Zdalne zarządzanie: BMC, IPMI i Redfish w osobnej sieci

Poziom: średnio

Dotyczy: serwery z BMC (iDRAC, iLO, XClarity i podobne), ipmitool 1.8, Redfish, FortiGate 100F

Czas: ~60 min

BMC to mały komputer w serwerze, który działa także wtedy, gdy system leży albo serwer jest wyłączony, i pozwala go włączyć, zobaczyć ekran i odczytać czujniki przez sieć. Wyjaśniamy BMC, IPMI i Redfish, konsole producentów i to, dlaczego BMC trzymamy w osobnej sieci, do której wchodzi tylko administrator przez VPN. Proponujemy też sieć zarządzania VLAN 98 dla Zielonej, do zatwierdzenia przez autora bazy.

ZAŁOŻENIA SCENARIUSZA

BMC serwerów stoją w VLAN 98 (10.20.98.0/24), którego bramą jest pojedynczy `fw01` (10.20.98.1), bez dostępu do internetu i z wejściem z VPN administratorów. W parze FortiGate adres 10.20.98.1 należy do pary, a sztuki mają własne adresy zarządzania: Para FortiGate w klastrze: FGCP aktywny-pasywny.

Skróty użyte na tej stronie (22)

Skrót	Co znaczy
BIOS	Basic Input/Output System: oprogramowanie płyty głównej, które startuje komputer
BMC	Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników
CVE	Common Vulnerabilities and Exposures: publiczny numer katalogowy konkretnej luki bezpieczeństwa, ten sam numer identyfikuje ją u każdego producenta
DMTF	Distributed Management Task Force: organizacja, która opracowała standard Redfish
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
iDRAC	Zdalny kontroler zarządzania w serwerach Dell, pokazuje m.in. pobór mocy serwera
iLO	Zdalny kontroler zarządzania w serwerach HPE, pokazuje m.in. pobór mocy serwera

Skrót	Co znaczy
IPMI	Intelligent Platform Management Interface: standard, przez który administrator pyta kontroler BMC serwera o temperatury, napięcia i obroty wentylatorów
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
JSON	JavaScript Object Notation: tekstowy format danych z klamrami i cudzysłowami
KVM	Keyboard, Video, Mouse: konsola albo przełącznik, który daje jedną klawiaturę, ekran i mysz do wielu serwerów (w Linuksie KVM to też technika wirtualizacji)
LAN	Local Area Network: sieć lokalna; w BMC port LAN to jego własne gniazdo sieciowe
NAS	Network Attached Storage: dysk sieciowy
RAKP	Remote Authenticated Key-Exchange Protocol: część uwierzytelniania IPMI 2.0, z którego atakujący może odebrać skrót hasła i zgadywać je offline (CVE-2013-4786)
REST	sposób budowania API przez zwykłe żądania HTTP (GET, POST) zamiast osobnego protokołu
RMCP	Remote Management and Control Protocol: protokół UDP na porcie 623, którym ipmitool rozmawia z BMC; wersja RMCP+ to lanplus
SEL	Select: pin wyboru interfejsu czujnika pyłu SPS30, który po połączeniu z masą włącza komunikację I2C
SNIA	Storage Networking Industry Association: organizacja standardów pamięci masowych, autor Swordfish, rozszerzenia Redfish
UDP	User Datagram Protocol: szybki protokół sieciowy bez potwierdzeń
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

□□ ZMIENIA SYSTEM

Odczyt informacji o BMC: ipmitool mc info

```
export IPMI_PASSWORD='HasloKontaBMC'
ipmitool -I lanplus -H AdresBMC -U NazwaUsera -E mc info
```

> (gdzie `AdresBMC` to adres BMC serwera, na przykład 10.20.98.22 dla `hv02`, a `NazwaUsera` to konto BMC; opcja `-E` czyta hasło ze zmiennej, żeby nie wisiało w historii poleceń i liście procesów)

Przykład (poglądowy, hv02):

```
Device ID                 : 32
Device Revision           : 1
Firmware Revision         : 6.10
IPMI Version              : 2.0
Manufacturer ID           : 674
Product ID                : 2243
```

Wersja firmware BMC jest tą liczbą, którą porównujemy z biuletynami producenta przy aktualizacji.

BMC = Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników · **export** = ustaw zmienną środowiskową widoczną dla uruchamianych programów · **ipmitool** = Intelligent Platform Management Interface tool: program, który przez IPMI pyta kontroler BMC serwera o czujniki, np. sdr type temperature wypisuje temperatury

TYLKO ODCZYT

Odczyt ustawień sieci BMC z systemu: ipmitool lan print

```
sudo ipmitool lan print 1
```

> (gdzie `1` to numer kanału LAN, najczęściej 1, a komenda działa na samym serwerze, bez sieci, przez sterownik IPMI)

Przykład (poglądowy, ora01):

```
IP Address Source       : Static Address
IP Address              : 10.20.98.32
Subnet Mask             : 255.255.255.0
Default Gateway IP      : 10.20.98.1
MAC Address             : aa:bb:cc:dd:ee:32
```

□□ **BMC** = Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników ·**LAN** = Local Area Network: sieć lokalna; w BMC port LAN to jego własne gniazdo sieciowe ·**IPMI** = Intelligent Platform Management Interface: standard, przez który administrator pyta kontroler BMC serwera o temperatury, napięcia i obroty wentylatorów · **ipmitool** = Intelligent Platform Management Interface tool: program, który przez IPMI pyta kontroler BMC serwera o czujniki, np. sdr type temperature wypisuje temperatury

□□ ZMIENIA SYSTEM

Ustawienie stałego adresu BMC: ipmitool lan set

```
sudo ipmitool lan set 1 ipsrc static
sudo ipmitool lan set 1 ipaddr 10.20.98.32
sudo ipmitool lan set 1 netmask 255.255.255.0
sudo ipmitool lan set 1 defgw ipaddr 10.20.98.1
```

Komendy można wykonać jako blok. Zmieniają adres, pod którym działa BMC, więc robimy to z konsoli albo z samego serwera, a nie przez połączenie, które ten adres zerwie.

□□ **BMC** = Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników ·**ipmitool** = Intelligent Platform Management Interface tool: program, który przez IPMI pyta kontroler BMC serwera o czujniki, np. sdr type temperature wypisuje temperatury

□□ TYLKO ODCZYT

Wylistowanie kont BMC: ipmitool user list

```
sudo ipmitool user list 1
```

Pokazuje konta, ich numery i poziomy uprawnień. Konto domyślne producenta ma być zmienione lub wyłączone przy montażu.

□□ **BMC** = Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników ·**ipmitool** = Intelligent Platform Management Interface tool: program, który przez IPMI pyta kontroler BMC serwera o czujniki, np. sdr type temperature wypisuje temperatury

□□ ZMIENIA SYSTEM

Utworzenie konta do odczytu dla Zabbixa: ipmitool user set

```
sudo ipmitool user set name NumerKonta zabbix_bmc
sudo ipmitool user set password NumerKonta
sudo ipmitool user priv NumerKonta 2 1
sudo ipmitool channel setaccess 1 NumerKonta callin=on ipmi=on link=on privilege=2
sudo ipmitool user enable NumerKonta
```

> (gdzie `NumerKonta` to wolny numer konta z `ipmitool user list 1`, na przykład 3; poziom uprawnień 2 to USER, czyli odczyt bez sterowania zasilaniem; drugie polecenie zapyta o hasło)

Konto z rolą tylko do odczytu wystarcza monitoringowi i nie pozwala mu wyłączyć serwera. Producenci mają też własne menu użytkowników w BMC i tam robimy to samo, jeśli wolimy.

BMC = Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników · **ipmitool** = Intelligent Platform Management Interface tool: program, który przez IPMI pyta kontroler BMC serwera o czujniki, np. sdr type temperature wypisuje temperatury

TYLKO ODCZYT

Odczyt stanu zasilania serwera: ipmitool chassis power status

```
ipmitool -I lanplus -H AdresBMC -U NazwaUsera -E chassis power status
```

Przykład: `Chassis Power is on`. Do włączania i wyłączania są osobne polecenia (`power on`, `power off`, `power cycle`), ale z kont do odczytu ich nie wywołamy, i tak ma zostać.

ipmitool = Intelligent Platform Management Interface tool: program, który przez IPMI pyta kontroler BMC serwera o czujniki, np. sdr type temperature wypisuje temperatury

ZMIENIA SYSTEM

Sprawdzenie, czy Redfish odpowiada: curl /redfish/v1/

```
export REDFISH_HASLO='HasloKontaBMC'
curl -s --cacert PlikCertyfikatuCA -u "NazwaUsera:$REDFISH_HASLO"
https://AdresBMC/redfish/v1/ | jq '{RedfishVersion, Systems, Chassis, Managers}'
```

> (gdzie `PlikCertyfikatuCA` to certyfikat urzędu, który podpisał certyfikat BMC; do pierwszej próby na BMC z certyfikatem producenta bywa potrzebna opcja `-k`, ale tylko tymczasowo, w sieci zarządzania)

Przykład (poglądowy):

```
{
  "RedfishVersion": "1.15.1",
  "Systems": { "@odata.id": "/redfish/v1/Systems" },
  "Chassis": { "@odata.id": "/redfish/v1/Chassis" },
  "Managers": { "@odata.id": "/redfish/v1/Managers" }
}
```

Adres główny `/redfish/v1/` jest taki sam u wszystkich producentów. Nazwy zasobów pod nim (identyfikatory systemu i obudowy) różnią się, więc je odczytujemy z odpowiedzi, a nie zgadujemy.

BMC = Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników · **export** = ustaw zmienną środowiskową widoczną dla uruchamianych programów · **curl** = client URL: pobieranie i wysyłanie przez HTTP z terminala

TYLKO ODCZYT

Odczyt stanu systemu przez Redfish: curl /redfish/v1/Systems

```
curl -s --cacert PlikCertyfikatuCA -u "NazwaUsera:$REDFISH_HASLO"
https://AdresBMC/redfish/v1/Systems | jq '.Members'
curl -s --cacert PlikCertyfikatuCA -u "NazwaUsera:$REDFISH_HASLO"
https://AdresBMC/redfish/v1/Systems/NazwaSystemu | jq '{Model, PowerState, Status,
ProcessorSummary, MemorySummary}'
```

> (gdzie `NazwaSystemu` to identyfikator z listy `Members`, na przykład `1` u części producentów albo `System.Embedded.1` u Dell)

Pierwsza komenda pokazuje, jakie systemy BMC zna, a druga czyta stan wybranego: model, zasilanie, zdrowie oraz podsumowanie procesorów i pamięci.

BMC = Baseboard Management Controller: osobny malutki komputer na płycie serwera, który działa nawet przy wyłączonym serwerze i odczytuje m.in. temperatury czujników · **curl** = client URL: pobieranie i wysyłanie przez HTTP z terminala

Z życia wzięte

Z ŻYCIA WZIĘTE

Sobota, 23:10. Zabbix zgłasza, że `ora01` nie odpowiada, a Marek planuje rano zmianę 6:00 na WMS. Z domu otwieramy VPN, wchodzimy w konsolę BMC pod adresem 10.20.98.32 i widzimy na wirtualnym ekranie komunikat o błędzie dysku systemowego przy starcie. Montujemy obraz ratunkowy jako wirtualny napęd, naprawiamy bootloader i o 23:50 serwer wstaje, bez jazdy do Pamiątkowa.

Skąd się wzięło

Pierwsze zdalne sterowanie serwerami wykonywano przez port szeregowy i przełączniki KVM (urządzenia, które przekazują ekran, klawiaturę i mysz serwera przez sieć). W 1998 roku firmy Intel, HP, NEC i Dell opublikowały specyfikację IPMI 1.0 (Intelligent Platform Management Interface), czyli wspólny sposób zarządzania serwerem niezależnie od jego systemu operacyjnego [1]. Specyfikacja opisała czujniki, dziennik zdarzeń, sterowanie zasilaniem i dostęp przez sieć.

IPMI okazało się jednak niewygodne w nowoczesnych narzędziach i miało słabości bezpieczeństwa. W 2013 roku opublikowano lukę w uwierzytelnianiu IPMI 2.0 (CVE-2013-4786), a w 2015 roku DMTF wydało Redfish 1.0, interfejs oparty na HTTPS i formacie JSON [2][3]. Redfish ma czytelne adresy, rozszerzalne schematy i zwykłe narzędzia (curl, przeglądarka, Python), więc dziś producenci dodają go do każdego nowego BMC.

Układ BMC ASPEED AST2400 na płycie serwera. To osobny procesor z własną pamięcią i systemem,

Układ BMC ASPEED AST2400 na płycie serwera. To osobny procesor z własną pamięcią i systemem, który pracuje, nawet gdy główny procesor jest wyłączony. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

Rodzaje i zasada działania

BMC: komputer w komputerze

> **Pojęcie: BMC (Baseboard Management Controller).** Osobny, mały procesor na płycie serwera z własnym oprogramowaniem i własnym portem sieciowym. Czyta czujniki, steruje wentylatorami i zasilaniem, udostępnia konsolę wirtualną i działa, gdy zasilanie główne jest wyłączone, a w gniazdach jest prąd.

BMC rozmawia z czujnikami (temperatury, napięcia, wentylatory, zasilacze) i zapisuje zdarzenia w dzienniku (SEL). Z systemu serwera rozmawia przez wewnętrzny interfejs, a z siecią przez własny port, najlepiej dedykowany, a nie współdzielony z kartą sieciową serwera.

Schemat blokowy IPMI: BMC w środku, czujniki i zasilanie po jednej stronie, sieć zarządzania po drug

Schemat blokowy IPMI: BMC w środku, czujniki i zasilanie po jednej stronie, sieć zarządzania po drugiej. Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

IPMI

IPMI to starszy standard z 1998 roku, nadal obecny w większości serwerów. Używa protokołu UDP na porcie 623, a nowszą wersję tego połączenia (IPMI 2.0) nazywa się RMCP+ (lanplus). Narzędzie `ipmitool` jest ogólnym klientem.

Zalety IPMI: działa wszędzie i ma gotowy klient w Zabbixie. Wady: stara kryptografia, ograniczone hasła i luka w uwierzytelnianiu opisana niżej.

Redfish

> **Pojęcie: Redfish.** Standard DMTF z 2015 roku, w którym BMC udostępnia dane i operacje jako zwykły interfejs REST po HTTPS, z odpowiedziami w JSON. Zasoby mają stałą strukturę (`/redfish/v1/Systems` , `/Chassis` , `/Managers`), a detale producenta dochodzą jako rozszerzenia.

Redfish pozwala odczytać czujniki, firmware, dysk i pamięć, a także wykonywać akcje (restart, aktualizacja). Dla administratora z jego przyzwyczajeniami to zwykła komenda `curl` i JSON przetwarzany przez `jq`. Rozszerzeniem Redfish dla pamięci masowych jest Swordfish organizacji SNIA.

Konsole producentów

Każdy producent dodaje do BMC własny interfejs webowy: iDRAC w serwerach Dell, iLO w HPE, XClarity Controller w Lenovo, a w Supermicro po prostu BMC z interfejsem IPMI. Pokazują stan serwera, dziennik zdarzeń, czujniki i dają dostęp do konsoli wirtualnej. Nazwy to przykłady klas rozwiązań, a nie rekomendacja.

W niektórych modelach część funkcji (konsola wirtualna, wirtualne nośniki, zdalna aktualizacja) wymaga osobnej licencji. Sprawdzamy to w ofercie, żeby po odbiorze nie okazało się, że konsola nie działa.

Konsola wirtualna i wirtualne nośniki

Konsola wirtualna pokazuje ekran serwera i przekazuje klawiaturę oraz mysz przez przeglądarkę, więc widzimy start serwera, BIOS i błędy bootloadera. Wirtualne nośniki pozwalają zamontować plik ISO z komputera administratora albo z udziału sieciowego jako napęd w serwerze, co wystarcza do instalacji lub naprawy systemu.

□□ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: konsola BMC serwera `hv02` z wirtualnym ekranem w trakcie startu i menu „Wirtualne nośniki" z zamontowanym obrazem ISO. Nazwy menu zależą od producenta, więc podpisujemy zrzut modelem serwera.

Złącza na tylnej płycie płyty serwerowej Supermicro: obok portów danych jest osobne gniazdo LAN d

□□ Złącza na tylnej płycie płyty serwerowej Supermicro: obok portów danych jest osobne gniazdo LAN dla BMC (IPMI). Źródło: Wikimedia Commons (autor i wolna licencja podane na stronie pliku).

Bezpieczeństwo BMC

BMC ma pełną władzę nad serwerem: włącza, wyłącza, instaluje system i zmienia firmware. Dlatego jest jednym z najlepszych celów dla atakującego, który wejdzie do sieci. Zasady, które stosujemy zawsze:

- BMC stoi w osobnej sieci zarządzania, bez drogi do internetu i bez dostępu z biura.
- Domyślne konto producenta zmieniamy albo wyłączamy, hasła mają co najmniej kilkanaście losowych znaków.
- Konto monitoringu ma rolę tylko do odczytu.

- Firmware BMC aktualizujemy w planie przeglądów, bo podatności w BMC są publikowane regularnie.
- IPMI przez LAN wyłączamy tam, gdzie wystarcza Redfish, a gdzie jest potrzebne, wybieramy najsilniejszy zestaw szyfrów, jaki BMC obsługuje (opcja `-C 17` w `ipmitool`).
- Certyfikat BMC podpisujemy własnym urzędem, żeby klient mógł zweryfikować serwer.

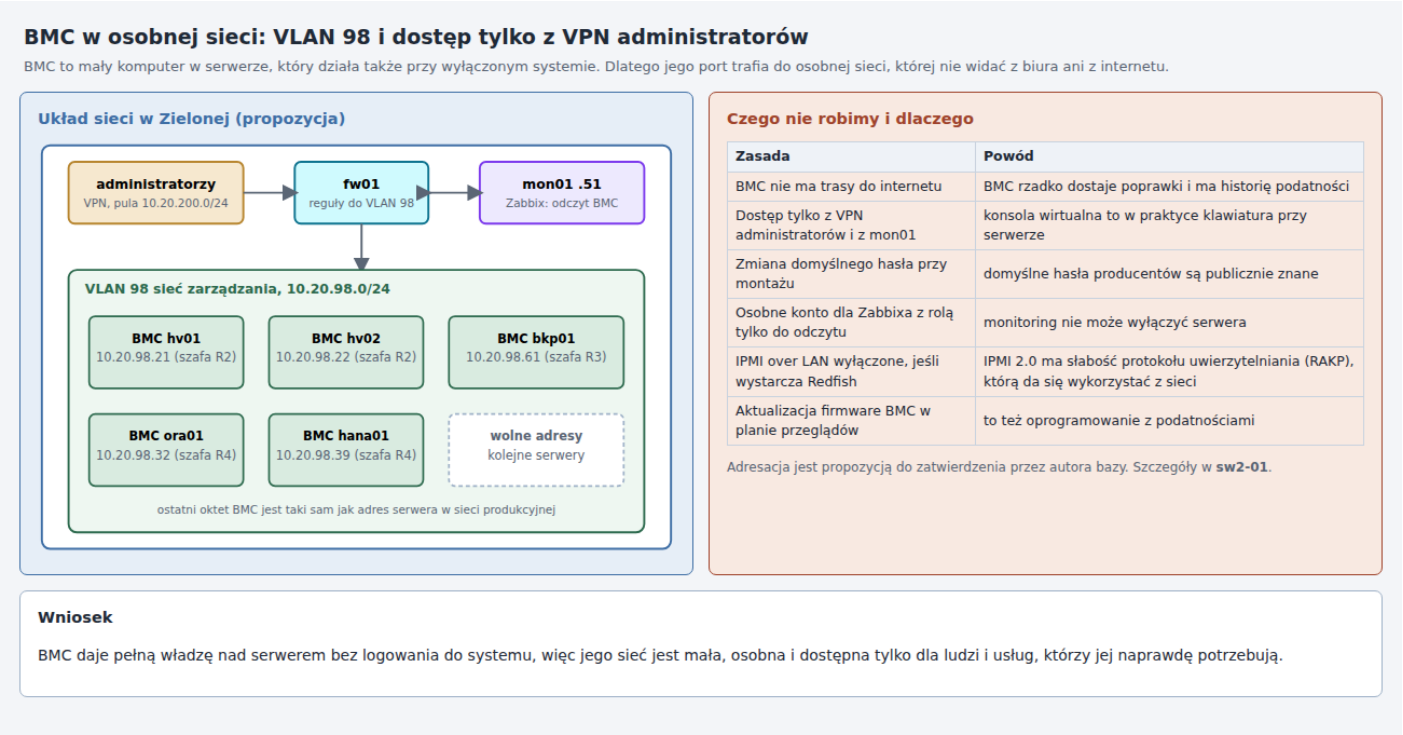
> **Pojęcie: luka RAKP w IPMI 2.0.** Protokół uwierzytelniania IPMI 2.0 (RAKP) pozwala atakującemu, który może wysłać pakiet do BMC, odebrać odpowiedź zawierającą skrót hasła użytkownika i zgadywać hasło offline. Opis w rejestrze CVE-2013-4786 mówi, że jest to cecha samej specyfikacji, więc nie da się jej w pełni załatać [3].

Skutek praktyczny: ochrona to mocne, długie hasło i niedostępność portu 623 z sieci, w której mógłby być atakujący. To właśnie robi osobna sieć zarządzania.

Sieć zarządzania VLAN 98 w Zielonej (propozycja)

Dla Zielonej proponujemy osobną sieć zarządzania, VLAN 98, o adresacji 10.20.98.0/24 (do zatwierdzenia przez autora bazy; w bazie nie ma jeszcze takiej sieci). Zapora `fw01` ma w niej adres 10.20.98.1 i filtruje dostęp. Adres BMC ma ten sam ostatni oktet co adres serwera w sieci serwerowej, żeby nie trzeba było pamiętać tabeli.

Serwer	Szafa	Adres serwera	Adres BMC (VLAN 98)
`hv01`	R2	10.20.10.21	10.20.98.21
`hv02`	R2	10.20.10.22	10.20.98.22
`bkp01`	R3	10.20.10.61	10.20.98.61
`ora01`	R4	10.20.10.32	10.20.98.32
`hana01`	R4	10.20.10.39	10.20.98.39



Rysunek 1. Sieć zarządzania VLAN 98 z pięcioma BMC, zaporą fw01, VPN administratorów i serwerem mon01 oraz zasady, których przestrzegamy. (kliknięcie otwiera pełny rozmiar)

Reguły na `fw01`, które proponujemy (porty konsoli wirtualnej i wirtualnych nośników zależą od producenta i generacji BMC, więc sprawdzamy je w dokumentacji):

Źródło	Cel	Port	Po co
pula VPN administratorów 10.20.200.0/24 (tylko grupa administratorów)	10.20.98.0/24	TCP 443	konsola webowa i Redfish
pula VPN administratorów	10.20.98.0/24	porty konsoli według producenta	konsola wirtualna i nośniki
`mon01` 10.20.10.51	10.20.98.0/24	TCP 443, UDP 623	odczyt przez Redfish albo IPMI
10.20.98.0/24	`dc01` 10.20.10.11	UDP 123	czas dla dziennika BMC (do ustalenia)
wszystko inne	10.20.98.0/24 i z niej	brak	blokada, bez trasy do internetu

Gdy `gpu01` ma BMC, jego adres w tej sieci rezerwujemy jako 10.20.98.45, ale czy ma, do potwierdzenia. Wpisy dodajemy do NetBoxa.

Wszystkie rodzaje w jednej tabeli

Cecha	IPMI over LAN	Redfish	Konsola producenta
Rok	1998	2015	różnie
Protokół	UDP 623 (RMCP+)	HTTPS, JSON	HTTPS, aplikacja webowa
Narzędzia	`ipmitool`, Zabbix IPMI	`curl`, `jq`, Python	przeglądarka
Bezpieczeństwo	słabsze (RAKP)	TLS i konta	TLS i konta
Do czego	czujniki, zasilanie, dziennik	czujniki, firmware, akcje	pełna obsługa i konsola
Licencja	zwykle bez	zwykle bez	część funkcji płatna

W serwerowni

Przy montażu nowego serwera wykonujemy stały zestaw czynności: ustawiamy adres BMC w VLAN 98, zmieniamy hasło konta domyślnego, zakładamy konto do odczytu dla Zabbixa, instalujemy certyfikat i wpisujemy serwer do NetBoxa. Port BMC łączymy z przełącznikiem zarządzania w szafie, osobnym od przełączników serwerowych, a kabel oznaczamy.

Monitoring: Zabbix odczytuje BMC z `mon01` przez Redfish albo IPMI, a opis skryptu jest na stronie Odczyt czujników BMC do Zabbixa. Ten sam kanał pokazuje stan zasilaczy i wentylatorów z Zasilacze, wentylatory i diagnostyka.

Poza serwerownią BMC występuje w serwerach w oddziałach, a w domu w serwerach NAS klasy serwerowej i płytach z IPMI. Te same zasady dotyczą kamer i rejestratorów, które także mają zdalny dostęp: osobny segment, zmienione hasło i aktualizacje.

Co sprawdzamy u dostawcy

- Obecność BMC w każdym serwerze, osobny port sieciowy BMC i rodzaj licencji (konsola wirtualna, wirtualne nośniki).
- Obsługę Redfish w oferowanej wersji firmware i dostępność dokumentacji interfejsu.
- Hasło konta domyślnego zmienione przy odbiorze, a nie pozostawione z fabryki.
- Możliwość wyłączenia IPMI przez LAN i listę obsługiwanych zestawów szyfrów.
- Politykę aktualizacji firmware BMC producenta i czas publikacji poprawek bezpieczeństwa.
- Konto do odczytu dla monitoringu i konto administracyjne oddzielne od niego.
- Próbę dostępu z VPN przy odbiorze: konsola wirtualna, montowanie ISO, odczyt czujników.

Mity i sprostowania

Obiegowa wersja	Jak jest naprawdę
BMC działa tylko, gdy serwer jest włączony	Działa też przy wyłączonym serwerze, jeśli w gniazdach jest prąd
Zmiana domyślnego hasła wystarczy	Dodatkowo potrzebna jest osobna sieć, bo luka RAKP wyciąga skrót hasła z BMC
VLAN sam w sobie zabezpiecza	Zabezpiecza razem z regułami zapory, a bez nich wszyscy w VLAN-ie widzą wszystkich
IPMI jest przestarzałe i nie trzeba się nim zajmować	Wciąż jest włączone w większości BMC, więc wyłączamy je świadomie, jeśli go nie używamy
BMC to zabezpieczenie serwera	BMC to też powierzchnia ataku, jak każdy serwer z własnym systemem

Oś czasu

Data	Wydarzenie
1998	Intel, HP, NEC i Dell publikują IPMI 1.0
2013	Opublikowanie CVE-2013-4786, luki RAKP w IPMI 2.0
2015	DMTF publikuje Redfish 1.0

Częste błędy

Objaw	Przyczyna	Co robimy
`ipmitool` wisi i kończy z limitem czasu	brak reguły UDP 623 albo zły adres	sprawdzamy regułę `fw01` i adres BMC
`curl` zgłasza błąd certyfikatu	certyfikat producenta	instalujemy certyfikat z własnego urzędu, nie wyłączamy sprawdzania na stałe
BMC odpowiada z sieci serwerowej	port BMC współdzielony z kartą serwera	przestawiamy BMC na dedykowany port w VLAN 98
Konto monitoringu może restartować serwer	rola administratora zamiast odczytu	zmieniamy poziom uprawnień na USER
Konsola wirtualna nie działa po aktualizacji	zmiana wymagań przeglądarki lub licencji	sprawdzamy notatki wydania i licencję

□□ Ćwiczenia

1. Dlaczego adres BMC `hana01` w VLAN 98 to 10.20.98.39?

Odpowiedź

Bo przyjęliśmy zasadę, że ostatni oktet BMC jest taki sam jak adres serwera w sieci serwerowej (`hana01` ma 10.20.10.39), żeby nie pamiętać osobnej tabeli.

1. Chcemy, żeby Zabbix odczytywał czujniki BMC, ale nie mógł wyłączyć serwera. Co robimy?

Odpowiedź

Zakładamy w BMC osobne konto z rolą tylko do odczytu (poziom USER w IPMI albo rola odczytu w Redfish) i tylko je wpisujemy w makrach Zabbixa.

1. Dlaczego silne hasło nie wystarcza do zabezpieczenia IPMI 2.0?

Odpowiedź

Bo luka RAKP pozwala atakującemu, który dotrze do portu 623, odebrać skrót hasła i zgadywać je offline. Mocne hasło utrudnia to bardzo, ale nie zastępuje odcięcia portu od wszystkich poza administratorami i monitoringiem.

Powiązane: Serwer od środka: od szafy mainframe'u do bursztynowej diody na hv02 · Zasilacze, wentylatory i diagnostyka · Firmware i wymiana na gorąco · Odczyt czujników BMC do Zabbixa · Serwerownia Zielonej: mapa czujników

Źródła:

1. en.wikipedia.org: Intelligent Platform Management Interface
2. DMTF, ogłoszenie Redfish 1.0 z 4 sierpnia 2015: dmtf.org
3. Rejestr CVE: CVE-2013-4786 oraz biuletyn Dell: IPMI v2.0 Password Hash Disclosure
4. Strona podręcznika: ipmitool

Revision #13
Created 2026-10-03 15:34:24 UTC by Tomasz Konieczny
Updated 2026-10-26 14:22:46 UTC by Tomasz Konieczny