Cybersécurité Dell CloudIQ pour PowerEdge : les avantages de l'automatisation

Synthèse

Les équipes chargées de l'infrastructure des clients peuvent sélectionner de nombreux paramètres pour mieux protéger les serveurs contre les cybermenaces croissantes. Cependant, comment peuvent-elles trouver les pratiques d'excellence liées aux paramètres de configuration de sécurité Dell ? De plus, comment peuvent-elles savoir de manière efficace et continue si les paramètres sont mal configurés ou modifiés ? C'est là que la fonctionnalité de cybersécurité de la solution AIOps CloudIQ pour PowerEdge entre en jeu. Elle compare la configuration des serveurs PowerEdge déployés à une politique de configuration liée à la sécurité. Lorsque CloudIQ identifie une différence entre le paramètre de configuration réel et celui recommandé, l'administrateur en est informé et se voit recommander des mesures correctives pour éliminer le ou les problèmes.

Cette note technique Direct from Development (DfD) présente les gains de temps que les clients peuvent réaliser en utilisant le moteur de règle de cybersécurité automatisée CloudIQ par rapport à un examen manuel de la conformité.

Auteurs

Mark Maclean
Ingénierie marketing technique

Kyle Shannon
Gestion de produits

Version 1.1, juillet 2022

Introduction

Dans l'environnement actuel toujours connecté, toutes les organisations doivent constamment améliorer leur stratégie de cybersécurité afin de limiter les menaces d'attaques croissantes. À l'aide de la fonctionnalité de cybersécurité intégrée Dell CloudIQ, les clients sont en mesure de créer facilement des stratégies de sécurité pour la protection des serveurs PowerEdge. Une politique se compose de tests prêts à l'emploi que les clients peuvent simplement activer en cochant une case. Les tests contiennent des paramètres de sécurité de l'infrastructure basés sur les bonnes pratiques Dell et le cadre de cybersécurité du NIST (National Institute of Standards and Technology) américain. La cybersécurité Dell CloudIQ pour PowerEdge facilite et automatise la création des politiques, d'où un processus plus simple, plus efficace et plus prévisible.

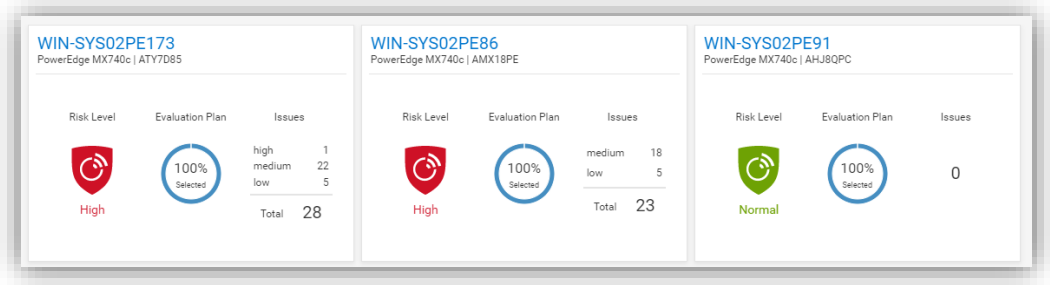


Figure 1 Tableau de bord de cybersécurité CloudIQ

CloudIQ est l'application AIOps d'analytique et de surveillance proactive qui fournit des informations et des recommandations sur l'intégrité des systèmes pour les solutions d'infrastructure Dell, y compris le stockage, la protection des données, la gestion de réseau et, bien sûr, les serveurs PowerEdge. Le moteur de règle de cybersécurité intégré à CloudIQ dispose de plus de 30 règles de configuration de sécurité pour PowerEdge qui peuvent être implémentées en toute simplicité. CloudIQ est basé sur le Cloud et peut donc s'intégrer avec de nombreuses instances OpenManage Enterprise (OME) dans plusieurs datacenters via le plug-in OME CloudIQ. Cela signifie que CloudIQ peut appliquer la même règle à plusieurs serveurs gérés par OME, où qu'ils se trouvent. Cette fonctionnalité est fournie par CloudIQ sans aucune configuration supplémentaire au niveau de l'iDRAC ou d'OME. Une fois qu'une règle est établie, CloudIQ vérifie en permanence l'état souhaité des paramètres de configuration de sécurité PowerEdge par rapport à la configuration actuelle « en l'état ». Si un serveur n'est pas conforme aux règles, il est signalé visuellement. Les résultats sont notés par CloudIQ, sachant que les serveurs les plus vulnérables se voient octroyer un niveau de risque « élevé ». Chaque problème peut être accompagné des mesures correctives recommandées. Ces recommandations de correction de la configuration de sécurité peuvent ensuite être exécutées l'une après l'autre sur chaque serveur à l'aide de l'interface graphique de l'iDRAC. Si plusieurs hôtes sont estimés non conformes, OME peut être utilisé pour fournir un modèle de mise à jour de configuration ou exécuter un script RACADM pour modifier les configurations de sécurité de plusieurs serveurs.

Les avantages de l'automatisation

Pour comprendre l'impact important de l'automatisation de ce processus, nous l'avons comparé à un processus manuel pour 1, 10, 100* et 1 000* serveurs. D'après les tests de l'approche de cybersécurité CloudIQ pour un client disposant de 1 000* serveurs, nous avons constaté les éléments suivants :

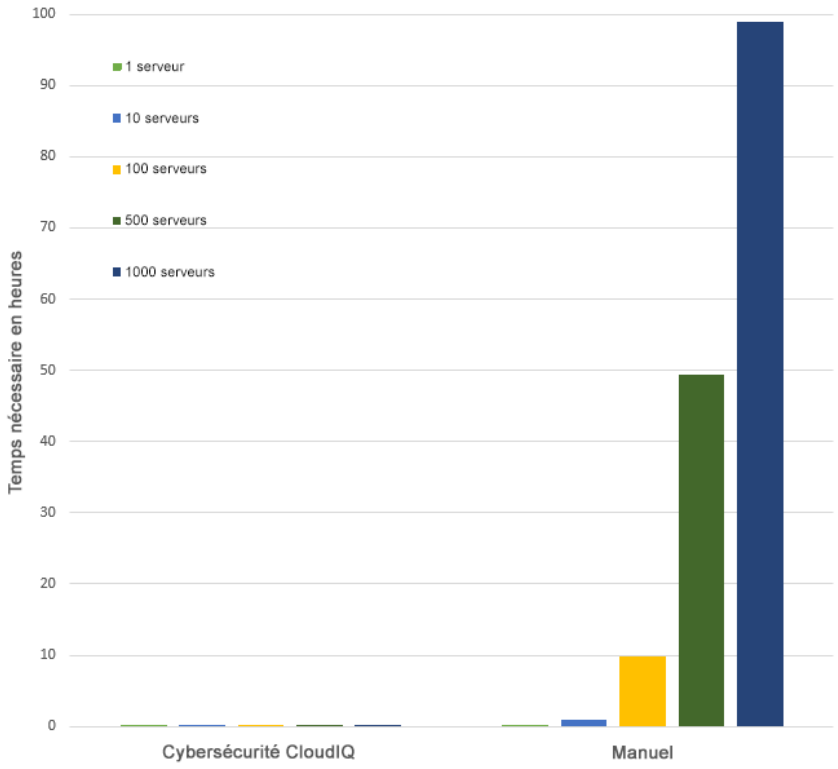
- Créez une politique de 15 tests et appliquez-la à 1 000 serveurs en moins de 3 minutes*
- La tâche CloudIQ s'est terminée 99 % plus rapidement qu'une vérification manuelle*
- CloudIQ a mis 98 heures en moins pour terminer la tâche en une seule fois*
- L'utilisation de l'automatisation de la cybersécurité CloudIQ permet d'économiser plus d'une semaine d'efforts immédiatement par rapport à un processus manuel*
- Une fois l'application CloudIQ activée, elle continue de surveiller régulièrement tous ces paramètres de configuration de sécurité clés.

*Résultats estimés basés sur l'analyse des résultats de la configuration avec 1 et 10 serveurs, les résultats du client peuvent varier

Lors des tests en laboratoire, nous avons constaté que la vérification manuelle de 15 paramètres dans l'interface graphique de l'iDRAC prenait 5 minutes 56 secondes, tandis que la création d'une stratégie de cybersécurité CloudIQ composée de 15 éléments de test actifs et de la sélection du ou des serveurs cibles ne prenait que 2 minutes 58 secondes. En outre, que vous deviez créer la règle pour 1, 10, 100 ou 1 000 serveurs, cette tâche a pris le même temps. Toutefois, dans le cas du processus manuel, pour chaque serveur supplémentaire, il a fallu 5 minutes 56 secondes de temps de vérification en plus. De plus, une fois la règle définie, CloudIQ continue de vérifier la conformité des paramètres des serveurs.

Synthèse des résultats

Sachant qu'il est toujours mieux de réduire le temps nécessaire, le graphique ci-dessous met en évidence les différences entre l'automatisation et le processus manuel, afin d'illustrer le gain de temps considérable offert par l'automatisation.



Reportez-vous au tableau 1 à la fin de ce document pour obtenir des données complètes sur les résultats.

Présentation des tests

Pour démontrer à la fois la facilité d'utilisation et l'impact de l'automatisation, nous avons testé deux approches différentes : une manuelle et une automatisée. Afin d'utiliser cette fonctionnalité de cybersécurité CloudIQ, vous devez avoir installé OpenManage Enterprise 3.9 « OME » ou une version supérieure et avoir activé le plug-in CloudIQ 1.1 ou une version supérieure. Par ailleurs, le ou les serveurs PowerEdge doivent être couverts par Dell ProSupport et les serveurs cibles de la politique doivent déjà avoir été détectés par OME. Pour créer la règle, l'utilisateur doit disposer des droits d'administrateur de cybersécurité attribués dans CloudIQ. Certaines des règles de configuration utilisées dans la politique de sécurité de test correspondent aux valeurs par défaut de l'iDRAC. Toutefois, toutes ces valeurs peuvent être modifiées sur chaque iDRAC par des administrateurs disposant des droits appropriés, d'où l'apparition d'une faille de sécurité.

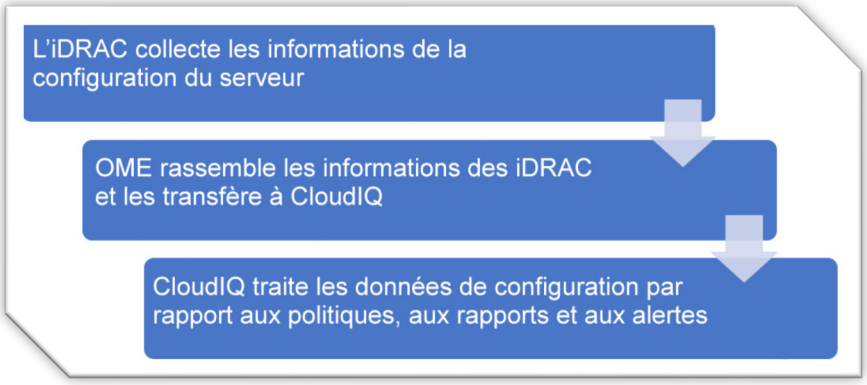


Figure 2 Flux de données de configuration

Procédure de test

Pour pouvoir effectuer une comparaison précise des approches de test, nous avons rigoureusement testé et documenté nos tests. Nous avons sélectionné 15 paramètres courants ainsi qu'une combinaison de valeurs de configuration du BIOS et de l'iDRAC, et nous avons activé 15 tests dans la politique d'évaluation. Les tests ont été réalisés en interne sur le site Dell d'Austin dans les locaux du laboratoire marketing technique et en ligne à l'aide de l'offre Dell CloudIQ du 6 juillet 2022.

I. Ports USB : désactivés
II. Carte NIC de l'iDRAC active : dédiée
III. Verrouillage du système : activé
IV. Configuration de l'iDRAC à partir de l'hôte : désactivée
V. IPMI sur LAN : désactivé
VI. Secure Boot : activé
VII. Politique de mots de passe : forte
VIII. VNC : désactivé
IX. SNMP version 3 : activé
X. SSH : désactivé
XI. Journal syslog : activé
XII. Authentification Active Directory : activée
XIII. Blocage IP : activé
XIV. Chiffrement des supports virtuels : activé
XV. Synchronisation de l'heure NTP : activée

Étapes d’une approche automatisée utilisant la politique de cybersécurité CloudIQ PowerEdge

Accédez à la page de connexion CloudIQ https://cloudiq.emc.com :

1. Connectez-vous à CloudIQ
2. Dans le menu situé à gauche de l’écran, sélectionnez Cybersécurité
3. Sélectionnez Politique
4. Sélectionnez l’onglet des modèles
5. Sélectionnez Ajouter un modèle
6. Nommez le modèle
7. Sélectionnez PowerEdge dans le menu déroulant des produits, puis cliquez sur Suivant
8. Dans le modèle de plan d’évaluation, configurez les éléments suivants :
9. Contrôle d’accès : cochez : Le blocage IP est activé/SSH est désactivé/SNMP configuré pour V3/L’authentification Active Directory est activée/VNC est désactivé
10. Audit et responsabilité : cochez : La synchronisation de l’heure NTP est activée/Le journal syslog est activé
11. Gestion de la configuration : cochez : Configuration de l’iDRAC à partir du test POST/System Lockdown activé/Ports USB désactivés
12. Identification et authentification : cochez : Le mot de passe respecte les critères minimaux de protection forte
13. Protection du système et des communications : cochez : IPMI sur LAN désactivé/Chiffrement des supports virtuels activé/Carte NIC dédiée
14. Système et informations : Secure Boot activé
15. Cliquez sur Terminer
16. Sélectionnez l’onglet des systèmes
17. Sélectionnez les hôtes requis dans la liste des hôtes (lors de notre test, nous avons sélectionné une liste de 1, 10, 100 ou 1 000)
18. Cliquez sur Attribuer
19. Sélectionnez le modèle requis dans le menu déroulant de la liste des modèles
20. Dans le menu en bas à gauche de l’écran, sélectionnez le risque système pour afficher les résultats

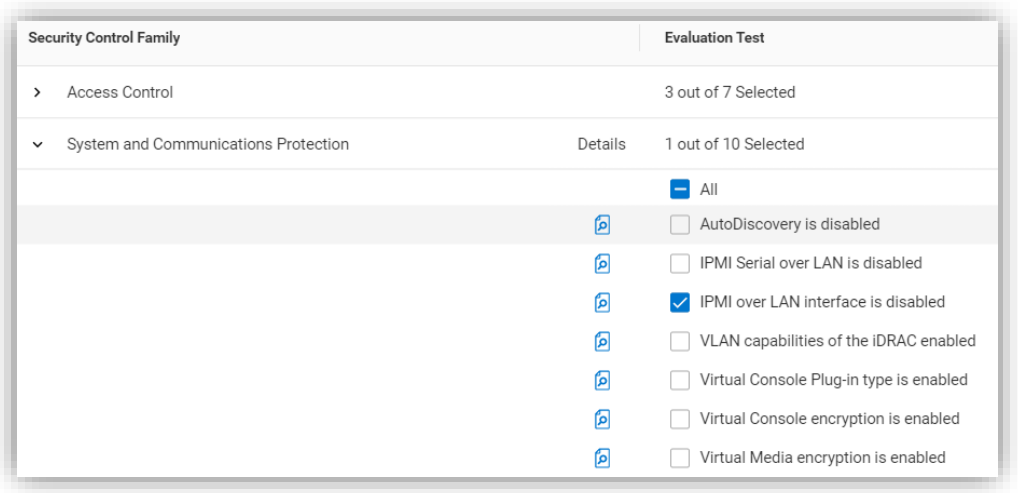


Figure 3 Sélectionner des règles pour créer une politique

Étapes d'une approche manuelle de vérification des valeurs de configuration dans l'interface utilisateur de l'iDRAC

Dans un navigateur affichant l'écran de connexion de l'iDRAC :

1. Se connecter
2. USB : configuration/paramètres du BIOS/appareils intégrés/ports USB accessibles par l'utilisateur : tous les ports désactivés
3. Secure Boot : configuration/paramètres du BIOS/TPM avancé/Secure Boot : activé
4. VNC : configuration/console virtuelle/serveur VNC/activer le serveur VNC : désactivé
5. SNMPv3 : configuration/paramètre système/configuration des alertes/trap SNMP/paramètre SNMP/format de trap SNMP : SNMP v3
6. Journal syslog : configuration/paramètres système/configuration des alertes/paramètres du journal syslog distant/journal syslog distant : activé
7. Chiffrement des supports virtuels : configuration/support virtuel/support connecté/chiffrement des supports virtuels : activé
8. Port dédié : paramètres de l'iDRAC : interface de la carte NIC active : dédiée
9. Configuration locale de l'iDRAC : paramètres de l'iDRAC/services/configuration locale/désactiver la configuration locale de l'iDRAC : activé
10. IPMI : paramètres de l'iDRAC/connectivité/réseau/paramètres IPMI/activer IPMI sur LAN : désactivé
11. Politique de mots de passe : paramètres de l'iDRAC/utilisateurs/paramètres utilisateurs globaux/paramètre de mot de passe/politique/score : fort[1]
12. Authentification AD : paramètres de l'iDRAC/utilisateurs/services de répertoire/Microsoft AD : activé
13. SSH : paramètres de l'iDRAC/services/SSH/activé : désactivé
14. Blocage IP : paramètres de l'iDRAC/connectivité/réseau/paramètre de gestion de réseau avancé/blocage IP/blocage : activé
15. Synchronisation de l'heure NTP : paramètres de l'iDRAC/paramètres/fuseau horaire/serveur NTP/activation du protocole NTP : activé
16. Verrouillage : l'icône de verrouillage située en haut à droite de l'écran indique le mode verrouillé

Testé à l'aide du BIOS Dell PowerEdge R540 2.12.2 et du firmware iDRAC9 : 5.10.00.00

1. L'application manuelle de la politique de mots de passe forts garantit la conformité des nouveaux mots de passe avec la politique de mots de passe, mais les comptes préexistants peuvent toujours avoir des mots de passe faibles, CloudIQ signalant tout iDRAC avec un mot de passe faible.

Résultats

Nombre de serveurs	Politique de cybersécurité CloudIQ	Vérification manuelle
1	2 min 58 s	5 min 56 s
10	2 min 58 s	59 min
100	2 min 58 s	9 heures 53 min*
500	2 min 58 s	49 heures 26 min*
1 000	2 min 58 s	98 heures 53 min*

Tableau 1 : résultats des tests

*Résultats estimés basés sur l'analyse des résultats de la configuration avec 1 et 10 serveurs, les résultats du client peuvent varier

Synthèse

Nos tests ont montré que l'automatisation à l'aide de Dell CloudIQ pour le moteur de règle de cybersécurité PowerEdge offrait des avantages majeurs en matière de gain de temps, de reproductibilité, de prévisibilité et, bien sûr, de tranquillité d'esprit. Les avantages ont également considérablement augmenté lorsque nous avons extrapolé le nombre de serveurs dans les données de test.

Références

CloudIQ sur Dell.com : fiches techniques et vidéos de démo

Blog : Prenez le contrôle de la cybersécurité des serveurs avec une solution de surveillance intelligente basée sur le Cloud

Vidéo : Création et suivi des politiques de cybersécurité Dell CloudIQ pour les serveurs PowerEdge

Page de connaissances techniques sur le plug-in OpenManage Enterprise CloudIQ

Solutions Dell supplémentaires liées à la cybersécurité

En savoir plus sur les serveurs PowerEdge

Contactez-nous pour tout commentaire et toute demande

Suivez-nous pour les actualités PowerEdge