Das Intelligent Platform Management Interface (IPMI) ist eine Sammlung von standardisierten Schnittstellen in Computer-Hardware und Firmware, die benutzt wird, um den Computer zu warten und zu verwalten. Außerdem wird es eingesetzt, um automatische Berichte über auftretende Fehler zu erzeugen.

Installation

Hinweis:

Dieses Howto wurde für openSUSE 11.2 erstellt. Es müsste mit kleinen Abweichungen aber auch für andere Distributionen gültig sein

per YaST folgende Pakete installieren:

- openIPMI (Device-Schnittstelle)
- ipmitool (Um auf die Schnittstelle zuzugreifen)

Ist alles installiert, muss man den Dienst starten

```
/etc/init.d/ipmi start
```

und in den Runlevels eintragen, damit der Dienst bei jedem Start gestartet wird.

Testen

Zu Testzwecken kann man jetzt schon mal einigen Kommandos testen

Einfach in der Konsole folgende Befehle eintragen

Aufruf	**Funktion**
ipmitool chassis status	Zeige Power- und Chassis-Status
ipmitool sensor	Zeige Informationen der Umgebungs-Sensoren (Lüfter, Temperaturen)
ipmitool mc list	Zeige Informationen über BMC (Firmware, Hersteller, ...)

eine Übersicht über weitere Kommandos bekommt man, wenn man nur

```
ipmitool
```

eingibt.

Auslesen über LAN

Vorteil von ipmi ist, dass man die Komponenten nicht nur lokal auslesen kann. Dies funktioniert auch per serieller Schnittstelle und auch per LAN.

Dabei gilt grundsätzlich:

- Kanal 0: Systeminterface
- Kanal 1-…: LAN Interfaces

Da die Rechner aber nicht immer an sind (z.B. Weil Lüfter ausgefallen sind), kann man diese Schnittstellen auch abfragen, wenn der Rechner aus(!) ist.

Konfiguration

Zur Konfiguration reicht es nicht, der Schnittstelle eine IP-Adresse zu geben. Es müssen auch Standardgateway, Userprivilegien und User konfiguriert werden

Schnittstellenkonfiguration

Um die ipmitools über die LAN-Schnittstelle nutzen zu können, muss man den Kanal konfigurieren, der für das Netzwerkinterface zuständig ist

Am Besten man lässt sich per

```
ipmitool channel info 1
```

anzeigen, ob dies der richtige Kanal ist. Wenn nicht, muss man mit dem zweiten Chanel fortsetzen usw..

In meinem Fall ist das LAN-Interface auf Chanel 2

```
[root@ipmisrv ~]# ipmitool lan set 2 ipsrc static
[root@ipmisrv ~]# ipmitool lan set 2 ipaddr <IP-Adresse>
Setting LAN IP Address to <IP-Adresse>
[root@ipmisrv ~]# ipmitool lan set 2 netmask <Netzwerkmaske>
Setting LAN Subnet Mask to <Netzwerkmaske>
[root@ipmisrv ~]# ipmitool lan set 2 defgw ipaddr <IP-Adresse>
Setting LAN Default Gateway IP to <IP-Adresse>
[root@ipmisrv ~]# ipmitool lan set 2 defgw macaddr <MAC-Adresse>
Setting LAN Default Gateway MAC to <MAC-Adresse>
[root@ipmisrv ~]# ipmitool lan set 2 arp respond on
Enabling BMC-generated ARP responses
[root@ipmisrv ~]# ipmitool lan set 2 auth ADMIN MD5
```

Erklärung:

Befehl	Erklärung
ipmitool lan set 2 ipsrc static	Setzen der Netzwerkkarte auf Statische Vergabe der IP-Adresse
ipmitool lan set 2 ipaddr <IP-Adresse>	Setzen der IP-Adresse
ipmitool lan set 2 netmask <Netzwerkmaske>	Setzen der Netzwerkmaske
ipmitool lan set 2 defgw ipaddr <IP-Adresse>	Setzen des Default-Gateways (Standardgateway)
ipmitool lan set 2 defgw macaddr <MAC-Adresse>	
ipmitool lan set 2 arp respond on	Die Schnittstelle darf auf MAC-Adressen-Anfragen antworten
ipmitool lan set 2 auth ADMIN MD5	Nur ADMIN darf auf die Schnittstelle von außen zugreifen. die Passwortverschlüsselung erfolgt über MD5

Zum überprüfen der Einstellungen kann man sich eine Liste anzeigen lassen mit

```
ipmitool lan print 2
```

Die Ausgabe sieht dann ungefähr aus wie diese:

```
Auth Type Support       : NONE MD5 PASSWORD
Auth Type Enable        : Callback : NONE MD5 PASSWORD
                        : User     : NONE MD5 PASSWORD
                        : Operator : NONE MD5 PASSWORD
                        : Admin    : MD5
                        : OEM      : NONE MD5 PASSWORD
IP Address Source       : Static Address
IP Address              : 189.193.30.114
Subnet Mask             : 255.255.255.240
MAC Address             : 00:0a:e4:7e:08:2e
SNMP Community String   : public
BMC ARP Control         : ARP Responses Enabled, Gratuitous ARP Disabled
```

Userkonfiguration

Damit wir jetzt auf die Schnittstelle zugreifen dürfen, müssen wir noch einen User konfigurieren, der die entsprechenden Rechte hat.

```
[root@ipmisrv ~]# ipmitool user set name 2 admin
[root@ipmisrv ~]# ipmitool user set password 2
Password for user 2:
Password for user 2:
[root@ipmisrv ~]# ipmitool channel setaccess 1 2 link=on ipmi=on callin=on
privilege=4
[root@ipmisrv ~]# ipmitool user enable 2
```

Erklärung:

Befehl	Erklärung
ipmitool user set name 2 admin	User Admin erstellen mit der ID-Nummer 2
ipmitool user set password 2	Setzen des Passwortes für Admin
ipmitool channel setaccess 2 2 link=on ipmi=on callin=on privilege=4	Was darf der User? Auf Kanal2 darf der User mit der ID 2 auf ipmi zugreifen... (Privilegien sind in der folgendenen Tabelle aufgeführt)
ipmitool user enable 2	Aktivieren des users

Mögliche Privilegien-levels sind:

Nummer	Was
1	Callback level
2	User level
3	Operator level
4	Administrator level
5	OEM Proprietary level
15	No access

Aufruf

Zum Aufruf muss man nur an einem anderen Rechner ipmitool wie folgt aufrufen. Dabei ist es egal, welches Betriebssystem verwendet wird.

```
ipmitool -I lan -H <IP-Adresse> -U <Username> <Kommando>
```

- **IP-Adresse** ist die Adresse des entfernten Rechners
- Bei **Kommando** muss ein Kommando eingegeben werden, wie es bei der eingabe von ipmitool üblich ist (z.B.: chassis status, sensor status)

Am folgenden Beispiel wird gezeigt, wie ein Server, der heruntergefahren ist, über ipmi angeschaltet wird.

```
[user@ipmiadmin ~]$ ipmitool -I lan -H <IP-Adresse> -U <User> power status
Password:
Chassis Power is off
[user@ipmiadmin ~]$ ipmitool -I lan -H <IP-Adresse> -U <User> -P relation
power on
Chassis Power Control: Up/On
```

Sollte man es leid sein, immer das Passwort eingeben zu müssen, kann man es mit der Option *-P <password>* setzen

Operationen

Kommando	Beschreibung
raw	Send a RAW IPMI request and print response
i2c	Send an I2C Master Write-Read command and print response

Kommando	Beschreibung
spd	Print SPD info from remote I2C device
lan	Configure LAN Channels
chassis	Get chassis status and set power state
power	Shortcut to chassis power commands
event	Send pre-defined events to MC
mc	Management Controller status and global enables
sdr	Print Sensor Data Repository entries and readings
sensor	Print detailed sensor information
fru	Print built-in FRU and scan SDR for FRU locators
sel	Print System Event Log (SEL)
pef	Configure Platform Event Filtering (PEF)
sol	Configure and connect IPMIv2.0 Serial-over-LAN
tsol	Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
isol	Configure IPMIv1.5 Serial-over-LAN
user	Configure Management Controller users
channel	Configure Management Controller channels
session	Print session information
sunoem	OEM Commands for Sun servers
kontronoem	OEM Commands for Kontron devices
picmg	Run a PICMG/ATCA extended cmd
fwum	Update IPMC using Kontron OEM Firmware Update Manager
firewall	Configure Firmware Firewall
shell	Launch interactive IPMI shell
exec	Run list of commands from file
set	Set runtime variable for shell and exec
hpm	Update HPM components using PICMG HPM.1 file
ekanalyzer	run FRU-Ekeying analyzer using FRU files