FAQ Fernwartung per IPMI und AMT

Antworten auf die häufigsten Fragen

Von Christof Windeck

Wozu Fernwartung?

? Einen Server oder PC erreiche ich per SSH, Remote-Desktop-Verbindung, TeamViewer oder auch RealVNC – wozu brauche ich Fernwartungsfunktionen wie Intel AMT oder einen BMC?

! Mit Out-of-Band-(OOB-)Fernwartung erreichen Sie den Computer auch, wenn es Probleme gibt oder um ihn erstmalig einzurichten. OOB-Fernwartung funktioniert auch im BIOS-Setup und kann schlafende Systeme wecken. Schon einfache Funktionen sparen Zeit: der ferngesteuerte Neustart eines abgestürzten Systems, das Starten in der Nacht zum Einspielen von Updates, das Auslesen von Gerätenummern für die Inventarisierung oder von Konfigurationsinformationen zu CPU, RAM und Massenspeicher, um Entscheidungen über Upgrades zu fällen.

Ausgewachsene Remote-Management-Systeme „orchestrieren“ und überwachen ganze Horden von Servern und verteilen BIOS- und Firmware-Updates. Großunternehmen automatisieren Admin-Aufgaben: Das Fernwartungssystem spielt das Betriebssystem auf fabrikneue PCs (Deployment, Rollout).

Baseboard Management Controller

? Was tut ein Baseboard Management Controller (BMC)?

! Auf den meisten Serverboards sitzen BMC-Chips, die dort auch als Grafikprozessor dienen: Sie binden eine simple VGA-Buchse an, damit ein Admin vor Ort am Server arbeiten kann – für eine Textkonsole oder den Windows-Server-Desktop reicht VGA.

Die integrierte 2D-GPU im BMC – oft die Embedded-Version einer uralten Matrox G200 – läuft mit Standardtreibern. Außer dem VGA-Signal liefert sie vor allem ein digitalisiertes Bild, das der BMC über seinen Ethernet-Controller an die Admin-Konsole schickt. Damit der Administrator umgekehrt Befehle ans System schicken kann, enthält der BMC einen USB-Controller, der Tastatur, Maus und Boot-Laufwerke emuliert: IDE Redirection (IDE-R) für Platte oder CD, USB-R als USB-Stick. Der Inhalt dieser emulierten Laufwerke kommt dabei von einem ISO-Image, welches der Admin im Netz bereitstellt: etwa das Abbild der Windows-Setup-DVD.

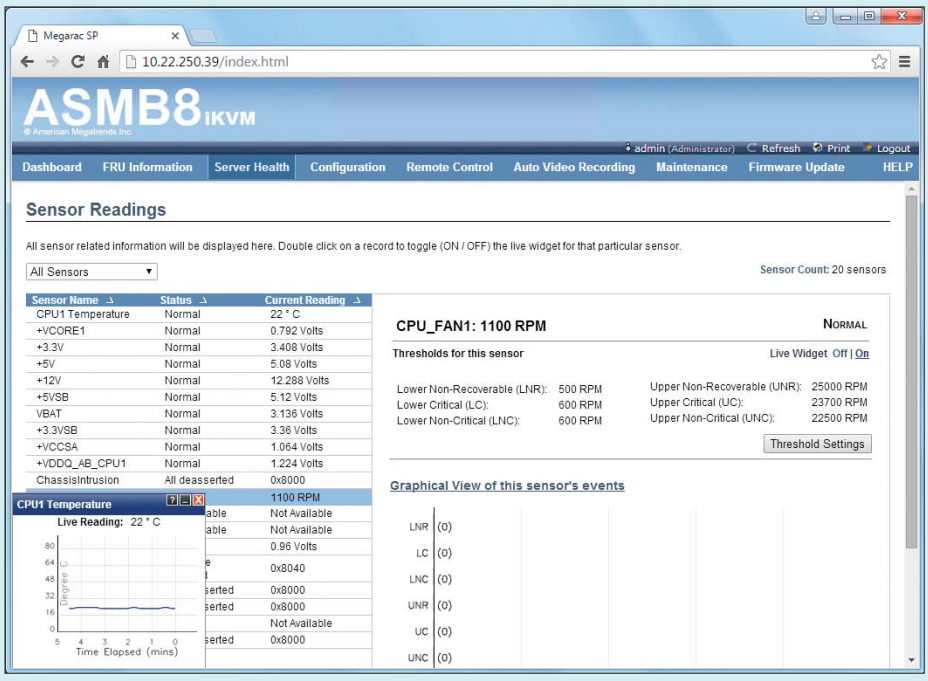
Der BMC liest Sensoren aus (Lüfterdrehzahlen, Betriebsspannungen, Temperaturen, Leistungsabgabe des Netzteils, Case-Open-Sensor) und kann eine LED am Gehäuse blinken lassen, damit ein Techniker die Maschine im Rack schneller findet. Üblicherweise läuft auf dem BMC auch ein Webserver, der Sensordaten und Schaltknöpfe für Steuerfunktionen (An/Aus/Reboot) präsentiert.

AMT versus IPMI

? Was unterscheidet Intels Active Management Technology von IPMI-Fernwartung für Server?

! In allen Rechnern mit Intel-Prozessoren steckt seit ungefähr 2006 die sogenannte Management Engine (ME). Das ist ein Mikrocontroller, der unabhängig von der CPU eine signierte ME-Firmware ausführt. Die ME erledigt unterschiedliche Aufgaben, bei vPRO-Systemen eben auch die Fernwartung.

Intel vPRO bezeichnet Business-Notebooks und Bürocomputer mit einer Kombination aus „Q“-Chipsätzen wie Q87 oder Q170, Prozessoren der Reihen Core i5 oder Core i7 sowie bestimmten Intel-Netzwerkchips für Ethernet und WLAN. Die AMT-Funktionen muss man per BIOS-Setup oder über spezielle Server aktivieren. Anschließend kann ein Administrator aus der Ferne beispielsweise den Rechner neustarten, Inventarnummern und CPU-Bezeichnung auslesen oder auf den grafischen Desktop zugreifen, sofern das System die „Intel HD Graphic“ in der CPU nutzt. Dieser Fernzugriff auf den PC nennt man Remote KVM (Keyboard, Video, Mouse).



Der BMC dieses Asus-Serverboards liefert eine Webseite aus, die Sensordaten anzeigt.

Das Intelligent Platform Management Interface (IPMI) bezeichnet Protokolle für die Fernwartung. Dabei haben sich eine Reihe von Standardfunktionen etabliert, die über AMT hinausgehen. So werden per IPMI Sensordaten übertragen, etwa Drehzahlen von Ventilatoren und die CPU-Temperatur – das fehlt bei AMT. IPMI-taugliche Fernwartung läuft meistens auf einem separaten Controllerchip auf dem Mainboard, dem sogenannten Baseboard Management Controller (BMC, siehe oben). Er enthält typischerweise einen einfachen 2D-Grafikkern, einen USB-Controller sowie ein Ethernet-Interface: In Servern erfolgt die Fernwartung üblicherweise über ein separates LAN und wird nicht mit dem Nutz-Netzverkehr vermischt wie bei Intel AMT. Die BMC-Fernwartung nennt HPE integrated Lights-out Management (iLO) und Dell Remote Access Card (DRAC).

Fallback

? Ich habe ein Server-Mainboard mit BMC und separatem Ethernet-Port. Seltsamerweise erreiche ich die Webseite der Fernwartung aber auch an einem der beiden anderen (Gigabit-)Ethernet-Ports – warum?

! Die BMC-Firmware beziehungsweise das BIOS vieler Serverboards besitzen eine Fallback-Automatik: Wird der separate Netzwerkport für die Fernwartung nicht benutzt (Kabel vergessen, Kabelfehler, Routerdefekt), dann meldet sich der BMC stattdessen auf einem der anderen Onboard-Netzwerkports. Er verwendet dabei eine eigene MAC-Adresse und bekommt via DHCP auch eine eigene IP-Adresse.

Da der Zugriff auf den BMC oft mit Standardpasswörtern wie admin/admin gelingt, ist die Fallback-Option ein Sicherheitsrisiko – man sollte sie unbedingt im BIOS-Setup oder in den Setup-Optionen der Fernwartung abschalten. Nach BIOS-Updates oder nach dem Laden der BIOS Setup Defaults kann es passieren, dass Remote Management Fallback wieder aktiv ist.

Risiko IPMI

? Funktioniert IPMI-Fernwartung sicher?

! Nein! Einerseits gibt es prinzipielle Schwächen in älteren IPMI-Versionen, andererseits finden Sicherheitsforscher immer wieder Bugs und Lücken in der IPMI-Firmware vieler Serverboards. Ein Angreifer steuert per Remote KVM die gesamte Maschine, als säße er davor.

Fernwarten sollte man in einem separaten, geschützten Netz, mindestens per VLAN abgetrennt. Vergeben Sie sichere Passwörter und schalten Sie nur unbedingt nötige Funktionen der Fernwartung frei. Falls möglich, verlegen Sie den Zugriff von den Standard-TCP-Ports auf andere: Portscans suchen meistens nach den „üblichen Verdächtigen“. Man sollte außerdem ein Passwort für den Zugriff aufs BIOS-Setup vergeben, damit ein Angreifer die Einstellungen für die Fernwartung nicht so leicht aus der Ferne ändern kann. Auch Festplatten-Verschlüsselung ist sinnvoll. *(ciw@ct.de)*