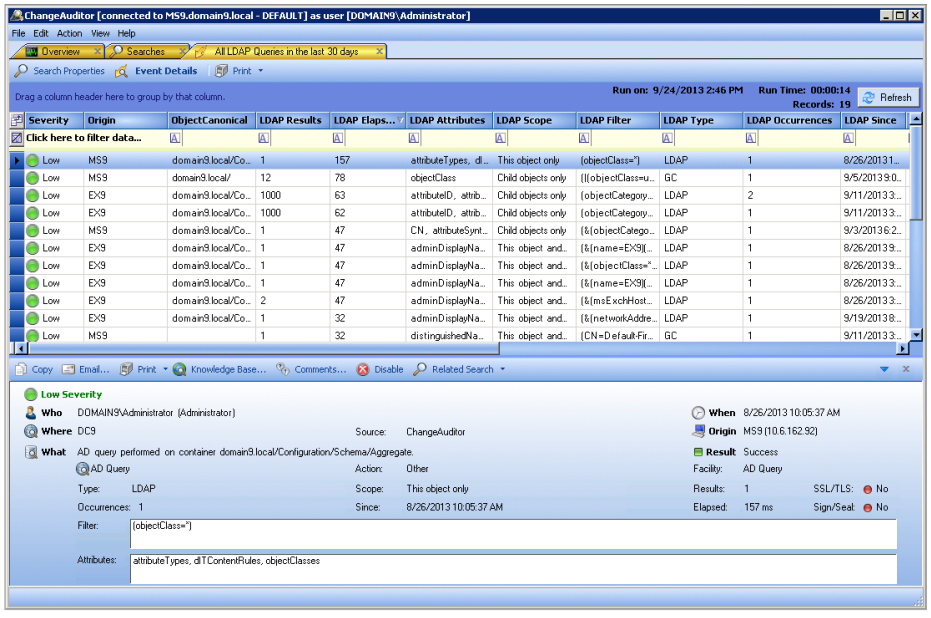
Change Auditor for Active Directory Queries

使用本机工具确定哪些应用程序和用户正在访问Microsoft Active Directory (AD)可谓天方夜谭，并且充满了风险，如果未正确监控这些访问，可能导致Active Directory环境无法运行。管理员将面临遗漏编写不当的查询或影响性能的缓慢查询的风险，如果不知道哪些应用程序已硬编码，哪些应用程序依靠AD，则可能给迁移和整合造成中断。由于无法监控和评估查询，组织发现很难优化他们为用户提供的服务，也很难计划迁移或者执行目录整合。为了实现和维护AD的稳定性以及对法规和策略的合规性，组织必须能够确定和衡量Active Directory查询的性能。

Quest® Change Auditor for Active Directory Queries可以实时跟踪、分析和报告所有Active Directory查询，将其转换为简单的术语，从而消除审核所需的时间以及复杂性。只需进行一次快速的浏览即可立即探明查询及其结果，从而确定是否需要进一步调查。

最重要的是，使用Change Auditor for Active Directory Queries，您可以通过有关人物、事件、时间、地点和工作站的取证数据全面地洞察随着时间的推移进行的所有查询，包括任何相关查询。利用发送到任意设备的实时警报，您可以立即解决问题并避免系统停机。



使用Change Auditor，您可以实时查看所有Active Directory查询的结果，并即时洞察不符合内部安全策略的查询。

优势：

- 缩短每个Active Directory查询获取详细信息所花费的时间
- 通过识别针对Active Directory的不符合内部安全策略的不安全或未签名查询，加强内部控制
- 通过识别正在执行可能影响域控制器性能的查询的工作站和服务器，提高可用性
- 通过确定哪些计算机需要连接，协助执行迁移的发现过程
- 实时向任意设备发送警报，以便立即做出响应，从而降低安全风险
- 优化内部策略和合规法规（包括GDPR、SOX、PCI DSS、HIPAA、FISMA、SAS 70等）
- 将信息转化为智能的详细取证数据，供审核人员和管理人员使用

审核所有重要的AD查询

Change Auditor为针对Active Directory的所有查询提供广泛且可自定义的审核和报告。此外，每个事件都将显示查询的范围、使用的过滤器、属性和返回结果的数量。您还能发现针对Active Directory的不符合内部安全策略的查询以及编写不当从而降低Active Directory性能的查询。

跟踪查询活动

Change Auditor for Active Directory Queries可以定位所有查询，然后按类型、位置、用户等来过滤搜索。您可以轻松查看哪些工作站和服务器正在执行影响AD性能的查询，并了解哪些计算机在迁移过程中和迁移之后需要连接。

利用全天候的实时警报、深入的分析和报告功能，您始终可以了解在您的环境中正在发生的情况。

将相关数据转化为有意义的信息以提高运营效率

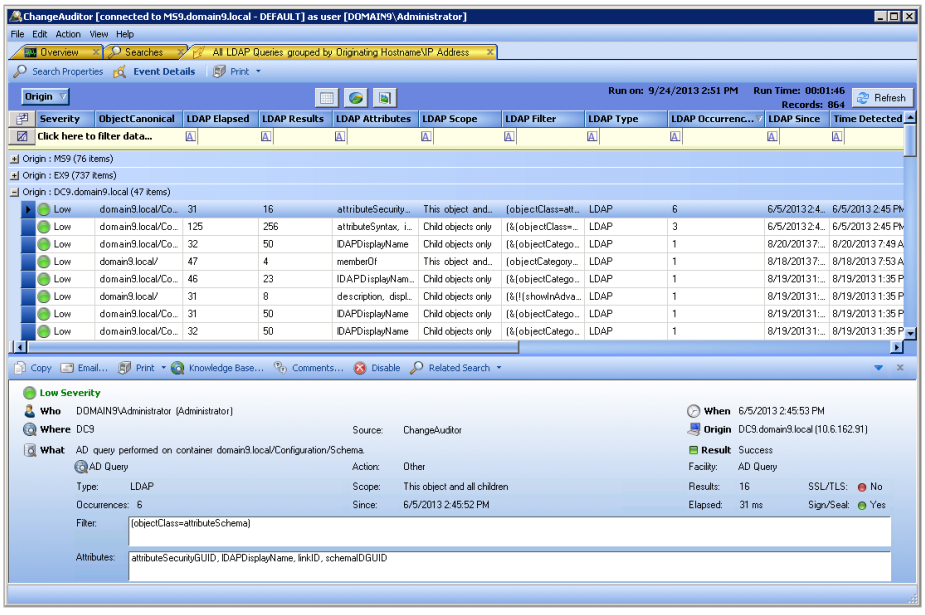
Change Auditor for Active Directory Queries可以跟踪针对Active Directory环境的查询，然后将原始数据转化为有意义的智能数据，以确保基础架构高效并提供详细的分析。无需本机审核日志，您可以更快获得结果并节省存储资源。

透视您的ACTIVE DIRECTORY环境

您将能够详细了解在您环境的后台中进行的所有活动。Change Auditor for Active Directory Queries是准备进行迁移的企业的理想选择，可以帮助他们做好准备来制定灾难恢复一致性计划或收集Active Directory深度信息。

关于QUEST

Quest致力于为瞬息万变的企业IT领域提供软件解决方案。我们帮助简化数据爆炸、云扩展、混合数据中心、安全威胁以及合规要求所带来的挑战。我们的产品组合包括用于数据库管理、数据保护、统一端点管理、身份和访问管理以及Microsoft平台管理的解决方案。



利用按起因和发生次数对结果进行分组、排序和过滤的功能，消除降低性能的重复查询。

Quest
quest.com/cn
有关当地办事处信息，请访问 (quest.com/cn-zh/locations)

DataSheet-ChangeAuditor4ADQ-US-KS-zh_CN-WL-39991