Linnéuniversitetet
Institutionen för datavetenskap, fysik och matematik

Rapport

IPMI

Författare: Johan Nyquist

Handledare: Marcus Wilhelmsson

Datum: 2012-01-07

Kurskod: 1DV427

Innehåll

1 Introduktion

Att kunna övervaka servrar i ett nätverk är viktigt för att kunna säkerställa dess status och tillgänglighet. Övervakningen är ofta centraliserad med en eller flera NMS (Network Management System) som tillsammans övervakar nätverket och enheter i syfte att snabbt upptäcka fel eller brister. Detta bygger på att NMS-systemen sckickar förfrågan till den övervakade enheten om en viss status, alternativt skickas statusen automatiskt med jämna mellanrum eller när något har inträffat. Den övervakade enheter är alltså delaktig i själva övervakningen vilket ofta kräver både systemkraft och mjukvara speciellt för att kunna utföra mer utförliga kontroller. Mjukvara för att kunna utföra detta måste då finnas på den övervakade enheten och köras för att kunna leverera information till NMS-systemet. IPMI utgör ett interface som är oberoende av ett systems övriga operativsystem/mjukvara. IPMI är ett hårdvaru interface som har kontakt med annan hårdvara i systemet och kan kommunicera med dessa. På så sätt kan IPMI hämta status från olika komponenter i systemet och skicka dessa till en NMS på egen hand. Syftet med denna rapporten är att sammanställa de mest grundläggande bitarna gällande IPMIs uppbyggnad och funktionalitet.

2 Teori

2.1 Förkortningar

Förkortning	**Betydelse**
ASF	Alert Standard Format
BMC	Baseboard Management Controller
BIOS	Basic Input/Output System
FRU	Field Replaceable Unit
I²C	Inter-Integrated Circuit
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
NMS	Network Management System
OEM	Original Equipment Manufacturer
PEF	Platform Event Filtering
RCMP	Remote Control Management Protocol
SDR	Sensor Data Record
SEEPROM	Serial Electrically Erasable Programmable ROM
SEL	System Event Log

2.2 Funktionalitet

IPMI kommunicerar med hårdvaran utan något underliggande operativsystem.IPMI sköts med egna komponenter helt oberoende av systemets huvudprocessor, vilket gör systemet åtkomligt och managerbart i situationer där systemet annars hade varit oåtkomligt. Det enda som krävs är att strömförsörjning finns tillgängligt och att anslutningen är intakt. IPMI ger möjligheten att övervaka och administrera ett system via något av de tillgängliga interfacen. Inställningar i BIOS kan göras samt påslagning/avstängning av systemet. Många komponenter i systemet kan även övervakas så som terperaturer, fläktar, spänning och strömförsörjning. IPMI kan även lagra felmeddelanden och händelser i systemet. Detta kan ske genom att en Management Controller skickar ett ”Event Message” till BMCn som i sin tur lagrar händelsen i ett SEEPROM (Serial Electrically Erasable Programmable ROM) dedikerat för SEL data. IPMI kan även skicka larm när något har hänt i systemet. Managering och övervakning kan ske dirket på det lokala systemet via ett operativsystem men även över nätverk. [1]

2.3 Komponenter

Vilka komponenter som finns kan variera från system till system. Det finns dock alltid en BMC som beskrivs närme i 2.3.1 BMC. För kommunikation mellan de olika komponenterna finns IPMB som beskrivs i 2.3.2 IPMB.

2.3.1 BMC

Baseboard management controller är en mikrokontroller placerad på moderkortet som är dedikerad till IPMI. BMC är den mest centrala komponenten i IPMIs arkitektur då alla resterande medverkande moduler är anslutna till denna. Den kan beskrivas som interfacet mellan systemets management mjukvara och systemets management hårdvara. Systemets management mjukvara innebär den mjukvara som används för att ansluta till BMCn och systemets management hårdvara syftar till den hårdvara BMCn har kontakt med. Det finns ofta flera Management Controllers i systemet som ansvarar för olika delar i systemet, exempelvis chassi. IPMB är den buss som ansluter Management Controller till BMC. En management controller kan ha Private Management Busses, vilket innebär att bussen endast är till för management kontrollern i fråga. Dessa används oftast till SEEPROMs som kan innehålla exempelvis FRU (Field Replaceable Unit) information. [1, pp. 12, 29]

2.3.2 IPMB

IPMB Intelligent Platform Management Bus är den främsta I²C baserade buss som går runt till de olika modulerna i systemet som är anslutna till BMCn. Exempel på moduler som är anslutna via IPMB är Management Controller,

ICMB och BMC. Kommunikationen över IPMB adresseras i form av Logical Units (LUN). [1, pp. 67]

2.4 Sensor Data Record

IPMI är ett anpassningsbart och skalbart interface och omgivningen kan variera. BMCn kan inte på förväg veta vilka komponenter som finns kopplade via IPMB. Information om detta kan dock skickas från övriga Management Controllers till BMCn genom ”Capabilities Commands” och SDRs. Denna information beskriver i stort sett vad det är för något, vilken information den kan leverera och vilka kommandon den kan hantera. BMCn har en dedikerad lagring som kallas Sensor Data Record Repository, där SDR information lagras. [1, pp, 15]

2.5 FRU

Field Replaceable Unit (FRU) information finns åtkomligt via IPMI. Exempel på information som kan finnas är serienummer, modell och tillverkare. Informationen kan kommas åt via management controller genom IPMI kommandon. BMCn kan även lagra Information om FRU i ett SEEPROM dedikerat för FRU information. [1, pp. 15-16]

2.6 Platform Event Filtering (PEF)

PEF används för att konfigurera IPMI att utföra en viss uppgift när ett Event Message inkommer eller genereras internt. Detta kan innebära att systemet stängs av, startas om eller att ett larm skickas. IPMI har stöd för att exempelvis skicka SNMP traps över en LAN anslutning. När IPMI skickar SNMP traps över LAN anvämds formatet Platform Event Trap (PET) vilket ger mottagaren möjlighet att skicka en bekräftelse på att ett trap har mottagits. Det finns även möjlighet att skapa Alert Policies över hur ett larm ska hanteras. Ett exempel på detta är att ett larm först skickas till ett IP och om detta misslyckas skickas det till ett andra alternativ. [1. pp. 20]

2.7 IPMI över LAN

IPMI kommandon kan skickas över LAN till en BMC. Detta görs via ett LAN interface. Ett LAN Interface kan dedikeras för BMCn, men delas ofta tillsammans med övriga systemet. Om interfacet delas med övriga systemet detekteras IPMI trafik genom IPMIs management portnummer. Trafik som ska till BMCn skickas går från LAN kontrollern till BMCn via en System Management Bus (SMBus). IPMI kommunikationen över LAN är sessionsbaserad vilket ger möjlighet för autentisiering samt flera IPMI sessioner över samma kanal, till skillnad från intern kommunikation över IPMB som är sessionslös. För att skicka IPMI kommandon över LAN

används Remote Control Management Protocol som beskrivs närmre i 2.6.1 RCMP. [1. pp. 122]

2.7.1 RCMP

RCMP är ett protokoll som används för att skicka IPMI kommandon över LAN med UDP. De två vanligaste portarna som RCMP använder är 623 och 664, där den sistnämnda används vid krypterad trafik. RCMP kapslar in IMPI för att kunna skickas över nätverk. RCMP kan även användas för att kapsla in OEM (Original Equipment Manufacturer) och ASF (Alerting Standard Forum). Vilken typ av data som är inkapslat specifieras i RCMP headern under Class of Message. Headern innehåller även version, sekvensnummer, ett reserverat fält och RCMP data. RCMP data innehåller den inkapslade datan som skickas med. RCMP är således en ganska minimalt och simpelt protokoll. Eventuella mer avancerade funktioner förlitas till den inkapslade datan. [1. pp. 123-125]

2.7.2 RCMP+

RCMP+ är i grunden samma protocol som RCMP men tillför några extra funktioner. Paketformatet är densamma och förändringarna sker istället i den inkapslade datan. RCMP+ ger möjlighet att kryptera trafiken vilket är en stor fördel vid överföring av känslig data. Det finns även stöd för att skicka med OEM payloads i en IPMI session. Säkrare autentisieringmetod har tillkommit med hjälp av nycklar och stödet för ASF 2.0 är förbättrat. Eftersom förändringarna sker i den inkapslade datan är RCMP+ främst en benämning för att kommunikationen har stöd för dessa funktioner. IPMI v2.0 är den version av IPMI som har stöd för detta och det är här de egentliga förändringarna skett. [1. pp. 128-134]

2.8 IPMI kommunikation interface

IPMI har flera olika interface för kommunikation mellan BMCn och systemets mjukvara. Dessa är System Management Interface Chip (SMIC), Keyboard Controller Style (KCS) och Block Transfer (BT). Det finns även Intelligent Chassis Management Bus (ICMB), LAN och seriell/modem interface för kommunikation från ett remote system. [1. pp. 44]

2.8.1 Channel Access

De kanaler som är sessionsbaserade (exempelvis LAN) kan konfigureras till olika Access Modes. Kanal i det här fallet syftar till det interface/buss kommunikationen går via. Det innebär att tillgängligheten på en kanal kan variera beroende på systemets status. Följande Access Modes finns: Pre-boot Only, Always Available, Shared och Disabled. Pre-Boot Only innebär att kanalen endast är tillgänging när systemet är avstängt. Shared innebär att

kanalen kan delas mellan BMCn och systemets mjukvara. Always Available innebär att kanalen är helt dedikerad för BMCn samt att den är tillgänglig i alla systemets lägen. När en kanal är Disabled går BMCn inte att komma åt via den kanalen. Access Mode påverkar dock inte larm, vilket innebär att ett SNMP traps kan skickas via en kanal äve om den är Disabled. Larm har egna Channel Access kommandon för att konfigurera hur en kanal ska hantera larm. [1. pp. 47-48]

2.8.2 Privilege Levels

Varje kanal kan ha en egen uppsättning användare som har specifika behörigheter över just den kanalen. Det finns en antal behörighetsnivåer, dessa binds till en viss användare över en viss kanal. Det går även att begränsa vilken behörighetsnivå som är den högst tillåtna på en kanal. De nivåer som finns är Callback, User, Operator och Administrator. Administrator har högst behörighet och kan i princip utföra alla kommandon som finns tillgängliga i systemet. En Operator för utföra alla kommandon förutom de som kan påverka något interface/kanal eller ändra behörigheter. User får läsa data och göra status förfrågningar mot BMCn, dock får inga kommandon som kan ändra konfiguration eller skriva data utföras. Callback är den lägsta behörighetsnivån som endast tillåter kommandon som initierar ett Callback. [1. pp. 48]

3 Diskussion

IPMI är ett intressant management interface på många vis. Kanske främst för att det bygger på egna komponenter och kan arbeta oberoende från övriga systemets operativsystem. Detta ger ett stort övertag gällande tillgängligheten då IPMI kan vara åtkomligt så länge strömförsörjning finns. Arkitekturen är modulärt uppbyggt vilket gör det väldigt anpassningsbart. IPMI anpassar sig efter vilken miljö den befinner sig i genom att ta reda på information om vilka komponenter som finns anslutna till BMCn. Detta är också ett av målen med IPMI, just att det ska vara skalbart och kunna anpassa sig allt eftersom tekniken utvecklas [1, pp. 7]. IPMI har många funktioner och denna rapportern berör endast vissa av dem. När jag började efterforska kring IPMI visade det sig att det var mer avancerat och hade fler funktioner än jag hade trott på förhand, vilket gjorde att jag valde att skriva om de saker jag tyckte kunde vara bra att veta samt intressanta.

4 Referenser

[1] Intel Corporation. (2004, February 12.). Intelligent Platform Management Specification Second Generation v2.0. [Online]. Available: download.intel.com/design/servers/ipmi/IPMIv2_0rev1_0.pdf