THOMAS KRENN®

server.hosting.customized.

IPMI Sicherheit – Best Practices

Webinar November 2014, Georg Schönberger

1
2

```
1 $ telnet ipmi.example.com 49152
2 $ GET /PSBlock
```

heise Security

News | Hintergrund | Erste Hilfe

Security > News > 7-Tage-News > 2014 > KW 23 > Hunderttausende Server über Fernwartungsproto

05.06.2014 17:59

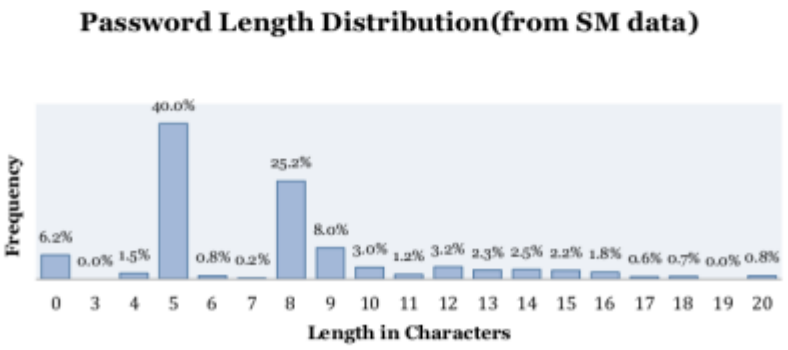
« Vorige | Nächste »

Hunderttausende Server über Fernwartungsprotokolle angreifbar

vorlesen / MP3-Download

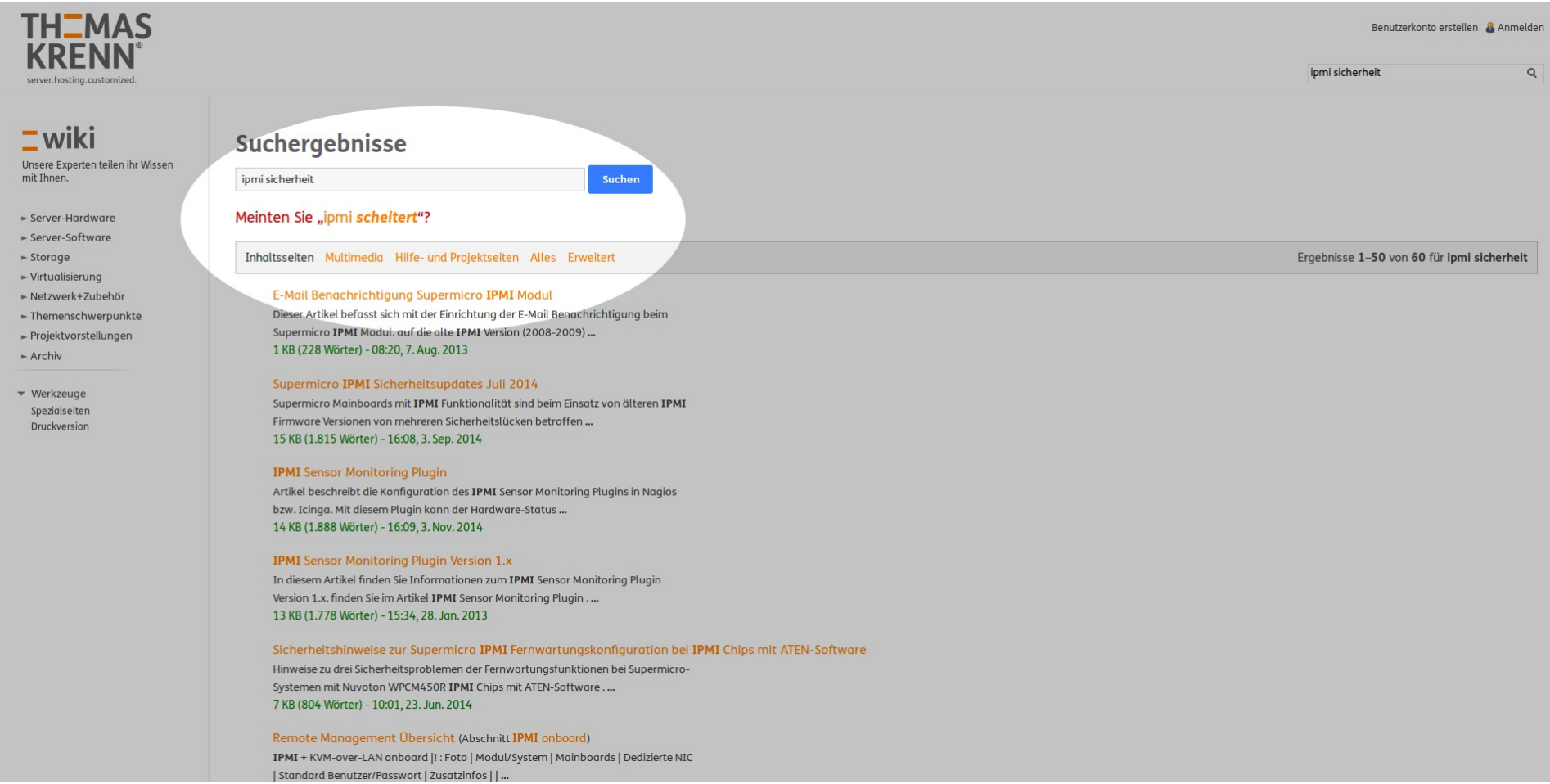
Das Fernwartungsprotokoll IPMI, mit dem Server über die Firmware des Motherboards gewartet werden können, hat gravierende Sicherheitslücken. Forscher haben bei einem Scan des Internets haufenweise Server gefunden, die angreifbar sind.

Sicherheitsforscher Dan Farmer warnt erneut vor den Risiken des Fernwartungsprotokolls IPMI und der Firmware von Baseboard Management Controllern (BMC). Zusammen mit Metasploit-Entwickler HD Moore hat er die Ergebnisse einer Untersuchung (PDF) präsentiert, die über 230.000 Server im Netz entdeckt hat, welche über das Protokoll angegriffen werden können. Mehr als 90 Prozent dieser Server seien leicht zu knacken, sagt Farmer. Die entsprechenden Schwachstellen hatten Moore und Farmer bereits vor einem Jahr angeprangert.



Viele für Fernwartungszugänge verwendete Passwörter sind viel zu kurz

Bild: Dan Farmer

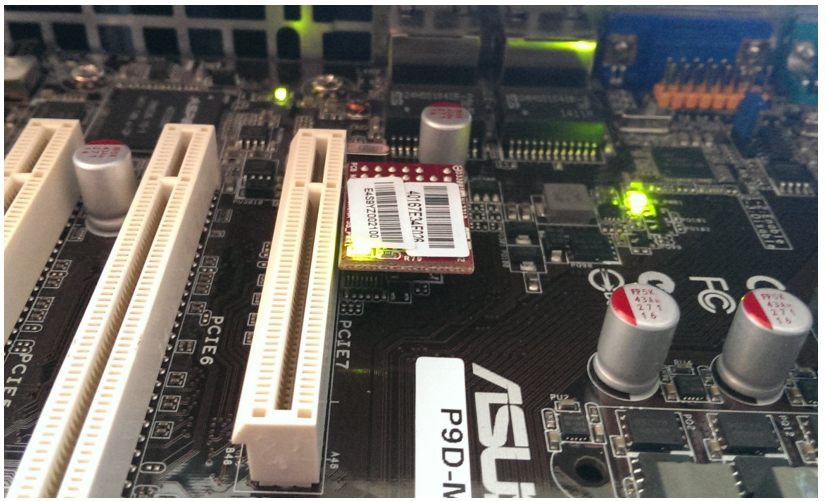

THOMAS KRENN
server.hosting.customized.
Benutzerkonto erstellen
Anmelden
ipmi sicherheit
wiki
Unsere Experten teilen ihr Wissen mit Ihnen.
► Server-Hardware
► Server-Software
► Storage
► Virtualisierung
► Netzwerk+Zubehör
► Themenschwerpunkte
► Projektvorstellungen
► Archiv
Werkzeuge
Spezialseiten
Druckversion
Suchergebnisse
ipmi sicherheit
Suchen
Meinten Sie „ipmi scheitert“?
Inhaltsseiten Multimedia Hilfe- und Projektseiten Alles Erweitert
Ergebnisse 1–50 von 60 für ipmi sicherheit
E-Mail Benachrichtigung Supermicro IPMI Modul
Dieser Artikel befasst sich mit der Einrichtung der E-Mail Benachrichtigung beim Supermicro IPMI Modul. auf die alte IPMI Version (2008-2009) ...
1 KB (228 Wörter) - 08:20, 7. Aug. 2013
Supermicro IPMI Sicherheitsupdates Juli 2014
Supermicro Mainboards mit IPMI Funktionalität sind beim Einsatz von älteren IPMI Firmware Versionen von mehreren Sicherheitslücken betroffen ...
15 KB (1.815 Wörter) - 16:08, 3. Sep. 2014
IPMI Sensor Monitoring Plugin
Artikel beschreibt die Konfiguration des IPMI Sensor Monitoring Plugins in Nagios bzw. Icinga. Mit diesem Plugin kann der Hardware-Status ...
14 KB (1.888 Wörter) - 16:09, 3. Nov. 2014
IPMI Sensor Monitoring Plugin Version 1.x
In diesem Artikel finden Sie Informationen zum IPMI Sensor Monitoring Plugin Version 1.x. finden Sie im Artikel IPMI Sensor Monitoring Plugin . ...
13 KB (1.778 Wörter) - 15:34, 28. Jan. 2013
Sicherheitshinweise zur Supermicro IPMI Fernwartungskonfiguration bei IPMI Chips mit ATEN-Software
Hinweise zu drei Sicherheitsproblemen der Fernwartungsfunktionen bei Supermicro-Systemen mit Nuvoton WPCM450R IPMI Chips mit ATEN-Software . ...
7 KB (804 Wörter) - 10:01, 23. Jun. 2014
Remote Management Übersicht (Abschnitt IPMI onboard)
IPMI + KVM-over-LAN onboard |! : Foto | Modul/System | Mainboards | Dedizierte NIC | Standard Benutzer/Passwort | Zusatzinfos | | ...

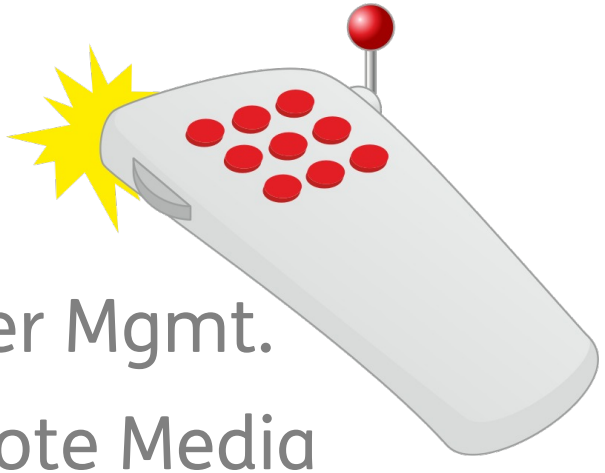
Intelligent Platform Management Interface

Ein dedizierter BMC

Baseboard Management Controller

- Bei den meisten Servern vorhanden
  - Evtl. auch als Add In Card
- Unabhängige Komponenten
  - CPU, Memory, Storage, Netzwerk
- Nahezu komplette Kontrolle über die Server-Hardware





- Power Mgmt.
- Remote Media

```
# /usr/lib/nagios/plugins/check_ipmi_sensor -H localhost
IPMI Status: OK | 'System Temp'=27.00 'Peripheral Temp'=28.00 'FAN
1'=2775.00 'FAN 2'=2700.00 'FAN 3'=2700.00 'FAN 4'=1050.00
'Vcore'=0.66 '3.3VCC'=3.36 '12V'=12.14 'VDIMM'=1.53 '5VCC'=5.12 '-
12V'=-11.90 'VBAT'=3.15 'VSB'=3.34 'AVCC'=3.36
```

IPMI Sensor Monitoring Plugin (thomas-krenn.com/wiki)

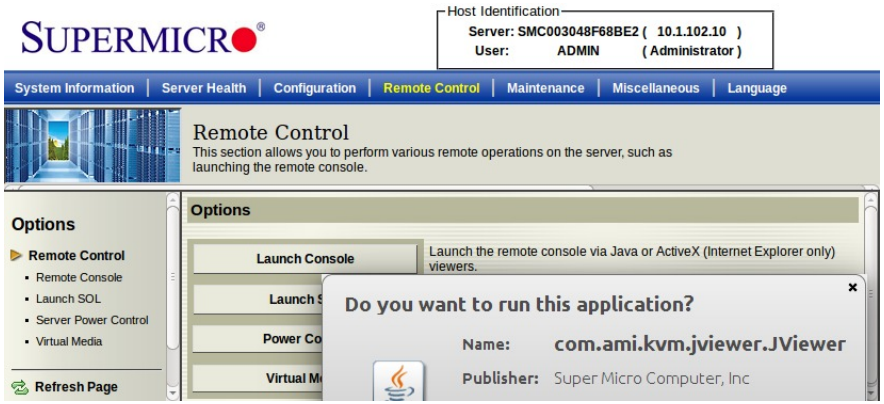
The Eavesdropping System in Your Computer

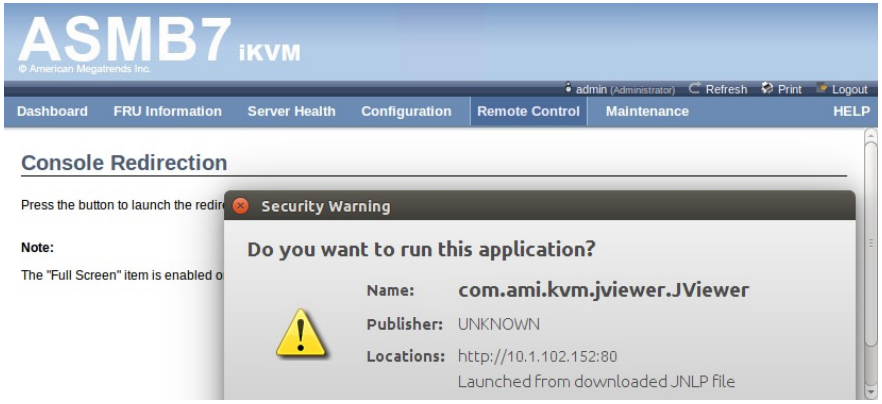
(Bruce Schneier, Schneier on Security)


Black box

IPMI Firmware by ATEN / AMI

- Mainboard-Hersteller passen Firmware an
- OS = Embedded Linux
- IPMI Firmware Teile Closed-Source





IPMI Firmware

```
$ uname -a
Linux AMI40167E34F026 2.6.28.10-ami #1 Wed Dec 11 15:17:46 CST 2013
armv5tejl unknown
$ cat /proc/cpuinfo
Processor         : ARM926EJ-S rev 5 (v5l)
BogoMIPS        : 191.69
Features        : swp half fastmult edsp java
CPU implementer         : 0x41
CPU architecture: 5TEJ
CPU variant        : 0x0
CPU part        : 0x926
CPU revision          : 5

Hardware        : AST2300EVB
Revision        : 0000
Serial                : 0000000000000000
```

IPMI Firmware

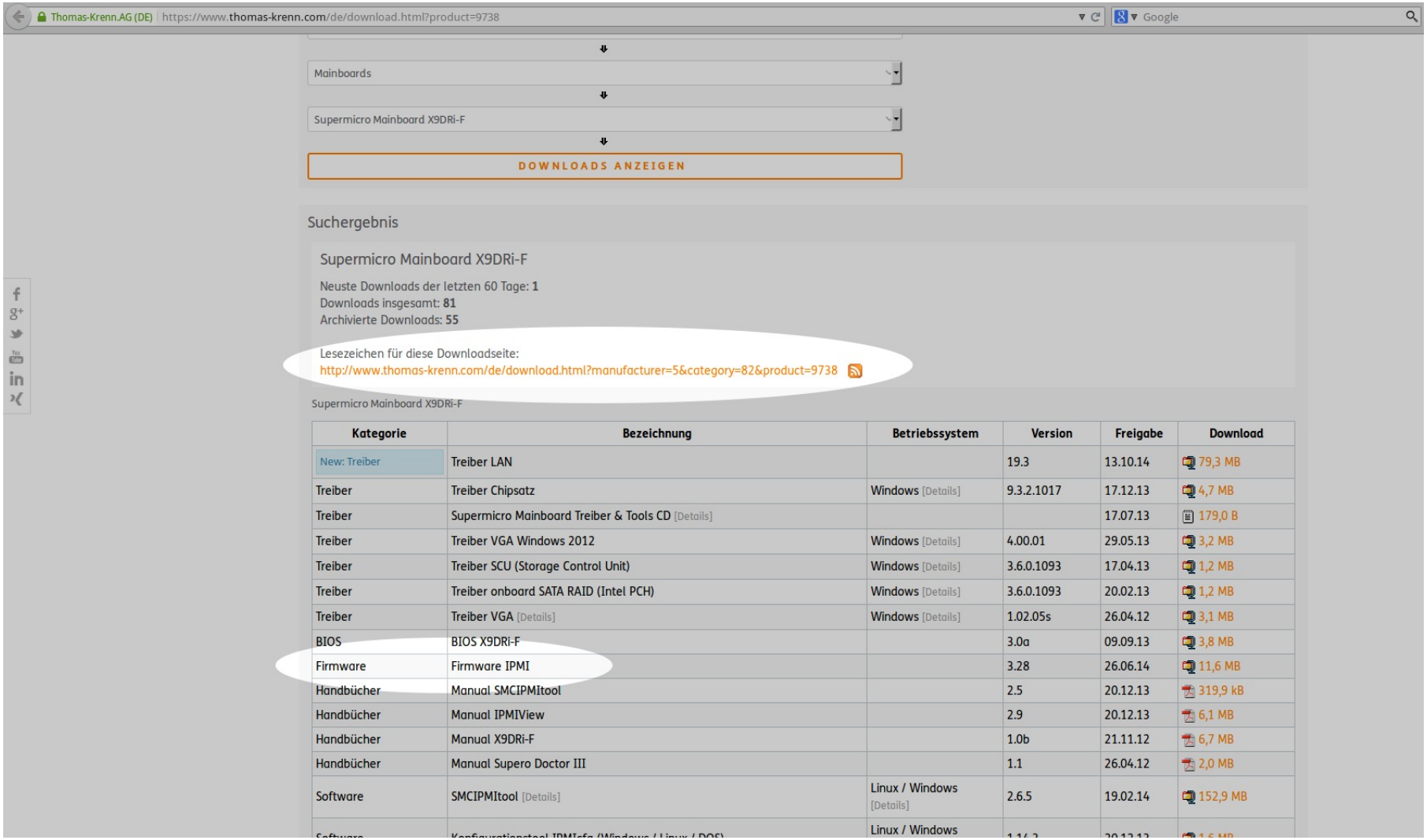
Wikimedia Commons

- HP Integrated Lights Out
- Dell DRAC
- IBM Remote Supervisor Adapter
- Einige Probleme spezifikations-spezifisch

Firmware Updates

- Nicht nur IPMI spezifische Teile betroffen
  - libupnp
  - NTP
- Als Beispiel
  - Supermicro „wartet“ auf ATEN/AMI
  - Thomas-Krenn „wartet“ auf Supermicro
    - Firmware-Tests auf allen betroffenen Boards

Firmware Updates



Kategorie	Bezeichnung	Betriebssystem	Version	Freigabe	Download
New: Treiber	Treiber LAN		19.3	13.10.14	79,3 MB
Treiber	Treiber Chipsatz	Windows [Details]	9.3.2.1017	17.12.13	4,7 MB
Treiber	Supermicro Mainboard Treiber & Tools CD [Details]			17.07.13	179,0 B
Treiber	Treiber VGA Windows 2012	Windows [Details]	4.00.01	29.05.13	3,2 MB
Treiber	Treiber SCU (Storage Control Unit)	Windows [Details]	3.6.0.1093	17.04.13	1,2 MB
Treiber	Treiber onboard SATA RAID (Intel PCH)	Windows [Details]	3.6.0.1093	20.02.13	1,2 MB
Treiber	Treiber VGA [Details]	Windows [Details]	1.02.05s	26.04.12	3,1 MB
BIOS	BIOS X9DRi-F		3.0a	09.09.13	3,8 MB
Firmware	Firmware IPMI		3.28	26.06.14	11,6 MB
Handbücher	Manual SMCIPMItool		2.5	20.12.13	319,9 kB
Handbücher	Manual IPMIView		2.9	20.12.13	6,1 MB
Handbücher	Manual X9DRi-F		1.0b	21.11.12	6,7 MB
Handbücher	Manual Supero Doctor III		1.1	26.04.12	2,0 MB
Software	SMCIPMItool [Details]	Linux / Windows [Details]	2.6.5	19.02.14	152,9 MB
Software	Konfigurationstool IPMIcfg (Windows / Linux / DOS)	Linux / Windows	1.14.2	20.12.13	1,6 MB

Firmware Updates

www.thomas-krenn.com/de/wiki/Kategorie:Remote-Management

THOMAS KRENN
server.hosting.customized.

Gschoenberger Diskussion Einstellungen Beoba

Lesen Quelltext bearbeiten Versionsgeschichte Suchen

wiki
Unsere Experten teilen ihr Wissen mit Ihnen.

- Server-Hardware
- Server-Software
- Storage
- Virtualisierung
- Netzwerk+Zubehör
- Themenschwerpunkte
- Projektvorstellungen
- Archiv

Werkzeuge
Links auf diese Seite
Änderungen an verlinkten Seiten
Datei hochladen
Spezialseiten
Druckversion
Permanenter Link
Seiteninformationen

In anderen Sprachen
English
Polski

Kategorie:Remote-Management

Hauptseite > Netzwerk+Zubehör

Kategorie Remote-Management

In dieser Kategorie finden Sie Artikel zum Thema Remote-Management.

Artikel speziell zu IPMI finden Sie in der

- Unterkategorie zu IPMI

Neueste Artikel dieser Kategorie

- FreeIPMI authentication type unavailable for attempted privilege l
- Bootdevice mit ipmitool setzen (15.09.2014)
- Asus IPMI / ASMB7 + iKVM (28.08.2014)

Unterkategorien

Diese Kategorie enthält folgende Unterkategorie:

I
- IPMI (40 S)

Seiten in der Kategorie „Remote-Management“

Es werden 33 von insgesamt 33 Seiten in dieser Kategorie angezeigt:

A
- ASPEED AST2400 IPMI Chip mit ATEN-Software

C
- ClickBIOS

E
- E-Mail Benachrichtigung Supermicro IPMI Modul
- E-Mail Benachrichtigung Supermicro IPMI Modul v3.xx

F
- Fehlerhafte IPMI Sensoren durch vollständige Initialisierung des IPMI Moduls richtigstellen
- Full Remote Management Supermicro

I (Fortsetzung)
- IPMI Konfiguration Supermicro mittels BIOS oder Webinterface
- IPMI Virtual Media einbinden
- IPMI zeigt falsche Werte
- IPMI-Konfiguration im BIOS und Webinterface beim X8DT3-F

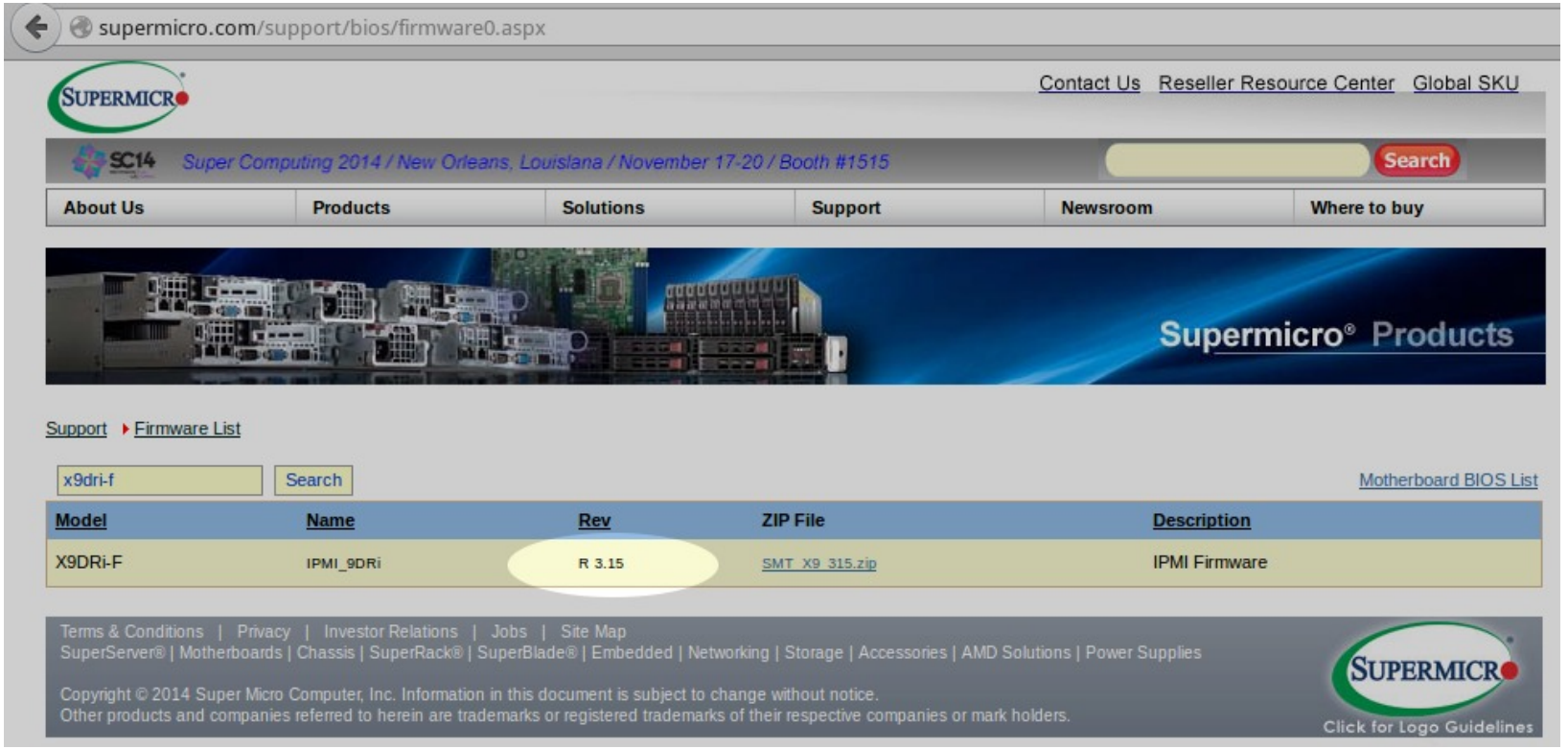
J
- Java Cache unter Windows leeren

L
- Libupnp Pufferüberlauf bei Mainboards mit Nuvoton WPCM450R IPMI Chips mit ATEN-Software
- Login im Supermicro Remote Management Webinterface funktioniert nicht

R (Fortsetzung)
- Remote Management Übersicht

S
- Sicherheitshinweise zur Supermicro IPMI Fernwartu
  Chips mit ATEN-Software
- SNMP Informationen per MIB Browser auslesen
- Supermicro IPMI Sicherheitsupdates Juli 2014
- Supermicro IPMI Sicherheitsupdates November 201
- Supermicro IPMI SNMP MIB
- Supermicro IPMIView
- Supermicro Remote Management Netzwerk Ports
- Supermicro X8DT3-F IP Konfiguration IPMI und KVM

Firmware Updates



Best Practices

Wir empfehlen administrative Zugänge wie IPMI- aber auch etwa SSH-Dienste nicht offen im Internet zu betreiben, sondern mittels Firewall/VPN den Zugriff auf solche Dienste ausschließlich berechtigten Personen zu ermöglichen.

#1 Netzwerk

_ nmap + ndiff

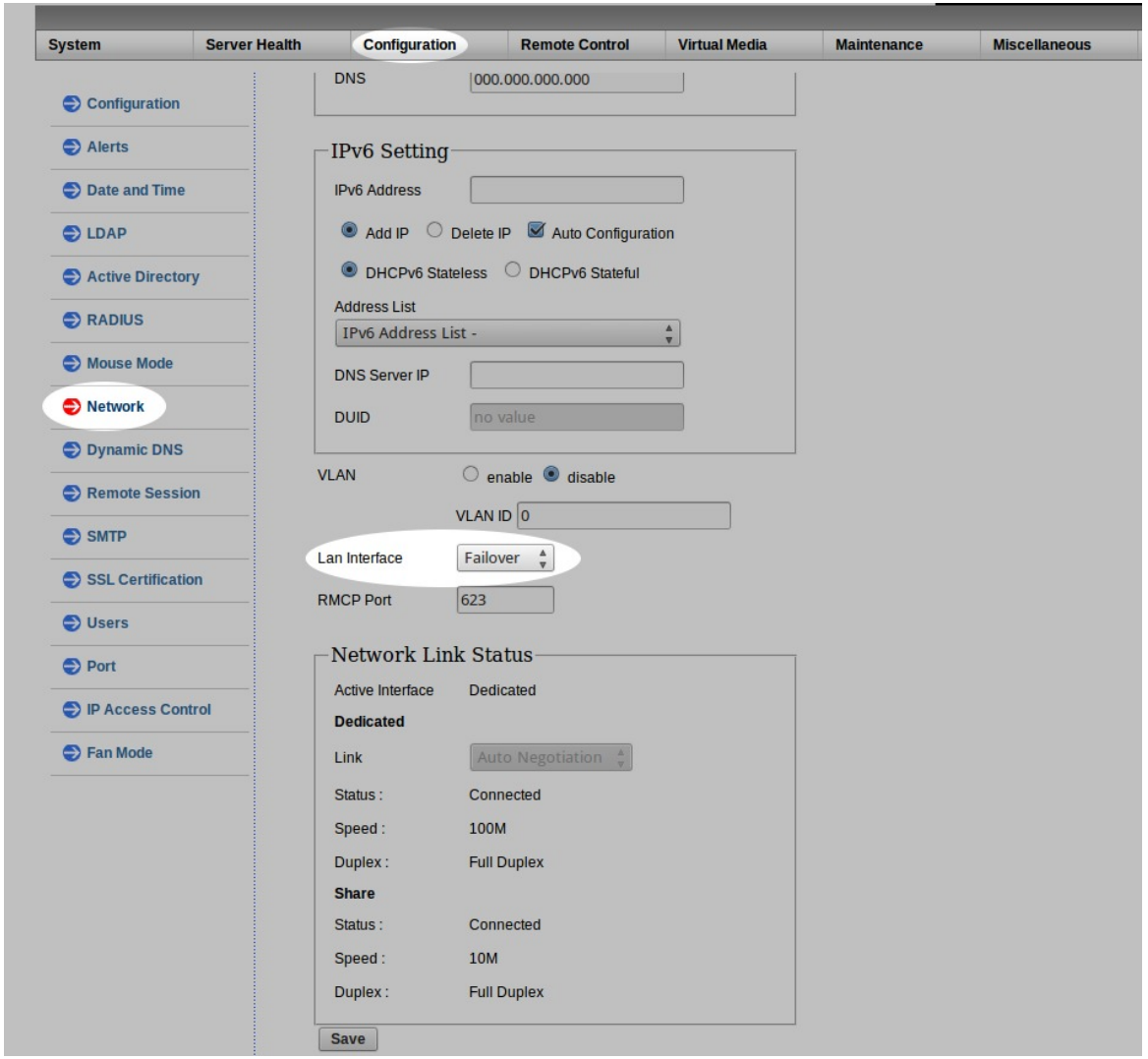
```
-Nmap 5.21 at 2014-05-01 00:00
+Nmap 5.21 at 2014-06-01 00:00

[…]
(XX.XX.XXX.XXX):
-Not shown: 1000 open|filtered ports, 998 filtered
ports
+Not shown: 1000 open|filtered ports, 1000 filtered
ports
 PORT    STATE SERVICE VERSION
-80/tcp  open  http
-443/tcp open  https
```

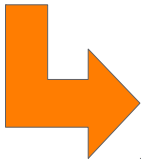
```
msf > use auxiliary/scanner/ipmi/ipmi_version
msf auxiliary(ipmi_version) > set RHOSTS 10.1.102.0/24
RHOSTS => 10.1.102.0/24
msf auxiliary(ipmi_version) > run

[*] Sending IPMI requests to 10.1.102.0->10.1.102.255 (256 hosts)
[+] 10.1.102.141:623 - IPMI - IPMI-2.0 OEMID:21317 UserAuth(auth_msg,
auth_user, non_null_user, null_user, anonymous_user)
PassAuth(password, md5, md2) Level(1.5, 2.0)
[+] 10.1.102.152:623 - IPMI - IPMI-2.0 UserAuth(auth_msg, auth_user,
non_null_user) PassAuth(oem_auth, password, md5, md2, null)
Level(1.5, 2.0)
[+] 10.1.102.10:623 - IPMI - IPMI-2.0 UserAuth(auth_msg, auth_user,
non_null_user) PassAuth(oem_auth, md5, md2) Level(1.5, 2.0)
[+] 10.1.102.182:623 - IPMI - IPMI-2.0 OEMID:21317 UserAuth(auth_msg,
auth_user, non_null_user, null_user) PassAuth(password, md5, md2)
Level(1.5, 2.0)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

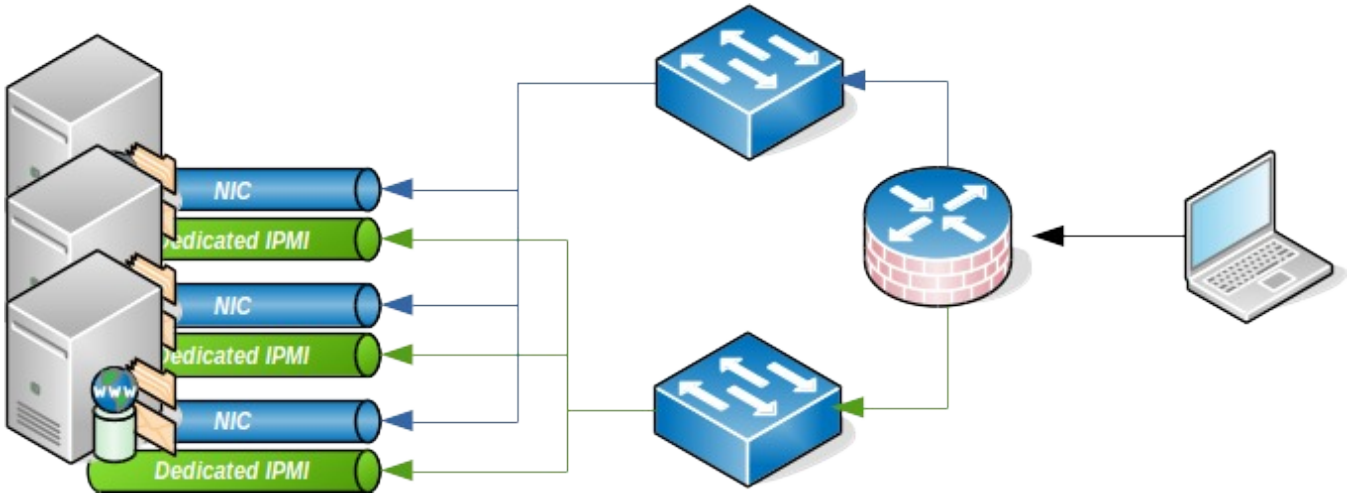
IPMI Netzwerk-Modi

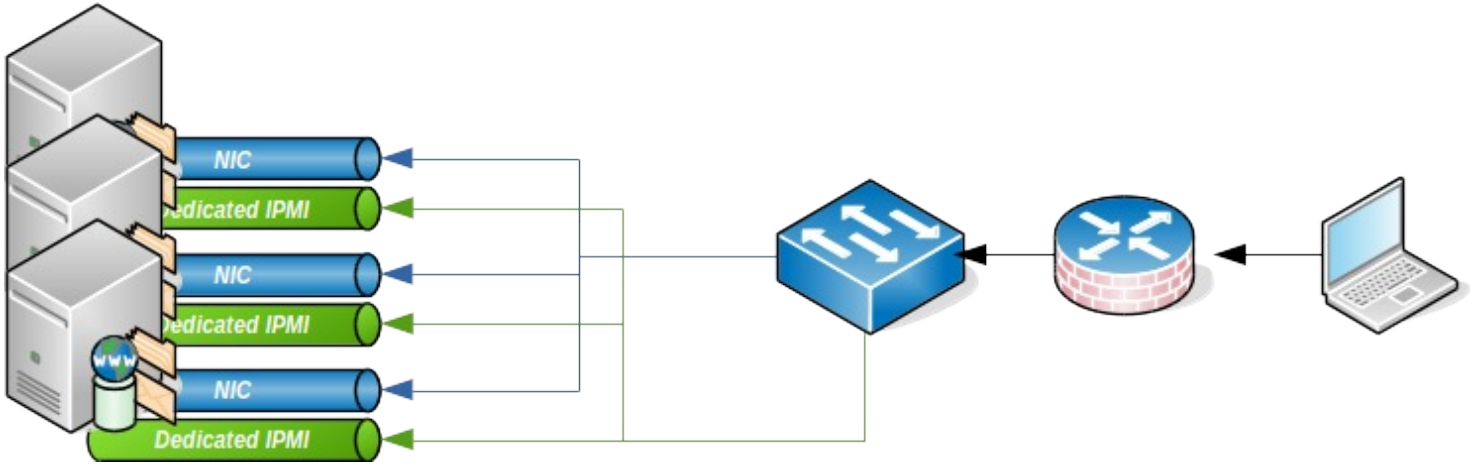
- Dedicated
- Shared
- Failover
- IPMI RAW command LAN mode (supermicro.com)

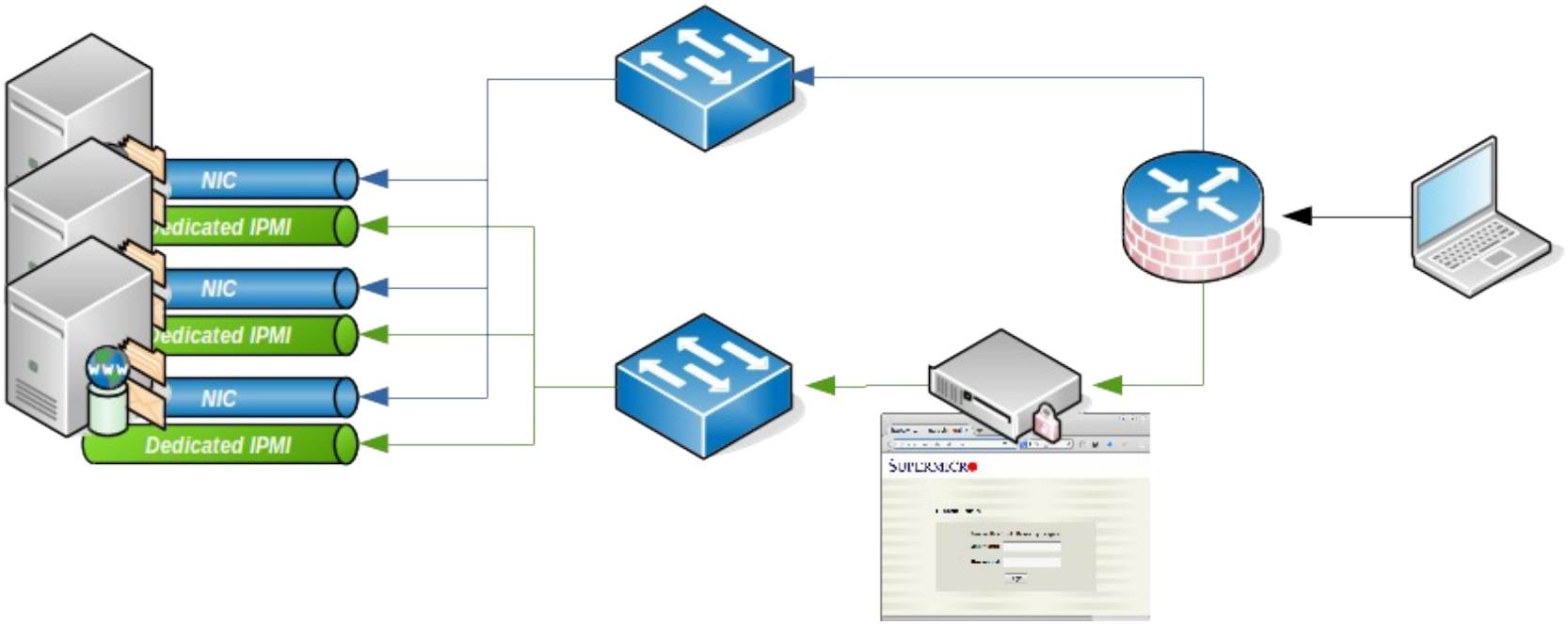
```
$ ipmi-raw -h 10.1.102.182 -u ADMIN -p **** -l ADMIN 0x0 0x30 0x70
0x0c 0
rcvd: 70 00 02
```

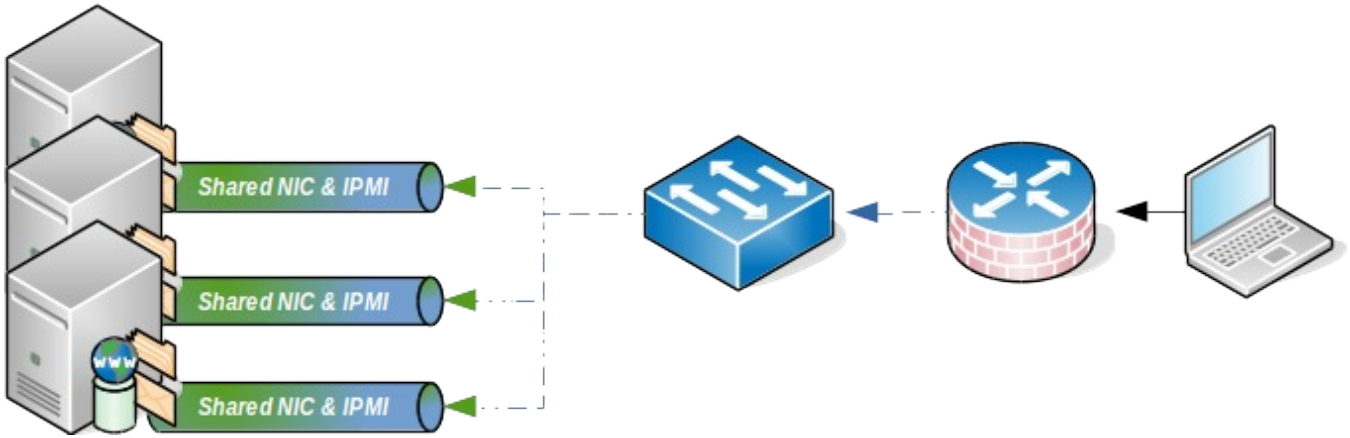

System
Server Health
Configuration
Remote Control
Virtual Media
Maintenance
Miscellaneous
Configuration
Alerts
Date and Time
LDAP
Active Directory
RADIUS
Mouse Mode
Network
Dynamic DNS
Remote Session
SMTP
SSL Certification
Users
Port
IP Access Control
Fan Mode
DNS
000.000.000.000
IPv6 Setting
IPv6 Address
Add IP
Delete IP
Auto Configuration
DHCPv6 Stateless
DHCPv6 Stateful
Address List
IPv6 Address List -
DNS Server IP
DUID
no value
VLAN
enable
disable
VLAN ID
0
Lan Interface
Failover
RMCP Port
623
Network Link Status
Active Interface
Dedicated
Dedicated
Link
Auto Negotiation
Status :
Connected
Speed :
100M
Duplex :
Full Duplex
Share
Status :
Connected
Speed :
10M
Duplex :
Full Duplex
Save

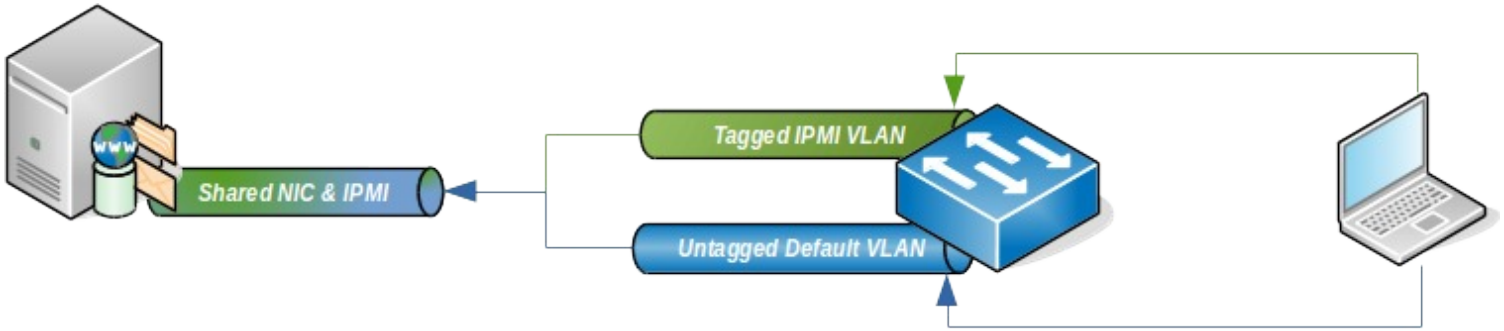


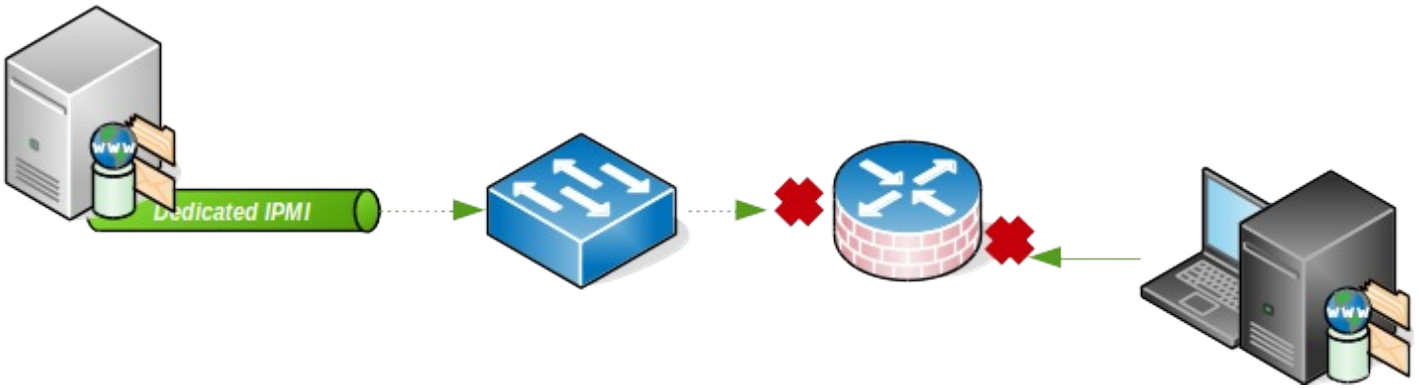

NIC
dicated IPMI
NIC
dicated IPMI
NIC
Dedicated IPMI


NIC
dicated IPMI
NIC
dicated IPMI
NIC
Dedicated IPMI


NIC
dicated IPMI
NIC
dicated IPMI
NIC
Dedicated IPMI
SUPERMICR


Shared NIC & IPMI
Shared NIC & IPMI
Shared NIC & IPMI

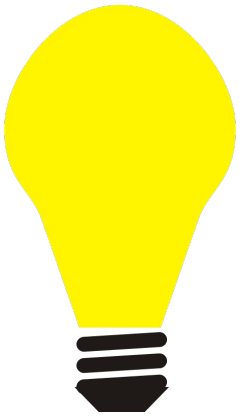

Shared NIC & IPMI
Tagged IPMI VLAN
Untagged Default VLAN



_ Ausnahme z.B. NTP

Was wenn doch?

- Ports ändern
- IP Access Control Lists
- System Event Log überwachen
  - Feature für check_ipmi_sensor im Test
- Nicht benötigte Dienste ausschalten
  - Bei Supermicro ab X10 Boards



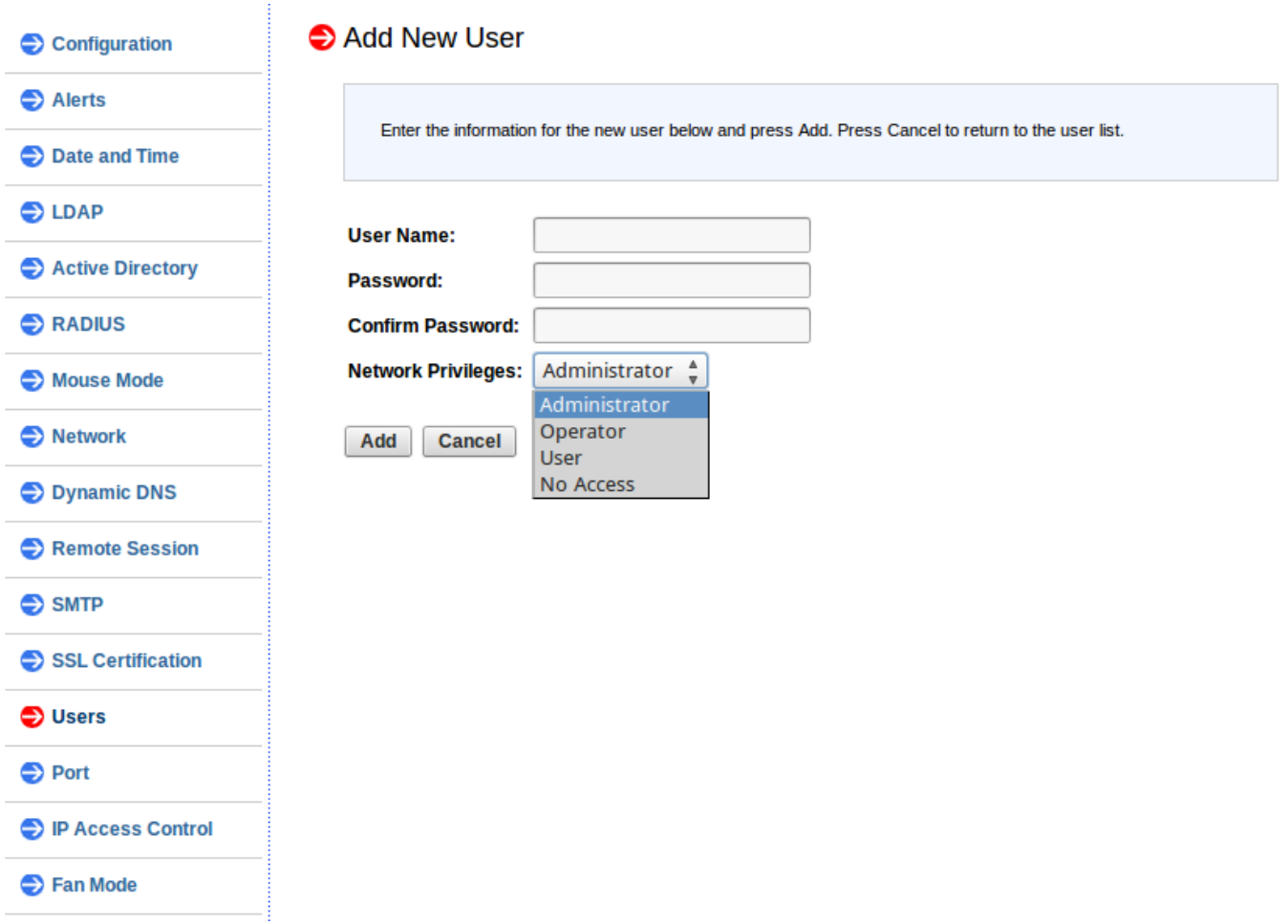
#2 User Management


ADMIN

Privilege Levels

Level	Beschreibung
Callback	Dies ist der niedrigste Privilege Level. Erlaubt nur die Initiierung eines Callbacks.
User	Nur IPMI begin Kommandos sind erlaubt. Dies sind hauptsächlich Kommandos zum Lesen und Abfragen von Status Informationen (Sensoren).
Operator	Alle BMC Kommandos bis auf jene zur Änderung der Out-Of-Band Interfaces.
Administrator	Alle BMC Kommandos sind erlaubt.

```
# ./ipmicfg-linux.x86_64 -user add 3 monitor ***** 2
Done.
# ./ipmicfg-linux.x86_64 -user list
Maximum number of Users          : 10
Count of currently enabled Users : 3
User ID | User Name        | Privilege Level | Enable
------- | -----------      | --------------- | ------
      2 | ADMIN            | Administrator   | Yes
      3 | monitor          | User            | Yes
```


Configuration
Alerts
Date and Time
LDAP
Active Directory
RADIUS
Mouse Mode
Network
Dynamic DNS
Remote Session
SMTP
SSL Certification
Users
Port
IP Access Control
Fan Mode
Add New User
Enter the information for the new user below and press Add. Press Cancel to return to the user list.
User Name:
Password:
Confirm Password:
Network Privileges:
Administrator
Administrator
Operator
User
No Access
Add
Cancel

User List

The list below shows the current list of configured users. If you would like to delete or modify a user, select their name in the list and press Delete User or Modify User. To add a new user, select an unconfigured slot and press Add User.

Number of configured u

User ID	User Name	Network Privilege
1	Anonymous	Reserved
2	ADMIN123	Administrator
3	sdjalk	Administrator
4	~	Reserved
5	~	Reserved
6	~	Reserved
7	~	Reserved
8	~	Reserved
9	~	Reserved
10	~	Reserved

Add User | Modify User | Delete User

sjfaiklaz

Administrator

afjhuijoh

User

RAKP+ Dump Hashes

In short, the authentication process for IPMI 2.0 mandates that the server send a salted SHA1 or MD5 hash of the requested user's password to the client, prior to the client authenticating.

A Penetration Tester's Guide to IPMI and BMCs (rapid7.com)

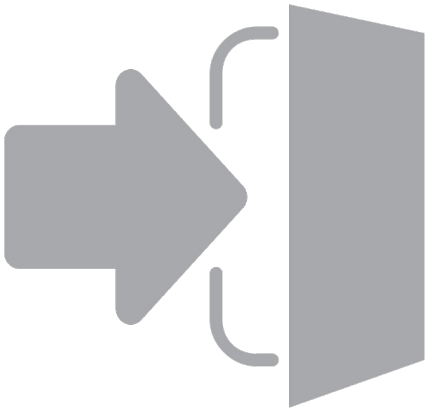
```
msf > use auxiliary/scanner/ipmi/ipmi_dumphashes
msf auxiliary(ipmi_dumphashes) > set RHOSTS 10.1.102.141
RHOSTS => 10.1.102.141
msf auxiliary(ipmi_dumphashes) > set THREADS 128
THREADS => 128
msf auxiliary(ipmi_dumphashes) > run

[+] 10.1.102.141:623 - IPMI - Hash found:
admin:1466752325000004ec525d3852f4fa73c93b674788217fe0000000000000000000000000000000000000000000000000000000000140561646d696e:2c76e372d89ac7cd4e3bfecb423962f708d0741c
```

RAKP+ Dump Hashes

```
$ ./cudaHashcat64.bin --outfile=ipmi.out -m 7300 hash.txt -a 3 ?lu?
lu?lu?lu?lu?lu
[...]
Session.Name...: cudaHashcat
Status.........: Exhausted
Input.Mode.....: Mask (?lu?lu?lu?lu?lu?lu) [12]
Hash.Target....:
54414378fb2db5ff365e4bc5856adaf4c1b8a2f2153efd1b81fb54dfe1bf56478788
ea7ba154375b40167e34f026e1020010d21d1ea3162504056164 6d696e:0a0b16023
1e204a6d0bd086e26718002409b35b7
Hash.Type......: IPMI2 RAKP HMAC-SHA1
Time.Started...: Thu Sep 18 10:11:17 2014 (6 secs)
Time.Estimated.: 0 secs
Speed.GPU.#1...: 52732.3 kH/s
Recovered......: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.......: 308915776/308915776 (100.00%)
Skipped........: 0/308915776 (0.00%)
Rejected.......: 0/308915776 (0.00%)
HWMon.GPU.#1...: -1% Util, 41c Temp, 31% Fan
```

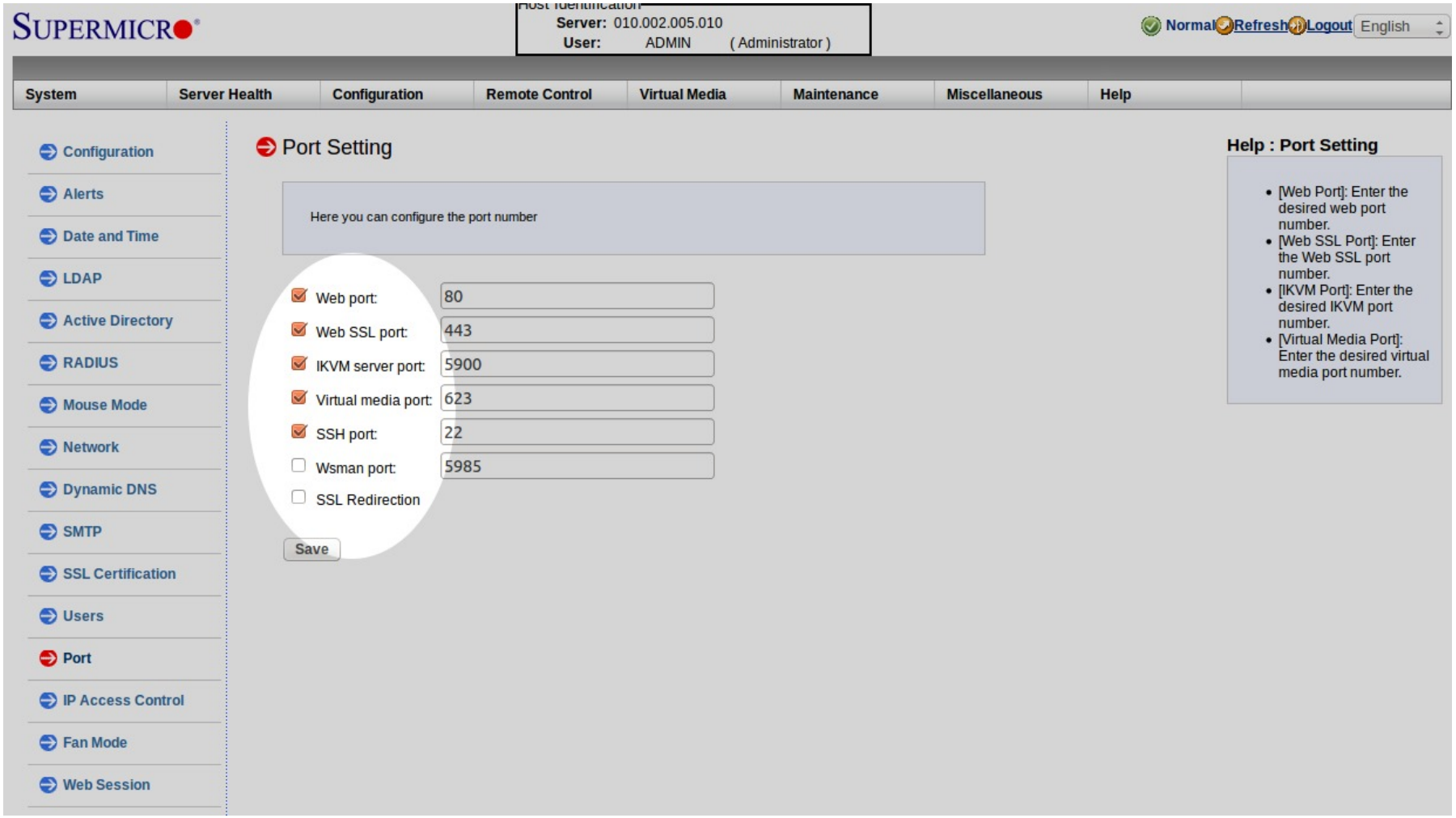
Komplexe Passwörter

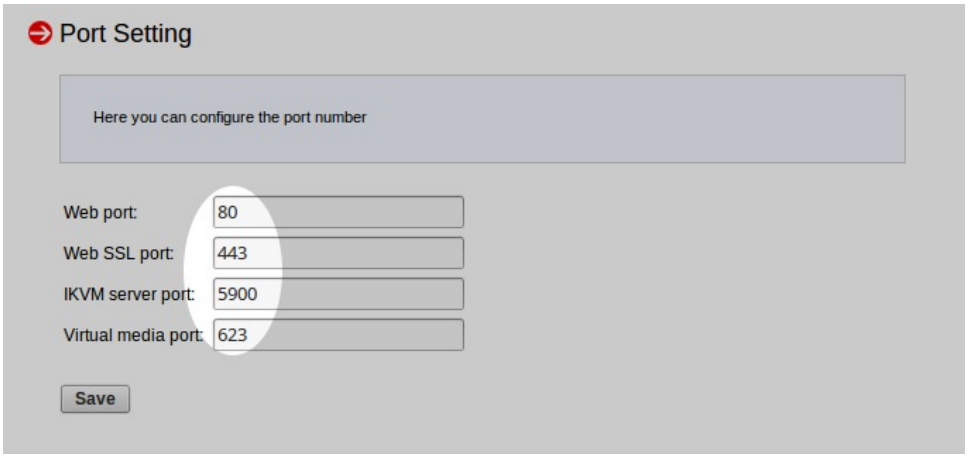
Passwort Management

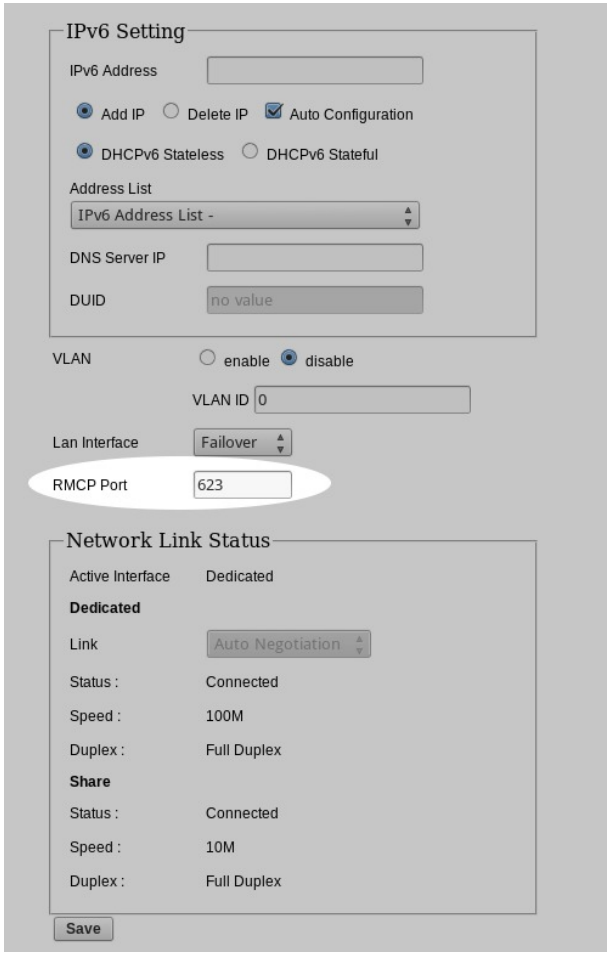


#3 Dienste

```
$ sudo nmap -sS -sU -T2 10.1.102.182

Starting Nmap 6.40 ( http://nmap.org ) at 2014-11-13
10:59 CET
Nmap scan report for 10.1.102.182
Host is up (0.00052s latency).
Not shown: 1994 closed ports
PORT     STATE         SERVICE
22/tcp   open          ssh
80/tcp   open          http
443/tcp  open          https
5900/tcp open          vnc
123/udp  open          ntp
623/udp  open|filtered asf-rmcp
MAC Address: 00:25:90:A9:62:CB (Super Micro Computer)

Nmap done: 1 IP address (1 host up) scanned in 1392.77
seconds
```


SUPERMICRO
Server: 010.002.005.010
User: ADMIN (Administrator)
Normal
Refresh
Logout
English
System
Server Health
Configuration
Remote Control
Virtual Media
Maintenance
Miscellaneous
Help
Configuration
Alerts
Date and Time
LDAP
Active Directory
RADIUS
Mouse Mode
Network
Dynamic DNS
SMTP
SSL Certification
Users
Port
IP Access Control
Fan Mode
Web Session
Port Setting
Here you can configure the port number
Web port: 80
Web SSL port: 443
IKVM server port: 5900
Virtual media port: 623
SSH port: 22
Wsman port: 5985
SSL Redirection
Save
Help : Port Setting
[Web Port]: Enter the desired web port number.
[Web SSL Port]: Enter the Web SSL port number.
[IKVM Port]: Enter the desired IKVM port number.
[Virtual Media Port]: Enter the desired virtual media port number.

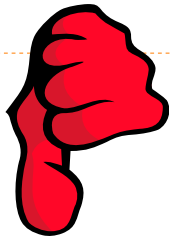

Port Setting
Here you can configure the port number
Web port:
80
Web SSL port:
443
IKVM server port:
5900
Virtual media port:
623
Save


IPv6 Setting
IPv6 Address
Add IP
Delete IP
Auto Configuration
DHCPv6 Stateless
DHCPv6 Stateful
Address List
IPv6 Address List -
DNS Server IP
DUID
no value
VLAN
enable
disable
VLAN ID
0
Lan Interface
Failover
RMCP Port
623
Network Link Status
Active Interface
Dedicated
Dedicated
Link
Auto Negotiation
Status :
Connected
Speed :
100M
Duplex :
Full Duplex
Share
Status :
Connected
Speed :
10M
Duplex :
Full Duplex
Save

#4 Konfiguration

NONE Authentifizierung

```
[…]
Auth Type Support       : NONE MD2 MD5 PASSWORD OEM
Auth Type Enable        : Callback : NONE MD2 MD5 PASSWORD OEM
                        : User     : NONE MD2 MD5 PASSWORD OEM
                        : Operator : NONE MD2 MD5 PASSWORD OEM
                        : Admin    : NONE MD2 MD5 PASSWORD OEM
$ ipmitool -A none -H 10.1.102.152 -U admin lan print
Set in Progress         : Set Complete
Auth Type Support       : NONE MD2 MD5 PASSWORD OEM
Auth Type Enable        : Callback : NONE MD2 MD5 PASSWORD OEM
                        : User     : NONE MD2 MD5 PASSWORD OEM
                        : Operator : NONE MD2 MD5 PASSWORD OEM
                        : Admin    : NONE MD2 MD5 PASSWORD OEM
                        : OEM      :
IP Address Source       : Static Address
IP Address              : 10.1.102.152
Subnet Mask             : 255.255.255.0
```



Authentifizierung

- Nur MD5, kein MD2 oder PASSWORD oder gar NONE

```
$ ipmitool -I lanplus -H 10.1.102.141 -U ADMIN -P **** lan print
Set in Progress         : Set Complete
Auth Type Support       : NONE MD2 MD5 PASSWORD
Auth Type Enable        : Callback : MD2 MD5 PASSWORD
                        : User     : MD2 MD5 PASSWORD
                        : Operator : MD2 MD5 PASSWORD
                        : Admin    : MD2 MD5 PASSWORD
                        : OEM      : MD2 MD5 PASSWORD
$ ipmitool -I lanplus -H 10.1.102.141 -U ADMIN -P **** lan set 1
auth Admin MD5
```

NONE Authentifizierung bei IPMI deaktivieren (thomas-krenn.com/wiki)

LAN Interface Protocol

- RMCP+

  [...] these extensions support enhanced authentication, encryption[...]

  IPMI Spec. 2.0 Rev. 1.1 (intel.com)

```
$ ipmitool -I lanplus -H 10.1.102.141 -U ADMIN -P **** lan print
[...]
$ bmc-config -D LAN_2_0 -h 10.1.102.141 -u ADMIN -p **** –checkout
[...]
```

[...] it's really no cipher at all, or the un-cipher

Dan Farmer, The Brain-Death in the IPMI Specification (fish2.com)

Cipher 0

Wikimedia Commons

```
$ ipmitool -I lanplus -H 10.1.102.152 -U admin -P **** lan print
[…]
RMCP+ Cipher Suites      : 0,1,2,3,6,7,8,11,12
Cipher Suite Priv Max    : aaaaXXaaaXXaaXX
$ ipmitool -I lanplus -C 0 -H 10.1.102.152 -U admin -P FluffyWabbit
user list
ID  Name         Callin  Link Auth  IPMI Msg   Channel Priv Limit
1                 false   false      true       ADMINISTRATOR
2   admin         false   false      true       ADMINISTRATOR
3   monitoring    true    true       true       USER
```

Cipher 3, 8, 12

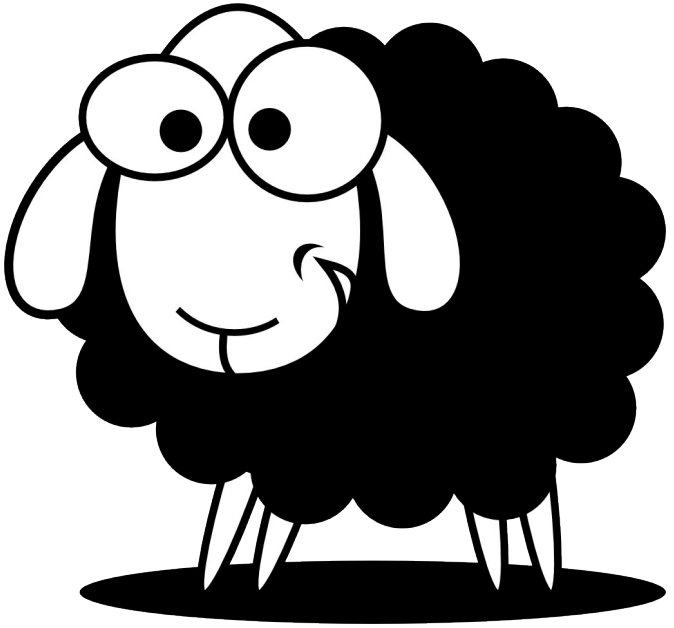
Table 22-, Cipher Suite IDs

ID	characteristics	Cipher Suite	Authentication Algorithm	Integrity Algorithm(s)	Confidentiality Algorithm(s)
0	"no password"	00h, 00h, 00h	RAKP-none	None	None
1	S	01h, 00h, 00h	RAKP-HMAC-SHA1	None	None
2	S, A	01h, 01h, 00h		HMAC-SHA1-96	None
3	S, A, E	01h, 01h, 01h			AES-CBC-128
4	S, A, E	01h, 01h, 02h			xRC4-128
5	S, A, E	01h, 01h, 03h			xRC4-40
6	S	02h, 00h, 00h	RAKP-HMAC-MD5	None	None
7	S, A	02h, 02h, 00h		HMAC-MD5-128	None
8	S, A, E	02h, 02h, 01h			AES-CBC-128
9	S, A, E	02h, 02h, 02h			xRC4-128
10	S, A, E	02h, 02h, 03h			xRC4-40
11	S, A	02h, 03h, 00h		MD5-128	None
12	S, A, E	02h, 03h, 01h			AES-CBC-128

IPMI Spec. 2.0 Rev. 1.1, S. 292 (intel.com)

```
$ ipmitool -I lanplus -H 10.1.102.152 -P **** -U admin lan set 1
cipher_privs XXXaXXXXXXXXXXX
[…]
$ ipmitool -I lanplus -C 3 -H 10.1.102.152 -P **** -U admin lan print
[…]
```

#5 Management



- Asset/CM Datenbank
- Patch Management

Checkliste

- [ ] _ Firmware Updates
- [ ] _ Netzwerkkonfiguration
- [ ] _ User Management
- [ ] _ Services
- [ ] _ Protokolle

Weitere Informationen

- Widespread Vulnerabilities in BMCs (rapid7.com)
- Best Practices BMC Security (supermicro.com)
- IPMI Security Best Practices (fish2.com)

Einzelnachweise

- https://openclipart.org/detail/10906/xtremely-flammable-by-yves_guillou-10906
- https://openclipart.org/detail/202651/remote-control-complex-by-pnx-202651
- https://openclipart.org/detail/30139/tango-waether-severe-alert-by-warszawianka
- https://openclipart.org/detail/168588/sheep-using-a-switch-by-dodger2
- https://openclipart.org/detail/102817/e.t.-hand-by-heiland-stark
- https://openclipart.org/detail/68/trash-can-by-andy
- https://openclipart.org/detail/71467/muscle-by-hector-gomez
- https://openclipart.org/detail/189459/exit-icon-by-ckhoo-189459


THOMAS
KRENN®
server.hosting.customized.