



Förbättra säkerheten, hållbarheten och administratörens effektivitet med Dells serverhanteringsportfölj

jämfört med jämförbara serverhanteringsverktyg från HPE

När det gäller att välja servrar bör specifikationer inte vara det enda du överväger. Genom att välja en leverantör med hanteringsverktyg som minskar den tid administratörer gör praktiska ingrepp, förbättrar säkerheten och erbjuder hållbarhetsplanering kan infrastrukturen hjälpa dig att uppfylla ett antal affärs mål. I Principled Technologies datacenter jämförde vi funktionerna i serverhanteringsportföljerna från Dell och HPE för att se vad de kan erbjuda administratörer. Vi jämförde:

Tabell 1: Hanteringsverktygen vi testade.

	Dell	HPE
Inbyggd/fjärrstyrd serverhantering	Dell Technologies Integrated Dell Remote Access Controller (iDRAC9)	HPE Integrated Lights-Out (iLO 6)
Enhetshanteringskon-sol för en-till-många	Dell Technologies OpenManage™ Enterprise (OME)	HPE OneView

Vi tittade även på APEX AIOps Infrastructure Observability (tidigare CloudIQ) och några av de funktioner och fördelar som det här molnbaserade övervakningsverktyget ger för serverhantering.

I alla de funktioner och användningsfall som vi testade erbjöd verktygen från Dells hanteringsportfölj starkare säkerhetsfunktioner, omfattade ett bredare utbud av hållbarhetsverktyg och gav mer detaljerad kontroll och större flexibilitet för administratörerna, samtidigt som tiden och arbetet för att slutföra vanliga uppgifter minskade.

Förbättra säkerheten med systemlåsning i **95 % mindre tid och 83 % färre steg**

med iDRAC9 jämfört med iLO 6



Optimera energieffektiviteten med **fyra gånger fler strömhanteringsmätvärden**

och 25 anpassningsbara rapporter i OME jämfört med 0 rapporter i OneView



Förbättra fjärrfunktionerna med **16 gånger fler fjärranslutna BIOS-funktioner**

med 51 i iDRAC9 jämfört med 3 i iLO 6

Stärk heltäckande säkerhet

Cyberattacker, där skadliga aktörer infiltrerar system för att hämta och exploatera privat data, ökar. En rapport från 2023 noterade att "83 % av organisationerna upplevde mer än ett dataintrång under 2022",¹ vilket visar att cybersäkerhet är ett globalt problem. Att välja hårdvara med heltäckande säkerhetsfunktioner kan hjälpa till att skydda organisationens data från dessa kostsamma attacker. Dell erbjuder starka säkerhetsfunktioner som både är inbyggda i servern via iDRAC9 och finns i övergripande konsol- och molnhanteringsmjukvara för att stärka organisationens säkerhet.

Inbyggd säkerhet

Varje Dell PowerEdge™-server har inbyggda säkerhetsfunktioner via iDRAC9 för att förhindra att illvilliga aktörer får åtkomst till data. Två sådana viktiga funktioner är:

- **Aktivering/avaktivering av dynamisk USB-port:** Med avaktivering och aktivering av USB-portar får administratörer kontroll över åtkomsten till servern via en USB-port. Dynamisk avser möjligheten att aktivera och avaktivera dessa USB-portar utan att starta om servern eller operativsystemet. Innan administratören har gett åtkomst kan ingen ansluta en minnessticka eller ett tangentbord för att ändra några konfigurationsinställningar för systemet, operativsystemet eller BIOS.
- **Dynamisk systemlåsning:** Systemlåsning hjälper till att förhindra att oavsiktlig eller skadlig aktivitet ändrar system-BIOS, iDRAC och inställningar för fast mjukvara. Dynamisk avser möjligheten att konfigurera dessa funktioner en gång och sedan verkställa efter behov. (Obs! Den här funktionen är tillgänglig med iDRAC9 Enterprise- eller Datacenter-licenser.)

Bild 1 visar resultaten av vår praktiska jämförelse med iDRAC9 och iLO 6 för att dynamiskt avaktivera USB-portar.

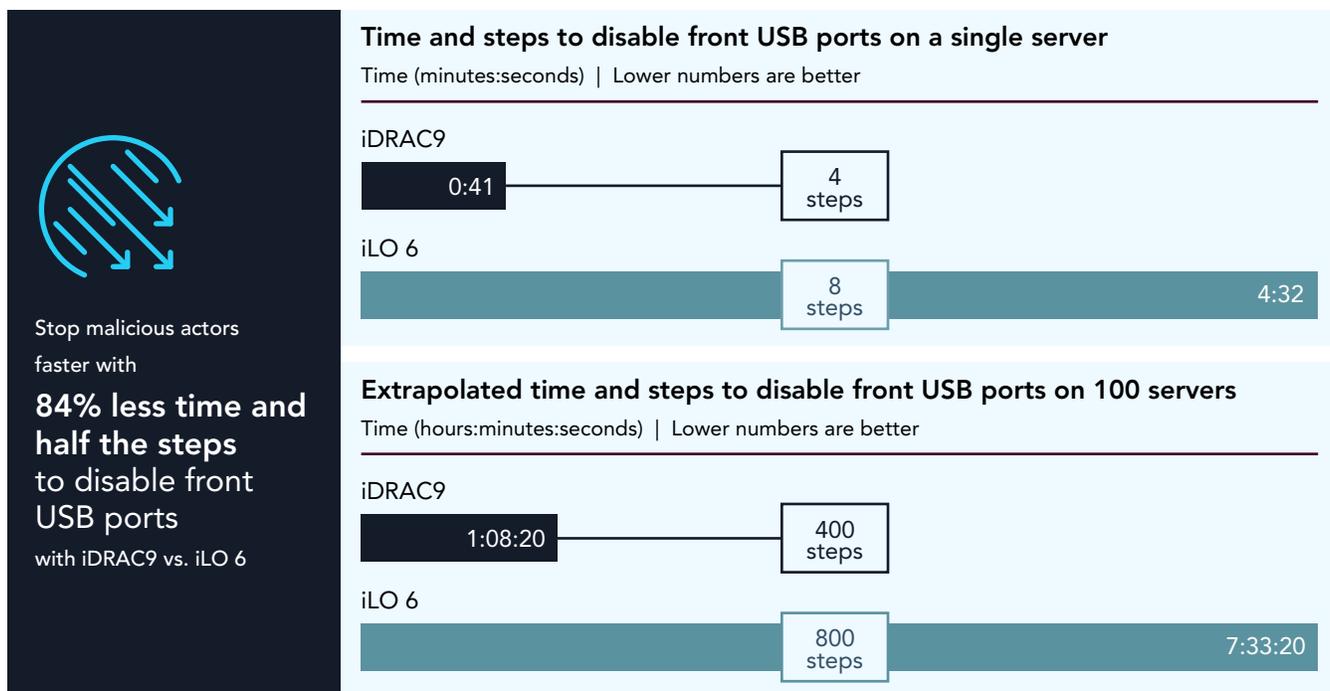


Bild 1: Tid för att avaktivera främre USB-portar för en enda server och extrapolerad tid för att avaktivera främre USB-portar för 100 servrar. Mindre tid och färre steg är bättre. Källa: Principled Technologies.

Obs! Diagrammen i den här rapporten använder olika skalor för att bibehålla en konsekvent storlek. Var uppmärksam på de olika diagrammens dataintervall när du jämför.

Med hjälp av iDRAC9 upptäckte vi att administratörer kunde avaktivera främre USB-portar på en enda server på bara 41 sekunder och med 4 steg. Jämförelsevis skulle samma process med iLO 6 ta 4 minuter 32 sekunder med 8 steg per server. Det innebär att **iDRAC9 tar 84 % mindre tid och använder hälften så många steg för att avaktivera främre USB-portar.**² När man tänker sig att dessa steg ska utföras i ett datacenter ökar tidsbesparingarna. I en distribution med 100 servrar kan administratörer avaktivera USB-portar på 6 timmar kortare tid med iDRAC9 än med iLO 6.

Dessa funktioner är inte bara enklare och snabbare att komma åt med iDRAC9 än med iLO 6, utan med iDRAC9 kan administratörerna också **ha kvar serverna i produktion** samtidigt som de aktiverar eller avaktiverar dessa funktioner, **vilket undviker driftavbrott**. Med iLO 6 måste man både ändra BIOS-konfigurationen och starta om varje gång.

Möjligheten att snabbt låsa upp ett system för uppdateringar och låsa det snabbt är avgörande. Som bild 2 visar såg vi att **administratörerna kunde slutföra systemlåsning av en server på 95 % kortare tid och 83 % färre steg med iDRAC9** jämfört med iLO 6, vilket tog över 5 minuter och 12 steg per server.

Om man extrapolerar detta till ett datacenter med 100 servrar kan administratörer låsa system på något mer än en halvtimme med iDRAC9, medan det skulle ta över en hel arbetsdag, nästan 9 timmar, att låsa 100 servrar med iLO 6. Det kan innebära avsevärd tid för angripare att få tillgång till data. Dessutom krävs serverdriftavbrott för att använda iLO 6-lösningen för systemlåsning, medan det inte gör det för iDRAC9-lösningen. Funktionen iDRAC9-låsning är mycket snabbare och enklare att använda än funktionen iLO 6-låsning.

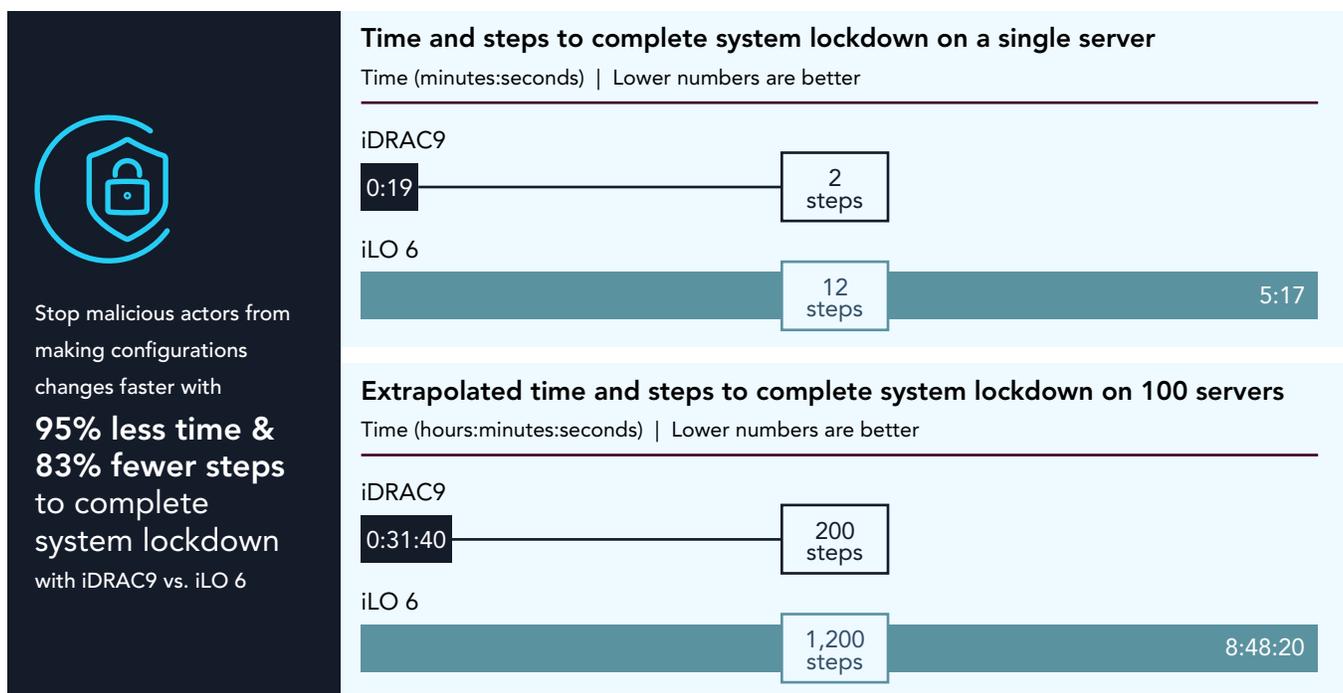


Bild 2: Tid för att slutföra systemlåsning för en enda server och extrapolerad tid för att slutföra systemlåsning för 100 servrar. Mindre tid och färre steg är bättre. Källa: Principled Technologies.

Håll dig säker med enklare hantering av inloggningsuppgifter i OME

OME ger administratörer ett enklare sätt att hantera iDRAC9-lösenordsrotation. I stället för att kräva ett statiskt, känt administratörskonto hanterar OME ett servicekonto där kunderna väljer den policy för lösenordsrotation som lösenordet aldrig avslöjas för. **OneView har inte den här funktionen.** I vårt datacenter bekräftade vi att iDRAC9-hanterade servrar integrerades med OME-kontot med fullständig administratörsbehörighet för enklare hantering av inloggningsuppgifter.

Hjälper dig att uppfylla dina hållbarhetsmål

Datacenter har stora ström- och kylningsbehov, men värme- och strömhantering kan hjälpa administratörer att optimera datacenterkostnaderna och arbeta mot hållbarhetsmål, samtidigt som de ger arbetsbelastningarna resurserna de behöver för bästa prestanda. OME innehåller flera funktioner som möjliggör noggrann övervakning och hantering av strömförbrukning, vilket potentiellt hjälper 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 OME och OneView. Källa: Principled Technologies.

Funktionen	OME	OneView
Kalkylator för koldioxidutsläpp och verktyg för kapacitetsplanering	✓	x
Temperaturaktiverad strömhanteringspolicy	✓	x
Statisk strömhanteringspolicy	✓	x
Instrumentpanel för strömhantering	✓	x
Rapporter för strömhantering med schemalagd e-postdistribution	✓	x

Tabell 3: Sammanfattning av vår jämförelse av hållbarhetsfunktioner mellan OME och OneView. Källa: Principled Technologies.

Funktionen	Viktiga fördelar med Dells hanteringsverktyg	Nackdel med HPE-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 hållbarhetsmål
 Automatiserad ström- och värmehantering	Statiska och temperaturaktiverade policyalternativ med möjlighet att aktivera när servern överskrider en strömförbruknings- eller temperaturtröskel	Inga jämförbara funktioner för automatiserad strömhantering
 Instrumentpanel för strömförbrukning och rapporter	Instrumentpanelen för insticksprogrammet OME Power Manager ger snabb åtkomst till Power Manager-data. Insticksprogrammet OME Power Manager innehåller 25 olika standard- och/eller anpassningsbara rapporter som snabbt identifierar de största energikonsumenterna, energitjuvar, underutnyttjade rack och inaktiva servrar	OneView har ingen instrumentpanel för Power Manager och har inga rapporter för strömhantering
 Mätvärden för strömhantering	Upp till fem gånger så många mätvärden , vilket ger mer detaljerad insikt i strömförbrukningshantering med 15 mätvärden	Endast 3 mätvärden , vilket ger mindre insikt och kontroll över strömförbrukningen

Koldioxidutsläpp och analys av koldioxidutsläpp

En av de funktioner som **OME omfattar är en kalkylator för koldioxidutsläpp och ett verktyg för kapacitetsplanering**. Det här verktyget hjälper organisationer att uppskatta sina utsläpp av växthusgaser, vilket ger standardvärden för energikostnader och koldioxidutsläpp per energienhet. Den här funktionen möjliggör även anpassning, vilket ger organisationer möjlighet att mata in värden för sin egen regions elkostnader och koldioxidutsläpp för varje förbrukad strömenhet för data som är specifika för datacentrets förbrukningsmodell. **OneView har ingen jämförbar funktion**, vilket gör det svårare för organisationer att planera med hållbarhet i åtanke.

Automatiserad ström- och värmehantering

OME Power Manager erbjuder automatiserad ström- och värmehantering genom både ström- och temperaturaktiverade policyalternativ som gör det möjligt för administratörer att ställa in gränser för strömförbrukning eller temperaturtröskelvärden för att minska kylningskostnaderna. **OneView erbjuder däremot ingen funktion för automatiserad ström- och värmehantering.** Eftersom administratörer inte kan ställa in gränser baserat på temperatur kan kylningskostnaderna öka på grund av brist på automatiserade kontroller.

Att optimera energiförbrukningen är en viktig strategi för att nå hållbarhetsmålen. Insticksprogrammet OME Power Manager innehåller **25 standardrapporter och/eller anpassningsbara Power Manager-relaterade rapporter** (17 i Power Manager-enheter och 8 till i Power Manager-grupper) som gör det möjligt för administratörer att optimera kapacitetsplanering och hantera ström för att maximera effektiviteten. **OneView erbjuder inga liknande rapporter om strömhantering** (se bild 3).

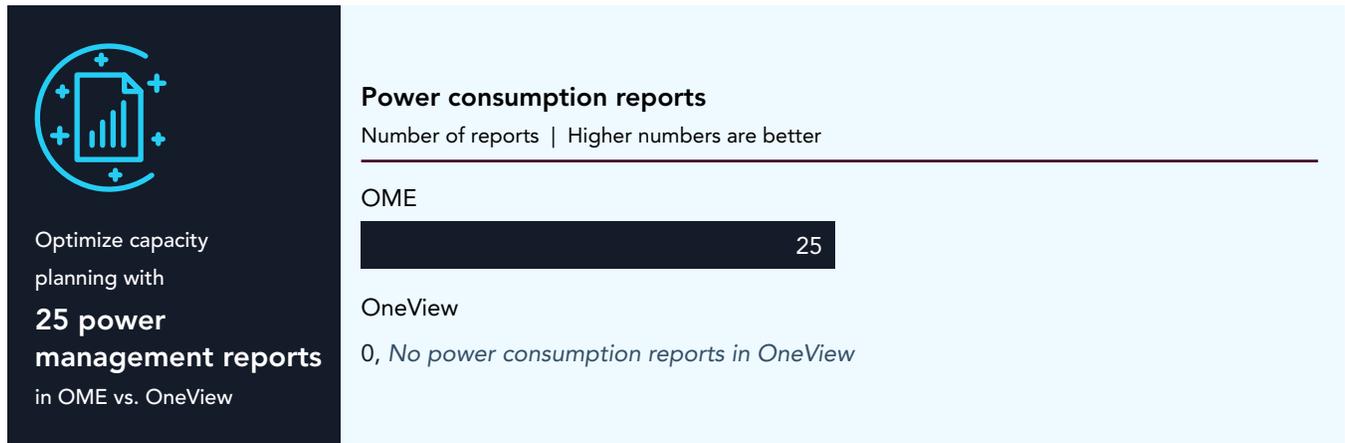


Bild 3: Jämförelse av antalet rapporter om strömhantering som finns tillgängliga i OME och OneView. Fler rapporter är bättre. Källa: Principled Technologies.

I syfte att optimera strömhanteringen ytterligare gör insticksprogrammet OME Power Manager det möjligt för administratörer att visa upp till fyra gånger fler mätvärden jämfört med OneView (se bild 4). OME tillhandahåller 15 mätvärden, inklusive strömförbrukning för **enskilda komponenter, virtuella maskiner, luftflöde och komponentanvändning**, medan OneView endast tillhandahåller 3 mätvärden.

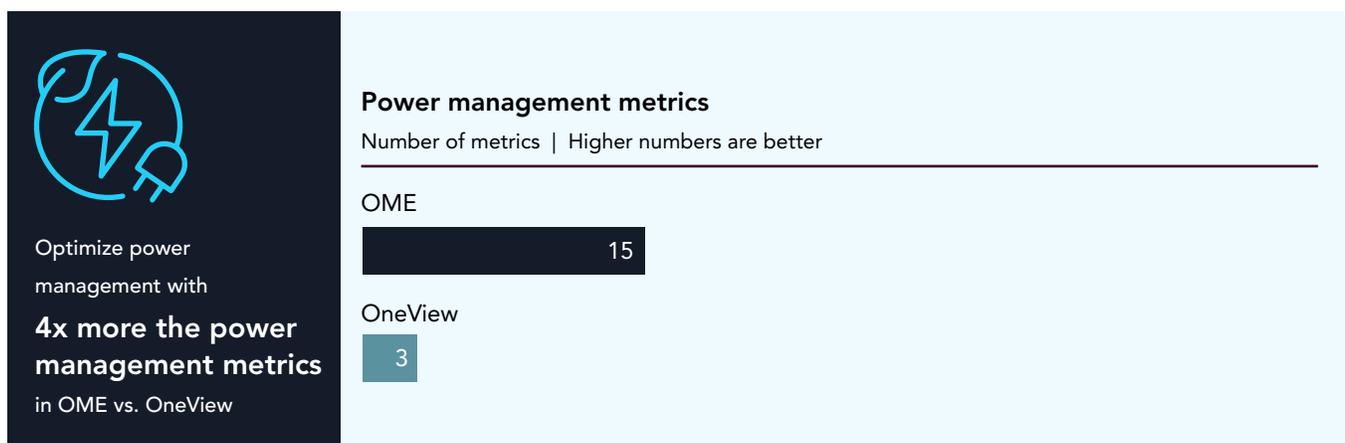


Bild 4: Jämförelse av antalet mätvärden för strömhantering som finns tillgängliga i OME och OneView. Fler mätvärden är bättre. Källa: Principled Technologies.

Gör administratörsuppgifter enklare med bättre användarvänliga funktioner

Datacenteradministratörer har mycket att göra, men rätt hanteringsverktyg kan automatisera vissa uppgifter, förbättra den dagliga hanteringen och minska arbetsbördan så att de får tid att skapa nytt. Vi har sett att Dells hanteringsportfölj erbjuder ett antal funktioner som kan förenkla administratörsuppgifter. Tabell 4 innehåller en sammanfattning av viktiga användarvänliga funktioner som finns i Dells hanteringsportfölj jämfört med HPE-hanteringsverktyg.

Tabell 4: Översikt över viktiga användarvänliga funktioner som finns i iDRAC9 och OME jämfört med iLO 6 och OneView. Källa: Principled Technologies.

Funktionen	Viktiga fördelar med Dells hanteringsverktyg	Nackdel med HPE-hanteringsverktyg
 Fler fjärranslutna BIOS- och HTML5-funktioner	iDRAC9 erbjuder 2,5 gånger så många HTML5-funktioner (med 10) och 16 gånger fler fjärranslutna BIOS-funktioner (med 51)	iLO 6 erbjuder endast 4 HTML-fjärrfunktioner och 3 fjärranslutna BIOS-funktioner
 Enklare BIOS-konfigurationsändringar	87 % mindre tid och hälften så många steg för att göra en BIOS-konfigurationsändring	Kräver administratörsnärvaro för att göra ändringar
 Telemetriströmning	iDRAC9 tillhandahåller telemetri för 8 moduler	iLO 6 tillhandahåller telemetri för endast 3 moduler med JSON-utmatning från HPE
 Anslutningsvisning	Anslutningsvyn i iDRAC9 innehåller information om den fysiska mappningen av switchportar till serverns nätverksportar och iDRAC-dedikerade portanslutningar	iLO 6 har ingen fysisk anslutningsinformation till switchar uppströms
 Skalbarhet	OME kan hantera upp till 8 000 enheter³	OneView kan endast hantera 1 024 enheter⁴
 Varningsbaserade åtgärder	OME tillhandahåller varningspolicyer som utlöser åtgärder baserat på indata från en varning för en server, en grupp med servrar eller alla servrar Konfiguration av en varning kräver en engångsinställning på 13 steg och 65 sekunder, sedan utförs åtgärden automatiskt	OneView erbjuder inte varningsbaserade åtgärder Konfiguration av en varning kräver 5 steg och 36 sekunder för varje server , vilket innebär betydande administratörstid för storskaliga distributioner
 Hantering av fast mjukvara	OME-hantering av fast mjukvara gör det möjligt att uppdatera en enskild komponent, eller alla komponenter , för överensstämmelse med en definierad baslinje	OneView erbjuder endast grundläggande överensstämmelse för fast mjukvara genom att bifoga i serverprofilen
 Övervakning av enheter från tredje part	OME har stöd för enhetsövervakning och serverövervakning från tredje part	OneView stöder inte övervakning av enheter och servrar från tredje part.
 Rapportering	OME erbjuder 4,2 gånger så många rapporter med 42 inbyggda rapporter med anpassning för ett detaljerat urval av de viktigaste data för deras ändamål	OneView erbjuder endast 10 inbyggda rapporter utan anpassning
 Mobil övervakning/hantering	OME integreras med OpenManage Mobile , vilket ger synlighet och hanterbarhet för infrastruktur på en administratörs iOS- eller Android-mobilenhet	OneView har ingen mobilapplikation , vilket gör hanteringen mindre flexibel för administratörer

I syfte att underlätta hanteringen och ge administratörer en enda plats för hantering och övervakning erbjuder OME utökad stöd för ett stort antal servrar, chassin, nätverksenheter med mera. Fullständig OpenManage-stödmatris finns på <https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix>.⁵

Enklare serverdistribution med en-till-många-konfigurationsmallar

För distributioner med flera servrar kan användning av OME förkorta tiden för att distribuera konfigurationsmallar jämfört med att använda OneView. Distribution av en konfigurationsmall för en enda server tar liknande tid med båda lösningarna: 47 sekunder och 10 steg för OME, 49 sekunder och 5 steg för OneView. Men administratörerna kan driftsätta konfigurationsmallar på servergrupper i OME, medan administratörer i OneView måste driftsätta konfigurationer på varje server individuellt.

Det innebär att för en identiskt konfigurerad distribution med 100 servrar skulle det bara krävas 47 sekunder och 10 administratörssteg med OME, medan det i OneView skulle krävas ungefär 1 timme och 21 minuter och 500 steg för att distribuera konfigurationsmallar till servrar, vilket innebär 99 % mindre tid och 98 % färre steg (se bild 5).

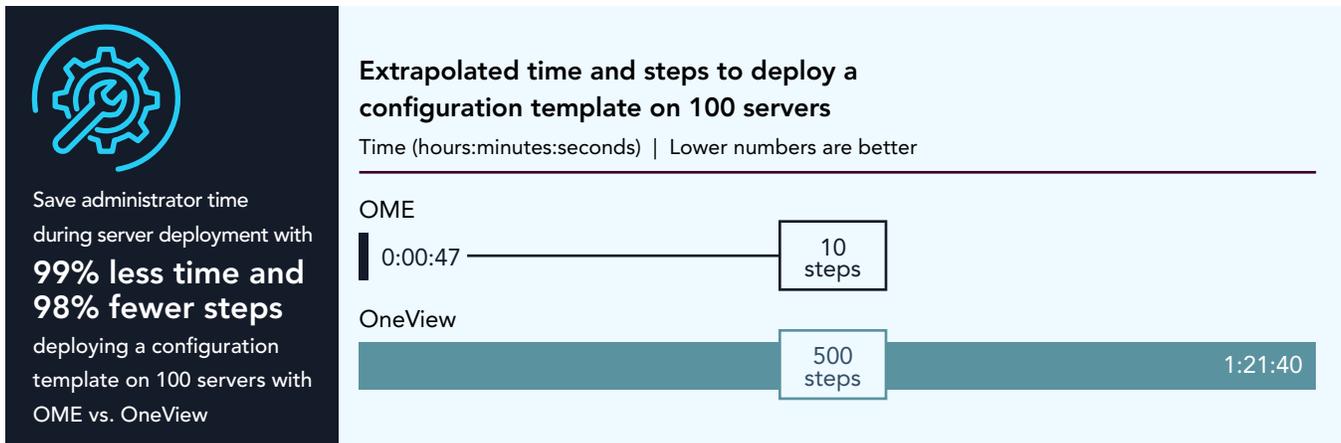


Bild 5: Jämförelse av tid och steg som krävdes för att distribuera konfigurationsmallar med OME jämfört med OneView. OME kan tillämpa en mall på många servrar samtidigt, vilket ökar tidsbesparingarna ännu mer. Mindre tid och färre steg är bättre. Källa: Principled Technologies.

Enklare konfiguration av varningar

Vi upptäckte att OME erbjöd fler alternativ för att övervaka infrastruktur. OME gör det möjligt för användarna att konfigurera varningspolicyer en gång och sedan tilldela dem automatiskt för framtida varningar. Vi skapade en varningspolicy som skulle utföra en smidig avstängning om systemet fick en varning om kritisk temperatur från iDRAC9. Policyn hade 13 steg och tog 65 sekunder. Medan engångskonfigurationen för automatisering av varningar tar längre tid (1 minut och 5 sekunder) jämfört med att använda OneView (36 sekunder och 5 steg), har OneView inga automatiserade alternativ för varningar och administratörerna måste därför utföra åtgärderna manuellt varje gång. Det innebär att för en distribution med 100 servrar skulle användning av OME kunna spara upp till 98 % i tid och 97 % i steg genom att automatisera åtgärder baserat på varningar efter att administratörer har skapat en policy jämfört med OneView.

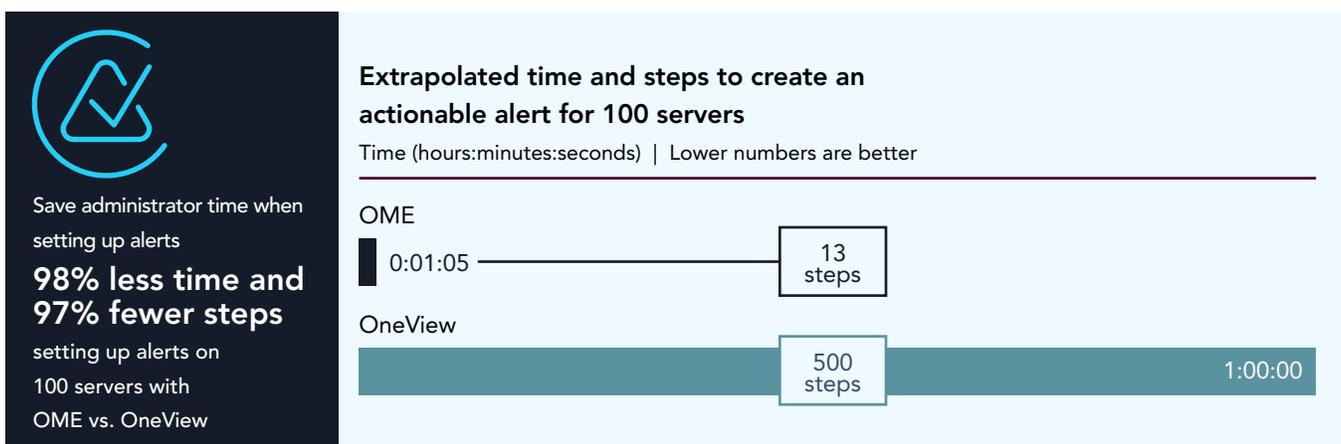


Bild 6: Jämförelse av tid och steg som krävdes för att konfigurera varningar med OME jämfört med OneView. OME automatiserar varningar efter en enda konfiguration, vilket sparar administratörstid och arbete. Mindre tid och färre steg är bättre. Källa: Principled Technologies.

Om Dell Technologies OpenManage Enterprise

OME är en en-till-många-systemhanteringskonsol för datacentret och mer därtill. 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). OME erbjuder fullständig livscykelhantering av Dell PowerEdge-serverar och kan upptäcka och inventera IPV4- och IPV6-nätverk för upp till 8 000 enheter, inklusive Dell-rackserverar, Dell-tornserverar och Dell-blad och -chassin.⁶ I en PT-studie som utfördes nyligen såg vi att en Dell-miljö med OME 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.⁷

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

Fjärrhantering

Funktioner för fjärrhantering ger administratörerna friheten att göra fler ändringar utanför datacentret. Vi såg att iDRAC9 erbjuder 1,5 gånger fler HTML5-fjärrkonsolfunktioner än iLO 6, med totalt 10 funktioner jämfört med bara 4, vilket gör iDRAC9-fjärrserverhantering enkel och effektiv. iDRAC9 erbjuder också 16 gånger fler BIOS-konfigurationsfunktioner än iLO 6 (51 funktioner jämfört med bara 3 funktioner), vilket ger administratörerna mer detaljerad kontroll över BIOS-konfigurationen (se bild 7 och bild 8).

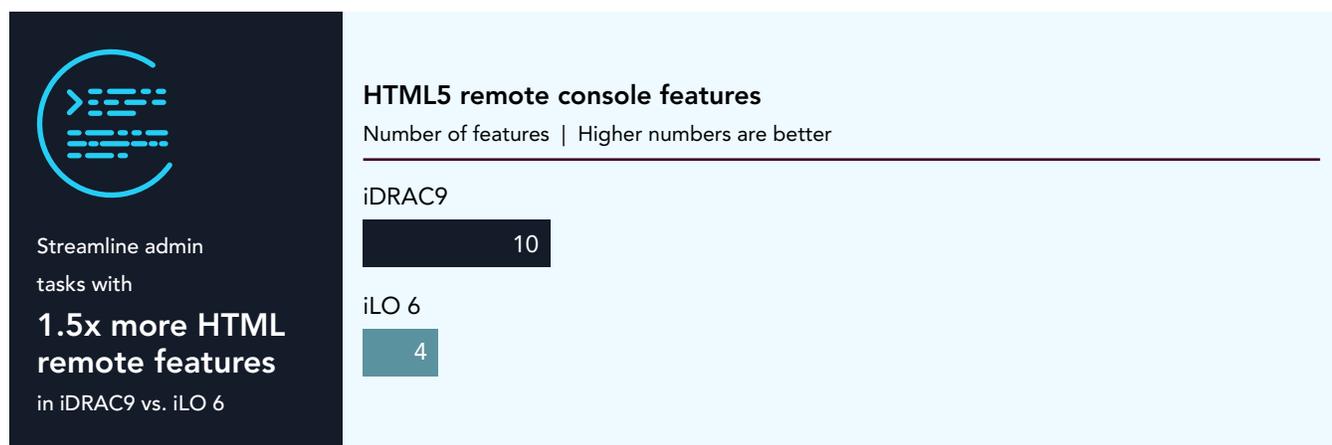


Bild 7: Jämförelse av HTML5-fjärrfunktioner som de olika hanteringsverktygen erbjuder. Fler funktioner är bättre. Källa: Principled Technologies.

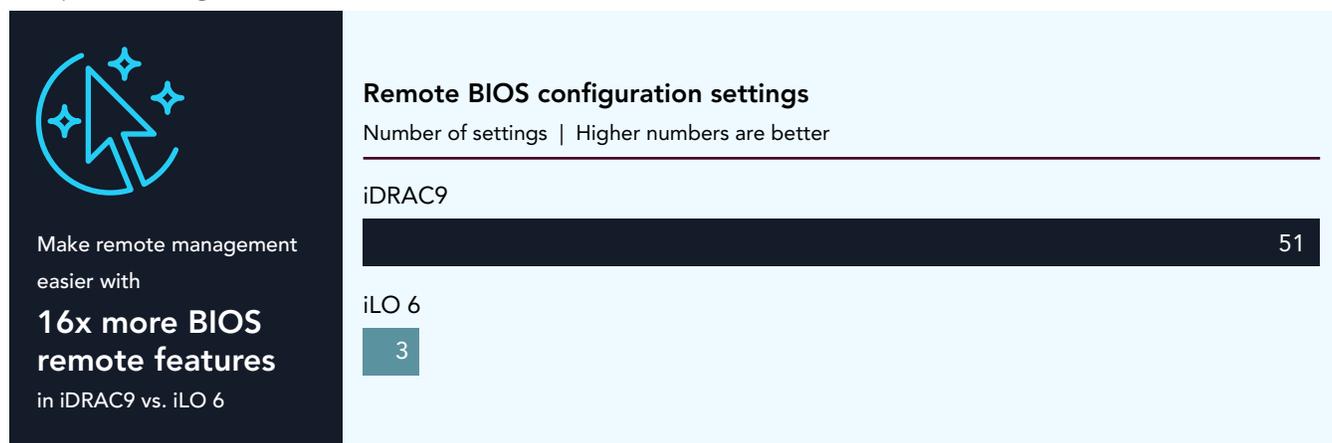


Bild 8: Jämförelse av fjärranslutna BIOS-funktioner som de olika hanteringsverktygen erbjuder. Fler funktioner är bättre. Källa: Principled Technologies.

Göra BIOS-konfigurationsändringar

Med iDRAC9 kan administratörerna ändra inställningarna för BIOS-konfigurationen och stega upp uppdateringen för en senare omstart utan att ytterligare administratörsnärvaro krävs. iLO 6 kräver däremot ändringar från systemverktygen och manuella administratörsåtgärder under ändringen. Som bild 9 visar tog förberedelse av BIOS-konfigurationsändringen för en schemalagd omstart 87 % mindre tid och omfattade hälften så många steg med iDRAC9 jämfört med iLO 6. Dessa tidsbesparingar per server kan leda till att man sparar viktig administratörstid i större distributioner. I en distribution med 100 servrar kan man till exempel spara mer än 6 timmar. Både iDRAC9 och iLO 6 kräver individuella BIOS-konfigurationsändringar per server.

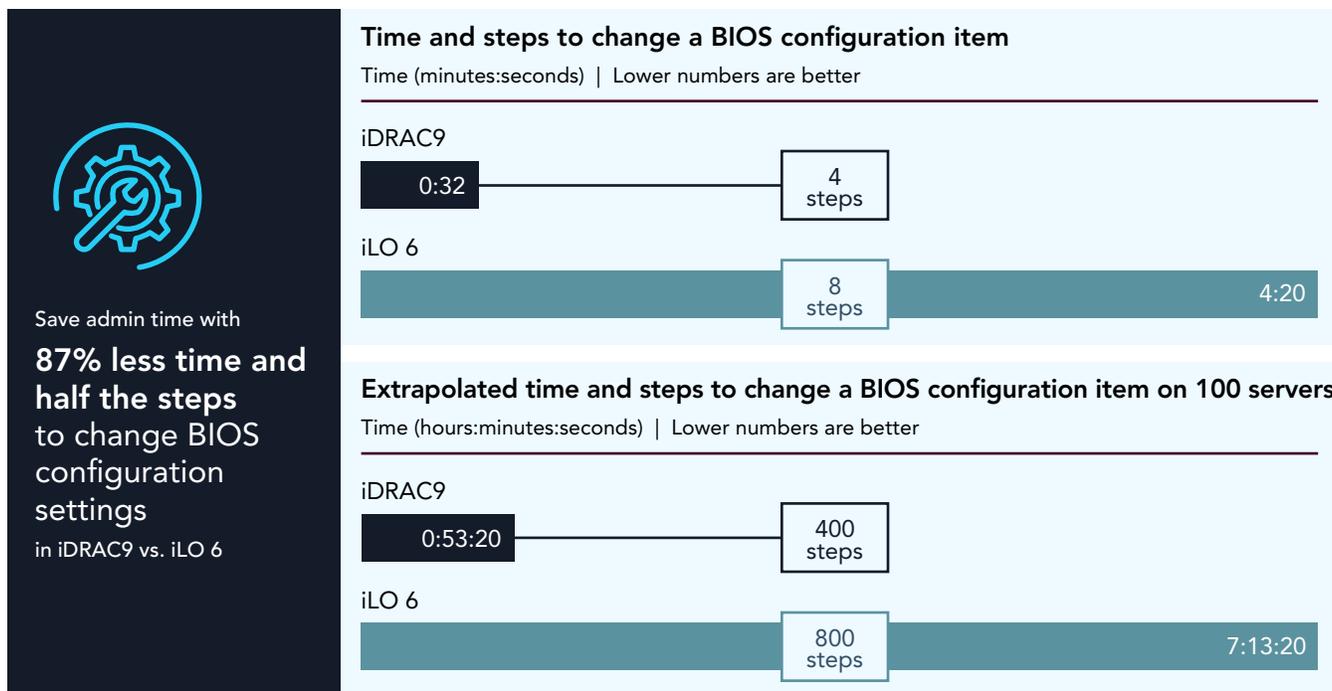


Bild 9: Tiden för att ändra BIOS-konfigurationsinställningarna och förbereda en uppdatering för en senare omstart för en enda server och extrapolerad tid för 100 servrar. Mindre tid och färre steg är bättre. Källa: Principled Technologies.

Om Dell Technologies Integrated Dell Remote Access Controller 9

Dell PowerEdge™-servrar omfattar iDRAC9 med Dell Lifecycle Controller för att tillhandahålla 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
- Telemetri och automatisering
- Starka säkerhetsfunktioner och alternativ⁸

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

Öka säkerheten, hållbarheten och administratörseffektiviteten med APEX AIOps Infrastructure Observability (tidigare CloudIQ)

Det molnbaserade övervakningsverktyget APEX AIOps Infrastructure Observability (tidigare CloudIQ) ger administratörer ett sätt att övervaka, hantera och analysera prestanda över distributioner av Dell PowerEdge-infrastruktur, inklusive servrar, lagring och mycket mer. APEX AIOps Infrastructure Observability (tidigare CloudIQ) erbjuder flera säkerhetsfunktioner som kan stärka organisationen ytterligare mot attacker. Vi lyfter fram några av dessa funktioner i tabell 5.

Tabell 5: Översikt över viktiga säkerhetsfunktioner som är tillgängliga i APEX AIOps Infrastructure Observability (tidigare CloudIQ). Källa: Principled Technologies.

Funktionen	Så fungerar APEX AIOps Infrastructure Observability (tidigare CloudIQ) för att skydda din miljö
 Varningar på cybersäkerhetsrisknivå	Tillhandahåller täta insikter för cybersäkerhet med specifika varningar på säkerhetsrisknivå så att administratörer kan reagera snabbare och åtgärda problem snabbt för att skydda sina data.
 Policybaserad säkerhetskfiguration	Erbjuder policybaserade inställningar för säkerhetskfiguration och lättanvända mallar som gör det möjligt för en administratör att säkerställa att inställningar för bästa säkerhetspraxis finns på plats och skyddar PowerEdge-miljön.
 Rådgivning om cybersäkerhet	Tillhandahåller relevant rapportering av säkerhetsrekommendationer, med specifik sårbarhetsinformation och förslag på åtgärder, vilket möjliggör snabba insatser för att åtgärda säkerhetsluckor.

Med hjälp av dessa funktioner för säkerhetsövervakning från molnet ger APEX AIOps Infrastructure Observability (tidigare CloudIQ) administratörerna ett annat användarvänligt automatiserat sätt att hålla infrastrukturens hälsa och säkerhet under kontroll.

Ytterligare funktioner för hållbarhet och effektivitet i APEX AIOps Infrastructure Observability (tidigare CloudIQ)

Den molnbaserade övervakningsplattformen APEX AIOps Infrastructure Observability (tidigare CloudIQ) erbjuder ytterligare användarvänliga funktioner som integreras med iDRAC9 och OME för att göra det lättare för administratörer att övervaka statusen för PowerEdge-miljön och vidta åtgärder där det behövs. Dessa är några av funktionerna:

- **Analys av koldioxidutsläpp:** Det här verktyget finns i övervakningsavsnittet och ger en högre vy och prognos för koldioxidutsläpp i olika miljöer.
- **Prestandavyer:** APEX AIOps Infrastructure Observability (tidigare CloudIQ) tillhandahåller prestandavyer och diagram för avvikelser och användning som kan varna administratörerna vid första tecken på problem.
- **Anpassningsbara prestanda- och lagerrapporter:** APEX AIOps Infrastructure Observability (tidigare CloudIQ) innehåller anpassade rapporteringsalternativ för serverprestanda och lagerdata, vilket ger administratörerna mer kontroll över de prestanda- och enhetsmätvärden som de är intresserade av att följa.

Om APEX AIOps Infrastructure Observability (tidigare CloudIQ)

APEX AIOps Infrastructure Observability (tidigare 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 APEX AIOps Infrastructure Observability (tidigare CloudIQ) hade försumbar inverkan på nätverksbandbredden samtidigt som vi kunde övervaka telemetri, hälsostatus, varningar och lager från en enda konsol.¹⁰ Läs mer om APEX AIOps Infrastructure Observability (tidigare CloudIQ) på <https://www.dell.com/en-us/dt/apex/aiops.htm>.

När vi hade slutfört testerna släppte Dell nya funktioner som gör det möjligt för administratörer att göra **systemuppdateringar** inifrån APEX AIOps Infrastructure Observability (tidigare CloudIQ). Enligt Dells dokumentation har sidan System Updates (Systemuppdateringar) upp till fem kategorier för systemuppdateringar: lagring, nätverk, HCI, dataskydd och server. Även om vi inte testade den här funktionen vid detta tillfälle planerar vi att validera dess kapacitet i en kommande rapport.¹¹

Sammanfattning

När du köper en hårdvara får du också tillgång till hårdvaruleverantörens portfölj av hanteringsverktyg för att hantera och övervaka din infrastruktur. Specifikationerna är viktiga, men det är också heltäckande säkerhet, att uppfylla hållbarhetsmål och att kunna effektivisera administratörsuppgifter. I vårt datacenter jämförde vi funktionerna i serverhanteringsverktyg från Dell och HPE, där iDRAC9 jämfördes med iLO 6 för inbäddad serverhantering och OME med OneView för enhets- och konsolhantering och övervakning för en-till-många.

När det gäller säkerhet, hållbarhet och hantering/övervakning såg vi att Dells serverhanteringsverktyg hade mer att erbjuda än jämförbara HPE-verktyg. Det gav administratörerna fler alternativ för fjärrhantering, minskade tiden för att låsa system och erbjöd mer detaljerad kontroll för att hjälpa till att uppfylla hållbarhetsmålen. Genom att minska administratörens tid och arbete för vissa rutinmässiga övervaknings- och underhållsuppgifter med Dells hanteringsportfölj kan du ge teamet tid att skapa nytt och stödja andra initiativ.

1. Harvard Business Review, "The Devastating Business Impacts of a Cyber Breach", läst 10 april 2024, <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach>.
2. Obs! Den här metoden på HPE ILO 6 stänger av alla externa USB-portar, inte bara de främre portarna.
3. Dell, "OpenManage Enterprise 4.0.x Support Matrix", läst 19 april 2024, <https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix>.
4. HPE, "HPE OneView 8.7 Support Matrix", läst 19 april 2024, https://support.hpe.com/hpsc/public/docDisplay?docId=sd00003831en_us&page=GUID-D7147C7F-2016-0901-066B-000000000529.html.
5. Dell, "OpenManage Enterprise 4.0.x Support Matrix", läst 19 april 2024, <https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix>.
6. Dell, "OpenManage Enterprise", läst 9 april 2024, <https://www.dell.com/en-us/work/learn/openmanage-enterprise>.
7. Principled Technologies, "A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators", läst 9 april 2024, <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>.

-
8. Dell, "Integrated Dell Remote Access Controller (iDRAC)", läst 9 april 2024, <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.
 9. Dell, "APEX AIOps: Tame IT complexity in your digital business", läst 10 juni 2024, <https://www.dell.com/en-us/dt/apex/aiops.htm>.
 10. Principled Technologies, "Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests", läst 9 april 2024, <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>.
 11. Dell, "System Updates", läst 19 april 2024, <https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/system-updates-2/>.

Läs vetenskapen bakom rapporten ►

► Se den ursprungliga, engelska versionen av den här rapporten



Facts matter.®

Det här projektet har beställts av Dell Technologies.

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.