Rafforza i processi di sicurezza con

funzionalità di sicurezza 3,5 volte maggiori

Tra cui l'autenticazione a due fattori e la gestione delle chiavi esterne con iDRAC9

Ottimizza l'efficienza energetica con

report sul consumo energetico oltre 6 volte maggiori

Con 20 report in Dell OME rispetto a 3 report in Supermicro SSM

Aumenta l'efficienza operativa risparmiando 1 ora e 50 minuti sul tempo di amministrazione

ogni 100 server

Utilizzo di aggiornamenti automatici con Dell iDRAC9 rispetto a nessun aggiornamento automatico disponibile con Supermicro IPMI

Aumenta la sicurezza, la sostenibilità e l'efficienza con i solidi strumenti di gestione dei server Dell

Rispetto al portafoglio di gestione Supermicro

Quando si investe in nuovi server per il data center, si fa molto di più che selezionare l'hardware: si sceglie anche la soluzione di gestibilità. Quando gli amministratori dispongono di strumenti efficienti e ricchi di funzionalità per implementare, monitorare, gestire e proteggere l'infrastruttura, migliorando al contempo l'efficienza energetica, possono occuparsi con facilità della gestione delle attività quotidiane e dedicare più tempo alle innovazioni che fanno progredire l'organizzazione. Scegliendo di acquistare da un vendor con strumenti di gestibilità affidabili, è possibile risparmiare tempo e denaro.

Abbiamo valutato i portafogli di gestione dei server di Dell™ e Supermicro®, confrontando tre strumenti Dell con due strumenti Supermicro.

Tabella 1: Gli strumenti di gestione che abbiamo testato. *Dell CloudIQ è uno strumento di monitoraggio e analisi basato sul cloud; Supermicro non offre uno strumento equivalente.
Fonte: Principled Technologies.

	Dell	Supermicro
Gestione integrata/ remota dei server	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
Console di gestione dei dispositivi one-to-many	Dell OpenManage™ Enterprise (OME) Dell CloudIQ*	Supermicro Server Manager (SSM)

In termini di sostenibilità, sicurezza ed esperienza di gestione quotidiana, dalle nostre rilevazioni è emerso che Dell ha fornito costantemente set di strumenti più ricchi di funzionalità che offrono agli amministratori più opzioni e funzionalità.

Funzionalità sempre più avanzate per automatizzare e semplificare la gestione dei server

I team IT hanno bisogno di strumenti di gestione moderni e ricchi di funzionalità, che consentano di risparmiare tempo nelle operazioni quotidiane e di stare al passo con gli standard di sicurezza ed efficienza. Gli strumenti di gestione Dell valutati includono una serie di funzionalità non presenti nel portafoglio di gestione Supermicro.

Sostenibilità

Man mano che i costi energetici aumentano e le normative ambientali si fanno più stringenti, molte organizzazioni rendono la sostenibilità una priorità. Per loro definizione, i data center richiedono grandi quantità di energia, ma la gestione termica e del consumo energetico attenta può consentire alle organizzazioni di ridurre la quantità di energia che consumano. Dell OpenManage Enterprise include diverse funzionalità che rendono possibile il monitoraggio ravvicinato e la gestione del consumo energetico, contribuendo potenzialmente al raggiungimento degli obiettivi di sostenibilità. Le Tabelle 2 e 3 evidenziano i vantaggi principali di queste funzionalità, che descriviamo più nel dettaglio di seguito.

Tabella 2: Differenze di sostenibilità tra Dell OpenManage Enterprise e SSM. Fonte: Principled Technologies.

Funzione	Strumenti di gestione Dell	Strumenti di gestione Supermicro
Calcolatore dell'utilizzo delle emissioni di anidride carbonica e strumento di pianificazione della capacità	✓	x
Analisi dell'impronta di carbonio	✓	x
Policy di gestione dell'alimentazione attivata in base alla temperatura	✓	x
Policy di gestione dell'alimentazione statica	✓	✓

Tabella 3: Riepilogo del confronto tra Dell OME e Supermicro SSM e IPMI. Fonte: Principled Technologies.

Funzione	Vantaggi principali degli strumenti di gestione Dell	Svantaggio degli strumenti di gestione Supermicro
Calcolatore dell'utilizzo delle emissioni di anidride carbonica e strumento di pianificazione della capacità	Possibilità di effettuare la stima delle **emissioni di gas serra** con valori personalizzabili per raggiungere gli obiettivi di sostenibilità	**Nessuna funzionalità paragonabile**; rende difficile pianificare il raggiungimento degli obiettivi di sostenibilità
Analisi dell'impronta di carbonio	**Disponibile** tramite OpenManage Enterprise Power Manager; fornisce dati sulle emissioni di carbonio, che possono aiutarti a raggiungere gli obiettivi di sostenibilità	**Nessuna funzionalità paragonabile**; nessun modo per tenere traccia dell'impronta di carbonio per aiutarti a monitorare il raggiungimento degli obiettivi di sostenibilità
Gestione termica e dell'alimentazione automatizzata	Opzioni di **policy statiche e attivate in base alla temperatura** con l'opzione di attivarsi quando il server supera una certa soglia di consumo energetico o della temperatura	**Un tipo di policy statica** senza opzioni di trigger associate
Report sul consumo energetico	**Più di 6 volte** il numero di report, con **20** report integrati con opzioni di distribuzione e personalizzazione pianificate tramite e-mail	**2 report integrati** in SSM e 1 report in Supermicro IPMI non esportabile
Metriche della gestione dell'alimentazione	**Metriche fino a 15 volte superiori**, che offrono informazioni più granulari sulla gestione del consumo energetico	**Solo 1 metrica**, che fornisce meno informazioni e controllo sul consumo energetico

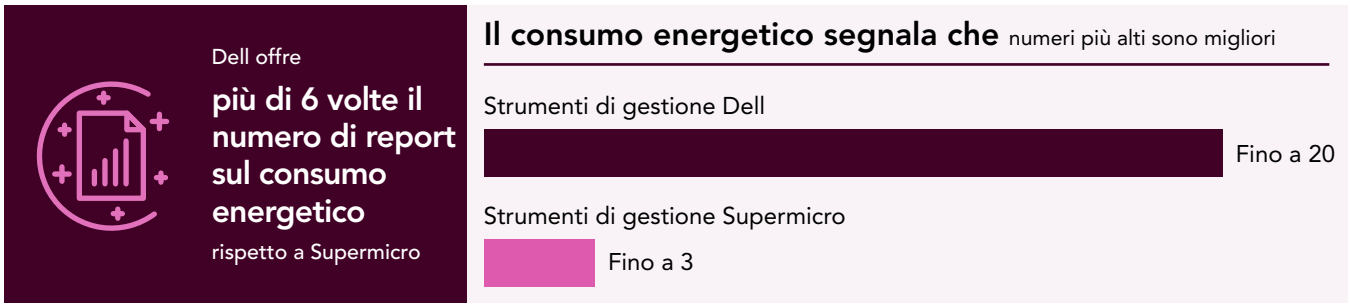

Figura 1. Numero di report sul consumo energetico disponibili in Dell OME e Supermicro SSM. Fonte: Principled Technologies.

Figura 2. Numero di metriche di gestione dell'alimentazione disponibili in Dell OME e Supermicro SSM. Fonte: Principled Technologies.

Gestione termica e dell'alimentazione automatizzata

OpenManage Enterprise Power Manager offre la gestione automatizzata energetica e termica tramite opzioni di policy attivate in base sia alla temperatura sia all'alimentazione statica, con cui gli amministratori possono impostare i limiti per il consumo energetico o le soglie della temperatura per ridurre i costi di raffreddamento. Al contrario, SSM dispone di un'unica policy, un limite statico sul consumo energetico che non viene attivato automaticamente quando un server supera il limite, il che potrebbe comportare costi energetici più elevati.

Le organizzazioni che desiderano analizzare nel dettaglio il consumo energetico del proprio data center nell'ottica dell'ottimizzazione possono trarre vantaggio dai **20 diversi report sul consumo energetico integrati** offerti da OpenManage Enterprise Power Manager. Questi report sono utili nella pianificazione della capacità e nella gestione energetica per massimizzare l'efficienza. Le opzioni di reporting in SSM sono molto più limitate. Gli amministratori possono eseguire un solo host con un report di servizio o visualizzare la tendenza del consumo energetico nella schermata di monitoraggio. Con Supermicro IPMI, gli utenti possono visualizzare un grafico dell'energia a livello di componente nel BMC; tuttavia, non possono esportare i dati nel grafico per l'analisi e salvarli solo come immagine.

Il plug-in OpenManage Enterprise Power Manager consente agli amministratori di **visualizzare fino a 15 metriche diverse**, tra cui l'utilizzo dell'energia da parte dei singoli componenti, il flusso d'aria e l'utilizzo dei componenti, mentre SSM offre solo il consumo energetico totale.

Analisi delle emissioni e dell'impronta di carbonio

OME include un calcolatore dell'utilizzo delle emissioni di carbonio e uno strumento di pianificazione della capacità che, tra le altre funzioni, può aiutare a stimare le proprie emissioni di gas serra. Fornisce valori predefiniti per i costi energetici e le emissioni di carbonio per un'unità di energia consumata, ma consente di personalizzare tali valori in base ai costi energetici della propria regione e al modello di consumo del data center. SSM non offre funzionalità paragonabili, il che può rendere difficile per le organizzazioni pianificare e monitorare i progressi verso i propri obiettivi di sostenibilità.

Sicurezza

La criminalità informatica sta aumentando in modo esponenziale, minacciando le aziende con "danni e distruzione dei dati, denaro rubato, perdita di produttività, furto di proprietà intellettuale, furto di dati personali e finanziari, appropriazione indebita, frode, interruzione post-attacco dei normali processi aziendali, indagini forensi, ripristino e cancellazione di dati e sistemi violati, e danno alla reputazione".[1] In questo contesto, i responsabili delle decisioni devono mettere in conto la sicurezza in ogni acquisto di server. Abbiamo riscontrato che Dell OpenManage Enterprise incorpora diverse funzionalità per mantenere i dati al sicuro che gli strumenti Supermicro non dispongono (vedere le tabelle 4 e 5).

Tabella 4: Differenze in termini di sicurezza tra gli strumenti di gestione Dell e Supermicro. Fonte: Principled Technologies.

Funzione	Strumenti di gestione Dell	Strumenti di gestione Supermicro
Autenticazione a più fattori	✓	x
Gestione esterna delle chiavi	✓	x
Controllo degli accessi basato sugli ambiti	✓	x
Configurazione della sicurezza basata sulle policy	✓	x
Avvisi sulla sicurezza informatica	✓	x
Controllo degli accessi basato sui ruoli	✓	✓
Disabilitazione dinamica delle porte USB	✓	✓

Tabella 5: Riepilogo del confronto delle funzioni di protezione tra gli strumenti di gestione Dell e Supermicro. Fonte: Principled Technologies.

Funzione	Vantaggi principali degli strumenti di gestione Dell	Svantaggio degli strumenti di gestione Supermicro
Autenticazione a più fattori (MFA)	**Autenticazione a due fattori** con iDRAC con **e-mail e RSA SecurID**, che impedisce agli utenti non autorizzati di accedere ai dati sensibili	**Nessuna funzionalità paragonabile**; si crea una lacuna della sicurezza che potrebbe aiutare gli utenti non autorizzati ad accedere ai dati sensibili
Gestione esterna delle chiavi	**Secure Enterprise Key Manager** in iDRAC per aggiungere un altro livello di sicurezza per proteggere i dati inattivi sui server utilizzando la crittografia delle unità e la gestione centralizzata	**Nessuna funzionalità paragonabile**; si crea un'altra lacuna della sicurezza
Controllo degli accessi	OME offre **sia** il controllo dell'accesso basato su ruoli **(RBAC)** che il controllo dell'accesso basato sulla portata **(SBAC)** per limitare i gruppi di dispositivi a cui un amministratore di dispositivi ha accesso	**Solo RBAC**, che restringe la capacità degli amministratori di limitare l'accesso
Configurazione della sicurezza basata sulle policy	Impostazioni di **configurazione della sicurezza basate su policy** tramite CloudIQ, che avvisa gli amministratori in caso di discrepanze	**Nessuna funzionalità paragonabile**, che può ritardare l'azione e la correzione delle violazioni
Avvisi sulla sicurezza informatica	**Reporting degli avvisi di sicurezza** tramite la sicurezza Dell CloudIQ, con dettagli sulle vulnerabilità e suggerimenti di correzione applicabili per consentire un'azione rapida	**Nessuna funzionalità paragonabile**, lasciando lacune di sicurezza che gli utenti malintenzionati possono sfruttare

Autenticazione a più fattori

L'autenticazione a più fattori (MFA) può impedire a utenti non autorizzati e malintenzionati di accedere ai dati sensibili. Abbiamo verificato che Dell iDRAC abilita l'autenticazione a due fattori sia con e-mail che con RSA SecurID, una serie di tecnologie di autenticazione a più fattori esterne utilizzate in molti settori.[2] Abbiamo anche verificato che né Supermicro IPMI né SSM offrono questa funzione, lasciando una lacuna in termini di sicurezza.

Gestione delle chiavi

I sistemi di gestione delle chiavi esterni (KMS) consentono ai team IT di utilizzare un server di terze parti separato per gestire le chiavi utilizzate per bloccare e sbloccare lo storage di un server, aggiungendo un livello di sicurezza. iDRAC include il gestore delle chiavi locale (LKM) per tutti i nuovi server Dell PowerEdge. Alcune licenze offrono anche Secure Enterprise Key Manager (SEKM), che offre una maggiore sicurezza con la crittografia completa del disco e la gestione delle chiavi esterne. SEKM supporta il protocollo OASIS KMIP standard del settore, offrendo alle organizzazioni la possibilità di scegliere qualsiasi provider KMS esterno che utilizza tale standard. Supermicro non offre questa funzione di sicurezza o un'altra funzione equivalente.

Controllo degli accessi

Il controllo degli accessi basato sui ruoli RBAC, in cui il ruolo di un utente determina le parti del sistema a cui ha accesso e le attività che può eseguire, è un componente fondamentale di molte strategie di sicurezza dei server. In OpenManage Enterprise, RBAC definisce i privilegi dell'utente per tre ruoli predefiniti: Amministratore, Gestore di dispositivi e Visualizzatore.[3] Offre inoltre il controllo degli accessi basato sull'ambito (SBAC), che consente agli amministratori di limitare i gruppi di dispositivi a cui un gestore di dispositivi ha accesso.[4] In questo modo gli amministratori possono fornire l'accesso a un sottoinsieme di dispositivi. Supermicro offre RBAC, ma non SBAC.

Gestione delle credenziali

La rotazione delle password iDRAC ha diversi scopi: ruota l'accesso a OpenManage Enterprise in conformità alla policy di sicurezza, con un'impostazione predefinita mensile, funziona con un gestore di password esterno e supporta CyberArk per la gestione delle password.[5][6]

Con OpenManage Enterprise, gli amministratori possono gestire la rotazione delle password iDRAC sostituendo la necessità di un account amministratore statico e noto con un account di servizio gestito da OME. SSM non dispone di questa funzionalità.

Configurazione della sicurezza basata sulle policy

Dell offre la funzionalità della sicurezza informatica basata sulle policy in CloudIQ per la soluzione PowerEdge AIOps. Questa funzionalità utilizza la configurazione di un server PowerEdge implementato e la confronta con una policy di configurazione correlata alla sicurezza basata sulle best practice Dell. Nel caso in cui CloudIQ rilevi una discrepanza, informa l'amministratore e fornisce la procedura per la correzione.[7] SSM non offre funzionalità equivalenti, il che potrebbe comportare ritardi nel rilevamento delle violazioni.

Avvisi sulla sicurezza informatica

Gli avvisi di sicurezza notificano al pubblico i problemi di sicurezza. Secondo Dell, la pagina degli avvisi di sicurezza Dell in CloudIQ fornisce un elenco completo delle avvertenze di sicurezza applicabili, insieme al relativo impatto, al numero di sistemi interessati e alla data di pubblicazione.[8] Dell CloudIQ fornisce un report sugli avvisi di sicurezza con dettagli sulle vulnerabilità e suggerimenti per la correzione. SSM non offre una funzionalità simile, il che potrebbe rendere i sistemi vulnerabili.

Informazioni su Dell CloudIQ

Dell CloudIQ è uno strumento AIOps basato sul cloud che offre "monitoraggio proattivo, apprendimento automatico e analisi predittiva" per un elevato numero di prodotti e servizi Dell, tra cui server, storage, appliance di protezione dei dati e infrastruttura iperconvergente.[9] In uno studio di Principled Technologies del 2022, abbiamo rilevato che CloudIQ ha avuto un impatto trascurabile sulla larghezza di banda della rete, ma al contempo ha reso possibile monitorare la telemetria, lo stato di integrità, gli avvisi e l'inventario da un'unica console.[10]

Ulteriori informazioni su CloudIQ sono disponibili all'indirizzo https://www.dell.com/en-us/dt/solutions/cloudiq.htm.

Disabilitazione dinamica delle porte USB

La disabilitazione e l'abilitazione delle porte USB consente agli amministratori di controllare l'accesso al server tramite una porta USB, evitandone così l'uso dannoso e introducendo il rischio di installazione di applicazioni o virus vietati.

Dell iDRAC offre la disabilitazione indipendente e dinamica della porta USB senza necessità di downtime. Sebbene Supermicro offra la disabilitazione dinamica delle porte USB anteriori (e USB posteriore) all'interno del BIOS, per attivarla è necessaria la chiave di licenza di Supermicro Datacenter Management Suite per nodo. L'IT può attivarla implementando il comando di blocco del sistema, che può essere eseguito dal BMC o dalla console Supermicro IPMI, ma non è indipendente dalla modalità di blocco del sistema.[11]

Come illustrato nella Figura 3, la disabilitazione delle porte tramite Dell iDRAC è stato un processo semplice **che ha richiesto solo 41 secondi e 4 passaggi**, mentre Supermicro IPMI ha richiesto **un tempo superiore di oltre quattro volte: 2 minuti e 50 secondi e 6 passaggi**. Proiettando questo risparmio di tempo su 100 sistemi, si risparmierebbe fino a 3 ore e 35 minuti, il che significa che un amministratore impiegherebbe quasi metà della giornata lavorativa nell'utilizzo di Supermicro IPMI, rispetto a poco più di un'ora utilizzando Dell iDRAC.

Figura 3. Tempo per disabilitare le porte USB anteriori per un singolo server e tempo estrapolato per disabilitare le porte USB anteriori per 100 server.
A un numero più basso corrispondono risultati migliori. Fonte: Principled Technologies.

Informazioni su Dell OpenManage Enterprise

OpenManage Enterprise è una console per la gestione dei sistemi di tipo "uno a molti" per il data center. La console offre un'interfaccia grafica utente HTML5 moderna e viene implementata come Virtual Appliance per ambienti VMware ESXi™, Microsoft Hyper-V e KVM (Kernel-Based Virtual Machine). OpenManage Enterprise è in grado di rilevare e inventariare le reti IPV4 e IPV6 per un massimo di 8.000 dispositivi, tra cui server rack Dell, server tower Dell e server blade e chassis Dell.[12] In un recente studio PT, abbiamo rilevato che un ambiente Dell con OpenManage Enterprise e OpenManage Enterprise Modular (OME-M) può ridurre il tempo necessario per apportare modifiche alle VLAN ed evitare interventi durante gli aggiornamenti pianificati del firmware.[13]

Ulteriori informazioni su OpenManage Enterprise sono disponibili all'indirizzo https://www.dell.com/en-us/lp/dt/open-manage-enterprise

Monitoraggio, analisi e facilità di utilizzo

Gli strumenti di gestione variano notevolmente in base al modo in cui supportano gli amministratori nello svolgimento delle attività di monitoraggio e analisi, nonché altre attività di routine, come la pianificazione degli aggiornamenti. In questa sezione esaminiamo le differenze che abbiamo studiato in queste aree tra gli strumenti di gestione Dell e Supermicro. Come abbiamo rilevato indagando sulle caratteristiche di sostenibilità e sicurezza, la suite di strumenti di gestione Dell offre numerose funzionalità, di cui gli strumenti Micro non dispongono, per rendere la vita degli amministratori più semplice. La Tabella 6 mette a confronto i vantaggi di gestione offerti dagli strumenti.

Tabella 6: Riepilogo del confronto tra gli strumenti di gestione Dell e Supermicro. Fonte: Principled Technologies.

Funzione	Vantaggi principali degli strumenti di gestione Dell	Svantaggio degli strumenti di gestione Supermicro
Telemetria in streaming	**Streaming di telemetria** iDRAC9 **disponibile** per i server syslog remoti; aiuta a prevedere i guasti e a ottimizzare le prestazioni; può eseguire lo streaming delle metriche del server a strumenti di analisi come Grafana e Splunk	**Nessuno streaming di telemetria automatico**
Monitoraggio e gestione mobile	App OpenManage Mobile ricca di funzionalità per iOS e Android, che si integra con OME e iDRAC9	App Supermicro IPMIView, che **non si integra** con SSM
Monitoraggio di server e dispositivi di terze parti	OME **supporta il monitoraggio di dispositivi e server di terze parti**, incluso il supporto per i principali concorrenti	**Supporta solo i dispositivi di terze parti che utilizzano i loro agent**, i loro BMCS, le versioni precedenti delle loro apparecchiature che sono compatibili con IPMI e i dispositivi compatibili con Redfish
Monitoraggio dell'ambiente	Disponibile tramite OME e CloudIQ; OME può trasmettere i dati su server gestiti con licenza a CloudIQ per il monitoraggio su più data center	**Nessun portale basato su cloud** per aggregare i dati di monitoraggio tra i data center
Azioni basate sugli avvisi	Policy in OME che attivano azioni in base all'input di un avviso	**Nessuna azione basata su avvisi disponibile**
Deployment più semplice dei server (possibilità di importare/esportare configurazioni di sistema)	Può utilizzare iDRAC9 per **importare/esportare** tutti gli elementi di configurazione per i server, richiedendo solo **48 secondi e 5 passaggi per l'importazione e 1 minuto e 9 secondi e 7 passaggi per l'esportazione**	Può importare/esportare **solo la configurazione BMC (Baseboard Management Controller)**, che richiede una configurazione manuale significativa per ogni server
Meno tempo per modificare le impostazioni di configurazione del BIOS	Può modificare rapidamente **le impostazioni complete del BIOS direttamente da iDRAC** e pianificare l'aggiornamento e il riavvio per una finestra di manutenzione, risparmiando notevole tempo di amministrazione	**Modifiche limitate al BIOS disponibili** dal BMC, altrimenti è necessario riavviare il server; richiede più passaggi manuali e tempo di amministrazione
Viene eseguito come appliance virtuale	**Disponibile** in OME, che elimina la necessità di aggiornare il sistema operativo	**Nessuna funzionalità paragonabile**; deve essere eseguito all'interno di un sistema operativo gestito. In questo modo, gli amministratori hanno un altro componente a cui applicare patch e da aggiornare
Visualizzazione delle connessioni	**Disponibile** in iDRAC; strumento di risoluzione dei problemi che utilizza LLDP per la diagnosi di problemi di rete come il cablaggio, le porte degli switch danneggiate e altro ancora	**Nessuna informazione sulla connessione**, nessuna informazione sulla connettività fisica sulle porte degli switch upstream
Possibilità di pianificare gli aggiornamenti di firmware e driver	**Disponibile** in OME e iDRAC	Può pianificare gli aggiornamenti del BIOS e del firmware BMC, ma **non può pianificare gli aggiornamenti dei driver**

Modifica dell'elemento di configurazione del BIOS

Dell offre modifiche complete alle impostazioni di configurazione del BIOS direttamente da iDRAC con la possibilità di eseguire tali modifiche per il riavvio successivo. Supermicro offre un set limitato di impostazioni del BIOS dal suo BMC. Oltre il set limitato, una modifica alla configurazione del BIOS sui server Supermicro per una singola voce di configurazione richiede all'amministratore di riavviare il server per accedere al menu di configurazione del BIOS dalla schermata di avvio.

La Figura 4 mostra il tempo necessario per eseguire una modifica alla configurazione del BIOS su un singolo server utilizzando Dell iDRAC e Supermicro IPMI. Il processo manuale che utilizza lo **strumento Supermicro richiede 2 minuti e 6 secondi aggiuntivi** o **4,9 volte più tempo** rispetto alla configurazione del processo automatizzato in iDRAC. Se proiettiamo questi tempi su 100 server configurati in modo identico, il risparmio di tempo con iDRAC sarebbe di 3,5 ore (se i server non fossero configurati in modo identico, non rileveremo questo risparmio di tempo).

Figura 4. Tempo necessario per eseguire una modifica alla configurazione del BIOS su un singolo server e su 100 server configurati in modo identico (estrapolati).
A un numero più basso corrispondono risultati migliori. Fonte: Principled Technologies.

Informazioni su iDRAC9

I server Dell PowerEdge™ includono Integrated Dell Remote Access Controller 9 con Dell Lifecycle Controller per fornire funzioni di amministrazione dei sistemi che includono avvisi di sistema e funzionalità di gestione remota. Secondo Dell, i vantaggi principali di iDRAC9 includono:

- La possibilità di gestire migliaia di server utilizzando API e strumenti di scripting
- Supporto integrato, che offre la panoramica dell'integrità e dello stato del server, con il monitoraggio di migliaia di parametri
- Funzionalità e opzioni di protezione avanzate[14]

Per ulteriori informazioni sulle funzionalità offerte da iDRAC9, visita il sito https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Aggiornamenti automatici di driver e firmware

iDRAC

A differenza di Supermicro IPMI, Dell iDRAC consente di pianificare gli aggiornamenti automatici del firmware. Ciò significa che la configurazione degli aggiornamenti automatici in base alla pianificazione è un'attività una tantum che consente di risparmiare tempo in ogni ciclo di aggiornamento. La Figura 5 mostra l'estrapolazione del tempo necessario per programmare automaticamente gli aggiornamenti del firmware per la prima volta per 100 server utilizzando Dell iDRAC e Supermicro IPMI. Il processo manuale che utilizza lo strumento Supermicro richiede **13 minuti in più** rispetto alla configurazione del processo automatizzato in iDRAC.

Se si presuppone che un amministratore configuri una pianificazione mensile il primo sabato sera di ogni mese, un amministratore che utilizza iDRAC avrebbe un investimento una tantum di 58 secondi per server. Per 100 server, si tratta di 1 ora, 36 minuti e 40 secondi come configurazione una tantum. In confronto, un amministratore che utilizza Supermicro IPMI avrebbe un investimento di 1 ora e 50 minuti per 100 server in ogni finestra di manutenzione. Se confrontiamo il tempo per la configurazione una tantum per iDRAC e la prima di molte configurazioni per Supermicro IPMI, lo strumento di gestione Dell consente di risparmiare circa 13 minuti e 20 secondi. (vedere la Figura 5).

Tuttavia, la seconda volta e ogni volta successiva, **Dell fa risparmiare 110 minuti perché non è più necessario che l'amministratore esegua l'attività**. (vedere la Figura 6). Questo risparmio di tempo si verifica anche se i 100 server non sono configurati in modo identico. Tenere presente che questi tempi includono solo il caricamento del firmware sul BMC e non riflettono i tempi di download ed estrazione per il firmware Supermicro.

OME

Dell OME supporta **gli aggiornamenti del firmware per tutti i componenti** e gli aggiornamenti dei driver Windows. SSM supporta l'aggiornamento del BIOS e del firmware BMC, ma **non gli aggiornamenti dei driver o di altri componenti**.

Figura 5. Tempo estrapolato per aggiornare il firmware su 100 server per la prima volta. A un numero più basso corrispondono risultati migliori. Fonte: Principled Technologies.

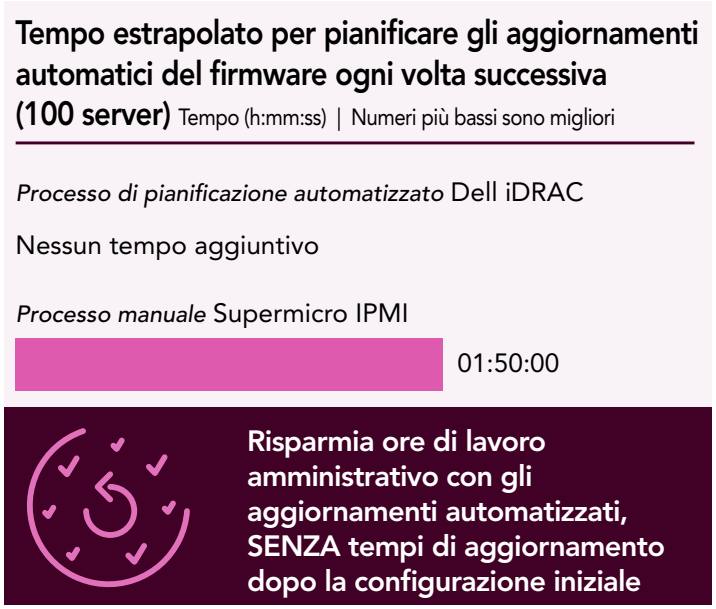

Figura 6. Tempo estrapolato per aggiornare il firmware su 100 server ogni volta successiva. A un numero più basso corrispondono risultati migliori. Fonte: Principled Technologies.

Conclusioni

La scelta di un vendor per l'acquisto di server non riguarda solo la piattaforma hardware. I responsabili delle decisioni devono anche prendere in considerazione le preoccupazioni a lungo termine, tra cui la sicurezza dei sistemi/dati, l'efficienza energetica e la facilità di gestione. Queste preoccupazioni rendono gli strumenti di gestione dei sistemi offerti da un vendor tanto importanti quanto l'hardware.

Abbiamo esaminato le caratteristiche e le funzionalità degli strumenti di gestione dei server di Dell e Supermicro, confrontando Dell iDRAC9 con Supermicro IPMI per la gestione dei server integrati e Dell OpenManage Enterprise e CloudIQ con Supermicro Server Manager per la gestione e il monitoraggio di dispositivi e console one-to-many. Abbiamo riscontrato che gli strumenti di gestione Dell forniscono funzionalità di sicurezza, sostenibilità e gestione/monitoraggio più complete rispetto ai server Supermicro. Inoltre, gli strumenti Dell hanno automatizzato più attività per semplificare la gestione dei server, con un notevole risparmio di tempo per gli amministratori rispetto alla necessità di eseguire le stesse attività manualmente con gli strumenti Supermicro.

Quando si acquista un server, i prodotti di gestione associati a un vendor sono fondamentali per proteggere i dati, supportare un ambiente più sostenibile e semplificare la manutenzione dei sistemi. I nostri test e le nostre ricerche hanno dimostrato che il portafoglio di gestione Dell per i server PowerEdge offre più funzionalità per aiutare le organizzazioni a raggiungere questi obiettivi rispetto ai prodotti di gestione Supermicro comparabili.

1. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", consultato il 15 febbraio 2024, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
2. Dell, "Using iDRAC9 RSA SecurID 2FA", consultato il 15 febbraio 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", consultato il 15 febbraio 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", consultato il 15 febbraio 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", consultato il 3 aprile 2024, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf.
7. Mark Maclean e Kyle Shannon, "Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation", consultato il 15 febbraio 2024, https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/.
8. Dell, "Security Advisories", consultato il 15 febbraio 2024, https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/.
9. Dell, "Dell CloudIQ - AIOps for Intelligent IT Infrastructure Insights", consultato il 15 febbraio 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", consultato il 17 gennaio 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.
11. Supermicro, "X13DEM User's Manual", consultato il 16 febbraio 2024, https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf.
12. Dell, "OpenManage Enterprise", consultato il 20 dicembre 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", consultato il 17 gennaio 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
14. Dell, "Integrated Dell Remote Access Controller (iDRAC)", consultato il 16 gennaio 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Leggi le basi scientifiche di questo report ▶

Principled Technologies®

Facts matter.®

Principled Technologies è un marchio registrato di Principled Technologies, Inc.
Tutti gli altri nomi di prodotto sono marchi dei rispettivi proprietari.
Per ulteriori informazioni, consultare le basi scientifiche di questo report.

Questo progetto è stato commissionato da Dell Technologies.