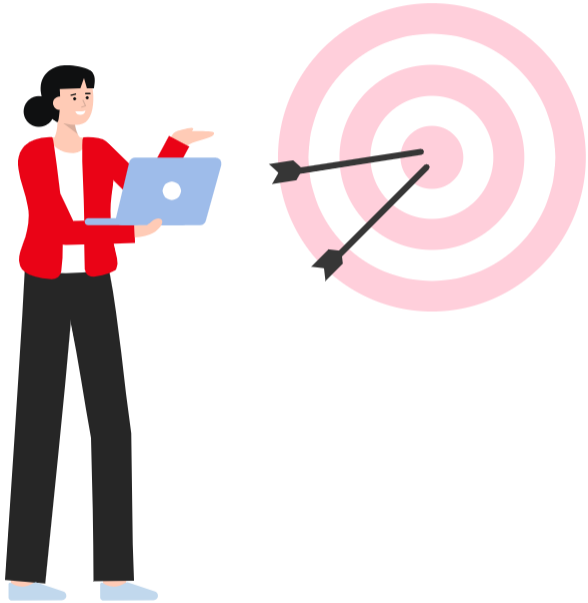
Windows Server的日志管理

2024-04-28

目录

01

Windows Server日志概述



Windows Server日志概述

日志管理概述:

简要介绍Windows Server上日志的作用和重要性。

表格章节内容:

日志管理常见术语表

日志管理概述

日志分类:

介绍Windows Server中常见的日志类型及其功能。

日志记录:

解释日志记录的过程以及如何查看和分析日志内容。

日志保留策略:

讨论日志保留的重要性，以及设置合适的日志保留策略。

表格章节内容

术语	解释	示例
日志级别	表示日志的优先级或严重程度	INFO, ERROR, WARNING
事件ID	标识特定事件或错误的唯一编号	1001, 2004
日志轮换	日志文件达到一定大小或时间后自动	每周轮换

日志轮换 日志轮换 日志轮换 每周轮换 每周轮换 每周轮换 或清除

02

Windows Server日志设置

Windows Server日志设置

日志配置:

步骤指南如何设置Windows Server的日志记录和存储选项。

章节内容:

Windows Server日志筛选与导出

日志配置

事件查看器设置

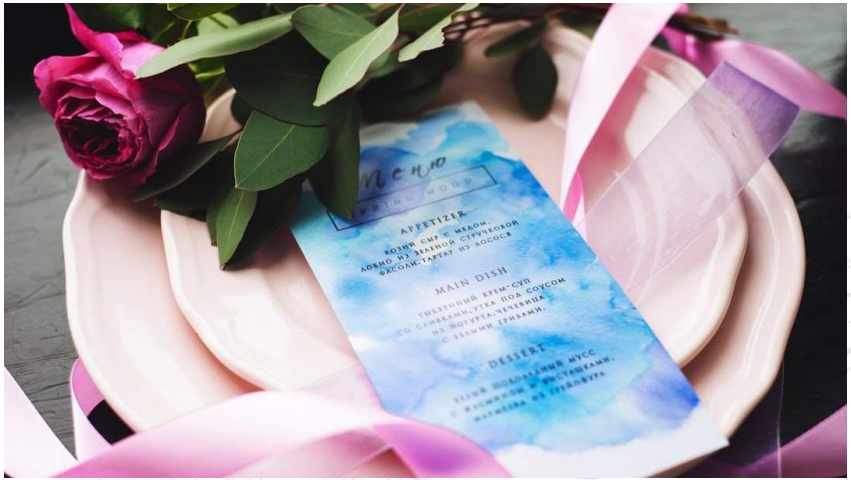
如何在事件查看器中配置日志记录参数。

日志文件位置

指导用户设置日志文件的存储位置和保留策略。

事件订阅

介绍如何创建和管理事件订阅，以便跟踪特定类型的事件。



章节内容

1

筛选条件设置:

指导如何根据特定条件筛选Windows Server日志。

2

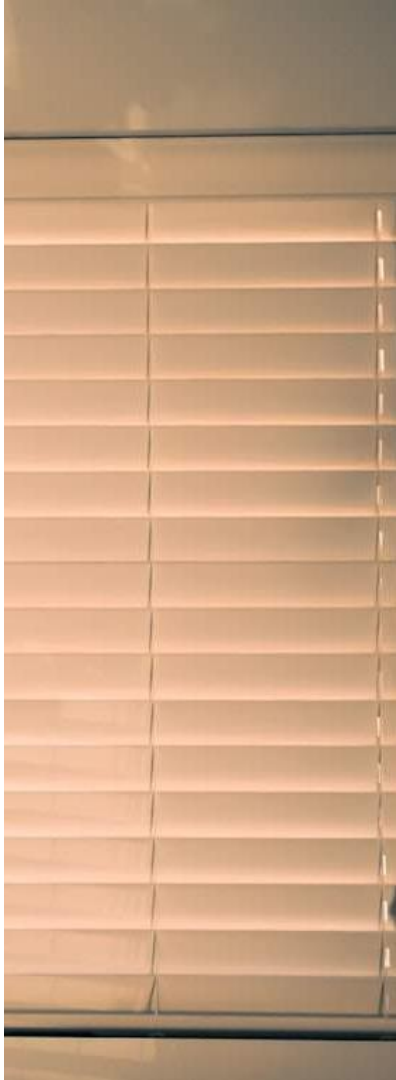
导出日志:

解释如何将日志数据导出到其他格式或工具进行进一步分析。

3

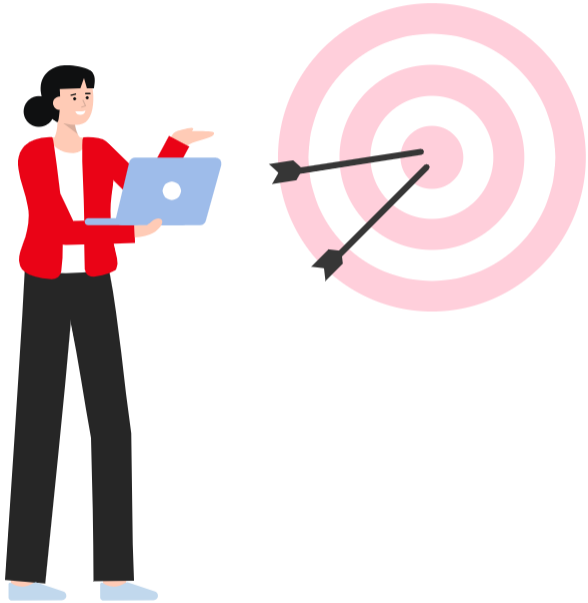
日志备份:

推荐最佳实践，以确保日志备份的安全和完整性。



03

Windows Server日志分析



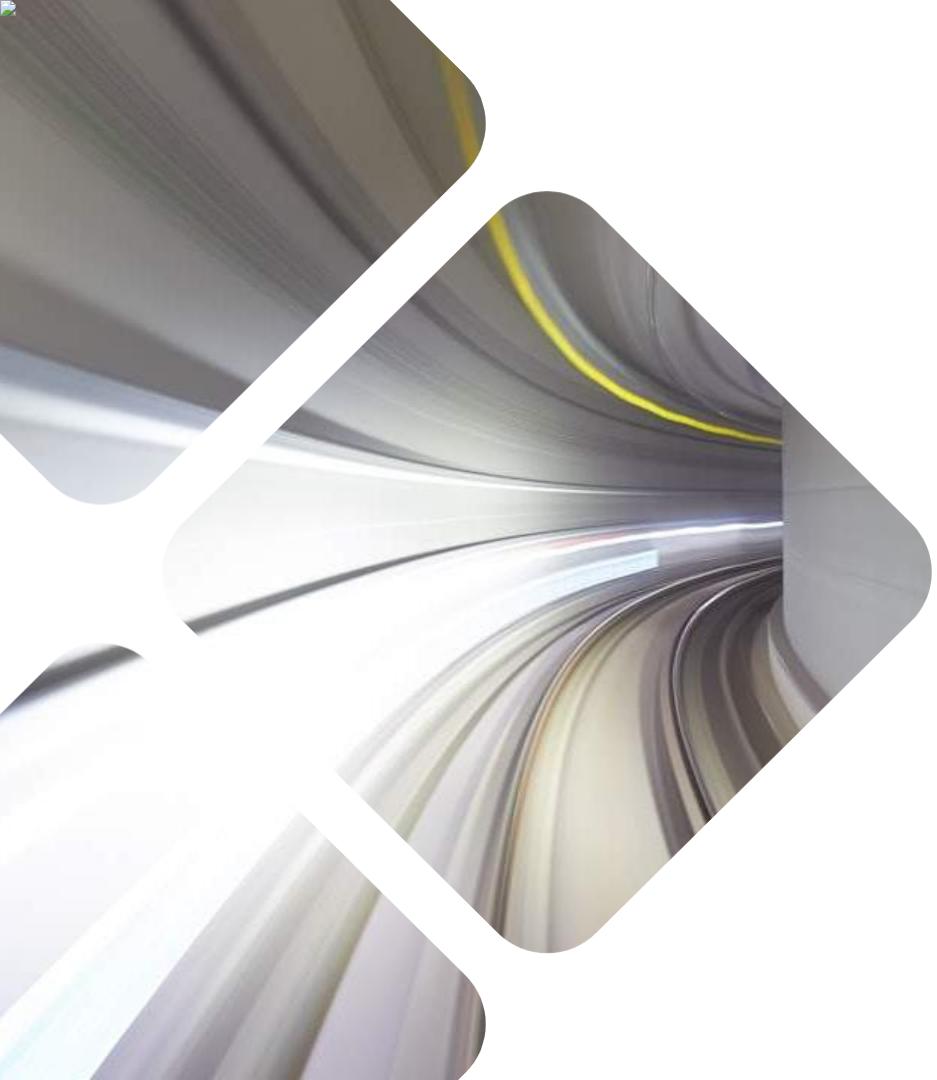
Windows Server日志分析

日志分析工具:

推荐一些用于分析Windows Server日志的工具和技术。

章节内容:

Windows Server日志异常检测



日志分析工具

Windows PowerShell:

介绍如何使用PowerShell脚本来分析和处理日志数据。

第三方工具:

推荐一些功能强大的第三方日志分析工具和软件。

图形化分析:

如何使用图形化界面进行日志分析和可视化呈现。

章节内容

异常检测算法:

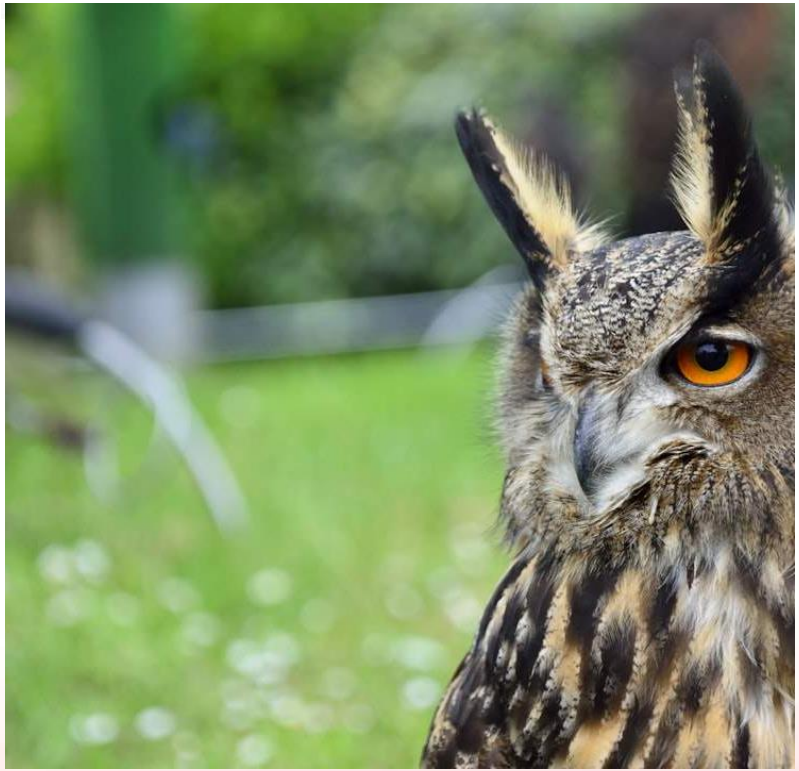
探讨常用的异常检测算法在日志分析中的应用。

异常事件警报:

设置异常事件警报，以便及时发现系统问题。

实时监控:

介绍如何实时监控日志以快速响应异常情况。



04

Windows Server日志安全性

Windows Server日志安全性

日志保护:

讨论如何保护Windows Server日志免受篡改和未经授权访问。

章节内容:

Windows Server日志审计

日志保护

访问控制:

设定合适的访问权限，防止未经授权的用户查看或修改日志。

加密传输:

如何加密传输日志数据，确保在传输过程中的安全性。

完整性验证:

检查日志文件的完整性，以确保日志未被篡改。

章节内容

审计设置

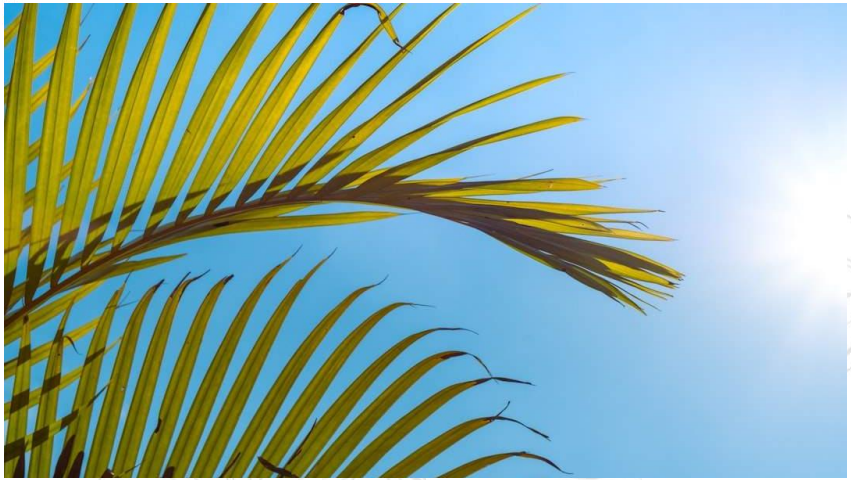
详细介绍如何配置Windows Server的审计功能，跟踪系统操作。

审计策略

制定合适的审计策略，以满足安全合规要求。

审计日志分析

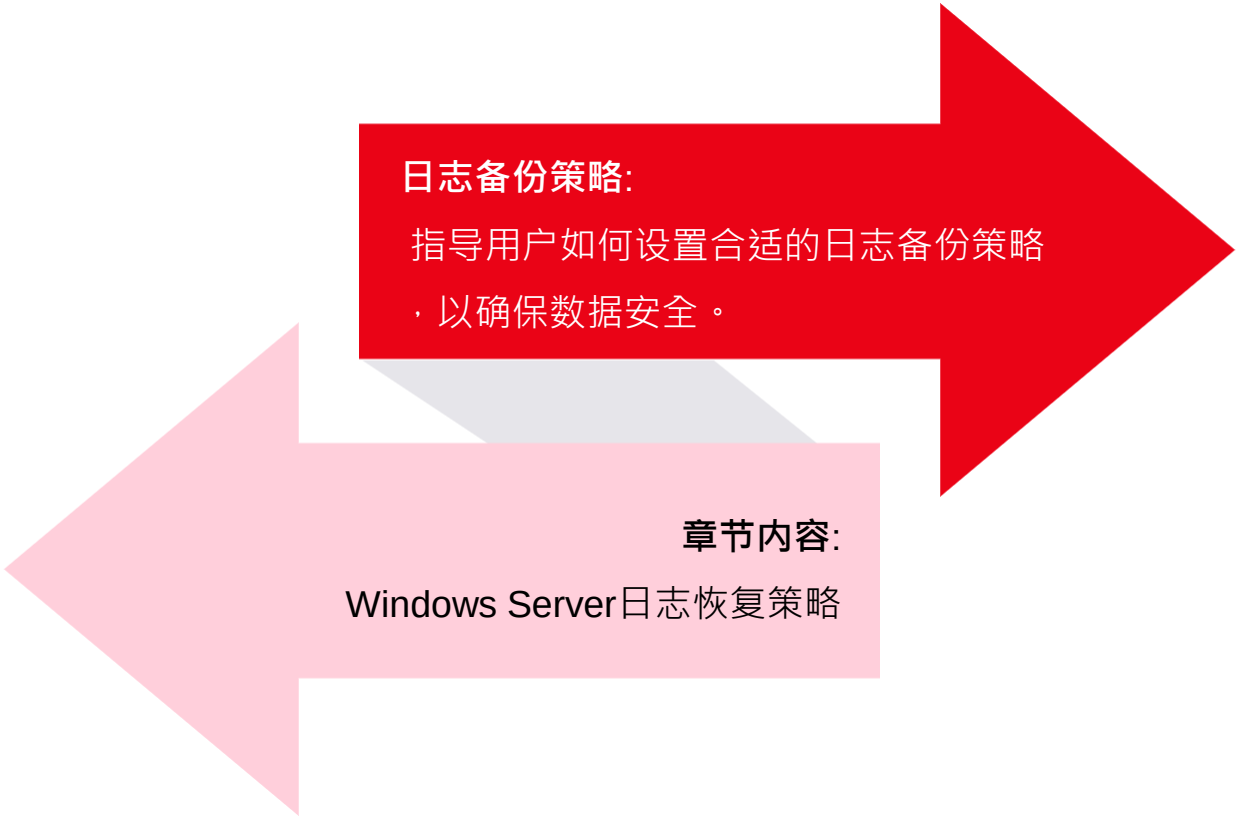
如何分析审计日志并识别潜在的安全威胁。



05

Windows Server日志备份与恢复

Windows Server日志备份与恢复

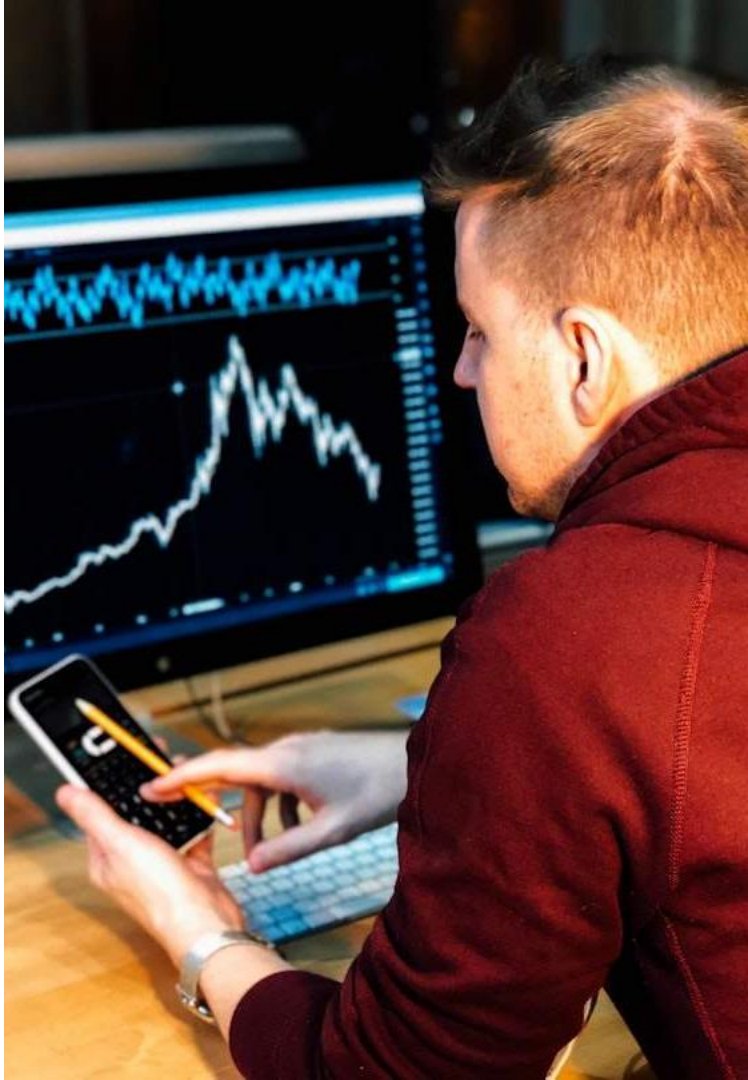


日志备份策略

1. **定期备份**:
   建议定期备份日志数据，以防止数据丢失。

2. **备份存储**:
   如何选择合适的备份存储介质，如云存储或外部硬盘。

3. **恢复流程**:
   解释日志数据的恢复流程，包括如何恢复被误删除的日志文件。



章节内容

日志恢复方法:

介绍不同情况下的日志数据恢复方法和工具。

灾难恢复:

讨论如何在灾难情况下快速恢复日志数据。

数据完整性校验:

如何验证恢复的日志数据的完整性和准确性。

汇报结束

谢谢观看