Mehr Sicherheit durch eine Systemsperre in

95 % weniger Zeit und mit 83 % weniger Schritten

mit iDRAC9 im Vergleich zu iLO 6

Optimierung der Energieeffizienz mit

4-mal mehr Energiemanage-mentkennzahlen

und 25 anpassbaren Berichten in OME im Vergleich zu 0 Berichten in OneView

Erweiterung der Remotefunktionalität mit

16-mal mehr Remote-BIOS-Funktionen,

51 in iDRAC9 im Vergleich zu 3 in iLO 6

Mehr Sicherheit, Nachhaltigkeit und Administratoreffizienz mit dem Servermanagementportfolio von Dell

als bei vergleichbaren Servermanagementtools von HPE

Bei der Auswahl von Servern sollten technische Daten nicht die einzige Überlegung auf Ihrer Liste sein. Wenn Sie sich für einen Anbieter mit Managementtools entscheiden, die den praktischen Zeitaufwand für AdministratorInnen reduzieren, die Sicherheit erhöhen und eine Nachhaltigkeitsplanung bieten, können Sie mithilfe Ihrer Infrastruktur eine Reihe von Geschäftszielen erreichen. Wir haben im Rechenzentrum von Principled Technologies die Funktionen der Servermanagementportfolios von Dell und HPE verglichen, um festzustellen, was sie AdministratorInnen zu bieten haben. Wir haben verglichen:

Tabelle 1: Die von uns getesteten Managementtools

	Dell	HPE
Integriertes/ Remoteservermanagement	Dell Technologies Integrated Dell Remote Access Controller (iDRAC9)	HPE Integrated Lights-Out (iLO 6)
1:n-Gerätemanagementkonsole	Dell Technologies OpenManage™ Enterprise (OME)	HPE OneView

Wir haben uns außerdem Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) und einige der Funktionen und Vorteile dieses cloudbasierten Monitoringtools für das Servermanagement angesehen.

Bei allen von uns getesteten Funktionen und Anwendungsfällen boten die Tools aus dem Dell Managementportfolio robustere Sicherheitsfunktionen und ein breiteres Angebot an Nachhaltigkeitstools. Sie ermöglichten außerdem eine feiner abgestimmte Kontrolle und mehr Flexibilität für AdministratorInnen sowie weniger Zeit- und Arbeitsaufwand für die Durchführung gängiger Aufgaben.

Stärkere End-to-End-Sicherheit

Cyberangriffe, bei denen böswillige AkteurInnen Systeme infiltrieren, um private Daten abzurufen und auszunutzen, nehmen zu. In einem Bericht aus dem Jahr 2023 wurde festgestellt, dass „83 % der Unternehmen im Jahr 2022 mehr als eine Datenschutzverletzung erlebt haben“[1], was zeigt, dass Cybersicherheit ein globales Anliegen ist. Die Auswahl von Hardware mit End-to-End-Sicherheitsfunktionen kann dazu beitragen, die Daten Ihres Unternehmens vor diesen kostspieligen Angriffen zu schützen. Dell bietet robuste Sicherheitsfunktionen, die sowohl über iDRAC9 in den Server als auch in die übergreifende Konsole und Cloud-Managementsoftware integriert sind, um die Sicherheit Ihres Unternehmens zu verstärken.

Integrierte Sicherheit

Jeder Dell PowerEdge™-Server verfügt über Sicherheitsfunktionen, die über iDRAC9 integriert sind und verhindern, dass böswillige AkteurInnen Zugriff auf Daten erhalten. Zwei dieser wichtigen Funktionen sind:

- **Aktivierung/Deaktivierung des dynamischen USB-Anschlusses**: Durch das Deaktivieren und Aktivieren von USB-Anschlüssen können AdministratorInnen den Zugriff auf den Server über einen USB-Anschluss steuern. „Dynamisch“ bezieht sich auf die Möglichkeit, diese USB-Anschlüsse zu aktivieren und zu deaktivieren, ohne den Server oder das Betriebssystem neu starten zu müssen. Solange AdministratorInnen keinen Zugriff gewähren, kann niemand einen USB-Stick oder eine Tastatur anschließen, um Konfigurationseinstellungen des Systems, des Betriebssystems oder des BIOS zu ändern.
- **Dynamische Systemsperre**: Die Systemsperre verhindert, dass unbeabsichtigte oder bösartige Aktivitäten zu Änderungen der System-BIOS-, iDRAC- und Firmwareeinstellungen führen. „Dynamisch“ bezieht sich auf die Möglichkeit, diese Funktionen einmal einzurichten und dann nach Bedarf zu implementieren. (Hinweis: Diese Funktion ist mit einer iDRAC9 Enterprise- oder Datacenter-Lizenz verfügbar.)

In Abbildung 1 sind die Ergebnisse unseres praktischen Vergleichs beim dynamischen Deaktivieren von USB-Anschlüssen mit iDRAC9 und iLO 6 gezeigt.

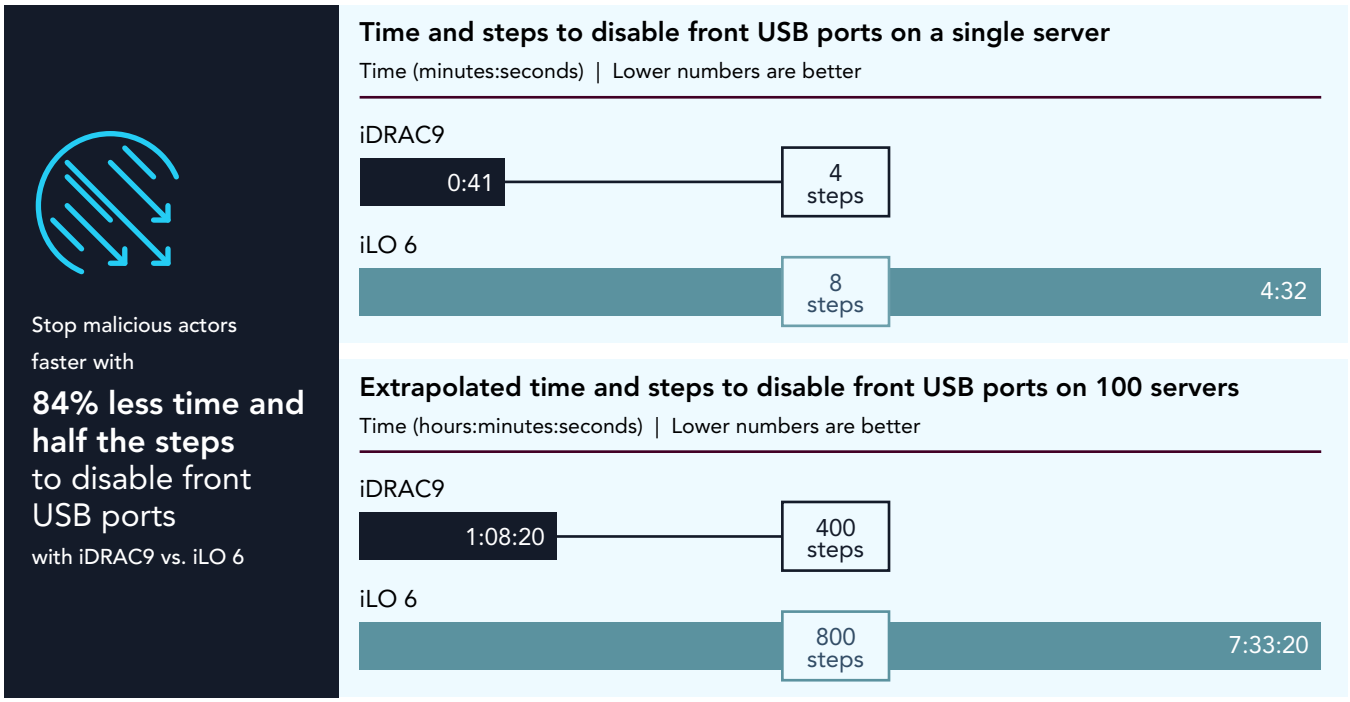

Abbildung 1: Zeit zum Deaktivieren der vorderen USB-Anschlüsse für einen einzelnen Server und hochgerechnete Zeit zum Deaktivieren der vorderen USB-Anschlüsse für 100 Server. Weniger Zeit und weniger Schritte sind besser. Quelle: Principled Technologies.

Hinweis: In den Diagrammen in diesem Bericht werden unterschiedliche Skalierungen verwendet, um eine konsistente Größe sicherzustellen. Achten Sie beim Vergleich auf den Datenbereich jedes Diagramms.

Bei iDRAC9 haben wir festgestellt, dass AdministratorInnen die vorderen USB-Anschlüsse auf einem einzigen Server in nur 41 Sekunden mit 4 Schritten deaktivieren konnten. Im Vergleich dazu dauerte derselbe Prozess mit iLO 6 4 Minuten und 32 Sekunden und umfasste 8 Schritte pro Server. Das bedeutet, dass **iDRAC9 84 % weniger Zeit und die Hälfte der Schritte benötigt, um die vorderen USB-Anschlüsse zu deaktivieren**.[2] Wenn Sie in Betracht ziehen, diese Schritte in einem Rechenzentrum durchzuführen, summiert sich die Zeitersparnis. Bei einer Bereitstellung mit 100 Servern können AdministratorInnen USB-Anschlüsse mit iDRAC9 in 6 Stunden weniger Zeit deaktivieren als mit iLO 6.

Diese Funktionen sind mit iDRAC9 nicht nur einfacher und schneller zugänglich als mit iLO 6, sondern AdministratorInnen können mit iDRAC9 auch **Server in der Produktion halten**, während sie diese Funktionen aktivieren oder deaktivieren, **und so Ausfallzeiten vermeiden**. Bei iLO 6 sind jedes Mal sowohl eine Änderung der BIOS-Konfiguration als auch ein Neustart erforderlich.

Es ist von entscheidender Bedeutung, ein System schnell entsperren zu können, um Updates vorzunehmen, und es dann schnell wieder zu sperren. Wie in Abbildung 2 gezeigt, **konnten AdministratorInnen die Systemsperre eines Servers mit iDRAC9 in 95 % weniger Zeit und mit 83 % weniger Schritten** als mit iLO 6 abschließen, bei dem der Vorgang pro Server mehr als 5 Minuten dauerte und 12 Schritte benötigte.

Wenn Sie dies auf ein Rechenzentrum mit 100 Servern hochrechnen, könnten AdministratorInnen Systeme mit iDRAC9 in etwas mehr als einer halben Stunde sperren, während das Sperren von 100 Servern mit iLO 6 mehr als einen ganzen Arbeitstag (fast 9 Stunden) dauern würde. Das könnte für AngreiferInnen mehr als genug Zeit sein, um Zugriff auf Daten zu erhalten. Darüber sind bei Verwendung der iLO 6-Lösung für die Systemsperre Serverausfallzeiten erforderlich, während das bei der iDRAC9-Lösung nicht der Fall ist. Die iDRAC9-Sperrfunktion ist viel schneller und einfacher zu verwenden als die iLO 6-Sperrfunktion.

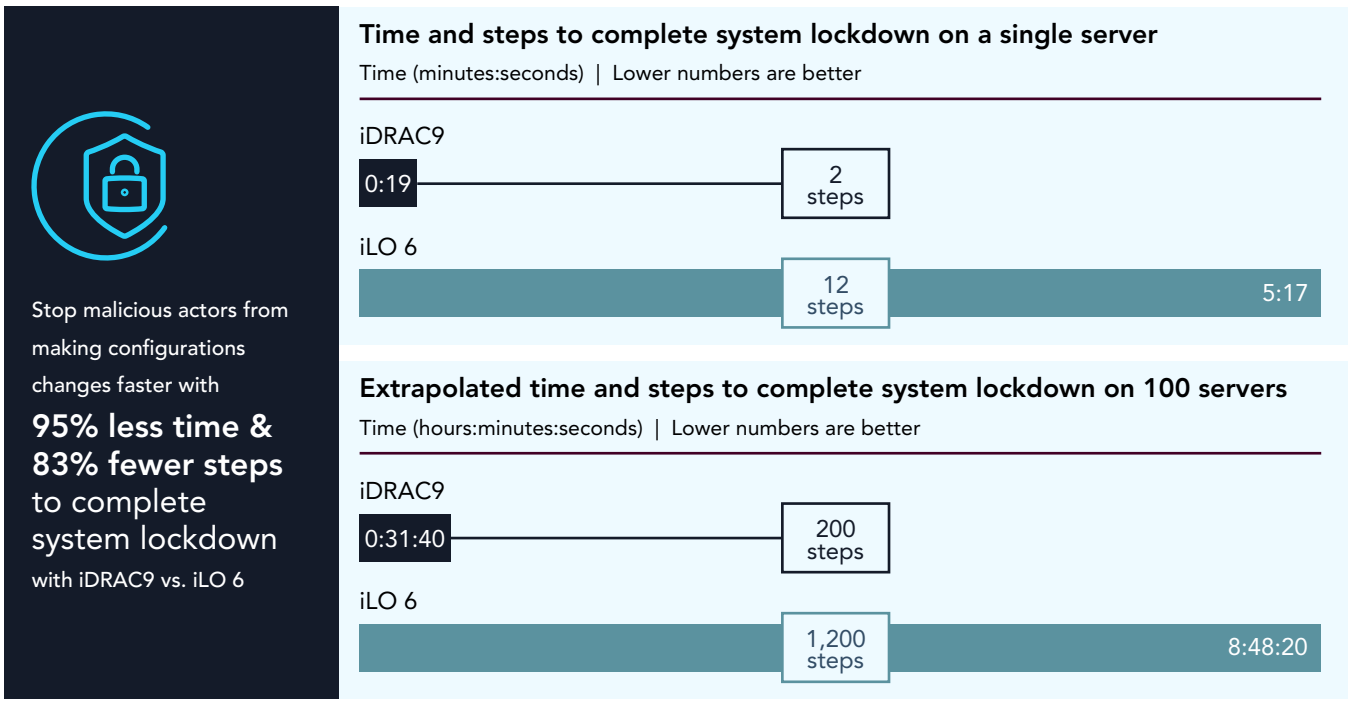

Abbildung 2: Zeit bis zum Abschluss der Systemsperre für einen einzelnen Server und hochgerechnete Zeit zum Durchführen der Systemsperre für 100 Server. Weniger Zeit und weniger Schritte sind besser. Quelle: Principled Technologies.

Sicherheit durch ein einfacheres Zugangsdatenmanagement in OME

OME bietet AdministratorInnen eine einfachere Möglichkeit, die iDRAC9-Kennwortrotation zu managen. Statt ein statisches, bekanntes Administratorkonto zu benötigen, managt OME ein Servicekonto, bei dem Kunden die erforderliche Kennwortrotationsrichtlinie auswählen, bei der das Kennwort nie offengelegt wird. **OneView bietet diese Funktion nicht**. Wir haben in unserem Rechenzentrum bestätigt, dass mit iDRAC9 gemanagte Server in das OME-Konto integriert sind und vollständige Administratorrechte für ein einfacheres Zugangsdatenmanagement bieten.

Unterstützung beim Erreichen Ihrer Nachhaltigkeitsziele

In Rechenzentren bestehen erhebliche Strom- und Kühlungsanforderungen, aber das Temperatur- und Energiemanagement kann AdministratorInnen dabei unterstützen, die Rechenzentrumskosten zu optimieren und Nachhaltigkeitsziele zu erreichen. Gleichzeitig erhalten Workloads die Ressourcen, die sie für eine optimale Performance benötigen. OME verfügt über mehrere integrierte Funktionen, die ein genaues Monitoring und Management des Stromverbrauchs ermöglichen und dazu beitragen, dass Sie Ihre Nachhaltigkeitsziele erreichen können. Tabelle 2 und 3 enthalten die wichtigsten Vorteile dieser Funktionen, die weiter unten ausführlicher beschrieben sind.

Tabelle 2: Unterschiede in Bezug auf Nachhaltigkeit zwischen OME und OneView. Quelle: Principled Technologies.

Funktion	OME	OneView
Rechner für die Kohlendioxidemissionsnutzung und Kapazitätsplanungstool	✓	x
Richtlinie für das temperaturgesteuerte Energiemanagement	✓	x
Richtlinie für das statische Energiemanagement	✓	x
Power Manager-Dashboard	✓	x
Energiemanagementberichte mit geplanter E-Mail-Verteilung	✓	x

Tabelle 3: Zusammenfassung unserer Nachhaltigkeitsmerkmale für den Vergleich zwischen OME und OneView. Quelle: Principled Technologies.

Funktion	Wichtige Vorteile der Dell Managementtools	Nachteile der HPE-Managementtools
Rechner für die Kohlendioxidemissionsnutzung und Kapazitätsplanungstool	Möglichkeit, **Treibhausgasemissionen** mit anpassbaren Werten zu schätzen, um Nachhaltigkeitsziele zu erreichen	**Keine vergleichbare Funktion**, wodurch die Planung von Nachhaltigkeitszielen erschwert wird
Automatisiertes Energie- und Temperaturmanagement	**Statische und temperaturgesteuerte Richtlinienoptionen** mit der Möglichkeit zum Auslösen, wenn der Server einen Stromverbrauchs- oder Temperaturschwellenwert überschreitet	**Keine vergleichbaren Funktionen** für ein automatisiertes Energiemanagement
Dashboard und Berichte zum Stromverbrauch	**Schneller Zugriff** auf Power Manager-Daten über das OME Power Manager-Plug-in-Dashboard; **25 verschiedene standardmäßige und/oder anpassbare Berichte** im OME Power Manager-Plug-in, die schnell die wichtigsten Systeme mit dem höchsten Energieverbrauch und Verursacher von Energieverstößen sowie nicht ausgelastete Racks und inaktive Server identifizieren	**Kein Power Manager-Dashboard** und **keine Energiemanagementberichte** in OneView
Energiemanagementkennzahlen	Bis zu **5-mal mehr Kennzahlen**, d. h. insgesamt 15 Kennzahlen, die detailliertere Einblicke in das Stromverbrauchsmanagement bieten	**Nur 3 Kennzahlen**, die weniger Einblicke und Kontrolle über den Stromverbrauch bieten

Analyse der Kohlendioxidemissionen und des CO_2-Fußabdrucks

Eine der **in OME integrierten Funktionen ist ein Tool für die Berechnung der Kohlendioxidemissionsnutzung und die Kapazitätsplanung**. Mit diesem Tool können Unternehmen ihre Treibhausgasemissionen schätzen und Standardwerte für Stromkosten und Kohlendioxidemissionen pro verbrauchter Energieeinheit bereitstellen. Diese Funktion ermöglicht außerdem eine Anpassung, sodass Unternehmen Werte für die Stromkosten und Kohlendioxidemissionen ihrer eigenen Region für jede Stromeinheit für Daten nutzen können, die für das Nutzungsmodell ihres Rechenzentrums spezifisch sind. **OneView verfügt nicht über eine vergleichbare Funktion**, was Unternehmen eine auf Nachhaltigkeit ausgelegte Planung erschwert.

Automatisiertes Energie- und Temperaturmanagement

OME Power Manager bietet ein automatisiertes Energie- und Temperaturmanagement durch energie- und temperaturgesteuerte Richtlinienoptionen, mit denen AdministratorInnen Grenzwerte für den Stromverbrauch oder Temperaturschwellenwerte festlegen können, um die Kühlkosten zu senken. Im Gegensatz dazu **bietet OneView keine automatisierte Energie- und Temperaturmanagementfunktion**. Da AdministratorInnen keine Temperaturgrenzen festlegen können, könnten die Kühlkosten aufgrund fehlender automatisierter Kontrollen steigen.

Die Optimierung des Stromverbrauchs ist eine wichtige Strategie, um Nachhaltigkeitsziele zu erreichen. Das OME Power Manager-Plug-in bietet **25 standardmäßige und/oder anpassbare Power Manager-bezogene Berichte** (17 für Power Manager-Geräte und 8 weitere für Power Manager-Gruppen), mit denen AdministratorInnen die Kapazitätsplanung optimieren und den Stromverbrauch managen können, um die Effizienz zu maximieren. **OneView bietet keine ähnlichen Energiemanagementberichte** (siehe Abbildung 3).

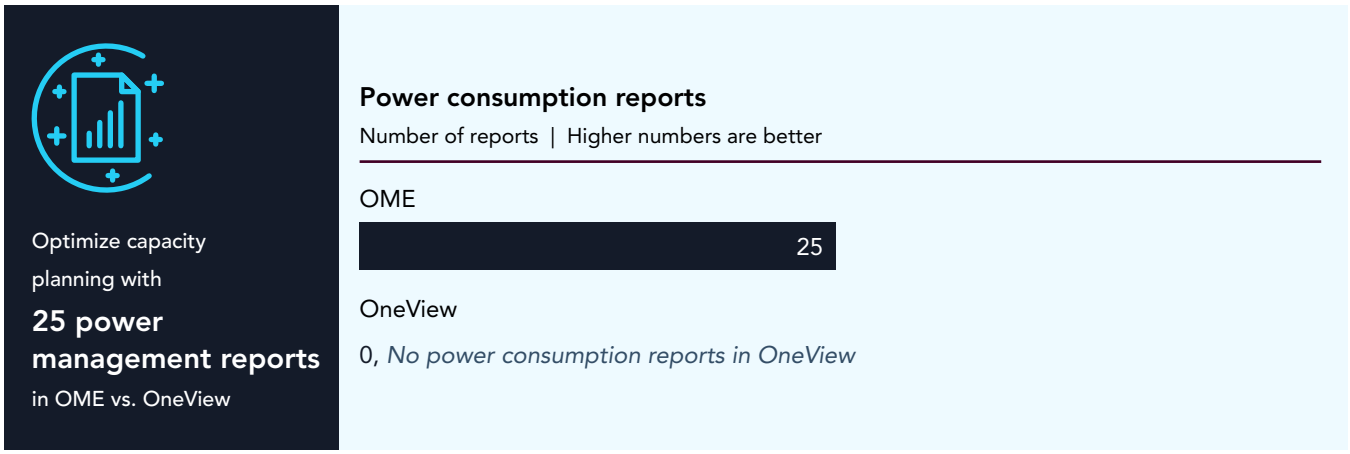

Abbildung 3: Vergleich der Anzahl der Energiemanagementberichte, die in OME und OneView verfügbar sind. Mehr Berichte sind besser. Quelle: Principled Technologies.

Um das Energiemanagement weiter zu optimieren, können AdministratorInnen mit dem OME Power Manager-Plug-in bis zu 4-mal mehr Kennzahlen im Vergleich zu OneView anzeigen (siehe Abbildung 4). OME bietet 15 Kennzahlen, einschließlich Stromverbrauch durch **einzelne Komponenten, virtuelle Maschinen, Luftstrom und Komponentenauslastung**, während OneView nur 3 Kennzahlen bereitstellt.

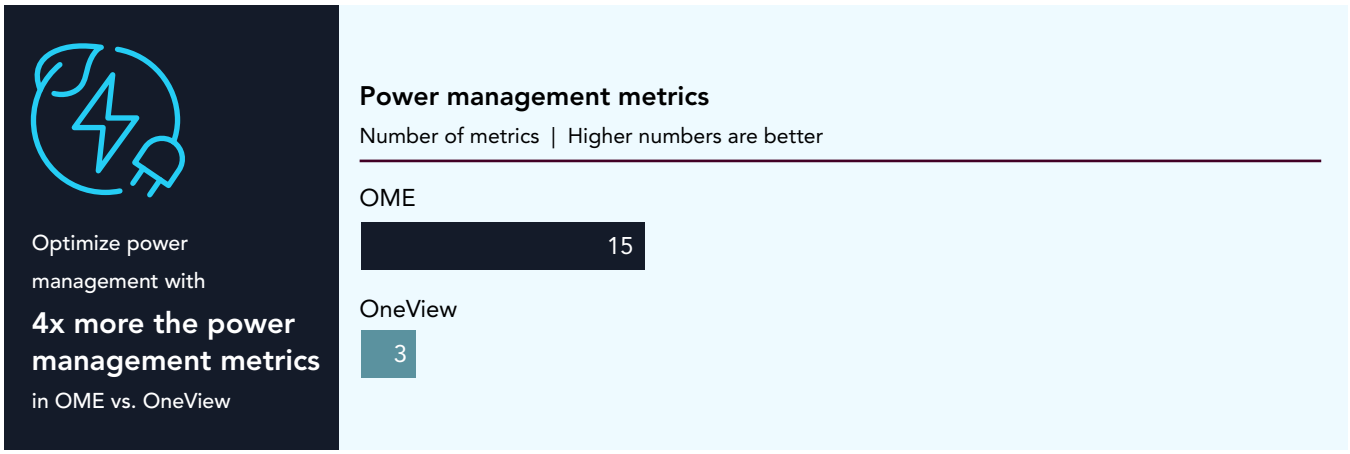

Abbildung 4: Vergleich der Anzahl der Energiemanagementkennzahlen, die in OME und OneView verfügbar sind. Mehr Kennzahlen sind besser. Quelle: Principled Technologies.

Vereinfachen der Administratoraufgaben mit robusteren nutzerfreundlichen Funktionen

AdministratorInnen von Rechenzentren sind viel beschäftigte Menschen, aber die richtigen Managementtools können bestimmte Aufgaben automatisieren, das alltägliche Management optimieren und Belastungen beseitigen, damit sie mehr Zeit für Innovationen haben. Wir haben festgestellt, dass das Dell Managementportfolio eine Reihe von Funktionen bietet, die Administratoraufgaben vereinfachen können. Tabelle 4 enthält eine Zusammenfassung der wichtigsten nutzerfreundlichen Funktionen, die im Dell Managementportfolio im Vergleich zu HPE-Managementtools verfügbar sind.

Tabelle 4: Übersicht über die wichtigsten nutzerfreundlichen Funktionen, die in iDRAC9 und OME im Vergleich zu iLO 6 und OneView verfügbar sind. Quelle: Principled Technologies.

Funktion	Wichtige Vorteile der Dell Managementtools	Nachteile der HPE-Managementtools
Mehr Remote-BIOS- und HTML5-Funktionen	iDRAC9 bietet **2,5-mal mehr HTML5-Funktionen (insgesamt 10)** und **16-mal mehr Remote-BIOS-Funktionen (insgesamt 51)**.	In iLO 6 sind **nur 4 HTML-Remotefunktionen** und 3 Remote-BIOS-Funktionen verfügbar.
Einfachere BIOS-Konfigurationsänderungen	Für eine Änderung der BIOS-Konfiguration sind **87 % weniger Zeit und die Hälfte der Schritte** erforderlich.	Um Änderungen vorzunehmen, muss **ein/e AdministratorIn anwesend sein**.
Telemetrie-Streaming	iDRAC9 **bietet Telemetrie für 8 Module**.	iLO 6 bietet Telemetrie für **nur 3 Module** mithilfe der JSON-Ausgabe von HPE.
Verbindungsanzeige	Die Verbindungsanzeige in iDRAC9 **bietet Details zur physischen Zuordnung von Switchports** zu den Netzwerkports des Servers und zu dedizierten iDRAC-Portverbindungen.	iLO 6 stellt **keine physischen Verbindungsinformationen** zu Upstreamswitches bereit.
Skalierbarkeit	OME kann **bis zu 8.000 Geräte managen**.[3]	OneView kann **nur 1.024 Geräte** managen.[4]
Warnmeldungsbasierte Aktionen	OME **bietet Warnmeldungsrichtlinien**, die Aktionen basierend auf der Eingabe einer Warnmeldung für einen Server, eine Gruppe von Servern oder alle Server auslösen Das Einrichten einer Warnmeldung erfordert eine **einmalige Einrichtung** mit 13 Schritten, die 65 Sekunden in Anspruch nimmt, danach **erfolgt die Aktion automatisch**.	OneView **bietet keine warnungsmeldungsbasierten Aktionen**. Das Einrichten einer Warnmeldung erfordert **5 Schritte und 36 Sekunden für jeden einzelnen Server**, was bei großen Bereitstellungen einen enormen Zeitaufwand für AdministratorInnen bedeutet.
Firmwaremanagement	Das OME-Firmwaremanagement **ermöglicht die Aktualisierung einer einzelnen Komponente oder aller Komponenten**, um für Compliance mit einer definierten Baseline zu sorgen.	OneView **bietet nur die Compliance mit der Firmwarebaseline** durch Anhängen innerhalb des Serverprofils.
Monitoring von Drittanbietergeräten	OME **unterstützt das Monitoring von Drittanbietergeräten und -servern**.	OneView **bietet keine Unterstützung** für das Monitoring von Drittanbietergeräten und -servern.
Berichterstellung	OME bietet **4,2-mal mehr Berichte** mit **42 integrierten Berichten**, die angepasst werden können, um die wichtigsten Daten für den jeweiligen Zweck granular auszuwählen.	OneView bietet nur **10 integrierte Berichte ohne Anpassung**.
Mobiles Monitoring/ Management	OME **lässt sich in OpenManage Mobile integrieren** und bietet so Transparenz und Verwaltbarkeit für die Infrastruktur auf dem iOS- oder Android-Mobilgerät von AdministratorInnen.	OneView **umfasst keine mobile Anwendung**, wodurch das Management für AdministratorInnen weniger flexibel ist.

Um den Managementaufwand zu verringern und AdministratorInnen einen zentralen Standort für Management und Monitoring bereitzustellen, bietet OME erweiterte Unterstützung für eine Vielzahl von Servern, Gehäusen, Netzwerkgeräten und mehr. Die vollständige OpenManage-Supportmatrix finden Sie unter https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix.[5]

Einfachere Serverbereitstellung mit 1:n-Konfigurationsvorlagen

Bei Bereitstellungen mit mehreren Servern kann die Verwendung von OME die Zeit für die Bereitstellung von Konfigurationsvorlagen im Vergleich zu OneView verkürzen. Die Bereitstellung einer Konfigurationsvorlage für einen einzelnen Server dauert bei beiden Lösungen ähnlich lange: 47 Sekunden und 10 Schritte bei OME im Vergleich zu 49 Sekunden und 5 Schritten bei OneView. AdministratorInnen können jedoch Konfigurationsvorlagen für Servergruppen in OME bereitstellen, während sie in OneView Konfigurationen für jeden Server einzeln bereitstellen müssen.

Das bedeutet, dass OME bei einer identisch konfigurierten Bereitstellung mit 100 Servern nur 47 Sekunden und 10 Administratorschritte benötigt, bei OneView jedoch etwa 1 Stunde 21 Minuten und 500 Schritte für die Bereitstellung von Konfigurationsvorlagen auf Servern erforderlich sind, was 99 % weniger Zeit und 98 % weniger Schritte bei OME bedeutet (siehe Abbildung 5).

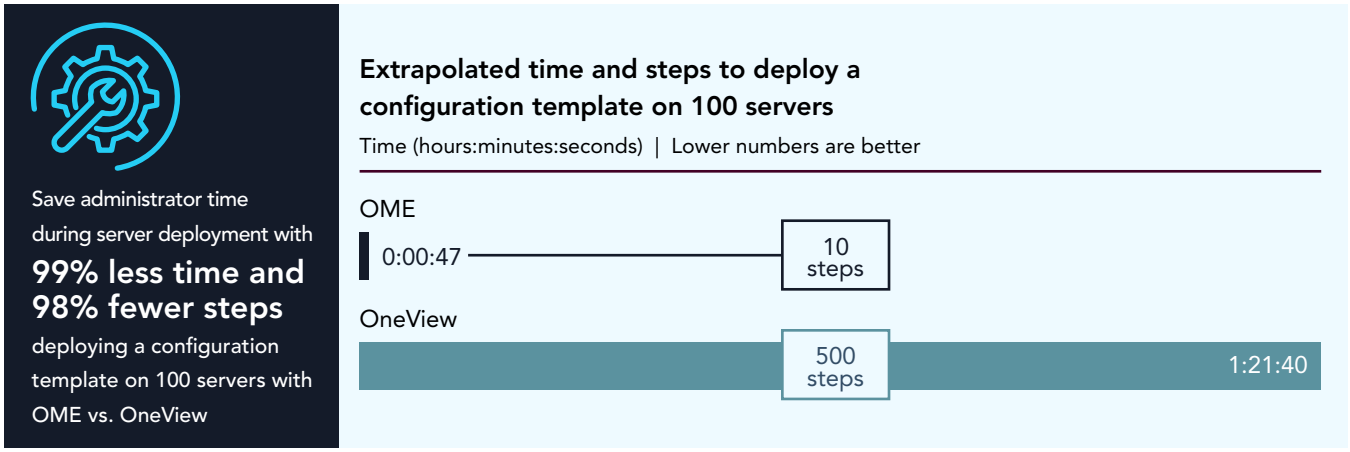

Abbildung 5: Vergleich der Zeit und Schritte für die Bereitstellung von Konfigurationsvorlagen mit OME und OneView. OME kann eine Vorlage auf viele Server gleichzeitig anwenden, was die Zeitersparnis noch weiter erhöht. Weniger Zeit und weniger Schritte sind besser. Quelle: Principled Technologies.

Einfachere Einrichtung von Warnmeldungen

Wir haben festgestellt, dass OME mehr Optionen für das Monitoring der Infrastruktur bietet. Mit OME können NutzerInnen Warnmeldungsrichtlinien einmal einrichten und sie dann automatisch für zukünftige Warnmeldungen zuweisen. Wir haben in 13 Schritten und 65 Sekunden eine Warnmeldungsrichtlinie erstellt, die ein ordnungsgemäßes Herunterfahren durchführt, wenn das System eine kritische Temperaturwarnung von iDRAC9 erhält. Zwar dauert der Einrichtungsprozess für die Automatisierung von Warnmeldungen länger (1 Minute, 5 Sekunden) als bei OneView (36 Sekunden und 5 Schritte), aber OneView verfügt nicht über automatisierte Optionen für Warnmeldungen, sodass AdministratorInnen jedes Mal manuell Aktionen ausführen müssen. Das bedeutet, dass OME im Vergleich zu OneView bei einer Bereitstellung mit 100 Servern bis zu 98 % Zeitaufwand und 97 % Schritte einspart, indem Aktionen basierend auf Warnmeldungen automatisiert werden, nachdem AdministratorInnen eine Richtlinie erstellt haben.

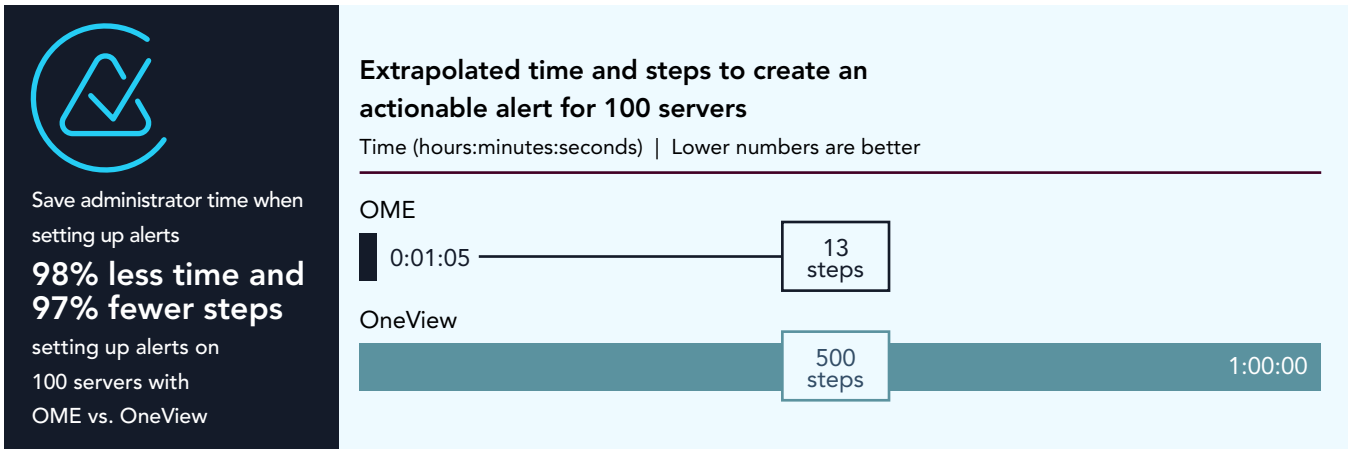

Abbildung 6: Vergleich der Zeit und Schritte, die für die Einrichtung von Warnmeldungen mit OME und OneView erforderlich waren. OME automatisiert Warnmeldungen nach einer einzigen Einrichtung, wodurch AdministratorInnen Zeit und Aufwand sparen. Weniger Zeit und weniger Schritte sind besser. Quelle: Principled Technologies.

Informationen zu Dell Technologies OpenManage Enterprise

OME ist eine 1:n-Systemmanagementkonsole für das Rechenzentrum und darüber hinaus. 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. OME bietet ein umfassendes Lebenszyklusmanagement von Dell PowerEdge-Servern und 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.[6] In einer kürzlich durchgeführten PT-Studie haben wir festgestellt, dass eine Dell Umgebung mit OME und OpenManage Enterprise Modular (OME-M) Zeit bei Änderungen an VLANs einsparen und Interventionen während geplanter Firmwareupdates vermeiden kann.[7]

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

Remotemanagement

Remotemanagementfunktionen geben AdministratorInnen die Flexibilität, mehr Änderungen außerhalb des Rechenzentrums vorzunehmen. Wir haben festgestellt, dass iDRAC9 1,5-mal mehr HTML5-Remotekonsolenfunktionen als iLO 6 bietet – insgesamt 10 Funktionen im Vergleich zu nur 4. Damit ist das iDRAC9-Remoteservermanagement einfach und effizient. iDRAC9 bietet außerdem 16-mal mehr BIOS-Konfigurationsfunktionen als iLO 6 (51 Funktionen im Vergleich zu nur 3 Funktionen), sodass AdministratorInnen eine granulare Kontrolle über die BIOS-Konfiguration erhalten (siehe Abbildung 7 und Abbildung 8).

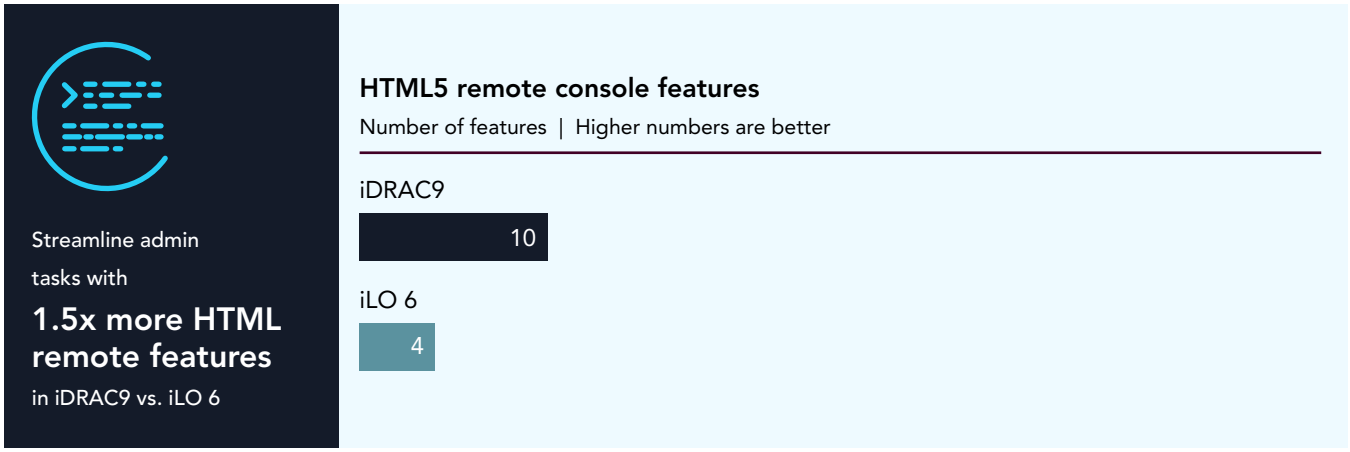

Abbildung 7: Vergleich der HTML5-Remotefunktionen, die das jeweilige Managementtool bietet. Mehr Funktionen sind besser. Quelle: Principled Technologies.

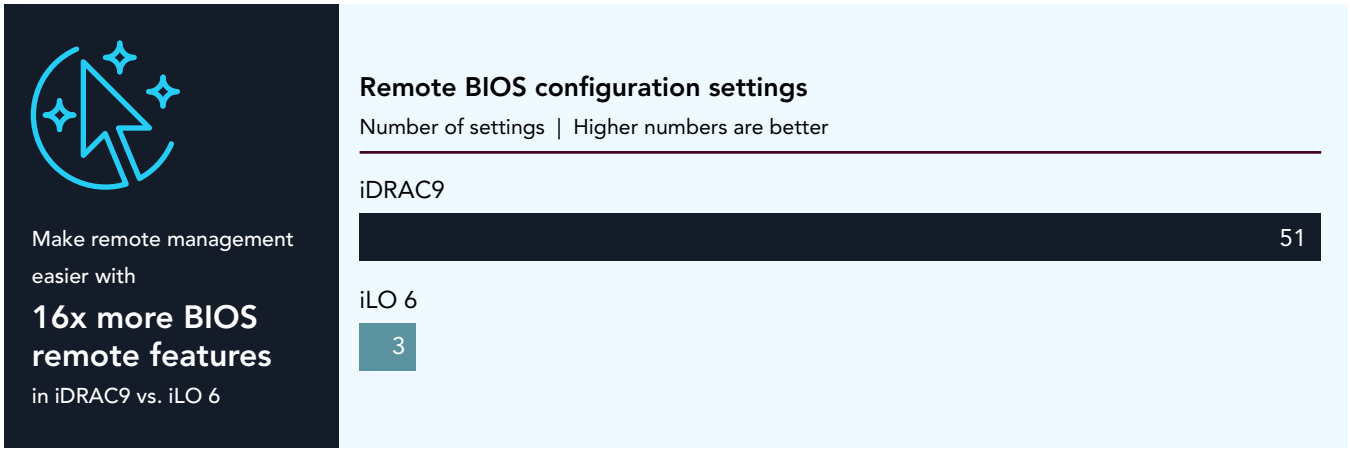

Abbildung 8: Vergleich der BIOS-Remotefunktionen, die das jeweilige Managementtool bietet. Mehr Funktionen sind besser. Quelle: Principled Technologies.

Durchführung von BIOS-Konfigurationsänderungen

Mit iDRAC9 können AdministratorInnen BIOS-Konfigurationseinstellungen ändern und das Update für einen späteren Neustart bereitstellen, ohne dass AdministratorInnen anwesend sein müssen. Bei iLO 6 müssen Änderungen dagegen innerhalb der Systemdienstprogramme durchgeführt werden, was bedeutet, dass während der Änderung manuelle Administratoreingriffe erforderlich sind. Wie in Abbildung 9 gezeigt, nahm die Bereitstellung der BIOS-Konfigurationsänderung für einen geplanten Neustart mit iDRAC9 im Vergleich zu iLO 6 87 % weniger Zeit und die Hälfte der Schritte in Anspruch. Diese Zeitersparnis pro Server kann zu einer signifikanteren Einsparung von Administratorzeit bei größeren Bereitstellungen führen. Beispiel: Bei einer Bereitstellung mit 100 Servern können Sie über 6 Stunden einsparen. iDRAC9 und iLO 6 erfordern beide individuelle BIOS-Konfigurationsänderungen pro Server.

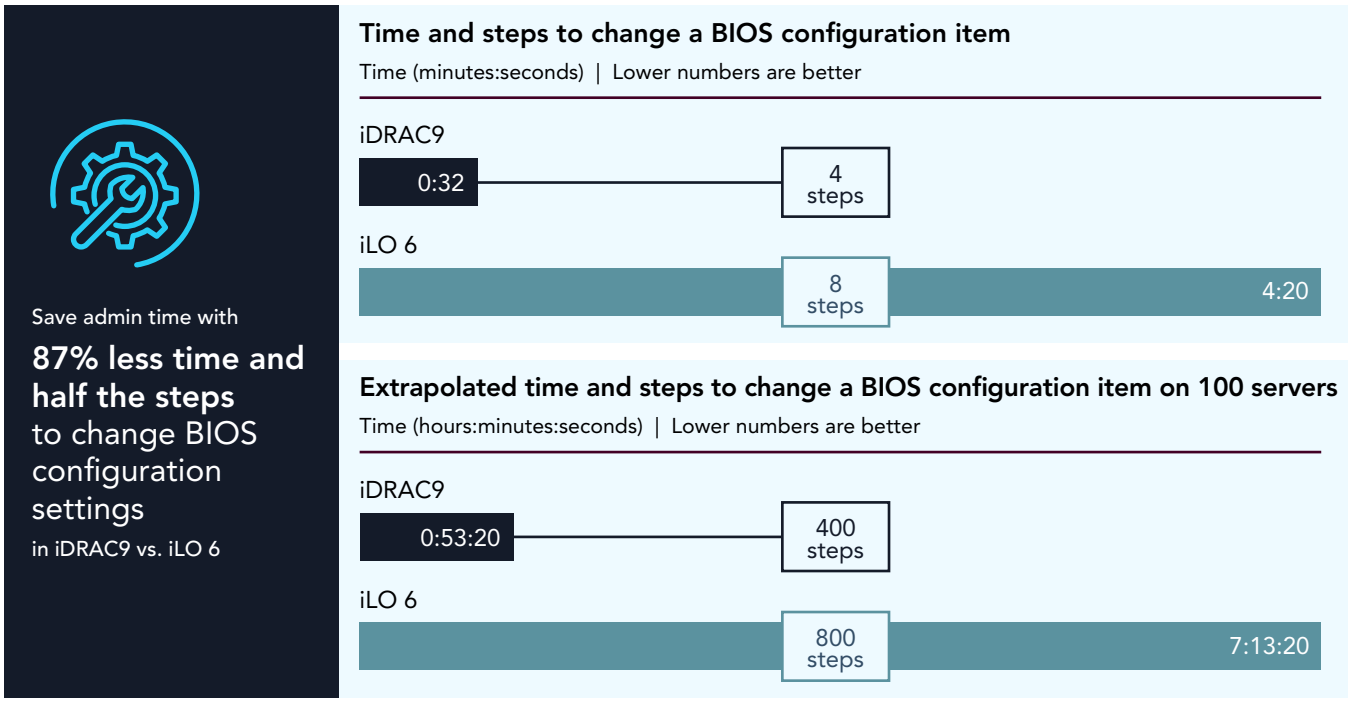

Abbildung 9: Erforderliche Zeit für die Änderung der BIOS-Konfigurationseinstellungen und die Bereitstellung des Updates für einen späteren Neustart für einen einzelnen Server und hochgerechnete Zeit für 100 Server. Weniger Zeit und weniger Schritte sind besser. Quelle: Principled Technologies.

Informationen zu Dell Technologies Integrated Dell Remote Access Controller 9

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

- 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
- Telemetrie und Automatisierung
- Robuste Sicherheitsfunktionen und -optionen[8]

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

Mehr Sicherheit, Nachhaltigkeit und Administratoreffizienz mit Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ)

Das cloudbasierte Monitoringtool Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) bietet AdministratorInnen eine Möglichkeit, die Performance über alle Dell PowerEdge-Infrastrukturbereitstellungen, einschließlich Servern, Storage und mehr, zu überwachen, zu managen und zu analysieren. Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) bietet mehrere Sicherheitsfunktionen, die den Schutz Ihres Unternehmens vor Angriffen weiter stärken. Einige dieser Funktionen sind in Tabelle 5 näher beschrieben.

Tabelle 5: Übersicht über die wichtigsten Sicherheitsfunktionen, die in Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) verfügbar sind. Quelle: Principled Technologies.

Funktion	So schützt Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) Ihre Umgebung
Warnmeldungen auf Cybersicherheitsrisiko-Ebene	Häufige Einblicke in die Cybersicherheit mit spezifischen Warnmeldungen auf Sicherheitsrisikoebene, damit AdministratorInnen schneller reagieren und Probleme schnell beheben können, um ihre Daten zu schützen
Richtlinienbasierte Sicherheitskonfiguration	Richtlinienbasierte Sicherheitskonfigurationseinstellungen und einfach anzuwendende Vorlagen, mit denen AdministratorInnen sicherstellen können, dass Best-Practice-Einstellungen für die Sicherheit vorhanden sind, um die PowerEdge-Umgebung zu schützen
Cybersicherheitsratgeber	Relevante Sicherheitsratgeber mit Details zu spezifischen Sicherheitslücken und Empfehlungen zur Korrektur, sodass schnelle Maßnahmen zum Schließen von Sicherheitslücken ergriffen werden können

Durch die Verwendung dieser Sicherheitsmonitoringfunktionen über die Cloud bietet Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) AdministratorInnen eine weitere nutzerfreundliche und automatisierte Möglichkeit, die Integrität und Sicherheit ihrer Infrastruktur unter Kontrolle zu halten.

Zusätzliche Nachhaltigkeits- und Effizienzfunktionen in Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ)

Die cloudbasierte Monitoringplattform Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) bietet zusätzliche nutzerfreundliche Funktionen, die in iDRAC9 und OME integriert werden können. So können AdministratorInnen den Status ihrer PowerEdge-Umgebung einfacher beobachten und bei Bedarf Maßnahmen ergreifen. Zu diesen Funktionen zählen:

- **Analyse des CO_2-Fußabdrucks**: Dieses Tool befindet sich im Abschnitt „Monitoring“ und bietet eine bessere Übersicht und bessere Prognose der Kohlendioxidemissionsnutzung in allen Umgebungen.
- **Performanceansichten**: Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) bietet Performanceansichten sowie Diagramme zu Anomalien und Auslastung, um AdministratorInnen beim ersten Anzeichen von Problemen zu warnen.
- **Anpassbare Performance- und Bestandsberichte**: Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) bietet kundenspezifische Reportingoptionen für Serverperformance- und Bestandsdaten, sodass AdministratorInnen mehr Kontrolle über die Performance- und Gerätekennzahlen erhalten, die sie verfolgen möchten.

Informationen zu Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ)

Dell APEX AIOps Infrastructure Observability (ehemals 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 Dell APEX AIOps Infrastructure Observability (ehemals 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 Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) finden Sie unter https://www.dell.com/en-us/dt/apex/aiops.htm.

Nach Abschluss der Tests hat Dell neue Funktionen veröffentlicht, mit denen AdministratorInnen **Systemupdates** über Dell APEX AIOps Infrastructure Observability (ehemals CloudIQ) durchführen können. Laut Dell Dokumentation stehen auf der Seite „Systemupdates" bis zu fünf Kategorien für Systemupdates zur Verfügung: Storage, Netzwerke, HCI, Data Protection und Server. Wir haben diese Funktion zu diesem Zeitpunkt nicht getestet, planen jedoch, diese Funktion in einem späteren Whitepaper zu validieren.[11]

Entscheidung

Jedes Mal, wenn Sie Hardware kaufen, erhalten Sie auch das Portfolio an Managementtools, die der Hardwareanbieter zum Managen und Überwachen Ihrer Infrastruktur anbietet. Technische Daten sind wichtig, aber ebenso wichtig sind End-to-End-Sicherheit, das Erreichen von Nachhaltigkeitszielen und die Möglichkeit, Administratoraufgaben zu optimieren. Wir haben in unserem Rechenzentrum die Funktionen und Merkmale der Servermanagementtools von Dell und HPE verglichen, d. h. iDRAC9 und iLO 6 für das integrierte Servermanagement sowie OME und OneView für das 1:n-Geräte- und Konsolenmanagement und -monitoring.

In den Bereichen Sicherheit, Nachhaltigkeit und Management-/Monitoringfunktionen haben wir festgestellt, dass Dell Servermanagementtools mehr zu bieten haben als vergleichbare HPE-Tools. Sie stellen AdministratorInnen mehr Remotemanagementoptionen bereit, verkürzen die Zeit für das Sperren von Systemen und bieten eine feiner abgestimmte Kontrolle, um Nachhaltigkeitsziele zu erreichen. Durch die Reduzierung des Administratorzeitaufwands für bestimmte routinemäßige Monitoring- und Wartungsaufgaben mit dem Dell Managementportfolio hat Ihr Team mehr Zeit für Innovationen und andere Initiativen.

---

1. Harvard Business Review, „The Devastating Business Impacts of a Cyber Breach", abgerufen am 10. April 2024, https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.
2. Hinweis: Mit dieser Methode in HPE iLO 6 werden alle externen USB-Anschlüsse heruntergefahren, nicht nur die Anschlüsse auf der Vorderseite.
3. Dell, „OpenManage Enterprise 4.0.x – Supportmatrix", abgerufen am 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", abgerufen am 19. April 2024, https://support.hpe.com/hpesc/public/docDisplay?docId=sd00003831en_us&page=GUID-D7147C7F-2016-0901-066B-000000000529.html.
5. Dell, „OpenManage Enterprise 4.0.x – Supportmatrix", abgerufen am 19. April 2024, https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix.
6. Dell, „OpenManage Enterprise", abgerufen am 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 Easy for Administrators", abgerufen am 9. April 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
8. Dell, „Integrated Dell Remote Access Controller (iDRAC)", abgerufen am 9. April 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.
9. Dell, „APEX AIOps: Bewältigung der IT-Komplexität in Ihrem digitalen Unternehmen", abgerufen am 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", abgerufen am 9. April 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.
11. Dell, „System Updates", abgerufen am 19. April 2024, https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/system-updates-2/.

Lesen Sie den wissenschaftlichen Hintergrund dieses Berichts ▶

▶ Lesen Sie die Originalversion dieses Berichts in englischer Sprache

Principled Technologies®

Facts matter.®

Principled Technologies ist eine eingetragene Marke von Principled Technologies, Inc.
Alle anderen Produktnamen sind Marken der jeweiligen Inhaber. Zusätzliche Informationen finden Sie im wissenschaftlichen Hintergrund dieses Berichts.

Dieses Projekt wurde in Auftrag gegeben von Dell Technologies.