Segurança cibernética do Dell CloudIQ para PowerEdge: os benefícios da automação

Resumo

Há muitas configurações de servidor que as equipes de infraestrutura dos clientes podem escolher para proteger os servidores contra as crescentes ameaças cibernéticas. No entanto, como podem encontrar as práticas recomendadas de configurações de segurança da Dell e, além disso, como podem verificar com frequência e eficiência se as configurações estão definidas incorretamente ou foram alteradas? A resposta é o recurso de segurança cibernética na solução CloudIQ para PowerEdge AIOps. Ele compara a configuração dos servidores PowerEdge implementados com uma política de configuração relacionada à segurança. Quando o CloudIQ identifica uma divergência entre a configuração em vigor e recomendada, ele notifica o administrador e recomenda as etapas de correção para corrigir o(s) problema(s).

Esta nota técnica Direct from Development (DfD) detalha a economia de tempo que os clientes podem obter usando o mecanismo automatizado de política de segurança cibernética do CloudIQ versus o exame manual de conformidade.

Autores

Mark Maclean
Engenharia Técnica de Marketing

Kyle Shannon
Gerenciamento de produtos

Versão 1.1 de julho de 2022

Introdução

No ambiente sempre ativo e sempre conectado atual, todas as organizações precisam aprimorar o tempo todo a estratégia de segurança cibernética para reduzir a crescente ameaça de ataque. Usando o recurso integrado de segurança cibernética do Dell CloudIQ, os clientes podem criar facilmente políticas de segurança para a proteção dos servidores PowerEdge. Uma política consiste em testes prontos para uso que os clientes podem habilitar apenas marcando uma opção. Os testes contêm configurações de segurança de infraestrutura baseadas nas práticas recomendadas da Dell e na estrutura de segurança cibernética do NIST (National Institute of Standards and Technology, Instituto Nacional de Padrões e Tecnologia). A segurança cibernética do Dell CloudIQ para PowerEdge permite a criação fácil de políticas e automatiza o monitoramento de políticas, tornando-o simples, eficiente e previsível.

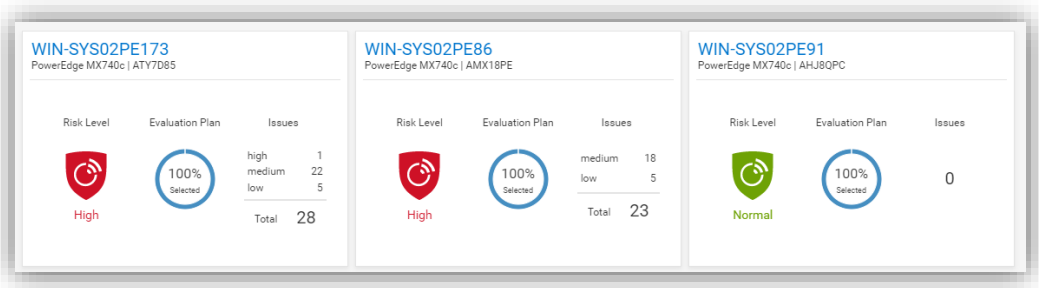


Figura 1 Painel de indicadores de segurança cibernética do CloudIQ

O CloudIQ é o aplicativo de lógica analítica e monitoramento proativo de AIOPs que oferece insights e recomendações sobre a integridade dos sistemas para as soluções de infraestrutura da Dell, incluindo armazenamento, proteção de dados, rede e, é claro, servidores PowerEdge. O mecanismo de política de segurança cibernética integrado ao CloudIQ tem mais de 30 regras de configuração de segurança para o PowerEdge que podem ser implementadas com facilidade. O CloudIQ é baseado em nuvem, portanto, pode ser integrado a qualquer número de instâncias do OpenManage Enterprise (OME) em vários data centers por meio do plug-in OME CloudIQ. Isso significa que o CloudIQ pode aplicar a mesma política a vários servidores gerenciados pelo OME, independentemente da localização. Não é necessário fazer qualquer configuração a mais no nível do iDRAC ou do OME para usar esse recurso. Depois que uma política é estabelecida, o CloudIQ verifica continuamente o estado desejado das definições de configuração de segurança do PowerEdge em relação à configuração atual “do jeito que estiver”. Se um servidor não estiver em conformidade com a política, ele será destacado. Os resultados são pontuados pelo CloudIQ com os servidores mais vulneráveis com um nível de risco “alto”. Problemas individuais podem ser visualizados com a correção recomendada. Essas correções de configuração de segurança recomendadas podem ser executadas individualmente por servidor usando a interface gráfica do iDRAC ou, se vários hosts não estiverem em conformidade, o OME pode ser utilizado para fornecer um arquivo de modelo de atualização de configuração ou executar um script do RACADM para corrigir as configurações de segurança de vários servidores.

Os benefícios da automação

Para entender o profundo impacto da automação desse processo, ele foi testado e comparado a um processo manual com 1, 10, 100* e 1.000* servidores. Com base nos testes da abordagem de segurança cibernética do CloudIQ de um cliente com 1.000* servidores, foi descoberto que:

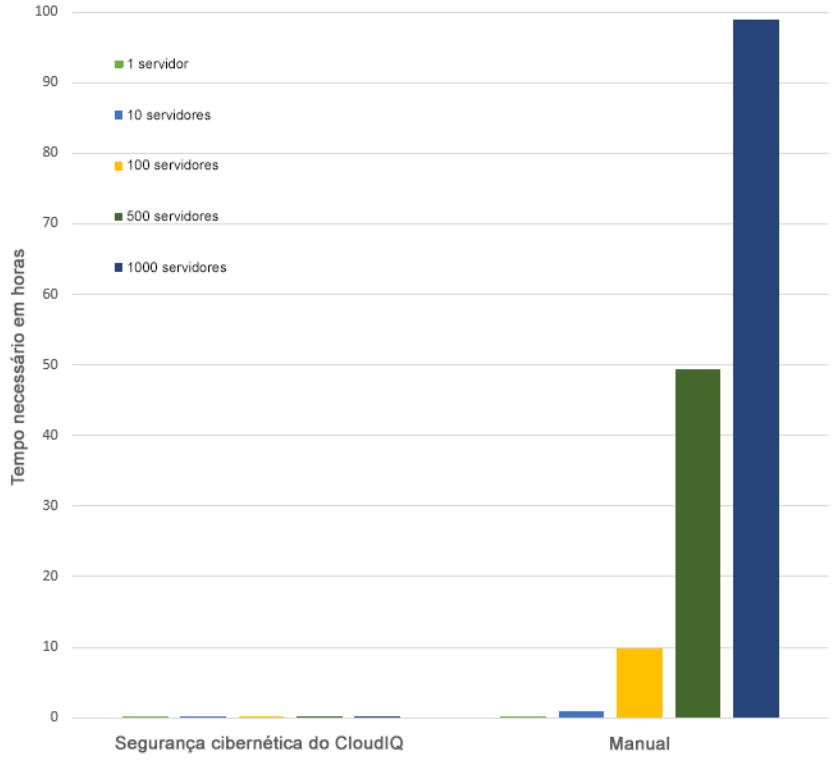
- é possível criar uma política de 15 testes e aplicá-la a 1.000 servidores em menos de 3 minutos*;
- a tarefa do CloudIQ foi concluída 99% mais rápido do que na análise manual*;
- o CloudIQ reduziu o tempo em 98 horas para concluir a tarefa uma vez*;
- usar a automação de segurança cibernética do CloudIQ economiza mais de uma semana de esforço imediatamente em comparação com a opção manual*;
- depois de ativado, o CloudIQ continua monitorando todas as principais definições de configuração de segurança regularmente.

*Resultados projetados com base na análise dos resultados de 1 e 10 servidores; os resultados do cliente podem variar

Nos testes de laboratório, descobriu-se que a verificação manual de 15 configurações na interface gráfica do iDRAC levou 5 minutos e 56 segundos, enquanto a criação de uma política de segurança cibernética do CloudIQ composta por 15 itens de teste ativos e a seleção de servidores de destino levou apenas 2 minutos e 58 segundos. Além disso, ao criar a política para 1, 10, 100 ou 1.000 servidores, essa tarefa levava o mesmo tempo. No entanto, usando o processo manual, cada servidor a mais acrescentava 5 minutos e 56 segundos no tempo para a conclusão das verificações. Além disso, depois que a política é definida, o CloudIQ continua verificando a conformidade das configurações atuais dos servidores.

Resumo dos resultados

Considerando que menos tempo é melhor, o gráfico abaixo destaca as diferenças entre a automação e o processo manual, ilustrando a significativa economia de tempo fornecida pela automação.



Consulte a Tabela 1 no final deste documento para obter os dados completos dos resultados,

Visão geral do teste

Para demonstrar a facilidade de uso e o impacto da automação, duas abordagens diferentes foram testadas, a manual versus a automação. Para utilizar esse recurso de segurança cibernética do CloudIQ, é necessário instalar o OpenManage Enterprise 3.9 “OME” ou superior com o plug-in 1.1 ou superior do CloudIQ ativado, os servidores PowerEdge são cobertos pelo Dell Pro Support e os servidores de destino para a política já foram identificados pelo OME. Para criar a política, o usuário deve ter os direitos de administrador do CyberSec atribuídos no CloudIQ. Algumas das regras de configuração usadas na política de segurança de teste são os valores padrão do iDRAC. Contudo, qualquer um desses valores pode ser alterado em um iDRAC individual pelos administradores com as devidas permissões, o que possibilita falhas de segurança.

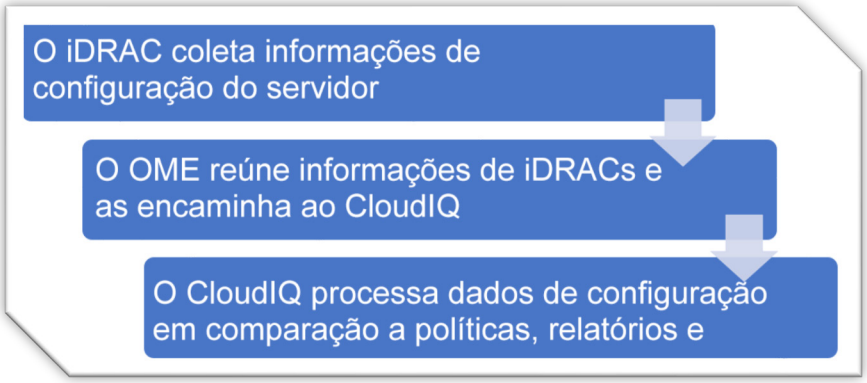


Figura 2 Fluxo de dados de configuração

Procedimento de teste

Para garantir uma comparação precisa das abordagens de teste, os testes são realizados e documentados rigorosamente. Foram selecionadas 15 configurações comuns, uma combinação de valores de configuração do BIOS e do iDRAC e 15 testes foram ativados na política de avaliação. Os testes foram realizados internamente na Dell, em Austin, nas instalações do laboratório de marketing técnico e on-line usando a oferta CloudIQ da Dell em 6 de julho de 2022.

I. Portas USB: desativadas
II. NIC ativa do iDRAC: dedicada
III. Bloqueio do sistema: ativado
IV. Configuração do iDRAC a partir do host: desativada
V. IPMI na LAN: desativada
VI. Inicialização segura: ativada
VII. Política de senha: forte
VIII. VNC: desativada
IX. SNMP versão 3: ativado
X. SSH: desativado
XI. Syslog: ativado
XII. Autenticação do Active Directory: ativada
XIII. Bloqueio de IP: ativado
XIV. Mídia virtual criptografada: ativada
XV. Sincronização de tempo NTP: ativada

Etapas para uma abordagem automatizada usando a política de segurança cibernética do CloudIQ PowerEdge

Na “página de login” do CloudIQ https://cloudiq.emc.com:

1. Faça login no CloudIQ
2. No menu do lado esquerdo da tela, selecione Segurança cibernética
3. Selecione Política
4. Selecione a guia Modelos
5. Selecione adicionar modelo
6. Forneça um nome ao modelo
7. Selecione PowerEdge no menu suspenso Produto e clique em Avançar
8. No plano de avaliação do modelo, configure as opções a seguir
9. Controle de acesso – marque: O bloqueio de IP está ativado/O SSH está desativado/O SNMP está configurado para V3/A autenticação do Active Directory está ativada/VNC desativada
10. Auditoria e responsabilidade – marque: Sincronização de tempo NTP ativada/Syslog remoto ativado
11. Gerenciamento de configuração – marque: Configurar o iDRAC a partir de Post/Bloqueio do sistema ativado/Portas USB desativadas
12. Identificação e autenticação – marque: A senha tem a pontuação mínima para o nível de segurança Forte
13. Proteção de sistema e comunicação – marque: IPMI na LAN desativada/Criptografia de mídia virtual ativada/NIC dedicada
14. Sistema e informações – Inicialização segura ativada
15. Selecione Concluir
16. Selecione a guia Sistemas
17. Selecione os hosts necessários na lista de hosts (em nosso teste, uma lista de 1, 10, 100 ou 1000 foi selecionada)
18. Clique em Atribuir
19. Selecione o modelo necessário no menu suspenso da lista de modelos
20. No menu do lado esquerdo da tela, selecione o risco do sistema para visualizar os resultados

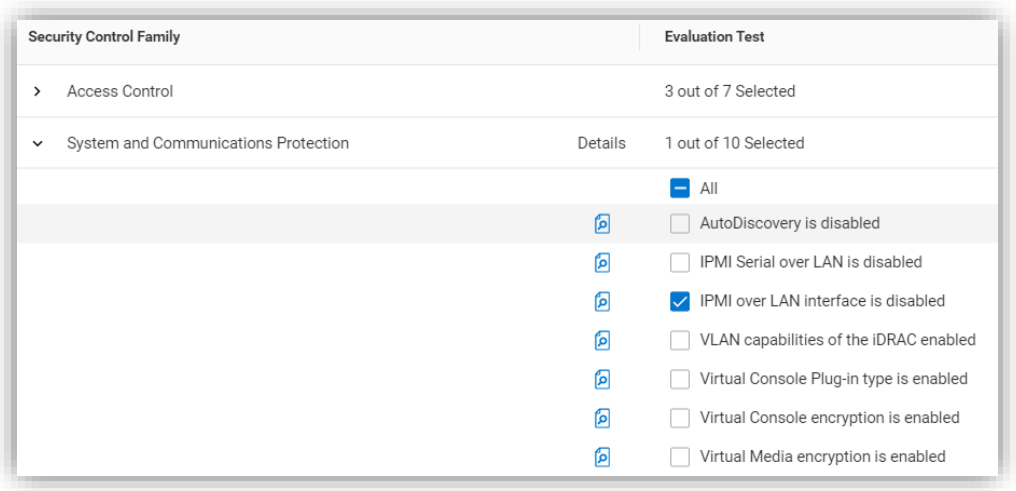


Figura 3 Seleção das regras para criar a política

Etapas para a abordagem manual de verificação dos valores de configuração na interface gráfica do iDRAC

A partir de um navegador que exiba a tela de login do iDRAC:

1. Faça login
2. USB – Configuração > Configurações do BIOS > Dispositivos integrados > Portas USB acessíveis ao usuário: todas as portas desativadas
3. Inicialização segura – Configuração > Configurações do BIOS > TPM avançado > Inicialização segura: ativada
4. VNC – Configuração > Console virtual > Servidor VNC > Ativar servidor VNC: desativado
5. SNMPv3 – Configuração > Configuração do sistema > Configuração de alerta > Trap SNMP > Configuração de SNMP > Formato da trap SNMP: SNMP v3
6. Syslog – Configuração > Configurações do sistema > Configuração de alerta > Configurações de Syslog remoto > Syslog remoto: ativado
7. Criptografia de mídia virtual – Configuração > Mídia virtual > Mídia anexada > Criptografia de mídia virtual: ativada
8. Porta dedicada – Configurações do iDRAC: interface NIC ativa: dedicada
9. Configuração local do iDRAC – Configurações do iDRAC > Serviços > Configuração local > Desativar configuração local do iDRAC: ativado
10. IPMI – Configurações do iDRAC > Conectividade > Rede > Configurações de IPMI > Ativar IPMI na LAN: desativado
11. Política de senhas – Configurações do iDRAC > Usuários > Configurações de usuários globais > Configuração de senhas > Política > Nível de segurança: Forte[1]
12. Autenticação do AD – Configurações do iDRAC > Usuários > Serviços de diretório > Microsoft AD: ativado
13. SSH – Configurações > Serviços do iDRAC > SSH > Ativado: desativado
14. Bloqueio de IP – Configurações do iDRAC > Conectividade > Rede > Configuração de rede avançada > Bloqueio de IP > Bloqueio: ativado
15. Sincronização de tempo NTP – Configurações > Configurações do iDRAC > Fuso horário > Servidor NTP > Ativar NTP: ativado
16. Bloqueio - verifique se o ícone do cadeado no canto superior direito da tela está exibindo o modo bloqueado

Teste realizado usando o Dell PowerEdge R540 BIOS 2.12.2 e firmware do iDRAC9: 5.10.00.00

1. A aplicação manual da política de senha forte garante a conformidade da nova senha com a política de senha, porém, as contas preexistentes ainda podem ter senhas fracas. O CloudIQ sinaliza qualquer iDRAC com senha fraca.

Resultados

Número de servidores	Política de segurança cibernética do CloudIQ	Verificação manual
1	2 minutos 58 segundos	5 minutos e 56 segundos
10	2 minutos 58 segundos	59 minutos
100	2 minutos 58 segundos	9 horas e 53 minutos*
500	2 minutos 58 segundos	49 horas e 26 minutos*
1000	2 minutos 58 segundos	98 horas e 53 minutos*

Tabela 1 – Resultados dos testes

*Resultados projetados com base na análise dos resultados de 1 e 10 servidores; os resultados do cliente podem variar

Resumo

Nossos testes mostraram que a automação usando o mecanismo de política de segurança cibernética do Dell CloudIQ para PowerEdge trouxe grandes benefícios em eficiência de tempo, repetibilidade, previsibilidade e, claro, tranquilidade. Os benefícios também aumentaram drasticamente à medida que o número de servidores foi extrapolado nos dados de teste.

Referências

CloudIQ em Dell.com - para data sheets e vídeos de demonstração

Blog Assuma o controle da segurança cibernética de servidores com o monitoramento inteligente baseado em nuvem

Vídeo sobre como criar e acompanhar as políticas de segurança cibernética do Dell CloudIQ para servidores PowerEdge

Página de conhecimento técnico do plug-in OpenManage Enterprise do CloudIQ

Soluções adicionais relacionadas à segurança cibernética da Dell