



Fortaleça a segurança com
**3,5x mais recursos
de segurança**

*Inclusive a autenticação de dois
fatores e o gerenciamento de
chaves externas do iDRAC9*



Otimize a eficiência
energética com mais de
**6x a quantidade
de relatórios
de consumo de
energia**

*Com 20 relatórios no Dell OME
e 3 relatórios no Supermicro
SSM*



**Aumente a eficiência
operacional
economizando 1
hora e 50 minutos
do tempo dos
administradores**

para cada 100 servidores

*Usando atualizações
automáticas do Dell iDRAC9,
em comparação com nenhuma
atualização automática
disponível no Supermicro IPMI*

Aumente a segurança, a sustentabilidade e a eficiência com as sólidas ferramentas de gerenciamento de servidores da Dell

Em comparação com o portfólio de gerenciamento da Supermicro

Ao investir em novos servidores para o datacenter, você não está apenas selecionando hardware, mas também está escolhendo uma solução de gerenciamento. Com ferramentas eficientes e repletas de recursos disponíveis para implementar, monitorar, manter e proteger a infraestrutura, enquanto aprimoram a eficiência no consumo de energia, os administradores podem lidar facilmente com o gerenciamento diário e dedicar mais tempo para inovações que impulsionam a organização. Ao optar por comprar de um fornecedor com sólidas ferramentas de gerenciamento, você pode economizar tempo e dinheiro.

Nós avaliamos os portfólios de gerenciamento de servidores da Dell™ e da Supermicro®, comparando três ferramentas da Dell com duas ferramentas da Supermicro.

Tabela 1: As ferramentas de gerenciamento que testamos. *Dell CloudIQ é uma ferramenta de lógica analítica e monitoramento em nuvem; a Supermicro não oferece uma ferramenta equivalente.

Fonte: Principled Technologies.

	Dell	Supermicro
Gerenciamento remoto/integrado de servidores	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
Console de gerenciamento de dispositivos de um para muitos	Dell OpenManage™ Enterprise (OME) Dell CloudIQ*	Supermicro Server Manager (SSM)

Em termos de sustentabilidade, segurança e experiência diária de gerenciamento, constatamos que a Dell sempre ofereceu conjuntos de ferramentas com mais recursos para capacitar os administradores com mais opções e funcionalidades.

Recursos numerosos e mais avançados para automatizar e facilitar o gerenciamento de servidores

As equipes de TI precisam de ferramentas modernas de gerenciamento, repletas de recursos, que acelerem o trabalho diário e acompanhem os padrões de segurança e eficiência. As ferramentas de gerenciamento da Dell que avaliamos incluem vários recursos e funcionalidades que não estão presentes no portfólio de gerenciamento da Supermicro.

Sustentabilidade

À medida que os custos de energia vão aumentando e as normas ambientais vão se intensificando, muitas organizações estão tornando a sustentabilidade uma prioridade. Os datacenters exigem inerentemente grandes quantidades de energia, mas o gerenciamento cuidadoso do consumo de energia e temperatura pode permitir que as organizações reduzam esse consumo. O Dell OpenManage Enterprise incorpora vários recursos que podem permitir o monitoramento e o gerenciamento rigorosos do consumo de energia, o que ajuda você a atingir suas metas de sustentabilidade. As Tabelas 2 e 3 destacam os principais benefícios desses recursos, que nós descrevemos em mais detalhes abaixo.

Tabela 2: Diferenças de sustentabilidade entre o Dell OpenManage Enterprise e o SSM. Fonte: Principled Technologies.

Recurso	Ferramentas de gerenciamento da Dell		Ferramentas de gerenciamento da Supermicro	
Ferramenta de planejamento de capacidade e calculadora de emissões de carbono		✓		x
Análise da pegada de carbono		✓		x
Política de gerenciamento de energia acionada por temperatura		✓		x
Política de gerenciamento estático de energia		✓		✓

Tabela 3: Resumo da comparação entre o Dell OME e o Supermicro SSM e IPMI. Fonte: Principled Technologies.

Recurso	Principais benefícios das ferramentas de gerenciamento da Dell	Desvantagem das ferramentas de gerenciamento da Supermicro
 Ferramenta de planejamento de capacidade e calculadora de emissões de carbono	Capacidade de estimar as emissões de gases do efeito estufa com valores personalizáveis para ajudar você a atingir as metas de sustentabilidade	Nenhum recurso equivalente; dificulta o planejamento a fim de atingir as metas de sustentabilidade
 Análise da pegada de carbono	Disponível por meio do OpenManage Enterprise Power Manager; apresenta dados sobre emissões de carbono, que podem ajudar você a atingir as metas de sustentabilidade	Nenhum recurso equivalente; não há como monitorar a pegada de carbono para ajudar você a avaliar o progresso em relação às metas de sustentabilidade
 Gerenciamento automatizado de temperatura e energia	Opções de políticas estáticas e acionadas por temperatura, com a opção de acionamento quando o servidor ultrapassar um limite de consumo de energia ou de temperatura	Um tipo de política estática sem opções associadas de acionamento
 Relatórios de consumo de energia	Mais de 6x o número de relatórios, sendo 20 relatórios integrados com opções de personalização e distribuição agendada de e-mails	2 relatórios integrados no SSM; 1 relatório no Supermicro IPMI que não pode ser exportado
 Métricas de gerenciamento de energia	Número até 15x maior de métricas , apresentando informações mais específicas sobre o gerenciamento do consumo de energia	Apenas 1 métrica , apresentando menos insights e menos controle do consumo de energia

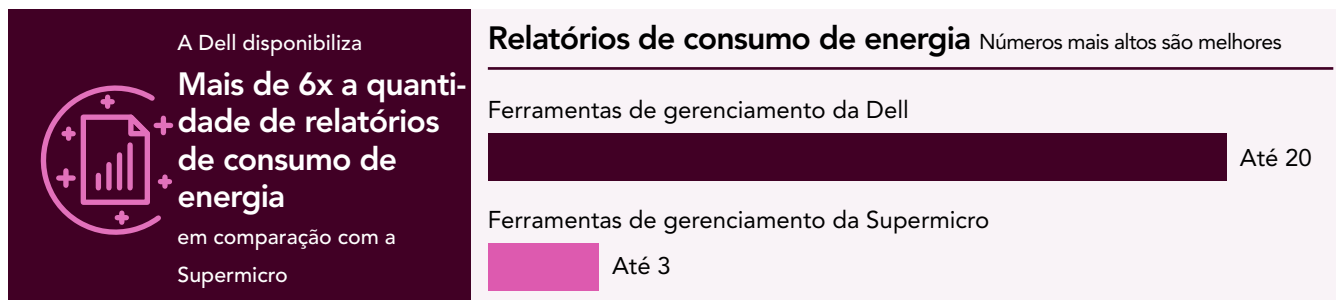


Figura 1: Número de relatórios de consumo de energia disponíveis no Dell OME e no Supermicro SSM. Fonte: Principled Technologies.

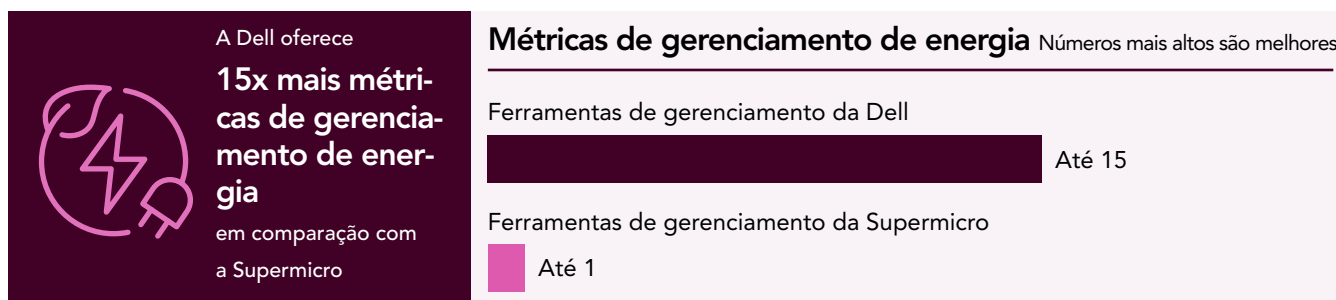


Figura 2: Número de métricas de gerenciamento de energia disponíveis no Dell OME e no Supermicro SSM. Fonte: Principled Technologies.

Gerenciamento automatizado de temperatura e energia

O OpenManage Enterprise Power Manager oferece gerenciamento automatizado de energia e temperatura por meio de opções de políticas estáticas, acionadas por energia e temperatura. Essas políticas permitem que os administradores definam limites de consumo de energia ou de temperatura para ajudar a reduzir os custos de resfriamento. Em contrapartida, o SSM tem uma só política, com um limite fixo de consumo de energia que não é acionado automaticamente quando o servidor ultrapassa esse limite, o que pode levar a um aumento nos custos de energia.

As organizações que buscam uma análise aprofundada sobre o consumo de energia dos datacenters, com foco na otimização, podem se beneficiar dos **20 diferentes relatórios integrados sobre consumo de energia** que o OpenManage Enterprise Power Manager oferece. Esses relatórios são úteis para o planejamento de capacidade e o gerenciamento de energia a fim de maximizar a eficiência. As opções de relatórios no SSM são muito mais limitadas. Os administradores podem executar somente um só host com um relatório de serviço ou ver uma tendência de consumo de energia na tela de monitoramento. Com o Supermicro IPMI, os usuários podem visualizar um gráfico de energia em nível de componente no BMC. No entanto, eles não podem exportar os dados do gráfico para análise e só podem salvá-los como imagem.

O plug-in OpenManage Enterprise Power Manager permite que os administradores **visualizem até 15 métricas diferentes**, inclusive de uso de energia por componentes individuais, fluxo de ar e utilização de componentes, enquanto o SSM oferece apenas a métrica de uso total de energia.

Análise das emissões e da pegada de carbono

O OME inclui uma ferramenta de planejamento de capacidade e uma calculadora de emissões de carbono que, entre outras funções, podem ajudar você a estimar suas próprias emissões de gases do efeito estufa. Ele apresenta valores padrão para custos de energia e emissões de carbono para uma unidade de energia consumida, mas permite que você personalize esses valores de acordo com os custos de energia da sua própria região e o modelo de consumo de seu próprio datacenter. O SSM não oferece nenhum recurso equivalente, o que torna difícil para as organizações planejar e monitorar o progresso em relação às metas de sustentabilidade.

Segurança

O crime cibernético está aumentando exponencialmente e ameaçando as empresas com "danos e destruição de dados, roubo de dinheiro, perda de produtividade, roubo de propriedade intelectual, roubo de dados pessoais e financeiros, desfalque, fraude, interrupção pós-ataque até o andamento normal dos negócios, investigação forense, restauração e exclusão de dados e sistemas invadidos e danos à reputação".¹ Nesse cenário, os tomadores de decisões devem considerar a segurança em qualquer compra de servidor. Constatamos que o Dell OpenManage Enterprise apresenta vários recursos para ajudar a manter os dados seguros que não estão disponíveis nas ferramentas da Supermicro (consulte as Tabelas 4 e 5).

Tabela 4: Diferenças na segurança entre as ferramentas de gerenciamento da Dell e as ferramentas de gerenciamento da Supermicro. Fonte: Principled Technologies.

Recurso	Ferramentas de gerenciamento da Dell	Ferramentas de gerenciamento da Supermicro
Autenticação baseada em vários fatores	✓	x
Gerenciamento de chaves externas	✓	x
Controles de acesso com base no escopo	✓	x
Configuração de segurança com base em políticas	✓	x
Aconselhamentos de segurança cibernética	✓	x
Controles de acesso baseados em função	✓	✓
Desativação dinâmica de portas USB	✓	✓

Tabela 5: Resumo da comparação de recursos de segurança entre as ferramentas de gerenciamento da Dell e as da Supermicro. Fonte: Principled Technologies.

Recurso	Principais benefícios das ferramentas de gerenciamento da Dell	Desvantagem das ferramentas de gerenciamento da Supermicro
 Autenticação baseada em vários fatores (MFA)	Autenticação de dois fatores por meio do iDRAC, com e-mail e RSA SecurID , impedindo que usuários não autorizados obtenham acesso a dados confidenciais	Nenhum recurso equivalente , deixando uma lacuna de segurança que pode auxiliar usuários não autorizados a obter acesso a dados confidenciais
 Gerenciamento de chaves externas	Secure Enterprise Key Manager no iDRAC para adicionar outra camada de segurança para proteger os dados em repouso nos servidores usando criptografia de unidade e gerenciamento centralizado	Nenhum recurso equivalente , deixando outra lacuna na segurança
 Controles de acesso	O OME oferece controle de acesso baseado em função (RBAC) e controle de acesso baseado em escopo (SBAC) para limitar os grupos de dispositivos aos quais um gerenciador de dispositivos tem acesso	Somente RBAC , limitando a capacidade dos administradores de restringir o acesso
 Configuração de segurança com base em políticas	Configurações de segurança baseadas em políticas por meio do CloudIQ, para alertar os administradores sobre discrepâncias	Nenhum recurso equivalente , o que pode atrasar a tomada de medidas e a reparação de violações
 Aconselhamentos de segurança cibernética	Relatórios de consultoria de segurança por meio da segurança do Dell CloudIQ, com detalhes de vulnerabilidade e sugestões de reparação aplicáveis para permitir uma ação rápida	Nenhum recurso equivalente , deixando brechas de segurança para os agentes mal-intencionados explorarem

Autenticação baseada em vários fatores

A autenticação baseada em vários fatores (MFA) pode ajudar a impedir que usuários não autorizados e agentes mal-intencionados obtenham acesso a dados confidenciais. Verificamos que o Dell iDRAC permite a autenticação de dois fatores com e-mail e com RSA SecurID, um conjunto de tecnologias externas de autenticação baseada em vários fatores, usado em diversos setores.² Também verificamos que o Supermicro IPMI e o Supermicro SSM não oferecem esse recurso, deixando uma lacuna de segurança.

Gerenciamento de chaves

Os sistemas de gerenciamento externo de chaves (KMS) permitem que as equipes de TI recorram a um servidor separado de terceiros para gerenciar as chaves usadas para bloquear e desbloquear o armazenamento de um servidor, adicionando uma camada de segurança. O iDRAC inclui o Local Key Manager (LKM) em todos os novos servidores Dell PowerEdge. Algumas licenças também oferecem o Secure Enterprise Key Manager (SEKM), adicionando uma camada extra de segurança com criptografia completa de discos e gerenciamento externo de chaves. O SEKM tem compatibilidade com o protocolo OASIS KMIP padrão do setor, permitindo que as organizações escolham qualquer provedor de KMS externo que utilize esse padrão. As ferramentas da Supermicro não oferecem esse recurso de segurança, nem um equivalente.

Controles de acesso

O controle de acesso baseado em função (RBAC), no qual a função de um usuário determina as partes do sistema às quais ele tem acesso e as tarefas que ele pode executar, é um componente integrante de muitas estratégias de segurança de servidor. No OpenManage Enterprise, o RBAC define os privilégios de usuário para três funções integradas: administrador, gerenciador de dispositivos e visualizador.³ Ele também oferece o controle de acesso baseado em escopo (SBAC), que permite que os administradores limitem os grupos de dispositivos aos quais um gerenciador de dispositivos tem acesso.⁴ Com isso,

os administradores conseguem oferecer acesso a um subconjunto de dispositivos. As ferramentas da Supermicro oferecem o RBAC, mas não o SBAC.

Gerenciamento de credenciais

A rotação de senhas do iDRAC tem várias finalidades: ela rotaciona o acesso ao OpenManage Enterprise de acordo com a política de segurança, com um padrão mensal; ela funciona com um manipulador de senhas externas; e tem compatibilidade com a ferramenta CyberArk para gerenciar senhas.^{5,6}

Com o OpenManage Enterprise, os administradores podem gerenciar a rotação de senhas do iDRAC, substituindo a necessidade de uma conta de administrador estática e conhecida por uma conta de serviço gerenciada pelo OME. O SSM não tem esse recurso.

Configuração de segurança com base em políticas

A Dell oferece o recurso de segurança cibernética baseado em políticas na solução CloudIQ para PowerEdge AIOps. Esse recurso usa a configuração de um servidor PowerEdge implementado e a compara com uma política de configuração relacionada à segurança, de acordo com as práticas recomendadas da Dell. Se o CloudIQ detectar uma discrepância, ele notificará o administrador e informará as etapas para correção.⁷ O SSM não oferece nenhum recurso equivalente, o que pode significar atrasos na detecção de violações.

Aconselhamentos de segurança cibernética

Os aconselhamentos de segurança notificam o público sobre problemas de segurança. De acordo com a Dell, a página "Dell Security Advisories" do CloudIQ apresenta uma lista completa dos aconselhamentos de segurança aplicáveis, juntamente com os respectivos impactos, o número de sistemas afetados e a data de publicação.⁸ O Dell CloudIQ disponibiliza relatórios de aconselhamentos de segurança com detalhes sobre vulnerabilidades e sugestões de correção. O SSM não oferece um recurso equivalente, o que pode deixar os sistemas vulneráveis.

Sobre o Dell CloudIQ

O Dell CloudIQ é uma ferramenta de AIOps em nuvem que oferece "monitoramento proativo, aprendizado de máquina e análise preditiva" a muitos produtos e serviços da Dell, inclusive servidores, armazenamento, equipamentos de proteção de dados e infraestrutura hiperconvergente.⁹ Em um estudo da Principled Technologies de 2022, nós constatamos que o CloudIQ causava um impacto insignificante sobre a largura de banda da rede e, ao mesmo tempo, nos permitia monitorar a telemetria, o status de integridade, os alertas e o inventário em um só console.¹⁰

Saiba mais sobre o CloudIQ, em <https://www.dell.com/pt-br/dt/apex/aiops.htm#tab0=0>.

Desativação dinâmica de portas USB

A opção de ativar e desativar portas USB permite que os administradores controlem o acesso ao servidor por uma porta USB, evitando assim o uso mal-intencionado, e introduz o risco de instalação de aplicativos proibidos ou vírus.

O Dell iDRAC oferece a desativação dinâmica e independente de portas USB, sem tempo de inatividade. Embora as ofertas da Supermicro permitam a desativação dinâmica de USB frontal (e USB traseira) no BIOS, elas exigem a chave de licença do Supermicro DataCenter Management Suite per Node para ativar esse recurso. A equipe de TI pode acionar esse recurso implementando o comando de bloqueio do sistema, que pode ser executado no BMC ou no console do Supermicro IPMI, mas ele não é independente do modo de bloqueio do sistema.¹¹

Como mostra a Figura 3, a desativação das portas usando o Dell iDRAC foi um processo simples, **exigindo apenas 41 segundos e 4 etapas**. Já no Supermicro IPMI, esse processo demorou **cerca de quatro vezes mais, ou seja, 2 minutos e 50 segundos e 6 etapas**. Aplicando o método de extrapolação para 100 sistemas, a economia de tempo pode aumentar para 3 horas e 35 minutos. Isto é, um administrador pode gastar quase metade de um dia de trabalho para realizar esse processo usando o Supermicro IPMI e um pouco mais de uma hora usando o Dell iDRAC.



Figura 3: Tempo para desativar as portas USB frontais de um só servidor e tempo extrapolado para desativar as portas USB frontais de 100 servidores. Quanto menos, melhor. Fonte: Principled Technologies.

Sobre o Dell OpenManage Enterprise

O OpenManage Enterprise é um console de gerenciamento de sistemas de um para muitos voltado para o data center. O console oferece uma moderna interface gráfica do usuário HTML5 e é implementado como um Virtual Appliance para ambientes VMware ESXi™, Microsoft Hyper-V e de máquinas virtuais com base em Kernel (KVM). O OpenManage Enterprise pode detectar e inventariar até 8.000 dispositivos em redes IPv4 e IPv6, inclusive servidores em rack Dell, servidores em torre Dell e blades e chassis Dell.¹² Em um recente estudo da PT, nós constatamos que um ambiente Dell com o OpenManage Enterprise e o OpenManage Enterprise Modular (OME-M) pode economizar tempo na realização de alterações nas VLANs e evitar intervenções durante atualizações agendadas de firmware.¹³

Saiba mais sobre o OpenManage Enterprise, em <https://www.dell.com/pt-br/lp/dt/open-manage-enterprise>

Monitoramento, análise e facilidade de uso

As ferramentas de gerenciabilidade variam muito em como elas dão suporte aos administradores que realizam atividades de monitoramento e análise, bem como outras tarefas rotineiras, como agendar atualizações. Nesta seção, analisamos as diferenças nessas áreas entre as ferramentas de gerenciamento da Dell e as da Supermicro que estudamos. Conforme constatamos ao analisar os recursos de sustentabilidade e segurança, o conjunto de ferramentas de gerenciamento da Dell oferece várias funcionalidades para facilitar a vida dos administradores que não estão disponíveis nas ferramentas da Supermicro. A Tabela 6 apresenta uma comparação dos benefícios de gerenciamento que as ferramentas oferecem.

Tabela 6: Resumo de nossa comparação entre as ferramentas de gerenciamento da Dell e as da Supermicro. Fonte: Principled Technologies.

Recurso	Principais benefícios das ferramentas de gerenciamento da Dell	Desvantagem das ferramentas de gerenciamento da Supermicro
 Streaming de telemetria	O streaming de telemetria do iDRAC9, disponível para servidores syslog remotos, ajuda a prever falhas e otimizar o desempenho e pode transmitir métricas de servidor para ferramentas de lógica analítica, como Grafana e Splunk	Sem streaming automático de telemetria
 Gerenciamento e monitoramento móveis	Aplicativo OpenManage Mobile repleto de recursos para iOS e Android, que se integra ao OME e ao iDRAC9	Aplicativo Supermicro IPMIView, que não se integra ao SSM
 Monitoramento de dispositivos e servidores de terceiros	O OME oferece suporte ao monitoramento de servidores e dispositivos de terceiros , incluindo o suporte para aos principais concorrentes	Oferece suporte apenas a dispositivos de terceiros que usam os próprios agentes e BMCs, quando as versões anteriores de equipamentos são compatíveis com IPMI e com dispositivos compatíveis com Redfish
 Monitoramento do patrimônio	Disponível via OME e CloudIQ; o OME pode transmitir dados de servidores gerenciados licenciados ao CloudIQ para monitoramento em vários data centers	Nenhum portal baseado em nuvem para agregar dados de monitoramento entre datacenters
 Ações com base em alertas	Políticas no OME que acionam ações com base na entrada de um alerta	Nenhuma ação disponível com base em alertas
 Implementação mais fácil de servidores (capacidade de importar/exportar configurações do sistema)	Pode usar o iDRAC9 para importar/exportar todos os itens de configuração de servidores, exigindo apenas 48 segundos e 5 etapas para importação e 1 minuto e 9 segundos e 7 etapas para exportação	Pode importar/exportar somente a configuração do Baseboard Management Controller (BMC) , exigindo uma configuração manual significativa para cada servidor
 Menos tempo para alterar as configuração do BIOS	Pode alterar com rapidez as configurações completas do BIOS diretamente no iDRAC e preparar a atualização e a reinicialização para uma janela de manutenção, economizando tempo significativo de administração	Alterações limitadas do BIOS disponíveis a partir do BMC. Em outros casos, uma reinicialização do servidor é necessária. Requer mais etapas manuais e mais tempo de administração
 Execução como um equipamento virtual	Disponível no OME, eliminando a necessidade de atualizar o SO	Nenhum recurso equivalente ; a execução deve ser feita em um SO gerenciado. Isso faz com que os administradores tenham mais um componente para aplicar patches e atualizar
 Connection View	Disponível no iDRAC; ferramenta de solução de problemas que usa LLDP para diagnosticar problemas de rede, como cabeamento, portas de switch com defeito e muito mais	Não há Connection View ; nenhuma informação de conectividade física sobre as portas de switch upstream
 Capacidade de agendar atualizações de firmware e driver	Disponível no OME e no iDRAC	Pode agendar atualizações de firmware do BMC e BIOS, mas não pode agendar atualizações de driver

Alteração de itens de configuração do BIOS

A Dell oferece alterações completas de configurações do BIOS diretamente pelo iDRAC, com a capacidade de preparar essas alterações para a próxima reinicialização. A Supermicro oferece um conjunto limitado de configurações do BIOS no BMC. Além do conjunto limitado, uma alteração de um só item de configuração do BIOS em servidores Supermicro requer que o administrador reinicialize o servidor para acessar o menu de configuração do BIOS na tela de inicialização.

A Figura 4 mostra o tempo para realizar uma alteração de configurações do BIOS em um só servidor usando o Dell iDRAC e o Supermicro IPMI. O processo manual ao usar a **ferramenta da Supermicro leva 2 minutos e 6 segundos a mais**, ou **4,9x mais tempo**, do que configurar o processo automatizado no iDRAC. Se aplicarmos o método de extrapolação para 100 servidores configurados de maneira idêntica, a economia de tempo com o iDRAC poderá ser de 3,5 horas. (Se os servidores estiverem configurados de modo diferente, poderemos não ver essas economias de tempo.)

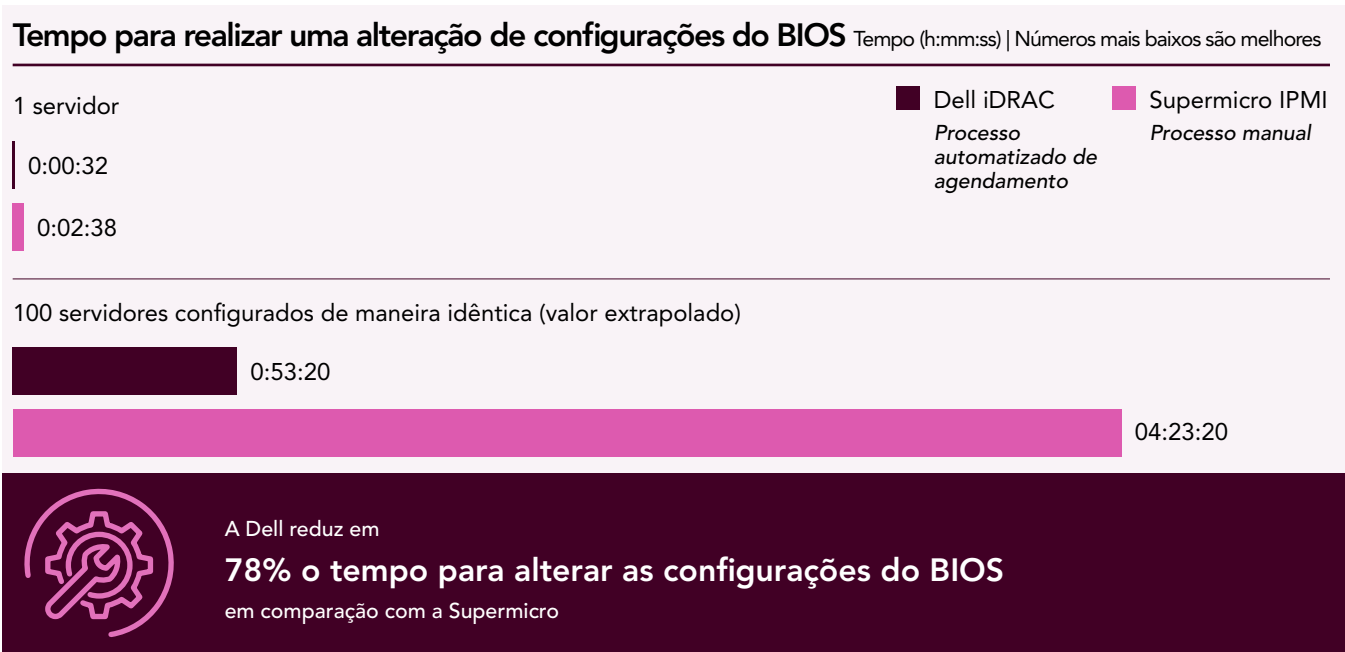


Figura 4: Tempo para realizar uma alteração de configurações do BIOS em um só servidor e em 100 servidores configurados de maneira idêntica (valor extrapolado). Quanto menos, melhor. Fonte: Principled Technologies.

Sobre o iDRAC9

Os servidores Dell PowerEdge™ incluem o Integrated Dell Remote Access Controller 9 com Dell Lifecycle Controller para oferecer funções de administração de sistemas, que incluem alertas do sistema e recursos de gerenciamento remoto. De acordo com a Dell, os principais benefícios do iDRAC9 são:

- A capacidade de gerenciar milhares de servidores usando APIs e ferramentas de script
- Suporte integrado, apresentando uma exibição da integridade do servidor e monitorando o status de milhares de parâmetros
- Sólidos recursos e opções de segurança¹⁴

Para saber mais sobre os recursos que o iDRAC9 oferece, acesse <https://www.dell.com/pt-br/lp/dt/open-manage-idrac>.

Atualizações automatizadas de firmware e driver

iDRAC

Ao contrário do Supermicro IPMI, o Dell iDRAC permite agendar atualizações automáticas de firmware. Isso significa que configurar atualizações automáticas, de acordo com um agendamento, é uma tarefa única que traz economia de tempo em cada ciclo de atualização. A Figura 5 mostra o tempo extrapolado para agendar atualizações automáticas de firmware pela primeira vez, em 100 servidores, usando o Dell iDRAC e o Supermicro IPMI. O processo manual usando a ferramenta da Supermicro leva **13 minutos** a mais do que configurar o processo automatizado no iDRAC.

Se presumirmos que um administrador configura um agendamento mensal na primeira noite de sábado de cada mês, um administrador que usa o iDRAC teria um investimento de tempo único de 58 segundos por servidor. Para 100 servidores, esse tempo chegará a 1 hora, 36 minutos e 40 segundos, como uma configuração única. Em comparação, um administrador que usa o Supermicro IPMI teria um investimento de tempo de 1 hora e 50 minutos para 100 servidores, em cada janela de manutenção. Se compararmos a configuração única do iDRAC com a primeira das várias configurações do Supermicro IPMI, a ferramenta de gerenciamento da Dell economizará cerca de 13 minutos e 20 segundos. (Consulte a Figura 5.)

No entanto, a partir da segunda vez, **a ferramenta da Dell permitirá uma economia de 110 minutos porque o administrador não precisará mais executar a tarefa.** (Consulte a Figura 6.) Essa economia de tempo ocorrerá mesmo se os 100 servidores não estiverem configurados de maneira idêntica. Observe que esses tempos incluem apenas o carregamento do firmware no BMC e não refletem os tempos de download e extração do firmware da Supermicro.

OME

O Dell OME oferece suporte a **atualizações de firmware para todos os componentes** e atualizações de driver do Windows. O SSM oferece suporte a atualizações de firmware do BMC e BIOS, mas **não a atualizações de driver ou de outros componentes.**

Tempo extrapolado para agendar atualizações automáticas de firmware pela primeira vez (100 servidores) Tempo (h:mm:ss) | Números mais baixos são melhores

Dell iDRAC *Processo automatizado de agendamento*



Supermicro IPMI *Processo manual*





Economize até 13 minutos para agendar pela primeira vez atualizações automáticas de firmware para 100 servidores

Figura 5: Tempo extrapolado para atualizar o firmware em 100 servidores pela primeira vez. Quanto menos, melhor. Fonte: Principled Technologies.

Tempo extrapolado para agendar atualizações automáticas de firmware nas próximas vezes (100 servidores) Tempo (h:mm:ss) | Números mais baixos são melhores

Dell iDRAC *Processo automatizado de agendamento*

Sem tempo adicional

Supermicro IPMI *Processo manual*





Economize tempo de administração com atualizações automatizadas, SEM gastar tempo com atualizações após a configuração inicial

Figura 6: O tempo para atualizar o firmware em 100 servidores é extrapolado em todas as tentativas. Quanto menos, melhor. Fonte: Principled Technologies.

Conclusão

Ao escolher um fornecedor para comprar servidores, é preciso considerar muito mais do que só a plataforma de hardware. Os tomadores de decisões também precisam considerar questões de longo prazo, como segurança do sistema/dos dados, eficiência no consumo de energia e facilidade de gerenciamento. Essas questões tornam as ferramentas de gerenciamento de sistemas de um fornecedor tão importantes quanto o hardware.

Nós analisamos os recursos e as capacidades das ferramentas de gerenciamento de servidores da Dell e da Supermicro, comparando o Dell iDRAC9 com o Supermicro IPMI para gerenciamento integrado de servidores e o Dell OpenManage Enterprise e o CloudIQ com o Supermicro Server Manager para gerenciamento e monitoramento de dispositivos e consoles de um para muitos. Constatamos que as ferramentas de gerenciamento da Dell ofereceram recursos e funcionalidades mais abrangentes de segurança, sustentabilidade e gerenciamento/monitoramento do que os servidores da Supermicro. Além disso, as ferramentas da Dell automatizaram mais tarefas para facilitar o gerenciamento de servidores, proporcionando uma economia significativa de tempo aos administradores, em comparação com a necessidade de executar as mesmas tarefas manualmente com as ferramentas da Supermicro.

Ao fazer uma compra de servidor, os produtos de gerenciamento associados de um fornecedor são essenciais para proteger os dados, oferecer suporte a um ambiente mais sustentável e facilitar a manutenção dos sistemas. Nossos testes e pesquisas mostraram que o portfólio de gerenciamento da Dell para servidores PowerEdge ofereceu mais recursos para ajudar as organizações a atingir esses objetivos do que os produtos comparáveis de gerenciamento da Supermicro.

1. Steve Morgan, "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025", acessado em 15 de fevereiro de 2024, <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>.
2. Dell, "Using iDRAC9 RSA SecurID 2FA", acessado em 15 de fevereiro de 2024, <https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-securid-2fa.pdf>.
3. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide", acessado em 15 de fevereiro de 2024, <https://www.dell.com/support/manuals/pt-br/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?>.
4. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide".
5. Dell, "OpenManage Enterprise 4.0: rodízio e gerenciamento de senhas do iDRAC", acessado em 15 de fevereiro de 2024, <https://www.dell.com/support/kbdoc/pt-br/000219279/openmanage-enterprise-4-0-idrac-gerenciamento-de-senha-e-rodizio?lwp=rt>.
6. Dell, "OpenManage Portfolio Software Licensing Guide", acessado em 3 de abril de 2024, <https://www.delltechnologies.com/asset/pt-br/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf>.
7. Mark Maclean e Kyle Shannon, "Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation", acessado em 15 de fevereiro de 2024, <https://infohub.delltechnologies.com/pt-br/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/>.
8. Dell, "Security Advisories", acessado em 15 de fevereiro de 2024, <https://infohub.delltechnologies.com/pt-br/l/dell-apex-aiops-infrastructure-observability-a-detailed-review/security-advisories/>.
9. Dell, "Dell CloudIQ - AIOPS for Intelligent IT Infrastructure Insight", acessado em 15 de fevereiro de 2024, <https://www.dell.com/pt-br/dt/apex/aiops.htm#tab0=0>.
10. Principled Technologies, "Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests", acessado em 17 de janeiro de 2024, <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>.
11. Supermicro, "X13DEM User's Manual", acessado em 16 de fevereiro de 2024, <https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf>.
12. Dell, "OpenManage Enterprise", acessado em 20 de dezembro de 2023, <https://www.dell.com/pt-br/lp/dt/openmanage-enterprise?dgc=SM&cid=243908&lid=spr3470526067&linkId=92952834>.
13. Principled Technologies, "A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators", acessado em 17 de janeiro de 2024, <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>.
14. "Integrated Dell Remote Access Controller (iDRAC)", acessado em 16 de janeiro de 2024, <https://www.dell.com/pt-br/lp/dt/openmanage-idrac>.

Veja a ciência que respalda este relatório



Facts matter.®

Principled Technologies é uma marca registrada da Principled Technologies, Inc. Todos os outros nomes de produtos são marcas comerciais de seus respectivos proprietários. Para obter mais informações, consulte a ciência por trás desse relatório.

Este projeto foi encomendado por Dell Technologies.