适用于 PowerEdge 的 Dell CloudIQ 网络安全功能：自动化带来的优势

摘要

客户基础架构团队可以有很多服务器设置选择来强化服务器，以抵御与日俱增的网络威胁。但是，他们如何才能找到要使用的戴尔安全配置设置最佳实践呢？此外，如何才能有效地持续检查设置是否出现了配置错误或发生了更改呢？答案是，适用于 PowerEdge AIOps 的 CloudIQ 解决方案中提供的网络安全功能。它将所部署的 PowerEdge 服务器的配置与安全相关的配置策略进行比较。当 CloudIQ 识别出实际配置设置与建议的配置设置之间存在偏差时，便会通知管理员并建议采取补救步骤来纠正问题。

本 Direct from Development (DfD) 技术说明详细介绍了客户通过使用 CloudIQ 自动网络安全策略引擎，相较于手动合规性检查所节省的时间。

作者

Mark Maclean
技术营销工程

Kyle Shannon
产品管理

版本 1.1 - 2022 年 7 月

简介

在当今时刻在线、时刻互连的环境中，所有组织都需要不断加强其网络安全战略，以缓解与日俱增的攻击威胁。使用 Dell CloudIQ 的内置网络安全功能，客户能够轻松构建安全策略来保护 PowerEdge 服务器。策略包含现成的测试，客户只需勾选方框便可启用相应的测试。这些测试包含基于戴尔最佳实践和美国 NIST（国家标准技术研究所）网络安全框架的基础架构安全设置。适用于 PowerEdge 的 Dell CloudIQ 网络安全功能既支持轻松地创建策略，又能自动执行策略监管，具有简单、高效且可预测的优点。

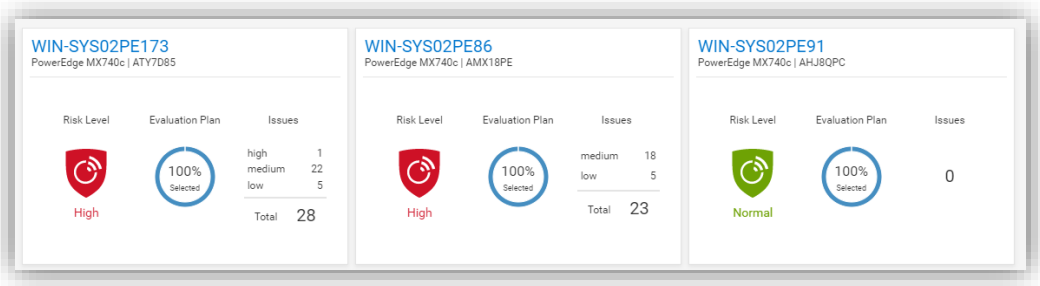


图 1 CloudIQ 网络安全控制面板

CloudIQ 是 AIOPs 主动监视和分析应用程序，针对戴尔基础架构解决方案（包括存储、数据保护、网络，当然还有 PowerEdge 服务器）提供系统运行状况见解和建议。CloudIQ 内置的网络安全策略引擎具有 30 多条可轻松实施的 PowerEdge 安全配置规则。CloudIQ 基于云，因此可通过 OME CloudIQ 插件在多个数据中心与任意数量的 OpenManage Enterprise (OME) 实例集成。这意味着 CloudIQ 可以将同一策略应用于任意位置的多台 OME 托管服务器。此功能由 CloudIQ 提供，无需在 iDRAC 或 OME 级别进行额外配置。建立策略后，CloudIQ 会参照当前“原样”配置持续检查 PowerEdge 安全配置设置的期望状态。如果发现服务器偏离策略合规性，便会突出显示该服务器。结果由 CloudIQ 进行评分，容易受攻击的服务器将被评为“高”风险级别。可以单独查看各个问题及建议的补救措施。然后，可使用 iDRAC GUI 对每台服务器逐一执行这些建议的安全配置更正，或者如果发现有多台主机不合规，则可使用 OME 提供配置更新模板文件，或执行 RACADM 脚本以更正多台服务器的安全配置。

自动化带来的好处

为了解自动执行此过程的深远影响，我们分别参照 1 台、10 台、100 台* 和 1,000 台* 服务器的手动过程进行了测试。基于我们对一个拥有 1000 台* 服务器的客户所用的 CloudIQ 网络安全方法进行的测试，我们发现了以下几点：

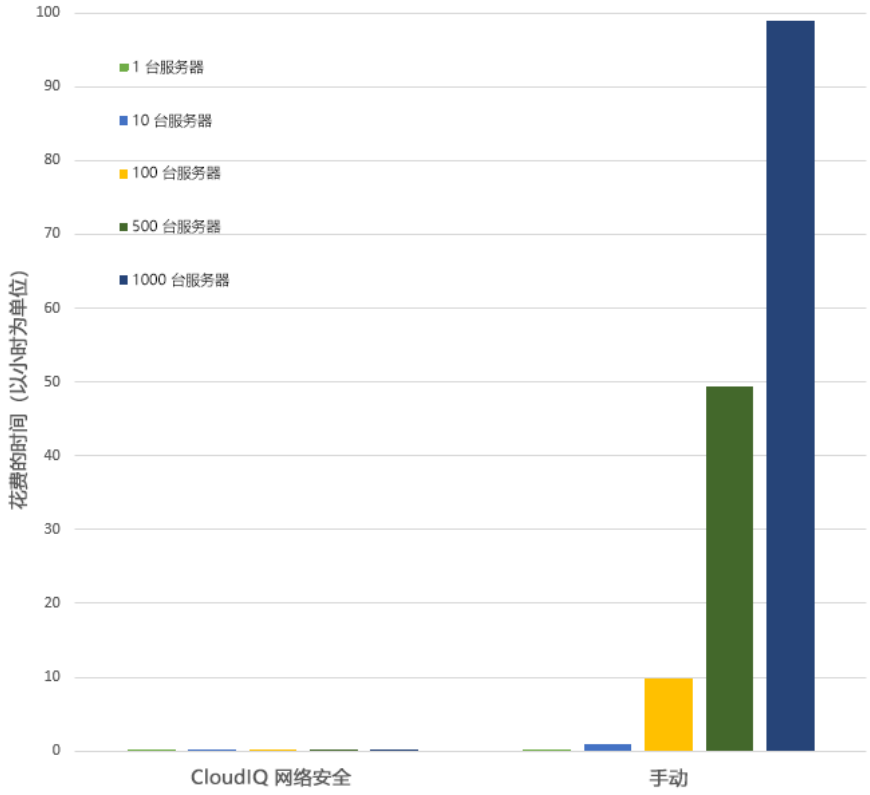
- 在不到 3 分钟的时间内创建一条包含 15 项测试的策略，并将其应用于 1000 台服务器*
- CloudIQ 完成任务的速度要比手动检查快 99%*。
- CloudIQ 将完成一次任务的时间缩短了 98 小时*。
- 与手动方法相比，使用 CloudIQ 网络安全自动化可立即节省超过一周的工作量*
- 启用后，CloudIQ 会持续定期监视所有这些关键安全配置设置

*基于对 1 台和 10 台服务器的结果分析得出的预计结果，客户结果可能有所不同

在实验室测试中，我们发现，在 iDRAC GUI 上手动检查 15 项设置需要 5 分 56 秒，而创建一条包含 15 个活动测试项的 CloudIQ 网络安全策略只花了 2 分 58 秒。此外，无论是为 1 台、10 台、100 台还是 1000 台服务器创建策略，该任务所花费的时间都是相同的。但是，使用手动过程时，每增加一台服务器就会额外增加 5 分 56 秒以完成检查。此外，在设置策略后，CloudIQ 会持续检查服务器是否符合“原样”设置。

结果摘要

考虑到所用的时间越短越好，以下图表突出显示了自动化与手动过程之间的差异，表明自动化可以节省大量时间。



有关完整的结果数据，请参阅本文档末尾的表 1。

测试概述

为了展示自动化的易用性和影响，我们测试了两种不同的方法：手动和自动化。要使用此 CloudIQ 网络安全功能，需要安装 OpenManage Enterprise 3.9“OME”或更高版本并启用 CloudIQ 插件 1.1 版或更高版本，PowerEdge 服务器享受 Dell ProSupport 服务，并且策略的目标服务器已被 OME 发现。要构建策略，必须在 CloudIQ 中为用户分配 CyberSec 管理员权限。测试安全策略中使用的一些配置规则是 iDRAC 默认值。但是，具有正确权限的管理员可以在单独的 iDRAC 上更改其中的任意值，这会造成安全缺陷。

图 2 配置数据流

测试程序

为确保准确比较测试方法，我们严格执行并记录了我们的测试。我们选择了 15 项常见设置，其中混合了 BIOS 和 iDRAC 配置值，并在试用策略中启用了 15 项测试。测试于 2022 年 7 月 6 日在戴尔位于奥斯汀的技术营销实验室设施内，使用戴尔的 CloudIQ 产品以在线方式进行。

I. USB 端口：禁用
II. iDRAC 主动 NIC：专用
III. 系统锁定：启用
IV. 来自主机的 iDRAC 配置：禁用
V. 基于 LAN 的 IPMI：禁用
VI. 安全启动：启用
VII. 密码策略：强
VIII. VNC：禁用
IX. SNMP 版本 3：启用
X. SSH：禁用
XI. 系统日志：启用
XII. Active Directory 身份验证：启用
XIII. IP 阻止：启用
XIV. 已加密虚拟介质：启用
XV. NTP 时间同步：启用

使用 CloudIQ PowerEdge 网络安全策略的自动化方法的步骤

从 CloudIQ“登录页面”https://cloudiq.emc.com 开始：

1. 登录 CloudIQ
2. 从屏幕左侧的菜单中选择“Cybersecurity”
3. 选择“Policy”
4. 选择“Templates”选项卡
5. 选择“Add Template”
6. 为模板命名
7. 从“Product”下拉菜单中选择“PowerEdge”，然后单击“Next”
8. 在“Template Evaluation Plan”中配置以下各项
9. Access Control — 勾选：IP blocking is enabled/SSH is disabled/The SNMP configured for V3/Active directory authentication is enable/VNC disabled
10. Audit and Accountability — 勾选：NTP time synchronization enabled /Remote Syslog enabled
11. Configuration Management — 勾选：configure iDRAC from Post/System lockdown enabled/USB ports disabled
12. Identification and Authentication — 勾选：Password has minimum strength score of strong
13. System and Communications Protection — 勾选：IPMI over lan disabled/virtual media encryption enabled/dedicated nic
14. System and Information Integrity — 勾选：secure boot enabled
15. 选择“Finish”
16. 选择“Systems”选项卡
17. 从主机列表中选择所需的主机（在我们的测试中，我们选择了 1、10、100 或 1000 的列表）
18. 单击“Assign”
19. 从模板下拉列表菜单中选择所需的模板
20. 从屏幕左侧的下拉菜单中选择“System Risk”以查看结果

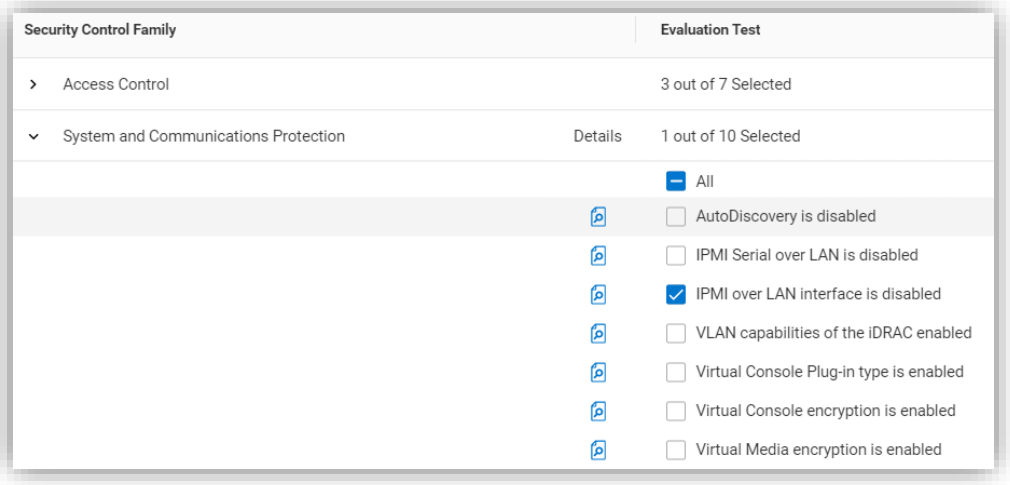


图 3 选择用于构建策略的规则

采用手动方法检查 iDRAC GIU 中的配置值的步骤

在显示 iDRAC 登录屏幕的浏览器中：

1. 登录
2. USB — Configuration/BIOS settings/integrated devices/user accessible USB ports：所有端口关闭
3. 安全启动 — Configuration/BIOS settings/TPM advanced /secure boot：启用
4. VNC — Configuration/Virtual console/VNC server/Enable VNC server：禁用
5. SNMPv3 — Configuration/System setting/Alert config/SNMP trap/SNMP setting/SNMP Trap format：SNMP v3
6. 系统日志 — Configuration/System settings/Alert configuration/Remote syslog settings/Remote syslog：启用
7. 虚拟介质加密 — Configuration/Virtual media/Attached media/Virtual Media encryption：启用
8. 专用端口 — iDRAC settings: Active NIC interface：专用
9. 本地 iDRAC 配置 — iDRAC settings/services/local config/disable iDRAC local configuration：启用
10. IPMI — iDRAC settings/connectivity/network/IPMI settings/Enable IPMI over lan：禁用
11. 密码策略 — iDRAC settings/users/global users settings/Password setting/Policy/Score：强 [1]
12. AD 身份验证 — iDRAC settings/Users/Directory services/Microsoft AD：启用
13. SSH — iDRAC settings/services/SSH/Enabled：禁用
14. IP 阻止 — iDRAC settings/Connectivity/Network/Advanced networking setting/IP blocking/Blocking：启用
15. NTP 时间同步 — iDRAC settings/settings/Time zone/NTP server/Enable NTP：启用
16. 锁定 — 检查屏幕右上角的挂锁图标是否显示锁定模式

使用 Dell PowerEdge R540 BIOS 2.12.2 和 iDRAC9 固件：5.10.00.00 进行测试

1. 手动强制执行强密码策略可确保新密码符合密码策略要求，但预先存在的帐户仍可能具有弱密码，CloudIQ 会标记任何具有弱密码的 iDRAC。

结果

服务器数量	CloudIQ 网络安全策略	手动检查
1	2 分 58 秒	5 分 56 秒
10	2 分 58 秒	59 分钟
100	2 分 58 秒	9 小时 53 分钟*
500	2 分 58 秒	49 小时 26 分钟*
1000	2 分 58 秒	98 小时 53 分钟*

表 1 — 测试结果

*基于对 1 台和 10 台服务器的结果分析得出的预计结果，客户结果可能有所不同

摘要

我们的测试表明，在 PowerEdge 网络安全策略引擎中使用 Dell CloudIQ 的自动化，在时间效率、可重复性、可预测性等方面都会带来很大优势，而且还能使您高枕无忧。我们推断，随着测试数据中的服务器数量增加，这些优势也会显著增加。

参考资料

Dell.com 上的 CloudIQ — 数据表和演示视频

博文《Take Control of Server Cybersecurity with Intelligent Cloud-Based Monitoring》

“构建和跟踪适用于 PowerEdge 服务器的 Dell CloudIQ 网络安全策略”视频

OpenManage Enterprise CloudIQ 插件技术知识页面

戴尔提供的其他网络安全相关解决方案

详细了解
PowerEdge 服务器

联系我们提供反馈
和请求

关注我们，获取 PowerEdge 新闻资讯