DELL Technologies

White paper

White paper técnico: Segurança com resiliência cibernética nos servidores Dell EMC PowerEdge

Dezembro de 2020

Revisões

Data	Descrição
Janeiro de 2018	Versão inicial
Novembro de 2020	Versão revisada

Sumário

Sumário

Sumário Executivo

A abordagem de segurança da Dell Technologies é intrínseca por natureza: é integrada, ou seja, não é adicionada posteriormente e está presente em cada etapa do Ciclo de vida do desenvolvimento de segurança da Dell. Nós nos empenhamos em continuar desenvolvendo os controles, recursos e soluções de segurança do PowerEdge para atender ao ambiente de ameaças crescente e seguimos consolidando a segurança com uma raiz de confiança de silício. Este documento detalha os recursos de segurança integrados à Plataforma com resiliência cibernética do PowerEdge, muitos deles ativados pelo Dell Remote Access Controller (iDRAC9). Muitos recursos novos foram adicionados desde o white paper anterior sobre segurança do PowerEdge e eles abrangem do controle de acesso à criptografia de dados e à garantia da cadeia de suprimentos. Dentre eles: Varredura em tempo real do BIOS, personalização da inicialização segura UEFI, MFA do RSA SecurID, gerenciamento de chaves empresarial seguro (SEKM), verificação de componentes protegidos (SCV), System Erase aprimorado, inscrição e renovação automáticas de certificado, Cipher Select e suporte a CNSA. Todos os recursos fazem uso extensivo de inteligência e automação para ajudar você a se manter à frente da curva de ameaças e permitem o dimensionamento exigido por modelos de uso em constante expansão.

1. Introdução

À medida que o ambiente de ameaças expande, os profissionais de TI e de segurança se esforçam para gerenciar os riscos impostos aos seus dados e recursos. Os dados são utilizados em vários dispositivos, no local e na nuvem, e o número de violações de dados de alto impacto continua aumentando. Historicamente, a ênfase da segurança tem sido colocada no SO, nos aplicativos e firewalls e em sistemas IPS e IDS. Todas elas continuam sendo áreas importantes que precisam de atenção. No entanto, tendo em vista os eventos dos últimos um ou dois anos que revelaram ameaças ao hardware, vemos como essencial a necessidade de proteger a infraestrutura baseada em hardware, como firmware, BIOS, BMC e outras proteções de hardware, como a garantia da cadeia de suprimentos.

De acordo com o Índice de transformação digital 2020 da Dell Technologies, as preocupações com a privacidade dos dados e a cibersegurança são a principal barreira para a transformação digital.[1] 63% das empresas tiveram comprometimento de dados devido a uma vulnerabilidade explorada[2]. Os danos globais relacionados a crimes cibernéticos chegarão aos US$ 6 trilhões em 2021[3].

Conforme os servidores ganham relevância em uma arquitetura de data center definida por software, a segurança desses servidores se torna a base de toda a segurança empresarial. Os servidores devem enfatizar a segurança no nível do hardware e do firmware, aproveitando uma raiz de confiança imutável que pode ser usada para verificar as operações subsequentes no servidor. Isso estabelece uma cadeia de confiança que se estende por todo o ciclo de vida útil do servidor, da implementação à manutenção e à desativação.

A 14ª e a 15ª geração de servidores Dell EMC PowerEdge com iDRAC9 propiciam essa cadeia de confiança, que é combinada a controles de segurança e ferramentas de gerenciamento abrangente para fornecer camadas robustas de segurança no hardware e no firmware. O resultado é uma arquitetura com resiliência cibernética que abrange todos os aspectos do servidor, incluindo o firmware do servidor incorporado, os dados armazenados no sistema, o sistema operacional, os dispositivos periféricos e as operações de gerenciamento. As organizações podem elaborar um processo para proteger sua valiosa infraestrutura de servidor e os dados nela contidos. Elas também podem detectar anomalias, violações ou operações não autorizadas e se recuperar de eventos indesejados ou mal-intencionados.

[1] Índice de transformação digital 2020 da Dell Technologies

[2] Match Present-Day Security threats with BIOS-Level Control. Documento da Forrester Consulting sobre liderança inovadora encomendado pela Dell, 2019

[3] Ransomware Attacks Predicted to Occur... The National Law Review, 2020

2. O caminho para uma infraestrutura de servidor segura

Há muitas gerações, os servidores Dell EMC PowerEdge contam com segurança robusta, incluindo a inovação do uso de segurança de dados baseada em silício. Os servidores Dell EMC PowerEdge de 14ª geração ampliaram a segurança baseada em silício para autenticar o BIOS e o firmware com uma raiz de confiança criptográfica durante o processo de inicialização do servidor. Em resposta às ameaças à segurança enfrentadas nos ambientes de TI modernos, a equipe de produtos da Dell EMC considerou vários requisitos importantes durante o desenvolvimento da 14ª e da 15ª geração de servidores PowerEdge:

- **Proteção:** proteger o servidor durante todos os aspectos do ciclo de vida, inclusive BIOS, firmware, dados e hardware físico
- **Detecção:** detectar ataques cibernéticos mal-intencionados e alterações não aprovadas e envolver proativamente os administradores de TI
- **Recuperação:** recuperar o BIOS, o firmware e o SO para um estado bom conhecido e desativar ou reutilizar os servidores com segurança

Conforme descrito neste documento, os servidores Dell EMC PowerEdge estão em conformidade com os principais padrões do setor no que concerne à criptografia e segurança. Eles executam o rastreamento e o gerenciamento contínuos de novas vulnerabilidades.

A Dell EMC implementou o processo Ciclo de vida do desenvolvimento de segurança considerando a segurança como elemento-chave em todos os aspectos das etapas de desenvolvimento, compras, fabricação, transporte e suporte. O resultado é uma arquitetura com resiliência cibernética.

2.1 Ciclo de vida do desenvolvimento de segurança

A elaboração da arquitetura com resiliência cibernética exige disciplina e consciência da segurança em cada estágio do desenvolvimento. A esse processo damos o nome de modelo Ciclo de Vida do Desenvolvimento de Segurança (SDL). Nele, a segurança não é apenas uma intenção futura, mas parte integral de todo o processo de desenvolvimento do servidor. O processo de desenvolvimento inclui uma visão das necessidades de segurança em todo o ciclo de vida do servidor, conforme demonstrado a seguir e como pode ser visto na Figura 1:

- Os recursos são concebidos, projetados, prototipados, implementados, colocados em produção, implantados e mantidos, sempre tendo a segurança como prioridade principal
- O firmware do servidor é projetado para obstruir, opor-se e combater a entrada de código mal-intencionado durante todas as fases do ciclo de vida do desenvolvimento do produto
  - » Há modelagem de ameaças e cobertura de testes de intrusão durante o processo de design
  - » Práticas de codificação segura são aplicadas em cada etapa do desenvolvimento do firmware

Figura 1: Ciclo de vida do desenvolvimento de segurança da Dell EMC

- Para tecnologias críticas, as auditorias externas complementam o processo SDL interno a fim de garantir que o firmware adote as práticas recomendadas de segurança conhecidas
- A avaliação e o teste contínuos das novas vulnerabilidades possíveis usam as mais recentes ferramentas de avaliação de segurança
- Há resposta rápida a Vulnerabilidades e Exposições Comuns (CVEs), incluindo medidas de correção recomendadas, se necessário.

2.2 Arquitetura com resiliência cibernética

Os servidores Dell EMC PowerEdge de 14ª e 15ª geração têm uma arquitetura com resiliência cibernética avançada que fornece um design de servidor reforçado para proteger, detectar e se recuperar de ataques cibernéticos. Alguns dos principais aspectos dessa arquitetura são os seguintes:

- **Proteção efetiva contra ataques**
  - » Raiz de confiança baseada em silício
  - » Secure Boot
  - » Atualizações de firmware assinadas
  - » Bloqueio dinâmico do sistema
  - » Criptografia de disco rígido e gerenciamento de chaves empresarial
- **Detecção confiável de ataques**
  - » Configuração e detecção de desvio de firmware
  - » Registro persistente de eventos
  - » Alertas e logs de auditoria
  - » Detecção de violação do chassi
- **Recuperação rápida com pouca ou nenhuma interrupção comercial**
  - » Recuperação automatizada do BIOS
  - » Rapid OS Recovery
  - » Reversão de firmware
  - » Limpeza rápida do sistema

2.3 Ameaças atuais

O cenário atual em constante mudança oferece muitos vetores de ameaça. A Tabela 1 resume a abordagem da Dell EMC no gerenciamento de ameaças críticas de back-end.

Tabela 1: Como a Dell EMC lida com vetores comuns de ameaças

Camadas da plataforma do servidor		
Camada de segurança	**Vetor de ameaça**	**Solução da Dell EMC**
Servidor físico	Violação de servidores/componentes	Verificação de componentes protegidos (SCV), detecção de invasão do chassi
Firmware e software	Corrupção do firmware e entrada de malware	Raiz de confiança baseada em silício, Intel Boot Guard, raiz de confiança do AMD Secure, Personalização da inicialização segura UEFI Firmware assinado e validado criptograficamente;
	Software	Relatórios de CVE, aplicação de patches conforme necessário
Recursos de confiança de atestado	Spoofing da identidade do servidor	TPM, TXT, Cadeia de confiança
Gerenciamento do servidor	Configuração e atualizações invasoras, ataques de porta aberta não autorizados	iDRAC9. Atestado remoto,

Camadas do ambiente de servidor		
Camada de segurança	**Vetor de ameaça**	**Solução da Dell EMC**
Dados	Violação dos dados	SED (Self Encrypting Drives, Unidades com Criptografia Automática) – FIPS ou Opal/TCG Unidades com gerenciamento de chaves empresarial seguro somente ISE (Instance Secure Erase) Autenticação segura do usuário
Integridade da cadeia de suprimentos	Componentes falsificados Ameaças de malware	Certificação ISO9001 para todos os locais globais de produção de servidores, verificação de componentes protegidos, comprovação de posse Medidas de segurança implementadas como parte do processo SDL
Segurança da cadeia de suprimentos	Segurança física nos locais de fabricação Roubo e violação durante o transporte	Requisitos de segurança da instalação da Transported Asset Protection Association (TAPA) Customs-Trade Partnership Against Terrorism (C-TPAT), SCV

3. Proteção

A função "proteger" é um componente essencial do NIST Cybersecurity Framework e serve para proteger contra ataques de cibersegurança. Essa função tem várias categorias, incluindo controle de acesso, segurança de dados, manutenção e tecnologia de proteção. A principal filosofia subjacente é que os ativos de infraestrutura devem fornecer proteção robusta contra acesso não autorizado a recursos e dados como parte de um ambiente abrangente e seguro de instalação e computação. Isso inclui proteção contra modificações não autorizadas de componentes críticos, como BIOS e firmware. A plataforma cumpre as recomendações atuais do NIST SP 800-193.

A arquitetura com resiliência cibernética dos servidores PowerEdge oferece um alto nível de proteção de plataforma, que inclui os seguintes recursos:

- Inicialização confiável verificada criptograficamente
- Segurança de acesso do usuário
- Atualizações de firmware assinadas
- Armazenamento de dados criptografados
- Segurança física
- Integridade e segurança da cadeia de suprimentos

3.1 Inicialização confiável verificada criptograficamente

Um dos aspectos mais críticos da segurança do servidor é garantir que o processo de inicialização pode ser verificado como seguro. Esse processo fornece uma âncora confiável para todas as operações subsequentes, como inicializar um SO ou atualizar o firmware. Por muitas gerações, os servidores PowerEdge usaram a segurança baseada em silício para recursos como o iDRAC Credential Vault, uma memória segura criptografada no iDRAC para armazenar dados confidenciais. O processo de inicialização é verificado usando uma raiz de confiança baseada em silício para atender às recomendações do NIST SP 800-147B (“BIOS Protection Guidelines for Servers”) e do NIST SP 800-155 (“BIOS Integrity Measurement Guidelines”).

3.1.1 Raiz de confiança baseada em silício

Agora, a 14ª e a 15ª gerações dos servidores PowerEdge (Intel e AMD) usam uma raiz de confiança imutável baseada em silício para atestar criptograficamente a integridade do BIOS e do firmware do iDRAC. Essa raiz de confiança tem como base chaves públicas únicas, programáveis e somente leitura que fornecem proteção contra violação de malware. O processo de inicialização do BIOS aproveita a tecnologia Intel Boot Guard ou a tecnologia de raiz de confiança da AMD que verifica se a assinatura digital do hash criptográfico da imagem de inicialização corresponde à assinatura armazenada em silício pela Dell EMC na fábrica. Uma falha na verificação resulta no encerramento do servidor, em uma notificação do usuário no Registro do Lifecycle Controller e no processo de recuperação do BIOS que pode ser iniciado pelo usuário. Se o Boot Guard é validado com êxito, os demais módulos do BIOS são validados usando um procedimento de cadeia de confiança até que o controle seja passado para o SO ou o hypervisor.

Além do mecanismo de verificação do Boot Guard, o iDRAC9 4.10.10.10 ou superior fornece um mecanismo de raiz de confiança para verificar a imagem do BIOS na inicialização do host. O host só pode inicializar depois que a imagem do BIOS for validada com êxito. O iDRAC9 também fornece um mecanismo para validar a imagem do BIOS em tempo de execução, sob demanda ou em intervalos programados pelo usuário

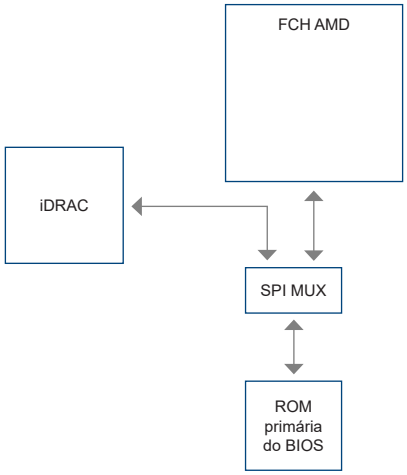
Vejamos a cadeia de confiança com mais detalhes. Cada módulo do BIOS contém um hash do módulo seguinte na cadeia. Os principais módulos do BIOS são IBB (Initial Boot Block), SEC (Security), PEI (Pre-EFI Initialization), MRC (Memory Reference Code), DXE (Driver Execution Environment) e BDS (Boot Device Selection). Se o Intel Boot Guard autentica o IBB, o IBB valida os módulos SEC+PEI antes de passar o controle a eles. Em seguida, SEC+PEI valida PEI+MRC que, na sequência, valida os módulos DXE+BDS. Nesse momento, o controle é passado para a Inicialização segura UEFI, conforme explicado na próxima seção.

Da mesma forma, no caso dos servidores Dell EMC PowerEdge com base no AMD EPYC, a tecnologia raiz de confiança do AMD Secure garante que os servidores só serão inicializados de imagens de firmware confiáveis. Além disso, a tecnologia AMD Secure Run foi desenvolvida para criptografar a memória principal, mantendo-a privada contra invasores mal-intencionados que tenham acesso ao hardware. Nenhuma modificação no aplicativo é necessária para usar esse recurso, e o processador de segurança nunca expõe as chaves de criptografia fora do processador.

O iDRAC também assume a função de tecnologias de segurança baseadas em hardware e acessa a ROM do BIOS primário por meio do SPI, além do Fusion Controller Hub (FCH) da AMD, e executa o processo de RoT.

Nas condições a seguir, o iDRAC9 recupera o BIOS.

1. Falha na verificação de integridade do BIOS.
2. Falha na verificação automática do BIOS.
3. Uso do comando RACADM – **racadm recover BIOS.Setup.1-1**



O processo de inicialização do iDRAC usa sua própria raiz de confiança independente baseada em silício, que verifica a imagem do firmware do iDRAC. A raiz de confiança do iDRAC também fornece uma âncora de confiança crítica para autenticar as assinaturas dos pacotes Dell EMC Update (DUPs) de firmware.

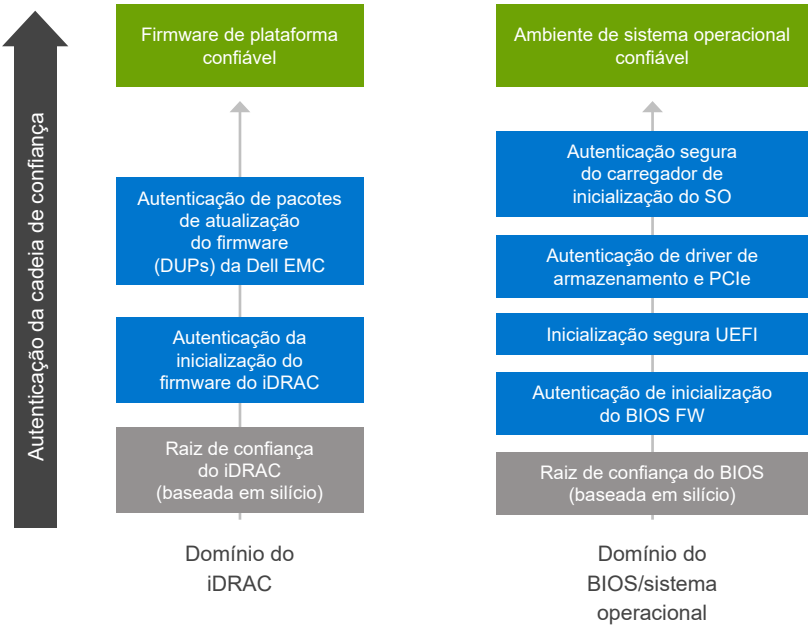


Figura 2: Domínios de raiz de confiança baseada em silício nos servidores PowerEdge

3.1.2 Varredura em tempo real do BIOS

A varredura em tempo real do BIOS verifica a integridade e a autenticidade da imagem do BIOS na ROM primária quando o host é ligado, mas não no processo de POST. Este recurso é exclusivo da AMD e está disponível somente no iDRAC9 4.10.10.10 ou superior com a licença Datacenter. Você deve ter privilégios de administrador ou privilégios de operador com o privilégio de depuração “Execute Debug Commands” para realizar esta operação. A varredura pode ser programada por meio das interfaces do iDRAC, RACADM e Redfish

3.1.3 Personalização da inicialização segura UEFI

Os servidores PowerEdge também oferecem suporte à inicialização segura UEFI (Unified Extensible Firmware Interface) padrão do setor, que verifica as assinaturas criptográficas de drivers UEFI e outros códigos carregados antes da execução do SO. Secure Boot é um padrão amplo do setor para segurança no ambiente anterior à inicialização. Fornecedores de sistemas de computadores e de placas de expansão e provedores de sistemas operacionais colaboram nessa especificação para promover a interoperabilidade.

Quando ativada, a inicialização segura UEFI impede o carregamento de drivers de dispositivo UEFI não assinados (ou seja, não confiáveis), exibe uma mensagem de erro e não permite que o dispositivo funcione. Desative a inicialização segura para carregar drivers de dispositivo não assinados.

Além disso, os servidores PowerEdge de 14ª e 15ª geração oferecem aos clientes a flexibilidade exclusiva de usar um certificado personalizado do carregador de inicialização não assinado pela Microsoft. Esse é um recurso dedicado prioritariamente a administradores de ambientes Linux que desejam assinar seus próprios carregadores de inicialização do SO. É possível fazer o upload dos certificados personalizados com a API do iDRAC para autenticar o carregador de inicialização do SO específico do cliente. Este método de personalização de UEFI do PowerEdge é citado pela NSA por atenuar as vulnerabilidades de Grub2 nos servidores.

3.1.4 Suporte a TPM

Os servidores PowerEdge oferecem suporte a três versões do TPM:

- TPM 1.2 FIPS + Common Criteria + Certificação TCG (Nuvoton)
- TPM 2.0 FIPS + Common Criteria + Certificação TCG (Nuvoton)
- TPM 2.0 China (NationZ)

O TPM pode ser usado para realizar funções criptográficas de chave pública, calcular funções de hash, gerar, gerenciar e armazenar chaves com segurança e gerar atestados. Também há suporte para a funcionalidade Intel Trusted Execution Technology (TXT) e para o recurso de Garantia da Plataforma da Microsoft no Windows Server 2016. O TPM também pode ser usado para habilitar o recurso de criptografia de disco rígido BitLocker™ do Windows Server 2012/2016.

O atestado e as soluções de atestado remoto podem usar o TPM para fazer medições no momento da inicialização do hardware, hypervisor, BIOS e SO de um servidor, além de compará-las de maneira criptograficamente segura com as medições básicas armazenadas no TPM. Se elas não forem idênticas, a identidade do servidor pode ter sido comprometida e os administradores do sistema podem desativar e desconectar o servidor local ou remotamente.

É possível encomendar os servidores com ou sem TPM, mas para muitos SOs e outras disposições de segurança ele está se tornando um padrão. O TPM é ativado por uma opção do BIOS. Ele é uma solução de Módulo plug-in e conta com um conector para esse módulo.

3.1.5 Certificações de segurança

A Dell EMC recebeu certificações para padrões como o NIST FIPS 140-2 e o Common Criteria EAL-4. Esses padrões são importantes para atender aos requisitos governamentais e do Departamento de Defesa dos EUA. Os servidores PowerEdge receberam as seguintes certificações:

- Plataforma de servidor: Com certificação Common Criteria EAL4+ com RHEL e também estão sendo usados para oferecer suporte às certificações CC de parceiro
- iDRAC e certificação CMC FIPS 140-2 Nível 1
- OpenManage Enterprise – modular com certificação EAL2+
- Certificação FIPS 140-2 e Common Criteria para TPM 1.2 e 2.0

3.2 Segurança de acesso do usuário

Garantir autenticação e autorização adequadas é um requisito fundamental de qualquer política moderna de controle de acesso. As interfaces de acesso primário para servidores PowerEdge são por meio de APIs, CLIs ou da GUI do iDRAC incorporado. As APIs e CLIs preferenciais para automatizar o gerenciamento de servidores são:

- API Restful do iDRAC com Redfish
- CLI do RACADM
- SELinux

Cada uma delas fornece credenciais robustas, como segurança de senha e nome de usuário, transportadas por uma conexão criptografada, como HTTPS, se desejado. O SSH autentica um usuário com um conjunto correspondente de chaves criptográficas. Assim, não há a necessidade de inserir senhas que sejam menos seguras. Há suporte para protocolos mais antigos, como o IPMI. No entanto, não é recomendável usá-los para novas implementações devido aos vários problemas de segurança que não foram resolvidos mais recentemente. Se, no momento, você usa o protocolo IPMI, recomendamos que avalie a transição para a API Restful do iDRAC com Redfish.

É possível fazer o upload dos **certificados TLS/SSL** para o iDRAC a fim de autenticar as sessões do navegador da Web. Há três opções disponíveis:

- **Certificado TLS/SSL autoassinado pela Dell EMC —** O certificado é gerado automaticamente e autoassinado pelo iDRAC.
  - » Vantagem: Não é necessário manter uma autoridade de certificação separada (consulte os padrões X.509/IETF PKIX).
- **Certificado TLS/SSL assinado personalizado —** o certificado é gerado automaticamente e assinado com uma chave privada que já foi carregada para o iDRAC.
  - » Vantagem: Uma única CA confiável para todos os iDRACs. É possível que sua CA interna já seja confiável em suas estações de gerenciamento.
- **Certificado TLS/SSL assinado pela CA —** uma solicitação de assinatura de certificado (CSR) é gerada e enviada para a sua CA interna ou por uma CA de terceiros, como a VeriSign, a Thawte e a Go Daddy, para assinatura.
  - » Vantagens: É possível usar uma autoridade de certificação comercial (consulte os padrões X.509/IETF PKIX). Uma única CA confiável para todos os seus iDRACs. Se uma CA comercial for usada, é muito provável que ela já seja confiável em suas estações de gerenciamento.

O iDRAC9 permite a integração ao **Active Directory** e ao **LDAP** aproveitando os esquemas existentes de autenticação e autorização dos clientes, que já fornecem acesso seguro aos servidores PowerEdge. Também inclui suporte ao **Controle de acesso baseado em função** para conceder o nível de acesso adequado (administrador, operador ou somente leitura) exigido para corresponder à função da pessoa nas operações do servidor. É altamente recomendável usar o RBAC dessa maneira e não apenas conceder o nível mais alto de acesso (ou seja, Administrador) a todos os usuários.

O iDRAC9 também fornece outras formas de proteção contra acesso não autorizado, incluindo **bloqueio e filtragem de IP**. O bloqueio de IP determina dinamicamente quando ocorrem falhas excessivas de login em um endereço IP específico e bloqueia (ou impede) que o endereço efetue login no iDRAC9 por um período de tempo pré-selecionado. A filtragem de IP limita o intervalo de endereços IP dos clients que acessam o iDRAC. Ela compara o endereço IP de um login de entrada com o intervalo especificado e somente permite o acesso ao iDRAC de uma estação de gerenciamento cujo endereço IP de origem esteja dentro do intervalo. Todas as outras solicitações de login serão negadas.

A **autenticação baseada em vários fatores (AMF)** está sendo usada mais amplamente hoje devido à crescente vulnerabilidade dos esquemas de autenticação baseada em um único fator, que utiliza nome de usuário e senha. O iDRAC9 permite o uso de Smart Cards para acesso remoto à GUI e também oferece suporte ao token RSA. Nos dois casos, os vários fatores são a presença física de um dispositivo ou cartão e o PIN associado.

3.2.1 MFA do RSA SecurID

O RSA SecurID pode ser usado como outro meio de autenticar o usuário em um sistema. O iDRAC9 começa a oferecer suporte ao RSA SecurID com a licença Datacenter e o firmware 4.40.00.00 como outro método de autenticação baseada em dois fatores.

3.2.2 2FA simplificada

Outro método de autenticação disponível é o Easy 2FA, que envia um token gerado aleatoriamente para a caixa de e-mail do usuário quando ele efetua login no iDRAC.

3.2.3 Estrutura SELinux

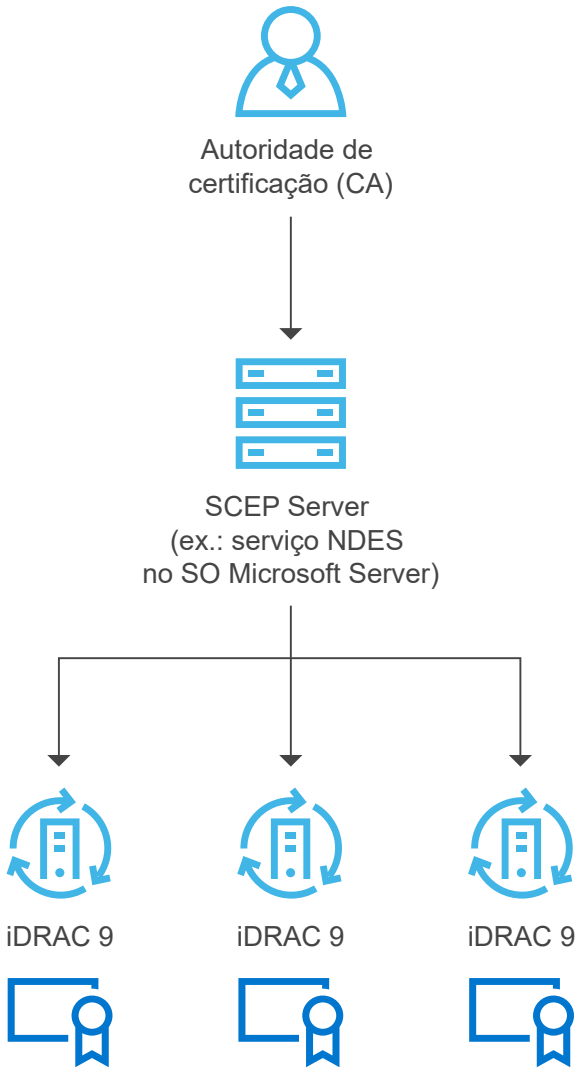
O SELinux opera no nível de kernel do núcleo no iDRAC e não precisa de entrada ou configuração por parte dos usuários. O SELinux registra mensagens de segurança quando um ataque é detectado. Essas mensagens indicam quando e como um invasor tentou entrar no sistema. No momento, esses logs estão disponíveis por meio do SupportAssist para os clientes inscritos neste novo recurso. Na versão futura do iDRAC, esses logs estarão disponíveis nos logs do Lifecycle Controller.

3.2.4 Privilégio mínimo obrigatório

Todos os processos internos executados no iDRAC são executados com os privilégios mínimos obrigatórios, um conceito de segurança central do UNIX. Essa proteção garante que o processo de um sistema que possa ser atacado não tenha acesso a arquivos ou itens de hardware fora do escopo desse processo. Por exemplo, o processo que fornece suporte para Virtual KVM não deve ser capaz de alterar as velocidades do ventilador. A execução desses dois processos como funções separadas ajuda a proteger o sistema impedindo que os ataques se propaguem de um processo para outro.

3.2.5 Inscrição e renovação automáticas de certificado

O iDRAC9 v4.0 adicionou um cliente para suporte a SCEP (Simple Certificate Enrollment Protocol) e requer a licença Datacenter. O SCEP é um padrão de protocolo usado para gerenciar certificados em muitos dispositivos de rede por meio de um processo de inscrição automática. Agora, o iDRAC pode ser integrado a servidores compatíveis com SCEP, como o serviço ServerNDES da Microsoft, para manter certificados SSL/TLS automaticamente. Esse recurso pode ser usado para inscrever e atualizar um certificado de servidor Web que vencerá em breve e pode ser aplicado um a um na GUI do iDRAC, definido via Perfil de Configuração do Servidor ou por scripts usando ferramentas como a RACADM.



3.2.6 Senha padrão de fábrica

Por padrão, para fornecer segurança adicional, todos os servidores PowerEdge de 14ª geração são fornecidos com uma única senha iDRAC exclusiva de fábrica. Essa senha é gerada na fábrica e pode ser encontrada na etiqueta de informações destacável localizada na parte frontal do chassi, perto da etiqueta do ativo do servidor. Os usuários que escolhem essa opção padrão devem tomar nota da senha e usá-la para fazer login no iDRAC pela primeira vez, em vez de usar uma senha padrão universal. Para fins de segurança, a Dell EMC recomenda fortemente a alteração da senha padrão.

3.2.7 Bloqueio dinâmico do sistema

O iDRAC9 oferece um novo recurso que “bloqueia” a configuração de hardware e firmware de um servidor ou servidores e requer a licença Enterprise ou Datacenter. Esse modo pode ser habilitado usando a GUI, CLIs como a RACADM, ou então como parte do Perfil de Configuração do Servidor. Usuários com privilégios administrativos podem definir o modo System Lockdown. Isso impede que usuários com menos privilégios façam alterações no servidor. Esse recurso pode ser ativado/desativado pelo administrador de TI. Quaisquer alterações feitas quando o System Lockdown está desativado são rastreadas no Registro do Lifecycle Controller. Ao ativar o modo de bloqueio, você pode impedir desvios de configuração no data center ao usar as ferramentas e os agentes da Dell EMC, além de se proteger de ataques mal-intencionados contra firmware incorporado ao usar os pacotes Dell EMC Update. O modo de bloqueio pode ser ativado dinamicamente, sem a necessidade de reinicializar o sistema. O iDRAC9 v4.40 introduz aprimoramentos além do bloqueio do sistema atual, que só controla as atualizações usando o Dell Update Package (DUP). Essa funcionalidade é expandida para NICs selecionadas. (Observação: o bloqueio aprimorado para NICs inclui apenas o bloqueio de firmware para evitar atualizações de firmware.) Não há suporte para bloqueio de configuração (x-UEFI). Quando o cliente definir o sistema no modo de bloqueio ativando/definindo o atributo de qualquer uma das interfaces compatíveis, o iDRAC executará outras ações, dependendo da configuração do sistema. Essas ações dependem dos dispositivos de terceiros detectados no processo de descoberta do iDRAC.

3.2.8 Isolamento do domínio

Os servidores PowerEdge de 14ª e 15ª geração oferecem segurança adicional graças ao **Isolamento do domínio**, um recurso importante para ambientes de hospedagem multiusuário. Para proteger a configuração de hardware do servidor, talvez os fornecedores de hospedagem queiram bloquear qualquer reconfiguração pelos locatários. O isolamento de domínio é uma opção de configuração que garante que os aplicativos de gerenciamento no SO host não tenham acesso ao iDRAC fora de banda ou às funções do chipset Intel, como Management Engine (ME) ou Innovation Engine (IE).

3.3 Atualizações de firmware assinadas

Por várias gerações, os servidores PowerEdge usaram assinaturas digitais nas atualizações de firmware para garantir que apenas o firmware autêntico esteja em execução na plataforma do servidor. Assinamos digitalmente todos os nossos pacotes de firmware usando hashing SHA-256 com criptografia RSA de 2048 bits para todos os principais componentes de servidor, incluindo firmware do iDRAC, BIOS, PERC, adaptadores de E/S e LOMs, PSUs, unidades de armazenamento, CPLD e controladores backplane. O iDRAC vai varrer as atualizações de firmware e comparar as assinaturas com o que é esperado usando a raiz de confiança baseada em silício; qualquer pacote de firmware que não for aprovado na validação será abortado, e uma mensagem de erro será registrada no Registro do ciclo de vida (LCL) para alertar os administradores de TI.

A autenticação avançada de firmware é incorporada em muitos dispositivos de terceiros que fornecem validação de assinatura com seus próprios mecanismos de raiz de confiança. Isso evita o possível uso de uma ferramenta de atualização comprometida de terceiros para carregar firmware mal-intencionado em, por exemplo, uma NIC ou unidade de armazenamento (ignorando o uso de pacotes Dell EMC Update assinados). Muitos dos dispositivos PCIe e de armazenamento de terceiros fornecidos com os servidores PowerEdge usam uma raiz de confiança de hardware para validar as respectivas atualizações de firmware.

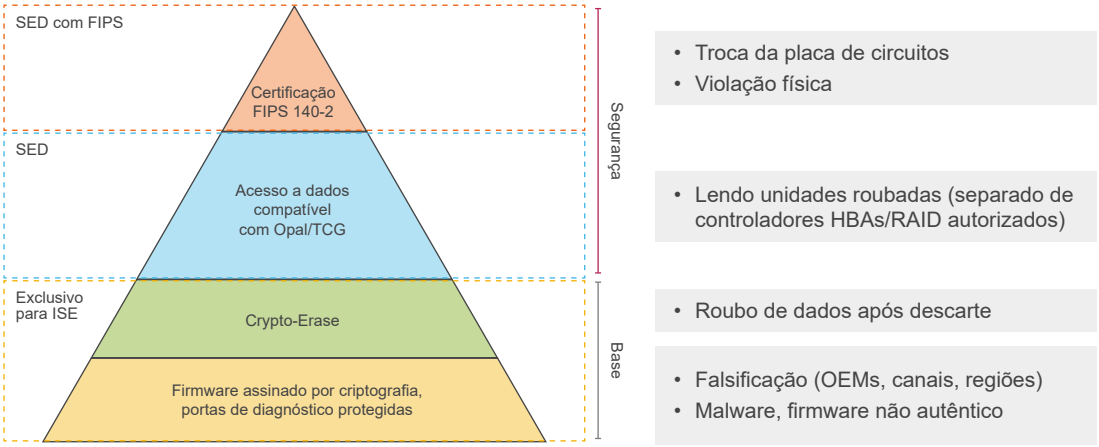
Se qualquer firmware de qualquer dispositivo for suspeito de violação mal-intencionada, os administradores de TI poderão reverter muitas das imagens de firmware da plataforma para uma versão anterior confiável armazenada no iDRAC. Mantemos duas versões do firmware do dispositivo no servidor – a versão de produção atual (“N”) e uma versão anterior confiável (“N-1”).

3.4 Armazenamento de dados criptografados

Os servidores PowerEdge de 14ª e 15ª geração oferecem diversas opções de unidades de armazenamento para proteger os dados. Conforme mostrado abaixo, as opções começam com unidades compatíveis com Instant Secure Erase (ISE), uma tecnologia nova para apagar dados de usuários de forma instantânea e segura. Como padrão, os servidores de 14ª e 15ª geração oferecem unidades compatíveis com ISE. Mais adiante neste documento, abordaremos a ISE em detalhes como parte da descrição do recurso System Erase.

As unidades com criptografia automática (SEDs) são a próxima opção de segurança mais alta. Elas oferecem proteção de bloqueio que vincula a unidade de armazenamento ao servidor e à placa RAID usado. Isso protege contra furto e a subsequente perda de dados confidenciais do usuário. Quando um ladrão tentar usar a unidade, ele não saberá a frase secreta da chave de bloqueio necessária. Por isso, ele será impedido de acessar os dados criptografados da unidade. Os clientes podem se proteger contra o roubo do servidor inteiro usando o Secure Enterprise Key Manager (SEKM), que abordaremos mais adiante neste documento.

O mais alto nível de proteção é oferecido por SEDs com certificação NIST FIPS 140-2. As unidades em conformidade com esta norma foram credenciadas por laboratórios de teste e têm adesivos resistentes a violações aplicados à unidade. Por padrão, as unidades SED da Dell EMC têm certificação FIPS 140-2.



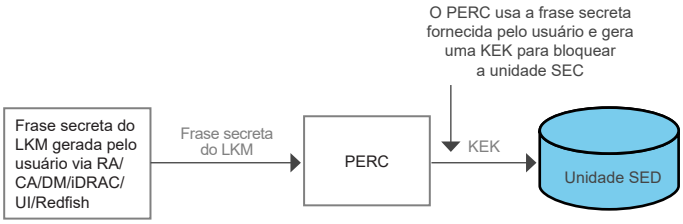
3.4.1 iDRAC Credential Vault

O processador de serviço do iDRAC fornece uma memória de armazenamento segura que protege vários dados confidenciais, como credenciais do usuário do iDRAC e chaves privadas de certificados SSL autoassinados. Outro exemplo de segurança baseada em silício, esta memória é criptografada com uma chave raiz única e imutável, programada em cada chip iDRAC durante a produção. Isso protege contra ataques físicos, em que o invasor dessolda o chip para tentar obter acesso aos dados.

3.4.2 Gerenciamento de chaves locais (LKM)

Com os servidores PowerEdge atuais, os usuários conseguem proteger unidades SED conectadas a um controlador PERC usando o Gerenciamento de chaves locais.

Para garantir a proteção dos dados do usuário quando uma unidade é roubada, a SED precisa ser bloqueada com uma chave separada para que os dados não sejam descriptografados, a menos que essa chave seja fornecida. Ela é chamada de KEK (Key Encryption Key). Para fazer isso, um usuário define uma keyId/frase secreta no controlador PERC ao qual a SED está conectada, o controlador PERC gera uma KEK usando a frase secreta e a utiliza para bloquear a SED. Agora, quando a unidade é ligada, ela aparece como uma SED bloqueada e vai criptografar ou descriptografar os dados do usuário somente quando a KEK for fornecida para desbloqueá-la. O PERC fornece a KEK à unidade para desbloqueá-la — desse modo, se a unidade for roubada, ela será exibida como “bloqueada” e, se o invasor não fornecer a KEK, os dados do usuário estarão protegidos. Ela é local porque a frase secreta e a KEK são armazenadas localmente no PERC. O diagrama a seguir mostra a solução LKM.

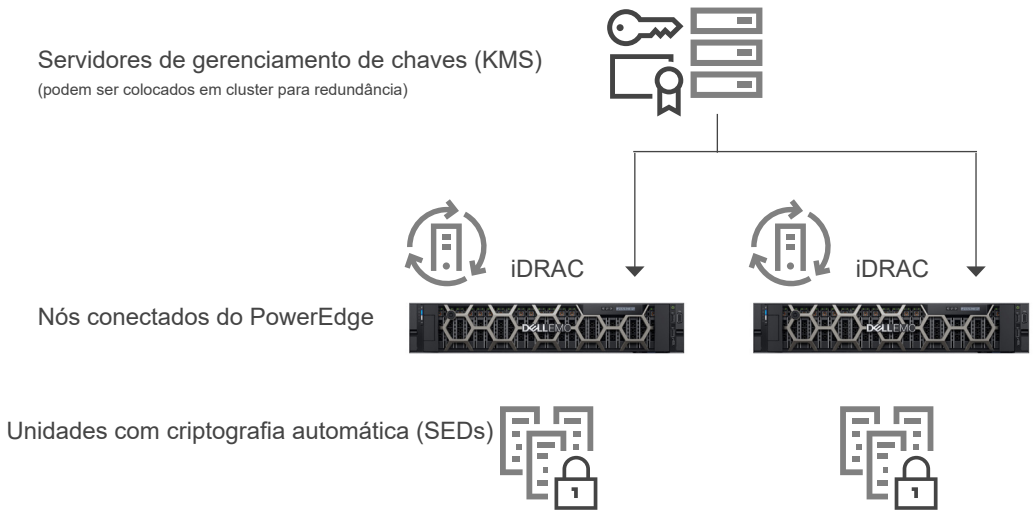


3.4.3 Secure Enterprise Key Manager (SEKM)

O SEKM do OpenManage oferece uma solução de gerenciamento de chaves central para gerenciar dados em repouso na organização inteira. Ele permite que o cliente use um servidor de gerenciamento de chaves (KMS) externo para gerenciar chaves que podem ser usadas pelo iDRAC para bloquear e desbloquear dispositivos de armazenamento em um servidor Dell EMC PowerEdge. Usando o código incorporado ativado com uma licença especial, o iDRAC solicita que o KMS crie uma chave para cada controlador de armazenamento, que ele busca e fornece ao controlador de armazenamento em cada inicialização do host, de modo que o controlador de armazenamento possa desbloquear as unidades com criptografia automática (SEDs).

As vantagens do SEKM em relação ao gerenciamento de chaves locais (LKM) são as seguintes:

- Proteção contra “roubo de servidor”, uma vez que as chaves não ficam armazenadas no servidor e são armazenadas externamente e recuperadas por nós do servidor PowerEdge conectados (via iDRAC)
- Gerenciamento de chaves centralizado e escalável para dispositivos criptografados com alta disponibilidade
- Oferece suporte ao protocolo KMIP padrão do setor, permitindo o uso de outros dispositivos compatíveis com KMIP
- Protege os dados em repouso quando as unidades ou o servidor inteiro são comprometidos
- O desempenho de criptografia na unidade se ajusta de acordo com o número de unidades



3.5 Segurança de hardware

A segurança de hardware é uma parte essencial de qualquer solução de segurança abrangente. Alguns clientes querem limitar o acesso a portas de entrada, como USB. Em geral, um chassi de servidor não deve ser aberto depois de ser colocado em produção. Em todo caso, os clientes gostariam de, no mínimo, rastrear e registrar tais atividades. O objetivo geral é desmotivar e limitar as violações físicas.

3.5.1 Alerta de invasão do chassi

Os servidores PowerEdge fornecem detecção e log de invasões ao hardware, e a detecção funciona mesmo sem energia CA disponível. Os sensores no chassi detectam quando alguém abre ou viola o chassi, mesmo durante o transporte. Os servidores que foram abertos em transporte geram uma entrada no registro do ciclo de vida do iDRAC depois que a energia é fornecida.

3.5.2 Gerenciamento dinâmico de portas USB

Para obter mais segurança, é possível desativar as portas USB por completo. Também é possível desativar apenas as portas USB frontais. Por exemplo, as portas USB podem ser desativadas para produção e ativadas temporariamente para conceder acesso a um carrinho de recuperação para fins de depuração.

3.5.3 iDRAC Direct

O iDRAC Direct é uma porta USB especial que é fisicamente conectada ao processador de serviço iDRAC para depuração e gerenciamento no servidor da parte frontal do servidor (corredor frio). Permite que o usuário conecte um cabo USB Micro-AB padrão a esta porta e à outra extremidade (Type-A) em um notebook. Um navegador da Web padrão pode então acessar a GUI do iDRAC para gerenciamento e depuração extensivos do servidor. Se houver uma licença do iDRAC Enterprise instalada, o usuário pode até mesmo acessar a área de trabalho do SO por meio do console virtual do iDRAC.

Como as credenciais normais do iDRAC são usadas para fazer login, o iDRAC Direct atua como um carrinho de restauração seguro, com a vantagem adicional de oferecer gerenciamento de hardware e diagnóstico do serviço extensivos. Essa pode ser uma opção atraente para proteger o acesso físico ao servidor em locais remotos (nesse caso, as portas USB e as saídas VGA do host podem ser desativadas).

3.5.4 iDRAC Connection View com localização geográfica

O Connection View permite ao iDRAC descrever os switches e portas externos conectados à E/S do servidor. Ele é um recurso encontrado em dispositivos de sistema de rede selecionados e exige que o LLDP (Link Layer Discovery Protocol) esteja ativado nos switches conectados.

Alguns dos benefícios do Connection View são:

- Verificar remota e rapidamente se os módulos de E/S do servidor (LOMs, NDCs e placas PCIe adicionais) estão conectados aos switches e portas corretos
- Evitar o despacho remoto oneroso de técnicos para corrigir erros de fiação
- Fim dos cabos cruzando os corredores quentes da sala do servidor
- Pode ser feito pela GUI, ou então os comandos RACADM podem fornecer informações para todas as conexões do servidor de 14ª geração

Além das economias óbvias de tempo e dinheiro, o Connection View oferece uma vantagem adicional: fornecer a localização geográfica de um servidor físico ou máquina virtual em tempo real. Usando o iDRAC Connection View, os administradores podem identificar um servidor para ver exatamente a qual comutador e porta o servidor está conectado. Isso ajuda a proteger os servidores contra conexões a redes e dispositivos que não atendam às diretrizes ou melhores práticas de segurança corporativa.

O Connection View valida a localização do servidor indiretamente ao relatar as identidades dos comutadores aos quais o servidor está conectado. A identidade do switch ajuda a determinar a localização geográfica e garantir que o servidor não invada um local não autorizado, fornecendo outra camada de segurança física. Ela também confirma que um aplicativo ou VM não “cruzou” fronteiras e está sendo executado em um ambiente seguro e aprovado.

3.6 Integridade e segurança da cadeia de suprimentos

A integridade da cadeia de suprimentos se concentra em dois desafios principais:

1. Manutenção da integridade do hardware: garantir que não haja violação do produto ou inserção de componentes desconhecidos antes do envio do produto aos clientes
2. Manutenção da integridade do software: garantir que não haja inserção de malware no firmware ou nos drivers do dispositivo antes do envio do produto aos clientes, além de impedir vulnerabilidades de codificação

A Dell EMC define a segurança da cadeia de suprimentos como a prática e aplicação de medidas de prevenção e detecção que protegem ativos físicos, inventário, informações, propriedade intelectual e pessoas. Essas medidas de segurança também ajudam a fornecer a garantia e integridade da cadeia de suprimentos reduzindo as oportunidades de introdução negligente ou mal-intencionada de malware e componentes desconhecidos na cadeia de suprimentos.

3.6.1 Integridade do hardware e do software

A Dell EMC tem como foco garantir que os processos de controle de qualidade sejam aplicados a fim de ajudar a minimizar as chances de componentes desconhecidos infiltrarem nossa cadeia de suprimentos. Os controles que a Dell EMC tem em vigor cobrem a seleção de fornecedores, suprimento, processos de produção e governança por meio de auditorias e testes. Depois que um fornecedor é selecionado, o processo de introdução do novo produto verifica se todos os materiais usados em todos os estágios de fabricação são provenientes da lista de fornecedores aprovados e correspondem à lista de materiais, conforme adequado. As fiscalizações de materiais durante a produção ajudam a identificar componentes com defeitos, que desviam dos parâmetros de desempenho normais ou que contêm um identificador eletrônico incorreto.

As peças são adquiridas diretamente dos fabricantes de design originais (ODM) ou dos fabricantes de componentes originais (OCM) sempre que possível. A fiscalização de materiais que ocorre durante o processo de introdução do novo produto oferece várias oportunidades de identificar componentes desconhecidos ou corrompidos que possam ter entrado na cadeia de suprimentos.

Além disso, a Dell EMC mantém a certificação ISO 9001 para todos os locais de produção globais. Seguir esses processos e controles rigorosamente ajuda a minimizar o risco de componentes falsificados serem incorporados aos produtos da Dell EMC ou de malware ser inserido em firmware ou drivers de dispositivos. Essas medidas são implementadas como parte do processo Ciclo de Vida do Desenvolvimento de Segurança (SDL).

3.6.2 Segurança física

A Dell EMC tem diversas práticas essenciais de longa data que estabelecem e mantêm a segurança nas instalações de fabricação e redes logísticas. Por exemplo, algumas das fábricas de produtos da Dell EMC precisam atender a requisitos específicos de segurança de instalações da Transported Asset Protection Association (TAPA), incluindo o uso de câmeras com circuito fechado monitorado nas áreas principais, controles de acesso e entradas e saídas vigiadas a todo momento. Também foram implementadas medidas de proteção contra roubo e violação de produtos durante o transporte como parte de um programa de logística líder do setor. Esse programa fornece uma central de comando com uma equipe sempre disponível para monitorar a chegada e a saída de cargas no mundo todo, a fim de garantir que as cargas vão de um destino a outro sem disrupção.

A Dell EMC também se envolve ativamente com diversos programas e iniciativas voluntários de segurança da cadeia de suprimentos. Uma dessas iniciativas é o Customs-Trade Partnership Against Terrorism (C-TPAT), introduzido pelo governo dos Estados Unidos após os atentados de 11 de setembro para ajudar a reduzir as chances de terrorismo fortalecendo as medidas de segurança da cadeia de suprimentos e das fronteiras. Como parte dessa iniciativa, a Alfândega e Proteção de Fronteiras dos EUA solicita que membros participantes garantam a integridade de suas práticas de segurança e compartilhem suas diretrizes de segurança com parceiros comerciais na cadeia de suprimentos. A Dell EMC é participante ativa desde 2002 e ocupa o mais alto status de associação.

3.6.3 Verificação de componentes protegidos (SCV) da Dell Technologies para PowerEdge

A Verificação de componentes protegidos (SCV) da Dell Technologies para PowerEdge é uma oferta de garantia da cadeia de suprimentos que permite aos clientes da Dell EMC verificar se um servidor PowerEdge recebido pelo cliente corresponde ao que foi produzido na fábrica. Para validar os componentes de uma forma criptograficamente segura, durante o processo de fabricação, é gerado um certificado na fábrica contendo as IDs exclusivas dos componentes de um servidor específico. Esse certificado é assinado na fábrica da Dell Technologies, armazenado no iDRAC e usado posteriormente pelo cliente no aplicativo SCV. O cliente usa o aplicativo SCV para coletar o inventário do sistema atual, incluindo as IDs exclusivas dos componentes, e o valida em relação ao inventário no certificado SCV.

O relatório gerado pelo aplicativo SCV verifica quais componentes correspondem e quais não correspondem ao que foi instalado na fábrica. Ele também verifica o certificado e a cadeia de confiança, junto com a comprovação de posse da chave privada SCV para iDRAC. A implementação atual oferece suporte a clientes de envio direto e não inclui cenários de VAR ou de substituição de peças.

4. Detecção

É essencial ter um recurso de detecção que fornece visibilidade completa da configuração, do status de integridade e dos eventos de alteração de um sistema de servidor. Essa visibilidade também deve detectar ações mal-intencionadas ou outras alterações no BIOS, firmware e Option ROMs na inicialização e no processo de tempo de execução do SO. A sondagem proativa deve ser combinada à capacidade de enviar alertas para todos os eventos no sistema. Os registros devem fornecer informações completas sobre acessos e alterações no servidor. E, mais importante, o servidor deve estender esses recursos a todos os componentes.

4.1 Monitoramento abrangente via iDRAC

Em vez de depender dos agentes do SO para estabelecer comunicação com os recursos gerenciados de um servidor, o iDRAC utiliza um caminho lateral direto para cada dispositivo. A Dell EMC utiliza protocolos padrão do setor, como MCTP, NC-SI e NVMe-MI, para estabelecer comunicação com dispositivos periféricos, como controladores RAID PERC, NICs Ethernet, HBAs de Fibre Channel, HBAs SAS e unidades NVMe. Essa arquitetura é resultado de parcerias de longa data com fornecedores líderes do setor para fornecer um gerenciamento de dispositivo sem agentes nos servidores PowerEdge. As operações de configuração e atualização de firmware também aproveitam os recursos avançados de UEFI e HII que a Dell EMC e nossos parceiros oferecem.

Com essa funcionalidade, o iDRAC pode monitorar o sistema quanto a eventos de configuração, eventos de violação (como a detecção de invasão do chassi mencionada anteriormente) e alterações de integridade. Os eventos de configuração são diretamente vinculados à identidade do usuário que iniciou a alteração, seja da GUI, da API ou do console.

4.1.1 Registro do ciclo de vida

O registro do ciclo de vida é um conjunto de eventos que ocorrem em um servidor durante certo tempo. Esse registro fornece uma descrição de eventos com carimbos de data/hora, gravidade, origem ou ID do usuário, ações recomendadas e outras informações técnicas que podem ser úteis para fins de rastreamento ou alertas.

Os seguintes tipos de informações são gravados no registro do ciclo de vida (LCL):

- Alterações de configuração nos componentes de hardware do sistema
- Alterações de configuração no iDRAC, BIOS, NIC e RAID
- Registros de todas as operações remotas
- Histórico de atualização do firmware com base no dispositivo, versão e data
- Informações sobre peças substituídas
- Informações sobre peças com falha
- IDs de mensagens de erro e eventos
- Eventos relacionados à alimentação do host
- Erros de POST
- Eventos de login do usuário
- Eventos de alteração de estado do sensor

4.1.2 Alertas

O iDRAC permite configurar diferentes alertas de eventos, bem como as ações a serem executadas quando ocorre um evento específico nos registros do ciclo de vida. Depois de ser gerado, o evento será encaminhado aos destinos configurados usando os mecanismos de tipo de alerta selecionados. Você pode ativar ou desativar alertas por meio da interface Web do iDRAC, RACADM ou com o utilitário de configurações do iDRAC.

O iDRAC oferece diferentes tipos de alerta, como:

- Alerta de IPMI ou e-mail
- Trap SNMP
- Registros do sistema remoto e do SO
- Evento do Redfish

Os alertas também podem ser categorizados por gravidade: crítico, aviso ou informativo.

Os seguintes filtros podem ser aplicados aos alertas:

- Integridade do sistema: por exemplo, erros de temperatura, tensão ou dispositivo
- Integridade do armazenamento: por exemplo, erros de controlador e discos virtual e físico
- Alterações de configuração: por exemplo, alteração na configuração do RAID, remoção da placa PCIe
- Registros de auditoria: por exemplo, falha na autenticação da senha
- Firmware/driver: por exemplo, upgrades ou downgrades

Por fim, o administrador de TI pode definir diferentes ações para alertas: Reinicializar, Ciclo de alimentação, Desligar ou Nenhuma ação.

4.2 Detecção de desvio

Ao aplicar configurações padrão e adotar a política de tolerância zero a alterações, as organizações conseguem reduzir as chances de explorações. O console Dell EMC OpenManage Enterprise permite que o cliente defina a linha de base de configurações do servidor e monitore o desvio dos servidores de produção a partir dessas linhas de base. A linha de base pode ser criada seguindo diversos critérios para se adequar a aplicações de produção diferentes, como segurança e desempenho. O OpenManage Enterprise pode relatar quaisquer desvios da linha de base e oferece a opção de reparar o desvio com um fluxo de trabalho simples para preparar as alterações no iDRAC fora de banda. Essas alterações poderão ser aplicadas no intervalo de tempo da próxima manutenção durante a reinicialização dos servidores para retomar a conformidade do ambiente de produção. Esse processo em etapas permite ao cliente implementar alterações de configuração na produção sem tempo de inatividade do servidor fora do horário de manutenção. Ele aumenta a disponibilidade do servidor sem comprometer a facilidade de manutenção ou a segurança.

5. Recuperação

As soluções de servidor devem permitir a recuperação para um estado conhecido e consistente como resposta a diversos eventos:

- Vulnerabilidades recém-descobertas
- Ataques mal-intencionados e violação de dados
- Corrupção do firmware devido a falhas de memória ou procedimentos de atualização inadequados
- Substituição de componentes do servidor
- Desativação ou reutilização do servidor

Abaixo, será discutido em detalhes como respondemos a novas vulnerabilidades e problemas de corrupção, e como recuperamos o servidor para o estado original, se necessário.

5.1 Resposta rápida a novas vulnerabilidades

As vulnerabilidades e exposições comuns (CVEs) são vetores de ataque recém-descobertos que comprometem produtos de hardware e software. A maioria das empresas precisa de respostas rápidas a CVEs para que seja possível avaliar a exposição e tomar as ações apropriadas.

As CVEs podem ser publicadas em resposta a novas vulnerabilidades identificadas em diversos itens, incluindo o seguinte:

- Código aberto, como OpenSSL
- Navegadores da Web e outro software de acesso à Internet
- Hardware e firmware de produtos do fornecedor
- Sistemas operacionais e hypervisors

A Dell EMC trabalha ativamente para responder rapidamente a novas CVEs nos servidores PowerEdge e fornece aos clientes informações em tempo hábil, incluindo o seguinte:

- Produtos afetados
- Etapas de correção que podem ser seguidas
- Se necessário, quando atualizações forem disponibilizadas para solucionar a CVE

5.2 Recuperação do BIOS e do SO

Os servidores Dell EMC PowerEdge de 14ª e 15ª geração incluem dois tipos de recuperação: recuperação do BIOS e recuperação rápida do sistema operacional (SO). Esses recursos permitem a recuperação rápida de imagens do SO ou do BIOS corrompidos. Nos dois casos, a área de armazenamento especial é ocultada do software de tempo de execução (BIOS, SO, firmware do dispositivo, etc.). Essas áreas de armazenamento contêm imagens intactas que podem ser usadas como alternativas ao software principal comprometido.

O Rapid OS Recovery permite a recuperação rápida de uma imagem de SO corrompida (ou uma imagem de SO suspeita de violação mal-intencionada). A mídia de recuperação pode ser um cartão SD interno, portas SATA, unidades M.2 ou USB interno. O dispositivo selecionado pode ser exposto à lista de inicialização e ao SO para a instalação da imagem de recuperação. Em seguida, ele pode ser desativado e ocultado da lista de inicialização e do SO. No estado oculto, o BIOS desativa o dispositivo para que não possa ser acessado pelo SO. No caso de uma imagem de SO corrompida, o local de recuperação pode ser ativado para inicialização. Essas configurações podem ser acessadas por meio do BIOS ou da interface do iDRAC.

Em casos extremos, quando o BIOS está corrompido (seja devido a um ataque mal-intencionado, a uma queda de energia durante o processo de atualização ou a qualquer outro evento inesperado), é importante fornecer uma maneira de restaurar o BIOS para seu estado original. Uma imagem de backup do BIOS é armazenada no iDRAC para ser usada na recuperação da imagem, se necessário. O iDRAC orquestra o processo de recuperação completo.

- A recuperação automática do BIOS é iniciada pelo próprio BIOS.
- A recuperação do BIOS sob demanda pode ser iniciada por usuários com o comando RACADM CLI.

5.3 Reversão de firmware

É recomendado manter o firmware atualizado para garantir que você tenha os recursos e atualizações de segurança mais recentes. No entanto, será preciso reverter uma atualização ou instalar uma versão anterior caso você identifique problemas após uma atualização. Ao reverter para a versão anterior, a assinatura dela também será verificada.

A reversão de firmware de uma versão de produto "N" para a versão anterior "N-1", no momento, é compatível com as seguintes imagens de firmware:

- BIOS
- iDRAC com Lifecycle Controller
- Placa de interface de rede (NIC)
- Controlador RAID PowerEdge (PERC)
- Unidade de distribuição de energia (PSU)
- Backplane

Você pode reverter o firmware para a versão instalada anteriormente ("N-1") usando um dos métodos a seguir:

- Interface Web do iDRAC
- Interface Web do CMC
- RACADM CLI – iDRAC e CMC
- GUI do Lifecycle Controller
- Serviços remotos do Lifecycle Controller

Você pode reverter o firmware para iDRAC ou qualquer dispositivo compatível com o Lifecycle Controller, mesmo se o upgrade tiver sido realizado anteriormente usando outra interface. Por exemplo, se foi feito upgrade do firmware usando a GUI do Lifecycle Controller, você poderá reverter o firmware usando a interface Web do iDRAC. É possível reverter o firmware de diversos dispositivos com uma única reinicialização do sistema.

Nos servidores PowerEdge de 14ª e 15ª geração com um único firmware do Lifecycle Controller e do iDRAC, reverter o firmware do iDRAC também reverte o firmware do Lifecycle Controller.

5.4 Restauração da configuração do servidor após a manutenção do hardware

Corrigir eventos de serviço é uma parte essencial das operações de TI. A capacidade de atender aos objetivos de tempo e de ponto de recuperação tem implicações diretas na segurança da solução. A restauração do firmware e da configuração do servidor garante que as políticas de segurança das operações do servidor sejam atendidas automaticamente.

Os servidores PowerEdge oferecem recursos que rapidamente restauram a configuração do servidor nas seguintes situações:

- Substituição de peças individuais
- Substituição da placa-mãe (backup e restauração completa do perfil do servidor)
- Substituição da placa-mãe (Easy Restore)

5.4.1 Substituição de peças

O iDRAC salva automaticamente a imagem de firmware e as definições de configuração de placas NIC, controladores RAID e unidades de distribuição de energia (PSUs). Ao realizar a substituição em campo dessas peças, o iDRAC automaticamente detecta a nova placa e restaura o firmware e as configurações na placa substituída. Esse recurso economiza tempo essencial e garante a consistência da configuração e da política de segurança. A atualização ocorre automaticamente ao reinicializar o sistema após a substituição da peça compatível.

5.4.2 Easy Restore (para substituição da placa-mãe)

As substituições da placa-mãe podem consumir muito tempo e afetar a produtividade. O iDRAC possibilita fazer backup e restaurar a configuração e o firmware de um servidor PowerEdge para minimizar o esforço necessário para substituir uma placa-mãe com defeito.

O servidor PowerEdge oferece duas maneiras de fazer backup e restauração:

1. Os servidores PowerEdge fazem backup automático das configurações do sistema (BIOS, iDRAC, NIC), etiqueta de serviço, aplicativo de diagnóstico de UEFI e outros dados licenciados na memória flash.

   Depois de substituir a placa-mãe no servidor, o Easy Restore solicita que você restaure esses dados automaticamente.

2. Para obter um backup mais abrangente, o usuário pode fazer backup das configurações do sistema, incluindo as imagens de firmware instaladas em vários componentes, como BIOS, RAID, NIC, iDRAC, Lifecycle Controller e placas auxiliares de rede (NDCs), e as configurações desses componentes. A operação de backup também inclui os dados de configuração do disco rígido, placa-mãe e peças de substituição. O backup cria um arquivo único que você pode salvar em um cartão SD vFlash ou em compartilhamento de rede (CIFS, NFS, HTTP ou HTTPS).

   O backup do perfil pode ser restaurado a qualquer momento pelo usuário. A Dell EMC recomenda que você realize uma operação de backup para cada perfil do sistema que você acredita que precisará restaurar em algum momento.

5.5 System Erase

Ao chegar ao fim do ciclo de vida, um sistema deve ser desativado ou reutilizado. O objetivo do System Erase é apagar dados confidenciais e configurações dos dispositivos de armazenamento do servidor e dos armazenamentos não voláteis do servidor, como caches e logs, de modo que nenhuma informação confidencial seja vazada inadvertidamente. É um utilitário do Lifecycle Controller projetado para apagar registros, dados de configuração, dados de armazenamento cache e aplicativos incorporados.

Os seguintes dispositivos, definições de configuração e aplicativos podem ser apagados usando o recurso System Erase:

- O iDRAC é redefinido para o padrão
- Dados do Lifecycle Controller (LC)
- BIOS
- Pacotes de drivers do SO e diagnóstico incorporados
- iSM
- Relatórios do SupportAssist Collection

Além disso, os seguintes componentes podem ser apagados:

- Cache do hardware (limpar PERC NVCache)
- Cartão SD vFlash (inicializar cartão) (Observação: vFlash não disponível em servidores da 15ª geração ou posterior.)

Os dados nos seguintes componentes são criptograficamente descartados pelo System Erase conforme descrito abaixo:

- SED (unidades com criptografia automática)
- Unidades somente ISE (unidades com Instant Secure Erase)
- Dispositivos NVM (Apache Pass, NVDIMMs)

Além disso, discos rígidos que não são ISE SATA podem ser apagados usando a substituição de dados.

Observe que o Instant Secure Erase (ISE) destrói a chave de criptografia interna em unidades de 14ª e 15ª geração, tornando os dados do usuário irrecuperáveis. O ISE é um método reconhecido de eliminação de dados nas unidades de armazenamento mencionado no NIST Special Publication 800-88 "Guidelines for Media Sanitization".

Confira as vantagens do novo recurso ISE com System Erase:

- **Velocidade:** muito mais rápido do que técnicas de substituição de dados, como DoD 5220.22-M (segundos versus horas)
- **Eficácia:** O ISE torna todos os dados da unidade completamente ilegíveis, inclusive os blocos reservados
- **TCO melhor:** os dispositivos de armazenamento podem ser reutilizados, em vez de comprimidos ou fisicamente destruídos de outra forma

O System Erase pode ser executado pelos seguintes métodos:

- Lifecycle Controller GUI (F10)
- CLI do RACADM
- Redfish

5.6 iDRAC9 Cipher Select

O Cipher Suite Selection pode ser usado para limitar as cifras que o navegador da Web pode usar para se comunicar com o iDRAC. Ele também pode determinar o nível de segurança da conexão. Essas configurações podem ser feitas por meio da interface Web do iDRAC, da RACADM e do Redfish. A funcionalidade está disponível em várias versões do iDRAC: iDRAC7, iDRAC8 (2.60.60.60 e superior) e no iDRAC9 atual (3.30.30.30 e superior).

5.7 Suporte a CNSA

As cifras compatíveis disponíveis no iDRAC9 com TLS1.2 e criptografia de 256 bits são mostradas na imagem da captura de tela abaixo. As cifras disponíveis estão incluídas no conjunto aprovado do CNSA.

5.8 Ciclo de alimentação completo

Em um Ciclo de alimentação completo, o servidor e todos os seus componentes são reinicializados. Ele utiliza a alimentação principal e auxiliar do servidor e de todos os componentes. Todos os dados na memória volátil também são apagados.

Para ter um ciclo de alimentação completo físico, é preciso desconectar o cabo de corrente alternada, aguardar 30 segundos e reconectá-lo. Isso representa um desafio para sistemas remotos. Um novo recurso nos servidores de 14ª e 15ª geração permite que você realize um Ciclo de alimentação completo a partir de iSM, da GUI do IDRAC, do BIOS ou de um script. O Ciclo de alimentação completo entra em vigor no ciclo de alimentação seguinte.

O recurso Ciclo de alimentação completo elimina a necessidade de ter alguém presente no local do data center, reduzindo o tempo para solucionar problemas. Pode eliminar, por exemplo, qualquer malware que ainda resida na memória.

6. Resumo

A segurança do data center é fundamental para o sucesso dos negócios, bem como a segurança da infraestrutura de servidor subjacente. Os ataques cibernéticos têm potencial de gerar tempo de inatividade estendido do sistema e dos negócios, perda de receita e clientes, danos jurídicos e na reputação corporativa. Para proteger, detectar e se recuperar de ataques cibernéticos direcionados ao hardware, a segurança precisa ser integrada ao projeto de hardware de servidor, e não incluída depois do ocorrido.

A Dell EMC é líder no aproveitamento de segurança baseada em silício para proteger firmware e dados confidenciais do usuário há duas gerações de servidores PowerEdge. As linhas de produtos PowerEdge de 14ª e 15ª geração contam com uma arquitetura com resiliência cibernética aprimorada, que usa a raiz de confiança baseada em silício para reforçar ainda mais a segurança do servidor, incluindo os seguintes recursos:

- **Inicialização confiável com verificação criptográfica** que consolida a segurança completa do servidor e a segurança geral do data center. Inclui recursos como raiz de confiança baseada em silício, firmware digitalmente assinado e recuperação do BIOS automática
- **Inicialização segura**, que verifica as assinaturas criptográficas dos drivers UEFI e outros códigos carregados antes da execução do SO.
- **iDRAC Credential Vault**, um espaço de armazenamento seguro para credenciais, certificados e outros dados confidenciais que são criptografados com uma chave baseada em silício exclusiva para cada servidor
- **Bloqueio dinâmico do sistema**, um recurso exclusivo do PowerEdge, ajuda a proteger as configurações do sistema e firmware contra alterações mal-intencionadas ou indesejadas, alertando os usuários sobre qualquer tentativa de realizar alterações no sistema
- O **Gerenciamento de chaves empresarial** oferece uma solução de gerenciamento de chaves central para gerenciar dados em repouso na organização inteira.
- **System Erase**, que permite aos usuários desativar ou reutilizar os servidores PowerEdge de 14ª e 15ª geração de maneira simples, apagando os dados de unidades de armazenamento e de outras memórias não voláteis incorporadas com rapidez e segurança
- A **segurança da cadeia de suprimentos** garante que não haja violação de produtos ou componentes falsificados antes do envio de produtos aos clientes.

Para concluir, os servidores PowerEdge de 14ª e 15ª geração, com a segurança líder do setor, formam uma base confiável para a transformação da TI na qual os clientes podem executar suas cargas de trabalho e operações de TI de maneira segura.

A. Apêndice: Leitura adicional

White Papers e material de apoio de segurança

- (Direct from Dev) SYSTEM ERASE ON POWEREDGE SERVERS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242
- SECURING 14TH GENERATION DELL EMC POWEREDGE SERVERS WITH SYSTEM ERASE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- (Direct from Dev) SECURITY IN SERVER DESIGN
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444243
- (Direct from Dev) CYBER-RESILIENCY STARTS AT THE CHIPSET AND BIOS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061
- FACTORY GENERATED DEFAULT IDRAC9 PASSWORD
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368
- DELL EMC IDRAC RESPONSE TO CVE-2017-1000251 “BLUEBORNE”
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605
- (Vídeo) SECURE BOOT CONFIGURATION AND CERTIFICATE MANAGEMENT USING RACADM
  https://youtu.be/mrIIN4X380c
- SECURE BOOT MANAGEMENT ON DELL EMC POWEREDGE SERVERS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- Signing UEFI images for Secure Boot feature in the 14th and 15th generation and later Dell EMC PowerEdge servers
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255
- RAPID OPERATING SYSTEM RECOVERY
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- Managing iDRAC9 Event Alerts on 14th generation (14G) Dell EMC PowerEdge Servers
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266
- UEFI Secure Boot Customization
  https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

Informes oficiais do PowerEdge

- Visão geral do iDRAC
  http://www.DellTechCenter.com/iDRAC
- Visão geral do console do OpenManage
  http://www.DellTechCenter.com/OME
- Visão geral do OpenManage Mobile
  http://www.DellTechCenter.com/OMM
- Lifecycle Controller Part Replacement
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457
- Motherboard Replacement
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832
- iDRAC Automatic Certificate Enrollment
  https://www.dellemc.com/resources/en-us/asset/white-papers/products/software/direct-from-development-idrac-automatic-certificate-enrollment.pdf
- Improved Server Security features in iDRAC9 using SELinux
  https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/dell-management-solution-resources_white-papers20_en-us.pdf
- iDRAC9 Cipher Select - Improved Security for Dell EMC PowerEdge Servers
  https://downloads.dell.com/manuals/all-products/esuprt_software_int/esuprt_software_ent_systems_mgmt/idrac9-lifecycle-controller-v33-series_white-papers11_en-us.pdf

Descubra mais sobre os servidores PowerEdge

Saiba mais sobre nossos servidores PowerEdge

Saiba mais sobre nossas soluções de gerenciamento de sistemas

Pesquise em nossa biblioteca de recursos

Siga servidores PowerEdge no Twitter

Entre em contato com um especialista da Dell Technologies em vendas ou suporte

DELL Technologies