Sécurité renforcée avec le verrouillage du système

95 % de temps en moins et 83 % d'étapes en moins

avec iDRAC9 par rapport à iLO 6

Optimisez l'efficacité énergétique avec

4 fois plus de mesures de gestion de l'alimentation

et 25 rapports personnalisables dans OME par rapport à 0 rapports dans OneView

Fonctionnalité distante améliorée avec

16 fois plus de fonctionnalités de BIOS distant

avec 51 fonctionnalités dans iDRAC9 contre 3 dans iLO 6

Améliorer la sécurité, la durabilité et l'efficacité des administrateurs avec la gamme de solutions de gestion de serveurs Dell

par rapport aux outils de gestion de serveurs comparables de HPE

Lors du choix des serveurs, les spécifications ne doivent pas être les seuls éléments à prendre en compte. En choisissant un fournisseur doté d'outils de gestion qui réduisent le temps de manipulation pour les administrateurs, renforcent la sécurité et offrent une planification du développement durable, votre infrastructure peut vous aider à atteindre un certain nombre des objectifs de votre entreprise. Dans le datacenter Principled Technologies, nous avons comparé les fonctionnalités des portefeuilles de gestion de serveurs Dell et HPE pour voir ce qu'ils ont à offrir aux administrateurs. Nous avons comparé :

Tableau 1 : Les outils de gestion que nous avons testés.

	Dell	HPE
Gestion des serveurs intégrée/à distance	Dell Technologies Integrated Dell Remote Access Controller (iDRAC9)	HPE Integrated Lights-Out (iLO 6)
Console de gestion des appareils un-à-plusieurs	Dell Technologies OpenManage™ Enterprise (OME)	HPE OneView

Nous avons également examiné APEX AIOps Infrastructure Observability (anciennement CloudIQ), certaines des fonctionnalités et certains avantages de cet outil de surveillance basé sur le Cloud pour la gestion des serveurs.

Sur l'ensemble des fonctionnalités et des cas d'utilisation que nous avons testés, les outils de la gamme de gestion Dell offraient de meilleures fonctionnalités de sécurité et un plus large éventail d'outils de gestion du développement durable. Ils offraient également aux administrateurs un contrôle plus précis et une plus grande flexibilité, tout en réduisant le temps et les efforts nécessaires à l'exécution des tâches courantes.

Fournir une sécurité de bout en bout

Les cyberattaques, dans lesquelles des acteurs malveillants s'infiltrent dans les systèmes pour récupérer et exploiter des données privées, se multiplient. Selon un rapport publié en 2023, « 83 % des organisations ont subi au moins une violation de données en 2022 »,[1] ce qui montre que la question de la cybersécurité touche les entreprises du monde entier. Choisir du matériel doté de fonctionnalités de sécurité de bout en bout peut vous aider à protéger les données de votre organisation contre ces attaques coûteuses. Dell propose de solides fonctionnalités de sécurité intégrées au serveur via iDRAC9, dans la console globale et le logiciel de gestion Cloud pour renforcer la sécurité de votre organisation.

Sécurité intégrée

Chaque serveur Dell PowerEdge™ dispose de fonctionnalités de sécurité intégrées via iDRAC9 pour empêcher les acteurs malveillants d'accéder aux données. Voici deux de ces importantes fonctionnalités :

- **Activation/désactivation dynamique des ports USB** : la désactivation et l'activation des ports USB permettent aux administrateurs de contrôler l'accès au serveur via un port USB. Le terme « dynamique » renvoie à la possibilité d'activer et de désactiver ces ports USB sans redémarrer le serveur ou le système d'exploitation. Tant que l'administrateur ne fournit pas l'accès, personne ne peut brancher une clé USB ou un clavier pour modifier les paramètres de configuration du système, du système d'exploitation ou du BIOS.
- **Verrouillage dynamique du système :** le verrouillage du système permet d'empêcher toute activité involontaire ou malveillante de modifier les paramètres du BIOS du système, de l'iDRAC et du firmware. Le terme « dynamique » fait référence à la capacité de mettre en place ces capacités une seule fois, puis de les activer au besoin. (Remarque : Cette fonctionnalité est disponible avec les licences iDRAC9 Enterprise ou Datacenter.)

La Figure 1 illustre les résultats de notre comparaison pratique lors de l'utilisation d'iDRAC9 et d'iLO 6 pour désactiver dynamiquement les ports USB.

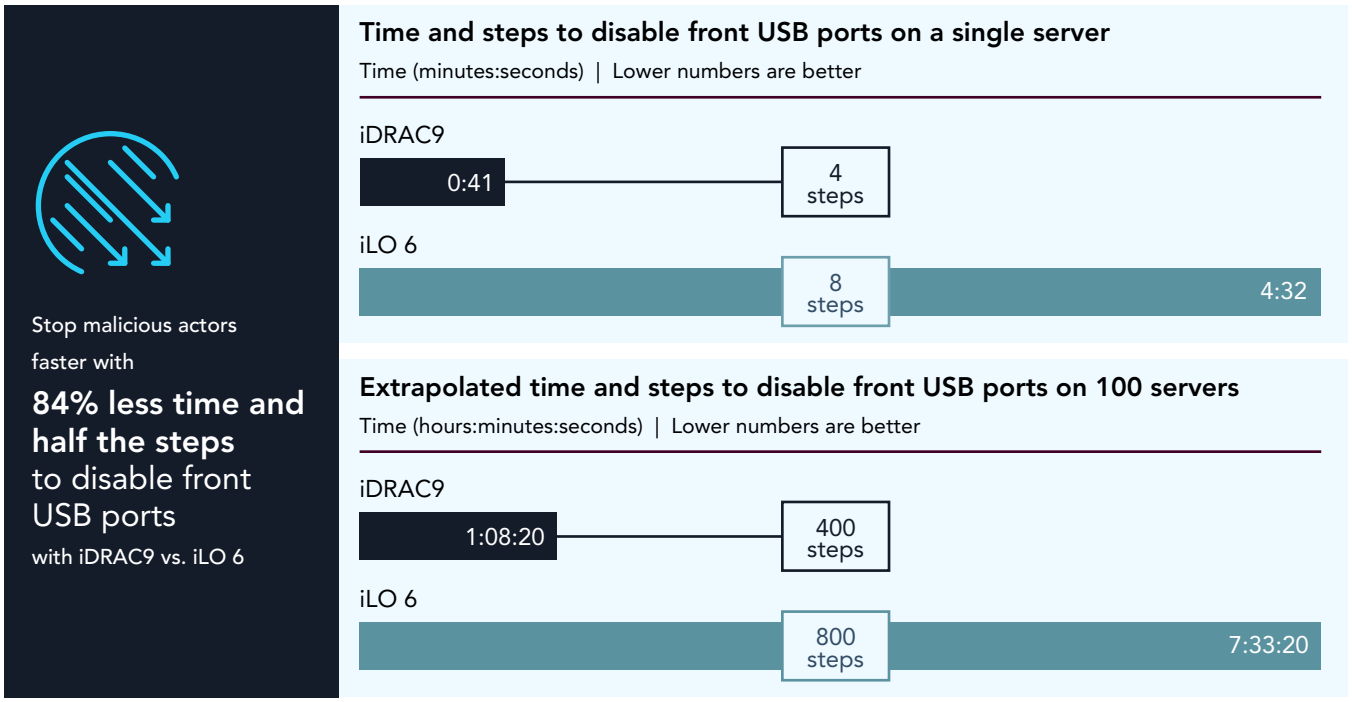

Figure 1 : Temps nécessaire pour désactiver les ports USB frontaux pour un seul serveur, avec extrapolation du délai de désactivation des ports USB frontaux pour 100 serveurs. Moins de temps et moins d'étapes pour plus d'efficacité. Source : Principled Technologies.

Remarque : Les graphiques de ce rapport utilisent différentes échelles pour conserver une taille cohérente. Faites attention à la plage de données de chaque graphique lors de la comparaison.

Avec iDRAC9, nous avons constaté que les administrateurs pouvaient désactiver les ports USB frontaux sur un seul serveur en seulement 41 secondes, moyennant 4 étapes. En comparaison, le même processus avec iLO 6 prendrait 4 minutes, 32 secondes et 8 étapes par serveur. Autrement dit, **il faut 84 % de temps en moins et deux fois moins d'étapes pour désactiver les ports USB frontaux avec iDRAC9**.[2] À l'échelle d'un datacenter, les gains de temps s'accumulent. Pour un déploiement de 100 serveurs, les administrateurs peuvent gagner 6 heures en utilisant iDRAC9 pour désactiver les ports USB, comparativement à iLO 6.

Non seulement ces fonctionnalités sont plus faciles et plus rapides d'accès avec iDRAC9 qu'avec iLO 6, mais avec iDRAC9, les administrateurs peuvent également **maintenir les serveurs en production** tout en activant ou en désactivant ces fonctionnalités, ce qui **évite les interruptions de service**. ILO 6 nécessite à la fois de modifier la configuration du BIOS et de redémarrer à chaque fois.

Il est très important de pouvoir déverrouiller rapidement un système pour appliquer des mises à jour et de pouvoir ensuite le reverrouiller rapidement. Comme le montre la Figure 2, nous avons constaté que **les administrateurs utilisant iDRAC9 pouvaient réduire de 95 % le temps nécessaire au verrouillage du système serveur et réduire de 83 % le nombre d'étapes** par rapport à l'utilisation d'iLO 6, qui prenait plus de 5 minutes et 12 étapes par serveur.

En extrapolant ces données à un datacenter de 100 serveurs, les administrateurs pourraient verrouiller les systèmes en un peu plus d'une demi-heure à l'aide d'iDRAC9, alors qu'il leur faudrait plus d'une journée de travail complète (près de 9 heures) pour verrouiller 100 serveurs à l'aide d'iLO 6. Ce temps pourrait s'avérer significatif pour les pirates informatiques afin d'accéder aux données. De plus, l'utilisation de la solution iLO 6 pour le verrouillage du système nécessite une interruption de service du serveur, contrairement à la solution iDRAC9. La fonctionnalité de verrouillage iDRAC9 est beaucoup plus rapide et plus facile à utiliser que la fonctionnalité de verrouillage iLO 6.

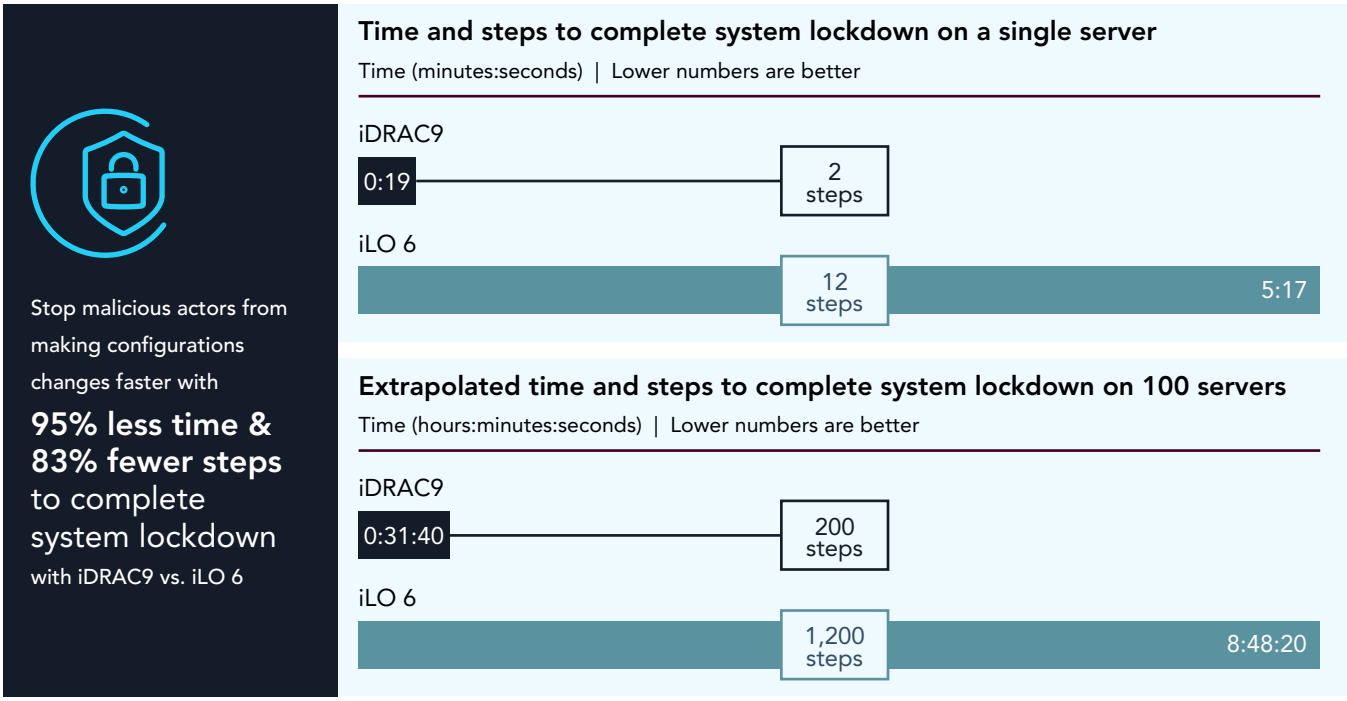

Figure 2 : Temps nécessaire pour terminer le verrouillage du système pour un seul serveur et temps extrapolé pour terminer le verrouillage du système pour 100 serveurs. Moins de temps et moins d'étapes pour plus d'efficacité. Source : Principled Technologies.

Maintenir la sécurité grâce à une gestion simplifiée des informations d'identification dans OME

OME fournit aux administrateurs un moyen plus facile de gérer la rotation des mots de passe iDRAC9. Plutôt que d'exiger un compte administrateur statique et connu, OME gère un compte de service dans lequel les clients sélectionnent la règle de rotation des mots de passe requise, dont le mot de passe n'est jamais divulgué. **OneView ne dispose pas de cette fonctionnalité**. Dans notre datacenter, nous avons confirmé que les serveurs gérés par iDRAC9 étaient intégrés au compte OME avec des privilèges d'administrateur complets pour faciliter la gestion des informations d'identification.

Aider à atteindre vos objectifs de développement durable

Les datacenters ont des besoins importants en matière d'alimentation et de refroidissement, mais la gestion thermique et de l'alimentation peut aider les administrateurs à optimiser les coûts du datacenter et à atteindre les objectifs de développement durable, tout en fournissant aux charges applicatives les ressources dont elles ont besoin pour obtenir des performances optimales. OME intègre plusieurs fonctionnalités qui permettent de surveiller et de gérer étroitement la consommation électrique, ce qui vous aide potentiellement à atteindre vos objectifs de développement durable. Les tableaux 2 et 3 mettent en évidence les principaux avantages de ces fonctionnalités, que nous décrivons plus en détail ci-dessous.

Tableau 2 : Différences entre OME et OneView en termes de développement durable. Source : Principled Technologies.

Fonctionnalité	OME	OneView
Calculateur d'utilisation des émissions de carbone et outil de planification de la capacité	✓	x
Règle de gestion de l'alimentation déclenchée par la température	✓	x
Règle de gestion de l'alimentation statique	✓	x
Tableau de bord Power Manager	✓	x
Rapports de gestion de l'alimentation avec distribution planifiée des e-mails	✓	x

Tableau 3 : Récapitulatif de notre comparaison des fonctionnalités liées au développement durable entre OME et OneView. Source : Principled Technologies.

Fonctionnalité	Avantages clés des outils de gestion Dell	Inconvénients des outils de gestion HPE
Calculateur d'utilisation des émissions de carbone et outil de planification de la capacité	Estimation des **émissions de gaz à effet de serre** avec des valeurs personnalisables pour vous aider à atteindre vos objectifs de développement durable	**Aucune fonctionnalité comparable** ; rend difficile la planification des objectifs de développement durable
Gestion thermique et de l'alimentation automatisée	**Options de règles statiques et à déclenchement thermique**, avec la possibilité de déclencher une action lorsque le serveur dépasse un seuil de consommation électrique ou de température	**Aucune fonctionnalité comparable** pour la gestion automatisée de l'alimentation
Tableau de bord et rapports de consommation électrique	Le tableau de bord du plug-in OME Power Manager **fournit un accès rapide** aux données de Power Manager. Le plug-in OME Power Manager propose **25 rapports par défaut et/ou personnalisables différents,** qui identifient rapidement les principaux consommateurs d'énergie, les contrevenants énergétiques, les racks sous-utilisés et les serveurs inactifs	OneView **n'a pas de tableau de bord Power Manager** et **ne dispose pas de rapports de gestion de l'alimentation**
Mesures de gestion de l'alimentation	**Jusqu'à 5 fois plus de mesures**, offrant des informations plus granulaires sur la gestion de la consommation électrique avec 15 mesures	**Seulement 3 mesures**, ce qui donne moins de visibilité et de contrôle de la consommation électrique

Émissions de carbone et analyse de l'empreinte carbone

Parmi ses fonctionnalités, **OME propose un calculateur d'utilisation des émissions de carbone et un outil de planification de la capacité**. Cet outil aide les organisations à estimer leurs émissions de gaz à effet de serre, en fournissant des valeurs par défaut pour les coûts énergétiques et les émissions de carbone par unité d'énergie consommée. Cette fonctionnalité permet également la personnalisation, ce qui permet aux organisations d'intégrer des valeurs pour les coûts énergétiques et les émissions de carbone de leur propre région pour chaque unité d'énergie consommée pour les données spécifiques au modèle de consommation de leur datacenter. **OneView ne dispose pas de fonctionnalité comparable**, ce qui rend plus difficile pour les organisations de planifier en tenant compte du développement durable.

Gestion thermique et de l'alimentation automatisée

OME Power Manager offre une gestion automatisée de l'alimentation et de la température via des options de règles déclenchées par la température et l'alimentation qui permettent aux administrateurs de définir des limites de consommation électrique ou des seuils de température, afin de réduire les coûts de refroidissement. En revanche, **OneView n'offre aucune fonctionnalité automatisée de gestion de l'alimentation et de la température**. Étant donné que les administrateurs ne peuvent pas définir de limites en fonction de la température, les coûts de refroidissement peuvent augmenter en raison du manque de contrôles automatisés.

L'optimisation de la consommation électrique est une stratégie importante pour atteindre les objectifs de développement durable. Le plugin OME Power Manager offre **25 rapports par défaut et/ou personnalisables liés à Power Manager** (17 dans les appareils Power Manager et 8 dans les groupes Power Manager) qui permettent aux administrateurs d'optimiser la planification de la capacité et de gérer l'alimentation pour optimiser l'efficacité. **OneView ne propose aucun rapport de gestion de l'alimentation similaire** (voir figure 3).

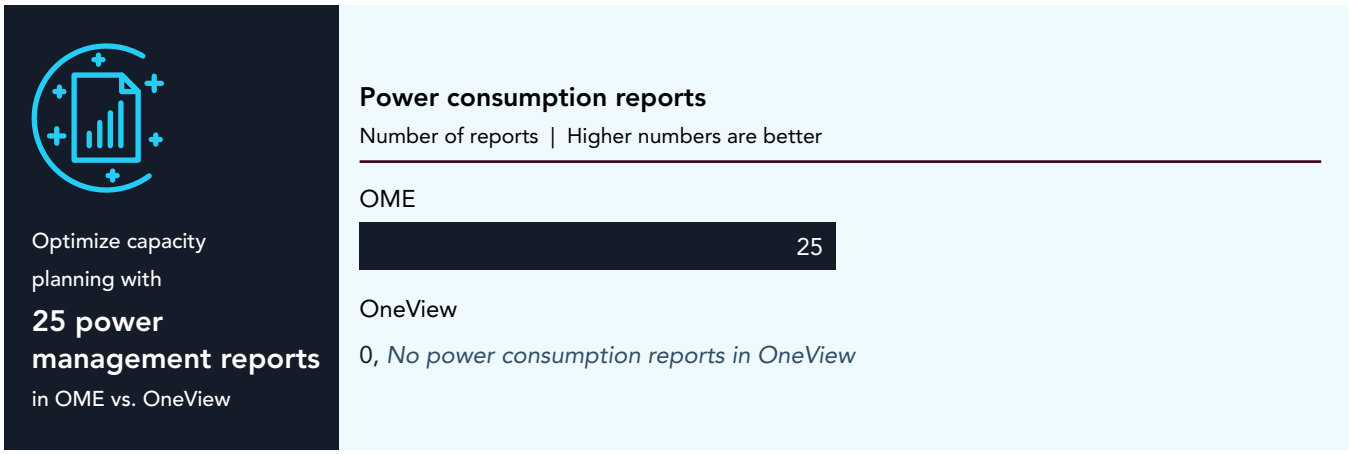

Figure 3 : Comparaison du nombre de rapports de gestion de l'alimentation disponibles dans OME et OneView. Des rapports plus nombreux offrent plus d'efficacité. Source : Principled Technologies.

Pour optimiser davantage la gestion de l'alimentation, le plug-in OME Power Manager permet aux administrateurs d'afficher jusqu'à 4 fois plus de mesures que OneView (voir Figure 4). OME fournit 15 mesures, y compris l'utilisation de l'alimentation par **les composants individuels, les machines virtuelles, le flux d'air et l'utilisation des composants**, tandis que OneView ne fournit que 3 mesures.

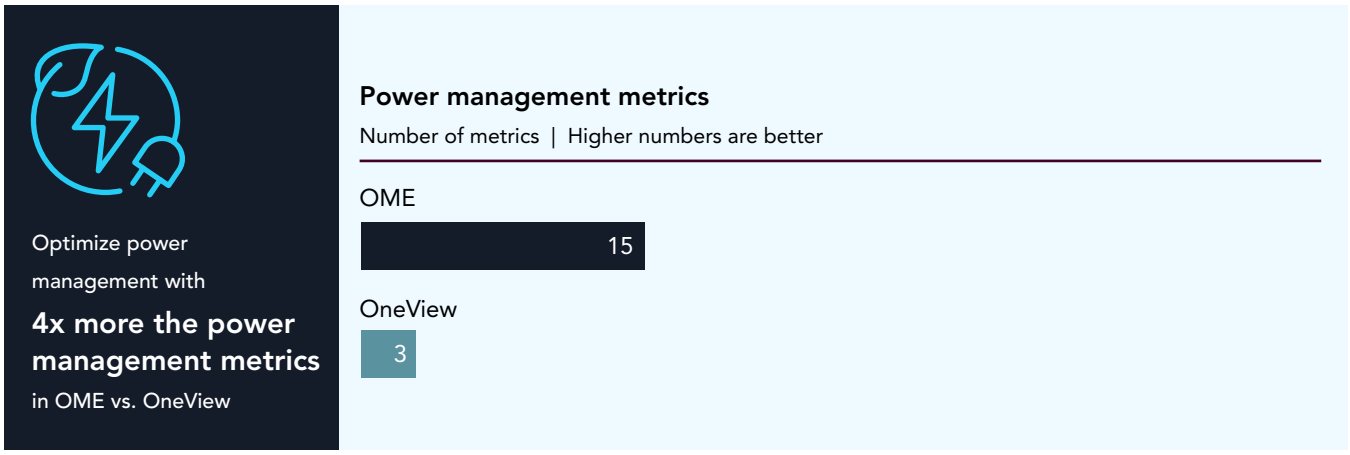

Figure 4 : Comparaison du nombre de mesures de gestion de l'alimentation disponibles dans OME et OneView. Un plus grand nombre de mesures offre plus d'efficacité. Source : Principled Technologies.

Des tâches d'administrateur simplifiées grâce à des fonctionnalités plus faciles à utiliser

Les administrateurs de datacenter sont des personnes très occupées, mais les outils de gestion appropriés peuvent automatiser certaines tâches, améliorer la gestion quotidienne et supprimer les charges pour leur laisser le temps d'innover. Nous avons constaté que la gamme de solutions de gestion Dell offrait un certain nombre de fonctionnalités qui peuvent simplifier les tâches des administrateurs. Le tableau 4 fournit un récapitulatif des principales fonctionnalités faciles d'utilisation disponibles dans la gamme de gestion Dell par rapport aux outils de gestion HPE.

Tableau 4 : Présentation des principales fonctionnalités faciles d'utilisation disponibles dans iDRAC9 et OME par rapport à iLO 6 et OneView. Source : Principled Technologies.

Fonctionnalité	Avantages clés des outils de gestion Dell	Inconvénients des outils de gestion HPE
Plus de fonctionnalités HTML5 et de BIOS à distance	iDRAC9 offre **2,5 fois plus de fonctionnalités HTML5 (10)** et **16 fois plus de fonctionnalités BIOS à distance (51)**	iLO 6 offre **seulement 4 fonctionnalités HTML distantes** et 3 fonctionnalités BIOS distantes
Modifications simplifiées de la configuration du BIOS	**87 % de temps en moins et deux fois moins d'étapes** pour apporter une modification à la configuration du BIOS	**Présence de l'administrateur requise** pour apporter des modifications
Télémétrie en streaming	iDRAC9 **fournit la télémétrie pour 8 modules**	iLO 6 fournit la télémétrie pour **3 modules uniquement** à l'aide de la sortie JSON de HPE
Affichage des connexions	La fonction Affichage des connexions dans iDRAC9 **établit un mappage physique détaillé entre les ports du commutateur**, et les ports réseau du serveur et les connexions des ports dédiés à l'iDRAC	iLO 6 ne fournit **aucune information de connexion physique** aux commutateurs en amont
l'évolutivité	OME est capable de **gérer jusqu'à 8 000 appareils**[3]	OneView ne peut gérer **que 1 024 appareils**[4]
Actions basées sur des alertes	OME **fournit des règles d'alerte** qui déclenchent des actions à partir d'une entrée d'une alerte pour un serveur, un groupe de serveurs ou tous les serveurs La configuration d'une alerte nécessite une **configuration ponctuelle** de 13 étapes et 65 secondes, puis **l'action se produit automatiquement**	OneView **n'offre pas d'actions basées sur des alertes** La configuration d'une alerte nécessite **5 étapes et 36 secondes pour chaque serveur**, ce qui nécessite un temps d'administration important pour les déploiements de grande envergure
Gestion du firmware	La gestion des firmwares OME **permet de mettre à jour un seul composant ou tous les composants** pour assurer la conformité à une base de référence définie	OneView **n'assure qu'une conformité à la base de référence du firmware** par une connexion au sein du profil de serveur
Surveillance des appareils tiers	OME **prend en charge la surveillance des appareils et des serveurs tiers**	OneView **ne prend pas en charge** la surveillance des appareils et des serveurs tiers.
Rapports	OME offre **4,2 fois plus de rapports**, dont **42 rapports intégrés** qu'il est possible de personnaliser pour sélectionner à un niveau granulaire les données les plus importantes qui serviront à les alimenter	OneView ne propose que **10 rapports intégrés sans personnalisation**
Surveillance/ gestion mobile	**OME s'intègre à OpenManage Mobile**, fournissant ainsi visibilité et gestion pour l'infrastructure sur un appareil mobile iOS ou Android de l'administrateur.	OneView **n'a pas d'application mobile**, ce qui rend la gestion moins flexible pour les administrateurs

Afin d'alléger la charge de gestion et d'offrir aux administrateurs un emplacement unique pour la gestion et la surveillance, OME offre une prise en charge étendue d'un large éventail de serveurs, de boîtiers, d'appareils de gestion de réseau, etc. Pour consulter la matrice de support d'OpenManage complète, rendez-vous sur https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix.[5]

Un déploiement de serveur plus facile grâce à des modèles de configuration un-à-plusieurs

Pour les déploiements avec plusieurs serveurs, l'utilisation d'OME peut réduire le temps de déploiement des modèles de configuration par rapport à l'utilisation de OneView. Le déploiement d'un modèle de configuration pour un seul serveur prend le même temps avec les deux solutions : 47 secondes et 10 étapes pour OME, et 49 secondes et 5 étapes pour OneView. Toutefois, les administrateurs peuvent déployer des modèles de configuration sur des groupes de serveurs dans OME, tandis que dans OneView, les administrateurs doivent déployer des configurations sur chaque serveur individuellement.

Cela signifie que pour un déploiement de 100 serveurs configurés de manière identique, OME ne prendrait que 47 secondes et 10 étapes administrateur, tandis qu'il faudrait à OneView environ 1 heure 21 minutes et 500 étapes pour déployer des modèles de configuration sur les serveurs, soit 99 % de temps en moins et 98 % d'étapes en moins (voir Figure 5).

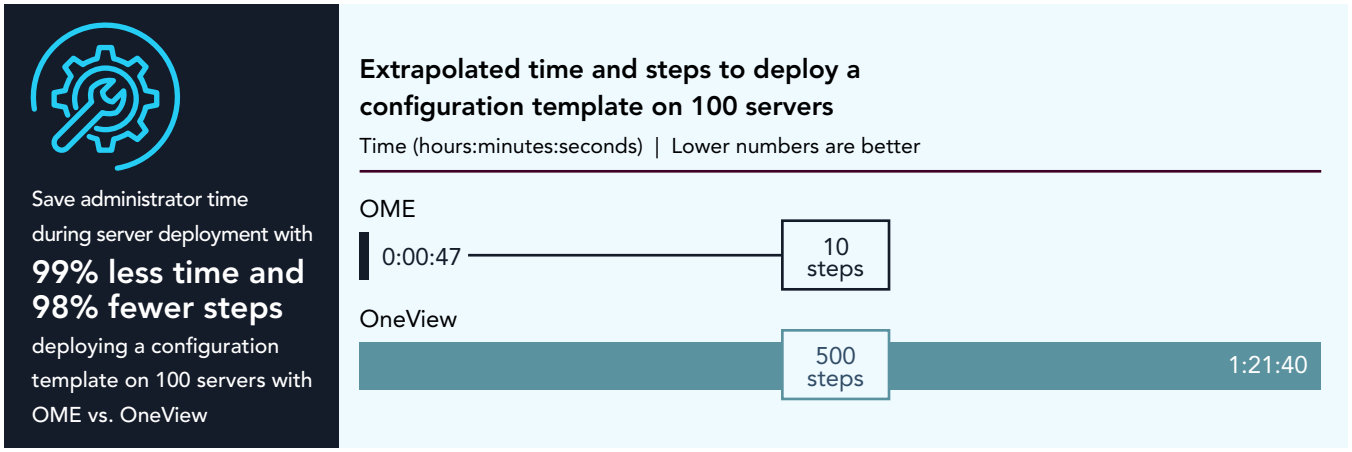

Figure 5 : Comparaison du temps et des étapes de déploiement des modèles de configuration avec OME et OneView. OME peut appliquer un modèle à de nombreux serveurs en même temps, ce qui augmente encore davantage les gains de temps. Moins de temps et moins d'étapes pour plus d'efficacité. Source : Principled Technologies.

Configuration simplifiée des alertes

OME offre davantage d'options pour la surveillance d'une infrastructure. OME permet aux utilisateurs de configurer des stratégies d'alerte une seule fois, puis de les attribuer automatiquement pour les alertes futures. Nous avons créé une règle d'alerte qui déclencherait un arrêt normal en 13 étapes et 65 secondes si le système recevait d'iDRAC9 un avertissement concernant un niveau de température critique. Même si le processus de configuration unique pour l'automatisation des alertes prend plus de temps (1 minute 5 secondes) que l'utilisation de OneView (36 secondes et 5 étapes), OneView ne dispose d'aucune option automatisée pour les alertes. Les administrateurs doivent donc exécuter des actions manuellement à chaque fois. En d'autres termes, pour un déploiement de 100 serveurs, l'utilisation d'OME permettrait d'économiser jusqu'à 98 % de temps et 97 % d'étapes par rapport à OneView en automatisant les actions en fonction des alertes après la création d'une règle.

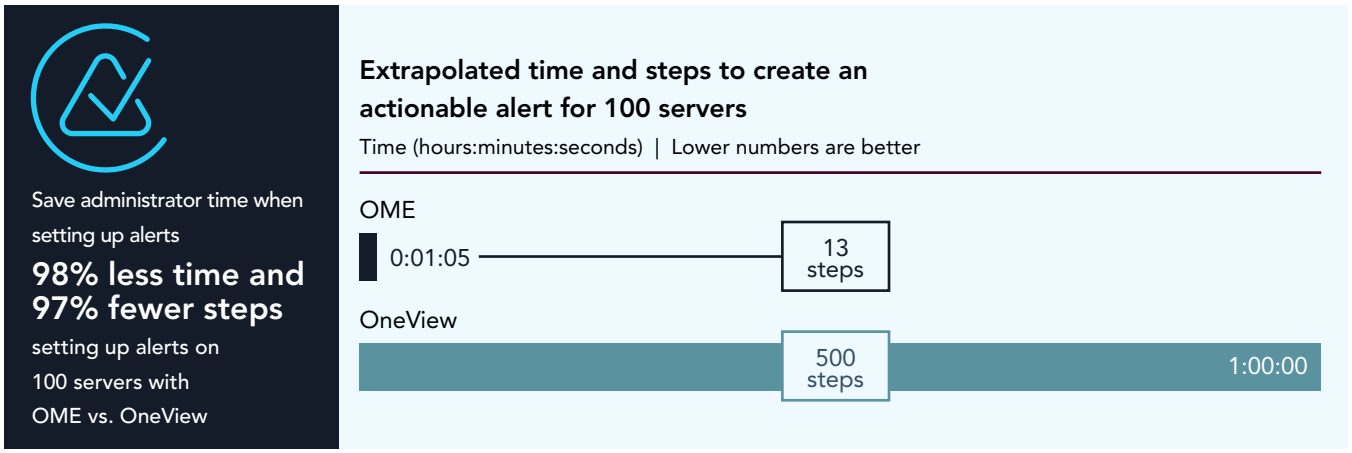

Figure 6 : Comparaison du temps et des étapes de configuration des alertes avec OME par rapport à OneView. OME automatise les alertes après une seule configuration, ce qui permet aux administrateurs d'économiser du temps et des efforts. Moins de temps et moins d'étapes pour plus d'efficacité. Source : Principled Technologies.

À propos de Dell Technologies OpenManage Enterprise

OME est une console de gestion de systèmes « un-à-plusieurs » conçue pour le datacenter et d'autres environnements. La console offre une interface utilisateur graphique HTML5 moderne et se déploie en tant qu'appliance virtuelle pour les environnements VMware ESXi™, Microsoft Hyper-V et de machine virtuelle basée sur le noyau (KVM). OME assure la gestion complète du cycle de vie des serveurs Dell PowerEdge, et peut détecter et inventorier jusqu'à 8 000 appareils sur les réseaux IPv4 et IPv6, notamment les serveurs rack Dell, les serveurs tour Dell, ainsi que les serveurs lames et boîtiers Dell.[6] Dans une récente étude PT, nous avons constaté qu'un environnement Dell avec OME et OpenManage Enterprise Modular (OME-M) peut faire gagner du temps lors de la modification des VLAN et éviter les interventions lors des mises à jour planifiées du firmware.[7]

Pour en savoir plus sur OME, accédez à https://www.dell.com/en-us/lp/dt/open-manage-enterprise.

Gestion à distance

Les fonctionnalités de gestion à distance donnent aux administrateurs la liberté d'apporter davantage de modifications en dehors du datacenter. Nous avons constaté que iDRAC9 offre 1,5 fois plus de fonctionnalités de console à distance HTML5 que iLO 6, avec 10 fonctionnalités totales comparées à seulement 4, ce qui rend la gestion à distance des serveurs avec iDRAC9 facile et efficace. IDRAC9 offre également 16 fois plus de fonctionnalités de configuration du BIOS que iLO 6 (51 fonctionnalités contre seulement 3 fonctionnalités), ce qui offre aux administrateurs un contrôle plus granulaire sur la configuration du BIOS (voir Figure 7 et Figure 8).

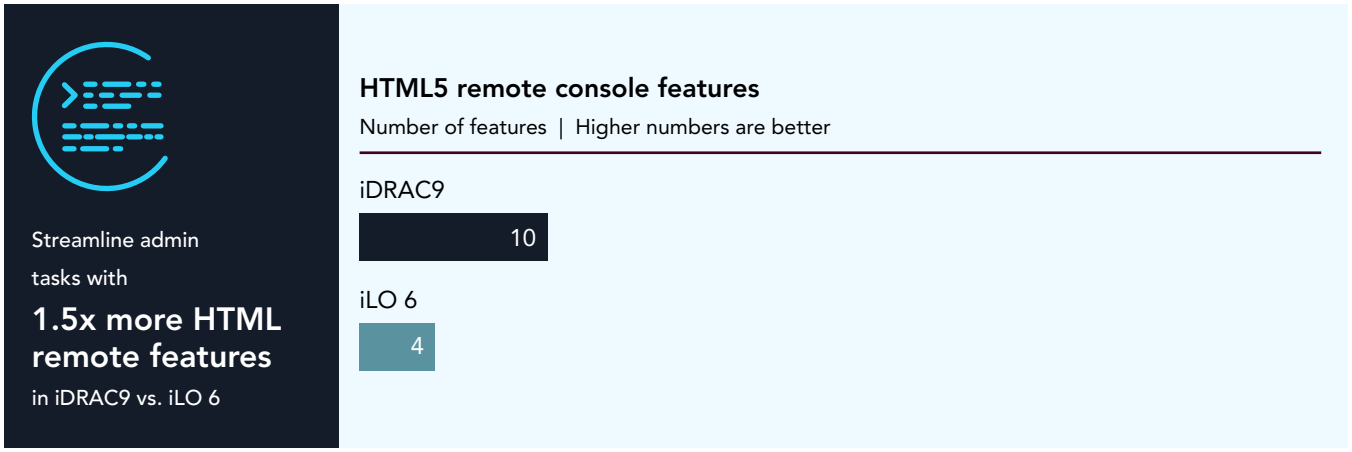

Figure 7 : Comparaison des fonctionnalités HTML5 distantes offertes par chaque outil de gestion. Un plus grand nombre de fonctionnalités offre plus d'efficacité. Source : Principled Technologies.

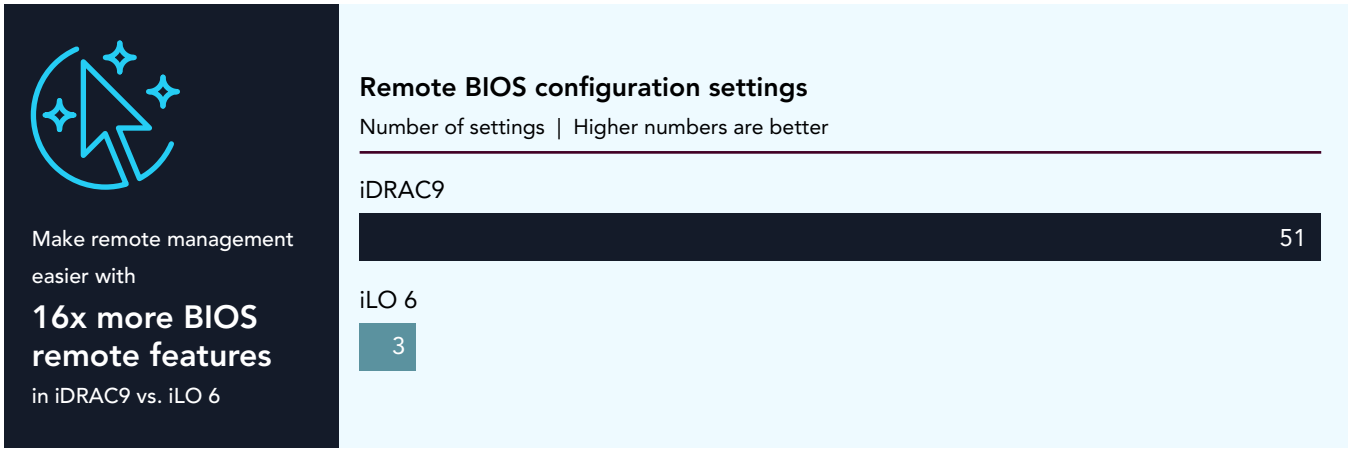

Figure 8 : Comparaison des fonctionnalités du BIOS distantes offertes par chaque outil de gestion. Un plus grand nombre de fonctionnalités offre plus d'efficacité. Source : Principled Technologies.

Apporter des modifications à la configuration du BIOS

Avec iDRAC9, les administrateurs peuvent modifier les paramètres de configuration du BIOS et mettre en place la mise à jour pour un redémarrage ultérieur sans nécessiter la présence de l'administrateur, tandis que iLO 6 requiert des modifications à partir des utilitaires système et une intervention manuelle de l'administrateur lors du changement. Comme le montre la Figure 9, le fait de planifier le changement de configuration du BIOS pour un redémarrage planifié a permis de gagner 87 % de temps et de réduire de moitié le nombre d'étapes avec iDRAC9 par rapport à iLO 6. Ces gains de temps par serveur peuvent se traduire par un gain de temps plus important pour l'administrateur dans les déploiements de plus grande envergure. Par exemple, dans un déploiement de 100 serveurs, vous pouvez gagner plus de 6 heures. IDRAC9 et iLO 6 nécessitent tous deux des modifications individuelles de configuration du BIOS par serveur.

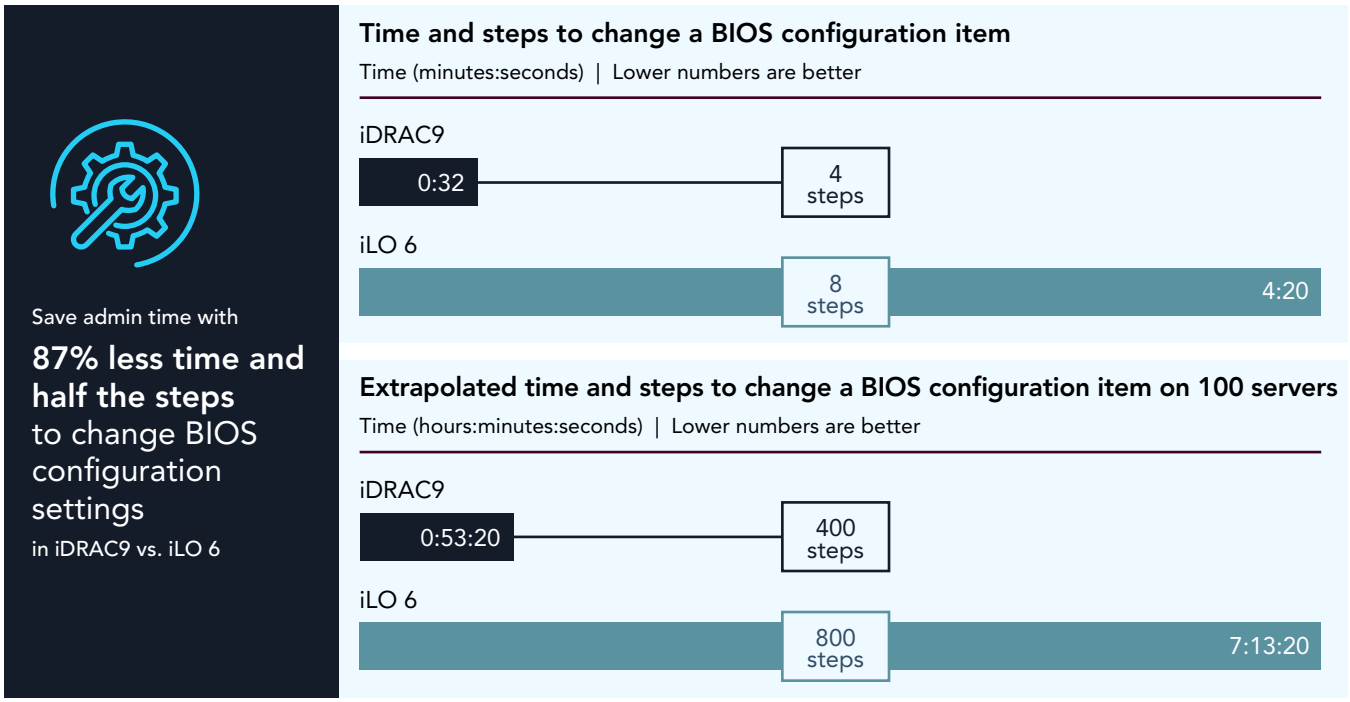

Figure 9 : Temps nécessaire pour modifier les paramètres de configuration du BIOS et organiser la mise à jour en vue d'un redémarrage ultérieur pour un seul serveur, avec extrapolation de la durée nécessaire pour 100 serveurs. Moins de temps et moins d'étapes pour plus d'efficacité. Source : Principled Technologies.

À propos de Dell Technologies Integrated Dell Remote Access Controller 9

Les serveurs Dell PowerEdge™ comprennent IDRAC9 avec Dell Lifecycle Controller pour fournir des fonctions d'administration de systèmes qui incluent des alertes système et des fonctionnalités de gestion à distance. Selon Dell, les principaux avantages de iDRAC9 sont les suivants :

- Gestion de milliers de serveurs à l'aide d'API et d'outils de script
- Prise en charge intégrée, offrant une vue de l'intégrité et de l'état des serveurs avec une surveillance de plusieurs milliers de paramètres
- Télémétrie et automatisation
- Puissantes fonctionnalités et options de sécurité[8]

Pour en savoir plus sur les fonctionnalités fournies par iDRAC9, rendez-vous sur https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Améliorer la sécurité, la durabilité et l'efficacité des administrateurs avec APEX AIOps Infrastructure Observability (anciennement CloudIQ)

APEX AIOps Infrastructure Observability (anciennement CloudIQ) offre aux administrateurs un moyen de surveiller, de gérer et d'analyser les performances sur l'ensemble des déploiements de l'infrastructure Dell PowerEdge, y compris les serveurs, le stockage, etc. Apex AIOps Infrastructure Observability (anciennement CloudIQ) offre plusieurs fonctionnalités de sécurité qui peuvent renforcer votre organisation contre les attaques. Certaines de ces fonctionnalités sont mises en évidence dans le Tableau 5.

Tableau 5 : Présentation des principales fonctionnalités de sécurité disponibles dans APEX AIOps Infrastructure Observability (anciennement CloudIQ). Source : Principled Technologies.

Fonctionnalité	Comment fonctionne APEX AIOps Infrastructure Observability (anciennement CloudIQ) pour sécuriser votre environnement ?
Alertes de niveaux de risque de cybersécurité	Fournit des informations fréquentes sur la cybersécurité avec des alertes de niveau de risque de sécurité spécifiques afin que les administrateurs puissent réagir plus vite et résoudre les problèmes rapidement afin de protéger leurs données.
Configuration de la sécurité basée sur des règles	Propose des paramètres de configuration de la sécurité basés sur des règles et des modèles faciles à appliquer qui permettent à un administrateur de s'assurer que les paramètres des pratiques d'excellence en matière de sécurité sont en place, protégeant ainsi l'environnement PowerEdge.
Conseils en cybersécurité	Fournit des rapports de conseils de sécurité pertinents apportant des détails spécifiques sur la vulnérabilité et des suggestions de mesures correctives, permettant ainsi d'agir rapidement pour combler les failles de sécurité.

En utilisant ces fonctionnalités de surveillance de la sécurité à partir du Cloud, APEX AIOps Infrastructure Observability (anciennement CloudIQ) offre aux administrateurs un autre moyen automatisé et facile à utiliser de contrôler l'intégrité et la sécurité de leur infrastructure.

Fonctionnalités supplémentaires de développement durable et d'efficacité dans APEX AIOps Infrastructure Observability (anciennement CloudIQ)

APEX AIOps Infrastructure Observability (anciennement CloudIQ) offre des fonctionnalités conviviales supplémentaires qui s'intègrent à iDRAC9 et à OME et permettent aux administrateurs d'observer plus facilement l'état de leur environnement PowerEdge et de prendre des mesures si nécessaire. En voici quelques-unes :

- **Analyse de l'empreinte carbone** : cet outil, accessible depuis la section Monitoring, permet d'obtenir une vision plus globale et de mieux prévoir l'utilisation des émissions de carbone dans tous les environnements.
- **Vues de performance :** APEX AIOps Infrastructure Observability (anciennement CloudIQ) fournit des vues de performance et des graphiques d'anomalies et d'utilisation pour alerter les administrateurs dès les premiers signes de problèmes.
- **Rapports d'inventaire et de performances personnalisables :** APEX AIOps Infrastructure Observability (anciennement CloudIQ) fournit des options de création de rapports personnalisées pour les données de performances et d'inventaire des serveurs, qui permettent aux administrateurs de mieux contrôler les performances et les mesures des appareils qu'ils souhaitent suivre.

À propos d'APEX AIOps Infrastructure Observability (anciennement CloudIQ)

Apex AIOps Infrastructure Observability (anciennement CloudIQ) est un outil AIOps basé sur le Cloud offrant une surveillance proactive, un apprentissage automatique et une analytique prédictive pour un grand nombre de produits et services Dell, y compris les serveurs, le stockage, les appliances de protection des données et l'infrastructure hyperconvergée.[9] Une étude réalisée en 2022 par Principled technologies a montré qu'APEX AIOps Infrastructure Observability (anciennement CloudIQ) avait un impact négligeable sur la bande passante réseau, tout en permettant de surveiller la télémétrie, l'état d'intégrité, les alertes et l'inventaire à partir d'une seule et même console.[10] Pour en savoir plus sur APEX AIOps Infrastructure Observability (anciennement CloudIQ), accédez à https://www.dell.com/en-us/dt/apex/aiops.htm.

À l'issue des tests, Dell a publié de nouvelles fonctionnalités qui permettent aux administrateurs d'effectuer des **mises à jour système** à partir d'APEX AIOps Infrastructure Observability (anciennement CloudIQ). Selon la documentation Dell, la page des mises à jour système comporte jusqu'à cinq catégories disponibles pour les mises à jour du système : stockage, gestion de réseau, HCI, protection des données et serveur. Même si nous n'avons pas testé cette fonctionnalité pour le moment, nous prévoyons de la valider dans un article ultérieur.[11]

Conclusion

À chaque fois que vous achetez du matériel, vous bénéficiez également de la gamme d'outils de gestion proposés par le fournisseur de matériel pour gérer et surveiller votre infrastructure. Les spécifications sont importantes, tout comme la sécurité de bout en bout, la réalisation des objectifs de développement durable et la possibilité de rationaliser les tâches de l'administrateur. Dans notre datacenter, nous avons comparé les caractéristiques et fonctionnalités des outils de gestion de serveurs de Dell et de HPE, en comparant iDRAC9 à iLO 6 pour la gestion intégrée des serveurs, et OME à OneView pour la gestion et la surveillance des appareils et des consoles un-à-plusieurs.

Dans les domaines de la sécurité, du développement durable et des fonctionnalités de gestion/surveillance, nous avons constaté que les outils de gestion de serveurs Dell avaient davantage à offrir que les outils HPE comparables : ils offrent aux administrateurs un plus grand nombre d'options de gestion à distance, réduisent le temps de verrouillage des systèmes et offrent un contrôle plus granulaire pour atteindre les objectifs de développement durable. En utilisant la gamme de gestion Dell, vous pouvez réduire le temps et les efforts engagés par les administrateurs pour effectuer certaines tâches courantes de surveillance et de maintenance, et libérer ainsi du temps à votre équipe pour innover et soutenir d'autres initiatives.

---

1. Harvard Business Review, « The Devastating Business Impacts of a Cyber Breach », consulté le 10 avril 2024, https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.
2. Remarque : Cette méthode sur HPE iLO 6 arrête tous les ports USB externes, pas seulement les ports avant.
3. Dell, « OpenManage Enterprise 4.0.x Support Matrix », consulté le 19 avril 2024, https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix.
4. HPE, « HPE OneView 8.7 Support Matrix », consulté le 19 avril 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 Support Matrix », consulté le 19 avril 2024, https://www.dell.com/support/kbdoc/en-us/000217909/openmanage-enterprise-4-0-support-matrix.
6. Dell, « OpenManage Enterprise », consulté le 9 avril 2024, https://www.dell.com/en-us/work/learn/openmanage-enterprise.
7. Principled Technologies, « A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators », consulté le 9 avril 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.

8. Dell, « Integrated Dell Remote Access Controller (iDRAC) », consulté le 9 avril 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.
9. Dell, « APEX AIOps: Tame IT Complexity in your digital business », consulté le 10 juin 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 », consulté le 9 avril 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.
11. Dell, « System Updates », consulté le 19 avril 2024, https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/system-updates-2/.

Consultez les données scientifiques qui sous-tendent ce rapport

Consultez la version en anglais d'origine de ce rapport

Principled Technologies®

Facts matter.®

Ce projet a été réalisé à la demande de Dell Technologies.