



Stärk säkerheten med
**3,5 gånger fler
säkerhetsfunktioner**

Inklusive tvåfaktorsautentisering
och extern nyckelhantering med
iDRAC9



Optimera
energieffektiviteten
med mer än
**6 gånger fler
strömförbrukning
srapporter**

Med 20 rapporter i Dell OME
jämfört med 3 rapporter i
Supermicro SSM



**Öka
driftseffektiviteten
genom att spara
1 tim 50 min i
administratörstid
per 100 servrar**

Använda automatiska
uppdateringar med Dell iDRAC9
jämfört med inga automatiska
uppdateringar tillgängliga med
Supermicro IPMI

Öka säkerheten, hållbarheten och effektiviteten med robusta serverhanteringsverktyg från Dell

Jämfört med Supermicros hanteringsportfölj

När du investerar i nya servrar för ditt datacenter gör du mer än att bara välja hårdvara – du väljer också en hanterbarhetslösning. När administratörerna har tillgång till effektiva verktyg med flera funktioner för att installera, övervaka, underhålla och skydda infrastrukturen samtidigt som de förbättrar energieffektiviteten, kan de enkelt hantera den dagliga hanteringen och ägna mer tid åt innovationer som driver företaget framåt. Genom att handla från en leverantör med robusta hanteringsverktyg kan du spara tid och pengar.

Vi utvärderade serverhanteringsportföljerna för Dell™ och Supermicro® och jämförde tre verktyg från Dell med två verktyg från Supermicro.

Tabell 1: Hanteringsverktygen vi testade. * Dell CloudIQ är ett molnbaserat övervaknings- och analysverktyg. Supermicro erbjuder inget motsvarande verktyg. Källa: Principled Technologies.

	Dell	Supermicro
Inbyggd serverhantering/ fjärrhantering	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
Enhetshanteringskonsol för en-till-många	Dell OpenManage™ Enterprise (OME) Dell CloudIQ*	Supermicro Server Manager (SSM)

När det gäller hållbarhet, säkerhet och daglig hantering såg vi att Dell konsekvent tillhandahöll mer funktionsrika verktygsuppsättningar som ger administratörer fler alternativ och funktioner.

Fler och mer omfattande funktioner för att automatisera och förenkla serverhanteringen

IT-teamen behöver moderna hanteringsverktyg med många funktioner som kan spara tid i det dagliga arbetet och hålla jämna steg med standarder för säkerhet och effektivitet. Dells hanteringsverktyg som vi utvärderade omfattar ett antal funktioner som inte finns i Supermicros hanteringsportfölj.

Hållbarhet

I takt med att energikostnaderna ökar och miljöreglerna ökar fokuserar många organisationer på hållbarhet. Datacenter kräver i sig stora mängder ström, men noggrann hantering av värme- och strömförbrukning kan göra det möjligt för företag att minska den mängd ström de förbrukar. Dell OpenManage Enterprise innehåller flera funktioner som kan möjliggöra noggrann övervakning och hantering av strömförbrukning, vilket kan hjälpa dig att nå dina hållbarhetsmål. I tabellerna 2 och 3 anges de viktigaste fördelarna med dessa funktioner, som vi beskriver mer detaljerat nedan.

Tabell 2: Hållbarhetsskillnader mellan Dell OpenManage Enterprise och SSM. Källa: Principled Technologies.

Funktionen	Dells hanteringsverktyg		Supermicros hanteringsverktyg
Kalkylator för koldioxidutsläpp och verktyg för kapacitetsplanering		✓	x
Analys av koldioxidutsläpp		✓	x
Temperaturaktiverad strömhanteringspolicy		✓	x
Statisk strömhanteringspolicy		✓	✓

Tabell 3: Sammanfattning av vår jämförelse mellan Dell OME och Supermicro SSM och IPMI. Källa: Principled Technologies.

Funktionen	Viktiga fördelar med Dells hanteringsverktyg	Nackdel med Supermicros hanteringsverktyg
 Kalkylator för koldioxidutsläpp och verktyg för kapacitetsplanering	Möjlighet att uppskatta utsläpp av växthusgaser med anpassningsbara värden som hjälper dig att uppfylla hållbarhetsmålen	Ingen jämförbar funktion: gör det svårt att planera för att hjälpa dig att uppfylla hållbarhetsmålen
 Analys av koldioxidutsläpp	Tillgängligt via OpenManage Enterprise Power Manager: ger data om koldioxidutsläpp som kan hjälpa dig att uppfylla hållbarhetsmålen	Ingen jämförbar funktion: inget sätt att spåra koldioxidavtryck för att hjälpa dig att övervaka att du uppfyller hållbarhetsmålen
 Automatiserad ström- och värmehantering	Statiska och temperaturaktiverade policyalternativ med möjlighet att aktivera när servern överskrider en strömförbruknings- eller temperaturtröskel	En statisk policytyp utan associerade utlösaralternativ
 Rapporter om strömförbrukning	Mer än 6 gånger så många rapporter med 20 inbyggda rapporter med schemalagd e-postdistribution och anpassningsalternativ	2 inbyggda rapporter i SSM, 1 rapport i Supermicro IPMI som inte kan exporteras
 Mätvärden för strömhantering	Upp till 15 gånger så många mätvärden , vilket ger mer detaljerad insikt i strömförbrukningen	Endast ett mätvärde , vilket ger mindre insikt och kontroll över strömförbrukningen



Bild 1: Antal rapporter om strömförbrukning som finns tillgängliga i Dell OME och Supermicro SSM. Källa: Principled Technologies.



Bild 2: Antal mätvärden för strömhantering som finns tillgängliga i Dell OME och Supermicro SSM. Källa: Principled Technologies.

Automatiserad ström- och värmehantering

OpenManage Enterprise Power Manager erbjuder automatiserad ström- och värmehantering genom både statisk ström och temperaturaktiverade policyalternativ som gör det möjligt för administratörer att ställa in gränser för strömförbrukning eller temperaturtröskelvärden för att minska kylningskostnaderna. I stället har SSM en enda policy, som är en statisk gräns för strömförbrukning som inte automatiskt löses ut av en server som går bortom gränsen, vilket kan leda till högre energikostnader.

Företag som vill ha en detaljerad bild av datacentrets strömförbrukning med sikte på optimering kan dra nytta av de **20 olika inbyggda strömförbrukningsrapporterna** som OpenManage Enterprise Power Manager erbjuder. Dessa rapporter är användbara för kapacitetsplanering och hantering av ström för att maximera effektiviteten. Rapporteringsalternativen i SSM är mycket mer begränsade. Administratörer kan bara köra en enda värde med en servicerapport eller se en strömförbrukningstrend på övervakningsskärmen. Med Supermicro IPMI kan användare visa ett effektdiagram på komponentnivå i BMC, men de kan inte exportera data i diagrammet för analys och kan bara spara dem som en bild.

OpenManage Enterprise Power Manager-insticksprogrammet gör det möjligt för administratörer att **visa upp till 15 olika mätvärden** som strömförbrukning för enskilda komponenter, luftflöde och komponentanvändning. Med SSM visas endast total strömförbrukning.

Koldioxidutsläpp och analys av koldioxidutsläpp

OME har en kalkylator för koldioxidutsläpp och ett verktyg för kapacitetsplanering som bland annat kan hjälpa dig att uppskatta utsläppen av växthusgaser. Det ger standardvärden för energikostnader och koldioxidutsläpp för en enhet som förbrukas, men gör att du kan anpassa dessa värden för din regions strömkostnader och ditt datacenters förbrukningsmodell. SSM erbjuder ingen jämförbar funktion, något som kan göra det svårt för företag att planera och övervaka framsteg mot sina hållbarhetsmål.

Säkerhet

Cyberbrottslighet ökar exponentiellt och hotar företag med "skador och förstörelse av data, stulna pengar, förlorad produktivitet, stöld av immateriell egendom, stöld av personliga och ekonomiska data, förskingring, bedrägeri, störningar efter attack mot normal verksamhet, kriminalteknisk utredning, återställning och radering av hackade data och system och skador på anseendet".¹ I det här landskapet bör beslutsfattare ta hänsyn till säkerheten vid alla serverinköp. Vi såg att Dell OpenManage Enterprise innehåller flera funktioner som hjälper dig att skydda data som Supermicro-verktygen inte har (se tabell 4 och 5).

Tabell 4: Säkerhetsskillnader mellan Dells hanteringsverktyg och Supermicros hanteringsverktyg. Källa: Principled Technologies.

Funktionen	Dells hanteringsverktyg		Supermicros hanteringsverktyg	
Autentisering med flera faktorer		✓		x
Extern nyckelhanterare		✓		x
Omfattningsbaserad åtkomstkontroll		✓		x
Policybaserad säkerhetskfiguration		✓		x
Rådgivning om cybersäkerhet		✓		x
Rollbaserad åtkomstkontroll		✓		✓
Dynamisk avaktivering av USB-portar		✓		✓

Tabell 5: Sammanfattning av vår jämförelse av säkerhetsfunktioner mellan Dells och Supermicros hanteringsverktyg. Källa: Principled Technologies.

Funktionen	Viktiga fördelar med Dells hanteringsverktyg	Nackdel med Supermicros hanteringsverktyg
 Flerfaktorsautentisering (MFA)	Tvåfaktorsautentisering med iDRAC med antingen e-post och RSA SecurID : förhindrar obehöriga användare från att få åtkomst till känsliga data	Ingen jämförbar funktion : lämnar en säkerhetslucka som kan hjälpa obehöriga användare att få åtkomst till känsliga data
 Extern nyckelhanterare	Secure Enterprise Key Manager i iDRAC lägger till ytterligare ett säkerhetslager som skyddar vilande data på servrar med drivrutinskryptering och centraliserad hantering	Ingen jämförbar funktion : lämnar ytterligare en lucka i säkerheten
 Åtkomstkontroller	OME erbjuder både rollbaserad åtkomstkontroll (RBAC) och omfattningsbaserad åtkomstkontroll (SBAC) för att begränsa de enhetsgrupper som en enhetshanterare har åtkomst till	Endast RBAC begränsar administratörernas möjlighet att begränsa åtkomsten
 Policybaserad säkerhetskfiguration	Policybaserade inställningar för säkerhetskfiguration via CloudIQ, som varnar administratörer om avvikelser	Ingen jämförbar funktion , något som kan fördröja åtgärder och åtgärder för att åtgärda brister
 Rådgivning om cybersäkerhet	Säkerhetsrådgivningsrapportering via Dell CloudIQ-säkerhet, med sårbarhetsinformation och tillämpliga åtgärdsförslag för att möjliggöra snabba åtgärder	Ingen jämförbar funktion , något som innebär att säkerhetsluckor kan utnyttjas av illvilliga aktörer

Autentisering med flera faktorer

Multifaktorautentisering (MFA) kan hjälpa till att förhindra att obehöriga användare och illvilliga aktörer får åtkomst till känsliga data. Vi har verifierat att Dell iDRAC möjliggör tvåfaktorsautentisering både med e-post och med RSA SecurID, en uppsättning externa autentiseringstekniker med flera faktorer som används i många branscher.² Vi har också verifierat att varken Supermicro IPMI eller SSM erbjuder den här funktionen, vilket lämnar en säkerhetslucka.

Nyckelhantering

Externa nyckelhanteringssystem (KMS) gör det möjligt för IT-team att använda en separat tredjepartsserver för att hantera de nycklar de använder för att låsa och låsa upp en servers lagring, och lägger därmed till ytterligare ett säkerhetslager. iDRAC inkluderar Local Key Manager (LKM) för alla nya Dell PowerEdge-servrar. Vissa licenser erbjuder även Secure Enterprise Key Manager (SEKM), vilket möjliggör extra säkerhet med fullständig diskkryptering och extern nyckelhantering. SEKM stöder branschstandarden OASIS KMIP-protokoll. Det ger företag möjlighet att välja alla externa KMS-leverantörer som använder den standarden. Supermicro erbjuder inte denna säkerhetsfunktion eller motsvarande.

Åtkomstkontroller

En integrerad del av många serversäkerhetsstrategier är rollbaserad åtkomstkontroll (RBAC) där en användares roll bestämmer vilka delar av systemet som personen har åtkomst till och vilka uppgifter hen kan utföra. I OpenManage Enterprise definierar RBAC användarbehörigheter för tre inbyggda roller: administratör, enhetshanterare och besökare.³ Det erbjuder också omfattningsbaserad åtkomstkontroll (SBAC) som gör det möjligt för administratörer att begränsa de enhetsgrupper som en enhetshanterare

har åtkomst till.⁴ Detta ger administratörer möjlighet att ge åtkomst till en delmängd enheter. Supermicro erbjuder RBAC, men inte SBAC.

Hantering av inloggningsuppgifter

iDRAC-lösenordsrotation har flera syften: den roterar åtkomst till OpenManage Enterprise i enlighet med säkerhetspolicy med en månatlig standard, den fungerar med en extern lösenordshanterare, och den stöder CyberArk för att hantera lösenord.^{5,6}

Med OpenManage Enterprise kan administratörer hantera iDRAC-lösenordsrotation genom att ersätta behovet av ett statiskt känt administratörskonto med ett tjänstkonto som hanteras av OME. SSM har inte den här funktionen.

Policybaserad säkerhetskfiguration

Dell erbjuder en policybaserad cybersäkerhetsfunktion i CloudIQ för PowerEdge AIOps-lösningen. Den här funktionen tar konfigurationen från en installerad PowerEdge-server och jämför den med en säkerhetsrelaterad konfigurationspolicy baserat på Dells bästa praxis. Om CloudIQ upptäcker en avvikelse meddelar den administratören och erbjuder olika åtgärder.⁷ SSM erbjuder ingen motsvarande funktion, vilket kan innebära förseningar vid upptäckt av intrång.

Rådgivning om cybersäkerhet

Säkerhetsrekommendationer informerar allmänheten om säkerhetsproblem. Enligt Dell tillhandahåller sidan för Dell Security Advisor i CloudIQ en fullständig lista över tillämpliga säkerhetsrekommendationer tillsammans med deras inverkan, antal system som de påverkar och publiceringsdatum.⁸ Dell CloudIQ tillhandahåller säkerhetsrådgivningsrapportering med sårbarhetsinformation och åtgärdsförslag. SSM erbjuder ingen liknande funktion, vilket kan göra systemen sårbara.

Om Dell CloudIQ

Dell CloudIQ är ett molnbaserat AIOps-verktyg som erbjuder "proaktiv övervakning, maskininlärning och prediktiv analys" för ett stort antal produkter och tjänster från Dell, inklusive servrar, lagring, dataskyddsenheter och hyperkonvergerad infrastruktur.⁹ I en studie från Principled Technologies 2022 såg vi att CloudIQ hade försumbar inverkan på nätverksbandbredden samtidigt som vi kunde övervaka telemetri, hälsostatus, varningar och lager från en enda konsol.¹⁰

Mer information om CloudIQ finns på <https://www.dell.com/en-us/dt/solutions/cloudiq.htm>.

Dynamisk avaktivering av USB-portar

Genom att avaktivera och aktivera USB-portar får administratörer kontroll över åtkomsten till servern via en USB-port. Därmed undviker man skadlig användning och risken för installation av förbjudna program eller virus.

Dell iDRAC erbjuder oberoende, dynamisk avaktivering av USB-portar utan driftavbrott. Supermicro erbjuder dynamisk avaktivering av främre USB-portar (och bakre USB-portar) i BIOS, men det kräver licensnyckeln för Supermicro DataCenter Management Suites per nod för att aktiveras. IT kan utlösa det genom att implementera kommandot för systemlåsning som kan utföras från antingen BMC eller Supermicro IPMI-konsolen, men det är inte oberoende av systemlåsningsläge.¹¹

Som bild 3 visar var det en enkel process att avaktivera portarna med Dell iDRAC, det **tog bara 41 sekunder och 4 steg**, medan Supermicro IPMI tog **mer än fyra gånger så lång tid: 2 minuter och 50 sekunder och 6 steg**. Genom att extrapolera dessa tidsbesparingar till 100 system skulle tidsbesparingarna öka till 3 timmar och 35 minuter. Det innebär att en administratör skulle spendera nästan hälften av en arbetsdag med Supermicro IPMI jämfört med lite mer än en timme med Dell iDRAC.

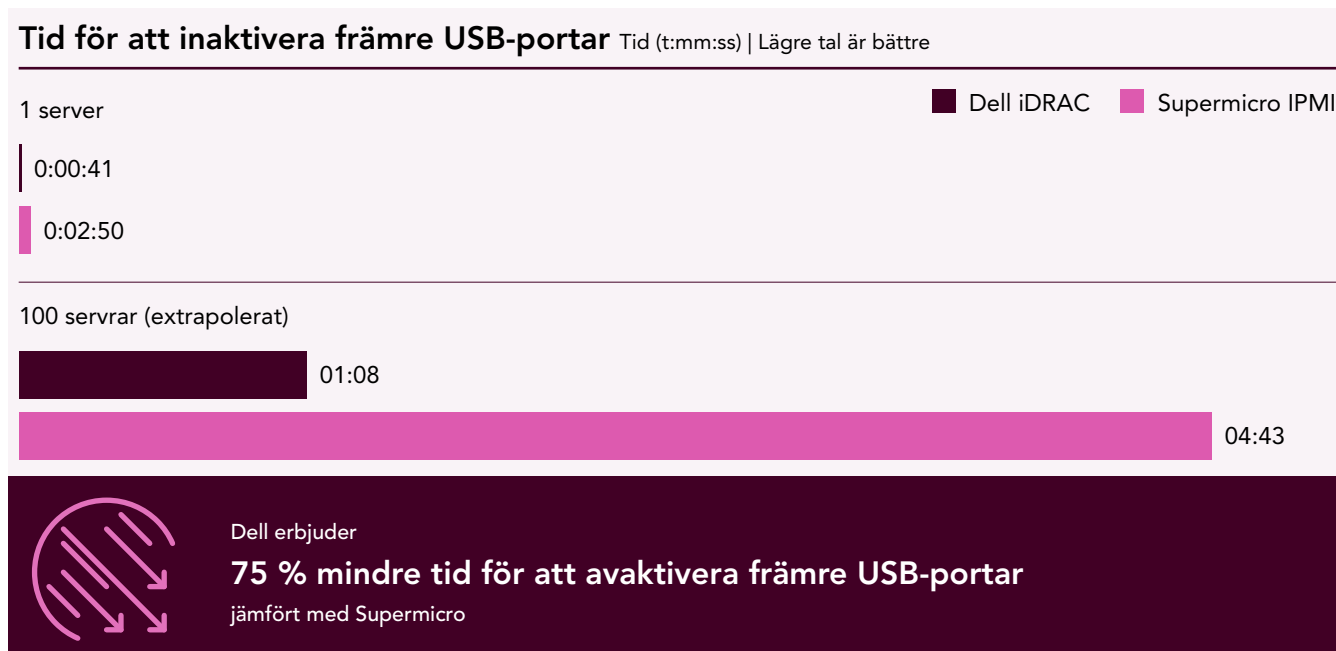


Bild 3: Tid för att avaktivera främre USB-portar för en enda server och extrapolerad tid för att avaktivera främre USB-portar för 100 servrar. Lägre är bättre. Källa: Principled Technologies.

Om Dell OpenManage Enterprise

OpenManage Enterprise är en en-till-många-systemhanteringskonsol för datacentret. Konsolen har ett modernt grafiskt HTML5-användargränssnitt och installeras som en virtuell enhet för miljöer med VMware ESXi™, Microsoft Hyper-V och KVM (Kernel-based Virtual Machine). OpenManage Enterprise kan upptäcka och inventera IPv4- och IPv6-nätverk för upp till 8 000 enheter, inklusive Dell-rackserverar, Dell-tornserverar och Dell-blad och -chassin.¹² I en PT-studie som utfördes nyligen såg vi att en Dell-miljö med OpenManage Enterprise och OpenManage Enterprise Modular (OME-M) kan spara tid på att göra ändringar i VLAN och hjälpa till att undvika åtgärder under schemalagda uppdateringar av fast mjukvara.¹³

Läs mer om OpenManage Enterprise på <https://www.dell.com/en-us/lp/dt/open-manage-enterprise>

Övervakning, analys och användarvänlighet

Hanteringsverktyg varierar kraftigt i hur de stöder administratörer som utför övervaknings- och analysaktiviteter samt andra rutinuppgifter, till exempel schemaläggning av uppdateringar. I det här avsnittet tittar vi på skillnaderna inom dessa områden mellan Dells och Supermicros hanteringsverktyg. När vi undersökte hållbarhet och säkerhetsfunktioner såg vi att Dells svit med hanteringsverktyg erbjuder många funktioner som gör administratörernas liv enklare – funktioner som Supermicros verktyg inte har. I tabell 6 jämförs de fördelar som verktygen erbjuder.

Tabell 6: Sammanfattning av vår jämförelse mellan Dells och Supermicros hanteringsverktyg. Källa: Principled Technologies.

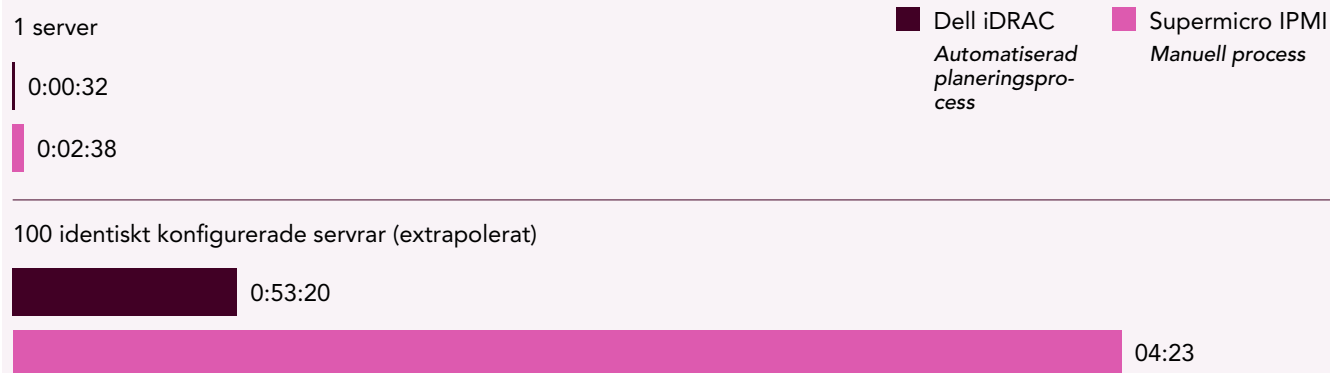
Funktionen	Viktiga fördelar med Dells hanteringsverktyg	Nackdel med Supermicros hanteringsverktyg
 Telemetriströmning	iDRAC9 telemetriströmning som är tillgänglig för fjärranslutna syslog-servrar hjälper till att förutsäga fel och optimera prestanda och kan strömma servermätvärden till analysverktyg som Grafana och Splunk	Ingen automatisk telemetriströmning
 Mobil övervakning och hantering	Funktionsrik OpenManage Mobile-app för iOS och Android som integreras med OME och iDRAC9	Supermicro IPMIView-appen som inte integreras med SSM
 Övervakning av enheter och servrar från tredje part	OME har stöd för enheter och serverövervakning från tredje part, inklusive stöd för sina större konkurrenter	Stöder endast enheter från tredje part som använder sina agenter , sina BMC:er, tidigare versioner av sin utrustning som är IPMI-kompatibel, och Redfish-kompatibla enheter
 Kombinerad övervakning av datacenter	Tillgängligt via OME och CloudIQ: OME kan överföra data på licensierade hanterade servrar till CloudIQ för övervakning i flera datacenter	Ingen molnbaserad portal för att sammanställa övervakningsdata över datacenter
 Varningsbaserade åtgärder	Policyer i OME som utlöser åtgärder baserat på indata från en varning	Inga varningsbaserade åtgärder tillgängliga
 Enklare serverdistribution (möjlighet att importera/exportera systemkonfigurationer)	Kan använda iDRAC9 för att importera/exportera alla konfigurationsobjekt för servrar, kräver endast 48 sekunder och 5 steg för import och 1 minut och 9 sekunder och 7 steg för export	Kan endast importera/exportera konfiguration för Baseboard Management Controller (BMC) och kräver en betydande manuell konfiguration för varje server
 Kortare tid för att ändra BIOS-konfigurationsinställningarna	Kan snabbt ändra alla BIOS-inställningar direkt från iDRAC och ställa in uppdatering och omstart för ett underhållsfönster, vilket sparar betydande administrativ tid	Begränsade BIOS-ändringar är tillgängliga från BMC, annars krävs serveromstart som kräver fler manuella steg och mer administratörstid
 Körs som en virtuell enhet	Finns i OME , vilket gör att operativsystemet inte behöver uppdateras	Ingen jämförbar funktion utan måste köras i ett hanterat operativsystem. Detta ger administratörer ytterligare en komponent som måste korrigeras och uppdateras
 Anslutningsvisning	Tillgängligt i iDRAC : felsökningsverktyg med LLDP för att diagnostisera nätverksproblem som kablar, felaktiga switchportar och mycket mer	Ingen anslutningsvy , ingen fysisk anslutningsinformation om switchportarna uppströms
 Möjlighet att schemalägga uppdateringar av fast mjukvara och drivrutiner	Finns i OME och iDRAC	Kan schemalägga uppdateringar av fast mjukvara för BIOS och BMC , men kan inte schemalägga drivrutinsuppdateringar

Ändring av BIOS-konfigurationsobjekt

Dell erbjuder fullständiga BIOS-konfigurationsinställningar direkt från iDRAC med möjlighet att göra dessa ändringar inför nästa omstart. Supermicro erbjuder en begränsad uppsättning BIOS-inställningar från sin BMC. Förutom den begränsade uppsättningen kräver en BIOS-konfigurationsändring på Supermicro-serverar för ett enda konfigurationsobjekt att administratören startar om servern för att komma åt BIOS-konfigurationsmenyn från startskärmen.

Bild 4 visar tiden det tar att utföra en BIOS-konfigurationsändring på en enda server med hjälp av Dell iDRAC och Supermicro IPMI. Den manuella processen med **Supermicro-verktyget tar ytterligare 2 minuter och 6 sekunder**, eller **4,9 gånger längre** jämfört med att konfigurera den automatiserade processen i iDRAC. Om vi extrapolerar dessa tider till 100 servrar som är konfigurerade på samma sätt skulle tidsbesparingarna med iDRAC vara 3,5 timmar. (Om serverna inte vore identiskt konfigurerade skulle vi inte se dessa tidsbesparingar.)

Tid för att utföra en ändring av BIOS-konfigurationen (t:mm:ss) | Lägre tal är bättre



Dell erbjuder

78 % mindre tid att ändra BIOS-konfigurationer

jämfört med Supermicro

Bild 4: Tid för att utföra en BIOS-konfigurationsändring på både en enda server och 100 identiska konfigurerade servrar (extrapolerad). Lägre är bättre. Källa: Principled Technologies.

Om iDRAC9

Dell PowerEdge™-servrar omfattar Integrated Dell Remote Access Controller 9 med Dell Lifecycle Controller med systemadministrationsfunktioner som ger systemvarningar och fjärrhanteringsfunktioner. Enligt Dell omfattar de viktigaste fördelarna med iDRAC9:

- Möjligheten att hantera tusentals servrar med API:er och skriptverktyg
- Inbyggd support som ger en vy över serverhälsa och statusövervakning för tusentals parametrar
- Starka säkerhetsfunktioner och alternativ¹⁴

Mer information om de funktioner iDRAC9 tillhandahåller finns på <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

Automatiserade uppdateringar av den fasta mjukvaran och drivrutiner

iDRAC

Till skillnad från Supermicro IPMI gör Dell iDRAC det möjligt att schemalägga automatiska uppdateringar av fast mjukvara. Det innebär att konfiguration av automatiska uppdateringar enligt ett schema blir en engångsuppgift som sparar tid för varje uppdateringscykel. Bild 5 visar den extrapolerade tiden för att schemalägga automatiska uppdateringar av fast mjukvara för första gången för 100 servrar med Dell iDRAC och Supermicro IPMI. Den manuella processen med Supermicro-verktyget tar **ytterligare 13 minuter** jämfört med att konfigurera den automatiserade processen i iDRAC.

Om vi antar att en administratör konfigurerar ett månadsschema den första lördagskvällen i varje månad, skulle en administratör som använder iDRAC lägga 58 sekunder per server. För 100 servrar blir det 1 timme, 36 minuter och 40 sekunder som en engångskonfiguration. I jämförelse skulle en administratör som använder Supermicro IPMI lägga 1 timme och 50 minuter för 100 servrar i varje underhållsfönster. Om vi jämför engångskonfigurationen för iDRAC och den första av många konfigurationstider för Supermicro IPMI sparar Dell-hanteringsverktyget cirka 13 minuter och 20 sekunder. (Se bild 5)

Men den andra gången, och varje efterföljande gång, **sparar Dell 110 minuter eftersom det inte längre är nödvändigt för administratören att utföra uppgiften.** (Se bild 6) Denna tidsbesparing sker även om de 100 serverna inte är identiskt konfigurerade. Observera att dessa tider endast omfattar uppladdning av den fasta mjukvaran till BMC och inte återspeglar nedladdnings- och extraktionstiderna för den fasta mjukvaran för Supermicro.

OME

Dell OME har stöd för **uppdateringar av fast mjukvara för alla komponenter** och uppdateringar av Windows-drivrutiner. SSM stöder uppdatering av fast mjukvara för BIOS och BMC, **men inte drivrutinsuppdateringar eller uppdatering av andra komponenter.**

Extrapolerad tid för att schemalägga automatiska uppdateringar av fast mjukvara första gången (100 servrar) tid (t:mm:ss) | Lägre tal är bättre

Automatiserad planeringsprocess för Dell iDRAC

01:36

Supermicro IPMI Manuell process

01:50

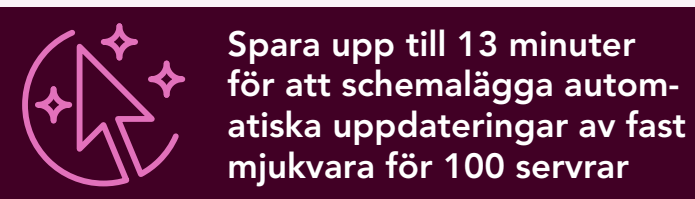


Bild 5: Extrapolerad tid för att uppdatera fast mjukvara på 100 servrar första gången. Lägre är bättre. Källa: Principled Technologies.

Extrapolerad tid som krävs för att schemalägga automatiska uppdateringar av fast mjukvara varje efterföljande gång (100 servrar) Tid (t:mm:ss) | Lägre tal är bättre

Automatiserad planeringsprocess för Dell iDRAC

Ingen ytterligare tid

Supermicro IPMI Manuell process

01:50

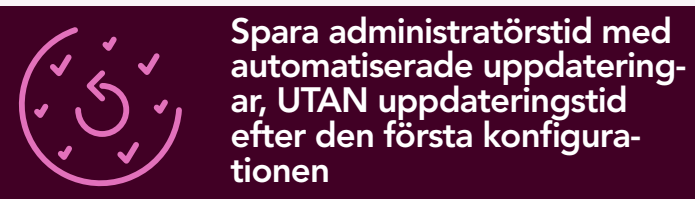


Bild 6: Extrapolerad tid för att uppdatera fast mjukvara på 100 servrar varje gång. Lägre är bättre. Källa: Principled Technologies.

Sammanfattning

När man ska välja en leverantör för serverinköp finns det mer att tänka på än bara hårdvaruplattformen. Beslutsfattare måste också överväga mer långsiktiga problem som system-/datasäkerhet, energieffektivitet och enkel hantering. Dessa bekymmer gör systemhanteringsverktygen lika viktiga som hårdvaran.

Vi undersökte funktionerna i serverhanteringsverktyg från Dell och Supermicro, där Dell iDRAC9 jämfördes med Supermicro IPMI för inbäddad serverhantering och Dell OpenManage Enterprise och CloudIQ med Supermicro Server Manager för en enhetshanterings- och övervakningskonsol för en-till-många. Vi såg att Dells hanteringsverktyg gav mer omfattande funktioner för säkerhet, hållbarhet och hantering/övervakning än Supermicros servrar. Dessutom automatiserade Dells verktyg fler uppgifter för att underlätta serverhanteringen. Det ledde till betydande tidsbesparingar för administratörer jämfört med att behöva utföra samma uppgifter manuellt med Supermicros verktyg.

När du ska göra ett serverköp är leverantörens associerade hanteringsprodukter avgörande för att skydda data, stödja en mer hållbar miljö och underlätta underhållet av system. Våra tester och vår forskning visade att Dells hanteringsportfölj för PowerEdge-servrar erbjöd fler funktioner för att hjälpa organisationer att uppfylla dessa mål än de jämförbara Supermicro-hanteringsprodukterna.

1. Steve Morgan, "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025", hämtat den 15 februari 2024, <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>.
2. Dell, "Using iDRAC9 RSA SecurID 2FA", hämtat den 15 februari 2024, <https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-secrid-2fa.pdf>.
3. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide", hämtat den 15 februari 2024, <https://www.dell.com/support/manuals/en-us/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?>.
4. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide".
5. Dell, "OpenManage Enterprise 4.0: iDRAC Password Management and Rotation", hämtat den 15 februari 2024, <https://www.dell.com/support/kbdoc/en-us/000219279/openmanage-enterprise-4-0-idrac-password-management-and-rotation>.
6. Dell, "OpenManage Portfolio Software Licensing Guide", hämtat den 3 april 2024, <https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf>.
7. Mark Maclean and Kyle Shannon, "Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation", hämtat den 15 februari 2024, <https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/>.
8. Dell, "Security Advisories", hämtat den 15 februari 2024, <https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/>.
9. Dell, "Dell CloudIQ - AIOps for Intelligent IT Infrastructure Insights", hämtat den 15 februari 2024, <https://www.dell.com/en-us/dt/solutions/cloudiq.htm>.
10. Principled Technologies, "Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests", hämtat den 17 januari 2024, <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>.
11. Supermicro, "X13DEM User's Manual", hämtat den 16 februari, 2024, <https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf>.
12. Dell, "OpenManage Enterprise", hämtat den 20 december 2023, <https://www.dell.com/en-us/work/learn/openmanage-enterprise>.
13. Principled Technologies, "A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators", hämtat den 17 januari 2024, <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>.
14. "Integrated Dell Remote Access Controller (iDRAC)", hämtat den 16 januari 2024, <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

Läs vetenskapen bakom rapporten ►



Facts matter.®

Principled Technologies är ett registrerat varumärke som tillhör Principled Technologies, Inc. Alla andra produktnamn är varumärken som tillhör respektive ägare. Granska vetenskapen bakom denna rapport om du vill ha mer information.

Det här projektet har beställts av Dell Technologies.