Versterk de beveiliging met

3,5 keer zoveel beveiligingsfuncties

Inclusief tweeledige verificatie en extern sleutelbeheer met iDRAC9

Optimaliseer energie-efficiëntie met meer dan

6 keer zoveel energieverbruiksrapporten,

in totaal 20 rapporten in Dell OME vergeleken met 3 rapporten in Supermicro SSM

Verhoog de operationele efficiëntie door 1 uur en 50 minuten beheertijd te besparen

per 100 servers

Automatische updates gebruiken met Dell iDRAC9 versus geen automatische updates beschikbaar met Supermicro IPMI

Verhoog de beveiliging, duurzaamheid en efficiëntie met de robuuste Dell serverbeheertools

Vergeleken met het Supermicro-beheerportfolio

Wanneer u investeert in nieuwe servers voor uw datacenter, doet u meer dan alleen hardware kiezen. U kiest ook een beheeroplossing. Als uw beheerders efficiënte, uitgebreide tools hebben om uw infrastructuur te implementeren, te bewaken, te onderhouden en te beveiligen en tegelijkertijd de energie-efficiëntie te verbeteren, kunnen ze het dagelijkse beheer makkelijker afhandelen en meer tijd besteden aan innovaties die uw organisatie vooruit helpen. Door te kiezen voor een leverancier met krachtige beheertools bespaart u op de lange termijn tijd en geld.

We hebben de serverbeheerportfolio's van Dell™ en Supermicro® beoordeeld, waarbij drie tools van Dell werden vergeleken met twee tools van Supermicro.

Tabel 1: De beheertools die we hebben getest. *Dell CloudIQ is een cloudgebaseerde monitoring- en analysetool; Supermicro biedt geen vergelijkbare tool.
Bron: Principled Technologies.

	Dell	Supermicro
Geïntegreerd/extern serverbeheer	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
One-to-many apparaatbeheerconsole	Dell OpenManage™ Enterprise (OME) Dell CloudIQ*	Supermicro Server Manager (SSM)

Op het gebied van duurzaamheid, beveiliging en dagelijkse beheerervaring hebben we vastgesteld dat Dell consistent meer functierijke toolsets bood die beheerders meer opties en mogelijkheden geven.

Meer en uitgebreidere functies om serverbeheer te automatiseren en makkelijker te maken

Uw IT-teams hebben moderne, veelzijdige beheertools nodig waarmee ze tijd kunnen besparen in hun dagelijkse werk en de normen voor beveiliging en efficiëntie kunnen naleven. De beheertools van Dell die we hebben beoordeeld, bevatten een aantal functies en mogelijkheden die niet aanwezig zijn in het beheerportfolio van Supermicro.

Duurzaamheid

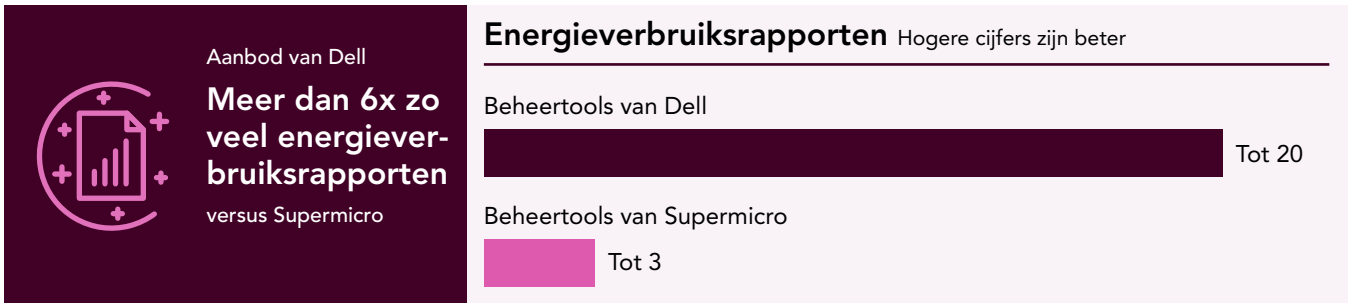
Naarmate de energiekosten stijgen en de milieuwetgeving toeneemt, richten veel organisaties zich op duurzaamheid. Datacenters hebben inherent grote hoeveelheden stroom nodig, maar zorgvuldig beheer van het thermische en stroomverbruik kan zorgen dat organisaties minder energie verbruiken. Dell OpenManage Enterprise bevat verschillende functies die nauwkeurige bewaking en beheer van het energieverbruik mogelijk maken, zodat u wordt geholpen uw duurzaamheidsdoelstellingen te bereiken. Tabel 2 en 3 belichten de belangrijkste voordelen van deze functies, die we hieronder in meer detail beschrijven.

Tabel 2: Duurzaamheidsverschillen tussen Dell OpenManage Enterprise en SSM. Bron: Principled Technologies.

Functie	Beheertools van Dell	Beheertools van Supermicro
CO_2-uitstootcalculator en capaciteitsplanningstool	✓	x
Analyse van de CO_2-voetafdruk	✓	x
Temperatuurgeactiveerd energiebeheerbeleid	✓	x
Statisch energiebeheerbeleid	✓	✓

Tabel 3: Samenvatting van onze vergelijking tussen Dell OME en Supermicro SSM en IPMI. Bron: Principled Technologies.

Functie	Belangrijkste voordelen van Dell beheertools	Nadeel van de beheertools van Supermicro
CO_2-uitstootcalculator en capaciteitsplanningstool	Mogelijkheid om **broeikasgasuitstoot** te schatten met aanpasbare waarden om u te helpen uw duurzaamheidsdoelstellingen te behalen	**Geen vergelijkbare functie**, dit maakt het moeilijk om te plannen uw duurzaamheidsdoelstellingen te behalen
Analyse van de CO_2-voetafdruk	**Beschikbaar** via OpenManage Enterprise Power Manager, biedt informatie over CO_2-uitstoot, wat u kan helpen uw duurzaamheidsdoelstellingen te behalen	**Geen vergelijkbare functie**, geen manier om de CO2-voetafdruk in kaart te brengen om u te helpen uw duurzaamheidsdoelstellingen te behalen
Geautomatiseerd energie- en thermisch beheer	**Statische en temperatuurgeactiveerde beleidsopties** met de optie om te activeren wanneer de server een stroomverbruik- of temperatuurdrempel overschrijdt	**Eén statisch beleidstype** zonder bijbehorende triggeropties
Rapporten over energieverbruik	**Meer dan 6x** zo veel rapporten, met **20 ingebouwde** rapporten met geplande e-maildistributie en aanpassingsopties	**2 ingebouwde rapporten** in SSM, 1 rapport in Supermicro IPMI dat niet kan worden geëxporteerd
Statistieken voor energiebeheer	Tot **15 keer zo veel statistieken**, met gedetailleerder inzicht in het beheer van energieverbruik	**Maar 1 statistiek**, die minder inzicht en controle biedt over het energieverbruik



Afbeelding 1: Aantal rapporten over energieverbruik beschikbaar in Dell OME en Supermicro SSM. Bron: Principled Technologies.

Afbeelding 2: Aantal statistieken voor energiebeheer beschikbaar in Dell OME en Supermicro SSM. Bron: Principled Technologies.

Geautomatiseerd energie- en thermisch beheer

OpenManage Enterprise Power Manager biedt geautomatiseerd energie- en thermisch beheer via zowel stroom- als temperatuurgeactiveerde beleidsopties, waarmee beheerders limieten voor energieverbruik of temperatuurdrempels kunnen instellen om de koelingskosten te verlagen. SSM heeft daarentegen maar één beleid, een statische limiet voor het energieverbruik die niet automatisch wordt geactiveerd als een server de limiet overschrijdt, wat kan leiden tot hogere energiekosten.

Organisaties die diepgaande inzichten willen in het energieverbruik van hun datacenter met het oog op optimalisatie, kunnen de **20 verschillende ingebouwde energieverbruiksrapporten** gebruiken die OpenManage Enterprise Power Manager biedt. Deze rapporten zijn nuttig voor capaciteitsplanning en energiebeheer om de efficiëntie te maximaliseren. De rapportageopties in SSM zijn veel beperkter. Beheerders kunnen slechts één host uitvoeren met een servicerapport of een trend in het energieverbruik bekijken op het controlescherm. Met de Supermicro IPMI kunnen gebruikers een energiegrafiek op componentniveau bekijken in de BMC. Ze kunnen de gegevens echter niet exporteren voor analyse en alleen opslaan als afbeelding.

Met de OpenManage Enterprise Power Manager plug-in kunnen beheerders **tot wel 15 verschillende statistieken bekijken**, inclusief energieverbruik per component, luchtstroom en componentgebruik, terwijl SSM alleen het totale energieverbruik toont.

Analyse van CO_2-uitstoot en ecologische voetafdruk

OME bevat een calculator voor CO_2-uitstoot en een tool voor capaciteitsplanning waarmee u onder andere uw eigen broeikasgasuitstoot kunt inschatten. Het biedt standaardwaarden voor energiekosten en CO_2-uitstoot voor een eenheid van verbruikte energie, maar u kunt deze waarden aanpassen aan de energiekosten in uw eigen regio en het verbruiksmodel van uw datacenter. SSM biedt geen vergelijkbare functie, waardoor het voor organisaties moeilijk kan zijn om de voortgang van hun duurzaamheidsdoelstellingen te plannen en te bewaken.

Beveiliging

Cybercriminaliteit neemt exponentieel toe en bedreigt bedrijven met "schade en vernietiging van data, gestolen geld, verloren productiviteit, diefstal van intellectueel eigendom, diefstal van persoonlijke en financiële data, verduistering, fraude, verstoring van de normale bedrijfsvoering na een aanval, forensisch onderzoek, herstel en verwijdering van gehackte data en systemen, en reputatieschade."[1] In dit landschap moeten besluitvormers bij elke serveraankoop rekening houden met de beveiliging. We hebben vastgesteld dat Dell OpenManage Enterprise verschillende functies bevat om uw data veilig te houden die de Supermicro-tools niet hebben (zie tabellen 4 en 5).

Tabel 4: Beveiligingsverschillen tussen de beheertools van Dell en Supermicro. Bron: Principled Technologies.

Functie	Beheertools van Dell	Beheertools van Supermicro
Meervoudige authenticatie	✓	x
Externe-sleutelbeheerder	✓	x
Bereikgebaseerde toegangscontrole	✓	x
Beleidsgebaseerde beveiligingsconfiguratie	✓	x
Cyberbeveiligingsadviezen	✓	x
Toegangscontroles op basis van rollen	✓	✓
Dynamische uitschakeling van USB-poorten	✓	✓

Tabel 5: Samenvatting van onze vergelijking van de beveiligingsfuncties in de beheertools van Dell en Supermicro. Bron: Principled Technologies.

Functie	Belangrijkste voordelen van Dell beheertools	Nadeel van de beheertools van Supermicro
Meervoudige verificatie (MFA)	**Tweevoudige verificatie** met iDRAC met **e-mail en RSA SecurID**, waardoor onbevoegde gebruikers geen toegang krijgen tot gevoelige data	**Geen vergelijkbare functie**, waardoor er een beveiligingskloof ontstaat en onbevoegde gebruikers mogelijk toegang krijgen tot gevoelige data
Externe-sleutelbeheerder	**Secure Enterprise Key Manager** in iDRAC voegt een extra beveiligingslaag toe om data-at-rest op servers te beschermen met schijfversleuteling en gecentraliseerd beheer	**Geen vergelijkbare functie**, waardoor er nog een gat in de beveiliging overblijft
Toegangscontrole	OME biedt **zowel** op rollen gebaseerde toegangscontrole **(RBAC)** als scope-gebaseerde toegangscontrole **(SBAC)** om de apparaatgroepen te beperken waartoe een apparaatbeheerder toegang heeft	**Alleen RBAC**, waardoor beheerders minder mogelijkheden hebben om de toegang te beperken
Beleidsgebaseerde beveiligingsconfiguratie	Instellingen voor **beleidsgebaseerde beveiligingsconfiguratie** via CloudIQ, waardoor beheerders worden gewaarschuwd bij afwijkingen	**Geen vergelijkbare functie**, waardoor actie en herstel van inbreuken kan vertragen
Cyberbeveiligingsadviezen	**Rapportage met beveiligingsadviezen** via Dell CloudIQ beveiliging, met informatie over kwetsbaarheden en toepasselijke suggesties voor probleemoplossing om snelle actie mogelijk te maken	**Geen vergelijkbare functie**, waardoor beveiligingsgaten ontstaan die kwaadwillenden kunnen exploiteren

Meervoudige verificatie

Meervoudige verificatie (MFA) kan helpen voorkomen dat onbevoegde gebruikers en kwaadwillenden toegang krijgen tot gevoelige data. We hebben geverifieerd dat Dell iDRAC tweevoudige verificatie mogelijk maakt, zowel via e-mail als RSA SecurID, een set externe technologieën voor meervoudige verificatie die in veel sectoren worden gebruikt.[2] We hebben ook geverifieerd dat Supermicro IPMI en SSM deze functie niet bieden, waardoor er een beveiligingsgat ontstaat.

Sleutelbeheer

Met externe sleutelbeheersystemen (KMS) kunnen IT-teams een afzonderlijke server van derden gebruiken om de sleutels te beheren waarmee ze de storage van een server vergrendelen en ontgrendelen, waardoor een extra beveiligingslaag wordt toegevoegd. iDRAC bevat Local Key Manager (LKM) voor alle nieuwe Dell PowerEdge servers. Sommige licenties bieden ook Secure Enterprise Key Manager (SEKM), waardoor extra beveiliging wordt toegevoegd met volledige schijfversleuteling en extern sleutelbeheer. SEKM ondersteunt het OASIS KMIP-protocol dat standaard is in de branche, zodat organisaties elke externe KMS-provider kunnen kiezen die deze standaard gebruikt. Supermicro biedt deze beveiligingsfunctie of een gelijkwaardig product niet.

Toegangscontrole

Op rollen gebaseerde toegangscontrole (RBAC), waarbij de rol van een gebruiker bepaalt tot welke onderdelen van het systeem deze toegang heeft en welke taken deze daar kan uitvoeren, is een integraal onderdeel van veel strategieën voor serverbeveiliging. In OpenManage Enterprise bepaalt u met RBAC de gebruikersrechten voor drie geïntegreerde rollen: Beheerder, Apparaatmanager en Kijker.[3] Het biedt ook SBAC (scope-gebaseerde toegangscontrole), waarmee beheerders kunnen beperken tot welke apparaatgroepen een apparaatbeheerder toegang heeft.[4] Zo kunnen beheerders toegang bieden tot een subset van apparaten. Supermicro biedt RBAC, maar niet SBAC.

Beheer van inloggegevens

iDRAC-wachtwoordrotatie heeft verschillende doelen: Het roteert de toegang tot OpenManage Enterprise in overeenstemming met het beveiligingsbeleid, met een maandelijkse standaard; het werkt met een externe wachtwoordhandler; en het ondersteunt CyberArk om wachtwoorden te beheren.[5,6]

Met OpenManage Enterprise kunnen beheerders iDRAC-wachtwoordrotatie beheren door de noodzaak van een statisch bekend beheerdersaccount te vervangen door een serviceaccount dat wordt beheerd door OME. SSM biedt deze mogelijkheid niet.

Beleidsgebaseerde beveiligingsconfiguratie

Dell biedt een beleidsgebaseerde cyberbeveiligingsfunctie, de CloudIQ voor PowerEdge AIOps-oplossing. Deze functie neemt de configuratie van een geïmplementeerde PowerEdge server en vergelijkt deze met een beveiligingsgerelateerd configuratiebeleid op basis van de best practices van Dell. Als CloudIQ een afwijking detecteert, wordt de beheerder hiervan op de hoogte gesteld en worden herstelstappen voorgesteld.[7] SSM biedt geen vergelijkbare functie, wat ertoe kan leiden dat inbreuken later worden gedetecteerd.

Cyberbeveiligingsadviezen

Beveiligingsadviezen informeren het publiek over beveiligingsproblemen. Volgens Dell biedt de pagina Dell beveiligingsadviezen in CloudIQ een volledige lijst met toepasselijke beveiligingsadviezen, samen met hun impact, het aantal systemen dat ze hebben getroffen en de publicatiedatum.[8] Dell CloudIQ biedt rapporten van beveiligingsadviezen met informatie over kwetsbaarheden en suggesties voor probleemoplossing. SSM biedt geen vergelijkbare functie, waardoor systemen kwetsbaar kunnen zijn.

Over Dell CloudIQ

Dell CloudIQ is een cloudgebaseerde AIOps-tool die "proactieve bewaking, machine learning en voorspellende analyses"' biedt voor een groot aantal Dell producten en services, waaronder servers, storage, databeschermingsapparaten en hyperconverged infrastructuur.[9] In een onderzoek van Principled Technologies uit 2022 hebben we vastgesteld dat CloudIQ een verwaarloosbare impact had op de netwerkbandbreedte, terwijl het ons tegelijkertijd in staat stelde om telemetrie, status, waarschuwingen en inventaris vanuit één centrale console te monitoren.[10]

U vindt meer informatie over CloudIQ via https://www.dell.com/nl-nl/dt/solutions/cloudiq.htm.

Dynamische uitschakeling van USB-poorten

Door USB-poorten uit en in te schakelen, hebben beheerders controle over de toegang tot de server via een USB-poort, waardoor schadelijk gebruik en het risico op installatie van verboden apps of virussen wordt voorkomen.

Dell iDRAC biedt onafhankelijke, dynamische uitschakeling van USB-poorten zonder vereiste downtime. Supermicro biedt dynamische uitschakeling van de USB-poorten aan de voorzijde (en aan de achterzijde) via de BIOS, maar de Supermicro DataCenter Management Suite per Node License-key is nodig om dit in te schakelen. IT kan dit activeren door de opdracht voor systeemvergrendeling te implementeren, die kan worden uitgevoerd via de BMC of de Supermicro IPMI-console, maar deze werkt niet onafhankelijk van de systeemvergrendelingsmodus.[11]

Zoals Figuur 3 laat zien, was het uitschakelen van de poorten met Dell iDRAC een eenvoudig proces **waarbij slechts 41 seconden en 4 stappen nodig waren**, terwijl de Supermicro IPMI **meer dan vier keer zo lang duurde, namelijk 2 minuten en 50 seconden, en er 6 stappen moesten worden uitgevoerd**. Als we deze tijdbesparingen extrapoleren naar 100 systemen, zou de tijdsbesparing 3 uur en 35 minuten zijn. Dit betekent dat een beheerder hier bijna een halve werkdag aan zou besteden bij gebruik Supermicro IPMI in plaats van iets meer dan een uur bij gebruik van Dell iDRAC.

Afbeelding 3: Tijd om de voorste USB-poorten uit te schakelen voor een enkele server en de geëxtrapoleerde tijd om de voorste USB-poorten uit te schakelen voor 100 servers. Minder is beter. Bron: Principled Technologies.

Over Dell OpenManage Enterprise

OpenManage Enterprise is een één-naar-veel systeembeheerconsole voor het datacenter. De console biedt een moderne grafische HTML5-gebruikersinterface en kan worden geïmplementeerd als een virtuele appliance voor VMware ESXi™, Microsoft Hyper-V en Kernel-based Virtual Machine (KVM)-omgevingen. OpenManage Enterprise kan op IPV4- en IPV6-netwerken tot 8.000 apparaten detecteren en inventariseren, waaronder Dell rackservers, Dell towerservers en Dell blades en chassis.[12] In een recent PT-onderzoek hebben we vastgesteld dat een Dell omgeving met OpenManage Enterprise en OpenManage Enterprise Modular (OME-M) tijd kan besparen bij het aanbrengen van wijzigingen in VLAN's en interventies tijdens geplande firmware-updates kan helpen voorkomen.[13]

U vindt meer informatie over OpenManage Enterprise via https://www.dell.com/nl-nl/lp/dt/open-manage-enterprise

Controle, analyse en gebruiksgemak

Beheertools verschillen sterk in de manier waarop ze beheerders ondersteunen bij het uitvoeren van controle- en analyseactiviteiten en andere routinetaken, zoals het plannen van updates. In dit gedeelte brengen we de verschillen op deze gebieden in kaart tussen de beheertools van Dell en Supermicro die we hebben onderzocht. Zoals we ontdekten toen we duurzaamheids- en beveiligingsfuncties onderzochten, biedt het pakket beheertools van Dell tal van functies om het leven van beheerders gemakkelijker te maken. Functies die de Supermicro-tools niet bieden. In Tabel 6 worden de beheervoordelen van de tools vergeleken.

Tabel 6: Samenvatting van onze vergelijking tussen de beheertools van Dell en Supermicro. Bron: Principled Technologies.

Functie	Belangrijkste voordelen van Dell beheertools	Nadeel van de beheertools van Supermicro
Telemetriestreaming	iDRAC9 **telemetriestreaming beschikbaar** voor externe syslog-servers. helpt fouten te voorspellen en prestaties te optimaliseren, kan serverstatistieken streamen naar analysetools zoals Grafana en Splunk	**Geen automatische telemetriestreaming**
Mobiele controle en beheer	Uitgebreide OpenManage Mobile app voor iOS en Android, die is geïntegreerd met OME en iDRAC9	Supermicro IPMIView-app, die **niet is geïntegreerd** met SSM
Controle van apparaten en servers van derden	OME ondersteunt **controle van apparaten en servers van derden**, inclusief ondersteuning voor de belangrijkste concurrenten	**Ondersteunt alleen apparaten van derden die gebruikmaken van hun agents**, hun BMC's, eerdere versies van hun apparatuur die geschikt zijn voor IPMI en apparaten die geschikt zijn voor Redfish
Estatecontrole	Beschikbaar via OME en CloudIQ, OME kan data op beheerde servers met een licentie naar CloudIQ sturen voor controle in meerdere datacenters	**Geen cloudgebaseerde portal** om de controle van data in meerdere datacenters te verzamelen
Op waarschuwingen gebaseerde acties	Beleidsregels in OME die acties activeren op basis van invoer van een waarschuwing	**Geen op waarschuwingen gebaseerde acties beschikbaar**
Eenvoudigere serverimplementatie (mogelijkheid om systeemconfiguraties te importeren/exporteren)	Kan iDRAC9 gebruiken om alle configuratie-items voor servers te **importeren/exporteren**, waarbij slechts **48 seconden en 5 stappen nodig zijn voor importeren en 1 minuut 9 seconden en 7 stappen voor exporteren**	Kan **alleen BMC-configuratie (Baseboard Management Controller)** importeren/exporteren, waarvoor aanzienlijke handmatige configuratie voor elke server vereist is
Minder tijd om de BIOS-configuratie-instellingen te wijzigen	Kan snel **de volledige BIOS-instellingen rechtstreeks vanuit iDRAC** wijzigen en de update en opnieuw opstarten faseren binnen een onderhoudsvenster, waardoor beheerders aanzienlijk veel tijd besparen	**Beperkte BIOS-wijzigingen beschikbaar** via de BMC, anders is opnieuw opstarten van de server vereist, kost meer handmatige stappen en beheertijd
Uitvoeren als een virtueel apparaat	**Beschikbaar** in OME, waardoor het besturingssysteem niet meer hoeft te worden bijgewerkt	**Geen vergelijkbare functie**, moet worden uitgevoerd binnen een beheerd besturingssysteem. waardoor beheerders nog een component hebben om te patchen en bij te werken
Connection View	**Beschikbaar** in iDRAC, tool voor probleemoplossing via LLDP voor het diagnosticeren van netwerkproblemen, zoals bekabeling en slechte switchpoorten	**Geen verbindingsweergave**, geen fysieke connectiviteitsinformatie over de upstreamswitchpoorten
Mogelijkheid om firmware- en driverupdates te plannen	**Beschikbaar** in OME en iDRAC	Kan BIOS- en BMC-firmware-updates plannen, maar **kan geen driverupdates plannen**

Wijziging van BIOS-configuratie-items

Dell biedt volledige wijziging van BIOS-configuratie-instellingen rechtstreeks vanuit iDRAC met de mogelijkheid om die in te laten gaan bij de volgende keer opnieuw opstarten. Supermicro biedt een beperkte set BIOS-instellingen via de BMC. Afgezien van de beperkte set vereist een BIOS-configuratiewijziging op Supermicro-servers voor één configuratie-item dat de beheerder de server opnieuw opstart om toegang te krijgen tot het BIOS-configuratiemenu via het opstartscherm.

Figuur 4 toont hoelang het duurt om een BIOS-configuratiewijziging uit te voeren op één server met Dell iDRAC en Supermicro IPMI. Het handmatige proces met de **Supermicro-tool duurt 2 minuten en 6 seconden**, of **4,9x langer** dan het instellen van het geautomatiseerde proces in iDRAC. Als we deze tijden extrapoleren naar 100 servers met een identieke configuratie, zou de tijdsbesparing met iDRAC 3,5 uur zijn. (Bij servers zonder identieke configuratie zou er geen tijdsbesparing zijn.)

Afbeelding 4: Tijd om een BIOS-configuratiewijziging uit te voeren op één server en 100 identiek geconfigureerde servers (geëxtrapoleerd). Minder is beter. Bron: Principled Technologies.

Over iDRAC9

Dell PowerEdge™ servers bevatten de Integrated Dell Remote Access Controller 9 met Dell Lifecycle Controller, die beheermogelijkheden biedt als systeemwaarschuwingen en externe beheerfuncties. Volgens Dell zijn de belangrijkste voordelen van iDRAC9:

- De mogelijkheid om duizenden servers te beheren met API's en scriptingtools
- Geïntegreerde ondersteuning, met een overzicht van serverstatus en statusbewaking van duizenden parameters
- Krachtige beveiligingsfuncties en -opties[14]

Voor meer informatie over de functies van iDRAC9, ga naar https://www.dell.com/nl-nl/lp/dt/open-manage-idrac.

Automatische firmware- en driverupdates

iDRAC

In tegenstelling tot Supermicro IPMI kunt u met Dell iDRAC automatische firmware-updates plannen. Zo is het configureren van automatische updates volgens een schema een eenmalige taak die tijd bespaart bij elke updatecyclus. Figuur 5 toont de geëxtrapoleerde tijd om automatische firmware-updates voor de eerste keer te plannen voor 100 servers via Dell iDRAC en Supermicro IPMI. Het handmatige proces in de Supermicro-tool duurt **13 minuten** langer dan het instellen van het geautomatiseerde proces in iDRAC.

Als we ervan uitgaan dat een beheerder een maandelijks schema instelt op de eerste zaterdagavond van elke maand, heeft een beheerder die iDRAC gebruikt eenmalig 58 seconden per server nodig. Voor 100 servers is dit eenmalig 1 uur, 36 minuten en 40 seconden. Een beheerder die Supermicro IPMI gebruikt, zou voor 100 servers tijdens elk onderhoudsvenster 1 uur en 50 minuten kwijt zijn. Als we de eenmalige installatie voor iDRAC vergelijken met de eerste van vele installaties voor Supermicro IPMI, bespaart de Dell beheertool ongeveer 13 minuten en 20 seconden. (Zie afbeelding 5.)

Maar de tweede keer en elke volgende keer **bespaart de beheerder met Dell 110 minuten omdat die deze taak niet nog een keer hoeft uit te voeren**. (Zie afbeelding 6.) Deze tijdsbesparing komt zelfs voor als de 100 servers niet identiek zijn geconfigureerd. Houd er rekening mee dat deze tijden alleen het uploaden van de firmware naar de BMC omvatten en niet de download- en extractietijden voor de Supermicro-firmware.

OME

Dell OME ondersteunt **firmware-updates voor alle componenten** en Windows-driverupdates. SSM ondersteunt BIOS- en BMC-firmware-updates, maar **geen driverupdates of het bijwerken van andere componenten**.

Afbeelding 5: Geëxtrapoleerde tijd om de firmware van 100 servers voor de eerste keer bij te werken. Minder is beter. Bron: Principled Technologies.

Afbeelding 6: Afgeleide tijd voor het elke opeenvolgende keer bijwerken van firmware op 100 servers. Minder is beter. Bron: Principled Technologies.

Conclusie

Het kiezen van een leverancier voor serveraankopen gaat om meer dan alleen het hardwareplatform. Besluitvormers moeten ook rekening houden met de lange termijn, zoals systeem-/databeveiliging, energie-efficiëntie en beheergemak. Daarom zijn de systeembeheertools die een leverancier aanbiedt net zo belangrijk als de hardware.

We hebben de functies en mogelijkheden van de serverbeheertools van Dell en Supermicro onderzocht, waarbij Dell iDRAC9 werd vergeleken met Supermicro IPMI voor geïntegreerd serverbeheer en Dell OpenManage Enterprise en CloudIQ werden vergeleken met Supermicro Server Manager voor één-naar-veel apparaat- en consolebeheer en -controle. We ontdekten dat de beheertools van Dell uitgebreidere beveiligings-, duurzaamheids- en beheer-/controlefuncties en -mogelijkheden boden dan de Supermicro-servers. Bovendien automatiseerden de Dell tools meer taken om serverbeheer te vereenvoudigen, wat zorgt voor aanzienlijke tijdbesparingen voor beheerders in plaats van dat ze dezelfde taken handmatig moeten uitvoeren met Supermicro-tools.

Bij het aanschaffen van een server zijn de bijbehorende beheerproducten van een leverancier van cruciaal belang om data te beschermen, een duurzamere omgeving te ondersteunen en het onderhoud van systemen te vergemakkelijken. Uit onze tests en onderzoeken bleek dat het Dell beheerportfolio voor PowerEdge servers meer functies bood om organisaties te helpen deze doelen te bereiken dan de vergelijkbare Supermicro-beheerproducten.

1. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", geraadpleegd op 15 februari 2024, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
2. Dell, "Using iDRAC9 RSA SecurID 2FA", geraadpleegd op 15 februari 2024, https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-securid-2fa.pdf.
3. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide", geraadpleegd op 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 wachtwoordbeheer en -rotatie", geraadpleegd op 15 februari 2024, https://www.dell.com/support/kbdoc/nl-nl/000219279/openmanage-enterprise-4-0-idrac-password-management-and-rotation.
6. Dell, "OpenManage Portfolio Software Licensing Guide", geraadpleegd op 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", geraadpleegd op 15 februari 2024, https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/.
8. Dell, "Security Advisories", geraadpleegd op 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", geraadpleegd op 15 februari 2024, https://www.dell.com/nl-nl/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", geraadpleegd op 17 januari 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.
11. Supermicro, "X13DEM User's Manual", geraadpleegd op 16 februari 2024, https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf.
12. Dell, "OpenManage Enterprise", geraadpleegd op 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", geraadpleegd op 17 januari 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
14. "Integrated Dell Remote Access Controller (iDRAC)", geraadpleegd op 16 januari 2024, https://www.dell.com/nl-nl/lp/dt/open-manage-idrac.

Lees de wetenschap achter dit rapport ▶

Principled Technologies®

Facts matter.®

Dit project is uitgevoerd in opdracht van Dell Technologies.