Renforcez la sécurité avec

3,5 fois plus de fonctions de sécurité

Dont l'authentification → deux facteurs et la gestion des clés externes avec l'iDRAC9

Efficacité énergétique optimisée avec plus de

6 fois la consommation électrique rapportée

Avec 20 rapports dans Dell OME contre 3 rapports dans Supermicro SSM

Plus d'efficacité opérationnelle avec 1 h 50 de temps d'administration en moins

pour 100 serveurs

Utilisation des mises → jour automatiques avec Dell iDRAC9 ; mises → jour automatiques non disponibles avec Supermicro IPMI

Améliorez la sécurité, la durabilité et l'efficacité grâce aux outils robustes de gestion des serveurs Dell

Par rapport à la gamme de gestion Supermicro

En investissant dans de nouveaux serveurs pour votre datacenter, vous ne vous contentez pas de sélectionner du matériel, mais vous choisissez également une solution de facilité de gestion. Lorsque vos administrateurs disposent d'outils efficaces et riches en fonctionnalités pour déployer, surveiller, entretenir et sécuriser votre infrastructure tout en améliorant son efficacité énergétique, la gestion quotidienne est plus simple et ils peuvent consacrer plus de temps aux innovations qui font avancer votre organisation. En choisissant d'acheter auprès d'un fournisseur disposant d'outils de gestion robustes, vous pouvez gagner du temps et de l'argent.

Nous avons évalué les gammes de gestion de serveurs de Dell™ et Supermicro® en comparant trois outils Dell à deux outils Supermicro.

Tableau 1 : Les outils de gestion que nous avons testés. *Dell CloudIQ est un outil de surveillance et d'analytique basé sur le Cloud ; Supermicro n'offre aucun outil équivalent.
Source : Principled Technologies.

	Dell	Supermicro
Gestion intégrée/à distance des serveurs	iDRAC 9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
Console de gestion des appareils (un-à-plusieurs)	Dell OpenManage™ Enterprise (OME) Dell CloudIQ*	Supermicro Server Manager (SSM)

En matière de durabilité, de sécurité et de gestion au quotidien, nous avons constaté que Dell fournit toujours des ensembles d'outils plus riches en fonctionnalités qui offrent aux administrateurs davantage d'options et de possibilités.

Fonctionnalités plus nombreuses et plus variées pour automatiser et faciliter la gestion de votre serveur

Vos équipes IT ont besoin d'outils de gestion modernes et riches en fonctionnalités qui leur permettent de gagner du temps dans leur travail quotidien tout en respectant les normes de sécurité et d'efficacité. Les outils de gestion Dell que nous avons évalués incluent un certain nombre de fonctionnalités qui ne sont pas présentes dans la gamme de gestion Supermicro.

Développement durable

Face à l'augmentation des coûts énergétiques et à la multiplication des réglementations environnementales, de nombreuses organisations mettent l'accent sur le développement durable. Par nature, les datacenters nécessitent de grandes quantités d'énergie, mais une gestion prudente de la consommation thermique et électrique peut permettre aux organisations de réduire la quantité d'énergie qu'elles consomment. Dell OpenManage Enterprise intègre plusieurs fonctionnalités qui permettent de surveiller et de gérer étroitement la consommation électrique, vous aidant 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 en matière de durabilité entre Dell OpenManage Enterprise et SSM. Source : Principled Technologies.

Fonctionnalité	Outils de gestion Dell	Outils de gestion Supermicro
Calculateur d'utilisation des émissions de carbone et outil de planification de la capacité	✓	x
Analyse de l'empreinte carbone	✓	x
Politique de gestion de l'alimentation à déclenchement thermique	✓	x
Stratégie de gestion de l'alimentation statique	✓	✓

Tableau 3 : Récapitulatif de notre comparaison entre Dell OME et Supermicro SSM et IPMI. Source : Principled Technologies.

Fonctionnalité	Avantages clés des outils de gestion Dell	Inconvénients des outils de gestion Supermicro
Calculateur d'utilisation des émissions de carbone et outil de planification de la capacité	Capacité d'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** ; il est difficile de planifier pour vous aider à atteindre vos objectifs de développement durable
Analyse de l'empreinte carbone	**Disponible** via OpenManage Enterprise Power Manager ; fournit des données sur les émissions de carbone, ce qui peut vous aider à atteindre vos objectifs de développement durable	**Aucune fonctionnalité comparable** ; aucun moyen de suivre l'empreinte carbone pour vous aider à atteindre vos objectifs de développement durable
Alimentation automatisée et gestion thermique	Options de **stratégies statiques et à déclenchement thermique**, avec possibilité de déclenchement lorsque le serveur franchit un seuil de consommation d'énergie ou de température	**Un seul type de stratégie statique** sans options de déclencheur associées
Rapports de consommation électrique	**Plus de 6 fois** plus de rapports, avec **20 rapports intégrés** avec des options de distribution planifiée par e-mail et de personnalisation	**2 rapports intégrés** dans SSM ; 1 rapport dans Supermicro IPMI, non exportable
Métriques de gestion de l'alimentation	Jusqu'à **15 fois plus de métriques**, avec des informations plus granulaires sur la gestion de la consommation électrique	**Une seule métrique**, qui donne moins de visibilité et de contrôle sur la consommation d'énergie

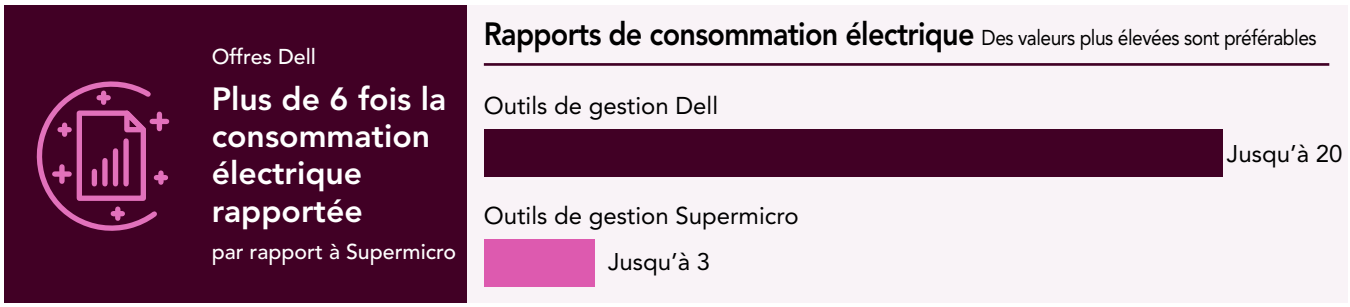

Figure 1 : Nombre de rapports de consommation électrique disponibles dans Dell OME et Supermicro SSM. Source : Principled Technologies.

Figure 2 : Nombre de métriques de gestion de l'alimentation disponibles dans Dell OME et Supermicro SSM. Source : Principled Technologies.

Alimentation automatisée et gestion thermique

OpenManage Enterprise Power Manager offre une gestion automatisée de l'alimentation et de la température via des options de stratégie déclenchées par la température et l'alimentation statique qui permettent aux administrateurs de définir des limites de consommation électrique ou des seuils de température afin de réduire les coûts de refroidissement. SSM dispose d'une seule stratégie, à savoir une limite statique de consommation électrique qui n'est pas déclenchée automatiquement lorsqu'un serveur dépasse la limite, ce qui peut entraîner une hausse des coûts énergétiques.

Les organisations souhaitant bénéficier d'analyses approfondies de la consommation électrique de leur datacenter dans un souci d'optimisation peuvent tirer parti des **20 rapports intégrés sur la consommation électrique** proposés par OpenManage Enterprise Power Manager. Ces rapports sont utiles pour planifier la capacité et gérer l'alimentation afin d'optimiser l'efficacité. Les options relatives aux rapports dans SSM sont beaucoup plus limitées. Les administrateurs ne peuvent exécuter qu'un seul hôte avec un rapport de service ou voir une tendance de la consommation électrique dans l'écran de surveillance. Avec Supermicro IPMI, les utilisateurs peuvent afficher un graphique d'alimentation au niveau des composants dans le BMC. Toutefois, ils ne peuvent pas exporter les données du graphique pour analyse et ne peuvent les enregistrer qu'en tant qu'image.

Le plug-in OpenManage Enterprise Power Manager permet aux administrateurs de **consulter jusqu'à 15 métriques différentes**, notamment sur la consommation d'énergie pour chaque composant, le flux d'air et l'utilisation des composants, tandis que SSM ne fournit que la consommation d'énergie totale.

Émissions de carbone et analyse de l'empreinte carbone

OME inclut un calculateur d'utilisation des émissions de carbone et un outil de planification de la capacité qui, entre autres fonctions, peuvent vous aider à estimer vos propres émissions de gaz à effet de serre. La solution fournit des valeurs par défaut pour les coûts d'alimentation et les émissions de carbone pour une unité d'énergie consommée, mais vous pouvez personnaliser ces valeurs pour les coûts d'alimentation de votre propre région et le modèle de consommation de votre datacenter. SSM n'offre aucune fonctionnalité comparable, ce qui peut compliquer la planification et le suivi de la progression vers les objectifs de développement durable.

Sécurité

La cybercriminalité augmente de façon exponentielle, menaçant les entreprises de « dommages et destruction de données, vol d'argent, perte de productivité, vol de propriété intellectuelle, vol de données personnelles et financières, détournement de fonds, fraude, interruption post-attaque du cours normal des affaires, investigation scientifique, restauration et suppression des données et systèmes piratés, et atteinte à la réputation ».[1] Dans un tel contexte, les décideurs doivent prendre en compte la sécurité dans tout achat de serveurs. Dell OpenManage Enterprise intègre plusieurs fonctionnalités vous aidant à protéger vos données, que les outils Supermicro n'ont pas (voir tableaux 4 et 5).

Tableau 4 : Différences de sécurité entre les outils de gestion Dell et les outils de gestion Supermicro. Source : Principled Technologies.

Fonctionnalité	Outils de gestion Dell	Outils de gestion Supermicro
Authentification multifacteur	✓	x
Gestion des clés externe	✓	x
Contrôle d'accès basé sur le périmètre	✓	x
Configuration de la sécurité basée sur les stratégies	✓	x
Conseils en matière de cybersécurité	✓	x
Contrôle d'accès basé sur les rôles	✓	✓
Désactivation dynamique des ports USB	✓	✓

Tableau 5 : Résumé du rapport sur les fonctionnalités de sécurité comparant les outils de gestion de Dell et de Supermicro. Source : Principled Technologies.

Fonctionnalité	Avantages clés des outils de gestion Dell	Inconvénients des outils de gestion Supermicro
Authentication multifacteur (MFA)	**Authentification à deux facteurs** avec l'iDRAC avec **e-mail et RSA SecurID**, empêchant les utilisateurs non autorisés d'accéder aux données sensibles	**Aucune fonctionnalité comparable**, ce qui entraîne une faille de sécurité permettant aux utilisateurs non autorisés d'accéder aux données sensibles
Gestion des clés externe	**Secure Enterprise Key Manager** dans l'iDRAC pour ajouter une autre couche de sécurité afin de protéger les données au repos sur les serveurs en utilisant le chiffrement des lecteurs et une gestion centralisée	**Aucune fonctionnalité comparable**, ce qui entraîne une autre faille de sécurité
Contrôles d'accès	OME offre **à la fois** un contrôle d'accès basé sur les rôles **(RBAC)** et un contrôle d'accès basé sur le périmètre **(SBAC)** pour limiter les groupes d'appareils auxquels le gestionnaire de périphériques a accès	**RBAC uniquement**, ce qui limite la capacité des administrateurs à restreindre l'accès
Configuration de la sécurité basée sur les stratégies	Paramètres de **configuration de la sécurité basée sur les stratégies** via CloudIQ, qui alerte les administrateurs en cas d'incohérences	**Aucune fonctionnalité comparable**, ce qui peut retarder la prise de mesures et la correction des violations
Conseils en matière de cybersécurité	**Rapports sur les conseils de sécurité** via la sécurité Dell CloudIQ, avec des détails sur les failles de sécurité et des suggestions de mesures correctives applicables pour permettre une action rapide	**Aucune fonctionnalité comparable**, ce qui entraîne des failles de sécurité que les acteurs malveillants peuvent exploiter

Authentification multifacteur

L'authentification multifacteur (MFA) peut aider à empêcher les utilisateurs non autorisés et les acteurs malveillants d'accéder aux données sensibles. Dell iDRAC permet une authentification à deux facteurs à la fois avec la messagerie électronique et RSA SecurID, un ensemble de technologies d'authentification multifacteur externe utilisées dans de nombreux secteurs.[2] Ni IPMI ni SSM de Supermicro n'offrent cette fonctionnalité, ce qui entraîne une faille de sécurité.

Gestion des clés

Les systèmes de gestion des clés externes (KMS) permettent aux équipes IT d'utiliser un serveur tiers distinct pour gérer les clés qu'elles utilisent pour verrouiller et déverrouiller le stockage d'un serveur, ajoutant ainsi une couche de sécurité. L'iDRAC inclut le gestionnaire de clés locales (LKM) pour tous les nouveaux serveurs Dell PowerEdge. Certaines licences offrent également Secure Enterprise Key Manager (SEKM), qui permet une sécurité supplémentaire avec le chiffrement complet du disque et la gestion des clés externes. SEKM prend en charge le protocole standard KMIP OASIS, qui permet aux organisations de choisir n'importe quel fournisseur KMS externe ayant recours à cette norme. Supermicro n'offre pas cette fonctionnalité de sécurité ou un équivalent.

Contrôles d'accès

Le contrôle d'accès basé sur les rôles (RBAC), où le rôle d'un utilisateur détermine les parties du système auxquelles il a accès et les tâches qu'il peut effectuer sur ces parties, est un élément essentiel de nombreuses stratégies de sécurité des serveurs. Dans OpenManage Enterprise, RBAC définit les privilèges des utilisateurs pour trois rôles intégrés : Administrateur, Gestionnaire d'appareils et Observateur.[3] Il offre également un contrôle d'accès basé sur le périmètre (SBAC), qui permet aux administrateurs de limiter les groupes d'appareils auxquels un gestionnaire d'appareils a accès.[4] Cela permet aux administrateurs de fournir un accès à un sous-ensemble d'appareils. Supermicro propose RBAC, mais pas SBAC.

Gestion des informations d'identification

La rotation des mots de passe dans l'iDRAC a plusieurs objectifs : faire tourner l'accès à OpenManage Enterprise conformément à la stratégie de sécurité, avec une valeur mensuelle par défaut ; elle fonctionne avec un gestionnaire de mot de passe externe ; et elle prend en charge CyberArk pour gérer les mots de passe[5,6]

Avec OpenManage Enterprise, les administrateurs peuvent gérer la rotation des mots de passe iDRAC en remplaçant le besoin d'un compte administrateur statique connu par un compte de service géré par OME. SSM ne dispose pas de cette fonctionnalité.

Configuration de la sécurité basée sur les stratégies

Dell propose une fonctionnalité de cybersécurité basée sur les stratégies dans la solution CloudIQ pour PowerEdge AIOps. Cette fonctionnalité compare la configuration d'un serveur PowerEdge déployé à une politique de configuration liée à la sécurité basée sur les pratiques d'excellence Dell. Si CloudIQ détecte une divergence, l'administrateur en est informé et des étapes de correction sont fournies.[7] SSM n'offre aucune fonctionnalité équivalente, ce qui peut entraîner des retards dans la détection des violations.

Conseils en matière de cybersécurité

Des conseils de sécurité informent le public des problèmes de sécurité. Selon Dell, la page Conseils de sécurité Dell dans CloudIQ fournit une liste complète des conseils de sécurité applicables, ainsi que leur impact, le nombre de systèmes qu'ils concernent et la date de publication.[8] Rapports de conseils de sécurité Dell CloudIQ avec des détails sur les failles de sécurité et des suggestions de mesures correctives. SSM n'offre pas de fonctionnalité similaire, laissant les systèmes vulnérables.

À propos de Dell CloudIQ

Dell 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] Dans une étude réalisée par Principled Technologies en 2022, nous avons constaté que CloudIQ avait un impact négligeable sur la bande passante du réseau tout en nous permettant de surveiller la télémétrie, l'état de santé, les alertes et l'inventaire à partir d'une console unique.[10]

En savoir plus sur CloudIQ sur https://www.dell.com/en-us/dt/solutions/cloudiq.htm.

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, ce qui permet d'éviter les utilisations malveillantes et d'introduire le risque d'installation d'applications interdites ou de virus.

Dell iDRAC offre une désactivation indépendante et dynamique des ports USB sans interruption de service. Bien que Supermicro propose une désactivation dynamique du port USB avant (et du port USB arrière) dans le BIOS, la clé de licence Supermicro DataCenter Management Suite par nœud est nécessaire pour l'activer. L'équipe IT peut la déclencher en implémentant la commande de verrouillage du système, qui peut être exécutée à partir du BMC ou de la console Supermicro IPMI, mais elle n'est pas indépendante du mode de verrouillage du système.[11]

Comme le montre la Figure 3, la désactivation des ports à l'aide de Dell iDRAC est un processus simple qui **ne nécessite que 41 secondes et 4 étapes**, tandis qu'IPMI de Supermicro prend **plus de quatre fois plus de temps, soit 2 minutes 50 secondes et 6 étapes**. Si on l'extrapole à 100 systèmes, on obtient un gain de temps de 3 h 35 min, ce qui signifie qu'un administrateur passe près de la moitié d'une journée de travail à utiliser Supermicro IPMI, contre un peu plus d'une heure à utiliser Dell iDRAC.

Figure 3 : Temps nécessaire pour désactiver les ports USB avant d'un seul serveur et temps extrapolé nécessaire pour désactiver les ports USB avant de 100 serveurs.
Des valeurs basses sont préférables. Source : Principled Technologies.

À propos de Dell OpenManage Enterprise

OpenManage Enterprise est une console de gestion de systèmes « un-à-plusieurs » pour datacenter. 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 KVM (Kernel-based Virtual Machine). OpenManage Enterprise peut découvrir et inventorier sur les réseaux IPV4 et IPV6 jusqu'à 8 000 appareils, y compris les serveurs au format rack Dell, les serveurs tour Dell et les pales et boîtiers Dell.[12] Dans une étude récente de PT, nous avons constaté qu'un environnement Dell doté d'OpenManage Enterprise et d'OpenManage Enterprise Modular (OME-M) permet de gagner du temps lors de la modification des VLAN et d'éviter les interventions lors des mises à jour programmées du firmware.[13]

Pour en savoir plus sur OpenManage Enterprise, rendez-vous sur https://www.dell.com/en-us/lp/dt/open-manage-enterprise

Surveillance, analytique et facilité d'utilisation

Les outils de gestion varient considérablement en ce qui concerne l'aide qu'ils apportent aux administrateurs qui effectuent des activités de surveillance et d'analytique, ainsi que d'autres tâches de routine, telles que la planification des mises à jour. Dans cette section, nous examinons les différences en la matière entre les outils de gestion Dell et Supermicro que nous avons étudiés. Comme nous l'avons constaté lorsque nous avons analysé les fonctionnalités de développement durable et de sécurité, la suite d'outils de gestion Dell offre de nombreuses fonctionnalités qui facilitent la vie des administrateurs, que les outils Supermicro n'ont pas. Le Tableau 6 compare les avantages offerts par ces outils en matière de gestion.

Tableau 6 : Résumé du rapport comparant les outils de gestion de Dell et de Supermicro. Source : Principled Technologies.

Fonctionnalité	Avantages clés des outils de gestion Dell	Inconvénients des outils de gestion Supermicro
Télémétrie en streaming	**Télémétrie en streaming** iDRAC9 **disponible** sur les serveurs syslog distants ; permet de prévoir les pannes et d'optimiser les performances ; peut envoyer les métriques de serveur à des outils d'analytique tels que Grafana et Splunk	**Pas de télémétrie en streaming automatique**
Gestion et surveillance mobile	Application OpenManage Mobile pour iOS et Android riche en fonctionnalités, qui s'intègre à OME et iDRAC9	Application Supermicro IPMIView, qui **ne s'intègre pas** à SSM
Surveillance des appareils et serveurs tiers	OME **prend en charge la surveillance des appareils et des serveurs tiers**, y compris de ses principaux concurrents	**Ne prend en charge que les appareils tiers qui utilisent ses agents**, ses BMC, les versions antérieures de ses équipements compatibles avec IPMI et les appareils compatibles avec Redfish
Gestion du parc	Disponible via OME et CloudIQ ; OME peut transmettre des données sur des serveurs gérés sous licence à CloudIQ pour la surveillance de plusieurs datacenters	**Pas de portail basé sur le Cloud** pour agréger les données de surveillance entre les datacenters
Actions basées sur des alertes	Stratégies dans OME qui déclenchent des actions en fonction des entrées d'une alerte	**Aucune action basée sur des alertes disponible**
Déploiement de serveur simplifié (possibilité d'importer/exporter des configurations système)	Peut utiliser l'iDRAC 9 pour **importer/exporter** tous les éléments de configuration pour les serveurs, ce qui ne nécessite que **48 s et 5 étapes pour l'importation et 1 min 9 s et 7 étapes pour l'exportation**	Peut importer/exporter **uniquement la configuration de base du Baseboard Management Controller (BMC)**, nécessitant une configuration manuelle significative pour chaque serveur
Moins de temps pour modifier les paramètres de configuration du BIOS	Possibilité de modifier rapidement les **paramètres complets du BIOS directement à partir de l'iDRAC** et de planifier la mise à jour et le redémarrage pour une fenêtre de maintenance, ce qui permet de gagner un temps considérable en termes d'administration	**Modifications du BIOS disponibles mais limitées** à partir du BMC, sinon le redémarrage du serveur est requis ; nécessite plus d'étapes manuelles et de temps d'administration
S'exécute sous forme d'appliance virtuelle	**Disponible** dans OME, ce qui élimine la nécessité de mettre à jour le système d'exploitation	**Aucune fonctionnalité comparable**, doit s'exécuter dans un système d'exploitation géré. Les administrateurs ont un composant de plus à corriger et à mettre à jour
Affichage des connexions	**Disponible** dans l'iDRAC ; outil de dépannage utilisant LLDP pour diagnostiquer les problèmes de réseau tels que le câblage, les ports de commutateur défectueux, etc.	**Pas d'affichage des connexions**, aucune information sur la connectivité physique des ports de commutateur en amont
Possibilité de planifier les mises à jour du firmware et des pilotes	**Disponible** dans OME et iDRAC	Possibilité de planifier les mises à jour du BIOS et du firmware du BMC, mais **impossibilité de planifier les mises à jour des pilotes**

Modification des éléments de configuration du BIOS

Dell offre la possibilité de modifier les paramètres de configuration du BIOS directement à partir de l'iDRAC, avec la possibilité de mettre en place ces modifications pour le prochain redémarrage. Supermicro propose un ensemble limité de paramètres de configuration du BIOS à partir de son BMC. En plus de ces paramètres limités, la modification d'un seul élément de configuration du BIOS sur les serveurs Supermicro exige que l'administrateur redémarre le serveur pour accéder au menu de configuration du BIOS à partir de l'écran de démarrage.

La Figure 4 illustre le temps nécessaire pour effectuer une modification de la configuration du BIOS sur un seul serveur à l'aide de Dell iDRAC et de Supermicro IPMI. Le processus manuel à l'aide de l'**outil Supermicro prend 2 minutes et 6 secondes supplémentaires**, soit **4,9 fois plus de temps** que la configuration du processus automatisé dans l'iDRAC. Si nous extrapolons ces temps à 100 serveurs configurés de manière identique, le gain de temps avec l'iDRAC serait de 3,5 heures. (Si les serveurs n'étaient pas configurés de manière identique, nous ne verrions pas ces gains de temps.)

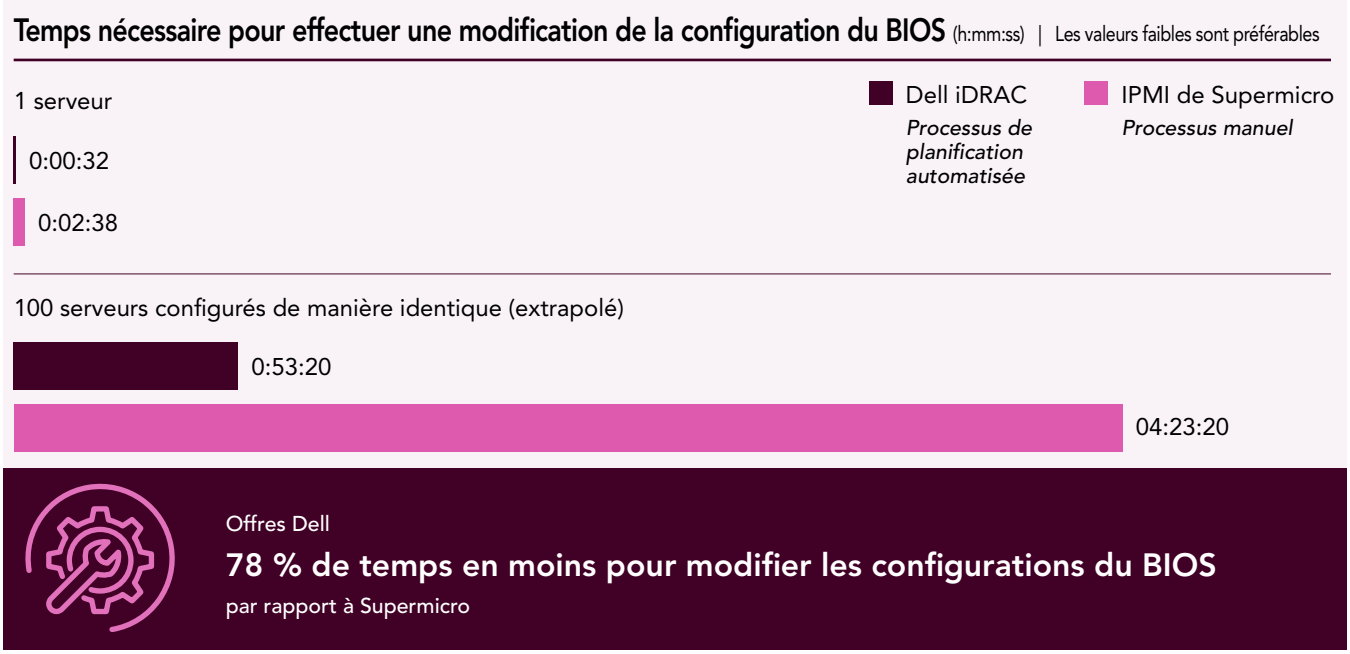

Figure 4 : Durée nécessaire pour modifier la configuration du BIOS sur un seul serveur et sur 100 serveurs configurés de manière identique (extrapolé).
Des valeurs basses sont préférables. Source : Principled Technologies.

À propos de iDRAC9

Les serveurs Dell PowerEdge™ incluent Integrated Dell Remote Access Controller 9 avec Dell Lifecycle Controller pour fournir des fonctions d'administration des systèmes qui incluent des alertes système et des fonctionnalités de gestion à distance. Selon Dell, les principaux avantages de l'iDRAC9 sont les suivants :

- Gestion de milliers de serveurs à l'aide d'API et d'outils de script
- Support intégré, offrant une vue de la santé et de l'état du serveur et surveillant des milliers de paramètres
- Puissantes fonctionnalités et options de sécurité[14]

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

Mises à jour automatisées du firmware et des pilotes

iDRAC

Contrairement à Supermicro IPMI, Dell iDRAC vous permet de planifier des mises à jour automatiques du firmware. Cela signifie que la configuration des mises à jour automatiques selon un planning est une tâche ponctuelle qui permet de gagner du temps à chaque cycle de mise à jour. La Figure 5 illustre le temps extrapolé pour planifier les mises à jour automatiques du firmware pour la première fois pour 100 serveurs utilisant Dell iDRAC et Supermicro IPMI. Le processus manuel à l'aide de l'outil Supermicro prend **13 minutes supplémentaires** par rapport à la configuration du processus automatisé dans l'iDRAC.

En supposant qu'un administrateur configure un planning mensuel le premier samedi soir de chaque mois, un administrateur utilisant l'iDRAC investit 58 secondes par serveur, et ce une seule fois. Pour 100 serveurs, cela représente 1 h 36 min 40 s pour une configuration unique. En comparaison, un administrateur utilisant Supermicro IPMI investit 1 h 50 min pour 100 serveurs à chaque fenêtre de maintenance. Si nous comparons la configuration ponctuelle de l'iDRAC et la première des nombreuses configurations de Supermicro IPMI, l'outil de gestion Dell permet de gagner environ 13 minutes et 20 secondes. (Voir Figure 5)

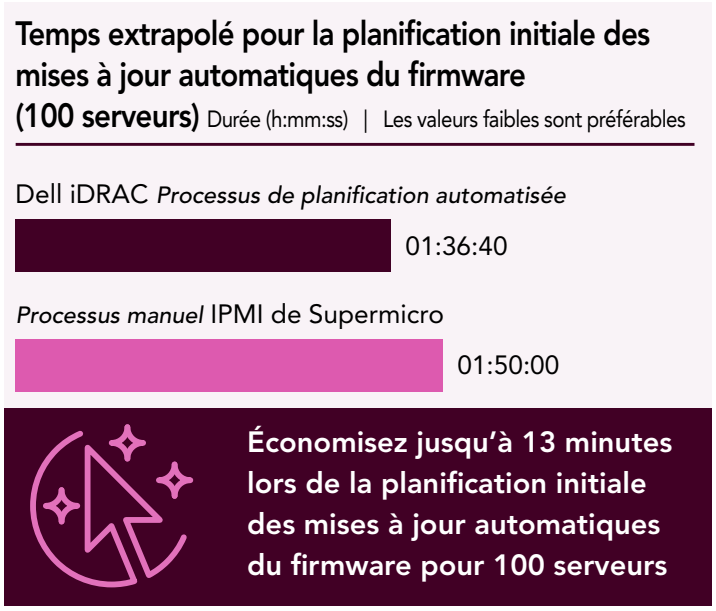

Figure 5 : Temps extrapolé pour mettre à jour le firmware sur 100 serveurs la première fois. Des valeurs basses sont préférables. Source : Principled Technologies.

Toutefois, la deuxième fois, et chaque fois suivante, **Dell permet d'économiser 110 minutes, car l'administrateur n'a plus besoin d'effectuer la tâche**. (Voir Figure 6) Ce gain de temps se vérifie même si les 100 serveurs ne sont pas configurés de manière identique. Ces durées incluent uniquement le téléchargement du firmware sur le BMC et ne reflètent pas les durées de téléchargement et d'extraction du firmware Supermicro.

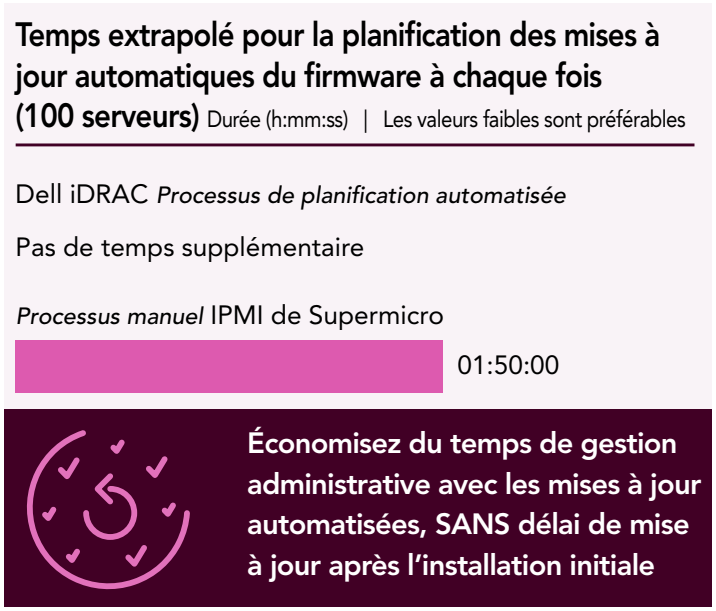

Figure 6 : Temps extrapolé pour mettre à jour le firmware sur 100 serveurs à chaque fois. Des valeurs basses sont préférables. Source : Principled Technologies.

OME

Dell OME prend en charge les **mises à jour du firmware pour tous les composants** et les mises à jour des pilotes Windows. SSM prend en charge la mise à jour du firmware du BIOS et du BMC, mais **pas les mises à jour des pilotes ou les mises à jour d'autres composants**.

Conclusion

Choisir un fournisseur pour les achats de serveurs ne se limite pas à la plateforme matérielle. Les décideurs doivent également prendre en compte des aspects à plus long terme, notamment la sécurité des systèmes/des données, l'efficacité énergétique et la facilité de gestion. C'est pourquoi les outils de gestion des systèmes proposés par un fournisseur sont tout aussi importants que le matériel.

Nous avons étudié les fonctionnalités et les capacités des outils de gestion de serveurs Dell et Supermicro, en comparant Dell iDRAC 9 à Supermicro IPMI pour la gestion intégrée des serveurs et Dell OpenManage Enterprise et CloudIQ à Supermicro Server Manager pour la gestion et la surveillance des appareils et des consoles un-à-plusieurs. Nous avons constaté que les outils de gestion Dell offraient des fonctionnalités et des capacités de sécurité, de durabilité et de gestion/surveillance plus complètes que celles des serveurs Supermicro. En outre, les outils Dell automatisent davantage de tâches pour faciliter la gestion des serveurs, ce qui permet aux administrateurs de gagner beaucoup de temps au lieu d'avoir à effectuer manuellement les mêmes tâches avec les outils Supermicro.

Lors de l'achat d'un serveur, les produits de gestion associés d'un fournisseur sont essentiels pour protéger les données, permettre un environnement plus durable et faciliter la maintenance des systèmes. Nos tests et nos recherches ont montré que la gamme de solutions de gestion Dell pour les serveurs PowerEdge offrait davantage de fonctionnalités pour aider les organisations à atteindre ces objectifs que les produits de gestion Supermicro comparables.

1. Steve Morgan, « Cybercrime To Cost The World $10.5 Trillion Annually By 2025 », consulté le 15 février 2024, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
2. Dell, « Using iDRAC9 RSA SecurID 2FA », consulté le 15 février 2024, https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-securid-2fa.pdf.
3. Dell, « Guide de l'utilisateur de Dell EMC OpenManage Enterprise SupportAssist Version 1.1 », consulté le 15 février 2024, https://www.dell.com/support/manuals/en-us/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?.
4. Dell, « Guide de l'utilisateur de Dell EMC OpenManage Enterprise SupportAssist version 1.1 »
5. Dell, « OpenManage Enterprise 4.0 : gestion et rotation des mots de passe iDRAC », consulté le 15 février 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 », consulté le 3 avril 2024, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf.
7. Mark Maclean et Kyle Shannon, « Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation », consulté le 15 février 2024, https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/.
8. Dell, « Security Advisories », consulté le 15 février 2024, https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/.
9. Dell, « Dell CloudIQ - AIOps for Intelligent IT Infrastructure Insights », consulté le 15 février 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 », consulté le 17 janvier 2024, https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf.
11. Supermicro, « X13DEM User's Manual » consulté le 16 février 2024, https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf.
12. Dell, « OpenManage Enterprise », consulté le 20 décembre 2023, https://www.dell.com/en-us/work/learn/openmanage-enterprise.
13. Principled Technologies, « A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators », consulté le 17 janvier 2024, https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf.
14. « Integrated Dell Remote Access Controller (iDRAC) », consulté le 16 janvier 2024, https://www.dell.com/en-us/lp/dt/open-manage-idrac.

Consultez les données scientifiques qui sous-tendent ce rapport ▶

Principled Technologies®

Facts matter.®

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