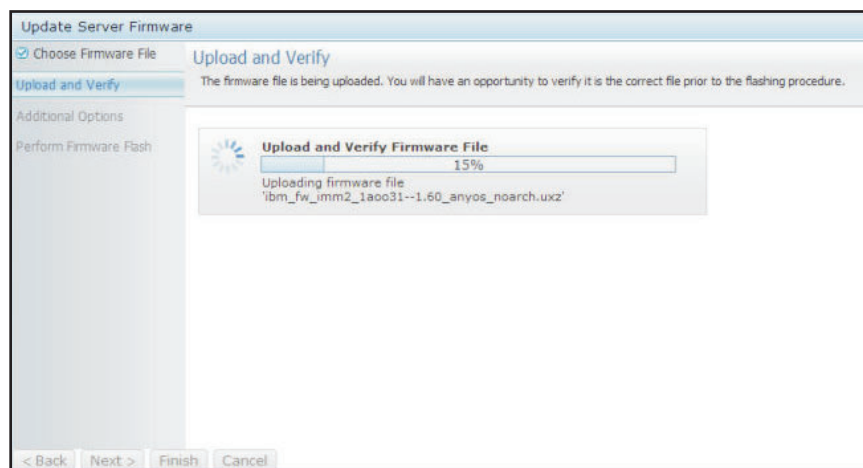
Wenn Sie auf die Schaltfläche **Select File...** klicken, wird das Fenster "File Upload" (Hochladen von Datei) angezeigt, in dem Sie nach der gewünschten Datei suchen können.



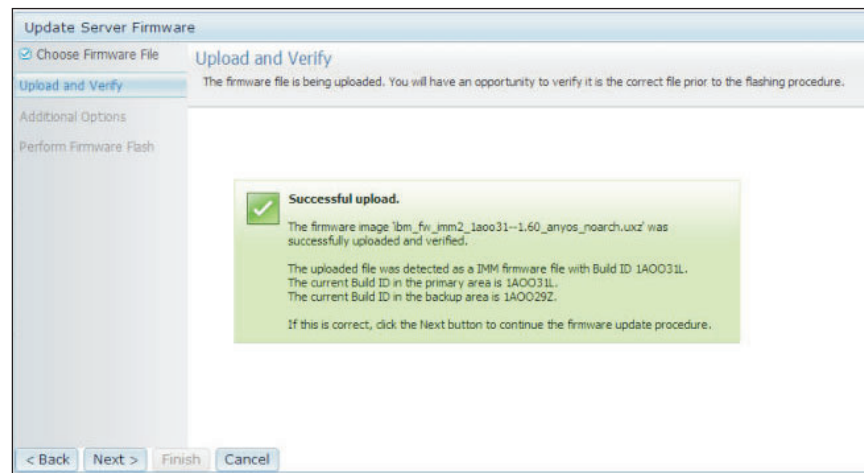
Klicken Sie, nachdem Sie zu der Datei navigiert sind, die Sie auswählen möchten, auf die Schaltfläche **Open** (Öffnen). Sie gelangen zurück zum Fenster "Update Server Firmware", in dem nun die ausgewählte Datei angezeigt wird (wie in der folgenden Abbildung dargestellt).



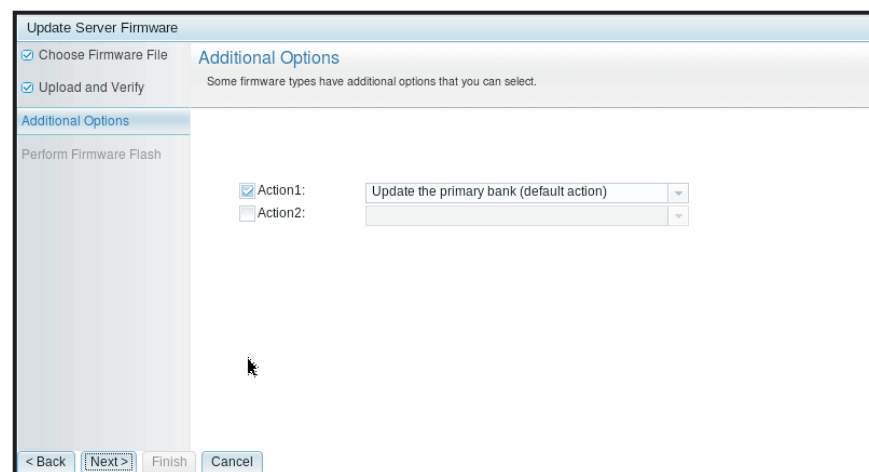
Klicken Sie auf die Schaltfläche **Next >** (Weiter), um den Upload- und Überprüfungsprozess für die ausgewählte Datei zu starten (wie in der folgenden Abbildung dargestellt). Eine Fortschrittsanzeige erscheint, während die Datei hochgeladen und überprüft wird.



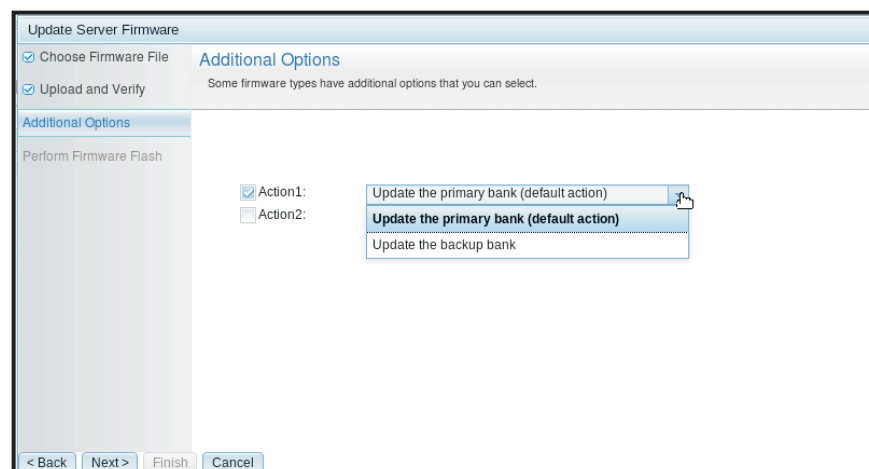
Ein Statusfenster wird geöffnet (wie in der folgenden Abbildung dargestellt), in dem Sie überprüfen können, ob es sich bei der ausgewählten zu aktualisierenden Datei um die richtige Datei handelt. Das Fenster enthält Informationen zum Typ der zu aktualisierenden Firmwaredatei, z. B. DSA, IMM2 oder UEFI.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



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



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.



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.

The screenshot shows the 'Update Server Firmware' window with the 'Additional Options' tab selected. On the left, there are three checkboxes: 'Choose Firmware File', 'Upload and Verify', and 'Additional Options' (which is checked). Below these is a section titled 'Perform Firmware Flash'. In the center, there are two checked checkboxes: 'Action1:' and 'Action2:'. To the right of 'Action1:' is a dropdown menu showing 'Update the primary bank (default action)'. To the right of 'Action2:' is a dropdown menu showing 'Update the backup bank'. At the bottom, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

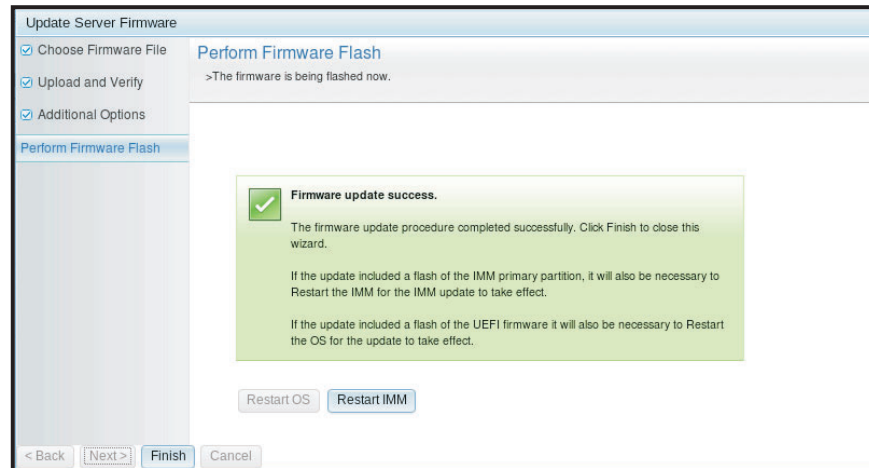
In der vorherigen Anzeige sehen Sie, dass für "Action 1" die primäre Speichergruppe zum Aktualisieren ausgewählt ist. Sie können auch auswählen, dass die Sicherungsspeichergruppe unter "Action 2" aktualisiert werden soll (wie im vorherigen Fenster dargestellt). Die primäre Speichergruppe und die Sicherungsspeichergruppe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

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

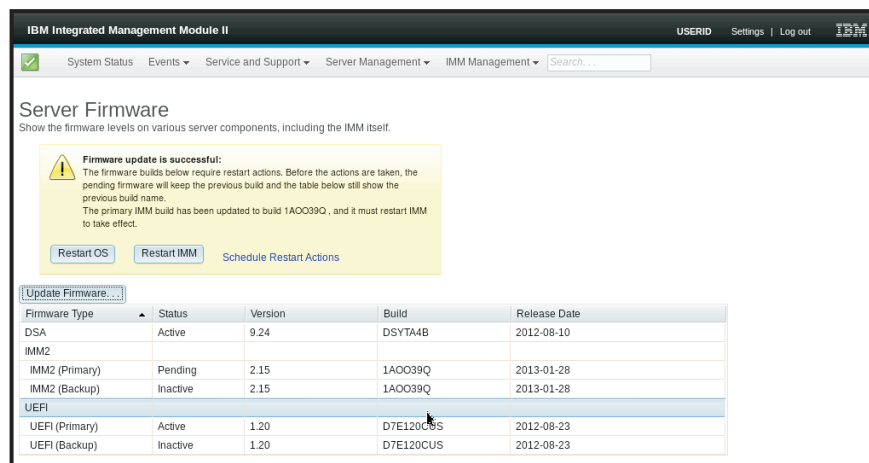
In einer Fortschrittsanzeige wird der Fortschritt der Firmwareaktualisierung angezeigt (wie in der folgenden Abbildung dargestellt).

The screenshot shows the 'Update Server Firmware' window with the 'Perform Firmware Flash' tab selected. On the left, there are three checkboxes: 'Choose Firmware File', 'Upload and Verify', and 'Additional Options' (which is checked). Below these is a section titled 'Perform Firmware Flash'. In the center, there is a progress bar with a circular arrow icon on the left and the text '27%' on the right. Above the progress bar, it says 'Action 1 of 2: 'Update the primary bank (default action)'' and 'Action 2 of 2: 'Update the backup bank''. At the bottom, there are four buttons: '< Back', 'Next >', 'Finish', and '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.



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 1.7 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.

Anmerkung: Der Video Viewer kann nur das vom Videocontroller auf der Systemplatine generierte Video anzeigen. Wenn ein separater Videocontroller installiert und anstelle des Systemvideocontrollers verwendet wird, kann das IMM2 den Videoinhalt aus dem hinzugefügten Adapter nicht auf dem fernen Video Viewer anzeigen.

- **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.

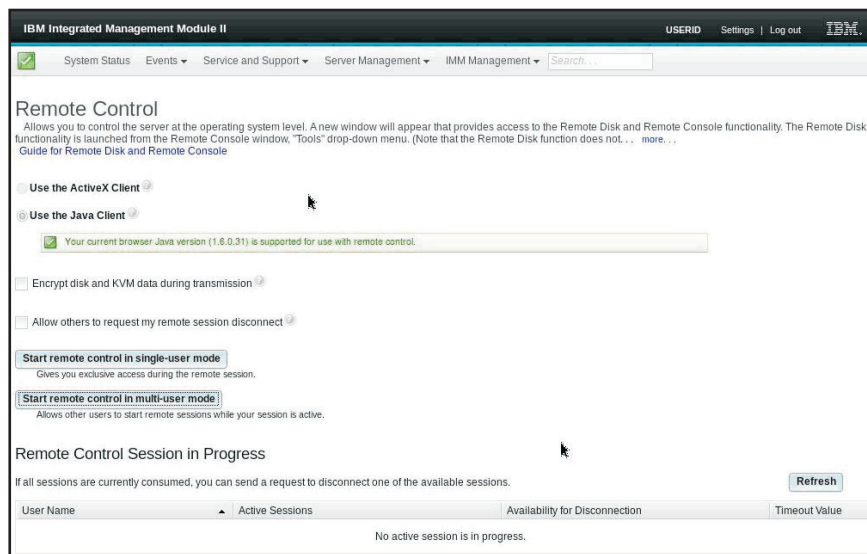
Anmerkungen:

- 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.

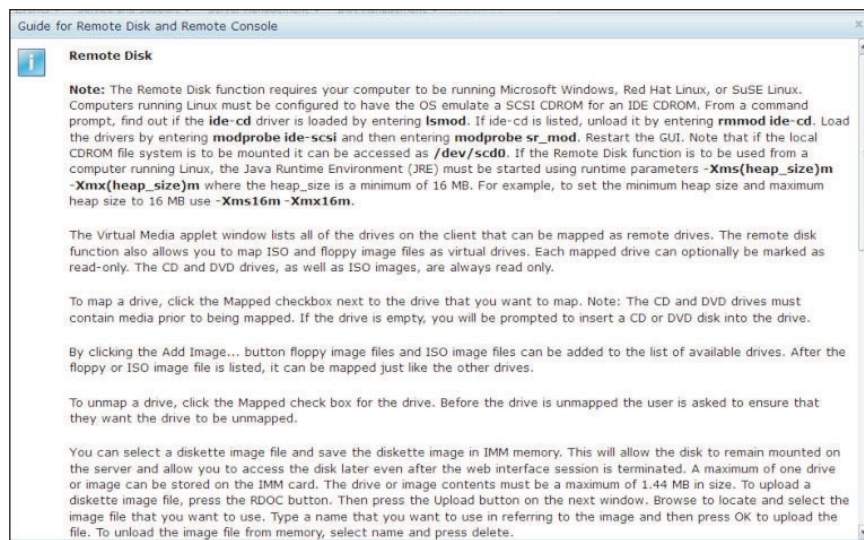
Gehen Sie wie folgt vor, um über Fernzugriff auf eine Serverkonsole zuzugreifen:

1. Melden Sie sich beim IMM2 an (weitere Informationen hierzu finden Sie unter „Am IMM2 anmelden“ auf Seite 12).
2. Greifen Sie auf die Seite "Remote Control" (Fernsteuerung) zu, indem Sie eine der folgenden Menüoptionen auswählen:
 - Wählen Sie auf der Registerkarte **Server Management** die Option **Remote Control** (Fernsteuerung) aus.
 - Klicken Sie auf der Seite "System Status" (Systemstatus) auf **Remote Control....**

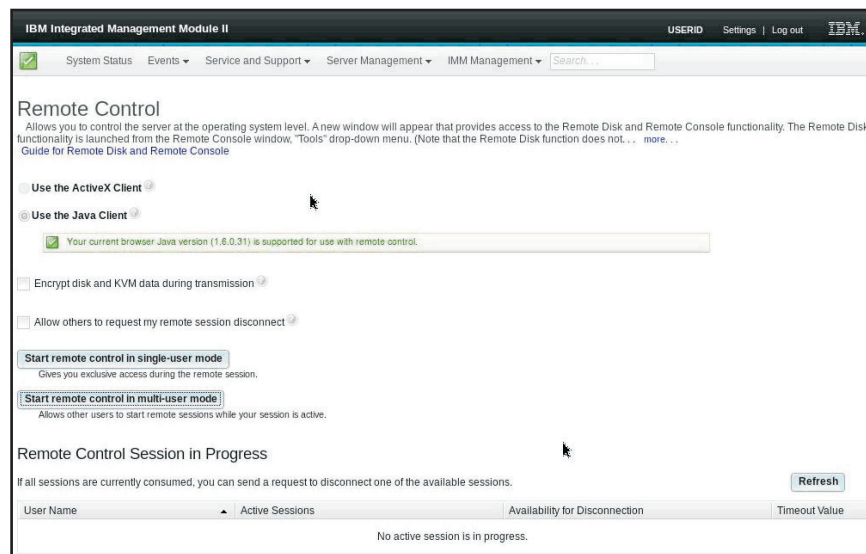
Die Seite "Remote Control" wird geöffnet, wie in der folgenden Abbildung dargestellt.



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.



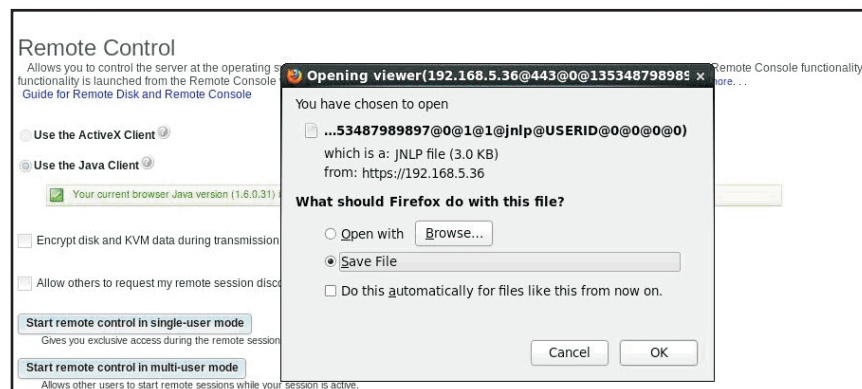
- a. Klicken Sie auf **Close** (Schließen), um das Fenster "Guide for Remote Disk and Remote Console" zu verlassen.
4. Wählen Sie eine der folgenden Optionen der grafischen fernen Konsole aus:
 - Um den Internet Explorer als Browser zu verwenden, wählen Sie die Option **Use the ActiveX Client** (ActiveX-Client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



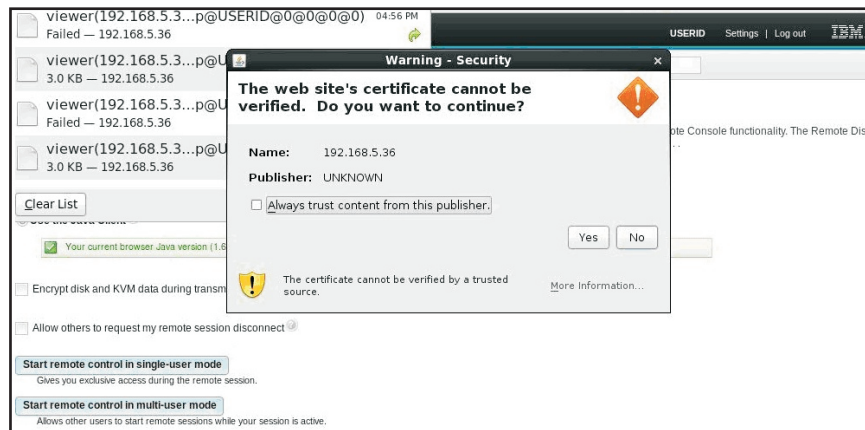
Anmerkungen:

- 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.



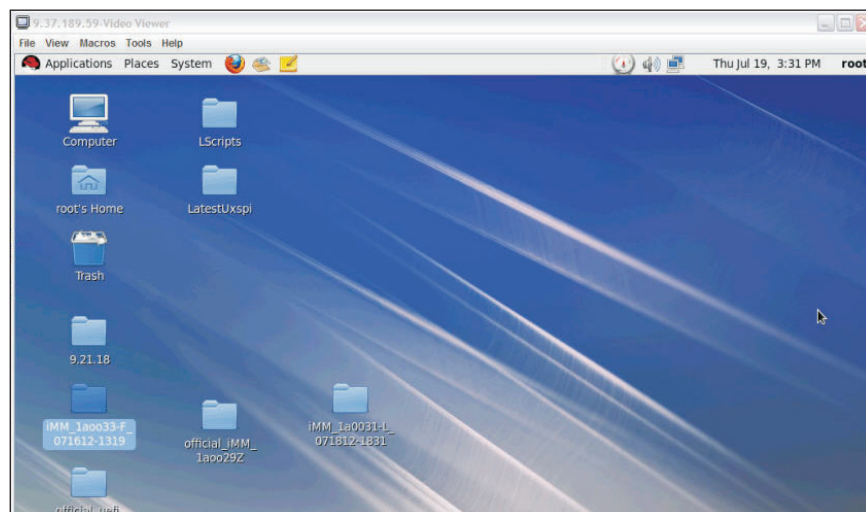
5. Nachdem der Browser die Viewer-Datei heruntergeladen und geöffnet hat, wird ein Bestätigungsfenster mit einer Warnung zur Überprüfung des Websitezertifikats angezeigt (wie in der folgenden Abbildung dargestellt). Klicken Sie auf **Yes**, um das Zertifikat zu akzeptieren.



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** (Datenträger- und 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 "Virtual Media Session", wenn Sie mit dem Verwenden der Funktion "Remote Control" fertig sind.

Anmerkungen:

- Durch Schließen des Fensters "Video Viewer" wird automatisch auch das Fenster "Virtual Media Session" geschlossen.

- 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 141.
- 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 lokalen 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 1.7 unter Windows:

1. Klicken Sie auf **Start** → **Settings (Einstellungen)** → **Control Panel (Steuerkonsole)**.
2. Klicken Sie doppelt auf **Java Plug-in 1.7**. 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 aus:
 - 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 144.

Weitere Informationen zum Verwenden der Fernsteuerungsfunktion finden Sie unter „Remote-Presence- und Fernsteuerungsfunktionen“ auf Seite 130.

Server Properties (Servereigenschaften)

Wählen Sie die Option **Server Properties** (Servereigenschaften) auf der Registerkarte **Server Management** (Serververwaltung) aus, um unterschiedliche Parameter zum Identifizieren des Systems festzulegen. Sie können den beschreibenden Systemnamen (**System descriptive name**), den Ansprechpartner (**Contact person**), den Standort (**Location**) und zusätzliche Informationen angeben, wie in der folgenden Abbildung dargestellt. 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

System Status | Events | Service and Support | Server Management | IMM Management | Search...

Server Properties

Various properties, status and settings related to your system.

Apply | 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 (site, geographical coordinates, etc.):

Room ID:

Rack ID:

Lowest unit of system:

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 Chassis Management Module) erforderlich.

IBM Integrated Management Module II

System Status | Events | Service and Support | Server Management | IMM Management | Search...

Server Properties

Various properties, status and settings related to your system.

Apply | 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 (site, geographical coordinates, etc.):

Room ID:

Rack ID:

Lowest unit of system:

U height of system: 0

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

Server Properties

Various properties, status and settings related to your system.

Apply | Reset

General Settings | LEDs | Hardware Information | Environmentals | Hardware Activity

LEDs

This web page shows the status of the LEDs on the server's chassis and front panel. It also provides the ability to view the status of those LEDs that are internal to the server without having to remove the server's cover(s). Click [here](#) to refresh LEDs.

LEDs in front panel

LED Label	Status	Description
Power	On	Go to Power Action Page to do power action.
Enclosure Identify	Off	Use it to identify the location of the system.
Check Log	Off	Check Event Log to identify the problem.
Fault LED	Off	Check LEDs in below to isolate the failed components.

Detailed LEDs and Recommended Actions

The left two columns present primary LED types and status, note that the left LEDs not classified into the Primary LED types will be shown in Others. Click any row to check detailed LEDs and recommended actions in right panel.

Primary LED/LED Type	Status	Description: If any FAN LED lit, the fan has failed.
MMR	Off	Action: Reset fan(s) with it error LEDs. Replace indicated fan(s).
TEMP (Temperature)	Off	
CONFIG (Configuration Mismatch)	Off	
PS (Power Supply)	Off	
HDD	Off	
OVER SPEC	Off	
FAN	Off	
LINK	Off	
PCI	Off	
BOARD	Off	

LED Label	Status
FAN 1	Off
FAN 2	Off
FAN 3	Off
FAN 4	Off
FAN 5	Off
FAN 6	Off

Um Informationen zum System, zu Systemkomponenten und zur Netzhardware anzuzeigen, klicken Sie auf die Registerkarte **Hardware Information** (Hardware-Informationen). Wählen Sie die entsprechende untergeordnete Registerkarte auf der Registerkarte **Hardware Information** aus, um verschiedene Informationen zu elementaren Produktdaten (VPD - Vital Product Data) anzuzeigen.

Die untergeordnete Registerkarte **System Information** (Systeminformationen) bietet Informationen wie den Maschinennamen, die Seriennummer und das Modell. In der folgenden Abbildung ist das Fenster "System Information" dargestellt.

Name	Value
Machine Name	System x3550 M4
Machine Type-Model	7914A2A
Serial Number	06KNKL9
UUID	39B8A0803A7E11E284EF6CAE8B4E83C2
Server Power	On
Server State	OS booted
Total hours powered-on	1005
Restart count	29
Ambient Temperature	66.20 F / 19.00 C
Enclosure Identify LED	Off Change...
Check Log LED	Off

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".

Change Enclosure Identify LED

Choose the desired state for the Enclosure Identify LED

The Location LED is on the front of the Light Path panel. It is called Identify in the LED table.

Note: The system might need to be powered on for the Location LED to turn on or blink.

Current state: Off

☐ Turn Off
☐ Turn On
☐ Blink

Ok Cancel

Wählen Sie die untergeordnete Registerkarte **System Component Information** aus, um Informationen wie z. B. den Namen der FRU, die Seriennummer, die Hersteller-ID und das Herstellungsdatum anzuzeigen. In der folgenden Abbildung sehen Sie die Informationen, die angezeigt werden, wenn Sie auf die Registerkarte **System Component Information** klicken.

IBM Integrated Management Module II

System Status Events Service and Support Server Management IMM Management Search...

Server Properties

Various properties, status and settings related to your system.

Apply Reset

General Settings LEDs **Hardware Information** Environmentals Hardware Activity

Hardware Information

This section lists vital product data (VPD) on a system, component and network basis.

System Information System Component Information Network Hardware

FRU Name	Serial Number	Manufacturer ID	Manufacturer Date
CPU 1	Not Available	Intel(R) Corporation	Not Available
DASD Backplane 1	Y010RW2AM12X	USIS	1996-01-01
DIMM 1	3B9F3344	Hynix Semiconductor	2012-10-15
Power Supply 1	YK10112BC2B2	ACBE	1996-01-01
System Board	Y010RW2BG0DZ	IBM Corporation	2012-11-05

Wählen Sie die untergeordnete 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

System Status Events Service and Support Server Management IMM Management Search...

Server Properties

Various properties, status and settings related to your system.

Apply Reset

General Settings LEDs Hardware Information Environmentals Hardware Activity

Hardware Information

This section lists vital product data (VPD) on a system, component and network basis.

System Information System Component Information Network Hardware

Host Ethernet MAC Address Number	MAC Address
Host Ethernet MAC Address 1	5C:F3:FC:3C:13:D0
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.

IBM Integrated Management Module II

USERID Settings Log out IBM

System Status Events Service and Support Server Management IMM Management Search

Server Properties

Various properties, status and settings related to your system.

Apply Reset

General Settings LEDs Hardware Information Environmentals Hardware Activity

Environmentals

This section displays the current voltage and temperature readings for various hardware components in this system. All voltage readings are displayed in Volts. All temperature readings are displayed in degrees Fahrenheit or degrees Celsius depending on your location.

Voltages

Show Thresholds

Source	Value (Volts)	Status	Fatal Lower Threshold	Critical Lower Threshold	Non-critical Lower Threshold	Non-critical Upper Threshold	Critical Upper Threshold	Fatal Upper Threshold
Planar 3.3V	3.39	Normal	N/A	3.04	N/A	N/A	3.56	N/A
Planar 5V	5.08	Normal	N/A	4.44	N/A	N/A	5.53	N/A
Planar 12V	12.25	Normal	N/A	10.95	N/A	N/A	13.23	N/A
Planar VBAT	3.20	Normal	N/A	2.00	2.27	N/A	N/A	N/A

Temperatures

Show Thresholds

Source	Value (°F)	Status	Fatal Lower Threshold	Critical Lower Threshold	Non-critical Lower Threshold	Non-critical Upper Threshold	Critical Upper Threshold	Fatal Upper Threshold
Ambient Temp	78.80	Normal	N/A	N/A	N/A	109.40	114.80	122.00
PCI Riser Temp	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CPU 1 Temp	95.00	Normal	N/A	N/A	N/A	N/A	N/A	N/A

Die Registerkarte **Hardware Activity** (Hardware-Aktivität) auf der Seite "Server Properties" (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 Management Module II

USERID Settings Log out IBM

System Status Events Service and Support Server Management IMM Management Search

Server Properties

Various properties, status and settings related to your system.

Apply Reset

General Settings LEDs Hardware Information Environmentals Hardware Activity

Hardware Activity

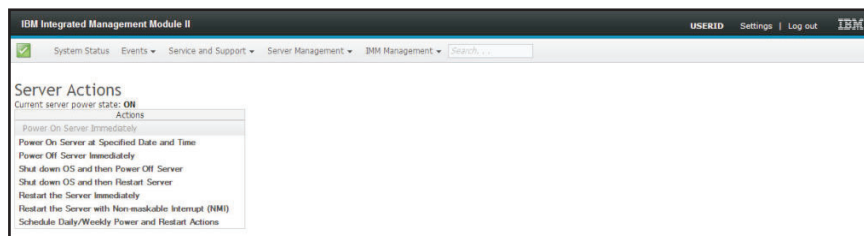
This table contains a history of Field Replaceable Unit (FRU) components which have been added to or removed from the system.

FRU Name	Serial Number	Manufacturer ID	Action	Time of Action
CPU/IMM Tray	Y135B61C000R	CLON	Added	19 Jul 2012 09:12 AM
Power Supply 1	K10511BE085	Delta	Added	19 Jul 2012 09:12 AM
Power Supply 2	K10511BE00F	Delta	Added	19 Jul 2012 09:12 AM
SAS Backplane 1	Y011U515G98C	MOLX	Added	19 Jul 2012 09:12 AM
CPU 1	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM
CPU 2	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM
CPU 3	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM
CPU 4	Not Available	Intel(R) Corporation	Added	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.

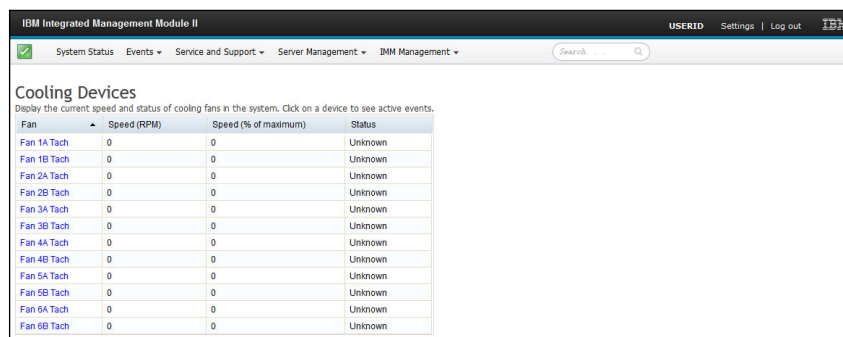


Sie können auswählen, dass der Server sofort oder zu einem geplanten Zeitpunkt eingeschaltet wird. Sie können auch auswählen, dass das Betriebssystem heruntergefahren und erneut gestartet wird. Weitere Informationen zum Steuern der Stromversorgung des Servers finden Sie unter „Stromversorgungsstatus des Servers steuern“ auf Seite 128.

Cooling Devices (Kühlungseinheiten)

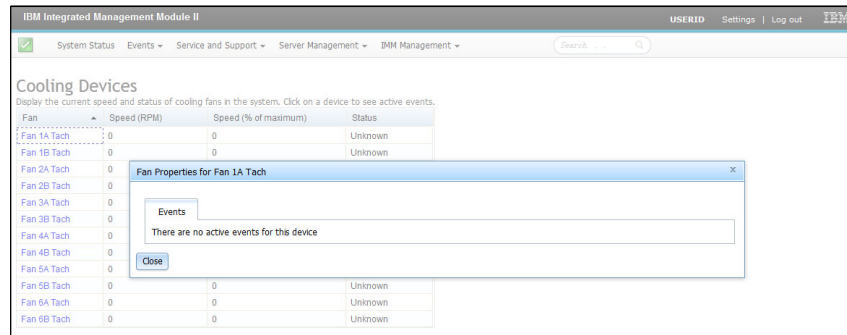
Wählen Sie die Option **Cooling Devices** (Kühlungseinheiten) auf der Registerkarte **Server Management** (Serververwaltung) aus, um die aktuelle Geschwindigkeit und den aktuellen Status von Lüftern im Server anzuzeigen (wie in der folgenden Abbildung gezeigt).

Anmerkung: In einem IBM Flex System werden Einstellungen für die Kühlungseinheiten vom IBM Flex System Chassis Management Module (CMM) verwaltet und können auf dem IMM2 nicht geändert werden.



Fan	Speed (RPM)	Speed (% of maximum)	Status
Fan 1A Tach	0	0	Unknown
Fan 1B Tach	0	0	Unknown
Fan 2A Tach	0	0	Unknown
Fan 2B Tach	0	0	Unknown
Fan 3A Tach	0	0	Unknown
Fan 3B Tach	0	0	Unknown
Fan 4A Tach	0	0	Unknown
Fan 4B Tach	0	0	Unknown
Fan 5A Tach	0	0	Unknown
Fan 5B Tach	0	0	Unknown
Fan 6A Tach	0	0	Unknown
Fan 6B Tach	0	0	Unknown

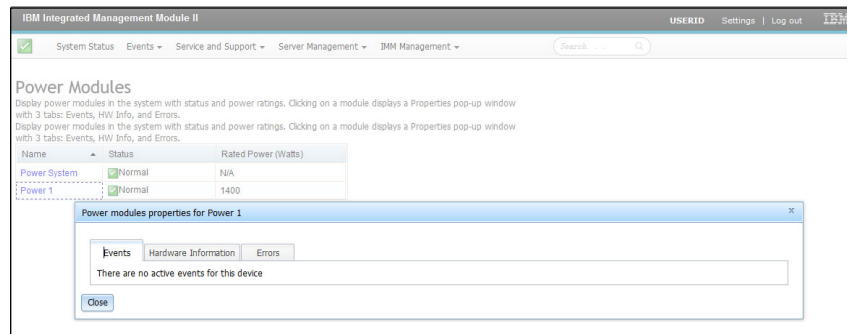
Klicken Sie auf eine Kühlungseinheit (Link zu einem Lüfter) in der Tabelle, um die aktiven Ereignisse für die Einheit anzuzeigen (wie in der folgenden Anzeige dargestellt).



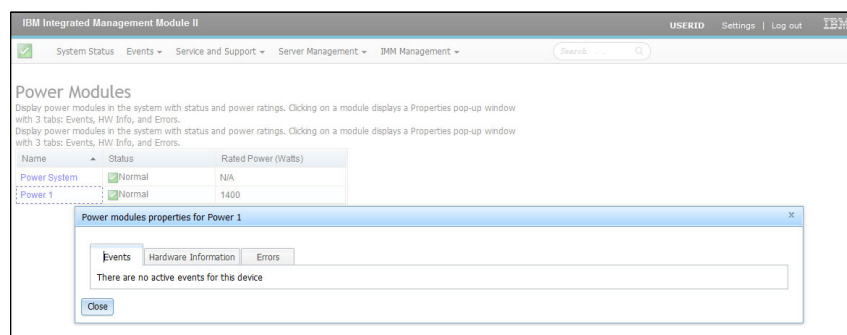
Power Modules (Stromversorgungsmodule)

Wählen Sie die Option **Power Modules** (Stromversorgungsmodule) auf der Registerkarte **Server Management** (Serververwaltung) aus, um die Stromversorgungsmodule im System samt deren Status und Belastbarkeit anzuzeigen. Klicken Sie in der Tabelle auf einen Link, um dem Stromversorgungsmodul zugeordnete aktive Ereignisse, Hardwareinformationen und Fehler anzuzeigen (wie in der folgenden Abbildung dargestellt).

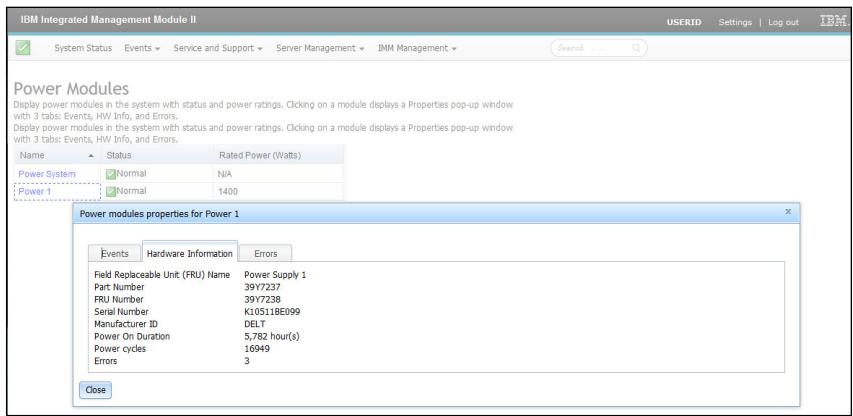
Anmerkung: In einem IBM Flex System werden Einstellungen für die Stromversorgungsmodule vom IBM Flex System Chassis Management Module (CMM) verwaltet und können auf dem IMM2 nicht geändert werden.



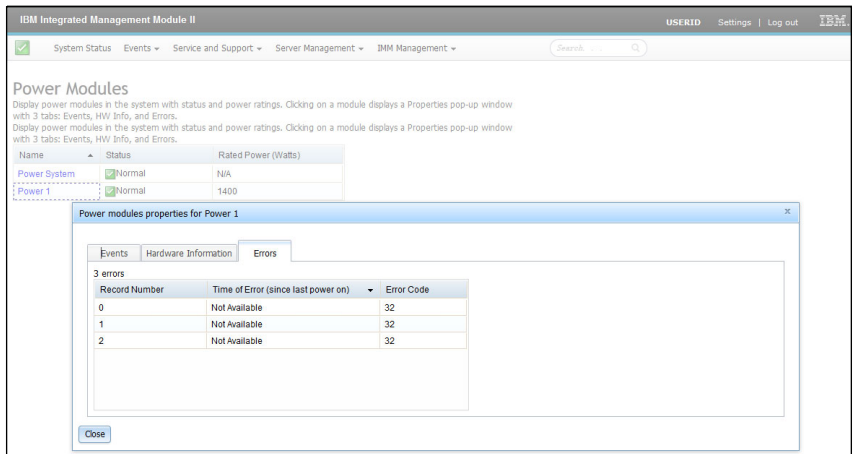
Auf der Registerkarte **Events** (Ereignisse) werden aktive Ereignisse (falls vorhanden) angezeigt (wie in der folgenden Anzeige dargestellt).



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).



Klicken Sie auf die Registerkarte **Errors** (Fehler), um detaillierte Informationen zu den Fehlern bei den Stromversorgungsmodulen anzuzeigen (wie in der folgenden Abbildung dargestellt).



Option "Local Storage"

Wählen Sie die Option **Local Storage** (Lokaler Speicher) auf der Registerkarte **Server Management** (Serververwaltung) oder den Link "Local Storage" in der Tabelle "Hardware Health" (Hardwarezustand) auf der Seite "System Status and Health" (Systemstatus und -zustand) aus, um Informationen zur Konfiguration des lokalen Speichers für den Server anzuzeigen. Mit dieser Option können Sie detaillierte Informationen zu den lokalen Speichereinheiten im Server anzeigen (wie in der folgenden Abbildung dargestellt). Sie können die physischen und die logischen Informationen für die lokalen Speichereinheiten anzeigen. Es werden Informationen zu unterstützten RAID-Controllern und den zugehörigen Platten sowie zu Speicher-pools und Datenträgerinformationen bereitgestellt.

Anmerkung: Wenn der Server die Option **Local Storage** nicht unterstützt, werden nur der Status der Platten und die zugehörigen aktiven Ereignisse angezeigt.

Local Storage

Display storage devices physical structure and storage configuration. You can refresh to get latest status.

[Refresh](#)

[Physical Resource](#) [Storage RAID Configuration](#)

Click on a device to see active events and properties.

RAID Controllers and Physical Drives

Name	Health Status	Capacity	Serial No
ServeRAID M5110e(PCI Slot 0)			23V04K
Drive 0	Normal	68.366GB	BSF032F1
Drive 1	Normal	68.366GB	3TA0M77Y
Drive 2	Normal	68.366GB	D3A04350
Drive 3	Critical	232.886GB	9XE0925FST9250610NS
Drive 4	Normal	68.366GB	D3A0439D
Drive 5	Normal	279.397GB	S0K0ATYN
Drive 6	Critical	232.886GB	9XE05Q69ST9250610NS
Drive 7	Normal	136.732GB	6TB1YZK2

Flash DIMMs

Name	Health Status	Capacity
No FlashDIMM is installed in the system or FlashDIMM information is not retrieved at this time		

Memory (Speicher)

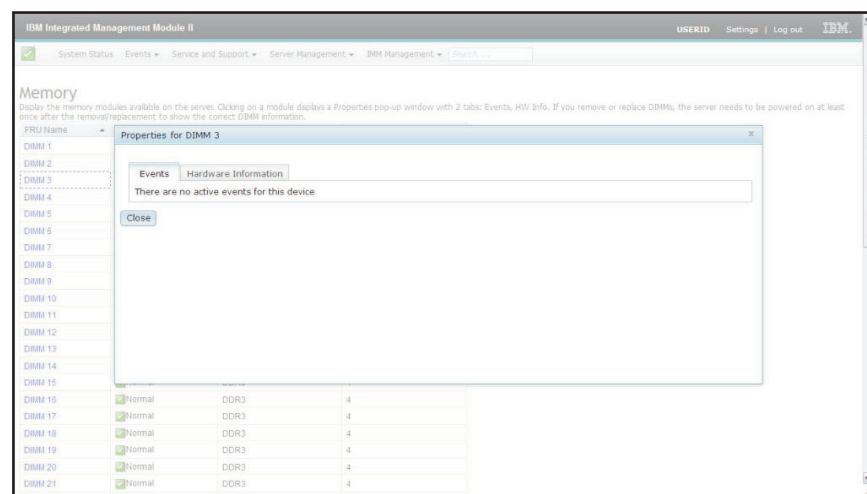
Wählen Sie auf der Registerkarte **Server Management** die Option **Memory** (Speicher) aus, um Informationen zu den im System installierten Speichermodulen anzuzeigen. Eine Seite, die der folgenden Abbildung ähnelt, wird angezeigt. In der Tabelle wird jedes Speichermodul als Link angezeigt, auf den 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.

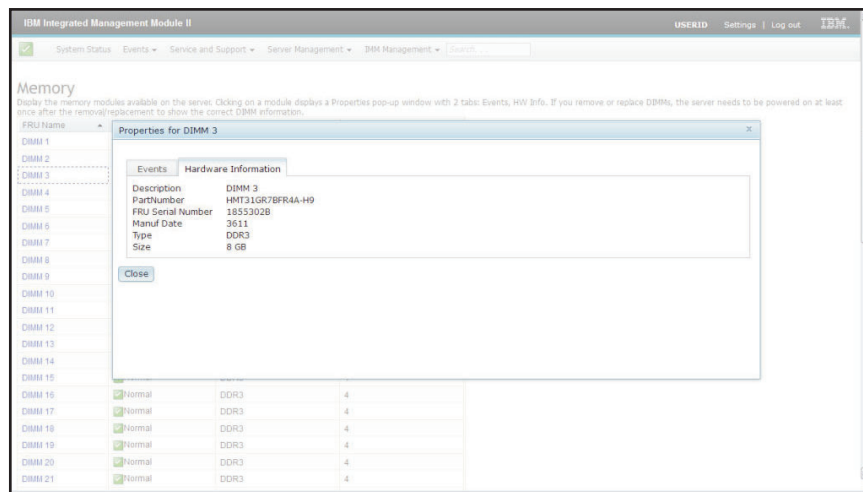
Memory
Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Events, HW Info. If you remove or replace DIMMs, the server needs to be powered on at least once after the removal/replacement to show the correct DIMM information.

FRU Name	Status	Type	Capacity (GB)
DIMM 1	Normal	DDR3	8
DIMM 2	Normal	DDR3	8
DIMM 3	Normal	DDR3	8
DIMM 4	Normal	DDR3	8
DIMM 5	Normal	DDR3	8
DIMM 6	Normal	DDR3	8
DIMM 7	Normal	DDR3	8
DIMM 8	Normal	DDR3	8
DIMM 9	Normal	DDR3	8
DIMM 10	Normal	DDR3	8
DIMM 11	Normal	DDR3	8
DIMM 12	Normal	DDR3	8
DIMM 13	Normal	DDR3	4
DIMM 14	Normal	DDR3	4
DIMM 15	Normal	DDR3	4
DIMM 16	Normal	DDR3	4
DIMM 17	Normal	DDR3	4
DIMM 18	Normal	DDR3	4
DIMM 19	Normal	DDR3	4
DIMM 20	Normal	DDR3	4
DIMM 21	Normal	DDR3	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).

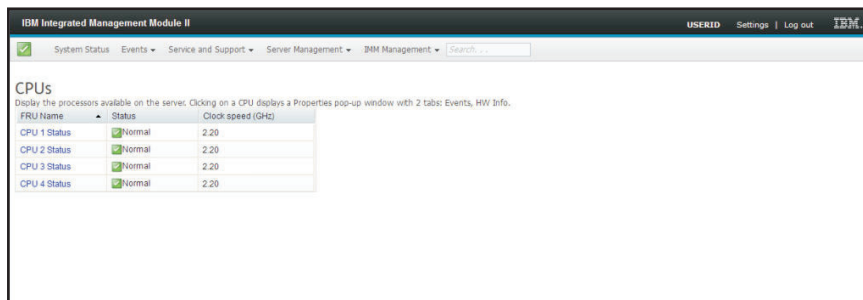


Klicken Sie auf die Registerkarte **Hardware Information**, um Details zu der betreffenden Komponente anzuzeigen, wie z. B. Beschreibung, Teilenummer, FRU-Seriennummer, Produktionsdatum (Woche/Jahr), Typ (z. B. DDR3) und Größe in Gigabyte (wie in der folgenden Abbildung dargestellt).

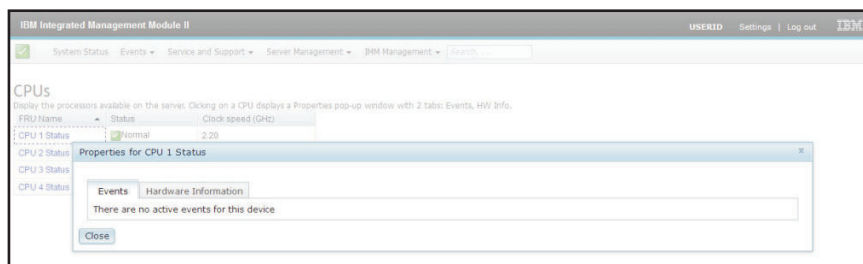


Processors (Prozessoren)

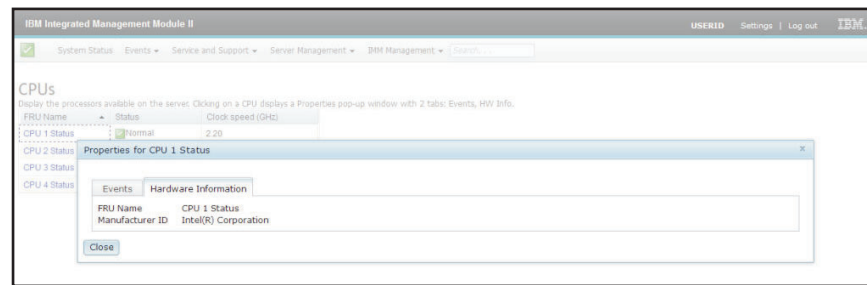
Wählen Sie die Option **Processors** (Prozessoren) auf der Registerkarte **Server Management** (Serververwaltung) aus, um Informationen zu den im System installierten Mikroprozessoren anzuzeigen. Das folgende Fenster wird geöffnet.



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).



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).



Adapter

Wählen Sie die Option **Adapters** (Adapter) auf der Registerkarte **Server Management** (Serververwaltung) aus, um Informationen zu den im Server installierten PCIe-Adaptoren anzuzeigen. Jeder Adapter und seine Funktion werden mit der zugehörigen Kartensteckplatznummer, dem Einheitentyp und den Kartenschnittstelleninformationen aufgelistet (wie in der der folgenden Abbildung dargestellt).

Anmerkungen:

- Wenn der Server die Option "Adapters" nicht unterstützt, ist diese Option nicht sichtbar.
- Wenn Sie Adapter entfernen, austauschen oder konfigurieren, müssen Sie den Server (mindestens ein mal) erneut starten, um die aktualisierten Adapterinformationen anzeigen zu können.

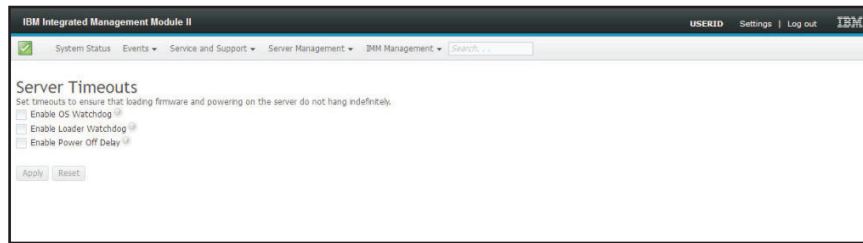
Adapters			
Display Adapters information. Click the link of each device to view more details. If you remove or replace adapters, the server needs to be powered on at least once after the removal/replacement to show the correct adapters information.			
Slot No.	Device Name	Device Type	Card Interface
OnBoard	Adapter 8B:01:07		Onboard
	...Function 8B:01:00	Ethernet	
	...Function 8B:01:01	Ethernet	
	...Function 8B:01:02	Ethernet	
OnBoard	...Function 8B:01:03	Ethernet	
	Adapter 09:00:00	GPU	Onboard
OnBoard	IBM Flex System 4-port 10GbE LOM Virtual Fabric Adapter 8B:00:00		Onboard
	...IBM Flex System 4-port 10GbE LOM Virtual Fabric Adapter 8B:00:00	Ethernet	
	...IBM Flex System 4-port 10GbE LOM Virtual Fabric Adapter 8B:00:01	Ethernet	
	...IBM Flex System 4-port 10GbE LOM Virtual Fabric Adapter 8B:00:02	Ethernet	
2	...IBM Flex System 4-port 10GbE LOM Virtual Fabric Adapter 8B:00:03	Ethernet	
	IBM Flex System IB6132D 2-port FDR InfiniBand Adapter	Ethernet	FlexSystem Mezzanine Connector

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 der Server bei einer Firmwareaktualisierung oder beim Einschalten nicht auf unabsehbare Zeit 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 103.

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



Weitere Informationen zu Zeitlimits für Server finden Sie unter „Serverzeitlimits festlegen“ auf Seite 74.

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 143.

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.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

Weitere Informationen zur Option "Latest OS Failure Screen" finden Sie im Abschnitt „Daten der letzten Betriebssystem-Fehleranzeige erfassen“ auf Seite 158.

Stromverbrauchssteuerung

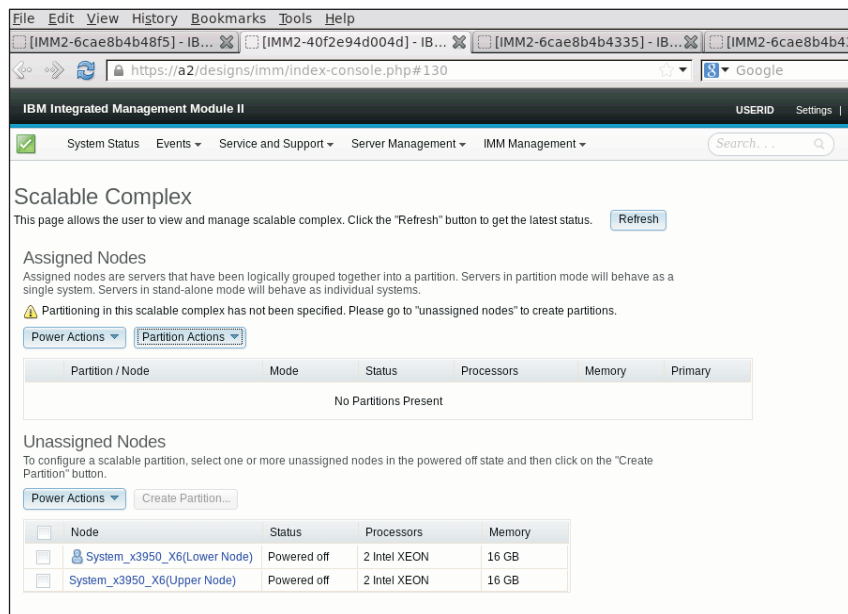
Verwenden Sie die Option **Power Management**, um die folgenden Tasks auszuführen:

- 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. Weitere Informationen zur Option **Power Management** finden Sie im Abschnitt „Serverstromversorgung verwalten“ auf Seite 159.

Skalierbarer Komplex

Wählen Sie die Option **Scalable Complex** (Skalierbarer Komplex) auf der Registerkarte **Server Management** (Serververwaltung) aus, um den aktuellen Zustand aller verfügbaren Knoten (Server) anzuzeigen und zu verwalten. Ein skalierbarer Komplex ermöglicht das Gruppieren von Knoten in logische Gruppen ("Partitionen") oder das Trennen voneinander in unabhängige Knoten. Knoten in einer Partition agieren als ein einzelnes System und können gemeinsam Ressourcen nutzen. Ein Knoten im Standalone-Modus (unabhängigen Modus) agiert als einzelner Knoten. Weitere Informationen zur Option **Scalable Complex** finden Sie im Abschnitt „Skalierbaren Komplex verwalten“ auf Seite 166. In der folgenden Abbildung ist das Fenster "Scalable Complex" dargestellt.



Registerkarte "IMM Management" (IMM-Verwaltung)

Dieser Abschnitt enthält Informationen zu den Optionen auf der Registerkarte **IMM Management** (IMM-Verwaltung) auf der Homepage der IMM2-Webbenutzerschnittstelle.

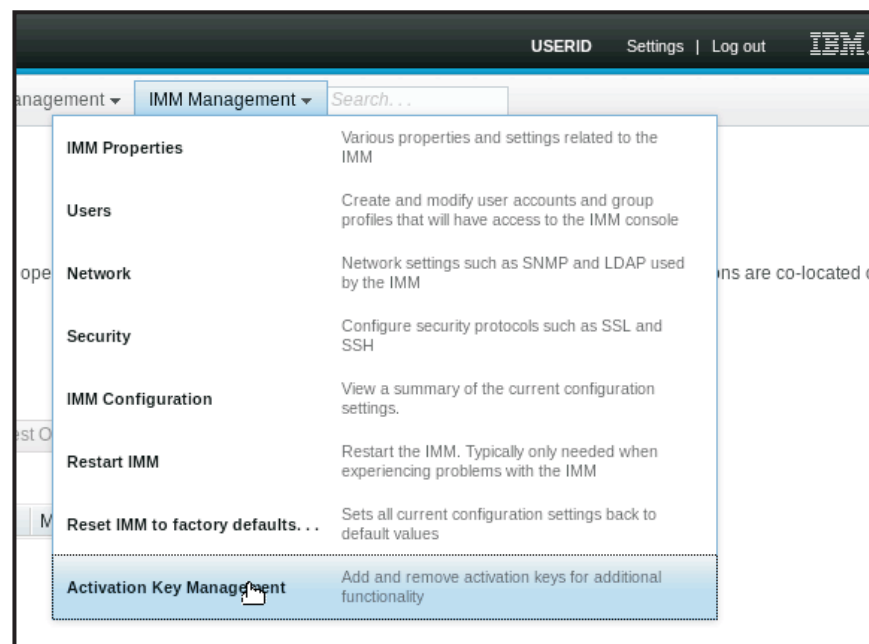
Die Optionen auf der Registerkarte **IMM Management** ermöglichen Ihnen das Anzeigen und Ändern der IMM2-Einstellungen. Eine Liste der Optionen und ausführliche Informationen zur Verwendung dieser Optionen zum Konfigurieren des IMM2 finden Sie in Kapitel 4, „IMM2 konfigurieren“, auf Seite 71.

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 zurücksetzen)
- Activation Key Management (Aktivierungsschlüsselverwaltung)

Anmerkung: In einem IBM Flex System werden manche Einstellungen vom IBM Flex System Chassis Management Module (CMM) verwaltet und können auf dem IMM2 nicht geändert werden.



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
- Zeitzoneinformationen für das IMM2 festlegen
- Auf Informationen zum seriellen Anschluss des IMM2 zugreifen:
 - Seriellen Anschluss des IMM2 konfigurieren
 - Tastenkombinationen für die Befehlszeilenschnittstelle (CLI - Command-Line Interface) 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 für 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
 - Virtual LAN (VLAN) aktivieren
- SNMP-Einstellungen konfigurieren:
 - Aktivierung und Konfiguration von SNMPv1:
 - Kontaktinformationen festlegen
 - Communityverwaltung
 - Aktivierung und Konfiguration von SNMPv3:
 - Kontaktinformationen festlegen
 - Konfiguration von Benutzerkonten
 - Aktivierung und Konfiguration von SNMP-Traps

- Ereignisse, auf die in der Registerkarte "Traps" aufmerksam gemacht wird, konfigurieren
- 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 Servicennamen 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 für 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-über-USB
 - Aktivierung und Verwaltung der Weiterleitung von externem Ethernet-Port zu Ethernet-über-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
- Verschlüsselungsverwaltung

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.

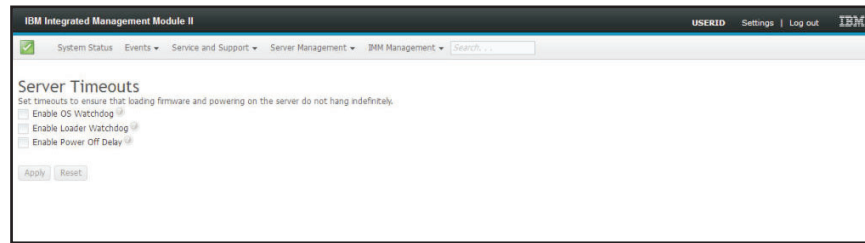
Über die Seite "Reset IMM2 to factory defaults..." (IMM2 auf werkseitige Voreinstellungen zurücksetzen) können Sie die IMM2-Konfiguration auf die werkseitig vorgenommenen Standardeinstellungen zurücksetzen.

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 179.

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, damit Befehle verwendet werden können. Weitere Informationen zur Aktivierung und Inaktivierung der USB-Schnittstelle finden Sie im Abschnitt „USB konfigurieren“ auf Seite 103.



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 „Am IMM2 anmelden“ auf Seite 12).
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 aus- und 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)

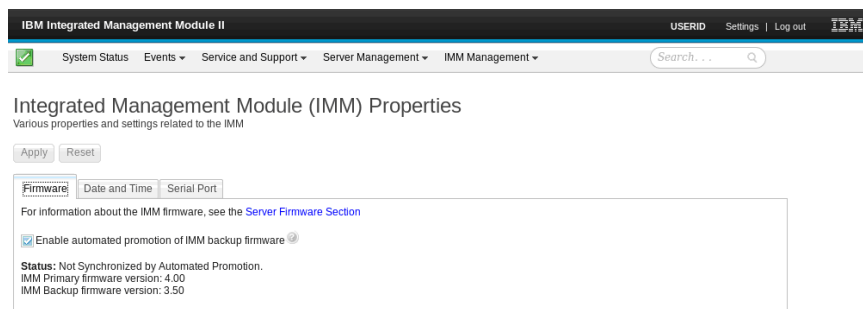
Verwenden Sie das Feld **Enable Power Off Delay**, um anzugeben, wie viele Minuten das IMM2-Subsystem darauf warten soll, dass das Betriebssystem herunterfährt, bevor es die Stromversorgung des Servers abschaltet. Zum Festlegen des Wertes für die Ausschaltverzögerung wählen Sie aus, wie lange das IMM2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

Einstellungen für die automatisierte Hochstufung der IMM2-Firmware ändern

Wählen Sie die Registerkarte **Firmware** aus, um die Einstellung für die automatisierte Firmwarehochstufung für die IMM2-Sicherungsfirmware anzuzeigen oder zu ändern. Wenn sie aktiviert ist, kopiert die Funktion "Automated Promotion" (Automatisierte Hochstufung) automatisch die IMM2-Firmware aus dem Primärbereich in den Sicherungsbereich, wenn die Firmware im Primärbereich eine bestimmte Zeit erfolgreich ausgeführt wurde. Diese Aktion bewirkt, dass die Firmwareversion im Primär- und im Sicherungsbereich die gleiche ist. Wenn Sie möchten, dass der Primär- und der Sicherungsbereich unterschiedliche Versionen der IMM2-Firmware enthalten, sollten Sie das Kontrollkästchen bei **Enable automated promotion of IMM backup firmware** (Automatisierte Hochstufung der IMM-Sicherungsfirmware aktivieren) nicht auswählen.

Die IMM2-Firmware verwendet unterschiedliche Kennzahlen wie beispielsweise die Menge an Ausführungszeit und Firmwareaktivität, um die Stabilität der Firmware im Primärbereich zu überprüfen, bevor diese in den Sicherungsbereich kopiert wird. Das Mindestintervall vor der automatisierten Hochstufung beträgt zwei Wochen. Das tatsächliche Intervall kann jedoch länger sein, je nach der IMM2-Aktivität während dieses Zeitraums.

In der folgenden Abbildung ist die Registerkarte **Firmware** mit ausgewähltem Kontrollkästchen bei **Enable automated promotion of IMM backup firmware** dargestellt.



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.

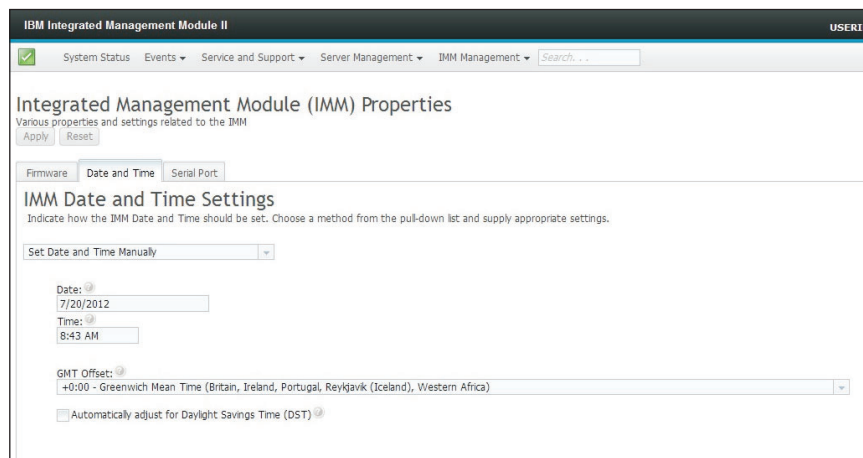
Die Datums- und Uhrzeiteinstellung des IMM2 wirkt sich nur auf den IMM2-Taktgeber und nicht auf den Servertaktgeber aus. Beim IMM2-Taktgeber und beim Servertaktgeber handelt es sich um separate, voneinander unabhängige Taktgeber, die auf unterschiedliche Uhrzeiten eingestellt werden können.

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** (Angaben, 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.



Einstellungen für Datum und Uhrzeit ändern (NTP-Servermodus)

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

1. Klicken Sie in der Liste **Indicate how the IMM date and time should be set** (Angaben, 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.

Einstellungen für den seriellen Anschluss konfigurieren

Wählen Sie die Registerkarte **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 Intelligent Platform Management Interface (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".

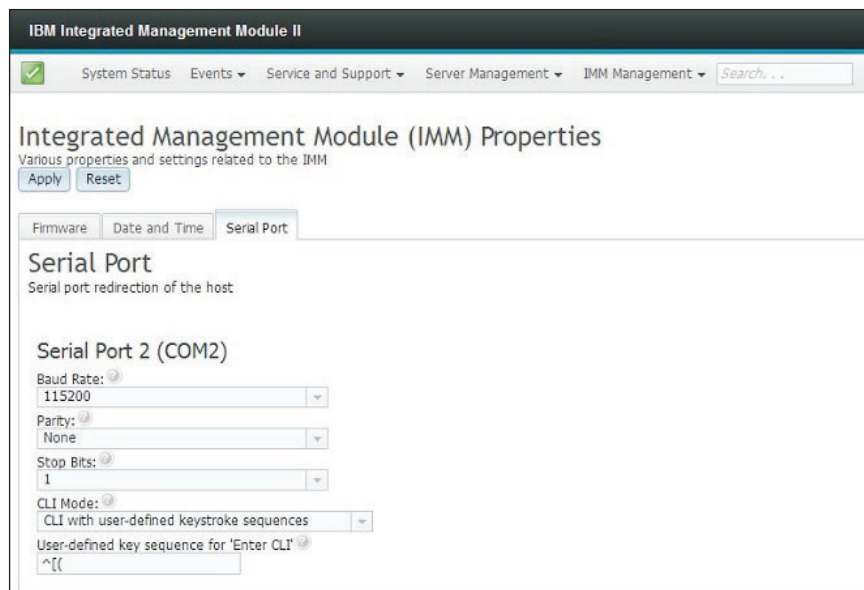
CLI Mode (CLI-Modus)

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** (Serieller Anschluss) dargestellt.



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.



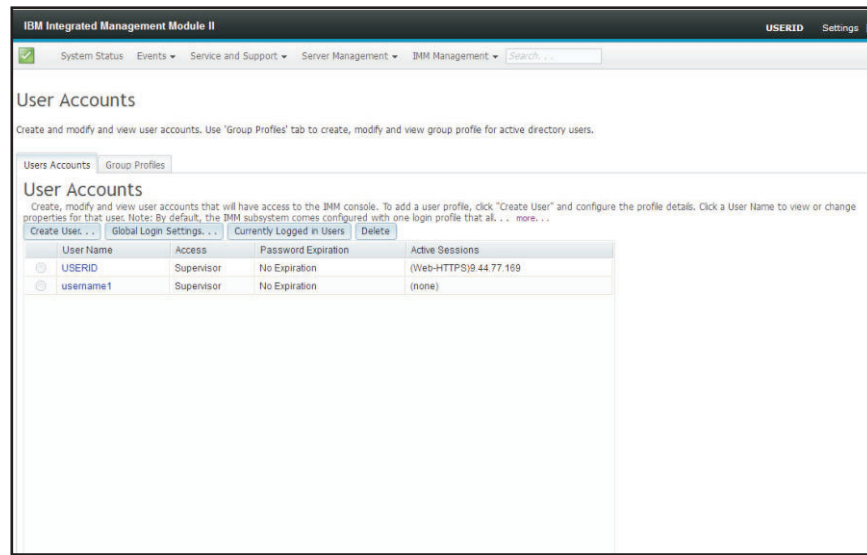
In einem IBM Flex System wird von in den IMM2-Einstellungen konfigurierten Benutzerkonten nur der Zugriff auf das IMM2 über IPMI- und SNMPv3-Protokolle authentifiziert. Wenn ein Benutzer das CMM für die zentrale Verwaltung der IPMI- und SNMPv3-Benutzerkonten auf dem IMM2 konfiguriert hat, können Sie die Konten nicht direkt im IMM2 selbst konfigurieren. Der Zugriff auf andere IMM2-Schnittstellen wie beispielsweise das Web und die Befehlszeilenschnittstelle wird

mithilfe der Kontoberechtigungsnachweise authentifiziert, die sich auf dem LDAP-Server befinden, für dessen Verwendung das IMM2 vom CMM konfiguriert wurde.

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.



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 User

User Credentials

Enter a user name and password.

Authority: SNMPv3

User name: username1

Password:

Confirm password:

User name rules:

- ☒ Must be 1-16 characters
- ☒ Cannot contain white space characters
- ☒ Can only contain the characters A-Z, a-z, 0-9, '.' (underscore) and '.' (period)
- ☒ Must be different for each user

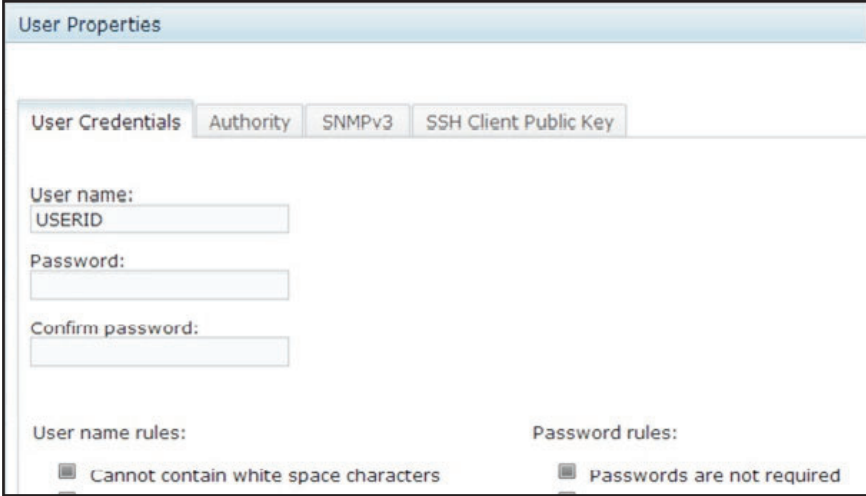
Password rules:

- ☒ Passwords are not required
- ☒ Must be 0-20 characters
- ☒ Cannot contain white space characters
- ☒ Password and password confirm values must match
- ☒ Can only contain the characters A-Z, a-z, 0-9, ~, !, @, #, \$, %, ^, &, * (), +, =, {, }, [], ;, ' ", <, >, /

< Back Next > Finish Cancel

Benutzereigenschaften

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



Benutzerberechtigung

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

Supervisor (Administrator)

Für die Benutzerberechtigungsstufe "Supervisor" gelten keine Einschränkungen.

Read only (Lesezugriff)

Die Benutzerberechtigungsstufe "Read only" (Lesezugriff) verfügt nur über Lesezugriff und kann keine Aktionen wie z. B. Dateiübertragungen, Einschalt- und Neustartaktionen sowie Remote-Presence-Funktionen ausführen.

Custom (Angepasst)

Die Benutzerberechtigungsstufe "Custom" ermöglicht ein besser angepasstes Profil für Benutzerberechtigungen mit Einstellungen für die Aktionen, die ein Benutzer ausführen darf.

Wählen Sie mindestens eine der folgenden Benutzerberechtigungsstufen für "Custom" aus:

User Account Management (Benutzerkontenverwaltung)

Benutzer können andere Benutzer hinzufügen, ändern oder löschen und die globalen Anmeldungseinstellungen ändern.

Remote Console Access (Zugriff auf ferne Konsole)

Benutzer können auf die ferne Konsole zugreifen.

Remote Console and Virtual Media Access (Zugriff auf ferne Konsole und virtuelle Datenträger)

Benutzer können auf die ferne Konsole und auf die Funktion für virtuelle Datenträger zugreifen.

Remote Server Power/Restart Access (Berechtigung für Einschalten/Neustart des fernen Servers)

Benutzer können Einschalt- und Neustartfunktionen für den fernen Server ausführen.

Ability to Clear Event Logs (Fähigkeit, Ereignisprotokolle zu löschen)

Benutzer können die Ereignisprotokolle löschen. Jeder kann die Ereignisprotokolle einsehen; zum Löschen der Protokolle ist jedoch diese Berechtigungsstufe erforderlich.

Adapter Configuration - Basic (Adapterkonfiguration - Allgemein)

Benutzer können Konfigurationsparameter auf den Seiten "Server Properties" (Servereigenschaften) und "Events" (Ereignisse) ändern.

Adapter Configuration - Networking & Security (Adapterkonfiguration - Netzbetrieb & Sicherheit)

Benutzer können Konfigurationsparameter auf den Seiten "Security" (Sicherheit), "Network" (Netz) und "Serial Port" (Serieller Anschluss) ändern.

Adapter Configuration - Advanced (Adapterkonfiguration - Erweitert)

Für Benutzer gelten keine Einschränkungen beim Konfigurieren des IMM2. Außerdem soll der Benutzer über Verwaltungszugriff auf das IMM2 verfügen. Der Verwaltungszugriff umfasst die folgenden erweiterten Funktionen: Firmwareaktualisierungen, PXE-Netzboot, Wiederherstellen von werkseitigen IMM2-Voreinstellungen, Ändern und Wiederherstellen von IMM2-Einstellungen aus einer Konfigurationsdatei sowie Neustart und Zurücksetzen des IMM2.

Wenn ein Benutzer die Berechtigungsstufe einer IMM2-Anmelde-ID festlegt, wird die daraus resultierende IPMI-Berechtigungsstufe der zugehörigen IPMI-Benutzer-ID entsprechend den folgenden Prioritäten festgelegt:

- Wenn ein Benutzer die Berechtigungsstufe für die IMM2-Anmelde-ID auf **Super-visor** setzt, wird die IPMI-Berechtigungsstufe auf "Administrator" gesetzt.
- Wenn ein Benutzer die Berechtigungsstufe für die IMM2-Anmelde-ID auf **Read Only** setzt, wird die IPMI-Berechtigungsstufe auf "User" (Benutzer) gesetzt.
- Wenn ein Benutzer die Berechtigungsstufe für die IMM2-Anmelde-ID auf einen der folgenden Zugriffstypen setzt, wird die IPMI-Berechtigungsstufe auf "Administrator" gesetzt:
 - User Account Management Access (Zugriff auf Benutzerkontenverwaltung)
 - Remote Console Access (Zugriff auf ferne Konsole)
 - Remote Console and Remote Disk Access (Zugriff auf ferne Konsole und fernen Datenträger)
 - Adapter Configuration - Networking & Security (Adapterkonfiguration - Netzbetrieb & Sicherheit)
 - Adapter Configuration - Advanced (Adapterkonfiguration - Erweitert)
- Wenn ein Benutzer die Berechtigungsstufe für die IMM2-Anmelde-ID auf **Remote Server Power/Restart Access** (Berechtigung für Einschalten/Neustart des fernen Servers) oder auf **Ability to Clear Event Logs** (Fähigkeit, Ereignisprotokolle zu löschen) setzt, wird die IPMI-Berechtigungsstufe auf "Operator" (Bediener) gesetzt.
- Wenn ein Benutzer die Berechtigungsstufe für die IMM2-Anmelde-ID auf **Adapter Configuration - Basic** (Adapterkonfiguration - Allgemein) setzt, wird die IPMI-Berechtigungsstufe auf "User" (Benutzer) gesetzt.

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 SNMPv3-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)

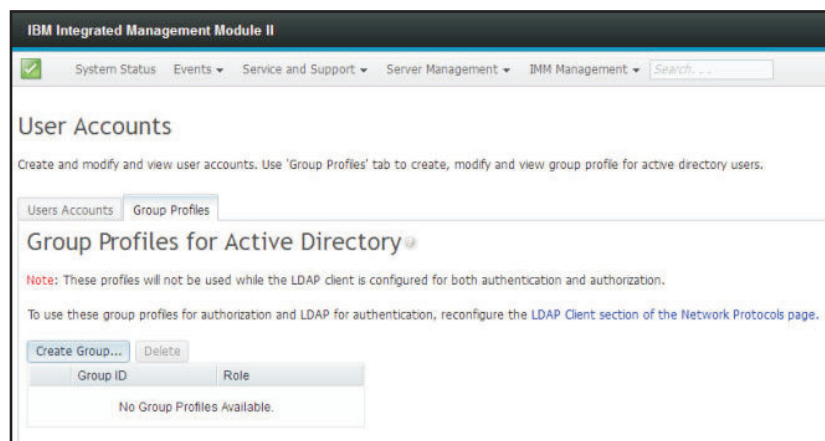
Geben Sie als Zugriffstyp entweder **Get** (Abrufen) oder **Set** (Festlegen) an. SNMPv3-Benutzer mit dem Zugriffstyp **Get** können nur Abfrageoperationen ausführen. SNMPv3-Benutzer mit dem Zugriffstyp **Set** können Abfrageoperationen ausführen und Einstellungen ändern (z. B. das Kennwort für einen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



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

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, etc.)

☐ **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 82).

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 Management Module II

System Status Events Service and Support Server Management IMM Management Search

User Accounts

Create and modify and view user accounts. Use 'Group Profiles' tab to create, modify and view group profile for active directory users.

Users Accounts **Group Profiles**

Group Profiles for Active Directory

Note: These profiles will not be used while the LDAP client is configured for both authentication and authorization.

To use these group profiles for authorization and LDAP for authentication, reconfigure the LDAP Client section of the Network Protocols page.

Create Group... Delete

Group ID	Role
groupProfile1	Supervisor

Confirm Group Deletion

Do you want to delete the group "groupProfile1"?

OK Cancel

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.

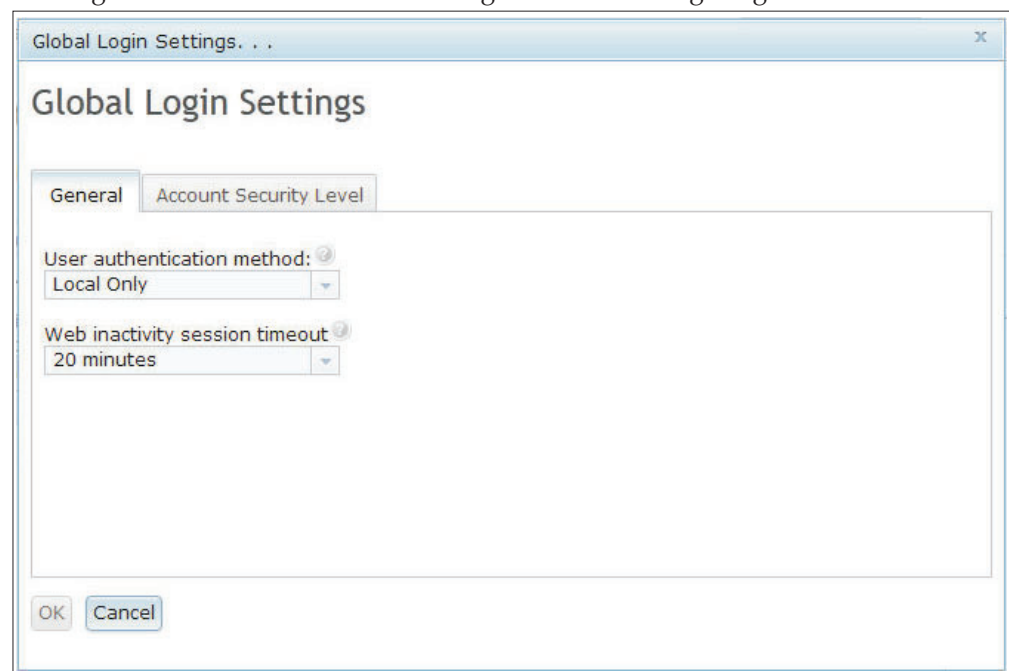
Anmerkungen:

- 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 21.

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



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.

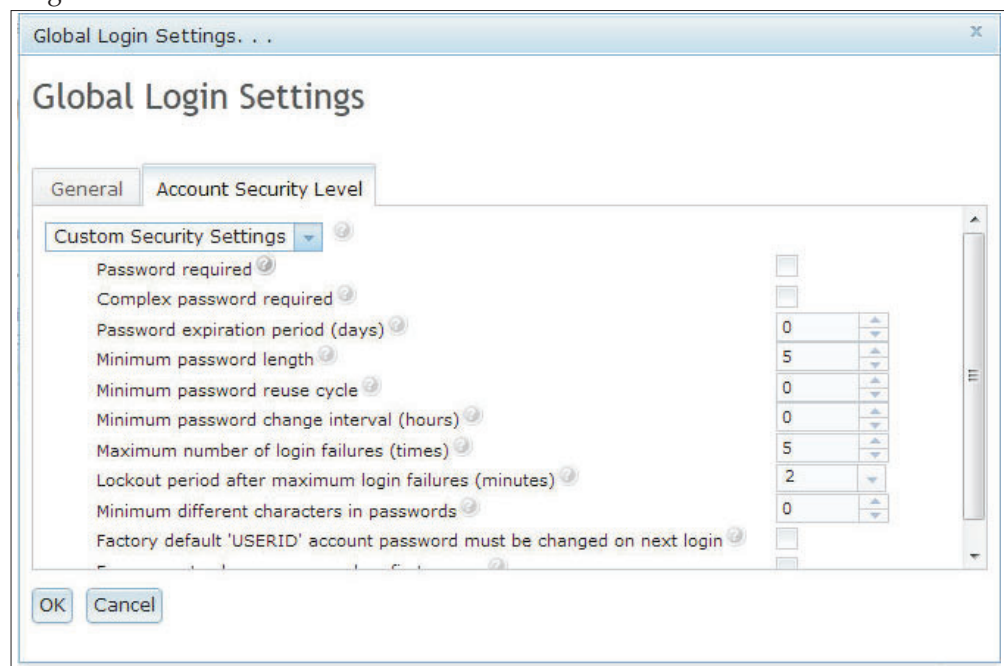
Anmerkung: Wenn Sie das Browserfenster geöffnet lassen, während Sie eine IMM2-Webseite anzeigen, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch aufgrund von Inaktivität geschlossen.

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.



Wählen Sie aus der Elementliste mit Sicherheitseinstellungen die Einstellungen für die Kontensicherheitsrichtlinie aus.

Anmerkungen:

- 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 4. Werte für Sicherheitseinstellungsrichtlinie

Richtlinieneinstellung/-feld	Legacy Security Settings	High Security Settings	Custom Security Settings
Password required (Kennwort erforderlich)	Nein	Ja	Ja oder Nein
Complex password required (Komplexes Kennwort erforderlich)	Nein	Ja	Ja oder Nein
Password expiration period (days) (Kennwortablaufdauer (Tage))	Keine	90	0 - 365
Minimum password length (Mindestlänge des Kennworts)	Keine	8	5 - 20
Minimum password reuse cycle (Mindestwiederverwendungszyklus des Kennworts)	Keiner	5	0 - 5
Minimum password change interval (hours) (Mindeständerungsintervall für Kennwörter (Stunden))	Keines	24	0 - 240
Maximum number of login failures (times) (Maximale Anzahl an Anmeldefehlern (Anzahl))	5	5	0 - 10
Lockout period after maximum login failures (minutes)	2	60	0 - 240
Minimum different characters in passwords (Mindestanzahl unterschiedlicher Zeichen in Kennwörtern)	Keine	2	0 - 19

Tabelle 4. Werte für Sicherheitseinstellungsrichtlinie (Forts.)

Richtlinieneinstellung/-feld	Legacy Security Settings	High Security Settings	Custom Security Settings
Factory default 'USERID' account password must be changed on next login	Nein	Ja	Ja oder Nein
Force user to change password on first access (Benutzer zwingen, das Kennwort beim ersten Zugriff zu ändern)	Nein	Ja	Ja oder Nein

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 Kennworts) 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 (Mindestanzahl unterschiedlicher 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)

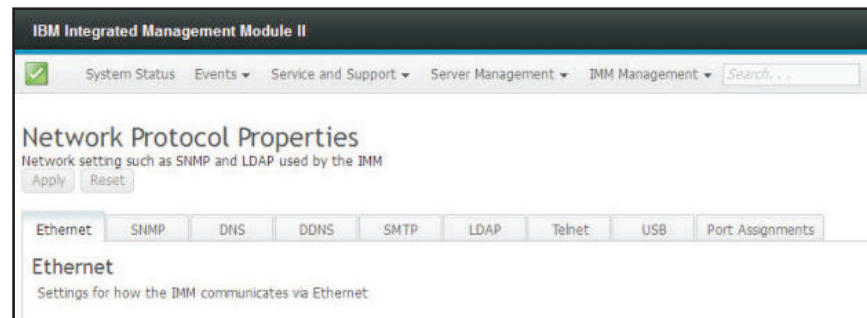
Nachdem ein neuer Benutzer mit einem Standardkennwort konfiguriert wurde, erzwingt die Auswahl dieses Kontrollkästchens, dass der betreffende Benutzer sein Kennwort bei der ersten Anmeldung ändern muss.

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).



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.

Ethernet Advanced Ethernet

Host name: IMM2-e41f13d90631

IPv4 IPv6

☒ Enable IPv4

Currently assigned IPv4 address information

	Address
Host name	IMM2-e41f13d90631
IP address	9.37.189.59
Subnet mask	255.255.240.0
Gateway address	9.37.176.1
Domain name	raleigh.ibm.com
Primary DNS Server	9.0.128.50
Second DNS Server	9.0.130.50
Tertiary DNS Server	0.0.0.0

Configure IP address settings

Obtain IP address from DHCP server

Use static IP address

Obtain IP address from DHCP server

Static address: 192.168.70.125

Subnet mask: 255.255.255.0

Default gateway: 0.0.0.0

Erweiterte Ethernet-Einstellungen konfigurieren

Klicken Sie auf die Registerkarte **Advanced Ethernet** (Erweitertes Ethernet), um zusätzliche Ethernet-Einstellungen festzulegen.

Anmerkung: In einem IBM Flex System werden die VLAN-Einstellungen vom IBM Flex System Chassis Management Module (CMM) verwaltet und können auf dem IMM2 nicht geändert werden.

Zum Aktivieren von VLAN-Tagging wählen Sie das Kontrollkästchen **Enable VLAN** (VLAN aktivieren) aus. Wenn VLAN aktiviert und eine VLAN-ID konfiguriert ist, nimmt das IMM2 nur Pakete mit den angegebenen VLAN-IDs an. Die VLAN-IDs können mit numerischen Werten zwischen 1 und 4094 konfiguriert werden.

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)
 - Wenn ein Wert angegeben wird, setzt die lokal verwaltete Adresse die Herstellerkennung der MAC-Adresse außer Kraft. Die lokal verwaltete Adresse muss ein Hexadezimalwert von 000000000000 bis FFFFFFFF sein. Dieser Wert muss im Format `xx:xx:xx:xx:xx:xx` angegeben werden, wobei `x` für eine Zahl von 0 bis 9 steht. Das IMM2 unterstützt die Verwendung von Multicast-

adressen nicht. Das erste Byte einer Multicastadresse ist eine ungerade Zahl (das niedrigstwertige Bit hat den Wert 1). Aus diesem Grund muss das erste Byte eine gerade Zahl sein.

Geben Sie im Feld **Maximum transmission unit** (Größe zu übertragende Einheit) die größte zu übertragende Einheit eines Datenpakets (in Byte) für Ihre Netz-schnittstelle 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.

The screenshot shows the 'Network Protocol Properties' page for the IBM Integrated Management Module II. The 'Ethernet' tab is selected, and the 'Advanced Ethernet' sub-tab is active. The page displays settings for how the IMM communicates via Ethernet. Key settings include: 'Use Autonegotiation' (checked), 'Enable VLAN' (checked) with a value of 4094, 'MAC selection' set to 'Use burned-in MAC address' with a burned-in address of 6cae:8b:4b:3d:red, and 'Maximum transmission unit (bytes)' set to 1,500. Buttons for 'Apply' and 'Reset' are visible at the top left of the settings area.

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).

The screenshot shows the 'Network Protocol Properties' page for the IBM Integrated Management Module II, with the 'SNMP' tab selected. The page displays settings for the Simple Network Management Protocol (SNMP). Key settings include: 'Enable SNMPv1 Agent' (unchecked), 'Enable SNMPv3 Agent' (unchecked), and 'Enable SNMP Traps' (unchecked). Buttons for 'Apply' and 'Reset' are visible at the top left of the settings area.

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 95 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 SNMP-Managern zu konfigurieren. Sie müssen mindestens eine Community definieren.

Anmerkungen:

- Wenn ein Fenster mit einer Fehlermeldung 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.

- c. 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.

Network Protocol Properties
Network setting such as SNMP and LDAP used by the IMM

Apply Reset

Ethernet **SNMP** DNS DDNS SMTP LDAP Telnet USB Port Assignments

Simple Network Management Protocol (SNMP)
Configure SNMP v1 and/or v3 agents.

☒ Enable SNMPv1 Agent
☐ Enable SNMPv3 Agent
☐ Enable SNMP Traps

Contact Users **Communities** Traps

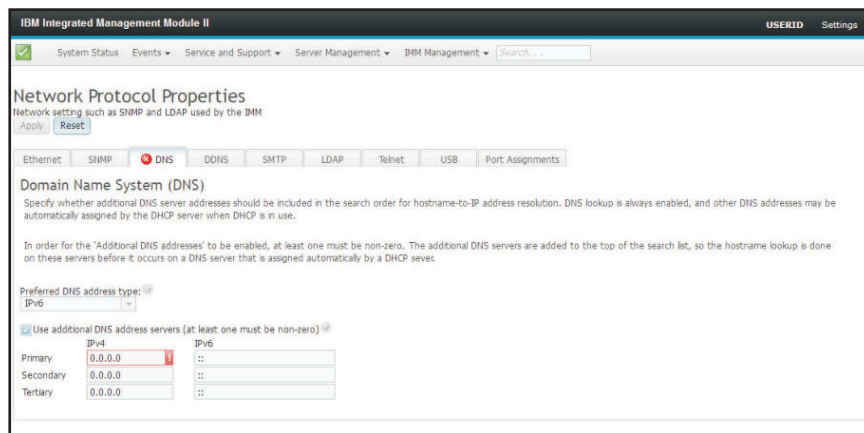
SNMPv1 Communities
Select communities to configure. At least one community must be configured.

Community 1	Enable Community 2	Enable Community 3
Community name: pub_get	Community name: pub_set	
Access type: Get	Access type: Set	
Allow any host to query MIB objects	Allow any host to query MIB objects	
Allow only specific hosts to query MIB objects and receive traps	Accept IPv4 Hosts	
Set trap destination that also be allowed to query MIB objects:	Accept IPv6 Hosts	
	Set trap destination that also be allowed to set MIB objects:	

DNS konfigurieren

Anmerkung: In einem IBM Flex System können DNS-Einstellungen auf dem IMM2 nicht geändert werden. DNS-Einstellungen werden vom CMM verwaltet.

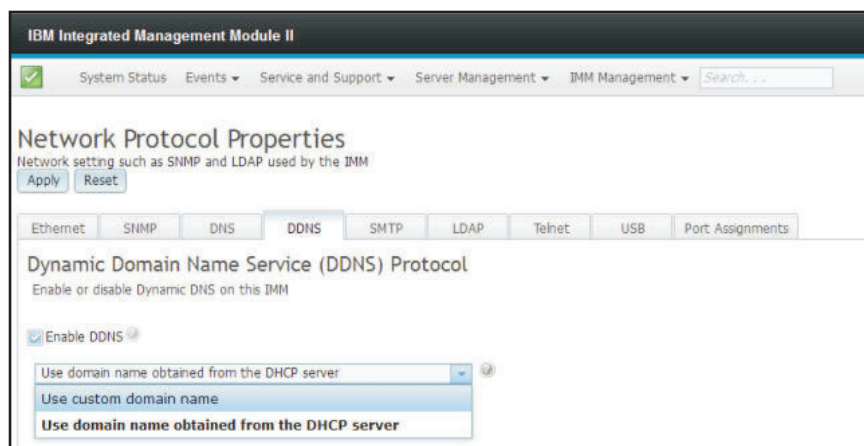
Klicken Sie auf die Registerkarte **DNS**, um die Einstellungen für das IMM2-DNS (Domain Name System) anzuzeigen oder zu ändern. Wenn Sie das Kontrollkästchen **Use additional DNS address servers** (Zusätzliche DNS-Adressserver verwenden) auswählen, können Sie die IP-Adressen von bis zu drei DNS-Servern (Domain Name System) 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 Domänennamensserver (DNS), wenn die aktive DNS-Konfiguration der konfigurierten Hostnamen, Adressen oder anderer im DNS gespeicherter Informationen in Echtzeit geändert werden soll.

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)

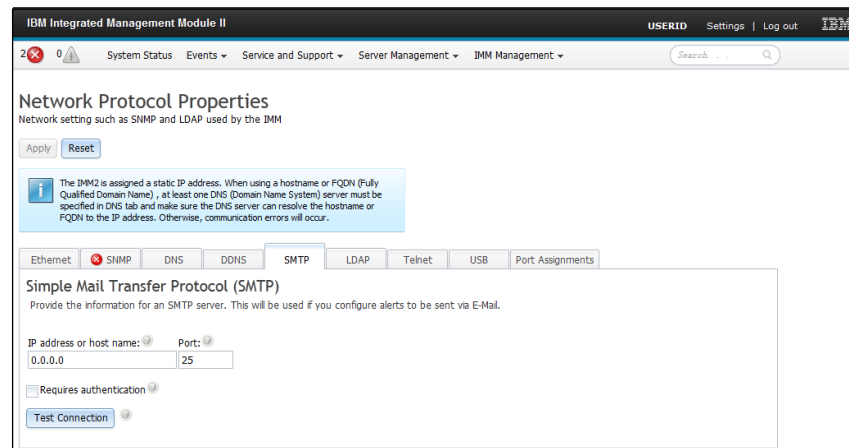
Geben Sie den Hostnamen des SMTP-Servers ein. Geben Sie in diesem Feld die IP-Adresse oder, wenn DNS aktiviert und konfiguriert ist, den Hostnamen des SMTP-Servers ein.

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.

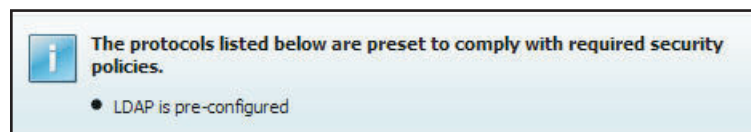
In der folgenden Abbildung ist die Registerkarte **SMTP** dargestellt.



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).



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. Das IMM2 kann jeden Benutzerzugriff über einen zentralen LDAP-Server über Fernzugriff authentifizieren. Sie können Berechtigungsstufen auf der Basis der Informationen auf dem LDAP-Server zuordnen. Sie können den LDAP-Server 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 Module II

System Status Events Service and Support Server Management IMM Management Search...

Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Apply Reset

Ethernet SNMP DNS DDNS SMTP **LDAP** Telnet USB Port Assignments

Lightweight Directory Access Protocol (LDAP) Client

The IMM contains a Version 2.2 OpenLDAP client that can be configured to provide user authentication through one or more LDAP servers. The LDAP server(s) to be used for authentication can be discovered dynamically or manually pre-configured. Use the pull-down list to select which of these two methods should be used.

Use LDAP Servers for: Authentication and Authorization

Active Directory Settings:

☐ Enable enhanced role-based security for Active Directory Users

Use Pre-configured LDAP servers

Host name or IP address	Port
0.0.0.0	389
	389
	389
	389

Miscellaneous Settings

Root distinguished name:

UID search attribute:
sAMAccountName

Binding method:
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 abrufen, 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 an-

deren 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=010000000000". 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 wieder verwenden und eine Erweiterung des LDAP-Schemas verhindern. Außer-

dem 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 kann eine frei formatierte Zeichenfolge zulassen. Wenn das Attribut erfolgreich abgerufen werden kann, wird der Wert, der vom LDAP-Server zurückgegeben wird, entsprechend den Informationen in der folgenden Tabelle interpretiert.

Tabelle 5. Berechtigungsbits

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 einstellen, 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 Wiederherstellen) 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)	Benutzer können die Konfiguration für "Security" (Sicherheit), "Network Protocols" (Netzprotokolle), "Network Interface" (Netzschnittstelle), "Port Assignments" (Portzuordnungen) und "Serial Port" (Serieller Anschluss) ändern.
4	User Account Management (Benutzerkontenverwaltung)	Benutzer können andere Benutzer hinzufügen, ändern oder löschen und die "Global Login Settings" (Globale Anmeldungseinstellungen) im Fenster "Login Profiles" (Anmeldeprofile) ändern.
5	Remote Console Access (Zugriff auf ferne Konsole)	Benutzer können auf die Remote-Server-Konsole zugreifen.
6	Remote Console and Remote Disk Access (Zugriff auf ferne Konsole und fernen Datenträger)	Benutzer können auf die Remote-Server-Konsole und die Funktionen für ferne Datenträger für den fernen Server zugreifen.
7	Remote Server Power/Restart Access (Berechtigung für Einschalten/Neustart des fernen Servers)	Benutzer können auf die Einschalt- und Neustartfunktionen für den fernen Server zugreifen.

Tabelle 5. Berechtigungsbits (Forts.)

Bit-position	Funktion	Erläuterung
8	Basic Adapter Configuration (Basisadapterkonfiguration)	Benutzer können Konfigurationsparameter auf den Seiten "System Settings" (Systemeinstellungen) und "Alerts" ändern.
9	Ability to Clear Event Logs (Fähigkeit, Ereignisprotokolle zu löschen)	Benutzer können die Ereignisprotokolle löschen. Anmerkung: Alle Benutzer können die Ereignisprotokolle einsehen; um jedoch die Protokolle löschen zu können, muss der Benutzer diese Berechtigungsstufe haben.
10	Advanced Adapter Configuration (Erweiterte Adapterkonfiguration)	Für Benutzer gelten keine Einschränkungen 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 wiederherstellen 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 werden. 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 ausgeführt. Dem Benutzer wird das inklusive 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.

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:

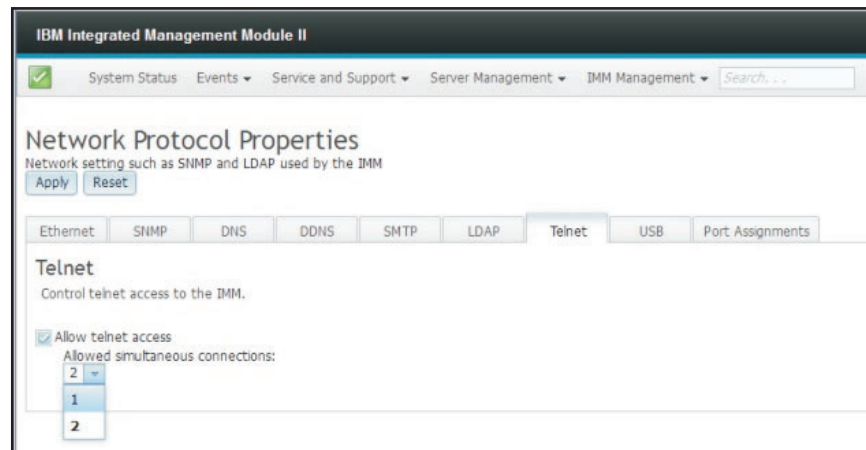
Allow telnet access (Telnet-Zugriff zulassen)

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-über-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.

Network Protocol Properties
Network setting such as SNMP and LDAP used by the IMM

Apply Reset

Ethernet SNMP DNS DDNS SMTP LDAP Telnet **USB**

Universal Serial Bus (USB) Settings
Control the USB interface used for in-band communication between the server and the IMM. This setting does not take effect until the server is restarted.

☒ Enable Ethernet over USB

☒ Enable external Ethernet to Ethernet over USB port forwarding

Add Mapping... Remove...

External Ethernet port number	Ethernet over USB port number
☐ 3389	3389
☐ 5900	5900
☐ 0	0
☐ 0	0
☐ 0	0
☐ 0	0
☐ 0	0
☐ 0	0
☐ 0	0
☐ 0	0
☐ 0	0

☒ Configure IP Settings for Ethernet over USB

IMM Ethernet over USB IP Settings

IP Address: 169.254.95.118

Subnet Mask: 255.255.0.0

OS Ethernet over USB IP Settings

IP Address: 169.254.95.120

Die Zuordnung von externen Ethernet-Portnummern zu Ethernet-über-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-über-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.

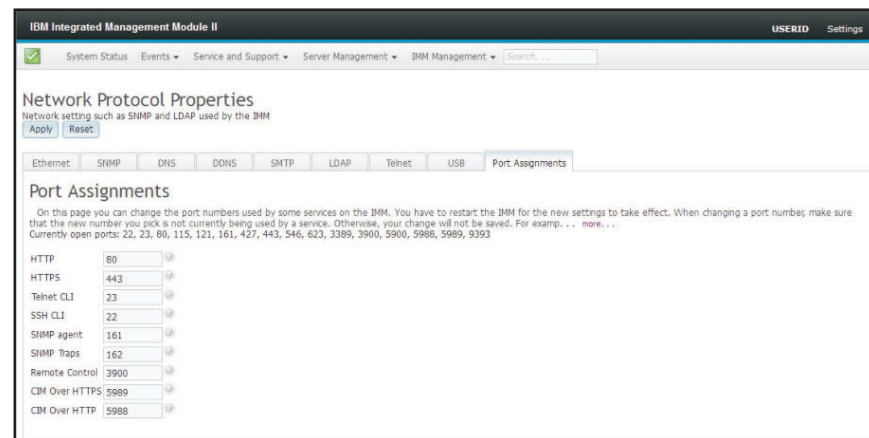
CIM over HTTP

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.

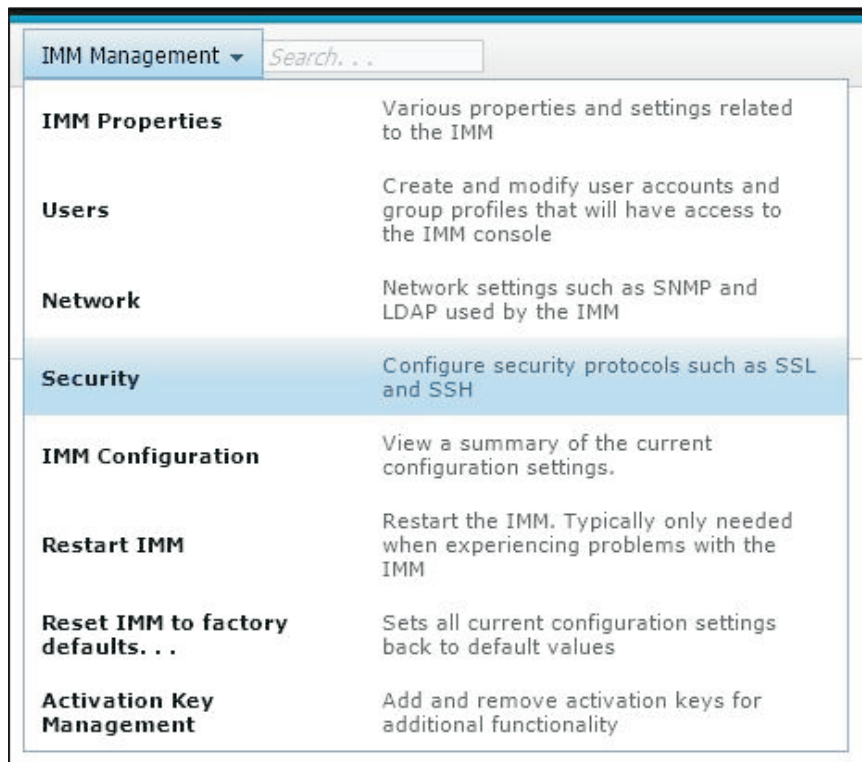
In der folgenden Abbildung ist die Registerkarte **Port Assignments** dargestellt.



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).



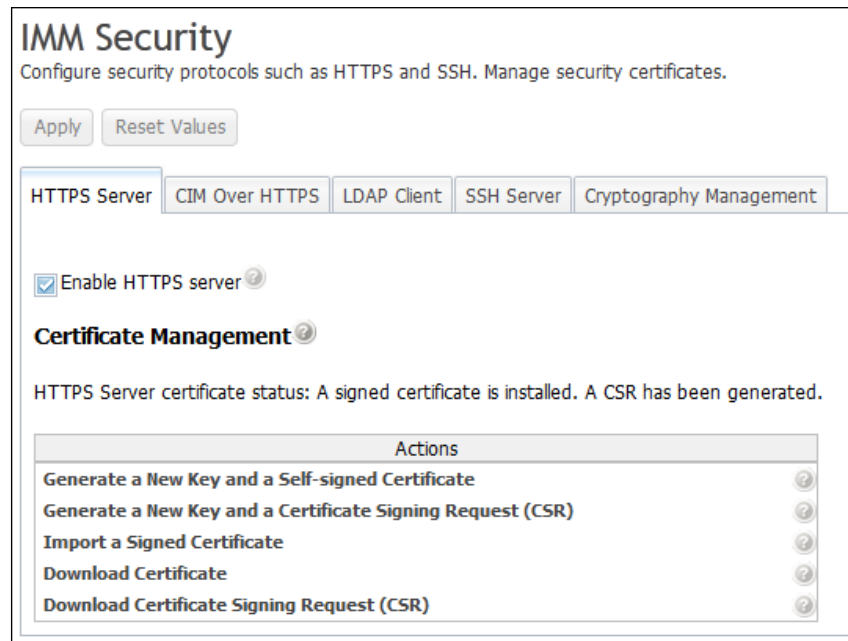
HTTPS-Protokoll konfigurieren

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 jeweils 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 111. In der folgenden Abbildung ist die Registerkarte **HTTPS Server** dargestellt.



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 111.

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

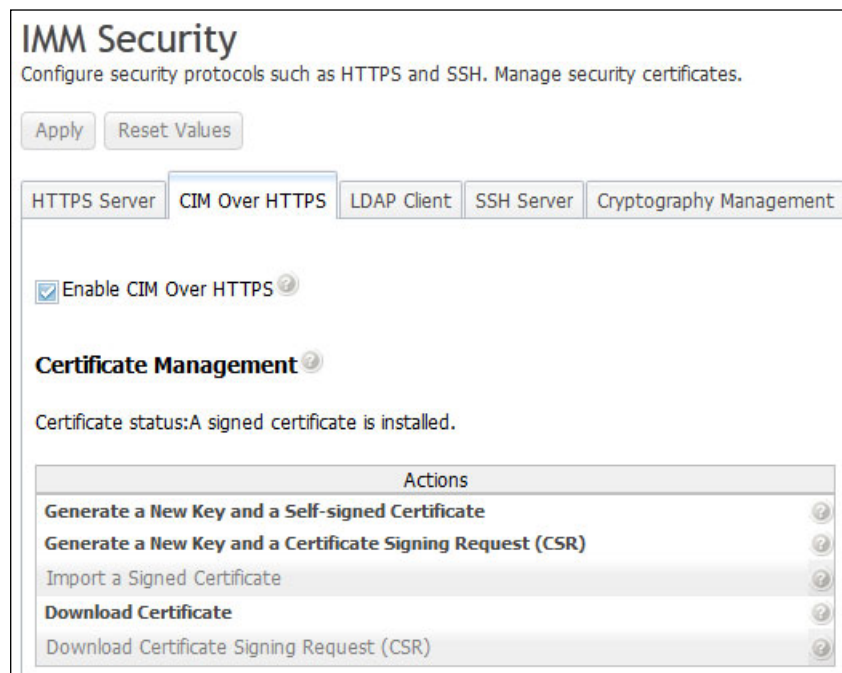
CIM-over-HTTPS-Protokoll konfigurieren

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 jeweils 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 111. In der folgenden Abbildung ist die Registerkarte **CIM over HTTPS** dargestellt.



Handhabung von CIM-over-HTTPS-Zertifikaten

Verwenden Sie die Optionen im Menü "Actions" für die Handhabung von CIM-over-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 111.

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 111.

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

IMM Security
Configure security protocols such as HTTPS and SSH. Manage security certificates.

Apply Reset Values

HTTPS Server CIM Over HTTPS **LDAP Client** SSH Server Cryptography Management

LDAP security:
LDAP security: Disable secure LDAP

Certificate Management

Signed Certificate status: No certificate is installed.
Trusted certificates: No trusted certificates are installed

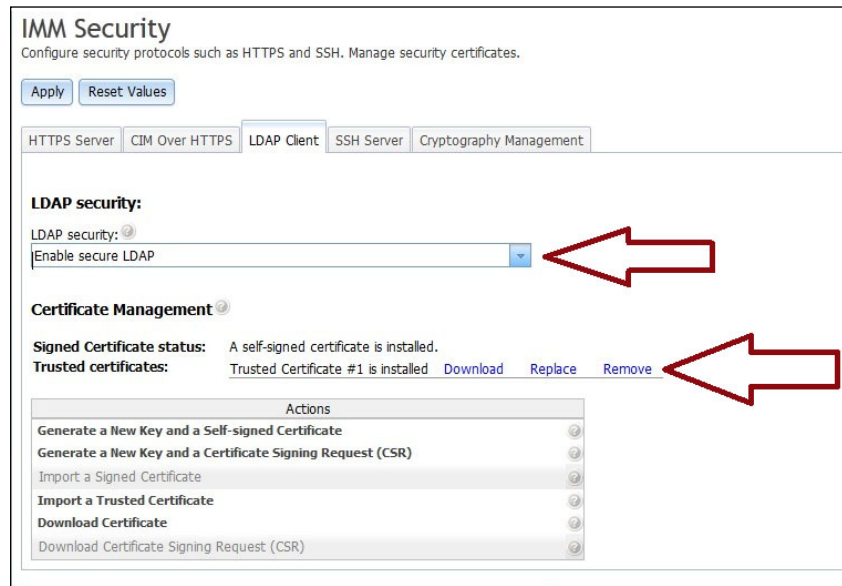
Actions
Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)
Import a Signed Certificate
Import a Trusted Certificate
Download Certificate
Download Certificate Signing Request (CSR)

Handhabung von Zertifikaten für sicheren LDAP-Client

Verwenden Sie die Optionen im Menü "Actions" für die Handhabung von LDAP-over-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 111. 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.



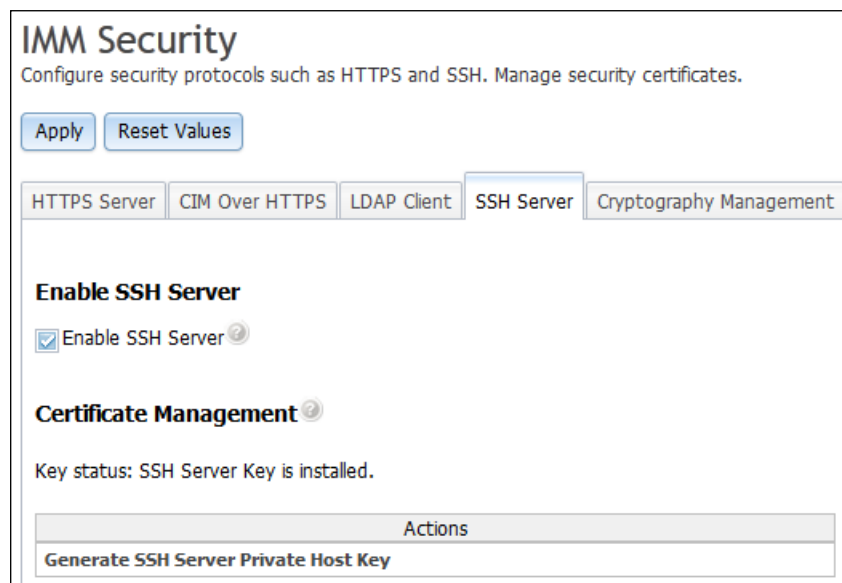
Secure Shell-Server konfigurieren

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.



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).



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 vertrauenswürdigen Zertifikat importiert. Klicken Sie auf **Import a Trusted Certificate** (Ein vertrauenswürdigen 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).

The image shows a dialog box titled "Generate New Key and Self-signed Certificate" with a close button (X) in the top right corner. The dialog is divided into two sections: "Required SSL Certificate Data" and "Optional SSL Certificate Data".

Required SSL Certificate Data

Country	US United States	?
State or Province	NY	?
City or Locality	New York	?
Organization Name	My Company	?
IMM Host Name	imm1234	?

Optional SSL Certificate Data

Contact Person	Chris Manager	?
E-Mail address	cmanager@mycomp.com	?
Organizational Unit	Sales	?
Surname		?
Given Name		?
Initials		?
DN Qualifier		?

At the bottom of the dialog are "Ok" and "Cancel" buttons.

Das Fenster "Generate New Key and Self-signed Certificate" fordert Sie auf, die Pflicht- und Wahlfelder (Required - Optional) 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).



Verschlüsselungsverwaltung konfigurieren

Klicken Sie auf die Registerkarte **Cryptography Management** (Verschlüsselungsverwaltung), um die IMM2-Firmware so zu konfigurieren, dass sie den Anforderungen für SP 800-131A entspricht.

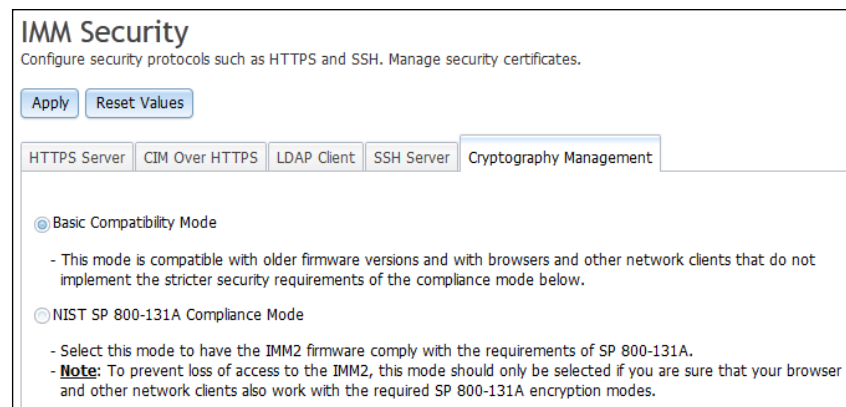
Wichtig: Bevor Sie ein Flash-Update der IMM2-Firmware auf eine ältere Version durchführen, legen Sie für die Option "IMM2 Security" (IMM2-Sicherheit) den Modus "Basic Compatibility Mode" (Modus für allgemeine Kompatibilität) fest. Dadurch wird verhindert, dass der Zugriff auf das IMM2 verloren geht.

Die Registerkarte **Cryptography Management** umfasst zwei Optionen:

- Basic Compatibility Mode (Modus für allgemeine Kompatibilität)
- NIST SP 800-131A Compliance Mode (Modus für Konformität mit NIST SP 800-131A)

Der Modus **Basic Compatibility Mode** ist mit älteren Firmwareversionen sowie mit Browsern und anderen Netzclients kompatibel, die nicht den Modus "NIST SP 800-131A Compliance Mode" verwenden.

In der folgenden Abbildung ist die Registerkarte **Cryptography Management** mit ausgewähltem Modus **Basic Compatibility Mode** dargestellt.

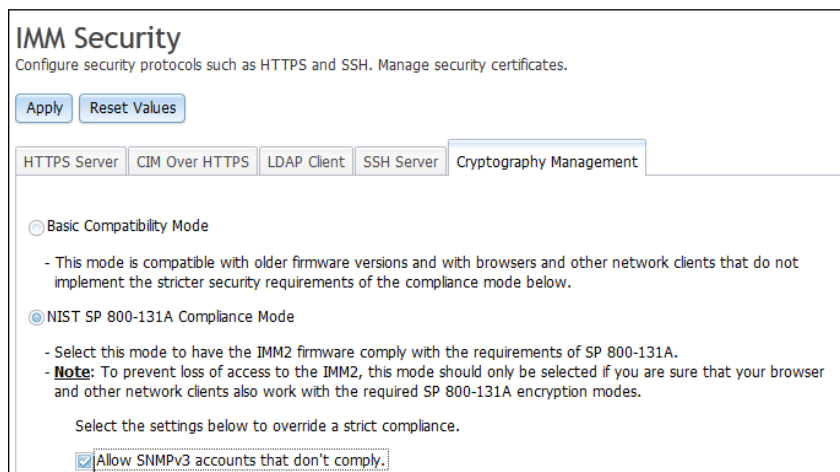


Der Modus **NIST SP 800-131A Compliance Mode** umfasst strenge Sicherheitsanforderungen. Bei Verwendung des Modus **NIST SP 800-131A Compliance Mode** hält die IMM2-Firmware die Anforderungen von SP 800-131A ein.

Anmerkungen:

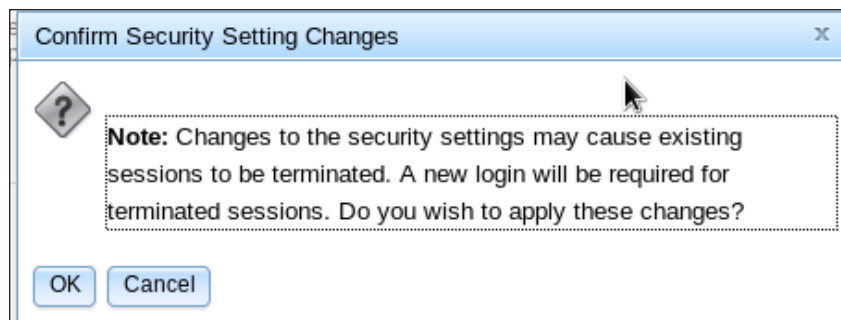
- Um einen Verlust des Zugriffs auf das IMM2 zu verhindern, verwenden Sie den Modus **NIST SP 800-131A Compliance Mode** nur, wenn Sie sicher sind, dass Ihr Browser und andere Netzclients mit den SP 800-131A-Verschlüsselungsmodi arbeiten können.
- Bei Verwendung des Modus **NIST SP 800-131A Compliance Mode** können Sie zulassen, dass SNMPv3-Konten die durch diesen Modus festgelegten Einschränkungen missachten.

In der folgenden Abbildung ist die Registerkarte **Cryptography Management** mit ausgewähltem Modus **NIST SP 800-131A Compliance Mode** dargestellt.

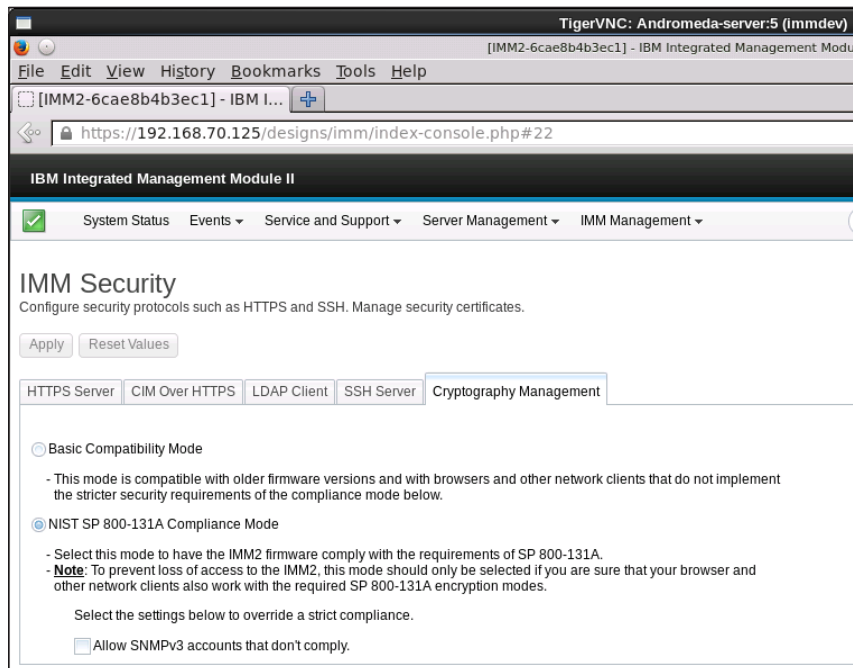


Gehen Sie wie folgt vor, um den Verschlüsselungsmodus für einen Standalone-Server zu konfigurieren:

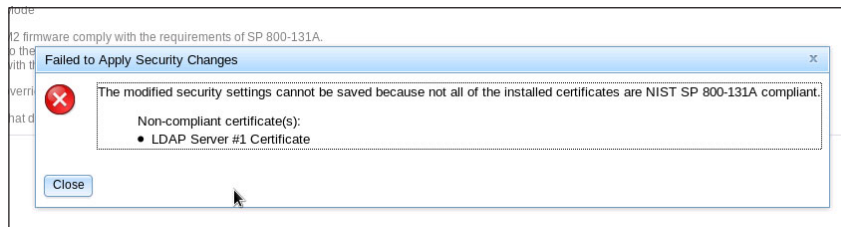
1. Melden Sie sich am IMM2 an.
2. Klicken Sie auf der Registerkarte **IMM Management** (IMM-Verwaltung) auf die Option **Security** (Sicherheit).
3. Klicken Sie auf die Registerkarte **Cryptography Management**.
4. Wählen Sie den Verschlüsselungsmodus auf der Seite "Cryptography Management" aus und klicken Sie dann auf die Schaltfläche **Apply** (Übernehmen). Sie werden aufgefordert, die Auswahl zu bestätigen, wie in der folgenden Abbildung dargestellt.



Wenn das IMM2 über kompatible Zertifikate und SSH-Schlüssel verfügt, wird der Verschlüsselungsmodus auf den Modus "NIST-800-131A Compliance Mode" festgelegt, wie in der folgenden Abbildung dargestellt.



Wenn die installierten Zertifikate nicht mit NIST-800-131A kompatibel sind, können die Sicherheitseinstellungen nicht geändert werden, wie in der folgenden Abbildung dargestellt.

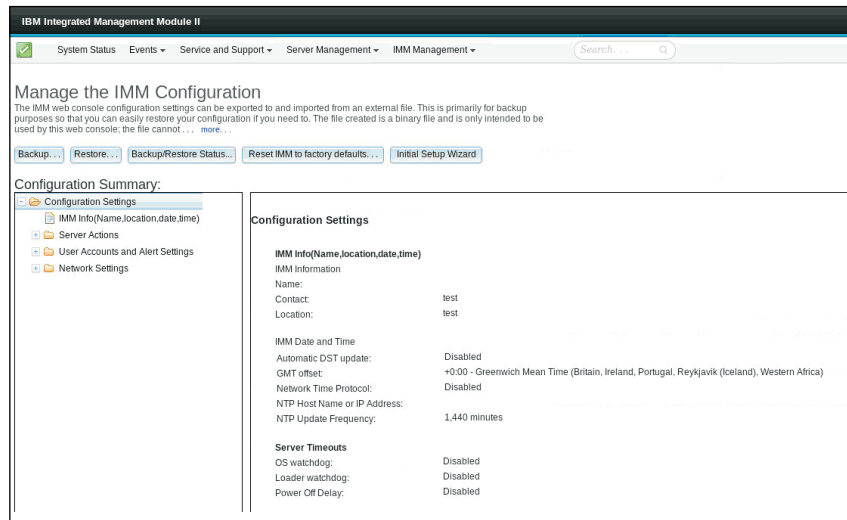


IMM-Konfiguration wiederherstellen und ändern

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

In der folgenden Abbildung ist das Fenster "Manage the IMM Configuration" (IMM-Konfiguration verwalten) dargestellt.

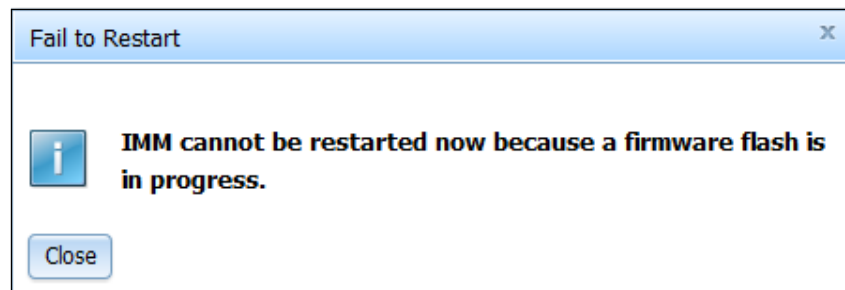


IMM2 erneut starten

Wählen Sie die Option **Restart IMM** (IMM erneut starten) auf der Registerkarte **IMM Management** (IMM-Verwaltung) aus, um das IMM2 erneut zu starten.

Anmerkungen:

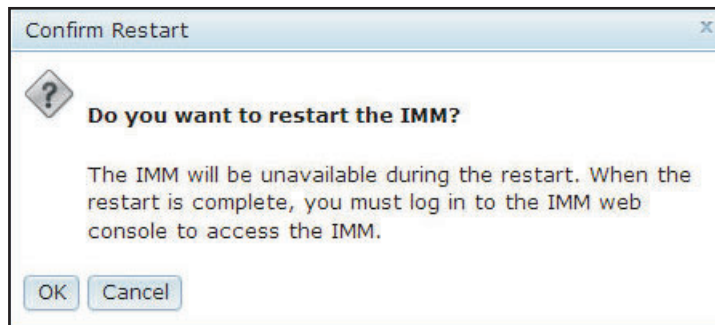
- Nur Benutzer mit der Benutzerberechtigungsstufe "Supervisor" können diese Funktion ausführen.
- Wenn Ethernet-Verbindungen vorübergehend unterbrochen wurden, müssen Sie sich am IMM2 anmelden, um auf die IMM2-Webschnittstelle zuzugreifen.
- Wenn ein anderer Benutzer gerade Server-Firmware aktualisiert, kann die Funktion "Restart IMM" (IMM erneut starten) nicht ausgeführt werden (wie in der folgenden Abbildung dargestellt).



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

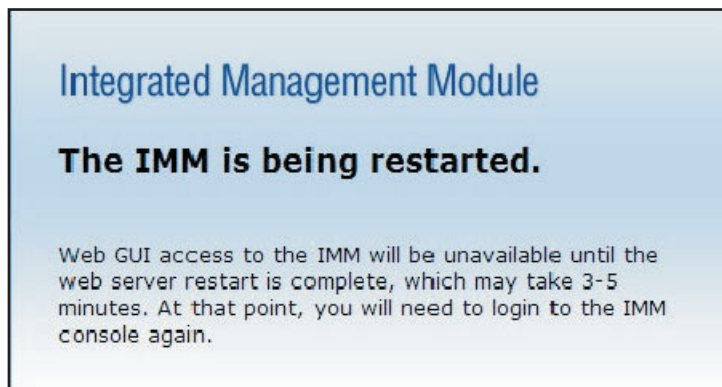
1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt „Am IMM2 anmelden“ auf Seite 12.
2. Klicken Sie auf die Registerkarte **IMM Management** und anschließend auf **Restart IMM**.
3. Klicken Sie auf die Schaltfläche **OK** im Fenster "Confirm Restart" (Neustart bestätigen). Das IMM2 wird erneut gestartet.

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



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 12).

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.

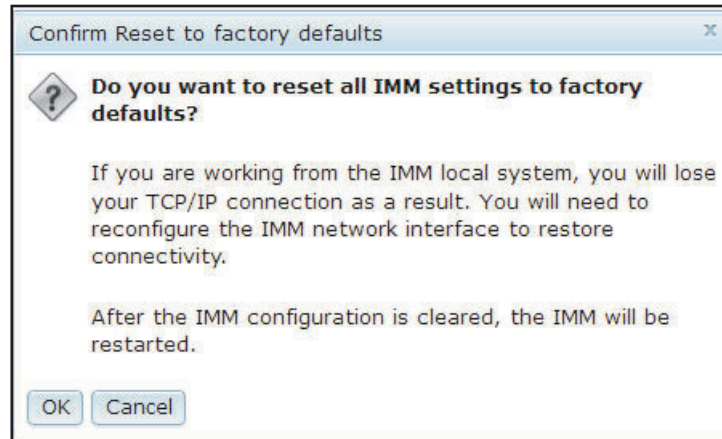
Anmerkungen:

- Nur Benutzer mit der Benutzerberechtigungsstufe "Supervisor" können diese Funktion ausführen.
- Wenn Ethernet-Verbindungen vorübergehend unterbrochen wurden, müssen Sie sich am IMM2 anmelden, um auf die IMM2-Webschnittstelle zuzugreifen.
- 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 12.
2. 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 Netzchnittstelle 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 12).
5. Rekonfigurieren Sie die Netzchnittstelle, 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 179.

Kapitel 5. Serverstatus überwachen

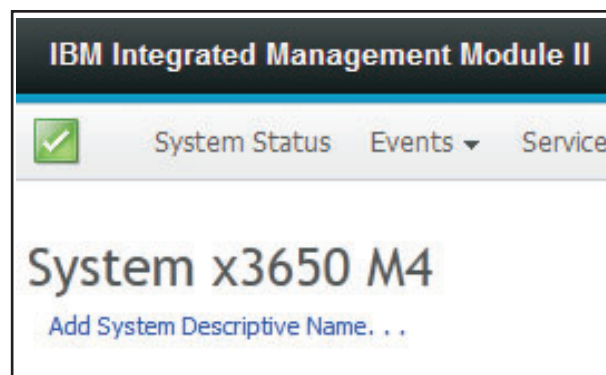
Dieses Kapitel enthält Informationen zum Anzeigen und Überwachen der Informationen zu dem Server, auf den Sie zugreifen.

Systemstatus anzeigen

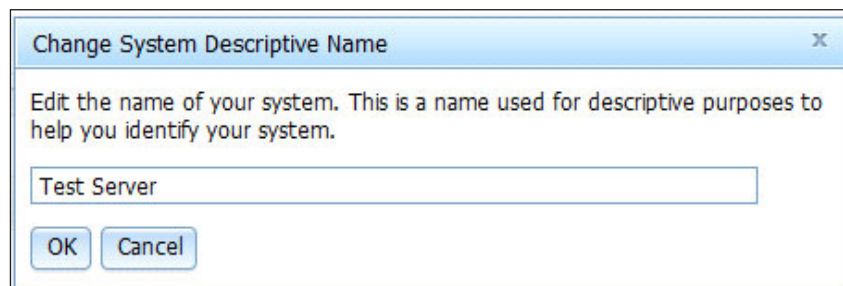
Die Seite "System Status" (Systemstatus) bietet eine Übersicht über den Betriebsstatus des IMM2-Servers. Auf dieser Seite werden Informationen zum Hardwarezustand des Servers und zu aktiven Ereignissen auf dem Server angezeigt.

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).

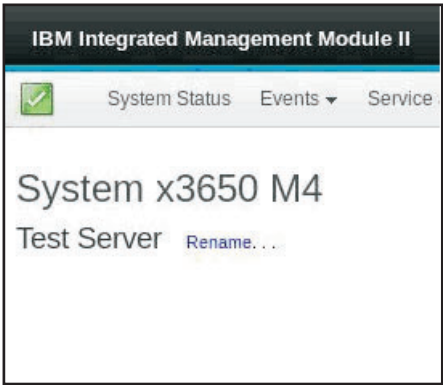


Geben Sie im Fenster "Change System Descriptive Name" (Beschreibenden Systemnamen ändern) einen Namen an, der dem IMM2 zugeordnet werden soll (wie in der folgenden Abbildung dargestellt).



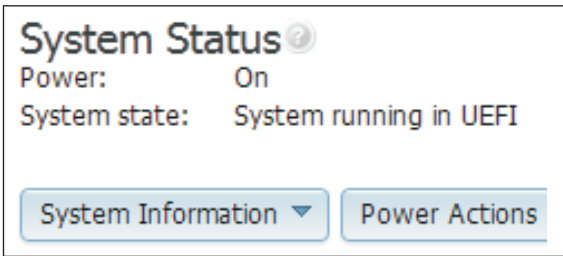
Sie können den beschreibenden Systemnamen ändern, indem Sie neben dem beschreibenden Systemnamen auf den Link **Rename...** (Umbenennen) klicken.

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



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 6. Systemstatusbeschreibungen

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 Ausführung wurde beendet.

Tabelle 6. Systemstatusbeschreibungen (Forts.)

Status	Beschreibung
Booting OS or in unsupported OS (Betriebssystem wird gebootet oder es wird ein nicht unterstütztes Betriebssystem gebootet)	Der Server kann sich aus einem der folgenden Gründe in diesem Status befinden: • Das Ladeprogramm des Betriebssystems wurde gestartet, aber das Betriebssystem wird nicht ausgeführt. • Die Ethernet-über-USB-Schnittstelle des IMM2 ist inaktiviert. • Das Betriebssystem hat die Treiber, die die Ethernet-über-USB-Schnittstelle unterstützen, nicht geladen.
OS booted (Betriebssystem gebootet)	Das Betriebssystem des Servers wird ausgeführt.
Suspend to RAM (Aussetzen in RAM)	Der Server wurde in den Bereitschafts- oder Ruhemodus versetzt.

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

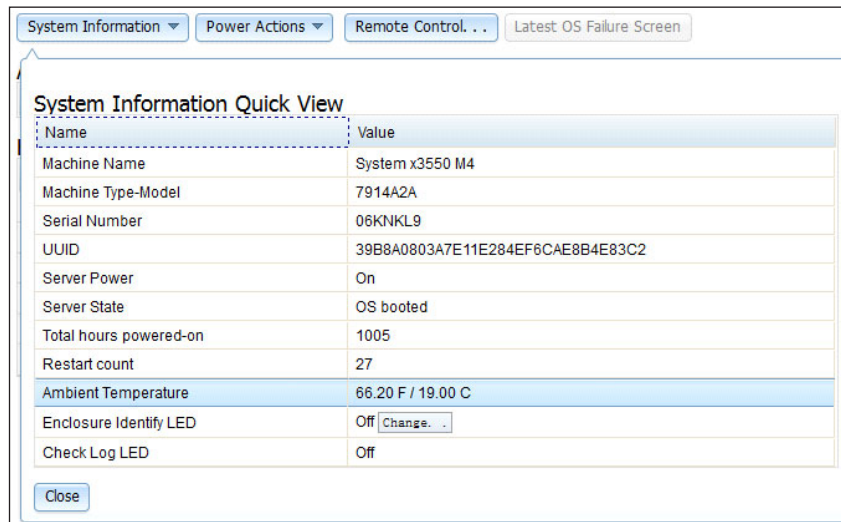
- System Information (Systeminformationen)
- Power Actions (Stromversorgungsaktionen)
- Remote Control (Fernsteuerung, weitere Informationen hierzu finden Sie unter „Remote-Presence- und Fernsteuerungsfunktionen“ auf Seite 130)
- Latest OS Failure Screen (Letzte Betriebssystem-Fehleranzeige, weitere Informationen hierzu finden Sie unter „Daten der letzten Betriebssystem-Fehleranzeige erfassen“ auf Seite 158)

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-Model (Maschinentyp und -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)

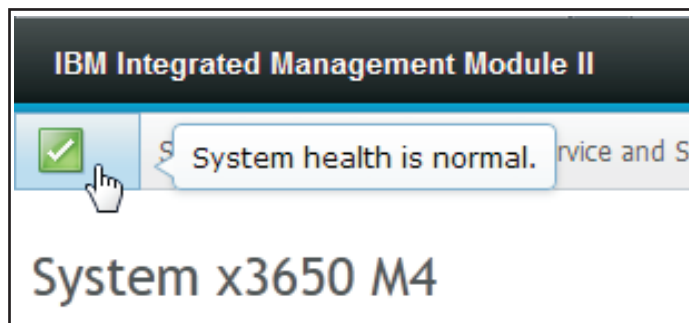
In der folgenden Abbildung ist das Fenster "System Information" dargestellt.



Serverzustand anzeigen

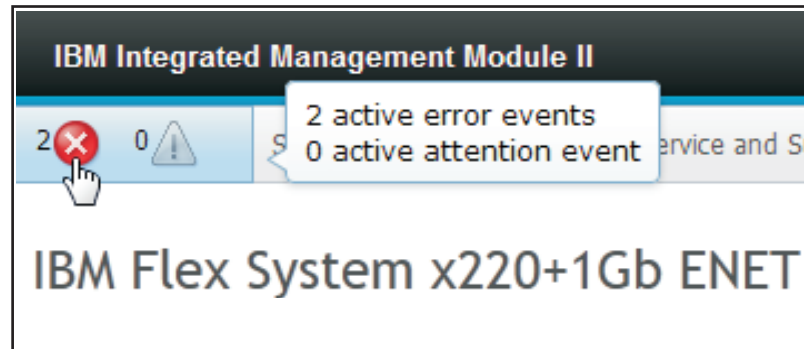
Der Serverzustand wird unter der Titelleiste in der linken oberen Ecke der Seite "System Status" (Systemstatus) angezeigt und ist durch ein Symbol gekennzeichnet. Ein grünes Häkchen gibt an, dass die Server-Hardware normal funktioniert. Bewegen Sie Ihren Cursor über das grüne Häkchen, um eine Kurzmeldung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

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
Local Storage	 Normal
Processors	 Normal
Memory	 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 modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Eve			
FRU Name	Status	Type	Capacity (GB)
DIMM 4	 Normal	DDR3	4
DIMM 9	 Normal	DDR3	4
DIMM 16	 Normal	DDR3	4
DIMM 21	 Normal	DDR3	4

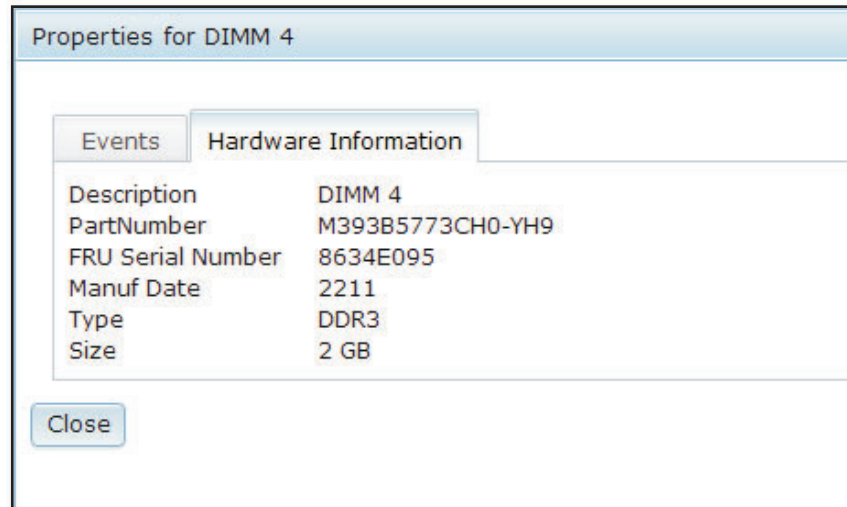
Sie können auf einen einzelnen FRU-Link (Field Replaceable Unit) in der Tabelle klicken, um weitere Informationen zu dieser Komponente zu erhalten. Alle aktiven Ereignisse für die Komponente werden auf der Registerkarte **Events** (Ereignisse) angezeigt.

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



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.



Kapitel 6. IMM2-Tasks ausführen

Verwenden Sie die Informationen in diesem Abschnitt und in Kapitel 3, „Übersicht über die IMM2-Webbenutzerschnittstelle“, auf Seite 21, 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 der folgenden Tasks auswählen.

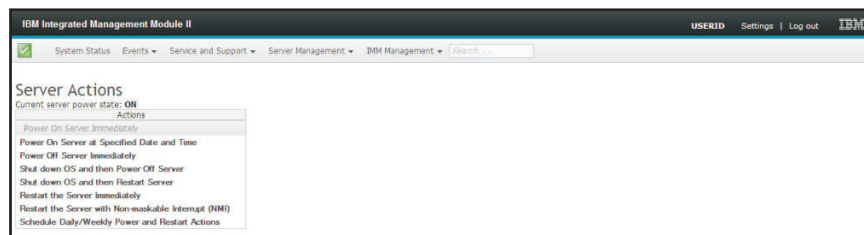
Wichtig: Einige Optionen sind möglicherweise auf Ihrem Server nicht verfügbar. Die Optionen, die auf der Registerkarte "Server Management" angezeigt werden, richten sich danach, auf welcher Serverplattform das IMM2 gespeichert ist und welche Adapter auf dem Server installiert sind.

- 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 "Local Storage" (Lokaler Speicher) können Sie die physische Struktur und die Speicherkonfiguration der Speichereinheit 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 "Adapters" (Adapter) können Sie Informationen zu den im Server installierten Adaptern 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.
- Mit der Option "Scalable Complex" (Skalierbarer Komplex) können Sie den aktuellen Zustand aller verfügbaren Knoten (Server) anzeigen und verwalten.

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.



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 7. Stromversorgungsaktionen und Beschreibungen

Stromversorgungsaktion	Beschreibung
Power on server immediately (Server sofort einschalten)	Wählen Sie dieses Aktionselement aus, um den Server einzuschalten und das Betriebssystem zu booten.
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 eingeschaltet wird.
Power off server immediately (Server sofort ausschalten)	Wählen Sie dieses Aktionselement aus, um den Server auszuschalten, ohne das Betriebssystem herunterzufahren.
Shut down operating system and then power off server (Betriebssystem herunterfahren und dann Server ausschalten) ¹	Wählen Sie dieses Aktionselement aus, um das Betriebssystem herunterzufahren und den Server anschließend auszuschalten.
Shut down OS and then restart server (Betriebssystem herunterfahren und Server anschließend erneut starten) ¹	Wählen Sie dieses Aktionselement aus, um einen Warmstart des Betriebssystems durchzuführen.
Restart the server immediately (Server sofort erneut starten)	Wählen Sie dieses Aktionselement aus, um den Server sofort aus- und anschließend wieder einzuschalten, ohne das Betriebssystem herunterzufahren.
Restart the server with non-maskable interrupt (NMI) (Server mit NMI erneut starten)	Wählen Sie dieses Aktionselement aus, um ein NMI für ein „blockiertes“ System zu erzwingen. Die Auswahl dieses Aktionselements ermöglicht es dem Plattformbetriebssystem, einen Hauptspeicherauszug zu erstellen, der für die Fehlerbehebung des blockierten Systems verwendet werden kann. Die IMM2-Firmware 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 planen)	Wählen Sie dieses Aktionselement aus, um tägliche oder wöchentliche Aktionen zum Einschalten und zum erneuten Starten für den Server zu planen.
Enter Sleep Mode (In Ruhemodus wechseln)	Wenn das Plattformbetriebssystem die S3-Funktion (Ruhemodus) unterstützt und die S3-Funktion aktiviert ist, wird dieses Aktionselement angezeigt. Wenn das Betriebssystem eingeschaltet ist, wählen Sie dieses Aktionselement aus, um das Betriebssystem in den Ruhemodus zu versetzen.
Exit Sleep Mode (Ruhemodus beenden)	Wenn das Plattformbetriebssystem die S3-Funktion (Ruhemodus) unterstützt und die S3-Funktion aktiviert ist, wird dieses Aktionselement angezeigt. Wählen Sie dieses Aktionselement aus, um den Ruhemodus für das Betriebssystem zu beenden.

Tabelle 7. Stromversorgungsaktionen und Beschreibungen (Forts.)

Stromversorgungsaktion	Beschreibung
1.	Falls sich das Betriebssystem im Bildschirmschonermodus oder im gesperrten Modus befindet, wenn die Anforderung zum Herunterfahren gesendet wird, kann das IMM2 möglicherweise keinen ordnungsgemäßen Systemabschluss einleiten. Das IMM2 führt dann einen Kaltstart oder einen Systemabschluss nach Ablauf des Ausschaltverzögerungsintervalls durch, während das Betriebssystem möglicherweise noch ausgeführt wird.

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.

Anmerkungen:

- Wenn die Fernsteuerungsfunktion im Mehrbenutzermodus gestartet wird, unterstützt das IMM2 bis zu sechs gleichzeitige Sitzungen. Die Funktion für ferne Datenträger kann jeweils nur von einer Sitzung ausgeführt werden.
- Der Video Viewer kann nur das vom Videocontroller auf der Systemplatine generierte Video anzeigen. Wenn ein separater Videocontroller installiert und anstelle des Systemvideocontrollers verwendet wird, kann das IMM2 den Videoinhalt aus dem hinzugefügten Adapter nicht auf dem fernen Video Viewer anzeigen.

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 Firmware

reversion aktualisiert wird, werden auch das Java-Applet und das ActiveX-Applet auf die neueste Version aktualisiert. Java stellt zuvor verwendete Applets standardmäßig in den lokalen 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 1.7 unter Windows:

1. Klicken Sie auf **Start → Settings (Einstellungen) → Control Panel (Steuerkonsole)**.
2. Klicken Sie doppelt auf **Java Plug-in 1.7**. 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 aus:
 - 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 144.

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 IMM Premium-Upgrade gekauft und erhalten haben, installieren Sie ihn. Lesen Sie dazu „Aktivierungsschlüssel installieren“ auf Seite 179.

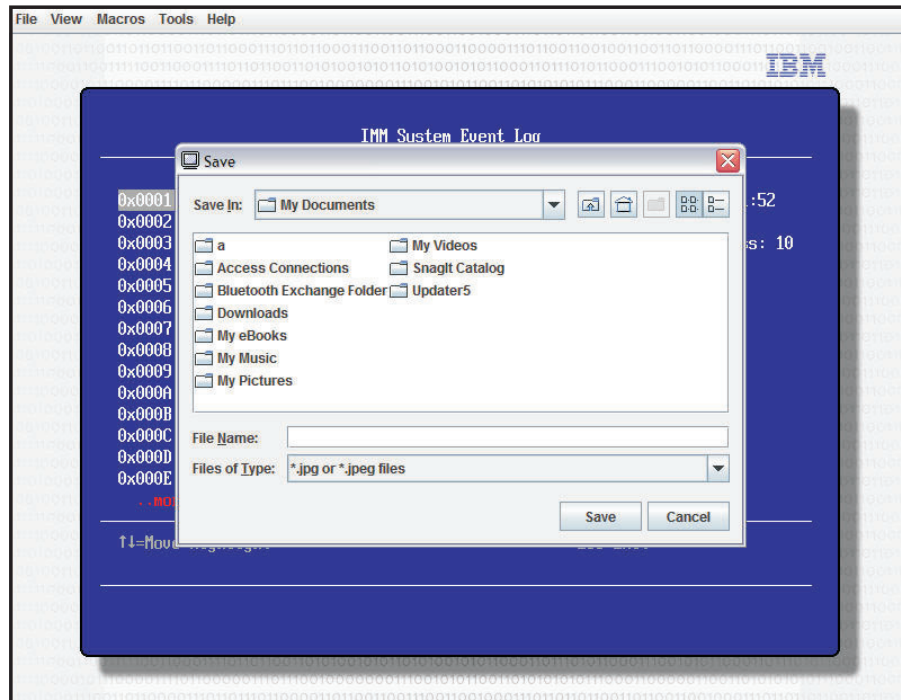
Anzeigenerfassung per Fernsteuerung

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.



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 eingblendeter 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 größengangepasste Fenster anzuzeigen.

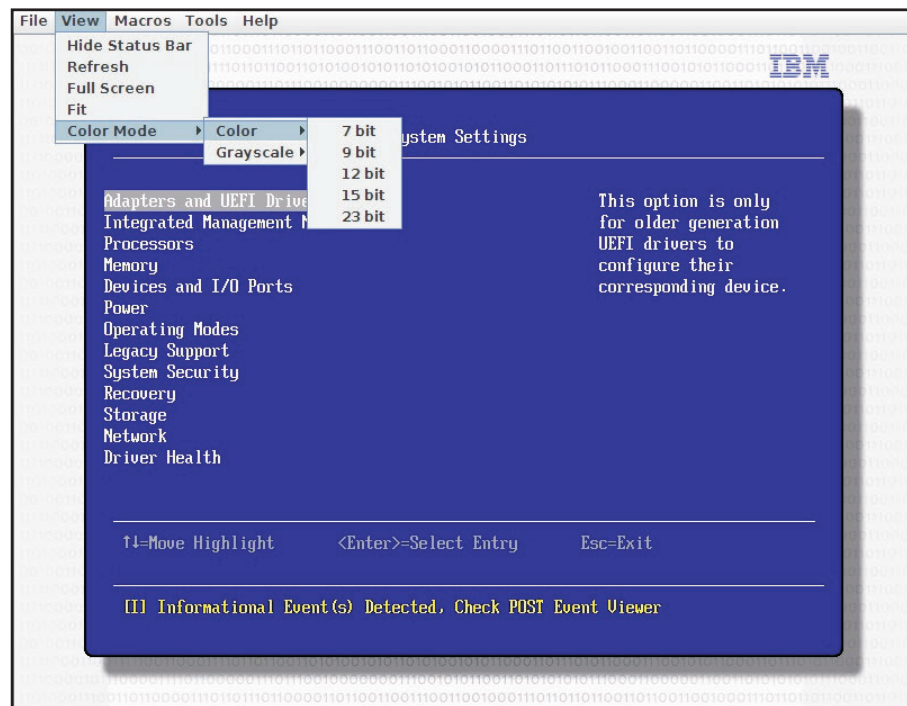
Fernsteuerung des Videofarbmodus

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



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

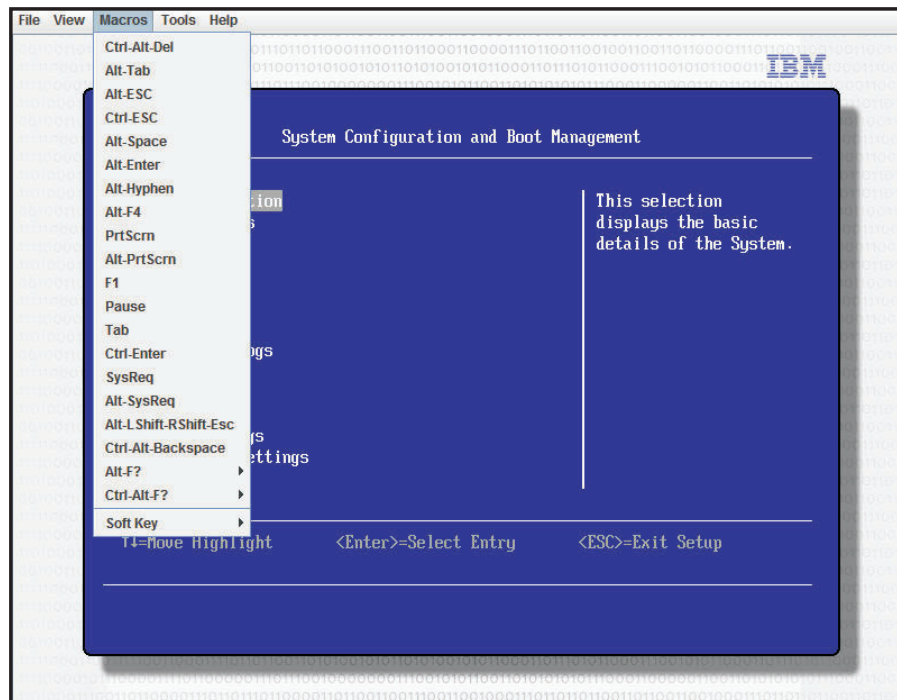
Tastaturunterstützung per Fernsteuerung

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).



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 aus 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 zu den physischen Tasten 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 müssen. 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 Verarbeitung 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.

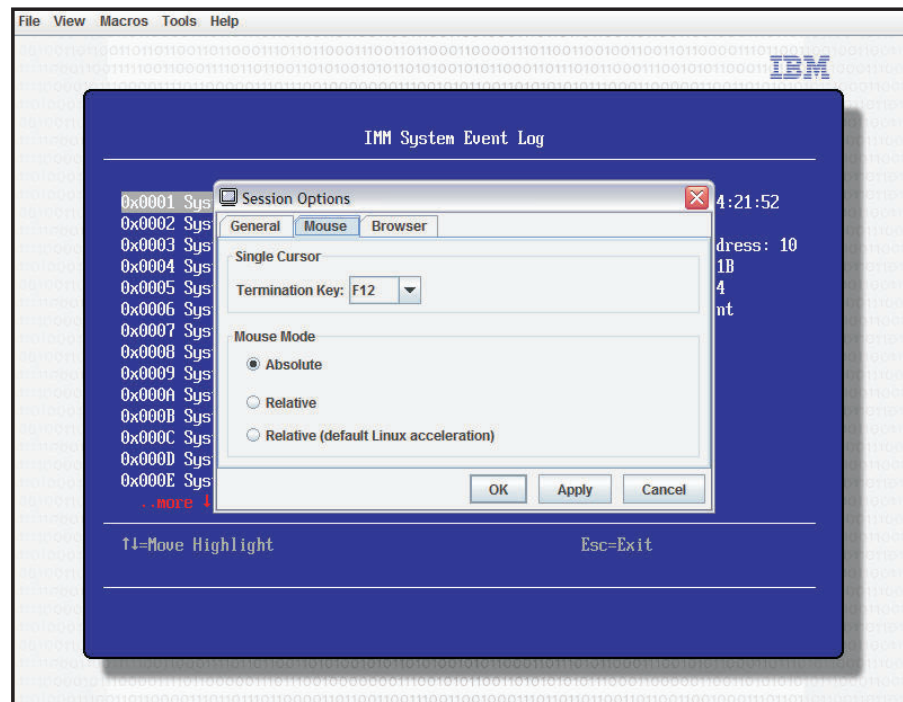
Mausunterstützung per Fernsteuerung

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).



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" aus 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 Sitzung in der Einzelbenutzeroption oder sechs Sitzungen in der Option für den Mehrbenutzermodus), kann ein anderer Webbenutzer eine Anforderung zum Trennen der Verbindung an einen Fernsteuerungsbenutzer senden, der die Funktion "Anklopfen" aktiviert hat. Dies ist nur möglich, wenn der Benutzer, der die Anklopffunktion aktiviert hat, 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 An-

forderung 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 multiuser mode (Fernsteuerung im Mehrbenutzermodus starten)

Anmerkungen:

- Das IMM2 unterstützt im Mehrbenutzermodus bis zu sechs gleichzeitige Videositzungen.
- Die Funktion "Anklopfen" wird automatisch aktiviert.

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

☒ Allow others to request my remote session disconnect ⓘ

No response time interval: ⓘ 1 hour ▼

Start remote control in single-user mode
Gives you exclusive access during the remote session.

Start remote control in multi-user mode
Allows other users to start remote sessions while your session is active.

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.			
Refresh			
User Name	Active Sessions	Availability for Disconnection	Timeout Value
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:

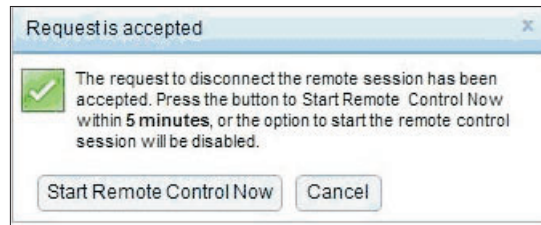
- **Request to connect** (Verbindung ist angefordert): Dieser Text wird angezeigt, wenn der Fernsteuerungsbenutzer die Funktion "Anklopfen" aktiviert hat und derzeit keine Anforderung zum Trennen der Verbindung von einem anderen Webbenutzer erhalten hat. Der aktuelle Webbenutzer hat keine Anforderung 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.

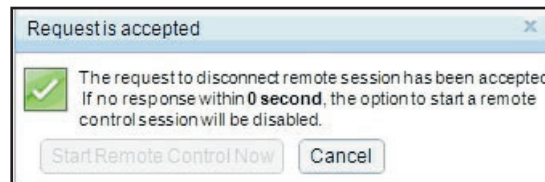


Wenn der Fernsteuerungsbenutzer die Anforderung zum Trennen der Verbindung akzeptiert, muss der Webbenutzer die Fernsteuerungssitzung innerhalb von fünf Minuten starten. Wenn der Webbenutzer die Sitzung nicht innerhalb von fünf Minuten startet, ist die Sitzung nicht mehr reserviert.

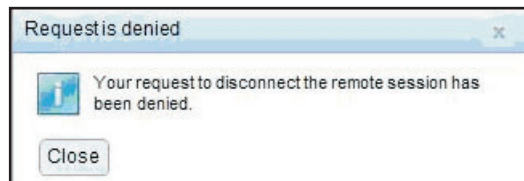
In der folgenden Abbildung sind die Informationen dargestellt, die angezeigt werden, wenn die Anforderung zum Trennen der Verbindung akzeptiert wird und die Anforderung sich im reservierten Zustand befindet.



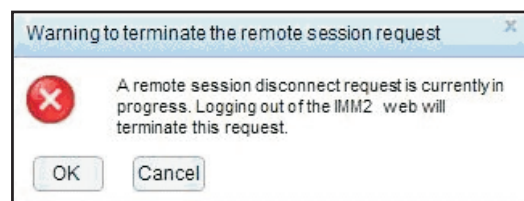
In der folgenden Abbildung sind die Informationen dargestellt, die angezeigt werden, wenn die Anforderung zum Trennen der Verbindung akzeptiert wird und die Anforderung sich nicht im reservierten Zustand befindet.



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).

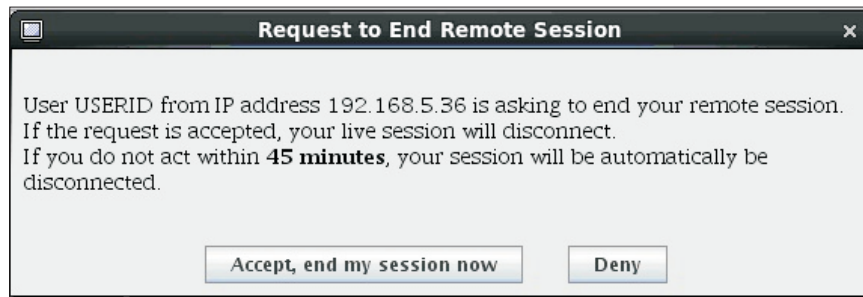


Wenn der Webbenutzer versucht, sich vom IMM2 abzumelden, bevor er eine Nachricht zu seiner Anforderung erhalten hat, erhält der Webbenutzer eine Nachricht (wie in der folgenden Abbildung dargestellt).

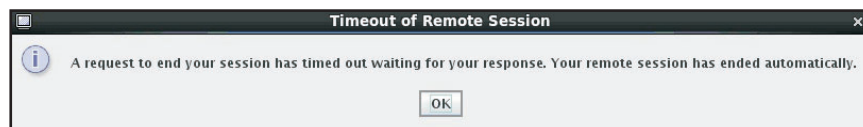


Nachdem der Fernsteuerungsbenutzer die Anforderung erhalten hat, muss er in dem ausgewählten Zeitintervall entscheiden, ob er die ferne Sitzung freigibt, bevor er die Fernsteuerungssitzung startet. Das Fenster "Request to End Remote Session" (Anforderung zur Beendigung der fernen Sitzung) wird angezeigt,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



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 Laufwerke und Plattenimages werden auf dem Server als USB-Laufwerke angezeigt.

Anmerkungen:

- Bei der Funktionalität für ferne Datenträger ist USB-Unterstützung erforderlich. Die folgenden Serverbetriebssysteme verfügen über USB-Unterstützung:
 - 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 1.7 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 wird, 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 Disketten- und 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 (Remote Disk-on-Card - ferne Datenträgerkarte)), öffnet sich ein Fenster. Dieses Fenster bietet Ihnen die 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

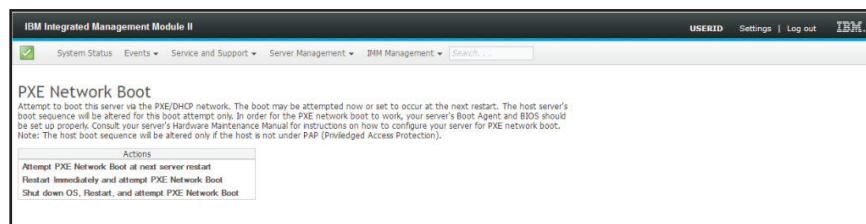
Schließen Sie die Fenster "Video Viewer" und "Virtual Media Session", wenn Sie die Verwendung der Fernsteuerungsfunktion beendet haben.

PXE-Netzboot einrichten

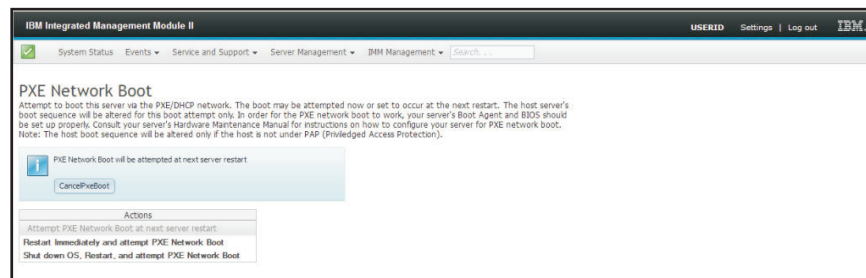
Verwenden Sie die Option **PXE Network Boot** (PXE-Netzboot), um Bootversuche der Server-Ausführungsumgebung vor dem Start einzurichten. Führen Sie die folgenden Schritte aus, um Ihren Server für den Versuch eines PXE-Netzboots (Pre-boot Execution Environment) beim nächsten Serverneustart einzurichten.

1. Melden Sie sich am IMM2 an. Weitere Informationen finden Sie im Abschnitt „Am IMM2 anmelden“ auf Seite 12.
2. Klicken Sie auf **Server Management** (Serververwaltung) und wählen Sie anschließend **PXE Network Boot** aus.

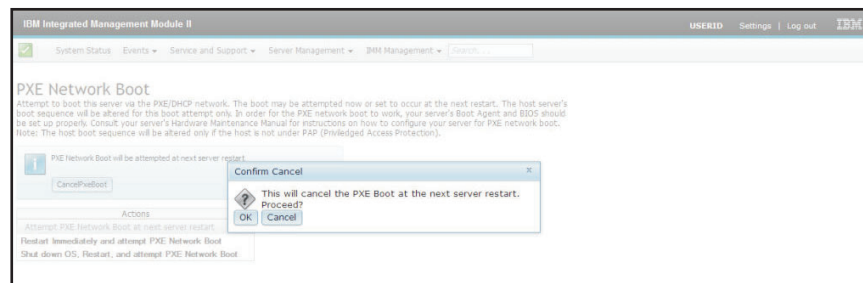
Das folgende Fenster wird geöffnet.



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.

Firmware Type	Status	Version	Build	Release Date
DSA	Active	9.24	DS1T44B	2012-08-10
IMM2	Active	2.15	1A0039Q	2013-01-28
IMM2 (Backup)	Inactive	3.00	1A0039T	2013-01-30
UEFI	Active	1.20	07E120CUB	2012-08-23
UEFI (Primary)	Active	1.20	07E120CUB	2012-08-23
UEFI (Backup)	Inactive	1.20	07E120CUB	2012-08-23

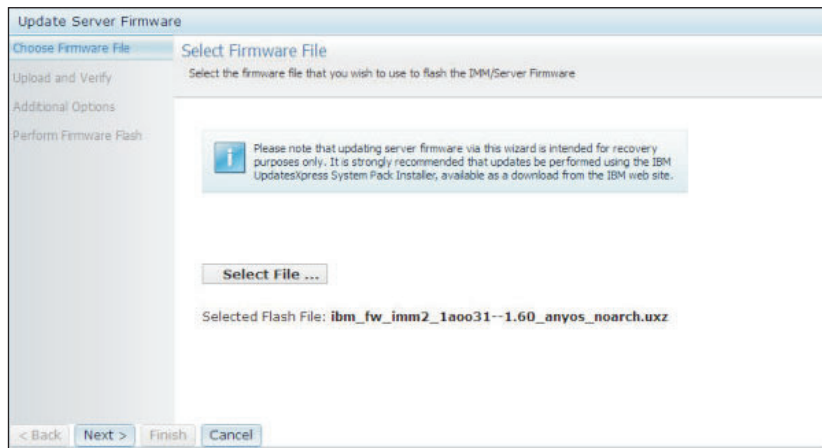
Der aktuelle Status und die aktuellen Versionen der IMM2-, UEFI- und DSA-Firmware werden angezeigt, einschließlich der primären Versionen und der Sicherungskopien. Der Status der Firmware wird in drei Kategorien angegeben:

- **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:

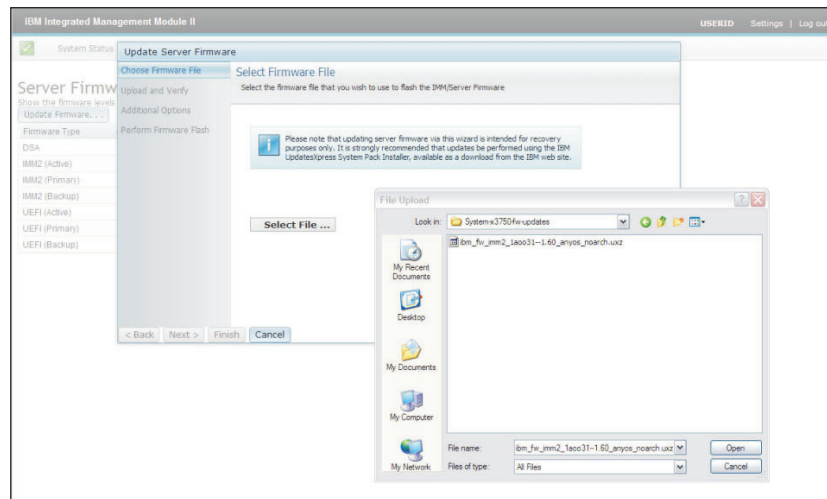
1. Klicken Sie in der Menüliste "Server Management" auf **Server Firmware**.
2. Klicken Sie auf **Update Firmware** (Firmware aktualisieren). Das Fenster "Update Server Firmware" (Server-Firmware aktualisieren) wird geöffnet (wie in der folgenden Abbildung dargestellt).



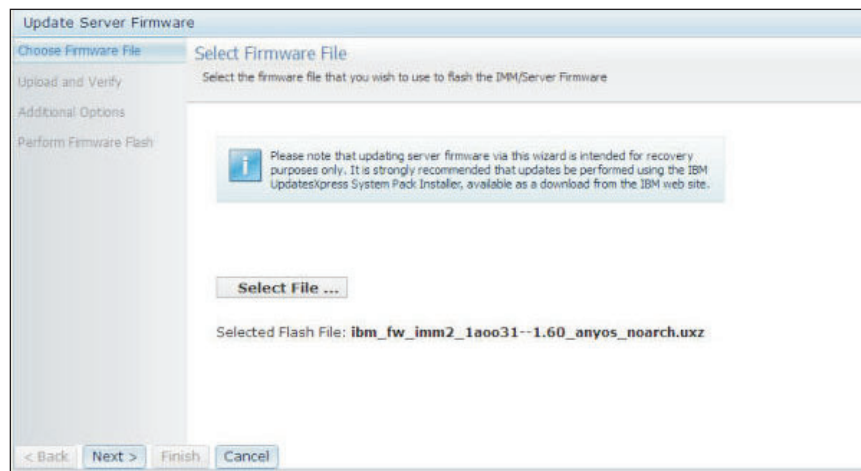
3. Lesen Sie den Warnhinweis, *bevor* Sie mit dem nächsten Schritt fortfahren.
4. Führen Sie einen der folgenden Schritte aus:
 - Klicken Sie auf **Cancel** (Abbrechen) und kehren Sie zum vorherigen Fenster "Server Firmware" zurück.
 - Klicken Sie auf **Select File...** (Datei auswählen), um die gewünschte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

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

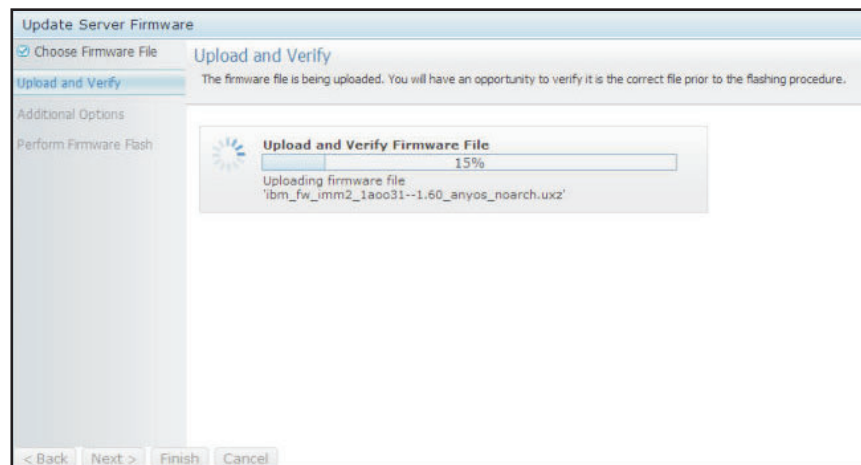
Wenn Sie auf **Select File...** klicken, wird das Fenster "File Upload" (Hochladen von Datei) geöffnet (wie in der folgenden Abbildung dargestellt). In diesem Fenster können Sie nach der gewünschten Datei suchen.



5. 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).

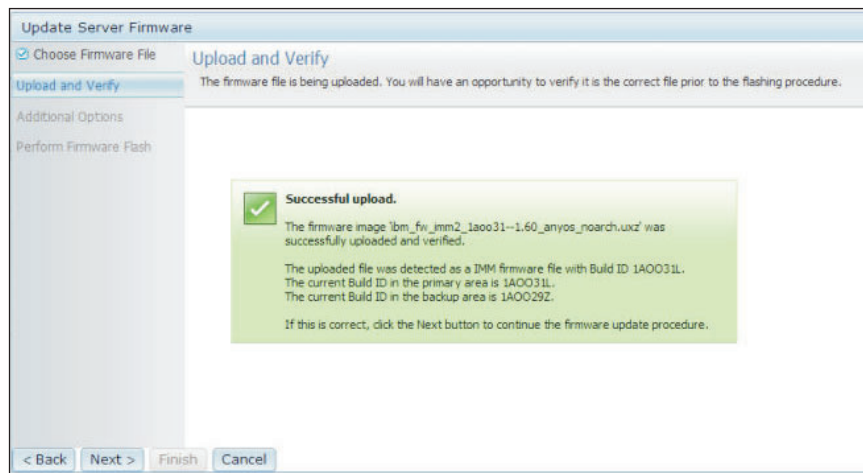


6. Klicken Sie auf **Next >** (Weiter), um die ausgewählte Datei hochzuladen und zu prüfen. Eine Fortschrittsanzeige wird angezeigt, während die Datei hochgeladen und geprüft wird (wie in der folgenden Abbildung dargestellt).

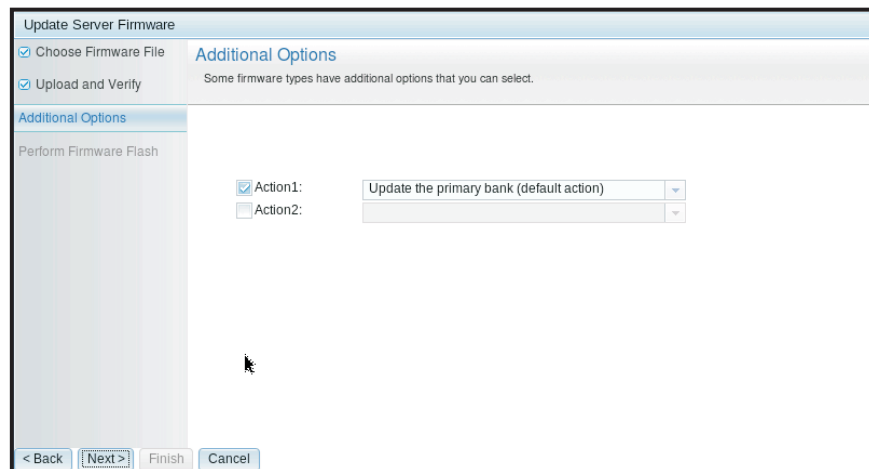


Sie können dieses Statusfenster anzeigen, um zu prüfen, ob Sie die richtige Datei zur Aktualisierung ausgewählt haben. Das Statusfenster enthält Informationen zum Dateityp der Firmware, die aktualisiert wird, wie DSA, IMM oder UEFI.

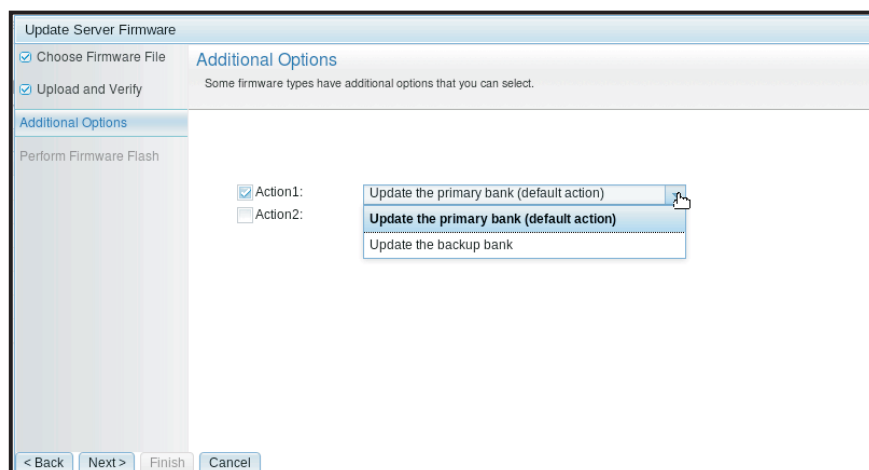
Nachdem die Firmwaredatei erfolgreich hochgeladen und geprüft wurde, erscheint ein Fenster mit der Meldung, dass das Hochladen erfolgreich war (Successful upload) (wie in der folgenden Abbildung dargestellt).



7. 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).



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).



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.

The screenshot shows the 'Update Server Firmware' window with the 'Additional Options' tab selected. On the left, a sidebar contains 'Choose Firmware File', 'Upload and Verify', 'Additional Options' (highlighted), and 'Perform Firmware Flash'. The main area has a sub-header 'Additional Options' with the text 'Some firmware types have additional options that you can select.' Below this, there are two checked checkboxes: 'Action1:' and 'Action2:'. To the right of 'Action1:' is a dropdown menu showing 'Update the primary bank (default action)'. To the right of 'Action2:' is a dropdown menu showing 'Update the backup bank'. At the bottom, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

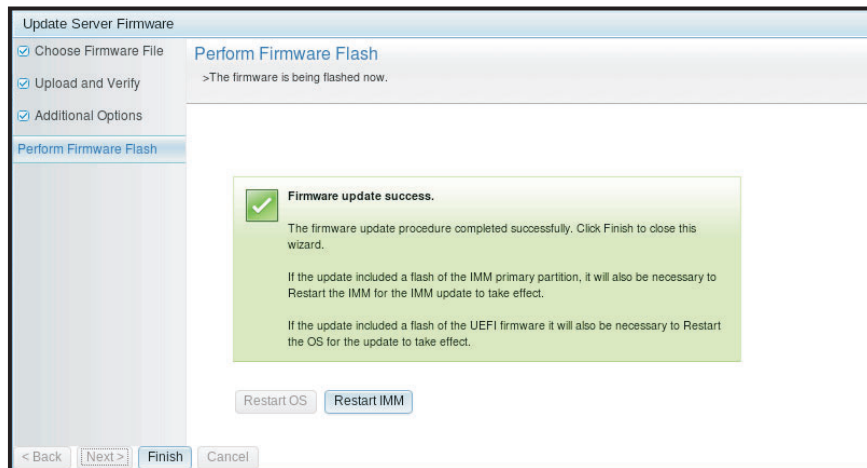
In der vorherigen Anzeige sehen Sie, dass für "Action 1" die primäre Speichergruppe zum Aktualisieren ausgewählt ist. Sie können auch auswählen, dass die Sicherungsspeichergruppe unter "Action 2" aktualisiert werden soll (wie in der vorherigen Abbildung dargestellt). Die primäre Speichergruppe und die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

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

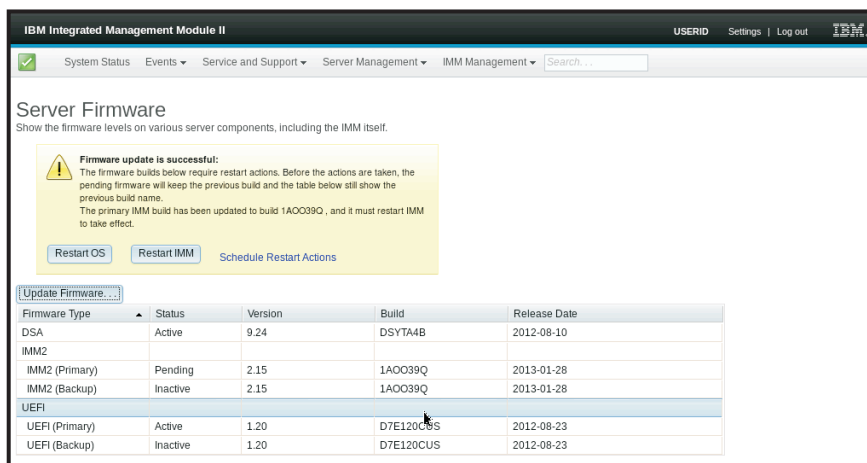
Eine Fortschrittsanzeige zeigt den Fortschritt der Aktualisierung der primären Speichergruppe und der Sicherungsspeichergruppe an (wie in der folgenden Abbildung dargestellt).

The screenshot shows the 'Update Server Firmware' window with the 'Perform Firmware Flash' tab selected. The sidebar on the left now highlights 'Perform Firmware Flash'. The main area has a sub-header 'Perform Firmware Flash' with the text '>The firmware is being flashed now.' Below this, it lists 'Action 1 of 2: 'Update the primary bank (default action)'' and 'Action 2 of 2: 'Update the backup bank''. A progress bar is shown with a circular arrow icon on the left and a percentage of '27%' on the right. At the bottom, the same four buttons are present: '< Back', 'Next >', 'Finish', and '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, wenn die Anzeige "Server Firmware" aufgerufen wird.



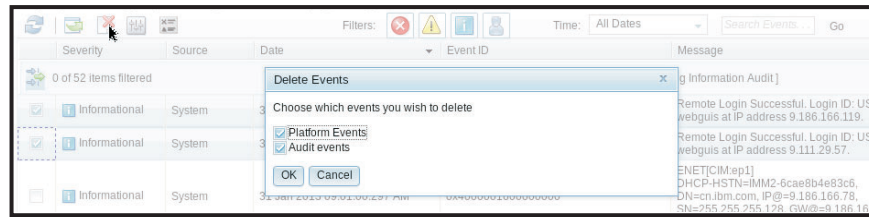
Systemereignisse verwalten

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. Die Kapazität der IMM2-Protokolle reicht für ungefähr 1024 Ereignisdatensätze und 1024 Prüfdatensätze aus. Die tatsächliche Anzahl an Datensätzen hängt von der Größe des Inhalts jedes Protokolldatensatzes ab.

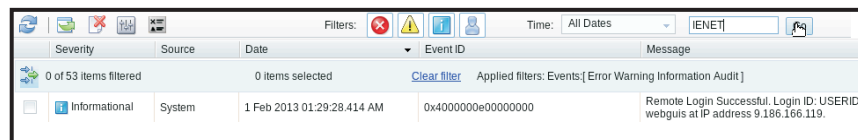
Klicken Sie auf die Option **Event Log**. Das folgende Fenster wird geöffnet.



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



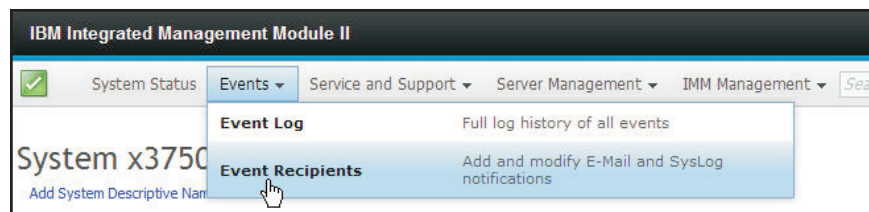
Um nach bestimmten Ereignistypen oder Suchbegriffen zu suchen, geben Sie den betreffenden Ereignistyp oder den Suchbegriff im Feld **Search Events** (Ereignisse suchen) ein. Klicken Sie dann auf **Go** (Start) (wie in der folgenden Abbildung dargestellt).



Benachrichtigung zu Systemereignissen

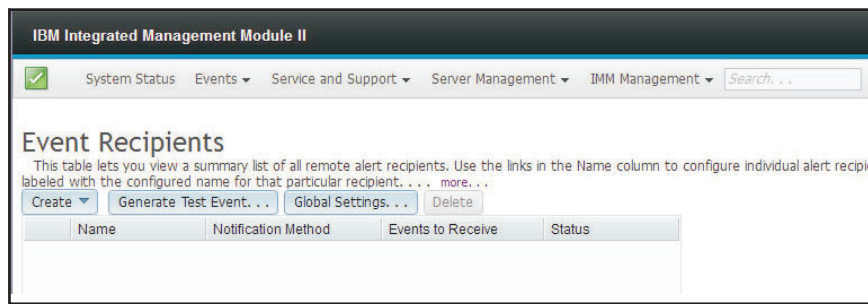
Wählen Sie die Option **Event Recipients** (Ereignisempfänger) aus, um E-Mail- und syslog-Benachrichtigungen hinzuzufügen und zu ändern.

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

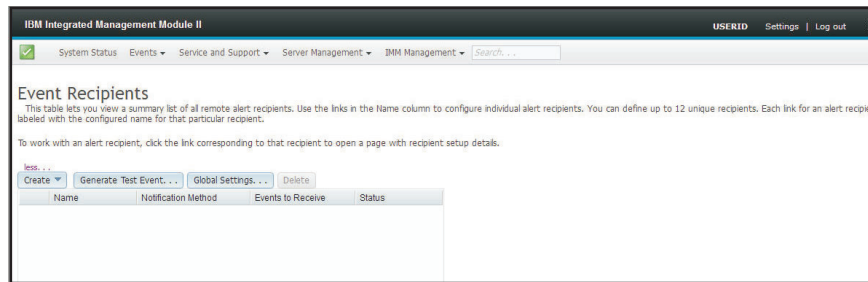


Mithilfe der Option **Event Recipients** (Ereignisempfänger) können Sie die Empfänger von Benachrichtigungen über Systemereignisse verwalten. Sie können die einzelnen Empfänger konfigurieren und die Einstellungen verwalten, die auf alle Ereignisempfänger angewendet werden. Sie können außerdem ein Testereignis erstellen, um zu überprüfen, ob die Benachrichtigungsfunktion funktioniert.

In der folgenden Abbildung ist die Seite "Event Recipients" dargestellt.



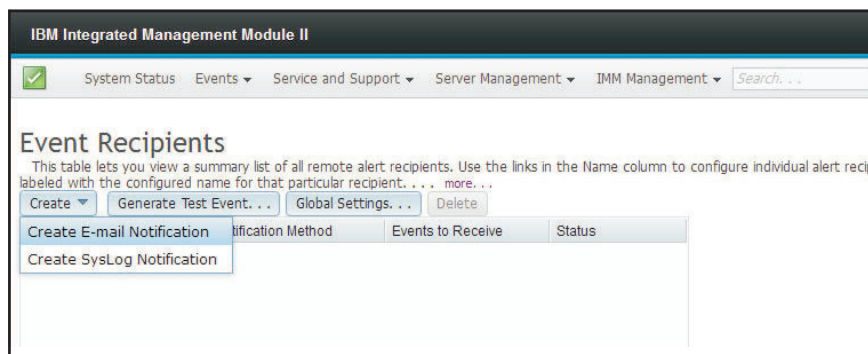
In der folgenden Abbildung sind weitere Informationen dargestellt, die angezeigt werden, wenn Sie auf den Link **more** (mehr) auf der Seite "Event Recipients" klicken.



E-Mail- und syslog-Benachrichtigungen erstellen

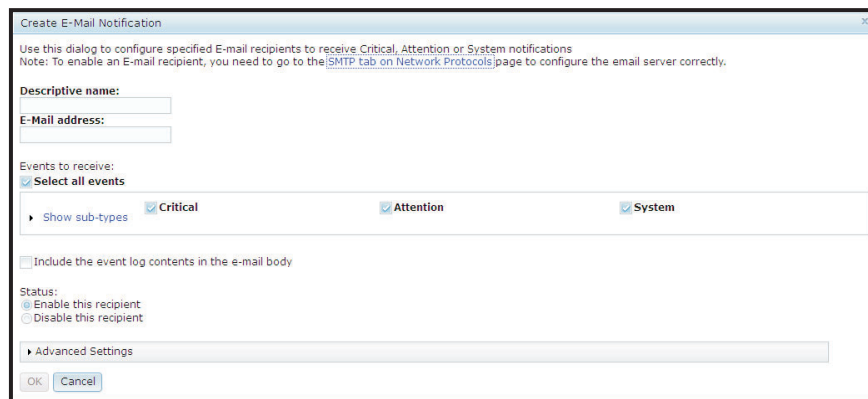
Wählen Sie die Registerkarte **Create** (Erstellen) aus, um E-Mail- und syslog-Benachrichtigungen zu erstellen.

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

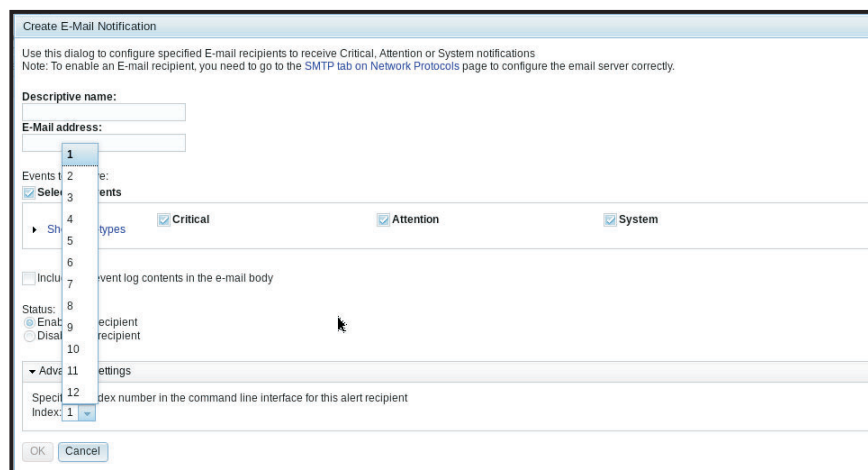


Mit der Option **Create E-mail Notification** (E-Mail-Benachrichtigung erstellen) können Sie eine Empfangs-E-Mail-Adresse einrichten und die Ereignistypen auswählen, über die Sie benachrichtigt werden möchten. Außerdem können Sie auf **Advanced Settings** (Erweiterte Einstellungen) klicken, um die Startindexzahl 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.

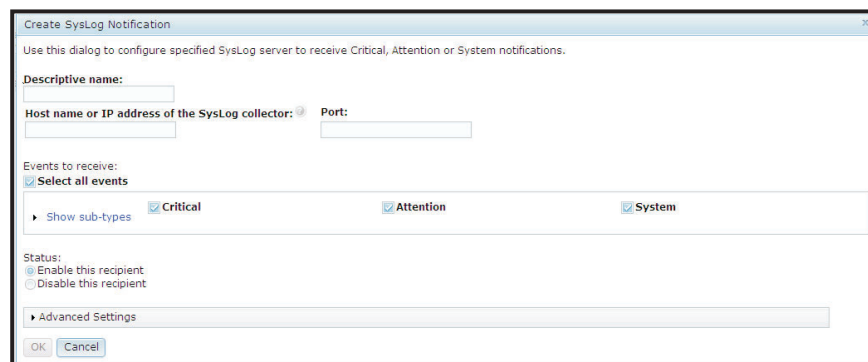


In der folgenden Abbildung sind die Optionen des Teilfensters "Advanced Settings" dargestellt.



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.



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

Testereignisse generieren

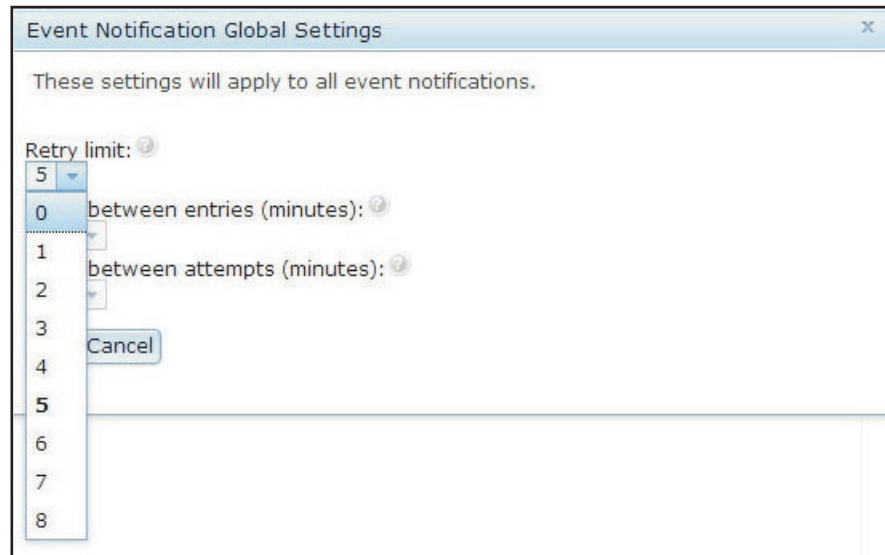
Verwenden Sie die Registerkarte **Generate Test Event...** (Testereignis generieren), um eine Test-E-Mail an eine bestimmte E-Mail-Adresse zu senden. Klicken Sie nach Auswahl der Ereignisbenachrichtigung auf **OK**, um ein Testereignis zu generieren. Das Testereignis mit dem Hinweis, dass es sich um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

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

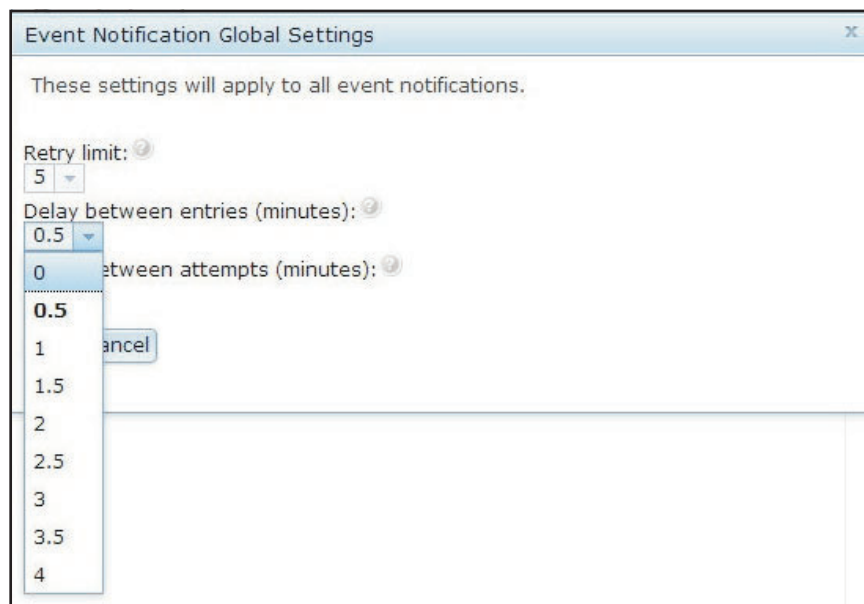
Wiederholungslimit für Benachrichtigungen festlegen

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).

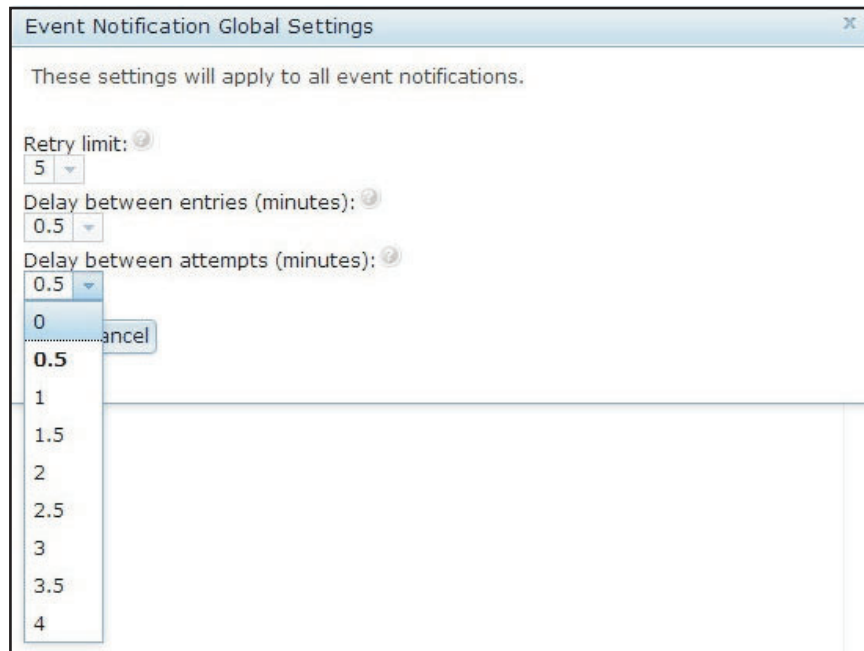
In der folgenden Abbildung sind die Einstellungen für die Option "Retry limit" (Wiederholungslimit) dargestellt.



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



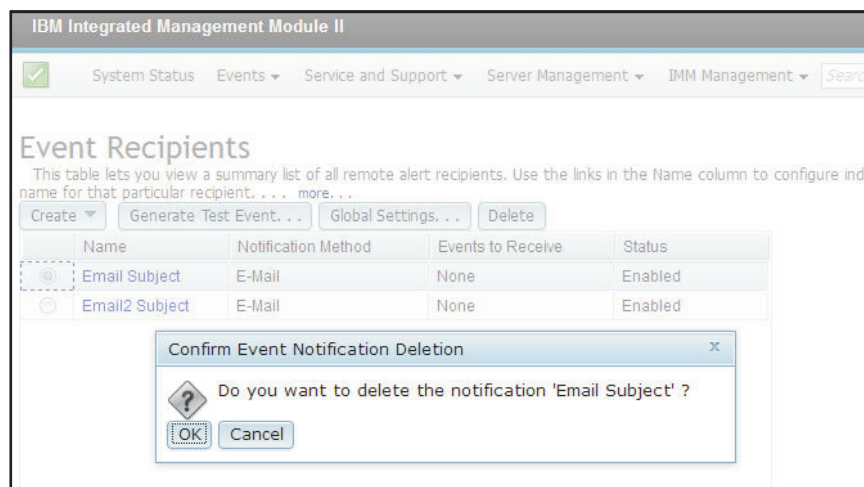
In der folgenden Abbildung sind die Einstellungen für die Option "Delay between attempts (minutes)" (Verzögerung zwischen Versuchen (Minuten)) dargestellt.



E-Mail- oder syslog-Benachrichtigungen löschen

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

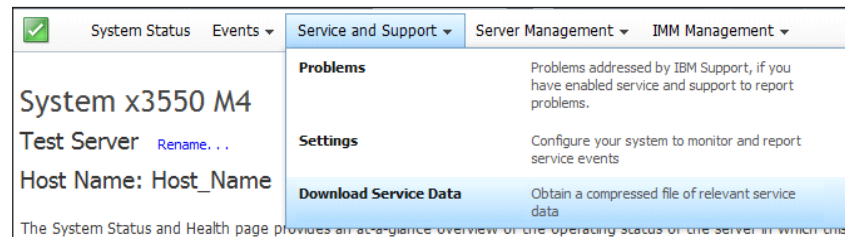
In der folgenden Abbildung ist das Fenster "Confirm Event Notification Deletion" (Löschen der Ereignisbenachrichtigung bestätigen) dargestellt.



Informationen für Service und Support erfassen

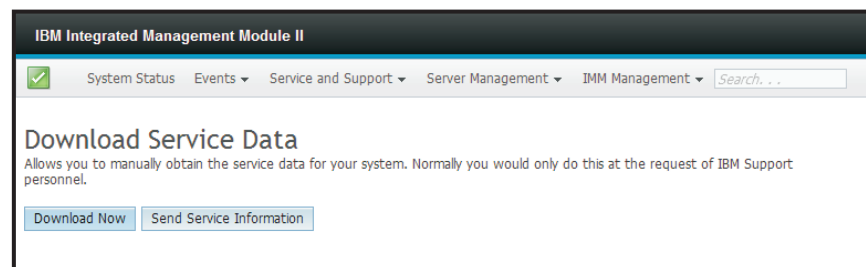
Klicken Sie auf die Option **Download Service Data** (Servicedaten herunterladen) im Menü "Service and Support" (Service und Support), um Informationen zum Server zu erfassen. Diese kann der IBM Support verwenden, um Sie bei der Lösung Ihres Problems zu unterstützen.

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



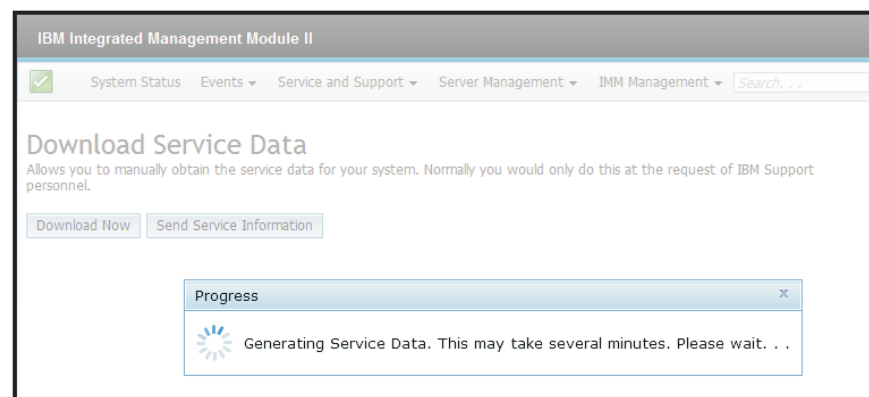
Klicken Sie auf die Schaltfläche **Download Now** (Jetzt herunterladen), wenn Sie die Daten für Service und Support herunterladen möchten.

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

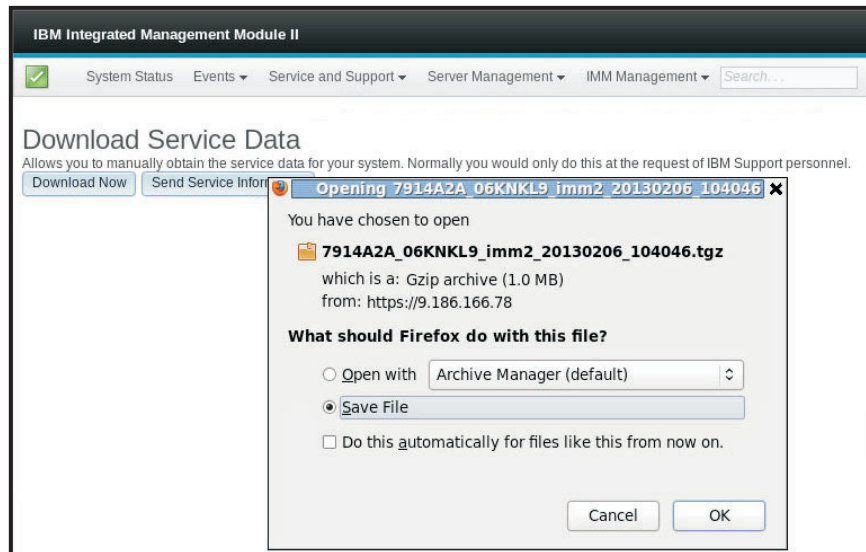


Der Erfassungsprozess der Daten für Service und Support wird gestartet. Dieser Prozess dauert ein paar Minuten; es werden die Servicedaten zum Speichern in einer Datei generiert.

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-Funktionalitätsversion "Advanced Level" verfügbar. Informationen zur Version 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.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

Serverstromversorgung verwalten

Wählen Sie die Option **Power Management** (Stromverbrauchssteuerung) unter der Registerkarte **Server Management** (Serververwaltung) aus, um Informationen zur Stromverbrauchssteuerung anzuzeigen und Funktionen zur Stromverbrauchssteuerung auszuführen.

Anmerkung: In einem IBM Flex System werden die Kühlung und die Stromversorgung des Gehäuses vom Chassis Management Module (CMM) gesteuert. Aus diesem Grund werden die Optionen "Cooling Devices" (Kühlungseinheiten) und "Power Modules" (Stromversorgungsmodule) nicht auf der Registerkarte **Server Management** angezeigt.

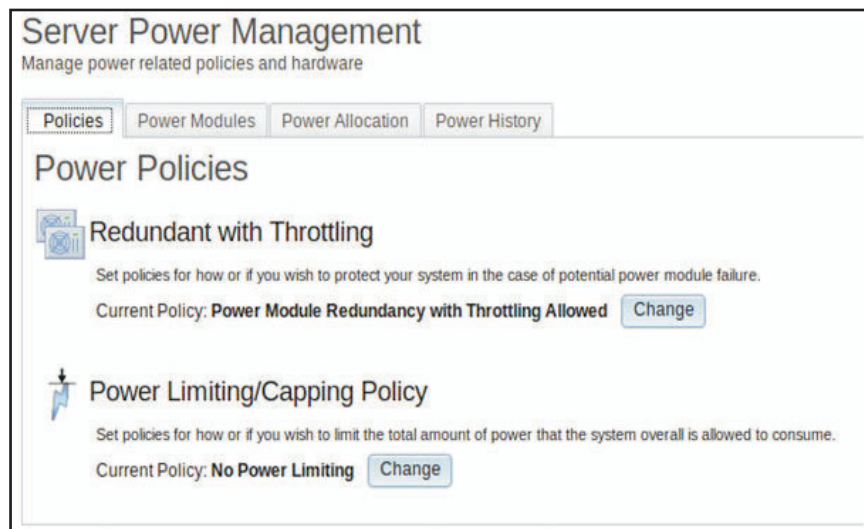
Stromversorgung und gesamte Stromversorgung des Systems steuern

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.

Anmerkung: Die Registerkarte **Policies** ist in einem IBM Flex System-Knoten nicht verfügbar.

Bis zu zwei Netzteile konfigurieren

In der folgenden Abbildung ist die Registerkarte **Policies** (Richtlinien) für Server dargestellt, die bis zu zwei Netzteile unterstützen können.



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.

Folgende Felder sind auf der Seite "Power Policies" (Stromversorgungsrichtlinien) verfügbar:

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.

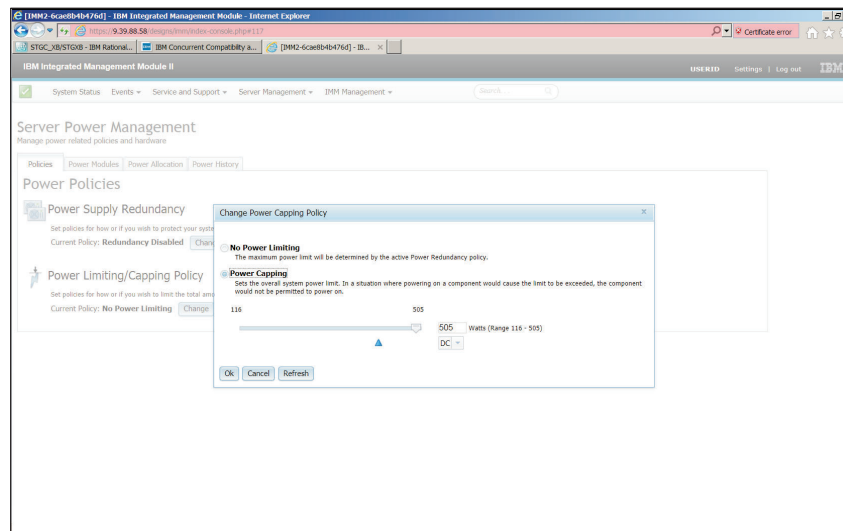
	Power Supply Failure Limit	Maximum Power Limit (Watts)	Estimated Usage ^{††}
☐ Redundant without Throttling System will be allowed to boot only if it is guaranteed to survive the loss of a power supply and continue to run without throttling.	1	550	100%
☒ Redundant with Throttling System will be allowed to boot only if it is guaranteed to survive the loss of a power 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 throttling 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%

[†] This is the maximum number of power supplies that can fail while still guaranteeing the operation of the selected policy.
^{††} The estimated usage is based on the maximum power limit allowed in this policy and the current aggregated power in use of all components in the chassis.

Ok Cancel

Über "Active Energy Manager" können Sie einen Grenzwert für den zulässigen Gesamtstromverbrauch 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).

Klicken Sie im Fenster "Change Power Capping Policy" (Netzstrombegrenzungsrichtlinie ändern) auf die Schaltfläche **Power Capping** und verschieben Sie die *Schiebereglernmarke* auf die gewünschte Wattzahl, um die allgemeine Strombegrenzung für den Server festzulegen (wie in der folgenden Abbildung dargestellt). Der Pfeil stellt einen Richtwert für das Festlegen eines Grenzwerts für die Netzstrombegrenzung dar.

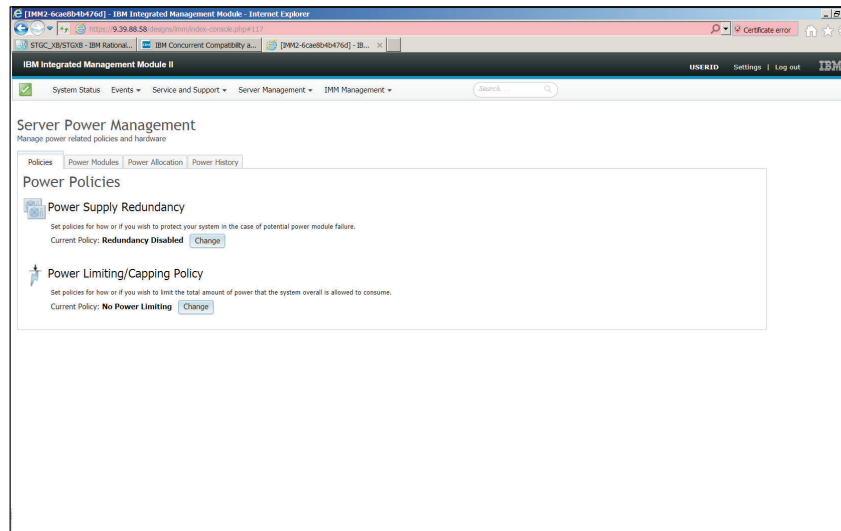


Bis zu vier Netzteile konfigurieren

Wenn der Server bis zu vier Netzteile unterstützt, können Sie den Server für die Bereitstellung einer *Netzstromzuführungsredundanz* konfigurieren. Bei einer *Netzstromzuführungsredundanz* werden ein oder zwei Netzteile mit einer Netzstromzuführung (bzw. einer Netzstromquelle) und ein oder zwei zusätzliche Netzteile mit einer anderen Netzstromzuführung (bzw. Netzstromquelle) verbunden. Wenn eine der Netzstromzuführungen (Netzstromquellen) fehlschlägt, verhindert das Netzteil (oder die Netzteile) an der anderen Netzstromzuführung (Netzstromquelle) den Ausfall des Servers.

Anmerkung: Damit die Netzstromzuführungsredundanz richtig funktioniert, müssen die Netzteile in den Positionen 1 und 3 mit einer Netzstromzuführung (Netzstromquelle) verbunden werden. Die Netzteile in den Positionen 2 und 4 müssen mit einer anderen Netzstromzuführung (Netzstromquelle) verbunden werden.

In der folgenden Abbildung ist die Registerkarte **Policies** (Richtlinien) für Server dargestellt, die bis zu vier Netzteile unterstützen können.



Um die Richtlinie auszuwählen, die Sie zum Schützen des Servers bei Ausfall eines Stromversorgungsmoduls verwenden möchten, klicken Sie im Fenster "Power Policies" (Stromversorgungsrichtlinien) auf die Schaltfläche **Change** (Ändern) für "Current Policy" (Aktuelle Richtlinie) für die Option "Power Supply Redundancy" (Netzteilredundanz). Ein Fenster ähnlich der folgenden Abbildung erscheint. Durch Auswahl einer Stromversorgungsrichtlinie können Sie einen Kompromiss zwischen Redundanz und verfügbarer Leistung finden.

Power supply configuration:	Nominal Rating	Voltage	Effective Rating	Feed 1	Feed 2
Bay 1	1400W	110Vac	900W	✓	
Bay 2	1400W	220Vac	1400W		✓
Bay 3	1400W	220Vac	1400W	✓	
Bay 4	1400W	110Vac	900W		✓

Non-Redundant Available power: 3192W

Maximum power consumption:

	With Full Throttling	With No Throttling
Budget for current configuration	461W	536W
Budget for all hot-plug components	596W	672W

Allow Throttling to keep system within power budget: ☒

N+1 Redundancy (specify desired configuration/budget):

	N+0	N+1
1+1 with one 900W power supply per feed	900W	1080W
1+1 with one 1400W power supply per feed	1400W	1680W
2+2 with two 900W power supplies per feed	1710W	2052W
2+2 with one 900W and 1400W power supply per feed	2160W	2592W

OK Cancel Refresh

Folgende Felder sind auf der Seite "Power Policies" (Stromversorgungsrichtlinien) verfügbar:

Power supply configuration (Netzteilkonfiguration)

Dieses Feld ist ein schreibgeschützter Abschnitt, in dem die Netzteile in den einzelnen Positionen und die zugehörigen Informationen zu den einzelnen Netzteilen angezeigt werden.

Non-Redundant Available power (Nicht redundanter verfügbarer Netzstrom)

Wenn der Server in einem nicht redundanten Betriebsmodus ausgeführt wird, wird der verfügbare, nicht redundante Netzstrom in diesem Feld angezeigt. Im nicht redundanten Betriebsmodus wird angenommen, dass der gesamte Netzstrom von allen Netzteilen verfügbar ist.

Maximum power consumption (Maximaler Stromverbrauch)

In diesem Feld wird der maximal mögliche Stromverbrauch des Servers angezeigt, unabhängig von den installierten Netzteilen. Sie können die Konfiguration auswählen, für die Sie den Stromverbrauch einschränken möchten, indem Sie eine der beiden folgenden Optionen auswählen:

- Budget for current configuration (Einschränkung für aktuelle Konfiguration)
- Budget for all hot-plug components (Einschränkung für alle im laufenden Betrieb anzuschließenden Komponenten)

Allow Throttling to keep system within power budget (Regulierung zulassen, damit das System den Maximalwert für den Stromverbrauch nicht überschreitet)

Klicken Sie auf dieses Kontrollkästchen, um eine Regulierung zuzulassen. Eine Regulierung des Mikroprozessors ist ein Prozess, mit dem Sie effizient Serverenergie und Netzstrom sparen können. Das heißt, Sie können den Stromverbrauch des Servers damit im gewünschten Rahmen halten.

Anmerkung: Eine Regulierung im normalen Betrieb kann jedoch die Leistung des Servers beeinträchtigen.

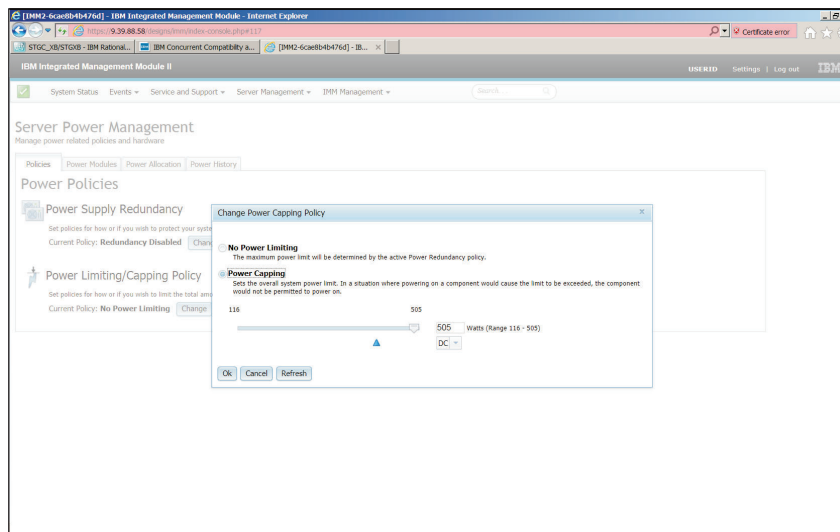
N+N Redundancy (specify desired configuration/budget) (N+N-Redundanz (gewünschte Konfiguration/Menge angeben))

Wählen Sie dieses Kontrollkästchen aus, wenn der Server im Redundanz-Betriebsmodus ausgeführt werden soll. Wenn Sie auf dieses Kontrollkästchen klicken, werden zusätzliche Redundanzkonfigurationen zur Auswahl angezeigt, sodass Sie die gewünschte Konfiguration oder den gewünschten Maximalwert für den Stromverbrauch noch detailliert festlegen können.

Anmerkung: Wenn dieses Kontrollkästchen nicht ausgewählt ist, wird der Server ohne Redundanz ausgeführt.

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).

Klicken Sie im Fenster "Change Power Capping Policy" (Netzstrombegrenzungsrichtlinie ändern) auf die Schaltfläche **Power Capping** und verschieben Sie die *Schiebereglermarke* auf die gewünschte Wattzahl, um die allgemeine Strombegrenzung für den Server festzulegen (wie in der folgenden Abbildung dargestellt). Der Pfeil stellt einen Richtwert für das Festlegen eines Grenzwerts für die Netzstrombegrenzung dar.



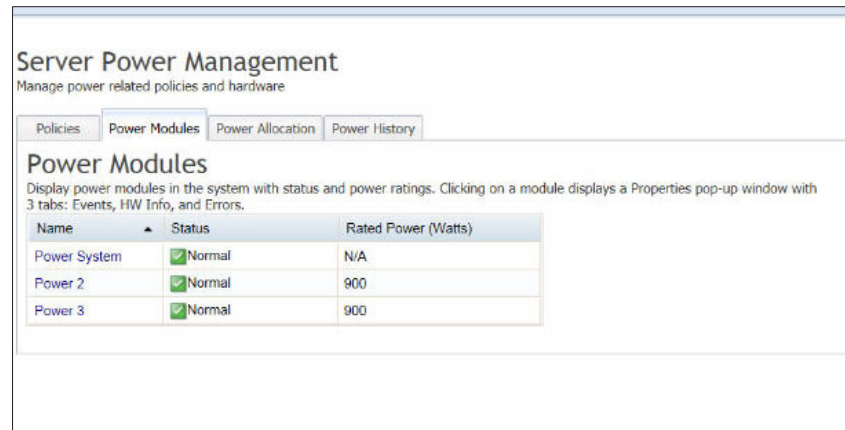
Aktuell installierte Netzteile anzeigen

Klicken Sie auf die Registerkarte **Power Modules** (Stromversorgungsmodule), um Informationen zu aktuell installierten Netzteilen anzuzeigen. Der Name jedes im Server installierten Stromversorgungsmoduls 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).

In der folgenden Abbildung ist die Registerkarte **Power Modules** für Server dargestellt, die bis zu zwei Netzteile unterstützen können.

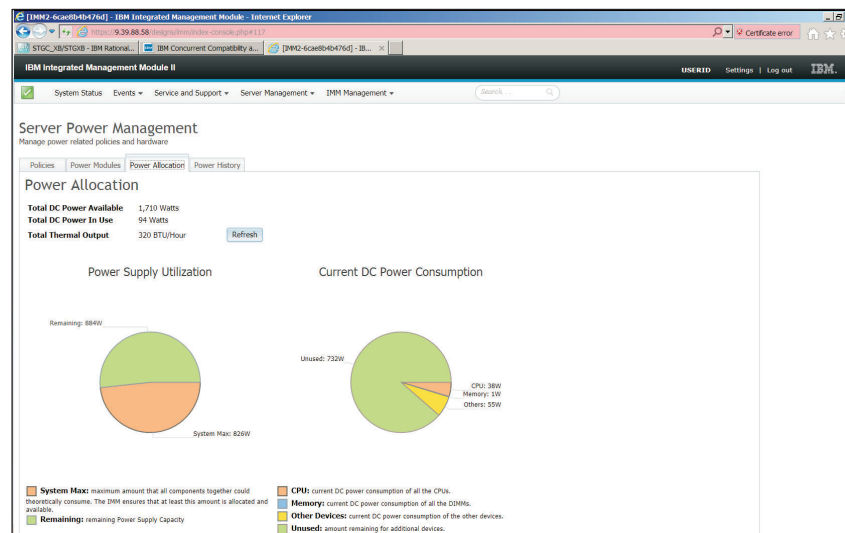
Server Power Management		
Manage power related policies and hardware		
Policies	Power Modules	Power Allocation Power History
Power Modules		
Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.		
Name	Status	Rated Power (Watts)
Power System	Normal	N/A
Power 1	Normal	550
Power 2	Normal	550

In der folgenden Abbildung ist die Registerkarte **Power Modules** für Server dargestellt, die bis zu vier Netzteile unterstützen können.



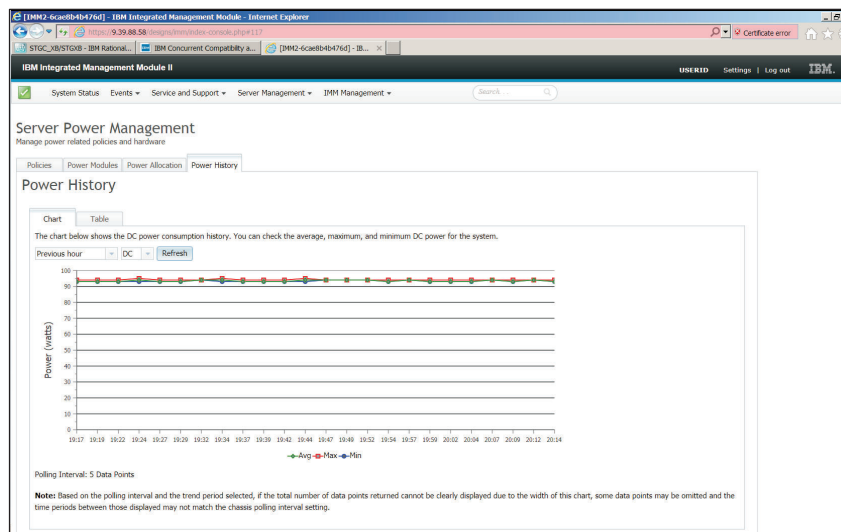
Stromversorgungskapazität anzeigen

Klicken Sie auf die Registerkarte **Power Allocation** (Netzstromzuordnung), um anzuzeigen, wie viel der Stromversorgungskapazität verwendet wird, und um den aktuellen Gleichstromverbrauch (Current DC Power Consumption) 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 Server verbraucht wird. Über die Registerkarte **Chart** (Diagramm) können Sie den Zeitraum auswählen. Außerdem haben Sie auch die Möglichkeit, den Wechsel- oder Gleichstrom anzuzeigen. Der durchschnittliche, maximale und minimale Stromverbrauch wird angezeigt (wie in der folgenden Abbildung dargestellt).



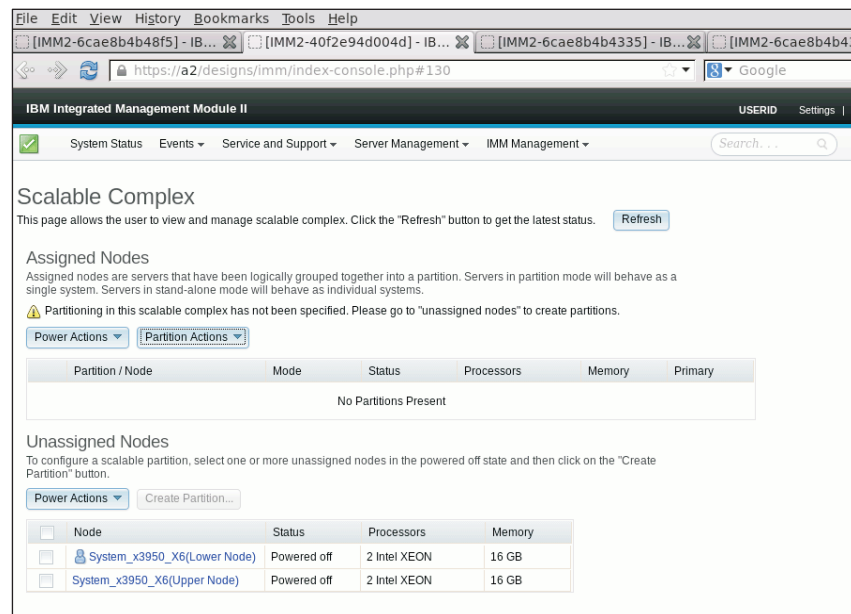
Skalierbaren Komplex verwalten

Anmerkung: In diesem Abschnitt werden die Begriffe *Knoten* und *Server* austauschbar verwendet.

Mit der Option **Scalable Complex** (Skalierbarer Komplex) können Sie den aktuellen Zustand aller verfügbaren Knoten (Server) anzeigen und verwalten. Ein skalierbarer Komplex ermöglicht das Unterteilen von Knoten in getrennte Partitionen oder unabhängige Knoten. Zugeordnete Knoten sind Server, die logisch in einer Partition zusammengefasst sind. Server in einer Partition agieren als ein *einzelnes* System und können gemeinsam Ressourcen nutzen. Die Knoten in einer Partition können ebenfalls in Standalone-Knoten (unabhängige Knoten) unterteilt werden. Ein Knoten im Standalone-Modus wird als *einzelnes* System ausgeführt. Wählen Sie die Option **Scalable Complex** (Skalierbarer Komplex) auf der Registerkarte **Server Management** (Serververwaltung) aus, um den Server zu konfigurieren. Die Seite "Scalable Complex" enthält die Abschnitte "Assigned Nodes" (Zugeordnete Knoten) und "Unassigned Nodes" (Nicht zugeordnete Knoten). Sie können auf die Schaltfläche **Refresh** (Aktualisieren) klicken, um die neuesten Statusinformationen für die Knoten abzurufen.

In der folgenden Abbildung sind keine zugeordneten Knoten enthalten. In dieser Abbildung werden die Knoten als einzelne Server ausgeführt. Ohne zugeordnete Knoten sind die einzigen verfügbaren Funktionen die Fernsteuerung der Serverstromversorgung oder das Erstellen einer Partition im Abschnitt "Assigned Nodes". Sie können die Serverstromversorgung auf der Registerkarte **Power Actions** (Stromversorgungsaktionen) steuern, wie im Abschnitt „Stromversorgungsstatus des Servers steuern“ auf Seite 128 erläutert.

Anmerkung: Um Partitionen hinzufügen oder entfernen zu können, muss die gesamte Stromversorgung des Servers ausgeschaltet werden.



Partition erstellen

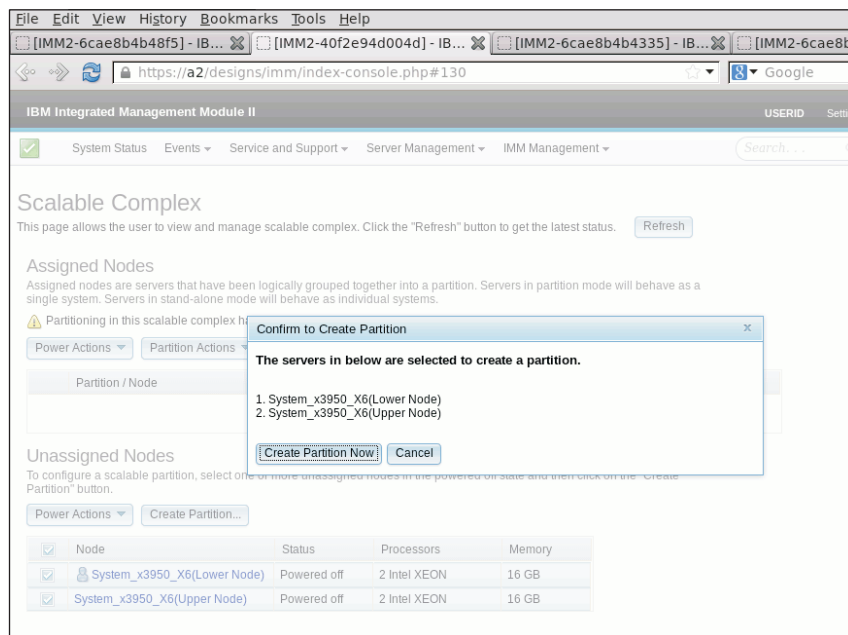
Wählen Sie im Abschnitt "Unassigned Nodes" (Nicht zugeordnete Knoten) auf der Seite "Scalable Complex" (Skalierbarer Komplex) das Kontrollkästchen aus, das den Knoten entspricht, die Sie zu Ihrer Partition hinzufügen möchten.

Anmerkungen:

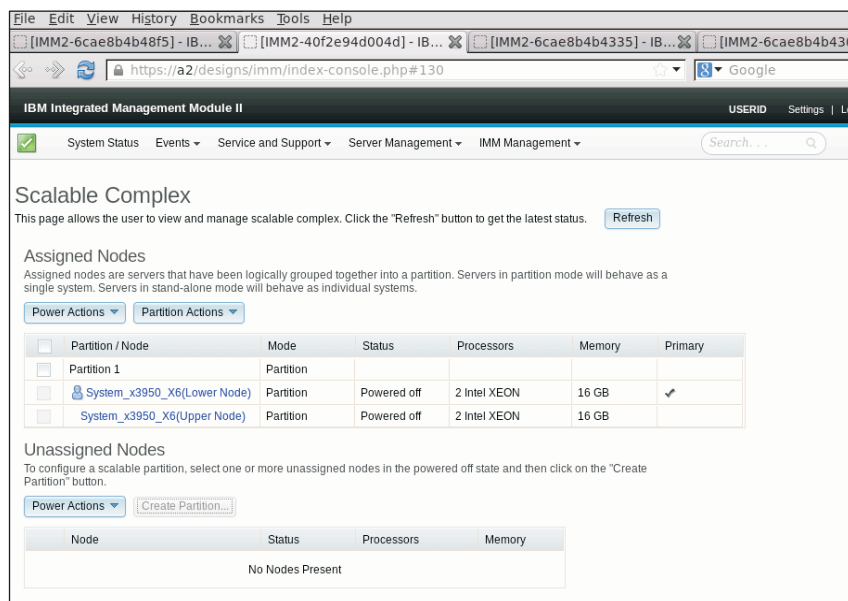
- Um eine Partition hinzuzufügen, muss die gesamte Stromversorgung für den Server ausgeschaltet werden.
- Die Schaltfläche **Create Partition** (Partition erstellen) wird abgeblendet dargestellt, bis ein Knoten ausgewählt ist.
- Wenn Sie das Kontrollkästchen "Node" (Knoten) auswählen, werden automatisch alle Knoten einbezogen und als ausgewählt markiert.
- Die Firmwareversionen der Knoten innerhalb des skalierbaren Komplexes müssen dieselben sein.

Ein Fenster mit dem Titel "Confirm to Create Partition" (Erstellen von Partition bestätigen) wird geöffnet, das die Knoten enthält, die zuvor ausgewählt wurden (wie in der folgenden Abbildung dargestellt). Klicken Sie auf die Schaltfläche **Create Partition Now** (Partition jetzt erstellen), um die Partition zu erstellen. Sie erhalten eine Bestätigungsnachricht, dass die Partition erfolgreich erstellt wurde. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um den neuen Partitionsstatus anzuzeigen, falls die Anzeige der Seite nicht automatisch aktualisiert wird. Nachdem die Partition erstellt wurde, werden der Status aller Partitionen und alle nicht zugeordnete Knoten angezeigt. Die Stromversorgung des Servers kann mithilfe der Schaltfläche **Power Actions** (Stromversorgungsaktionen) ein- oder ausgeschaltet werden. Außerdem kann die Partition entfernt oder der Betriebsmodus für die Partition geändert werden. Dies ist mithilfe der Schaltfläche **Partition Actions** (Partitionsaktionen) möglich.

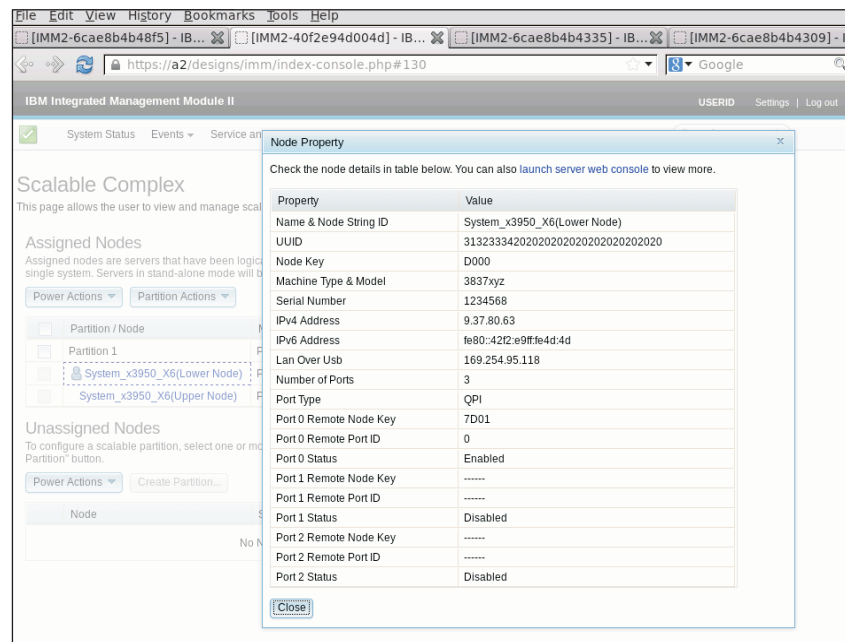
Anmerkung: Im Partitionsbetriebsmodus werden Knoten als einzelne, gemeinsam genutzte Systemressourcen ausgeführt.



Nachdem die Partition erstellt wurde, erscheint ein Fenster (ähnlich dem in der folgenden Abbildung dargestellten), in dem der Status aller Partitionen und der nicht zugeordneten Knoten angezeigt wird.

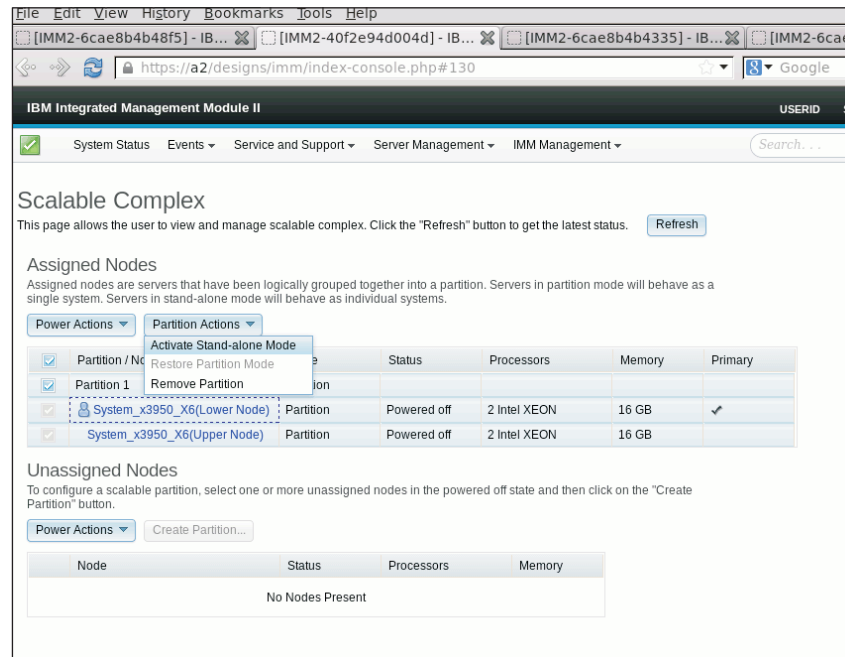


Durch Klicken auf einen einzelnen Knoten in der Partition können Sie Details zu diesem Knoten anzeigen. Das Fenster "Node Property" (Knoteneigenschaft) wird angezeigt (wie in der folgenden Abbildung dargestellt).



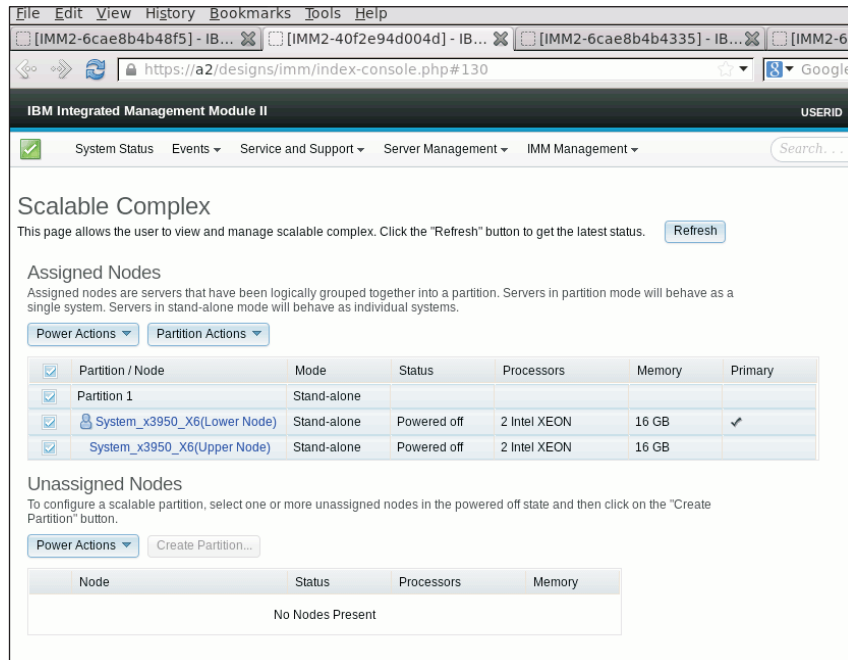
Modus zum Ändern einer Partition

Klicken Sie auf die Registerkarte **Partition Actions** (Partitionsaktionen) auf der Seite "Scalable Complex" (Skalierbarer Komplex), um den Betriebsmodus für die Partition zu ändern oder um die Partition zu entfernen (wie in der folgenden Abbildung dargestellt).



Klicken Sie auf **Activate Stand-alone Mode** (Standalone-Modus aktivieren), um zuzulassen, dass jeder einzelne Knoten unabhängig von den anderen Knoten agieren kann. Klicken Sie auf **Restore Partition Mode** (Modus zur Wiederherstellung der Partition), um zwischen dem Partitionsmodus und dem Standalone-Modus zu wechseln. Klicken Sie auf **Remove Partition** (Partition entfernen), um die Partition zu entfernen.

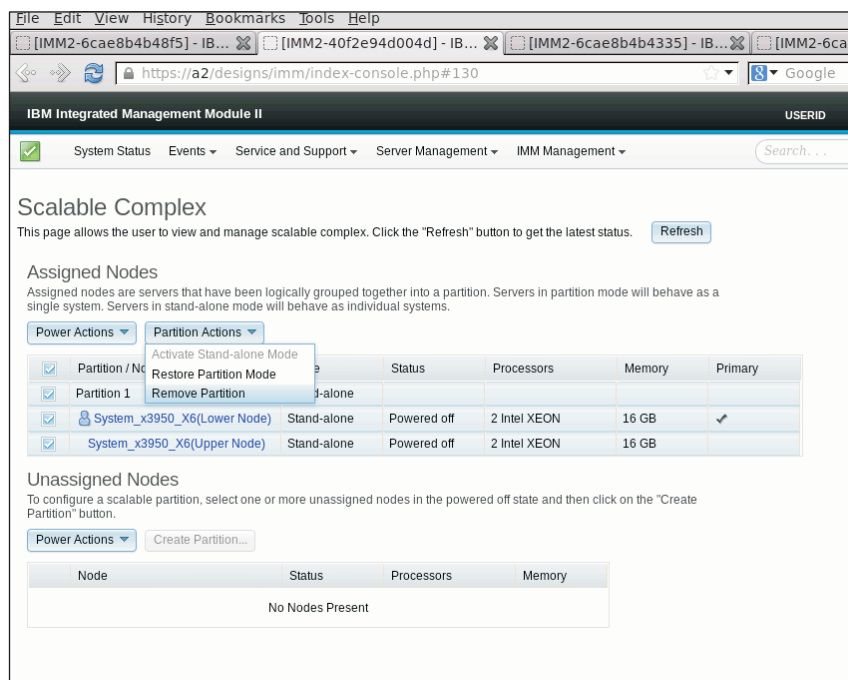
In der folgenden Abbildung sind die Knoten im Standalone-Betriebsmodus dargestellt.



Modus zum Löschen einer Partition

Wählen Sie die Registerkarte **Remove Partition** (Partition entfernen) aus, um eine Partition zu löschen (wie in der folgenden Abbildung dargestellt).

Anmerkung: Um eine Partition entfernen zu können, muss die Stromversorgung zum betreffenden Knoten ausgeschaltet werden.



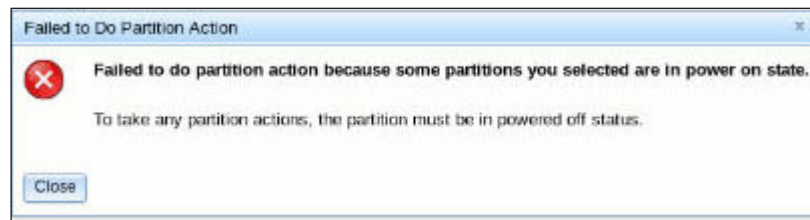
Partitionsfehler

Beim Arbeiten mit Partitionen können Fehlerbedingungen auftreten. Wenn eine Fehlerbedingung vorhanden ist, gibt das IMM2 einen Ereigniscode in die Ereignisprotokolle aus. In der folgenden Tabelle werden zwei Fehlerbedingungen beschrieben und in den nächsten beiden Abbildungen angezeigt.

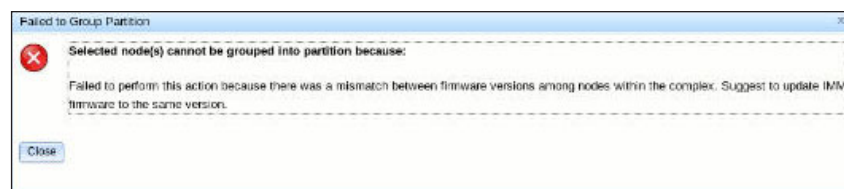
Tabelle 8. Partitionsfehlerbedingungen

Fehler	Beschreibung	Maßnahme
Failed to do partition action (Partitionsaktion ist fehlgeschlagen).	Einige der ausgewählten Partitionen befinden sich im eingeschalteten Zustand.	Schalten Sie die betreffende Partition aus.
Failed to group partition (Partitionsgruppieren ist fehlgeschlagen).	Zwischen den Firmwareversionen der Knoten innerhalb des Komplexes gibt es eine Abweichung.	Aktualisieren Sie die IMM2-Firmwareversion für alle Knoten auf dieselbe Firmwareversion.

In der folgenden Abbildung ist die Antwort dargestellt, die Sie empfangen, wenn Sie versuchen, eine Partitionsaktion durchzuführen, obwohl die Knoten in dieser Partition eingeschaltet sind. Um diesen Fehler zu beheben, schalten Sie alle Knoten in der Partition aus.



In der folgenden Abbildung ist die Antwort dargestellt, die Sie empfangen, wenn zwischen den Firmwareversionen der einzelnen Knoten eine Abweichung besteht. Um den Fehler zu beheben, stellen Sie sicher, dass alle Knoten dieselbe IMM2-Firmwareversion aufweisen.



Konfiguration des lokalen Speichers anzeigen

Klicken Sie auf die Option **Local Storage** (Lokaler Speicher) auf der Registerkarte **Server Management** (Serververwaltung) oder auf den Link "Local Storage" in der Tabelle "Hardware Health" (Hardwarezustand) auf der Seite "System Status and Health" (Systemstatus und -zustand) aus, um den Speicherstatus des Servers anzuzeigen. Mit dieser Option können Sie den Status des lokalen Speichers, die Konfiguration und detaillierte Informationen zum Server anzeigen.

Anmerkung: Wenn der Server die Option **Local Storage** nicht unterstützt, werden nur der Status der Platten und die zugehörigen aktiven Ereignisse angezeigt.

Informationen zu physischen Ressourcen anzeigen

Klicken Sie auf der Seite "Local Storage" (Lokaler Speicher) auf die Registerkarte **Physical Resource** (Physische Ressource), um eine Übersicht über die physische Ressource des Servers anzuzeigen (wie in der folgenden Abbildung dargestellt). Die Übersicht umfasst auch die unterstützten RAID-Controller und Informationen zu den zugehörigen Laufwerken. Um die neuesten Statusinformationen abzurufen, klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren).

Anmerkung: Auf der Seite "Physical Resource" werden die unterstützten RAID-Controller und die zugehörigen physischen Laufwerke angezeigt. Für physische Laufwerke, denen kein RAID-Controller zugeordnet ist, wird im Feld **Name** die Option "None-manageable drives to IMM" (Für IMM nicht verwaltbare Laufwerke) angezeigt.

IBM Integrated Management Module II

System Status Events Service and Support Server Management IMM Management

Local Storage

Display storage devices physical structure and storage configuration. You can refresh to get latest status.

Refresh

Physical Resource Storage RAID Configuration

Click on a device to see active events and properties.

RAID Controllers and Physical Drives

Name	Health Status	Capacity	Serial No
☐ ServeRAID M1210e(PCI Slot 0)			3B6015
☐ Drive 3	Normal	465.762GB	9XF2JL2T1018BD2E
☐ Non-manageable drives to IMM			
☐ Drive 0	Normal		

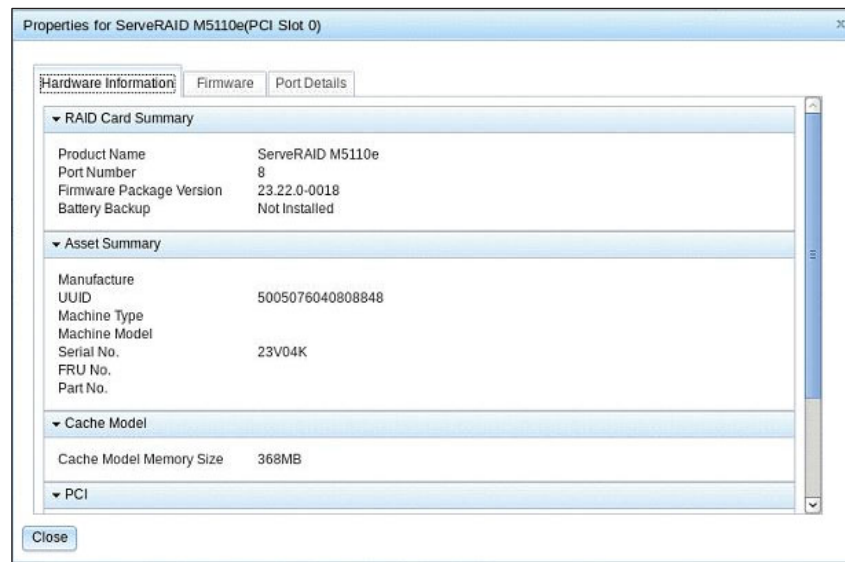
Flash DIMMs

Name	Health Status	Capacity
No FlashDIMM is installed in the system or FlashDIMM information is not retrieved at this time		

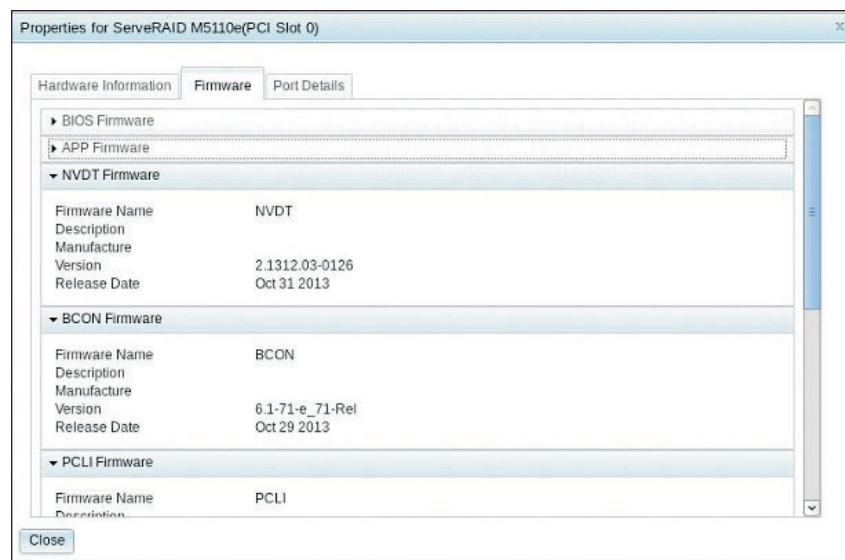
Klicken Sie auf den Link für den unterstützten RAID-Controller, um die aktiven Ereignisse sowie Informationen zur Hardware, Firmware und zu den Anschlüssen des Controllers anzuzeigen.

Die Registerkarte **Hardware Information** enthält die folgenden Informationen (wie in der folgenden Abbildung dargestellt):

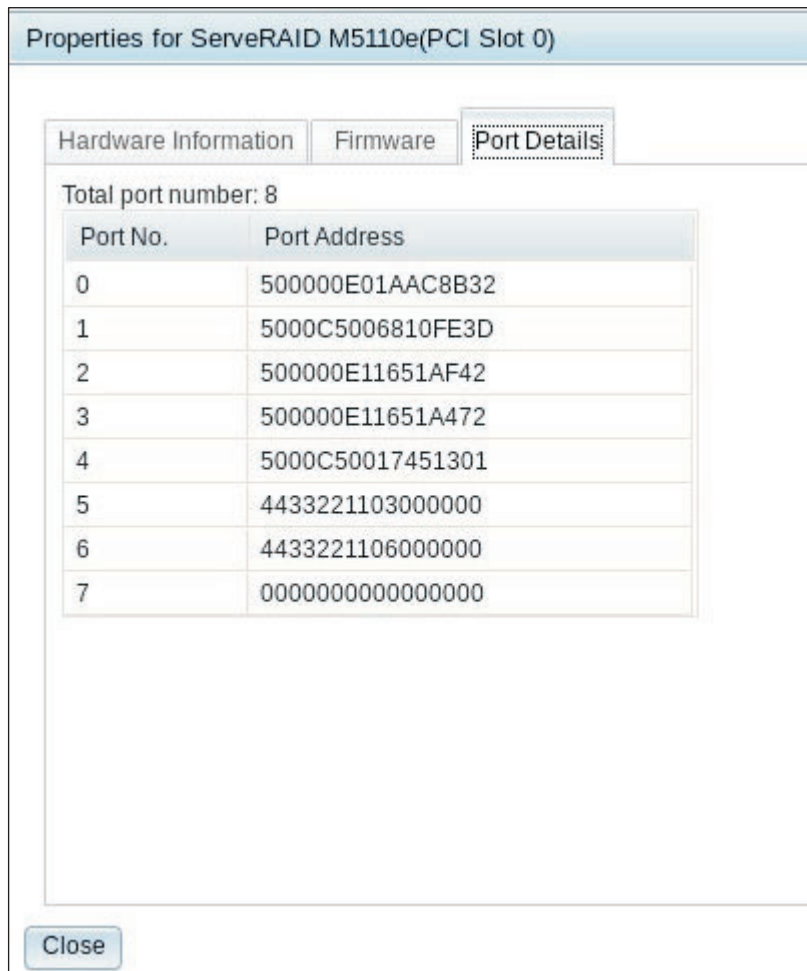
- RAID card summary (Übersicht zur RAID-Karte)
- Asset summary (Ressourcenübersicht)
- Cache model (Cachemodell)
- PCI
- Battery backup (Notstromversorgung) (falls eine Notstromversorgung installiert ist)



Die Registerkarte **Firmware** enthält detaillierte Firmwareinformationen zum RAID-Controller (wie in der folgenden Abbildung dargestellt).



Die Registerkarte **Port Details** (Details zum Anschluss) enthält Informationen zur Anschlussnummer und zur Anschlussadresse für den RAID-Controller (wie in der folgenden Abbildung dargestellt).



Klicken Sie auf den Link des dem RAID-Controller zugeordneten Laufwerks. Die Seite "Properties" (Eigenschaften) für das Laufwerk wird geöffnet. Klicken Sie auf die Registerkarte **Events**, **Hardware Information** oder **Firmware**, zu weitere Informationen zu diesem Laufwerk anzuzeigen.

Anmerkung: Wenn das Laufwerk auf der Seite "Physical Resource" als "Non-manageable drives to IMM" (Für IMM nicht verwaltbare Laufwerke) gekennzeichnet ist, werden nur die zugehörigen aktiven Ereignisse angezeigt.

In den folgenden beiden Abbildungen sind die Seiten "Hardware Information" und "Firmware" für das Laufwerk dargestellt, das dem RAID-Controller zugeordnet ist.

Properties for Drive 1

Events

Hardware Information

Firmware

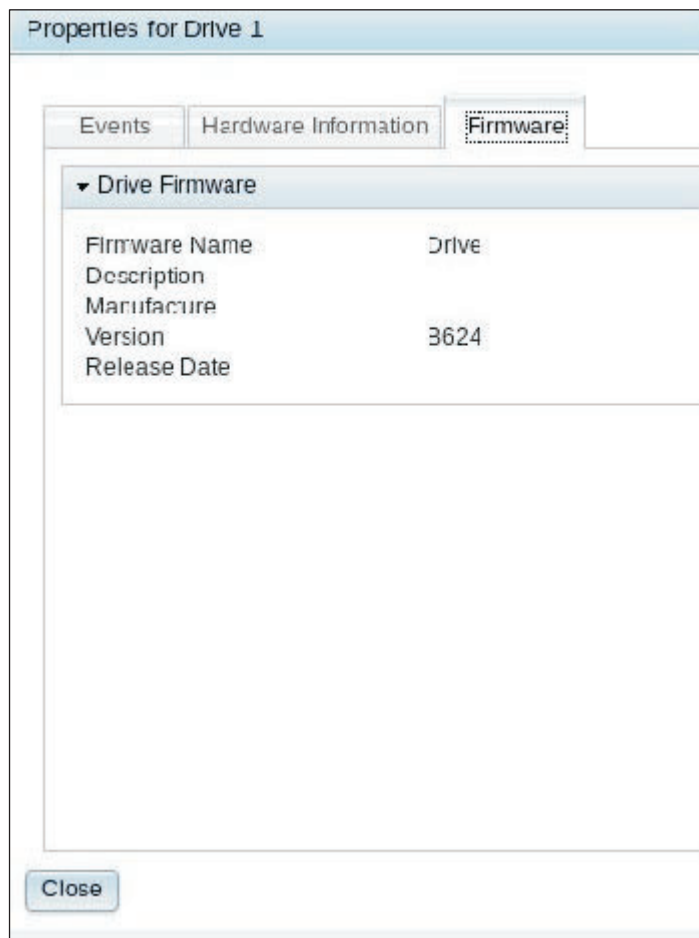
▼ Drive Summary

Product Name	ST973452SS
State	Online
Slot No.	1
Disk Type	SAS
Media Type	HDD
Speed	6.0Gb/s
Current Temperature	0° C

▼ Asset Summary

Manufacture	IBM-ESXS
Device ID	5
Enclosure ID	0x00FC
Machine Type	
Machine Model	
Serial No.	3TA0M7TY
FRU No.	42C0261
Part No.	43X0847

Close



Registerkarte "Storage RAID Configuration"

Klicken Sie auf der Seite "Local Storage" (Lokaler Speicher) auf die Registerkarte **Storage RAID Configuration** (RAID-Speicherkonfiguration), um den Speicher anzuzeigen, der von dem IMM2 verwaltet wird. Sie können die Speicherpools, zugehörige Datenträger und Laufwerke für den RAID-Controller anzeigen. Um die neuesten Statusinformationen abzurufen, klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren).

Auf der Registerkarte **View Logical Drives by Storage Pools** (Logische Laufwerke nach Speicherpools anzeigen) werden die logischen Laufwerke auf dem RAID-Controller angezeigt (wie in der folgenden Abbildung dargestellt). Die logischen Laufwerke sind nach Speicherpools und Controllern sortiert. Außerdem werden detaillierte Informationen zu den einzelnen Datenträgern, wie z. B. die Stripgröße und die Bootfähigkeit des Datenträgers, angezeigt.

IBM Integrated Management Module II			
System Status Events Service and Support Server Management IMM Management			
Local Storage Display storage devices physical structure and storage configuration. You can refresh to get latest status. Refresh			
Physical ResourceStorage RAID Configuration			
Display the storage that manageable by IMM2. You can view storage pools, associated volumes and drives. View Logical Drives by Storage PoolsView Physical Drives by Storage Pools			
Name	RAID State	Capacity	details
[-] ServeRAID M5110e(PCI Slot 0)			
[-] Storage Pool 0	RAID 1	67.055GB(0.055GB free)	1 Volume(s)
Volume 0	Optimal	67.000GB	Bootable, Strip Size 128KB
[-] Storage Pool 1	RAID 1	67.055GB(61.000GB free)	1 Volume(s)
VD_1	Optimal	6.055GB	Not Bootable, Strip Size 128KB

Um die physischen Laufwerke und die zugehörigen Speicherpools anzuzeigen, klicken Sie auf die Registerkarte **View Physical drives by Storage Pools** (Physische Laufwerke nach Speicherpools anzeigen) (wie in der folgenden Abbildung dargestellt). Die Kapazität und die RAID-Stufe des Speicherpools werden angezeigt. Der RAID-Zustand des Laufwerk sowie die Anzahl der Laufwerke im Speicherpool, die Schnittstelle und der Laufwerktyp werden ebenfalls angezeigt.

Local Storage			
Display storage devices physical structure and storage configuration. You can refresh to get latest status.			
Refresh			
Physical ResourceStorage RAID Configuration			
Display the storage that manageable by IMM2. You can view storage pools, associated volumes and drives.			
View Logical Drives by Storage PoolsView Physical Drives by Storage Pools			
Name	RAID State	Capacity	details
[-] ServeRAID M5110e(PCI Slot 0)			
[-] Storage Pool 0	RAID 1	67.055GB(0.055GB free)	2 Drive(s)
Drive 0	Online	68.366GB	SAS, HDD
Drive 1	Online	68.366GB	SAS, HDD
[-] Storage Pool 1	RAID 1	67.055GB(61.000GB free)	2 Drive(s)
Drive 2	Online	68.366GB	SAS, HDD
Drive 4	Online	68.366GB	SAS, HDD
[-] Non-RAID Drives			3 Drive(s)
Drive 3	Unconfigured Good	232.886GB	SATA, HDD
Drive 5	Hot Spare	279.397GB	SAS, HDD
Drive 6	Unconfigured Good	232.886GB	SATA, HDD

Adapterinformationen anzeigen

Klicken Sie auf die Option **Adapters** (Adapter) auf der Registerkarte **Server Management** (Serververwaltung), um Informationen zu den im Server installierten PCIe-Adaptern anzuzeigen.

Anmerkungen:

- Wenn der Server die Option **Adapters** unterstützt und Sie Adapter entfernen, austauschen oder konfigurieren, müssen Sie den Server (mindestens ein mal) erneut starten, um die aktualisierten Adapterinformationen anzeigen zu können.
- Wenn der Server die Option **Adapters** nicht unterstützt, ist diese Option auf der Registerkarte **Server Management** nicht verfügbar.

Klicken Sie auf einen Adapter und einen funktionalen Link auf der Seite "Adapters", um Details zur Komponente anzuzeigen (wie in der folgenden Abbildung dargestellt).

Slot No.	Device Name	Device Type	Card Interface
OnBoard	Adapter 06:00:00	SAS	Onboard
OnBoard	IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:00		Onboard
	... IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:00	Ethernet	
	... IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:01	Ethernet	
OnBoard	Adapter 04:00:00	GPU	Onboard
2	Adapter 16:00:00		Unknown
	... Function 16:00:00	Ethernet	
	... Function 16:00:00	Ethernet	

Auf der Seite "Properties" (Eigenschaften) können Sie die Hardware- und Firmwareinformationen sowie die Portdetails für die Komponente anzeigen (wie in der folgenden Abbildung dargestellt).

Network Adapter Summary	
Product Name	IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:00
Card Interface	Onboard
Slot No.	OnBoard
Physical Port Number	1
Max Logical Port Number	4

Asset Summary	
UUID	00000000000000000000000000000000CAE8B2C1668
Manufacturer	IBM
Serial No.	I3212CT05K
Part No.	OC111102-F-X
Model	OC111102-F-X
FRU No.	N/A
FoD UID	8NFZGMG2NJYK1MEGAHHA5AEGZ9HKMHDV
Max Data Width	8
Package Type	Onboard

Für Adapter, die ältere Firmware verwenden, oder Adapter, die eine Außerbandbestandsaufnahme nicht unterstützen, kann nur ein Teil der Hardwareinformationen angezeigt werden. Informationen zur Firmware, zu Ports und zum Chipsatz können nicht abgerufen werden.

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 Versionen von IMM2-Firmwarefunktionalitäten und -Funktionen. Die Version der auf Ihrem Server installierten IMM2-Firmwarefunktionen variiert 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 der IMM2-Funktionalitätsversion "Basic Level" 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 (CLI - Command-Line Interface), 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.

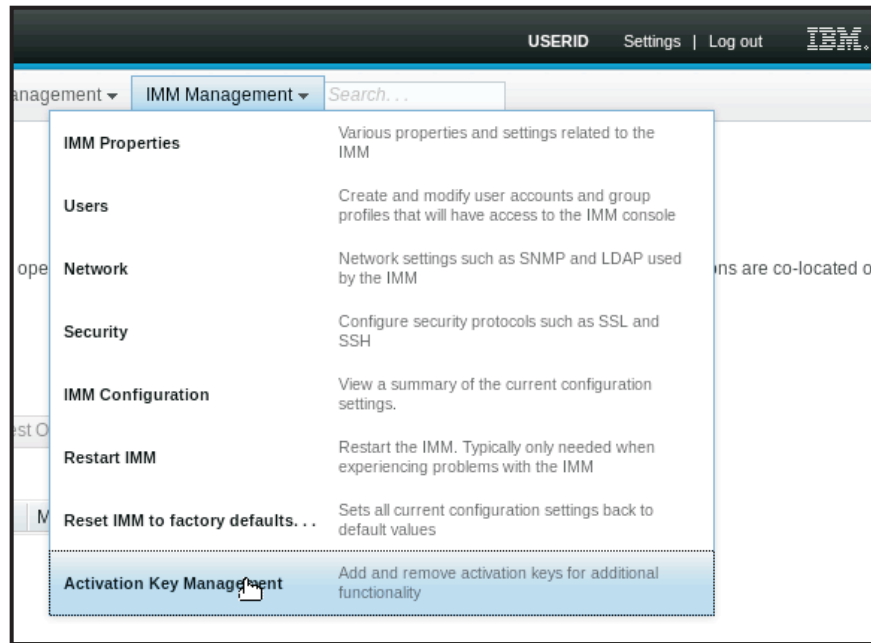
Informationen zur Verwaltung eines FoD-Aktivierungsschlüssels mithilfe der IMM2-Webschnittstelle finden Sie unter „Aktivierungsschlüssel installieren“, „Aktivierungsschlüssel entfernen“ auf Seite 182 oder „Aktivierungsschlüssel exportieren“ auf Seite 183. Informationen zur Verwaltung eines FoD-Aktivierungsschlüssels mithilfe der IMM2-Befehlszeilenschnittstelle finden Sie unter „Befehl "keycfg"“ auf Seite 225.

Aktivierungsschlüssel installieren

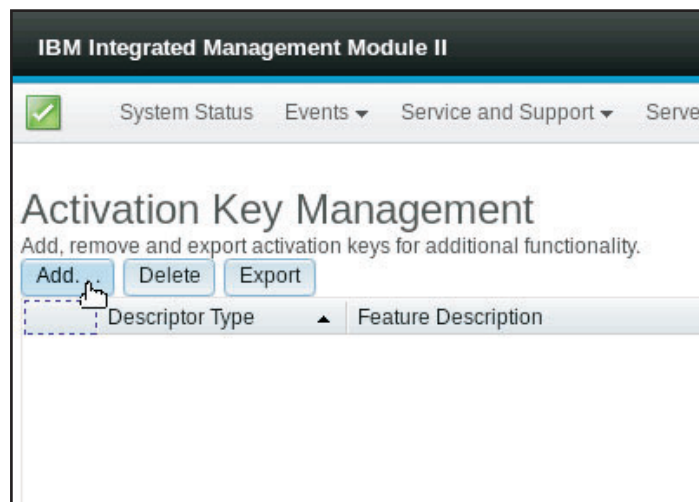
Sie können einen FoD-Aktivierungsschlüssel installieren, um eine Zusatzfunktion zu Ihrem Server hinzuzufügen.

Gehen Sie wie folgt vor, um einen FoD-Aktivierungsschlüssel zu installieren:

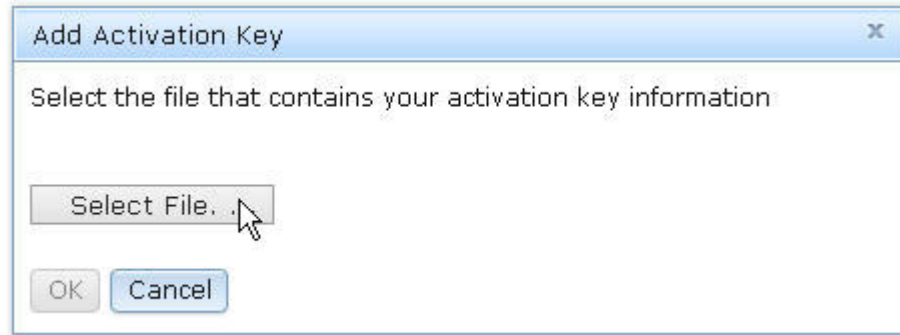
1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt „Am IMM2 anmelden“ auf Seite 12.
2. Klicken Sie in der IMM2-Webschnittstelle auf die Registerkarte **IMM Management** (IMM-Verwaltung). Klicken Sie anschließend auf **Activation Key Management** (Aktivierungsschlüsselverwaltung).



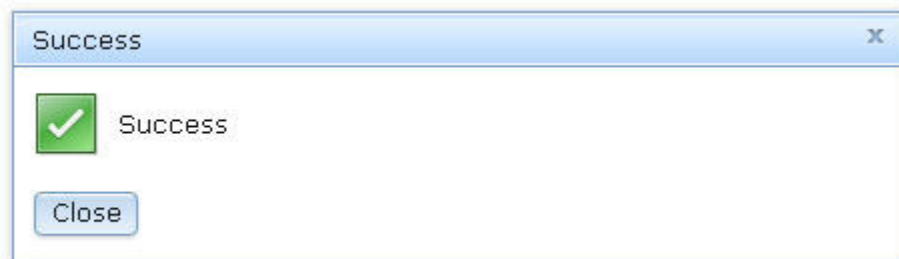
3. Klicken Sie auf der Seite "Activation Key Management" auf **Add...** (Hinzufügen).



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.

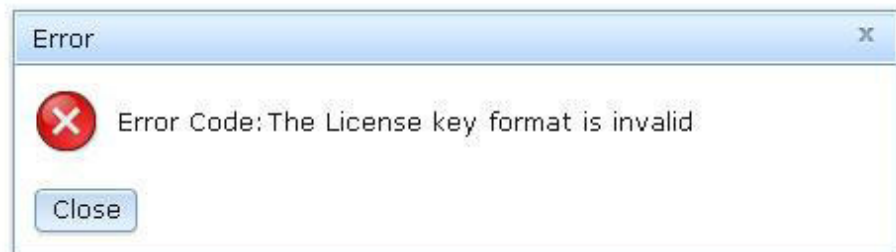


Das Fenster "Success" (Erfolg) gibt an, dass der Aktivierungsschlüssel installiert wurde.

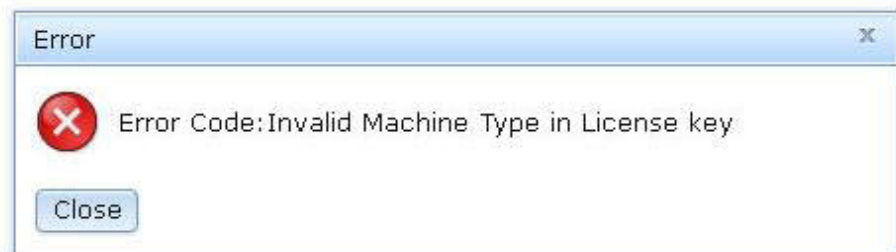


Anmerkung:

- Wenn der Aktivierungsschlüssel nicht gültig ist, wird das folgende Fehler-
nachrichtfenster angezeigt.



- Wenn Sie versuchen, den Aktivierungsschlüssel auf einem Maschinentyp zu
installieren, der die FoD-Funktion nicht unterstützt, wird das folgende Feh-
lernachrichtfenster angezeigt.



5. Klicken Sie auf **OK**, um das Fenster "Success" zu schließen.

Der ausgewählte Aktivierungsschlüssel wird zum Server hinzugefügt und er-
scheint auf der Seite "Activation Key Management".

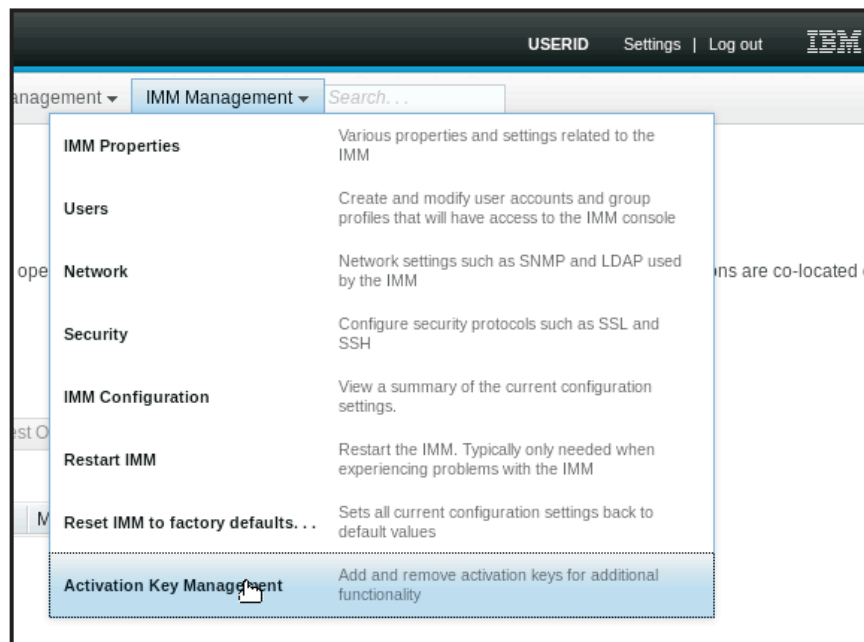
Activation Key Management			
Add, remove and export activation keys for additional functionality.			
Add... Delete Export			
Descriptor Type	Feature Description	Unique IDs	Constraints
1	IBM Integrated Management Module Advanced Upgrade	791406KNKL9	No Constraints

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:

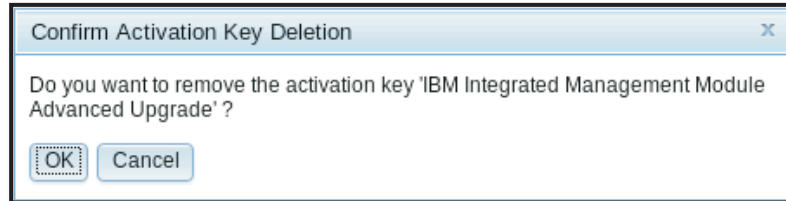
1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt „Am IMM2 anmelden“ auf Seite 12.
2. Klicken Sie in der IMM2-Webschnittstelle auf die Registerkarte **IMM Management** (IMM-Verwaltung). Klicken Sie anschließend auf **Activation Key Management** (Aktivierungsschlüsselverwaltung).



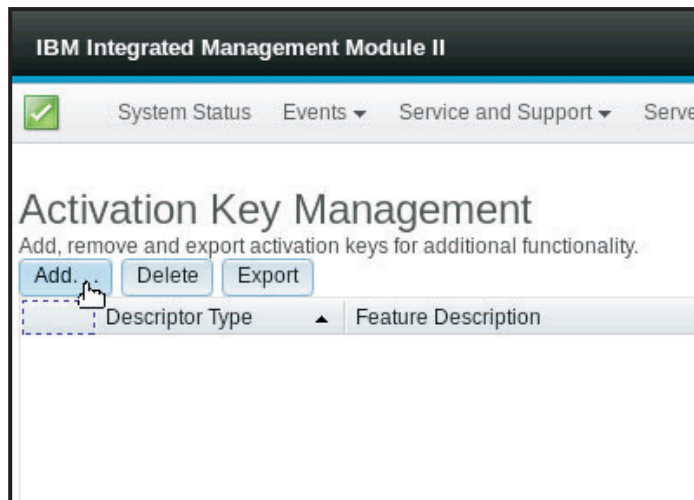
3. Wählen Sie auf der Seite "Activation Key Management" den Aktivierungsschlüssel aus, den Sie entfernen möchten. Klicken Sie anschließend auf **Delete** (Löschen).

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.

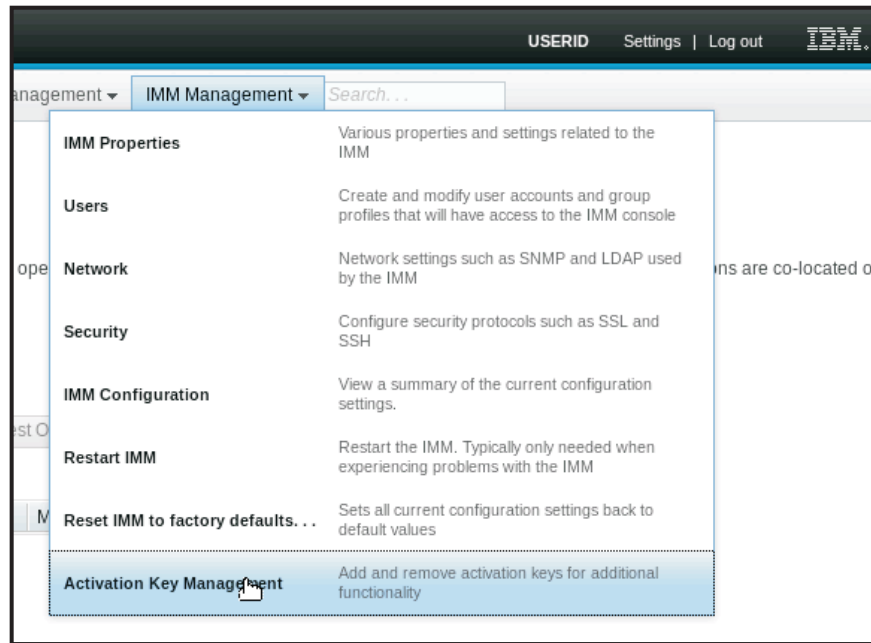


Aktivierungsschlüssel exportieren

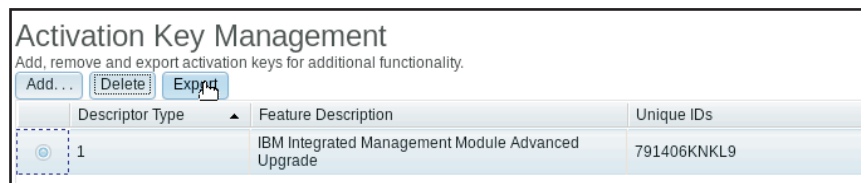
Sie können einen FoD-Aktivierungsschlüssel exportieren, um eine Zusatzfunktion vom Server zu exportieren.

Gehen Sie wie folgt vor, um einen FoD-Aktivierungsschlüssel zu exportieren:

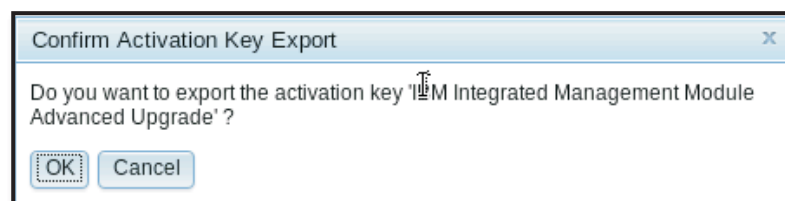
1. Melden Sie sich am IMM2 an. Weitere Informationen hierzu finden Sie im Abschnitt „Am IMM2 anmelden“ auf Seite 12.
2. Klicken Sie in der IMM2-Webschnittstelle auf die Registerkarte **IMM Management** (IMM-Verwaltung). Klicken Sie anschließend auf **Activation Key Management** (Aktivierungsschlüsselverwaltung).



3. Wählen Sie auf der Seite "Activation Key Management" den Aktivierungsschlüssel aus, den Sie exportieren möchten. Klicken Sie anschließend auf **Export** (Exportieren).



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 abubrechen.



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 "PASSWORD" (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.

In einem IBM Flex System kann ein Benutzer das IBM Flex System Chassis Management Module (CMM) zum zentralen Verwalten der Benutzerkonten auf der IMM2 Intelligent Platform Management Interface (IPMI) konfigurieren. In diesem Fall können Sie möglicherweise nicht mithilfe von IPMI auf das IMM2 zugreifen, bis das CMM die IPMI-Benutzer-IDs konfiguriert hat. Die vom CMM konfigurierten Benutzer-ID-Berechtigungsnachweise können sich von der oben beschriebenen Kombination aus Benutzer-ID und Kennwort unterscheiden.

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 IPMI-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 IPMITool 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“).

Anmeldung an der Befehlszeilsitzung

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 Befehlszeilsitzung 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 einer Telnet- oder SSH-Verbindung aus erfolgen, wenn die serielle Umleitung aktiviert ist.

Anmerkungen:

1. 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
-l 00:00:00:00:00:00
system>
```

- 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 Echtzeitausführungsstatus 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> ?
```

- In einem IBM Flex System werden manche Einstellungen vom CMM verwaltet und können auf dem IMM2 nicht geändert werden.

Alphabetische Befehlsliste

Die vollständige Liste aller Befehle der IMM2-Befehlszeilenschnittstelle in alphabetischer Reihenfolge lautet wie folgt:

- „Befehl "accsecfg" auf Seite 209
- „Befehl "adapter" auf Seite 191
- „Befehl "alertcfg" auf Seite 211
- „Befehl "alertentries" auf Seite 260
- „Befehl "asu" auf Seite 211
- „Befehl "autoftp" auf Seite 266
- „Befehl "autopromo" auf Seite 215
- „Befehl "backup" auf Seite 216
- „Befehl "batch" auf Seite 263

- „Befehl "chconfig"" auf Seite 267
- „Befehl "chlog"" auf Seite 269
- „Befehl "chmanual"" auf Seite 269
- „Befehl "clearcfg"" auf Seite 264
- „Befehl "clearlog"" auf Seite 193
- „Befehl "clock"" auf Seite 264
- „Befehl "console"" auf Seite 208
- „Befehl "cryptomode"" auf Seite 217
- „Befehl "dhcpinfo"" auf Seite 218
- „Befehl "dns"" auf Seite 219
- „Befehl "ethtousb"" auf Seite 220
- „Befehl "events"" auf Seite 270
- „Befehl "exit"" auf Seite 190
- „Befehl "fans"" auf Seite 193
- „Befehl "ffdc"" auf Seite 193
- „Befehl "fuelg"" auf Seite 203
- „Befehl "gprofile"" auf Seite 221
- „Befehl "help"" auf Seite 190
- „Befehl "history"" auf Seite 190
- „Befehl "identify"" auf Seite 265
- „Befehl "ifconfig"" auf Seite 222
- „Befehl "info"" auf Seite 265
- „Befehl "keycfg"" auf Seite 225
- „Befehl "ldap"" auf Seite 226
- „Befehl "led"" auf Seite 194
- „Befehl "ntp"" auf Seite 228
- „Befehl "passwordcfg"" auf Seite 228
- „Befehl "ports"" auf Seite 229
- „Befehl "portcfg"" auf Seite 230
- „Befehl "portcontrol"" auf Seite 231
- „Befehl "power"" auf Seite 204
- „Befehl "pxeboot"" auf Seite 207
- „Befehl "readlog"" auf Seite 196
- „Befehl "reset"" auf Seite 207
- „Befehl "resetp"" auf Seite 266
- „Befehl "restore"" auf Seite 232
- „Befehl "restoredefaults"" auf Seite 232
- „Befehl "scale"" auf Seite 233
- „Befehl "sdemail"" auf Seite 270
- „Befehl "set"" auf Seite 243
- „Befehl "smtp"" auf Seite 243
- „Befehl "snmp"" auf Seite 244
- „Befehl "snmpalerts"" auf Seite 247
- „Befehl "spreset"" auf Seite 266
- „Befehl "srcfg"" auf Seite 248

- „Befehl "sshcfg"" auf Seite 249
- „Befehl "ssl"" auf Seite 250
- „Befehl "sslcfg"" auf Seite 251
- „Befehl "storage"" auf Seite 197
- „Befehl "syshealth"" auf Seite 201
- „Befehl "telnetcfg"" auf Seite 254
- „Befehl "temps"" auf Seite 201
- „Befehl "thermal"" auf Seite 255
- „Befehl "timeouts"" auf Seite 255
- „Befehl "tls"" auf Seite 254
- „Befehl "usbeth"" auf Seite 256
- „Befehl "users"" auf Seite 256
- „Befehl "volts"" auf Seite 202
- „Befehl "vpd"" auf Seite 202

Dienstprogrammbefehle

Folgende Dienstprogrammbefehle sind verfügbar:

- „Befehl "exit""
- „Befehl "help""
- „Befehl "history""

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 Direktauf-rufe (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
-l 00:00:00:00:00:00
system>
```

Überwachungsbefehle

Folgende Überwachungsbefehle sind verfügbar:

- „Befehl "clearlog"" auf Seite 193
- „Befehl "fans"" auf Seite 193
- „Befehl "ffdc"" auf Seite 193
- „Befehl "led"" auf Seite 194
- „Befehl "readlog"" auf Seite 196
- „Befehl "storage"" auf Seite 197
- „Befehl "syshealth"" auf Seite 201
- „Befehl "temps"" auf Seite 201
- „Befehl "volts"" auf Seite 202
- „Befehl "vpd"" auf Seite 202

Befehl "adapter"

Mit dem Befehl **adapter** können Sie PCIe-Adapterinventarinformationen anzeigen. Zu den PCIe-Adaptern, die vom IMM2 verwaltet werden, gehören: Ethernet, Fibre Channel, InfiniBand und GPUs (Graphic Processing Units).

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-list	Alle PCIe-Adapter im Server auflisten	
-show <i>Ziel-ID</i>	Detaillierte Informationen zum PCIe-Zieladapter anzeigen	<i>Ziel-ID</i> [<i>info</i> <i>firmware</i> <i>ports</i> <i>chips</i>] Dabei gilt: • <i>info</i>: Hardwareinformationen zum Adapter anzeigen • <i>firmware</i>: Alle Firmwareinformationen zum Adapter anzeigen • <i>ports</i>: Alle Informationen zu den Ethernet-Anschlüssen des Adapters anzeigen • <i>chips</i>: Alle Informationen zum GPU-Chip des Adapters anzeigen
-h	Befehlssyntax und Optionen anzeigen	

Syntax:

```
adapter [Optionen]
```

Option:

```
-list
-show Ziel-ID [info | firmware | ports | chips]
-h Hilfe
```

Beispiele:

```
system> adapter
-list
ob-1      IBM Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2      GPU Card 1
slot-1    Raid Controller 1
slot-2    Adapter 01:02:03

system> adapter
-show ob-1 info
Product Name: IBM Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
```

Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici

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 ¹	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 ¹	Portnummer des TFTP/SFTP-Servers.	Der Standardwert ist 69/22.
-u ¹	Benutzername für den SFTP-Server.	
-pw ¹	Kennwort für den SFTP-Server.	
1. Zusätzliches Argument für die Befehle generate und copy		

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
-l	Den Status aller Anzeigen auf dem System und dessen Unterkomponenten abrufen	
-chklog	Anzeige für Prüfprotokoll ausschalten	off
-identify	Zustand der Gehäusebestimmungsanzeige ändern	off, on, blink
-d	Identifikationsanzeige für einen angegebenen Zeitraum einschalten	Zeitraum (Sekunden)

Syntax:

led [*Optionen*]

Option:

-l -chklog off
-identify *Zustand*
-d *Zeit*

Beispiel:

system> led

Fault	Off	
Identify	On	Blue
Chklog	Off	
Power	Off	

system> led -l

Label	Location	State	Color
Battery	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	Off	
Chklog	Front Panel	Off	
CNFG	Lightpath Card	Off	
CPU	Lightpath Card	Off	
CPU 1	Planar	Off	
CPU 2	Planar	Off	
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	Off	
DIMM 16	Planar	Off	
DIMM 2	Planar	Off	
DIMM 3	Planar	Off	
DIMM 4	Planar	Off	
DIMM 5	Planar	Off	
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	Off	
FAN 3	Planar	Off	
Fault	Front Panel (+)	Off	
Identify	Front Panel (+)	On	Blue
LINK	Lightpath Card	Off	
LOG	Lightpath Card	Off	
NMI	Lightpath Card	Off	
OVER SPEC	Lightpath Card	Off	
PCI 1	FRU	Off	
PCI 2	FRU	Off	
PCI 3	FRU	Off	
PCI 4	FRU	Off	
Planar	Planar	Off	
Power	Front Panel (+)	Off	
PS	Lightpath Card	Off	

RAID	Lightpath Card	Off
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 (|) 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 (|) 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 -l *filename* legt den Dateinamen der Ereignisprotokolldatei fest. Die Befehlsoptionen **-i** und **-l** 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 Environmental monitor not responding.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
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 "storage"

Mit dem Befehl **storage** können Sie Informationen zu den Speichereinheiten des Servers anzeigen, die durch das IMM2 überwacht werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-list	Durch das IMM2 verwaltete Speicherziele auflisten	<i>controllers pools volumes drives</i> Dabei steht <i>Ziel</i> für: • <i>controllers</i>: Unterstützte RAID-Controller auflisten ¹ • <i>pools</i>: Dem RAID-Controller zugehörige Speicherpools auflisten ¹ • <i>volumes</i>: Dem RAID-Controller zugehörige Speicherdatenträger auflisten ¹ • <i>drives</i>: Dem RAID-Controller zugehörige Speicherlaufwerke auflisten ¹
-list -Ziel Ziel-ID	Die Speicherziele, die vom IMM2 verwaltet werden, entsprechend ihrer Ziel-ID auflisten	<i>pools volumes drives ctrl[x] pool[x]</i> Dabei stehen <i>Ziel</i> und <i>Ziel-ID</i> für: • <i>pools ctrl[x]</i>: Dem RAID-Controller zugehörige Speicherpools auflisten, gemäß ihrer Ziel-ID ¹ • <i>volumes ctrl[x] pool[x]</i>: Dem RAID-Controller zugehörige Speicherdatenträger auflisten, gemäß ihrer Ziel-ID ¹ • <i>drives ctrl[x] pool[x]</i>: Dem RAID-Controller zugehörige Speicherlaufwerke auflisten, gemäß ihrer Ziel-ID ¹
-list flashdimms	Durch IMM2 verwaltete Flash-DIMMs auflisten	
-list devices	Status aller Platten und Flash-DIMMS anzeigen, die durch das IMM2 verwaltet werden	

Option	Beschreibung	Werte
-show <i>Ziel-ID</i>	Informationen zum ausgewählten Ziel anzeigen, das vom IMM2 verwaltet wird	Dabei steht <i>Ziel-ID</i> für: <i>ctrl[x] vol[x] disk[x] pool[x]</i> <i> flashdimm[x]</i> ³
-show <i>Ziel-ID info</i>	Detaillierte Informationen zum ausgewählten Ziel anzeigen, das vom IMM2 verwaltet wird	Dabei steht <i>Ziel-ID</i> für: <i>ctrl[x] vol[x] disk[x] pool[x]</i> <i> flashdimm[x]</i> ³
-show <i>Ziel-ID firmware</i>	Firmwareinformationen zum ausgewählten Ziel anzeigen, das vom IMM2 verwaltet wird	Dabei steht <i>Ziel-ID</i> für: <i>ctrl[x] disk[x] flashdimm[x]</i> ²
-help	Befehlssyntax und Optionen anzeigen	
Anmerkungen: 1. Dieser Befehl wird nur auf Systemen unterstützt, auf denen das IMM2 auf den RAID-Controller zugreifen kann. 2. Es werden nur Firmwareinformationen für die zugehörigen Controller, Platten und Flash-DIMMs angezeigt. Firmwareinformationen für zugehörige Pools und Datenträger werden nicht angezeigt. 3. Werte werden in mehreren Zeilen, je nach Platzeinschränkungen, angezeigt.		

Syntax:

storage [*Optionen*]

Option:

```
-list controllers | pools | volumes | drives
-list pools -target ctrl[x]
-list volumes -target ctrl[x] | pool[x]
-list drives -target ctrl[x] | pool[x]
-list devices
-list flashdimms
-show Ziel-ID
-show {ctrl[x] | pool[x] | disk[x] | vol[x] | flashdimm[x]} info
-show {ctrl[x] | disk[x] | flashdimm[x]} firmware
-h Hilfe
```

Beispiele:

```
system> storage
-list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
```

```
system> storage
-list pools
pool[0-0]   Storage Pool 0
pool[0-1]   Storage Pool 1
system>
```

```
system> storage
-list drives
disk[0-0]   Drive 0
disk[0-1]   Drive 1
disk[0-2]   Drive 2
system>
```

```
system> storage
-list volumes
system>storage -list volumes
```

```

vol[0-0]      Volume 0
vol[0-1]      Volume 1
Vol[0-2]      Volume 2
system>

system> storage
-list drives -target ctrl[0]
disk[0-0]      Drive 0
disk[0-1]      Drive 1
disk[0-2]      Drive 2
system>

system> storage
-list drives -target pool[0-0]
disk[0-0]      Drive 0
disk[0-1]      Drive 1
system>

system> storage
-list pools -target ctrl[0]
pool[0-0]      Storage Pool 0
system>

system> storage
-list volumes -target ctrl[0]
vol[0-0]      Volume 0
vol[0-1]      Volume 1
system>

system> storage
-list volumes -target pool[0-0]
vol[0-0]      Volume 0
vol[0-1]      Volume 1
system>

system> storage
-list flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>

system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0]      Storage Pool 0
pool[0-1]      Storage Pool 1
Drives: 3

```

```

disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>

system> storage
-show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manufacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>

system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HDD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclosure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>

system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>

system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]     Volume 0
vol[0-1]     Volume 1
system>

system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>

system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15

```

```

Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>

```

Befehl "syshealth"

Mit dem Befehl **syshealth** können Sie eine Zusammenfassung des Serverzustands oder der aktiven Ereignisse auf dem Server anzeigen. Es werden der Stromversorgungsstatus, der Systemstatus, der Zähler für den Neustart und der Status der IMM2-Software angezeigt.

Syntax:

```
syshealth [Argument]
```

Argument:

```

summary      -Zusammenfassung des Systemzustands anzeigen
activeevents  -aktive Ereignisse anzeigen

```

Beispiel:

```

system> syshealth summary
Power On
State    OS booted
Restarts 29

```

```

system> syshealth activeevents
No Active Event Available!

```

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:

- Die Ausgabe weist die folgenden Spaltenüberschriften auf:
WR: Warnungszurücksetzung
W: Warnung
T: Temperatur (aktueller Wert)
SS: Normaler Systemabschluss
HS: Erzwungener Systemabschluss
- 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> volts
      HSL  SSL  WL   WRL  V    WRH  WH   SSH   HSH
-----
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75  6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70  3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40 12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40 -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80 -2.70
VRM1                                     3.45
VRM2                                     5.45
system>
```

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)

HSR: 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 [Argument]
```

Argument:

sys

imm

uefi

dsa

fw

comp

Beispiel:

```
system> vpd dsa
Type      Version      Build      ReleaseDate
-----
DSA       9.25             DSYTA5A    2012/07/31
system>
```

Steuerbefehle für Serverstromversorgung und -neustart

Folgende Befehle für Serverstromversorgung und -neustart sind verfügbar:

- „Befehl "fuelg"“
- „Befehl "power"“ auf Seite 204
- „Befehl "pxeboot"“ auf Seite 207
- „Befehl "reset"“ auf Seite 207

Befehl "fuelg"

Mit dem Befehl **fuelg** können Sie die Stromverbrauchssteuerung des Servers anzeigen und konfigurieren.

Mit dem Befehl **fuelg** können Sie Informationen zum Stromverbrauch des Servers anzeigen und die Stromverbrauchssteuerung des Servers konfigurieren. Mit diesem Befehl werden auch Richtlinien für den Verlust von Stromversorgungsredundanz konfiguriert. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-pme	Stromverbrauchssteuerung und Netzstrombegrenzung für den Server aktivieren oder inaktivieren	on, off
-pcapmode	Netzstrombegrenzungsmodus für den Server festlegen	ac, dc
-pcap	Ein numerischer Wert innerhalb des Bereichs der Netzstrombegrenzungswerte, die bei Ausführung des fuelg-Befehls ohne Optionen für das Ziel angezeigt werden.	numerischer Leistungswert (Watt)
Wenn die redundante Stromversorgung nicht unterstützt wird, wird die folgende Option unterstützt:		
-pm	Richtlinienmodus für den Verlust der redundanten Stromversorgung festlegen	einfacher Modus mit Regulierung (bt, Standard), redundanter Modus ohne Regulierung (r), redundanter Modus mit Regulierung (rt)
Wenn die redundante Stromversorgung unterstützt wird, werden die folgenden Optionen unterstützt:		
-mpc	Maximalen Stromverbrauch für den Server festlegen	aktuelle Konfiguration (cc - current configuration), alle im laufenden Betrieb anzuschließenden Komponenten (ahp - all hot-plug components)
-at	Regulierung zulassen, damit der Server den Maximalwert für den Stromverbrauch nicht überschreitet	on, off
-r	Stromversorgungsredundanz für den Server zulassen	on, off
-nn	Wert der N+N-Redundanzkonfiguration	Redundanzkonfigurationswert

Syntax:

fuelg [Optionen]

Option:

- pme on|off
- pcapmode dc|ac
- pcap
- pm bt|r|rt
- mpc cc|ahp
- at on|off
- r on|off
- nn

Beispiel:

```
system> fuelg
-pme: on
system>
```

Befehl "power"

Mit dem Befehl **power** können Sie die Stromversorgung des Servers steuern. Um Befehle vom Typ **power** ausgeben zu können, benötigen Sie die Berechtigungsstufe zum Starten und zum erneuten Starten des fernen Servers.

Die folgende Tabelle enthält eine Untermenge von Befehlen, die zusammen mit dem Befehl **power** verwendet werden können.

Tabelle 9. Befehle vom Typ "power"

Befehl	Beschreibung	Wert
power on	Verwenden Sie diesen Befehl, um die Serverstromversorgung anzuschalten.	on, off
power off	Verwenden Sie diesen Befehl, um die Serverstromversorgung auszuschalten. Anmerkung: Mit der Option -s wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.	on, off
power cycle	Verwenden Sie diesen Befehl, um die Serverstromversorgung aus- und dann wieder anzuschalten. Anmerkung: Mit der Option -s wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.	
power enterS3	Verwenden Sie diesen Befehl, um das Betriebssystem in den S3-Modus (Ruhemodus) zu versetzen. Anmerkung: Dieser Befehl wird nur verwendet, wenn das Betriebssystem eingeschaltet ist. Der S3-Modus wird nicht auf allen Servern unterstützt.	

Tabelle 9. Befehle vom Typ "power" (Forts.)

Befehl	Beschreibung	Wert
power rp	Verwenden Sie diese Option, um die Richtlinie für die Wiederherstellung der Stromversorgung des Hosts anzugeben.	alwayson alwaysoff restore
power S3resume	Verwenden Sie diesen Befehl, um das Betriebssystem aus dem S3-Modus (Ruhemodus) zu aktivieren. Anmerkung: Dieser Befehl wird nur verwendet, wenn das Betriebssystem eingeschaltet ist. Der S3-Modus wird nicht auf allen Servern unterstützt.	
power state	Verwenden Sie diesen Befehl, um den Serverstromversorgungszustand und den aktuellen Zustand des Servers anzuzeigen.	on, off

Die folgende Tabelle enthält die Optionen für die Befehle **power on**, **power off** und **power cycle**.

Option	Beschreibung	Werte
-s	Verwenden Sie diese Option, um das Betriebssystem herunterzufahren, bevor der Server ausgeschaltet wird. Anmerkung: Die Option -s ist bei der Verwendung der Option -every für die Befehle power off und power cycle inbegriffen.	
-every	Verwenden Sie diese Option zusammen mit den Befehlen power on , power off und power cycle , um die Serverstromversorgung zu steuern. Sie können die Daten und Zeiten sowie die Häufigkeit (täglich oder wöchentlich) für das Einschalten, das Ausschalten und das Aus- und wieder Einschalten Ihres Servers konfigurieren.	Anmerkung: Die Werte für diese Option werden aufgrund von Zeilenbeschränkungen in separaten Zeilen angezeigt. Sun Mon Tue Wed Thu Fri Sat Day clear

Option	Beschreibung	Werte
-t	Verwenden Sie diese Option, um in Stunden und Minuten die Zeit für das Einschalten des Servers, das Herunterfahren des Betriebssystems und das Ausschalten oder Neustarten des Servers anzugeben.	Verwenden Sie das folgende Format: hh:mm
-d	Verwenden Sie diese Option, um das Datum für das Einschalten des Servers anzugeben. Dies ist eine zusätzliche Option für den Befehl power on . Anmerkung: Die Optionen -d und -every können nicht zusammen im gleichen Befehl verwendet werden.	Verwenden Sie das folgende Format: mm/tt/jjjj
-clear	Verwenden Sie diese Option, um den geplanten Wert für das Datum zum Einschalten zu löschen. Dies ist eine zusätzliche Option für den Befehl power on .	

Syntax:

```
power on
power off [-s]
power state
power cycle [-s]
```

Bei den folgenden Informationen handelt es sich um Beispiele zum Befehl **power**.

Um jeden Sonntag um 01:30 Uhr das Betriebssystem herunterzufahren und den Server auszuschalten, geben Sie den folgenden Befehl ein:

```
system> power off
-every Sun -t 01:30
```

Um jeden Tag um 01:30 Uhr das Betriebssystem herunterzufahren und den Server erneut zu starten, geben Sie den folgenden Befehl ein:

```
system> power cycle
-every Day -t 01:30
```

Um den Server jeden Montag um 01:30 Uhr einzuschalten, geben Sie den folgenden Befehl ein:

```
system> power on
-every Mon -t 13:00
```

Um den Server am 21. Dezember 2013 um 23:30 Uhr einzuschalten, geben Sie den folgenden Befehl ein:

```
system> power on
-d 12/31/2013 -t 23:30
```

Um ein wöchentliches Aus- und wieder Einschalten aufzuheben, geben Sie den folgenden Befehl ein:

```
system> power cycle
-every clear
```

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-Bedingung 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 Berechtigung zum Starten und erneuten Starten verfügen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-s	Betriebssystem herunterfahren, bevor der Server zurückgesetzt wird.	
-d	Zurücksetzen um die angegebene Anzahl an Sekunden verzögern.	0 - 120
-nmi	Einen nicht maskierbaren Interrupt (NMI) auf dem Server generieren.	

Syntax:

```
reset [Option]
Option:
-s
-d
-nmi
```

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 209
- „Befehl "alertcfg"“ auf Seite 211
- „Befehl "asu"“ auf Seite 211
- „Befehl "autopromo"“ auf Seite 215
- „Befehl "backup"“ auf Seite 216
- „Befehl "cryptomode"“ auf Seite 217
- „Befehl "dhcpinfo"“ auf Seite 218
- „Befehl "dns"“ auf Seite 219
- „Befehl "ethtousb"“ auf Seite 220
- „Befehl "gprofile"“ auf Seite 221
- „Befehl "ifconfig"“ auf Seite 222
- „Befehl "keycfg"“ auf Seite 225
- „Befehl "ldap"“ auf Seite 226
- „Befehl "ntp"“ auf Seite 228
- „Befehl "passwordcfg"“ auf Seite 228
- „Befehl "ports"“ auf Seite 229
- „Befehl "portcfg"“ auf Seite 230
- „Befehl "portcontrol"“ auf Seite 231
- „Befehl "restore"“ auf Seite 232
- „Befehl "restoredefaults"“ auf Seite 232
- „Befehl "set"“ auf Seite 243
- „Befehl "smtp"“ auf Seite 243
- „Befehl "snmp"“ auf Seite 244
- „Befehl "snmpalerts"“ auf Seite 247
- „Befehl "srcfg"“ auf Seite 248
- „Befehl "sshcfig"“ auf Seite 249
- „Befehl "ssl"“ auf Seite 250
- „Befehl "sslcfg"“ auf Seite 251
- „Befehl "telnetcfg"“ auf Seite 254

- „Befehl "thermal" auf Seite 255
- „Befehl "timeouts" auf Seite 255
- „Befehl "tls" auf Seite 254
- „Befehl "usbeth" auf Seite 256
- „Befehl "users" auf Seite 256

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 (legacy) Standardwerten fest	
-high	Legt für die Accountsicherheit eine vordefinierte Gruppe von hohen (high) Standardwerten fest	
-custom	Stellt Kontosicherheit auf benutzerdefinierte Werte ein	
-am	Legt Benutzerauthentifizierungsverfahren (authentication method) fest	local, ldap, localldap, ldaplocal
-lp	Aussperrungszeit (lockout period) 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 Verfallsdatum des Kennworts (password expiration) (Tage)	0 bis 365 Tage
-pr	Kennwort erforderlich (password required)	on, off
-pc	Regeln zur Kennwortkomplexität (password complexity)	on, off
-pd	Mindestanzahl unterschiedlicher Zeichen für ein Kennwort (password minimum number of different characters)	0 bis 19 Zeichen

Option	Beschreibung	Werte
-pl	Kennwortlänge (password length)	1 bis 20 Zeichen
-ci	Mindestintervall für Kennwortänderung (Stunden) (change interval)	0 bis 240 Stunden
-lf	Maximale Anzahl an Anmeldefehlern (login failures)	0 bis 10
-chgdft	Standardkennwort nach erster Anmeldung ändern (change default password after first login)	on, off
-chgnew	Neues Benutzerkennwort nach erster Anmeldung ändern (change new user password after first login)	on, off
-rc	Wiederverwendungszyklus für Kennwort (reuse cycle)	0 bis 5
-wt	Sitzungszeitlimit bei Webinaktivität (Minuten) (web inactivity session timeout (minutes))	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
-lp 2
-pe 0
-pr off
-pd 1
```

```

-pl 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 Wiederholungsversuchen liegen 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 Empfänger 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 versucht, einen Alert zu senden, wenn vorherige Versuche nicht erfolgreich 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.

Tabelle 10. ASU-Befehle

Befehl	Beschreibung	Wert
delete	Verwenden Sie diesen Befehl, um eine Instanz oder einen Datensatz einer Einstellung zu löschen. Bei der Einstellung muss es sich um eine Instanz handeln, für die das Löschen zulässig ist, z. B. "iSCSI.AttemptName.1".	<i>Einstellung_Instanz</i>
help	Verwenden Sie diesen Befehl, um Hilfetext zu einer oder mehreren Einstellungen anzuzeigen.	<i>Einstellung</i>
set	Verwenden Sie diesen Befehl, um den Wert einer Einstellung zu ändern. Legen Sie als UEFI-Einstellung den Eingabewert fest. Anmerkungen: • Legen Sie ein oder mehrere Paare aus Einstellung und Wert fest. • Die Einstellung kann Platzhalterzeichen enthalten, wenn sie für eine einzelne Einstellung gilt. • Der Wert muss in Anführungszeichen gesetzt werden, wenn er Leerzeichen enthält. • Sortierlistenwerte werden durch das Gleichheitszeichen (=) getrennt. Beispiel: set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network."	<i>Einstellung Wert</i>
showgroups	Verwenden Sie diesen Befehl, um die verfügbaren Einstellungsgruppen anzuzeigen. Dieser Befehl zeigt die Namen der bekannten Gruppen an. Gruppennamen können je nach den installierten Einheiten variieren.	<i>Einstellung</i>
show	Verwenden Sie diesen Befehl, um den aktuellen Wert einer oder mehrerer Einstellungen anzuzeigen.	<i>Einstellung</i>

Tabelle 10. ASU-Befehle (Forts.)

Befehl	Beschreibung	Wert
showvalues	Verwenden Sie diesen Befehl, um alle möglichen Werte für eine oder mehrere Einstellungen anzuzeigen. Anmerkungen: • Dieser Befehl zeigt Informationen zu den zulässigen Werten für die Einstellung an. • Die minimale und maximale Anzahl der für diese Einstellung zulässigen Instanzen werden angezeigt. • Der Standardwert wird angezeigt, falls er verfügbar ist. • Der Standardwert steht zwischen einer öffnenden und einer schließenden spitzen Klammer (< und >). • Die Textwerte zeigen die minimale und die maximale Länge sowie den regulären Ausdruck.	<i>Einstellung</i>
Anmerkungen: • In der Befehlssyntax ist <i>Einstellung</i> der Name einer Einstellung, die Sie anzeigen oder ändern möchten, und <i>Wert</i> ist der Wert, den Sie für die Einstellung festlegen. • Für <i>Einstellung</i> können mehrere Werte angegeben werden, außer bei Verwendung des Befehls set. • Der Wert für <i>Einstellung</i> kann Platzhalterzeichen enthalten, z. B. einen Stern (*) oder ein Fragezeichen (?). • Bei <i>Einstellung</i> kann es sich um eine Gruppe, einen Einstellungsnamen oder den Wert all (alles) handeln.		

In der folgenden Liste werden Beispiele für die Syntax des Befehls **asu** aufgeführt:

- 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 -l -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 ¹	Im Batchformat anzeigen.	
--help ³	Befehlssyntax und -optionen anzeigen. Die Option "--help" wird vor den Befehl gesetzt, wie z. B. asu --help show .	
--help ³	Hilfe zum Befehl anzeigen. Die Option "--help" wird hinter den Befehl gesetzt, z. B. asu show --help .	
-l ¹	Name der Einstellung im Langformat (Konfigurationsgruppe einschließen).	
-m ¹	Name der Einstellung im Mischformat (Konfigurations-ID verwenden).	
-v ²	Ausführliche Ausgabe.	
1. Die Option "-v" wird nur zwischen asu und dem Befehl verwendet. 2. 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.

Tabelle 11. Transaktionsbefehle

Befehl	Beschreibung	Wert
tropen <i>ID</i>	Dieser Befehl erstellt eine neue Transaktionsdatei mit mehreren festzulegenden Einstellungen.	<i>ID</i> ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trset <i>ID</i>	Dieser Befehl fügt eine oder mehrere Einstellungen oder Wertepaare zu einer Transaktion hinzu.	<i>ID</i> ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trlist <i>ID</i>	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 alphanumerischen Zeichen.
trcommit <i>ID</i>	Dieser Befehl schreibt die Inhalte der Transaktionsdatei fest und führt sie aus. Die Ergebnisse der Ausführung sowie eventuelle Fehler werden angezeigt.	<i>ID</i> ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trrm <i>ID</i>	Dieser Befehl entfernt die Transaktionsdatei, nachdem sie festgeschrieben wurde.	<i>ID</i> ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.

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 "autopromo"

Mithilfe des Befehls **autopromo** können Sie die Einstellung für die automatisierte Hochstufung der IMM2-Sicherungsfirmware anzeigen und konfigurieren. Wenn sie aktiviert ist, kopiert die Funktion "Automated Promotion" (Automatisierte Hochstufung) automatisch die IMM2-Firmware aus dem Primärbereich in den Sicherungsbereich, wenn die Firmware im Primärbereich eine bestimmte Zeit erfolgreich ausgeführt wurde.

Wird der Befehl **autopromo** ohne Optionen ausgeführt, so werden Informationen zu Parametern bei der automatisierten Hochstufung und zum Status angezeigt. In der folgenden Tabelle sind die Argumente für die Option aufgelistet.

Option	Beschreibung	Werte
-en	Automatisierte Hochstufung der Sicherungsfirmware für das IMM2 aktivieren oder inaktivieren.	enabled, disabled

Syntax:

autopromo [*Optionen*]

Optionen:

-en *enabled/disabled*

Beispiel:

```
system>autopromo -en enabled
```

```
ok
```

```
system>autopromo
```

```
-en: enabled
```

```
Status: Not Synced
```

```
Primary bank version: 4.00
```

```
Backup bank version: 2.60
```

Befehl "backup"

Mit dem Befehl **backup** können Sie eine Sicherungsdatei mit den aktuellen System-sicherheitseinstellungen erstellen.

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 Kennwörter innerhalb der Sicherungsdatei verschlüsselt sind	Gültiges Kennwort oder durch Anführungszeichen begrenzter 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

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 "cryptomode"

Verwenden Sie den Befehl **cryptomode**, um den Konformitätsmodus mit den Ausnahmen für die Verschlüsselung anzuzeigen und zu konfigurieren. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-set	Konformitätsmodus auswählen	basic, NIST ¹
-esnmpv3	Zulassen oder nicht zulassen, dass SNMPv3-Konten auf eine mit dem NIST-Konformitätsmodus nicht konforme Weise operieren	enable, disable
-h	Verwendung und Optionen auflisten	

1. Wenn für den Konformitätsmodus "NIST" festgelegt wird, muss für die TLS-Stufe "1.2" ausgewählt werden.

Syntax:

```
cryptomode [Optionen]
Optionen:
-set basic|nist
-esnmpv3 enabled|disabled
-h Verwendungsoptionen
```

Beispiele:

Um für "cryptomode" die Option "basic" festzulegen, geben Sie den folgenden Befehl ein:

```
system> cryptomode
-set basic
ok
system> cryptomode
Mode Exceptions
Basic Compatibility
system>
```

Um für "cryptomode" die Option "NIST Strict" festzulegen, geben Sie den folgenden Befehl ein:

```
system> cryptomode
-set NIST
ok
system> cryptomode
Mode Exceptions
NIST SP 800-131A
system>
```

Um für "cryptomode" die Option "NIST Strict" festzulegen und SNMP im Konformitätsmodus zuzulassen, geben Sie den folgenden Befehl ein:

```

system> cryptomode
-set NIST -esnmpv3 enabled
ok
system> cryptomode
Mode           Exceptions
NIST SP 800-131A  allow SNMPv3 accounts
system>

```

Bei Zertifikaten oder Verschlüsselungsgraden, die nicht mit dem NIST-Modus kompatibel sind, schlägt der Befehl fehl und eine Fehlermeldung wird generiert. Der Konformitätsmodus wird nicht geändert (siehe folgendes Beispiel):

```

system> cryptomode
-set NIST
LDAP Server 1 certificate invalid
fail
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
-g      : 192.168.70.29
-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

Option	Beschreibung
-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.

Anmerkung: In einem IBM Flex System können DNS-Einstellungen auf dem IMM2 nicht geändert werden. DNS-Einstellungen werden vom CMM verwaltet.

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.
-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

Syntax:

dns [*Optionen*]

Option:

```
-state Zustand
-ddns 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
-i1    : 192.168.70.202
-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
-dnsrsrc : dhcp
-p     : ipv6
```

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)
-dnsrsrc	Bevorzugter DDNS-Domänenname (dhcp oder manual)
-ddn	Manuell angegebenes DDN
-ddncur	Aktuelles DDN (Lesezugriff)
-p	Bevorzugte DNS-Server (ipv4 oder ipv6)

Befehl "ethtousb"

Mit dem Befehl **ethtousb** können Sie die Portzuordnung für Ethernet zu Ethernet-über-USB anzeigen und konfigurieren.

Mit diesem Befehl können Sie für Ethernet-über-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

Option	Beschreibung	Werte
-mx	Portzuordnung für Index <i>x</i> konfigurieren	Durch einen Doppelpunkt (:) getrenntes Portpaar in der Form <i>port1:port2</i> Dabei gilt: • Die Portindexnummer <i>x</i> wird in der Befehlsoption als Ganzzahl zwischen 1 und 10 angegeben. • Bei <i>port1</i> des Portpaares handelt es sich um die externe Ethernet-Portnummer. • Bei <i>port2</i> des Portpaares handelt es sich um die Ethernet-über-USB-Portnummer.
-rm	Portzuordnung für angegebenen Index entfernen	1 bis 10 Über den Befehl ethtousb 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.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-clear	Eine Gruppe löschen	enabled, disabled
-n	Der Name der Gruppe	Zeichenfolge mit bis zu 63 Zeichen für <i>Gruppenname</i> . Der <i>Gruppenname</i> muss eindeutig sein.
-a	Rollenbasierte Berechtigungsstufe	supervisor, operator, rbs <Rollenliste>: nsc am rca rcvma pr bc cel ac Die Rollenlistenwerte werden in einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, angegeben.
-h	Befehlssyntax und Optionen anzeigen	

Syntax:

```
gprofile [1 - 16  
Bereichsnummer_des_Gruppenprofils] [options]  
Optionen:  
-clear Zustand  
-n Gruppenname  
-a Berechtigungsstufe:  
    -nsc Netzbetrieb und Sicherheit  
    -am Benutzerkontenverwaltung  
    -rca Zugriff auf ferne Konsole  
    -rcvma Zugriff auf ferne Konsole und fernen Datenträger  
    -pr Berechtigung für Einschalten/Neustart eines fernen Servers  
    -bc Allgemeine Adapterkonfiguration  
    -cel Fähigkeit zum Löschen von Ereignisprotokollen  
    -ac Erweiterte Adapterkonfiguration  
-h Hilfe
```

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.

Anmerkung: In einem IBM Flex System werden die VLAN-Einstellungen vom IBM Flex System Chassis Management Module (CMM) verwaltet und können auf dem IMM2 nicht geändert werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-b	Herstellerkennung der MAC-Adresse (schreibgeschützt und nicht konfigurierbar)	
-state	Schnittstellenstatus	disabled, enabled
-c	Konfigurationsmethode	dhcp, static, dthens ("dthens" entspricht der Option Try dhcp server, if it fails use static config (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
-n	Hostname	Zeichenfolge von bis zu 63 Zeichen. Die Zeichenfolge kann Buchstaben, Ziffern, Punkte, Unterstriche und Bindestriche enthalten.
-r	Übertragungsgeschwindigkeit	10, 100, auto
-d	Duplexmodus	full, half, auto
-m	MTU	Numerisch zwischen 60 und 1500

Option	Beschreibung	Werte
-l	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 Übertragungsgeschwindigkeit und den Duplexmodus konfigurierbar sind.	true, false
-nic	Adresse des Netzschnittstellencontrollers. Diese Option bestimmt, welcher Netzanschluss vom IMM2 verwendet wird.	shared, dedicated, shared_option_1 ¹
-failover ²	Funktionsübernahmemodus	none, shared, shared_option_1
-nssync ³	Netzeinstellungssynchronisation	enabled, disabled
-address_table	Tabelle der automatisch generierten IPv6-Adressen und ihre Präfixlängen Anmerkung: Diese Option wird nur dann angezeigt, wenn IPv6 und die statusunabhängige automatische 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 Verbindungsadresse 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	Numerischer Wert 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	enabled, disabled
-sa6	Statusunabhängiger IPv6-Status mit automatischer Konfiguration	enabled, disabled
-vlan	VLAN-Tagging aktivieren oder inaktivieren	enabled, disabled
-vlanid	Identifikationsmarkierung des Netzpakets für das IMM2	Numerischer Wert zwischen 1 und 4094

Option	Beschreibung	Werte
Anmerkungen: 1. Der Wert "shared_option_1" ist auf Servern verfügbar, in denen eine Mezzanine-Netzkarte als Zusatzeinrichtung installiert ist. Diese Mezzanine-Netzkarte kann vom IMM2 verwendet werden. 2. Wenn das IMM2 für die Verwendung des dedizierten Management-Netzanschlusses konfiguriert ist, weist die Option -failover das IMM2 an, zum gemeinsam genutzten Netzanschluss zu wechseln, wenn der dedizierte Anschluss nicht verbunden ist. 3. Wenn der Funktionsübernahmemodus aktiviert ist, weist die Option -nssync das IMM2 an, dieselben Netzeinstellungen für den gemeinsam genutzten Netzanschluss wie für den dedizierten Management-Netzanschluss zu verwenden.		

Syntax:

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*
- l *Lokal verwalteter_MAC*
- b *Herstellerkennung_der_MAC-Adresse*
- dn *Domänenname*
- auto *Zustand*
- nic *Zustand*
- failover *Modus*
- nssync *Zustand*
- address_table
- lla *lokale_IPv6-Verbindungsadresse*
- dhcp6 *Zustand*
- ipv6 *Zustand*
- ipv6static *Zustand*
- sa6 *Zustand*
- i6 *Statische_IPv6-IP-Adresse*
- g6 *IPv6-Gateway-Adresse*
- p6 *Länge*
- vlan *Zustand*
- vlanid *VLAN-ID*

Beispiel:

```
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
-l 00:00:00:00:00:00
```

```
system> ifconfig eth0 -c static -i 192.168.70.133
```

Diese Konfigurationsänderungen werden nach der nächsten Zurücksetzung des IMM2 aktiv.
system>

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.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-add	Aktivierungsschlüssel hinzufügen	Werte für die Befehlsoptionen -ip, -pn, -u, -pw und -f.
-ip	IP-Adresse des TFTP-Servers mit hinzuzufügendem 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 hinzuzufügendem Aktivierungsschlüssel	Gültiger Benutzername für SFTP-Server
-pw	Kennwort für SFTP-Server mit hinzuzufügendem Aktivierungsschlüssel	Gültiges Kennwort für SFTP-Server
-f	Dateiname für hinzuzufügenden Aktivierungsschlüssel	Gültiger Dateiname für Aktivierungsschlüsseldatei.
-del	Aktivierungsschlüssel nach Indexzahl löschen	Gültige Indexzahl für Aktivierungsschlüssel aus keycfg -Liste.
-deltype	Aktivierungsschlüssel nach Schlüsseltyp löschen	Gültiger Wert für Schlüsseltyp.

Syntax:

```
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 "ldap"

Mit dem Befehl **ldap** können Sie die Konfigurationsparameter des LDAP-Protokolls anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-a	Benutzerauthentifizierungsverfahren	"local only", "LDAP only", "local first then LDAP", "LDAP first then local"
-aom	Modus nur für Authentifizierung	enabled, disabled
-b	Bindungsmethode	"anonymous", "bind with ClientDN and password", "bind with Login Credential"
-c	Definierter Name des Clients	Zeichenfolge mit bis zu 127 Zeichen für <i>Definierter_Name_des_Clients</i>
-d	Suchdomäne	Zeichenfolge mit bis zu 63 Zeichen für <i>Suchdomäne</i>
-f	Gruppenfilter	Zeichenfolge mit bis zu 127 Zeichen für <i>Gruppenfilter</i>
-fn	Gesamtstrukturname	Für aktive Verzeichnisumgebungen. Zeichenfolge mit bis zu 127 Zeichen.
-g	Gruppensuchattribut	Zeichenfolge mit bis zu 63 Zeichen für <i>Gruppensuchattribut</i>
-l	Anmeldeberechtigungsattribut	Zeichenfolge mit bis zu 63 Zeichen für <i>Zeichenfolge</i>
-p	Clientkennwort	Zeichenfolge mit bis zu 15 Zeichen für <i>Clientkennwort</i>
-pc	Clientkennwort bestätigen	Zeichenfolge mit bis zu 15 Zeichen für <i>Bestätigungskennwort</i> 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 beiden Argumente nicht miteinander übereinstimmen.
-ep	Verschlüsseltes Kennwort	Kennwort sichern/wiederherstellen (nur interne Verwendung)
-r	Definierter Name des Stammeintrags (DN)	Zeichenfolge mit bis zu 127 Zeichen für <i>definierter_Rootname</i>

Option	Beschreibung	Werte
-rbs	Erweiterte rollenbasierte Sicherheit für Active Directory-Benutzer	enabled, disabled
-s1ip	Hostname/IP-Adresse von Server 1	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für <i>Hostname/IP-Adresse</i>
-s2ip	Hostname/IP-Adresse von Server 2	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für <i>Hostname/IP-Adresse</i>
-s3ip	Hostname/IP-Adresse von Server 3	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für <i>Hostname/IP-Adresse</i>
-s4ip	Hostname/IP-Adresse von Server 4	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für <i>Hostname/IP-Adresse</i>
-s1pn	Portnummer von Server 1	Eine numerische Portnummer mit bis zu 5 Ziffern für <i>Portnummer</i>
-s2pn	Portnummer von Server 2	Eine numerische Portnummer mit bis zu 5 Ziffern für <i>Portnummer</i>
-s3pn	Portnummer von Server 3	Eine numerische Portnummer mit bis zu 5 Ziffern für <i>Portnummer</i>
-s4pn	Portnummer von Server 4	Eine numerische Portnummer mit bis zu 5 Ziffern für <i>Portnummer</i>
-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 <i>Suchattribut</i>
-v	LDAP-Serveradresse über DNS abrufen	off, on
-h	Zeigt die Befehlssyntax und die Optionen an	

Syntax:

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
-l Zeichenfolge
-p Clientkennwort
-pc Bestätigungskennwort
-ep verschlüsseltes_Kennwort
-r definierter_Rootname
-rbs enable|disabled
-s1ip 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.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-en	Aktiviert oder inaktiviert das Network Time Protocol.	enabled, disabled
-i ¹	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 werden soll. Die Reichweite der Indexnummer des NTP-Servers reicht von -i1 bis -i4.
-f	Die Häufigkeit (in Minuten), mit der der IMM2-Taktgeber mit dem Network Time Protocol-Server synchronisiert wird	3 - 1440 Minuten
-synch	Fordert eine sofortige Synchronisation mit dem Network Time Protocol-Server an	Mit diesem Parameter werden keine Werte verwendet.
1. -i entspricht i1.		

Syntax:

```

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

Option	Beschreibung
-high	Legt für die Accountsicherheit eine vordefinierte Gruppe von hohen Standardwerten fest
-exp	Maximale Gültigkeitsdauer des Kennworts (0 - 365 Tage). Der Wert "0" bedeutet, dass das Kennwort nie abläuft.
-cnt	Anzahl der vorherigen Kennwörter, die nicht erneut verwendet werden dürfen (0 - 5)
-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	
-http	HTTP-Portnummer	Standardportnummer: 80
-https	HTTPS-Portnummer	Standardportnummer: 443
-telnet	Traditionelle Telnet-CLI-Portnummer	Standardportnummer: 23
-ssh	Traditionelle SSH-CLI-Portnummer	Standardportnummer: 22

Option	Beschreibung	Werte
-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
- http *Portnummer*
- httpsp *Portnummer*
- telnetp *Portnummer*
- sshp *Portnummer*
- snmpap *Portnummer*
- snmptp *Portnummer*
- rpp *Portnummer*
- cimhp *Portnummer*
- cimhsp *Portnummer*

Beispiel:

```
System> Ports
-http 80
-httpsp 443
-rpp 3900
-snmppap 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 **cliath**, 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.

Anmerkung: Die Anzahl an Datenbits (8) ist in der Hardware festgelegt und kann nicht geändert werden.

Option	Beschreibung	Werte
-b	Baudrate	9600, 19200, 38400, 57600, 115200
-p	Parität	none, odd, even
-s	Bits stoppen	1, 2
-climode	CLI-Modus	0, 1, 2 Dabei gilt: • 0 = none: Die Befehlszeilenschnittstelle wird inaktiviert • 1 = cliems: Die Befehlszeilenschnittstelle wird mit EMS-kompatiblen Tastenfolgen aktiviert • 2 = cliuser: Die Befehlszeilenschnittstelle wird mit benutzerdefinierten Tastenfolgen aktiviert

Syntax:

portcfg [*Optionen*]

Optionen:

-b *Baudrate*
-p *Parität*
-s *Bits_stoppen*
-climode *Modus*

Beispiel:

```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

Befehl "portcontrol"

Verwenden Sie den Befehl **portcontrol**, um einen Netzserviceport zu aktivieren oder zu inaktivieren.

Derzeit unterstützt dieser Befehl lediglich die Steuerung des Ports für das IPMI-Protokoll. Geben Sie **portcontrol** ein, um den Status des IPMI-Ports anzuzeigen. Geben Sie zum Aktivieren oder Inaktivieren des IPMI-Netzports die Option **-ipmi** gefolgt vom Wert **on** oder **off** ein.

Option	Beschreibung	Werte
-ipmi	Port 623 des IPMI-Servers aktivieren oder inaktivieren	on, off
-h		

Syntax:

```
portcontrol [Optionen]
```

Optionen:

```
-ipmi on/off  
-h
```

Beispiel:

```
system> portcontrol  
-ipmi : on  
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 Kennwörter innerhalb der Sicherungsdatei verschlüsselt sind	Gültiges Kennwort oder durch Anführungszeichen begrenzter 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 "scale"

Mit dem Befehl **scale** können Sie die Einstellungen zur Partitionssteuerung und zur Konfiguration für mehrere Knoten (Server) in einem skalierbaren Komplex festlegen und anzeigen.

- Durch Eingabe des Befehls **scale** ohne Optionen werden alle skalierbaren Informationen des Komplexes angezeigt, zu dem der Knoten gehört.
- Alle Knoten in einem skalierbaren Komplex müssen dieselbe Firmwareversion verwenden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

-auto

Option	Beschreibung
-auto	Automatisch eine Partition erstellen, die sich über alle Knoten des skalierbaren Komplexes erstreckt.
-auto <i>Knotenschlüssel</i>	Eine Partition erstellen, die sich über alle Knoten des skalierbaren Komplexes erstreckt. Wenn das aktuelle System die Auswahl eines primären Knotens unterstützt, wird der Knoten mit dem angegebenen Knotenschlüssel als primärer Knoten der zu erstellenden Partition ausgewählt. Der Knotenschlüssel ist eine eindeutige ID für den Knoten.
-create <Schlüssel_von_Knoten1> <Schlüssel_von_Knoten2>_1	Eine Partition erstellen, die sich nur über die angegebenen Knoten des skalierbaren Komplexes erstreckt. Wenn das aktuelle System die Auswahl eines primären Knotens unterstützt, wird der Knoten mit dem ersten Knotenschlüssel in dieser Liste als primärer Knoten der zu erstellenden Partition ausgewählt. Die Knotenschlüsselliste ist eine Liste, die alle durch Leerzeichen voneinander getrennten Knotenschlüssel für die Knoten in der Partition enthält.

Option	Beschreibung
<code>-create _with_physical_node_id <Physische_Knoten-ID1> <Physische_Knoten-ID2>¹</code>	Eine Partition erstellen, die sich nur über die angegebenen Knoten des skalierbaren Komplexes erstreckt. Wenn das aktuelle System die Auswahl eines primären Knotens unterstützt, wird der Knoten mit der ersten physischen Knoten-ID in dieser Liste als primärer Knoten der zu erstellenden Partition ausgewählt. Die Liste der physischen Knoten-IDs ist eine Liste, die alle durch Leerzeichen voneinander getrennten physischen Knoten-IDs für die Knoten in der Partition enthält.
<code>-delete -partid <ID> -node <Knotenschlüssel>¹</code>	Eine bestimmte Partition im skalierbaren Komplex löschen. Anmerkung: Die Partition muss ausgeschaltet sein, damit sie gelöscht werden kann. Löschen Sie eine Partition, indem Sie eine der folgenden Kennungen angeben: • Die Partitions-ID einer Partition im skalierbaren Komplex. • Der Knotenschlüssel eines Knotens in der Partition im skalierbaren Komplex.
<code>-delete</code>	Alle Partitionen im skalierbaren Komplex löschen. Anmerkung: Die Partitionen müssen ausgeschaltet sein, damit sie gelöscht werden können.
<code>-mode [stand-alone partition] [-partid <ID> -node <Knotenschlüssel>]¹</code>	Den Modus für eine bestimmte Partition im skalierbaren Komplex als Standalone-Modus oder Partitionsmodus festlegen. Wenn Sie den Standalone-Modus auswählen, werden die Knoten in der Partition einzeln gebootet. Wenn Sie den Partitionsmodus auswählen, werden alle Knoten in der Partition gemeinsam gebootet. Um den Partitionsmodus festzulegen, können Sie eine der beiden folgenden Kennungen angeben: • Die Partitions-ID der Partition im skalierbaren Komplex. • Der Knotenschlüssel eines Knotens in der Partition im skalierbaren Komplex.

Option	Beschreibung
<code>-start -partid <ID> -node <Knotenschlüssel>¹</code>	Einen Knoten oder alle Knoten in einer Partition im skalierbaren Komplex einschalten. Um die Knoten in einer Partition einzuschalten, können Sie eine der beiden folgenden Kennungen angeben: • Die Partitions-ID der Partition im skalierbaren Komplex. • Der Knotenschlüssel eines Knotens in der Partition im skalierbaren Komplex. Wenn die Partitions-ID als Argument angegeben wird und wenn sich die Knoten in der Partition im Partitionsmodus befinden, werden mit dieser Option alle Knoten innerhalb der Partition eingeschaltet. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Partitionsmodus befindet, werden mit dieser Option alle Knoten innerhalb der Partition eingeschaltet, zu denen der Knotenschlüssel gehört. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Standalone-Modus befindet, wird mit dieser Option nur der Knoten eingeschaltet, zu dem der Knotenschlüssel gehört.
<code>-reset -partid <ID> -node <Knotenschlüssel>¹</code>	Einen Kaltstart eines Knotens oder aller Knoten in einer Partition im skalierbaren Komplex durchführen. Um einen Kaltstart der Knoten in einer Partition durchzuführen, können Sie eine der beiden folgenden Kennungen angeben: • Die Partitions-ID der Partition im skalierbaren Komplex. • Der Knotenschlüssel eines Knotens in der Partition im skalierbaren Komplex. Wenn die Partitions-ID als Argument angegeben wird und wenn sich die Knoten in der Partition im Partitionsmodus befinden, wird mit dieser Option für alle Knoten innerhalb der Partition ein Kaltstart durchgeführt. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Partitionsmodus befindet, wird mit dieser Option ein Kaltstart für alle Knoten innerhalb der Partition durchgeführt, zu denen der Knotenschlüssel gehört. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Standalone-Modus befindet, wird mit dieser Option nur ein Kaltstart für den Knoten durchgeführt, zu dem der Knotenschlüssel gehört.

Option	Beschreibung
<code>-stop -partid <ID> -node <Knotenschlüssel>¹</code>	Einen Knoten oder alle Knoten in einer Partition im skalierbaren Komplex ausschalten. Um die Knoten in einer Partition auszuschalten, können Sie eine der beiden folgenden Kennungen angeben: • Die Partitions-ID der Partition im skalierbaren Komplex. • Der Knotenschlüssel eines Knotens in der Partition im skalierbaren Komplex. Wenn die Partitions-ID als Argument angegeben wird und wenn sich die Knoten in der Partition im Partitionsmodus befinden, werden mit dieser Option alle Knoten innerhalb der Partition ausgeschaltet. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Partitionsmodus befindet, werden mit dieser Option alle Knoten innerhalb der Partition ausgeschaltet, zu denen der Knotenschlüssel gehört. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Standalone-Modus befindet, wird mit dieser Option nur der Knoten ausgeschaltet, zu dem der Knotenschlüssel gehört.
<code>-poweron -partid <ID> -node <Knotenschlüssel>¹</code>	Einen Knoten oder alle Knoten in einer Partition im skalierbaren Komplex einschalten. Um die Knoten in einer Partition einzuschalten, können Sie eine der beiden folgenden Kennungen angeben: • Die Partitions-ID der Partition im skalierbaren Komplex. • Der Knotenschlüssel eines Knotens in der Partition im skalierbaren Komplex. Wenn die Partitions-ID als Argument angegeben wird und wenn sich die Knoten in der Partition im Partitionsmodus befinden, werden mit dieser Option alle Knoten innerhalb der Partition eingeschaltet. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Partitionsmodus befindet, werden mit dieser Option alle Knoten innerhalb der Partition eingeschaltet, zu denen der Knotenschlüssel gehört. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Standalone-Modus befindet, wird mit dieser Option nur der Knoten eingeschaltet, zu dem der Knotenschlüssel gehört.

Option	Beschreibung
<code>-poweroff -partid <ID> -node <Knotenschlüssel>¹</code>	Einen Knoten oder alle Knoten in einer Partition im skalierbaren Komplex ausschalten. Um die Knoten in einer Partition auszuschalten, können Sie eine der beiden folgenden Kennungen angeben: • Die Partitions-ID der Partition im skalierbaren Komplex. • Der Knotenschlüssel eines Knotens in der Partition im skalierbaren Komplex. Wenn die Partitions-ID als Argument angegeben wird und wenn sich die Knoten in der Partition im Partitionsmodus befinden, werden mit dieser Option alle Knoten innerhalb der Partition ausgeschaltet. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Partitionsmodus befindet, werden mit dieser Option alle Knoten innerhalb der Partition ausgeschaltet, zu denen der Knotenschlüssel gehört. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Standalone-Modus befindet, wird mit dieser Option nur der Knoten ausgeschaltet, zu dem der Knotenschlüssel gehört.
<code>-powercycle -partid <ID> -node <Knotenschlüssel>¹</code>	Einen Knoten oder alle Knoten in einer Partition im skalierbaren Komplex aus- und wieder einschalten. Um die Knoten in einer Partition aus- und wieder einzuschalten, können Sie eine der beiden folgenden Kennungen angeben: • Die Partitions-ID der Partition im skalierbaren Komplex. • Der Knotenschlüssel eines Knotens in der Partition im skalierbaren Komplex. Wenn die Partitions-ID als Argument angegeben wird und wenn sich die Knoten in der Partition im Partitionsmodus befinden, werden mit dieser Option alle Knoten innerhalb der Partition aus- und wieder eingeschaltet. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Partitionsmodus befindet, werden mit dieser Option alle Knoten innerhalb der Partition aus- und wieder eingeschaltet, zu denen der Knotenschlüssel gehört. Wenn ein Knotenschlüssel als Argument angegeben wird und wenn sich der Knoten im Standalone-Modus befindet, wird mit dieser Option nur der Knoten aus- und wieder eingeschaltet, zu dem der Knotenschlüssel gehört.
<code>-partid ID</code>	Mit dieser Option können Informationen zu der Partition im skalierbaren Komplex angezeigt werden.
<code>-node Knotenschlüssel</code>	Mit dieser Option können Informationen zu einem Knoten im skalierbaren Komplex angezeigt werden.

Option	Beschreibung
-smp	Mit dieser Option können Informationen zur Skalierbarkeit von Hardware angezeigt werden.
-h oder -help	Mit dieser Option können Nutzungsinformationen zum Befehl "scale" angezeigt werden.
Anmerkung: 1. Die Option wird je nach Platzeinschränkungen in mehreren Zeilen angezeigt.	

Syntax:

scale

Beispiel:

system> **scale**

SMP Hardware =2-node SMP

```
Complex Signature      =COMD
Complex ID             =0x4062
Complex Partition Count =1
Complex Node Count     =2
  Node[0] UUID =575D2D11717411E382996CAE8B7037F0
  Node[0] Serial Number =23ZBVC8
  Node[0] Node Key =0x6F00
  Node[0] Machine Type & Model =7903AC1
  Node[0] Slot ID =3-4
  Node[0] Logical ID =0x00
  Node[0] Partition ID =0x01
  Node[0] Partition Node Count =0x02
  Node[0] Partition Flags =0x1F
  Node[0] String ID =23ZBVC8[3-4]
  Node[0] Port[0] Remote Node Key =0x3F01
  Node[0] Port[0] Remote Port Number =0x00
  Node[0] Port[0] Status =Enabled
  Node[0] Port[0] Type =QPI
  Node[0] Port[1] Remote Node Key =0xFFFF
  Node[0] Port[1] Remote Port Number =0xFF
  Node[0] Port[1] Status =Disabled
  Node[0] Port[1] Type =QPI
  Node[0] Port[2] Remote Node Key =0xFFFF
  Node[0] Port[2] Remote Port Number =0xFF
  Node[0] Port[2] Status =Disabled
  Node[0] Port[2] Type =QPI
  Node[1] UUID =DEDB90B572211E3BADB6CAE8B703620
  Node[1] Serial Number =23ZBVF0
  Node[1] Node Key =0x3F01
  Node[1] Machine Type & Model =7903AC1
  Node[1] Slot ID =5-6
  Node[1] Logical ID =0x01
  Node[1] Partition ID =0x01
  Node[1] Partition Node Count =0x02
  Node[1] Partition Flags =0x1F
  Node[1] String ID =23ZBVF0[5-6]
  Node[1] Port[0] Remote Node Key =0x6F00
  Node[1] Port[0] Remote Port Number =0x00
  Node[1] Port[0] Status =Enabled
  Node[1] Port[0] Type =QPI
  Node[1] Port[1] Remote Node Key =0xFFFF
  Node[1] Port[1] Remote Port Number =0xFF
  Node[1] Port[1] Status =Disabled
  Node[1] Port[1] Type =QPI
  Node[1] Port[2] Remote Node Key =0xFFFF
```

```

Node[1] Port[2] Remote Port Number =0xFF
Node[1] Port[2] Status =Disabled
Node[1] Port[2] Type =QPI
system>

```

Syntax:

```

scale [Optionen]
Optionen:
  -auto Knotenschlüssel

```

Beispiel:

```

system> scale
-auto 0x2f00
system>

system> scale
-auto
system>

```

Syntax:

```

scale [Optionen]
Optionen:
  -create erster_Knotenschlüssel zweiter_Knotenschlüssel

```

Beispiel:

```

system> scale
-create 0x2f00 0x8f01
system>

```

Syntax:

```

scale [Optionen]
Optionen:
  -create _with_physical_node_id

```

Beispiel:

```

system> scale
-create_with_physical_node_id <Physische_Knoten-ID1 Physische_Knoten-ID2>
system>

```

Syntax:

```

scale [Optionen]
Optionen:
  -delete

```

Beispiele:

```

system> scale
-delete -node 0x2f00
system>

system> scale
-delete -partid 1
system>

```

Syntax:

```

scale [Optionen]
Optionen:
  -mode

```

Beispiele:

```

system> scale
-mode standalone -partid 1
system>

system> scale
-mode partition -partid 1
system>

system> scale
-mode standalone -node 0x2f00
system>

system> scale
-mode partition -node 0x2f00
system>

```

Syntax:

`scale [Optionen]`

Option:
-start

Beispiele:

```

system> scale
-start -partid 1
system>

system> scale
-start -node 0x2f00
system>

```

Syntax:

`scale [Optionen]`

Option:
-reset

Beispiele:

```

system> scale
-reset -partid 1
system>

system> scale
-reset -node 0x2f00
system>

```

Syntax:

`scale [Optionen]`

Option:
-stop

Beispiele:

```

system> scale
-stop -partid 1
system>

system> scale
-stop -node 0x2f00
system>

```

Syntax:

`scale [Optionen]`

Option:
-poweron

Beispiele:

```

system> scale
-poweron -partid 1
system>

system> scale
-poweron -node 0x2f00
system>

```

Syntax:

```

scale [Optionen]
Option:
    -poweroff

```

Beispiele:

```

system> scale
-poweroff -partid 1
system>

system> scale
-poweroff -node 0x2f00
system>

```

Syntax:

```

scale [Optionen]
Option:
    -powercycle

```

Beispiele:

```

system> scale
-powercycle -partid 1
system>

system> scale
-powercycle -node 0x2f00
system>

```

Syntax:

```

scale [Optionen]
Option:
    -partid

```

Beispiel:

```

system> scale
-partid 1
Partition Id 1
    Node count = 2
    Complex id = 0x3360

    Node Logical id =0x00
    Node UUID = BA DF CC 0C DC A7 4E D6 96 44 D9 24 49 10 29 C3
    Node serial number = BOGUS04
    Node key =0x2F00
    Node machine type = 7903AC1
    Node partition id =0x01
    Node partition count =0x02
    Node partition flags =0x1F
    Node string id = []
        Node port[0] remote node key =0x0001
        Node port[0] remote node number =0x00
        Node port[0] port status =0x01
        Node port[0] port type =0x00
        Node port[1] remote node key =0x00FF
        Node port[1] remote node number =0xFF
        Node port[1] port status =0x00

```

```

Node port[1] port type =0x00
Node port[2] remote node key =0x00FF
Node port[2] remote node number =0xFF
Node port[2] port status =0x00
Node port[2] port type =0x00

Node Logical id =0x01
Node UUID = BA D4 FF 2D F7 49 45 36 A9 E5 4E 77 6C 41 8B A0
Node serial number = BOGUS05
Node key =0x8F01
Node machine type = 7903AC1
Node partition id =0x01
Node partition count =0x02
Node partition flags =0x1F
Node string id = []
Node port[0] remote node key =0x0000
Node port[0] remote node number =0x00
Node port[0] port status =0x01
Node port[0] port type =0x00
Node port[1] remote node key =0x00FF
Node port[1] remote node number =0xFF
Node port[1] port status =0x00
Node port[1] port type =0x00
Node port[2] remote node key =0x00FF
Node port[2] remote node number =0xFF
Node port[2] port status =0x00
Node port[2] port type =0x00
system>

```

Syntax:

```

scale [Optionen]
Option:
-node

```

Beispiel:

```

system> scale
-node 0x2f00
Node Logical id =0x00
Node UUID = BA DF CC 0C DC A7 4E D6 96 44 D9 24 49 10 29 C3
Node serial number = BOGUS04
Node key =0x2F00
Node machine type = 7903AC1
Node partition id =0x01
Node partition count =0x02
Node partition flags =0x1F
Node string id = []
Node port[0] remote node key =0x0001
Node port[0] remote node number =0x00
Node port[0] port status =0x01
Node port[0] port type =0x00
Node port[1] remote node key =0x00FF
Node port[1] remote node number =0xFF
Node port[1] port status =0x00
Node port[1] port type =0x00
Node port[2] remote node key =0x00FF
Node port[2] remote node number =0xFF
Node port[2] port status =0x00
Node port[2] port type =0x00
system>

```

Syntax:

```

scale [Optionen]
Option:
-smp

```

Beispiel:

```
system> scale
-smp -partid 1
SMP Hardware =2-node SMP
system>
```

Syntax:

```
scale [Optionen]
Option:
    -help
```

Beispiele:

```
system> scale
-h
system>
system> scale
-help
system>
```

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.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
<i>value</i>	Wert für angegebenen Pfad oder angegebene Einstellung festlegen	Entsprechender Wert für angegebenen Pfad oder angegebene 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	Authentifizierungssupport für SMTP	enabled, disabled
-authpw	verschlüsseltes Kennwort für die SMTP-Authentifizierung	Gültige Kennwort-Zeichenkette
-authmd	SMTP-Authentifizierungsverfahren	CRAM-MD5, LOGIN

Option	Beschreibung	Werte
-authn	Benutzername zur SMTP-Authentifizierung	Zeichenkette (auf 256 Zeichen begrenzt).
-authpw	SMTP-Authentifizierungskennwort	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).

Syntax:

smtp [*Optionen*]

Option:

```
-auth enabled|disabled
-authpw 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 Anmerkung: Folgende Kriterien müssen zur Aktivierung des SNMPv1-Agenten erfüllt sein: - Über die Befehlsoption "-cn" angegebener Ansprechpartner für das IMM2. - Über die Befehlsoption "-l" angegebener Standort des IMM2. - Mindestens ein über eine der "-cx"-Befehlsoptionen angegebener SNMP-Community-Name. - Mindestens eine gültige IP-Adresse wird über eine der "-cxiy"-Befehlsoptionen für jede SNMP-Community angegeben.

Option	Beschreibung	Werte
-a3	SNMPv3-Agent	on, off Anmerkung: Folgende Kriterien müssen zum Aktivieren des SNMPv3-Agenten erfüllt sein: • Über die Befehlsoption "-cn" angegebener Ansprechpartner für das IMM2. • Über die Befehlsoption "-l" angegebener Standort des IMM2.
-t	SNMP-Traps	on, off
-l	IMM2-Standort	Zeichenkette (auf 47 Zeichen begrenzt). Anmerkung: • Argumente mit Leerzeichen müssen in Anführungszeichen 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 Anführungszeichen gesetzt werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig. • Löschen Sie beim IMM2-Ansprechpartner den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa "".
-cx	Name von SNMP-Community x	Zeichenkette (auf 15 Zeichen begrenzt). Anmerkung: • x wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Communitynummer anzuzeigen. • Argumente mit Leerzeichen müssen in Anführungszeichen 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 angeben, etwa "".
-cxiy	IP-Adresse oder Hostname y von SNMP-Community x	Gültige IP-Adresse oder gültiger Hostname (auf 63 Zeichen begrenzt). Anmerkung: • x wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Communitynummer anzuzeigen. • y 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 Punkte, Unterstriche, Minuszeichen, Buchstaben und Ziffern enthalten. Eingebettete Leerzeichen oder aufeinanderfolgende Punkte sind nicht zulässig. • Löschen Sie den Inhalt bei der IP-Adresse oder beim Hostnamen einer SNMP-Community, indem Sie kein Argument angeben.

Option	Beschreibung	Werte
-cax	Zugriffstyp bei SNMPv3-Community x	get, set, trap Anmerkung: x wird in der Befehlsoption mit 1, 2 oder 3 angegeben, um die Communitynummer anzuzeigen.

Syntax:

snmp [Optionen]

Option:

- a Zustand
- a3 Zustand
- t Zustand
- l 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
- cli2 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
- ca1 Zugriffstyp_von_Community_1
- ca2 Zugriffstyp_von_Community_2
- ca3 Zugriffstyp_von_Community_3

Beispiel:

```
system> snmp
-a Enabled
-a3 Enabled
-t Enabled
-l RTC,NC
-cn Snmp Test
-c1 public
-c1i1 192.44.146.244
-c1i2 192.44.146.181
-c1i3 192.44.143.16
-ca1 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 gesendete 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 Ereignisse fest, die Alerts senden	all, none, custom:te vo po di fa cp me in re ot Benutzerdefinierte Einstellungen für kritische Alerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form snmpalerts -crt custom:te vo angegeben; benutzerdefinierte Werte sind: • te: kritischer Temperaturschwellenwert überschritten • vo: kritischer Spannungsschwellenwert überschritten • po: kritischer Netzausfall • di: Fehler beim Festplattenlaufwerk • fa: Lüfterfehler • cp: Mikroprozessorfehler • me: Speicherfehler • in: Hardwareinkompatibilität • re: Stromversorgungsredundanzfehler • ot: alle anderen kritischen Ereignisse
-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 snmpalerts -wrn custom:rp te 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	all, none, custom:lo tio ot po bf til pf el ne 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: • lo: erfolgreiche Fernanmeldung • tio: Zeitlimit des Betriebssystems • ot: alle anderen Informations- und Systemereignisse • po: Stromversorgung des Systems ein/aus • bf: Bootfehler des Betriebssystems • til: Watchdog-Zeitlimitüberschreitung des Betriebssystemladeprogramms • pf: vorhergesagter Fehler (PFA - Predictive Failure Analysis) • el: Ereignisprotokoll zu 75% voll • ne: Netzänderung
-sysen	Alerts bei Routineereignissen senden	enabled, disabled

Syntax:

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 Durchgriffsfunktion 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	Tastenfolge für Befehlszeilenschnittstelle eingeben	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 (.

Syntax:

```
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 anzeigen	

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 inaktiviert einen SSL-Client	on, off
-se	Aktiviert oder inaktiviert einen SSL-Server	on, off
-cime	Aktiviert oder inaktiviert 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 Anmerkung: Der SSL-Client kann nur bei Vorliegen eines gültigen Server- oder Clientzertifikats aktiviert werden.
-cim	CIM-over-HTTPS-Status	enabled, disabled Anmerkung: CIM over HTTPS kann nur bei Vorliegen eines gültigen Server- oder Clientzertifikats aktiviert werden.
-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
-l	Dateiname des Zertifikats	Gültiger Dateiname Anmerkung: Beim Herunterladen oder Hochladen eines Zertifikats oder einer Zertifikatssignieranforderung ist ein Dateiname erforderlich. Wenn beim Herunterladen kein Dateiname angegeben wird, wird der Standardname für die Datei verwendet und angezeigt.

Option	Beschreibung	Werte
-dnld	Zertifikatsdatei herunterladen	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 Option sind keine Argumente erforderlich; es müssen jedoch Werte für die Befehlsoption -i und die (optionale) Befehlsoption -l angegeben werden.
-upld	Importiert Zertifikatsdatei	Bei dieser Option sind keine Argumente erforderlich, es müssen jedoch Werte für die Befehlsoptionen -cert , -i und -l angegeben werden.
-tcx	Vertrauenswürdige Zertifikat <i>x</i> für SSL-Client	import, download, remove Anmerkung: 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) Anmerkung: Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cl	Ort oder Standort	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 50 Zeichen) Anmerkung: Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-on	Name des Unternehmens	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) Anmerkung: Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-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) Anmerkung: 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) Anmerkung: Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.

Option	Beschreibung	Werte
-s	Nachname	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) Anmerkung: Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-gn	Vorname	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) Anmerkung: Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-in	Initialen	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 20 Zeichen) Anmerkung: Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-dq	Qualifikationsmerkmal des Domänennamens	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) Anmerkung: Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cpwd	Kennwort abfragen	Zeichenkette (mindestens 6 Zeichen, höchstens 30 Zeichen) Anmerkung: Optional bei der Erstellung einer Zertifikatssignieranforderung.
-un	Unstrukturierter Name	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) Anmerkung: Optional bei der Erstellung einer Zertifikatssignieranforderung.

Syntax:

sslcfg [Optionen]

Option:

- server *Zustand*
- client *Zustand*
- cim *Zustand*
- i *IP-Adresse*
- pn *Portnummer*
- u *Benutzername*
- pw *Kennwort*
- l *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*

Beispiele:

```
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
```

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 Anmerkung: 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 "tls"

Verwenden Sie den Befehl **tls**, um die TLS-Mindeststufen festzulegen. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-min	TLS-Minimalstufe auswählen	1.0, 1.1, 1.2 ¹
-h	Verwendung und Optionen auflisten	
Anmerkung: 1. Wenn als Verschlüsselungsmodus der NIST-800-131A-Kompatibilitätsmodus festgelegt ist, muss als TLS-Version 1.2 festgelegt werden.		

Syntax:

```

tls [Optionen]
Option:
  -min 1.0|1.1|1.2
  -h

```

Beispiele:

Um die Verwendung für den Befehl "tls" abzurufen, geben Sie den folgenden Befehl aus:

```

system> tls
-h                                system>

```

Um die aktuelle TLS-Version abzurufen, geben Sie den folgenden Befehl aus:

```

system> tls
-min 1.0
system>

```

Um die aktuelle TLS-Version in 1.2 zu ändern, geben Sie den folgenden Befehl aus:

```

system> tls
-min 1.2
ok
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
-l	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
-o	Zeitlimit für das Betriebssystem	Minuten	disabled, 2.5, 3, 3.5, 4

Syntax:

`timeouts [Optionen]`

Optionen:

`-f Watchdogoption_für_Ausschaltverzögerung`

`-o Option_für_Betriebssystem-Watchdog`

`-l Option_für_Ladeprogramm-Watchdog`

Beispiel:

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 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
<i>-Benutzerindex</i>	Indexnummer des Benutzerkontos	1 bis 12 einschließlich oder <code>all</code> für alle Benutzer.
<i>-n</i>	Name des Benutzerkontos	Eindeutige Zeichenfolge, die nur Zahlen, Buchstaben, Punkte und Unterstriche enthält. Mindestens vier Zeichen; höchstens 16 Zeichen.
<i>-p</i>	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 festlegen.
<i>-a</i>	Benutzerberechtigungsstufe	super, ro, custom Dabei gilt: • super (Supervisor) • ro (Lesezugriff) • custom wird gefolgt von einem Doppelpunkt und einer Liste mit Werten, die durch Pipes voneinander getrennt sind, wie im folgenden Format: <code>custom:am rca</code>. Diese Werte können in beliebiger Kombination verwendet werden. - am (Benutzerkontenverwaltungszugriff) - rca (Zugriff auf ferne Konsole) - rcvma (Zugriff auf ferne Konsole und virtuelle Datenträger) - pr (Berechtigung für Einschalten/Neustart eines fernen Servers) - cel (Berechtigung zum Löschen von Ereignisprotokollen) - bc (Adapterkonfiguration - Allgemein) - nsc (Adapterkonfiguration - Netz und Sicherheit) - rcvma (Adapterkonfiguration - Erweitert)
<i>-ep</i>	Verschlüsselungskennwort (für Sicherung/Wiederherstellung)	Gültiges Kennwort
<i>-clear</i>	Angegebenes Benutzerkonto entfernen	Die Indexnummer des zu entfernenden Benutzerkontos muss im folgenden Format angegeben werden: <code>users -clear -Benutzerindex</code>
<i>-curr</i>	Aktuell angemeldete Benutzer anzeigen	
<i>-sauth</i>	SNMPv3-Authentifizierungsprotokoll	HMAC-MD5, HMAC-SHA, none
<i>-spriv</i>	SNMPv3-Datenschutzprotokoll	CBC-DES, AES, none
<i>-spw</i>	SNMPv3-Datenschutzkennwort	Gültiges Kennwort
<i>-sepw</i>	SNMPv3-Datenschutzkennwort (verschlüsselt)	Gültiges Kennwort
<i>-sacc</i>	SNMPv3-Zugriffstyp	get, set
<i>-strap</i>	SNMPv3-Trap-Hostname	Gültiger Hostname
<i>-pk</i>	Öffentlichen SSH-Schlüssel für Benutzer anzeigen	Indexnummer des Benutzerkontos. Anmerkung: • Es werden jeder dem Benutzer zugeordnete SSH-Schlüssel und die jeweilige Schlüsselindexnummer angezeigt. • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option <code>-pk</code> nach dem Benutzerindex (Option <i>-Benutzerindex</i>) im folgenden Format verwendet werden: <code>users -2 -pk</code>. • Alle Schlüssel weisen das OpenSSH-Format auf.
<i>-e</i>	Vollständigen SSH-Schlüssel im OpenSSH-Format anzeigen (Option für öffentliche SSH-Schlüssel)	Diese Option kann nur ohne Argumente verwendet werden. Sie muss ohne die anderen Optionen vom Typ <code>users -pk</code> verwendet werden. Anmerkung: Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option <code>-pk</code> nach dem Benutzerindex (Option <i>-Benutzerindex</i>) im folgenden Format verwendet werden: <code>users -2 -pk -e</code>.

Option	Beschreibung	Werte
-remove	Öffentlichen SSH-Schlüssel für Benutzer entfernen (Option für öffentliche SSH-Schlüssel)	Die Indexnummer des öffentlichen Schlüssels, der entfernt werden soll, muss für einen bestimmten Schlüssel mit <i>-Schlüsselindex</i> oder für alle dem Benutzer zugeordneten Schlüssel mit <i>-all</i> angegeben werden. Anmerkung: Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option <i>-pk</i> nach dem Benutzerindex (Option <i>-Benutzerindex</i>) im folgenden Format verwendet werden: <code>users -2 -pk -remove -1</code> .
-add	Öffentlichen SSH-Schlüssel für Benutzer hinzufügen (Option für öffentliche SSH-Schlüssel)	Durch Anführungszeichen begrenzter Schlüssel im OpenSSH-Format Anmerkung: - Die Option <i>-add</i> muss ohne die anderen Befehlsoptionen vom Typ <code>users -pk</code> verwendet werden. - Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option <i>-pk</i> nach dem Benutzerindex (Option <i>-Benutzerindex</i>) im folgenden Format verwendet werden: <code>users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAAQEAvmfntUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaN0y400ICEKcQjKEhrYymtAoVtfKApvY39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKHj46X7E+mq1fWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzCjy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2hIEpXR5dNUiupA1Yd8PSSMgduKASkeD3eRRZTB13SATMucUsTkYj1Xcqex10Qz4+N50R6MbNcw1sx+mTEAvvcPJhuga70UNPGhLJM16k7jeJiQ8Xd2p Xb0ZQ="</code>
-upld	Öffentlichen SSH-Schlüssel hochladen (Option für öffentliche SSH-Schlüssel)	Die Optionen <i>-i</i> und <i>-l</i> sind für die Angabe der Schlüsselposition erforderlich. Anmerkung: - Die Option <i>-upld</i> muss ohne die anderen Befehlsoptionen vom Typ <code>users -pk</code> verwendet werden (mit Ausnahme der Optionen <i>-i</i> und <i>-l</i>). - Um einen Schlüssel durch einen neuen Schlüssel zu ersetzen, müssen Sie einen <i>-Schlüsselindex</i> angeben. Wenn Sie einen Schlüssel zum Ende der Liste der aktuellen Schlüssel hinzufügen möchten, geben Sie keinen Schlüsselindex an. - Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option <i>-pk</i> nach dem Benutzerindex (Option <i>-Benutzerindex</i>) im folgenden Format verwendet werden: <code>users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key</code>.
-dnld	Angegebenen öffentlichen SSH-Schlüssel herunterladen (Option für öffentliche SSH-Schlüssel)	Der <i>-Schlüsselindex</i> zum Herunterladen des betreffenden Schlüssels und die Optionen <i>-i</i> und <i>-l</i> zum Angeben der Speicherposition für den Download (auf einem anderen Computer als auf dem, auf dem ein TFTP-Server ausgeführt wird) sind erforderlich. Anmerkung: - Die Option <i>-dnld</i> muss ohne die anderen Befehlsoptionen vom Typ <code>users -pk</code> verwendet werden (mit Ausnahme von <i>-i</i>, <i>-l</i> und <i>-Schlüsselindex</i>). - Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option <i>-pk</i> nach dem Benutzerindex (Option <i>-Benutzerindex</i>) im folgenden Format verwendet werden: <code>users -2 -pk -dnld -l -i tftp://9.72.216.40/ -l file.key</code>.
-i	IP-Adresse des TFTP/SFTP-Servers zum Hoch- oder Herunterladen einer Schlüsseldatei (Option für öffentliche SSH-Schlüssel)	Gültige IP-Adresse Anmerkung: Die Option <i>-i</i> ist für die Befehlsoptionen <code>users -pk -upld</code> und <code>users -pk -dnld</code> erforderlich.
-pn	Portnummer des TFTP-/SFTP-Servers (Option für öffentliche SSH-Schlüssel)	Gültige Portnummer (Standard 69/22) Anmerkung: Ein optionaler Parameter für die Befehlsoptionen <code>users -pk -upld</code> und <code>users -pk -dnld</code> .
-u	Benutzername für SFTP-Server (Option für öffentliche SSH-Schlüssel)	Gültiger Benutzername Anmerkung: Ein optionaler Parameter für die Befehlsoptionen <code>users -pk -upld</code> und <code>users -pk -dnld</code> .

Option	Beschreibung	Werte
-pw	Kennwort für SFTP-Server <i>(Option für öffentliche SSH-Schlüssel)</i>	Gültiges Kennwort Anmerkung: Ein optionaler Parameter für die Befehlsoptionen users -pk -upld und users -pk -dnld.
-l	Dateiname zum Hoch- oder Herunterladen einer Schlüsseldatei über TFTP oder SFTP <i>(Option für öffentliche SSH-Schlüssel)</i>	Gültiger Dateiname Anmerkung: Die Option -l ist für die Befehlsoptionen users -pk -upld und users -pk -dnld erforderlich.
-af	Verbindungen vom Host akzeptieren <i>(Option für öffentliche SSH-Schlüssel)</i>	Eine durch Kommas getrennte Liste von Hostnamen und IP-Adressen, begrenzt auf 511 Zeichen. Gültige Zeichen: alphanumerisch, Komma, Stern, Fragezeichen, Ausrufezeichen, Punkt, Bindestrich, Doppelpunkt und Prozentzeichen.
-cm	Kommentar <i>(Option für öffentliche SSH-Schlüssel)</i>	Eine durch Anführungszeichen begrenzte Zeichenfolge von bis zu 255 Zeichen. Anmerkung: Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option -pk nach dem Benutzerindex (Option <i>-Benutzerindex</i>) im folgenden Format verwendet werden: users -2 -pk -cm "This is my comment."

Syntax:

```

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
  -l 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. jacybyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSWORD -a custom:am|rca|cel|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. jacybyackenovic 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 263
- „Befehl "clearcfg"“ auf Seite 264
- „Befehl "clock"“ auf Seite 264
- „Befehl "identify"“ auf Seite 265
- „Befehl "info"“ auf Seite 265
- „Befehl "resetsp"“ auf Seite 266
- „Befehl "spreset"“ auf Seite 266

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 'number' für 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.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-number	Indexnummer des Alertempfängers, der angezeigt, hinzugefügt, 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 einschließen	on, off
-n	Alertempfängername	Zeichenkette
-e	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 Empfängerindexnummer löschen	
-test	Generiert einen Testalert an die angegebene Empfängerindexnummer	
-crt	Legt kritische Ereignisse fest, die Alerts senden	all, none, custom:te vo po di fa cp me in re ot Benutzerdefinierte Einstellungen für kritische Alerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form alertentries -crt custom:te vo angegeben; benutzerdefinierte Werte sind: • te: kritischer Temperaturschwellenwert überschritten • vo: kritischer Spannungsschwellenwert überschritten • po: kritischer Netzausfall • di: Fehler beim Festplattenlaufwerk • fa: Lüfterfehler • cp: Mikroprozessorfehler • me: Speicherfehler • in: Hardwareinkompatibilität • re: Stromversorgungsredundanzfehler • ot: alle anderen kritischen Ereignisse
-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 alertentries -wrn custom:rp te 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 Benutzerdefinierte Einstellungen für Routinealerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form alertentries -sys custom:lo tio angegeben; benutzerdefinierte Werte sind: • lo: erfolgreiche Fernanmeldung • tio: Zeitlimit des Betriebssystems • ot: alle anderen Informations- und Systemereignisse • po: Stromversorgung des Systems ein/aus • bf: Bootfehler des Betriebssystems • til: Watchdog-Zeitlimitüberschreitung des Betriebssystemladeprogramms • pf: vorhergesagter Fehler (PFA - Predictive Failure Analysis) • el: Ereignisprotokoll zu 75% voll • ne: Netzänderung
-sysen	Alerts bei Routineereignissen senden	enabled, disabled

Syntax:

```

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.

- Kommentarseilen 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.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

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

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-Abweichung kann im Format +2:00, +2 oder 2 (für positive Abweichungen) und im Format -5:00 oder -5 (für 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 Ansprechpartners für das IMM2	Zeichenkette
-location	IMM2-Standort	Zeichenkette
-room ¹	Raum-ID des IMM2	Zeichenkette
-rack ¹	Gehäuserahmen-ID des IMM2	Zeichenkette
-rup ¹	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.

Service Advisor-Befehle

Die Service Advisor-Befehle lauten wie folgt:

- „Befehl "autoftp"“
- „Befehl "chconfig"“ auf Seite 267
- „Befehl "chlog"“ auf Seite 269
- „Befehl "chmanual"“ auf Seite 269
- „Befehl "events"“ auf Seite 270
- „Befehl "sdemail"“ auf Seite 270

Befehl "autoftp"

Mit dem Befehl **autoftp** können Sie die FTP-/TFTP-/SFTP-Servereinstellungen für das IMM2 anzeigen und konfigurieren. Der Server sendet keine doppelten Ereignismeldungen, wenn sie im Aktivitätenprotokoll nicht bestätigt werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-m	Der automatisierte Problemmeldungsmodus	ftp, sftp, tftp, disabled Anmerkungen: • Für den ftp-Modus müssen alle Felder festgelegt werden. • Für den tftp-Modus sind nur die Optionen -i und -p erforderlich.

Option	Beschreibung	Werte
-i	Die IP-Adresse oder der Hostname für den FTP-, SFTP- oder TFTP-Server für die automatisierte Problemmeldung	Gültige IP-Adresse oder gültiger Hostname
-p	Der FTP-, SFTP- oder TFTP-Übertragungsport für die automatisierte Problemmeldung	Gültige Portnummer (1 - 65535)
-u	Der FTP-, SFTP- oder TFTP-Benutzername für die automatisierte Problemmeldung	Eine durch Anführungszeichen begrenzte Zeichenfolge von bis zu 63 Zeichen
-pw	FTP-Kennwort für die automatisierte Problemmeldung	Eine durch Anführungszeichen begrenzte Zeichenfolge von bis zu 63 Zeichen

Syntax:

autoftp [*Optionen*]

Option:

-m *Modus*
-i *IP-Adresse_oder_Hostname*
-p *Portnummer*
-u *Benutzername*
-pw *Kennwort*

Befehl "chconfig"

Mit dem Befehl **chconfig** können Sie die Service Advisor-Einstellungen anzeigen und konfigurieren.

Anmerkungen:

- Die Nutzungsbedingungen von Service Advisor müssen mithilfe der Befehlsoption **chconfig -li** akzeptiert werden, bevor weitere Parameter konfiguriert werden können.
- Alle Felder mit Kontaktinformationen sowie das Feld für das IBM Service Support Center sind erforderlich, bevor IBM Support für Service Advisor aktiviert werden kann.
- Alle Felder für den HTTP-Proxy müssen angegeben werden, wenn ein HTTP-Proxy erforderlich ist.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-li	Nutzungsbedingungen von Service Advisor anzeigen oder akzeptieren	view, accept
-sa	IBM Support-Status vom Service Advisor	enabled, disabled
-sc	Landescode für das IBM Service Support Center	ISO-Landescode aus zwei Zeichen
Optionen für Kontaktinformationen zu Service Advisor:		

Option	Beschreibung	Werte
-ce	E-Mail-Adresse des primären Ansprechpartners	Gültige E-Mail-Adresse im Format benutzer-id@hostname (höchstens 30 Zeichen)
-cn	Name des primären Ansprechpartners	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 30 Zeichen)
-co	Name der Organisation oder des Unternehmens des primären Ansprechpartners	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 30 Zeichen)
-cph	Telefonnummer des primären Ansprechpartners	Durch Anführungszeichen begrenzte Zeichenkette (5 bis 30 Zeichen)
-cpx	Telefondurchwahl des primären Ansprechpartners	Durch Anführungszeichen begrenzte Telefondurchwahl des Ansprechpartners (1 bis 5 Zeichen)
Optionen für alternative Kontaktinformationen zu Service Advisor:		
-ae	E-Mail-Adresse des alternativen Ansprechpartners	Gültige E-Mail-Adresse im Format benutzer-id@hostname (höchstens 30 Zeichen)
-an	Name des alternativen Ansprechpartners	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 30 Zeichen)
-aph	Telefonnummer des alternativen Ansprechpartners	Durch Anführungszeichen begrenzte Zeichenkette (5 bis 30 Zeichen)
-apx	Telefondurchwahl des alternativen Ansprechpartners	Durch Anführungszeichen begrenzte Zeichenkette (1 bis 5 Zeichen)
Option für Systemadressinformationen:		
-mp	Telefonnummer für den Maschinenstandort	Durch Anführungszeichen begrenzte Zeichenkette (5 bis 30 Zeichen)
Optionen für HTTP-Proxy-Einstellungen:		
-loc	Position des HTTP-Proxy	Vollständig qualifizierter Hostname oder IP-Adresse für HTTP-Proxy (höchstens 63 Zeichen)
-po	Port des HTTP-Proxy	Gültige Portnummer (1 - 65535)
-ps	Status des HTTP-Proxy	enabled, disabled
-pw	Kennwort des HTTP-Proxy	Gültiges Kennwort, durch Anführungszeichen getrennt (höchstens 15 Zeichen)
-u	Benutzername für HTTP-Proxy	Gültiger Benutzername, durch Anführungszeichen getrennt (höchstens 30 Zeichen)

Syntax:

chconfig [*Optionen*]

Option:

```

-li view|accept
-sa enable|disable
-sc Service-Landescode
-ce E-Mail-Adresse_des_Ansprechpartners
-cn Name_des_Ansprechpartners
-co Name_des_Unternehmens
-cph Telefonnummer_des_Ansprechpartners
-cpx Telefondurchwahl_des_Ansprechpartners
-an Name_des_alternativen_Ansprechpartners
-ae E-Mail-Adresse_des_alternativen_Ansprechpartners
-aph Telefonnummer_des_alternativen_Ansprechpartners
-apx Telefondurchwahl_des_alternativen_Ansprechpartners
-mp Telefonnummer_für_Maschine
-loc Hostname/IP-Adresse
-po Proxy-Port

```

```
-ps Proxy-Status
-pw Proxy-Kennwort
-ccl Landescode_für_Maschine
-u Proxy-Benutzername
```

Befehl "chlog"

Mit dem Befehl **chlog** können Aktivitätenprotokolleinträge zu Service Advisor angezeigt werden. Beim Befehl **chlog** werden die letzten fünf Einträge aus dem Call-Home-Aktivitätenprotokoll angezeigt, die durch den Server oder den Benutzer generiert wurden. Der neueste Call-Home-Eintrag wird zuerst aufgeführt. Der Server sendet keine doppelten Ereignismeldungen, wenn sie im Aktivitätenprotokoll nicht als korrigiert bestätigt werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-index	Einen Call-Home-Eintrag mithilfe des Index aus dem Aktivitätenprotokoll angeben	Indexnummer des Ereignisses. Die Indexnummern können über den Befehl chlog angezeigt werden.
-ack	Bestätigen oder nicht bestätigen, dass ein Call-Home-Ereignis korrigiert wurde	yes, no Anmerkung: Über die Befehlsoption <i>-event_index</i> wird das Ereignis angegeben, das bestätigt oder nicht bestätigt werden soll.
-s	Die letzten fünf Einträge des IBM Support aus dem Call-Home-Aktivitätenprotokoll werden angezeigt	
-f	Die letzten fünf FTP-/TFTP-Servereinträge aus dem Call-Home-Aktivitätenprotokoll werden angezeigt	

Syntax:

```
chlog [Optionen]
```

Option:

```
-index
-ack Zustand
-s -f
```

Befehl "chmanual"

Verwenden Sie den Befehl **chmanual**, um eine manuelle Call-Home-Anforderung oder ein Call-Home-Testereignis zu generieren.

Anmerkung: Empfänger von Call-Home-Nachrichten werden mithilfe des Befehls **chconfig** konfiguriert.

- Beim Befehl **chmanual -test** wird eine Call-Home-Testnachricht generiert.
- Beim Befehl **chmanual -desc** wird eine manuelle Call-Home-Nachricht generiert.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-test	Generiert eine Testnachricht für Call-Home-Empfänger	
-desc	Sendet eine benutzergenerierte Nachricht an Call-Home-Empfänger	Durch Anführungszeichen begrenzte Zeichenkette zum Beschreiben des Problems (höchstens 100 Zeichen)

Syntax:

chmanual [*Optionen*]

Option:

-test

-desc *Nachricht*

Befehl "events"

Anmerkung: Die Nutzungsbedingungen von Service Advisor müssen vor der Anwendung des Befehls **events** akzeptiert werden.

Verwenden Sie den Befehl **events**, um die Konfiguration für Call-Home-Ereignisse anzuzeigen und zu ändern. Für jeden vom IMM2 generierten Ereignistyp gibt es eine eindeutige Ereignis-ID. Sie können verhindern, dass bei bestimmten Ereignissen Call-Home-Nachrichten generiert werden, indem Sie sie zur *Ausschlussliste* für Call-Home-Ereignisse hinzufügen. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-add	Ein Call-Home-Ereignis zur Call-Home-Ausschlussliste hinzufügen	Ereignis-ID in der Form <i>0xhhhhhhhhhhhhhhhh</i> .
-rm	Ein Call-Home-Ereignis aus der Call-Home-Ausschlussliste entfernen	Ereignis-ID in der Form <i>0xhhhhhhhhhhhhhhhh</i> oder <i>alle</i> .

Syntax:

events -che [*Optionen*]

Option:

-add *Ereignis-ID*

-rm *Ereignis-ID*

Befehl "sdemail"

Verwenden Sie den Befehl **sdemail**, um Serviceinformationen per E-Mail zu versenden. Mit dem Befehl **sdemail** wird eine E-Mail mit dem IMM2-Serviceprotokoll als Anhang an den angegebenen Empfänger gesendet.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Option	Beschreibung	Werte
-to	Informationen zum Empfänger (<i>erforderliche Option</i>)	E-Mail-Adresse des Empfängers: • Mehrere Adressen werden im Format <code>userid1@hostname1,userid2@hostname2</code> (höchstens 119 Zeichen) durch Kommas voneinander getrennt. • Die Benutzer-ID kann aus alphanumerischen Zeichen und den Zeichen '.', '-' oder '_' bestehen; sie muss jedoch mit alphanumerischen Zeichen beginnen und enden. • Der Hostname kann aus alphanumerischen Zeichen und den Zeichen '.', '-' oder '_' bestehen. Er muss zwei Domänenelemente enthalten. Jedes Domänenelement sollte mit alphanumerischen Zeichen beginnen und enden. Das letzte Domänenelement sollte aus 2 bis 20 alphabetischen Zeichen bestehen
-subj	E-Mail-Betreff	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 119 Zeichen)

Syntax:

`sddemail [Optionen]`

Option:

-to *Informationen_zum_Empfänger*

-subj *Betreff*

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 Einheits-treiber 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. Fehlermeldungen 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 Fehlermeldungen 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, Online-dokumente, 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 Einheitsreiber oder andere Software benötigen. IBM verwaltet Seiten im World Wide Web, über die Sie nach den neuesten technischen Informationen suchen und Einheitsreiber 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 auf **Business Partner Locator**. 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.

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Kontaktinformationen für den IBM Produktservice in Taiwan:

IBM Taiwan 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 1.000.000.000 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 12. Grenzwerte für Staubpartikel und Gase

Verunreinigung	Grenzwerte
Staubpartikel	- Die Raumluft muss kontinuierlich mit einem Wirkungsgrad von 40 % gegenüber atmosphärischem Staub (MERV 9) nach ASHRAE-Norm 52.2¹ 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 % betragen². - Im Raum dürfen keine elektrisch leitenden Verunreinigungen wie Zink-Whisker vorhanden sein.
Gase	- Kupfer: Klasse G1 gemäß ANSI/ISA 71.04-1985³ - Silber: Korrosionsrate von weniger als 300 Å in 30 Tagen
¹ ASHRAE 52.2-2008 - <i>Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size</i>. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. ² Die relative hygroskopische Feuchtigkeit der Verunreinigung durch Staubpartikel ist die relative Feuchtigkeit, bei der der Staub genug Wasser absorbiert, um nass zu werden und Ionen leiten zu können. ³ ANSI/ISA-71.04-1985. <i>Environmental conditions for process measurement and control systems: Airborne contaminants</i>. 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 Standards für Barrierefreiheit. Falls beim Verwenden der PDF-Dateien Probleme auftreten und Sie ein webbasiertes Format oder ein barrierefreies 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.

Gesetzliche Bestimmungen 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, Germany
Tele: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@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 Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV-Vorschriften ist der Hersteller:

International Business Machines Corp. New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Deutschland
Telefon: +49 (0) 800 225 5423 oder +49 (0) 180 331 3233
E-Mail: halloibm@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 전자파적합기기로서
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

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Index

Sonderzeichen

- "Problems", Option
 - Services and Support 37
- "Settings", Option
 - Services and Support 40

A

- Absolute Maussteuerung 135
- Active Directory-Benutzer
 - LDAP 73, 256
- Active Energy Manager
 - Option "Power Management" 159
 - Registerkarte "Policies" 159, 161
 - Stromverbrauchssteuerung 159, 161
- ActiveX-Applet
 - aktualisieren 130
- Adapterkonfiguration
 - Registerkarte "Server Management" 177
- Advanced Level-Funktionen 3
- Aktionen
 - Partitionen 169
- Aktivierungsschlüssel
 - entfernen 182, 225
 - exportieren 183
 - installieren 179, 225
 - verwalten 74, 225
- Aktualisieren
 - ActiveX-Applet 130
 - Java-Applet 130
- Aktuelle anzeigen
 - Benutzer 72, 256
- Alphabetische Befehlsliste 188
- Anmeldeberechtigungsattribut
 - LDAP 73, 226
- Anmeldung, global
 - Einstellungen 85
- Anmeldung am IMM2 12
- Ansichtsmodi in Fernsteuerung 132
- Ansprechpartner für SNMPv1
 - festlegen 72, 244
- Ansprechpartner für SNMPv3
 - festlegen 72, 244
- Anzeigen
 - Hardwarezustand 123
 - Systemstatus 119
 - Systemzustand 122
- Anzeigen und Verwalten
 - Partitionen im skalierbaren Komplex 166
- Arbeiten mit
 - Ereignissen im Ereignisprotokoll 32
- Ausführen
 - IMM2-Tasks 127
- Australia Class A statement 281
- Automatische Vereinbarung
 - festlegen 72, 222

B

- Barrierefreie Dokumentation 280
- Baseboard Management Controller (BMC) 1
- Basic Level-Funktionen 3
- Befehl "accsecfg" 209
- Befehl "adapter" 191
- Befehl "alertcfg" 211
- Befehl "alertentries" 260
- Befehl "asu" 212
- Befehl "autoftp" 266
- Befehl "autopromo" 215
- Befehl "backup" 216
- Befehl "batch" 263
- Befehl "chconfig" 267
- Befehl "chlog" 269
- Befehl "chmanual" 269
- Befehl "clearcfg" 264
- Befehl "clearlog" 193
- Befehl "clock" 264
- Befehl "console" 208
- Befehl "cryptomode" 217
- Befehl "dhcpcinfo" 218
- Befehl "dns" 219
- Befehl "ethtousb" 220
- Befehl "events" 270
- Befehl "exit" 190
- Befehl "fans" 193
- Befehl "ffdc" 193
- Befehl "fuelg" 203
- Befehl "gprofile" 221
- Befehl "help" 190
- Befehl "history" 190
- Befehl "identify" 265
- Befehl "ifconfig" 222
- Befehl "info" 265
- Befehl "keycfg" 225
- Befehl "ldap" 226
- Befehl "led" 194
- Befehl "ntp" 228
- Befehl "passwordcfg" 228
- Befehl "portcfg" 230
- Befehl "portcontrol" 231
- Befehl "ports" 229
- Befehl "power" 204
- Befehl "pxeboot" 207
- Befehl "readlog" 196
- Befehl "reset" 207
- Befehl "resetsp" 266
- Befehl "restore" 232
- Befehl "restoredefaults" 232
- Befehl "scale" 233
- Befehl "sdemail" 270
- Befehl "set" 243
- Befehl "smtp" 243
- Befehl "snmp" 244
- Befehl "snmpalerts" 247
- Befehl "spreset" 266
- Befehl "srcfg" 248
- Befehl "sshcfcg" 249
- Befehl "ssl" 250
- Befehl "sslcfg" 251
- Befehl "storage" 197
 - Speichereinheiten 197
- Befehl "syshealth" 201
- Befehl "telnetcfg" 254
- Befehl "temps" 201
- Befehl "thermal" 255
- Befehl "timeouts" 255
- Befehl "usbeth" 256
- Befehl "users" 256
- Befehl "volts" 202
- Befehl "vpd" 202
- Befehl zur seriellen Umleitung 208
- Befehle
 - accsecfg 209
 - adapter 191
 - alertcfg 211
 - alertentries 260
 - asu 212
 - autoftp 266
 - autopromo 215
 - backup 216
 - batch 263
 - chconfig 267
 - chlog 269
 - chmanual 269
 - clearcfg 264
 - clearlog 193
 - clock 264
 - console 208
 - cryptomode 217
 - dhcpcinfo 218
 - dns 219
 - Ereignisse 270
 - ethtousb 220
 - exit 190
 - fans 193
 - ffdc 193
 - fuelg 203
 - gprofile 221
 - help 190
 - history 190
 - identify 265
 - ifconfig 222
 - info 265
 - keycfg 225
 - ldap 226
 - led 194
 - ntp 228
 - passwordcfg 228
 - portcfg 230
 - portcontrol 231
 - ports 229
 - power 204
 - pxeboot 207
 - readlog 196
 - reset 207
 - resetsp 266
 - restore 232
 - restoredefaults 232
 - scale 233

- Befehle (*Forts.*)
 - sdemail 270
 - set 243
 - smtp 243
 - snmp 244
 - snmpalerts 247
 - spreset 266
 - srcfg 248
 - sshcfg 249
 - ssl 250
 - sslcfg 251
 - storage 197
 - syshealth 201
 - telnetcfg 254
 - temps 201
 - thermal 255
 - timeouts 255
 - TLS 254
 - usbeth 256
 - users 256
 - volts 202
 - vpd 202
 - Befehle, alphabetische Liste 188
 - Befehle, Typen
 - Dienstprogramm 190
 - IMM2-Steuerung 260
 - Konfiguration 208
 - serielle Umleitung 208
 - Serverstromversorgung und Neustart 203
 - Service Advisor 266
 - Überwachung 191
 - Befehlszeilenschnittstelle (CLI - command-line interface)
 - Anmeldung 186
 - Befehlssyntax 187
 - Beschreibung 185
 - Merkmale und Einschränkungen 187
 - Zugriff 186
 - Bemerkungen 277
 - elektromagnetische Verträglichkeit 281
 - FCC, Class A 281
 - Bemerkungen und Hinweise 7
 - Benutzer
 - aktuelle anzeigen 72, 256
 - Kennwort 72, 256
 - löschen 72, 256
 - SNMPv3-Einstellungen 72, 256
 - SSH-Schlüssel 72, 256
 - verwalten 72, 256
 - Benutzerauthentifizierungsverfahren
 - festlegen 72, 209
 - Benutzerdefinierte Unterstützungswebseite 275
 - Benutzerkonten
 - konfigurieren 80
 - Benutzerkonto
 - erstellen 72, 256
 - Gruppenprofil 84
 - Verwaltung 81
 - Beschreibung
 - Partitionsfehler 171
 - Betriebssystem, Voraussetzungen 4
 - Bindungsmethode
 - LDAP-Server 73, 226
 - BIOS (Basic Input/Output System) 1
 - Blade-Server 1, 4, 9
 - BladeCenter 1, 4, 9
 - Booten, über Fernzugriff 141
 - Browservoraussetzungen 4
- ## C
- Canada Class A electronic emission statement 281
 - China Class A electronic emission statement 284
 - CIM-over-HTTP-Port
 - festlegen 74, 229
 - CIM over HTTPS
 - Sicherheit 74, 250, 251
 - Zertifikatsverwaltung 74, 250, 251
 - CIM-over-HTTPS-Port
 - festlegen 74, 229
 - Class A electronic emission notice 281
- ## D
- Daten der Betriebssystem-Fehleranzeige
 - erfassen 158
 - Daten für Service und Support
 - erfassen 157
 - herunterladen 157
 - Daten für Service und Support erfassen 157
 - Datenträger, fern 141
 - Datum
 - festlegen 71, 264
 - Datum und Uhrzeit, IMM2
 - einstellen 77
 - DDNS
 - benutzerdefinierter Domänenname 73, 219
 - konfigurieren 73, 219
 - Quelle für Domännennamen 73, 219
 - verwalten 73, 219
 - vom DHCP-Server angegebener Domänenname 73, 219
 - Definierter Name, Client
 - LDAP-Server 73, 226
 - Definierter Name, Stammeintrag
 - LDAP-Server 73, 226
 - Definierter Name des Clients
 - LDAP-Server 73, 226
 - Definierter Name für den Stammeintrag
 - LDAP-Server 73, 226
 - Deutschland, Hinweis zur Klasse A 282
 - Dienstprogramm für erweiterte Einstellungen 1
 - Dienstprogrammbefehle 190
 - DNS
 - IPv4-Adressierung 73, 219
 - IPv6-Adressierung 73, 219
 - konfigurieren 73, 219
 - LDAP-Server 73, 226
 - Serveradressierung 73, 219
 - Dokumentation
 - Format 280
 - verwenden 274
 - Domänenname, benutzerdefiniert
 - DDNS 73, 219
 - Domänenname, vom DHCP-Server angegeben
 - DDNS 73, 219
 - Download Service Data
 - Option, Übersicht 44
 - Registerkarte "Services and Support" 37
 - DSA, Senden von Daten an IBM 274
- ## E
- E-Mail-Empfänger
 - konfigurieren 35
 - Einstellen
 - Datum und Uhrzeit für IMM2 77
 - Einstellung
 - IMM2-Firmware, automatisierte Hochstufung 76
 - Einstellungen
 - Anmeldung, global 85
 - Registerkarte "Account Security Level" 87
 - Registerkarte "General" 85
 - CIM over HTTPS 107
 - DDNS 96
 - DNS 95
 - erweitert 91
 - Ethernet 91
 - für die Websitzung 21
 - HTTPS 106
 - LDAP 97
 - Portzuordnungen 104
 - Protokoll für LDAP-Client 108
 - Registerkarte "Services and Support" 37
 - Sicherheit 105
 - SMTP 96
 - SNMP-Alert 93
 - SSH-Server 110
 - Telnet 103
 - USB 103
 - Verschlüsselungsverwaltung 113
 - Einzelcursormodus 136
 - Electronic emission Class A notice 281
 - Entfernen
 - Aktivierungsschlüssel 182, 225
 - entfernen, wiederherstellen
 - Partition 169
 - Ereignis
 - Protokoll 149
 - Ereignis-ID
 - Problemliste 37
 - Ereignisbenachrichtigung 35
 - Ereignisempfänger 35
 - verwalten 149
 - Ereignisprotokoll 32
 - verwalten 149
 - Ereignisse
 - Empfänger 151
 - Erfassung der Betriebssystemanzeigen 131
 - Erfassung der Systemabsturzanzeige 131
 - Erneut starten
 - IMM 266
 - IMM2 74
 - Erstellen
 - Benutzerkonto 72, 256

- Erstellen (*Forts.*)
 - E-Mail-Benachrichtigung 151
 - syslog-Benachrichtigung 151
- Erstellen einer personalisierten Unterstützungswebseite 275
- Erweiterte rollenbasierte Sicherheit
 - LDAP 73, 256
- Erweitertes Managementmodul 1, 4, 9
- Ethernet
 - konfigurieren 72, 222
- Ethernet, erweitert
 - Einstellungen 91
- Ethernet-über-USB
 - konfigurieren 73, 220
 - Portweiterleitung 73, 220
- European Union EMC Directive conformance statement 282
- Exportieren
 - Aktivierungsschlüssel 183

F

- FCC Class A notice 281
- Features on Demand 179
 - Funktion entfernen 182, 225
 - Funktion exportieren 183
 - Funktion installieren 179, 225
 - verwalten 74, 225
- Fehler
 - Registerkarte "Services and Support" 37
- Ferne Datenträgerkarte 142
- Ferner Datenträger 141, 142
- Fernsteuerung
 - absolute Maussteuerung 135
 - Anzeigenerfassung 131
 - beenden 143
 - Befehle für Stromversorgung und Neustart 137
 - Einzelcursormodus 136
 - Leistungsstatistiken 137
 - Mausunterstützung 135
 - relative Maussteuerung 135
 - relative Maussteuerung für Linux (Linux-Standardbeschleunigung) 135
 - Tastaturdurchgriffsmodus 135
 - Tastaturunterstützung 133
 - Unterstützung für internationale Tastatur 135
 - Video Viewer 130, 132, 133
 - Virtual Media Session 130, 141
 - zugreifen 142
- Fernsteuerung, Fenster
 - Video Viewer 51
 - Virtual Media Session 51
- Fernsteuerung der Stromversorgung 137
- Fernsteuerungsfunktion 51, 130
- Fernsteuerungsport
 - festlegen 74, 229
- Fernzugriff 2
- Festlegen
 - Ansprechpartner für SNMPv1 72, 244
 - Ansprechpartner für SNMPv3 72, 244
 - automatische Vereinbarung 72, 222

- Festlegen (*Forts.*)
 - Benutzerauthifizierungsverfahren 72, 209
 - CIM-over-HTTP-Port 74, 229
 - CIM-over-HTTPS-Port 74, 229
 - Datum 71, 264
 - Fernsteuerungsport 74, 229
 - größte zu übertragende Einheit 72, 222
 - Hostname 72, 222
 - HTTP-Port 74, 229
 - HTTPS-Port 74, 229
 - Inaktivitätszeitlimit für das Web 72, 209
 - LDAP-Server-Port 73, 226
 - MTU 72, 222
 - SNMP-Agenten-Port 74, 229
 - SNMP-Traps-Port 74, 229
 - SSH-CLI-Port 74, 229
 - Tastenkombination für Befehlszeilenschnittstelle 72, 230
 - Telnet-CLI-Port 74, 229
 - Uhrzeit 71, 264
 - VLAN-Aktivierung 72
- Firewalls und Proxy-Server
 - IBM Systems Director 43
- Firmware
 - Server anzeigen 71, 202
- Firmware, automatisierte Hochstufung, IMM2
 - Einstellung 76
- Firmware, Server
 - aktualisieren 144
- Firmware aktualisieren 130
- Firmwaredaten anzeigen
 - Server 71, 202
- FoD 179
 - Funktion entfernen 182, 225
 - Funktion exportieren 183
 - Funktion installieren 179, 225
 - verwalten 74, 225
- Funktion
 - Anklopfen 137
 - ferne Datenträgerkarte 142
- Funktion "Anklopfen"
 - aktivieren 137
 - Benutzermodus
 - Einzelbenutzer 137
 - Mehrbenutzer 137
 - ferne Sitzung anfordern 137
- Funktion entfernen
 - Features on Demand 182, 225
 - FoD 182, 225
- Funktion exportieren
 - Features on Demand 183
 - FoD 183
- Funktion installieren
 - Features on Demand 179, 225
 - FoD 179, 225

G

- Gase, Verunreinigung 279
- Gesetzliche Bestimmungen zur Telekommunikation 281

- Globale Anmeldeeinstellungen
 - Registerkarte "Account Security Level" 87
 - Registerkarte "General" 85
- Größe zu übertragende Einheit festlegen 72, 222
- Gruppe löschen
 - aktivieren, inaktivieren 221
- Gruppenfilter
 - LDAP 73, 226
- Gruppenprofil
 - Verwaltung 84
- Gruppensuchattribut
 - LDAP 73, 226

H

- Handhabung von Zertifikaten
 - CIM over HTTPS 107
 - sicherer LDAP-Client 108
- Hardwarezustand 123
- Hilfe
 - im World Wide Web 274
 - Quellen 273
 - Senden von Diagnosedaten an IBM 274
- Hinweise, wichtige 278
- Hostname
 - festlegen 72, 222
 - LDAP-Server 73, 226
 - SMTP-Server 73, 243
- HTTP-Port
 - festlegen 74, 229
- HTTPS-Port
 - festlegen 74, 229
- HTTPS-Server
 - Sicherheit 74, 250, 251
 - Zertifikatsverwaltung 74, 250, 251

I

- IBM Blade-Server 1, 4, 9
- IBM BladeCenter 1, 4, 9
- IBM Produktservice in Taiwan 276
- IBM Systems Director
 - Firewalls und Proxy-Server 43
 - Systemmanagementtool 43
- IMM
 - erneut starten 266
 - Konfiguration wiederherstellen 232
 - Konfiguration zurücksetzen 232
 - konfigurieren 74
 - spreset 266
 - Standardkonfiguration 232
 - zurücksetzen 266
- IMM-Verwaltung
 - Aktivierungsschlüsselverwaltung 118
 - Benutzer
 - Gruppenprofile 84
 - Konten 81
 - Benutzerkonten konfigurieren 80
 - IMM-Eigenschaften
 - Einstellungen für den seriellen Anschluss 79

- IMM-Verwaltung (*Forts.*)
 - IMM-Konfiguration
 - IMM-Konfiguration wiederherstellen und ändern 115
 - IMM2 erneut starten 116
 - Netzprotokoll konfigurieren 90
 - Sicherheitseinstellungen 105
- IMM2
 - Aktionsbeschreibungen 13
 - Aktivierungsschlüsselverwaltung 118
 - Beschreibung 1
 - erneut starten 74, 116
 - Funktionen 2
 - IMM2 Advanced Level 2
 - IMM2 Basic Level 2
 - IMM2 Standard Level 2
 - Konfiguration anzeigen 74
 - Konfiguration sichern 74
 - Konfiguration wiederherstellen 74
 - Konfiguration zurücksetzen 74
 - Konfigurationsansicht 74
 - Konfigurationsassistent 74
 - Konfigurationsoptionen 71
 - Konfigurationssicherung 74
 - Konfigurationswiederherstellung 74, 232
 - Netzverbindung 10
 - neue Funktionen 1
 - serielle Umleitung 186
 - Sicherungsstatus anzeigen 74
 - Sicherungsstatusansicht 74
 - Standardkonfiguration 74
 - Übersicht über die Webbenutzerschnittstelle 21
 - Webschnittstelle 9
 - Wiederherstellungsstatus anzeigen 74
 - Wiederherstellungsstatusansicht 74
 - zurücksetzen 74, 117
- 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 71
- IMM2-Steuerbefehle 260
- IMM2-Tasks 127
- IMM2-Verwaltung
 - IMM-Eigenschaften
 - Datum und Uhrzeit 77
 - Firmware, automatisierte Hochstufung 76
 - IMM2 zurücksetzen 117
- IMM2-Webbenutzerschnittstelle
 - Registerkarte "Events"
 - Übersicht über die Optionen 32
 - Registerkarte "Service and Support"
 - Übersicht über Optionen 37
 - Registerkarte "System Status"
 - Übersicht 25
 - Übersicht 21
- IMM2-Websitzung
 - abmelden 24

- Inaktivitätszeitlimit für das Web festlegen 72, 209
- Information Center 274
- Installieren
 - Aktivierungsschlüssel 179, 225
- Installierte Netzteile
 - Registerkarte "Power Modules" 164
- IP-Adresse
 - IPv4 9
 - IPv6 9
 - konfigurieren 9
 - LDAP-Server 73, 226
 - SMTP-Server 73, 243
- IP-Adresse, statischer Standard 10
- IPMI
 - ferne Serververwaltung 185
- IPMItool 185
- IPv4
 - konfigurieren 72, 222
- IPv4-Adressierung
 - DNS 73, 219
- IPv6 9
 - konfigurieren 72, 222
- IPv6-Adressierung
 - DNS 73, 219

J

- Japan Class A electronic emission statement 283
- Java 4, 141
- Java-Applet
 - aktualisieren 130

K

- Kapazität
 - Stromversorgung 165
- Kennwort
 - Benutzer 72, 256
 - LDAP-Server 73, 226
- Konfiguration anzeigen
 - IMM2 74
- Konfiguration des lokalen Speichers
 - Registerkarte "Server Management" 171, 172, 176
- Konfiguration sichern
 - IMM2 74
- Konfiguration wiederherstellen
 - IMM2 74, 232
- Konfiguration zurücksetzen
 - IMM 232
 - IMM2 74
- Konfigurationsansicht
 - IMM2 74
- Konfigurationsassistent
 - IMM2 74
- Konfigurationsbefehle 208
- Konfigurationssicherung
 - IMM2 74
- Konfigurationswiederherstellung
 - IMM2 74, 232
- Konfigurationszusammenfassung anzeigen 13
- Konfigurieren
 - Alertempfänger 35

Konfigurieren (*Forts.*)

- bis zu vier Netzteile 161
- bis zu zwei Netzteile 159
- CIM-over-HTTPS-Protokoll 107
- DDNS 73, 219
- DDNS-Einstellungen 96
- DNS 73, 219
- DNS-Einstellungen 95
- Einstellungen für SNMP-Alerts 93
- Ethernet 72, 222
- Ethernet-Einstellungen 91
- Ethernet-über-USB 73, 220
- globale Anmeldeeinstellungen 85
- HTTPS-Protokoll 106
- IMM2 74
- IPv4 72, 222
- IPv6 72, 222
- LDAP 73, 226
- LDAP-Einstellungen 97
- LDAP-Server 73, 226
- Netzprotokolle 90
- Netzserviceport 231
- Ports 74, 229
- Portzuordnungen 104
- Protokoll für LDAP-Client 108
- Seriell-zu-SSH-Umleitung 186
- Seriell-zu-Telnet-Umleitung 186
- serieller Anschluss 72, 79, 230
- Sicherheit 74
- Sicherheitseinstellungen 105
- Sicherheitsstufen für Benutzerkonten 72, 209
- SMTP 73, 243
- SMTP-Einstellungen 96
- SNMPv1 72, 244
- SNMPv1-Traps 72, 244
- SNMPv3-Benutzerkonten 72, 256
- SSH-Server 110
- Telnet 254
- Telnet-Einstellungen 73, 103
- USB 73, 220
- USB-Einstellungen 103
- Verschlüsselungsverwaltung 113

Korea Class A electronic emission statement 283

L

- Laufwerke
 - zuordnen 142
 - Zuordnung aufheben 142
- Laufwerke zuordnen 142
- Laufwerkzuordnung aufheben 142
- LDAP
 - Active Directory-Benutzer 73, 256
 - Anmeldeberechtigungsattribut 73, 226
 - erweiterte rollenbasierte Sicherheit 73, 256
 - Gruppenfilter 73, 226
 - Gruppensuchattribut 73, 226
 - konfigurieren 73, 226
 - rollenbasierte Sicherheit, erweitert 73, 256
 - Sicherheit 74, 250, 251
 - Zertifikatsverwaltung 74, 250, 251
 - Zielname des Servers 73, 226

LDAP-Server
 Bindungsmethode 73, 226
 definierter Name des Clients 73, 226
 definierter Name für den Stammeintrag 73, 226
 DNS 73, 226
 Hostname 73, 226
 IP-Adresse 73, 226
 Kennwort 73, 226
 konfigurieren 73, 226
 Portnummer 73, 226
 Suchdomäne 73, 226
 UID-Suchattribut 73, 226
 vorkonfiguriert 73, 226
 LDAP-Server-Port
 festlegen 73, 226
 Logisch
 Speicherpools 171, 176
 Löschen
 Benutzer 72, 256
 E-Mail-Benachrichtigung 151
 syslog-Benachrichtigung 151

M

MAC-Adresse
 verwalten 72, 222
 Marken 277
 Maussteuerung
 absolute 135
 relative 135
 relative mit Linux-Standardbeschleunigung 135
 Mausunterstützung in Fernsteuerung 135
 Mausunterstützung per Fernsteuerung 135
 Maximale Anzahl an Sitzungen
 Telnet 73, 254
 Menü "Events" 149
 Mindeststufen
 TLS 254
 Modus zum Ändern einer Partition
 skalierbarer Komplex 169
 MTU
 festlegen 72, 222

N

Netzprotokolleigenschaften
 DDNS 96
 DNS 95
 Einstellungen für SNMP-Alerts 93
 Ethernet-Einstellungen 91
 LDAP 97
 Portzuordnungen 104
 SMTP 96
 Telnet 103
 USB 103
 Netzserviceport
 konfigurieren 231
 Netzverbindung 10
 IP-Adresse, statischer Standard 10
 statische IP-Adresse, Standard 10
 statische Standard-IP-Adresse 10
 New Zealand Class A statement 281

Nicht zugeordnete Knoten
 skalierbarer Komplex 166

O

Offene Ports anzeigen 74, 229
 Onlineveröffentlichungen
 Informationen zu Dokumentationsaktualisierungen 1
 Informationen zu Fehlercodes 1
 Informationen zu Firmwareaktualisierungen 1
 Option "Adapters"
 Registerkarte "Server Management" 67
 Serververwaltung 177
 Option "Cooling Devices"
 auf der Registerkarte "Server Management" 61
 Option "Latest OS Failure Screen"
 auf der Registerkarte "Server Management" 68
 Option "Local Storage"
 Registerkarte "Server Management" 64
 Serververwaltung 171, 172, 176
 Option "Memory"
 auf der Registerkarte "Server Management" 64
 Option "Page Auto Refresh" 21
 Option "Power Management"
 Active Energy Manager 159
 Registerkarte "Chart" 165
 Registerkarte "Policies" 159
 Registerkarte "Power Allocation" 165
 Registerkarte "Power History" 165
 Registerkarte "Power Modules" 164
 Registerkarte "Server Management" 159
 Option "Power Modules"
 auf der Registerkarte "Server Management" 62
 Option "Processors"
 auf der Registerkarte "Server Management" 66
 Option "PXE Network Boot"
 auf der Registerkarte "Server Management" 68
 Option "Server Firmware"
 auf der Registerkarte "Server Management" 46
 Option "Server Power Actions"
 auf der Registerkarte "Server Management" 61
 Option "Server Properties"
 auf der Registerkarte "Server Management" 56
 Option "Server Timeouts"
 auf der Registerkarte "Server Management" 67
 Option "Trespass Message" 23
 Optionen
 Registerkarte "IMM Management" 70
 Optionen auf
 Registerkarte "Server Management" 45

P

Partition
 Aktionen 169
 Standalone aktivieren
 entfernen, wiederherstellen 169
 Partition entfernen, Modus
 skalierbarer Komplex 170
 Partition erstellen
 skalierbarer Komplex 167
 Partition löschen
 skalierbarer Komplex 170
 Partitionen
 skalierbarer Komplex 166, 167
 Partitionsfehler
 Beschreibung 171
 skalierbarer Komplex 171
 People's Republic of China Class A electronic emission statement 284
 Physisch
 Speicherpools 171, 172
 Portnummer
 LDAP-Server 73, 226
 SMTP-Server 73, 243
 Portnummern
 festlegen 74, 229
 Portnummern festlegen 74, 229
 Ports
 konfigurieren 74, 229
 Nummern festlegen 74, 229
 offene anzeigen 74, 229
 Portweiterleitung
 Ethernet-über-USB 73, 220
 Problemliste
 Ereignis-ID 37
 Produktservice, IBM Taiwan 276
 PXE Boot Agent 13
 PXE-Netzboot
 einrichten 143

Q

Quelle für Domännennamen
 DDNS 73, 219

R

RDOC 142
 Registerkarte "Chart"
 Option "Power Management" 165
 Registerkarte "Power History" 165
 Registerkarte "Events"
 Protokoll 32
 Übersicht 32
 Registerkarte "IMM Management" 70
 Registerkarte "Power Allocation"
 Option "Power Management" 165
 Registerkarte "Power Modules"
 Installierte Netzteile 164
 Option "Power Management" 164
 Registerkarte "Server Management" 45
 Adapterkonfiguration 177
 Konfiguration des lokalen Speichers 171, 172, 176
 Option "Adapters" 67
 Option "Local Storage" 64
 Option "Power Management" 159

- Registerkarte "Server Management" (Forts.)
 - skalierbarer Komplex 69
- Registerkarte "Service and Support"
 - Übersicht 37
- Registerkarte "Services and Support"
 - Download Service Data 37
 - Einstellungen 37
 - Fehler 37
- Registerkarte "System Status"
 - Übersicht 25
- Relative Maussteuerung 135
- Relative Maussteuerung für Linux (Linux-Standardbeschleunigung) 135
- Remote Desktop Protocol (RDP)
 - Start 137
- Remote-Presence-Funktion 130
 - aktivieren 131
- Remote Supervisor Adapter II 1
- Rollenbasierte Sicherheit, erweitert
 - LDAP 73, 256
- Rollenbasierte Stufen
 - operator 221
 - rbs 221
 - supervisor 221
- Russia Class A electronic emission statement 284

S

- Seite "System Status", Übersicht 25
- Senden von Diagnosedaten an IBM 274
- Serial over LAN 185
- Seriell-zu-SSH-Umleitung 186
- Seriell-zu-Telnet-Umleitung 186
- Serieller Anschluss
 - konfigurieren 72, 79, 230
- Server-Firmware
 - aktualisieren 144
- Server-Firmware für IBM System x
 - Beschreibung 1
 - Konfigurationsdienstprogramm 10
- Server Management
 - Option "Latest OS Failure Screen" 68
 - Option "Memory" 64
 - Option "Power Modules" 62
 - Option "Processors" 66
 - Option "PXE Network Boot" 68
 - Option "Server Firmware" 46
 - Option "Server Power Actions" 61
 - Option "Server Properties" 56
 - Option "Server Timeouts" 67
 - Option für Kühlungseinheiten des Servers 61
- Server Management (Serververwaltung)
 - Stromverbrauchssteuerung 69
- Server Properties
 - Registerkarte "Environmentals" 56
 - Registerkarte "General Settings" 56
 - Registerkarte "Hardware Activity" 56
 - Registerkarte "Hardware Information"
 - Registerkarte "Network Hardware" 56
 - Registerkarte "System Component Information" 56
 - Registerkarte "System Information" 56
- Server Properties (Forts.)
 - Registerkarte "LED" 56
- Serveradressierung
 - DNS 73, 219
- Serverstatus
 - überwachen 119
- Serverstatus überwachen 119
- Serverstromversorgung
 - steuern 128
- Serverstromversorgung und Neustart
 - Befehle 203
- Serververwaltung
 - Daten der Betriebssystem-Fehleranzeige 158
 - Option "Adapters" 177
 - Option "Local Storage" 171, 172, 176
 - PXE-Netzboot 143
 - Server-Firmware 144
 - Serverzeitlimits, festlegen 74
- Serverzeitlimit
 - Optionen 74
- Serverzeitlimits festlegen 74
- Service Advisor-Befehle 266
- Service und Unterstützung
 - Bevor Sie sich an den Kundendienst wenden 273
 - Hardware 275
 - Software 275
- Services and Support
 - Option, "Problems" 37
 - Option, "Settings" 40
- Sicherheit
 - CIM over HTTPS 74, 250, 251
 - CIM-over-HTTPS-Protokoll 107
 - Handhabung von SSL-Zertifikaten 111
 - HTTPS-Protokoll 106
 - HTTPS-Server 74, 250, 251
 - konfigurieren 74
 - LDAP 74, 250, 251
 - LDAP-Client 108
 - SSH-Server 74, 110, 249
 - Übersicht über SSL 111
 - Verschlüsselungsverwaltung 113
 - Verwaltung von SSL-Zertifikaten 112
- Sicherheitsstufen für Benutzerkonten
 - konfigurieren 72, 209
- Sicherungsstatus anzeigen
 - IMM 74
- Sicherungsstatusansicht
 - IMM2 74
- Sitzungen, maximale Anzahl
 - Telnet 73, 254
- Skalierbarer Komplex
 - anzeigen 166
 - getrennte Knoten 166
 - Modus zum Ändern einer Partition 169
 - Partition entfernen, Modus 170
 - Partition erstellen 167
 - Partition löschen 170
 - Partitionen 167
 - Partitionsfehler 171
 - Registerkarte "Server Management" 69
 - verwalten 166

- SMTP
 - IP-Adresse des Servers 73, 243
 - konfigurieren 73, 243
 - Server-Hostname 73, 243
 - Server-Portnummer 73, 243
 - testen 73
- SNMP-Agenten-Port
 - festlegen 74, 229
- SNMP-Traps-Port
 - festlegen 74, 229
- SNMPv1
 - konfigurieren 72, 244
- SNMPv1-Communitys
 - verwalten 72, 244
- SNMPv1-Traps
 - konfigurieren 72, 244
- SNMPv3-Benutzerkonten
 - konfigurieren 72, 256
- SNMPv3-Einstellungen
 - Benutzer 72, 256
- Speichereinheiten
 - Befehl "storage" 197
- Speicherpools
 - logisch 176
 - physisch 171
 - physisch 172
- SSH-CLI-Port
 - festlegen 74, 229
- SSH-Schlüssel
 - Benutzer 72, 256
- SSH-Server
 - Sicherheit 74, 249
 - Zertifikatsverwaltung 74, 249
- SSL
 - Handhabung von Zertifikaten 111
 - Zertifikatsverwaltung 112
- Standalone aktivieren
 - Partition 169
- Standardkonfiguration
 - IMM 232
 - IMM2 74
- Startreihenfolge ändern 13
- Startreihenfolge des Host-Servers ändern 13
- Statische IP-Adresse, Standard 10
- Statische Standard-IP-Adresse 10
- Staubpartikel, Verunreinigung 279
- Stromverbrauchssteuerung
 - Active Energy Manager 159, 161
 - auf der Registerkarte "Server Management" 69
 - Registerkarte "Policies" 159, 161
- Stromversorgung
 - Kapazität 165
- Stromversorgungsaktionen 128
 - skalierbarer Komplex 166
- Stromversorgungsstatus steuern des Servers 128
- Suchdomäne
 - LDAP-Server 73, 226
- Systemereignis
 - Benachrichtigung 151
 - Benachrichtigung wiederholen 151
- Systemereignisbenachrichtigung 35
- Systeminformationen 121
 - anzeigen 121

Systemmanagementtool
 IBM Systems Director 43
Systems Director, IBM
 Systemmanagementtool 43
Systemstatus 119
Systemzustand 122

T

Taiwan Class A electronic emission state-
ment 284
Tastaturdurchgriffsmodus in Fernsteue-
rung 135
Tastaturunterstützung in Fernsteue-
rung 133
Tastenkombination für Befehlszeilen-
schnittstelle
 festlegen 72, 230
Telefonnummern 275
Telefonnummern für Hardware-Service
und -unterstützung 275
Telefonnummern für Software-Service
und -unterstützung 275
Telnet
 konfigurieren 254
 maximale Anzahl an Sitzungen 73,
 254
 Zugriff 73, 254
Telnet-CLI-Port
 festlegen 74, 229
Telnet-Einstellungen
 konfigurieren 73
Testen
 SMTP 73
Testereignisse
 generieren 151
TLS
 Mindeststufe 254
TLS-Befehl 254
Tools
 IPMItool 185

U

Übersicht
 Download Service Data 44
 SSL 111
Überwachungsbefehle 191
Uhrzeit
 festlegen 71, 264
UID-Suchattribut
 LDAP-Server 73, 226
United States FCC Class A notice 281
Unterstützung erhalten 273
Unterstützung für internationale Tastatur
in Fernsteuerung 135
Unterstützungswebseite, benutzerdefi-
niert 275
USB
 konfigurieren 73, 220

V

Verunreinigung, Staubpartikel und
Gase 279

Verwalten
 Aktivierungsschlüssel 74, 225
 Benutzer 72, 256
 DDNS 73, 219
 Features on Demand 74, 225
 FoD 74, 225
 MAC-Adresse 72, 222
 SNMPv1-Communitys 72, 244
Verwenden
 ActiveX-Client 51
 Fernsteuerungsfunktion 130
 Java-Client 51
 Remote-Presence-Funktion 130
Video Viewer
 absolute Maussteuerung 135
 Ansichtsmodi 132
 Anzeigenerfassung 131
 beenden 143
 Befehle für Stromversorgung und
 Neustart 137
 Einzelcursormodus 136
 Leistungsstatistiken 137
 Mausunterstützung 135
 relative Maussteuerung 135
 relative Maussteuerung für Linux (Li-
 nux-Standardbeschleunigung) 135
 Tastaturdurchgriffsmodus 135
 Unterstützung für internationale Tas-
 tatur 135
 Videofarbmodus 133
Videofarbmodus in Fernsteuerung 133
Vier Netzteile
 konfigurieren 161
Virtual Light Path 13
Virtual Media Session
 beenden 143
 ferner Datenträger 141
 Laufwerkzuordnung aufheben 142
 Laufwerkzuordnung festlegen 142
 Start 142
VLAN-Aktivierung
 festlegen 72
Von der IMM2-Sitzung abmelden 24
Voraussetzungen
 Betriebssystem 4
 Web-Browser 4
Voraussetzungen, Web-Browser 4
Vorkonfiguriert
 LDAP-Server 73, 226

W

Webschnittstelle
 Anmeldung an der Webschnittstel-
 le 12
Webschnittstelle öffnen und verwen-
den 9
Websitzungseinstellungen 21
Wichtige Hinweise 278
Wiederherstellungstatus anzeigen
 IMM2 74
Wiederherstellungstatusansicht
 IMM2 74

Z

Zertifikatsverwaltung
 CIM over HTTPS 74, 250, 251
 HTTPS-Server 74, 250, 251
 LDAP 74, 250, 251
 SSH-Server 74, 249
Zielname, Server
 LDAP 73, 226
Zielname des Servers
 LDAP 73, 226
Zugeordnete Knoten
 skalierbarer Komplex 166
Zugriff
 Fernsteuerung 142
 Telnet 73, 254
Zurücksetzen
 IMM 266
 IMM2 74
Zwei Netzteile
 konfigurieren 159



Teilenummer: 00FH711

(1P) P/N: 00FH711

