Stärkung der Sicherheit mit

3,5-mal mehr Sicherheitsfunktionen

einschließlich Zwei-Faktor-Authentifizierung und externem Key-Management mit iDRAC9

Optimierung der Energieeffizienz mit über

6-mal mehr Stromverbrauchs-berichten

Mit 20 Berichten in Dell OME im Vergleich zu 3 Berichten in Supermicro SSM

Steigerung der Betriebseffizienz durch Einsparung von 1 Stunde 50 Minuten Administratorzeit

pro 100 Servern

Automatische Updates mit Dell iDRAC9 im Vergleich zu keinen automatischen Updates mit Supermicro IPMI

Mehr Sicherheit, Flexibilität und Effizienz mit Servermanage-menttools von Dell

Im Vergleich zum Supermicro Managementportfolio

Wenn Sie in neue Server für Ihr Rechenzentrum investieren, entscheiden Sie sich nicht nur für Hardware, sondern auch für eine Verwaltbarkeitslösung. Wenn Ihren AdministratorInnen effiziente, funktionsreiche Tools für die Bereitstellung, Überwachung, Wartung und Sicherung Ihrer Infrastruktur zur Verfügung stehen und gleichzeitig die Energieeffizienz verbessert wird, können sie das tägliche Management problemlos bewältigen und mehr Zeit für Innovationen aufwenden, die Ihr Unternehmen voranbringen. Wenn Sie sich für den Kauf von einem Anbieter mit robusten Managementtools entscheiden, können Sie Zeit und Geld sparen.

Wir haben die Servermanagementportfolios von Dell™ und Supermicro® bewertet und drei Tools von Dell mit zwei Tools von Supermicro verglichen.

Tabelle 1: Die von uns getesteten Managementtools * Dell CloudIQ ist ein cloudbasiertes Monitoring- und Analysetool. Supermicro bietet kein gleichwertiges Tool an.
Quelle: Principled Technologies

	Dell	Supermicro
Integriertes/Remote-Servermanagement	iDRAC9 (integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
1:n-Geräteverwaltungskonsole	Dell OpenManage™ Enterprise (OME) Dell CloudIQ*	Supermicro Server Manager (SSM)

In Bezug auf Nachhaltigkeit, Sicherheit und alltägliche Managementerfahrung haben wir festgestellt, dass Dell konsistent funktionsreichere Toolsets bereitstellt, die AdministratorInnen mehr Optionen und Funktionen bieten.

Mehr und umfangreichere Funktionen zur Automatisierung und Vereinfachung Ihres Servermanagements

Ihre IT-Teams benötigen moderne, funktionsreiche Managementtools, die ihnen bei ihrer täglichen Arbeit Zeit sparen und mit den Standards für Sicherheit und Effizienz Schritt halten können. Die von uns bewerteten Dell Managementtools umfassen eine Reihe von Funktionen und Fähigkeiten, die nicht im Supermicro Managementportfolio vorhanden sind.

Nachhaltigkeit

Angesichts steigender Energiekosten und zunehmender Umweltvorschriften rücken viele Unternehmen die Nachhaltigkeit in den Mittelpunkt. Rechenzentren benötigen von Natur aus große Mengen an Strom, aber ein sorgfältiges Temperatur- und Stromverbrauchsmanagement kann es Unternehmen ermöglichen, den Stromverbrauch zu reduzieren. Dell OpenManage Enterprise verfügt über mehrere integrierte Funktionen, die ein genaues Monitoring und Management des Stromverbrauchs ermöglichen und dazu beitragen, dass Sie Ihre Nachhaltigkeitsziele erreichen können. Die Tabellen 2 und 3 enthalten die wichtigsten Vorteile dieser Funktionen, die weiter unten ausführlicher beschrieben sind.

Tabelle 2: Nachhaltigkeitsunterschiede zwischen Dell OpenManage Enterprise und SSM. Quelle: Principled Technologies

Funktion	Dell Managementtools	Supermicro Managementtools
Rechner für die Kohlendioxidemissionsnutzung und Kapazitätsplanungstool	✓	x
Analyse des CO2-Fußabdrucks	✓	x
Temperaturgesteuerte Energiemanagementrichtlinie	✓	x
Policy zum statischen Energiemanagement	✓	✓

Tabelle 3: Zusammenfassung unseres Vergleichs zwischen Dell OME und Supermicro SSM und IPMI. Quelle: Principled Technologies

Funktion	Die wichtigsten Vorteile der Dell Managementtools	Nachteil mit Supermicro Managementtools
Rechner für die Kohlendioxidemissionsnutzung und Kapazitätsplanungstool	Möglichkeit, **Treibhausgasemissionen** mit anpassbaren Werten zu schätzen, um Ihre Nachhaltigkeitsziele zu erreichen	**Keine vergleichbare Funktion**; erschwert die Einhaltung Ihrer Nachhaltigkeitsziele
Analyse des CO2-Fußabdrucks	**Verfügbar** über OpenManage Enterprise Power Manager; bietet Daten zu Kohlendioxidemissionen, die Ihnen helfen können, Nachhaltigkeitsziele zu erreichen	**Keine vergleichbare Funktion**; keine Möglichkeit, den CO2-Fußabdruck zu verfolgen, um die Einhaltung Ihrer Nachhaltigkeitsziele zu überwachen
Automatisches Energie- und Temperaturmanagement	**Statische und temperaturgesteuerte Richtlinienoptionen** mit der Möglichkeit zum Auslösen, wenn der Server einen Stromverbrauchs- oder Temperaturschwellenwert überschreitet	**Ein statischer Policy-Typ** ohne zugehörige Auslöseoptionen
Berichte zum Stromverbrauch	**Mehr als 6-mal** mehr Berichte mit **20 integrierten** Berichten mit geplanten E-Mail-Verteilungs- und Anpassungsoptionen	**2 integrierte Berichte** in SSM; 1 Bericht in Supermicro IPMI, der nicht exportiert werden kann
Energiemanagementkennzahlen	Bis zu **15-mal mehr Kennzahlen**, die detailliertere Einblicke in das Stromverbrauchsmanagement bieten	**Nur 1 Kennzahl**, die weniger Einblicke und Kontrolle über den Stromverbrauch bietet

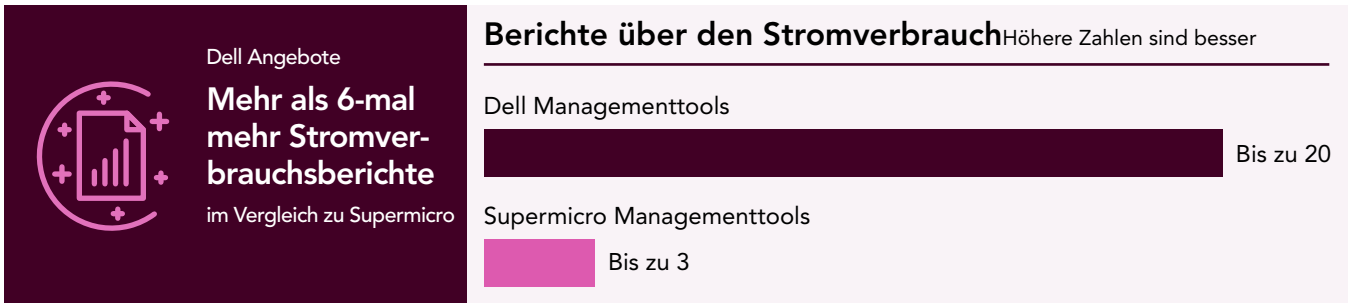

Abbildung 1: Anzahl der Stromverbrauchsberichte, die in Dell OME und Supermicro SSM verfügbar sind. Quelle: Principled Technologies

Abbildung 2: Anzahl der Energiemanagementkennzahlen, die in Dell OME und Supermicro SSM verfügbar sind. Quelle: Principled Technologies

Automatisches Energie- und Temperaturmanagement

OpenManage Enterprise Power Manager bietet ein automatisiertes Energie- und Temperaturmanagement über energie- und temperaturgesteuerte Richtlinienoptionen, mit denen AdministratorInnen Grenzwerte für den Stromverbrauch oder Temperaturschwellenwerte festlegen können, um die Kühlkosten zu senken. Im Gegensatz dazu verfügt SSM über eine einzige Policy, eine statische Begrenzung des Stromverbrauchs, die nicht automatisch ausgelöst wird, wenn ein Server den Grenzwert überschreitet, was zu höheren Energiekosten führen kann.

Unternehmen, die einen tiefen Einblick in den Stromverbrauch ihres Rechenzentrums mit Blick auf die Optimierung suchen, können von den **20 verschiedenen integrierten Stromverbrauchsberichten** profitieren, die OpenManage Enterprise Power Manager bietet. Diese Berichte sind nützlich bei der Kapazitätsplanung und dem Energiemanagement, um die Effizienz zu maximieren. Die Reportingoptionen in SSM sind viel begrenzter. AdministratorInnen können nur einen einzigen Host mit einem Servicebericht ausführen oder einen Stromverbrauchstrend auf dem Monitoringbildschirm anzeigen. Mit Supermicro IPMI können NutzerInnen ein Stromdiagramm auf Komponentenebene im BMC anzeigen. Sie können die Daten im Diagramm jedoch nicht zur Analyse exportieren und nur als Image speichern.

Mit dem OpenManage Enterprise Power Manager-Plug-in können AdministratorInnen **bis zu 15 verschiedene Kennzahlen anzeigen**, einschließlich Stromverbrauch einzelner Komponenten, Luftstrom und Komponenten-auslastung, während SSM nur den gesamten Stromverbrauch anzeigt.

Analyse der Kohlendioxidemissionen und des CO_2-Fußabdrucks

OME umfasst einen Rechner für die Kohlendioxidemissionsnutzung und ein Kapazitätsplanungstool, mit dem Sie unter anderem Ihre eigenen Kohlendioxidemissionen schätzen können. Es bietet Standardwerte für Stromkosten und Kohlendioxidemissionen für eine Einheit verbrauchter Energie, ermöglicht Ihnen aber die Anpassung dieser Werte an die Stromkosten Ihrer eigenen Region und das Verbrauchsmodell Ihres Rechenzentrums. SSM bietet keine vergleichbare Funktion, was es Unternehmen erschweren kann, den Fortschritt bei der Erreichung ihrer Nachhaltigkeitsziele zu planen und zu überwachen.

Sicherheit

Die Cyberkriminalität nimmt exponentiell zu und bedroht Unternehmen mit „Beschädigung und Zerstörung von Daten, gestohlenem Geld, Produktivitätsverlusten, Diebstahl von geistigem Eigentum, Diebstahl persönlicher und finanzieller Daten, Veruntreuung, Betrug, Unterbrechung des normalen Geschäftsablaufs nach einem Angriff, forensischen Untersuchungen, Wiederherstellung und Löschung von gehackten Daten und Systemen sowie Rufschädigung“.[1] In dieser Landschaft sollten EntscheidungsträgerInnen bei jeder Serveranschaffung die Sicherheit berücksichtigen. Wir haben festgestellt, dass Dell OpenManage Enterprise mehrere Funktionen zum Schutz Ihrer Daten enthält, die bei den Tools von Supermicro nicht vorhanden sind (siehe Tabellen 4 und 5).

Tabelle 4: Sicherheitsunterschiede zwischen Dell Managementtools und Supermicro Managementtools. Quelle: Principled Technologies

Funktion	Dell Managementtools	Supermicro Managementtools
Multi-Factor Authentication	✓	x
Externes Key-Management	✓	x
Umfangsbasierte Zugriffskontrollen	✓	x
Policy-basierte Sicherheitskonfiguration	✓	x
Cybersecurity Advisories	✓	x
Rollenbasierte Zugriffssteuerung	✓	✓
Deaktivierung des dynamischen USB-Anschlusses	✓	✓

Tabelle 5: Zusammenfassung unseres Vergleichs der Sicherheitsfunktionen von Dell und Supermicro Managementtools. Quelle: Principled Technologies

Funktion	Die wichtigsten Vorteile der Dell Managementtools	Nachteil mit Supermicro Managementtools
Multifaktor-Authentifizierung (MFA)	**Zwei-Faktor-Authentifizierung** mit iDRAC entweder **per E-Mail und mit RSA SecurID**, um unberechtigten NutzerInnen den Zugang zu sensiblen Daten zu verwehren	**Keine vergleichbare Funktion**, sodass eine Sicherheitslücke entsteht, durch die unbefugte NutzerInnen Zugang zu sensiblen Daten erhalten könnten
Externes Key-Management	**Secure Enterprise Key Manager** in iDRAC, um eine weitere Sicherheitsebene zum Schutz von Data-at-Rest auf Servern mithilfe von Laufwerksverschlüsselung und zentralem Management hinzuzufügen	**Keine vergleichbare Funktion**, sodass eine weitere Sicherheitslücke entsteht
Zugriffssteuerungen	OME bietet **sowohl** rollenbasierte Zugriffskontrolle **(Role-Based Access Control, RBAC)** als auch bereichsbasierte Zugriffskontrolle **(Scope-Based Access Control, SBAC)**, um die Gerätegruppen zu begrenzen, auf die ein Device Manager Zugriff hat	**Nur RBAC (Role-Based Access Control**) begrenzt die Fähigkeit von AdministratorInnen, den Zugriff einzuschränken.
Policy-basierte Sicherheitskonfiguration	**Policy-basierte Sicherheitskonfigurationseinstellungen** über CloudIQ, die AdministratorInnen auf Diskrepanzen hinweist	**Keine vergleichbare Funktion**, was die Maßnahmen und die Behebung von Verstößen verzögern kann
Cybersecurity Advisories	**Sicherheitsratgeber** werden über Dell CloudIQ Security gemeldet, mit Details zu Sicherheitslücken und entsprechenden Korrekturvorschlägen für schnelle Maßnahmen.	**Keine vergleichbare Funktion**, sodass Sicherheitslücken für böswillige Akteure entstehen

Multi-Faktor-Authentifizierung

Multifaktor-Authentifizierung (MFA) kann dazu beitragen, unbefugte NutzerInnen und böswillige Akteure daran zu hindern, Zugriff auf sensible Daten zu erhalten. Wir haben bestätigt, dass Dell iDRAC eine Zwei-Faktor-Authentifizierung sowohl per E-Mail als auch mit RSA SecurID ermöglicht, einer Reihe externer Multi-Faktor-Authentifizierungstechnologien, die in vielen Branchen eingesetzt werden.[2] Wir haben außerdem festgestellt, dass weder Supermicro IPMI noch SSM diese Funktion bieten, was eine Sicherheitslücke darstellt.

Key-Management

Externe Key-Management-Systems (KMS) ermöglichen es IT-Teams, einen separaten Server eines Drittanbieters für die Verwaltung der Schlüssel zu verwenden, die sie zum Sperren und Entsperren des Storage eines Servers einsetzen, was eine zusätzliche Sicherheitsebene darstellt. iDRAC umfasst Local Key Manager (LKM) für alle neuen Dell PowerEdge-Server. Einige Lizenzen bieten auch Secure Enterprise Key Manager (SEKM), der zusätzliche Sicherheit mit vollständiger Festplattenverschlüsselung und externem Key-Management ermöglicht. SEKM unterstützt das branchenübliche OASIS KMIP-Protokoll, sodass Unternehmen sich für jeden externen KMS-Anbieter entscheiden können, der diesen Standard verwendet. Supermicro bietet diese oder eine gleichwertige Sicherheitsfunktion nicht an.

Zugriffssteuerungen

Die rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC), bei der die Rolle eines/einer NutzerIn die Teile des Systems bestimmt, auf die er/sie Zugriff hat, und die Aufgaben, die er/sie dort ausführen kann, ist ein integraler Bestandteil vieler Serversicherheitsstrategien. In OpenManage Enterprise definiert RBAC die Nutzerberechtigungen für drei integrierte Rollen: Administrator, Device Manager und Viewer.[3] Außerdem bietet es eine bereichsbasierte Zugriffskontrolle (Scope-Based Access Control, SBAC), mit der AdministratorInnen die Gerätegruppen einschränken können, auf die ein Device Manager Zugriff hat.[4] Dadurch können AdministratorInnen Zugriff auf eine Teilmenge von Geräten gewähren. Supermicro bietet RBAC, aber nicht SBAC.

Qualifikationsmanagement

Die iDRAC-Kennwortrotation dient mehreren Zwecken: Sie rotiert den Zugriff auf OpenManage Enterprise gemäß der Sicherheits-Policy, mit einer monatlichen Vorgabe, arbeitet mit einem externen Kennworthandler und unterstützt CyberArk zur Verwaltung der Kennwörter.[5,6]

Mit OpenManage Enterprise können AdministratorInnen die iDRAC-Kennwortrotation verwalten, indem sie die Notwendigkeit eines statischen bekannten Administratorkontos durch ein Servicekonto ersetzen, das von OME verwaltet wird. SSM hat diese Möglichkeit nicht.

Policy-basierte Sicherheitskonfiguration

Dell bietet ein Cybersicherheitsfeature in der AIOps-Lösung „CloudIQ für PowerEdge". Diese Funktion verwendet die Konfiguration eines bereitgestellten PowerEdge-Servers und vergleicht sie mit einer sicherheitsbezogenen Konfigurations-Policy basierend auf den Best Practices von Dell. Für den Fall, dass CloudIQ eine Diskrepanz erkennt, benachrichtigt es den/die AdministratorIn und stellt Schritte zur Korrektur bereit.[7] SSM bietet keine gleichwertige Funktion, was zu Verzögerungen bei der Erkennung von Sicherheitsverletzungen führen kann.

Cybersecurity Advisories

Sicherheitsratgeber informieren die Öffentlichkeit über Sicherheitsprobleme. Laut Dell enthält die Seite „Dell Sicherheitsratgeber" in CloudIQ eine vollständige Liste der anwendbaren Sicherheitsratgeber sowie deren Auswirkungen, die Anzahl der betroffenen Systeme und das Veröffentlichungsdatum.[8] Dell CloudIQ bietet Sicherheitsberatungsberichte mit Details zu Sicherheitslücken und Korrekturvorschlägen. SSM bietet keine ähnliche Funktion, was die Systeme anfällig machen kann.

Über Dell CloudIQ

Dell CloudIQ ist ein cloudbasiertes AIOps-Tool, das „proaktives Monitoring, maschinelles Lernen und vorausschauende Analysen" für eine große Anzahl von Dell Produkten und Services bietet, darunter Server, Storage, Data Protection Appliances und hyperkonvergente Infrastruktur.[9] In einer Studie von Principled Technologies aus dem Jahr 2022 haben wir festgestellt, dass CloudIQ vernachlässigbare Auswirkungen auf die Netzwerkbandbreite hatte und es uns gleichzeitig ermöglichte, Telemetrie, Integritätsstatus, Warnmeldungen und Bestandsaufnahme über eine einzige Konsole zu überwachen.[10]

Weitere Informationen zu CloudIQ finden Sie unter https://www.dell.com/en-us/dt/solutions/cloudiq.htm.

Deaktivierung des dynamischen USB-Anschlusses

Durch das Deaktivieren und Aktivieren von USB-Anschlüssen erhalten AdministratorInnen die Kontrolle über den Zugriff auf den Server über einen USB-Anschluss und vermeiden so die böswillige Nutzung und das Risiko der Installation verbotener Anwendungen oder Viren.

Dell iDRAC bietet eine unabhängige, dynamische Deaktivierung des USB-Anschlusses ohne Ausfallzeiten. Während Supermicro eine dynamische Deaktivierung von USB auf der Vorderseite (und USB auf der Rückseite) im BIOS bietet, ist für die Aktivierung der Supermicro Datacenter Management Suite per Node-Lizenzschlüssel erforderlich. Die IT kann ihn auslösen, indem sie den System-Lockdown-Befehl implementiert, der entweder vom BMC oder von der Supermicro IPMI-Konsole ausgeführt werden kann, aber dies ist nicht unabhängig von Systemsperrmodus.[11]

Wie Abbildung 3 zeigt, war das Deaktivieren der Ports mit Dell iDRAC ein einfacher Prozess, **der nur 41 Sekunden und 4 Schritte benötigte**, während der Supermicro IPMI **mehr als viermal so lange brauchte, 2 Minuten und 50 Sekunden und 6 Schritte**. Wenn man diese Zeitersparnis auf 100 Systeme hochrechnet, würde die Zeitersparnis auf 3 Stunden und 35 Minuten ansteigen, was bedeutet, dass ein(e) AdministratorIn fast einen halben Arbeitstag mit Supermicro IPMI verbringen würde, statt etwas mehr als eine Stunde mit Dell iDRAC.

Abbildung 3: Zeit zum Deaktivieren der vorderen USB-Anschlüsse für einen einzelnen Server und hochgerechnete Zeit zum Deaktivieren der vorderen USB-Anschlüsse für 100 Server. Je niedriger, desto besser. Quelle: Principled Technologies

Über Dell OpenManage Enterprise

OpenManage Enterprise ist eine 1-zu-n-Systemverwaltungskonsole für das Rechenzentrum. Die Konsole bietet eine moderne grafische HTML5-Benutzeroberfläche und wird als virtuelle Appliance für VMware ESXi™-, Microsoft Hyper-V- und KVM-Umgebungen (kernelbasierte virtuelle Maschine) bereitgestellt. OpenManage Enterprise kann IPV4- und IPV6-Netzwerke für bis zu 8.000 Geräte ermitteln und inventarisieren, einschließlich Dell Rack-Server, Dell Tower-Server sowie Dell Blades und Gehäuse.[12] In einer kürzlich durchgeführten PT-Studie haben wir festgestellt, dass eine Dell Umgebung mit OpenManage Enterprise und OpenManage Enterprise Modular (OME-M) Zeit bei Änderungen an VLANs einsparen und Interventionen während geplanter Firmwareupdates vermeiden kann.[13]

Weitere Informationen zu OpenManage Enterprise finden Sie unter
https://www.dell.com/en-us/lp/dt/open-manage-enterprise

Monitoring, Analysen und Benutzerfreundlichkeit

Verwaltungstools unterscheiden sich stark in der Art und Weise, wie sie AdministratorInnen unterstützen, Monitoring- und Analyseaktivitäten sowie andere Routineaufgaben wie die Planung von Updates durchführen. In diesem Abschnitt sehen wir uns die Unterschiede in diesen Bereichen zwischen den von uns untersuchten Managementtools von Dell und Supermicro an. Wie wir bei der Untersuchung der Nachhaltigkeits- und Sicherheitsfunktionen festgestellt haben, bietet die Dell Suite von Managementtools zahlreiche Funktionen, die das Leben von AdministratorInnen erleichtern – Funktionen, die die Supermicro Tools nicht bieten. Tabelle 6 zeigt die Managementvorteile der Tools in Vergleich.

Tabelle 6: Zusammenfassung unseres Vergleichs der Managementtools von Dell und Supermicro. Quelle: Principled Technologies

Funktion	Die wichtigsten Vorteile der Dell Managementtools	Nachteil mit Supermicro Managementtools
Telemetrie-Streaming	iDRAC9-**Telemetriestreaming**, das für Remote-Syslog-Server **verfügbar ist**; hilft bei der Vorhersage von Ausfällen und der Optimierung der Performance und kann Serverkennzahlen an Analysetools wie Grafana und Splunk streamen.	**Kein automatisches Telemetriestreaming**
Mobiles Monitoring und Management	Funktionsreiche OpenManage Mobile-App für iOS und Android, die in OME und iDRAC9 integriert werden kann	Supermicro IPMIView-App, die **nicht in SSM integriert werden kann**
Monitoring von Geräten und Servern von Drittanbietern	OME **unterstützt das Monitoring von Drittanbietergeräten** und **-servern**, einschließlich Unterstützung seiner wichtigsten Mitbewerber.	**Unterstützt nur Geräte von Drittanbietern, die ihre Agenten**, ihre BMCs, frühere Versionen ihrer Geräte, die IPMI-fähig sind, und Redfish-fähige Geräte verwenden.
Bestandsüberwachung	Verfügbar über OME und CloudIQ; OME kann Daten auf lizenzierten gemanagten Servern zur Überwachung über mehrere Rechenzentren hinweg an CloudIQ übertragen	**Kein Cloud-basiertes Portal** für die Aggregation von Überwachungsdaten über Rechenzentren hinweg
Warnmeldungsbasierte Aktionen	Policies in OME, die Aktionen basierend auf der Eingabe einer Warnmeldung auslösen	**Keine warnmeldungsbasierten Aktionen verfügbar**
Einfachere Serverbereitstellung (Möglichkeit zum Importieren/Exportieren von Systemkonfigurationen)	Kann iDRAC9 verwenden, um alle Konfigurationselemente für Server zu **importieren/exportieren**, was nur **48 Sekunden und 5 Schritte für den Import sowie 1 Minute und 9 Sekunden und 7 Schritte für den Export erfordert.**	Kann **nur die BMC-Konfiguration (Baseboard Management Controller)** importieren/exportieren, was eine erhebliche manuelle Konfiguration für jeden Server erfordert.
Weniger Zeit für das Ändern der BIOS-Konfigurationseinstellungen	Kann die **vollständigen BIOS-Einstellungen schnell direkt über iDRAC** ändern und das Update und den Neustart für ein Wartungsfenster bereitstellen, was AdministratorInnen viel Zeit spart.	**Begrenzte BIOS-Änderungen sind über den BMC verfügbar**, andernfalls ist ein Serverneustart erforderlich; erfordert mehr manuelle Schritte und Administratorzeit.
Läuft als virtuelle Appliance	**Verfügbar** in OME, sodass das Betriebssystem nicht aktualisiert werden muss	Es darf **keine vergleichbare Funktion** in einem verwalteten Betriebssystem ausgeführt werden. Dadurch erhalten AdministratorInnen eine weitere Komponente zum Patchen und Aktualisieren.
Verbindungsanzeige	**Verfügbar** in iDRAC; Troubleshooting-Tool mit LLDP zur Diagnose von Netzwerkproblemen wie Verkabelung, fehlerhafte Switchports und mehr	**Keine Verbindungsansicht**, keine physischen Konnektivitätsinformationen zu den Upstream-Switchports
Möglichkeit zum Planen von Firmware- und Treiberupdates	**Verfügbar** in OME und iDRAC	Kann BIOS- und BMC-Firmwareupdates planen, aber **keine Treiberupdates**

Änderung des BIOS-Konfigurationselements

Dell bietet vollständige Änderungen der BIOS-Konfigurationseinstellungen direkt über iDRAC mit der Möglichkeit, diese Änderungen für den nächsten Neustart zu speichern. Supermicro bietet einen begrenzten Satz von BIOS-Einstellungen über den BMC. Abgesehen von dem begrenzten Satz erfordert eine Änderung der BIOS-Konfiguration auf Supermicro Servern für ein einzelnes Konfigurationselement, dass der/die AdministratorIn den Server neu startet, um vom Startbildschirm aus auf das BIOS-Konfigurationsmenü zuzugreifen.

Abbildung 4 zeigt die Zeit für die Durchführung einer BIOS-Konfigurationsänderung auf einem einzelnen Server mit Dell iDRAC und Supermicro IPMI. Der manuelle Prozess mit dem **Supermicro Tool dauert 2 Minuten und 6 Sekunden** oder **4,9-mal länger** als das Einrichten des automatisierten Prozesses in iDRAC. Wenn wir diese Zeiten auf 100 Server hochrechnen, die identisch konfiguriert sind, beträgt die Zeitersparnis mit iDRAC 3,5 Stunden. (Wären die Server nicht identisch konfiguriert, würden wir diese Zeiteinsparungen nicht sehen.)

Abbildung 4: Zeit für die Durchführung einer BIOS-Konfigurationsänderung auf einem einzigen Server und 100 identisch konfigurierten Servern (extrapoliert). Je niedriger, desto besser. Quelle: Principled Technologies

Informationen über iDRAC9

Dell PowerEdge™-Server umfassen den Integrated Dell Remote Access Controller 9 mit Dell Lifecycle Controller, um Systemmanagementfunktionen bereitzustellen, die Systemwarnmeldungen und Remotemanagementfunktionen umfassen. Laut Dell bietet iDRAC9 u. a. die folgenden wichtigen Vorteile:

- Die Möglichkeit, Tausende von Servern mithilfe von APIs und Scripting-Tools zu managen
- Integrierter Support, der eine Ansicht der Serverintegrität und des Serverstatus bietet und Tausende von Parametern überwacht
- Robuste Sicherheitsfunktionen und -optionen[14]

Weitere Informationen zu den Funktionen von iDRAC9 finden Sie unter https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Automatische Firmware- und Treiberupdates

iDRAC

Im Gegensatz zu Supermicro IPMI können Sie mit Dell iDRAC automatische Firmwareupdates planen. Das bedeutet, dass die Konfiguration automatischer Updates nach einem Zeitplan eine einmalige Aufgabe ist, die bei jedem Aktualisierungszyklus Zeit spart. Abbildung 5 zeigt die extrapolierte Zeit für die erstmalige Planung automatischer Firmwareupdates für 100 Server mit Dell iDRAC und Supermicro IPMI. Der manuelle Prozess mit dem Supermicro Tool dauert **13 Minuten mehr** als das Einrichten des automatisierten Prozesses in iDRAC.

Wenn wir davon ausgehen, dass ein(e) AdministratorIn einen monatlichen Zeitplan am ersten Samstagabend jedes Monats einrichtet, hätte ein(e) AdministratorIn, der/die iDRAC verwendet, einen einmaligen Zeitaufwand von 58 Sekunden pro Server. Bei 100 Servern sind das 1 Stunde, 36 Minuten, 40 Sekunden als einmalige Einrichtung. Im Vergleich dazu hätte ein(e) AdministratorIn, der/die Supermicro IPMI verwendet, eine Investition von 1 Stunde und 50 Minuten für 100 Server in jedem Wartungsfenster. Wenn wir die einmalige Einrichtung für iDRAC und die erste von vielen Einrichtungszeiten für Supermicro IPMI vergleichen, spart das Dell Managementtool etwa 13 Minuten und 20 Sekunden. (Siehe Abbildung 5.)

Extrapolierte Zeit für die Planung automatischer Firmwareupdates beim ersten Mal (100 Server) (h:mm:ss) | Niedrigere Zahlen sind besser

Abbildung 5: Hochgerechnete Zeit für das Update der Firmware auf 100 Servern beim ersten Mal. Je niedriger, desto besser. Quelle: Principled Technologies

Beim zweiten Mal und bei jedem weiteren Mal **spart Dell 110 Minuten ein, da der/die AdministratorIn die Aufgabe nicht mehr durchführen muss**. (Siehe Abbildung 6.) Diese Zeitersparnis gilt auch, wenn die 100 Server nicht identisch konfiguriert sind. Beachten Sie, dass diese Zeiten nur das Hochladen der Firmware auf den BMC umfassen und nicht die Download- und Extraktionszeiten für die Supermicro Firmware widerspiegeln.

Extrapolierte Zeit für die Planung automatischer Firmwareupdates bei jedem folgenden Mal (100 Server) Zeit (h:mm:ss) | Niedrigere Zahlen sind besser

Abbildung 6: Hochgerechnete Zeit für das Update der Firmware auf 100 Servern bei jedem weiteren Mal. Je niedriger, desto besser. Quelle: Principled Technologies

OME

Dell OME unterstützt **Firmwareupdates für alle Komponenten** und Windows-Treiberupdates. SSM unterstützt BIOS- und BMC-Firmwareupdates, **jedoch keine Treiberupdates oder das Update anderer Komponenten**.

Entscheidung

Bei der Wahl eines Anbieters für den Kauf von Servern geht es um mehr als nur um die Hardwareplattform. EntscheidungsträgerInnen müssen auch längerfristigere Bedenken berücksichtigen, darunter System-/Datensicherheit, Energieeffizienz und einfaches Management. Diese Bedenken machen die Systemmanagementtools, die ein Anbieter anbietet, genauso wichtig wie die Hardware.

Wir haben die Funktionen und Fähigkeiten der Servermanagementtools von Dell und Supermicro untersucht und Dell iDRAC9 mit Supermicro IPMI für das integrierte Servermanagement und Dell OpenManage Enterprise und CloudIQ mit Supermicro Server Manager für das 1:n-Geräte- und Konsolenmanagement und -Monitoring verglichen. Wir haben festgestellt, dass die Managementtools von Dell umfassendere Sicherheits-, Nachhaltigkeits- und Management-/Monitoringfunktionen bieten als Supermicro Server. Darüber hinaus automatisierten Dell Tools mehr Aufgaben, um das Servermanagement zu vereinfachen, was zu erheblichen Zeitersparnissen für AdministratorInnen führte, die dieselben Aufgaben mit den Supermicro Tools manuell erledigen mussten.

Beim Kauf eines Servers sind die zugehörigen Managementprodukte eines Anbieters entscheidend, um Daten zu schützen, eine nachhaltigere Umgebung zu unterstützen und die Wartung der Systeme zu vereinfachen. Unsere Tests und Untersuchungen haben gezeigt, dass das Dell Managementportfolio für PowerEdge-Server mehr Funktionen bietet, um Unternehmen dabei zu unterstützen, diese Ziele zu erreichen, als die vergleichbaren Managementprodukte von Supermicro.

---

1. Steve Morgan, „Cybercrime to Cost the World $10,5 Billion Annual by 2025“, abgerufen am 15. Februar 2024, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
2. Dell, „Using iDRAC9 RSA SecurID 2FA“, abgerufen am 15. Februar 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“, abgerufen am 15. Februar 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“, abgerufen am 15. Februar 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“, abgerufen am 3. April 2024, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf.
7. Mark Maclean und Kyle Shannon, „Dell CloudIQ Cybersecurity for PowerEdge: The Benefits of Automation“, abgerufen am 15. Februar 2024, https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/.
8. Dell, „Security Advisories“, abgerufen am 15. Februar 2024, https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/.
9. Dell, „Dell CloudIQ – AIOps for Intelligent IT Infrastructure Insights“, abgerufen am 15. Februar 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“, abgerufen am 17. Januar 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.
11. Supermicro, „X13DEM User's Manual“, abgerufen am 16. Februar 2024, https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf.
12. Dell, „OpenManage Enterprise“, abgerufen am 20. Dezember 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 Easy for Administrators“, abgerufen am 17. Januar 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
14. „Integrated Dell Remote Access Controller (iDRAC)“, abgerufen am 16. Januar 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Dieses Projekt wurde in Auftrag gegeben von Dell Technologies.

Lesen Sie den wissenschaftlichen Hintergrund dieses Berichts ▶

Principled Technologies®

Facts matter.®