利用 Dell CloudIQ 加强服务器网络安全

摘要

组织可能需要多年时间才能在客户中建立良好的声誉，而网络安全相关事件只用几分钟就能将其毁于一旦。因此，网络安全团队和服务器管理员必须使用可获取的所有工具来强化基础架构。以下是每个戴尔 PowerEdge 客户都应该了解的一项 Dell CloudIQ 功能。

此 Direct from Development (DfD) 技术说明介绍了 CloudIQ 内置的适用于 PowerEdge 服务器的网络安全功能。

CloudIQ 是基于云 AI/ML 的监视和预测性分析应用程序，适用于戴尔基础架构产品组合。CloudIQ 在安全可靠的戴尔 IT 云中托管，可收集并分析运行状况、性能和遥测信息，以查明风险并建议采取操作来快速解决问题。

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

Dell CloudIQ 提供的网络安全功能现在支持戴尔 PowerEdge 服务器。利用 CloudIQ 内置的网络安全功能，客户服务器团队可以构建一个称为“评估计划”的策略。此评估计划是从一些现成的“点击勾选”配置标准测试构建而成。配置设置和值列表则以戴尔的最佳实践和美国 NIST（国家标准技术研究所）网络安全框架为基础。

快速获得结果的方法

具有正确技能并且了解确切的安全配置设置及正确值的专家，可以构建一个服务器配置文件“SCP”，并将其与 iDRAC 或 OME 配置模板功能一起使用，以设置服务器配置。但是，CloudIQ 提供了一种更快捷的规范性方法来实施基于戴尔建议的设置和值构建的网络安全评估策略。为了进一步优化网络安全流程，CloudIQ 可以聚合多个 OME 实例，提供涵盖多个位置的统一服务器视图。一些组织可能选择同时使用 OME 和 CloudIQ，以展示配置合规性与安全管理的分离。

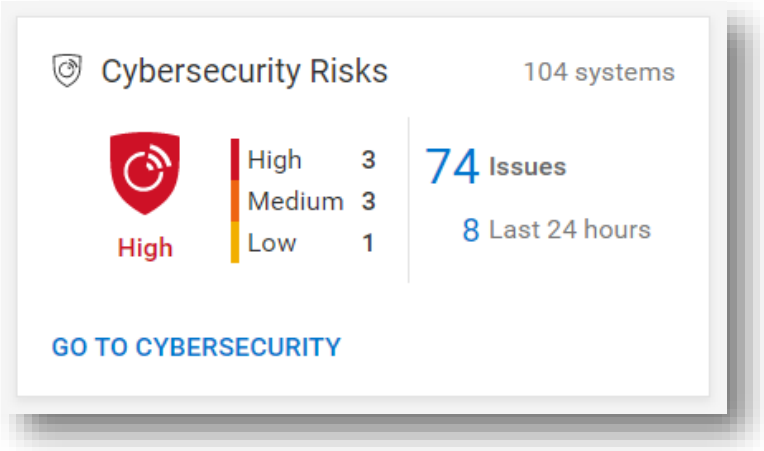

图 1 CloudIQ 概览页中的网络安全状态摘要

CloudIQ 概览页中的上述网络安全版块提供了汇总的风险级别状态视图（按每个风险类别划分系统数量）和检测到的问题总数。风险取决于每台服务器的问题数量和严重性。例如，具有一个或多个高风险问题的服务器被归为高风险类别，而具有五个以上非高风险问题且其中至少有一个为中等风险问题的服务器，也会被归为高风险类别。

快速识别风险

“System Risk”控制面板对每台应用了策略的服务器进行分类，在各自的卡中显示每台服务器的网络安全风险级别状态。这有助于客户快速确定各项措施的轻重缓急，并缩短解决问题花费的时间。

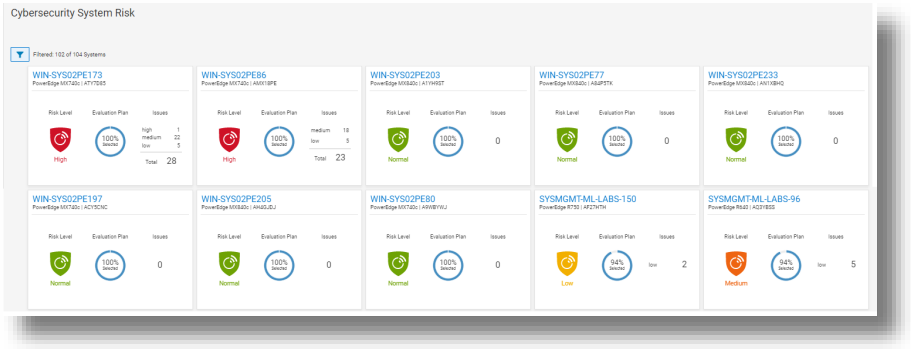

图 2 “Cybersecurity” -> “System Risk” -> “All Systems” 控制面板

除了该控制面板之外，安全评估状态还会显示每台服务器的详细信息，以及将任何偏离的安全配置恢复至首选状态的建议操作。环形图显示了所选规则数量占分配给特定服务器的风险评估计划中的测试总数的百分比。

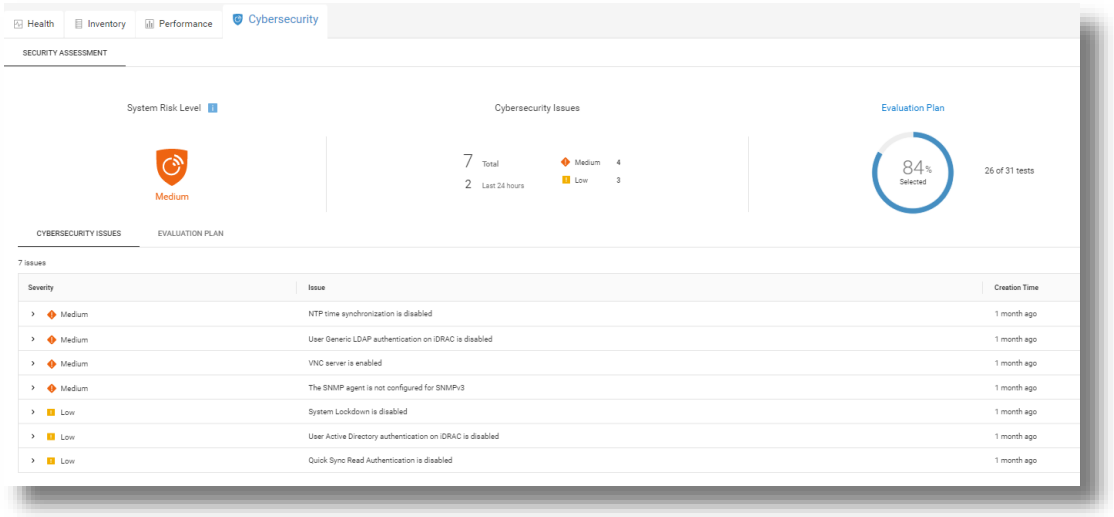

图 3　　网络安全风险详细信息和建议

在“Cybersecurity”选项卡下面的系统详细信息页面中，显示了有关评估计划及其状态的详细信息。页面底部有两个选项卡：“Cybersecurity Issues”详细说明了不合规元素及纠正措施；“Evaluation Plan”显示了整个计划及每项测试的选择状态。

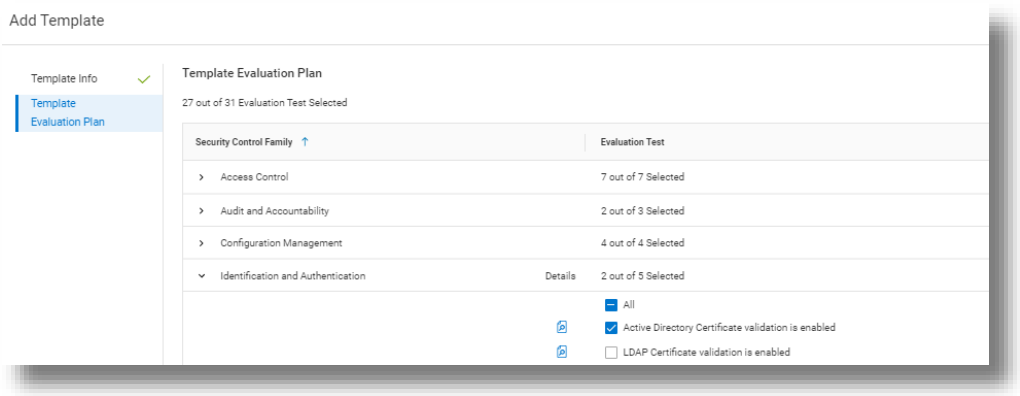

图 4 测试选择

CloudIQ 用户还可以选择接收每日摘要电子邮件，其中包含了网络安全状态摘要信息。

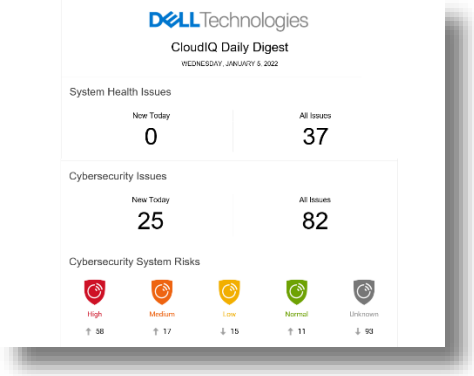

图 5 CloudIQ 每日摘要电子邮件

支持与安全性

如您所料，CloudIQ 内置了多种有关管理员和用户帐户的安全访问控制机制，以控制这些帐户的创建和报告。CloudIQ 内置了两个网络安全角色：“Cybersecurity Admin”和“Cybersecurity Viewer”。可以从具有 CloudIQ 管理员权限的帐户分配这些角色。

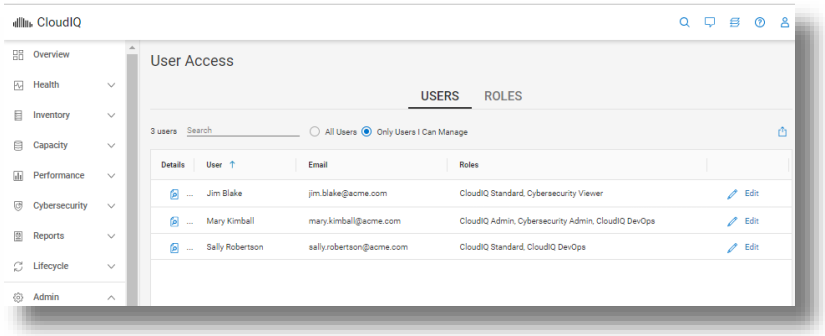

图 6 RBAC 设置

要在 CloudIQ 中支持适用于 PowerEdge 的网络安全功能，客户必须运行 OpenManage Enterpriser 3.9 或更高版本并启用 CloudIQ 插件 1.1 或更高版本。所有服务器都需要 Dell ProSupport 服务支持，并且必须已经被 OME 发现。

PowerEdge 网络安全评估计划测试元素

下表详细列出了每项测试标准及其所属的测试计划系列。

系列	标题
系统和通信	基于 LAN 的 IPMI 接口已禁用
系统和通信	基于 LAN 的 IPMI 串行已禁用
系统和通信	虚拟控制台加密已启用
系统和通信	虚拟介质加密已启用
系统和通信	自动发现已禁用
系统和通信	iDRAC 的 VLAN 功能已启用
系统和通信	iDRAC Web 服务器已启用 TLS 1.2 或 TLS 1.3
系统和通信	iDRAC Web 服务器 HTTP 请求已重定向到 HTTPS 请求
系统和通信	虚拟控制台插件类型已启用
系统和通信	iDRAC 正在使用专用 NIC
系统和通信	iDRAC Web 服务器已启用 TLS 1.2 或 TLS 1.3
访问控制	IP 阻止已启用
访问控制	VNC 服务器已禁用
访问控制	SNMP 代理程序配置为 SNMPv3
访问控制	对服务器的快速同步读取身份验证已启用
访问控制	SSH 已禁用
访问控制	iDRAC 上的用户通用 LDAP 身份验证已启用
访问控制	iDRAC 上的用户 Active Directory 身份验证已启用
配置管理	USB 端口已禁用
配置管理	Telnet 协议已禁用 [1]
配置管理	系统锁定已启用
配置管理	从 BIOS POST 配置 iDRAC 已禁用
审核和问责	NTP 时间同步已启用
审核和问责	NTP 受到保护
审核和问责	远程系统日志已启用
系统和信息完整性	主机系统上的“本地配置已启用”iDRAC 配置已禁用
系统和信息完整性	安全启动已启用
识别和身份验证	密码具有最低强保护评分
识别和身份验证	LDAP 证书验证已启用
识别和身份验证	Active Directory 证书验证已启用
识别和身份验证	使用 256 位或更高强度的 iDRAC Webserver SSL 加密
识别和身份验证	iDRAC Web 服务器 — SCEP 已启用

1. 从 iDRAC 固件版本 4.40.00.00 开始，从 iDRAC 中删除了 telnet 功能

摘要

不同于常见的 IT 团队成员，CloudIQ 不需要吃东西、休息，也不需要度假，因此组织可以依赖 CloudIQ 网络安全策略来持续监视不合规的服务器。CloudIQ 内置的网络安全让客户可以通过自动执行预定义的测试和状态可视化来加快实现服务器安全性。这为服务器管理员提供了极大的灵活性，同时还能保持网络安全团队需要实施的治理和控制。CloudIQ 通过在同一个基于云的便捷门户中显示服务器以及更广泛的戴尔基础架构产品组合的网络安全和系统运行状况，进一步降低了风险并提高了 IT 生产力。

参考资料

Dell.com 上的 CloudIQ — 获取产品信息、演示视频等

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