安全加社区

公益译文项目

2020

网络安全框架制造篇

低影响性示例实施指南：

第 2 卷—流程型制造系统用例

NISTIR 8183A-2

美国国家标准与技术研究院（NIST）

美国商务部

2019 年 9 月

文档信息			
原文名称	Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case		
原文作者	Keith Stouffer，Timothy Zimmerman，CheeYee Tang，Jeffrey Cichonski，Michael Pease，Neeraj Shah，Wesley Downard	原文发布日期	2019 年 9 月
原文发布单位	美国国家标准与技术研究院（NIST）		
原文出处	https://doi.org/10.6028/NIST.IR.8183A-2		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

免责声明

• 本文原文来自于互联网的公共方式，由“安全加”社区出于学习交流的目的进行翻译，而无任何商业利益的考虑和利用，“安全加”社区已经尽可能地对作者和来源进行了通告，但不保证能够穷尽，如您主张相关权利，请及时与“安全加”社区联系。

•“安全加”社区不对翻译版本的准确性、可靠性作任何保证，也不为由翻译不准确所导致的直接或间接损失承担责任。在使用翻译版本中所包含的技术信息时，用户同意“安全加”社区对可能出现的翻译不完整、或不准确导致的全部或部分损失不承担任何责任。用户亦保证不用做商业用途，也不以任何方式修改本译文，基于上述问题产生侵权行为的，法律责任由用户自负。

摘要

本文档提供了概念验证（PoC）方案示例，展示在流程型制造环境中如何按照《网络安全框架（CSF）制造篇》中的低影响性要求来部署使用开源产品和商用现成品（COTS）。PoC 方案示例包括在实施过程中观察到的对网络、设备和业务性能的影响。各制造商应自行确定实施哪些方案内容。实施时应考虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。《网络安全框架制造篇》与制造业的目标和行业最佳实践保持一致，为制造商管理网络安全风险提供了思路。它所提出的基于风险的方法可自愿实施，用于管理与制造系统相关的网络安全活动及网络风险。该文档是对制造商当前所采用的网络安全标准和行业指南的补充而非替代。

关键词

计算机安全；网络安全框架（CSF）；分布式控制系统（DCS）；工业控制系统（ICS）；信息安全；制造业；网络安全；可编程逻辑控制器（PLC）；风险管理；安全控制；数据采集与监控系统（SCADA）

补充内容

本指南其余两卷为：

NISTIR 8183A 第 1 卷，网络安全框架制造篇低影响性示例实施指南：第 1 卷—总体指导，https://doi.org/10.6028/NIST.IR.8183A-1

NISTIR 8183A 第 3 卷，网络安全框架制造篇低影响性示例实施指南：第 3 卷—离散型制造系统用例，https://doi.org/10.6028/NIST.IR.8183A-3

使用说明

本指南介绍了用于保护制造环境的 PoC 方案，该方案仅在实验室环境中进行了测试。各制造商应自行确定实施哪些方案内容。实施时应虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。欢迎您对指南内容提出反馈意见，后续版本将根据各方建议、意见和成功案例进行优化。请将反馈发至 CSF_Manufacturing_Profile_Implementation@nist.gov。

将根据《网络安全框架》1.1 版更新进行修订

《网络安全框架制造篇》（NISTIR 8183）起草并发布之时，《网络安全框架》为 1.0 版本。《实施指南》围绕《网络安全框架制造篇》初始版本中的内容，提供了实施指导和 PoC 方案示例。

《网络安全框架制造篇》（NISTIR 8183）拟根据《网络安全框架》1.1 版本中的更新内容进行修订并对外发布，代号为 NISTIR 8183（修订版 1）。

NISTIR 8183（修订版 1）发布后，《实施指南》会随即修订，合入《网络安全框架》1.1 版本中的内容，并对外发布，代号为 NISTIR 8183A（修订版 1）。

执行摘要

本文档提供了概念验证（PoC）方案示例，展示在流程型制造环境中如何按照《网络安全框架（CSF）制造篇》[4]中的低影响性要求来部署使用开源产品和商用现成品（COTS）。制造系统的完整性、可用性或机密性被破坏后，若预期对生产运营、制成品、资产、品牌形象、财务、人员、公众或环境仅会造成有限的负面影响，则该类系统的潜在影响级别为低。“有限的负面影响”指完整性、可用性或机密性被破坏后，可能会：

- 导致任务能力在一定时间内有一定程度的下降，系统仍可执行主要功能，但执行效果明显降低；
- 对运营资产造成较小损害；
- 造成轻微的财务损失；或
- 对个人造成轻微伤害。

PoC 方案示例包括在实施过程中观察到的对网络、设备和业务性能的影响。各制造商应自行确定实施哪些方案内容。实施时应虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。

《网络安全框架制造篇》与制造业的目标和行业最佳实践保持一致，为制造商管理网络安全风险提供了思路。它所提出的基于风险的方法可自愿实施，用于管理与制造系统相关的网络安全活动及网络风险。该文档是对制造商当前所采用的网络安全标准和行业指南的补充而非替代。

《网络安全框架制造篇》重点阐述了期望的网络安全结果，可作为规划方案，指导读者识别机会，改善制造系统的网络安全状况。它根据特定的业务/任务目标，为安全活动划分了优先级，同时确定了哪些安全实践具有可操作性，可以为关键业务/任务目标提供支撑。

PoC 方案采用了商业产品，但这并不代表本手册为这些产品背书或保证其符合法规要求。各组织的信息安全专家应选用与其现有工具和制造系统基础架构最为契合的产品。组织可自愿采用这些方案或采用整体上遵循这些指导方针的方案，也可以基于本手册，对方案进行部分定制和实施。本指南不包含任何规范或强制性实践内容，也不具有法律效力。

目录

1. 概述

根据 13636 号行政命令《提升关键基础设施的网络安全》[1]开发的自愿性《网络安全框架》提供了主次鲜明、基于性能的灵活方法，该方法可重复使用，具有成本效益，用以管理关键基础设施服务交付中直接涉及的流程、信息和系统的网络安全风险[1]。

《网络安全框架》是基于风险的自愿性指导文件，包括行业标准和最佳实践，旨在帮助组织管理网络安全风险[2]。本框架是政府和私有部门的合作成果，采用通用语言阐述了如何基于业务需求高效地应对并管理网络安全风险，但并未提出合规要求。

针对制造业需求，政府与私营部门再次合作，制定了《网络安全框架制造篇》[4]，为制造系统及其环境中实施网络安全控制提供了可行方法。《制造篇》为保护制造系统及其组件、设施和环境定义了网络安全活动和期望结果。基于该文档，制造商可将网络安全活动与业务需求、风险承受能力和资源对齐。《制造篇》包含标准、指导方针和行业最佳实践，提供了适用于制造业的网络安全方法。

1.1 目的与范围

许多中小型制造商表示，实施基于标准的网络安全计划颇具挑战性。本文档提供了概念验证（PoC）方案示例，展示在流程型制造环境中如何按照《网络安全框架（CSF）制造篇》中的低影响性要求来部署使用开源产品和商用现成品（COTS）。制造系统的完整性、可用性或机密性被破坏后，若预期对生产运营、制成品、资产、品牌形象、财务、人员、公众或环境仅会造成有限的负面影响，则该类系统的潜在影响级别为低。“有限的负面影响”指完整性、可用性或机密性被破坏后，可能会：

- 导致任务能力在一定时间内有一定程度的下降，系统仍可执行主要功能，但执行效果明显降低；
- 对运营资产造成较小损害；
- 造成轻微的财务损失；或
- 对个人造成轻微伤害。

PoC 方案示例分别针对流程型制造环境（第 2 卷）和离散型制造环境（第 3 卷），描述了实施方案对网络、设备和业务性能的影响。各制造商应自行确定实施哪些方案内容。实施时应虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。《网络安全框架制造篇》与制造业的目标和行业最佳实践保持一致，为制造商管理网络安全风险提供了思路。它所提出的基于风险的方法可自愿实施，用于管理与制造系统相关的网络安全活动及网络风险。该文档是对制造商当前所采用网络安全标准和行业指南的补充而非替代。

PoC 方案采用了商业产品，但这并不代表本手册为这些产品背书或保证其符合法规要求。各组织的信息安全专家应选用与其现有工具和制造系统基础架构最为契合的产品。组织可自愿采用这些方案或采用整体上遵循指导方针的方案，也可以基于本手册，对方案进行部分定制和实施。本指南不包含任何规范或强制性实践内容，也不具有法律效力。

本项目有以下假设：

- 方案基于实验室环境开发；
- 实验室环境模拟了典型的小型制造商环境；
- 实验室环境无法反映生产环境的复杂性；且
- 组织可获取实施制造业网络安全方案所需的技能和资源。

1.2 读者对象

本文档涉及制造系统相关细节信息。读者应熟知运营技术、计算机安全方面的一般概念以及通信协议（如网络中使用的协议）。目标受众包括如下各类人员：

- 设计或实施安全制造系统的控制工程师、集成人员和架构师；
- 管理、修复或保护制造系统的系统管理员、工程师等专业信息技术（IT）人员；
- 负责管理制造系统的人员；
- 高级管理人员，这部分人群为证明有必要实施制造系统网络安全计划以减轻对业务运行的影响而须了解前因后果；以及
- 欲了解制造系统独特安全需求的研究人员、学术机构和分析师。

1.3 文档结构

第 2 卷主要包括如下内容：

- 第 2 章概述了流程型制造系统用例。
- 第 3 章详述了适用于流程型制造系统用例的政策和程序文件。
- 第 4 章详述了适用于流程型制造系统用例的技术能力实现和相关性能测量方法。
- 附录 A 列举了本文档中使用的缩略词。
- 附录 B 提供了本文档使用的术语表。
- 附录 C 列举了本文档编写过程中所参考的文献。

2. 流程型制造系统低影响性用例

2.1 概述

本概念验证（PoC）用例展示了在流程型制造环境中如何按照《网络安全框架（CSF）制造篇》中的低影响性要求来部署使用开源产品和商用现成品（COTS）。各制造商应自行确定实施哪些方案内容。实施时应虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。

2.2 流程型制造系统低影响性用例

韦斯特曼工业公司（Westman Industries，简称“韦斯特曼”）是一家虚构的商用化工产品制造商，其产品用于运输、建筑施工等行业。公司总部位于韦斯特兰（Westland），一个人口约 10 万的城市。

除定期维护停机（每年约 2 周时间，通常在 12 月底）外，韦斯特曼的生产设施每天 24 小时、每周 7 天（24/7）连续运营。

为提高工业竞争力，韦斯特曼引进了过程自动化设备，以提高生产效率，降低生产成本。厂房里部署了工业自动化设备，如可编程逻辑控制器（PLC）、人机界面（HMI）和历史数据库（Data Historian），监控生产作业。

2.2.1 使命

韦斯特曼的使命是为工业应用提供优质化工产品。

2.2.2 厂区

韦斯特曼厂区是一座约 5000 平方米的单体建筑，拥有约 3500 平方米的生产空间，包括生产区、配送区和化学品地上储罐区。厂区的其余部分为行政管理和工程办公区。

厂区有围墙，围墙大门在上班时间打开，下班后上锁。主楼有两个入口，一个用于员工出入，部署了工卡访问系统，员工必须刷卡才能进入大楼。另一个入口位于前厅，在正常上班时间有专人在岗，接待访客。访客在进入大楼或厂房前须登记并领取相应身份证明。韦斯特曼厂区的大门或入口没有安排外包保安值守。

2.2.3 员工

韦斯特曼有 200 名正式员工，大部分在制造车间工作。由全职制造/控制工程师组成的小组采用制造、控制和自动化设备控制生产过程，确保生产系统安全高效运行。

韦斯特曼还拥有一支小型 IT 队伍，专门负责企业 IT 系统。

韦斯特曼高管的头衔和职责如下：

韦斯特曼管理层	主要职责
首席执行官（CEO）	管理整个公司。
运营总监	监管生产运营，管理生产人员和控制工程师，向CEO汇报。
产品开发总监	监管产品开发，管理现场化学专业人员，向CEO汇报。
市场总监	监管市场与销售业务，向CEO汇报。
财务总监	管理财务人员，向CEO汇报。
法务总监	处理所有的法律事宜，向CEO汇报。
IT经理	管理IT人员，向CEO汇报。
HR经理	管理HR人员，向CEO汇报。

2.2.4 供应链

生产过程要持续进行须使用原材料。原材料一般基于与供应商签订的长期合同供应，定期运至工厂。

制成品通常批发出售，产品运输分包给多家物流公司，负责从韦斯特曼工厂运送至最终客户，即其他工业制造商，他们通常在自己的化学生产过程中将韦斯特曼产品用作原材料或添加剂。

2.2.5 配套服务

韦斯特曼需要的配套服务包括电力、天然气、水和互联网。宽带互联网连接由一家大型全国网络服务商根据商业级服务水平协议提供。

2.2.6 法律法规要求

作为一家化工产品制造商，韦斯特曼及其员工必须遵守联邦和州对化学品和有害物质的所有法律法规要求。韦斯特曼还须遵守所有的法律、法规和安全要求。

2.2.7 关键基础设施

根据第 21 号总统政策令（PPD-21），化工行业属于关键基础设施。

2.2.8 生产过程

制造系统主要包括五个化学处理部件：反应器、产品冷凝器、气液分离器、循环压缩机和分离最终产品的汽提塔。制造系统有 12 个阀门，用于控制系统中的化学品流动，还有 41 个传感器进行测量，用于监控化学过程。所有阀门和传感器通过 DeviceNet 通信总线连接到自动化设备（PLC）。阀门配有手动超控装置，以便工人在紧急情况下超控自动化设备。

原料送入反应器后进行混合，发生反应，产生的物质流向下游的产品冷凝器和气液分离器。反应后仍是气态的物质在压缩机内循环，然后回送到主反应器中。组分在冷凝后连续流入产品汽提塔，汽提塔将其分离，形成最终产品。在此过程的各个阶段，采集质量保证样品，验证产品质量和流程效率。

2.2.9 系统

行政办公室的支持团队是 IT 小组，主要使用常规的企业 IT 应用程序（如电子邮件、Web 应用程序和企业规划应用程序）。

IT 人员维护一个中央文件存储系统，其中存储了源代码、化学式、图纸、工序和图表，并定期备份。产品开发人员和制造工程师有权访问该系统。

IT 人员还在制造车间安装配置了历史数据库，记录生产过程数据。IT 人员定期对历史数据库进行数据备份，制造工程师对该数据库进行配置和操作。

2.2.10 数据

通过公司网络传输、存储的数据包括：

- PLC 程序代码
- 化学式及计算过程
- 工作流和操作手册及文档
- 电气图
- 网络图
- 质量保证程序
- 历史生产数据

注：上述所有数据均为私有、商业机密或敏感数据。

2.2.11 网络

行政办公室内的 IT 系统连接到由 IT 团队管理的公司网络。制造车间有独立的自动化设备网络，由制造工程师管理。

制造网络包括典型的基于以太网的 TCP/IP 网络和其他工业协议如 DeviceNet。

有些生产设备厂商要求韦斯特曼允许远程访问设备。厂商获取授权后，通过远程访问连接到制造设备提供维护和支持。

2.2.12 任务目标

- 保护人员安全

  韦斯特曼以制造系统的安全运行为己任，始终将员工安全作为头等大事。所有的制造工艺、协议、自动化过程和设备、作业程序和指南在设计时都充分考虑了人员安全。

- 保护环境安全

  韦斯特曼遵守有关环境安全的所有适用法规。韦斯特曼确保其生产过程不影响环境，尽力减少环境足迹。每季度对生产造成的环境影响进行评审。

- 保证产品质量

  韦斯特曼拥有世界领先的生产设备和工艺，采用最先进的自动化、设备和技术确保产品质量。公司建立了质量保证程序，使用自动化设备（包括高速控制网络中的 PLC、历史数据库和高精度传感器）监控产品质量。

- 实现生产目标

  韦斯特曼的一个重要目标是完成月度生产目标，这不仅可确保向客户及时供货，也有助于维护公司的财务稳定性。

  韦斯特曼基于 7x24 生产模式规划生产运营，满足生产目标和客户需求。公司在自动化设备和熟练专业人员方面进行投资，确保完成月度生产目标。

- 保护商业机密

  韦斯特曼倾力保护其商业机密，包括产品开发、制造工艺、产品质量和供应链管理。

3. 政策和程序实施

本章以虚构的韦斯特曼公司为例，介绍了为其开发的政策程序文件和声明。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的政策程序文件和声明。

3.1 网络安全计划文件示例

本节以为韦斯特曼公司（虚构）开发的政策程序文件和声明为例，介绍了网络安全计划文件中所包含的内容。本文中提到的商业实体、设备、材料等或有标识，仅为准确描述概念之用，并非暗示 NIST 推荐或认可，也不表明这些实体、设备、材料是实现目的之最佳选择。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的内容及政策程序文件和声明。

韦斯特曼
网络安全计划

文件负责人	运营总监

版本信息

版本号	日期	说明	作者
1.0	2018-02-22	新建文档	运营总监
2.0	2018-04-21	对最初版本做了重大改动	运营总监

审批

（如下签名表示审批者对本文档所有条款和条件均表示认可。）

审批人	角色	签名	批准日期
S. Forthright	CEO	<数字签名>	2018-04-22
M. West	法务总监	<数字签名>	2018-04-23

3.1.1 目的

网络安全计划文件为韦斯特曼启动、实施、维护和改进网络安全管理提供了指导方针和原则。

本计划旨在：

- 确保员工安全，保证业务信息的安全和机密性；
- 保护此类信息的安全和完整性，防止受到预期威胁或危害；以及
- 保护此类信息，防止通过非法访问或使用此类信息对韦斯特曼及其合作伙伴或客户造成重大伤害或不便。

3.1.2 读者对象

本文件供 CEO、IT 经理、运营总监和管理层认可的其他人员使用，为公司实施网络安全计划提供支撑。

3.1.3 管理层承诺

韦斯特曼的领导团队负责制定这一信息安全计划，是该计划的最终负责人，全力支持计划实施。为践行这一承诺，管理团队须为信息安全工作划拨必要资金，及时应对各种新情况，还要参与所有与信息安全相关的活动。

3.1.4 公司概况

工业部门中的角色

韦斯特曼是一家生产商用级化工产品的化工制造商，其产品用于运输、建筑施工等工业产品。

除定期维护停机（每年约 2 周时间，通常在 12 月底）外，韦斯特曼的生产设施全天候连续运营。为提高工业竞争力，韦斯特曼引进了过程自动化设备，以提高生产效率，降低生产成本。厂房里部署了工业自动化设备，如可编程逻辑控制器（PLC）、人机界面（HMI）和历史数据库，监控生产作业。

根据第 21 号总统政策令（PPD-21），化工行业属于关键基础设施。

任务目标

保护人员安全

韦斯特曼以制造系统的安全运行为己任，始终将员工安全作为头等大事。所有的制造工艺、协议、自动化过程和设备、作业程序和指南在设计时都充分考虑了人员安全。

保护环境安全

韦斯特曼遵守有关环境安全的所有适用法规。韦斯特曼确保其生产过程不影响环境，尽力减少环境足迹。每季度对生产造成的环境影响进行评审。

保证产品质量

韦斯特曼拥有世界领先的生产设备和工艺，采用最先进的自动化、设备和技术确保产品质量。公司建立了质量保证程序，使用自动化设备（包括高速控制网络中的 PLC、历史数据库和高精度传感器）监控产品质量。

实现生产目标

韦斯特曼的一个重要目标是实现月度生产目标，确保向客户及时供货。也有助于维护公司的财务稳定性。

韦斯特曼基于 7x24 生产模式规划生产运营，满足生产目标和客户需求。公司在自动化设备和熟练专业人员方面进行投资，确保完成月度生产目标。

保护商业机密

韦斯特曼倾力保护其商业机密，包括产品开发、制造工艺、产品质量和供应链管理。

供应链中的角色

原材料一般基于与供应商签订的长期合同供应，定期运至工厂。

制成品通常批量出售，产品运输分包给多家物流公司，负责从韦斯特曼工厂运送至最终客户，即其他工业制造商，他们通常将韦斯特曼产品用作原材料或添加剂。

信息传递

制造系统所有的关键信息和操作以及关键资源应以网络图、手册等形式记录。运营总监在 IT 经理协助下，每年对文件进行一次审查。公司根据具体角色将信息与员工和承包商共享。

制造系统关键组件

制造系统的关键组件如下：

- 工程师站（Engineering Workstation）
- 管理型 PLC（Supervisory PLC）
- HMI 服务器
- OPC 和控制器服务器
- 历史数据库服务器（Historian Database Server）
- 网络设备

配套服务

韦斯特曼需要的配套服务包括宽带互联网、供电、天然气和供水。宽带互联网连接由一家大型全国网络服务商根据商业级服务水平协议提供。

3.1.5 信息安全政策

信息安全政策的目的是概括介绍构成韦斯特曼信息安全计划的政策、标准、程序和技术控制措施。本文件由运营总监制定实施，旨在保护韦斯特曼的 IT 和运营技术（OT）资产。

3.1.6 适用法律法规

作为一家化工产品制造商，韦斯特曼及其员工必须遵守联邦和州对化学品和有害物质的所有法律法规要求。韦斯特曼作为企业主还须遵守所有的法律、法规和安全要求。

3.1.7 安全组织和治理

信息安全是治理活动的组成部分，涉及领导层、组织结构和流程，目的是保护韦斯特曼的信息、运营、市场地位和声誉。

组织角色	安全责任
首席执行官（CEO）	审批信息安全计划和配套政策，至少一年一次； 指派运营总监制定政策和程序，规范组织对IT/OT资产的使用、实施、文件管理以及履行合规义务； 作为事件升级的联系人（Point of Escalation）； 负责协调数据泄露响应。
财务总监	向运营总监报告网络安全事件和问题。
控制工程师	向运营总监报告网络安全事件和问题； 协助确定所在领域的网络安全要求； 应总监要求，协助修复漏洞。
市场总监	向运营总监报告网络安全事件和问题。
产品开发总监	向运营总监报告网络安全事件和问题。
运营总监	负责所有IT/OT资产的总体网络安全； 负责修复漏洞及/或缓解风险； 制定、实施和维护网络安全计划和网络安全政策文件； 作为操作人员、厂商和管理层之间的信息安全事宜联络人； 向CEO汇报网络安全计划的现状以及网络安全相关风险或事件。
IT经理和IT团队	按照运营总监的指示修复漏洞； 向运营总监报告网络安全事件、运营问题和需要关注的其他问题； 协助确定所在业务部门和专业领域的网络安全要求； 将涉及敏感信息泄露的网络安全事件告知运营总监。
法务总监	处理网络安全事件相关的法律事宜； 审查网络安全事件相关的外部通信； 向运营总监报告网络安全事件和问题。
HR经理	处理网络安全事件相关的人事和纪律问题； 向运营总监报告网络安全事件和问题。

所有员工、承包商和厂商都要遵守公司的政策和程序，确保信息的安全性、机密性和完整性。

3.1.8 个人信息隐私

在韦斯特曼系统中，员工无隐私可言，韦斯特曼系统和网络中的所有活动都受到监控。韦斯特曼是私营公司，其信息系统中存储的任何信息都可能根据州法律进行披露。韦斯特曼不会泄露个人信息，但根据适用法律、法规、有效法律要求提供此类信息的情况除外。

3.1.9 运营安全

风险管理：

运营总监应进行一年一度的风险评估，识别可能影响威胁韦斯特曼安全性、机密性和完整性的内外部风险。

风险评估包括评估风险及其可能性，还要选择和实施控制措施，将风险降低到可接受水平。每次风险评估后，主要结论和风险缓解建议都要形成文件。

鼓励所有员工向运营总监报告任何潜在或现存风险。运营总监识别或确认风险后，将确定下一步行动（例如接受风险、寻求 IT 团队的帮助、联系厂商缓解风险等）。同样，如果厂商或承包商发现设备存在任何威胁或风险，也可以通知运营总监。有关风险通知流程的详细说明，见 3.4 节“风险管理文件”。

物理安全：

厂区有围墙，围墙大门在上班时间打开，下班后上锁。主楼有两个入口，一个用于员工出入，通常上锁，员工必须刷卡才能进入大楼。另一个入口位于前厅，在正常上班时间属于开放状态。访客须登记并领取相应身份证明才能进入。

此外，为确保人员安全，进行入职前筛选，对职位进行详细描述，明确雇用条件，提供网络安全教育和培训。有关物理安全要求方面的更多详细信息，参见“网络安全政策”中的 3.2.6 节“物理安全”。

访问控制：

对 IT 和 OT 系统的访问采用基于角色的最小权限原则，访问或操作制造系统的任何组件都需要提前获得运营总监的相关授权和批准，已部署控制措施，通过认证方法和其他技术手段限制访问，有正式的流程和安全登录程序管理密码，敏感系统明确标识，定期进行审计。

有相应的身份认证控件对外部连接和远程用户进行认证，对关键组件的物理和逻辑访问进行控制，系统保护和数据保护职责分开，定期审核访问权限。

3.1.10 网络安全意识培训

新员工入职时向其传达网络安全意识信息，提供在线资源，让员工了解安全最佳实践和上报网络安全事件的重要性。此外，运营总监确保员工明了自己在韦斯特曼网络安全计划中的角色和责任。

运营总监和外部厂商之间定期共享有关韦斯特曼系统潜在或现存网络威胁的所有信息。另外，会及时发布有关电子邮件欺诈、网络钓鱼企图和其他恶意行为的新闻，告知用户存在的潜在威胁。

用户和管理人员培训

员工须在管理层批准后接受在线计算机培训或课堂培训。可以采用的培训方案示例如下。订阅行业组织时事通讯和杂志能获取更多针对性的培训课程。

- 培训方案示例

  - ICS-CERT VLP[1]（虚拟学习门户）

  - SCADAhacker[2]

  - SANS 工业控制系统培训[3]

  - ISA 培训[4]

[1] https://ics-cert-training.inl.gov
[2] https://scadahacker.com/training.html
[3] https://ics.sans.org/training/courses
[4] https://www.isa.org/training-and-certification/isa-training/security-cybersecurity-and-ansi-isa99-training-courses/

特权用户培训

特权用户的培训内容涵盖普通用户的指定培训内容。高级培训由自动化行业组织或工控系统环境网络安全专业培训机构提供。

- 培训方案示例
  - 国际自动化协会（ISA）[5]
  - SANS（信息安全培训）[6]

第三方承包商培训

第三方承包商访问任何 IT/OT 系统之前，必须接受网络安全意识培训，培训方式包括培训机构面授和在线虚拟教室环境。

- 培训方案示例
  - SANS 工业控制系统培训[7]（讲师培训—收费）
  - ICS-CERT VLP[8]（虚拟学习门户）（免费虚拟教室环境）

3.1.11 第三方责任和要求

- 要求第三方承包商和厂商遵守网络安全政策，保护敏感信息，确保敏感信息的安全。
- 第三方承包商和厂商从第一次安全合规检查完成之日起每年重新评估一次。在重新认证过程中，将再次评审上述安全意识培训部分中列出的所有目标，确保合规。
- 所有第三方提供商的远程连接通过桌面共享程序实现，接受监控和审核。
- 所有软硬件工具在网络上使用或部署前必须获得运营总监的批准。
- 共享任何数据前双方都要签署书面谅解备忘录。
- 确有需要时才能创建和启用网络帐户，厂商使用远程访问帐户时需要获得运营总监的批准。有关审批流程的详细信息，参见网络安全政策文件中的“远程维护审批”。

3.1.12 消防、安全和环境系统

所有用于保护制造系统的消防和安全系统必须符合地方、州和联邦法律的要求，包括职业安全与健康管理局（OSHA）的人员安全条例。根据监管行业的指导，遵循行业安全法规。所有消防系统的设计都必须把保护生命作为第一要务，其次才是制造设备的安全。确保制造系统的消防措施可在电气设备周围（例如 PLC、HMI、机器人、服务器）安全使用。消防系统须经过认证，来自获得相应许可的特许厂商。

制造系统环境中使用的所有环境系统（如暖通空调系统）必须符合地方、州和联邦法律的要求，将保护生命作为第一要务，其次才是制造设备的安全。

3.1.13 应急电源

在发生重大停电事件时，使用短期不间断电源（UPS），组织可有序停工，有条不紊地准备好长期备用电源。

---

[5] https://www.isa.org
[6] https://www.sans.org
[7] https://ics.sans.org/training/courses
[8] https://ics-cert-training.inl.gov

3.1.14 安全事件管理

韦斯特曼的事件响应计划和系统恢复计划对网络安全事件的检测、分析、遏制、根除、恢复和审查进行规划。事件响应计划明确网络安全事件的响应流程，系统恢复计划定义系统恢复流程和恢复能力要求。运营总监负责管理网络安全事件，确保及时报告、调查、记录和解决网络安全事件，迅速恢复运营，并保留证据，根据需要进一步追究纪律、法律责任或进行执法行动。对事件响应计划和系统恢复计划进行年度审查，根据需要进行更新。

从网络安全事件中汲取经验教训，改善并提高检测能力，加强对组织和制造系统的保护。

3.1.15 信息共享计划

与外部实体（如行业组织和地方、州及或邦机构）共享信息有助于加强网络安全。信息共享，特别是从其他外部实体接收信息时，能提高态势感知，更好地保护制造系统。

行业组织

与行业组织建立关系，共享生产厂区内检测到的网络安全事件信息。与行业组织共享的网络安全事件信息必须删除所有私有信息和商业秘密，属于非机密信息。网络安全事件信息若包含私有、客户信息或商业秘密流程，在传输之前需要签订保密协议（NDA）；这些信息为敏感信息，在发送之前需要得到高管批准。

地方政府

与地方政府建立关系，以便共享网络安全事件数据。

州政府

与州政府组织建立关系，以便共享网络安全事件数据。州政府若有事件共享组织，行业组织应能够提供该组织的联系信息。

联邦政府

与联邦政府机构建立关系，以便共享网络安全事件数据，例如：

- 向国土安全部（CISA）[9]机构上报网络钓鱼、恶意软件、漏洞事件
- 向国土安全部（NCCIC）[10]机构上报工业控制系统网络安全事件

3.1.16 定期重新评估计划

网络安全计划文件根据制造系统的变化持续更新，提升网络安全。发生网络安全事件后，吸取经验教训，优化本文件。

运营总监应根据需要，随时评估和更新计划。具体说，应根据以下内容进行评估和更新：

- 风险评估和监控结果
- 韦斯特曼的运营、业务或基础设施组件发生的重大变化
- 网络安全事件

[9] https://www.us-cert.gov/report
[10] https://ics-cert.us-cert.gov/Report-Incident

3.1.17 其他资源

- 利用 SAN 资源实施有效的信息安全计划[11]
- 田纳西大学诺克斯维尔分校信息安全课程计划[12]
- GCADA 样本信息安全程序[13]
- 欧道明大学的 IT 安全计划[14]

[11] https://www.sans.org/reading-room/whitepapers/hsoffice/designing-implementing-effective-information-security-program- protecting-data-assets-of-1398

[12] https://oit.utk.edu/wp-content/uploads/2015-11-11-utk-sec-prog-plan.pdf

[13] http://www.gcada.org/pdf/Sample%20Information%20Security%20Procedure%20(safeguard%20policy).pdf

[14] https://www.odu.edu/content/dam/odu/offices/occs/docs/odu-it-security-program.pdf

3.2 网络安全政策文件示例

本节以为韦斯特曼公司（虚构）开发的政策程序文件和声明为例，介绍了网络安全政策文件中所包含的内容。本文中提到的商业实体、设备、材料等或有标识，仅为准确描述概念之用，并非暗示 NIST 推荐或认可，也不表明这些实体、设备、材料是实现目的之最佳选择。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的内容及政策程序文件和声明。

韦斯特曼
网络安全政策

文件负责人	运营总监

版本信息

版本号	**日期**	**说明**	**作者**
1.0	2018-02-22	新建文档	运营总监
2.0	2018-04-21	对最初版本做了重大改动	运营总监

审批

（如下签名表示审批者对本文档所有条款和条件均表示认可。）

审批人	**角色**	**签名**	**批准日期**
S. Forthright	CEO	<数字签名>	2018-04-22

3.2.1 目的

网络安全政策定义了安全要求，明确了在组织中如何正确、安全地使用 IT 和 OT 服务，目的是防止组织及其用户受到网络安全威胁，危及公司的完整性、隐私、声誉和业务成果。

3.2.2 范围

本网络安全政策适用于有权访问制造系统或其数据的员工、承包商或个人。

3.2.3 政策维护

网络安全政策必须在运营总监批准后才能分发给员工，而运营总监在决定前须征求 IT 经理和 CEO 的意见。对本文件的任何更新也须得到运营总监的批准。

本政策文件由运营总监每年审查一次，更新后通知所有员工。

3.2.4 基于角色的网络安全职责

网络安全责任因个人在公司中的角色而异，具体如下：

员工

组织角色	安全责任
首席执行官（CEO）	• 审批信息安全计划和配套政策，至少一年一次； • 指派运营总监负责制定政策和程序，规范组织对IT/OT资产的使用、实施、文件管理以及履行合规义务； • 作为事件升级的联系人； • 负责协调数据泄露响应。
财务总监	• 向运营总监报告网络安全事件和问题。
控制工程师	• 向运营总监报告网络安全事件和问题； • 就如何满足特定领域的网络安全要求提供帮助； • 按总监要求，协助修复漏洞。
市场总监	• 向运营总监报告网络安全事件和问题。
产品开发总监	• 向运营总监报告网络安全事件和问题。
运营总监	• 负责IT/OT资产的总体网络安全； • 负责修复漏洞及/或缓解风险； • 制定、实施和维护网络安全计划和网络安全政策文件； • 作为操作人员、厂商和管理层之间的信息安全事宜联络人； • 向CEO报告网络安全计划的现状以及与网络安全相关风险或事件。
IT经理和IT团队	• 按照运营总监的指示修复漏洞； • 向运营总监报告网络安全事件、运营问题和需要关注的问题； • 协助确定所在业务部门和专业领域的网络安全要求； • 将涉及敏感信息泄露的网络安全事件告知运营总监。
法务总监	• 处理网络安全事件相关的法律事宜； • 审查网络安全事件相关的外部通信； • 向运营总监报告网络安全事件和问题。
HR经理	• 处理网络安全事件相关的人事和纪律问题； • 向运营总监报告网络安全事件和问题。

外部人员

角色	安全责任
设备厂商	• 协助修复漏洞，根据需要升级软硬件； • 遵守韦斯特曼网络安全政策。
访客	• 遵守韦斯特曼网络安全政策。

3.2.5 员工要求

- 员工须完成网络安全意识培训，并同意遵守可接受使用政策（Acceptable Use Policy）。
- 若发现厂区内有未经陪同或授权的个人，员工须立即通知运营总监。
- 员工须始终按照密码策略在所有系统上使用安全密码，同一凭证不得跨系统，且不能用于外部系统或服务。
- 离职员工须返回所有的公司记录，无论是何种形式的记录。
- 外部人员连接到 IT 或 OT 网络之前，员工必须向运营总监核实确已授权。
- 员工须向运营总监报告所有的物理或网络安全事件。

3.2.6 物理安全

- 员工须始终使用并出示公司提供的物理身份证明（ID）。
- 员工、外部人员和访客的 ID 必须有明显区别，一眼看去，即可分辨。
- 严禁以任何理由共享 ID。
- 接待人员负责管理登记表，记录所有访客来访情况，运营总监会定期审查这些记录。
- 所有的访客、承包商和/或维护人员须由员工全程陪同。
- 未经运营总监授权，不得擅自将任何公司文件、设备或媒体设备带出厂区。
- 访客、承包商和维护人员在厂区的所有活动受到监控，在连接到公司网络时，运营总监或指定员工会监控其所有的计算机操作。
- 每月对公司进行安全状况监测，检查是否有物理安全事故。

3.2.7 信息技术（IT）资产

- IT 资产只能用于授权执行的份内业务活动。
- 每位员工都有责任保存和妥善使用名下的 IT 资产。
- 不得随意放置 IT 资产。
- 台式机和笔记本电脑无人在场时必须锁屏，应尽可能自动执行该策略。
- 个人未经授权不得访问 IT 资产，要访问资产，须获得运营总监的授权。
- 变更配置时须走变更控制流程，识别风险，了解实施过程中的明显变更。
- 所有资产必须受到身份认证技术（如密码）的保护。
- 遵守密码策略。
- 在发现资产丢失或被盗后，必须立即通知运营总监。
- 禁止使用个人设备访问 IT 资源。
- 除非经运营总监授权，否则不得在移动媒体上存储敏感信息。
- IT 资产上存储或移动设备上传输的任何敏感信息须妥善保护，禁止非法访问，并且必须按照行业最佳实践和适用的法律法规进行加密。

IT 资产清单

资产名称	数量
超微服务器	6
Allen Bradley 5700交换机	2
Allen Bradley 8300路由器	1
惠普塔式工作站	1

3.2.8 运营技术（OT）资产

- 不得将 OT 资产用于非授权、非份内的业务。
- 运营总监和操作人员负责保存和妥善使用名下的 OT 资产。
- 非授权人员禁止接触 OT 资产。
- 所有与 OT 资产直接交互的人员必须接受相应培训。
- 运营总监对所有 OT 设备负责。控制工程师全权负责 OT 设备的维护和配置，其他人员无权修改 OT 资产配置，包括对接口软硬件的任何修改。
- 在 OT 网络上使用安全工具必须经运营总监批准。
- 在 OT 网络中使用安全工具必须提前通知所有操作人员。
- 授权 OT 资产的访问权限时，必须遵循“最小权限”原则。
- 应始终将 OT 资产（如 PLC、安全系统等）的按键开关置于“运行”位置，根据需要进行调节。
- 禁止通过 OT 网络或 OT 资产非法访问 IT 设备或互联网。
- 禁止使用个人设备访问 OT 资源。

OT 资产清单

资产名称	数量
Allen Bradley ControlLogix PLC	1

3.2.9 资产生命周期管理责任

- 任何 IT 或 OT 资产在淘汰前必须按照制造商指南对所有数据进行过滤，该操作一般由 IT 支持人员执行。
- 员工离职后，其 IT 资产（如台式 PC 或笔记本电脑）分配给其他员工之前，必须重做映像。

3.2.10 系统维护

- 涉及外部人员（如承包商、厂商等）的所有维护任务须经运营总监批准。
- 有权访问公司资源的外部人员须妥善保护用于访问韦斯特曼网络或系统的所有资源。
- 对所有远程维护活动进行监控，防止有害或恶意活动的发生。由一名员工详细记录该活动。
- 所有系统和技术控制措施须在维护后进行验证，确定是否存在网络安全方面的影响。
- 运营总监用维护跟踪软件记录所有的维护活动。

3.2.11 数据

- 访问敏感数据时须提前获得运营总监的许可。
- 不得随意共享数据。当需要访问敏感信息时，可以向运营总监申请许可，并采取一切必要措施防止非法访问。
- 包含敏感数据的设备（如手机、笔记本电脑、USB 设备等）丢失后，必须立即告知运营总监。
- 转移或传输敏感公司数据时，必须使用加密的便携式媒体或安全协议。
- 远程操作员工必须采取额外的防护措施，确保敏感数据得到妥善保护。
- 数据的物理副本在不使用时应妥善存放。
- 切勿随意放置（例如，在打印机或桌子上）敏感数据的物理副本。
- 敏感数据的物理副本不再需要时应安全销毁或处置。

敏感、私有或包含商业秘密的数据类型

数据类型	数字文件	物理副本	数据库
PLC程序代码	□✓		
化学式	□✓	□✓	
质量保证程序	□✓	□✓	
操作手册和文件	□✓	□✓	
电气图	□✓	□✓	
网络图	□✓	□✓	
历史生产数据	□✓		□✓

3.2.12 凭证管理

该政策的目的是为设置强密码、保护密码、密码更改频率和员工期望建立标准。

所有员工、厂商、承包商或其他利益相关者在使用韦斯特曼的 IT 和 OT 系统时，应通过所分配的个人凭证（用户名和密码）进行认证，获得对这些系统的访问权。对于系统的访问授权和限制由凭证控制。

IT 系统帐号的创建和删除通过微软活动目录管理。此外，由 IT 经理批准并授权用户访问 IT 或 OT 系统。

韦斯特曼保留随时暂停用户访问系统或服务的权利。

3.2.13 活动目录帐号的密码政策

- 所有密码必须包含至少 10 个字符，由大小写字母、数字和特殊字符组成。
- 密码必须每 90 天更改一次，且不能与过去 12 个月内使用的密码相同。
- 不得使用字典中的单词或专有名词作为密码。
- 不得在电子邮件或其他形式的电子通信中提供密码。
- 不同的公司帐号须使用不同的密码，不得使用个人帐号密码。
- 尽可能使用多重身份认证。
- 在安装资产或将资产连接到任何组织网络之前，必须删除默认密码，如新购资产中预先配置的密码。
- 禁止共享密码。

- 不得泄露或公开密码。
- 切勿写下密码。
- 切勿使用应用程序中提供的“记住密码”功能。

3.2.14 特权帐号

特权用户

- 运营总监对韦斯特曼的制造系统有特权访问权限。
- IT 经理对韦斯特曼内部的 IT 基础设施有特权访问权限。
- 所有其他的特权用户帐号均由业务总监根据具体情况授予。

职责

- 制造环境中的所有特权用户都有两个帐号：一个是主帐号，用于正常活动；另一个是特权“管理员”帐号，用于执行特权功能。
  - 主帐号用于日常操作；
  - 主帐号拥有普通韦斯特曼用户帐号的所有权限（例如电子邮件访问、互联网访问等）；
  - 特权帐号具有管理权限，只能在制造系统内执行管理功能时使用（例如固件或软件的系统更新、系统重配、设备重启等）。
- 特权用户在制造系统内履行职责时，始终以安全方式使用管理帐号。若特权帐号被入侵，可能会对生产过程产生破坏性影响。

3.2.15 防病毒软件

- 在所有设备（如工作站和服务器）上安装防病毒软件，只要设备支持；配置时限制防病毒软件的资源占用，以免影响制造系统生产。
- 安装防病毒软件后，配置该软件从中央管理服务器或其他防病毒客户端（若支持）接收推送更新。

3.2.16 互联网

- 仅允许从制造系统网络访问互联网，且此种访问须经过授权。
- 个人设备接入互联网须经运营总监批准。
- 部署边界防火墙管控收发流量。
- 必须监控和记录所有内外部通信，工厂操作人员须定期审核日志并将日志报送运营总监。

3.2.17 持续监控

- 必须使用商业或开源工具进行全面的网络监控，以检测攻击、攻击迹象和非法网络连接。
- 监控制造系统，捕捉网络安全攻击迹象。
- 监控所有外部边界网络通信。
- 所有网络安全事件必须记录在事件响应管理系统中，方便后续输出和跟踪。
- 根据地方、州、联邦、法规和其他强制性要求检测制造系统时必须按照法律、法规或政策进行。
- 风险增加或出现其他因素时，加强监测。

- 所有网络安全事件必须通知以下人员：

事件严重性	通知人员
低 （所有事件）	控制工程师
中	IT人员、控制工程师
高 （须立即关注）	IT经理、运营总监

- 与 ICS-CERT[15]共享网络安全事件的详细信息，保护组织安全，进而保护行业安全。国土安全部网络安全和基础设施安全局（CISA）受理制造商所上报的网络安全事件。

3.2.18 用户访问协议

具有 IT 或 OT 资源（如制造系统、电子邮件、HR 系统等）访问权限的所有员工需阅读并接受用户访问协议的条款。

3.2.19 远程访问

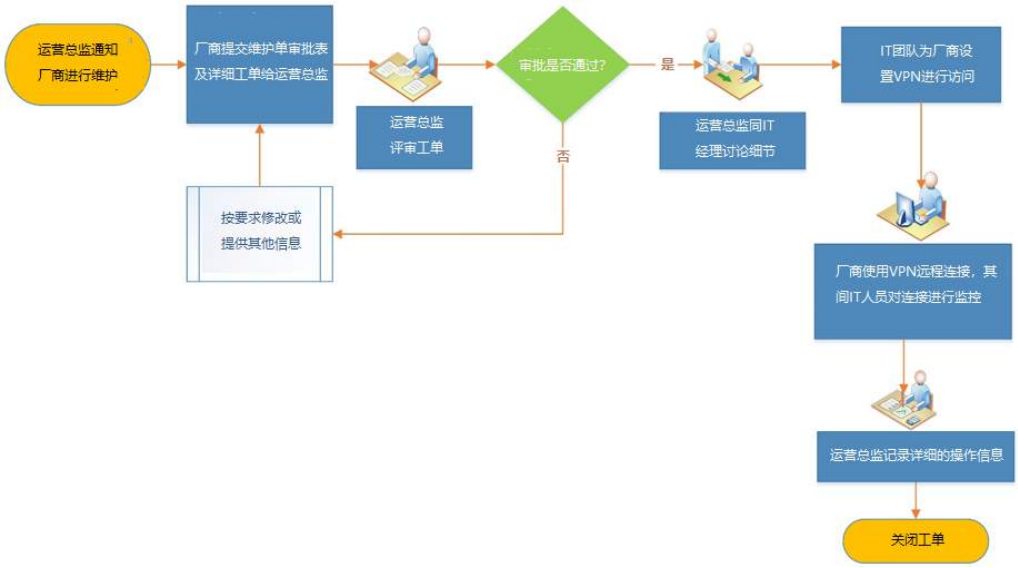
此政策适用于需要远程访问制造系统资源的用户和设备。以下规则适用于一次性请求：

- 所有远程访问须获得运营总监批准，同时通知 IT 经理。请求远程访问的厂商必须在公司注册，且必须填写工单的详细信息，提交维护订单审批表。
- 禁止通过未加密连接远程访问敏感信息。确需访问时，须进行例外授权。
- IT 团队设置 VPN 帐号，与厂商共享凭证，以便厂商通过远程桌面访问选定系统，如工程师站或 HMI 服务器，具体可访问什么系统取决于任务性质。工作完成后取消访问权限。
- 所有活动都要接受 IT 人员监控，此等监控会持续进行，直到不再需要远程会话或工作已完成。指定人员将明示远程会话何时处于活动状态，并确保制造系统环境返回到建立远程连接之前的状态。
- 在授权设备上安装任何软件（如桌面共享软件）均由 IT 人员执行。
- 禁止在个人设备上使用远程访问技术。
- 通过远程访问技术接入的所有设备必须使用最新的防病毒软件和病毒特征。
- 在现场访问期间，所有活动都要接受监控。当厂商在计算机上操作时，指派专门的 IT 人员对其进行密切监控。
- 禁用隧道分离。所有访问外网的流量都要通过 VPN 会话从公司网络转发。

[15] https://ics-cert.us-cert.gov/

3.2.20 远程维护审批流程

对 IT/OT 资产进行远程维护的审批流程和程序如下图所示。



3.2.21 维护审批表

维护单审批表	
厂商名	
厂商地址	
厂商电话号码	
厂商当前是否为韦斯特曼提供支持？	☐ 是 ☐ 否
厂商计划使用的系统是否安装了防病毒软件？	☐ 是 ☐ 否
此次会话要支持及/或使用哪些项目？	☐ PC/笔记本电脑 ☐ 服务器 ☐ 控制系统设备 ☐ 其他IT/OT设备 ☐ 软件 具体信息：
是否需要在韦斯特曼系统中安装任何软件或程序？	☐ 是 ☐ 否 具体信息（若是）：
该软件是否要求购买许可？	☐ 是 ☐ 否
欲执行任务的详细信息	
是否为经常性活动？	☐ 是 ☐ 否
厂商签名	
审批结果（由运营总监填写）	☐ 是 ☐ 否
运营总监签名	

3.2.22 缩略词

缩略词	全称	
AV	Anti-virus	防病毒软件
CEO	Chief Executive Officer	首席执行官
CISA	Cybersecurity and Infrastructure Security Agency	网络安全与基础设施安全局
DHS	Department of Homeland Security	国土安全部
HMI	Human Machine Interface	人机界面
HR	Human Resources	人力资源
ICS	Industrial Control System	工业控制系统
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team	工控系统网络应急响应小组
ID	Physical or Logical identification (e.g., badge，login name，etc.)	物理或逻辑身份证明（如徽章、登录名等）
INFOSEC	Information Security	信息安全
ISA	International Society of Automation	国际自动化协会
IT	Information Technology	信息技术
NCCIC	National Cybersecurity and Communications Integration Center	国家网络安全与通信集成中心
NDA	Non-Disclosure Agreement	保密协议
OSHA	Occupational Safety and Health Administration	职业安全与健康管理局
OT	Operational Technology	运营技术
PLC	Programmable Logic Controller	可编程逻辑控制器
PPD	Presidential Policy Directive	总统政策令
SCADA	Supervisory Control and Data Acquisition	数据采集与监视控制系统
UPS	Uninterruptible Power Supply	不间断电源
USB	Universal Serial Bus	通用串行总线
VPN	Virtual Private Network	虚拟专用网络

3.2.23 定义

术语	定义
访问管理	对访问组织资源进行管理的实践、政策、过程、数据、元数据以及技术和管理机制。
资产	组织拥有的设备。
AV扫描	扫描设备中的病毒。
设备	电子硬件（如机器、计算机、笔记本电脑、电话、网络设备）。
员工	直接受雇于组织的个人。
外部人员	承包商、访客之类的不属于组织的个人。

人机界面（HMI）	个人用于与OT接口和交互的资产（如机器）。
工控系统（ICS）	一般是指用于控制流程和生产过程或操作机器的软硬件。
信息技术（IT）	信息技术，包括服务器、笔记本电脑、工作站、交换机和路由器等设备。
最小权限	用户仅被授权执行其工作所需的功能。
操作系统	设备运行所必须的软件（如Windows、Linux），一般表现为用户界面。
运营技术（OT）	运营技术，包括生产过程中使用的工业控制系统设备。
个人设备	个人所有的设备；不由组织所有或控制。
人员	所有员工和外部人员，不包括访客。
便携式媒体	U盘、光盘（CD）、外部硬盘驱动器、笔记本电脑。
远程访问技术	远程人员通过互联网将设备连接到IT或OT网络的软件。
安全工具	
敏感信息	与组织运营相关的客户、人员、私有或商业机密信息数据；攻击者获取后可能对组织造成损害的数据。
隧道分离	远程用户或设备建立与系统的非远程连接，同时通过其他连接与外部网络中的资源进行通信的过程。通过这种网络访问方法，用户能够在访问不受控网络的同时访问远程设备（例如网络打印机）。[NIST SP 800-171 R1]
用户	使用设备的个人。
病毒特征	防病毒软件用以识别病毒的数据。
漏洞	攻击者可用来获取系统访问权限的弱点或缺陷。
漏洞扫描	用于检测设备上常见或已知漏洞的软件。

3.2.24 其他资源

- SANS 研究院所提供的安全政策资源[16]
- 项目管理文档网站的安全政策模板[17]
- Sophos 实验室的数据安全政策[18]

[16] https://www.sans.org/security-resources/policies
[17] http://www.projectmanagementdocs.com/template/Security-Policy.doc
[18] https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en

3.3 网络安全操作文件示例

本节以为韦斯特曼公司（虚构）开发的政策程序文件和声明为例，介绍了网络安全操作文件中所包含的内容。本文中提到的商业实体、设备、材料等或有标识，仅为准确描述概念之用，并非暗示 NIST 推荐或认可，也不表明这些实体、设备、材料是实现目的之最佳选择。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的内容及政策程序文件和声明。

韦斯特曼
网络安全政策

文件负责人	运营总监

版本信息

版本号	日期	说明	作者
1.0	2018-02-22	新建文档	运营总监
2.0	2018-04-21	对最初版本做了重大改动	运营总监

审批

（如下签名表示审批者对本文档所有条款和条件均表示认可。）

审批人	角色	签名	批准日期
S. Forthright	CEO	<数字签名>	4-22-2018

3.3.1 概述

网络安全操作文件制定了操作步骤，让管理人员及员工响应韦斯特曼制造系统内发生的事件时有标准可循。实际操作中应时常提及本文件内容，确保制造系统内的所有员工和个人熟悉网络安全操作。

3.3.2 目的

提供统一的网络安全操作环境，支持制造系统的运行。

3.3.3 范围

管理人员、员工、承包商等需要访问制造系统进行变更的人员应熟悉本文件内容。

3.3.4 资产盘点

统计制造系统内的资产是保护公司的第一个重要步骤，避免公司遭受恶意活动，导致生产中断。此外，确定哪些设备有权连接到网络后，可检测非法访问设备，发现潜在的恶意活动。同样，对网络设备上安装的软件进行跟踪，可获取更新和修补软件所需的重要信息，及时消除漏洞。韦斯特曼使用手动和自动资产盘点工具进行资产盘点管理，具体如下：

- **手动盘点** – 无法自动扫描的设备（例如 PLC、加工站） 手动输入到 Excel 表格中，至少每季度更新一次。
- **自动盘点** – 可自动扫描的设备使用资产盘点工具（Open-AudIT）进行配置和审计，只有经过授权的人员才能访问 Open-AudIT。

所有盘点操作都应在制造系统停工期间进行，软件和硬件都须盘点。定期对制

造系统内的设备进行软硬件扫描，检测其中的非法变更。制造系统中可能发生的变更包括更新软件、许可证、系统补丁、固件等，以及新增设备（如 PLC 或 HMI）或操作所需的其他工控系统组件。为检测制造系统中的此等变更，至少每季度进行一次扫描，记录现有设备信息、配置和安装的软件（例如许可证信息、软件版本和配置等）。基于这些扫描结果，可识别制造系统中非法接入的硬件及其安装的非必要软件应用程序。

此外，使用设备配置基线检测计划外变更，防止系统完整性被破坏，进而影响生产过程。使用手动和自动方法获取当前设备配置，将其与确立基线进行对比验证。手动方法适用于不支持自动扫描的工控系统设备。具体来说，在 Excel 表格中手动记录无 SSH、SNMP 和 WMI 服务的设备，使用 Open-AudIT 自动扫描设备配置。之所以选用 Open-AudIT，是因为该工具可根据需要扩展配置。

扫描完成后，将收集的信息与确立基线进行比较，记录所识别的变更，以供评审和调查。对于在制造系统中识别出的未授权或非必要软硬件，应安排时间，在不影响生产过程的情况下尽早移除。对于所识别的已批准变更，需要更新相关基线，反映此变更。对于未批准变更，将设备恢复到之前批准的配置状态，并对该变更进行调查，查明是否发生了网络安全事件。

设备配置基线至少每季度进行一次评审，并在制造系统经过批准进行工程变更后及时更新。在两次基线评审的间隔期间，新增任何设备或修改任何配置都会启动新一轮基线扫描。此外，使用 GRASSMARLIN[19]和 Wireshark[20]更新环境网络图，验证信息流，并在新设备添加到环境中后提供更新基线所需的补充信息。

3.3.5 网络

韦斯特曼的制造网络环境必须防止非法访问和篡改，确保生产过程所需信息的可用性、完整性和机密性。这要求制造系统组件的所有网络连接都要记录在案，线缆用标签正确标识，说明指定用途。此外，所有的网络交换机必须配置为支持网络分段和端口安全，以控制网络流量并防止未授权设备访问制造网络。制造环境在投入生产前，其所有的网络连接都要经过运营总监的审批。

为此目的，韦斯特曼创建并维护了一个全面的网络基线，对网络环境进行准确描述，支持制造系统网络内的异常检测过程。至少每季度对网络基线文件进行一次评审和更新，核实制造生产运营需要的所有组件和通信。这一过程中可使用的工具包括 Open-AudIT、GRASSMARLIN 和 Wireshark。此外，利用公司提供的网络图工具，在网络基线文档中加入所有内外部网络连接（包括云服务）的详细网络图。

具体而言，网络图会包括所提供连接服务的所有相关信息，包括：设备 IP、所提供的服务、数据流向、数据类型、支持服务电话号码、客户数量、联系人、支持级别协议和支持时间。网络基线文档还会包括环境中网络分段和端口安全的配置详情。

对韦斯特曼制造系统网络进行分割，以提高环境的速度和网络安全。网络分段之间的网络流量通过防火墙网络设备基于确立的网络基线进行控制，仅允许批准的网络流量出入制造网络各分段，丢弃所有其他流量。与网络分段、防火墙和防火墙规则相关的详细信息也应包含在网络基线文档中。

韦斯特曼制造系统网络还要部署可管理交换机，在交换机上配置并启用端口安全。端口安全允许授权设备基于其唯一的媒体访问控制（MAC）地址使用特定的网络交换机端口。端口安全文档提供了授权设备的资产信息引用，同时列出具有指定网络交换机和交换机端口的设备 MAC 地址。

[19] https://github.com/nsacyber/GRASSMARLIN
[20] https://www.wireshark.org

韦斯特曼需要厂商或承包商提供远程维护支持时，须提前协调和审批，同时指定相关员工对所有远程维护活动进行监控，防止有害或恶意活动的发生。所有需要连接到韦斯特曼进行远程维护的厂商或承包商应：在连接之前获得运营总监的批准；使用批准的远程安全接入程序；在完成批准的任务后取消远程访问权限。所有远程访问维护活动都记录在案，确保对制造系统内的活动进行充分的审计跟踪。

所有的网络设备都应将日志转发到韦斯特曼内部 Syslog 服务器。在韦斯特曼制造系统网络中，网络设备包括网络交换机、支持网络安全局域网的思科自适应安全设备（ASA）防火墙和工作单元中的 Stratix 8300 系列防火墙。

基于从这些设备和 GRASSMARLIN 工具收集的信息，授权韦斯特曼人员根据确立基线每月对现网活动至少检查一次。这些工作有助于识别异常流量，发现潜在系统问题或恶意活动。此外，每月至少检查一次交换机日志，防止恶意设备接入网络。发现任何基线外网络活动时都须进行核对，要么将其纳入基线，要么进行调查，查明是否为系统或网络事件。

另外，授权韦斯特曼人员使用无线笔记本电脑或移动设备，利用操作系统自带的功能或已批准的无线扫描软件每周一次在制造区域内进行扫描，检测未经授权的无线设备或恶意接入点。所有异常情况都将记录在案（包括检测位置）并提交以供进一步调查。

3.3.6 制造系统安全

全员遵守网络安全计划至关重要，可有效降低制造系统的网络安全事件风险。以下各节介绍了与制造系统安全相关的政策和程序。

变更控制

通过变更控制流程跟踪制造系统的变更，变更前通知所有人员，将其纳入变更流程。在实施变更前要进行正式评审和授权。

评审务必彻底，以确定：

- 变更是否影响制造系统性能；或
- 变更是否影响制造系统安全。

变更控制评审人最终确定是否进行变更，若有风险且认定风险可接受，须提供合理解释。

变更批准后将安排在停工期或其他维护活动期间进行，减少对生产的影响。完成变更后，进行安全评审，确定该变更是否导致网络安全控制措施发生变化。这类计划外变更须根据漏洞和修复管理流程进行评审和处理。

按季度评估制造系统，明确哪些设备对系统运行至关重要。基于此信息，撰写关键设备重要性报告，并更新公司的其他网络安全文件和程序。

下表列举了变更控制流程必须涵盖的设备：

设备名	设备类型	详细信息
工程师站	软件	BIOS/固件补丁、IT程序（防病毒软件、备份代理等）、工厂应用程序（FactoryTalk、RSLinx等）
	硬件	存储与内存升级
OPC服务器	软件	BIOS/固件补丁、IT程序（防病毒软件、备份代理等）、工厂应用程序（PI、FactoryTalk服务平台、RSLinx、Matrikon OPC等）
	硬件	存储与内存升级

历史数据库虚拟机	软件	BIOS/固件补丁、IT程序（防病毒软件、备份代理等）、SQL服务器补丁
	硬件	存储与内存升级
工厂模拟器	软件	BIOS/固件补丁、IT程序（防病毒软件、备份代理等）
	硬件	存储与内存升级
控制器主机	软件	BIOS/固件补丁、IT程序（防病毒软件、备份代理等）、工厂应用程序（MATLAB、Matrikon OPC）
	硬件	存储与内存升级
HMI主机	软件	操作系统补丁（Windows）、BIOS/固件补丁、IT程序（防病毒软件、备份代理等）、工厂应用程序（FactoryTalk View Site、FT服务平台、FT View Studio）
	硬件	存储与内存升级
PLC	软件	固件升级及任何形式的配置修改
Allen Bradley边界路由器	软件	固件升级、防火墙规则及任何形式的配置修改
Allen Bradley 2层交换机	软件	固件升级及任何形式的配置修改
思科ASA防火墙	软件	固件升级、防火墙规则及任何形式的配置修改
交换机	软件	固件升级及任何形式的配置修改
活动目录	软件	组策略部署、用户帐号新建/修改
赛门铁克防病毒	软件	防病毒软件版本升级、通过赛门铁克管理程序（Symantec Manager）部署的任意端点策略
Nessus	软件	进行漏洞扫描

人员操作

在制造系统设备上执行的操作可能需要认证，这些操作如下表所示。“所有用户”特指被授权与设备交互的用户。

与设备的物理/逻辑交互是否需要认证								
	工程师站	**管理型 PLC**	**HMI**	**控制器**	**本地历史数据库**	**OPC 服务器**	**VLAN 交换机**	**边界路由器**
物理交互（所有用户）	是	否	否	是	是	是	是	是
逻辑/网络交互（所有用户）	是	是	是	是	是	是	是	是

HMI用户操作是否需要认证			
	查看流程状态	修改流程设置点	静音/清除告警
所有用户	否	是	是

工程师站用户操作是否需要认证				
	登录工作站	查看/修改PLC逻辑	访问工程文件	其他操作
所有用户	是	是	是	是

历史数据库用户操作是否需要认证				
	查看历史数据	修改历史数据	修改配置	登录服务器桌面/CLI
所有用户	是	是	是	是

OPC服务器用户操作是否需要认证		
	修改配置	登录桌面/CLI
所有用户	是	是

控制器用户操作是否需要认证			
	修改配置	登录桌面/CLI	修改控制逻辑
所有用户	是	是	是

VLAN交换机用户操作是否需要认证		
	修改配置	查看交换机状态
所有用户	是	是

PLC操作是否需要认证					
	开关机	重启	流程交互（运行/停止/重置）	修改逻辑	修改模式（运行/配置）
所有用户	否	否	否	是	是

监控制造系统

对制造系统环境中与人员、软件、网络设备和无线接入点相关的未授权活动进行监控。韦斯特曼搭建了一个中央日志服务器（Syslog 服务器）来支持这一功能，配置该服务器汇总系统生成的所有日志，并保留日志以供存档和取证之用。同时，尽可能将制造系统中的设备配置为将日志数据发送到中央 Syslog 存储库。

定期检查日志，检测制造系统中生成的异常告警。具体而言，检查日志事件，确定是否有任何事件影响了生产过程。最起码应该在检测到设备发送了网络安全事件通知后进行调查，确定根因，采取合理补救措施，以清除事件并将制造系统恢复到之前的已知正常运行状态。审查影响生产过程的事件，判断与风险评估结果的相关性，确定采取哪些行动改善韦斯特曼的网络安全态势。

非公司员工对制造系统进行物理访问时，必须登记相关信息（包括日期、出入时间）并签名确认。访客若未经授权，会被护送出厂区。访客全程须由韦斯特曼员工陪同。

备份

制造系统服务器和主机的备份过程定义如下：

- **Veeam 目录备份 -** 针对的是制造系统配置和逻辑数据所在的目录，每周执行一次，执行时间为低产能运转期间（如夜间）。
- **Veeam 系统映像完整备份 -** 每季度执行一次，执行时间为低产能运转期间（如夜间）；另外，发生任何工程变更后，须执行一次完整备份。

主机	Veeam目录备份	Veeam系统映像完整备份	其他方法
工程师站	☐✓	☐✓	
OPC服务器		☐✓	
过程控制器服务器		☐✓	
HMI宿主服务器		☐✓	
本地历史数据库主机		☐✓	生产过程中的OSIsoft PI历史数据库数据实时复制到DMZ历史数据库。
Hyper-V宿主服务器		☐✓	
活动目录服务器		☐✓	
备份活动目录服务器		☐✓	
DMZ历史数据库		☐✓	本机OSIsoft PI应用程序备份功能将生产过程中的生产数据存档，这些备份存储在本地主机上；恢复主机，获取最新的备份版本。 说明：可以恢复的历史数据仅限于备份数据。

赛门铁克防病毒服务器		☐✓	
安全洋葱服务器		☐✓	
Graylog服务器		☐✓	
GTB Inspector服务器		☐✓	
GTB控制台服务器		☐✓	
TheHive项目事件响应服务器		☐✓	
Nessus漏洞扫描器服务器		☐✓	
Windows WSUS服务器		☐✓	

下述备份方法适用于不支持 Veeam 工具的主机和设备。

主机	备份方法
本地历史数据库虚拟机	要备份VHD，可通过宿主服务器（本地历史数据库主机，FGS-61338LHH）的Veeam系统映像完整实现。
控制器PLC	要备份PLC项目文件（存储在本地），可通过工程师站（FGS-47631EHH）的Veeam系统完整映像实现。
	PLC项目或其配置只要进行了工程变更，就要对工程师站（FGS-47631EHH）的Veeam系统映像进行手动完整备份。
	SD卡内容每年备份一次，备份时间为工厂停工期间。
制造系统路由器/防火墙	每次工程变更后，须通过命令行界面（CLI）或Web 界面备份配置。
边界路由器	每次工程变更后，须通过命令行界面（CLI）或Web 界面备份配置。
监控局域网交换机	每次工程变更后，须通过命令行界面（CLI）或Web 界面备份配置。
控制局域网交换机	每次工程变更后，须通过命令行界面（CLI）或Web 界面备份配置。
VMware宿主机	使用Veeam对VMware ESXi平台上运行的虚拟机定期备份。
	每次修改配置后，须对ESXi宿主机配置进行备份。（更多详细信息，参见VMware知识库[21]。）

[21] https://kb.vmware.com/s/article/2042141

媒体过滤

存储媒体（如闪存、内存卡、硬盘）在废弃或离厂之前必须进行过滤，步骤如下所述。

资产/设备类型	详细步骤
服务器硬盘驱动器、工作站	工具：DBAN[22] 步骤： • 下载DBAN，制作启动盘。 • 用启动盘启动服务器。 • 根据屏幕上的说明，反复进行数据清除。 • 上述操作后，在不使用DBAN启动盘的情况下启动服务器，验证数据是否成功清除。
Allen Bradley 8300边界路由器	下述内容见Allen-Bradley的Stratix可管理交换机手册[23]。 步骤： • 登录Web管理控制台。 • 选择**设备管理 > 重启/重置**菜单。 • 选择**【恢复交换机出厂设置】**，单击**【提交】**。
Allen Bradley 5700 2层交换机	下述内容见Allen-Bradley的Stratix可管理交换机手册。 步骤： • 登录Web管理控制台。 • 选择**设备管理 > 重启/重置**菜单。 • 选择**【恢复交换机出厂设置】**，单击**【提交】**。
HMI	HMI程序安装在Windows7系统上。要卸载该程序，执行如下步骤： • 用管理员帐号登录Windows系统。 • 选择**控制面板 > 程序和功能**。 • 选择**【FactoryTalk】**，卸载所有组件。 • 如果需要，重启电脑。
Allen Bradley PLC	Allen Bradley PLC包含下列模块： • DeviceNet扫描器 • ControlLogix模块 • HIPROM时间 要重置HIPROM时间模块，执行如下步骤[24]： • 旋转开关至888. • 模块上电。 要重置DeviceNet扫描器模块，执行如下步骤[25]： • 旋转开关至888. • 模块上电。 有关清除ControlLogix 5571模块内存的说明，见Allen-Bradley的ControlLogix 5000手册[26]。 • 从控制器中取出ESM。 • 切断控制器电源。

[22] https://www.dban.org
[23] http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf
[24] http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um538_-en-p.pdf
[25] http://literature.rockwellautomation.com/idc/groups/literature/documents/in/1756-in566_-en-p.pdf
[26] http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf

	通过以下方式切断电源： - 切断控制器所在机箱的电源。 - 从带电机箱中移除控制器。 • 在控制器中重新安装ESM。 • 恢复控制器供电。

资源维护

资源性能会影响生产效能。操作人员须对其操作或负责的制造系统组件进行日常检查，包括肉眼查看各部件、审查告警信息或指标以及运营总监指定的其他须关注领域。

3.3.7 人员培训

要防止公司受到网络安全威胁，培训至关重要。所有员工、承包商和厂商必须按要求完成年度网络安全培训才能在制造系统环境中工作或继续工作。拥有特权访问权限的个人还要完成相关设备的网络安全控制和配置管理培训，具体培训内容由运营总监或 IT 经理指定。

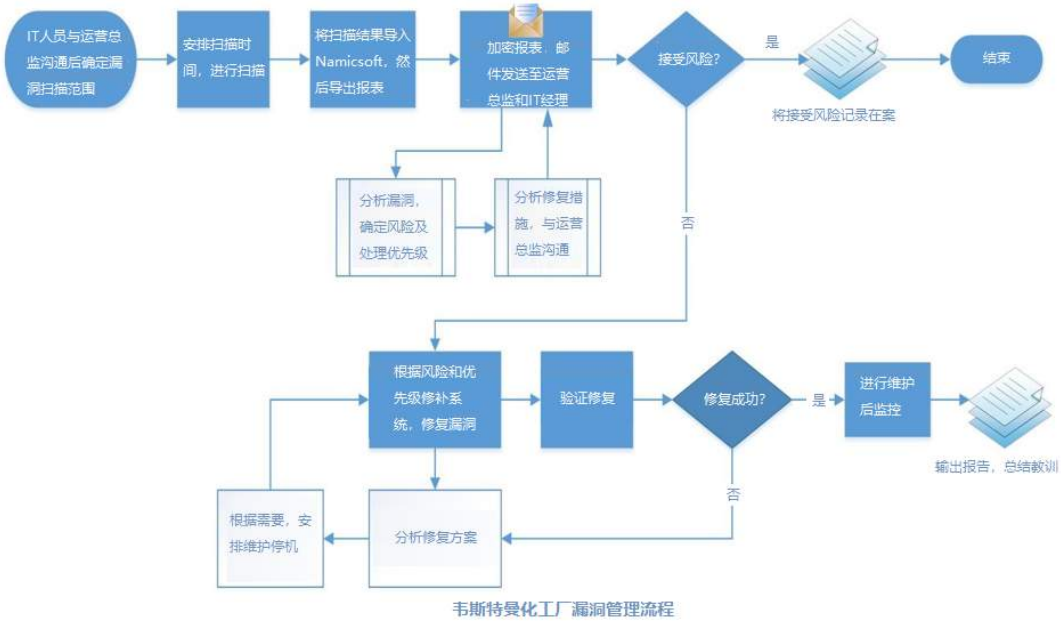
3.3.8 漏洞管理

漏洞管理是信息安全计划的重要组成部分，其中漏洞评估发挥着重要的作用。

漏洞管理的总体策略如下：

- 工程师或 IT 人员不得为了“通过”评估而对信息系统进行任何临时更改。应通过恰当的分析和修复方法，减轻和消除信息系统中的漏洞。
- 不得配置任何联网设备阻止授权扫描引擎的漏洞扫描。
- 对 OT 网络（如监控局域网和现场局域网网络）进行漏洞扫描时要谨慎行事，将扫描安排在非工作时间和维护期间。
- 建议用漏洞扫描程序进行认证扫描。

3.3.8.1 漏洞管理流程



韦斯特曼化工厂漏洞管理流程

3.3.8.2 漏洞扫描与管理工具

韦斯特曼使用 Tenable-Nessus 扫描漏洞。Nessus 完成扫描后，将扫描结果导入漏洞管理、解析和报表工具 NamicSoft，根据组织的统一工作流创建自定义报表和逻辑分组结果。报表由运营总监和 IT 经理审核，根据需要与 IT 人员共享，以协调补救或缓解活动。

漏洞扫描目标

所有连接到工厂和监控网段的设备都要接受扫描，IT 人员配置扫描任务，覆盖韦斯特曼的所有网段。

在向 IT 经理申请后，可以新建扫描任务或对现有扫描任务进行修改。

注意：发现扫描影响生产过程时，必须立即联系 IT 经理，请求停止扫描，并向运营总监报告情况。

漏洞扫描频率

IT 人员根据申请按需执行扫描。考虑到对生产过程的潜在影响，扫描仅在计划维护期间执行。运营总监和 IT 经理应在不影响生产过程的情况下每月至少安排一（1）次 DMZ、网络安全、管理和工程局域网段的评估。所有网段和设备均应在每年的工厂停工期间进行扫描。

所有设备扫描应根据组织的业务需要安排在适合的时间执行，尽量减少对正常运营的干扰。发现新设备需要上报，确认该设备已获得批准，准确归类。

漏洞上报

完成漏洞扫描后，将结果导入 NamicSoft，生成报表。将此类报表归档留存，作为评估证据并用以支持趋势分析。

所有 IT/OT 设备按照其所在系统在 NamicSoft 中进行分组，一台设备可归属多个群组。此类报表覆盖整个系统，方便 IT 员工、IT 经理和运营总监获取设备和漏洞情况。下表列出了可生成和分发的报表类型。

状态报表	频率	目的
漏洞影响的主机列表	每月一次	提供各主机的漏洞信息。
漏洞评估报告	每月一次	提供被扫描网络的漏洞信息。
主机报表	随时	提供特定扫描主机的漏洞信息。
漏洞缓解报告	漏洞修复后	重新扫描主机，确认漏洞是否已被修复。

3.3.9 修复管理和优先级

发现漏洞后，运营总监和 IT 经理在控制工程师和 OT 服务承包商（若有必要）的协助下进行分析，决定下一步行动。

应在下表中定义的修复时间内修复所发现的漏洞。

严重性	说明	修复时间
严重	Nessus使用通用漏洞评分系统（CVSS）对漏洞进行评级，该级别漏洞的CVSS分值为9.0–10.	发现后15天内
高	该级别漏洞的CVSS分值为7.0–8.9。	发现后30天内
中	该级别漏洞的CVSS分值为4.0–6.9，缓解期限较长。	发现后45天内
低	该级别漏洞的CVSS分值为1.0–3.9。考虑到应用程序和操作系统上的正常操作，并非所有低级别漏洞都可轻松修复。此类漏洞应记录在案。	发现后180天内
信息	该级别漏洞不存在网络安全风险，仅为提供信息，不	无需修复

	强制修复。	

例外管理

有时，为了和监管、网络安全和生产优先级对齐，组织风险管理流程中需要加入例外处理，这样才能用较低成本为制造系统创建安全的网络环境。例外请求主要出现在两种情况下：误报 – 误识别的漏洞或在系统中实际上不存在的漏洞；风险接受 – 无法避免、缓解或转移的风险。

误报相关的例外情况必须记录在案，由运营总监批准。误报确认后提交给 IT 人员，由其更新扫描任务和报表，避免再次误报。

对于操作系统、应用程序、Web 应用程序或 OT 设备中可能存在的无法补救或以其他方式避免的漏洞，风险接受是必要措施。这些漏洞包括：厂商设备未及时打补丁；应用程序要正常运行须开放服务；系统虽应报废（开发人员/制造商认定其生命周期终止）却仍在使用。对于确定对系统和组织不构成风险的漏洞，也可以请求例外处理（例如，漏洞只能通过使用 Web 浏览器访问被入侵网站才能利用，而修复漏洞一定会影响生产过程，这种情况就可以考虑接受风险，通过阻断制造网络段的外网接入请求缓解风险）。

风险接受这种例外情况必须由 IT 支持团队提出请求，并提供如下信息：

- **缓解控制：**实施了哪些变更、采用了哪些工具或程序将风险降至最低。
- **风险接受说明：**详细说明为何认为该风险对公司和系统无关紧要。
- **风险分析：**若漏洞确遭利用，会带来哪些风险，影响哪些系统。

其他例外情况，如漏洞评估豁免，必须经过内部讨论，由运营总监批准。

3.4 风险管理文件示例

本节以为韦斯特曼公司（虚构）开发的政策程序文件和声明为例，介绍了风险管理文件中所包含的内容。本文中提到的商业实体、设备、材料等或有标识，仅为准确描述概念之用，并非暗示 NIST 推荐或认可，也不表明这些实体、设备、材料是实现目的之最佳选择。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的内容及政策程序文件和声明。

韦斯特曼
风险管理策略

文件负责人	运营总监

版本信息

版本号	日期	说明	作者
1.0	2018-02-22	新建文档	运营总监
2.0	2018-04-21	对最初版本做了重大改动	运营总监

审批

（如下签名表示审批者对本文档所有条款和条件均表示认可。）

审批人	角色	签名	批准日期
S. Forthright	CEO	<数字签名>	2018-04-22

风险管理计划文件阐述了如何识别、分析与管理韦斯特曼制造系统所面临的网络安全风险。运营总监和高管可基于本文件预测风险，评估影响，确定应对措施。

3.4.1 范围

有权访问组织系统或数据的任何雇员、承包商或个人。

3.4.2 风险管理流程

风险管理是一个反复进行的过程。在执行计划的过程中，会获得越来越多的相关信息，需要根据掌握的信息随时调整风险说明书。整个风险管理流程包括识别、分析、分类、修复和报告。维护风险管理日志，以跟踪已知风险和修复措施。

3.4.3 风险管理流程

应尽早识别项目中的风险，最大可能地降低风险影响。就本流程而言，风险是指利用技术、流程或政策中的漏洞或弱点，对组织运营、组织资产或个人可能造成不利影响或损害的威胁。

影响 IT 和 OT 基础设施的威胁有多种类型，常见威胁源（基于 NIST SP 800-30[27]）包括：

- **敌对威胁** – 对组织的网络资源依赖性进行利用的个人、团体、组织或国家。
- **意外威胁** – 个人在履行日常职责过程中发生的意外错误行为。
- **结构性威胁** – 由于老化、资源消耗或其他非预期情况而导致的设备、环境控制或软件故障。

[27] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

- **环境威胁** – 不受组织控制的自然灾害和本组织所依赖的关键基础设施的故障。

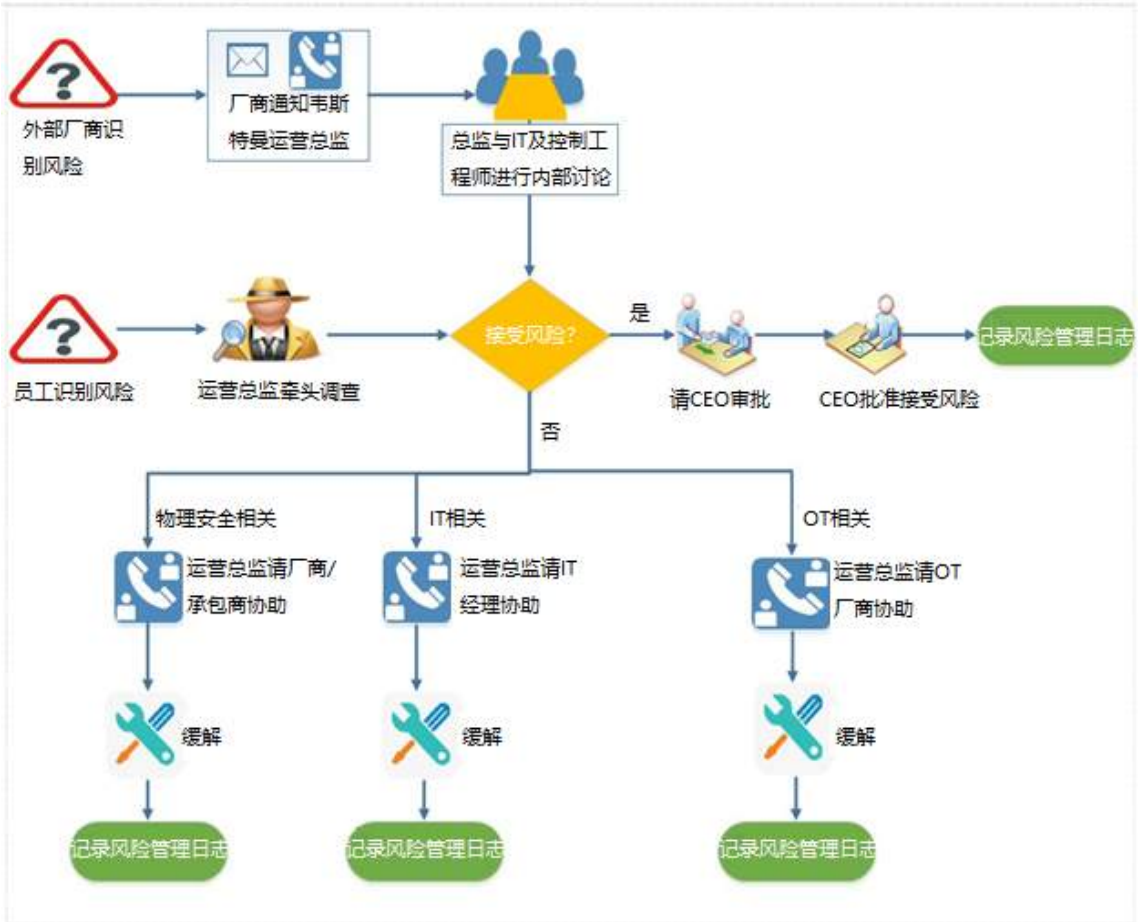
运营总监和 IT 团队以最新版本的 NIST SP 800-30[28]指南为依据，对正式的制造系统年度风险评估进行协调。在此过程中，识别和定义特定的组织威胁事件，以便评估漏洞和缺陷，确定是否存在风险。

要持续监控和管理风险，韦斯特曼的员工和外部承包商必须按照下述风险通知流程上报潜在风险。此外，使用软件工具（包括但不限于 Nessus 和 CSET[29]）识别组织的技术、流程或政策中的漏洞和缺陷，进而支持风险评估流程。

运营总监每年进行至少一次 CSET 评估。考虑到对生产过程的潜在影响，扫描仅在巡检期间执行。Nessus 结果导入 NamicSoft，生成报表，发送给运营总监和 IT 经理。此外，其他类型的风险，如硬件、物理或环境风险，进行手动识别和记录。

说明：无法根据漏洞管理计划修复的软件漏洞将纳入风险分析流程，以确定合理的纠正措施。

风险通知流程



3.4.4 分析

分析流程的第一步是为漏洞评分（1~10）。对于 CSET 识别的漏洞，评估人员基于严重性进行评分，分值范围为 1~10。对于通过 Nessus 等扫描工具识别的漏洞，使用相关的 CVSS 评分。

如果无法分析所有漏洞，最起码要分析高级别（漏洞得分：7.0~8.9）和严重（漏洞得分 9.0~10）漏洞，确定是否存在潜在（发生概率大于零）的相关威胁或威胁事

[28] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf
[29] https://ics-cert.us-cert.gov/Assessments

件。要评估每个漏洞及其威胁对运营的影响。参考下表，使用定性风险分析流程确定总体概率和影响水平。然后，将这些因素组合起来，得到风险的量化评估值，供报告和优先级排序使用。

风险概率	说明	数值
高	一年内发生的概率 > 70%	0.8
中	30% < 一年内发生的概率 < 70%	0.5
低	一年内发生的概率 < 30%	0.3

说明：为更准确地表示发生概率，评估人员或运营总监可酌情调整概率数值，最大为 1，表示 100%的发生概率，最小为 0，表示 0%的发生概率，说明未发现该漏洞或缺陷相关的威胁或威胁事件。

影响	说明	数值
高	可能严重影响生产成本、生产进度或绩效的风险	1
中	可能对生产成本、生产进度或绩效产生一般影响的风险	0.5
低	对成本、进度或性能影响较小的风险	0.1

说明：总体影响得分为影响表中影响数值与资产重要性（见下文定义）的乘积，分值 1~10。资产在未确定重要性之前，假设其重要性为 10，直到最终正确分类。

资产重要性矩阵

通过韦斯特曼硬件盘点流程确定了哪些资产或系统需要保护后，对它们进行重要性评分。资产价值表示资产不可用、发生故障或毁坏可能带来的潜在影响。

韦斯特曼按以下标准计算资产价值。

重要性	说明	资产价值
关键	该资产的损失或损坏将对制造系统的运行产生重大/严重影响，直接影响生产，导致主要服务、核心流程或功能不可用。此类资产为单点故障点。	10
高	该资产的损失或损坏将对制造系统的运行产生严重影响，直接影响生产，导致主要服务、核心流程或功能大多不可用。此类资产也可能为单点故障点。	7~9
中	该资产的损失或损坏将对制造系统的运行或生产产生一般影响，导致主要服务、核心流程或功能局部不可用。	3~6
低	该资产的损失或损坏将对制造系统的运行或生产产生微弱影响或没有影响，主要服务、核心流程或功能的可用性几乎不受影响。	1~2

下表为已分配分值的韦斯特曼的资产清单。

资产	重要性	资产价值
IT/通信系统	高	8
OT/现场设备 – PLC、HMI	关键	10
电气系统	关键	10
公用系统	中	6
站点	高	8

3.4.5 分类

要对风险进行分类，首先要计算总体风险评分，公式如下：

风险评分 = 漏洞评分 × 概率 × 影响 × 资产重要性

由此得出的风险评分（1~100）用于确定整体风险水平（基于 NIST SP 800-30[30]），计算修复措施的优先级。

风险级别	说明	风险评分
极高	极高风险表示识别出来的漏洞对组织运营、组织资产或个人可能产生多重严重或灾难性的不利影响。	96~100
高	高风险表示识别出来的漏洞对组织运营、组织资产或个人可能产生严重或灾难性的不利影响。	80~95
中	中风险表示识别出来的漏洞对组织运营、组织资产或个人可能产生严重的不利影响。	21~79
低	低风险表示识别出来的漏洞对组织运营、组织资产或个人产生的不利影响有限。	5~20
极低	极低风险表示识别出来的漏洞对组织运营、组织资产或个人产生的不利影响可以忽略。	0~4

将得到的风险信息输入到风险管理日志中，以方便跟踪，协调修复行动。

3.4.6 修复

对于中等及以上风险，选用以下修复方法：

- **规避** – 通过消除原因消除威胁。
- **缓解** – 找到方法，降低风险概率或影响。
- **接受** – 接受风险。
- **转移** – 让其他方对风险负责（购买保险、外包等），转移风险。

风险缓解和转移工作可能需要额外的研究和时间来实施。如有必要，运营总监会联系 IT/OT 厂商，了解风险情况，请求对方为修复工作提供援助。对于采取的任何纠正措施，包括风险接受，须记入风险管理日志。

所有风险缓解和转移工作都将记入风险管理日志，由运营总监跟踪，直至完成。之后，对实施的缓解措施进行评估，确定漏洞的最新残留风险水平以及残留风险是否在可接受范围内，不影响持续运行。

任何风险接受操作都必须遵循网络安全操作文件中“修复管理和优先级”及“例外管理”章节中定义的流程。

3.4.7 报告

下表列举了运营总监或 IT 经理记录、分析、沟通和升级风险管理结果的频率和形式。

报告方式	说明	频率
风险管理日志	报告风险识别、分析结果和响应计划的文件	一年一次
CSET报告	描述风险评估结果的文件	一年一次
NamicSoft报告	提供Nessus漏洞扫描结果的文件	手动漏洞评估或漏洞后评估

[30] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

运营总监向 CEO 上报风险评估结果（风险管理日志或 CSET 报告）。

风险管理日志样例

风险管理日志由运营总监维护，在月度高管会议上进行审核。日志内容包括最新的风险分析结果和按计划实施的纠正措施状态。

风险	类别（技术、管理、合约、外部）	概率	影响	风险评分	风险缓解策略（如规避、转移、缓解或接受风险）	必要措施	状态（未决、关闭、进行中）	截止日期

3.4.8 定义和缩略词

IT	信息技术，包括服务器、笔记本电脑、工作站、交换机和路由器等设备
OT	运营技术，包括生产过程中使用的工业控制系统设备
漏洞	攻击者可用来获取系统访问权限的弱点或缺陷

3.4.9 其他资源

- 风险管理计划 – 马里兰州信息技术部[31]
- 风险管理计划样例 – 北达科他州[32]

[31] doit.maryland.gov/SDLC/Documents/Project%20Risk%20Managment%20Plan.doc
[32] https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-sample.pdf

3.5 事件响应计划文件示例

本节以为韦斯特曼公司（虚构）开发的政策程序文件和声明为例，介绍了事件响应计划文件中所包含的内容。本文中提到的商业实体、设备、材料等或有标识，仅为准确描述概念之用，并非暗示 NIST 推荐或认可，也不表明这些实体、设备、材料是实现目的之最佳选择。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的内容及政策程序文件和声明。

韦斯特曼
事件响应计划

文件负责人	运营总监

版本信息

版本号	日期	说明	作者
1.0	2018-02-22	新建文档	运营总监
2.0	2018-04-21	对文档做了重要修订	运营总监

审批

（如下签名表示审批者对本文档所有条款和条件均表示认可。）

审批人	角色	签名	批准日期
S. Forthright	CEO	<数字签名>	2018-04-22

3.5.1 管理承诺书

韦斯特曼管理团队致力于保障信息安全，并对公司内部的意外或蓄意网络安全事件进行合理响应。韦斯特曼制定了事件响应计划，以建立切实可行的信息安全事件处理能力，包括网络安全事件规划、检测、分析、遏制和报告。

3.5.2 目的与范围

安全事件指实际或潜在影响制造系统或系统所处理、存储、传输信息的可用性、完整性或机密性的事件，或违反或有可能违反安全政策、安全程序或可接受使用策略的事件。本文件为韦斯特曼的网络安全事件响应计划，定义了人员的角色和职责、事件分类、事件响应工作流和报告要求，目的是确定网络安全事件的范围和风险，对事件做出正确响应，与所有利益相关者沟通，减轻事件的后续影响。本计划适用于韦斯特曼制造系统的所有人员、网络、系统和数据。

3.5.3 角色与职责

下表列举了事件响应团队的组成人员 及其职责。更多人员职责，详见计划。

角色	事件响应职责
运营总监	• 作为网络安全事件的主要联系人。 • 确保所有员工了解如何识别和报告网络安全事件。 • 牵头事件调查，完成事件报告，必要时向CEO汇报。 • 详细记录网络安全事件。
控制工程师	• 向运营总监报告网络安全事件、运营问题和需要关注的问题。 • 本计划启动后，协助进行事件响应。
IT经理	• 协助调查、解决和缓解网络安全事件。

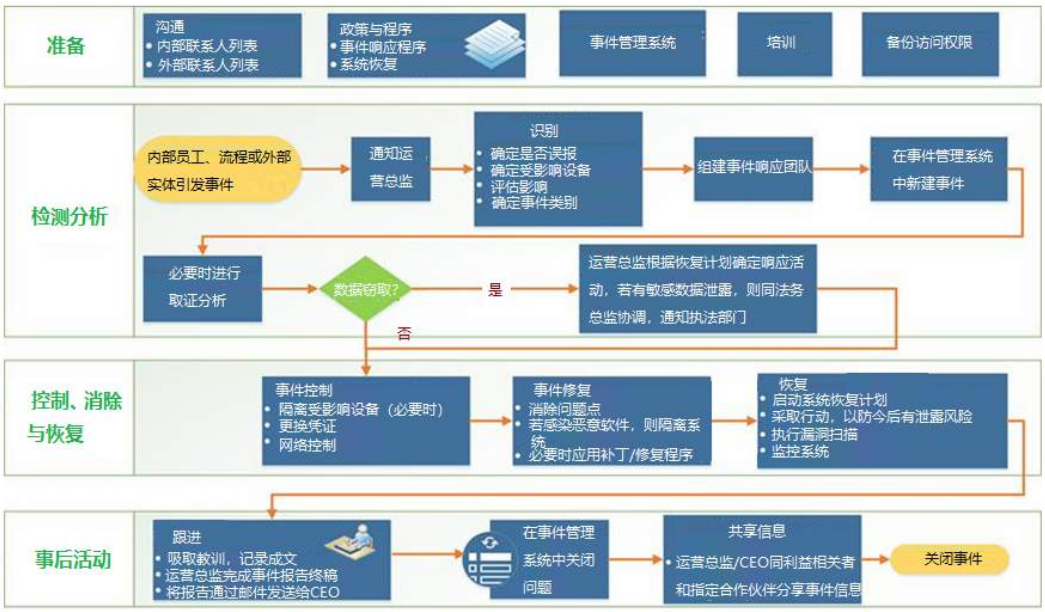
	• 就事件响应程序、政策和最佳实践向运营总监提供建议。
法务总监	• 处理与网络安全事件有关的法律事项或问题。 • 审查网络安全事件相关的外部通信。 • 网络安全事件涉及敏感信息（如PII）数据泄露时，与HR经理协调，通知执法部门。
HR经理	• 处理网络安全事件相关的人事和纪律问题。 • 将涉及敏感信息（如PII）泄露的网络安全事件上报运营总监。

3.5.4 政策

- 通告网络安全事件后，运营总监须根据手头掌握的相关信息确定是否应启动事件响应计划。
- 响应计划启动后，运营总监须通知本文件 3.5.7 节中列出的所有人员。
- 必须彻查事件，了解对制造系统的影响，确定事件类型和严重程度。应使用事件报告模板记录上述信息。事件的严重程度由运营总监与 IT 经理讨论后确定。
- 若需要联系额外资源（即外部实体，如取证调查员、IT 顾问、网络安全顾问、执法人员等）协助事件响应，须获得 CEO 和法务总监的批准。
- 运营总监或 IT 经理须与利益相关者协调事件响应计划。
- 事故发生后，要检视用户意识、培训和测试程序，根据需要进行更新。
- 考虑到事件可能引发法律诉讼，法务总监应全程参与事件响应活动

3.5.5 事件响应流程

须按如下流程进行事件响应。



3.5.6 内外部沟通

以下政策适用于事件响应期间进行的内外部沟通：

- CEO 须识别并及时联系主要合作伙伴、利益相关者和客户，向他们通报响应活动。这一操作的前提是确定了事件的影响，且公司已规划好响应活动。
- 计划启动后，运营总监须联系负责系统恢复的下表所有人员。
- 运营总监须制定要求，明确应如何向利益相关者通报事件响应活动进展。
- 与外部实体的沟通须由本计划明确授权的人员或由运营总监在计划执行期间授权的人员发起。
- 在事件响应期间，与外部实体合作须提前获得 CEO 和法务总监的批准。

3.5.7 联系人信息

韦斯特曼参与事件响应过程的关键人员及其联系信息如下表所示。

姓名	职位	联系方式	联系信息
S. Forthright	首席执行官（CEO）	办公电话	301-555-0141，分机号：102
		手机号	240-555-0159
		备用电话	301-555-3554
		Email	s.forthright@nist-westman.com
W. Lumbergh	运营总监	办公电话	301-555-0141，分机号：103
		手机号	240-555-0110
		备用电话	301-555-3110
		Email	w.lumbergh@nist-westman.com
E. Dufresne	控制工程师	办公电话	301-555-0141，分机号：110
		手机号	240-555-0543
		备用电话	301-555-3543
		Email	e.dufresne@nist-westman.com
M. West	法务总监	办公电话	301-555-0141，分机号：107
		手机号	240-555-2173
		备用电话	301-555-3173
		Email	m.west@nist-westman.com
E. Kenmore	IT经理	办公电话	301-555-0141，分机号：108
		手机号	240-555-0824
		备用电话	301-555-3824
		Email	e.kenmore@nist-westman.com
J. Smith	HR经理	办公电话	301-555-0141，分机号：109
		手机号	240-555-0543
		备用电话	301-555-3543
		Email	j.smith@nist-westman.com

3.5.8 外部联系信息

下表提供了外部实体的联系信息。在执行事件响应计划时，可能会联系这些外部实体，请求支援或提供相关信息以支持响应活动。根据本计划要求，下列外部实体和组织只能由授权人员联系。

实体名	职位	联系方式	联系信息
OT承包商 Cyberdyne系统公司 帐号# 88525462A	总体支持	办公电话	1-800-555-6543（根据提示，依次输入1、3、5）
		手机号	无
		备用电话	无
		Email	support@cyberdynesystems.com
电力公司 帐号# 5486548	总体支持	办公电话	1-800-555-4343（根据提示，依次输入1、4、7、9）
		手机号	无
		备用电话	无
		Email	无
电信运营商 帐号# 3340444	总体支持	办公电话	1-800-555-8769
		手机号	无
		备用电话	无
		Email	无
保险公司： 帐号# 8858444	代理（R. Parr）	办公电话	1-800-555-7643
		手机号	240-555-5698
		备用电话	240-555-5433
		Email	r.parr@insuricare.com

3.5.9 信息共享政策

- 运营总监须与 CEO、IT 经理和法务总监合作，及时编制报告，详细说明事件响应活动，并可与指定的共享伙伴共享该报告。
- 将事件或事件响应信息共享给外部各方之前，须征得 CEO 同意。
- 由 CEO、运营总监、IT 经理和法务总监确定哪些事件信息可与外部共享。

3.5.10 公共传播

- 回应公众时，信息必须清晰、一致、专业。
- 有关网络安全事件的所有公共传播信息须获得 CEO 和法务总监批准。
- 必要情况下，可与外部公关公司签约，由其协助规划响应活动及回应公众质询。
- 所有媒体采访必须得到 CEO 和法务总监的批准。
- 根据网络安全事件的严重程度，由 CEO、运营总监或法务总监回应公众。

3.5.11 计划维护

此计划在如下情况须重新审核并更新：

- 网络安全事件发生后启动响应计划；
- 事件响应演练期间启动计划；
- 组织发生变动；或
- 制造系统或其组件进行了修改或维护，可能影响本计划。

运营总监根据需要与控制工程师和其他人员讨论后更新文件，并将对本政策所做的任何更改或更新传达给执行人员。

3.5.12 计划测试

此计划须在每年的计划停机期间进行测试。在此期间，须召集事件响应团队成员执行以下活动：

- 事件响应桌面演练
- 重新审核响应程序文件
- 验证计划有效性
- 找出计划执行中的差距或缺陷
- 内容过时或不全时更新计划

3.5.13 事件分类

韦斯特曼内部定义了以下类型的网络安全事件。

事件类型	说明
入侵	构成安全事故的一起或多起安全事件，该等事件中，入侵者在没有授权的情况下获取或企图获取系统或系统资源的访问权限[33]。
拒绝服务（DoS）	阻止授权人员访问系统资源或延迟系统操作和功能[34]。
病毒或恶意软件	用于运行非法进程的软件或固件，该进程会对信息系统的机密性、完整性或可用性产生不利影响； 感染主机的病毒、蠕虫、木马或其他基于代码的实体； 间谍软件和有些广告软件也是恶意代码[35]。
社会工程	企图诱骗他人泄露信息（如密码），用于攻击系统或网络[36]。
数据外泄	通过数据窃取或泄露暴露私有、敏感或机密信息[37]。
IT/OT硬件丢失或失窃	去向不明的任何制造系统硬件（在用、备份、备用或剩余）。
用户帐号入侵	非法公开、修改或使用制造系统上的用户帐号。
非法使用系统	未经授权使用制造系统组件。

[33] CNSSI 4009-2015 (IETF RFC 4949 Ver 2)
[34] NIST SP 800-82 Rev. 2 under Denial of Service (DoS) (RFC 4949)
[35] NIST SP 800-82 Rev. 2 under Malware (NIST SP 800-53)
[36] NIST SP 800-82 Rev. 2 under Social Engineering (NIST SP 800-61)
[37] CNSSI 4009-2015 (NIST SP 800-137)

3.5.14 事件严重性分类

网络安全事件的严重性由三个因素决定：对制造业务和信息的影响、对未来业务或信息的潜在影响、可恢复性。事件严重性的分类级别及其依据如下表所述。

严重性	说明
高	• 公司所有用户均受影响。 • 一个或多个任务目标受到严重影响（如生产受到影响或停工）。 • 敏感信息外泄（即数据泄露）。 • 缺乏临时业务程序维持或恢复制造系统生产。 • 无法预测恢复时间、需要额外资源和外部援助或无法恢复[38]。
中	• 一个或多个任务目标受到影响。 • 可采用临时业务程序维持或恢复制造系统生产。 • 服务中断可能影响特定用户，但不涉及敏感或个人数据泄露。 • 非敏感信息外泄（即数据泄露）。 • 可利用现有或额外资源预测何时恢复。
低	• 对任务目标没有影响。 • 服务中断可能只影响单个用户，不涉及敏感信息外泄。 • 可利用现有资源预测何时恢复。

3.5.15 事件报告表模板

事件报告表[39][40]		
联系信息		
日期：		时间：
姓名：	职位：	部门：
办公电话：		
事件信息		
事件发生日期：		事件发生时间：
事件类型 – 勾选所有涉及的类型		
☐ 入侵 ☐ 拒绝服务 ☐ 病毒/恶意软件	☐ 非法使用系统 ☐ 数据泄露 ☐ 硬件被盗	☐ 社会工程 ☐ 用户帐号入侵 ☐ 其他
事件描述：		
（潜在）影响 – 勾选可能存在的所有影响		

[38] NIST SP 800-61 Rev. 2
[39] 宾夕法尼亚州公共服务部，
http://www.dhs.pa.gov/cs/groups/webcontent/documents/form/p_031584.doc
[40] AHIMA BOK，https://bok.ahima.org/doc?oid=76732

☐ 数据外泄或入侵	☐ 财务损失
☐ 破坏系统	☐ 影响其他组织
☐ 祸及公众	☐ 破坏完整性或生产
☐ 系统停机	☐ 目前未知

对影响的具体说明：

事件报告表（续）

受影响系统

主机	IP地址	应用程序（若有）	操作系统

数据外泄范围（若有）

☐ 公开 – 先前批准发布或公开的数据。

☐ 内部使用 – 供公司内部、附属机构或业务伙伴使用的数据。未经授权披露这些数据可能违反法律法规，并可能对公司或其业务伙伴或客户造成损害。

☐ 敏感 – 隐私、私有、客户或商业机密数据，仅限于出于合法业务需要访问。未经授权披露这些数据（如商业机密、源代码、人事数据、PII）会违反法律法规，可能对公司、业务伙伴或客户带来伤害。

数据外泄信息

对数据外泄进行具体说明：

启动后续跟进

☐ 通知执法机构	☐ 从网络中移除系统
☐ 备份恢复	☐ 查看日志文件
☐ 更新病毒库	☐ 无后续行动
☐ 系统重映像或隔离	☐ 其他

若已启动跟进行动，请进一步说明：

运营总监签字

姓名：	签名：	日期：

3.5.16 缩略词

缩略词	全称	中文含义
CEO	Chief Executive Officer	首席执行官
CNSSI	Committee on National Security Systems Instruction	国家安全系统指导委员会
DMZ	Demilitarized Zone	非军事区
DOS	Denial of Service	拒绝服务
HR	Human Resources	人力资源
IRP	Incident Response Plan	事件响应计划
IT	Information Technology	信息技术
LAN	Local Area Network	局域网
NIST SP	National Institute of Standards and Technology Special Publication	国家标准与技术研究院特刊
NTP	Network Time Protocol	网络时间协议
OT	Operational Technology	运营技术
PII	Personally Identifiable Information	个人身份信息
PLC	Programmable Logic Controller	可编程逻辑控制器
RFC	Request for Comment	征求意见稿
SD	Secure Digital	安全数字卡
VHD	Virtual Hard Drive	虚拟硬盘

3.5.17 定义

术语	定义
敏感	仅限于为合法业务需要才能访问的私有、客户、商业机密等信息，未经授权披露这些数据（如商业机密、源代码、人事数据、PII）会违反法律法规，很可能损害公司、业务伙伴或客户。
安全事件	实际或潜在影响制造系统或系统所处理、存储或传输信息的可用性、完整性或机密性的事件，或违反或有可能违反安全政策、安全程序或可接受使用策略的事件。
内部使用	供公司内部、附属机构或业务伙伴使用的数据。未经授权披露这些数据可能违反法律法规，并可能对公司或其业务伙伴或客户造成损害。
人员	所有员工、承包商、厂商和授权在厂区现场或远程工作的人。
公开	先前批准发布或公开的数据。
利益相关人	对系统拥有权利、份额、所有权或利益、或具有可满足需要和期望的特征的个人或组织。（这类人员包括企业所有人、系统所有人、集成商、厂商、人力资源办公室、物理和人员安全办公室、法务部门、运营人员等。）
漏洞	信息系统、系统安全程序、内部控制措施或实现中存在的可由威胁源利用或触发的缺陷。

3.6 系统恢复计划文件示例

本节以为韦斯特曼公司（虚构）开发的政策程序文件和声明为例，介绍了系统恢复计划文件中所包含的内容。本文中提到的商业实体、设备、材料等或有标识，仅为准确描述概念之用，并非暗示 NIST 推荐或认可，也不表明这些实体、设备、材料是实现目的之最佳选择。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的内容及政策程序文件和声明。

韦斯特曼
系统恢复计划

文件负责人	运营总监

版本信息

版本号	**日期**	**说明**	**作者**
1.0	2018-02-22	新建文档	运营总监
2.0	2018-04-21	对最初版本做了重大改动	运营总监

审批

（如下签名表示审批者对本文档所有条款和条件均表示认可。）

审批人	**角色**	**签名**	**批准日期**
S. Forthright	CEO	<数字签名>	2018-04-22

3.6.1 目的

系统恢复计划旨在确保发生网络安全事件时，重要的制造/业务流程不会中断。该计划利用与组织的 IT 和 OT 环境相关的基础设施存量和配置信息，为响应网络安全事件提供结构化方法，恢复运营能力。

3.6.2 目标

本系统恢复计划用以实现以下目标：

- 最大程度地缩短生产中断时间，控制损失；
- 评估损失，修复损坏，恢复制造系统运行；
- 有序、高效地管理恢复操作；及
- 安排人员在系统恢复场景下有效响应。

3.6.3 计划执行

在网络安全事件发生期间或之后，按运营总监的指示执行本计划。

3.6.4 角色与职责

在执行系统恢复计划时，事件响应团队将被调整为系统恢复团队。团队成员承担如下角色和职责：

角色	职责
运营总监	• 主导和监控整个系统恢复过程； • 根据需要，联系承包商或厂商寻求帮助； • 确保所有员工了解自己的角色和职责； • 根据维护政策更新本文件； • 定期向CEO汇报系统恢复的进展。
首席执行官（CEO）	• 根据需要协助运营总监履行其职责； • 作为事件升级的联系人。
控制工程师、IT人员	• 恢复、复原制造系统软硬件或系统以及排除、解决恢复过程中出现的问题； • 将恢复过程中的问题上报给运营总监； • 按恢复计划行事。
OT承包商	• 根据需要，协助恢复制造系统软硬件或系统； • 向运营总监推荐程序、政策和最佳实践，协助恢复过程； • 按恢复计划行事。

3.6.5 内外部沟通

事件响应计划中提供的所有沟通指导也同样适用于系统恢复计划。此外，还要遵循如下针对恢复过程的沟通指导：

- CEO 要联系主要合作伙伴和客户，向他们通报恢复活动。这一操作的前提是确定了事件的影响，且公司已规划好响应活动。
- 计划启动后，运营总监须联系负责系统恢复的下表所有人员。
- 考虑到网络安全事件可能引发法律诉讼，法务总监应全程参与事件恢复过程。
- 运营总监、IT 经理和控制工程师将定期向 CEO 和其他利益相关者通报恢复活动的进展。CEO 会根据事件的影响定义利益相关者和更新周期。
- 与外部实体的沟通须由本计划明确授权的人员或由运营总监在计划执行期间授权的人员发起。

3.6.6 恢复信任

- CEO 或运营总监根据外部顾问和取证专家的建议，通知合作伙伴、厂商和客户本公司为恢复制造系统和加强网络安全控制所采取的行动。
- 运营总监和 IT 经理与员工讨论计划启动的原因以及为避免将来发生类似事件所采取的措施。
- 缓解网络安全事件并获取了事件的所有信息之后，运营总监将提供一份完整报告，供公开发布。该报告包含网络安全事件相关信息、为保护制造系统而采取的步骤以及为避免今后发生类似事件所采取的行动。

3.6.7 联系人信息

韦斯特曼参与事件恢复过程的关键人员及其联系信息如下表所示。

姓名	职位	联系方式	联系信息
S. Forthright	首席执行官（CEO）	办公电话	301-555-0141，分机号：102
		手机号	240-555-0159
		备用电话	301-555-3554
		Email	s.forthright@nist-westman.com
W. Lumbergh	运营总监	办公电话	301-555-0141，分机号：103
		手机号	240-555-0110
		备用电话	301-555-3110
		Email	w.lumbergh@nist-westman.com
E. Dufresne	控制工程师	办公电话	301-555-0141，分机号：110
		手机号	240-555-0543
		备用电话	301-555-3543
		Email	e.dufresne@nist-westman.com
M. West	法务总监	办公电话	301-555-0141，分机号：107
		手机号	240-555-2173
		备用电话	301-555-3173
		Email	m.west@nist-westman.com
E. Kenmore	IT经理	办公电话	301-555-0141，分机号：108
		手机号	240-555-0824
		备用电话	301-555-3824
		Email	e.kenmore@nist-westman.com
J. Smith	HR经理	办公电话	301-555-0141，分机号：109
		手机号	240-555-0543
		备用电话	301-555-3543
		Email	j.smith@nist-westman.com

3.6.8 外部联系信息

下表提供了外部实体和组织的联系信息。在执行事件恢复计划时，可能会联系他们，请求支援或提供相关信息以支持恢复活动。根据本计划要求，下列外部实体和组织只能由授权人员联系。

实体名	职位	联系方式	联系信息
OT承包商 Cyberdyne系统公司 帐号：# 88525462A	总体支持	办公电话	1-800-555-6543（根据提示，依次输入1、3、5）
		手机号	无
		备用电话	无
		Email	support@cyberdynesystems.com

电力公司 帐号：# 5486548	总体支持	办公电话	1-800-555-4343（依次输入1、4、7、9）
		手机号	无
		备用电话	无
		Email	无
电信运营商 帐号：# 3340444	总体支持	办公电话	1-800-555-8769
		手机号	无
		备用电话	无
		Email	无
保险公司： 帐号：# 8858444	代理（R. Parr）	办公电话	1-800-555-7643
		手机号	240-555-5698
		备用电话	240-555-5433
		Email	r.parr@insuricare.com

3.6.9 计划维护

系统恢复计划在如下情况应重新审核并更新：

- 网络安全事件发生后启动恢复计划；
- 事件响应或恢复演练期间启动计划；
- 组织发生变动；或
- 制造系统或其组件进行了修改或维护，可能影响本计划。

根据需要，运营总监与控制工程师和其他人员进行协商，更新文件。

3.6.10 计划测试

此计划须在每年的计划停机期间进行测试。在此期间，须召集事件恢复团队成员执行以下活动：

- 事件恢复桌面演练
- 重新审核恢复程序文件
- 验证计划有效性
- 找出计划执行中的差距或缺陷
- 内容过时或不全时更新计划

3.6.11 需要恢复的硬件

下列各表列举了恢复制造系统设备所需的重要信息，每个表格列举一种设备的相关信息（如主机名、文件系统、物理位置、备份策略）。3.6.12 节介绍了这些设备的恢复策略。有关主机的更多系统信息，请参考“硬件清单”。

工厂服务器

工程师站	
主机名	FGS-47631EHH
型号	HP Z230
IP地址	172.16.3.10
网络	工程局域网

位置	101机柜
类型	物理
操作系统	Windows 7
文件系统	C盘：465 GB
备份策略	Veeam目录备份针对的是包含制造系统配置和逻辑数据的目录： 在低产能运转期间（如夜间）进行，每周一次。
	Veeam系统映像完整备份： 在低产能运转期间（如夜间）进行，每季度一次。 发生工程变更后执行。
恢复优先级	中
恢复策略	Veeam目录恢复（3.6.12.1节）
	Veeam映像完整恢复（3.6.12.2节）

OPC服务器	
主机名	FGS-61338OSH
型号	超微Z97X
IP地址	172.16.2.5
网络	监控局域网
位置	101机柜
类型	物理
操作系统	Windows 7
文件系统	C盘：233 GB
	O:\OPC_Share (\\172.16.2.5)
备份策略	Veeam系统映像完整备份： 在低产能运转期间（如夜间）进行，每季度一次。 发生工程变更后执行
恢复优先级	高
恢复策略	Veeam映像完整恢复（3.6.12.2节）

过程控制器服务器	
主机名	FGS-61338CH
型号	超微Z97X
IP地址	172.16.1.5
网络	运营局域网
位置	101机柜
类型	物理
操作系统	Windows 7
文件系统	C盘：233 GB

备份策略	Veeam系统映像完整备份： 在低产能运转期间（如夜间）进行，每季度一次。 发生工程变更后执行
恢复优先级	高
恢复策略	Veeam映像完整恢复（3.6.12.2节）

HMI宿主服务器	
主机名	FGS-61338HH
型号	超微Z97X
IP地址	172.16.1.4
网络	运营局域网
位置	101机柜
类型	物理
操作系统	Windows 7
文件系统	C盘：233G
	O:\OPC_Share (\\172.16.2.5)
备份策略	Veeam系统映像完整备份： 在低产能运转期间（如夜间）进行，每季度一次。 发生工程变更后执行
恢复优先级	高
恢复策略	Veeam映像完整恢复（3.6.12.2节）

本地历史数据库主机	
主机名	FGS-61338LHH
型号	超微Z97X
IP地址	172.16.2.5
网络	监控局域网
位置	101机柜
类型	物理
操作系统	Windows 7
宿主虚拟机	本地历史数据库虚拟机（WIN- FPVTDCDEUCR）
文件系统	C盘：233 GB
	O:\OPC_Share
备份策略	Veeam系统映像完整备份： 在低产能运转期间（如夜间）进行，每季度一次； 工程变更后进行。
	生产过程中的OSIsoft PI历史数据库数据实时复制到DMZ历史数据库（PI-DMZ）。
恢复优先级	高
恢复策略	Veeam映像完整恢复（3.6.12.2节）

本地历史数据库虚拟机	
主机名	WIN-FPVTDCDEUCR
型号	无
IP地址	172.16.2.14
网络	监控局域网
位置	本地历史数据库服务器（FGS-61338LHH）
类型	虚拟机
操作系统	Windows服务器2008
文件系统	C盘：50 GB虚拟硬盘
	W:\Eng_Workstation (\\172.16.3.10)
备份策略	要备份VHD，可使用宿主服务器、本地历史数据库主机（FGS-61338LHH）的Veeam系统映像完整备份方法。
恢复优先级	高
恢复策略	主机文件系统（FGS-61338LHH）的Veeam映像完整恢复（3.6.12.2节）

控制器PLC	
型号	Allen-Bradley Logix 5571
IP地址	172.16.2.102
网络	监控局域网
位置	101机柜
类型	物理
备份策略	要备份PLC项目文件（存储在本地），可使用工程师站（FGS-47631EHH）的Veeam系统映像完整备份方法。
	PLC项目或其配置只要进行了工程更改，就要手动执行工程师站（FGS-47631EHH）的Veeam系统映像完整备份。
	SD卡内容每年备份一次，备份时间为工厂停工期间。
恢复优先级	高
恢复策略	PLC逻辑恢复（3.6.12.4节）
	PLC SD卡恢复（3.6.12.5节）
	PLC固件恢复（3.6.12.6节）

网络设备

制造系统路由器/防火墙	
主机名	CiscoASA
型号	Cisco ASA 5512
IP地址	企业网络：REDACTED 网络安全局域网：10.100.0.1 DMZ局域网：10.100.1.1

	管理局域网：10.100.2.4
位置	102机柜
类型	物理
操作系统	固件：FTD 6.2.3.7 Build 51
备份策略	手动。通过CLI或Web界面进行。
恢复优先级	高
恢复策略	思科ASA恢复（3.6.12.7节）

边界路由器	
型号	Allen-Bradley 8300
IP地址	10.100.2.8
位置	101机柜
类型	物理
操作系统	固件：V15.2(4a) EA5 Crypto
备份策略	手动。通过CLI或Web用户界面进行。
恢复优先级	高
恢复策略	Allen-Bradley 8300恢复（3.6.12.8）

监控局域网交换机	
型号	Allen-Bradley 5700
IP地址	172.16.2.2
位置	101机柜
类型	物理
操作系统	固件：v15.2(5)EA.fc4
备份策略	手动。通过CLI或Web用户界面进行。
恢复优先级	高
恢复策略	Allen-Bradley 5700恢复（3.6.12.9）

控制局域网交换机	
型号	Allen-Bradley 5700
IP地址	172.16.1.3
位置	101机柜
类型	物理
操作系统	固件：v15.2(5)EA.fc4
备份策略	手动。通过CLI或Web用户界面进行。
恢复优先级	高
恢复策略	Allen-Bradley 5700恢复（3.6.12.9）

网络安全局域网服务器

Hyper-V宿主服务器	
主机名	LANVH
型号	Dell PowerEdge R620
IP地址	10.100.2.10
网络	管理局域网（宿主虚拟机位于网络安全局域网内）
位置	102机柜
类型	物理
操作系统	Windows服务器2012 R2数据中心x64版本
宿主虚拟机	LAN-AD LAN-AD02 SymantecMgrVM 安全洋葱 Graylog GTBInspector GTBCC TheHive NessusVM WSUS
文件系统	C盘：1T
	D盘：3.5 TB
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	高
恢复策略	Veeam映像完整恢复（3.6.12.2节）

活动目录服务器	
主机名	LAN-AD
型号	无
IP地址	10.100.0.13
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）
类型	虚拟
操作系统	Windows服务器2012 R2
文件系统	45 GB虚拟硬盘
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	高
恢复策略	Veeam映像完整恢复（3.6.12.2节）

备份活动目录服务器	
主机名	LAN-AD02
型号	无
IP地址	10.100.0.17
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）
类型	虚拟
操作系统	Windows服务器2012 R2
文件系统	250 GB虚拟硬盘
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	高
恢复策略	Veeam映像完整恢复（3.6.12.2节）

DMZ历史数据库	
主机名	PI-DMZ
型号	无
IP地址	10.100.1.4
网络	生产DMZ
位置	102机柜
类型	虚拟
操作系统	Windows 2008 R2标准版
文件系统	250 GB虚拟硬盘
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
	本机OSIsoft PI应用程序备份功能将生产过程中的生产数据存档，这些备份存储在本地主机上；恢复主机，获取最新的备份版本。说明：可以恢复的历史数据仅限于备份数据。
恢复优先级	中
恢复策略	Veeam映像完整恢复（3.6.12.2节）
	OSIsoft PI生产数据恢复

VMware宿主机	
主机名	ESXi-Host
型号	Dell R710
IP地址	10.100.2.9
网络	管理局域网
位置	102机柜
类型	物理

操作系统	VMware vSphere ESXi 6.0.0
宿主虚拟机	PI-DMZ Veeam
文件系统	4.5 TB（DataStore1）
备份策略	手动。通过CLI或Web用户界面进行。
恢复优先级	高
恢复策略	VMware ESXi恢复（3.6.12.11节）

Veeam备份服务器	
主机名	Veeam
型号	无
IP地址	10.100.0.10
网络	网络安全局域网
位置	VMware宿主机（ESXi-Host）
类型	虚拟
Operating System	Windows服务器2012 R2
文件系统	C盘：50 GB虚拟硬盘
	E盘：500 GB虚拟硬盘
	F盘：4 TB虚拟硬盘
	网络共享（宿主机，F:\Backup\Network Devices）
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	高
恢复策略	Veeam虚拟机即时恢复（3.6.12.3）

赛门铁克防病毒服务器	
主机名	SymantecMgrVM
型号	无
IP地址	10.100.0.5
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）
类型	虚拟
操作系统	Windows服务器2012 R2
文件系统	70 GB虚拟硬盘
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	中
恢复策略	Veeam映像完整恢复（3.6.12.2节）

安全洋葱服务器	
主机名	安全洋葱
型号	无
IP地址	10.100.0.26
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）
类型	虚拟
操作系统	Ubuntu 16.04
文件系统	根文件系统（500 GB，VHD）
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	低
恢复策略	Veeam映像完整恢复（3.6.12.2节）

Graylog服务器	
主机名	Graylog
型号	无
IP地址	10.100.0.14
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）
类型	虚拟
操作系统	Ubuntu 14.04
文件系统	根文件系统（50 GB）
	数据文件系统（500 GB）
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	低
恢复策略	Veeam映像完整恢复（3.6.12.2节）

GTB Inspector服务器	
主机名	GTBInspector
型号	无
IP地址	10.100.0.175
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）
类型	虚拟
操作系统	CentOS 7.4.1708
文件系统	162 GB（厂商配置）

备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	低
恢复策略	Veeam映像完整恢复（3.6.12.2节）

GTB控制台服务器	
主机名	GTBCC
型号	无
IP地址	10.100.0.176
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）
类型	虚拟
操作系统	CentOS 7.4.1708
文件系统	107 GB（厂商配置）
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	低
恢复策略	Veeam映像完整恢复（3.6.12.2节）

TheHive项目事件响应服务器	
主机名	The-Hive
型号	无
IP地址	10.100.0.51
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）
类型	虚拟
操作系统	Ubuntu 16.04
文件系统	根文件系统（50 GB虚拟硬盘）
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	低
恢复策略	Veeam映像完整恢复（3.6.12.2节）

Nessus漏洞扫描器服务器	
主机名	NessusVM
型号	无
IP地址	10.100.0.25
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）

类型	虚拟
操作系统	Windows服务器2012 R2
文件系统	C盘：65 GB虚拟硬盘
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	中
恢复策略	Veeam映像完整恢复（3.6.12.2节）

Windows WSUS服务器	
主机名	WSUS
型号	无
IP地址	10.100.0.12
网络	网络安全局域网
位置	Hyper-V宿主服务器（LANVH）
类型	虚拟
操作系统	Windows服务器2012 R2
文件系统	C盘：400 GB虚拟硬盘
备份策略	Veeam系统映像完整备份： 夜间进行，一日一次 配置更改后进行
恢复优先级	低
恢复策略	Veeam映像完整恢复（3.6.12.2节）

NTP服务器	
主机名	NTPSrv
型号	Meinberg LANTIME M900
IP地址	10.100.0.15
网络	网络安全局域网
位置	102机柜
类型	物理
操作系统	固件：6.20.023
备份策略	通过设备的Web界面手动备份配置： 配置更改后进行 配置备份文件手动（如通过闪存或网络共享）传输，存储在Veeam服务器中。
恢复优先级	中
恢复策略	厂商指定的恢复过程（3.6.12.10节）

3.6.12 恢复过程

Veeam 目录级恢复

目录级（文件级）备份允许还原和恢复单个文件和文件夹。此类恢复所需的数据存储在 Veeam 服务器中，参考 Veeam 指南[41]完成恢复过程。

警告：如果要恢复的主机位于运营局域网或监控局域网中，必须在制造系统停止运行时进行恢复。

Veeam 映像完整恢复

映像（卷级）完整备份允许还原和恢复主机或主机文件系统的特定卷。此类恢复所需的数据存储在 Veeam 服务器中，参考 Veeam 指南[42]完成恢复过程。

警告：如果要恢复的主机位于运营局域网或监控局域网中，必须在制造系统处于非运行状态时进行恢复。

Veeam 虚拟机即时恢复

虚拟机备份允许创建完整的系统映像，类似于物理主机的 Veeam 映像完整备份。这类备份可用于恢复文件、文件系统和完整恢复。参考 Veeam 恢复指南（分别针对 Hyper-V[43]和 VMware[44]）和还原指南[45]完成恢复。

PLC 逻辑恢复

在出现入侵或损坏时，PLC 逻辑恢复可将 PLC 逻辑恢复到事件发生之前的已知正常状态。此操作必须在工程师站上执行，参考 Allen-Bradley PLC 指南[46]完成恢复过程。

警告：必须在制造系统处于非运行状态时执行此类恢复。

PLC SD 卡恢复

在出现入侵或损坏时，PLC SD 卡恢复可将 PLC 逻辑迅速恢复到事件发生之前的正常状态。大致流程如下，更多信息，见制造商文件[47]。

- 关闭 PLC 电源，从设备前面板取出 SD 卡。
- 将 SD 卡插入工程师站。
- 删除 SD 卡中的所有内容，或干脆重新格式化 SD 卡。
- 将最近备份的文件复制到 SD 卡上。
- 将 SD 卡从工程师站安全取出。
- 将 SD 卡插入 PLC 并接通设备电源。

注意：这种恢复只能恢复逻辑，不会恢复 PLC 的配置或机箱内的其他模块。

警告：若更换了 PLC 或任何其他模块，请不要使用此恢复方法。

警告：必须在制造系统停止运行时执行此类恢复。

41 https://helpcenter.veeam.com/docs/backup/vsphere/restore_vead.html?ver=95u4
42 https://www.veeam.com/veeam_backup_9_5_u4_enterprise_manager_user_guide_pg.pdf
43 https://helpcenter.veeam.com/docs/backup/hyperv/data_recovery.html?ver=95u4
44 https://helpcenter.veeam.com/docs/backup/vsphere/data_recovery.html?ver=95u4
45 https://helpcenter.veeam.com/docs/backup/vsphere/vbr_config_restore.html?ver=95u4
46 https://literature.rockwellautomation.com/idc/groups/literature/documents/pm/1756-pm014_-en-p.pdf
47 https://literature.rockwellautomation.com/idc/groups/literature/documents/pm/1756-pm017_-en-p.pdf

PLC 固件恢复

PLC 固件恢复可用来恢复 PLC 操作系统，此操作必须在工程师站上执行。

- 从倍福网站下载最新的固件映像[48]。
- 关闭 PLC 电源，从设备前面板取出 SD 卡。
- 将 SD 卡插入工程师站。
- 删除 SD 卡中的所有内容，或干脆重新格式化 SD 卡。
- 将最近备份的新固件文件复制到 SD 卡上。
- 将 SD 卡从工程师站安全取出。
- 将 SD 卡插入 PLC 并接通设备电源。
- 将工程师站通过 TwinCAT 软件连接到 PLC，打开 PLC 项目，激活配置，部署 PLC 项目。
- 断开与 PLC 的连接。

警告：必须在制造系统处于非运行状态时执行此类恢复。

思科 ASA 5512 恢复

在出现入侵或损坏时，通过恢复过程可将思科 ASA 5512 恢复到事件发生之前的已知正常状态。执行该操作时，设备必须连接到网络安全局域网。参考思科指南[49]完成恢复过程。

Allen-Bradley 8300 恢复

在大多数情况下，只需要恢复配置，但在特定情况下，可能需要在恢复之前按厂商要求恢复出厂设置，步骤如下：

- 首先，断开交换机电源。
- 接下来，在通电时用细电线或回形针按下**【快速设置】**按钮。
- 当设备前面板上的 3 个 LED 灯（EIP 模块、EIP 网络和设置）变红时，松开按钮。交换机继续正常引导。（大约需要 3 分钟）
- 用保存的配置备份还原配置。具体操作说明，见用户手册[50]。

Allen-Bradley 5700 恢复

在大多数情况下，只需要恢复配置，但是在某些情况下，可能需要在恢复之前按厂商要求恢复出厂设置。

请按以下步骤恢复出厂设置：

进入设备管理器：

- 选择**管理 > 重启/重置**。
- 在**【重启/重置】**页签上，单击**【恢复交换机的出厂设置】**，然后重新启动交换机。

48 https://infosys.beckhoff.com
49 https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html
50 https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

- 用保存的配置备份还原配置。具体操作说明，见用户手册[51]。

NTP 服务器恢复

NTP 服务器恢复通过设备的 Web 界面执行[52]。设备不工作时，可通过设备前面的显示器/键盘按厂商要求恢复出厂设置。设备工作时，可通过 Web 界面用保存的配置备份还原配置。

VMware ESXi 恢复

从受信任媒体重新加载相同版本的 ESXi，用备份文件还原配置（详细信息，请参阅 VMware 知识库[53]）。可通过 ESXi 控制台恢复配置，具体方法如下：

进入 ESXi 控制台：

- 运行以下命令，将主机设置为维护模式：

  vim-cmd hostsvc/maintenance_mode_enter
- 使用 SCP 将备份配置文件复制到主机的/tmp 目录，将其命名为 configBundle.tgz。
- 运行以下命令，还原配置：

  vim-cmd hostsvc/firmware/restore_config /tmp/configBundle.tgz

  注意：该命令执行完毕后，主机会自动重启。
- 按照 Veeam 虚拟机即时恢复过程（3.6.12.3 节）用 Veeam 备份文件恢复各虚拟机。

51 https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf
52 https://www.meinbergglobal.com/download/docs/manuals/english/m900_gps.pdf
53 https://kb.vmware.com/s/article/2042141

3.7 服务水平协议

本节以为韦斯特曼公司（虚构）开发的政策程序文件和声明为例，介绍了厂商服务水平协议（SLA）文件中所包含的内容。本文中提到的商业实体、设备、材料等或有标识，仅为准确描述概念之用，并非暗示 NIST 推荐或认可，也不表明这些实体、设备、材料是实现目的之最佳选择。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的内容及政策程序文件和声明。

韦斯特曼

厂商服务水平协议

（SLA）

生效日期：2019-02-22

文件负责人	CEO

版本信息

版本号	日期	说明	作者
1.0	2019-02-22	服务水平协议	CEO

审批

（如下签名表示审批者对本协议所有条款和条件均表示认可。）

审批人	角色	签名	批准日期
韦斯特曼	客户	<数字签名>	2019-02-22
厂商	服务提供商	<数字签名>	2019-02-22

3.7.1 概述

本文件为韦斯特曼与厂商（服务提供商）就支持和维护产品或服务所需的 IT/OT 服务签订的服务水平协议（“SLA”或“协议”）。

本协议自签订之日起生效，若利益相关者同意修订协议，则修订后的协议取代当前协议。

本协议规定了主要利益相关者认可的所有 IT/OT 服务的相关参数。除非本协议明确规定，否则本协议不会取代当前的流程和程序。

3.7.2 目标与目的

本协议旨在明确服务要素和承诺，确保服务提供商按统一标准向韦斯特曼提供并交付 IT/OT 服务。本协议的目标是在服务提供商和韦斯特曼之间就提供 IT/OT 服务建立共识。

本协议的目的是：

- 明确服务的所有权、责任、角色和/或职责；
- 向客户简明扼要地描述服务，对服务进行量化；
- 描述对服务的预期，基于此衡量实际的服务支持和交付。

3.7.3 利益相关者

服务提供商和韦斯特曼作为签约方，为本 SLA 的**主要利益相关者：**

- **IT 服务提供商：**服务提供商
- **IT/OT 客户：**韦斯特曼

3.7.4 定期审核

本协议自上述生效日期起持续有效，直至另行通知为止。每财年应至少审核一次协议；但是，在指定期间内未审核的话，当前协议将继续有效。

业务关系管理人（“文件负责人”）负责督促对本文件进行定期审核。本文件内容可根据需要进行修改，前提是获得双方主要利益相关者的同意并传达给相关各方。文件负责人将所有后续修订合入协议，并根据需要获得双方同意/批准。

- **业务关系管理人：**韦斯特曼（CEO）
- **审核周期：**每年（12 个月）一次
- **上次审核日期：**2019-02-22
- **下次审核日期：**2020-02-22

3.7.5 服务范围

本协议包括以下服务：

- 根据厂商建议，更新制造环境系统；
- 各厂商发布补丁时，更新 IT 设备系统；
- 备份韦斯特曼所有 IT/OT 设备的配置信息；
- 确保网络安全工具在环境中正常运行；
- 作为 OT 厂商和韦斯特曼之间的沟通桥梁；
- 就韦斯特曼制造环境中欲购买安装的新设备提供产品建议；
- 人工电话支持；
- 监控邮件支持；
- 使用远程桌面和 VPN（若有）提供远程协助；
- 定期或紧急现场援助（须另外付费）；
- 月度系统健康检查。

3.7.6 对韦斯特曼的要求

为保证协议正常履行，韦斯特曼须按如下要求履行责任：

- 按商定的时间支付所有支持费用；
- 解决与服务相关的事件或请求时，韦斯特曼须指定代表，方便联系。

3.7.7 对服务提供商的要求

为保证协议正常执行，服务提供商须按如下要求履行责任：

- 按照要求，及时响应服务相关事件；
- 每次定期维护前，均提前通知韦斯特曼。

3.7.8 服务假设

与协议项下服务及其组成部分相关的假设包括：

- 将向所有利益相关者传达和记录服务变更。

3.7.9 服务管理

有效履约的前提是按照协议规定水平提供服务。以下各节就服务可用性以及监控协议项下服务及其组成部分进行了详细阐述。

3.7.10 服务可用性

本协议项下服务的具体条款如下：

- 电话支持：周一至周五上午 8:00 至下午 5:00
  - 非办公时间内，电话将被转接到手机上，尽量及时接听/处理；为以防万一，还提供备用电话接听服务。
- 电子邮件支持：周一至周五上午 8:00 至下午 5:00
  - 非办公时间内，电子邮件会被整理收集，但无法保证及时处理，待下一个工作日集中处理。
- 周一至周五期间，可保证 72 小时内提供现场支持。

3.7.11 服务请求

就本协议项下服务，服务提供商将在以下时间内对韦斯特曼提交的与服务相关的事件和/或请求作出响应：

- 高优先级问题须在 0 至 8 小时（办公时间）内处理
- 中优先级问题，须在 48 小时内处理
- 低优先级问题，须在 5 个工作日内处理

服务提供商根据韦斯特曼要求，按照上述时间表以及支持请求的优先级提供远程协助，但不得以远程访问替代本协议 3.7.10 节所规定的现场支持。

3.7.12 员变动

当为韦斯特曼提供支持的个人离职或转岗时，服务提供商将在 24 小时内通知韦斯特曼。韦斯特曼将在通知后的 24 小时内，取消该员工的远程访问权限（若有）。服务提供商将在 24 小时内撤销该员工对韦斯特曼信息和信息系统的访问权限。

此外，需要更改该员工的所有系统帐号密码，确保其对网络的访问权限被彻底取消。

4. 技术方案实施

4.1 概述

本章以虚构的韦斯特曼公司为例，介绍了为其开发的 PoC 技术方案实施方法。第 1 卷第 6 章概述了这些技术解决方案，第 7 章讨论了可能的技术方案。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的产品。

过程控制系统（PCS）主要收集五个方面的性能指标：

- 生产过程性能：衡量生产过程的性能，即化学连续过程。
- 网络性能：衡量底层 TCP/IP 网络的性能。
- 计算资源性能：衡量计算机、硬件和软件进程的性能。
- 工业协议性能：衡量工业通信协议的性能，即 PCS 中的 DeviceNet 协议。
- OPC 数据交换性能：衡量系统数据交换机制的性能。

这几个方面的指标从不同角度反映了整个系统的性能。生产过程性能指标衡量了总体生产过程和整个系统的性能，但可能无法充分反映子系统的性能，因此也要在子系统级别进行测量。例如，与可用的网络带宽相比，典型的化学连续制造是一个相对缓慢的过程，因此，轻微的 TCP/IP 网络延迟可能无法体现在总体生产过程性能指标中，但这种 TCP/IP 延迟可能会对子系统产生重大影响。这些影响在总体测量中无法体现，直到在子系统中聚沙成塔。多级测量提供了详细的性能信息，有助于深入了解整个系统的各方面关键性能，认识聚集效应对性能的影响。聚集效应对总体生产性能具有重要影响。

各技术方案采用实验方式实施。为便于测量，每个实验的运行时间固定为 4 小时（14400 秒）。在整个实验运行期间，收集性能指标并抓包。

实验完成后，所有采集到的指标和抓取的网络报文进入后处理阶段，进行过滤、排序和整理。最后，使用 NIST 开发的 Python 脚本基于排序后的数据集计算关键性能指标。

过程控制系统和测量过程的更多技术细节，见 NISTIR 8188[54]。

4.1.1 实施说明 – 谨慎实施技术方案

需要注意的是，这里描述的实施步骤（安装工具、评估影响等）不应在生产系统中执行。务必谨慎使用技术方案，特别是那些主动扫描制造系统网络及其设备的方案；制造商应提前摸清这些工具的工作原理以及对联网控制设备所产生的潜在影响[3]。进行技术评估时，可在类似的非生产控制系统环境中进行测试，确保工具不会对生产系统产生不良影响。造成影响的原因可能是信息性质，也可能是网络流量。有些影响在 IT 系统中也许可以接受，但在制造系统中却可能无法接受。一般来说，任何对制造网络的主动扫描都应安排在计划停机期间进行[3]。

> 本文中提到的商业实体、设备、材料等或有标识，仅为准确描述实验步骤或概念之用，并非暗示 NIST 推荐或认可，也不表明这些实体、设备、材料是实现目的之最佳选择。各组织的信息安全专家应选用与其现有网络安全计划和制造系统基础架构最为契合的技术方案。

[54] NISTIR 8188：Key Performance Indicators for Process Control System Cybersecurity Performance Analysis.

4.1.2 实施说明 – 测量数据的可用性

各实验中获取的所有原始数据和处理后测量数据可从以下网址免费获取：https://doi.org/10.18434/M32071.

各项实验结尾均提供了相关数据文件的链接，全部链接如下所示：

- Open-AudIT KPI 数据
- Open-AudIT 测量数据
- Wireshark KPI 数据
- Wireshark 测量数据
- Veeam 全量备份 KPI 数据
- Veeam 全量备份测量数据
- Veeam 增量备份 KPI 数据
- Veeam 增量备份测量数据
- 思科 PN KPI 数据
- 思科 VPN 测量数据
- 活动目录 KPI 数据
- 活动目录测量数据
- 赛门铁克防病毒 KPI 数据
- 赛门铁克防病毒测量数据
- Nessus KPI 数据
- Nessus 测量数据
- 文件加密 KPI 数据
- 文件加密测量数据
- 防火墙 KPI 数据
- 防火墙测量数据

4.2 Open-AudIT

4.2.1 技术方案概述

Open-AudIT 是一种资产清查工具，用于扫描制造环境中的软硬件。Open-AudIT 可针对具体环境，根据所需级别定制扫描任务。

Open-AudIT 的使用成本取决于业务环境所需的功能级别，工具有多个版本，低至免费的入门级社区版，高至企业版。这里选择了企业版，因为它可提供定时扫描配置、仪表盘和建立设备基线等功能。

Open-AudIT 是一款开放式虚拟设备（OVA），方便下载和安装。OVA 可在虚拟机监控程序（Hypervisor）环境中安装，好处是在现有虚拟环境安装时不需要购买额外硬件。初始发现扫描的配置很简单。

4.2.2 方案提供的技术能力

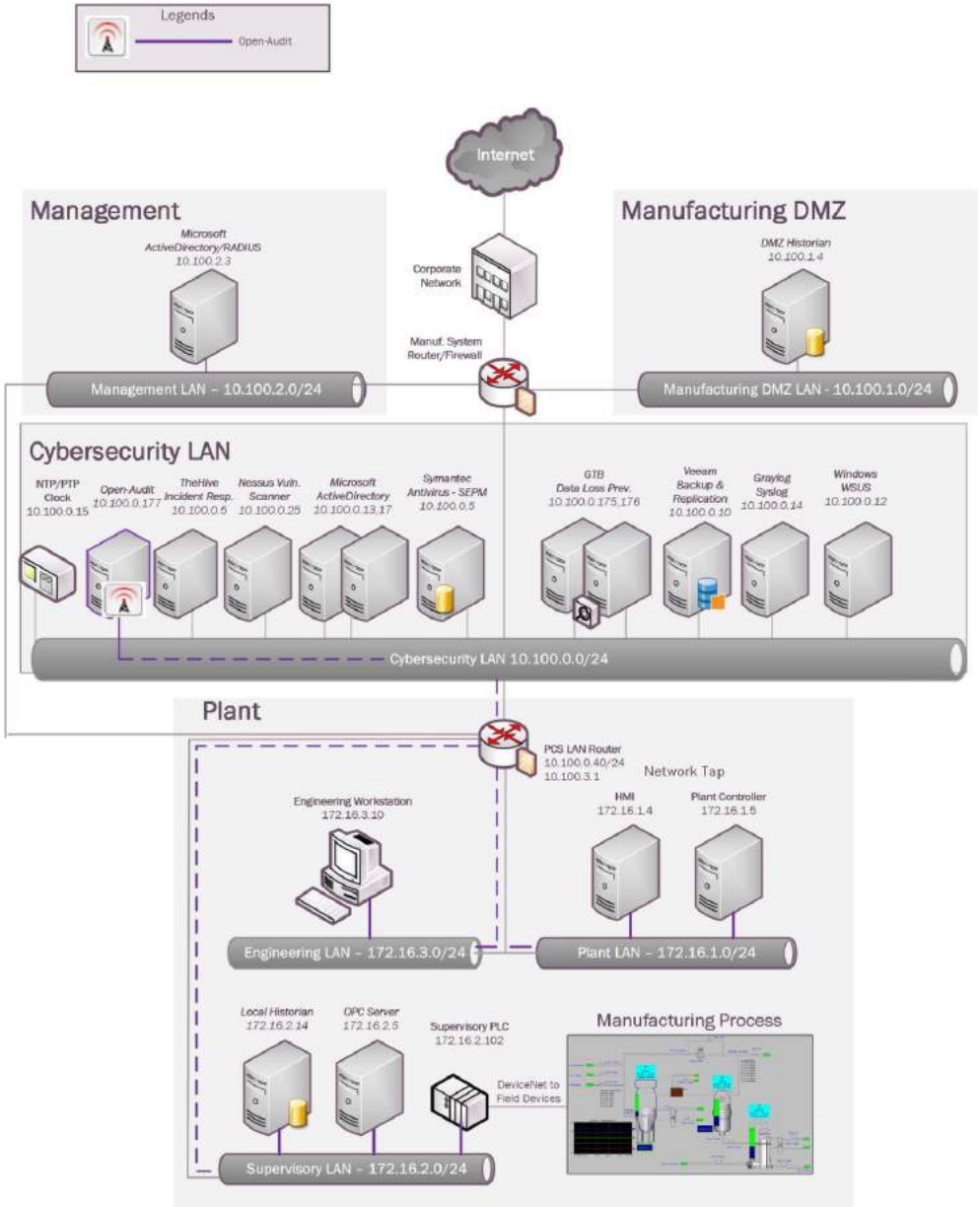
Open-AudIT 提供以下技术能力：

- 硬件盘点
- 软件盘点
- 系统开发生命周期管理
- 配置管理
- 建立基线（企业版）
- 变更控制

4.2.3 方案实现的子类

ID.AM-1，ID.AM-2，ID.AM-3，ID.AM-4，PR.DS-3，PR.IP-1，PR.IP-2，PR.IP-3，PR.IP-4，PR.IP-6，PR.MA-1，DE.AE-1，DE.CM-7

4.2.4 方案实施架构图



4.2.5 安装说明与配置

实施方案的详细信息：

方案名	版本	硬件规格
Open-AudIT	3.0.0	Hyper-V虚拟机（第一代）： • 处理器：虚拟双核 • 内存：2 GB • 磁盘空间：根据厂商提供的虚拟设备文件分配 • 网络：1个接口 • 操作系统：CentOS 7

Open-Audit 环境搭建

- 准备虚拟机，操作系统为 CentOS Linux 7，硬件规格见上表。
- 客户机操作系统的 IP 信息如下：
  - IP 地址：10.100.0.177
  - 网关：10.100.0.1
  - 子网掩码：255.255.255.0
  - 域名服务器：10.100.0.17

安装说明

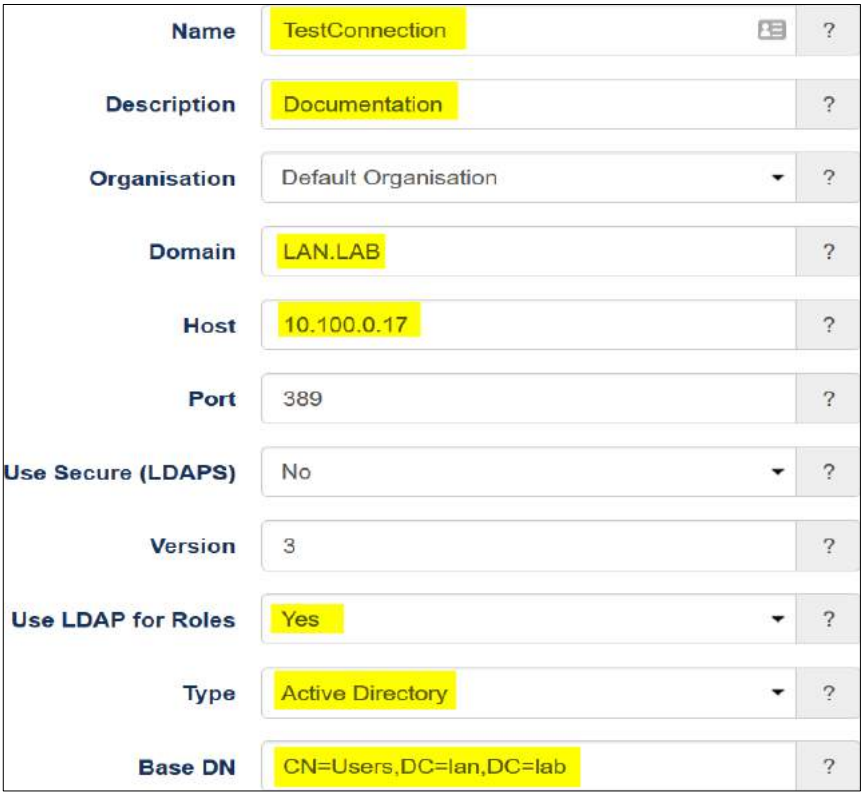
- 下载 Opmantek OVA[55]。
- 若使用 Hyper-V 宿主服务器[56]，请将下载的.ova 文件转换为.vhdx 格式。
- 使用默认凭证登录，设置主机名，为虚拟机分配静态 IP 地址。编辑 /etc./sysconfig/network scripts/ifcfg-eth0 文件，设置网络信息。
- 运行 service network restart 命令，重启网络服务。

通过 Web 浏览器进行其他配置

- 打开 **Open-AudIT 的 Web** 界面（如 http://<ip-address-of-server>）。
- 若提示进入不受信任的站点，请选择【**Yes**】。此错误是由于 SSL 尚未配置且 Open-AudIT 将 HTTP 会话重定向到 HTTPS 而产生的。
- 单击【**Open-AudIT Enterprise**】（Open-AudIT 企业版）。
- 使用网页上提供的默认用户名/密码登录。
- 依次单击 **Admin > LDAP Server > Create LDAP Servers**（管理 > LDAP 服务器 > 创建 LDAP 服务器），与活动目录集成。

[55] https://opmantek.com/
[56] https://blogs.msdn.microsoft.com/timomta/2015/06/11/how-to-convert-a-vmware-vmdk- to-hyper-v-vhd/

如下活动目录连接截图仅供参考。



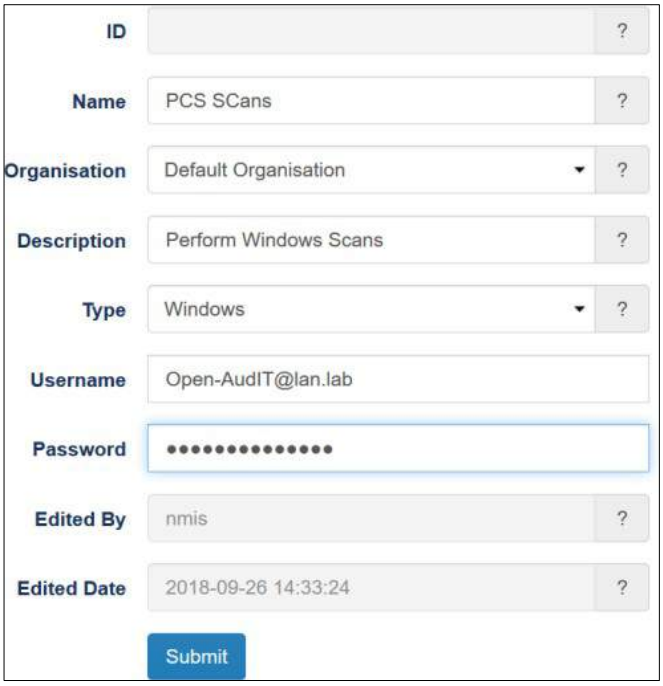
- 输入所有信息后，单击【**Submit**】(提交)。

用于 LDAP 集成的活动目录组

- 在活动目录中，创建以下**全局**类型的**安全**组，与 Open-AudIT 集成：
  - o**pen-audit_roles_admin**
  - **open-audit_roles_org_admin**
  - **open-audit_roles_reporter**
  - **open-audit_roles_user**
  - **open-audit_orgs_default_organisation**
- 将相关用户添加到这些组中。用活动目录凭证测试登陆。

配置发现凭证

- 选择 **Discover > Discoveries > Create Credentials**（发现 > 发现 > 新建凭证）。
- 配置下述参数：
  - **Name**（名称）：当前使用的凭证名称，如 **SSH**。
  - **Organization**（组织）：选择 **Default Organization**（默认组织）。若有其他组织，可根据需要选择。
  - **Description**（说明）：对新建项目的描述。
  - **Type**（类型）：选择要使用的凭证类型，即 **SNMP（v1/v2）、SNMP v3、SSH、SSH Key** 或 **Windows**。
  - **Credentials（凭证）**：根据上面选择的类型，输入相应凭证。
  - 下图显示了为扫描工厂网络创建的发现凭证。

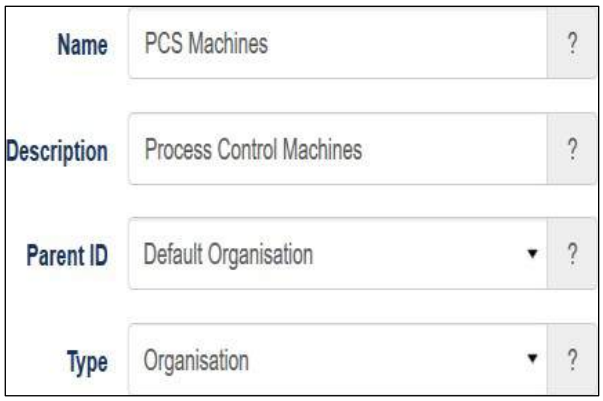


- 单击【**Submit**】（提交）。

组织群组

- 选择 **Manage > Orgs > Create Orgs**（管理 > 组织 > 新建组织）。
- 设置 **Name**（名称）和 **Description**（说明）。
- 单击【**Submit**】（提交）。

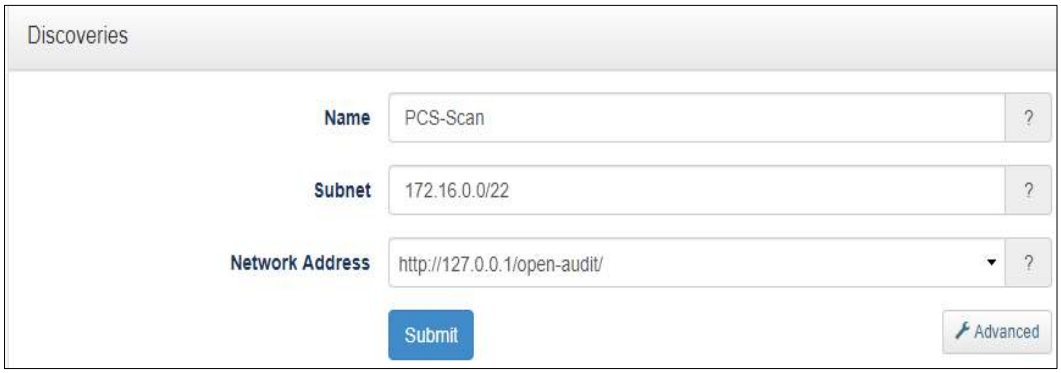
下图显示了为实验室环境创建的组织群组。



发现扫描

- 选择 **Discover > Discoveries > Create Discoveries**（发现 > 发现 > 新建发现）。
- 设置 **Name**（名称）。
- 设置要扫描的 **Subnet**（子网）。
- 在 **Network Address**（网络地址）处，输入 Open-Audit 服务器地址。
- 单击 **Advanced**（高级），根据需要设置其他参数。可设置的参数包括 **Org**（组织）、**Type**（类型）、**Devices Assigned to Org**（分配给组织的设备）及 **Devices Assigned to Location**（分配给位置的设备）。
- 单击【**Submit**】（提交）。

下图显示了为扫描工厂网络创建的发现任务。



其他信息

- 在生产环境中进行部署之前，更改所有默认密码。
- 使用安全 LDAP（LDAPS）。若无法使用 LDAPS，须确保用于同步群组的帐号仅有最低权限 （非管理员或域管理员）。
- 使用 SNMP 扫描设备时，须使用 SNMPv3。
- Open-AudIT 为开源软件。专业版允许多达 20 台机器，更高版本需要购买，但相对便宜。要进行系统基线扫描，须升级到企业版。
- 欲了解更多信息和硬件要求，请访问社区论坛[57]。

4.2.6 对性能的主要影响

在下面的实验中，我们测量了制造系统正常运行时 Open-AudIT 工具对系统性能的影响：

实验 PL003.1 – 用 Open-AudIT 资产盘点工具进行网络扫描和认证扫描

Open-AudIT 扫描对 PCS 系统中的网络行为有一定性能影响。扫描期间，PCS 系统局部网络流量略有增加，例如，PLC 到 OPC 的路径延迟略长，特别是在后半段 Open-AudIT 执行认证扫描时。然而，在整个扫描过程中，从控制器到 OPC 的往返时间基本相同。显然，工具对系统不同部分的影响存在差异。

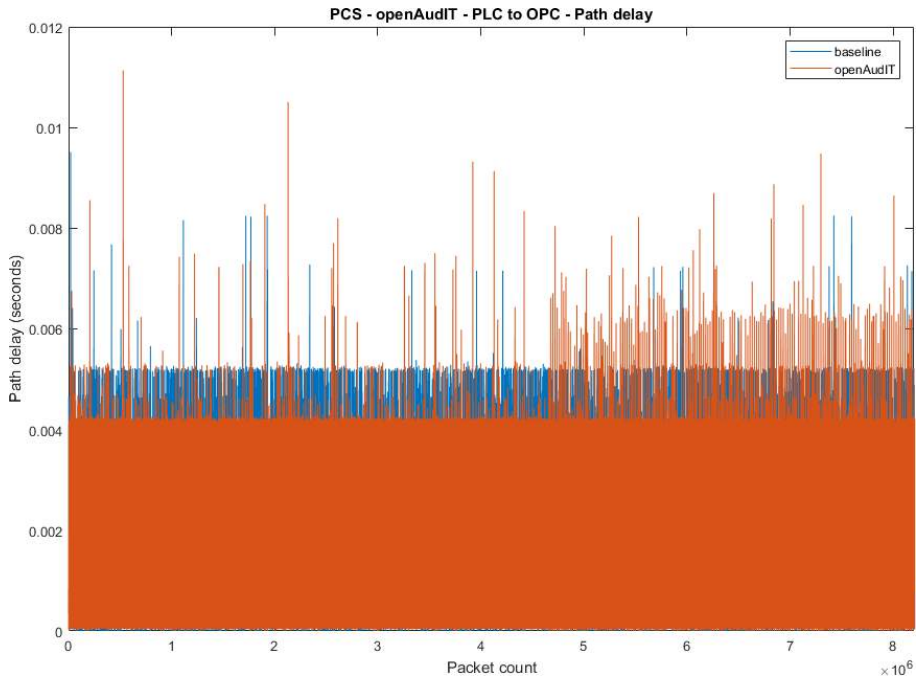


图 4-1 PLC 到 OPC 服务器之间的路径延迟

[57] https://community.opmantek.com

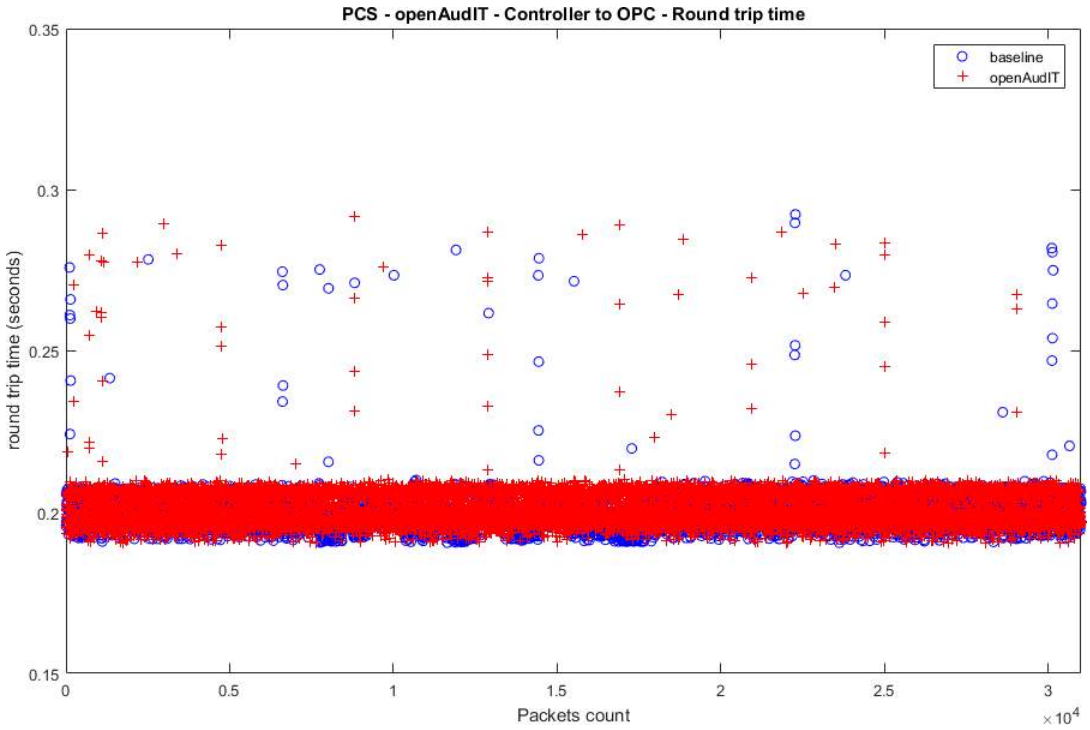


图 4-2 控制器到 OPC 的报文往返时间

根据观察，扫描对生产过程的影响很小，生产过程中的产品流速略高于最优水平。特别是在实验后期，当 Open-AudIT 执行认证扫描时，反应器压强略高于最优水平。但是，这种影响很小，在系统的容许范围内。

我们猜测，这些影响之所以存在是因为系统主机之间的网络延迟有所增加。由于过程模拟的迭代性质以及传感器和执行器之间存在值交换，网络影响不会立刻传递到生产过程，会有一定的时间延迟。

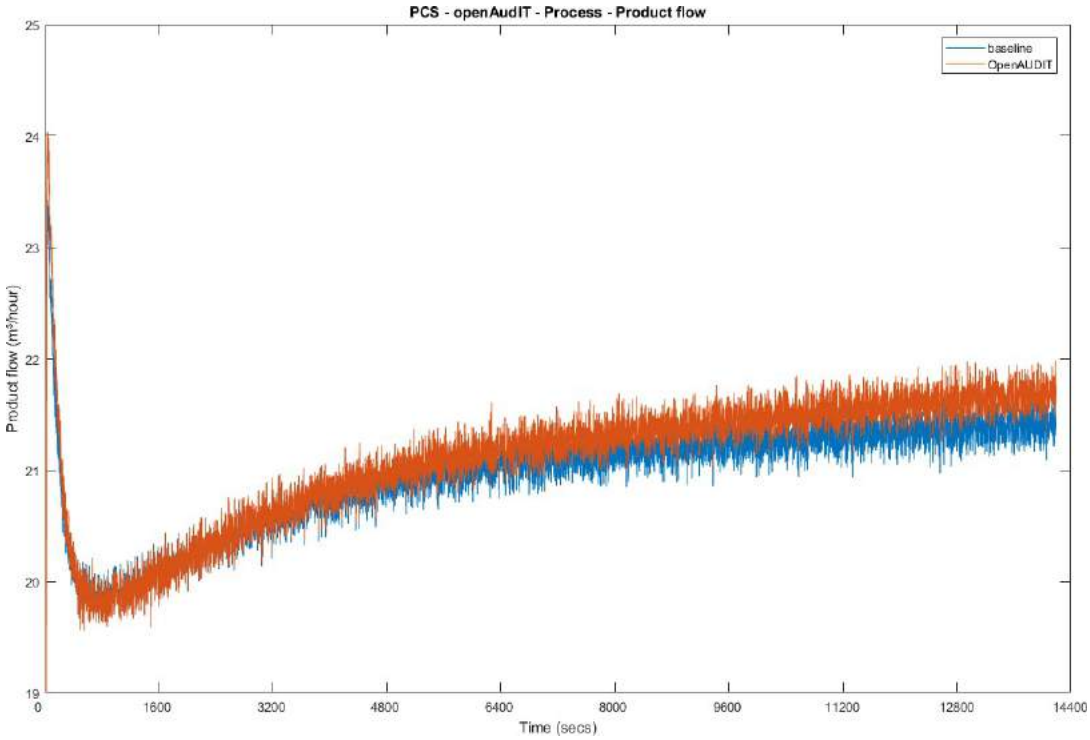


图 4-3 生产过程中的产品流速

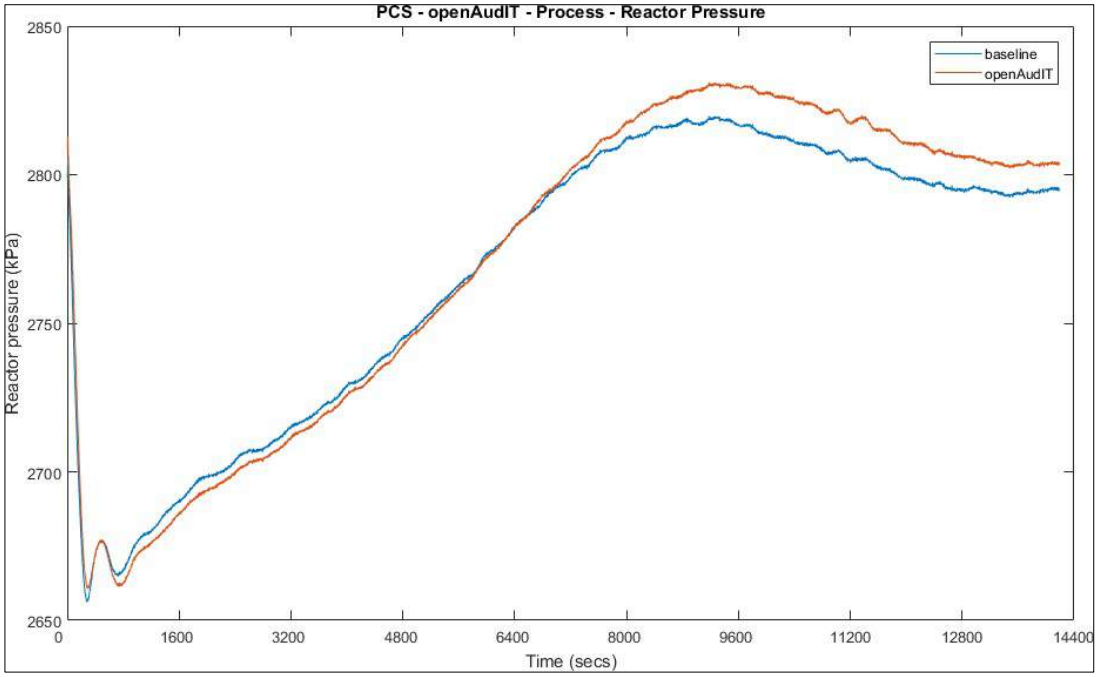


图 4-4 生产过程中的反应器压强

4.2.7 性能测量数据集的相关链接

- Open-AudIT KPI 数据
- Open-AudIT 测量数据

4.3 CSET

4.3.1 技术方案概述

网络安全评估工具（CSET）是国土安全部为评估组织的网络安全而提供的工具。该评估是一个全手动过程，需要根据所采用的网络安全实践和当前的网络安全状况回答多个问题，以确定组织的网络安全态势。评估后，组织可确定哪些领域需要更多关注和资源。

4.3.2 方案提供的技术能力

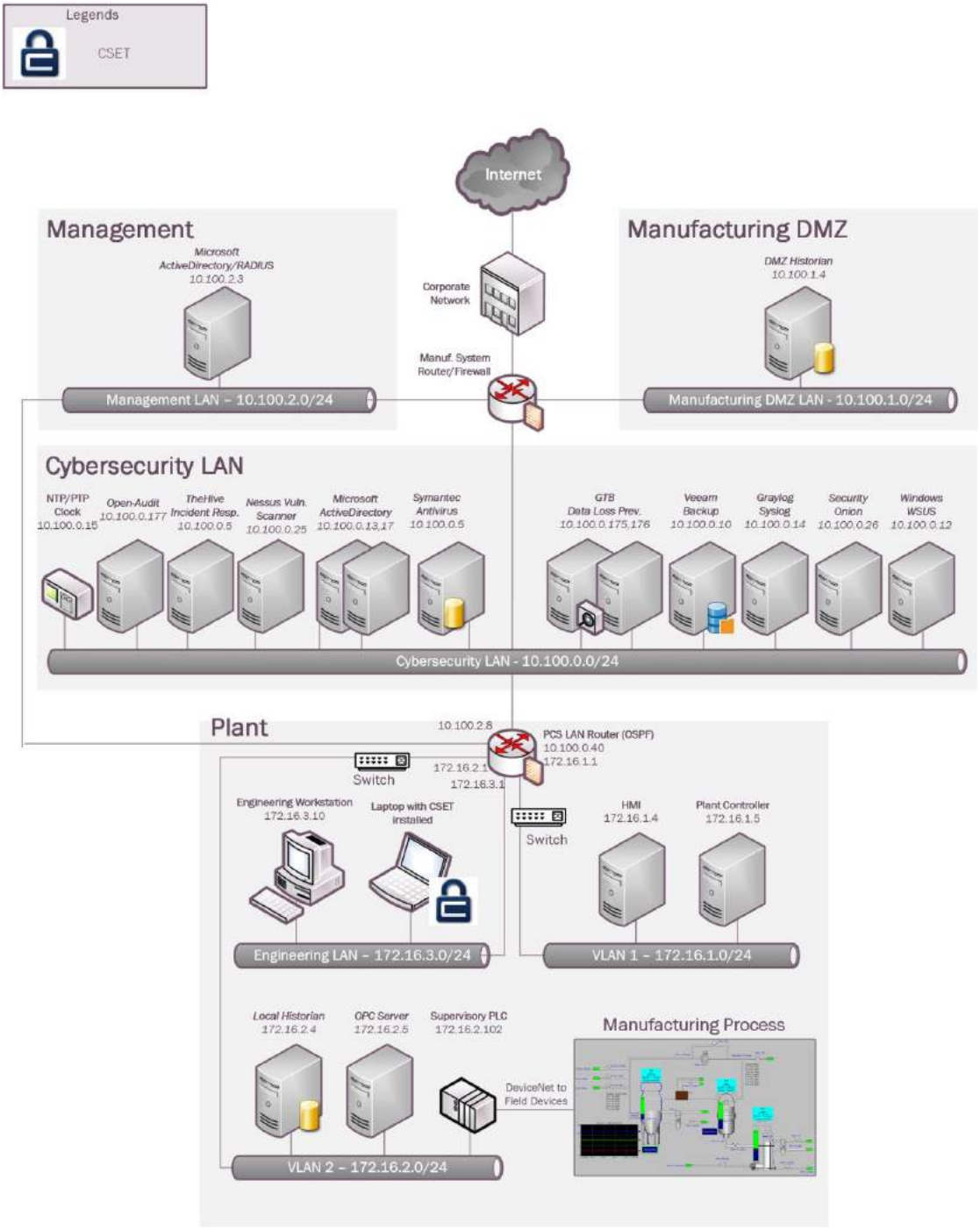
CSET 提供以下技术能力（参见第 1 卷第 6 章）：

- 网络架构文档
- 风险评估

4.3.3 方案实现的子类

ID.AM-3，ID.AM-4，ID.RA-1

4.3.4 方案实现的子类



4.3.5 安装说明与配置

实施方案的详细信息：；p 0 o l

方案名	版本	硬件规格
CSET	8.1	笔记本电脑规格如下： • 处理器：i7 • 内存：16 GB • 磁盘：256 GB • 操作系统：Windows 7专业版

环境搭建

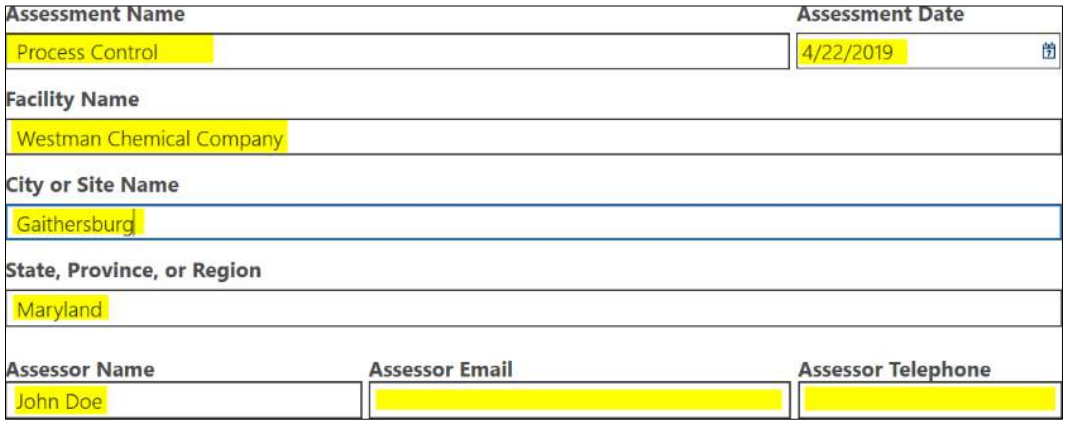
根据需要，在临时笔记本电脑（操作系统为 Windows）上安装 CSET，接入工厂网络。

安装

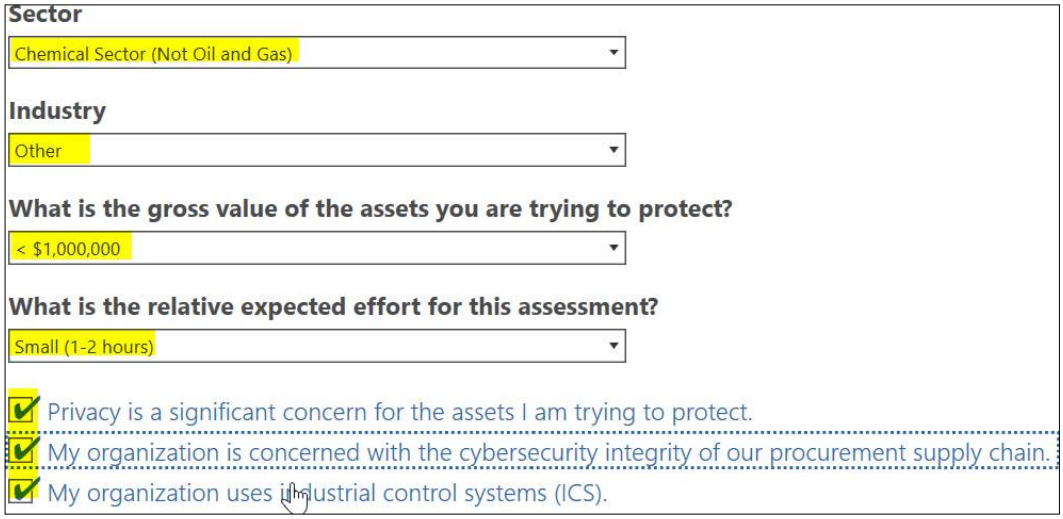
- 下载 CSET[58]。点击链接后，根据提示输入个人信息，然后下载 CSET_x.x.iso 文件（x.x.代表版本号）。
- 使用任一 ISO 专用程序，加载文件。
- 在文件夹、虚拟驱动器或 CD 中找到 **CSET_Setup.exe** 文件并运行。
- 根据安装向导提示，完成程序安装。

运行 CSET

- 双击桌面图标，启动程序。
- 在主页上单击【**New Assetment**】（新评估）。
- 单击程序右下角的【**Start Here**】（开始）。
- 填写所有信息。

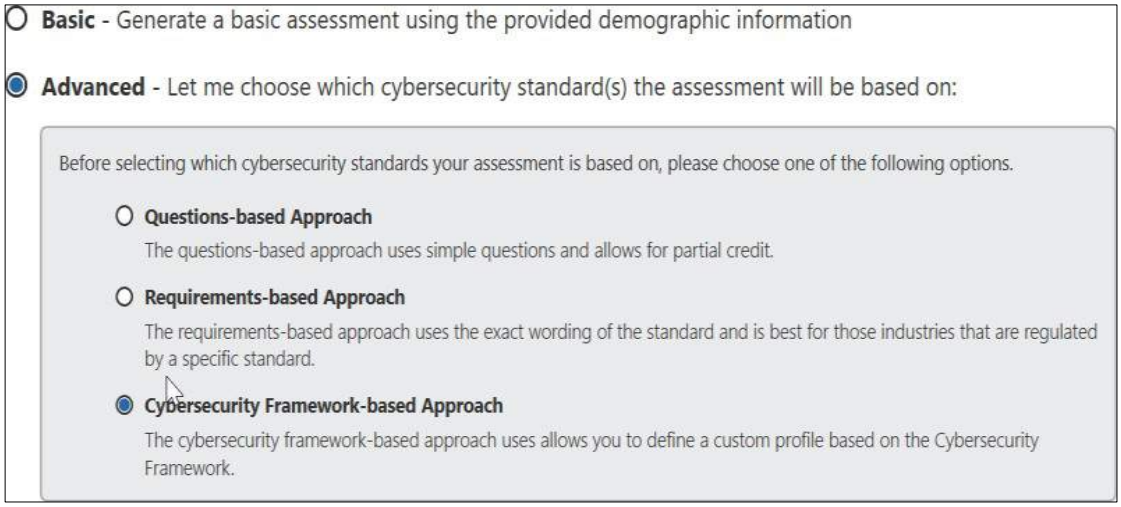


- 单击【**Continue**】（继续），进入下一步。
- 单击下拉菜单，选择合适的值。



[58] https://www.us-cert.gov/forms/csetiso.

- 单击【**Continue**】（继续），进入下一步。
- （可选）单击【**Create a network diagram**】（新建网络图），创建网络图；否则，单击【**Continue**】（继续）。
- 选择【**Advanced**】（高级）模式，再选择【**Cybersecurity Frame-based Approach**】（基于网络安全框架的方法）。



- 单击【**Continue**】（继续），使用默认 Profile 或新建 Profile。
- 单击【**Continue**】（继续）。
- 回答所有问题。
- 完成后输出最终报告。

其他信息

YouTube 的 CSET 频道提供了视频教程[59]，帮助用户快速掌握工具使用方法。

经验总结

- 工具的有效性取决于所输入的信息，回答问题之前一定要深思熟虑。
- 必要时，标记答案，以便后续跟进。
- 回答完所有问题后，系统给出评分（0~100），量化组织应对网络安全风险的准备度。

对性能的主要影响

CSET 一般独立于制造系统部署，所以没有测试其对系统性能的影响。

性能测量数据集的相关链接

无

[59] https://www.youtube.com/c/CSETCyberSecurityEvaluationTool

4.4 GRASSMARLIN

4.4.1 技术方案概述

GRASSMARLIN 是由国家安全局（NSA）开发的用于工业网络的开源、被动网络映射器。GRASSMARLIN 提供工业系统快照，包括如下信息：

- 网络设备
- 这些设备之间的通信
- 从这些通信中提取的元数据

重点说明[60]：

- 被动 IP 网络映射工具
- 不受硬件限制的基于 Java 的便携式工具
- 只能查看和映射被抓包的主机。

4.4.2 方案提供的技术能力

GRASSMARLIN 提供以下技术能力（参见第 1 卷第 6 章）：

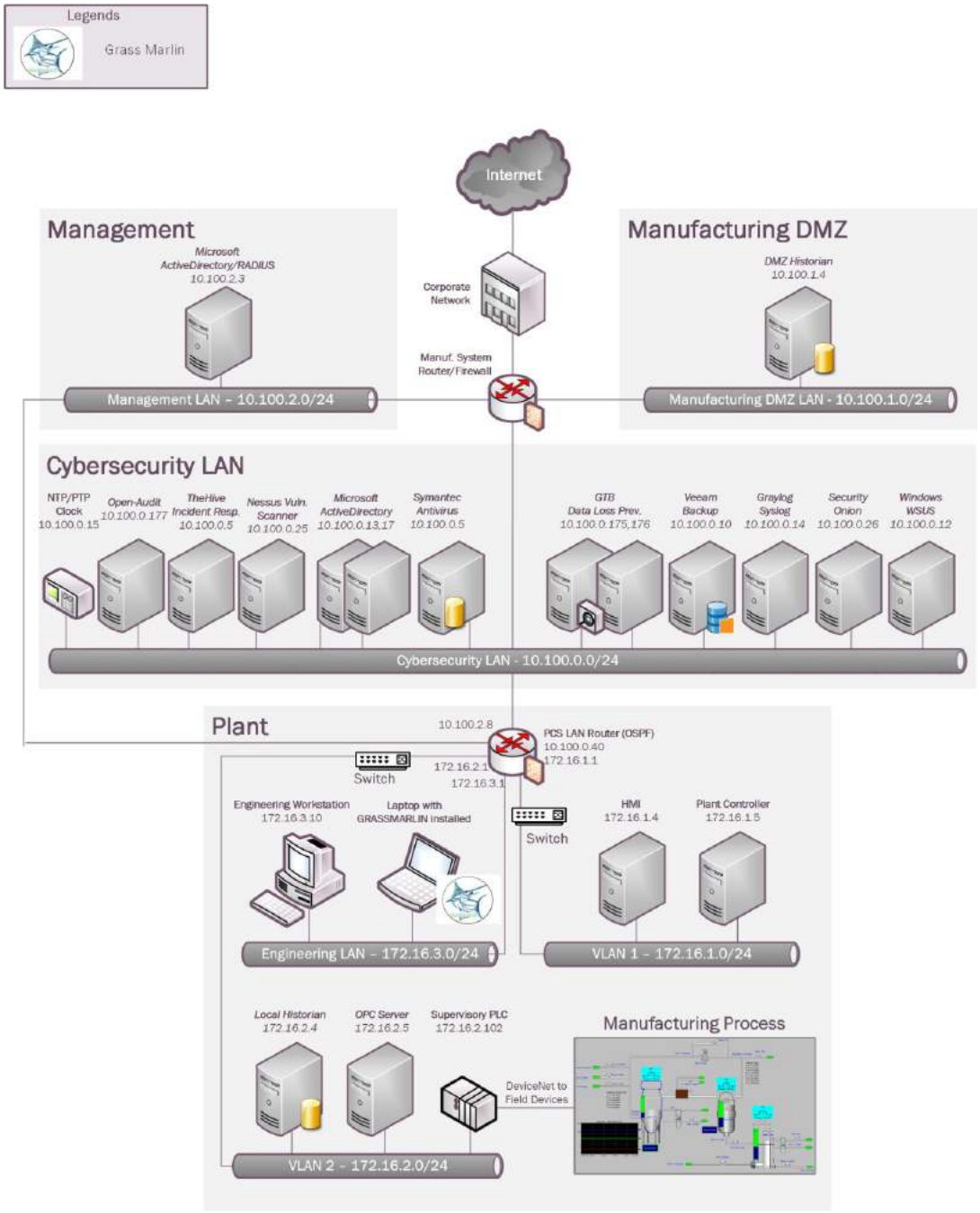
- 网络架构文档
- 建立基线
- 绘制数据流

4.4.3 方案实现的子类

ID.AM-3，ID.AM-4，PR.AC-5，PR.IP-1，DE.AE-1，DE.CM-7

[60] GRASSMARLIN Briefing PowerPoint 2017 ： https://github.com/nsacyber/GRASSMARLIN/blob/master/GRASSMARLIN_Briefing_20170210.pptx

4.4.4 案实施架构图



4.4.5 安装说明与配置

实施方案的详细信息：

方案名	版本	硬件规格
GRASSMARLIN	3.2.1	笔记本电脑规格如下： • 处理器：i7 • 内存：16 GB • 磁盘：256 GB • 操作系统：Windows 7专业版

环境搭建

- 根据需要，在临时笔记本电脑（操作系统为 Windows）上安装 GRASSMARLIN，接入工厂网络。

安装

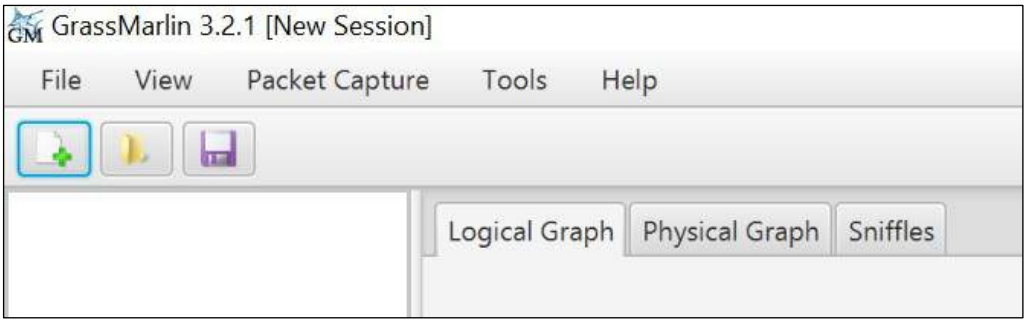
- 下载 GRASSMARLIN[61]。
- 运行安装程序。安装程序将在安装过程中安装其他程序，如 Java 和 Wireshark。

使用软件

GRASSMARLIN 以实时被动模式运行，嗅探实时流量，记录并导入 PCAP 文件。GRASSMARLIN 中的数据存储在会话中，其中包含导入的文件和可视状态信息。

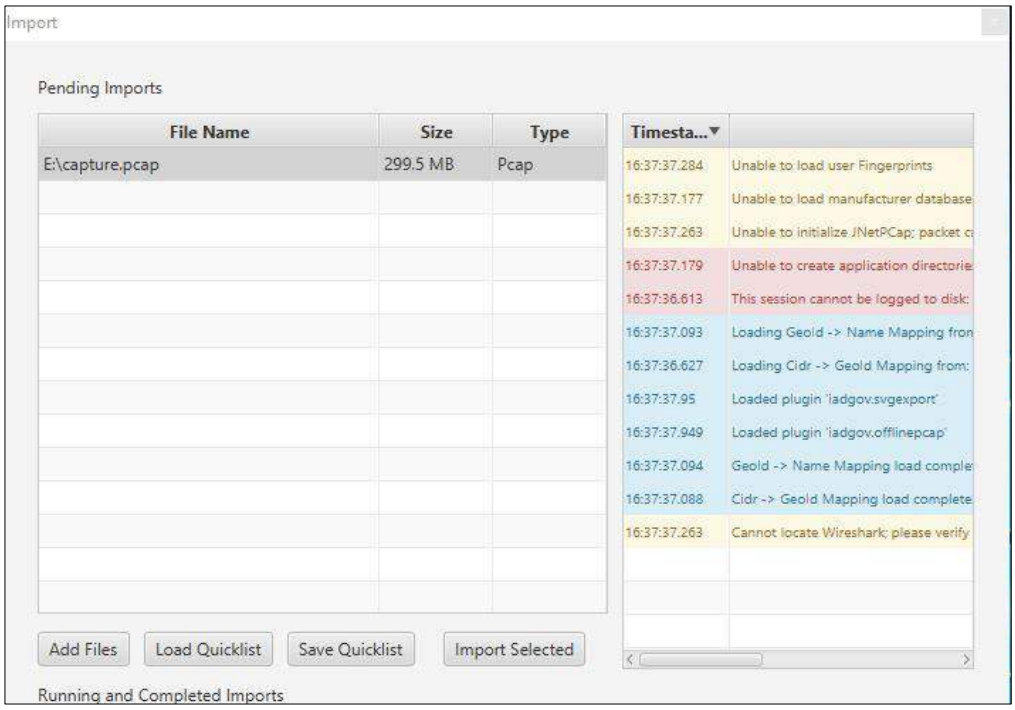
- 在 Linux 系统中，抓包并保存 PCAP 文件：
  - 安装 tcpdump（若当前系统无此工具）。
  - 运行 **tcpdump -i <mirror-port interface> - w mypcap.pcap** 命令。

    例如：tcpdump -i eth1 -w /home/icssec/pcs.pcap
  - 其中，eth1 指 SPAN/镜像端口连接。
- 双击【**程序**】菜单中的程序图标，在 Windows 系统上运行 GRASSMARLIN。在 Linux 系统上，运行 **sudo grassmarlin** 命令启动安装程序。
- 在 GRASSMARLIN 中导入 PCAP，如下所示：
  - 单击工具栏中的“导入”图标（或选择 **File > Import files**（文件 > 导入文件））。

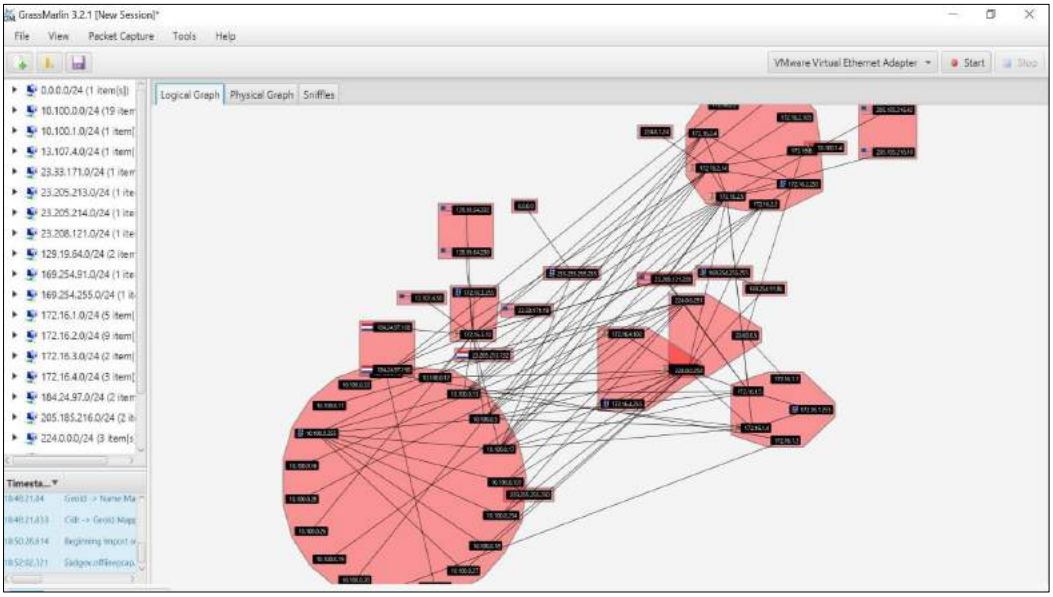


- 单击【**Add Files**】（添加文件），找到 PCAP 文件，确定后，该文件出现在 Pending Imports（待导入）列表中。
- 选中目标文件，单击【**Import Selected**】（导入选中文件）。完后成，单击【**Close**】（关闭）按钮，回到主界面。根据 PCAP 文件大小，导入时长可持续数分钟到数小时不等。

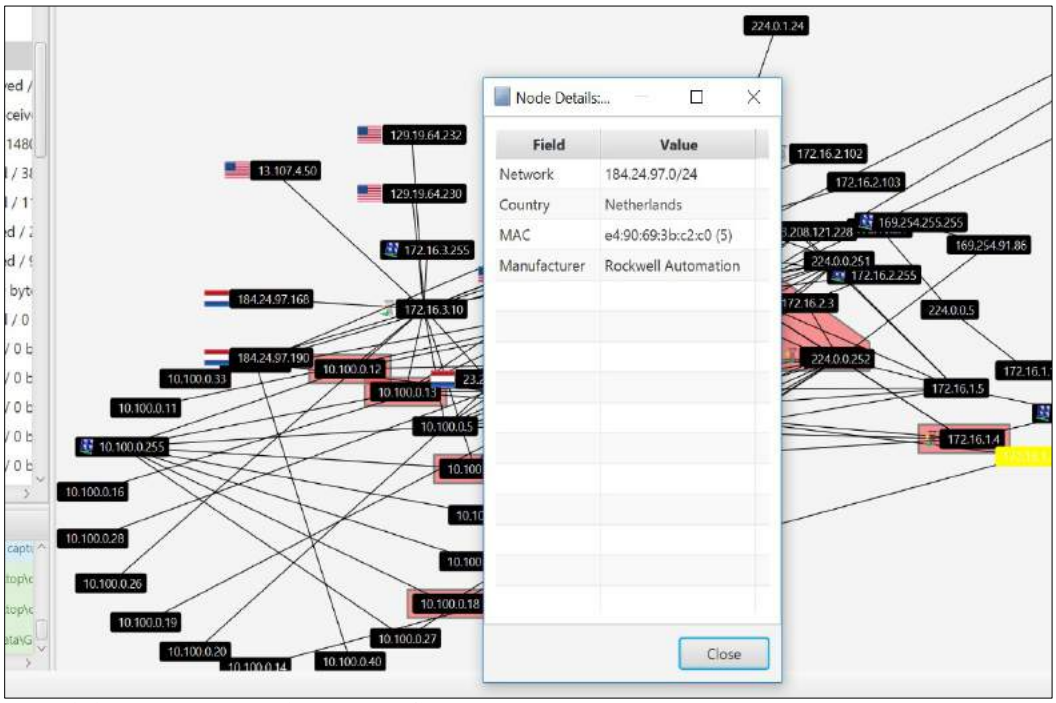
61 https://github.com/nsacyber/GRASSMARLIN/releases



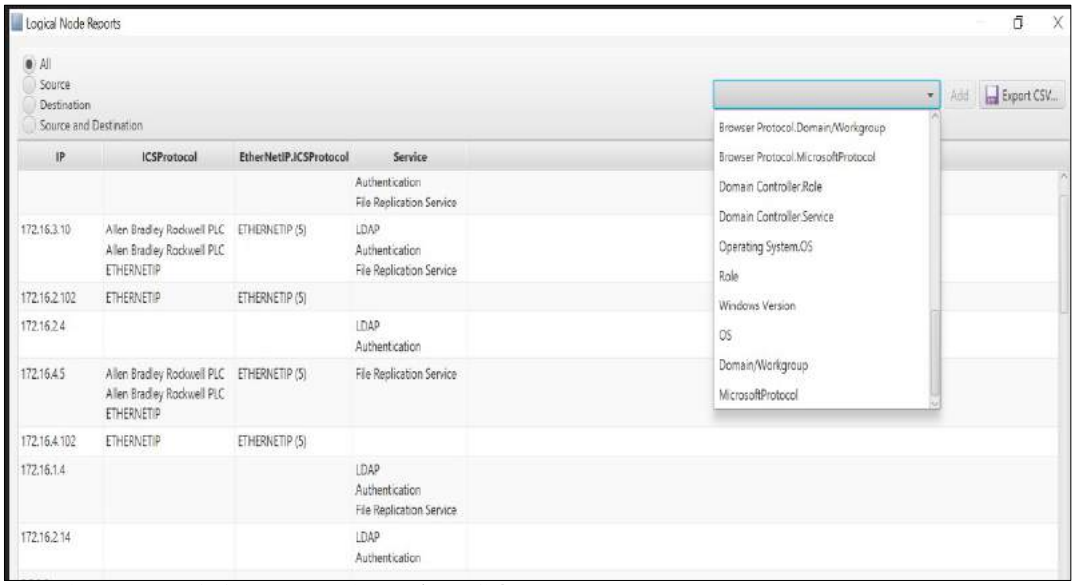
导入完成后，主屏幕将显示网络拓扑逻辑图，如下所示。



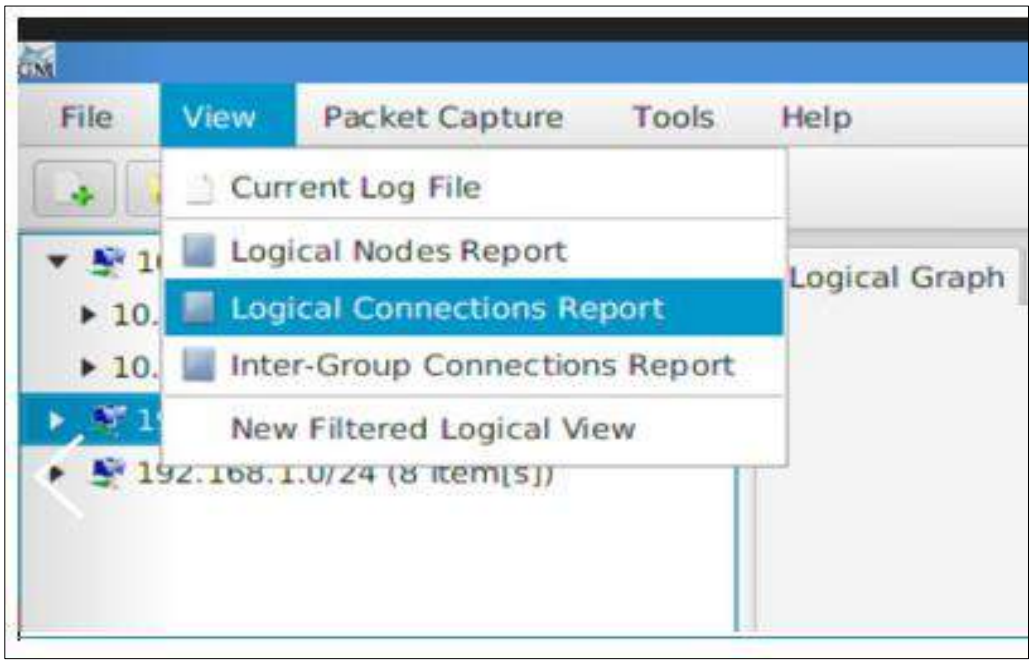
- 查看逻辑图。所有公网 IP 地址以对应国家国旗突出显示，这样可以快速发现本公司的网络正在与哪些外部 IP 通信。
- 右键单击外部 IP 地址，选择【**View Details**】（查看详细信息）。例如，172.16.3.10 主机与来自荷兰的 IP 地址通信，如下图所示。



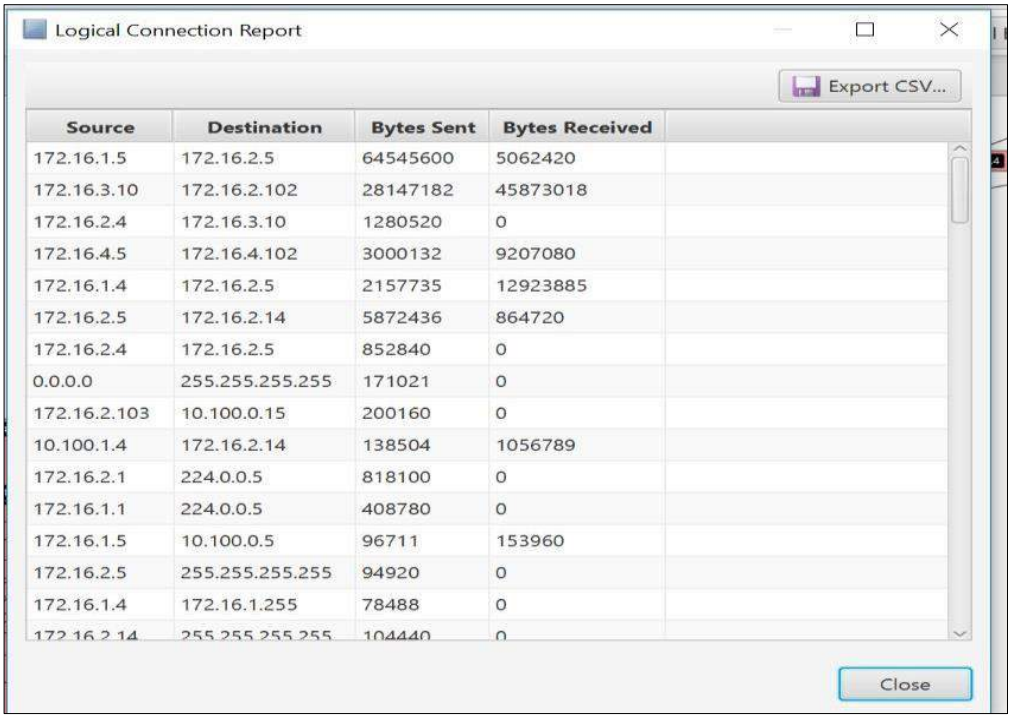
- 为逻辑图中的所有节点生成列表：
  - 选择 **View** (主菜单) > **Logical Nodes Report**（查看>逻辑节点报表）。默认情况下，只展示 IP 地址，但可以通过选择节点属性添加其他列。
  - 从下拉列表中选择属性，单击【**Add**】（添加）按钮，在报表中添加新列。



- 为 PCAP 文件中的所有连接生成报表：
  - 选择 **View** (主菜单) > **Logical Connections Report**（查看 > 逻辑连接报表）。



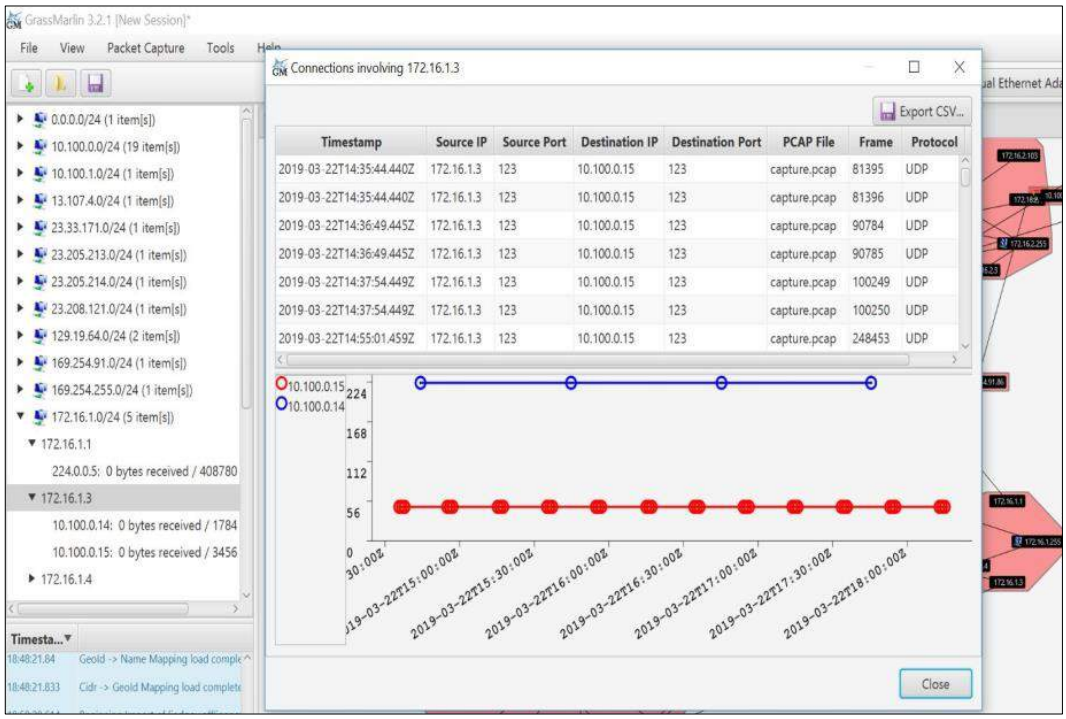
- 单击【**Export CSV**】（导出 CSV），进一步分析网络中的所有通信。输出信息如下图所示。



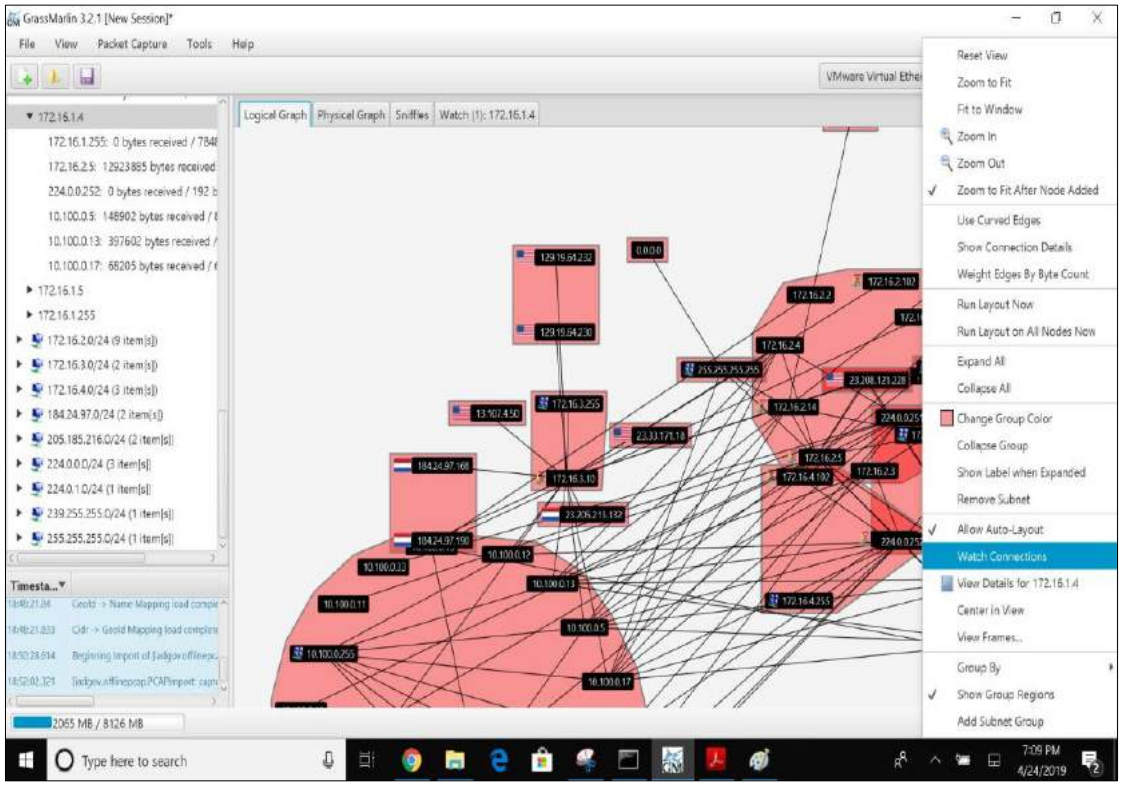
Source	Destination	Bytes Sent	Bytes Received
172.16.1.5	172.16.2.5	64545600	5062420
172.16.3.10	172.16.2.102	28147182	45873018
172.16.2.4	172.16.3.10	1280520	0
172.16.4.5	172.16.4.102	3000132	9207080
172.16.1.4	172.16.2.5	2157735	12923885
172.16.2.5	172.16.2.14	5872436	864720
172.16.2.4	172.16.2.5	852840	0
0.0.0.0	255.255.255.255	171021	0
172.16.2.103	10.100.0.15	200160	0
10.100.1.4	172.16.2.14	138504	1056789
172.16.2.1	224.0.0.5	818100	0
172.16.1.1	224.0.0.5	408780	0
172.16.1.5	10.100.0.5	96711	153960
172.16.2.5	255.255.255.255	94920	0
172.16.1.4	172.16.1.255	78488	0
172.16.2.14	255.255.255.255	104440	0

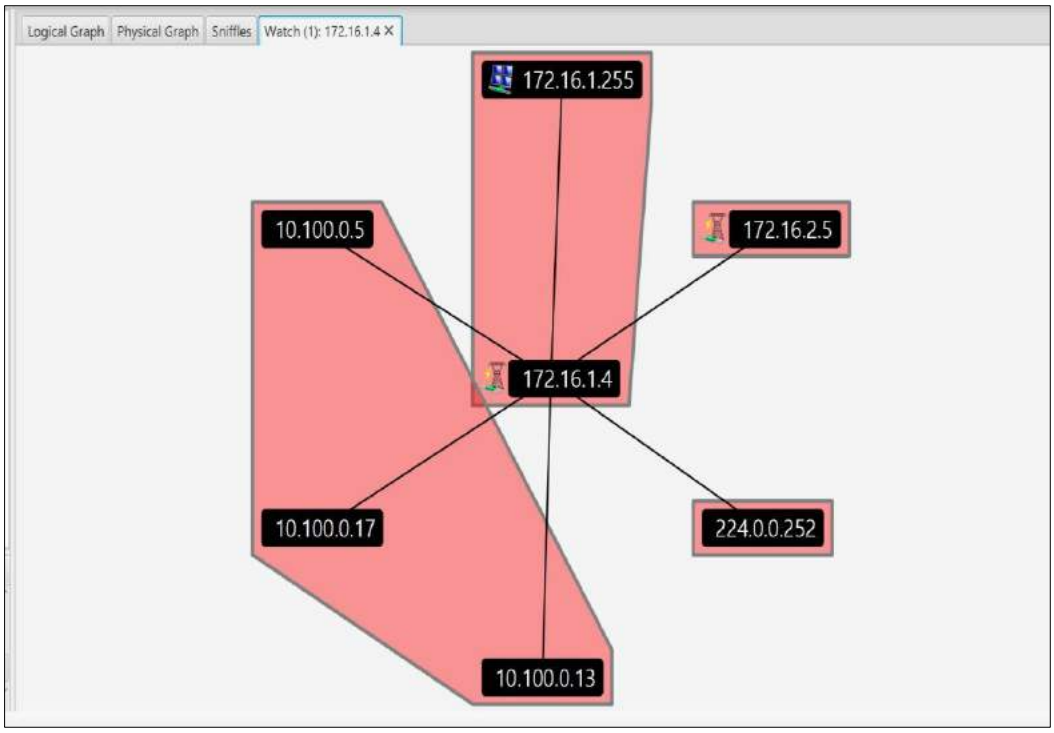
- 要获取基线，需查看特定主机的所有逻辑通信：
  - 右键单击【**Node**】（节点），选择【**View Frames**】（查看帧）。
  - 进入如下所示页面。该页面显示了正在与特定主机通信的所有 IP 地址，包括端口和协议信息。
  - 单击【**Export CSV**】（导出 CSV）按钮，导出 CSV 文件。

  说明：需针对各个节点，反复进行此过程。



- 生成监控图：
  - 右键单击某个节点，选择 **Watch Connections > Watch Connections**（查看连接）。
  - 生成监控图，显示在新窗口【**Watch <IP address>**】（监控<IP 地址>）中。





其他信息

可从网上获取 GRASSMARLIN 用户手册[62]。

对性能的主要影响

考虑到 GRASSMARLIN 的安装位置和使用方式（对其他软件抓取的 PCAP 文件进行离线分析），没有测试其对系统性能的影响。

性能测量数据集的相关链接

无

4.5 Wireshark

4.5.1 技术方案概述

Wireshark 是免费的开源报文分析程序。

4.5.2 方案提供的技术能力

Wireshark 提供以下技术能力（参见第 1 卷第 6 章）：

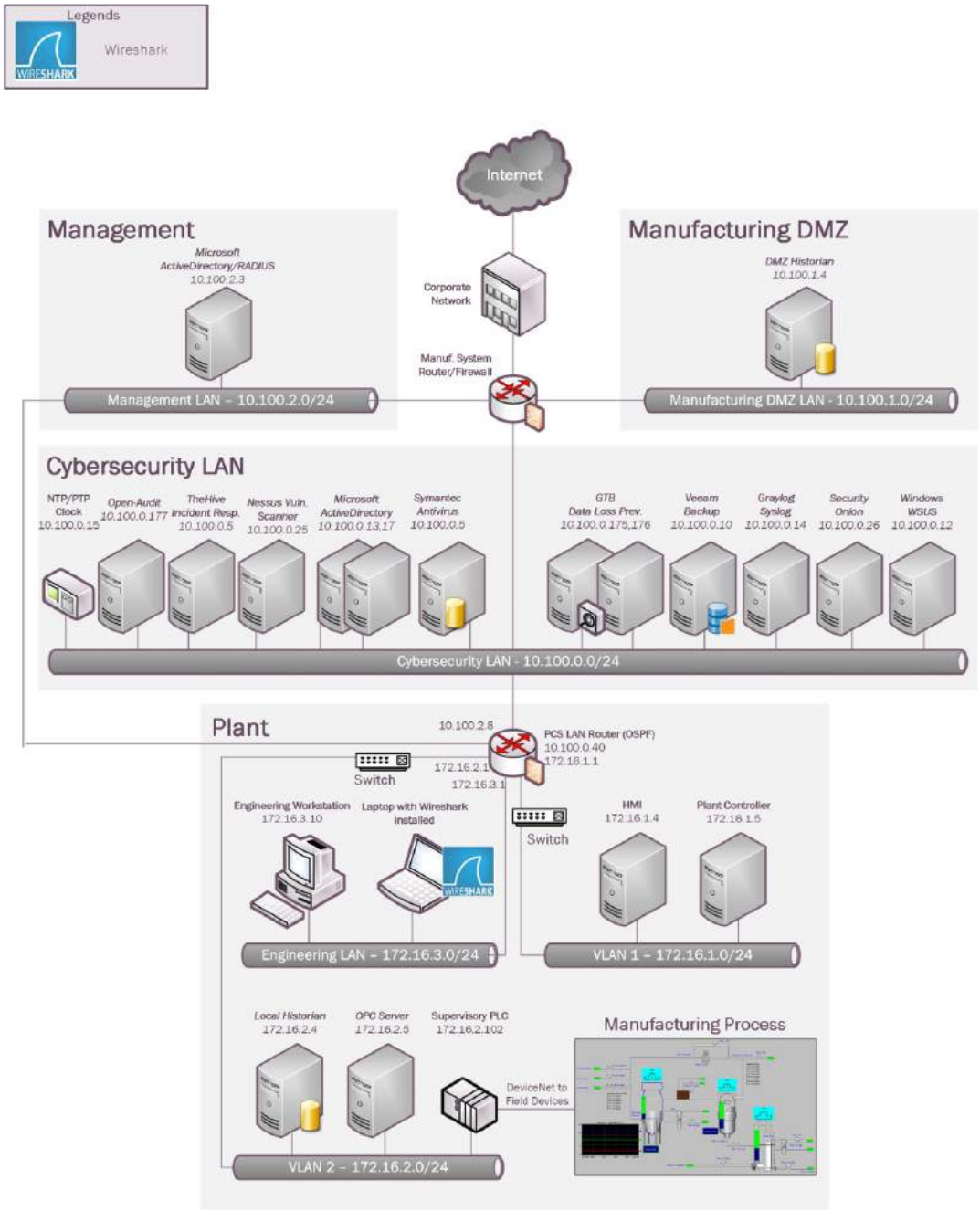
- 网络架构文档
- 建立基线
- 绘制数据流
- 取证

4.5.3 方案实现的子类

ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, DE.AE-1, DE.AE-2, DE.CM-7, RS.AN-3

62 https://github.com/nsacyber/GRASSMARLIN

4.5.4 方案实施架构图



4.5.5 安装说明与配置

实施方案的详细信息：

方案名	版本	硬件规格
Wireshark	3.0.2	笔记本电脑规格如下： • 处理器：i7 • 内存：16 GB • 磁盘：256 GB • 操作系统：Windows 7专业版

环境搭建

根据需要，在笔记本电脑（操作系统为 Windows）上安装 Wireshark。

安装

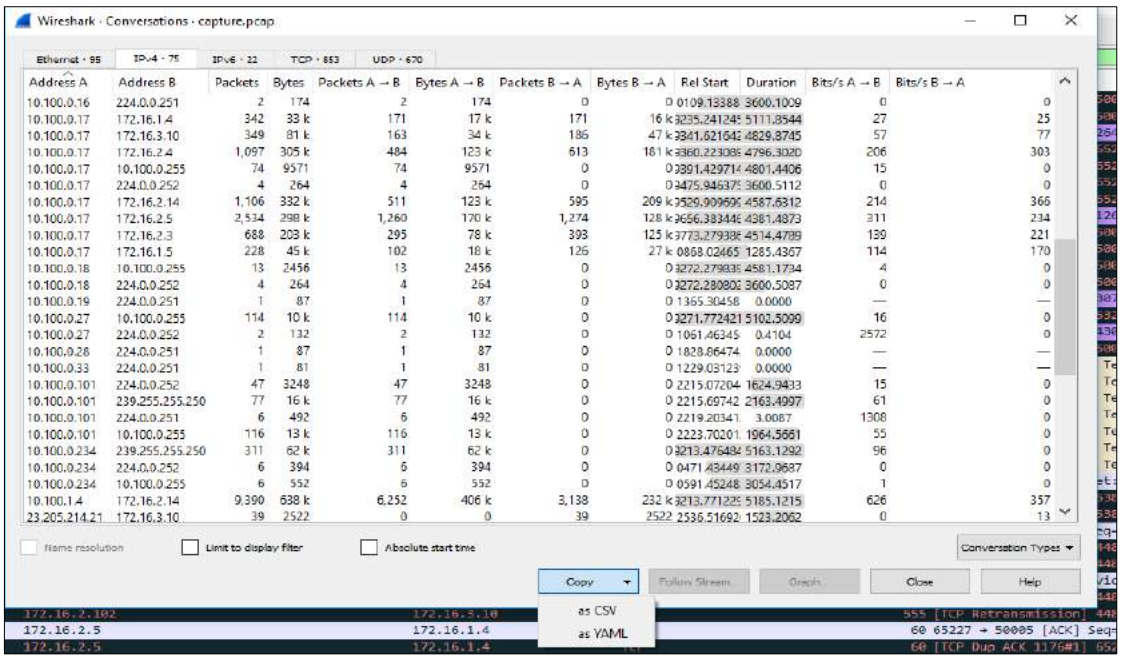
- 下载 Wireshark[63]（32 位或 64 位）。
- 运行 exe 文件，开始安装，例如，**Wireshark-win64-3.0.1.exe**。
- 单击【**Next**】（下一步），保留默认设置，继续安装。
- 提示安装 Npcap 时，单击【**I Agree**】（同意），继续安装。
- 单击【**Next and Finish**】（下一步并完成），启动程序。
- 选择【**Reboot Now**】（立刻重启）或【**I want to manually reboot later**】（稍后手动重启）。
- 单击【**Finish**】（完成），完成安装。

运行 Wireshark

- 右键单击 Wireshark 图标，选择【**Run as Administrator**】（**Windows 10**）（以管理员身份运行），启动 Wireshark。Wireshark 要求管理权限完全正常，否则，结果会不尽如人意。
- 从显示的接口列表中选取抓包接口。

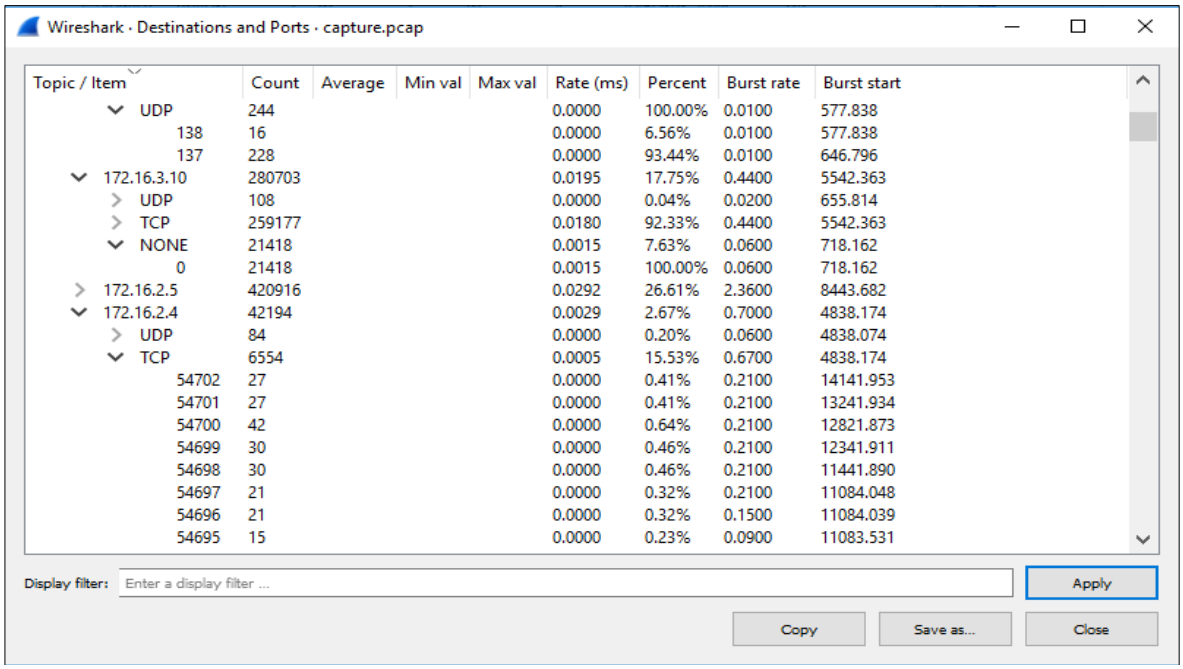
使用 Wireshark 获取网络基线数据

- 单击【**Open**】（打开），加载之前抓取的 PCAP 文件，或进行抓包。
- PCAP 文件加载完毕或完成抓包后，选择 **Statistics** > **Conversations**（统计 > 会话）。
- 单击【**Copy**】（复制）按钮，选择【**as CSV**】，导出 CSV 文件供进一步分析。如下截图仅供参考。



63 https://www.wireshark.org

- （可选）选择 **Statistics > IPv4 Statistics > Destination and Ports**（统计 > IPv4 统计 > 目标 IP 与端口），获取端口列表。这样，流量中所有 IP 地址使用的端口都会显示出来。单击【**Copy**】（复制），将结果复制到 Word 文档，或单击【**Save as**】（另存），另存为纯文本文件。完成后，单击【**Close**】（关闭）。



4.5.6 对性能的主要影响

在下面的实验中，我们测量了制造系统正常运行时 Wireshark 工具对系统性能的影响：

实验 L015.2 – Wireshark

根据观察，用 Wireshark 抓取网络流量对计算资源性能有显著影响，主机的处理器和内存使用率均明显高于正常值。不过，并未发现抓包对生产过程有任何性能方面的影响。

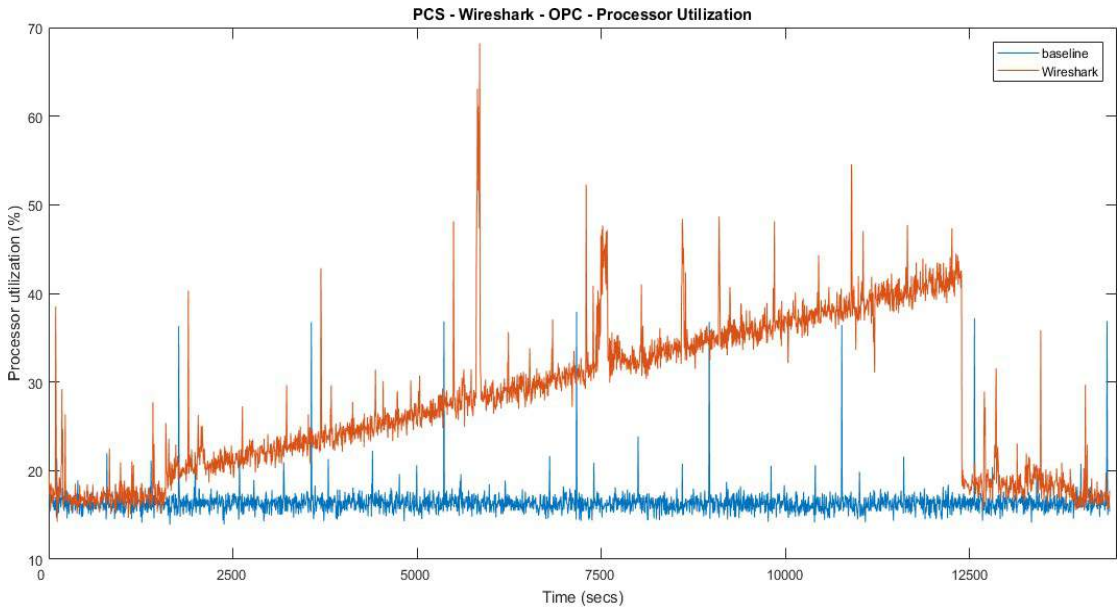


图 4-5 Wireshark 抓包时 OPC 计算机的处理器使用率

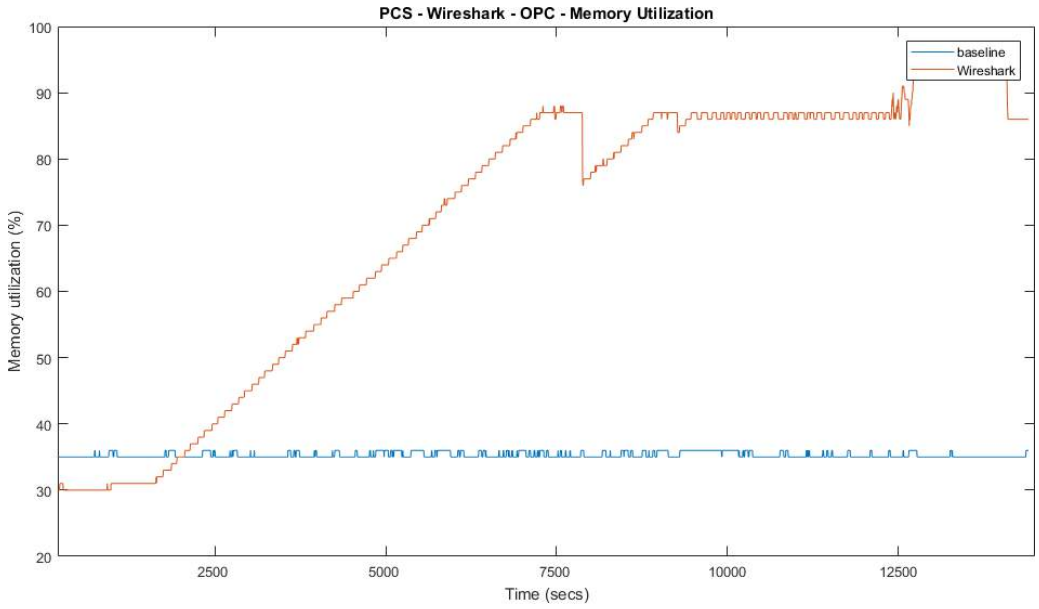


图 4-6 Wireshark 抓包时 OPC 计算机的内存使用率

从实验时间看，Wireshark 从大约 1900 秒处开始捕获网络流量，持续了大约 3 个小时。在此期间，OPC 计算机的处理器使用率不断升高。Wireshark 对处理器使用率的影响相当大。本实验中，Wireshark 数据文件大约为 2.3 GB。

对内存使用率的影响与对处理器使用率的影响类似，区别是 Wireshark 停止抓包后内存使用率仍然很高。我们猜测，在将抓取的数据保存到硬驱之前，Wireshark 将这些数据存储在内存中。因此，即使在 Wireshark 停止抓包后，内存使用率仍然很高。尽管处理器和内存使用率大幅提高，但仍未超过计算机的最大处理能力，因此对生产过程没有太大影响。不过，若制造系统正常运行需要占用大量资源，使用 Wireshark 可能会影响系统性能。

由于这个原因，PCS 系统将 Wireshark 安装在外部计算机上进行抓包。在生产系统上使用 Wireshark 时应谨慎。

4.5.7 性能测量数据集的相关链接

- Wireshark KPI 数据
- Wireshark 测量数据

4.6 Veeam 备份与复制

4.6.1 技术方案概述

Veeam 备份与复制[64]是 Veeam 为虚拟环境独立开发的备份和系统恢复软件。它基于 VMware vSphere 和 Microsoft Hyper-V 监控程序，提供备份、还原和复制功能。

Veeam 还提供 Windows 平台 Veeam 代理（Veeam agent for Windows）和 Linux 平台 Veeam 代理（Veeam agent for Linux）等产品，分别用于备份物理 Windows 和 Linux 服务器。

重点说明：

64 https://www.veeam.com/vm-backup-recovery-replication-software.html

- 有免费的虚拟和物理服务器备份版本；
- 支持文件级备份以及系统映像备份；
- 无需关闭系统即可进行备份，这对于制造环境至关重要；
- 为免费版用户提供技术支持。
- 易于安装使用。

4.6.2 方案提供的技术能力

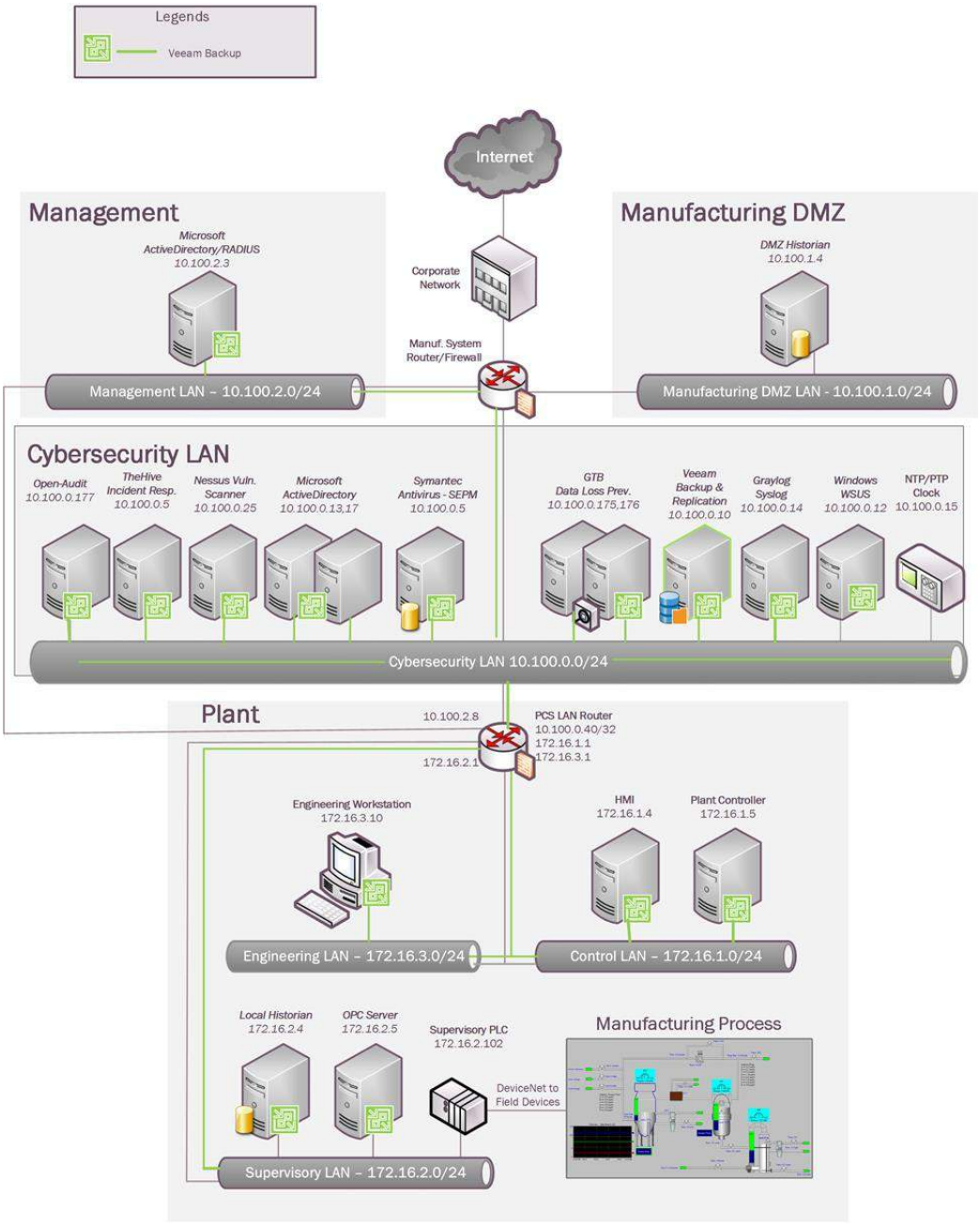
Veeam 备份与复制提供以下技术能力（参见第 1 卷第 6 章）：

- 数据备份
- 数据复制

4.6.3 方案实现的子类

PR.IP-4

4.6.4 方案实施架构图



4.6.5 安装说明与配置

实施方案的详细信息：

方案名	版本	硬件规格
Veeam备份与复制	9.5	VMware虚拟机： • 处理器：虚拟双核 • 内存：8 GB • 磁盘空间：4 TB • 网络：1个接口 • 操作系统：Windows 2012R2
Windows平台Veeam代理（免费版）	3.0.0.748	安装在工厂的所有物理设备（Windows计算机）上

环境搭建

- 准备虚拟机，操作系统为 Windows 2012 R2，硬件规格如上表所述。
- 客户机操作系统的 IP 信息如下：

  - IP 地址：10.100.0.10

  - 网关：10.100.0.1

  - 子网掩码：255.255.255.0

  - 域名服务器：10.100.0.17
- 在服务器上创建**备份**网络共享。在此文件夹中，根据要备份的各系统的主机名创建不同的子文件夹。接下来，将各系统备份通过 UNC 路径保存到 Veeam 服务器上具有对应名称的文件夹中。
- 在活动目录中创建用户帐号 **veeampuser**，为其分配上述备份共享的读/写权限。

初始配置

- 下载 Veeam 备份与复制[65]。
- 安装产品指南中提到的必备组件。运行安装程序，按照屏幕提示完成安装[66]。
- 在 Veeam 服务器上创建网络共享文件夹，用于存储所有备份。
- 在活动目录中创建服务帐号，为其分配网络共享文件夹的读/写权限。

利用免费版 Veeam 备份与复制，用户可通过中央 Veeam 备份与复制控制台管理虚拟机备份。但是，使用免费版 Windows 平台 Veeam 代理的物理服务器不能通过中央控制台进行管理，只能通过自己的客户端系统本地管理。

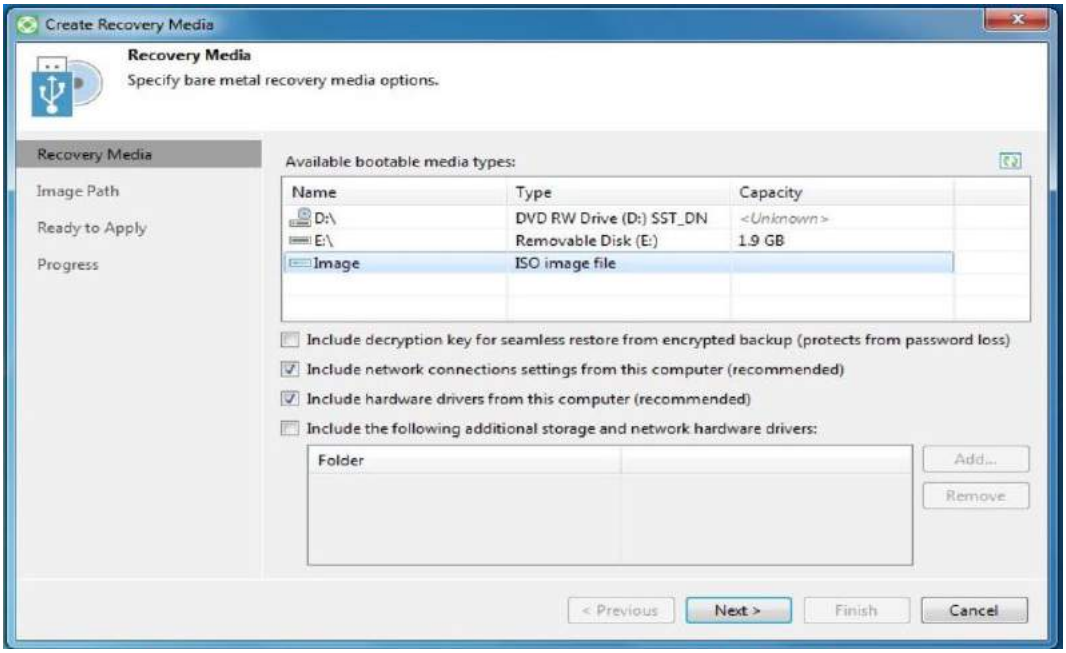
备份操作

使用 Windows 平台 Veeam 代理对工厂网络中的所有 Windows 系统进行备份[67]。在所有 Windows 物理客户端上已提前安装好代理。从各客户端访问之前创建的共享文件夹，查看其中的备份，验证客户端和 Veeam 服务器之间是否正常连接。

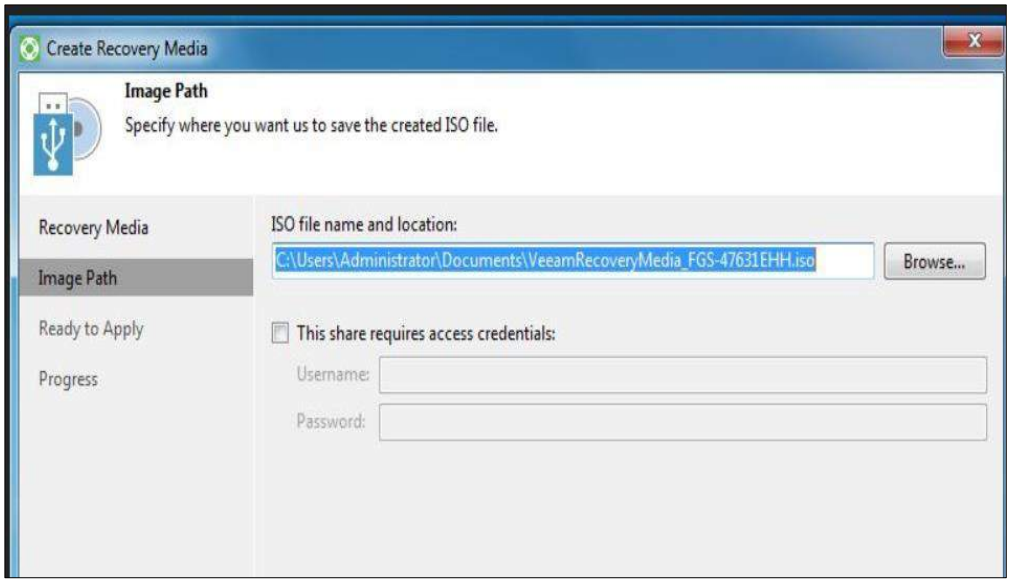
---

65 https://www.veeam.com
66 https://helpcenter.veeam.com/docs/backup/hyperv/install_vbr.html?ver=95u4
67 https://www.veeam.com/windows-endpoint-server-backup-free.html

- 根据需要，在 Windows 系统物理机上下载并安装 Windows 平台 Veeam 代理。免费版代理需要从客户端系统启动备份或还原操作。
- 双击系统托盘中的 Veeam 备份图标，启动向导。
- 按如下步骤创建 **Recovery Media**（恢复媒体）：
  - 在安装过程中按照屏幕提示创建恢复媒体；或
  - 在 **C:\Program Files\Veeam\Endpoint Backup** 目录下运行 **Veeam.Endpoint.RecoveryMedia.exe** 程序，手动创建恢复媒体。
  - 在【**Available Bootable Media Types**】（可用可引导媒体类型）下选择【**ISO**】。



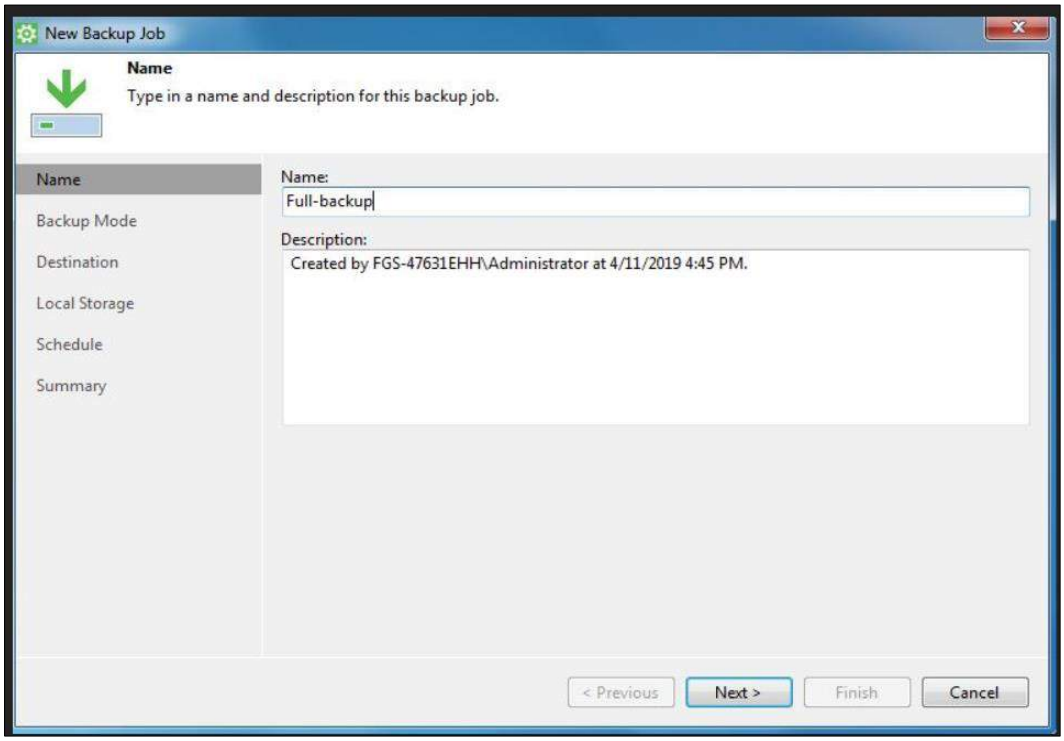
  - 输入名称和位置，保存 ISO。



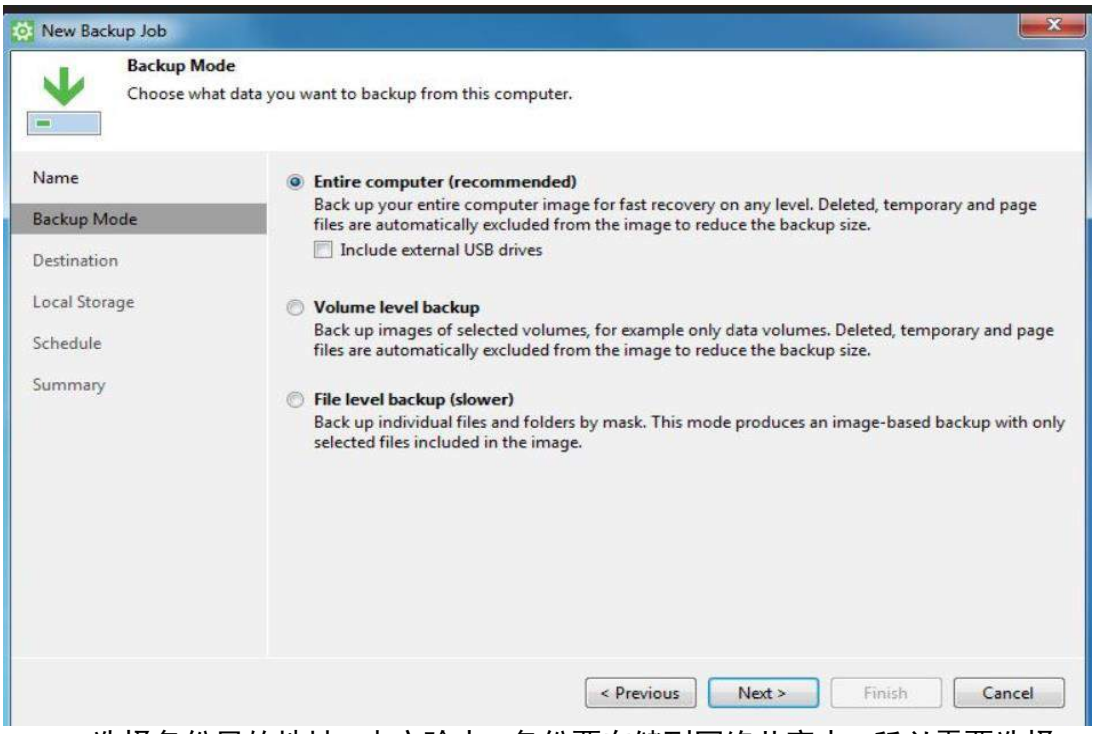
  - 涉及计算机映像完整备份或卷级备份的恢复操作必须使用此恢复媒体。
- 对**整个计算机**进行备份（系统映像）：

- 右键单击 Veeam 托盘，选择 **Control Panel > Backup > Add New Job**（控制面板 > 备份 >新建任务）。

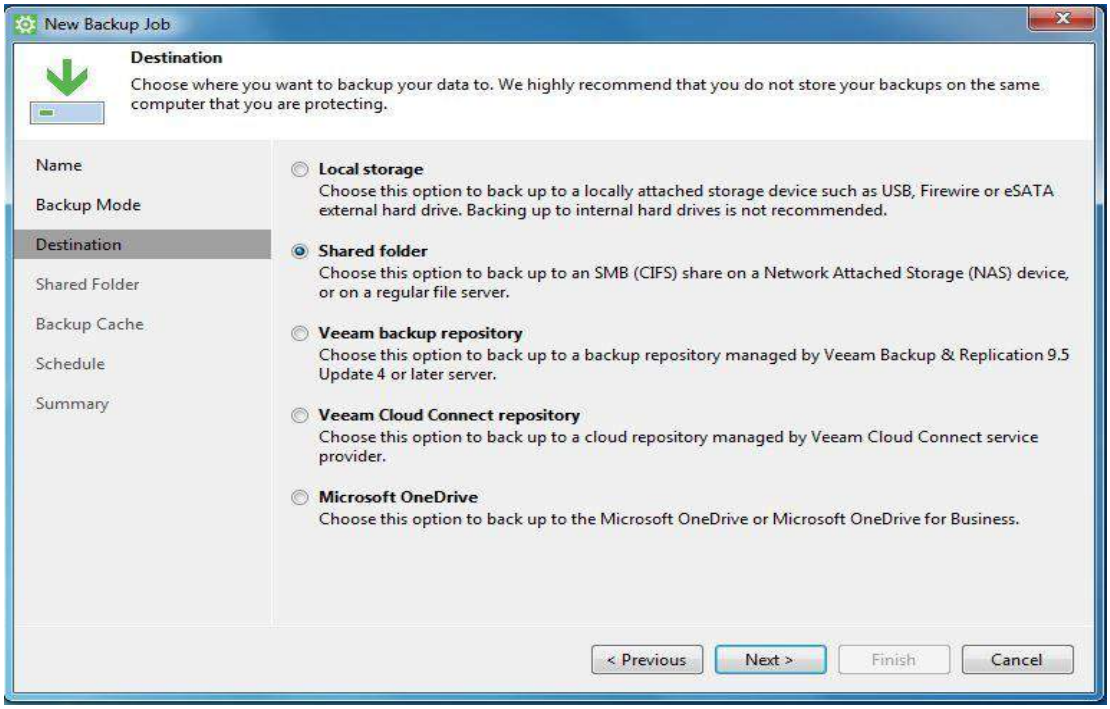
- 输入备份任务名。



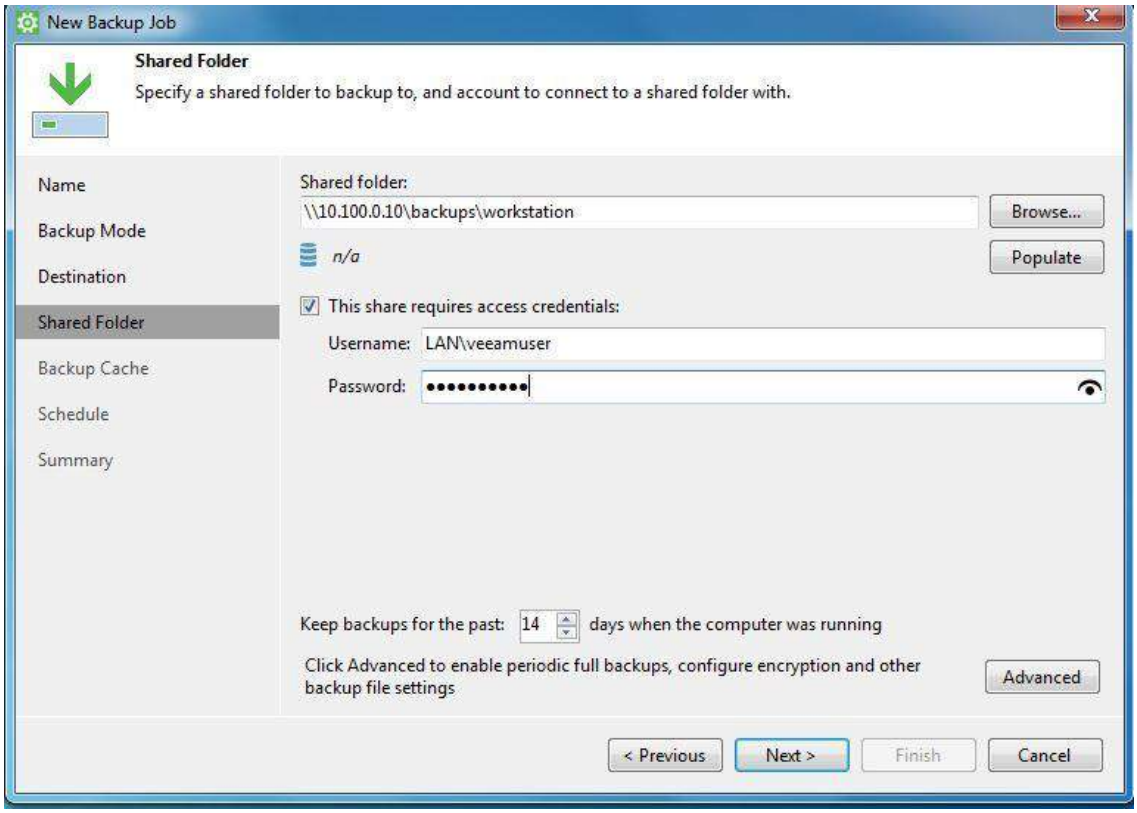
- **【Backup Mode】**（备份模式）选择**【Entire Computer】**（整个计算机）。



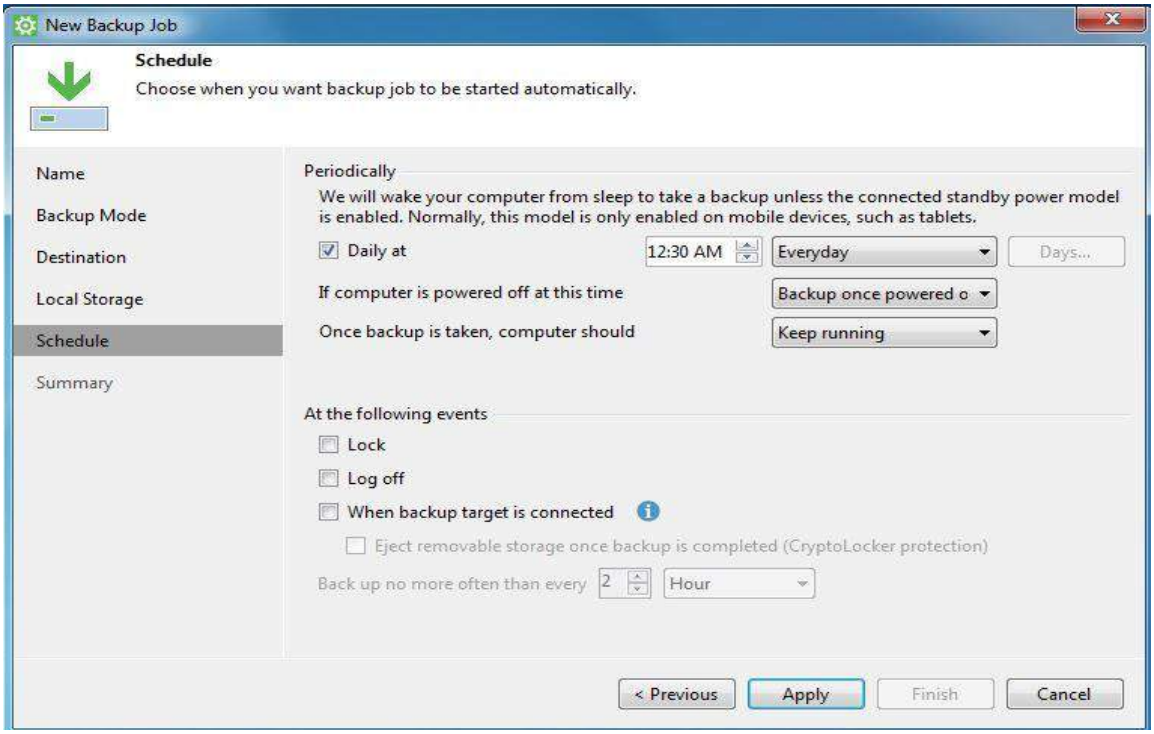
- 选择备份目的地址。本实验中，备份要存储到网络共享中，所以需要选择**【Shared folder】**（共享文件夹）。



- 输入网络共享路径和之前创建的活动目录用户凭证。 根据保留策略，输入还原点数量。



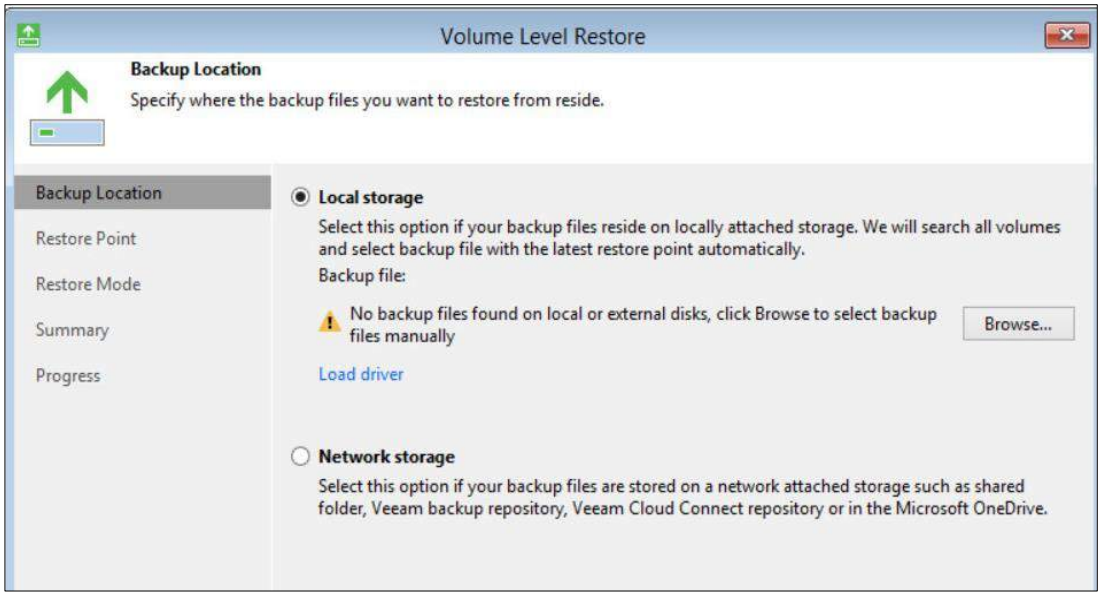
- 配置备份周期，单击【**Apply**】（应用）。



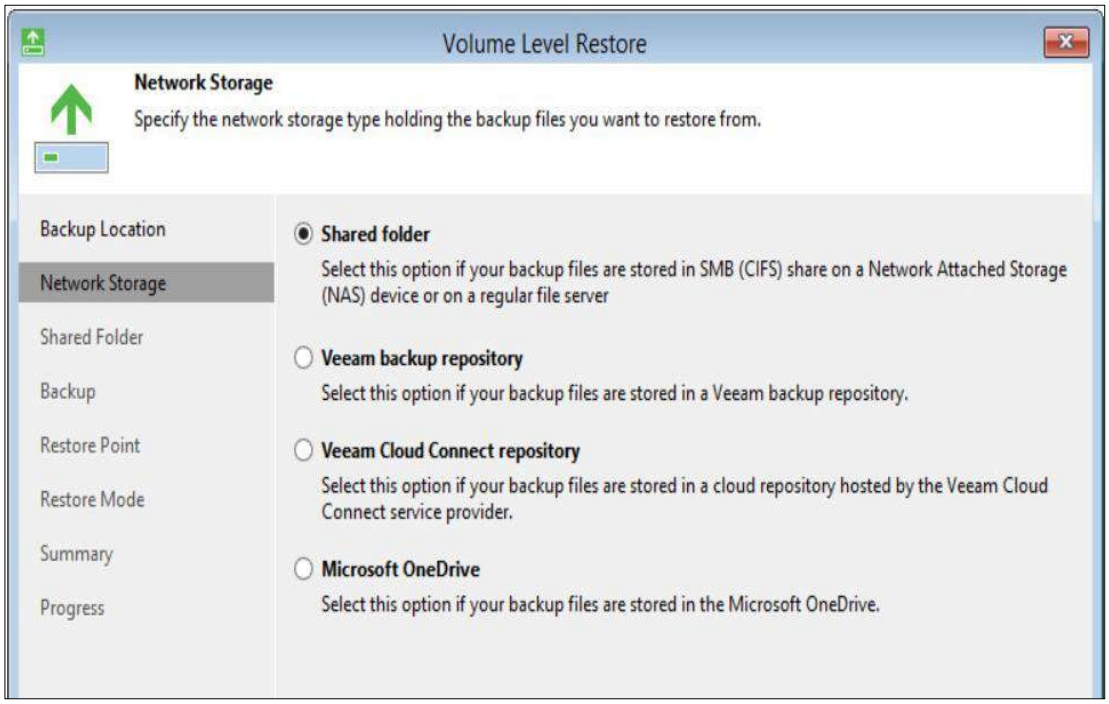
- 执行文件级备份：
  - 重复步骤 4 中各子步骤，但需要 将备份模式设置为【**File level backup (slower)**】（文件级备份（较慢））。
  - 选择要备份的目录，单击【**Next**】（下一步），完成后面各步。

恢复操作

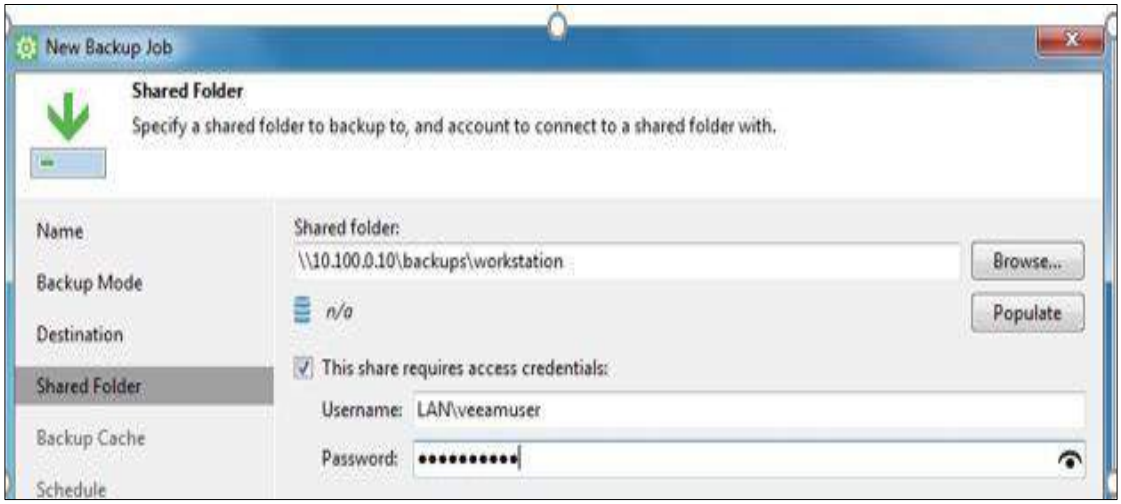
- 按照以下步骤还原单个文件：
  - 双击客户端的 Windows 平台 Veeam 客户端系统托盘，选择 **Restore > Individual Files**（恢复 > 单个文件）。
  - 在【**Backup Location**】（备份位置）页面，选择【**Network Storage**】（网络存储），单击【**Next**】（**下一步**）。
  - 【Remote Storage】（远程存储）选择【Shared folder】（共享文件夹），单击 **Next**（**下一步**）。
  - 在【Shared folder】（共享文件夹）下，输入共享文件夹的 UNC 路径和访问凭证，例如，本实验中，输入**\\10.100.0.10\backups\workstation**。
  - 在还原点步骤中，选择要从中恢复数据的还原点，单击【**Next**】（**下一步**），启动恢复。
  - 在【**Summary**】（摘要）页面，查看所执行的各步骤。
- 按照以下步骤，恢复卷或整个计算机的映像：
  - 使用先前创建的恢复媒体引导系统，单击【**Bare Metal Recovery**】（裸机恢复）。
  - 如果从外部 USB 驱动还原备份，请选择【**Local Storage**】（本地存储）；如果从网络共享还原（如本例所示），请选择【**Network Storage**】（网络存储）。



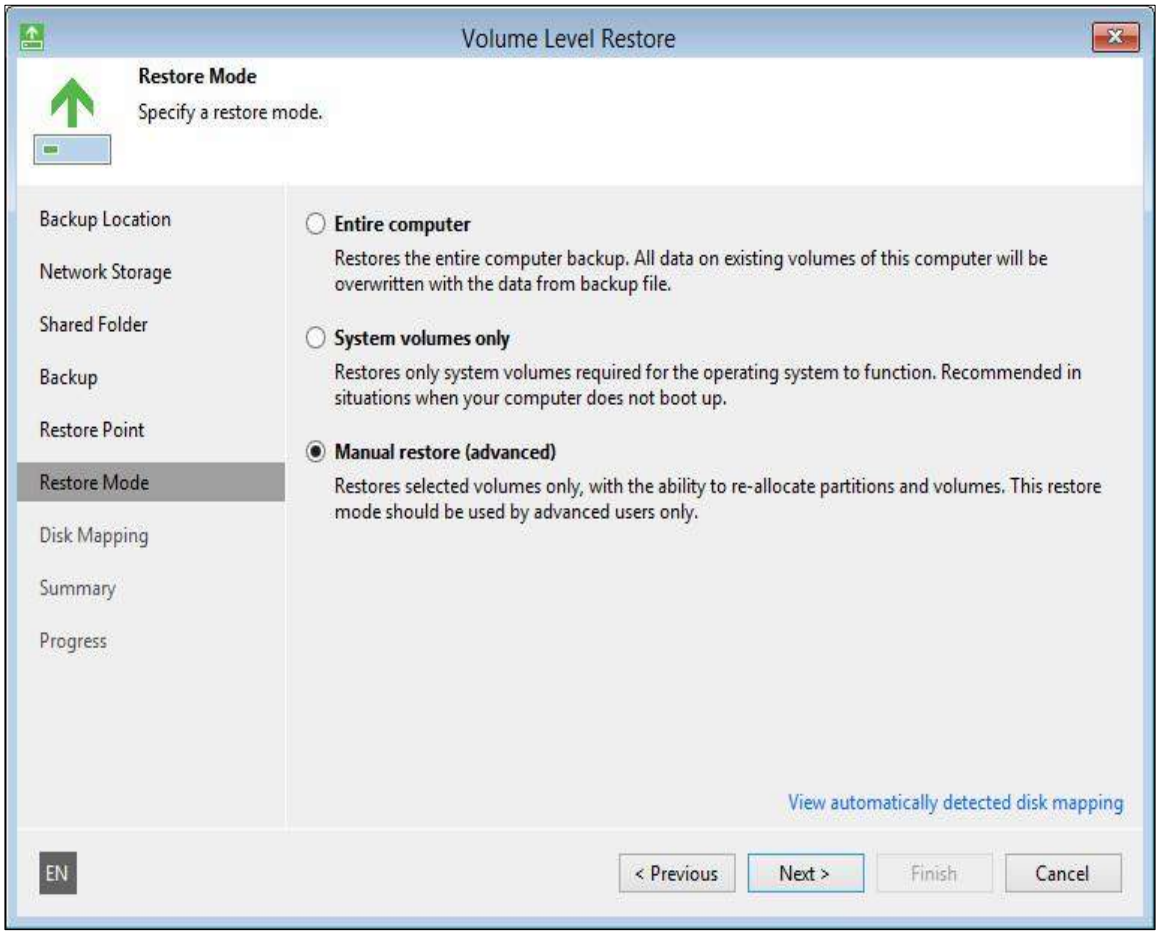
- 配置网络，选择 DHCP 或静态 IP，单击【**Continue**】（继续）。
- 在【**Network Storage**】（网络存储）页面，选择【**Share folder**】（共享文件夹），单击【**Next**】（下一步）。



- 输入 UNC 路径和要恢复的共享文件夹的访问凭证。



- 从向导所展示的备份列表中选择目标备份，单击【**Next**】（下一步）。
- 在【**Restore Points**】（还原点）下选择目标还原点，恢复数据。
- 在【**Restore Mode**】（还原模式）页面，选择还原模式。若不更改磁盘类型和系统布局，选择【**Entire computer**】（整个计算机）。高级用户会有手动恢复选项。



- 在【**Disk Mapping**】（磁盘映射）页面，根据系统布局映射已恢复驱动[68]。
- 在【**Summary**】（摘要）页面，查看摘要信息。单击【**Restore**】（恢复），启动恢复。

4.6.6 对性能的主要影响

在下面的实验中，我们测量了制造系统正常运行时 Veeam 备份工具对系统性能的影响：

- 实验 PL009.2 – Veeam 完整备份
- 实验 PL010.1 – Veeam 增量备份

根据我们的观察，工具对生产过程的性能影响很小，但是对网络流量的影响较为明显。例如，在备份期间，从控制器到 OPC 的往返时间显著增加，从 OPC 到 HMI 的路径延迟也有明显增长。备份流量会大量占用可用带宽。

此外，还有存储方面的考虑，例如 PCS 系统中的备份大小：HMI：96 GB；OPC：29 GB；控制器：31 GB；历史数据库：194 GB。

在执行完整备份时应考虑网络使用情况，在网络使用非高峰期进行备份会减少对系统的影响。Veeam 备份的一个重要特点是能够根据网络使用情况进行调整，从而避免备份流量耗尽可用带宽。

若定期执行备份，应考虑使用增量备份方法而非完整映像备份。

在完整备份期间，网络流量急剧增加，HMI 和控制器主机的备份一度占到总流量的 99.6%，而正常流量只有 0.4%。

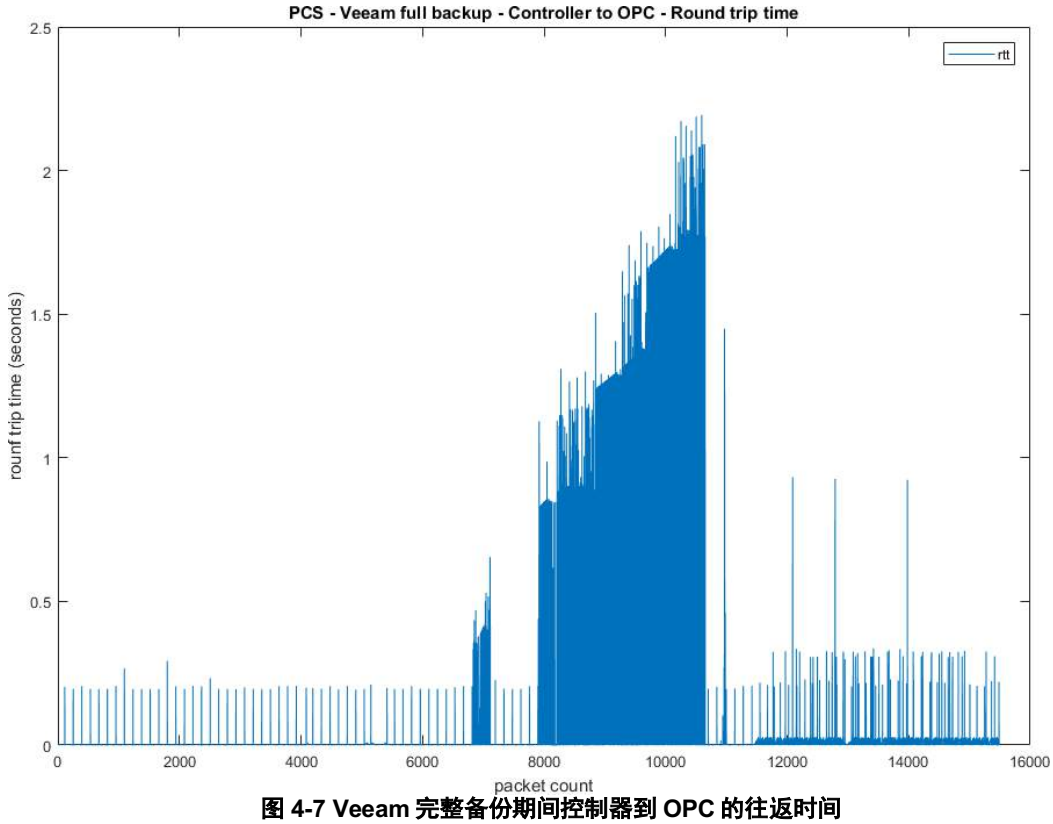


图 4-7 Veeam 完整备份期间控制器到 OPC 的往返时间

68 https://helpcenter.veeam.com/docs/agentforwindows/userguide/baremetal_disk_mapping.html?ver=30

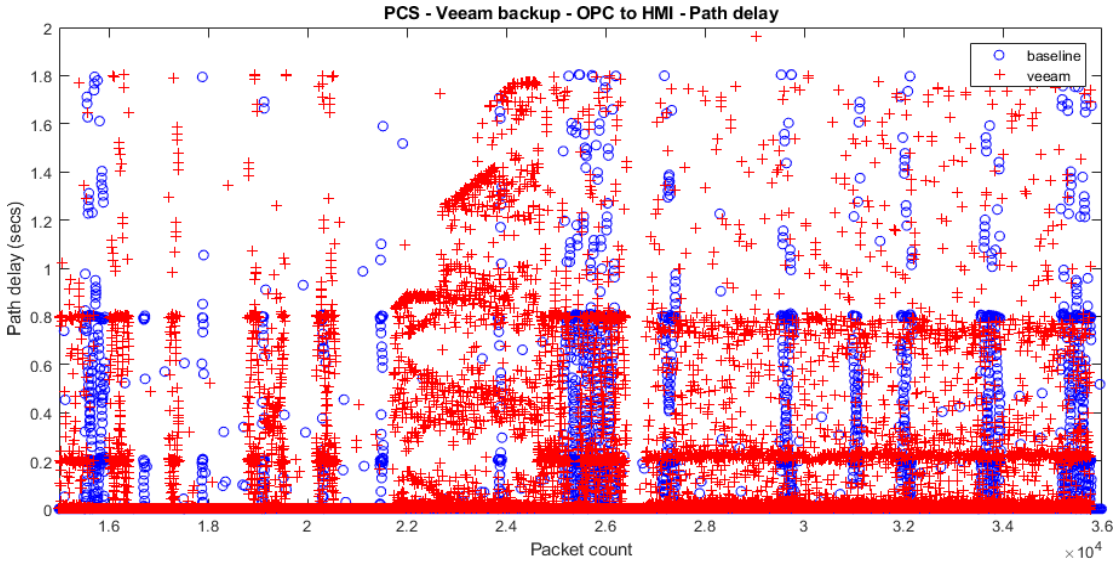


图 4-8 Veeam 完整备份期间 OPC 到 HMI 的路径延迟

应考虑增量备份。与完整备份相比，这种备份方式的网络资源占用量要低得多。增量备份期间，从控制器到 OPC 的往返时间只有些许增长。

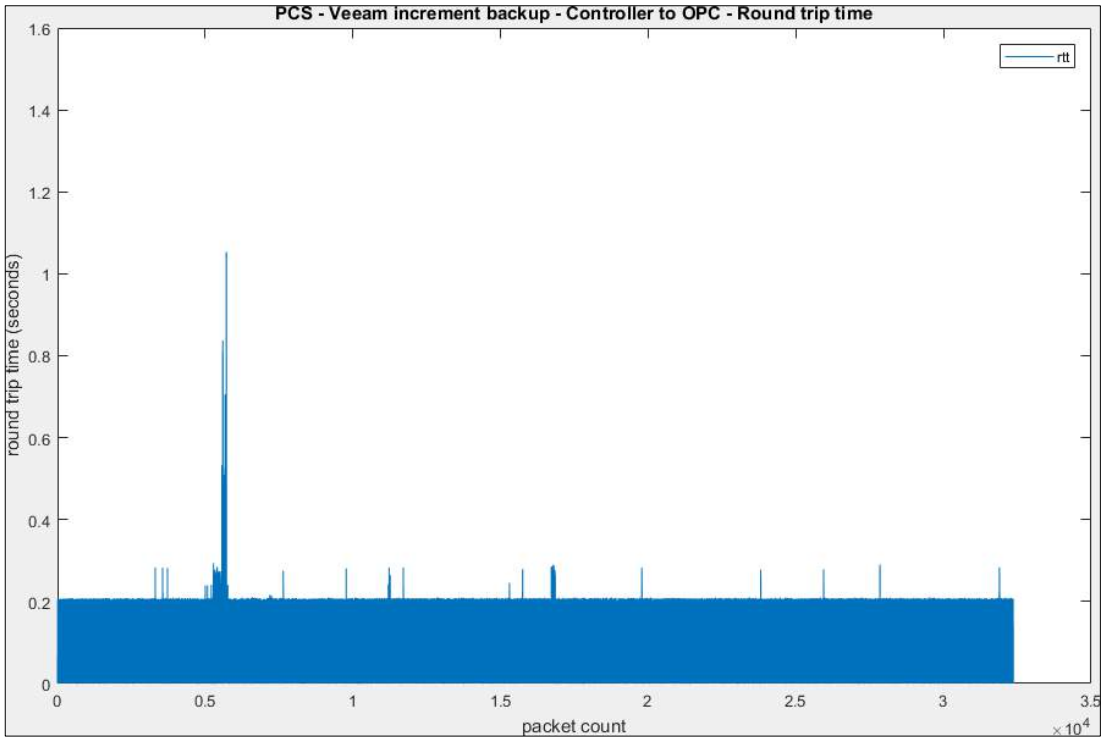


图 4-9 Veeam 增量备份期间控制器到 OPC 的往返时间

完整备份对生产过程的性能影响很小，实验中，产品流速略低，反应器压强超过正常水平。

我们猜测，网络延迟和流量的增加导致了控制器和模拟厂房之间的传感器和执行器信息交换的延迟，进而造成上述影响。因此，控制回路性能的下降对系统性能的影响不大。Veeam 备份能够根据网络状况限制备份速率，可降低完整备份对网络流量和延迟的影响。

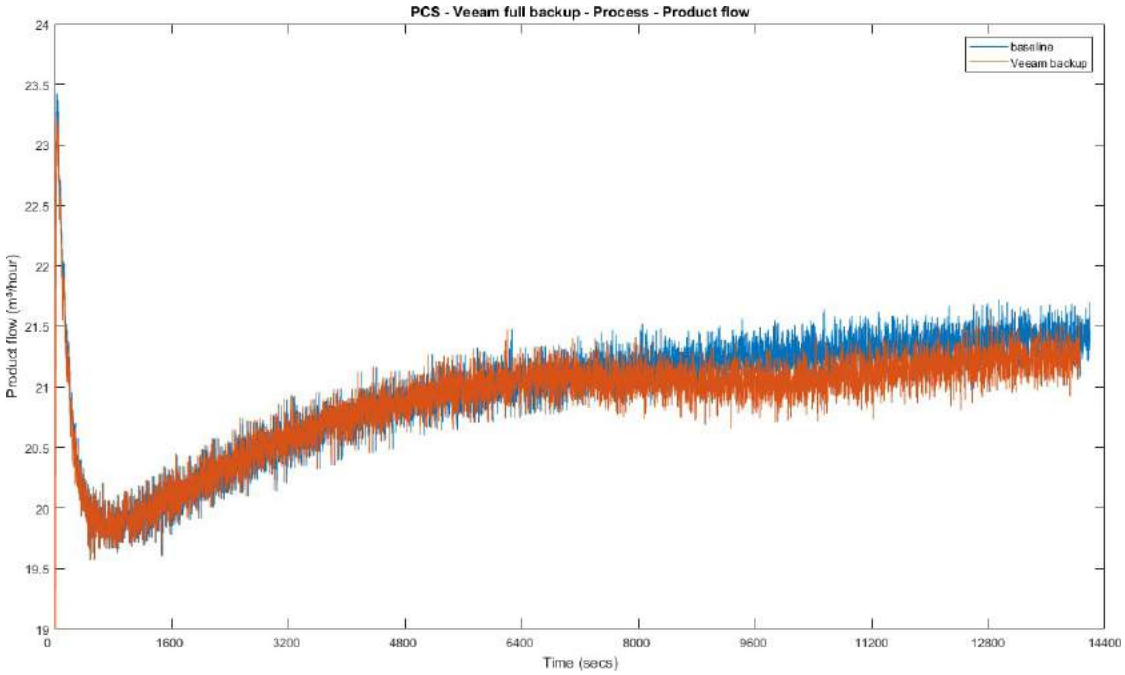


图 4-10 Veeam 完整备份期间生产过程中的产品流速

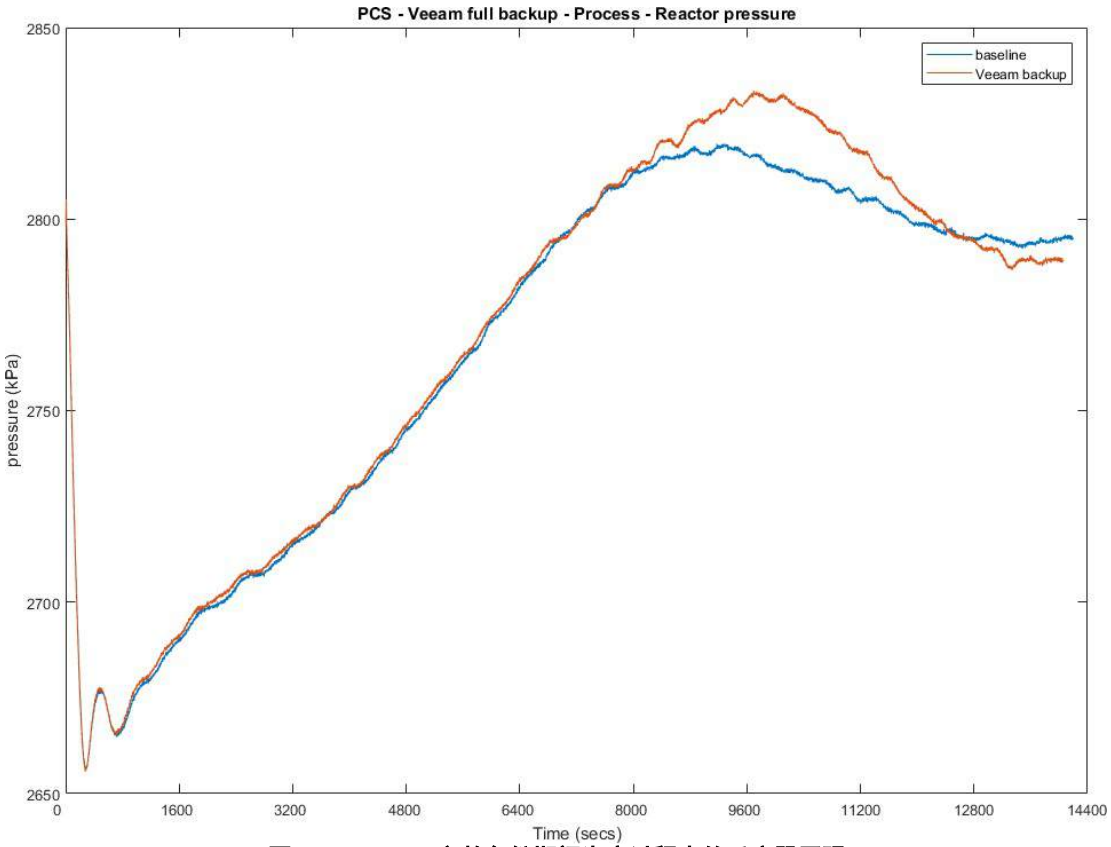


图 4-11 Veeam 完整备份期间生产过程中的反应器压强

4.6.7 性能测量数据集的相关链接

- Veeam 全量备份 KPI 数据
- Veeam 全量备份测量数据
- Veeam 增量备份 KPI 数据
- Veeam 增量备份测量数据

4.7 安全洋葱

4.7.1 技术方案概述

安全洋葱是基于 Linux 的免费开源工具，用于入侵检测、企业网络安全监控和日志管理，包括 Elasticsearch、Logstash、Kibana、Snort、Suricata、Bro、OSSEC、Sguil、Squert、NetworkMiner 等网络安全工具[69]。

安全洋葱有三个核心功能：

- 全包捕获
- 基于网络和基于主机的入侵检测系统（分别为 NIDS 和 HIDS）
- 强大的分析工具

重点说明：

- 以 ISO 形式提供的开源软件，可部署在任何类型的环境（物理或虚拟）中；
- 集多种开源工具（包括 SNORT、BRO、OSSEC SGQUIL、KIBANA、ELSA）于一身，省去了手动集成的麻烦；
- 支持单机部署，也支持大型组织的分布式部署；
- 提供前端用以访问基于命令行的 Snort 和 BRO IDS；
- 规则集可定制，具有内置的检测规则，可检测 IT 和 OT 环境中的各种网络攻击和异常；
- 关联学习曲线，熟悉 SNORT 和 BRO-IDS 规则集；
- 硬件资源密集型；
- 无报表功能。

4.7.2 方案提供的技术能力

安全洋葱提供以下技术能力（参见第 1 卷第 6 章）：

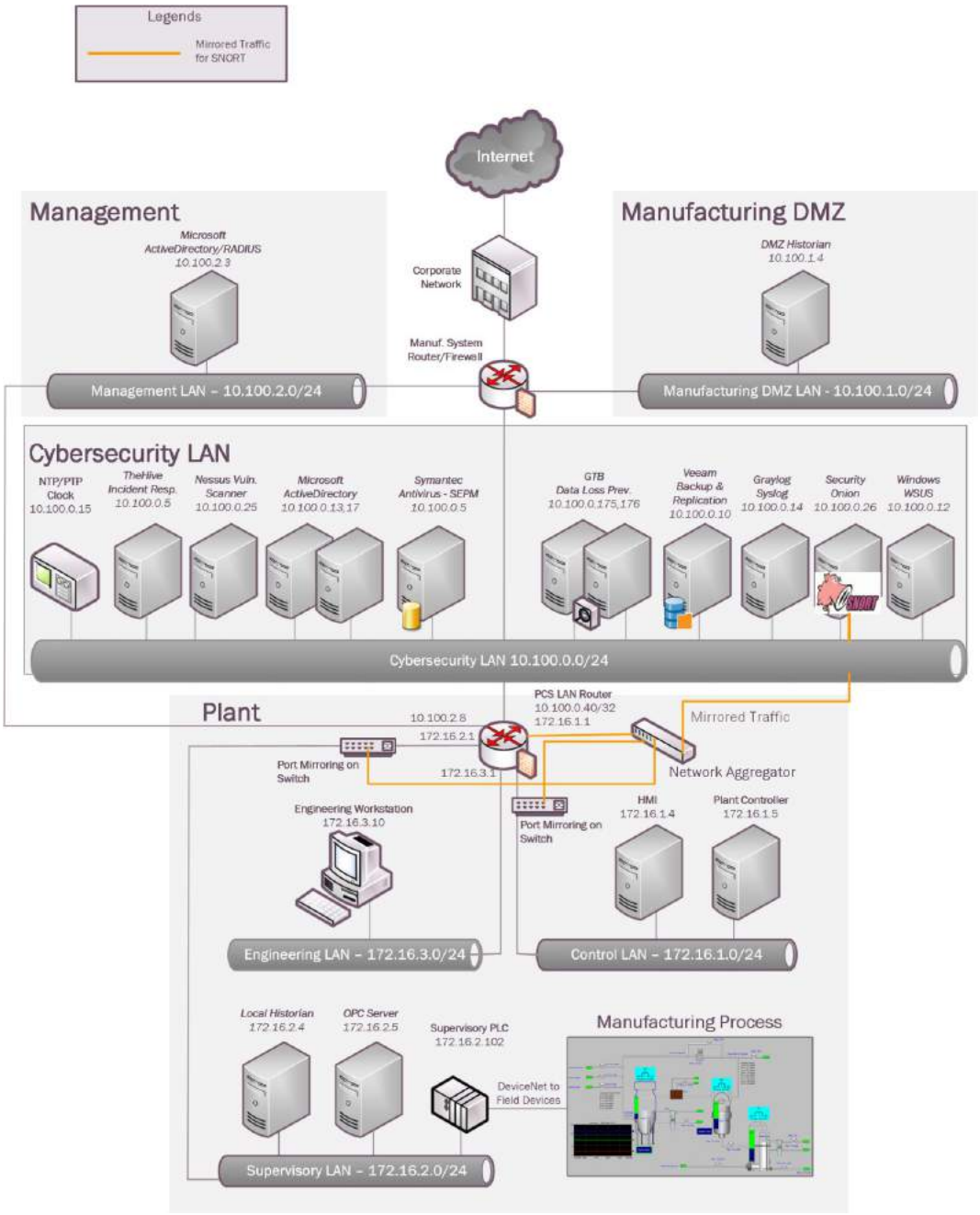
- 网络边界防护
- 网络监控
- 事件日志
- 取证

4.7.3 方案实现的子类

PR.AC-5，PR.DS-5，PR.MA-2，PR.PT-1，PR.PT-4，DE.AE-2，DE.AE-3，DE.CM-1，DE.CM-6，DE.CM-7，DE.DP-3，RS.AN-3

[69] https://securityonion.net/

4.7.4 案实施架构图



4.7.5 安装说明与配置

实施方案的详细信息：

方案名	版本	硬件规格
安全洋葱	16.04.5.2	Hyper-V虚拟机： • 处理器：虚拟4核 • 内存：20 GB • 磁盘空间：500 GB • 网络：2 interfaces • 操作系统：Ubuntu 16.04

安全洋葱环境搭建

- 准备虚拟机，操作系统为 Ubuntu Linux 16.04 定制版本，硬件规格见上表。
- 为虚拟机配置如下两个网络连接：
  - 接口：eth0
  - 模式：管理主接口
  - 接口：eth1
  - 模式：监控端口，与网络聚合器设备连接，接收工厂的所有（3 个）网络设备的镜像流量。
- 客户机操作系统的 IP 信息如下：
  - 接口：eth0
  - IP 地址：10.100.0.26
  - 网关：10.100.0.1
  - 子网掩码：255.255.255.0
  - 域名服务器：10.100.0.17

安装说明

- 下载安全洋葱[70]的 ISO 映像，部署到所选择的虚拟机监控程序上。
- 在继续下一步之前，查看硬件要求[71]。
- 在启动虚拟机之前，为其设置如下两个网络连接：
  - **eth0**：管理 IP 地址
  - **eth1**：监控接口。可将此接口连接到 SPAN 端口，也可以连接到网络分流器，接收所有网络设备的镜像流量。
- 打开虚拟机电源，完成默认操作系统设置，重启系统。
- 确保将操作系统时区设置为 UTC 时间，因为安全洋葱默认使用 UTC。更改时区可能会导致其他问题。
- 本地登录控制台，点击桌面上的设置图标，配置网络接口。完成后重新启动。
- 再次单击安装图标，完成后续步骤。
- 单击【**YES，Continue**】（确认，继续），进入下一页面，单机部署选择【**Evaluation Mode**】（评估模式）。
- 按照界面提示，完成安装。再次重启系统。
- 为远程连接配置相应的防火墙规则：
  - 运行 **sudo so-allow** 命令。
  - 选择 **a – analyst**。
  - 输入访问安全洋葱接口的客户端 PC 的 IP 地址或 IP 范围。

[70] https://securityonion.net
[71] https://securityonion.readthedocs.io/en/latest/

- 安全洋葱对于配置防火墙72有相应说明。

- 运行 sudo nsm_sensor_ps-status 命令，检查各组件状态。
- 通过 SQUERT Web 界面[73]或 Kibana[74]访问安全洋葱程序。

配置 Snort 更新

- 在 https://snort.org 网站注册帐号，下载注册规则集。注册后，记下与帐号绑定的 OINK 码（OINK Code）。
- 服务器的**/etc./nsm/pulledpork/pulledpork.conf**文件中有**rule_url**参数，将 OINK 码复制粘贴到该参数中，保存修改。
  - rule_url=https://www.snort.org/reg-rules/|snortrules-snapshot.tar.gz|<**oink-code**>
- 对于具有互联网访问权限的系统，在**/etc./nsm/securityonion.conf** 文件中取消注释并设置 **LOCAL_NIDS_RULE_TUNING=no**。
- 运行 sudo rule-update 命令，更新规则集。这时，会从 Snort.org 网站下载新规则，保存到/etc./nsm/rules/downloaded.rules 文件。
- 对于气隙环境（无互联网访问权限）：
  - 在 securityonion.conf 文件中设置 **LOCAL_NIDS_RULE_TUNING=yes**。
  - 在具有互联网访问权限的其他系统上手动下载 Snort 更新，通过 USB 设备或网络将这些更新传输到安全洋葱服务器上的/tmp 文件夹。
  - 运行 **sudo rule-update** 命令。

配置 Snort 规则集

- 根据本组织环境，在**/etc./nsm/<hostname-MonitorInterface>/**目录下的 snort.conf 文件中定义网络变量，如**$HOME_NET**、**$EXTERNAL_NET** 等。
- 重启 Snort 服务：sudo nsm_sensor_ps-restart --only-snort

  下图为本实验所涉及 **snort.conf** 文件中的一段代码：


```
################################################
# Step #1: Set the network variables.  For more information, see README.variables
################################################

# Setup the network addresses you are protecting
ipvar HOME_NET [192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]

ipvar NETWORK_DEVICES [172.16.1.3,172.16.3.1,172.16.2.2,192.168.0.239,192.168.0.2,192.168.1.2]
ipvar ICS_DEVICES [172.16.2.102,172.16.4.102,192.168.0.30,192.168.0.60]
ipvar PCS_ICS_DEVICES [172.16.2.100/30]
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS [10.100.0.17]

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
```

- 定义自定义规则集：
  - 在**/etc./nsm/rules/local.rules** 文件中定义规则。
  - 运行 **sudo rule-update** 命令，更新规则集。
  - 运行 **tail -n 100 /etc./nsm/rules/downloaded.rules** 命令，确认

[72] https://github.com/Security-Onion-Solutions/security-onion/wiki/Firewall
[73] https://IP address-of-security-onion/
[74] https://ip-address-of-security-onion/app/kibana

local.rules 已合入 **downloaded.rules** 文件。

- 若 **downloaded.rules** 文件中未包含定义的本地规则，查看 **/etc./nsm/<interface>/snortu-1.log** 文件。

应用规则监控工厂网络

下面是 local.rules 文件中的部分规则，用于检测 IT 和 ICS 系统中的常见异常。

```
# Detect NMAP scan, ICMP attack , TCP-SYN Flood attack
alert UDP any any -> $PCS_ICS_DEVICES any (msg: "Nmap UDP Scan"; sid:10000002; rev:1;)
alert icmp any any -> $HOME_NET any (msg: "NMAP ping sweep Scan"; dsize:0; sid:10000004;
rev:1;)
alert icmp any any -> $HOME_NET any (msg: "Ping Large ICMP Packet"; dsize:>800; classtype:bad-
unknown; sid:10000030; rev:1;)
alert tcp any any -> $HOME_NET [80,22,443] (msg: "TCP SYN flood attack detected"; flow: stateless;
flags:S,12; detection_filter:track by_dst, count 100, seconds 10; classtype: attempted-recon;
sid:10000005; rev:1;)
```

```
# Detect FTP Attempt to Public IP-address & other FTP events
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg: "FTP attempt to Public IP"; sid:10000003;
rev:1;)
alert tcp $HOME_NET any -> any 21 (msg: "FTP upload attempt"; content: "|53 54 4f 52|";
sid:10000020; rev:1;)
alert tcp  any 21 -> $HOME_NET any (msg: "FTP file successfully uploaded"; content: "|54 72 61 6e 73
66 65 72 20 63 6f 6d 70 6c 65 74 65|"; sid:10000027; rev:1;)
alert tcp  any 21 -> $HOME_NET any (msg: "FTP PDF file successfully uploaded"; content: ".pdf";
sid:10000031; rev:1;)

# Detect Credit card number in cleartext
alert tcp any any <> any any (pcre:"/5\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; msg: "MasterCard
number detected in clear text"; content:"number"; nocase; sid:10000013; rev:1;)
alert tcp any any <> any any (pcre:"/3\d{3}(\s|-)?\d{6}(\s|-)?\d{5}/"; msg: "American Express number
detected in clear text"; content:"number";nocase; sid:10000014; rev:1;)
alert tcp any any <> any any (pcre:"/4\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; msg: "Visa number
detected in clear text"; content:"number";nocase; sid:10000015; rev:1;)

# Telnet activity monitoring
alert tcp $TELNET_SERVERS 23 ->  $HOME_NET any (msg: "Telnet Password in Clear text"; content:
"Password"; sid:10000010;rev:1;)
alert tcp $HOME_NET any -> $TELNET_SERVERS 23 (msg: "TELNET login attempt";
classtype:default-login-attempt; sid:10000007; rev:1;)
alert tcp $HOME_NET any ->  $TELNET_SERVERS 23 (msg: "Telnet Rockwell Automation Default
Password"; content: "|73 77 69 74 63 68|"; sid:10000008;rev:1;)
alert tcp any 23 -> any any (msg: "TELNET login failed"; flow:from_server,established; content:"Login
failed"; fast_pattern:only; nocase; classtype:bad-unknown; sid:10000038; rev:
```

ICS/SCADA 的 Snort 规则[75]：

[75] Snort Rules for ICS/ SCADA：https://github.com/ITI/ICS-Security-Tools/blob/master/configurations/rules/talos-snort.rules

```
#ICS-SCADA specific rules [4]
alert tcp $HOME_NET any -> $ICS_DEVICES 44818 (msg: "PROTOCOL-SCADA Rockwell firmware change attempt"; flow:to_server,established; content:"|6F 00|"; content:"|00 00 00 00|"; within:4; distance:6; content:"|00 00 00 00|"; within:4; distance:8; pcre:"/(\x20\xa1|\x21\x00\xa1\x00)(\x24[\x01-\xff]|\x25\x00[\x01-\xff]\x00)/smi"; reference:cve,2012-6437; reference:url,tools.cisco.com/security/center/viewAlert.x?alertId=27868; classtype:policy-violation; sid:10000019; rev:1;)
alert tcp $HOME_NET any -> $ICS_DEVICES $HTTP_PORTS (msg: "ICS-SCADA PLC Web access attempted "; sid:10000033; rev:1;)
alert tcp any any -> $HOME_NET 22350 (msg: "PROTOCOL-SCADA TwinCAT PLC DOS attempt"; flow:to_server,established; dsize:>2000; content:"|A2 1D CB AA AA 75 48 B4 91 DB F4 06 B0 B0 2D|"; fast_pattern:only; metadata:policy max-detect-ips drop, policy security-ips drop; reference:url,www.beckhoff.com/english.asp?twincat/overvw.htm; classtype:attempted-dos; sid:41743; rev:2;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus user-defined function code - 65 to 72"; flow:to_server,established; byte_test:1,>,64,7; byte_test:1,<,73,7; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:15074; rev:5;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus user-defined function code - 100 to 110"; flow:to_server,established; byte_test:1,>,99,7; byte_test:1,<,111,7; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:15075; rev:5;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus read multiple coils - too many inputs"; flow:to_server, established; modbus_func:read_coils; byte_test:2,>,2000,10; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:15077; rev:6;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write multiple registers from external source"; flow:to_server,established; modbus_func:write_multiple_registers; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:17782; rev:4;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write single coil from external source"; flow:to_server,established; modbus_func:write_single_coil; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:17784; rev:4;)
alert tcp any any -> $ICS_DEVICES 502 (msg: "PROTOCOL-SCADA Modbus write multiple coils from external source"; flow:to_server,established; modbus_func:write_multiple_coils; reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf; classtype:protocol-command-decode; sid:17785; rev:4;)
```



```
# Accessing switch via Web URL & use of default password
alert tcp  any ->  $NETWORK_DEVICES 80 (msg: " WEBAPP Netgear Default Password"; flow:established,to_server; content:"POST"; nocase; http_method; uricontent:"/base/cheetah_login.html"; content:"password"; nocase; sid:1000009; rev:1;)
alert tcp $HOME_NET any -> $NETWORK_DEVICES $HTTP_PORTS (msg: "WEBAPP Rockwell Automation default password login attempt"; flow:to_server,established; content:"Authorization|3A|"; nocase; http_header; content:"YWRtaW5pc3RyYXRvcjptbDE0MDA="; fast_pattern:only; http_header; metadata:service http; classtype:default-login-attempt; sid:10000011; rev:1;)

# SSH Activity monitoring
alert tcp any any -> $EXTERNAL_NET 22 (msg: "SSH Attempt to Public Host"; sid:10000018; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg: "Potential SSH Brute Force Attack"; flow:to_server, established; flags:S+; detection_filter:track by_src, count 30 , seconds 10; classtype:attempted-dos; priority:1; sid:10000006; rev:1;)

# DNS traffic to social media websites
alert udp $HOME_NET any -> $DNS_SERVERS 53 (msg: "DNS Request to Twitter.com Detected"; content: "|6e 69 73 74|"; sid:10000016; rev:1;)
alert udp $HOME_NET any -> $DNS_SERVERS 53 (msg: "DNS Request to Facebook.com Detected"; content: "|66 61 63 65 62 6f 6f 6b|"; sid:10000017; rev:1;)

# File upload activity to a public web server
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "WEB-PHP file upload attempt"; flow:to_server, established; uricontent:"/upload.php"; nocase; content:"filename="; reference:bugtraq,3361; reference:cve,2001-1032; classtype:attempted-admin; sid:10000029; rev:1;)
alert tcp $Robotics_devices any -> $EXTERNAL_NET $HTTP_PORTS (msg: "Web Access to Public IP attempted"; sid:10000039; rev:1;)
```

调整安全洋葱

- 在**/etc./nsm/securityonion.conf** 文件中设置 **DAYSTOKEEP** 参数，更改数据库保留时间。Sguil 数据库的默认保留时间为 30 天。
- 要使用 **downloaded.rules** 文件中注释掉的规则，记下该规则中的生成器 ID（GID）和签名 ID（SID），将其加入 **/etc./nsm/pulledpork/enablesid.conf** 文件。不要在 **downloaded.rules** 文件中直接取消注释这些规则。
- 要消除误报，记下产生误报的规则的 GID 和 SID，记入 **/etc./nsm/pulledpork/disablesid.conf** 文件。下图显示的是 **disablesid.conf** 文件中的代码片段，列举了禁用的 SID。

```
# example disablesid.conf V3.1

# Example of modifying state for individual rules
# 1:1034,1:9837,1:1270,1:3390,1:710,1:1249,3:13010
3:19187
119:19 # http_inspect： LONG HEADER
123:8 # frag3：Fragmentation overlap 128:4
# ssh：Protocol mismatch
129:4 # stream5：TCP Timestamp is outside of PAWS window
129:5 # stream5：Bad segment，overlap adjusted size less than/equal 0 129:7
# stream5：Limit on number of overlapping TCP packets reached 129:12 #
stream5：TCP Small Segment Threshold Exceeded
```

- 按照 wiki 说明，管理 PCAP 文件的大小，确保服务器有足够的存储空间。

BRO IDS 配置

Zeek（以前称为 BRO）是一个强大的 IDS 系统，与 Snort 一起预装在安全洋葱服务器中。BRO 的具体工作原理非本文讨论范围。大致步骤如下：

- 将 BRO 的所有自定义脚本放在**/opt/bro/share/bro/policy/**目录下。有关 BRO 的更多信息，参见安全洋葱 wiki[76]。
- 启用 Windows SMB 文件共享监控：
  - 在**/opt/bro/share/bro/site/local.bro** 文件末尾，添加下面这行：
  - @load policy/protocols/smb 重启 BRO：sudo nsm_sensor_ps-restart --only-bro

OSSEC 配置

OSSEC 是主机入侵检测系统（HIDS），支持 Windows 和 Linux 平台。OSSEC 服务器（已被 Wazuh 取代）预装了安全洋葱。OSSEC 产品的具体工作原理非本文讨论范围，有关信息，见 OSSEC 官方网站和参考文献中的其他文档链接。

- 根据所使用的操作系统，下载对应的 OSSEC 代理安装程序[77]。
- 将代理复制到客户端系统，根据 OSSEC 网站说明，启动安装过程。安装过程中，将安全洋葱服务器的 IP 地址作为 OSSEC 服务器的 IP 地址。
- 运行 **so-allow** 命令，管理安全洋葱服务器上的防火墙设置，从 OSSEC 客

[76] https://securityonion.readthedocs.io/en/latest/
[77] http://www.ossec.net/

户端接收数据[78]。

- 将自定义 OSSEC 监控规则添加至 **/var/ossec/rules** 目录下的 local_rules.xml 文件中。若需要解码器来解析自定义日志，则应在 /var/ossec/etc.目录下的 **local_decoder.xml** 文件中进行定义。
- 从 Kibana 界面或 Squert Web 界面查看 OSSEC 告警。
- 用 OSSEC 监控 USB 设备：

  - 在 Windows 终端的本地 Ossec.conf 文件中添加下列各行[79]：

```
<agent_config os="Windows">
 <localfile>
  <log_format>full_command</log_format>
       <command>reg QUERY
       HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR</command>
  <alias>usb-check</alias>
 </localfile>
</agent_config>
```

  - 在安全洋葱服务器上的/var/ossec/rules /local_rules.xml 文件中添加下列各行，以便监控到异常时进行告警：

```
<rule id="140125" level="7">
 <if_sid>530</if_sid>
 <match>ossec: output: 'usb-check':</match>
 <check_diff />
 <description>New USB device connected</description>
</rule>
```


- 监控网络中的非授权资产：

  - 在安全洋葱服务器上安装 arpwatch：
  - 运行 **arpwatch -i <interface>**命令，启动服务。

    例如：**arpwatch -i eth1**，其中 eth1 为监控端口。
  - 在 **local_rules.xml** 文件件中添加一条新规则，如下所示，引用 **/var/ossec/etc./arpwatch_decoder.xml** 中的内置解码器，当新设备接入网络时进行告警。

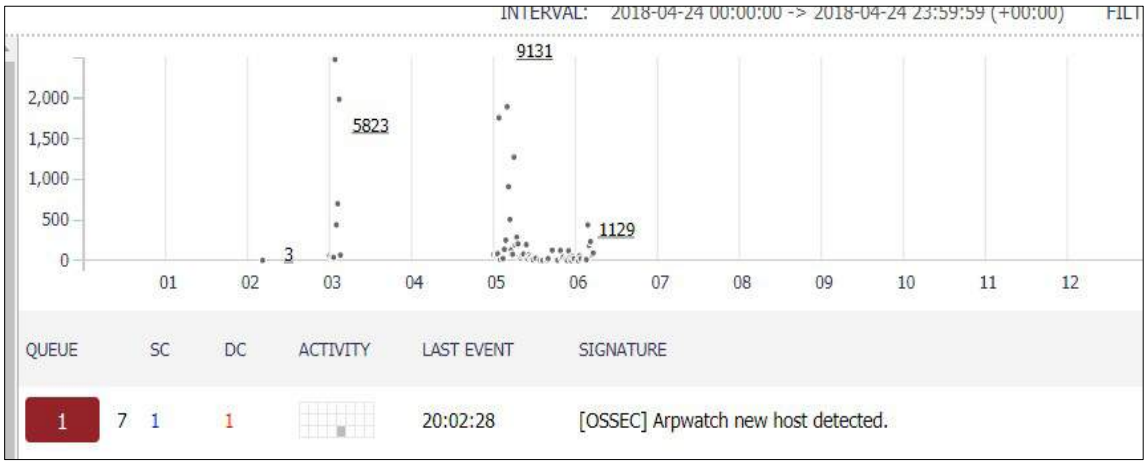
[78] https://github.com/Security-Onion-Solutions/security-onion/wiki/Firewall
[79] https://www.ossec.net/docs/manual/monitoring/process-monitoring.html

```
<rule id="110003" level="7">
  <if_sid>7200</if_sid>
  <match>new|logon</match>
  <description>Arpwatch new host detected. </description>
  <group>new_host,</group>
</rule>
```

- 添加本地规则后，运行下述命令，重启 OSSEC 服务器：

  sudo service ossec-hids-server restart

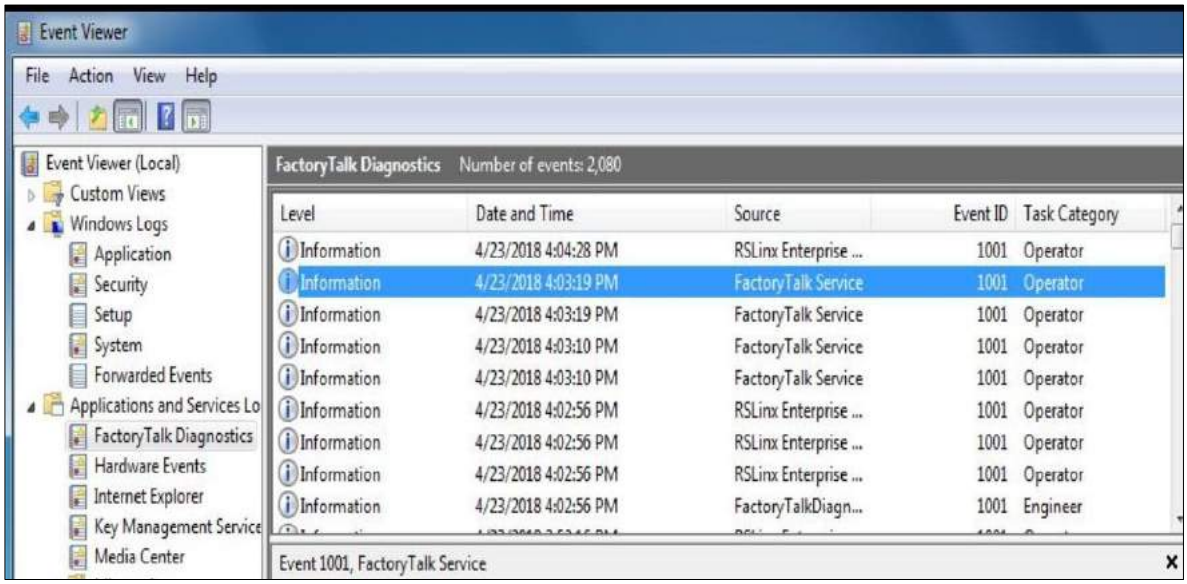
下图为新系统物理连接到网络时 Squert Web 界面所显示的告警示例：



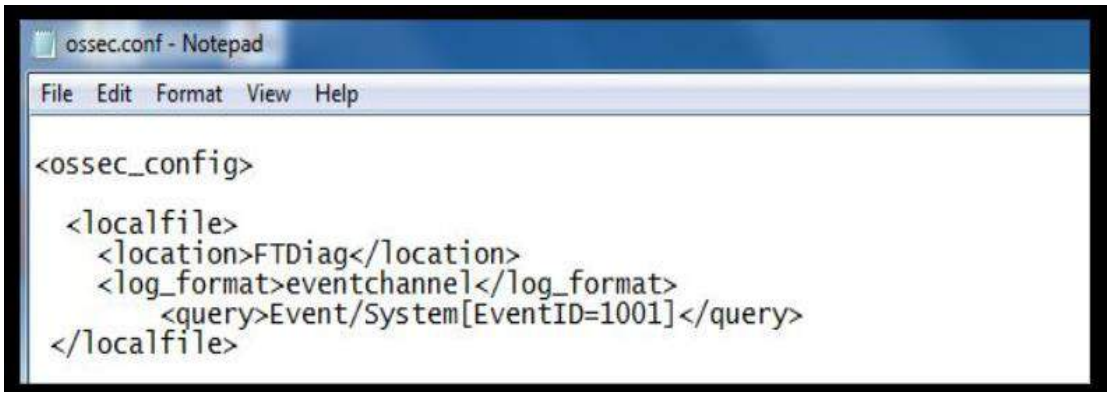
说明：该软件包依赖系统的本地 ARP 缓存检测新设备。

- 在 Windows 主机上通过 OSSEC 监控特定事件：

  - 在事件查看器中记下须告警的事件 ID。例如，假设需要监控 Factory Talk 服务的 ID 为 1001 的事件，即 Rockwell Factory Talk 软件登录失败。



- 编辑客户端本地的 ossec.conf 文件，在 Event 类别的<location>属性下加入该事件 ID。例如：



- 在 **local_rules.xml 文件中，定义对应告警规则。对 OSSEC，务必设置 level >=7**，确保异常发生时触发告警。例如：

```
<group name="syslog,">
<rule id="110001" level="0">
  <if_sid>18104</if_sid>
   <match>FactoryTalkDiagnostics</match>
  <description>FactoryTalk Audit Event</description>
 </rule>
<rule id="110002" level="7">
  <if_sid>110001</if_sid>
  <match>failure</match>
  <description>FactoryTalk Administration Console login failure</description>
 </rule>
```

经验总结：

根据环境中的网络流量情况，安全洋葱的全包捕获功能可能会很快耗尽硬盘空间。务必为服务器规划和分配足够存储空间，同时在 **securityonion.conf** 文件中配置必要的数据保留参数。PCAP 文件裁剪后可以保留更长时间[80]。

4.7.6 对性能的主要影响

考虑到安全洋葱的安装位置和使用方式（软件独立于制造系统，对网络流量进行被动分析），没有测试其对系统性能的影响。

4.7.7 性能测量数据集的相关链接

无

[80] https://www.netresec.com/?page=Blog&month=2017-12&post=Don%27t-Delete-PCAP-Files---Trim-Them

4.8 思科 AnyConnect VPN

4.8.1 技术方案概述

AnyConnect 安全移动客户端[81]是思科开发的模块化端点软件产品，通过安全套接字层（SSL）和 IPsec IKEv2 提供 VPN 访问，通过各种内置模块提升安全。AnyConnect 客户端可在多种平台上使用，包括 Windows、macOS、Linux、iOS、安卓、Windows Phone/Mobile、黑莓和 ChromeOS。

重点说明：

- 以 Web 安全和基于 DNS 的安全形式提供额外的网络安全；
- 独立于操作系统平台：Windows、Mac 和 Linux 均支持 VPN 客户端；
- 管理员能够控制端点要连接的网络或资源，产品提供了 IEEE 802.1X 请求程序，实现身份认证、授权和记帐（AAA）功能以及一些独特的加密技术，如 MACsec IEEE 802.1AE；
- 作为思科专有产品，替代了早期的免费产品 AnyConnect VPN 客户端，用户必须具有思科自适应安全设备（ASA）防火墙或思科 Firepower 服务设备和有效的 AnyConnect 安全移动客户端许可证。

4.8.2 方案提供的技术能力

思科 AnyConnect VPN 提供以下技术能力（参见第 1 卷第 6 章）：

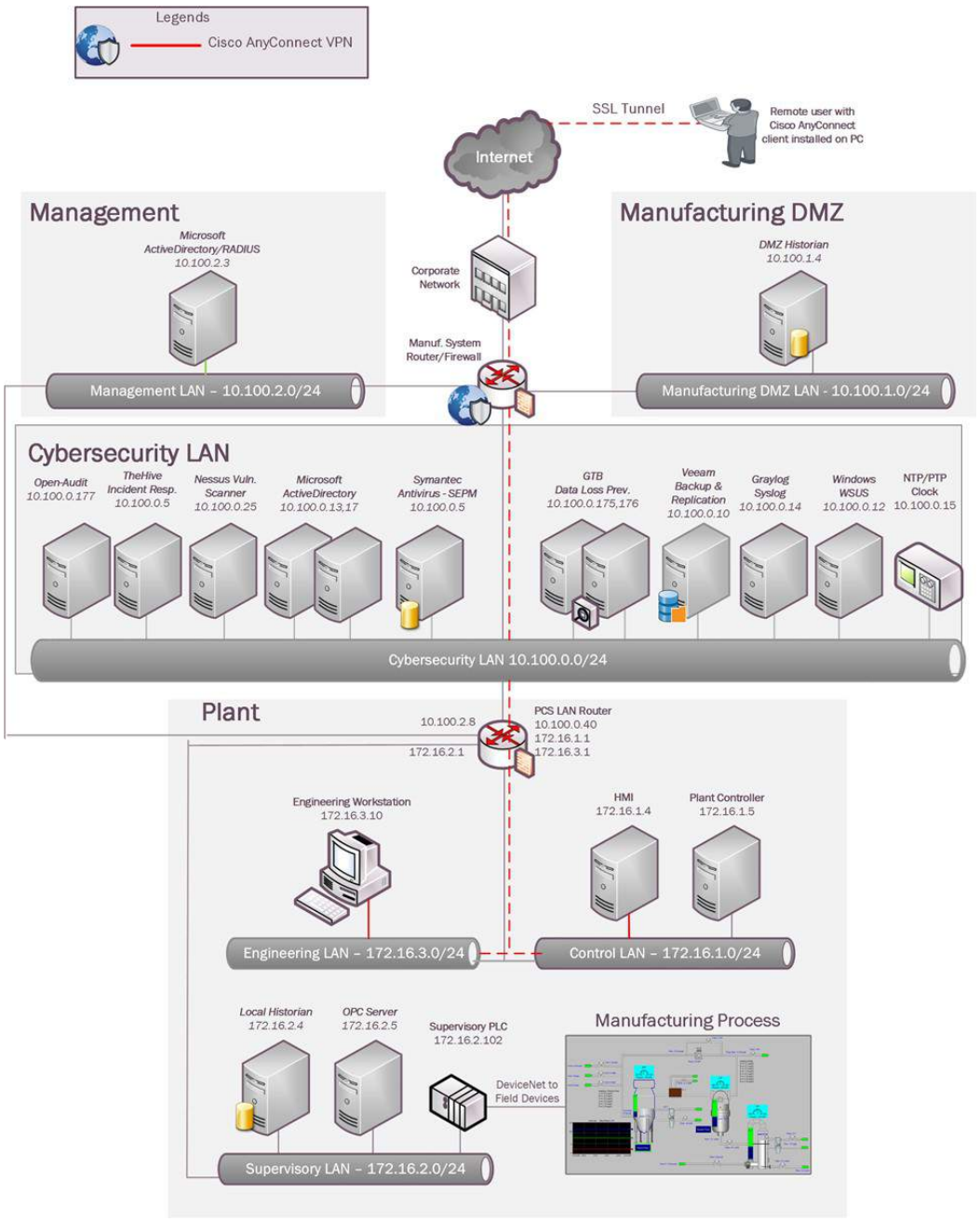
- 远程安全接入
- 数据复制

4.8.3 方案实现的子类

PR.AC-5，PR.IP-4，PR.MA-2

[81] https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/at_a_glance_c45- 578609.pdf

4.8.4 方案实施架构图



4.8.5 安装说明与配置

实施方案的详细信息：

设备	功能	操作系统及版本
提供Firepower服务的思科ASA 5512	防火墙	FTD 6.2.3
AnyConnect VPN	VPN客户端软件	4.7.01076
虚拟机（Mgmt-AD.mgmt.lab）	活动目录、DNS、NPS（Radius）	Windows 2012 R2

环境概述

使用思科 AnyConnect VPN 实现远程安全访问。在网络安全局域网中的思科 ASA 防火墙上配置 AnyConnect VPN，在工厂的管理局域网中配置 Windows 服务器，用于托管 VPN 客户端的活动目录和 Radius 身份认证服务。

在 Windows 平台配置 Radius 服务器

设置 Radius 服务器认证思科 ASA 用户的大概步骤如下：

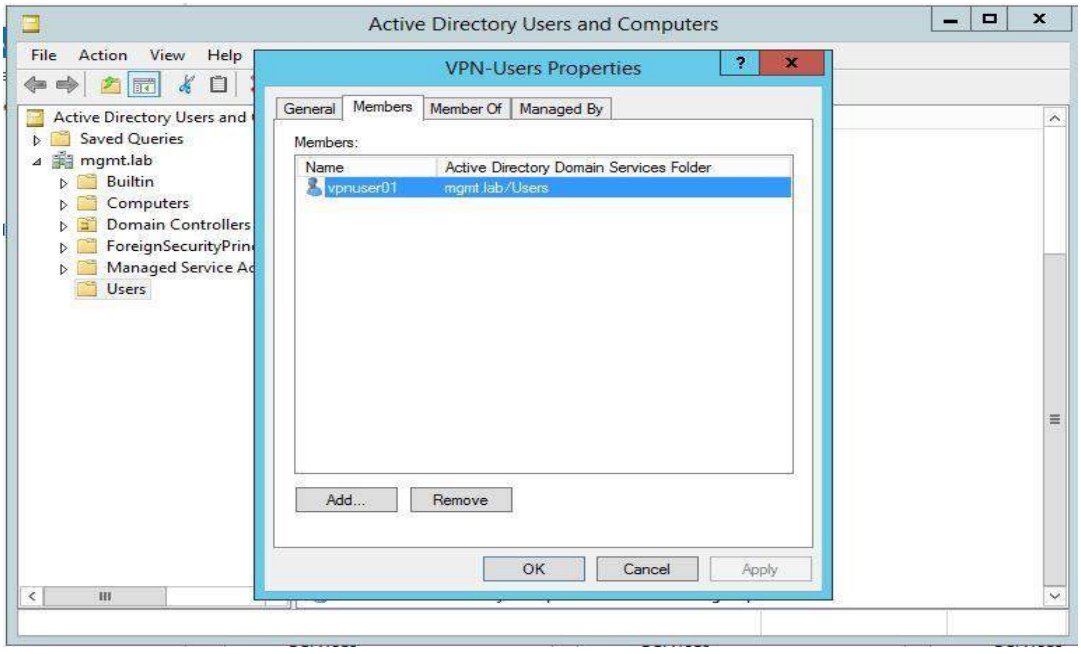
- 使用服务器管理器或 Power Shell 在服务器上安装以下角色。须使用不同的服务器来承担不同的角色并实现冗余。

  - 活动目录服务

  - DNS 服务器

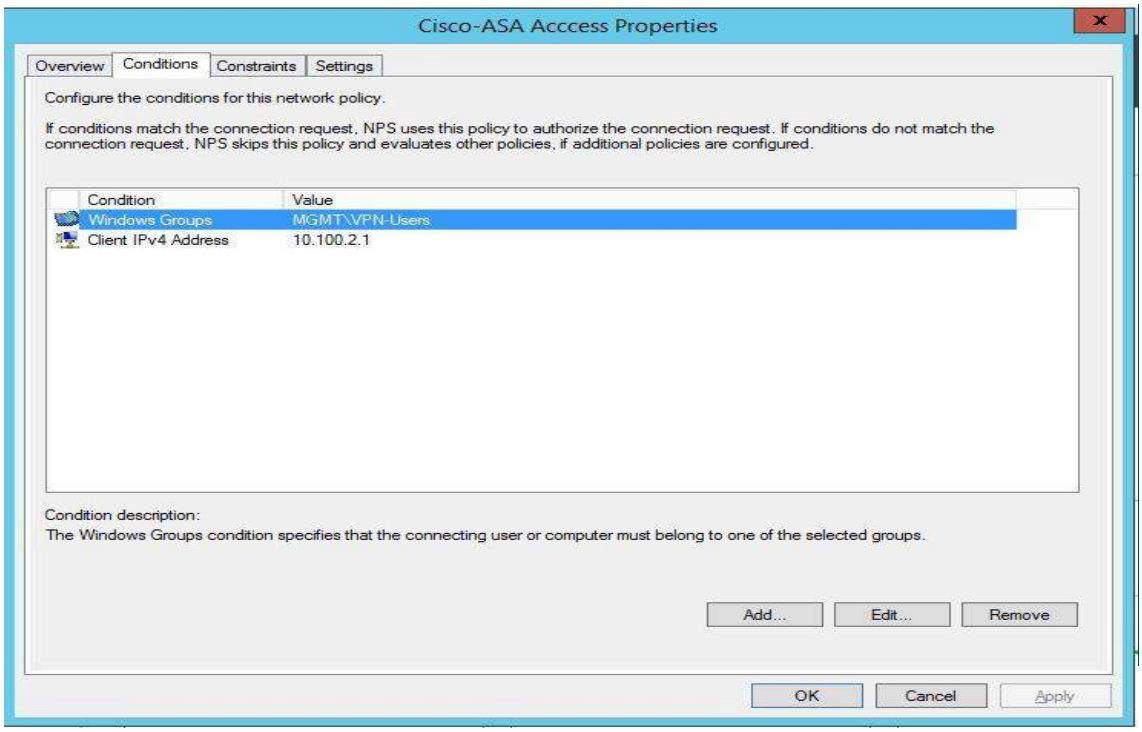
  - 网络策略服务器

- 在活动目录中为 VPN 用户创建安全组，将需要远程访问的用户添加到此组。例如，在活动目录服务器中创建名为 **VPN-users** 的组，将用户 **vpnuser01** 添加到该组中。

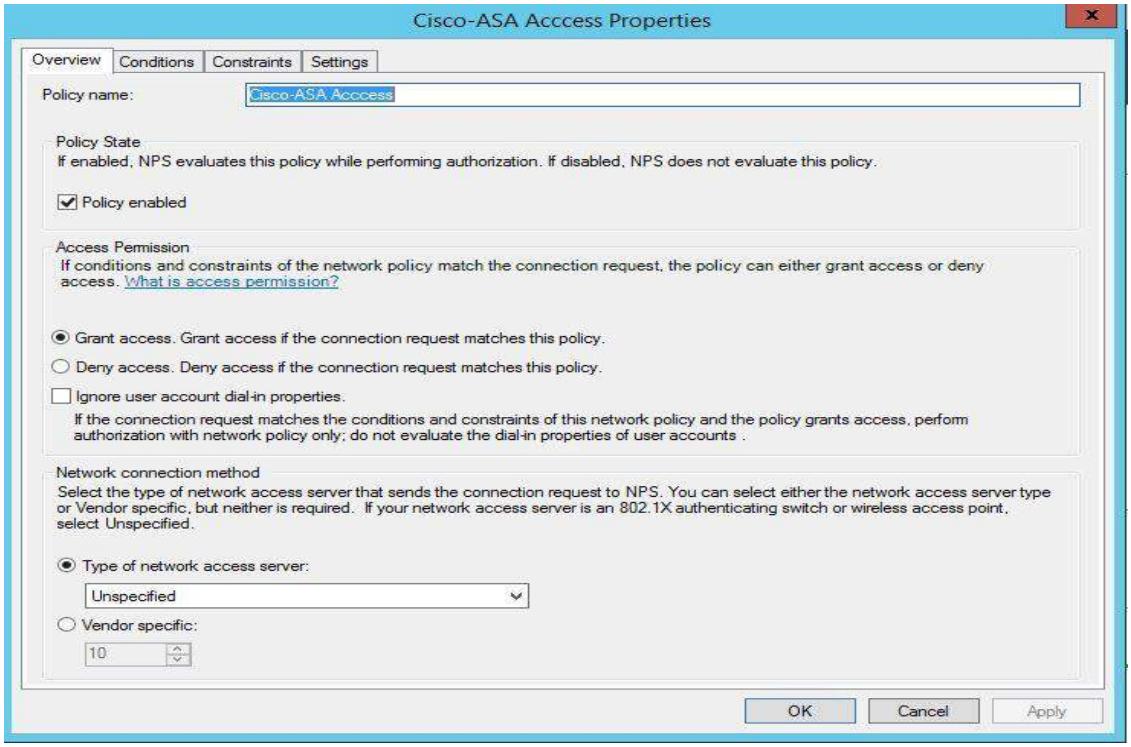


- 启动网络策略服务器控制台。单击 **Radius Clients > New**（Radius 客户端 > 新建），为防火墙设备添加一个 Radius 客户端。
- 在 ASA 上输入接口的 IP 地址，通常是活动目录/Radius 服务器所在子网的默认网关。输入强共享密钥。

下图显示了为思科 ASA 防火墙添加的 Radius 客户端。



- 单击【**Polices**】（策略）下的【**Network Policies**】（网络策略），为之前添加的 Radius 客户端设置对应的网络策略。下图显示了为思科 ASA 客户端创建的网络策略。务必启用该策略。

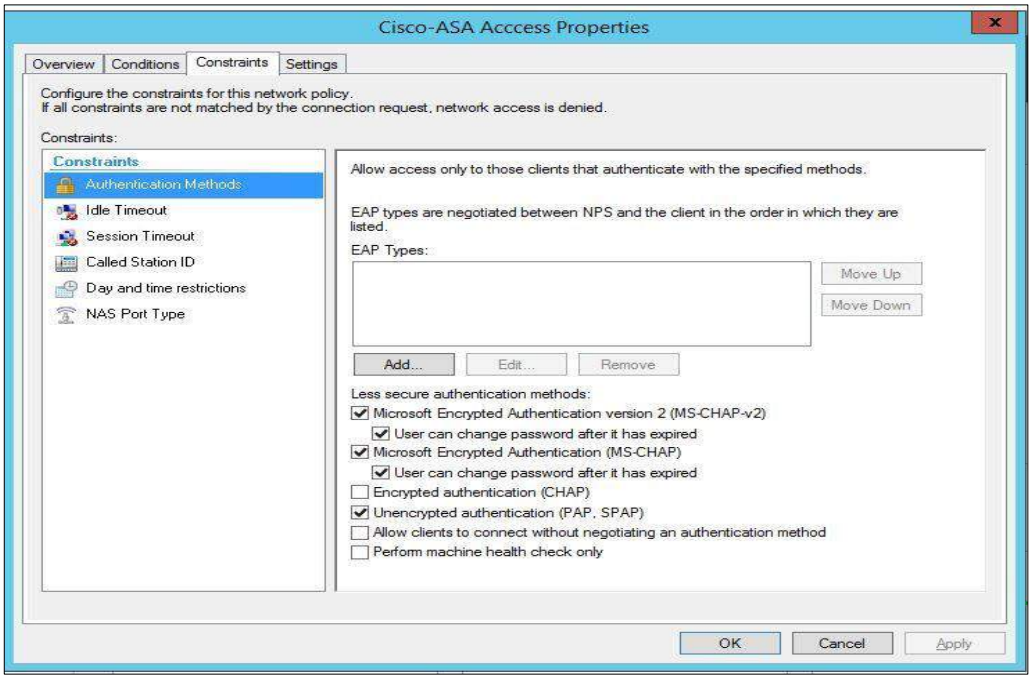


- 单击【**Conditions**】（条件）页签下的【**ADD**】（添加），至少添加以下两个条件，必要时，可添加更多条件。

  - **VPN-Users**：之前创建的安全组

  - **Client IPv4 Address**：之前添加的 Radius 客户端的 IP 地址

- 参照思科文档[82]，选择 **Constraints > Authentication Methods**（约束条件 > 认证方法）。

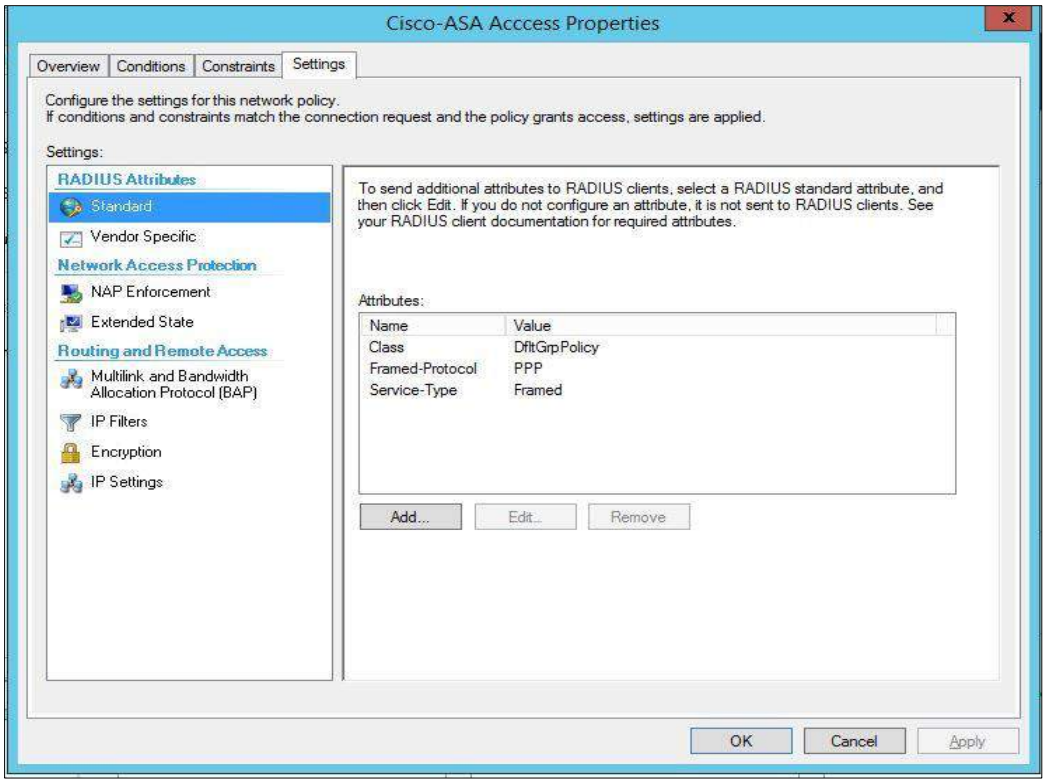


- 在 Settings 页签，选择 **RADIUS Attributes > Standard**（Radius 属性 > 标准），设置如下属性：

  - Framed Protocol= **PPP**

  - Service-Type=**Framed**

  - Class = <**Name of group policy**>. 此策略在 VPN 的防火墙中配置。

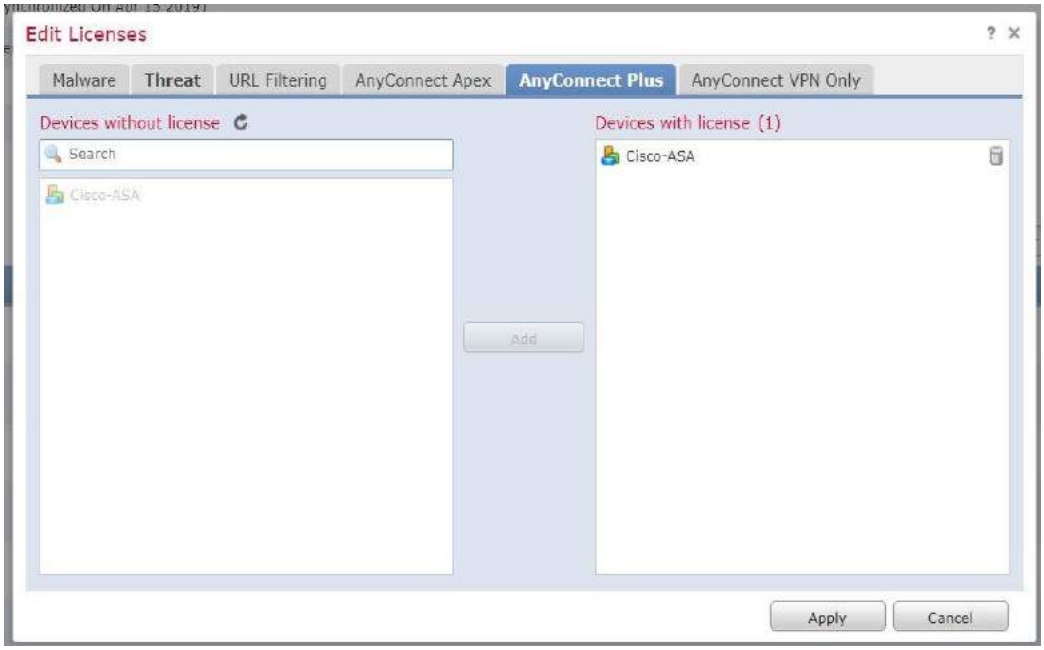


82 https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/117641-config-asa-00.html

在思科 ASA 防火墙上配置 AnyConnect VPN

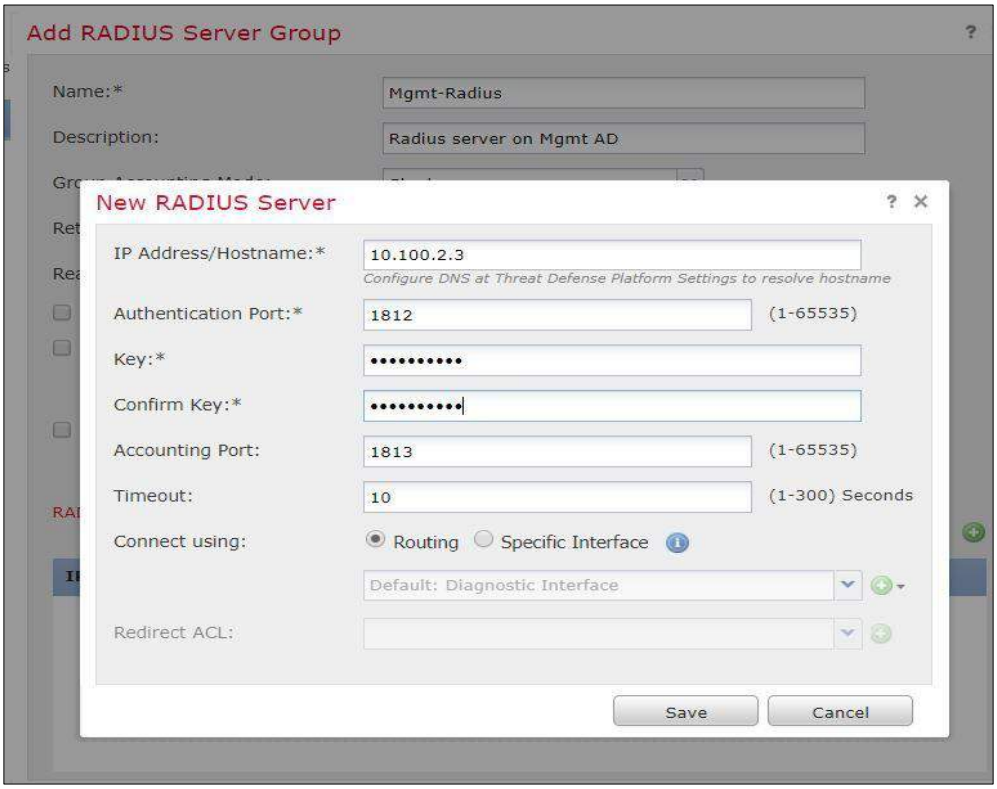
在 FMC（Firepower 管理控制台）中配置远程安全访问的大致步骤如下：

- 登录 FMC Web 界面，选择 **Licenses > Smart Licenses**（许可证 > 智能许可证），确认是否已启用 AnyConnect Plus 或 AnyConnect VPN 许可证。
- （可选）单击【**Edit Licenses**】（编辑许可证），从左侧的【**Devices without license**】（没有许可证的设备）中选择相应的防火墙设备，将其移动到右侧的【**Devices with license**】（有许可证的设备）下，启用许可证（假设已购买 AnyConnect 许可证并绑定到思科智能帐号）。单击【**Apply**】（应用）。



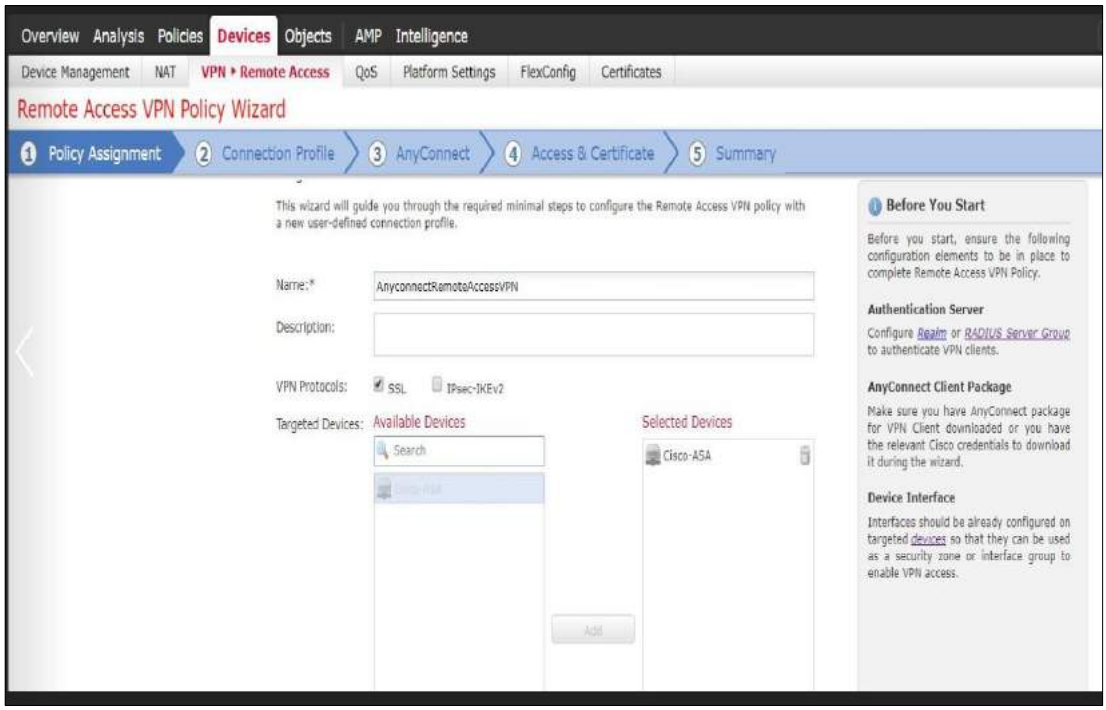
- 选择 **Objects > Object Management > Radius Server Group > Add Radius Server Group**（对象 > 对象管理 > Radius 服务器组 > 添加 Radius 服务器组）（若尚未配置）。

- 单击【**Add Radius Server Group**】(添加 Radius 服务器组),输入【**Name**】(名称)和【Description】(说明),移动鼠标至底部菜单的【**Radius Servers**】(Radius 服务器),单击"+",添加服务器。
- 在【**New RADIUS Server**】(新增 Radius 服务器)对话框中,输入 Radius 服务器的 IP 地址和强共享密钥,单击【**Save**】(保存)。

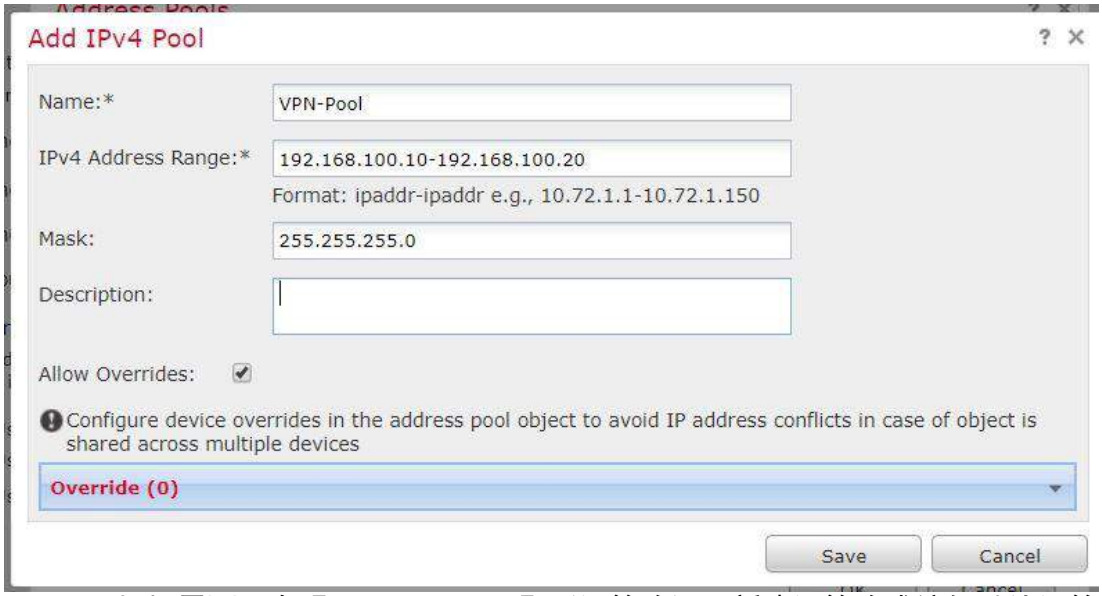


- 选择 **Devices > VPN > Remote Access > Wizard > Add a new Configuration**(设备 > VPN > 远程访问 > 向导 > 新增配置),启动远程访问 VPN 策略向导。
- 在【**Policy Assignment**】(策略分配)页面,执行以下操作:

  - 配置【**Name**】(名称)、【**Description**】(说明)。
  - 选择协议(SSL、IPSec-IKEv2)。可以同时选择两种协议。
  - 从左边的【**Available Devices**】(可用设备)列表中选择目标服务器设备,移动到右边的【**Selected Devices**】(选中设备)列表。



- 要求输入信息，配置【**Connection Profile**】（连接 Profile）：
  - 【**Authentication Method**】（认证方法）选择【**AAA Only**】（仅 AAA）。
  - 在【**Authentication Server**】（认证服务器）下，输入 Radius 服务器名称。
  - **单击**【Use IP Address Pool】（使用 IP 地址池）旁边的铅笔图标，创建一个新的 IPv4 地址池，例如，**VPN-Pool**，如下图所示。

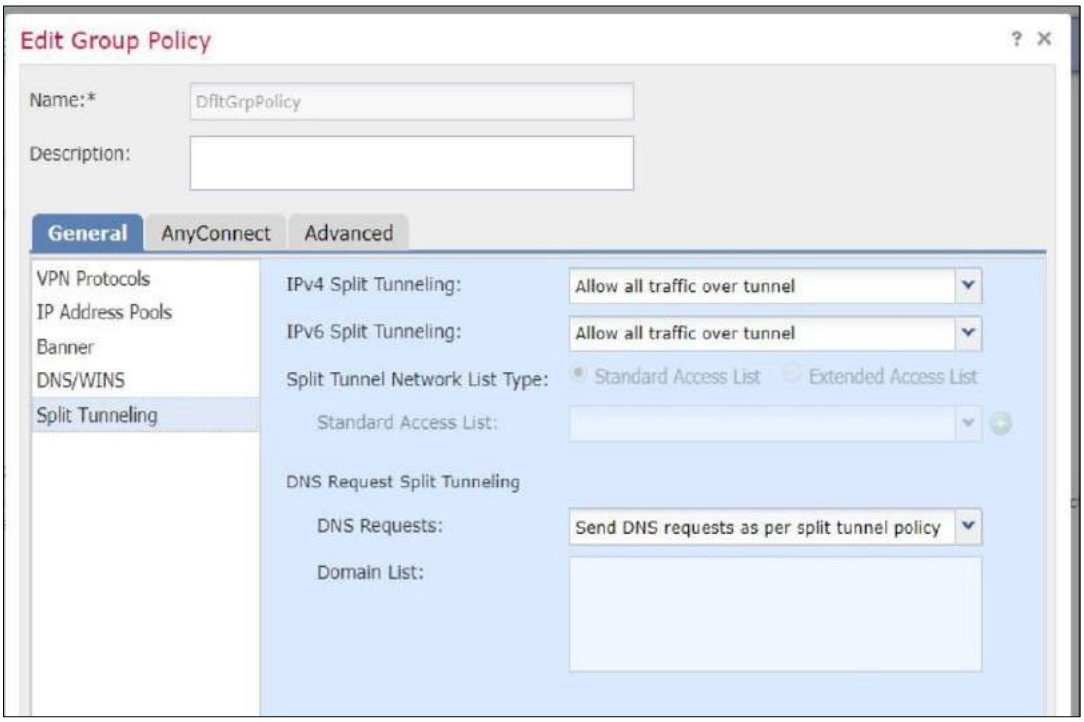


- 根据需要，在【**Group Policy**】（组策略）下新建组策略或编辑默认组策略，以便在 Windows 平台的 Radius 服务器配置中引用。

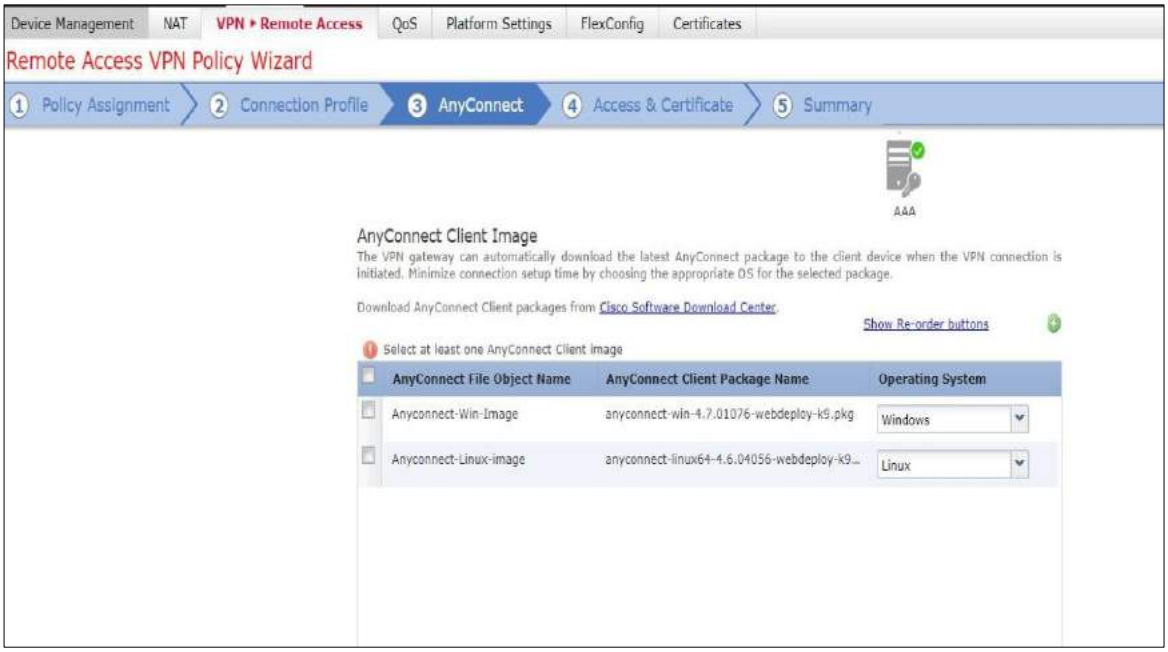
  下面为我们对默认组策略进行的修改，以供参考：
  - 选择 **General > VPN Protocols**（常规 > VPN 协议），选择 **SSL**。
  - 选择 **General > Banner**（常规 > 横幅），自定义欢迎信息。
  - 选择 **General > Split Tunneling**（常规 > 隧道分离），允许所有隧道流量（若隧道分离已禁用）。

- 在【**AnyConnect**】页签，新建【Client Profile】（客户端配置）（若无）。
- 选择 **Advanced > Session Settings**（高级 > 会话设置），将【**Idle Session Timeout**】（空闲会话超时）设置为 30 分钟。

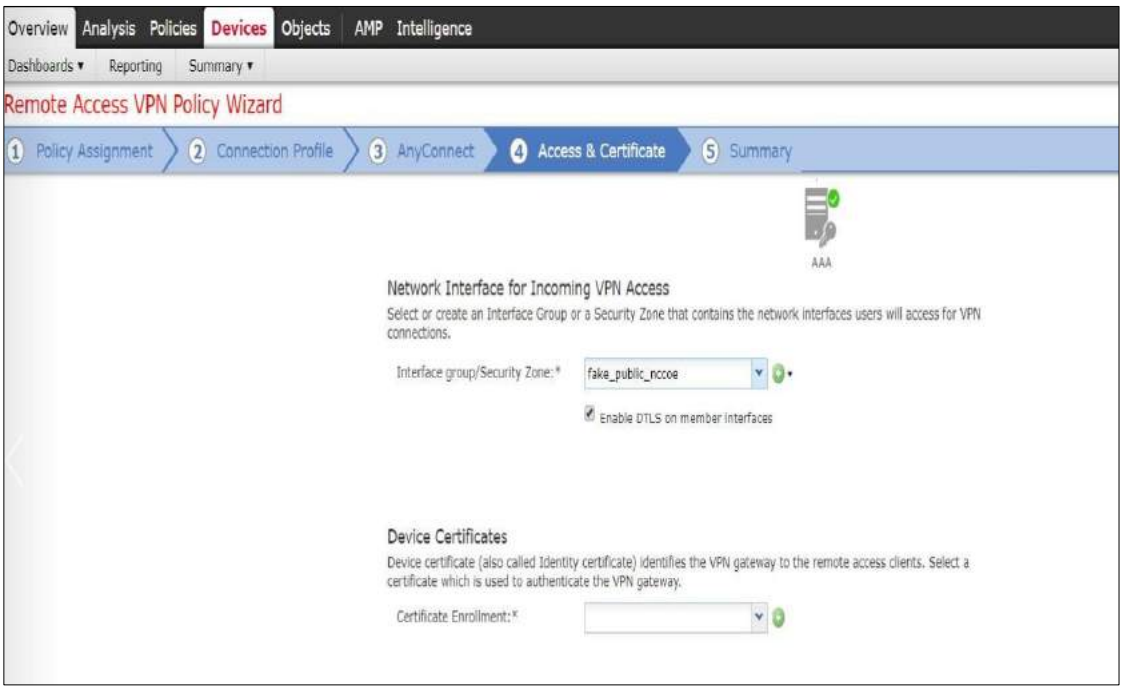
参见下图。



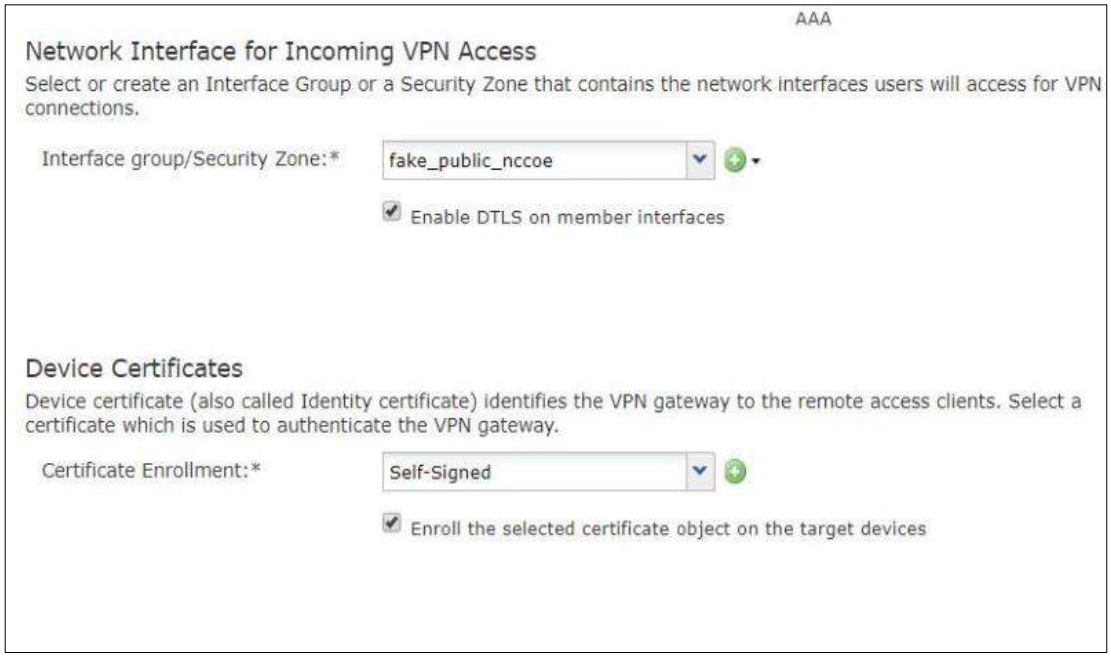
- 在 **AnyConnect** 页面，根据使用的操作系统（支持 Windows、Linux、MacOS）选择 AnyConnect 映像。单击“+”图标，手动上传其他安装程序映像。



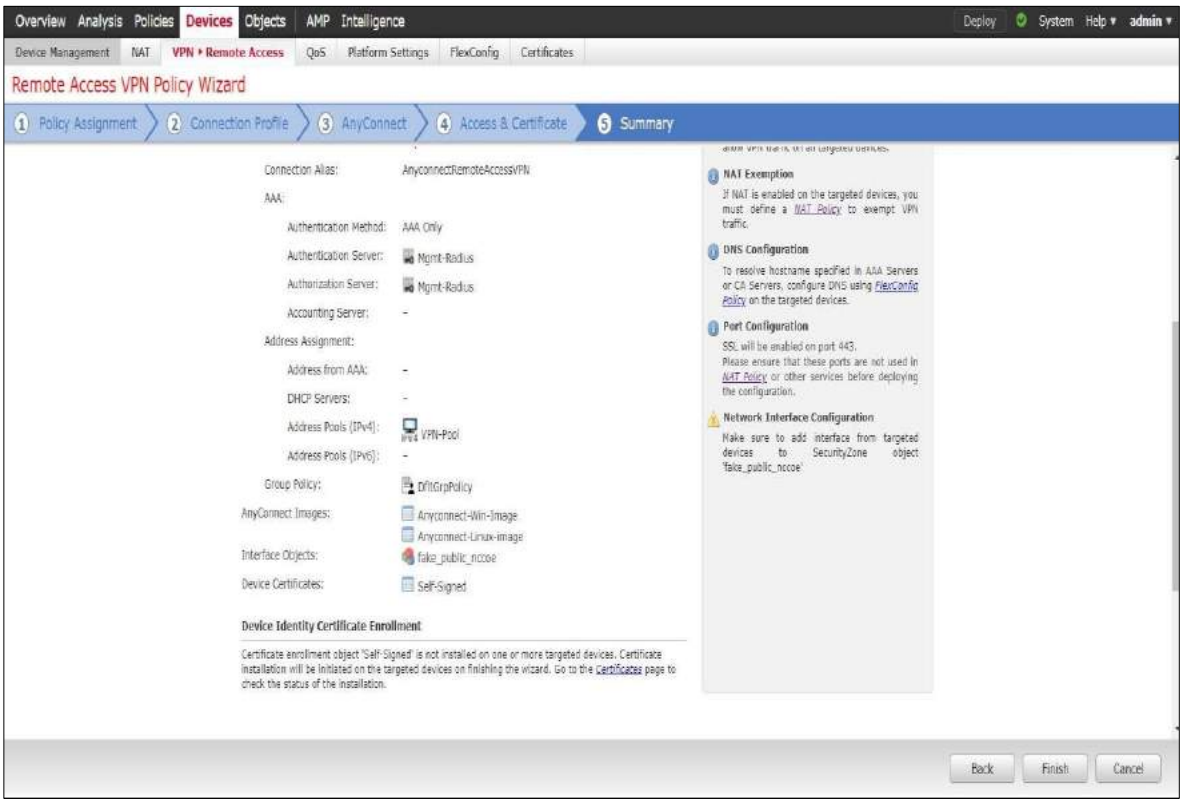
- 在 **Access & Certificate**（访问与证书）页面，配置如下项目：
  - 【**Interface group/Security Zone**】（接口组/安全区）选择外部防火墙接口。



- 在【**Device Certificates**】（设备证书）下，输入认证 VPN 网关的证书，可以选择现有证书，也可以单击“+”，创建自签名证书。实验环境中使用的是自签名证书。



- 在 Summary（摘要）页面，查看配置信息，若所有设置均准确无误，单击【Finish】（完成），提交应用。



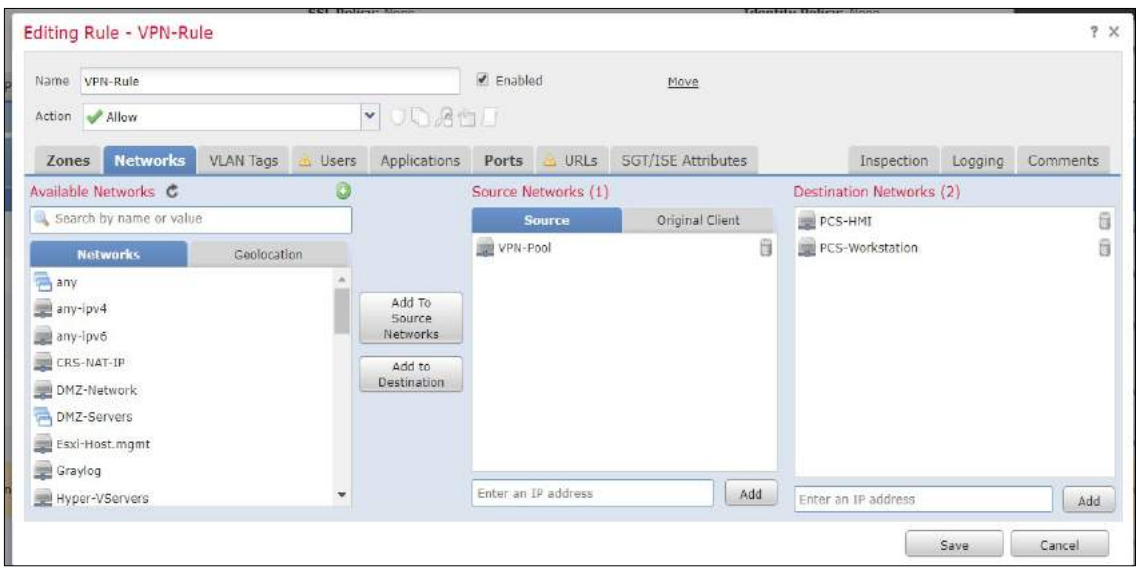
其他配置

远程访问 VPN 策略配置完成后，需要进行以下配置，远程访问 VPN 才能对各目标设备生效：

- 访问控制策略
- 设备证书
- NAT 豁免

- 新建访问控制策略：
  - 定义一条 ACL 规则，允许 VPN 流量进入指定目标网段。

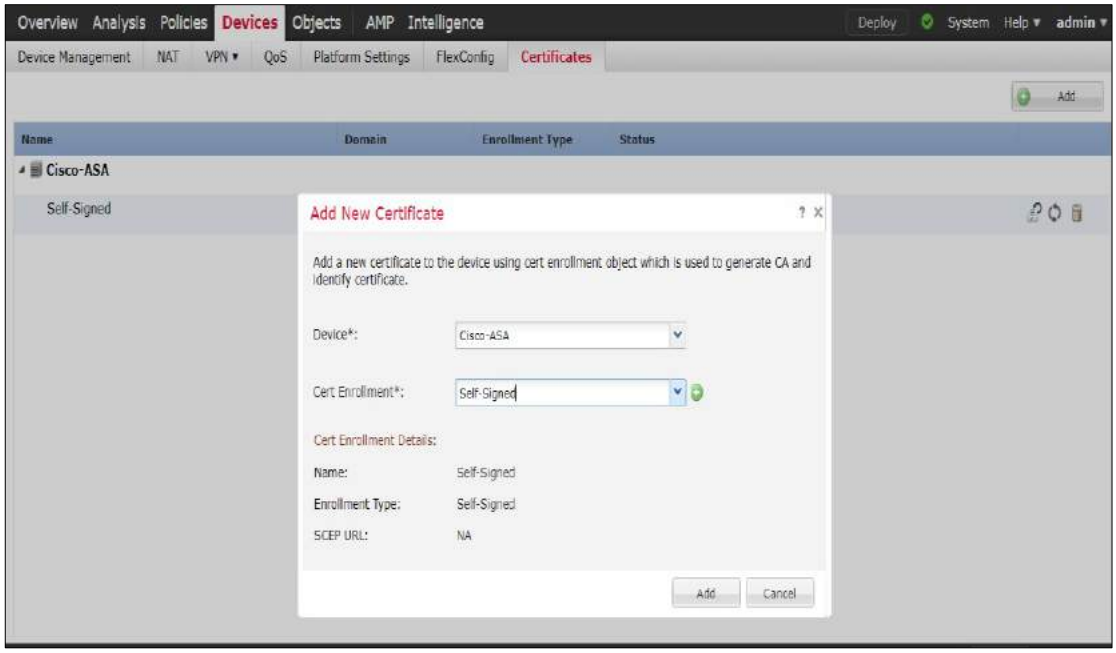
    例如，下图和下表为一条具体的 ACL 规则信息，该规则允许 VPN 流量通过远程桌面端口 3389 从外部传输到过程控制系统中的几个内部服务器。



	源	目的	设置
域	外部	内部	
网络	VPN_Pool（网络）	HMI 服务器（主机）和工作站（主机）	
端口	所有	TCP 3389端口	
动作			放行
检视			启用。选择“均衡的安全连接”。

- 添加设备证书。

  - 将先前创建的自签名证书或外部证书与防火墙设备相关联。



- 新建一条 NAT 豁免规则：

  - 定义一条 NAT 规则，豁免 VPN 流量（假设防火墙上已启用 NAT）。

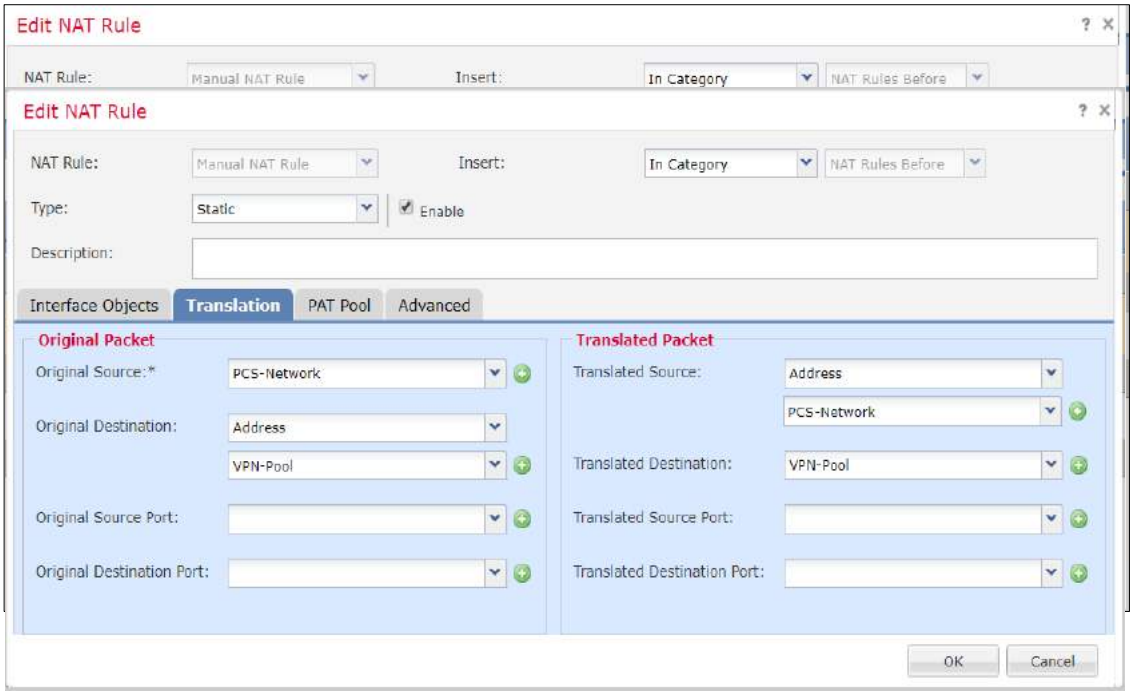
  - 选择 **Devices > NAT** （设备 > NAT）,单击【**NAT Policy**】（NAT 策略），新建规则。

  - 添加源、目标接口目标。

  - 在【**Translation**】（转换）页签，根据实际环境配置参数。

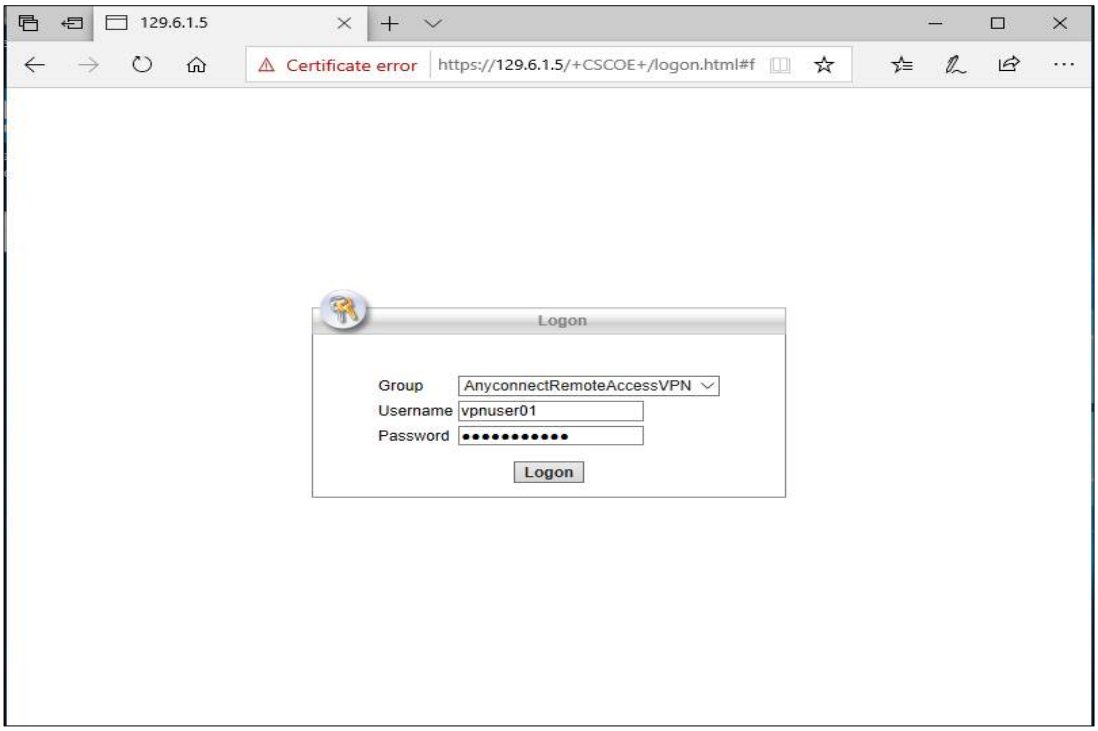
  - 在【**Advanced**】（高级）页签，选择【**Do not proxy ARP on Destination Interface**】（不对目标接口代理 ARP）。

下图显示了新建的 NAT 规则，该规则对 VPN 流量进行了豁免

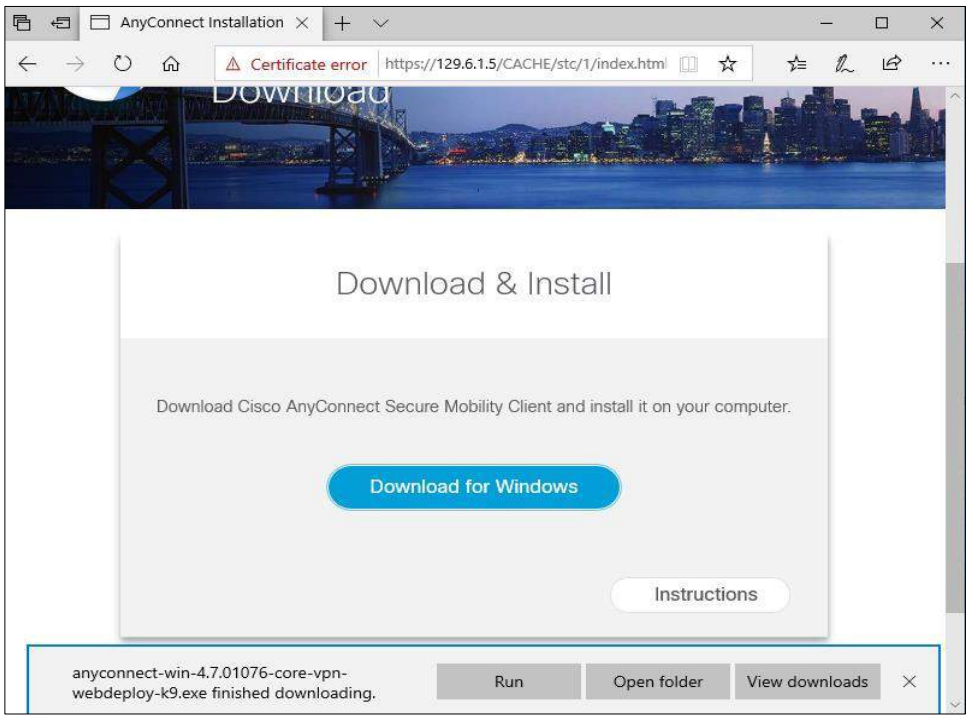


客户端连接

- 安装 VPN 软件（若为新安装的 Windows 客户系统）：
  - 打开 Web 浏览器，输入防火墙外部接口的 IP 地址。
  - 在登录界面，输入活动目录用户凭证。

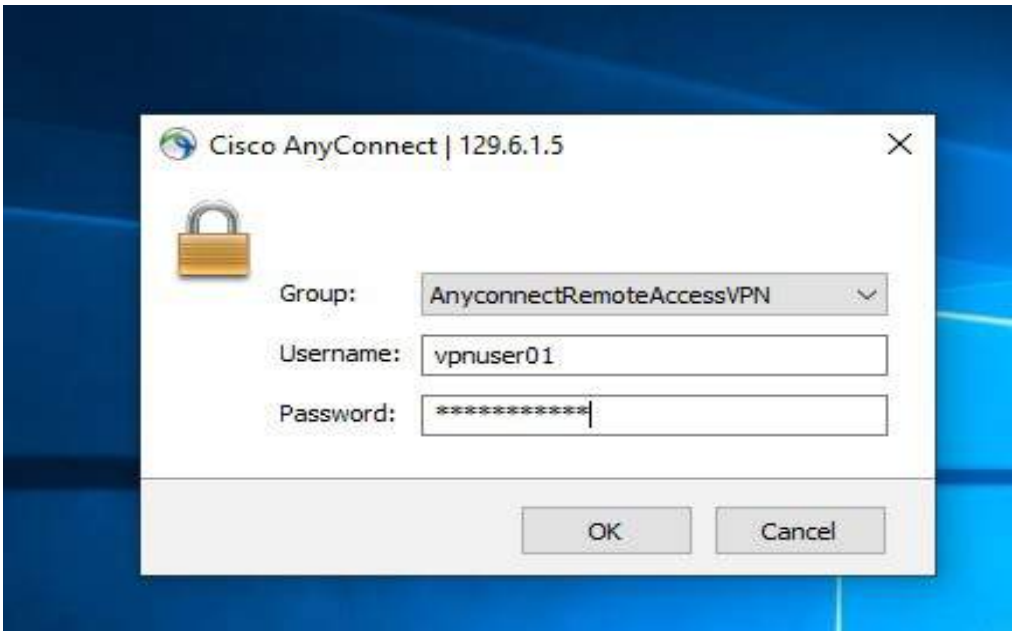


- 下载 AnyConnect 客户端软件，运行.exe 文件，安装软件。

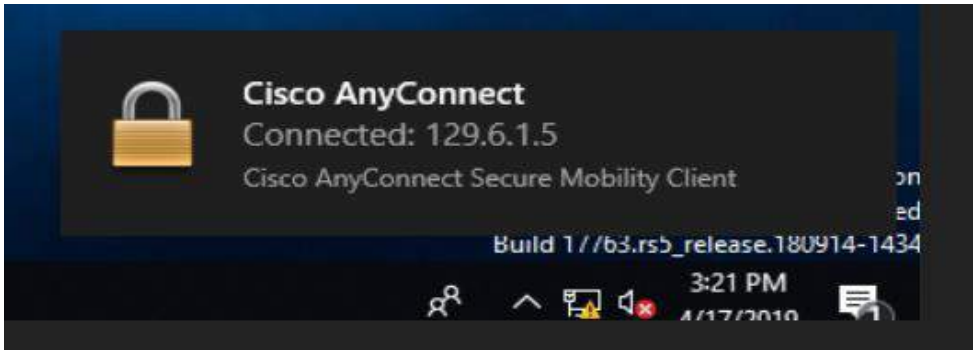


- 双击系统托盘里的思科 AnyConnect VPN 图标，启动软件。点击**【Connect】**（连接）。
- 若和本实验一样使用的是自签名证书，会出现“不受信任证书”警告，此时，单击**【Connect Anyway】**（仍然连接）。说明：使用公共 CA 证书时不会弹出此警告消息。

- 输入活动目录用户凭证。

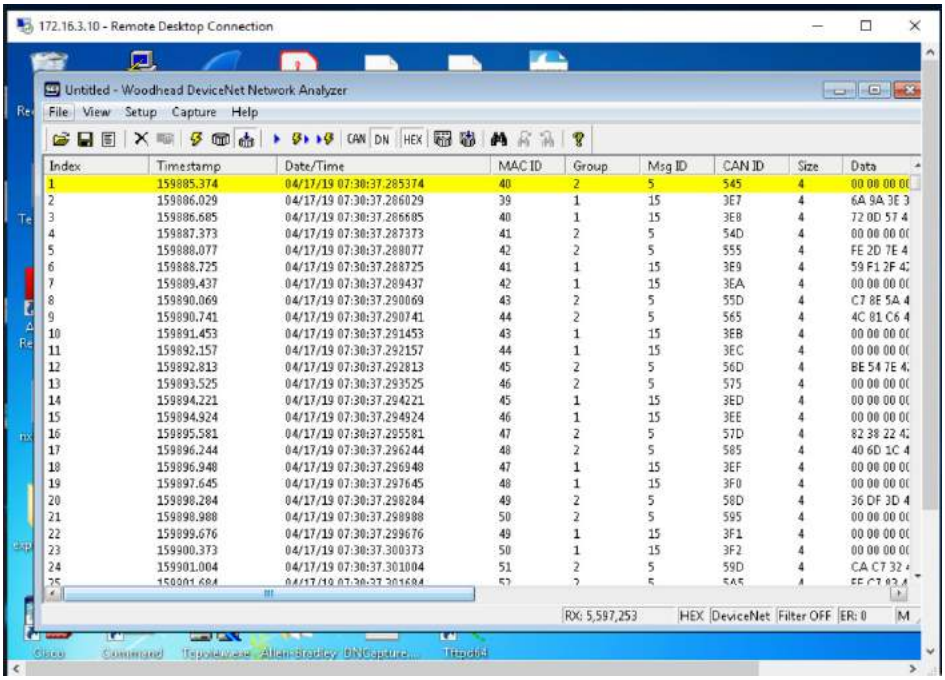


- 留意是否有弹出消息提示客户端已连接。



- 登录到主机，该主机须包含在之前设置的 ACL 规则中。

  例如，建立连接时，使用 RDP 访问 ACL 规则中放行的两个进程控制系统服务器，进行远程维护。



其他信息

思科 AnyConnect VPN[83]

思科 ASA VPN 用户认证[84]

4.8.6 对性能的主要影响

在下面的实验中，我们测量了制造系统正常运行时思科 AnyConnect VPN 工具对系统性能的影响：

实验 PL012.1 – 从实验环境局域网连接 VPN

实验中，远程用户通过 VPN 连接从远程计算机访问 HMI。远程计算机首先通过 VPN 连接到实验环境局域网，然后使用远程桌面连接到 HMI 计算机以访问 HMI 屏幕。

虽然由于远程桌面会话，实验环境局域网和 PCS 系统之间的网络流量略有增加，但在 PCS 系统中没有观察到对性能有显著影响。无论有无 VPN 连接，HMI 和 OPC 之间的报文往返时间基本保持恒定。

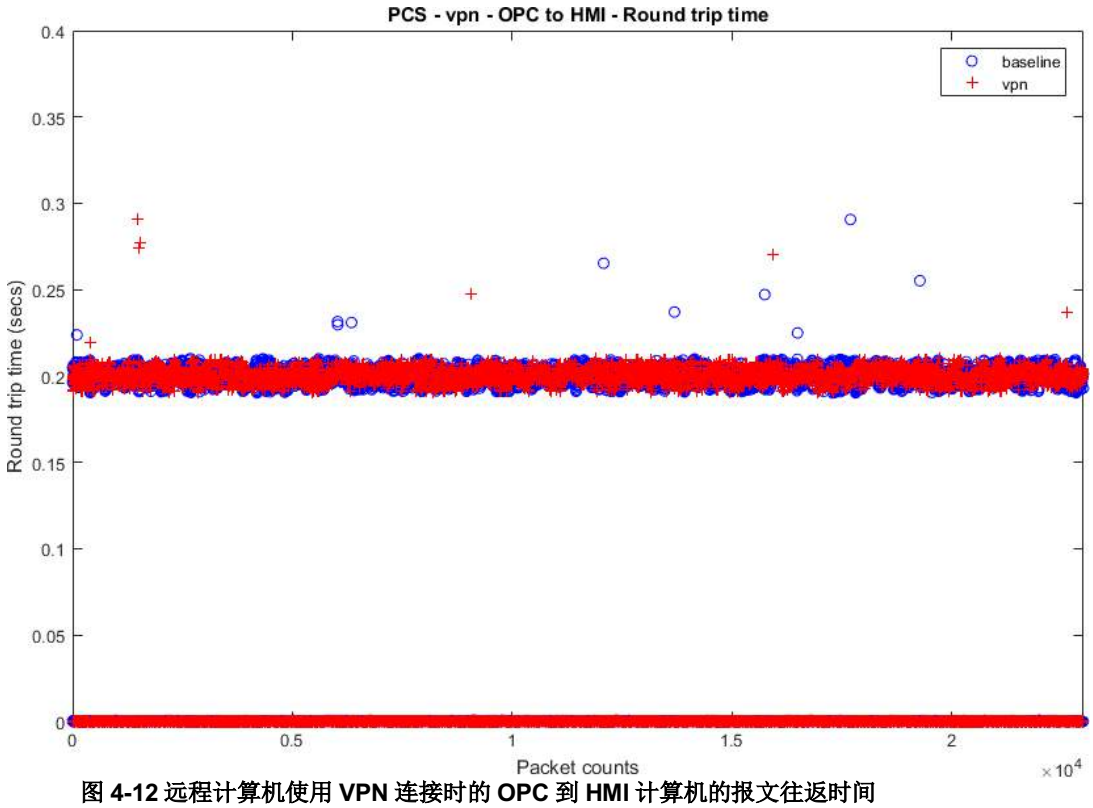


图 4-12 远程计算机使用 VPN 连接时的 OPC 到 HMI 计算机的报文往返时间

[83] https://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/at_a_glance_c45-578609.pdf

[84] https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/117641-config-asa-00.html

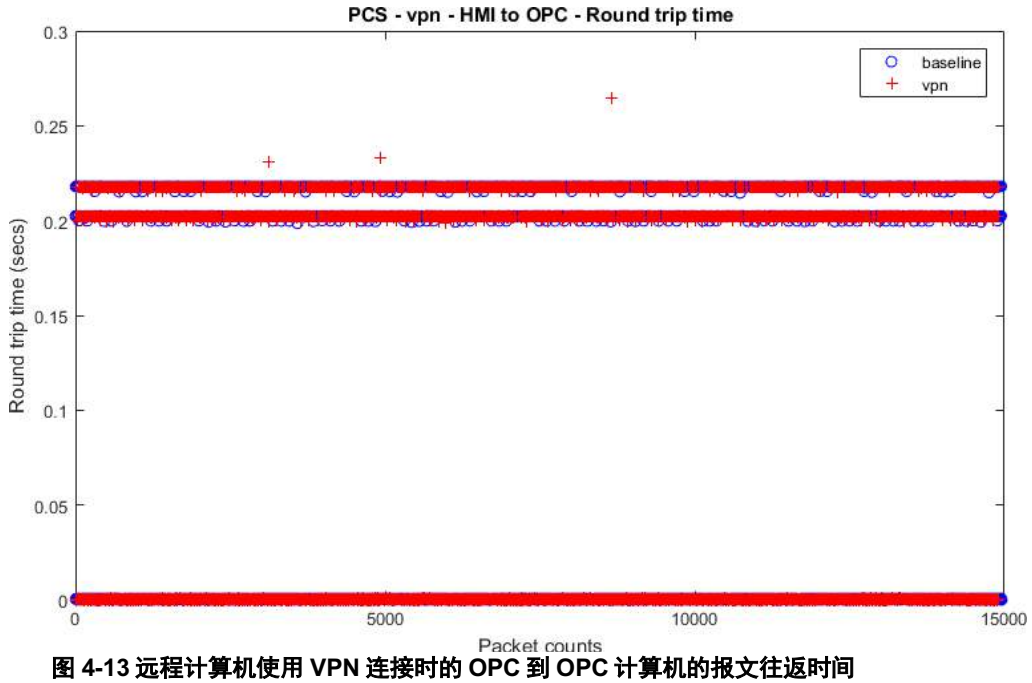


图 4-13 远程计算机使用 VPN 连接时的 OPC 到 OPC 计算机的报文往返时间

生产过程也保持稳定，没有观察到任何显著的性能影响。无论有无 VPN 连接，反应器压强和产品流速都保持不变。

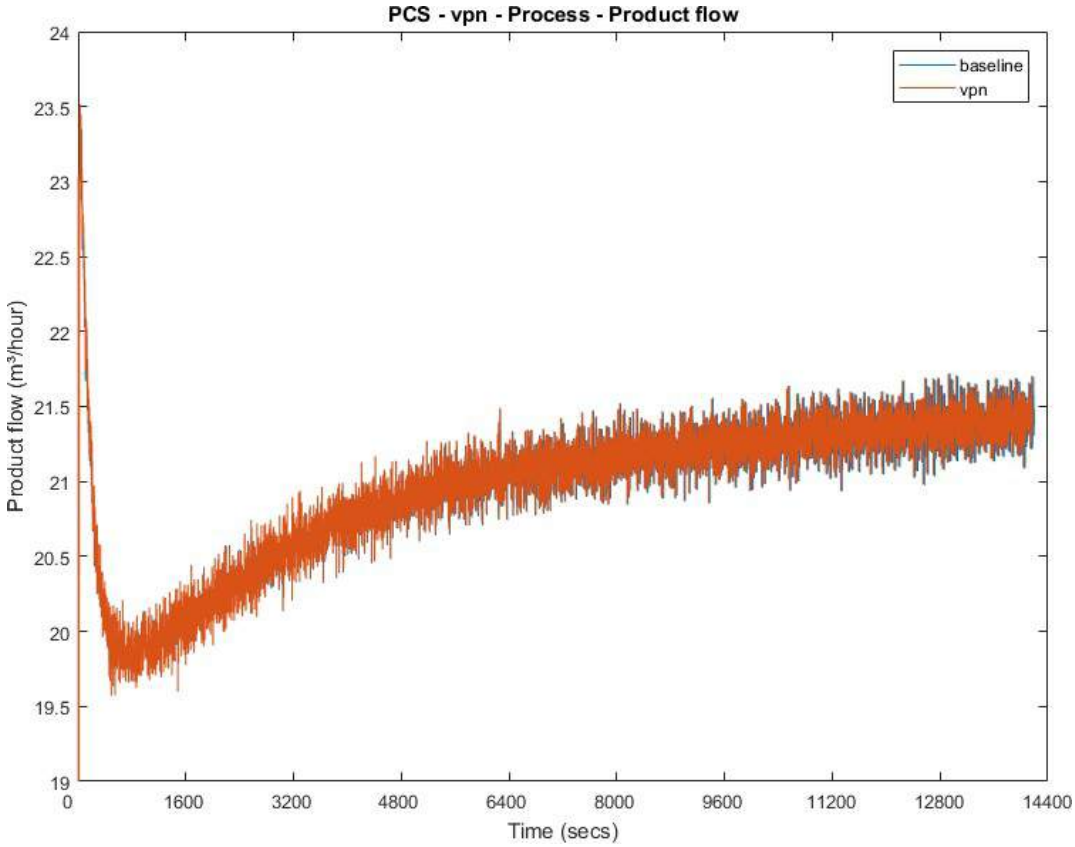


图 4-14 远程计算机使用 VPN 连接时生产过程中的产品流速

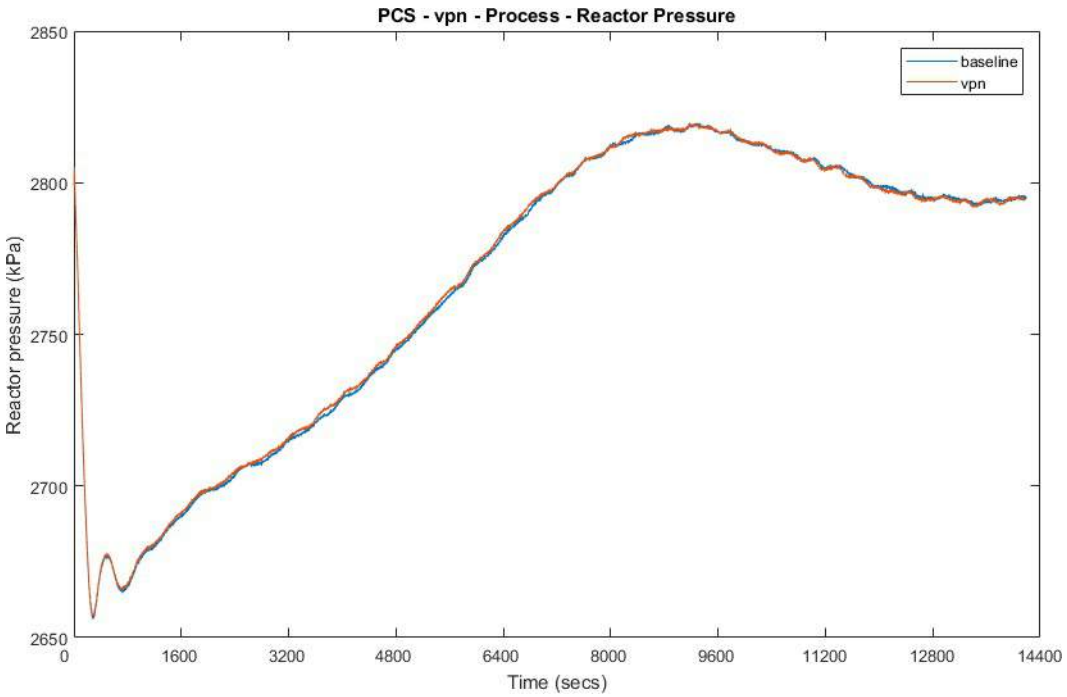


图 4-15 远程计算机使用 VPN 连接时生产过程中的反应器压强

4.8.7 性能测量数据集的相关链接

- 思科 VPN KPI 数据
- 思科 VPN 测量数据

4.9 微软活动目录

4.9.1 技术方案概述

活动目录（AD）是微软是为 Windows 域网络开发的目录服务。目录是一种层级结构，用于存储网络上对象的信息。目录服务（例如 AD 域服务（AD DS））提供目录数据存储方法，将数据提供给网络用户和管理员使用。例如，AD DS 存储用户名、密码和电话号码等用户帐户信息，允许同一网络上的其他授权用户访问此信息。运行 AD DS 的服务器称为域控制器。域控制器对 Windows 域类型网络中的所有用户和计算机进行身份认证和授权，为所有计算机分配、实施网络安全策略并安装、更新软件。活动目录利用轻型目录访问协议（LDAP）第 2 版和第 3 版以及微软版的 Kerberos 和 DNS[85]。

重点说明：

- 架构成本会很高。
- 配置和维护需要有专业技术，且配置需要进行详细规划。
- 容易遭受黑客攻击。

4.9.2 方案提供的技术能力

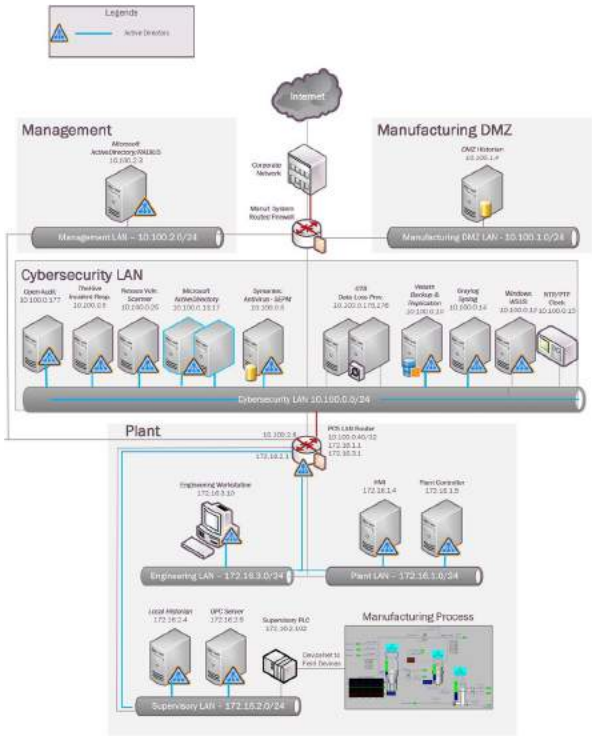
微软活动目录提供以下技术能力（参见第 1 卷第 6 章）：

- 凭证管理
- 认证授权

4.9.3 方案实现的子类

PR.AC-1、PR.MA-1、PR.MA-2、PR-PT-3、PR.PT-4 和 DE.CM-3

4.9.4 方案实施架构图



[85] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services- overview

4.9.5 安装说明与配置

环境信息如下：

主机名	角色	域名	硬件规格
LAN-AD	活动目录、DNS 服务器	LAN.lab	Hyper-V虚拟机（第2代） • 处理器：虚拟双核 • 内存：6 GB • 磁盘空间：70 GB • 网络：1个网络适配器 • 操作系统：Windows 2012 R2
LAN-AD02	活动目录、DNS 服务器	LAN.lab	Hyper-V虚拟机（第二代）： • 处理器：2 virtual cores虚拟双核 • 内存：6 GB • 磁盘空间：70 GB • 网络：1个网络适配器 • 操作系统：Windows 2012 R2
Mgmt-AD	活动目录、DNS、网络策略服务器（Radius）	Mgmt.lab	Hyper-V虚拟机（第2代）： • 处理器：虚拟双核 • 内存：4 GB • 磁盘空间：40 GB • 网络：1个网络适配器 • 操作系统：Windows 2012 R2

环境搭建

我们需为两个网络搭建独立的 AD 域环境：网络安全局域网和管理网络。出于安全考虑，将网络安全局域网中的 AD 域与管理网络中的域进行隔离。管理网络中的域控制器安装了 Windows NPS（Radius）服务对网络设备进行认证。

- 在网络安全局域网的 Hyper-V 宿主服务器上配置两个运行 Windows 2012 R2 的虚拟机，对 Windows/Linux 设备进行认证。详细硬件规格见上表。
- 管理网络中配置的运行 Windows 2012 R2 的虚拟机对 VPN 用户和边界路由器等网络设备进行认证。
- 这些服务器上的客户机操作系统的 IP 信息如下所示：

  - 主机名：LAN-AD.lan.lab

  - IP 地址：10.100.0.5

  - 网关：10.100.0.1

  - 子网掩码：255.255.255.0

  - 域名服务器：127.0.0.1, 10.100.0.13

  - 主机名：LAN-AD02.lan.lab

  - IP 地址：10.100.0.13

  - 网关：10.100.0.1

- 子网掩码：255.255.255.0
- 域名服务器：10.100.0.17, 127.0.0.1

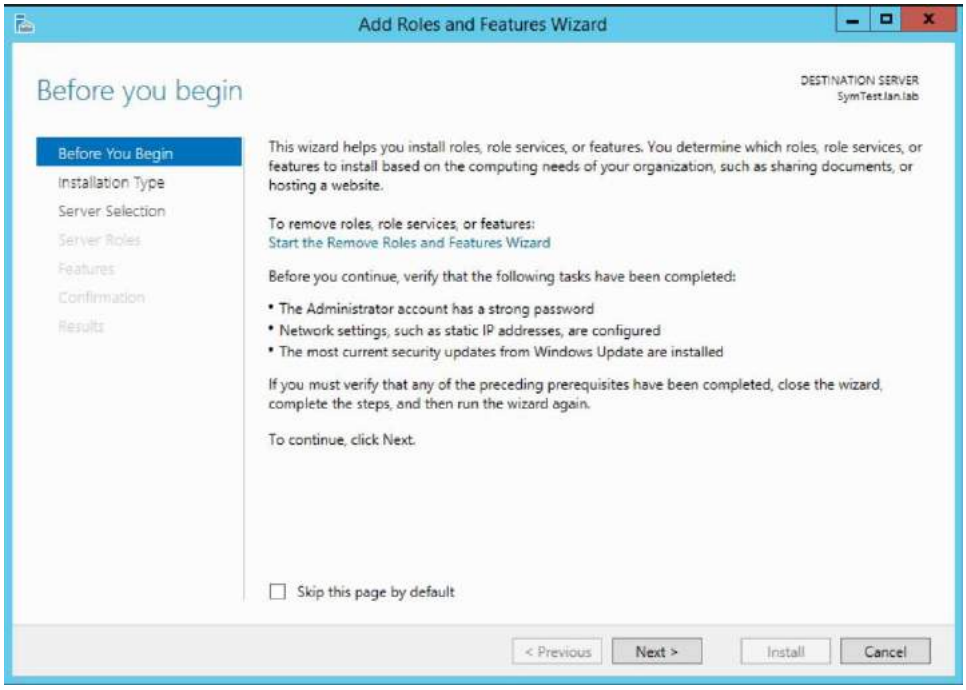
- 主机名：Mgmt-AD.mgmt.lab
- IP 地址：10.100.2.3
- 网关：10.100.2.1
- 子网掩码：255.255.255.0
- 域名服务器：127.0.0.1

安装 AD 域服务和 DNS 服务器

安装准备

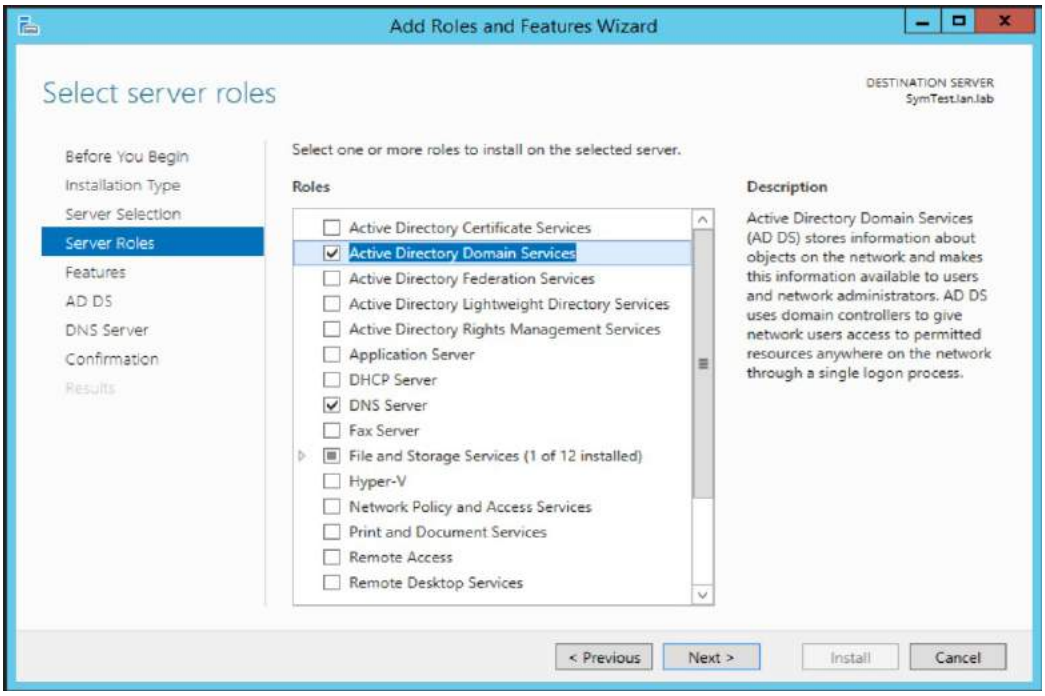
准备 Windows 2012 R2 server（最好准备两台进行冗余备份），安装最新补丁，为 DNS 主服务器配置静态 IP 地址 127.0.0.1（localhost）。

- 启动 Windows 服务器管理器，单击【**Add Roles and Features**】（添加角色和功能）。
- 在首页单击【**Next**】（下一步），如下图所示。



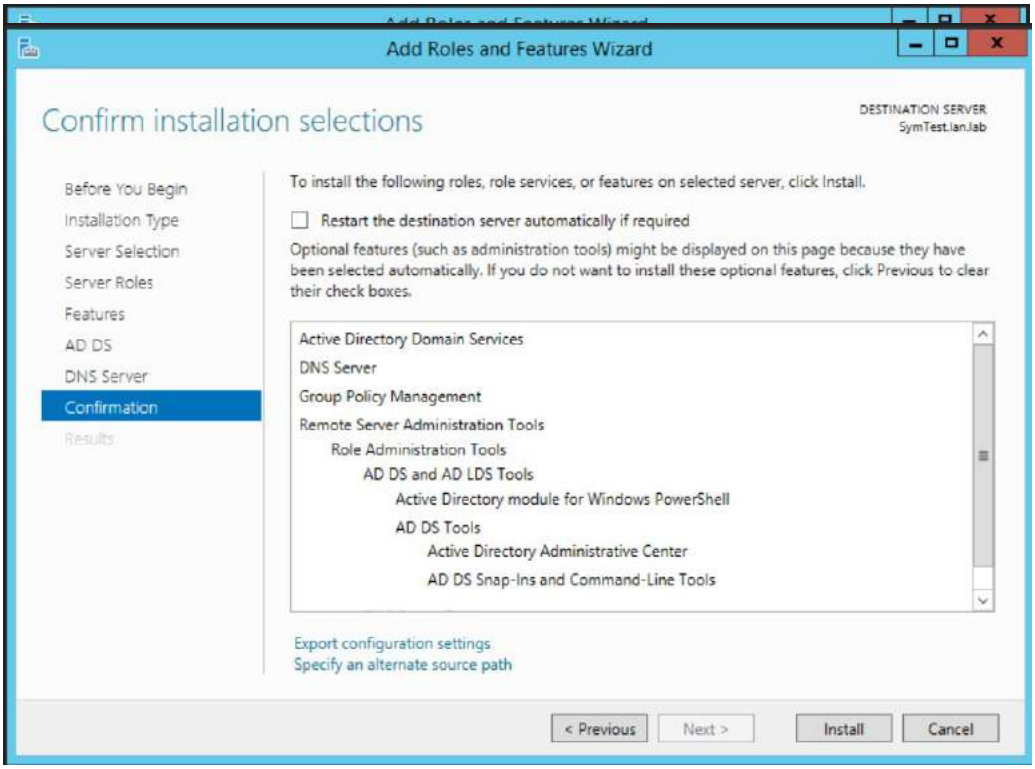
- 进入【**Installation Type**】（安装类型）页面，选择【**Role Based or Feature Based Installation**】（基于角色或基于功能的安装）。

- 选择安装【**Active Directory Domain Services**】（活动目录域服务）和【**DNS Server**】（DNS 服务器），单击【**Next**】（下一步）。

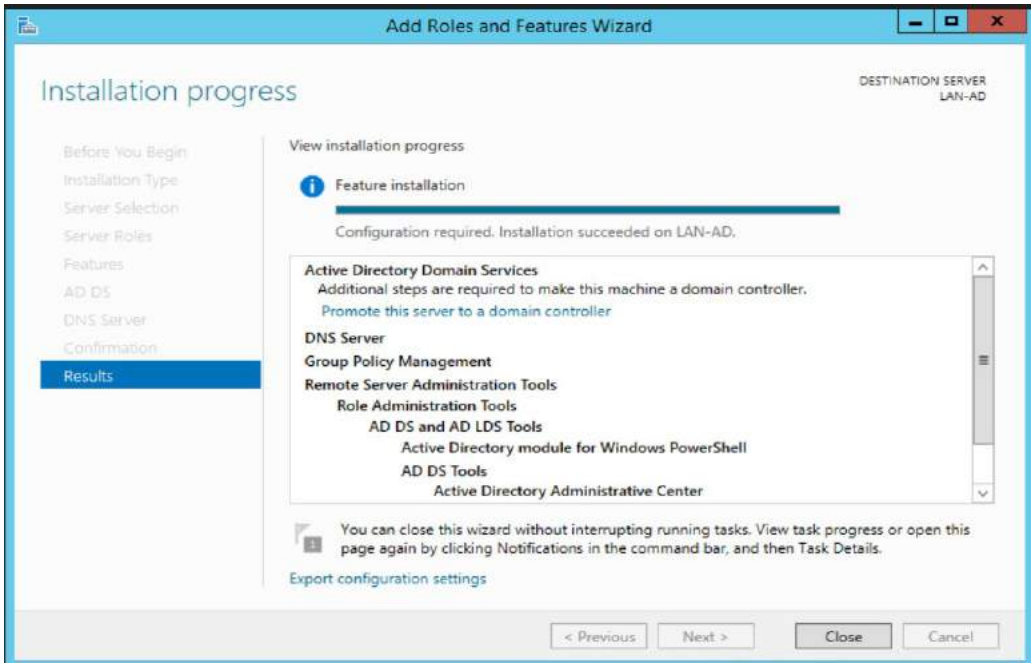


- 进入【**Features**】（功能）页面，单击【**Next**】（下一步），保持默认设置。

- 在【**AD DS**】页面和【**DNS Server**】（DNS 服务器）页面，分别单击【**Next**】（下一步）。

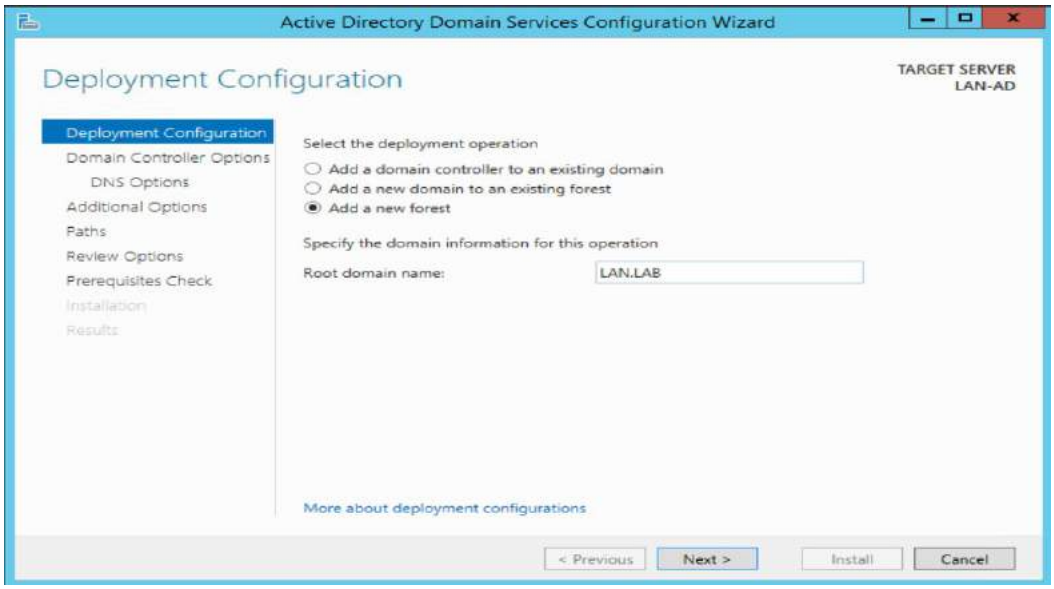


- 进入【**Confirmation**】（确认）页面，对设置进行确认，单击【**Install**】（安装），开始安装。
- 等待安装完成。界面提示“Installation succeeded”（安装成功）时，单击【**Close**】（关闭）按钮。

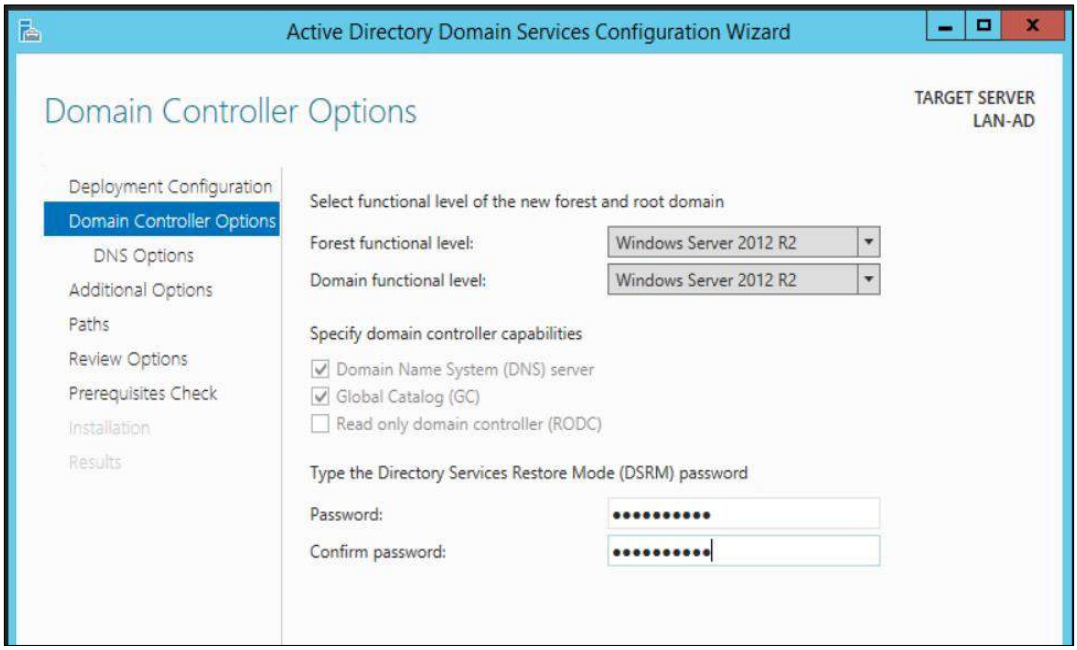


- 再次启动 Server Manager，单击【**Promote this server to a domain controller**】（将此服务器提升为域控制器）。

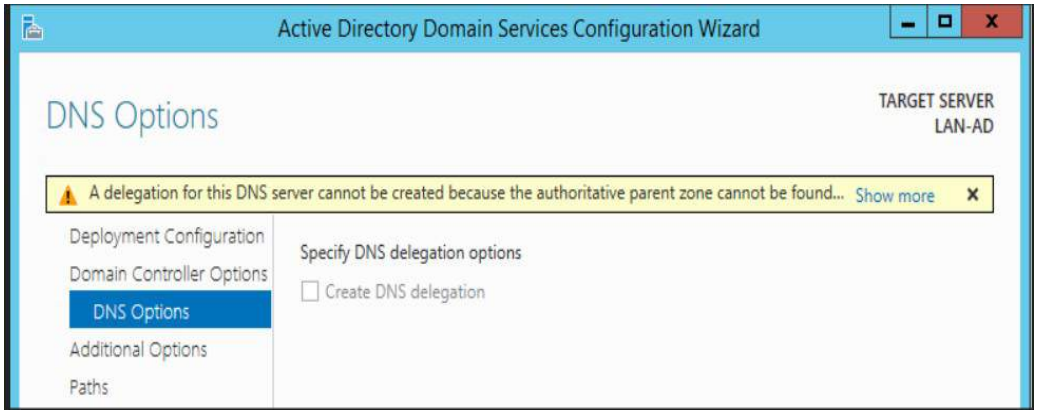
- 鉴于该服务器要加入新林，在【**Deployment Configuration**】（部署配置）步骤中选择【**Add a new forest**】（添加新林）。根据实际环境，设置【**Root Domain name**】（根域名）。



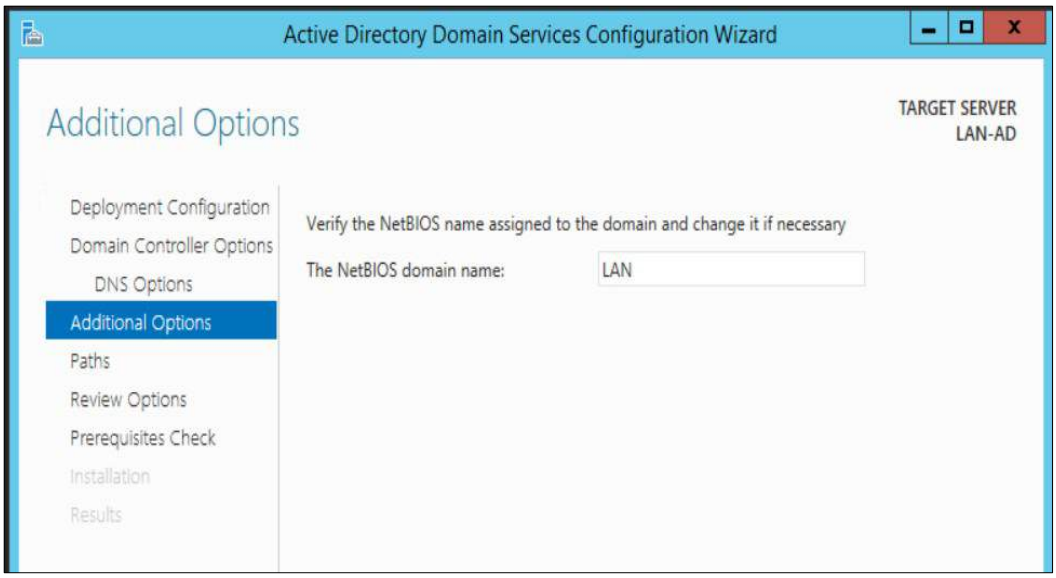
- 在下一步中设置 **Directory Services Restore Mode**（目录服务还原模式）密码，单击【**Next**】（下一步）。



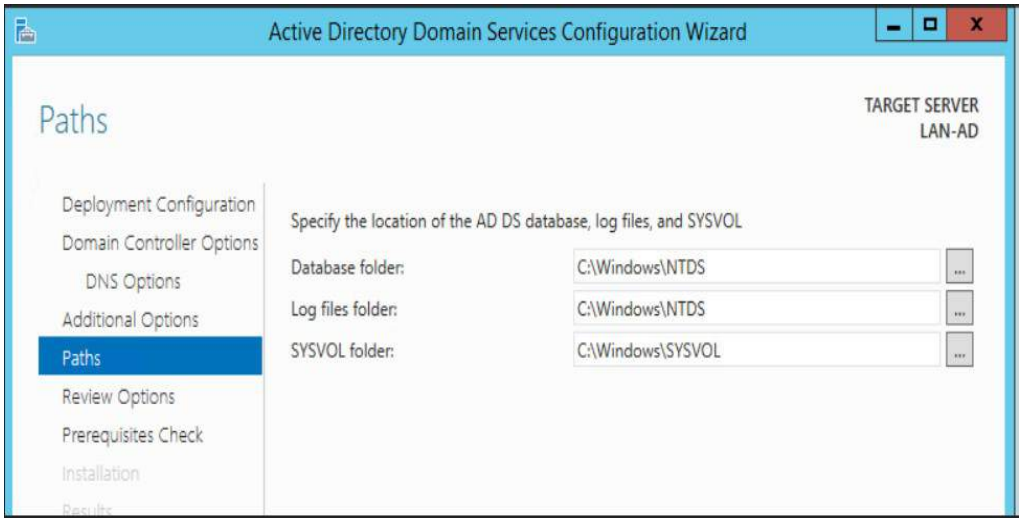
- 在【**DNS Option**】（DNS 选项）页面，保持默认设置，单击【**Next**】（下一步）。



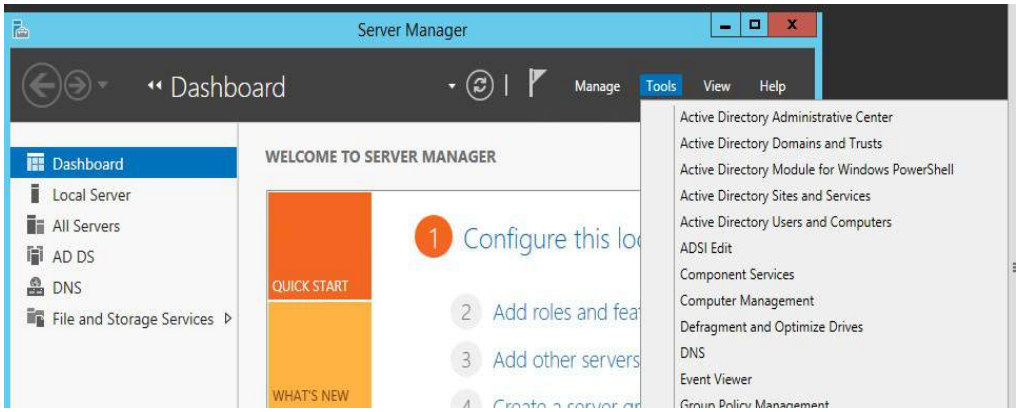
- 在【**Additional Options**】（其他选项）页面，确认 NETBIOS 域名，单击【**Next**】（下一步）。



- 在【**Paths**】（路径）页面，保持默认文件夹路径，单击【**Next**】（下一步）。



- 在【**Review Options**】（查看选项）页面，确认所有设置，单击【**Next**】（下一步）。
- 在【**Prerequisites Check**】（必备项检查）页面，单击【**Install**】（安装），启动安装程序。安装完毕，服务器会自动重启。
- 重启后，使用域管理员凭证登录。打开服务器管理器，选择界面右上角的【**Tools**】（工具）菜单，单击【**Active Directory Users and Computers**】（活动目录用户和计算机），对活动目录进行管理。



将 Windows 系统加入活动目录域

- 对所有客户端系统上的 DNS 设置进行修改，使其指向域控制器服务器的 IP 地址。
- 参考说明文档[86]，将 Windows 客户端加入活动目录域。
- 操作完毕，重启客户端系统。

Matrikon OPC 服务器的 DCOM 配置

工厂中运行 Matrikon OPC 服务器程序的 OPC 服务器需进行高级配置才能与活动目录互动。微软分布式组件对象模型（DCOM）服务在 OPC 服务器和活动目录之间的联动过程中起关键作用。使用活动目录时正确配置 DCOM 对于工厂运营至关重要。我们按照 Matrikon OPC 指南[87]中的步骤对所需的 DCOM 配置进行了应用。

安装准备

- 对于加入活动目录的 Windows 系统，需将其域名添加到 AD 服务器。
- 所有系统的时间务必与 AD 服务器同步，确认各服务器时间与活动目录（域控制器）一致。时间同步非常重要。
- 确保所有 OPC 客户端和 OPC 服务器之间的 TCP 端口 135 为开启状态。下表列举了 OPC 配置中所涉及的系统：

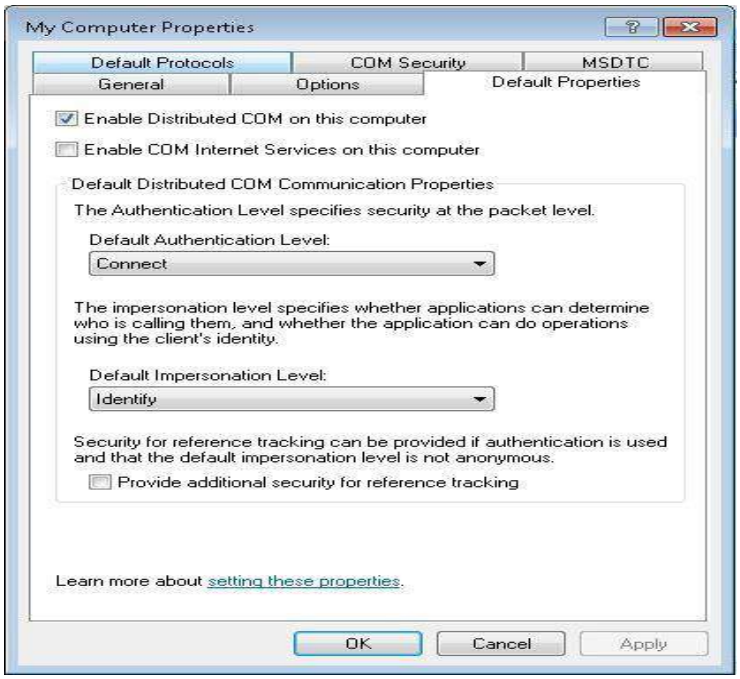
主机名	IP地址	角色	管理员
OPC服务器	172.16.2.5	OPC服务器	opcadmin
控制器	172.16.1.5	OPC服务器+客户端	opcadmin

[86] https://www.petri.com/join-a-domain-in-windows-7
[87] https://www.matrikonopc.com/downloads/1128/whitepapers/index.aspx

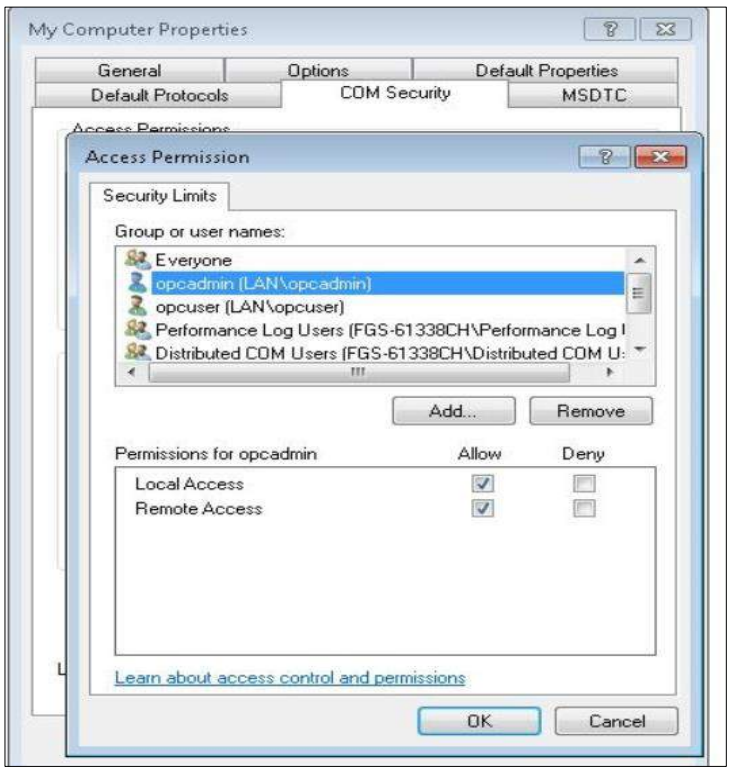
- 在 AD 中添加两个域用户。为其中一个用户账户分配 OPC 服务器的管理权限。例如，在我们的 AD 中配置 opcadmin 和 opcuser 账户。
- 将 opcadmin 用户添加到 OPC 服务器和客户端的本地管理员组中。
- 在 OPC 客户端系统中，对 DCOM 属性进行如下修改：

a. 选择【**Control Panel > Administrative Tools > Component Services**】（控制面板 > 管理工具 > 组件服务）单元，打开DCOM控制台。另外，您还可运行**dcomcnfg**命令。

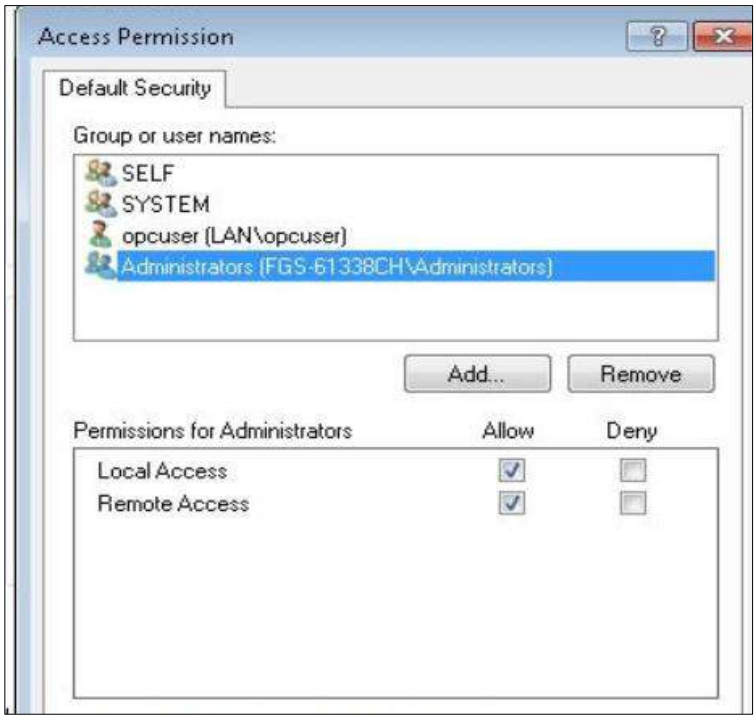
b. 选择**Console Root > Component Services > Computers**（控制台Root > 组件服务 > 计算机）。右击【**My Computer**】（我的电脑），选择【**Properties**】（属性）进行如下设置：



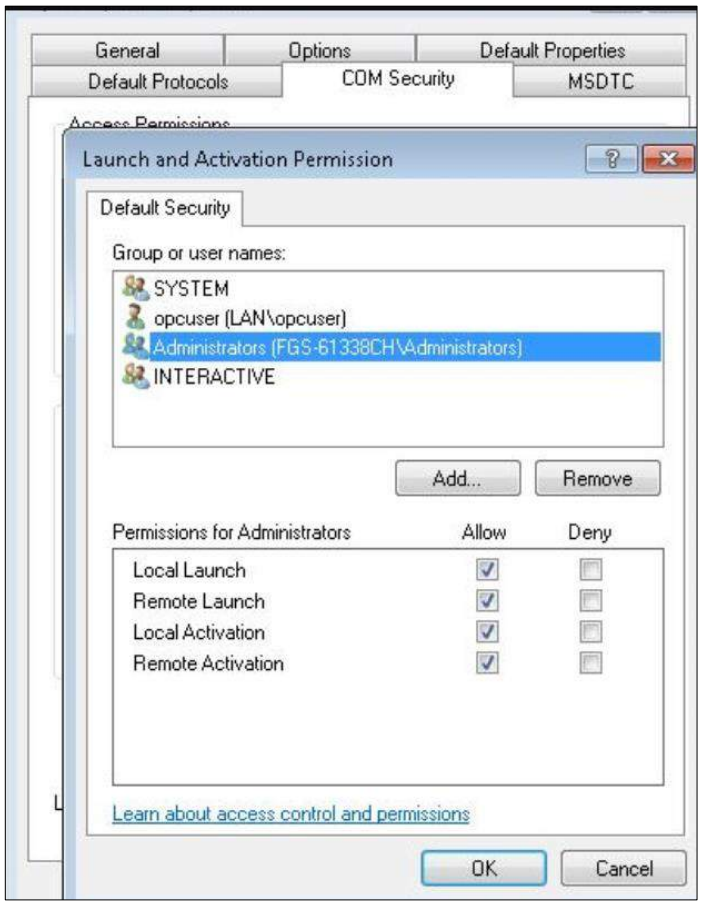
c. 单击【**COM Security**】（COM安全）页签。在【**Access Permissions**】（访问权限）区域中，单击【**Edit Limits**】（编辑限制），将opcadmin用户添加至列表。在【**Permissions for opcadmin**】（opcadmin权限）区域中，对【**Local Access**】（本地访问）和【**Remote Access**】（远程访问）勾选【**Allow**】（允许）。您也可根据需要添加opcuser用户，仅对【**Local Access**】（本地访问）勾选【**Allow**】（允许）。



d. 在【**Access Permissions**】（访问权限）区域中选择【**Edit Default**】（编辑默认设置）按钮，确保“<server-name>\Administrators”用户组具备所有权限。opcadmin用户已添加至管理员组。若添加opcuser用户，仅对【**Local Access**】（本地访问）勾选【**Allow**】（允许）。



在【**Launch and Activation Permissions**】（启动和激活权限）窗口，单击【**Edit Default**】（编辑默认设置）按钮，确保【**Administrators**】（管理员）组的四类权限均勾选了【**Allow**】（允许）。

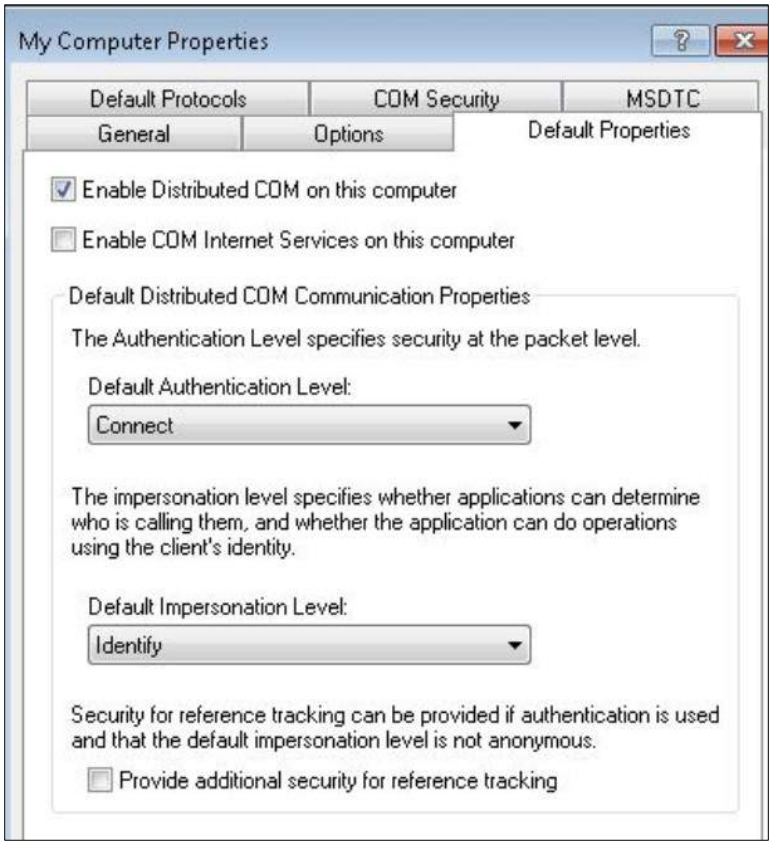


e. 配置后重启系统。在所有OPC客户端上执行以上步骤，完成DCOM属性配置。

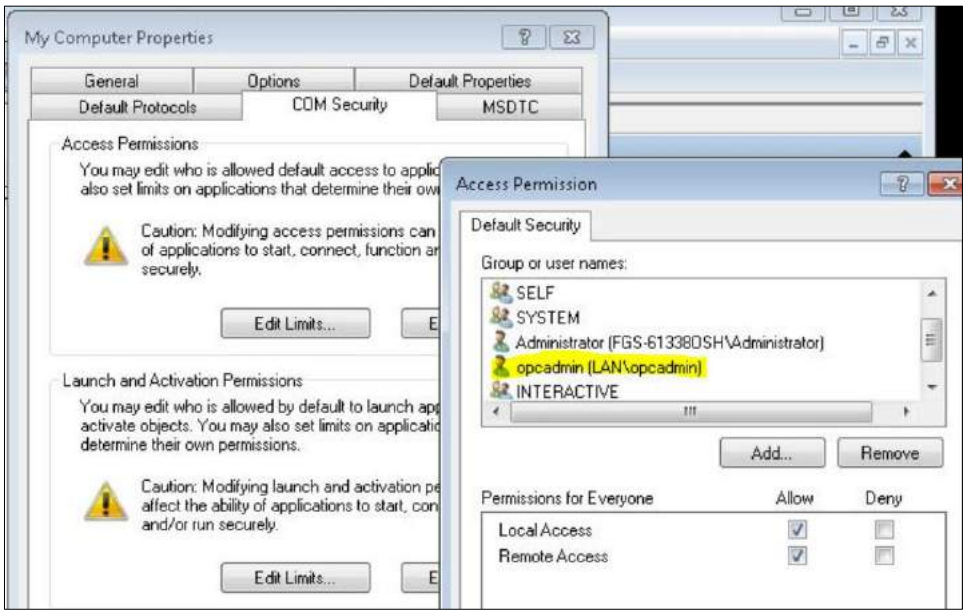
- 在 OPC 服务器系统中，对 DCOM 属性进行如下修改：

  a. 选择**Control Panel > Administrative Tools > Component Services**（控制面板 > 管理工具 > 组件服务管理单元），打开DCOM控制台。

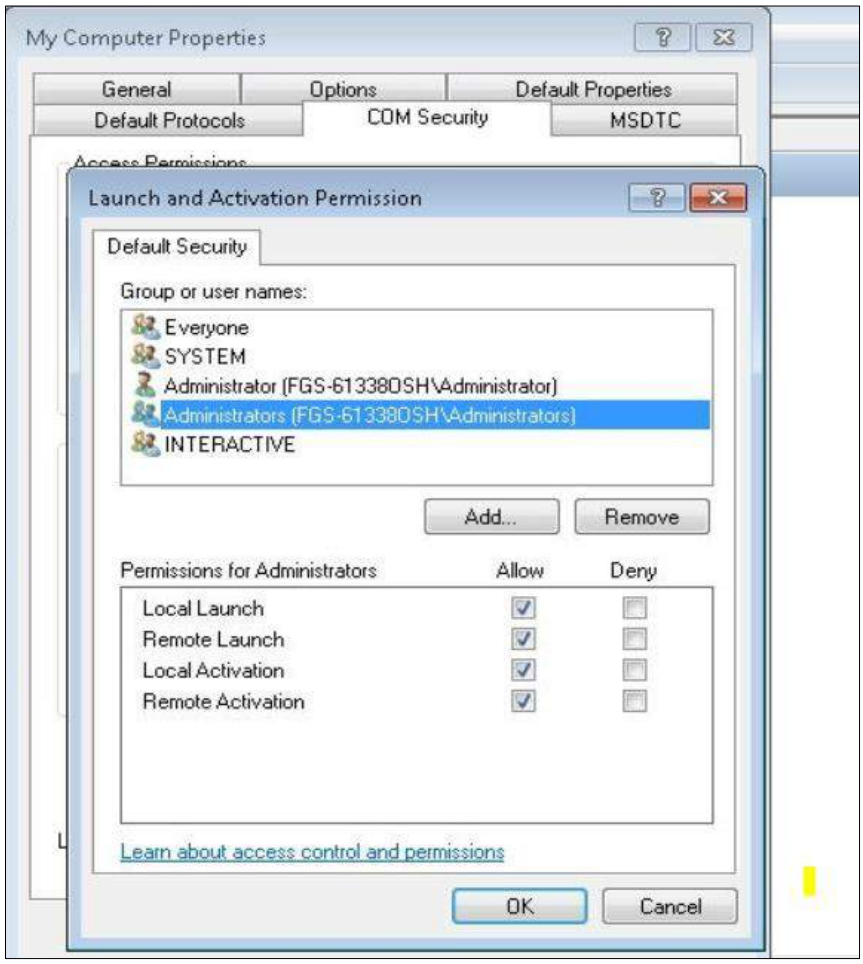
b. 选择**Console Root > Component Services > Computers**（控制台Root > 组件服务 > 计算机）。右击**【My Computer】**（我的电脑），选择**【Properties】**（属性），进行如下配置。



c. 单击**【COM Security】**（COM安全）页签，在**【Access Permissions】**（访问权限）区域下，单击**【Edit Default】**（编辑默认设置），添加opcadmin用户，对其**【Local Access】**（本地访问）和**【Remote Access】**（远程访问）两类权限勾选**【Allow】**（允许）。



d. 在【**Launch and Activation Permissions**】（启动和激活权限）窗口，添加【**Administrators**】（管理员）组。对该组的四类权限均勾选【**Allow**】（允许）。若添加opcuser用户，应仅为其分配【**Local Launch**】（本地启动）权限。



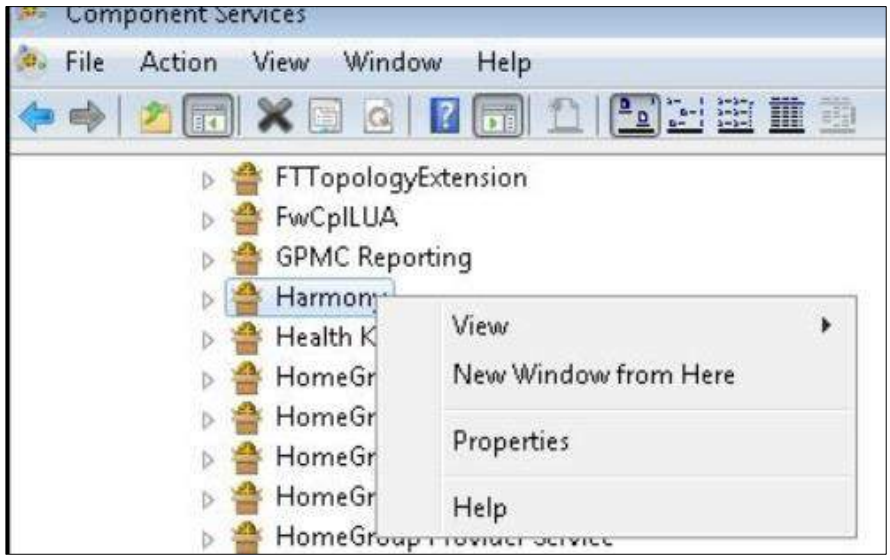
- 记录您环境中安装的 OPC 服务器软件的名称。在 OPC 系统的所有应用程序文件夹中进行 DCOM 配置修改。在我们的实验环境中涉及的软件如下所示：

  - Harmony（OPC 服务器上安装）
  - RSLINX（OPC 服务器上安装）
  - MATLAB（控制器上安装）

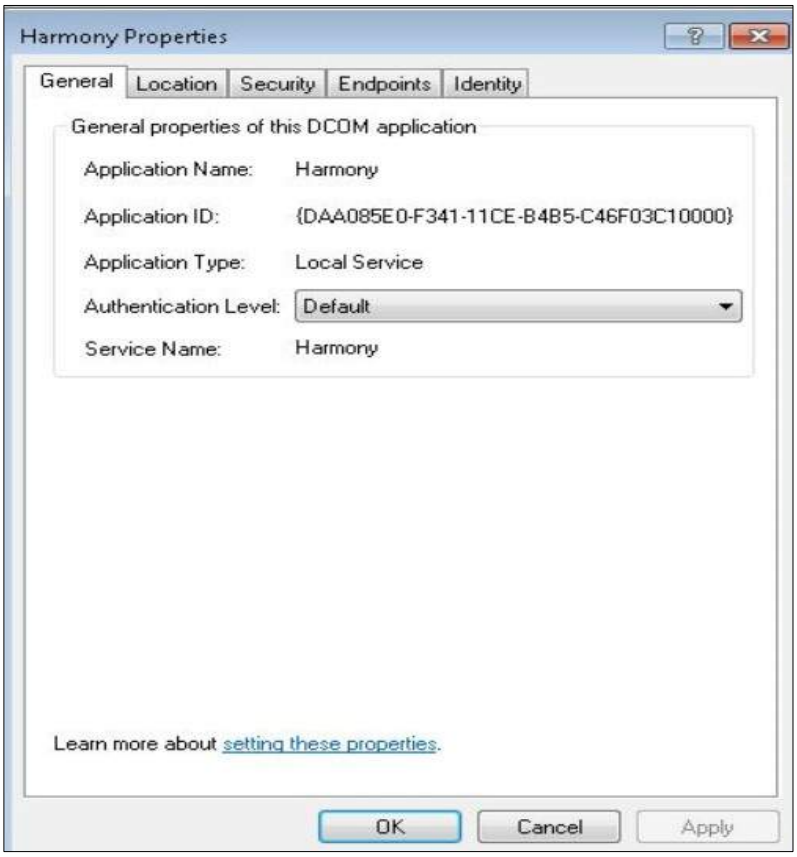
- 在 OPC 服务器和客户端系统的应用程序文件夹中进行如下修改：

a. 启动DCOM控制台。选择**Console Root > Component Services > Computers > My Computer > DCOM Config**（控制台Root > 组件服务 > 计算机 > 我的电脑 > DCOM配置）。

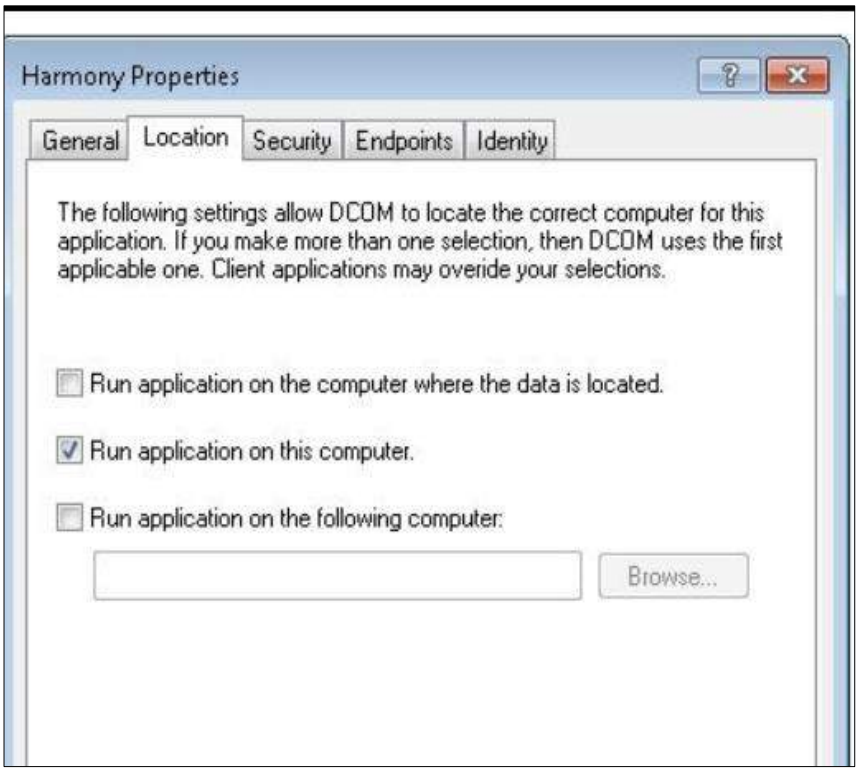
b. 在右侧面板的应用程序列表中，右击<应用程序文件夹>，选择**【Properties】**（属性）。例如，查找**“Harmony**”文件夹，右击该文件夹，选择**【Properties】**（属性）查看其属性。



c. 在【**General**】（常规）页面，将【**Authentication Level**】（认证级别）设置为【**Default**】（默认）。



d. 在【**Location**】（定位）页面，选择【**Run application on this computer**】（在该计算机上运行应用程序）。



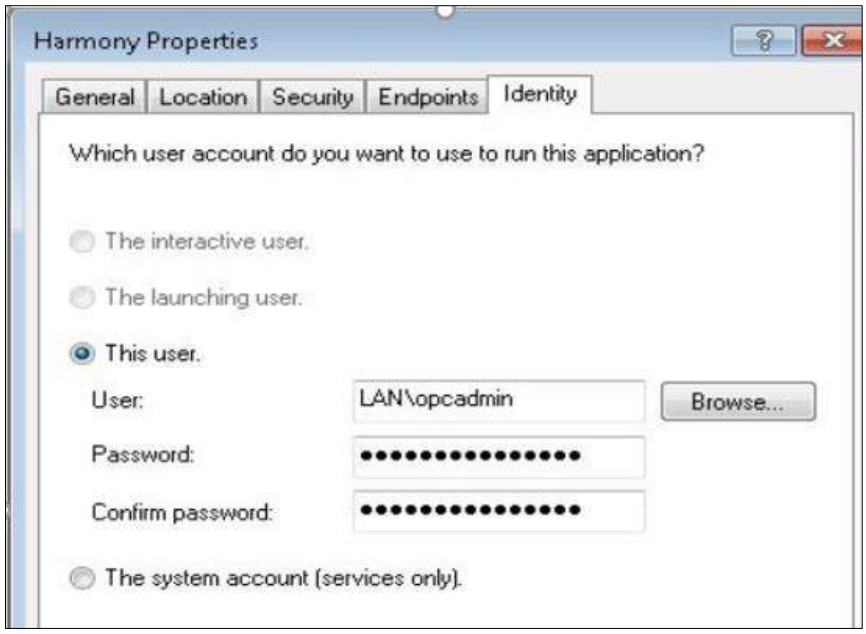
e. 在【**Security**】（安全）页面上，为opcadmin账户分配以下权限：

- 在【**Launch and Activation Permissions**】(启动和激活权限）区域，选择【**Use System Defaults**】（利用系统默认配置）。
- 在【**Access Permissions**】(访问权限)区域，选择【**Use System Defaults**】（使用系统默认配置）。
- 在【**Configuration Permissions**】（配置权限）区域，选择【**Customize**】（自定义）。下图为【**Full Control**】（完全控制）权限（注意：opcadmin 为 Administrators（管理员）组的成员）。

f. 在【**Security**】（安全）页面，对opcuser账户分配以下权限：

- 在【**Launch and Activation Permissions**】(启动和激活权限）区域，选择【**Use System Defaults**】（利用系统默认配置）。
- 在【**Access Permissions**】(访问权限)区域，选择【Use System Defaults】（使用系统默认配置）。
- Configuration Permissions：Allow Read 在【**Configuration Permissions**】（配置权限）区域，选择【**Allow Read**】（读取）。

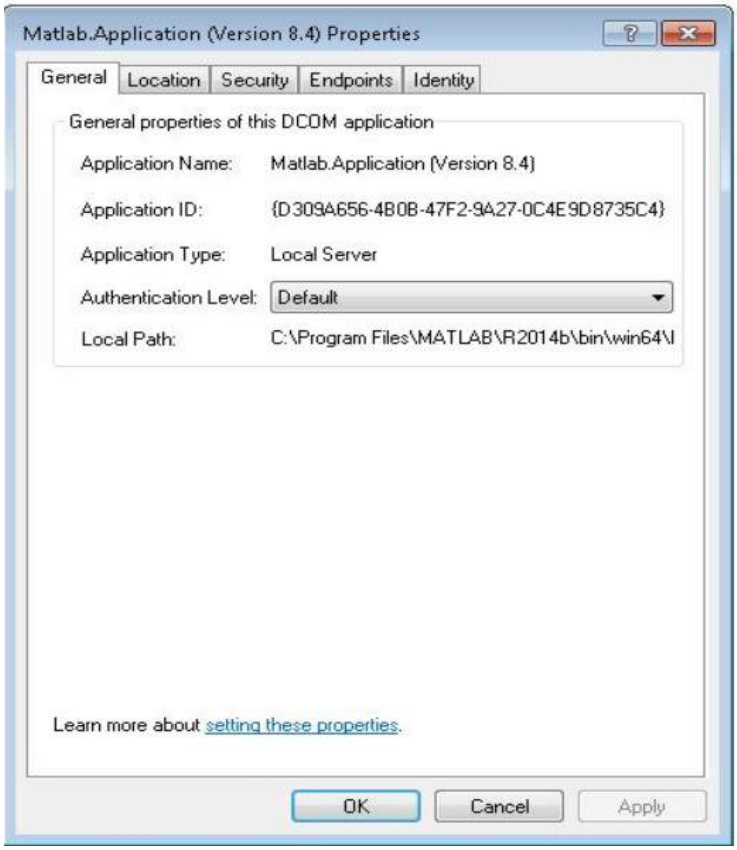
g. 在【**Identity**】（身份）页面上，选择【**This user**】（此用户）选项。输入AD管理员账户opcadmin的用户名和密码。单击【**OK**】（确定）保存设置。重启系统。

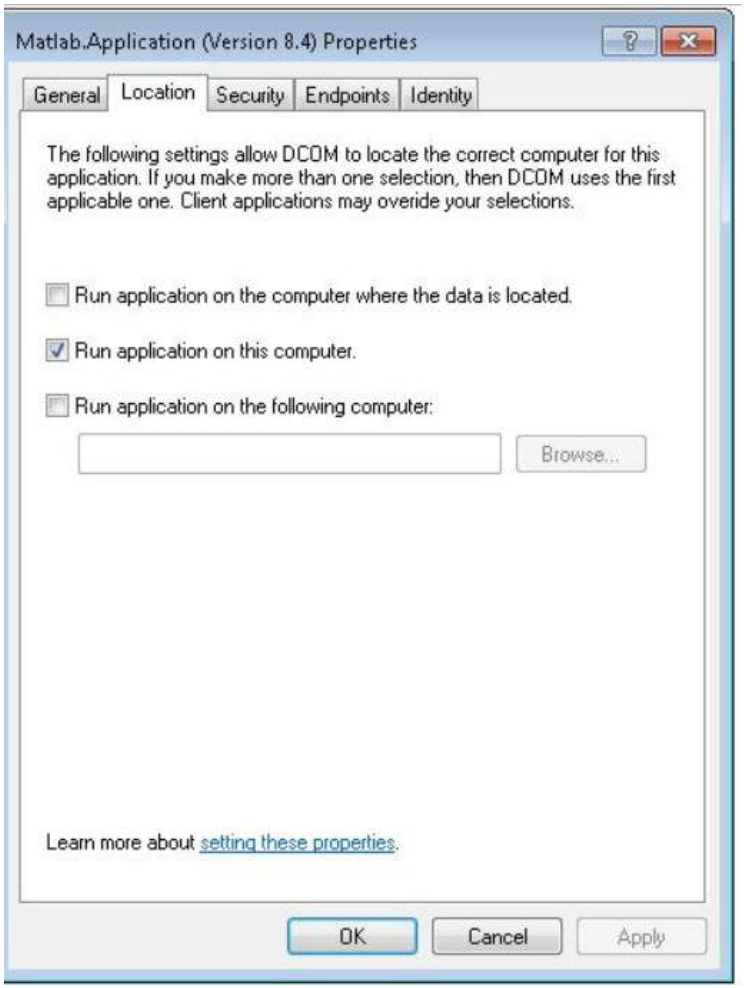


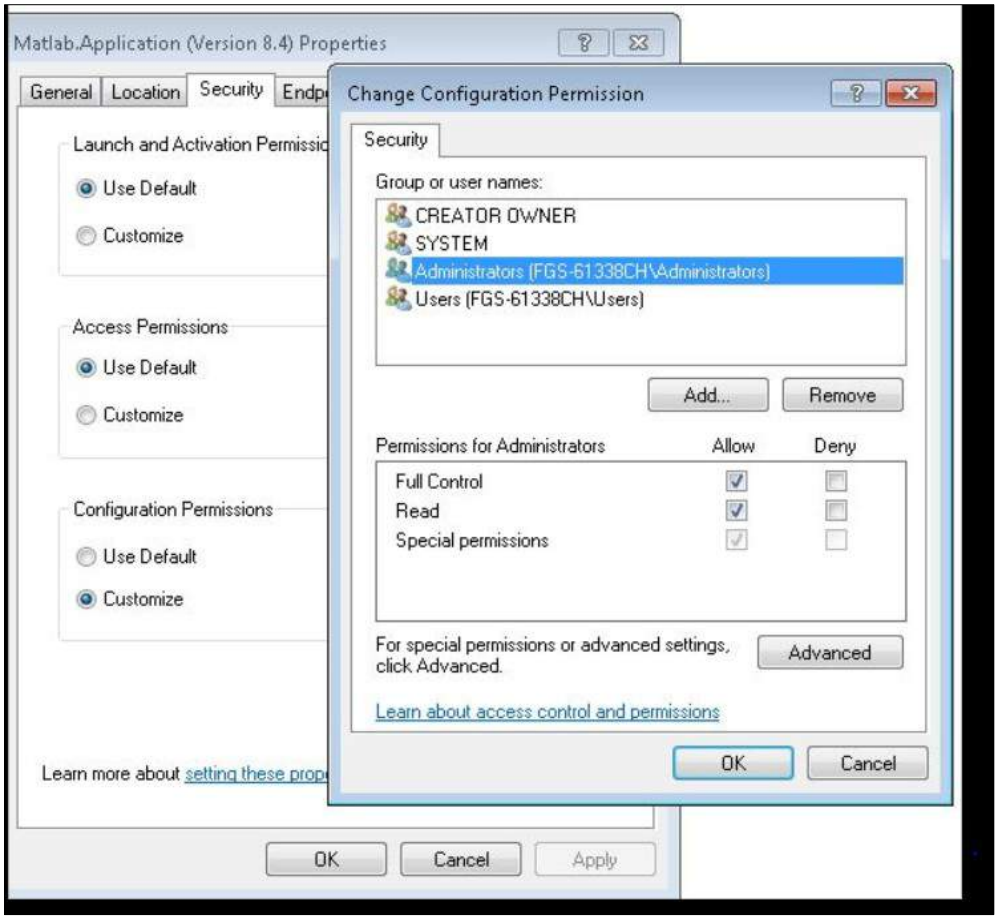
h. 对RSLINX和MATLAB等其他应用程序文件夹（本例中，这些文件夹存放在控制器服务器上）执行以上操作。

i. 操作完毕重启系统。

以下是 MATLAB 文件夹的一些截图供参考。







配置 Radius 服务器

为实现 VPN 用户认证和基于 AD 的网络设备认证配置，在管理局域网中配置 Windows 2012 R2 服务器运行活动目录和 Windows 网络策略服务器（NPS），对边界防火墙和 VPN 用户进行认证。

技术上，两种角色可在同一服务器上配置，但我们建议这两种角色单独配置，实现冗余备份。

管理网络中的 AD 服务器和域详情

主机名	IP地址	角色	域名
Mgmt-AD	10.100.2.3	活动目录、DNS、网络策略服务器（Radius）	Mgmt.lab

主要配置步骤如下：

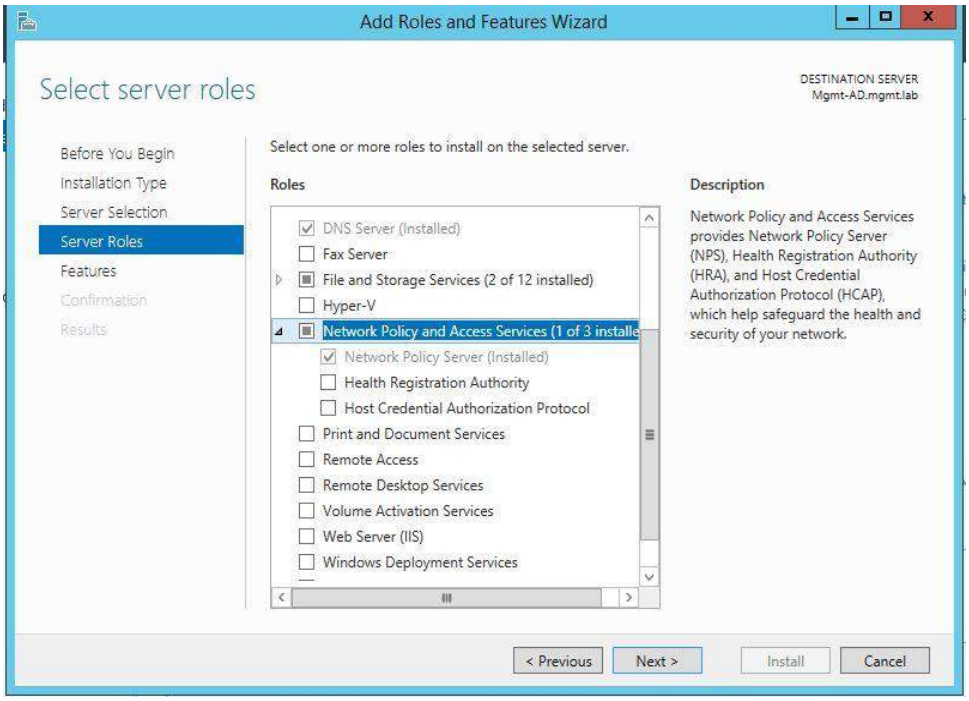
- 配置 AD 服务器，创建 AD 域。
- 在 AD 中配置用户账户和用户组对网络设备进行认证。
- 配置 Radius 服务器。
- 在 AD 中注册 Radius 服务器。
- 创建 Radius 客户端和网络策略。

1. 按照前一节描述的操作步骤配置AD服务器并创建域。
2. 在活动目录中添加用户账户，登录网络设备。必要时创建安全组，调整用户账户的权限。

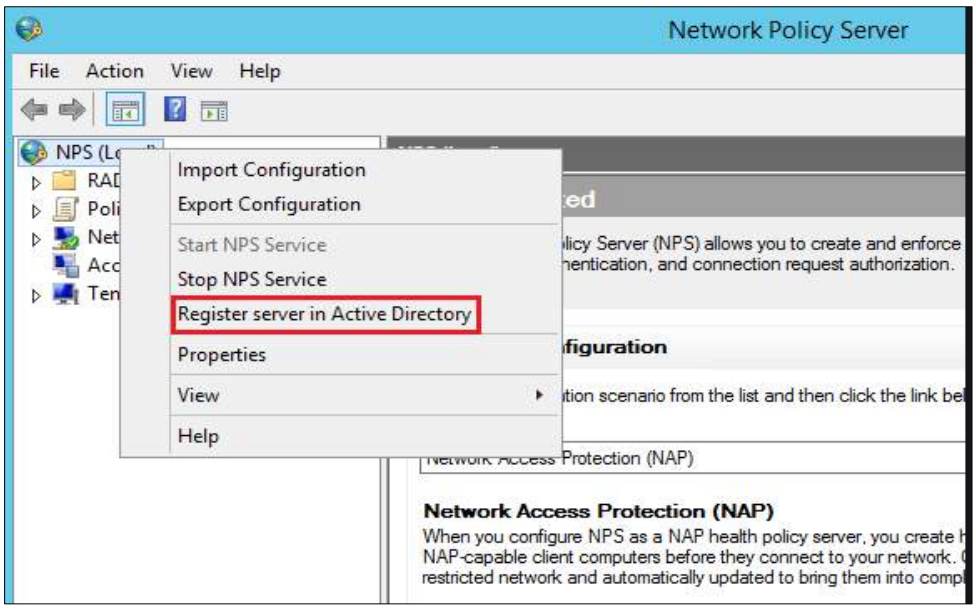
   例如，我们在**mgmt.lab**域中创建用户账户**icsuser01**和安全组**Network Admins**，将**icsuser01**用户添加至网络管理员组。
3. 按照以下步骤在Windows 2012 R2系统上配置Radius服务器：

   a. 启动Server Manager（服务器管理器），单击【**Add Roles and Features**】（添加角色和功能）。

   b. 创建**Network Policy Server**（网络策略服务器）角色。

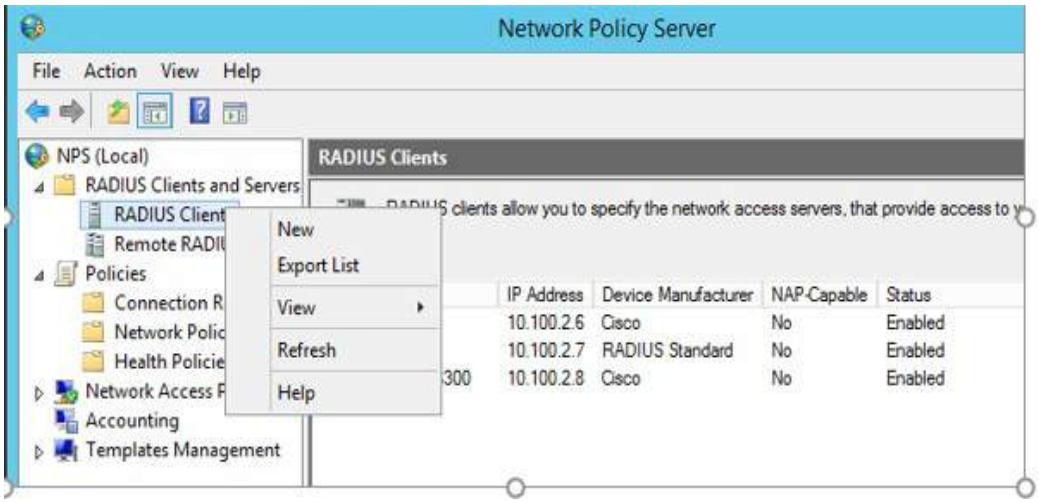


打开网络策略服务器工作台，右击【**NPS (local)**】（NPS（本地）），然后单击【**Register Server in Active Directory**】（在活动目录中注册服务器）。



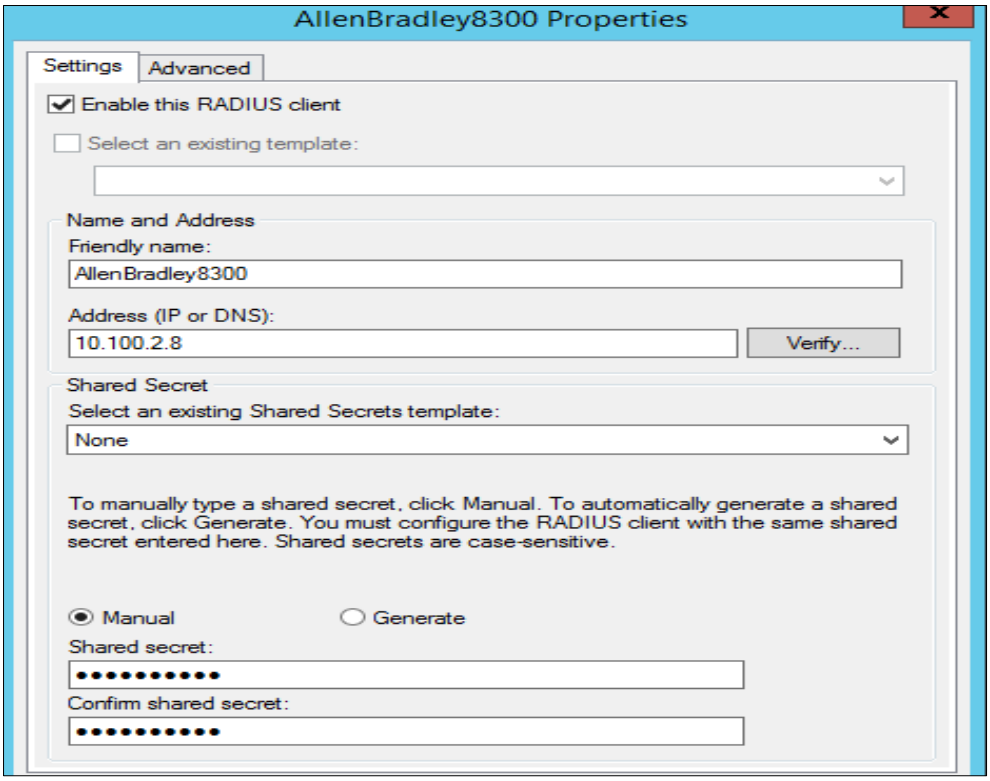
4. 按以下步骤在NPS中配置Radius客户端和策略：

a. 启动【**Network Policy Server**】（网络策略服务器）管理单元，右击【**Radius Client**】（Radius客户端），选择【**New**】（新建），为当前的网络设备配置Radius客户端。



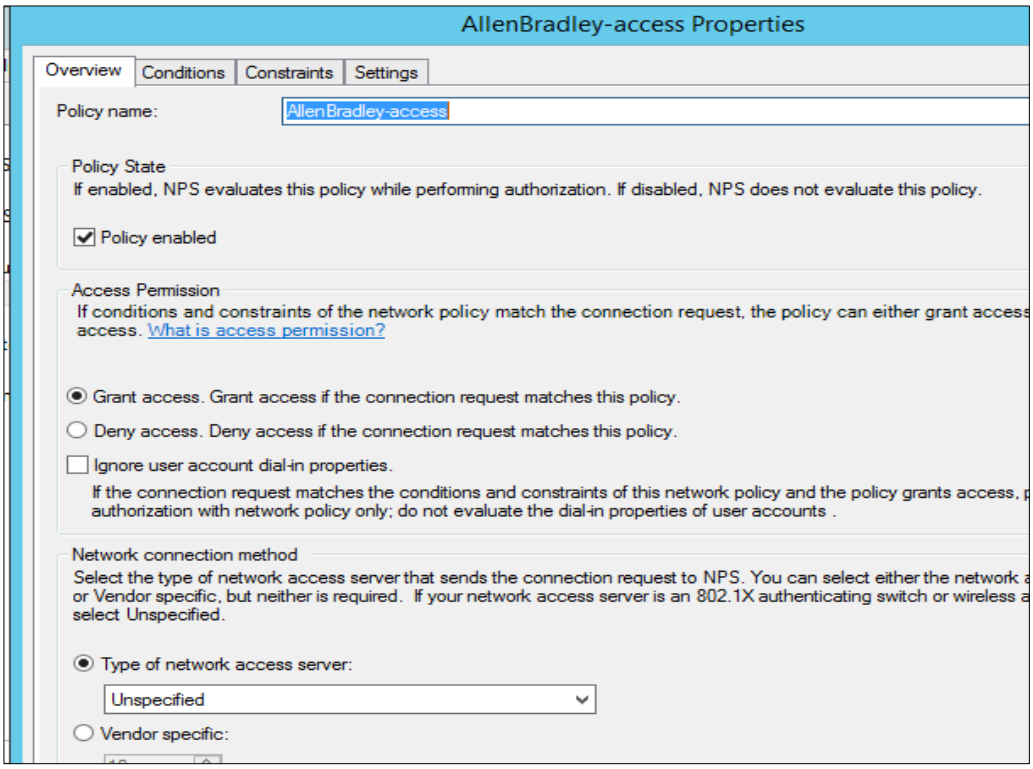
b. 输入匹配的网络设备名称、该设备的管理接口的IP地址，创建安全的强密码短语。操作完毕，单击【**OK**】。这就完成了Radius客户端的配置。确保可从Radius服务器Ping通网络设备的IP地址。

下图显示了为工厂的 Allen Bradley 边界路由器/防火墙设备创建的 Radius 客户端。



c. 择**Policies > Network Policies**（策略>网络策略），为Radius客户端配置策略。

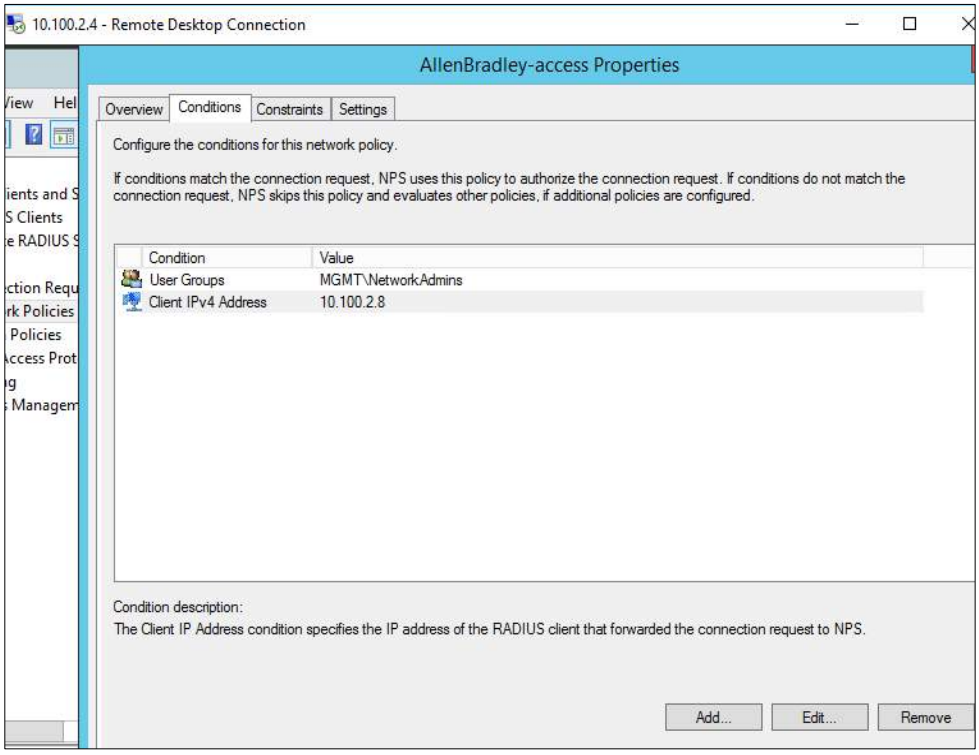
下图显示了为Allen Bradley防火墙配置的网络策略。



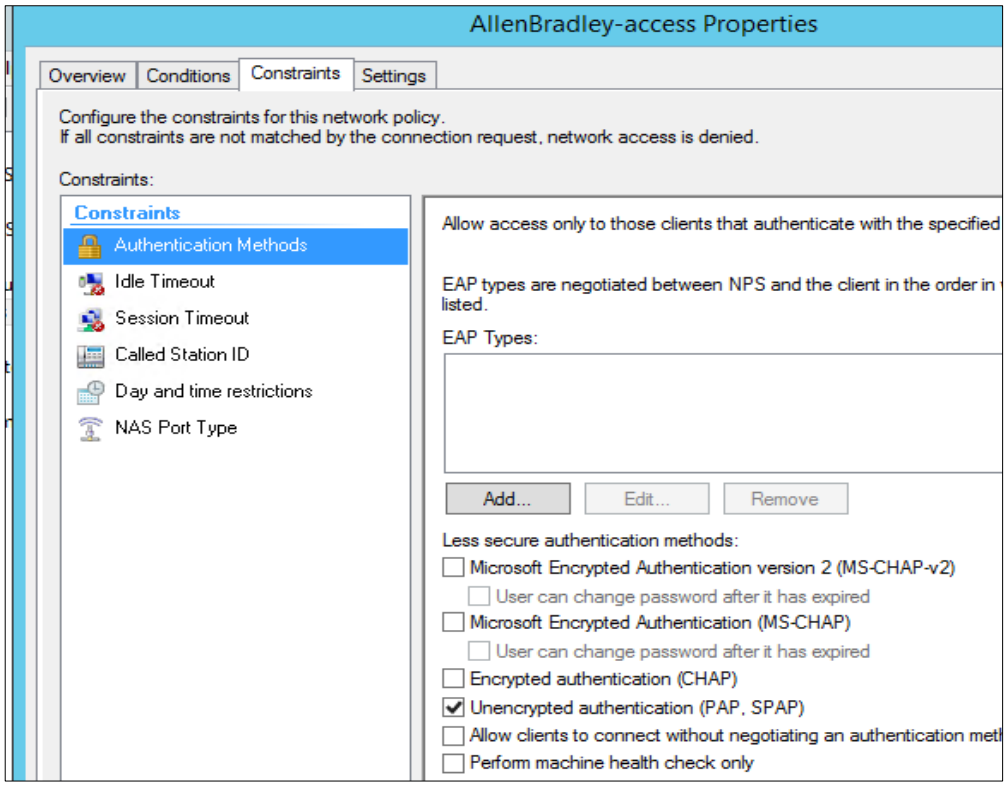
d. 单击【**Conditions**】（条件）页签，配置该策略的条件。

e. 单击【**Add**】（添加）按钮，从列表中选择【**user/groups**】，然后选择AD中配置的安全组（网络管理员）。配置完毕，该安全组中的用户即可以管理员身份登录，对交换机进行管理。

f. 添加Radius客户端IP地址检查条件。从列表中选择【**Client IPv4 address**】（客户端IPv4地址）。输入网络的IP地址并添加。配置完毕后，这两个条件会显示在【**Conditions**】（条件）页面，如下图所示。单击【**Next**】（下一步）打开下一个窗口。

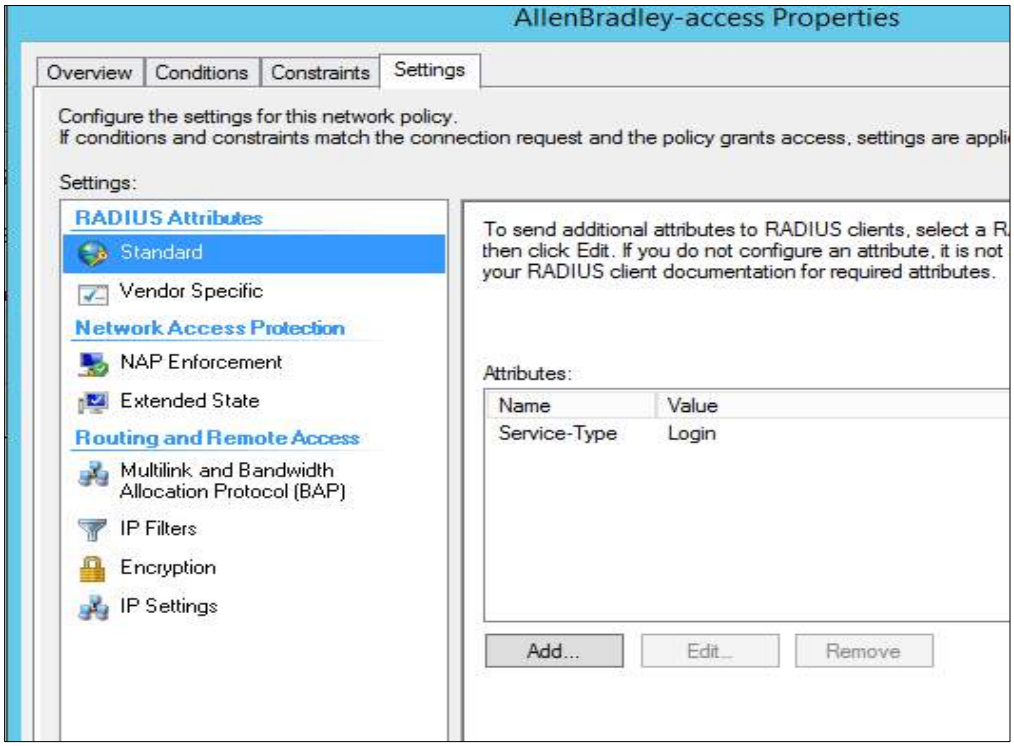


g. 根据思科的建议，选择PAP和SPAP认证方法。单击【**Next**】（下一步），进入【**Settings**】（设置）页面。



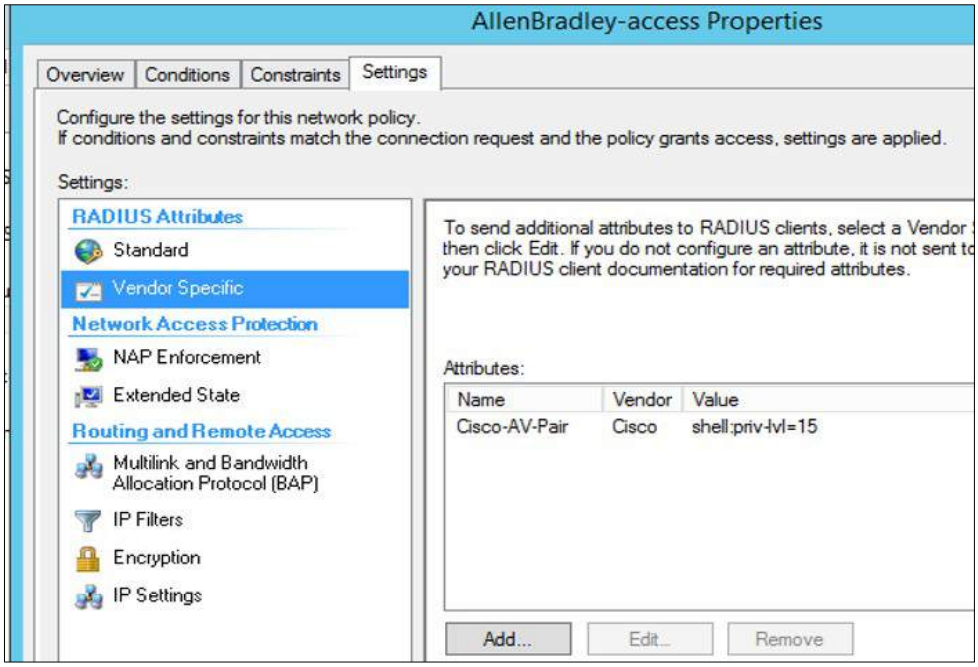
h. 在**Settings**（设置）页面上，单击**Radius Attributes**（Radius属性）下的**Standard**（标准）。

i. 删除两个默认属性。单击**Add**（添加），添加新属性，将**Name**（名称）设置为**Service-Type**（服务类型），**Value**（值）设置为**Login**（登录），如下图所示。



j. 在【**Vendor Specific**】（厂商自定义）下添加新属性：在列表中选择【**Cisco-AV-pair**】。
Vendor = Cisco
Value = shell:priv-lvl=15
这样就为用户分配了root权限（**privilege level =15**）。

k. 单击【**OK/Apply**】（确定/应用）按钮，保存更改。



配置边界路由器进行 Radius 认证

在边界路由器上配置 AAA 组用于 Radius 服务器认证。

在 Allen Bradley 边界防火墙上运行以下命令，使用 Radius 服务器进行认证。


```
#enable
#configure terminal
(config)#aaa new-model
(config)#aaa authentication login default group radius local (config)#aaa authorization exec default group radius local (config)#radius server host 10.100.2.3
(config)# radius server-key <passphrase>
(config)#
end #wr
mem
```

对性能的主要影响

在下面的实验中，我们测量了制造系统正常运行时活动目录服务对系统性能的影响：

PL002.1 – 为活动目录服务的非 OPC 账户配置非管理员权限

实验期间，未发现对生产过程造成性能影响，但发现实现活动目录服务对性能产生了影响。实现阶段一开始，主要进行了活动目录安装和用户配置，但当时并不知道要配置 DCOM，造成生产意外中断。之后，对各 OPC 客户端的 DCOM 和用户账户配置进行了修改，通过活动目录进行认证，而非本地认证。若不进行此修改，

OPC 客户端无法与 OPC DA 服务器进行通信，无法实现 OPC 数据交换，导致生产过程进入紧急关闭状态。

实现过程中的另一影响是活动目录的时间同步源问题。主机与活动目录之间的时间出现了偏差，导致认证失败。这是因为主机与其他时间源而非活动目录进行了时间同步，且时间偏差超过了 5 分钟。加入活动目录域后，主机应使用活动目录的时间源。例如，PCS 中的所有主机将活动目录视作时间源，而活动目录使用外部 NTP 服务器作为时间源。

应注意确保活动目录服务正常运行。认证失败会导致 OPC 服务器运行错误，而 OPC 服务器用于处理控制器和工厂之间的数据交换。生产过程之所以进入紧急关闭状态是因为控制器无法与传感器和执行器进行通信。强烈推荐进行冗余备份，保证主备活动目录无缝切换，避免对系统产生影响。

实验中，我们未发现对网络性能产生重大影响。例如，使用活动目录时，从 OPC 到 HMI 的往返时间基本一致。

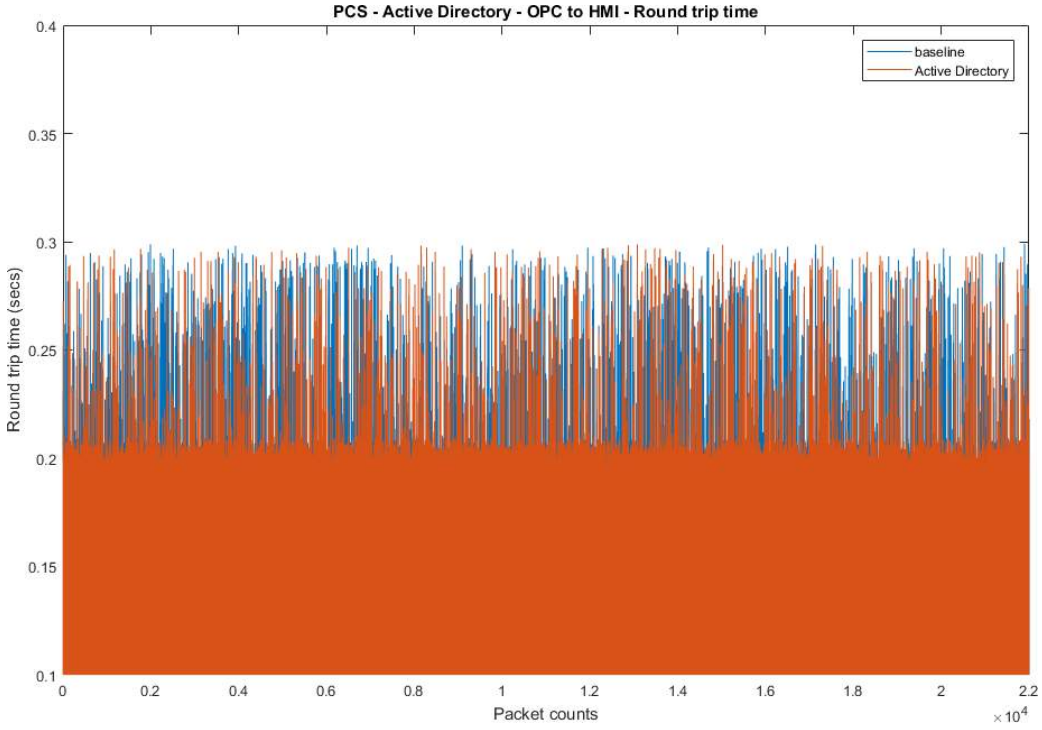


图 4-16：使用活动目录时 OPC 到 HMI 的报文往返时间

控制器是个重要组件，需对其配置进行修改才能使用活动目录。控制器用 AD 服务器进行认证，其 DCOM 配置也进行了更新，以便与 OPC 服务器通信。它与 OPC 之间的报文往返时间稍长一些，原因是少数报文的往返时间出现小幅增长。总体而言，控制器到 OPC 的往返时间没有明显增加。

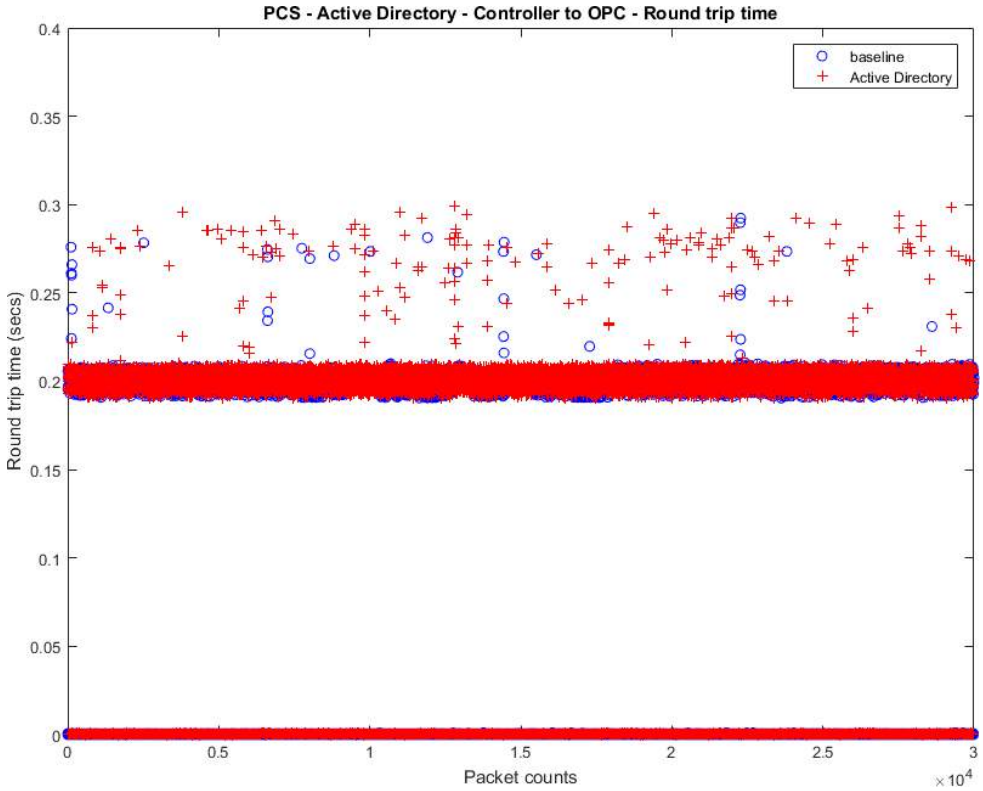


图 4-17：使用活动目录时控制器到 OPC 的报文往返时间（红色）

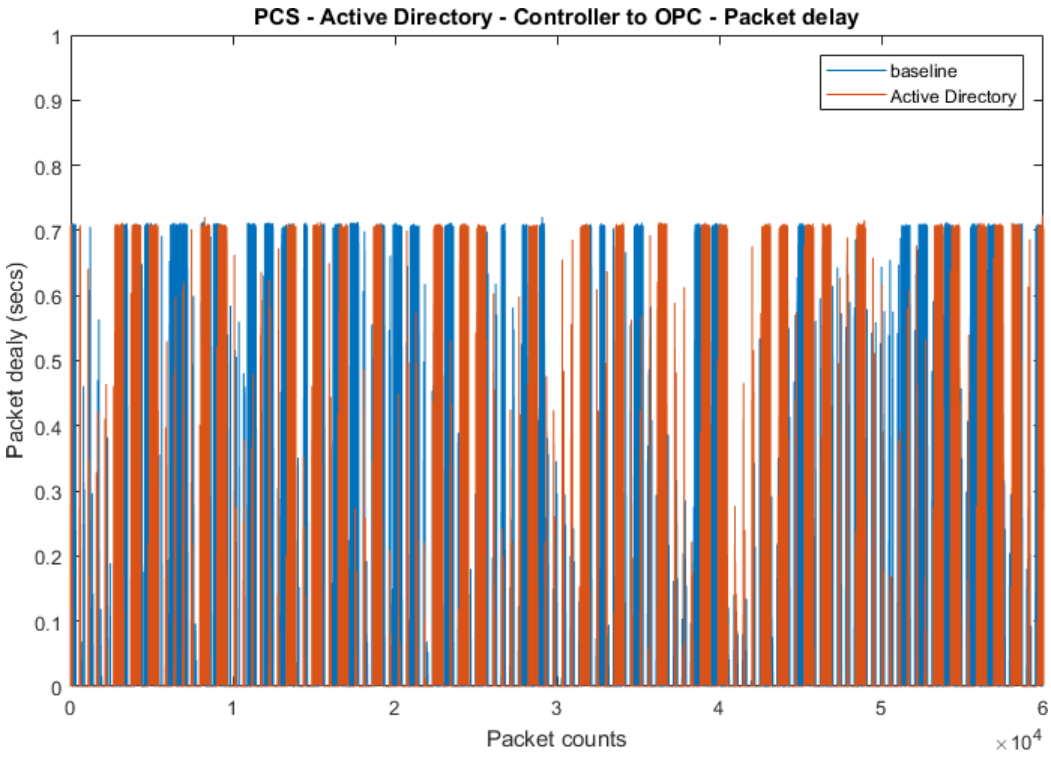


图 4-18：启用活动目录时控制器到 OPC 的包间延迟（红色）

用活动目录不会对生产过程带来明显的性能影响。例如，无论是否使用活动目录，产品流速均很稳定。

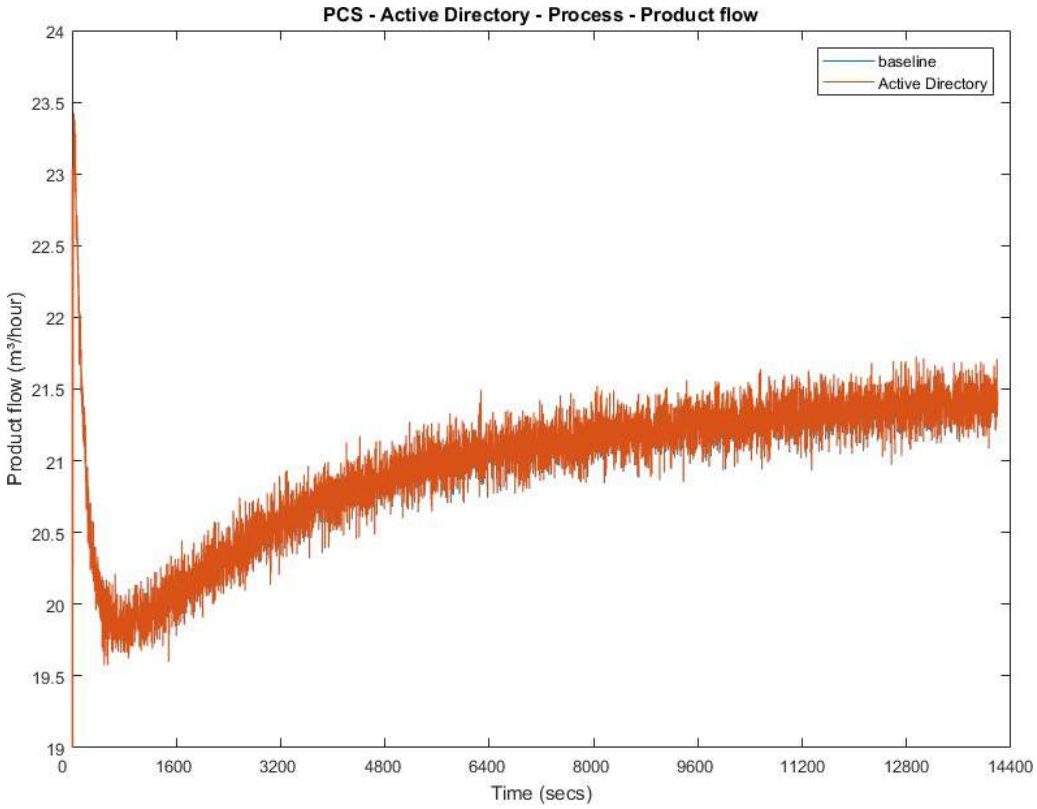


图 4-19：使用活动目录时生产过程中的产品流速（红色）

活动目录配置误配造成反应器压强过大，导致 600 秒（实验时间）时生产过程紧急停止。

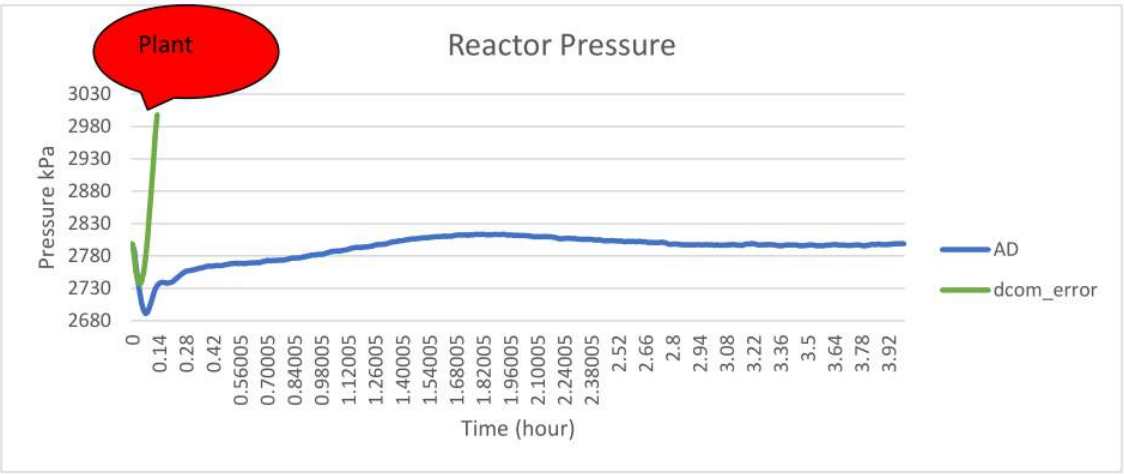


图 4-20：生产过程中的反应器压强图。DCOM 通信失败时，生产过程紧急停止。

4.9.6 性能评估数据集的相关链接

- 活动目录 KPI 数据
- 活动目录测量数据

4.10 赛门铁克端点防护

4.10.1 技术方案概述

赛门铁克端点保护（SEP）[88]是一种端点保护方案，用以防护勒索软件等新兴威胁。

重点说明：

- 下一代防病毒/端点保护方案，可防止病毒攻击和零日攻击、勒索软件等新兴网络威胁。
- 独立于操作系统平台：Windows 和 Linux 均支持端点代理。
- 自带轻量级代理和病毒定义集，最大程度地减少网络带宽占用。
- 丰富的特性：核心功能包括防病毒、主机防火墙、入侵防御、主机完整性、系统锁定、应用白名单和 USB 设备控制。
- 集中管理：所有端点、规则集、策略都可以从赛门铁克端点管理器控制台集中管理。
- 仅 Windows 操作系统支持赛门铁克管理器组件。
- Linux 代理要求 Linux 系统上的操作系统内核为特定的安装级别。此外，Linux 代理是 32 位的安装程序，若安装在 64 位 Linux 系统中，要求事先安装特定的 32 位软件包/库。这可能会导致与系统中现有软件包发生冲突。
- 默认情况下，各系统上的端点代理要与一系列公共 IP 地址进行出站通信，以便实现信誉分析和全球威胁情报功能。建议设置防火墙允许此类通信，以使用产品的高级功能。
- **重要提示：**要在客户端/端点上完成安装，务必重启系统。

4.10.2 方案提供的技术能力

SEP 提供以下技术能力（参见第 1 卷第 6 章）：

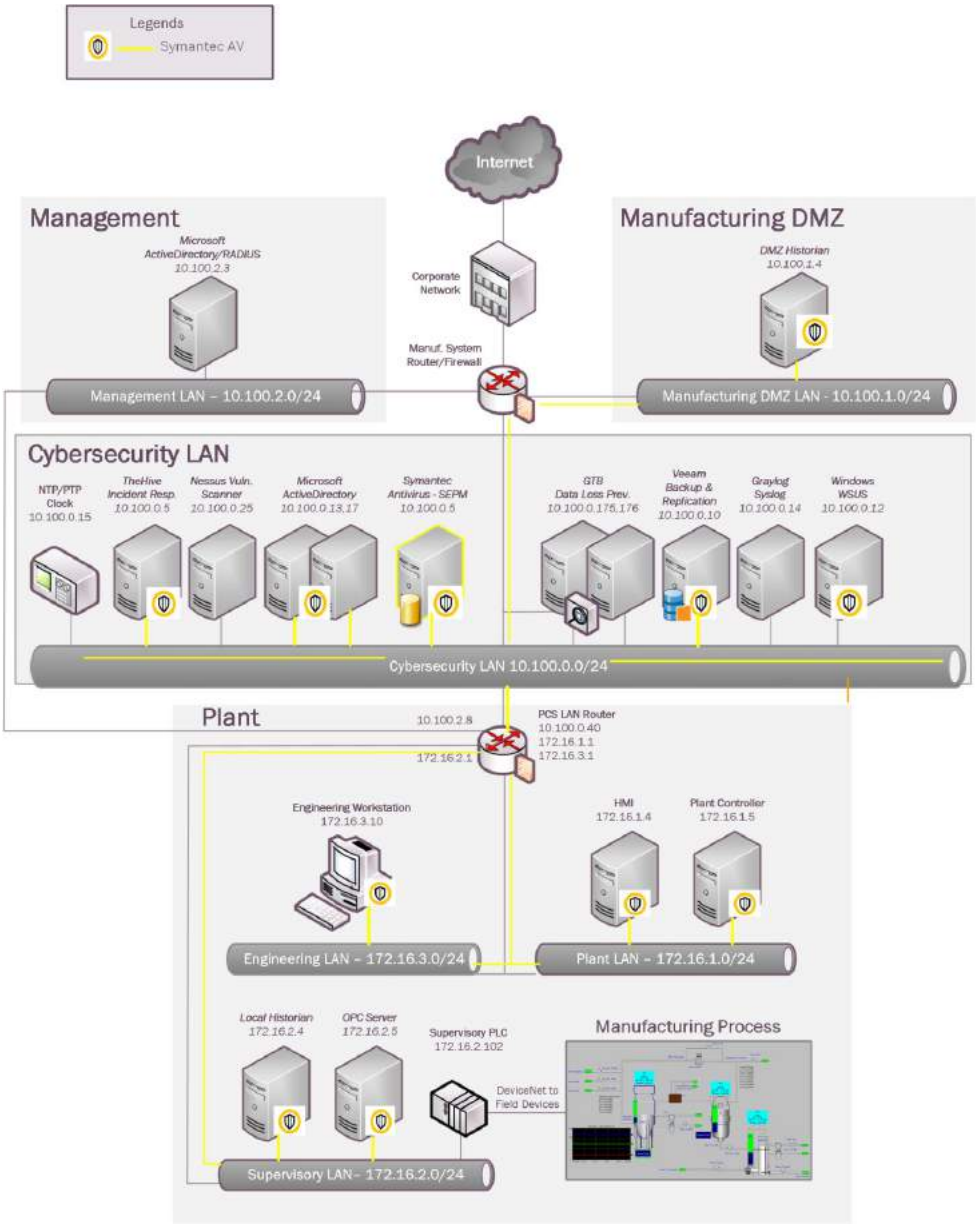
防病毒/恶意软件

4.10.3 方案实现的子类

DE.CM-4

4.10.4 方案实施架构图

[88] https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf



4.10.5 安装说明与配置

实施方案的详细信息：

方案名	版本	部署模式	硬件规格
赛门铁克端点保护管理器（SEPM）	14.2 Build 758	本地部署	Hyper-V虚拟机（第2代）： • 处理器：虚拟双核 • 内存：6 GB • 磁盘空间：70 GB • 网络：1个网络适配器 • 操作系统：Windows 2012 R2
Windows版赛门铁克端点代理（客户端）	14.2.758.0000		安装在工厂的所有Windows系统上

Environment setup 环境搭建

- 在工厂的网络安全局域网的 Hyper-V 宿主服务器上配置运行 Windows 2012 R2 的虚拟机。硬件规格见上表。
- 该服务器的客户机操作系统的 IP 配置如下所示：

  - IP 地址：10.100.0.5

  - 网关：10.100.0.1

  - 子网掩码：255.255.255.0

  - 域名服务器：10.100.0.17

- 在工厂的网络安全局域网中部署赛门铁克端点保护管理器（SEPM）虚拟机。此为核心实例，与过程控制系统上部署的所有端点代理进行通信。同时，所有端点向管理器服务器上报状态。Windows 客户端与 Mac/Linux 客户端在所需开启的通信端口方面存在差异。详细端口信息，见防火墙端口列表[89]。

SEPM 服务器安装

- 从赛门铁克网站上下载赛门铁克端点保护安装包（.zip）。产品注册和下载需要许可证。
- 打开解压缩的文件夹，运行 **Setup.exe** 文件。在安装期间，按提示输入 admin 的强密码。
- 在数据库选择页面，选择【**Backed Database**】（支持的数据库）。若未配置 MS SQL Server，选择 **Embedded database**（嵌入式数据库）。按界面提示完成安装。
- 安装完毕，重启服务器。
- 启动赛门铁克端点保护管理器（SEPM）控制台，使用创建的 admin 帐号登。
- 激活许可证密钥，开始使用该产品。

SEPM 服务器配置

- 配置客户端组，将设备分组：

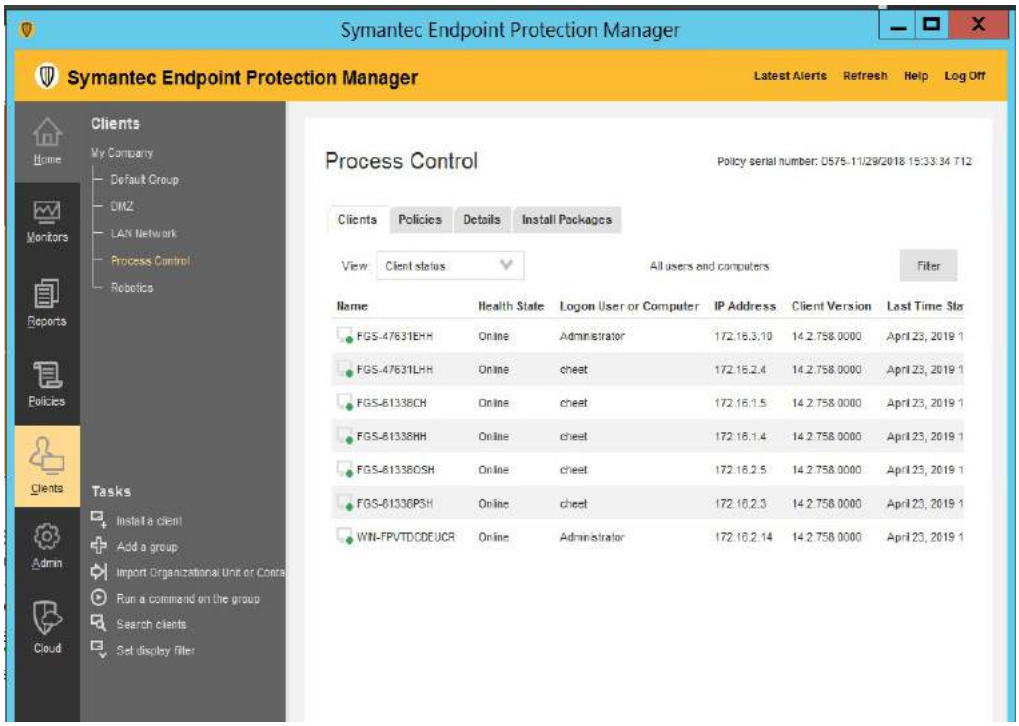
  - 从左侧菜单选择【**Clients**】（客户端）。

  - 单击【**Add a group**】（添加组）。

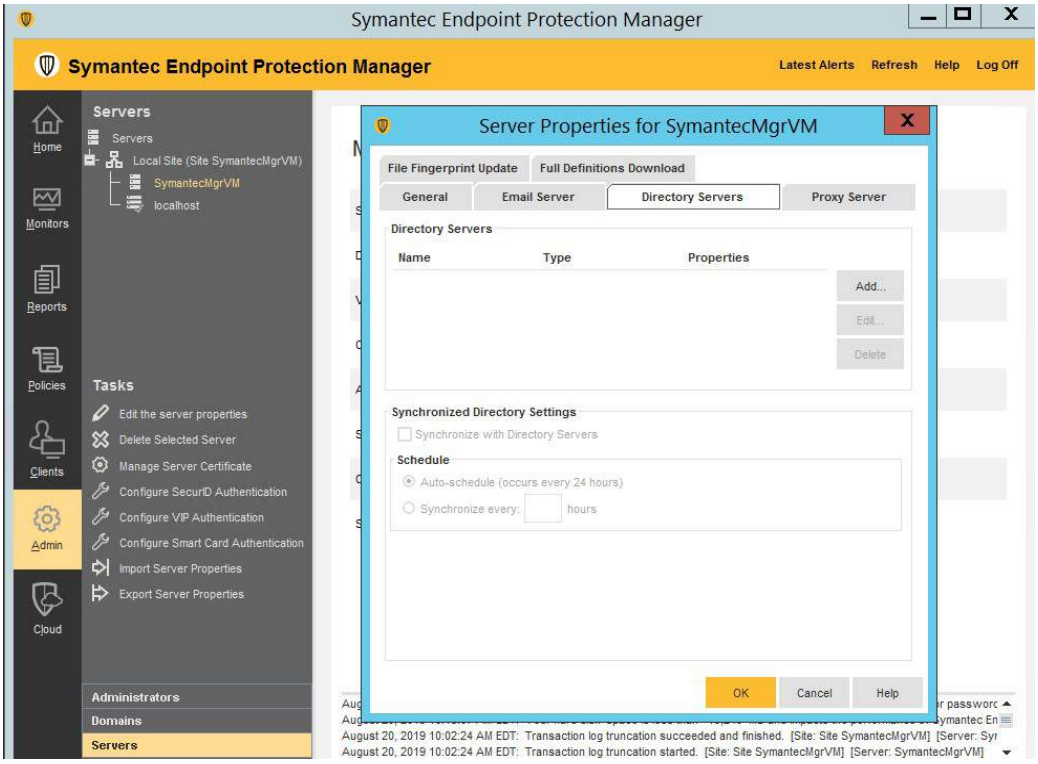
  - 输入【**Name**】（名称）。

  例如，在网络中创建多个客户端组，将不同系统中的设备分组，如下图所示。

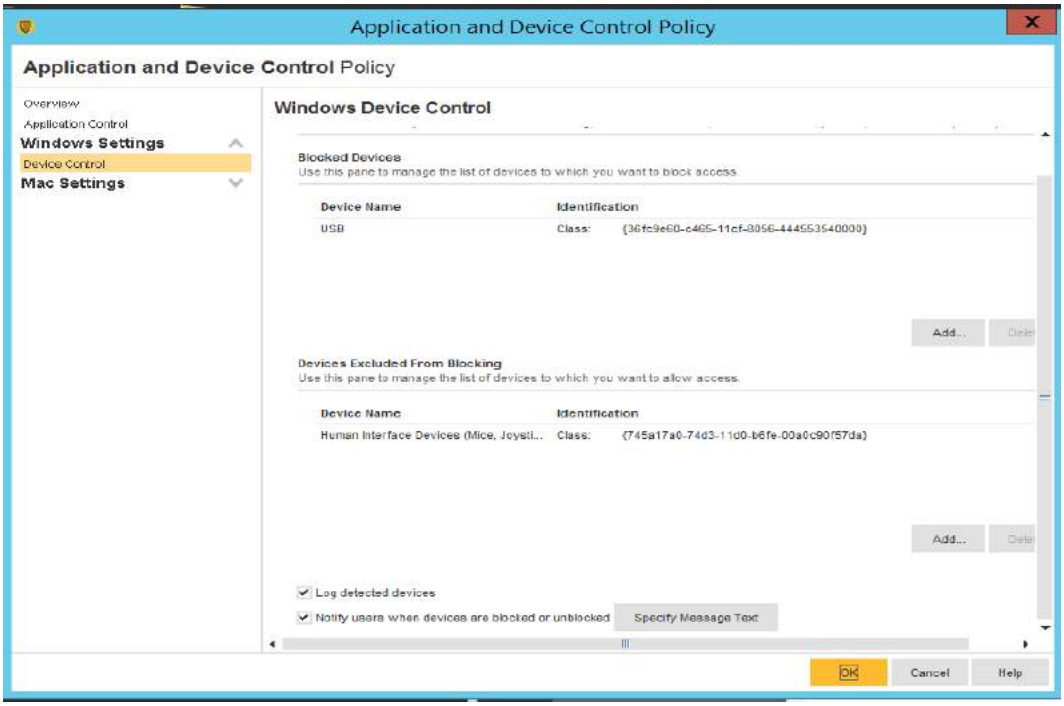
[89] https://support.symantec.com/en_US/article.HOWTO81103.html



- 按如下步骤，将 SEP Manager 与活动目录/LDAP 集成：
  - 单击 **ADMIN > Servers > Local Site > Server Name > Edit Server Properties**（ADMIN > 服务器 > 本地站点 > 服务器名称 > 编辑服务器属性）。
  - 在【**Server Properties for <Server>**】（<服务器>服务器属性）对话框，单击【**Directory servers**】（目录服务器）页签。
  - 单击【**ADD**】（添加）按钮，配置详细域信息
  - 配置完毕，退出登录，然后使用自己的活动目录凭证重新登录。



- 按如下步骤配置 SMTP 服务器：
  - 选择 **ADMIN > Servers > Local Site > Server Name > Edit Server Properties**（ADMIN > 服务器 > 本地站点 > 服务器名称 > 编辑服务器属性）。
  - 在【**Server Properties for <Server>**】（<服务器>服务器属性）对话框中，单击【Email server】（邮件服务器）页签。
  - 输入详细信息。配置完毕，单击【**OK**】（确定）。
  - 配置【**Excluded Hosts**】（排除主机）策略，指定需要排除的 IP 地址，如漏洞扫描器的 IP 地址，避免扫描时被阻断。
  - 选择 **Policies > Intrusion Prevention/Create a new policy**（策略 > 入侵防御/新建策略）。
  - 单击【**Excluded Hosts**】（排除的主机）。添加相关系统的 IP 地址。
  - 将策略与对应的客户端组相关联。
- （可选）采取以下步骤配置设备控制措施，例如限制 USB 设备。
  - 在【**Application and Device Control**】（应用和设备控制）页面，新建策略。
  - 单击【**Device Control**】（设备控制）。
  - 在【**Blocked Devices**】（阻断的设备）区域，单击【**Add**】（添加）。
  - 选择要阻断的一个或多个设备，例如 **USB**。
  - 对于【**Devices excluded from blocking**】（非阻断设备），务必选择键盘和鼠标[90]。



[90] https://support.symantec.com/us/en/article.howto80866.html

客户端系统上安装端点代理

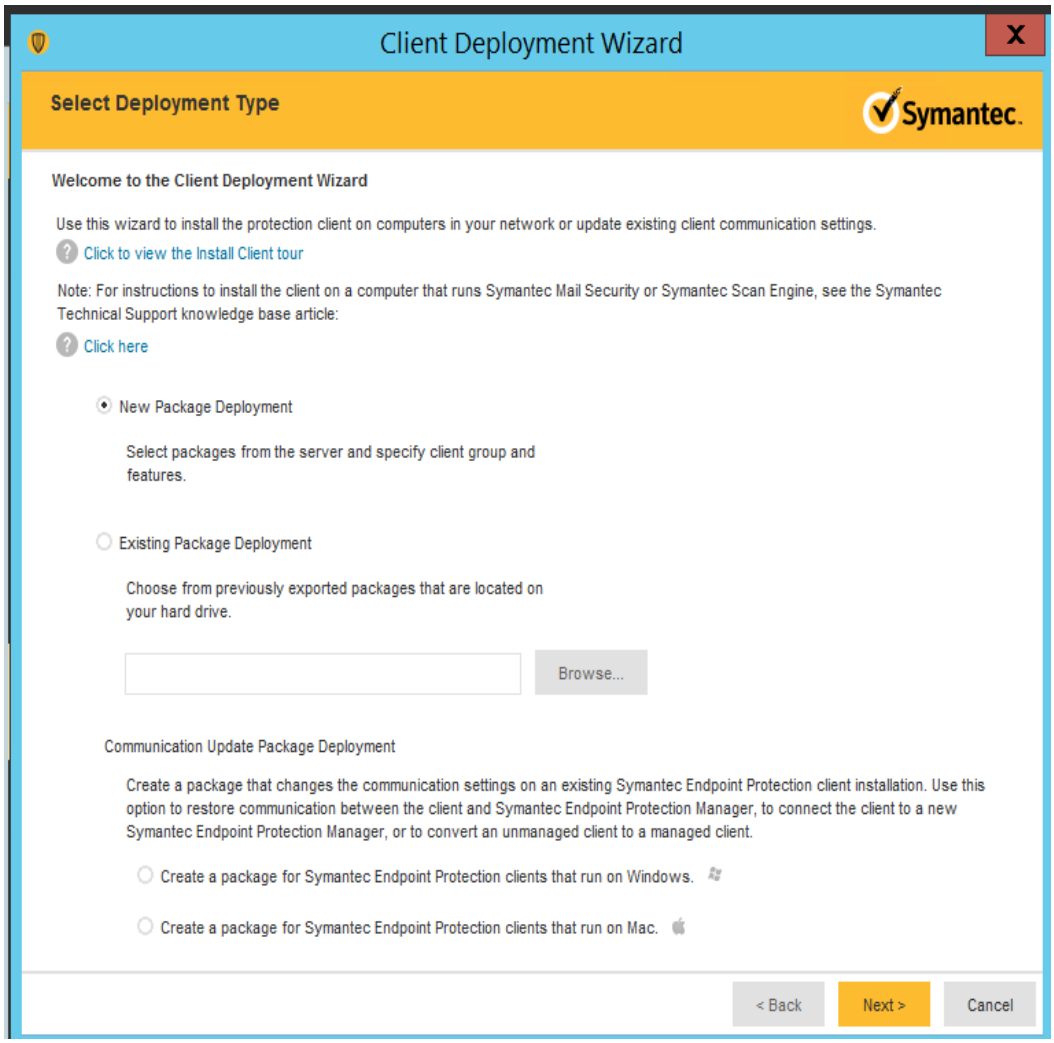
在客户端系统上安装防病毒软件的主要步骤如下：

为特定客户端组创建部署软件包。

部署该软件包。

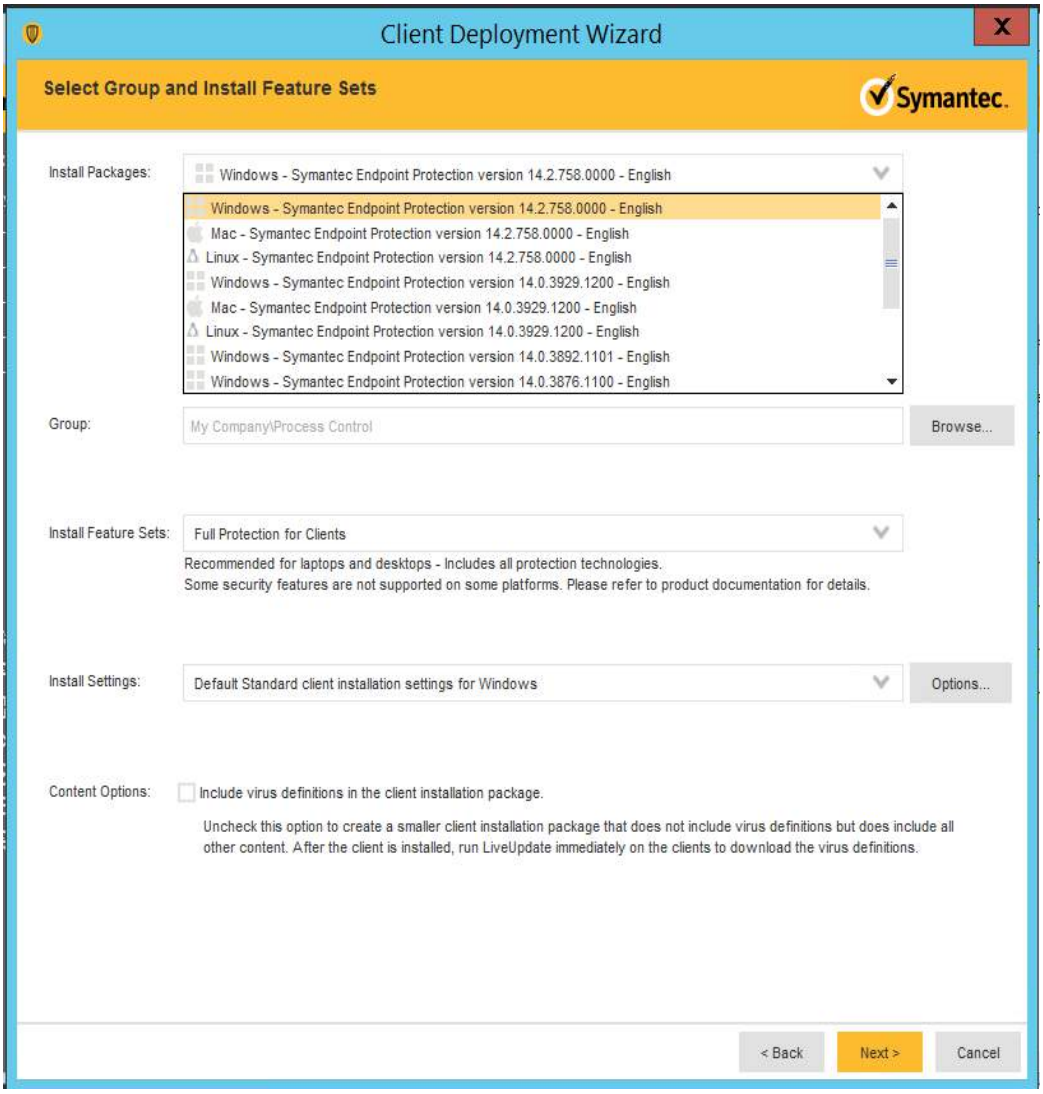
重启客户端系统，完成安装。

- 创建部署软件包：
  - 登录赛门铁克管理器控制台，选择 **Clients > Group Name**（客户端 > 组名），该组为端点设备所在的组。
  - 在【**Tasks**】（任务）页面，单击【**Install client**】（安装客户端）。例如，为 Process Control（过程控制）组创建部署软件包，首先单击该组名，然后单击【**Install Client**】（安装客户端）选项。
  - 若首次为该组安装代理，需选择【**New Package Deployment**】（新建软件包部署）。若已在该组的其他系统上部署了代理，可复用同一软件包，跳过本步。

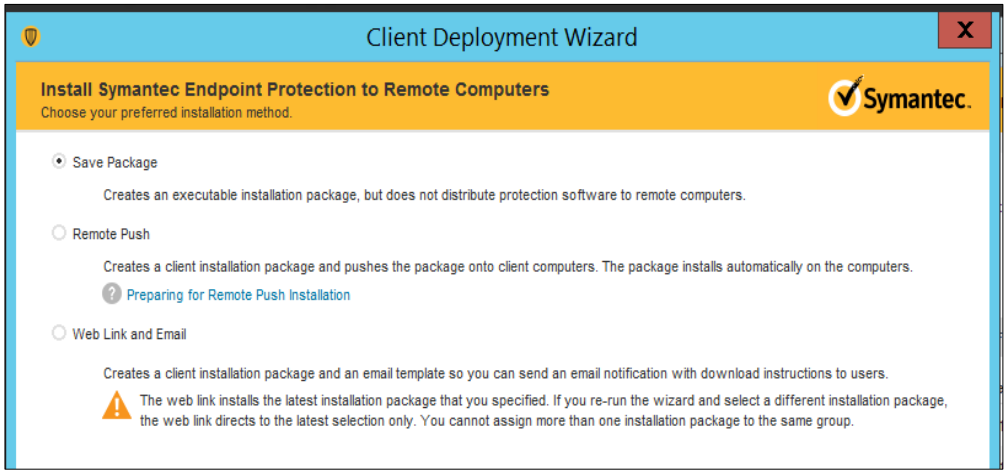


- 单击【**Next**】（下一步）。从【**Install Packages**】（安装软件包）下拉列表选择端点操作系统对应的操作系统平台。注意，组名已自动填充，这样，客户端将在安装后自动加入该组。

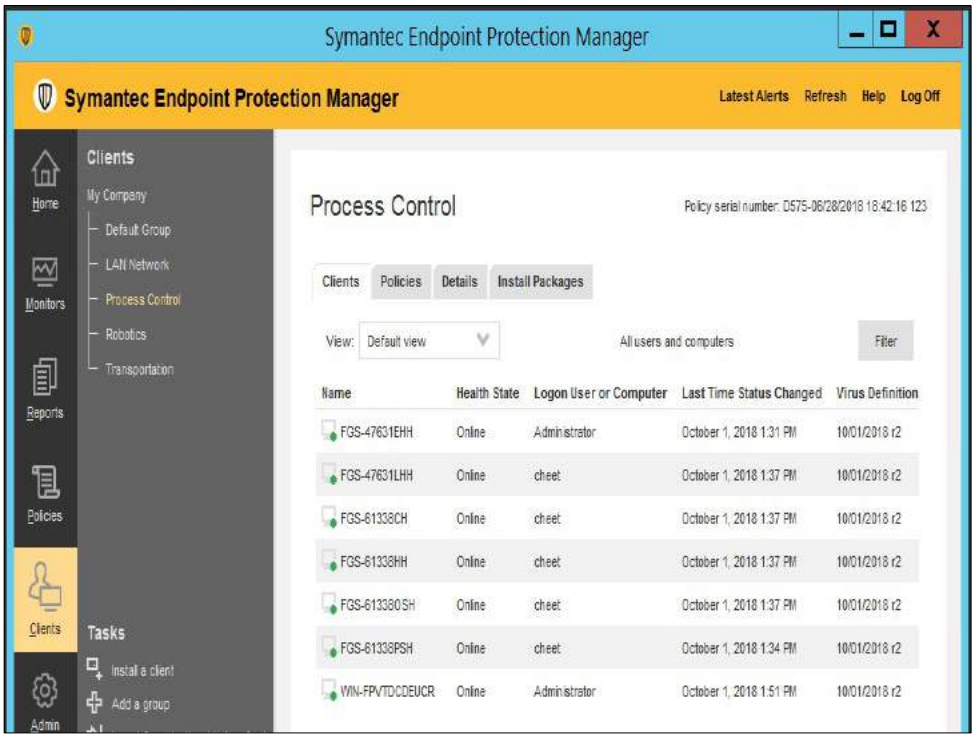
- （可选）对于【**Content Options**】（内容选项），选择【**Include virus definitions in the client installation package**】（在客户端安装包中包含病毒定义）。单击【**Next**】（下一步）。



- 部署软件包：
  - 在下一页，选择安装方法。
  - （方法 1）选择【**Save Package**】（保存软件包），创建本地安装程序。该安装程序需拷贝到目标机器。
  - （方法 2）选择【**Remote Push**】（远程推送）方法。SEPM 服务器会在目标机器上进行网络部署。确保用户使用管理员权限在目标系统上安装软件包。
  - （方法 3）选择【**Web Link and Email**】（Web 链接和邮件），以邮件方式将安装程序的链接发送给用户。
  - 单击【**Next**】（下一步）。



- 代理安装完毕，重启端点机器完成安装。在赛门铁克管理器控制台上，查看并确保客户端名称为**绿色**在线状态且病毒定义为当前最新。



补充信息

- 赛门铁克端点保护 v14 官方安装指南[91]
- 关于赛门铁克端点防护[92]的实践指南，请参见赛门铁克官方提供的 Windows 系统安装指南[93]。

经验总结

若使用赛门铁克防火墙，确保禁用客户端的操作系统防火墙，以避免冲突。若首次安装控制台，会自动向各组添加默认防火墙策略。同样，若未在控制台配置防火墙策略，客户端通常会获取默认防火墙设置。

91 https://support.symantec.com/en_US/article.DOC9449.html
92 https://support.symantec.com/us/en/how-to-guides.html
93 https://support.symantec.com/en_US/article.DOC9445.html

4.10.6 对性能的主要影响

在下面的实验中，我们测量了制造系统正常运行时赛门铁克防病毒工具对系统性能的影响：

实验 PL008.2 – 赛门铁克防病毒扫描

赛门铁克防病毒扫描对主机处理器的使用率影响很大，而对生产过程没有重大影响。赛门铁克全网扫描会占用大量处理器资源。

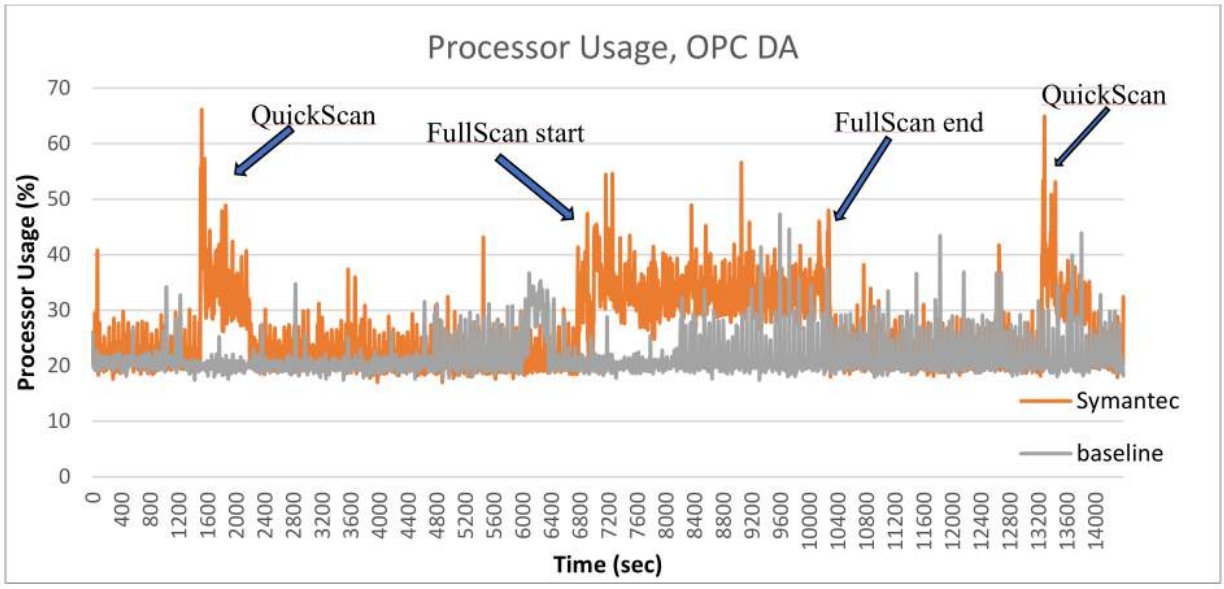


图 4-21：赛门铁克防病毒扫描期间的 OPC 计算机处理器使用率（红）以及处理器使用率基线（灰）

赛门铁克防病毒扫描对网络的性能没有重大影响。

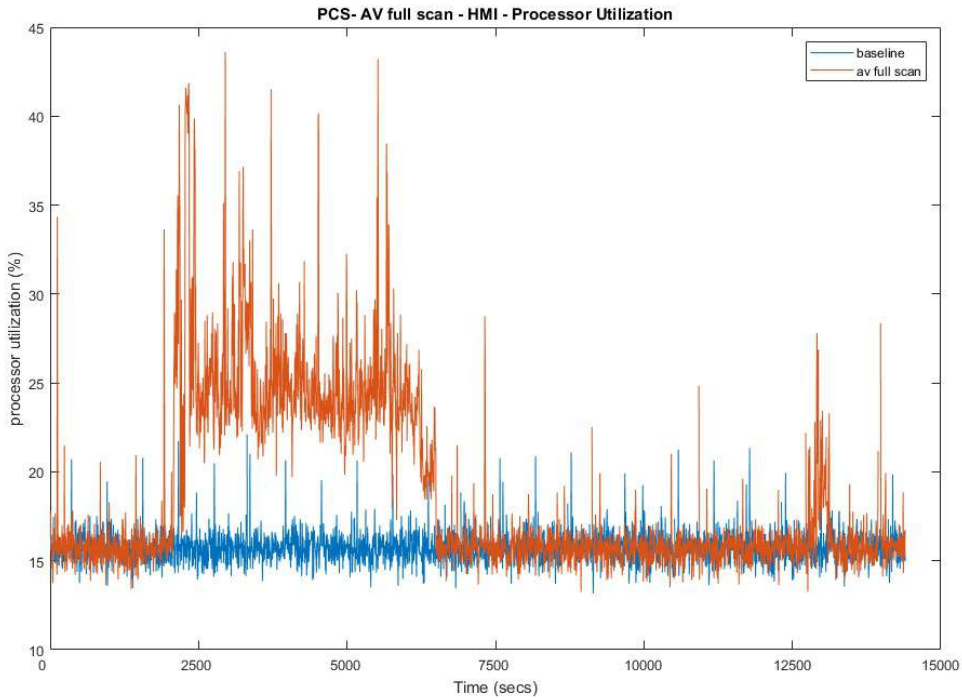


图 4-22：赛门铁克扫描开启（红）和未开启（蓝）时的 HMI 计算机的处理器使用率对比

赛门铁克防病毒扫描对网络性能没有重大影响。例如，OPC 和 PLC 之间的报文往返时间和扫描前基本一致。

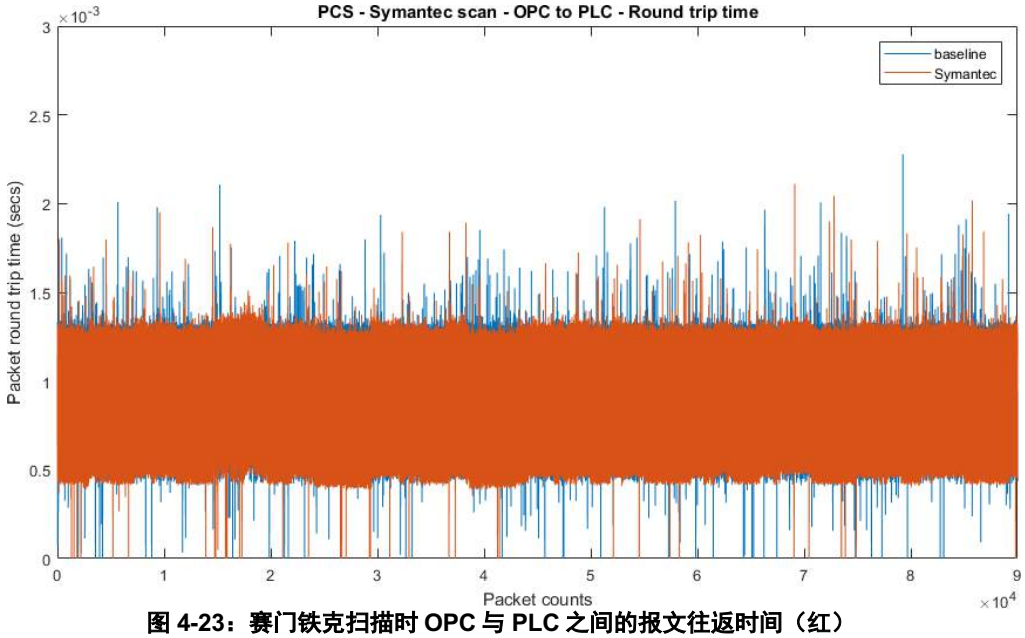


图 4-23：赛门铁克扫描时 OPC 与 PLC 之间的报文往返时间（红）

赛门铁克扫描对生产过程没有重大影响。在扫描期间，产品流速和反应器压强均与基线值相差无几。

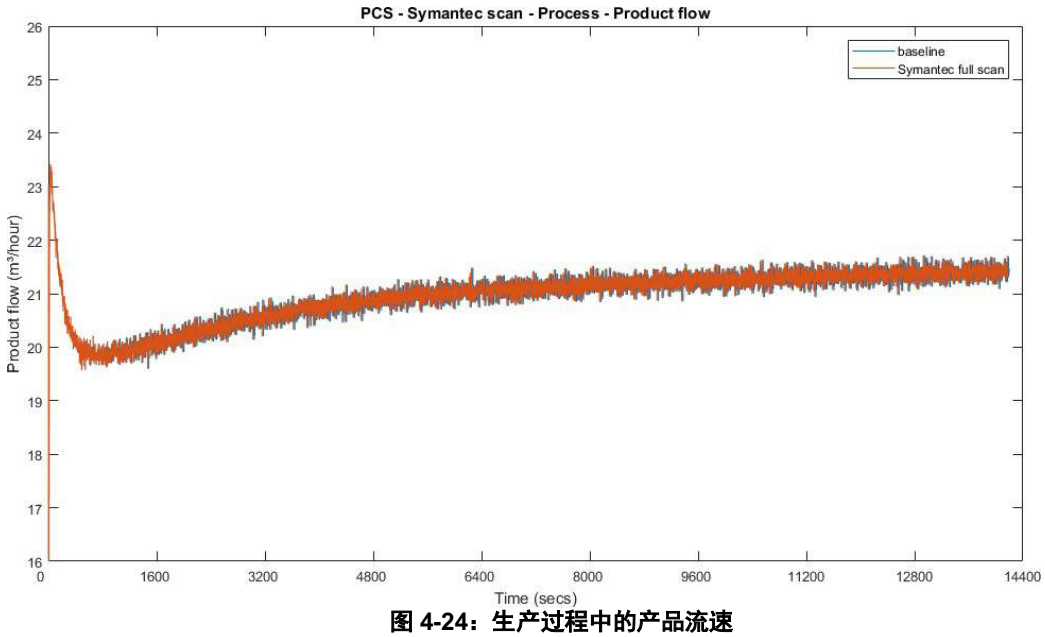


图 4-24：生产过程中的产品流速

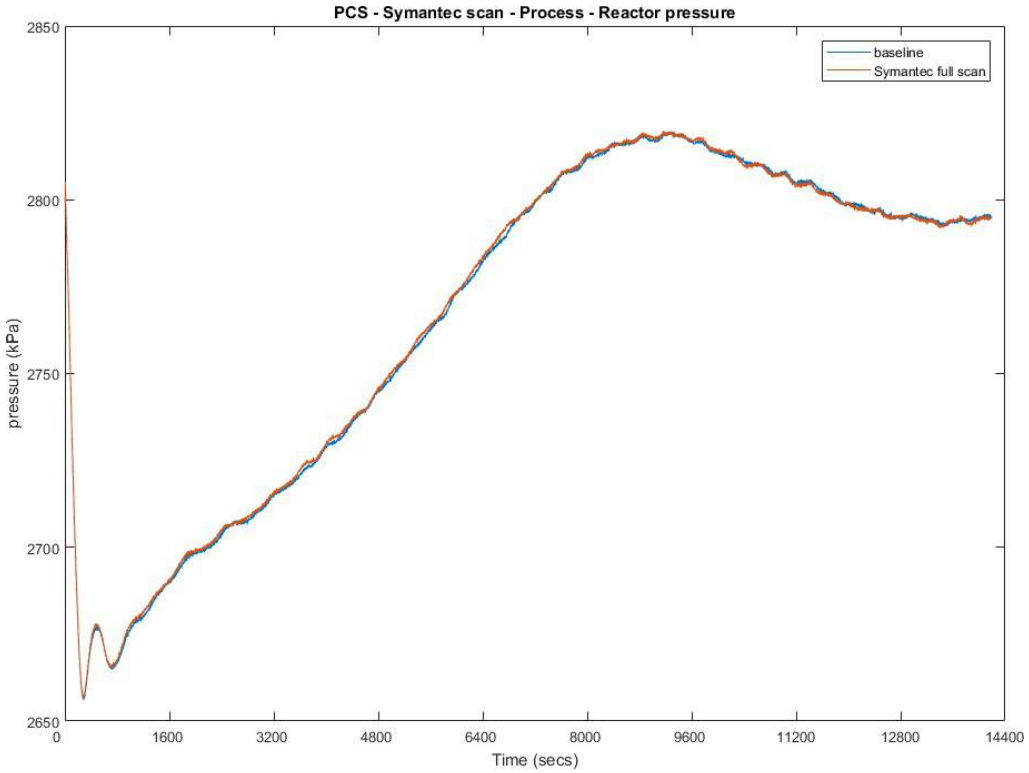


图 4-25：生产过程中的反应器压强

我们假定赛门铁克防病毒软件扫描时会影响处理器使用率。对于 PCS 系统来说，处理器使用率通常较低，因此使用率上升并不会对生产过程带来任何性能影响。若主机处理器的正常使用率接近 100%，则扫描时使用率上升会对性能造成影响。

4.10.7 性能测量数据集的相关链接

- 赛门铁克防病毒 KPI 数据
- 赛门铁克防病毒测量数据

4.11 Tenable Nessus

4.11.1 技术方案概述

Nessus 专业版是 Tenable 提供的一款评估软件，具备高速资产发现、配置审计、目标分析、恶意软件检测以及敏感数据发现等功能。Nessus 支持对操作系统、网络设备、下一代防火墙、虚拟机监控程序、数据库、Web 服务器和关键基础设施进行扫描，以发现漏洞、威胁和不合规情况[94]。该软件支持认证扫描和非认证扫描。

重点说明：

- 配置方便，仪表盘易于使用，扫描快速，可在分布式环境中配置使用；
- 支持 MODBUS 和 DNP3 等工业协议，提供 ICS/SCADA 系统所需的漏洞检测插件，是 OT 环境的理想选择。
- 内置各种策略模板和配置模板，开箱即用。
- IP 地址数量或评估次数不受限制。
- 可扫描部署在防火墙后面的设备。
- 专业版不支持与 LDAP 或活动目录配合使用。
- 不支持多用户账户同时登录 Web 界面。

4.11.2 方案提供的技术能力

Tenable Nessus 提供以下技术能力（参见第 1 卷第 6 章）：

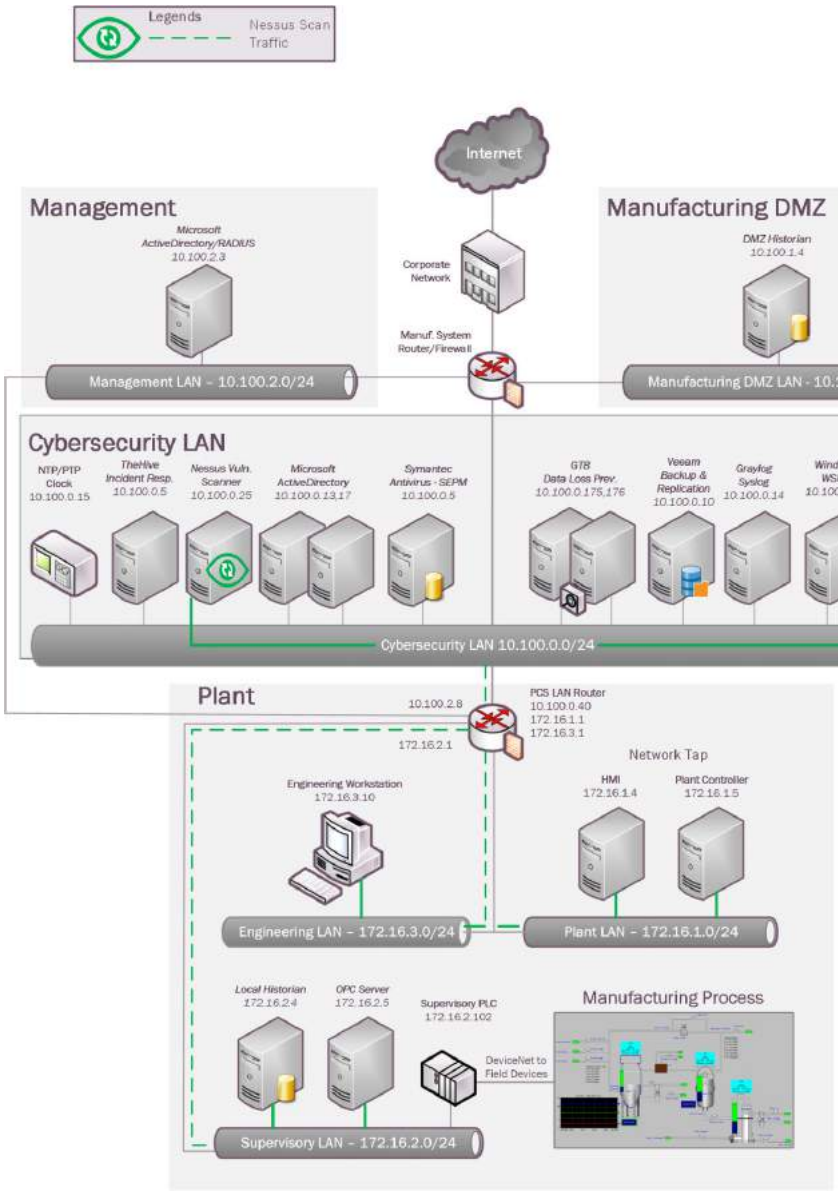
- 漏洞扫描
- 漏洞管理

4.11.3 方案实现的子类

ID.RA-1、DE.CM-4、DE.CM-8 和 RS.MI-3

4.11.4 方案实施架构图

[94] http://info.tenable.com/rs/934-XQB-568/images/NessusPro_DS_EN_v8.pdf



4.11.5 安装说明与配置

实施方案的详细信息：

工具名	版本	部署模式	硬件详情
Nessus专业版	7.2.0	单机	Hyper-V虚拟机（第2代）： • 处理器：虚拟双核 • 内存：6 GB • 磁盘空间：70 GB • 网络：1个网络适配器 • 操作系统：Windows 2012 R2

环境搭建

- 在工厂的网络安全局域网的 Hyper-V 宿主服务器上配置运行 Windows 2012 R2 的虚拟机。硬件规格见上表。
- 该服务器的客户机操作系统的 IP 信息如下所示：

- IP 地址：10.100.0.25

- 网关：10.100.0.1

- 子网掩码：255.255.255.0

- 域名服务器：10.100.0.17

安装说明

- 下载 Nessus 专业版安装程序[95]。
- 运行该安装程序，Follow the on-screen instructions of the setup wizard. 按界面提示完成安装。
- 安装过程中，以在线或离线模式注册产品。在线模式[96]适用于 Nessus 服务器能访问互联网的环境，而离线模式适用于气隙环境。
- 安装完毕，访问 Nessus 的 Web 界面[97]。
- 登录 Nessus 的用户界面，单击【Settings】（设置），配置 SMTP 服务器、LDAP 服务器和自定义 CA 证书（若有）。
- 参照 Nessus 文档，配置防火墙规则对凭证进行扫描，根据 Nessus 服务器和扫描目标之间的主机的类型判断是否放过 SSH、WMI 或 SNMP 流量。对于非认证扫描，防火墙应放过 Nessus 服务器和目标网络之间的所有流量。

扫描和策略配置

本节介绍基于凭证的 Windows 扫描的准备工作。在工厂网络中的 Windows 系统上启用以下各项：

- 在扫描目标上启用 Windows 管理规范（WMI）服务[98]。
- 在扫描目标上开启远程注册服务。
- 在扫描目标的网络配置中，开启文件和打印机共享。
- 利用具备扫描目标的本地管理员权限的 SMB 账户 （您可配置域账户，但须确保该账户为目标设备的本地管理员）。
- 开启 Nessus 扫描器和目标之间的 TCP 端口（139 和 445）。
- 开启默认的管理员共享（如 IPC$、ADMIN$和 C$）（**AutoShareServer** = 1）。这些默认为启用状态，若禁用可能会导致其他问题[99]。
- 在与扫描目标处于同一网络的另一主机上，在提升的命令提示符窗口或 PowerShell（右击 **CMD > Run as administrator**（命令 > 以管理员身份运行））中运行以下命令：

  - net use \\<IP-address of Target>\ipc$/user:

  - 该命令会检验我们是否可在不输入用户名的情况下访问 IPC$共享（Nessus 通过这种方式检查 SMB 是否在运行）。

  - net use \\x.x.x.x\ipc$ /user:username password net use \\x.x.x.x\admin$ /user:username password

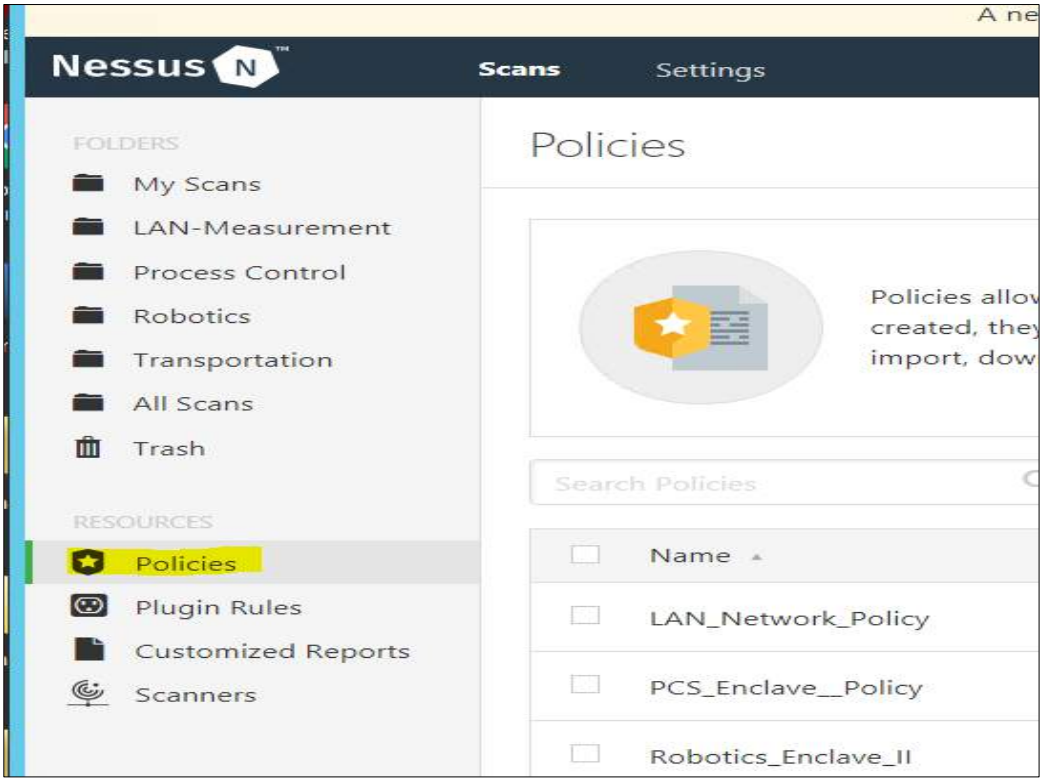
[95] https://www.tenable.com/
[96] https://docs.tenable.com/nessus/Content/ManageNessusOffline.htm
[97] https://<IP address of Nessus server>:8834
[98] https://technet.microsoft.com/en-us/library/cc180684.aspx
[99] http://support.microsoft.com/kb/842715/en-us.

- 这些命令用于 SMB 登录测试，运行后应返回“命令执行成功”的提示。若未返回该提示，说明凭证无效或账户的权限不充分。

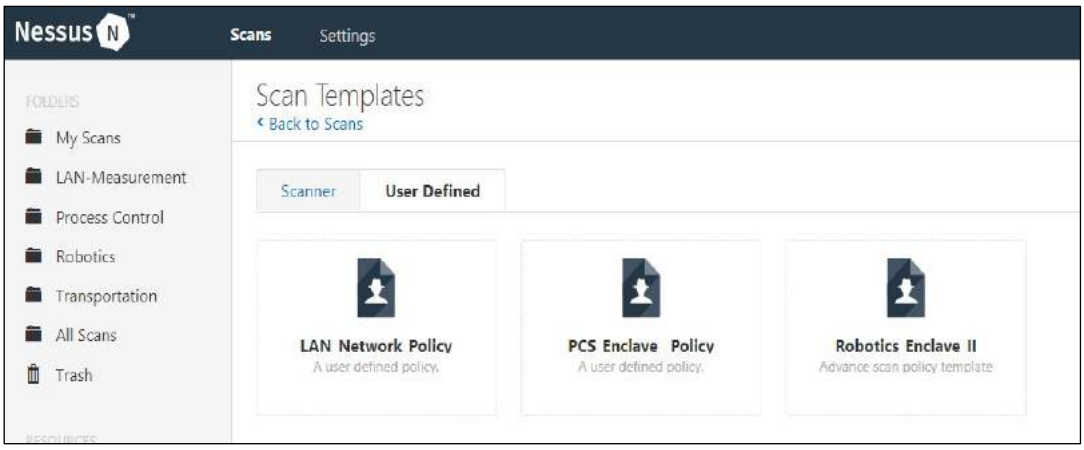
说明：若这些命令未返回错误，则可进行凭证扫描。

利用 Nessus 的策略特性检查凭证。该模块允许创建扫描模板，在模板中保存设备凭证和其他自定义设置，以便扫描资产。创建策略后，将其分配给具体的扫描任务。

- 按以下操作步骤创建策略：
  - 单击左侧浏览栏的【**Policies**】（策略）。
  - 单击【**New Policy**】（新建策略）按钮。



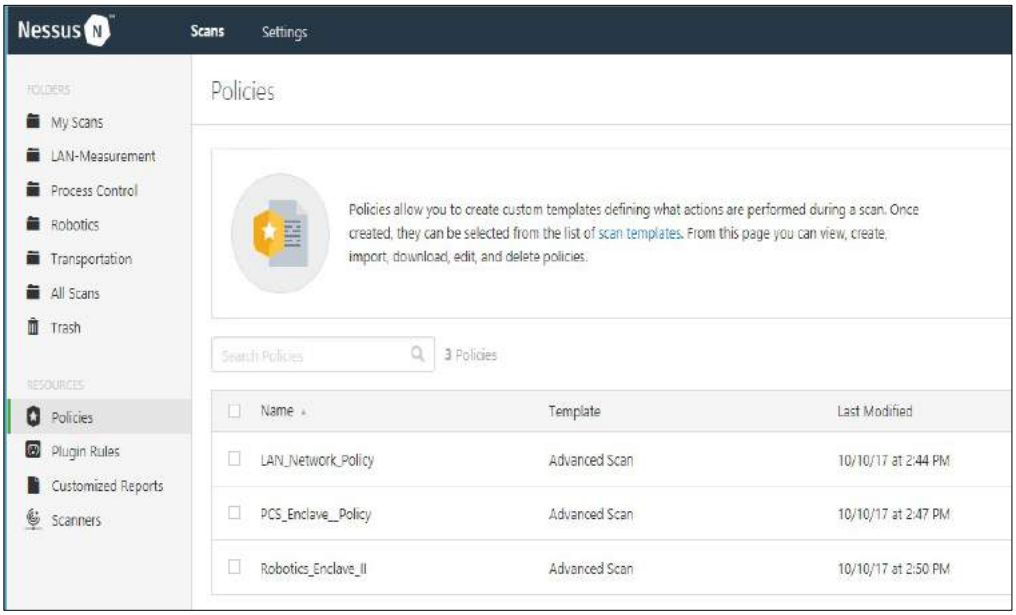
  - 选择默认模板。我们在这里选择【**Advanced Scan**】（高级扫描）模板。单击模板的【**Credentials**】（凭证）页签，配置基于主机的凭证（SSH、Windows 和 SNMP 等）。
  - 配置完毕，单击【**Save**】（保存）。
- 按以下步骤创建扫描任务：
  - 单击主页上的【**Scans**】（扫描），选择 **New Scan > User Defined > Select <Policy>**（新扫描 > 用户定义 > 选择<策略>）。
  - 输入【**Name**】（名称）、【**Description**】（描述）及【**Network Range**】（网络范围）或【**Host IP addresses**】（主机 IP 地址）。
  - 单击【**Schedule**】（定时任务），配置定时任务。
  - 单击【**Notifications**】（通知），配置邮件收件人。
  - 单击【**Save**】（保存）。



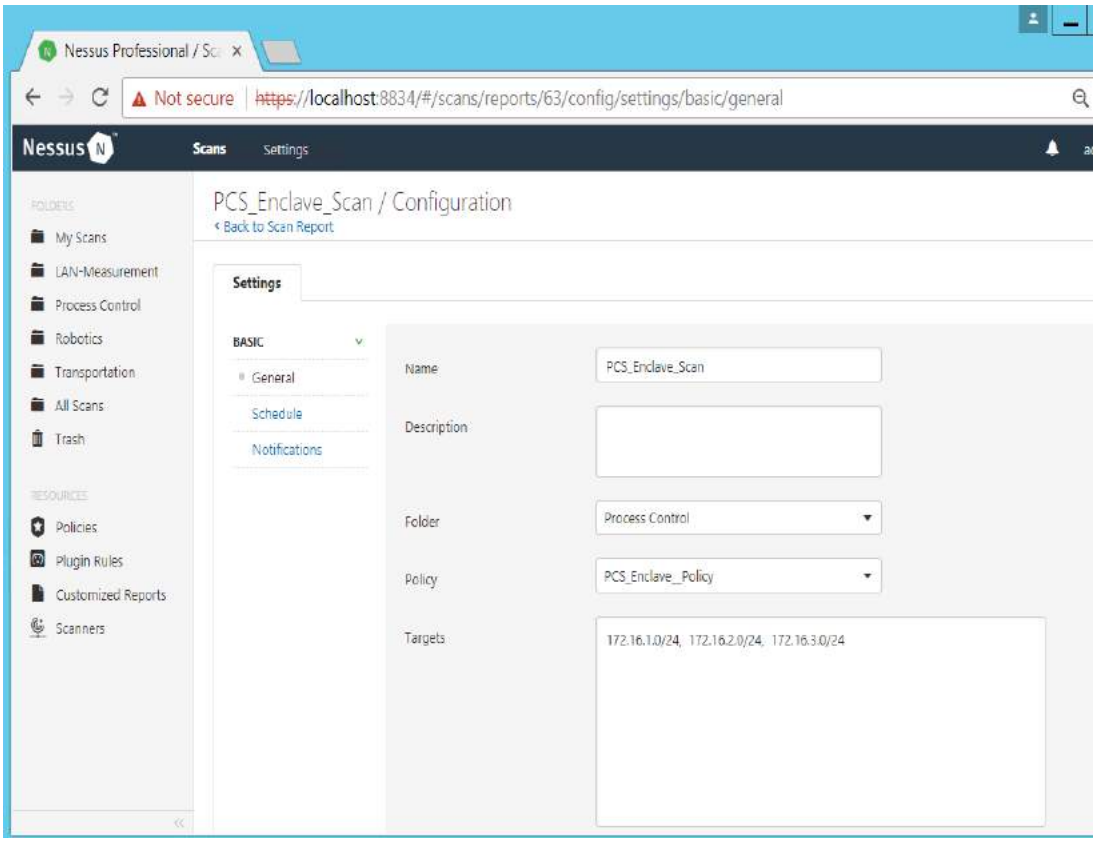
- 为新建的扫描任务分配策略：
  - 单击【**All Scans**】（所有扫描任务），再单击最新创建的扫描任务。
  - 从【**Policy**】（策略）下拉列表框中选择策略与扫描任务关联。
  - 单击【**Save**】（保存）。
- （可选）根据需要，单击扫描任务旁边的启动按钮，启动扫描任务。
- 扫描完毕查看扫描结果。

工厂网络的自定义配置

下图为每个系统的 Nessus Manager 中创建的各种策略。过程控制系统的策略为 PCS_Enclave_Policy。



下图为扫描任务配置，该任务关联的策略为 PCS_Enclave_Policy。



补充信息

- Nessus 官方文档[100]
- Windows 扫描目标的凭证检查[101]

对性能的主要影响

- 在下面的实验中，我们评估了制造系统正常运行时 Nessus 漏洞评估工具对系统性能的影响：
- 实验 PL006.1 – Nessus 网络漏洞扫描

Nessus 的漏洞扫描对生产过程的性能影响很小，扫描过程中，网络流量无明显上升。例如，在 Nessus 扫描期间，从控制器到 OPC 的报文往返时间基本稳定。

[100] https://docs.tenable.com/nessus/Content/GettingStarted.htm
[101] https://docs.tenable.com/nessus/Content/CredentialedChecksOnWindows.htm

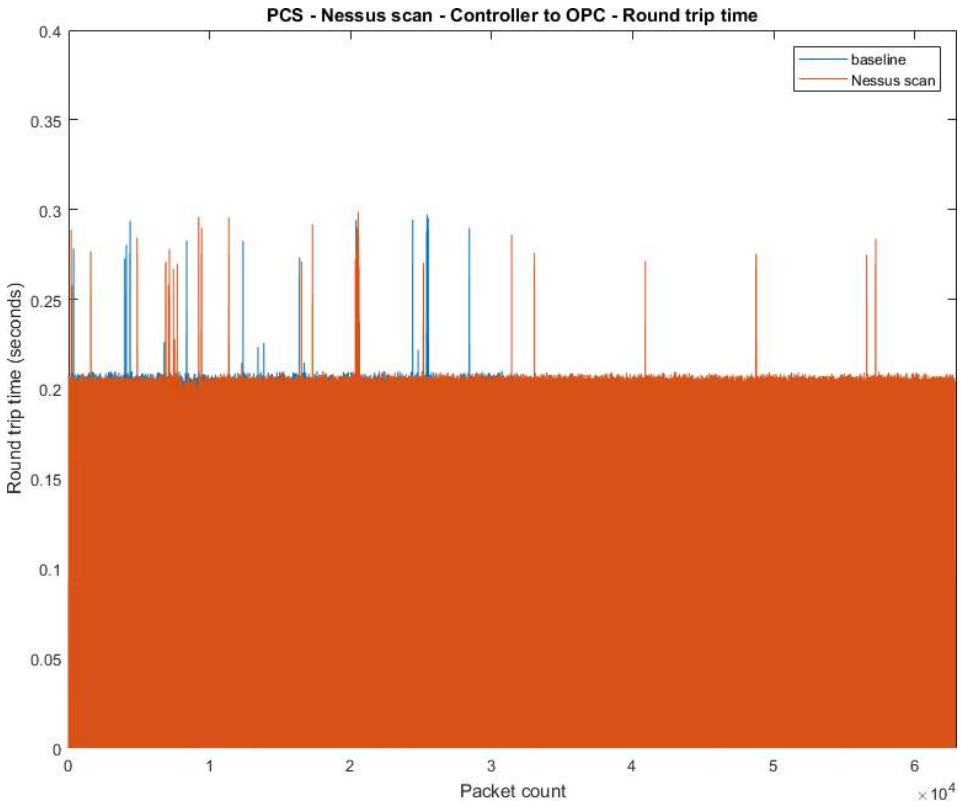


图 4-26：Nessus 扫描期间从控制器到 OPC 的报文往返时间

- 系统某些部分的网络流量略有增加，例如，Nessus 扫描期间，OPC 到 HMI 的网络使用率和平均比特率分别为 14.11%和 1.41 Mbps，而基线值分别为 13.81 %和 1.38 Mbps。可见，OPC 到 HMI 的网络使用率在 Nessus 扫描期间比基线值高出了 2.2%。
- 生产过程的性能基本不受影响。例如，产品流速和反应器压强与基线值持平。

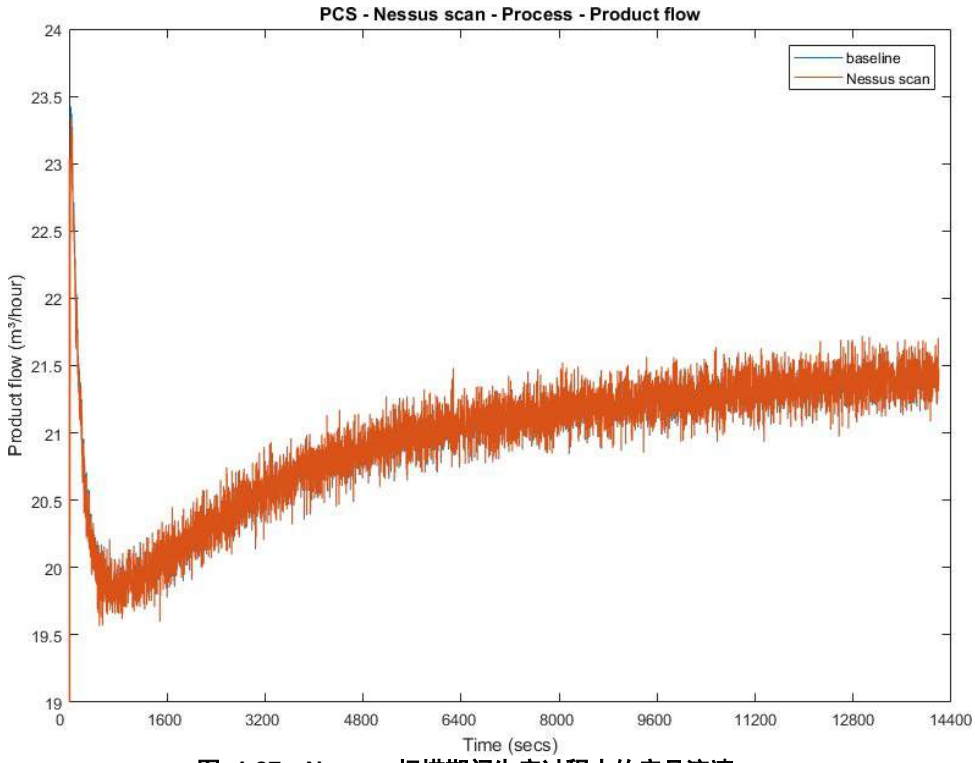


图 4-27：Nessus 扫描期间生产过程中的产品流速

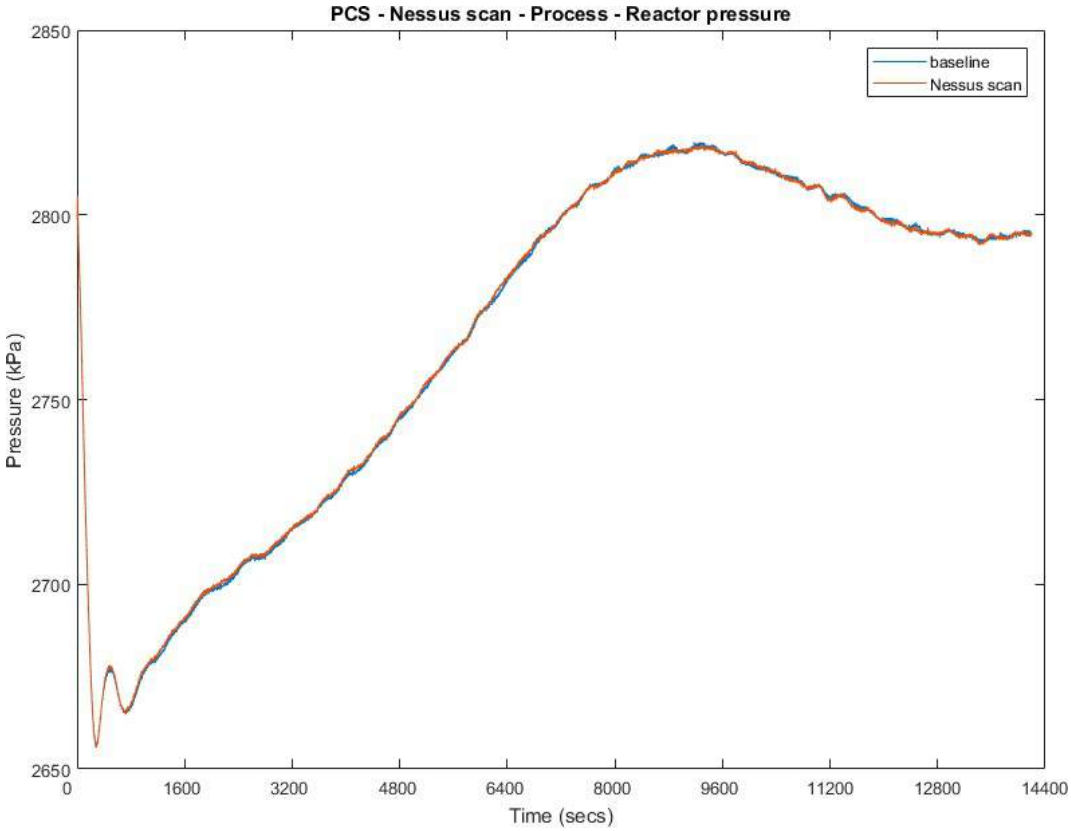


图 4-28：Nessus 扫描期间生产过程中的反应器压强

4.11.7 性能评估数据集的相关链接

- Nessus KPI 数据
- Nessus 测量数据

4.12 NamicSoft

4.12.1 技术方案概述

NamicSoft 扫描报告助手（NamicSoft Scan Report Assistant）是适用于 Nessus、Burp、Nexpose OpenVAS 和 NCATS 的解析器和报表工具。[102]

4.12.2 方案提供的技术能力

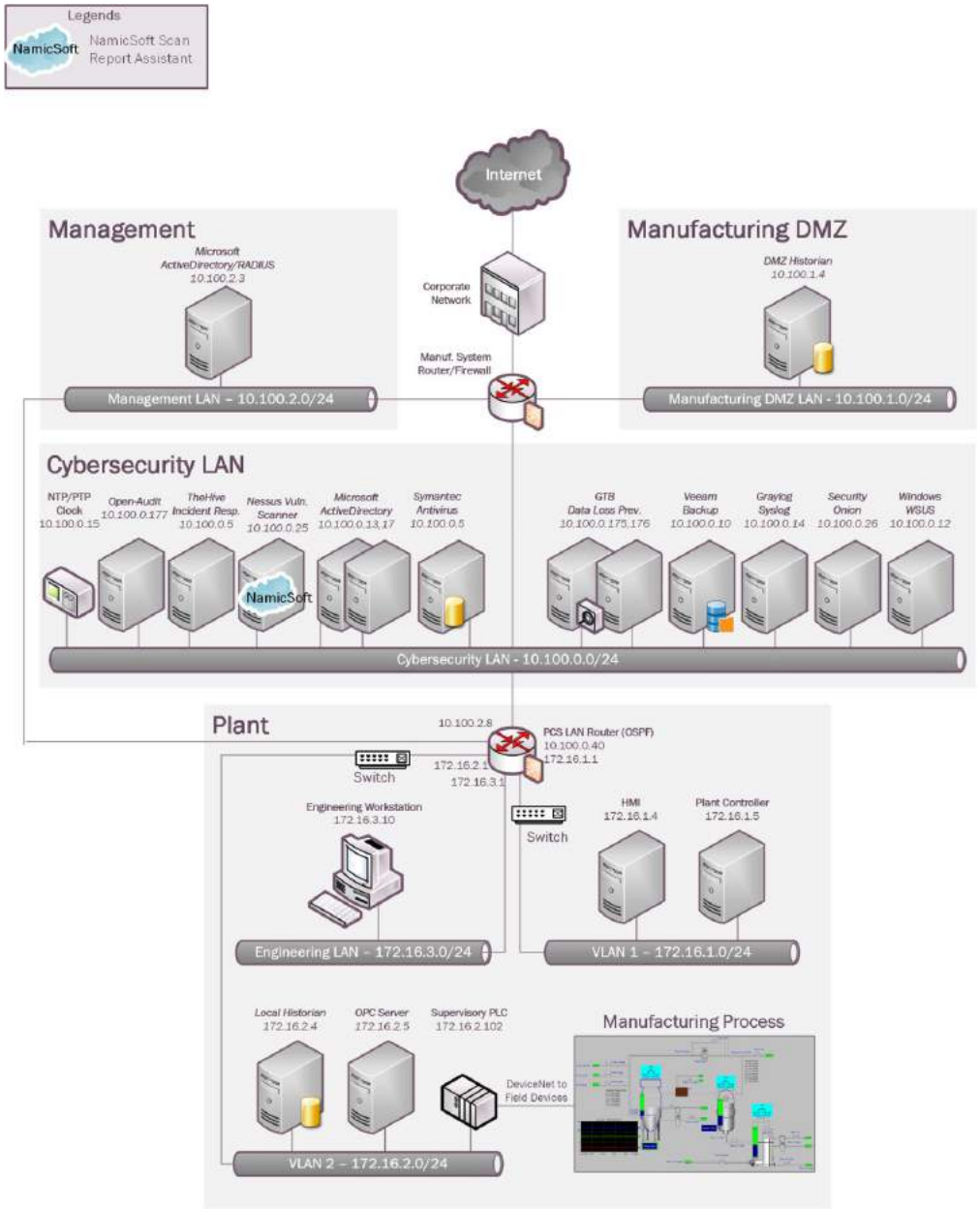
NamicSoft 提供以下技术能力（参见第 1 卷第 6 章）：

- 漏洞管理

4.12.3 方案实现的子类

ID.RA-1、DE.CM-4 和 RS.MI-3

4.12.4 方案实施架构图



[102] https://www.namicsoft.com/

4.12.5 安装说明与配置

实施方案的详细信息：

方案名	版本号
NamicSoft扫描报告助手	3.5.0

环境搭建

- 在 Nessus Scanner 服务器上安装 NamicSoft。安装详情请参见 4.11 节。
- 服务器的客户机操作系统的 IP 配置如下所示：

  - IP 地址：10.100.0.25

  - 网关：10.100.0.1

  - 子网掩码：255.255.255.0

  - 域名服务器：10.100.0.17

安装说明

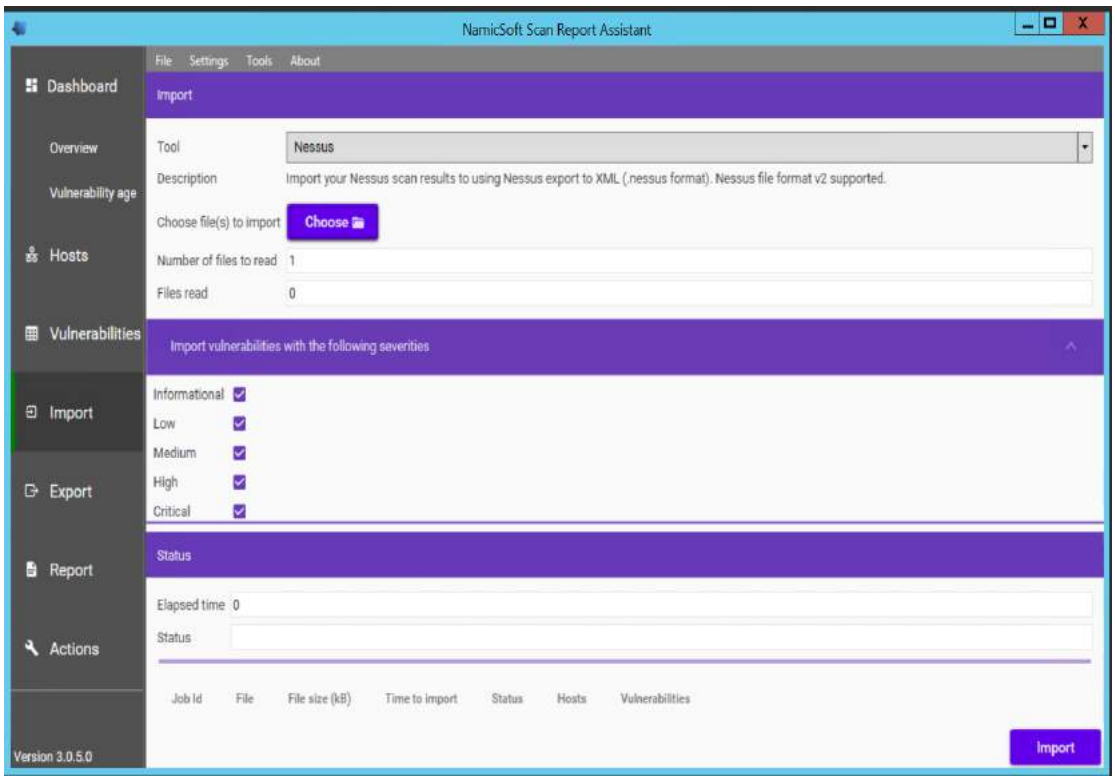
- 下载 NamicSoft[103]。
- 在 Windows PC 上运行安装程序。目前，NamicSoft 可在配置了.Net Framework 4.5 的 64 位 Windows 系统上运行。
- 双击桌面图标，启动程序。首次使用时，程序提示导入证书文件。若不导入证书，可使用免费模式。免费模式最多支持 5 个主机。

说明：软件与 Windows 用户帐号绑定，一个用户对配置所做的修改对其他用户无效。

Nessus 扫描报告配置

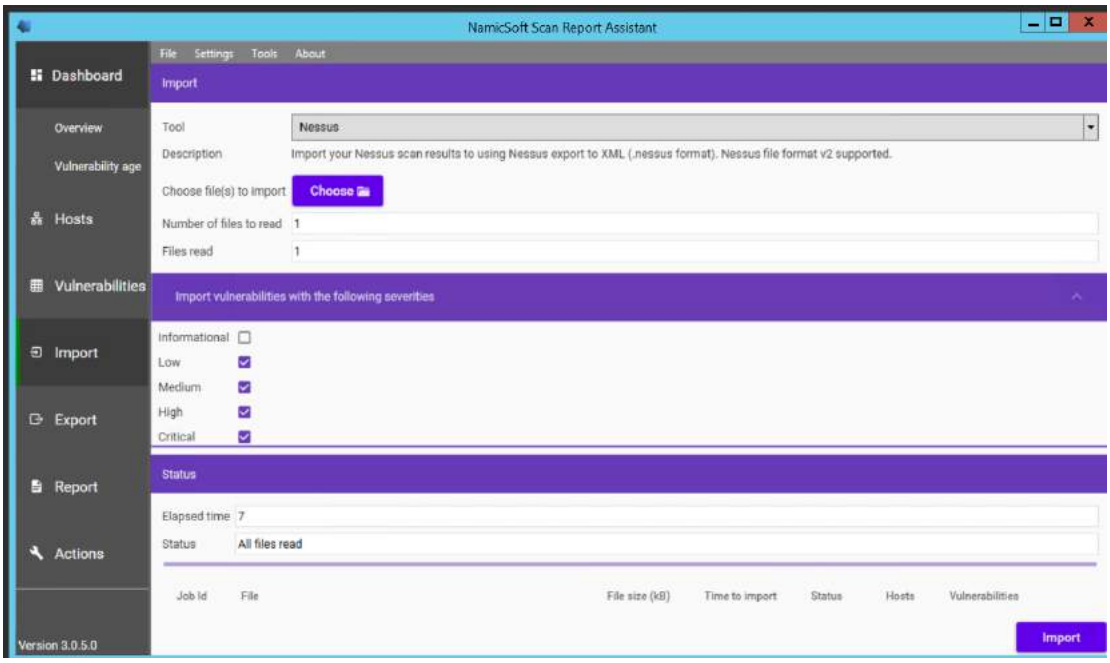
- 通过 Nessus 的 Web 界面导出 Nessus 格式的扫描报表。
- 启动 NamicSoft 报告助手。单击左侧浏览栏的【**Import**】（导入），选择 Nessus。
- 单击【**Choose**】（选择）按钮导入文件。

[103] https://www.namicsoft.com

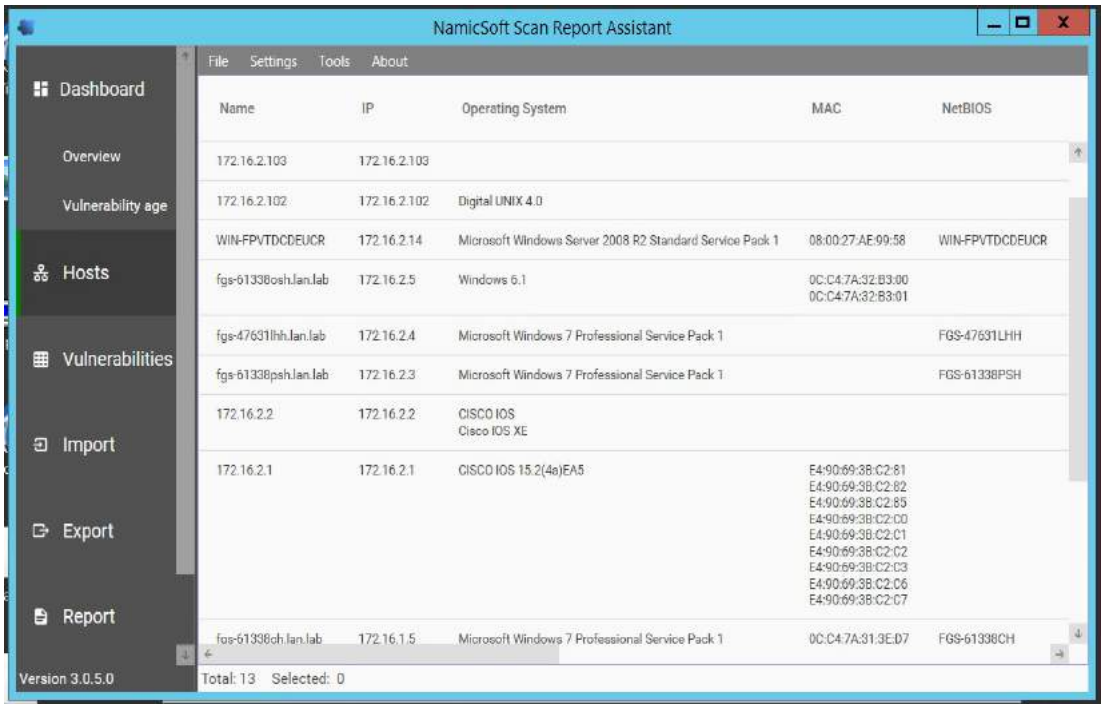


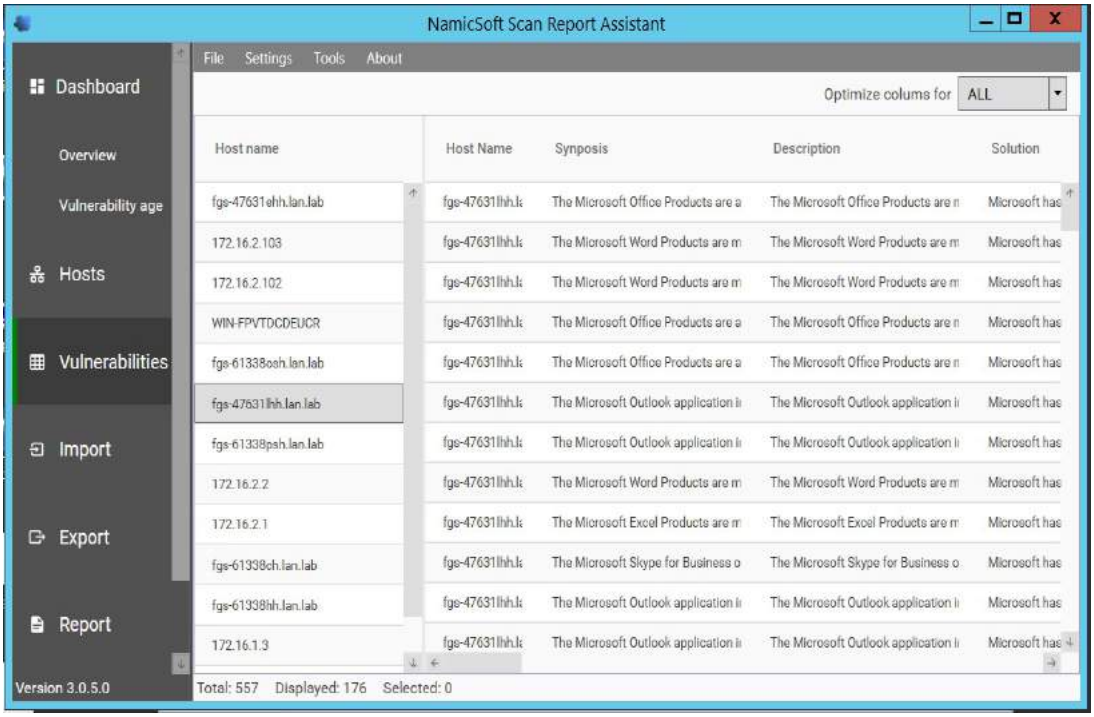
- 找到 Nessus 扫描报告。在【**Import vulnerabilities with the following severities**】(导入的漏洞风险等级)区域，选择风险等级，然后单击【**Import**】（导入）。

  例如，选择【**High**】（高）、【**Critical**】（严重）、【**Medium**】（中）和【**Low**】（低），不选择【**Informational**】（信息），如下图所示。导入完毕，状态栏会显示“All files read”（所有文件读取完毕）。

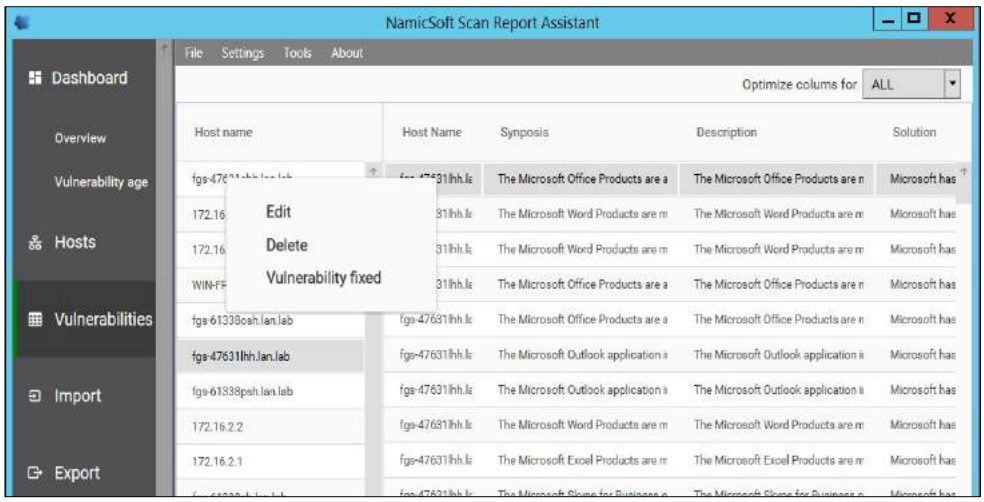


- 导入完成后，单击【**Hosts**】（主机）页签，查看主机级别的概要分析。单击【**Vulnerabilities**】（漏洞）则可查看所有漏洞。

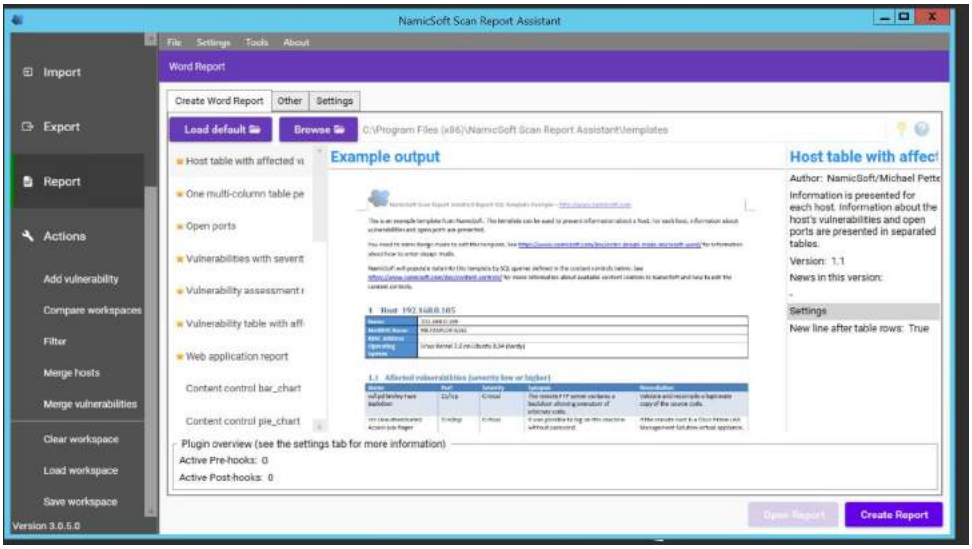




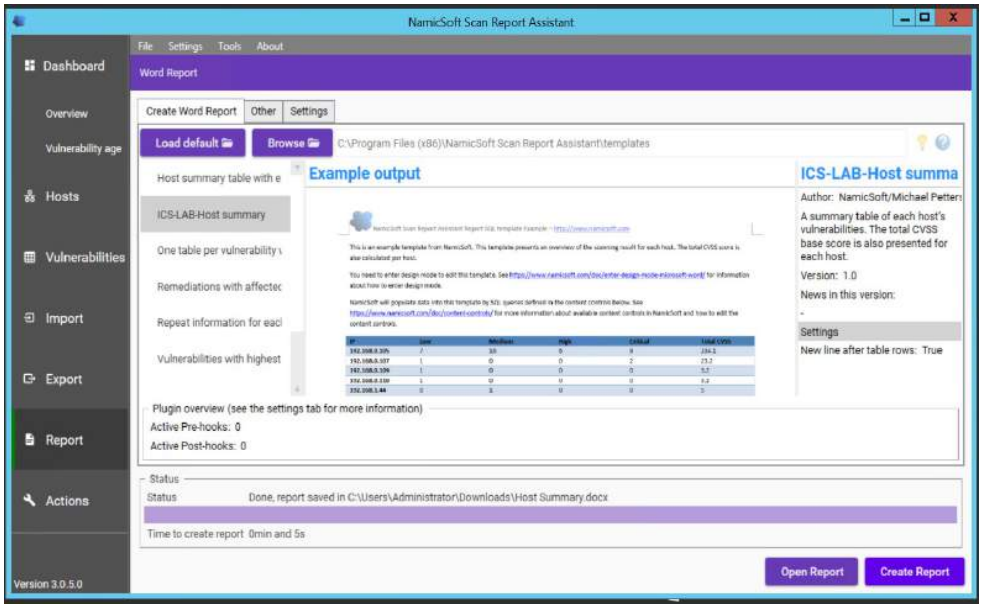
- （可选）右击漏洞，选择【**Vulnerability Fixed**】（漏洞修复），将该漏洞标记为 Fixed（已修复）。



- 单击页面左侧的【**Actions**】（操作），然后单击【**Save Workspace**】（保存工作区）。确保每次修改后保存工作区。这样，您在下次运行 NamicSoft 时可加载已保存的工作区文件。
- 击页面左侧的【**Report**】（报告），生成报告。在报表模板列表中选择默认报表模板或添加自定义模板。若采取默认模板，可在列表中选择默认模板，然后单击【**Create Report**】（创建报告）。



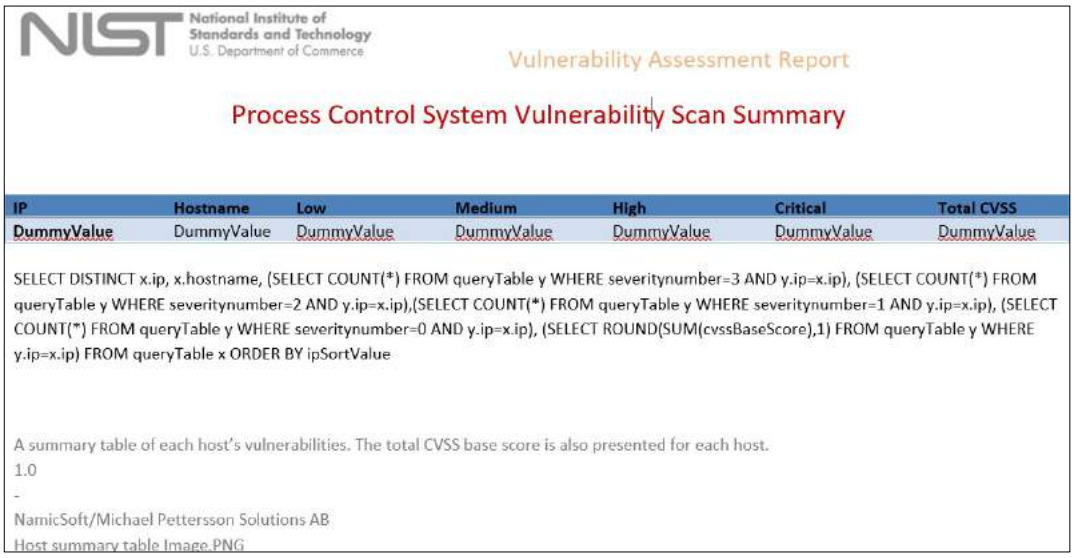
- 选择【**Open Report**】（打开报告），查看报告内容。



创建自定义模板

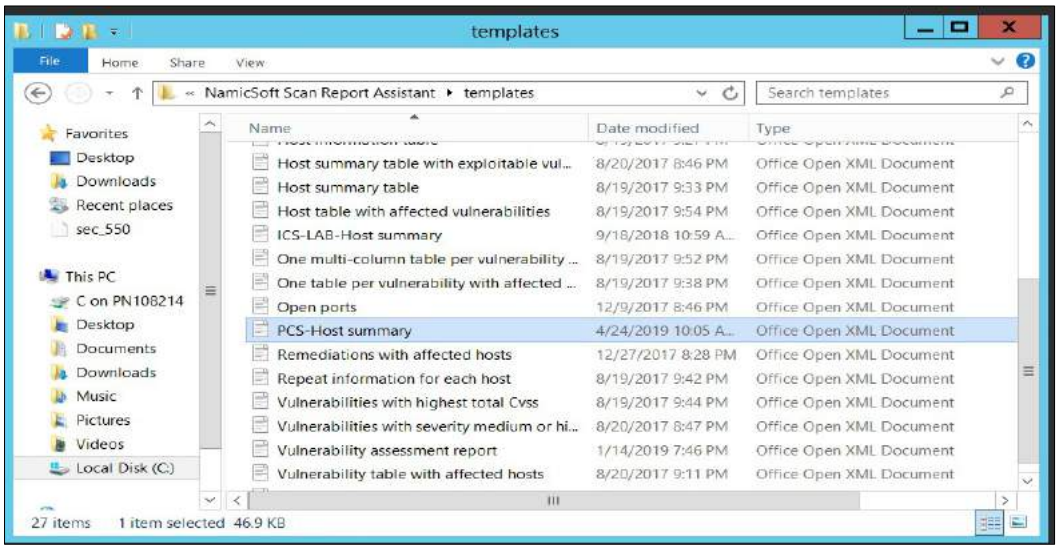
- 从 **C:\Program Files(x86)\NamicSoft Scan Report Assistant\templates** 路径下复制特定模板文件到另一个文件夹。
- 在 Microsoft Word 中打开复制的文件，开始编辑。下图显示的是为过程控制系统（PCS）创建的自定义模板文件。该报告包含主机的概要信息，并按照风险级别列出了各主机存在的漏洞。

  此外，还可创建自定义报告[104]。

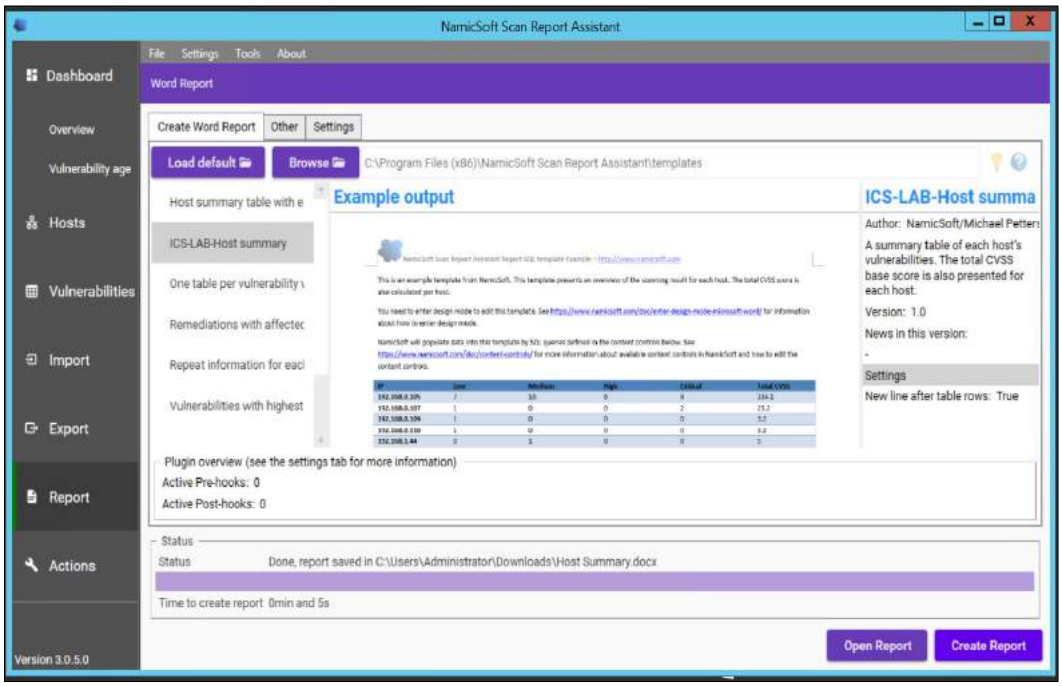


- 保存修改，输入文件名。
- 将该文件复制到 NamicSoft 机器上的 templates 目录中。例如，下图为复制到模板文件夹中保存的自定义文件 PCS-Host summary。

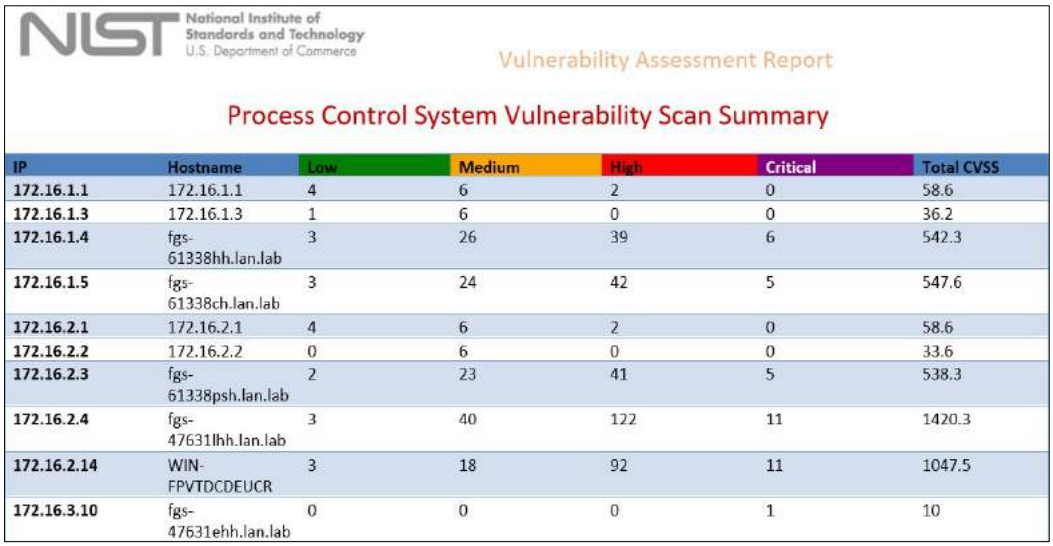
104 https://www.namicsoft.com/doc/content-controls/



- 重启 NamicSoft。自定义报告这时会现在显示在列表中。选择该模板，单击【**Create Report**】（创建报告）。



- 查输出，确认修改。



National Institute of Standards and Technology
U.S. Department of Commerce

Vulnerability Assessment Report

Process Control System Vulnerability Scan Summary

IP	Hostname	Low	Medium	High	Critical	Total CVSS
172.16.1.1	172.16.1.1	4	6	2	0	58.6
172.16.1.3	172.16.1.3	1	6	0	0	36.2
172.16.1.4	fgs-61338hh.lan.lab	3	26	39	6	542.3
172.16.1.5	fgs-61338ch.lan.lab	3	24	42	5	547.6
172.16.2.1	172.16.2.1	4	6	2	0	58.6
172.16.2.2	172.16.2.2	0	6	0	0	33.6
172.16.2.3	fgs-61338psh.lan.lab	2	23	41	5	538.3
172.16.2.4	fgs-47631lhh.lan.lab	3	40	122	11	1420.3
172.16.2.14	WIN-FPVTDCDEUCR	3	18	92	11	1047.5
172.16.3.10	fgs-47631ehh.lan.lab	0	0	0	1	10

- （可选）选择 **Action > Compare Workspaces**（操作 > 比较工作区），就上次扫描后已修复的漏洞创建报告。步骤如下：
  - 加载已完成扫描任务的 Nessus 扫描结果，另存为工作区。
  - 在用户界面上清除工作区（或重启 NamicSoft）。
  - 加载 Nessus 的最近一次扫描结果。
  - 选择 **Actions > Compare workspaces**（操作 > 比较工作区）。单击当前工作区的【**Compare**】（比较），将工作区 2 与刚保存的工作区进行比较。
  - 选择【**Excel output file (target)**】（输出 Excel 文件（目标））。
  - 单击【**Compare Workspaces**】（比较工作区）。

4.12.6 对性能的主要影响

考虑到 NamicSoft 的安装位置和使用方式（用制造系统外部的其他软件抓取的漏洞数据进行离线分析），没有测试其对系统性能的影响。

4.12.7 性能评估数据集的相关链接

无

4.13 TheHive 项目

4.13.1 技术方案概述

TheHive 项目是可扩展的免费开源的安全事件响应平台[105]。

4.13.2 方案提供的技术能力

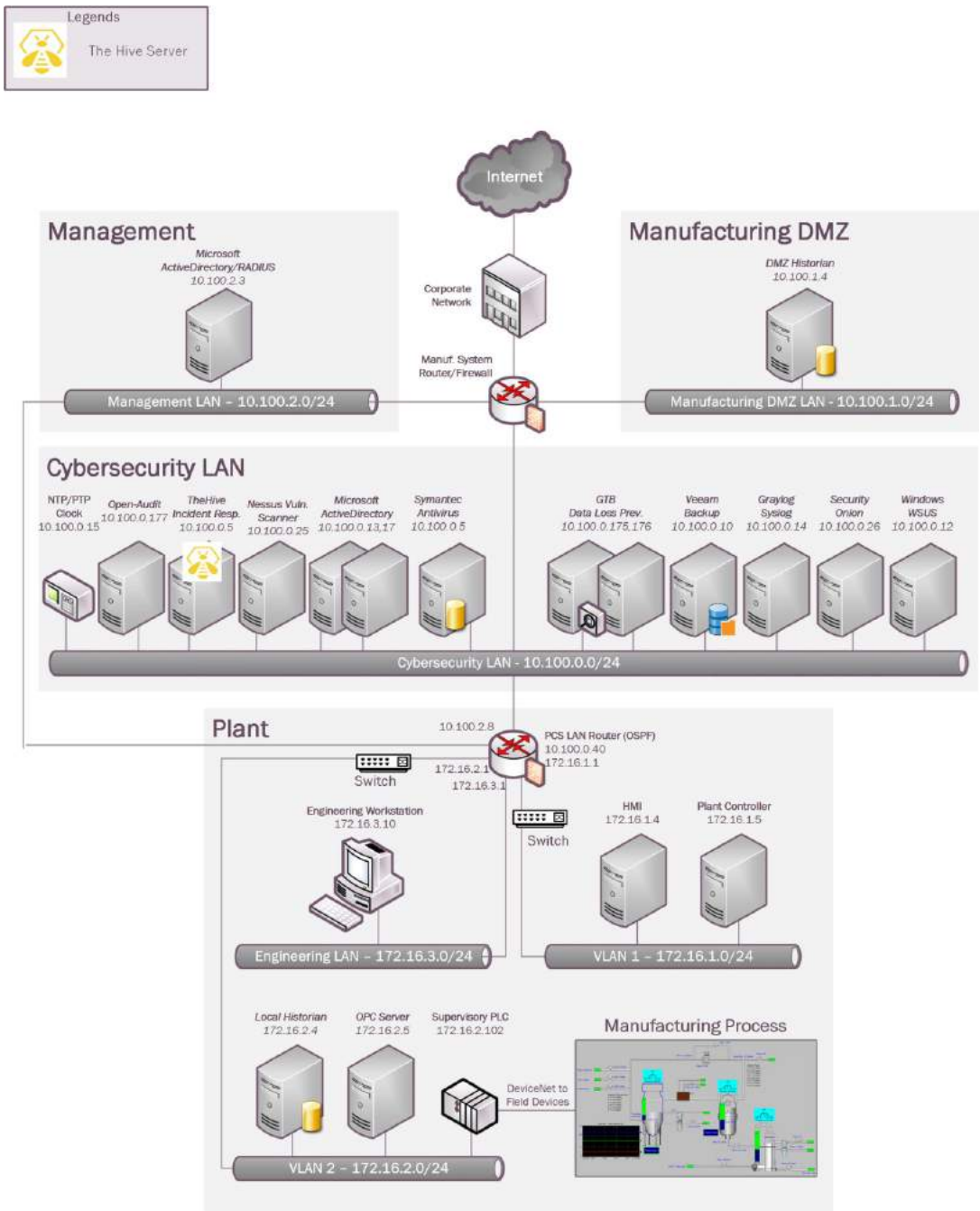
TheHive 项目提供以下技术能力（参见第 1 卷第 6 章）：

- 安全事件管理

4.13.3 方案实现的子类

RS.MI-2 和 RS.MI-3

4.13.4 方案实施架构图



105 https://thehive-project.org/

4.13.5 安装说明与配置

实施方案的详细信息：

方案名	版本号	硬件规格
TheHive	3.0.10	Hyper-V虚拟机： • 处理器：虚拟双核 • 内存：4 GB • 磁盘空间：50 GB • 网络：1个接口 • 操作系统：Ubuntu 16.04

环境搭建

- 将厂商提供的预配置培训虚拟机部署在 Hyper-V 宿主服务器上。硬件规格见上表。
- 客户机操作系统的 IP 信息如下：

  - IP 地址：10.100.0.51

  - 网关：10.100.0.1

  - 子网掩码：255.255.255.0

  - 域名服务器：10.100.0.17

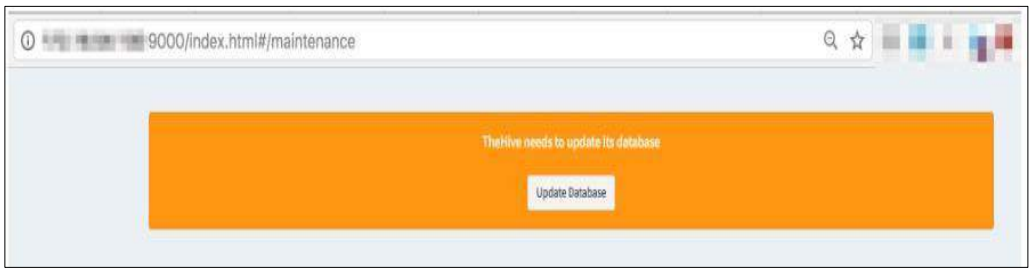
安装说明

- 下载软件[106]。
- 在所支持的 Linux 版本上安装二进制文件[107]。
- 按说明完成配置过程。完成后，输入

  http://<ip-address_of_hive_server>:9000 访问 TheHive。

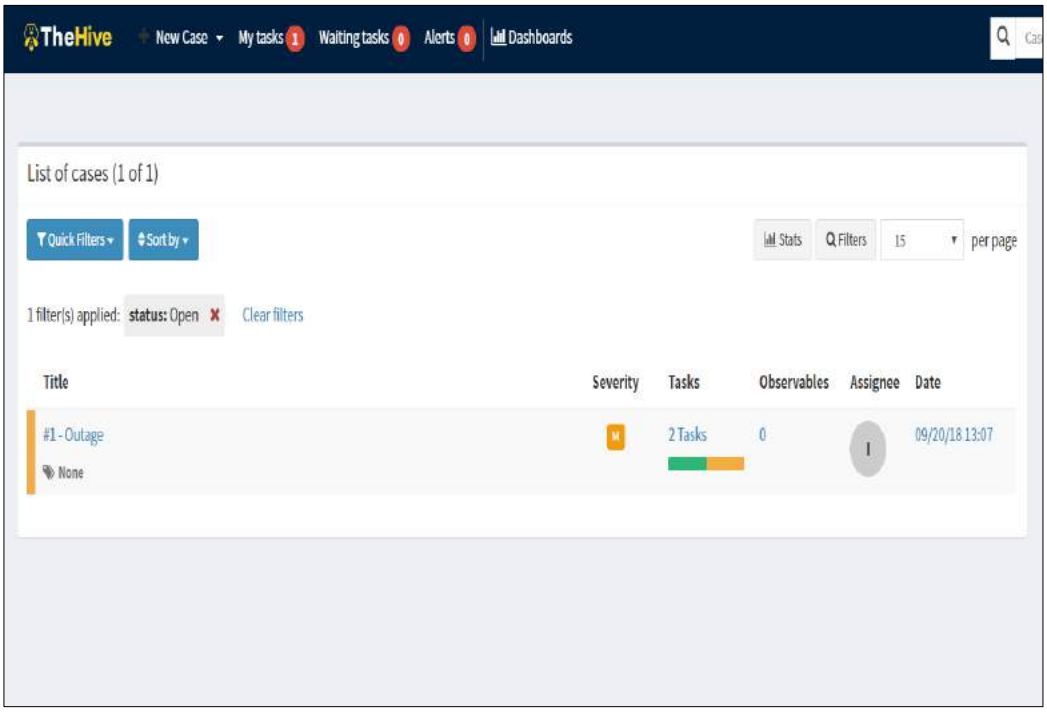
通过 Web 浏览器进行其他配置

- 首次访问 TheHive 时，需单击【**Update Database**】（更新数据库）按钮创建关联的数据库，如下图所示。

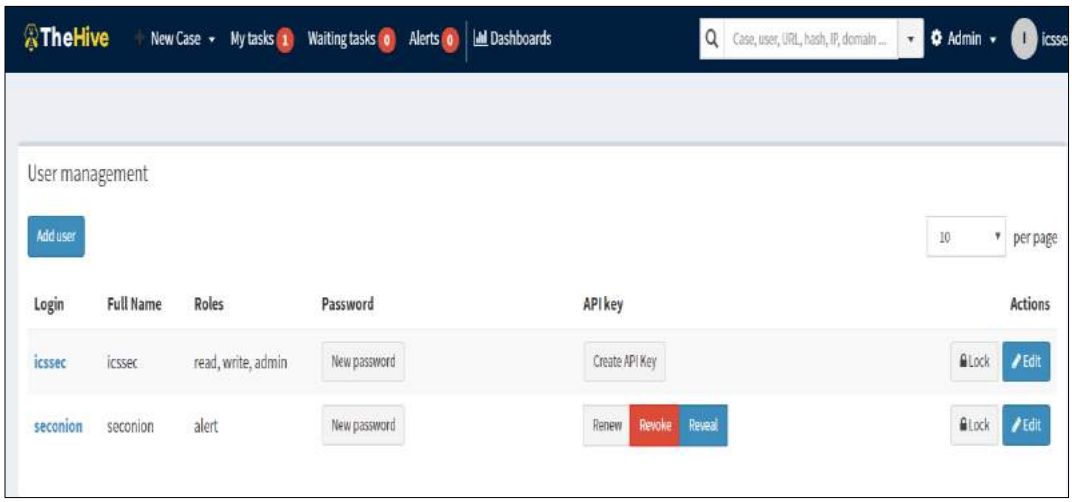


- 根据配置向导配置用户账户。
- 利用用户凭证登录 TheHive 链接。默认打开的页面会显示分配给当前账户的事件列表。对于新安装的 TheHive，页面上无数据展示。

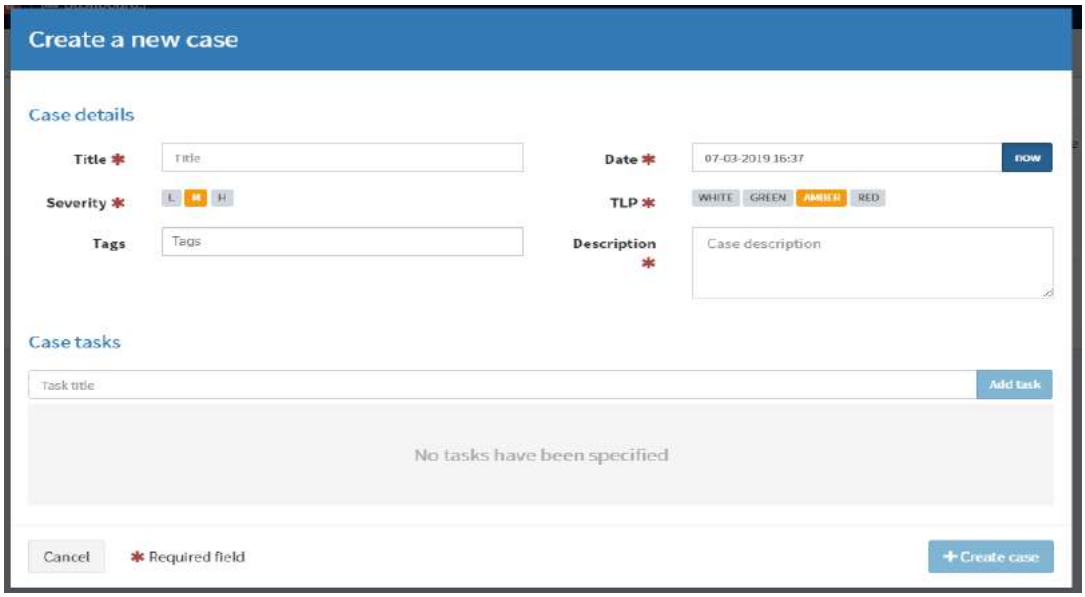
[106] https://github.com/TheHive-Project/TheHive
[107] https://github.com/TheHive-Project/TheHiveDocs/blob/master/installation/install-guide.md



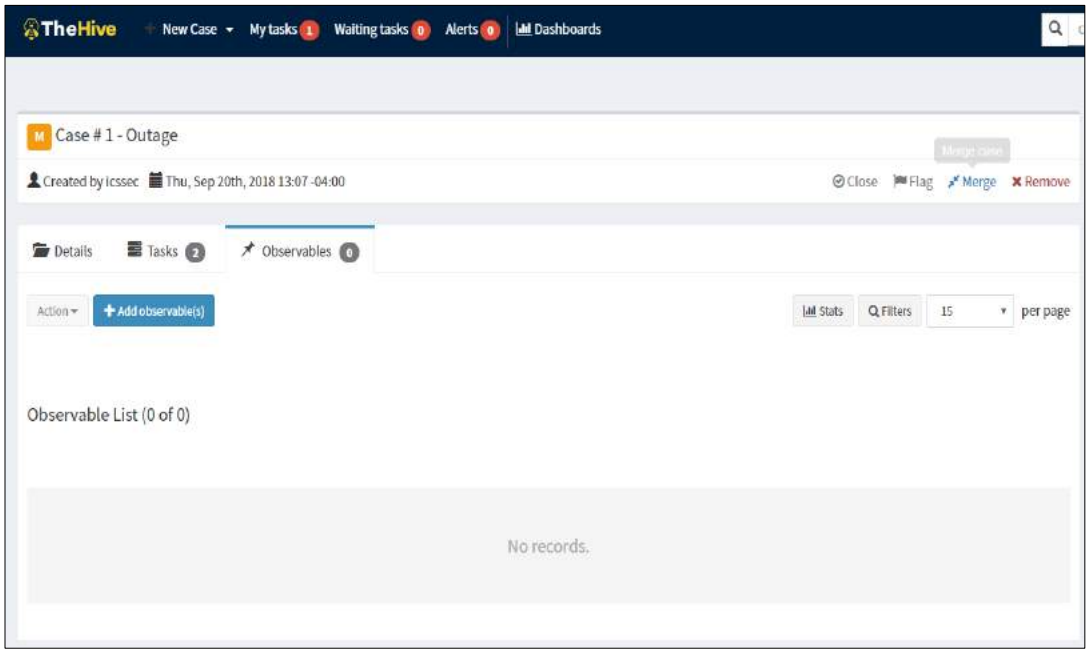
- 选择 **Admin > Users > User management**（管理 > 用户 > 用户管理），添加其他用户帐号。单击【**Add user**】（新建用户），添加新用户。

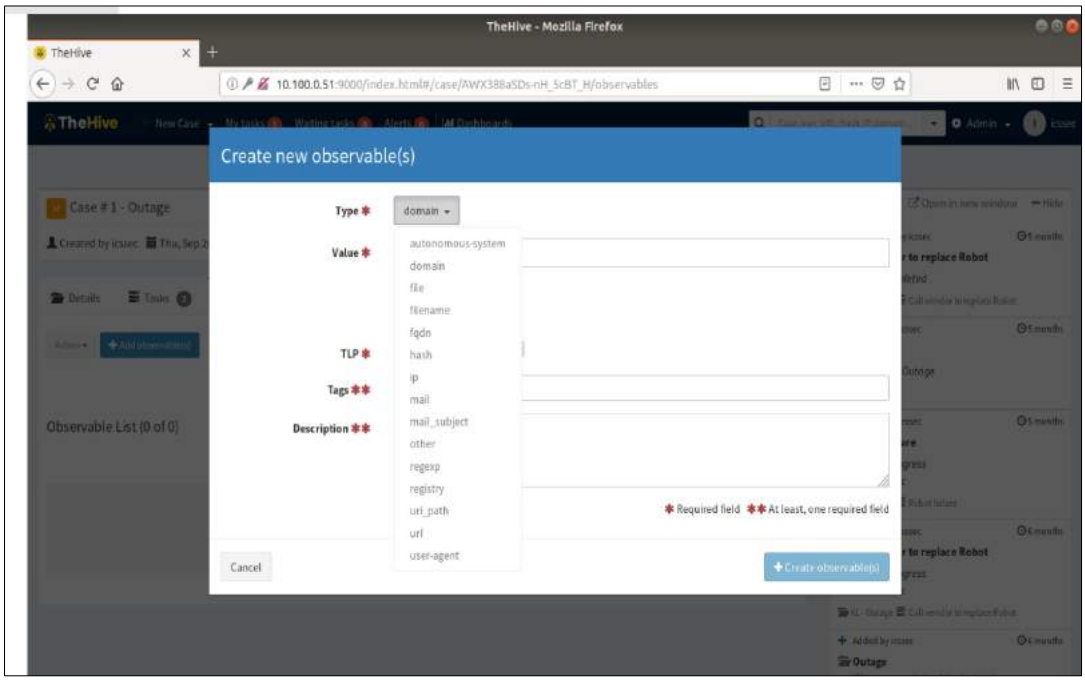


- 按以下步骤，创建新事故/事件：
  - 单击【**New Case**】（新建事件）菜单，填写事件详细信息。
  - 单击【**Add Task**】（新建任务），在该事件下创建新任务。每个任务均可分配给分析师执行。默认情况下，任务无负责人，除非用户单击该任务或将其从页面顶端菜单栏中的等待执行的任务队列中移出。
  - 配置完毕，单击【**Create case**】（新建事件）按钮。



- 按以下步骤新建自定义事件模板：
  - 在页面右上角，选择 **Admin > Case Templates**（管理 > 事件模板）。
  - 单击【**New Case Template**】（新建事件模板）。
  - 填写各字段信息。
  - 单击【**Save Case Template**】（保存事件模板）。
- （可选）打开一个事件，单击【**Observables**】（可观察对象）页签，然后单击【**Add observables**】（添加可观察对象），在事件中添加自定义可观察对象，如域名、IP 地址、文件和文件名等。此外，可将可观察对象标记为感染指标（IOC）。





- （可选）利用 Cortex 引擎[108]（http://<ip_of_hive_server>:9001）对可观察对象或 IOC（如域名、IP 地址和哈希）进行详细分析。为此，在 Cortex 中启用或创建分析器。

  配置 Cortex 的主要步骤如下：

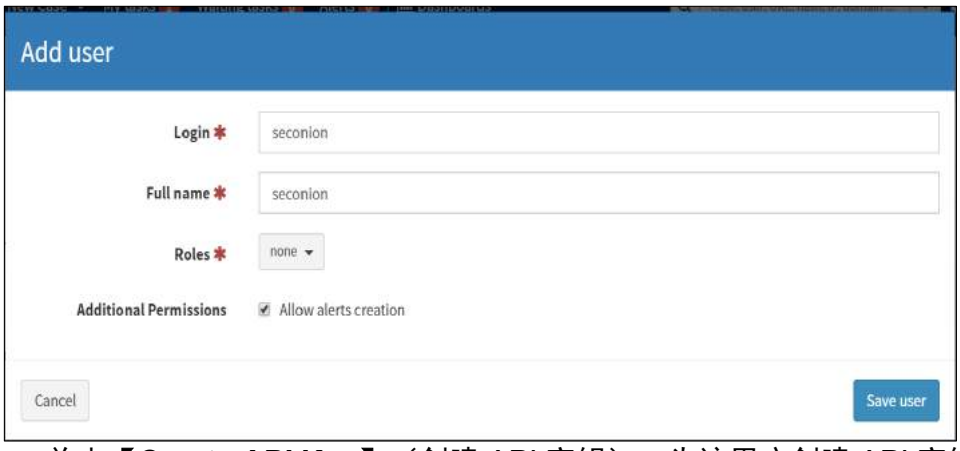
  - 安装 Cortex；
  - 创建管理员帐号；
  - 创建组织；
  - 创建组织管理员帐号；
  - 启用或配置分析器；
  - 集成 Hive 实例。

集成安全洋葱

将安全洋葱实例与 Hive 实例集成，为安全洋葱生成的 IDS 告警创建事件。

[108] https://github.com/TheHive- Project/CortexDocs

- 在 Hive 中创建专用用户帐号，为其分配【**Allow alerts creation**】（允许创建告警）权限。安全起见，将用户帐号的【**Roles**】（角色）参数设置为【**none**】（无）。



- 单击【**Create API Key**】（创建 API 密钥），为该用户创建 API 密钥。
- （在安全洋葱服务器上执行）在与 Hive Server 的 IP 地址连接的安全洋葱的**/etc./elastalert/rules** 目录下，创建新规则文件 **hive.yaml**，如下图所示[109]。

```
# hive.yaml
# Elastalert rule to forward IDS alerts from Security Onion to a specified TheHive instance.
#
es_host: elasticsearch
es_port: 9200
name: TheHive - New IDS Alert!
type: frequency
index: "*:logstash-ids*"
num_events: 1
timeframe:
   minutes: 10
buffer_time:
   minutes: 10
allow_buffer_time_overlap: true

filter:
- term:
   event_type: "snort"

alert: hivealerter

hive_connection:
  hive_host: https://10.100.0.51
  hive_port: 9000
  hive_apikey: APIKEY
```


4.13.6 对性能的主要影响

考虑到 Hive 项目的一般安装位置和使用方式（在制造系统外），没有测试其对系统性能的影响。

4.13.7 性能评估数据集的相关链接

无

[109] https://securityonion.readthedocs.io/en/latest/hive.html#thehive.

4.14 微软文件加密系统

4.14.1 技术方案概述

文件加密系统（EFS）是 Windows 提供的文件级加密工具，为文件和目录提供额外安全保护，利用公钥系统为 NTFS 文件系统卷上的文件提供加密保护[110]。

4.14.2 方案提供的技术能力

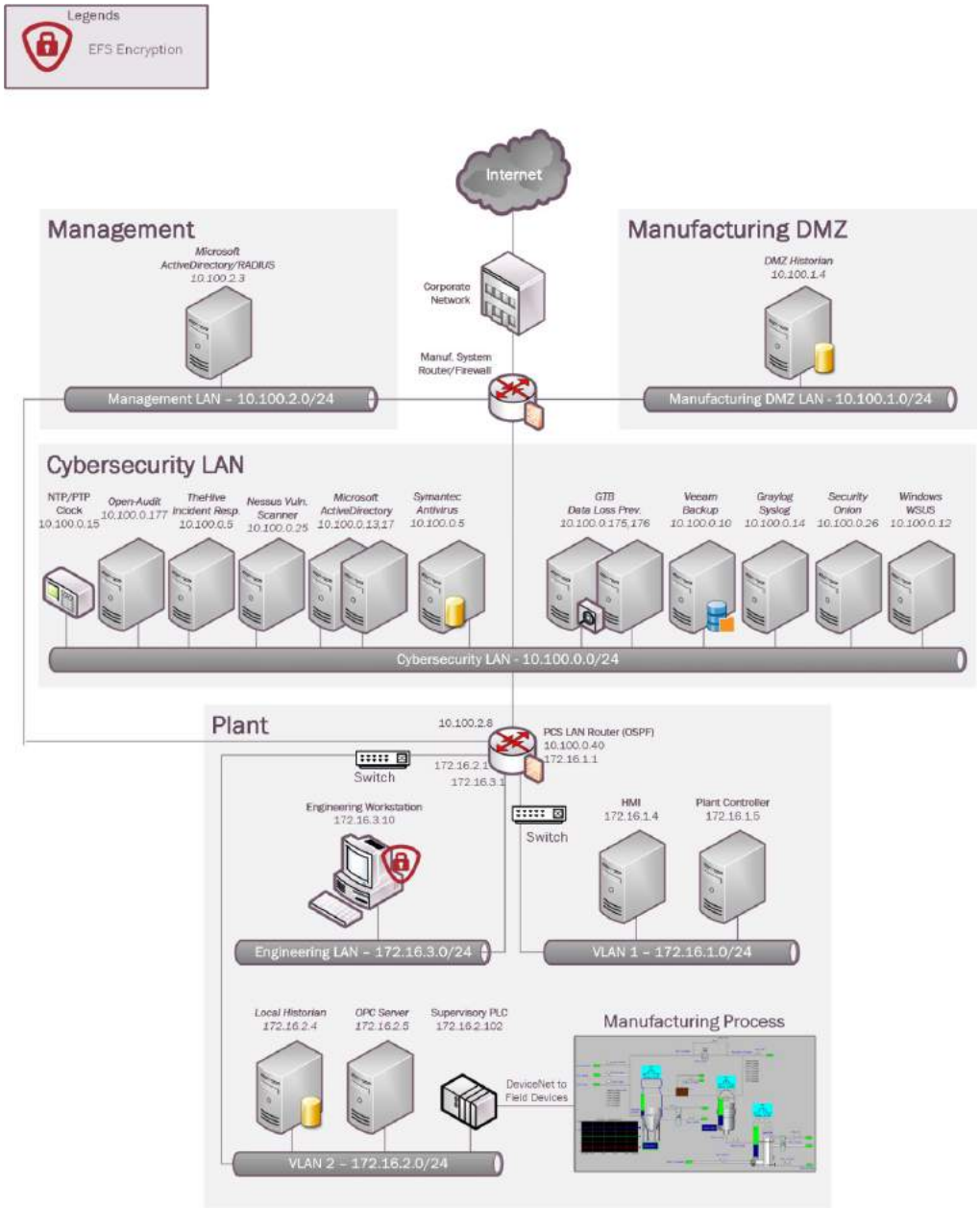
微软 EFS 提供以下技术能力（参见第 1 卷第 6 章）：

- 加密

4.14.3 方案实现的子类

PR.DS-5

4.14.4 方案实施架构图



[110] https://docs.microsoft.com/en-us/windows/desktop/fileio/file-encryption

4.14.5 安装说明与配置

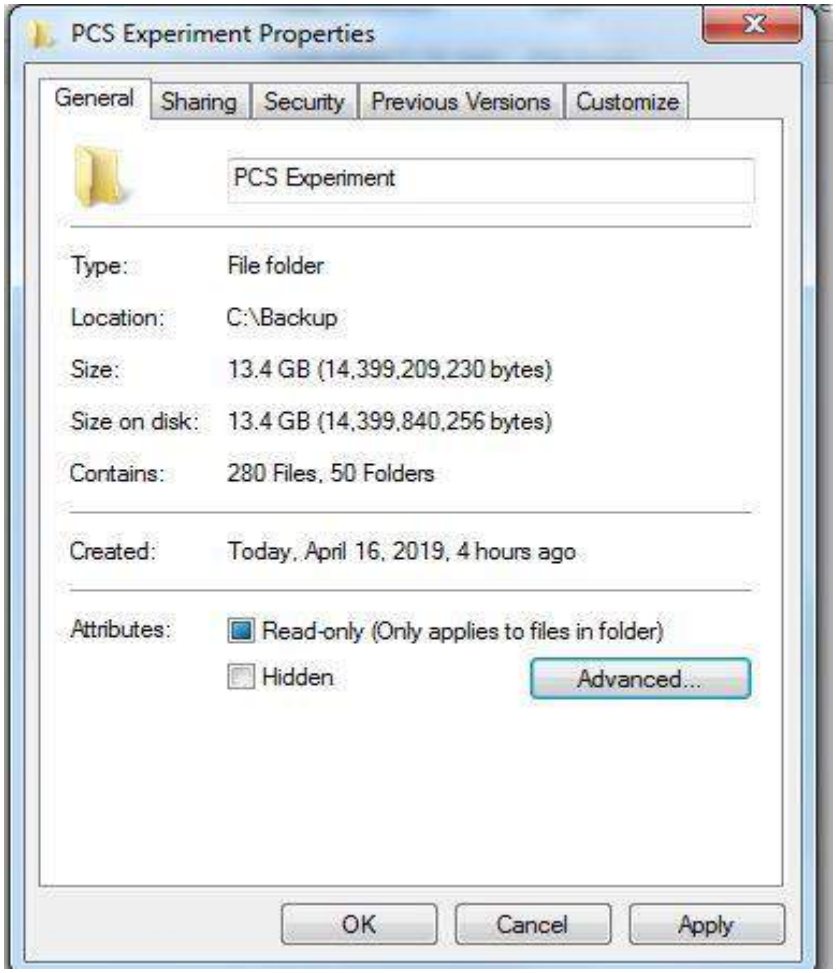
环境搭建

Windows EFS 用于对工厂的工程师站上的敏感文件夹进行加密。

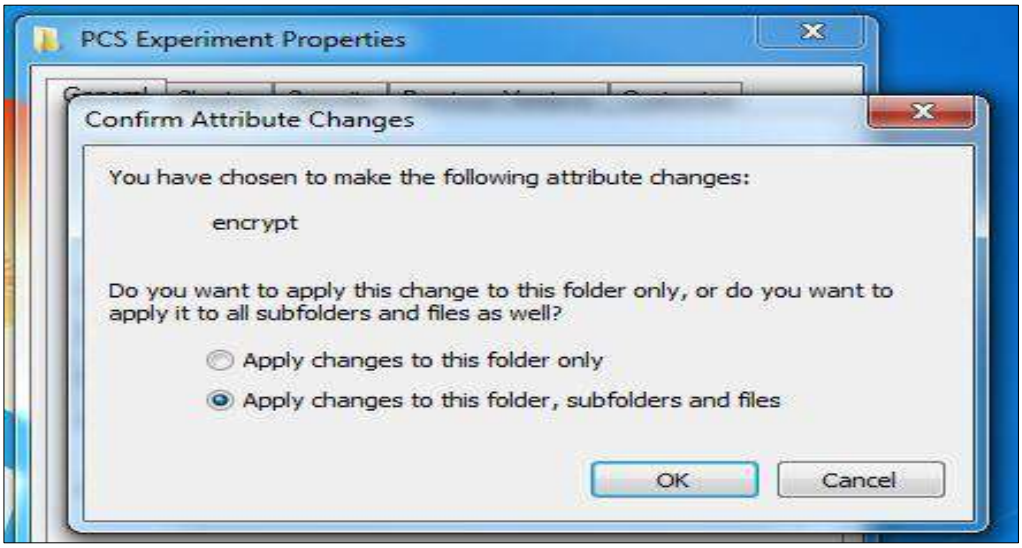
主机名	IP地址	操作系统
工程师站	172.16.3.10	Windows 7专业版（64位）

加密操作指南

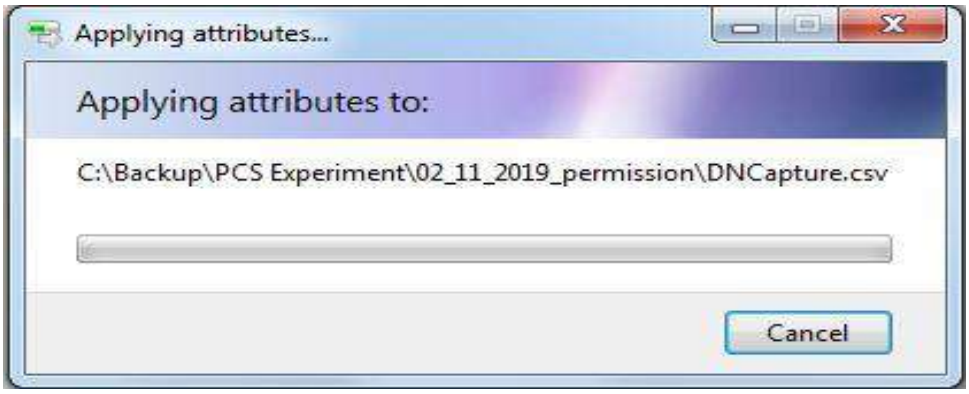
- 选择要加密的父文件夹。右击文件夹名称，选择【**Properties**】（属性），单击【**General**】（常规）页签，然后单击【**Advanced**】（高级）按钮。



- 选择【**Apply changes to folder, subfolders and files**】（将变更应用至文件夹、子文件夹和文件），单击【**OK**】（确定）。



- 单击【**Apply**】（应用），开始加密。



- 加密完毕，查看文件夹是否变成绿色，如下图所示。添加到该父文件夹中的任何新文件夹都会自动加密。

- 采取下列步骤对加密密钥进行备份：

  - 双击弹出的消息或选择 **Control Panel > All Control Panel Items > User Accounts > Manage your encryption certificates**（控制面板 > 所有控制面板项 > 用户帐号 > 管理加密证书）。

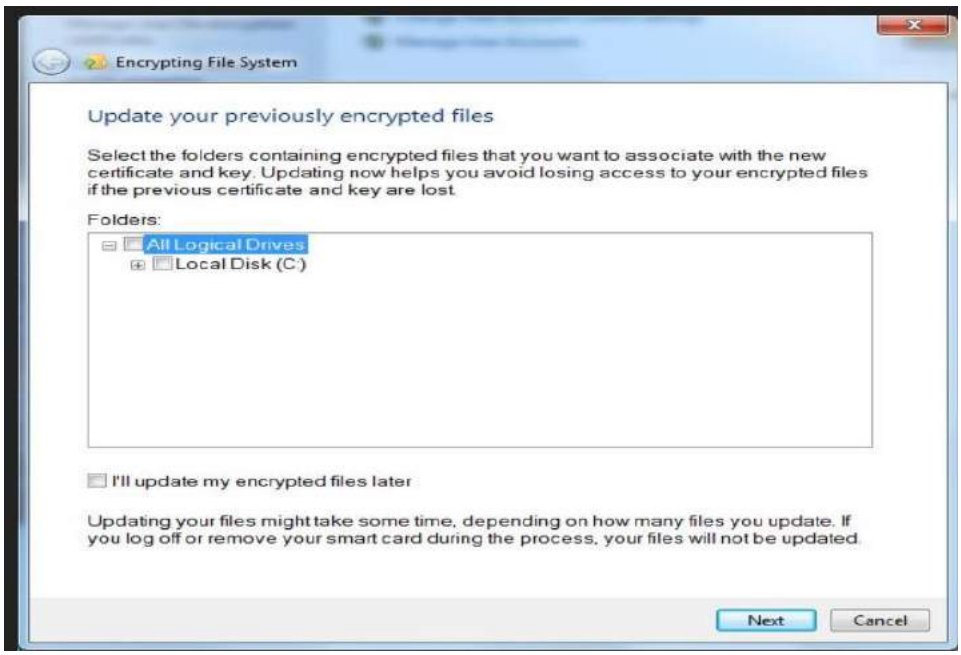
    说明：若系统为 Windows 10，则加密过程会有差别。

- 单击【**Next**】（下一步）。

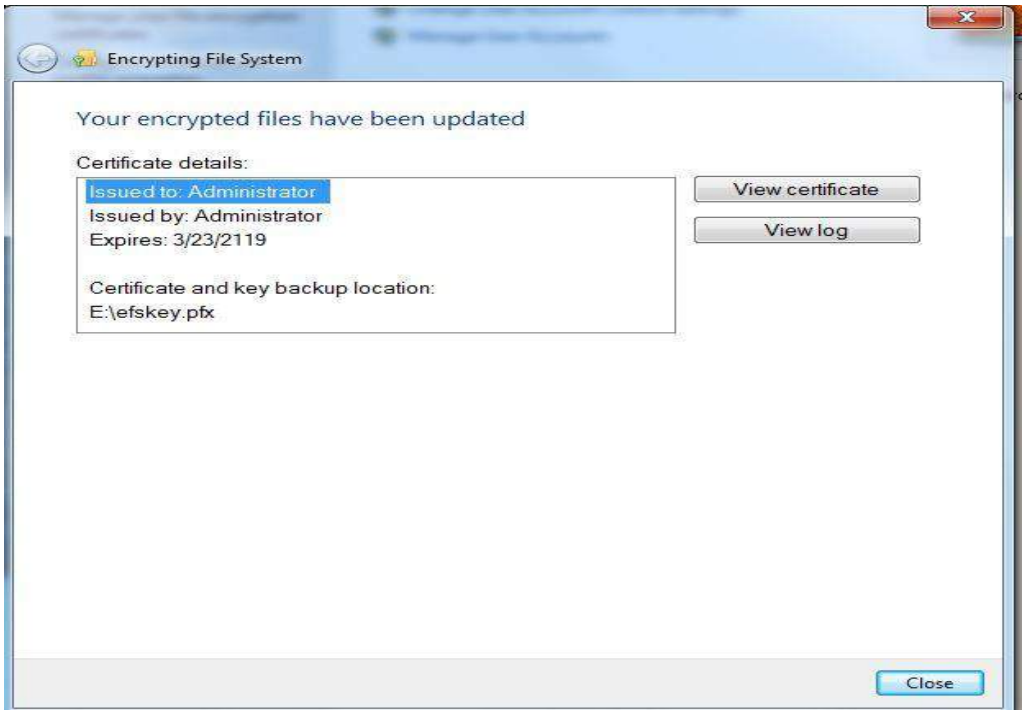
- 选择当前证书或创建新证书。可采取默认配置。

- 选择【**Back up the certificate and key now**】（现在备份证书和密钥）。单击【**Browse**】（浏览）按钮，选择 pfx 绑定文件的存储位置，例如 U 盘。输入密码，添加额外保护。

- 择对应文件夹与新证书和密钥相关联，或者选择【**I'll update my encrypted files later**】（将稍后更新我的加密文件）。单击【**Next**】（下一步）。



- 界面会弹出如下提示消息，说明恢复密钥已成功备份。



在另一台计算机上使用加密文件

若您想在另一台计算机上使用加密文件，需将您计算机或 U 盘中的 EFS 证书和密钥导出，然后再导入到这台计算机。

对性能的主要影响

在下面的实验中，我们评估了制造系统正常运行时微软 EFS 工具对系统性能的影响：

实验 PL013.1 – 在 HMI 主机上开启文件级加密

FactoryTalk HMI 应用程序中指定了专门的文件夹用以保存 HMI 数据的日志文件。EFS 工具用于加密本实验中的数据日志文件。

我们观察到，EFS 激活后加密数据日志文件时（尤其是 HMI 的初始操作时）会对计算资源性能产生明显影响。处理器利用率在实验的第 450~750 秒时间内上升幅度较大,在前 3000 秒内偶有上升。在实验开始的前 800 秒，磁盘写入速度上升较快。HMI 应用程序试图在初始化阶段访问数据日志文件，因此对性能的影响主要集中在操作初期。

网络方面未出现重大性能影响。在 EFS 启用前后，HMI 和 OPC 之间的双向报文往返时间基本保持一致。

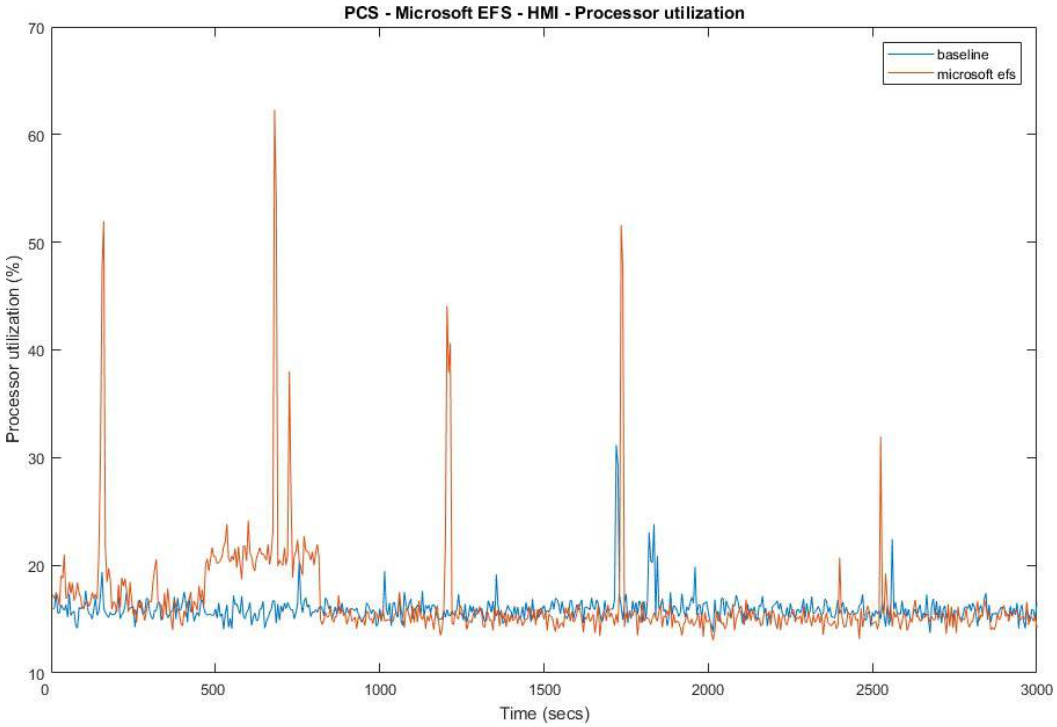


图 4-29：EFS 启用前（蓝）后（红）HMI 计算机处理器占用率对比

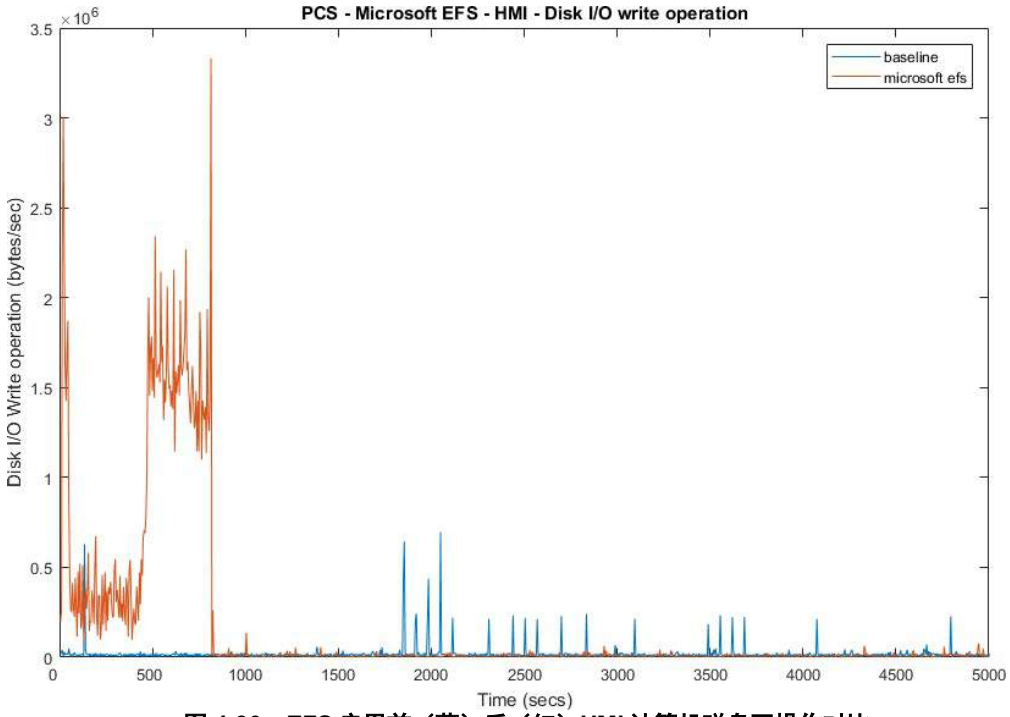


图 4-30：EFS 启用前（蓝）后（红）HMI 计算机磁盘写操作对比

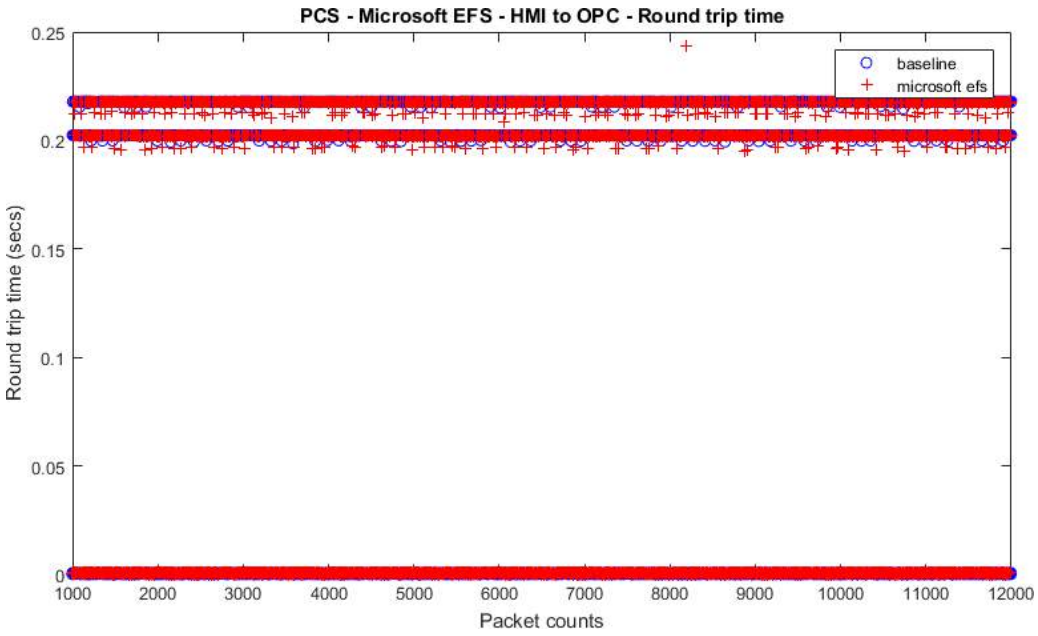


图 4-31：EFS 启用前（蓝）后（红）HMI 到 OPC 的报文往返时间对比

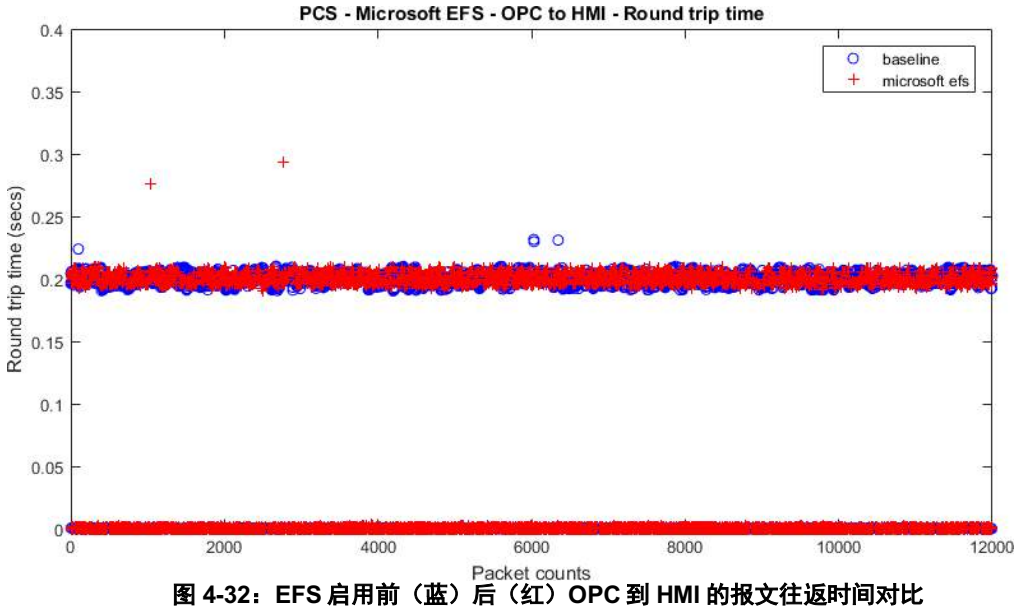


图 4-32：EFS 启用前（蓝）后（红）OPC 到 HMI 的报文往返时间对比

HMI 应用程序无法访问数据日志文件，也就无法记录新操作数据。HMI 对发送给操作员的错误/警告消息进行了标记。

对应用程序的相关文件或文件夹加密时务必谨慎。该操作对生产过程的性能影响为 HMI 无法记录数据文件。

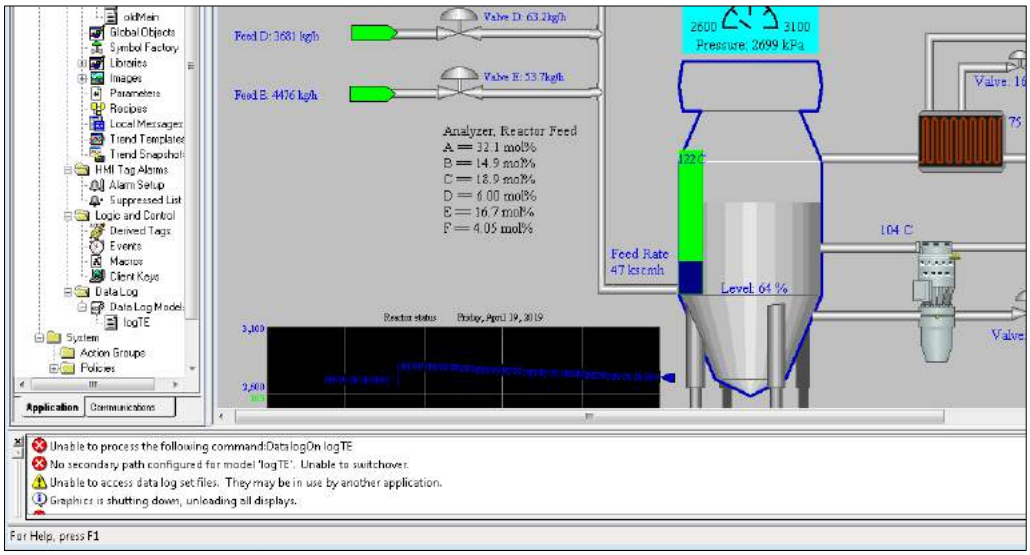


图 4-33：HMI 屏幕上显示警告消息【Unable to access data log set files】（无法访问数据日志集文件）

4.14.6 性能评估数据集的相关链接

- 文件加密 KPI 数据
- 文件加密测量数据

4.15 GTB Inspector

4.15.1 技术方案概述

GTB Technologies 提供的 GTB Inspector 是一种数据泄露防护（DLP）方案，可对网络出流量进行检测、记录和阻断。Inspector 可检测并阻断 FTP、邮件、HTTP、HTTPS（SSL/TLS）、带指纹的文件、USB 防护以及配置的其他外泄方法。Inspector 分析所有网络流量，将数据上报 GTB 中央控制台（GTB Central Console）。根据告警需要，中央控制台可提供群组和升级路径功能。

重点说明：

- 所有 DLP 产品的实施成本都很高。
- 所有 DLP 产品均需大量的配置工作。

4.15.2 方案提供的技术能力

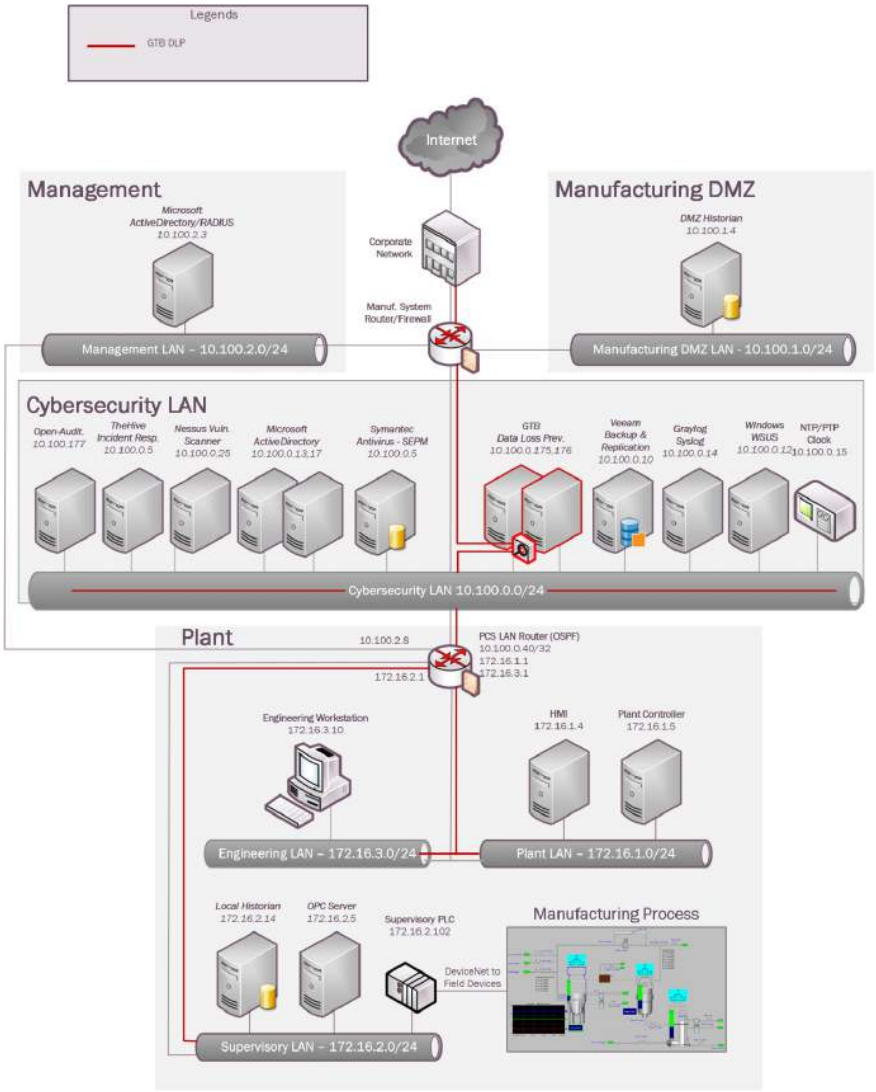
GTB Inspector 提供以下技术能力（参见第 1 卷第 6 章）：

- 数据泄露防护

4.15.3 方案实现的子类

PR.DS-5

4.15.4 方案实施架构图



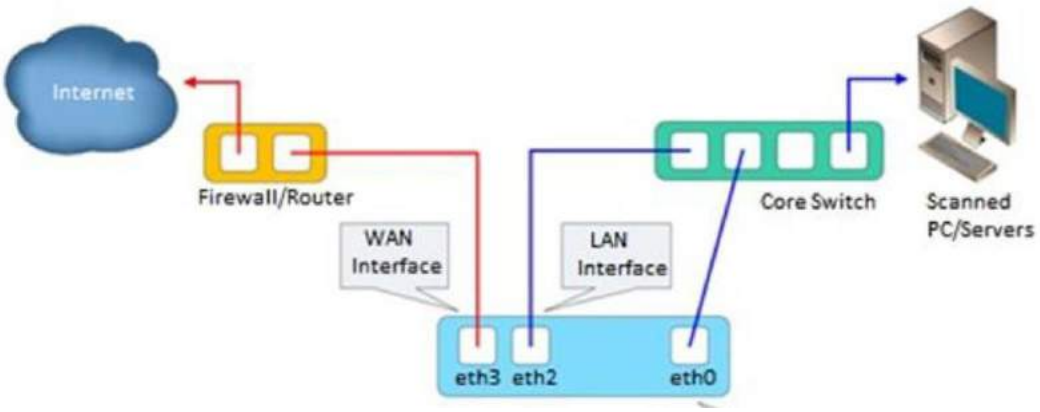
4.15.5 安装说明与配置

实施方案的详细信息：

名称	版本号	目的	硬件规格
GTB Inspector	15.6.0	网络数据泄露防护	Hyper-V虚拟机（第1代）： • 处理器：虚拟双核 • 内存：6 GB • 磁盘空间：20~30 GB（请参见厂商提供的虚拟设备文件） • 网络：3个网络适配器 • 操作系统：CentOS Linux 7核
GTB中央控制台	15.6.0	为所有GTB产品提供统一的报表管理功能	Hyper-V虚拟机（第1代）： • 处理器：虚拟双核 • 内存：6 GB • 磁盘空间：20~30 GB（请参见厂商提供的虚拟设备文件） • 网络：1个网络适配器 • 操作系统：CentOS Linux 7核

环境搭建

- 利用厂商提供的 ISO 映像文件，将两个虚拟机配置在工厂的网络安全局域网中。硬件规格参见上表。
- 根据厂商提供的官方拓扑图（如下图所示），采用桥接（串联）模式部署 GTB Inspector 服务器。如欲了解更多详情，请参见官方安装指南。



- 虚拟机的客户机操作系统的联网信息如下所示：

  - 虚拟机：GTB-Inspector

  - 网络接口：eth0

  - IP 地址：10.100.0.175

  - 网关：10.100.0.1

  - 子网掩码：255.255.255.0

  - 域名服务器：10.100.0.17

  - 网络接口：eth2->接入网络聚合设备的监听口 1

  - 网络接口：eth3->接入思科 ASA 防火墙的 WAN 口

  - 虚拟机：GTB-Central

  - 网络接口：eth0

  - IP address：10.100.0.176

  - 网关：10.100.0.1

  - 子网掩码：255.255.255.0

  - 域名服务器：10.100.0.17

配置 GTB 中央控制台

- 下载 GTB 中央控制台的 ISO 文件和安装指南[111]。
- 打开目标虚拟机监控程序，用 ISO 文件安装虚拟机。
- 完成初始配置，如创建 DNS 记录、为服务器分配静态 IP 地址等。
- 利用默认凭证登录 GTB 中央控制台的 Web 用户界面。单击 **Administration > Licensing**（管理 > 许可证），上传许可证文件。完成后，重启系统。
- 单击【**DLP Setup**】（DLP 配置）页签，选择【**Network**】（网络），配置 IP 地址。
- 单击【**DLP Setup**】（DLP 配置）页签，选择【**LDAP**】，配置 AD 服务器。
- 单击【**DLP Setup**】（DLP 配置）页签，选择【**Email & Alerts**】（邮件与告警），配置 SMTP 服务器。
- 单击【**DLP Setup**】（DLP 配置）页签，选择【**Date & Time**】（日期和时间），配置 NTP 服务器。
- 单击【**DLP Setup**】（DLP 配置）页签，选择【**SIEM**】，配置 Syslog/SIEM 服务器的 IP 地址。

配置 GTB Inspector

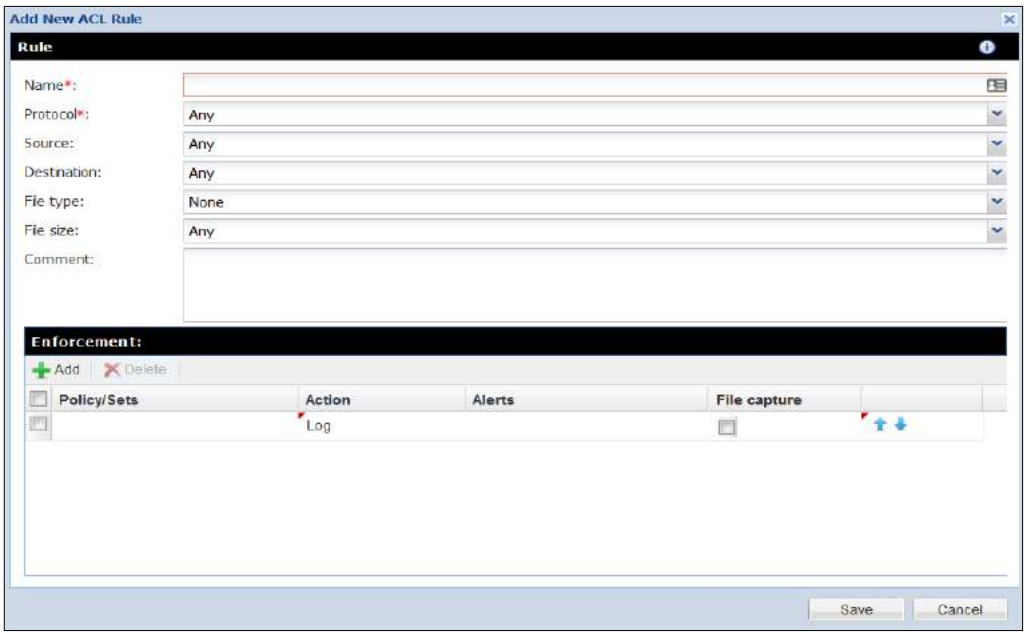
- 下载 GTB Inspector 的 ISO 文件和安装指南[112]。

[111] https://gttb.com/downloads/
[112] https://gttb.com/downloads/

- 打开目标虚拟机监控程序，用 ISO 文件安装虚拟机。
- 进行初始配置，如创建 DNS 记录、为 Inspector 服务器分配静态 IP 地址并配置 LAN 口和 WAN 口等。详细说明，参见 GTB 产品安装指南。
- 使用默认凭证，登录 GTB Inspector 服务器的 Web 用户界面。单击 **Administration > Licensing**（管理 > 许可证），上传许可证文件。完成后，重启系统。
- 单击【**Configuration**】（配置）页签，选择【**Email Alerts**】（邮件告警），配置 SMTP 服务器。
- 单击【**Configuration**】（配置）页签，选择【**LDAP Integration**】（LDAP 集成），配置活动目录服务器。
- 单击【**Configuration**】（配置）页签，选择【**Network**】（网络），根据需要设置部署模式。
- 单击【**Configuration**】（配置）页签，选择【**SIEM**】，配置 Syslog/SIEM 服务器的 IP 地址。
- 单击【**Configuration**】（配置）页签，选择【**SSL Proxy**】（SSL 代理），上传公共证书（若有），用于 SSL 解密。
- 单击【**Configuration**】（配置）页签，选择【**Central Console**】（中央控制台），输入 GTB 中央服务器的主机名。确保 Inspector 和中央控制台之间路径可达。

在 GTB 中央控制台上创建 ACL 规则

- 登录中央控制台的 Web 用户界面。单击 **DLP-Setup > Network DLP**（DLP-配置 > 网络 DLP）。
- 单击【**Categories**】（类别）下的<Inspector server name>（Inspector 服务器名称）。
- 单击【**Add**】（添加）按钮，弹出【**Add New ACL Rule**】（添加新 ACL 规则）窗口。



- 配置【**Name**】（名称）、【**Protocol**】（协议）、【**Source**】（源）、【**Destination**】（目的）和【**File type**】（文件类型）参数。

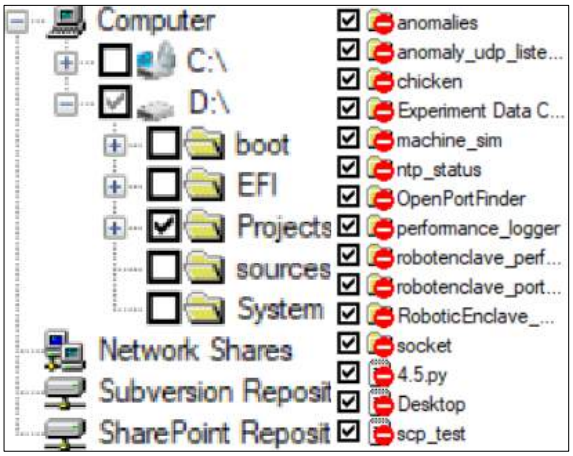
  若将【**Protocol**】设置为【**Any**】，Inspector 会检测所有协议。

  说明：这可能会影响性能（影响程度与组织中的客户端数量有关）。
- 在【**Enforcement to**】（应用）中，单击【**Add**】（添加）配置策略/集。选择针对信用卡号（CCN）或社保号的默认策略或创建新策略。
- 选择要执行的动作：Log（记录日志）、Block（阻断）、S-阻断和 Pass（放行）。
- 选择【**File Capture**】（文件采集）选项，保存入侵数据。
- 单击【**Save**】（保存）。
- 单击【**Deploy-All**】（部署全部），将新策略发送至 Inspector。
- （可选）若有多条规则，可单击上下箭头对规则进行排序。规则按从上至下的顺序匹配。

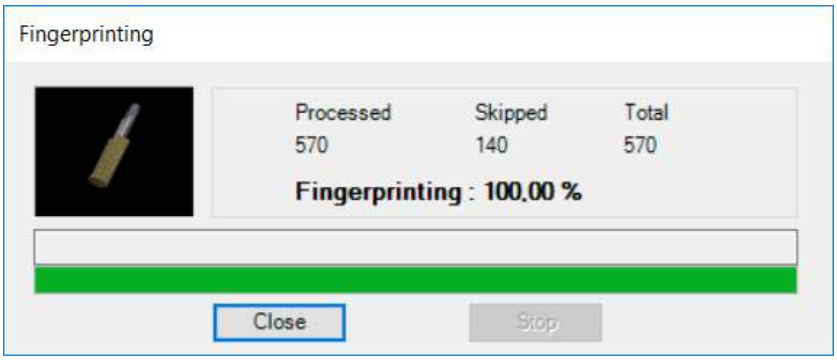
使用安全管理器为文件创建指纹

- 在中央控制台上单击【**Help**】（帮助）页签。在 Windows 系统中下载【**GTB Security Manager**】（GTB 安全管理器）。
- 运行安装程序（例如 **GTBSecurityManager_15.3.0.msi**）。按界面提示完成安装。安装完毕，重启系统。
- 选择【**Run as Administrator**】（以管理员身份运行）启动 GTB 安全管理器。
- 单击【**Settings**】（设置）。输入中央控制台服务器的 IP 地址。用户名和密码自动填充。单击【**OK**】（确定），保存配置。

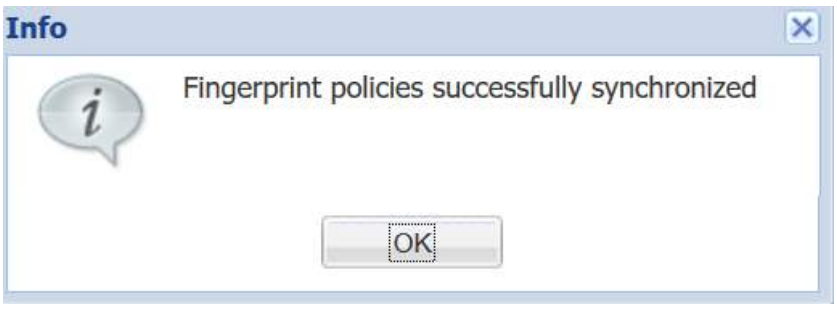
- 选择【**File**】（文件）菜单，单击【**New**】（新建）和【**New File Profile**】（新文件配置），打开新窗口，选择文件/文件夹创建指纹。
- 选择要创建指纹的文件或文件夹。若选择了文件夹，该文件夹下的所有文件均被选中，表明将为这些文件创建指纹。



- 单击【**Save**】（保存）。选择【**Location**】（位置），保存新建配置。
- 单击挂锁图标，开始创建指纹。
- 在【**Output**】（输出）窗口中查看添加进度。指纹创建完毕，单击【**Close**】（关闭）。



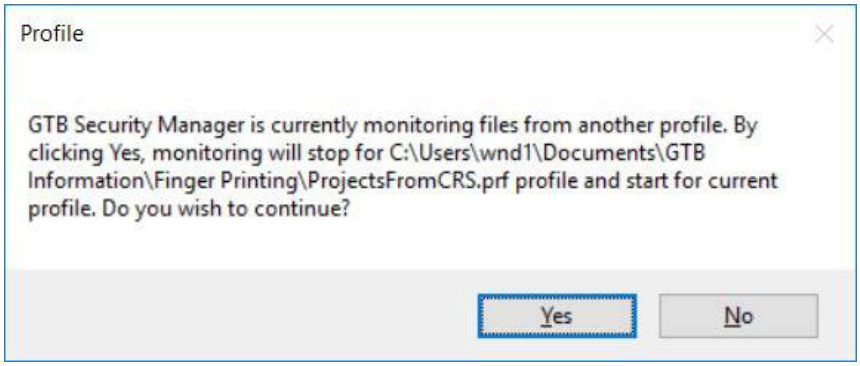
- 选择【**View**】（查看）菜单，单击【**Profiles**】（配置），打开配置窗口，查看具体的配置。
- 选择先前创建的配置，右键单击【**Start Monitoring**】（开始监控）。
- 监控开启后，文件会显示在【**Currently Monitoring**】（当前监控）页面中。
- 再次登录中央控制台，选择【**Account Manager**】（帐号管理器），单击【**Refesh Polices**】（刷新策略）。等待操作成功提示。



- 选择 **DLP Setup > Policy Management**（DLP 配置 > 策略管理），双击**【Default】**（默认），打开新窗口。
- 单击**【Add Policy】**（添加策略）。
- 单击下拉列表，选择文件。
- 单击**【Save】**（保存）。配置完成后，按上述步骤创建了指纹的文件会自动添加到应用了 ACL 的默认网络 DLP 策略中。新的默认值为 **SSN**，**CCN** 和 **File**。

与创建指纹相关的其他信息：

- 指纹功能一次只允许创建一个有效配置（Profile）。若其他配置处于 **Start Monitoring**（开始监控）状态，会显示如下警告信息：



- 在机器上安装 GTB 安全管理器，作为管理所有指纹文件的中央库。创建文件夹，将所有需要创建指纹的文件放置在其中。配置文件（Profile）创建指纹并上传到中央控制台后，就不再需要留在该文件夹中了。只有进行修改时才需要访问指纹文件。
- 指纹文件受中央控制台中创建的 ACL 规则控制。ACL 规则按从上至下的顺序匹配，命中规则的优先级高于其他规则。

4.15.6 对性能的主要影响

鉴于 GTB 在网络拓扑中的位置，没有测量 PCS 中安装 GTB 后对网络的性能影响。在系统运行期间，生产过程中各组件均未频繁进行跨边界通信。

4.15.7 性能测量数据集的相关链接

无

4.16 Graylog

4.16.1 技术方案概述

Graylog 是一个开源的日志管理工具。它能从各种数据源收集日志、连接数据和事件数据并进行解析和总结。Graylog 还为第三方收集器（如 beats、fluentd 和 nxlog）提供集中配置管理。消息进入 Graylog 时，可进行实时路由、黑名单、修改和充实操作，处理管道（Processing Pipeline）为这些操作提供了更大的灵活性。它有强大的搜索语法，可以精准查询内容。使用 Graylog，用户甚至可以创建仪表盘，集中展现指标，了解趋势[113]。

重点说明：

- 开源产品，有良好的社区支持；
- 安装、定制容易，可从任何操作系统平台收集日志；
- 适用于主流 Linux 版本，预装虚拟机，有现成的 Docker 映像；
- 仪表盘虽然与系统完美契合，使用方便，但缺少 Kibana（如聚合）等弹性搜索工具中所包含的多种功能和可视化效果。

4.16.2 方案提供的技术能力

Graylog 提供以下技术能力（参见第 1 卷第 6 章）：

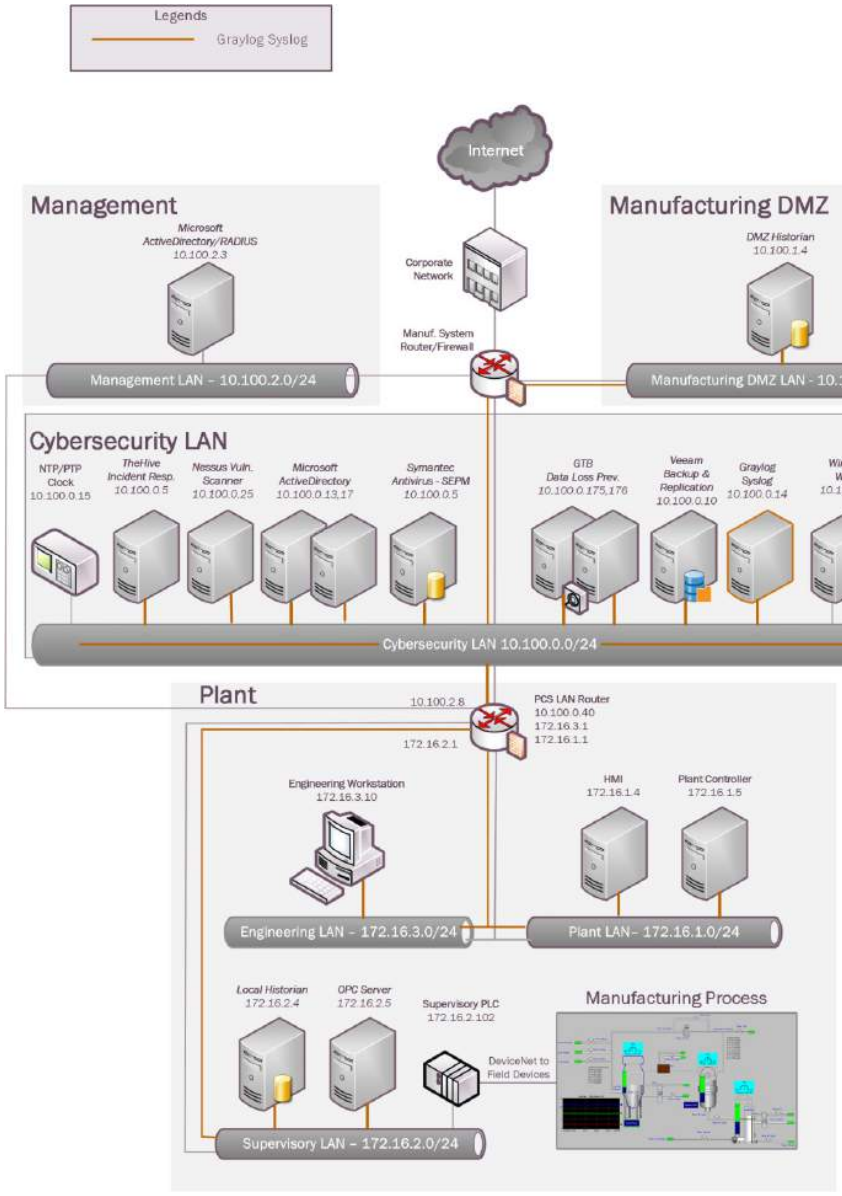
- 网络监控
- 事件日志
- 取证

4.16.3 方案实现的子类

PR.DS-5，PR.MA-2，PR.PT-1，PR.PT-4，DE.AE-2，DE.AE-3，DE.CM-1，DE.CM-6, DE.CM-7, DE.DP-3, RS.AN-3

4.16.4 方案实施架构图

[113] http://docs.graylog.org/en/3.0/



4.16.5 安装说明与配置

实施方案的详细信息：

工具名	版本	硬件规格
Graylog企业版	2.4.6	Hyper-V虚拟机（第1代）： • 处理器：虚拟双核 • 内存：6 GB • 磁盘空间：共400 GB 根据厂商提供的虚拟设备文件分配根卷 350+ GB数据卷用于存储日志 • 网络：1个网络适配器 • 操作系统：Ubuntu 14

环境搭建

- 在工厂的网络安全局域网的 Hyper-V 宿主服务器上，部署厂商配置好的虚拟机（.ova）。硬件规格见上表。
- 该服务器的客户机操作系统的 IP 配置如下所示：

  - IP 地址：10.100.0.14

  - 网关：10.100.0.1

  - 子网掩码：255.255.255.0

  - 域名服务器：10.100.0.17

- 根据 Graylog 要求，在防火墙上开放 UDP 514、5415 和 1202 端口，采集客户端的 Syslog 消息。详细信息，请访问 http://docs.graylog.org/en/3.0/。

初始配置

- 根据所使用的操作系统，从 Graylog 网站下载对应安装包[114]。

  说明：Graylog 提供了一个预配置的虚拟机，用于测试/培训环境。

- 为 Linux 系统分配一个静态 IP 地址（若还没有）。
- 参考 Graylog 的操作说明，安装软件包[115]。
- 使用默认凭证登录 Web 界面，更改管理员密码。
- 按如下步骤配置活动目录集成：

  - 选择 **System > Authentication**（系统 > 认证）。

  - 单击【**Authentication Management**】（认证管理）页面上的【**LDAP/Active Directory**】（LDAP/活动目录），配置 AD 服务器。详细说明，请参阅 Graylog 文档。

  - 单击【**LDAP Group Mapping**】（LDAP 组映射），配置组映射，以控制分配给用户的访问类型。根据需要，更改默认用户角色。

从 Windows 服务器接收 Syslog

使用 NXlog[116]程序将工厂的所有 Windows 系统中的事件转发到 Graylog 服务器。社区版 NXlog 可免费使用。

- 在所有相关 Windows 主机上下载、安装 NXlog。
- 编辑 **C:\Program Files(x86)\nxlog\conf** 目录下的 **nxlog.conf** 文件，根据需要，设置转发到 Graylog 服务器的事件类别[117]。

例如，配置从工厂的工程师站转发下列各类事件：

- **System**（系统）类别下的 1074 事件：系统重启
- **Application**（应用）类别下的 1034 事件
- **Security**（安全）类别下的 4625 事件
- **Security**（安全）类别下的 4689 事件和 C:\Program

---

114 https://www.graylog.org
115 http://docs.graylog.org/en/3.0/pages/installation/operating_system_packages.html
116 https://nxlog.co/
117 https://nxlog.co/documentation/nxlog-user-guide/

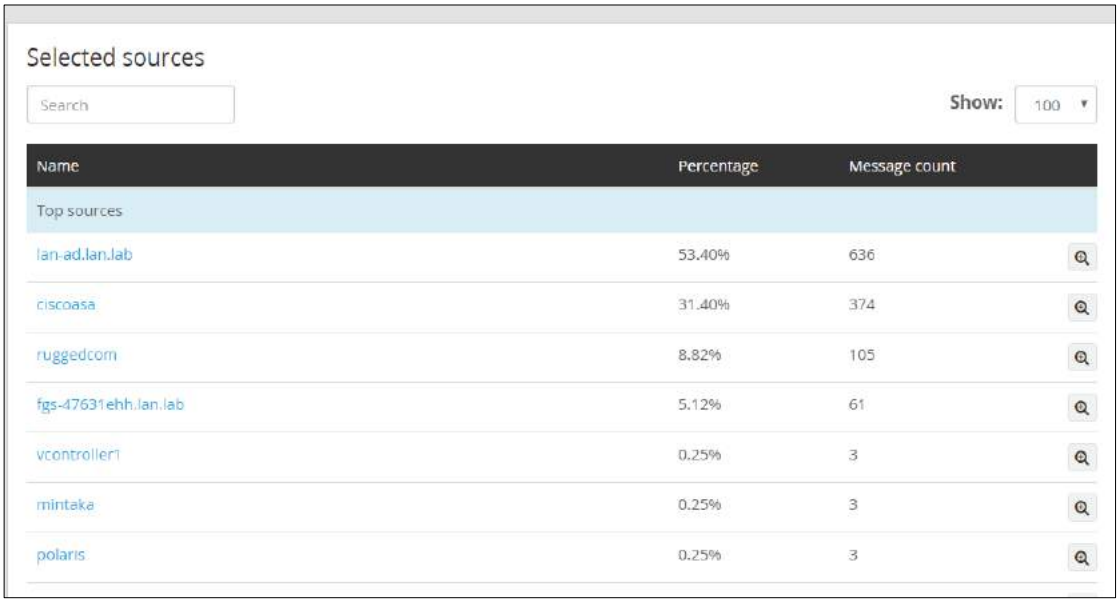
Files\..\Rockwell\Rsvsc.host.exe 进程：罗克韦尔自动化软件停止运行

- **Microsoft-Windows-TerminalServices-LocalSessionManager** 类别下的所有事件【*】：用户登录、登出系统
- **Veeam** 类别下的 190 事件：备份完成
- **FTDiag** 目录下的 1001 事件：这是由 Factory Talk 管理软件生成的自定义事件 ID，表示认证失败

修改后的 **nxlog.conf** 文件如下所示：

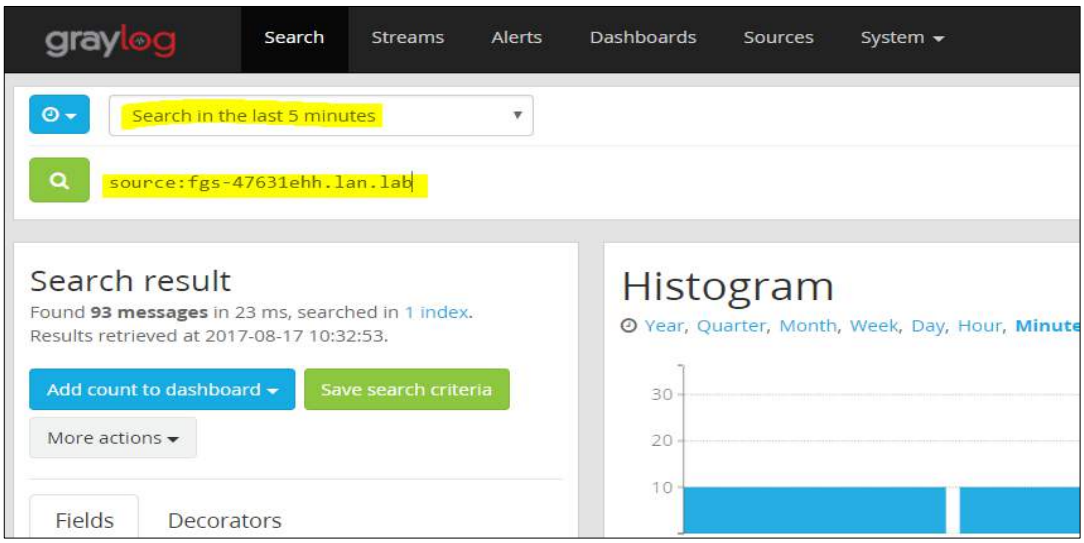
```
## Please set the ROOT to the folder your nxlog was installed into,
## otherwise it will not start.

#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<Extension _syslog>
  Module     xm_syslog
</Extension>

<Input in>
Module     im_msvistalog
ReadFromLast True
Query   <QueryList>\
          <Query Id="0">\
          <Select Path="System">*[System[(EventID=1074)]]</Select>\
    <Select Path="Application">*[System[(EventID=1034)]]</Select>\
          <Select Path="Security">*[System[(EventID=4625)]]</Select>\
          <Select Path="Security">*[System[(EventID=4689)] and
EventData[Data[@Name='ProcessName'] and (Data='C:\Program Files (x86)\Common
Files\Rockwell\RsvcHost.exe')]]</Select>\
          <Select Path='Microsoft-Windows-TerminalServices-
LocalSessionManager/Operational'>*</Select>\
    <Select Path="Veeam Agent">*[System[(EventID=190)]]</Select>\
          <Select Path="FTDiag">*[System[(EventID=1001)]]</Select>\
    </Query>\
     </QueryList>
</Input>

<Output out>
   Module     om_udp
   Host       10.100.0.14
   Port       514
   Exec       to_syslog_bsd();
</Output>
<Route 1>
   Path       in => out
```

- 保存 **nxlog.conf** 文件，重启 NXLOG Windows 服务。设备将向 Graylog 服务器发送 Syslog（事件）。若服务无法启动，请检查 nxlog.conf 文件中是否存在空格或缺少括号，**nxlog.conf** 文件对缩进非常敏感。
- 登录 Graylog Web 界面，查找 Windows 主机的事件。单击【**Sources**】（源）菜单，查看【**Selected sources**】（选中源）列表中是否包含 Windows 主机。



- 输入查询信息，在主页中选择有效时间段，搜索主机事件。

  例如，按主机名查找事件，在搜索框中输入“source：<windows hostname>”（源：<Windows 主机名>），如下图所示。



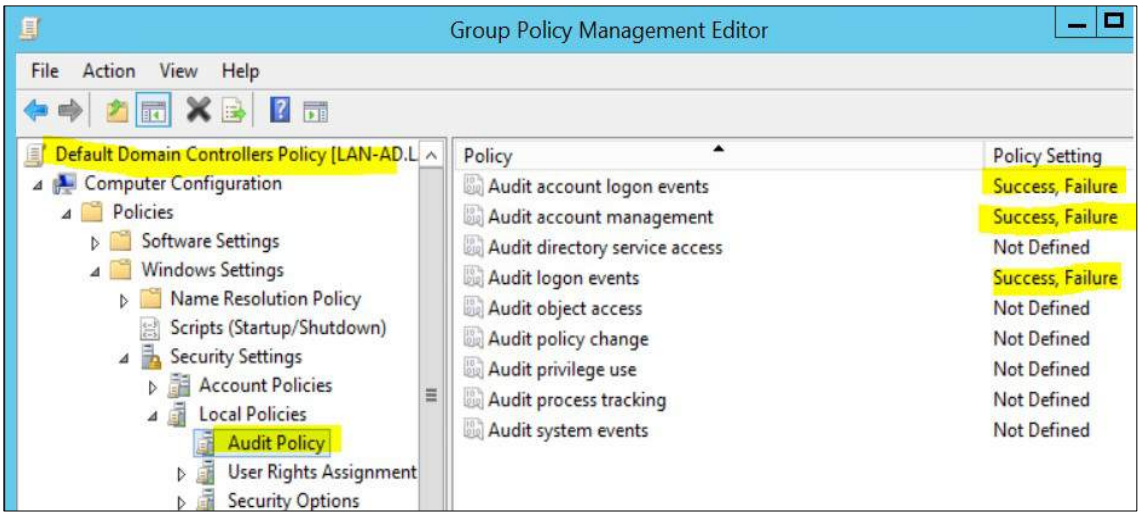
活动目录域控制器的 Syslog 配置

- 按如下步骤，在域控制器上启用审核：

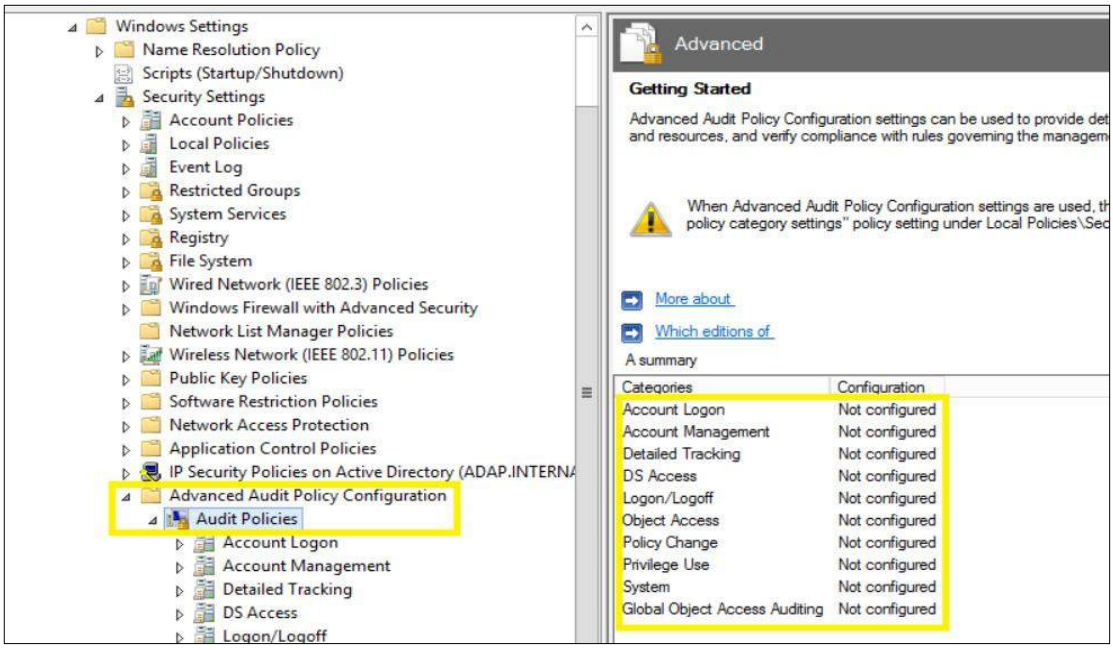
  a. 打开域控制器上的**Group Policy Management Console**（组策略管理控制台）。

  b. 编辑**Default Domain Controllers Policy**（默认域控制器策略）或创建新的GPO，链接到域控制器OU。

  c. 选择**Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies**（计算机配置 > 策略 > Windows设置 > 安全设置 > 本地策略），逐个选择或单击要审核的策略，启用**Success/Failure**（成功/失败）设置。
  下图为启用审核的部分默认域控制器策略，供参考。

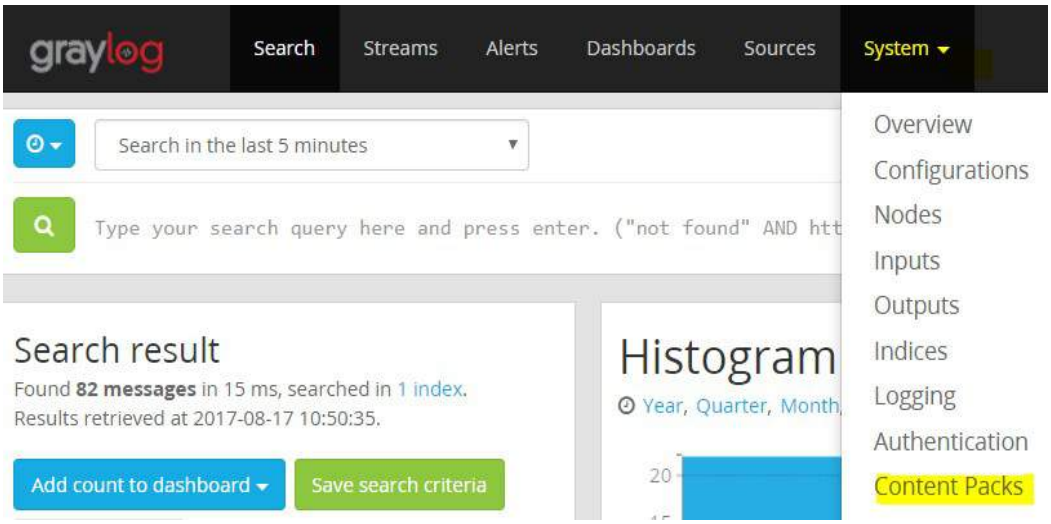


d. （可选）如果需要，使用Advanced Audit Policies（高级审核策略）来代替步骤C中提到的常规审核策略，以便对要审核的类别进行粒度更细的控制。

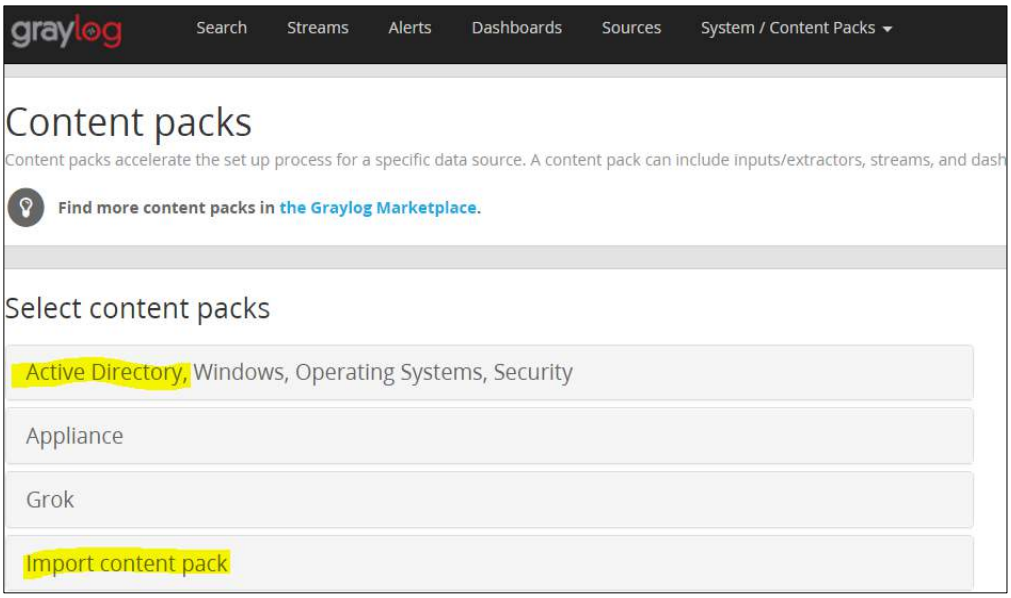


- 编辑域控制器上的 **nxlog.conf** 文件，转发安全类别事件。根据需要筛选事件 ID，重启 nxlog 服务。
- 按如下步骤安装 Active Directory Content Pack（活动目录内容包）：
  a. 从Graylog市场下载活动目录内容包[118]。
  b. 根据该活动目录内容包的要求，放行Graylog服务器上的UDP 5414端口以及网络防火墙的流量。
  c. 登录Graylog Web界面，单击**System > Content Packs**（系统 > 内容包）。

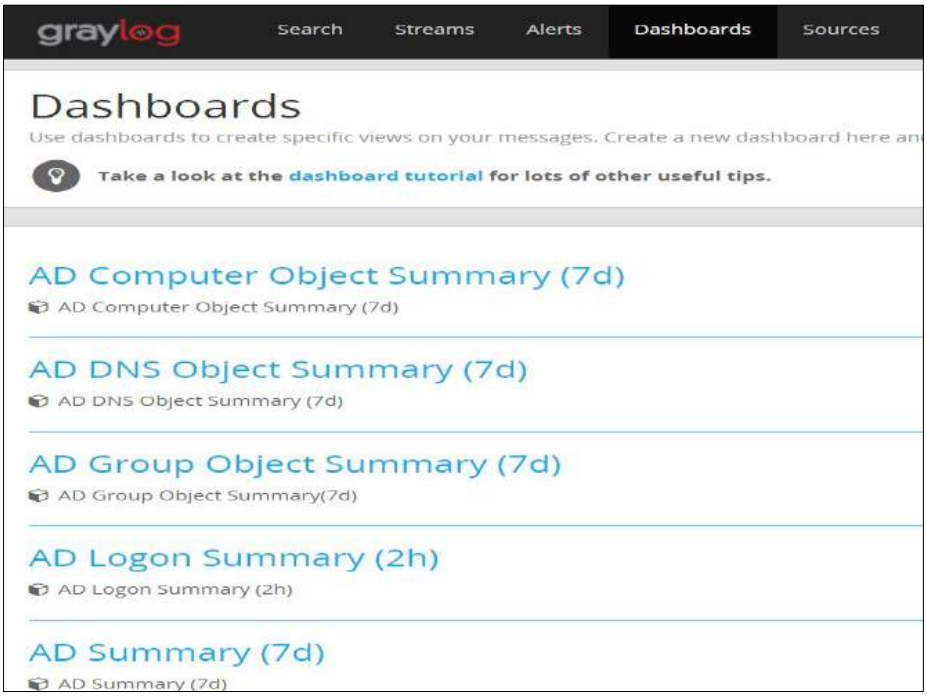
[118] https://marketplace.graylog.org/addons/750b88ea-67f7-47b1-9a6c-cbbc828d9e25



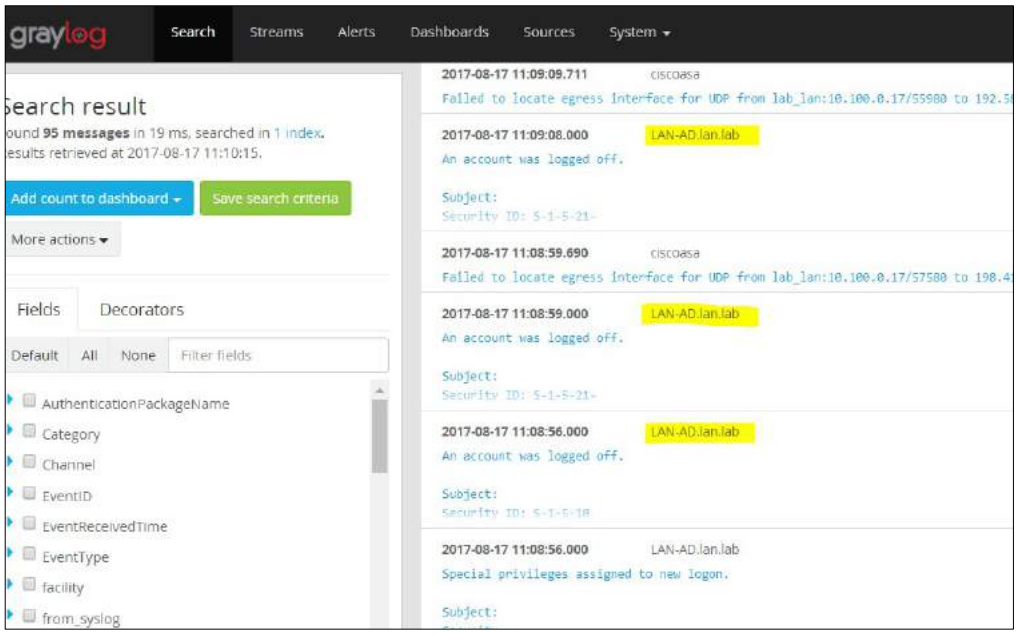
d. 单击【**Import content packs**】（导入内容包）。导入后，【**Select Content packs**】（选择内容包）下会显示活动目录，即刚导入的内容包。



e. 单击【**Dashboards**】（仪表盘），查看活动目录用户和组活动的新图表。系统假设AD服务器已成功发送事件给Graylog服务器，开始为图表自动赋值。



f. 主仪表盘中查找活动目录服务器的事件。输入服务器主机名，查找事件（如之前步骤中所述）。



从边界防火墙/网络设备接收 Syslog

- 通过 Web 界面或命令行界面登录网络交换机/路由器。
- （使用 Web 界面）选择【**Syslog**】或【**Monitoring**】（监控）菜单。
- 输入 Graylog 服务器的 IP 地址，保存设置。
- （使用命令行界面）参照厂商文档，启用日志。

例如，Allen Bradley Stratix 边界路由器上运行如下命令，转发 Syslog 到 Graylog 服务器的 IP 地址。

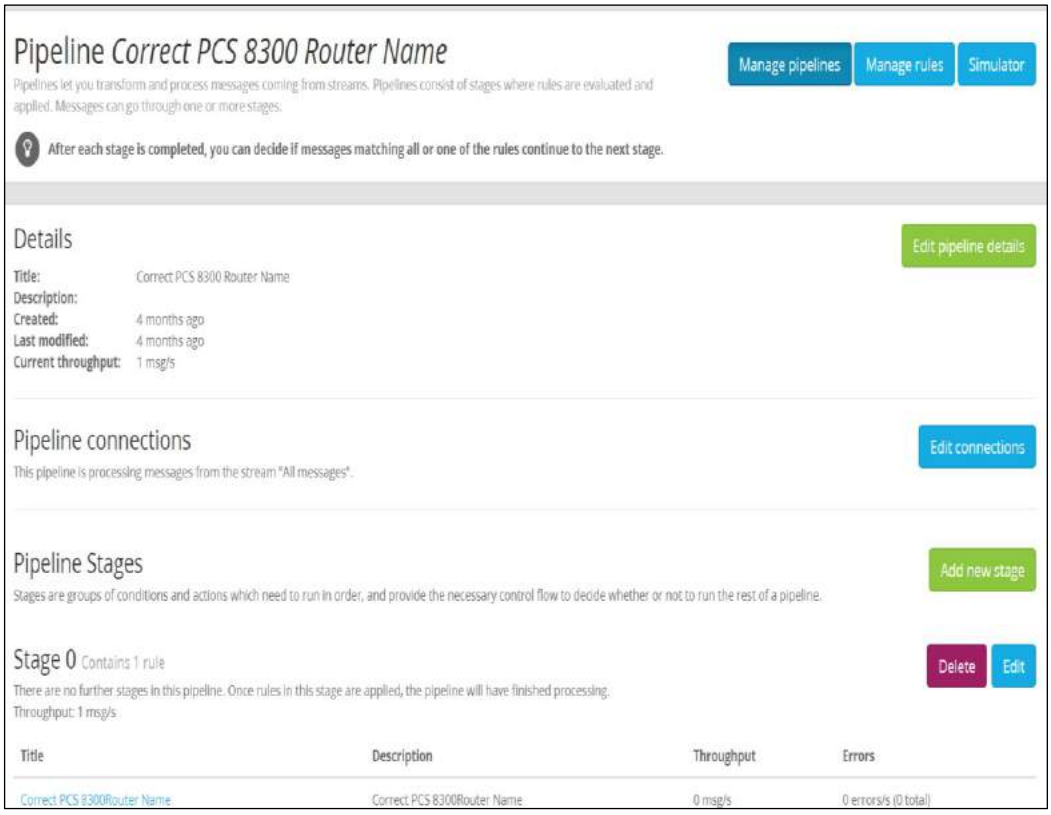
```
#enable
#configure terminal (config)#logging enable
(config)#logging 10.100.0.14 (config)#logging
trap informational (config)#end
#wr mem
```

配置管道/规则

我们发现，对于网络设备发送的消息，Graylog 将设备的 IP 地址而不是主机名记为“源”。这是因为不同厂商的设备记录日志的格式不同。为了解决这个问题，Graylog 内置了一些特性，比如管道、规则、Grok 模式和查找表[119]。

- 选择 **System > Pipelines**（系统 > 管道）。
- 单击【**Add new pipeline**】（新建管道），创建新管道。
- 单击【**Manage Rules**】（管理规则）按钮。
- 单击【**Create rule**】（创建规则）按钮，新建规则，将其与管道关联。

下图显示了名为 **Correct PCS 8300 Router Name** 的管道的详细信息及其相应的规则 **Correct PCS 8300 Router Name**，应用规则后，Allen-Bradley 边界路由器将在搜索结果中正确显示主机名。

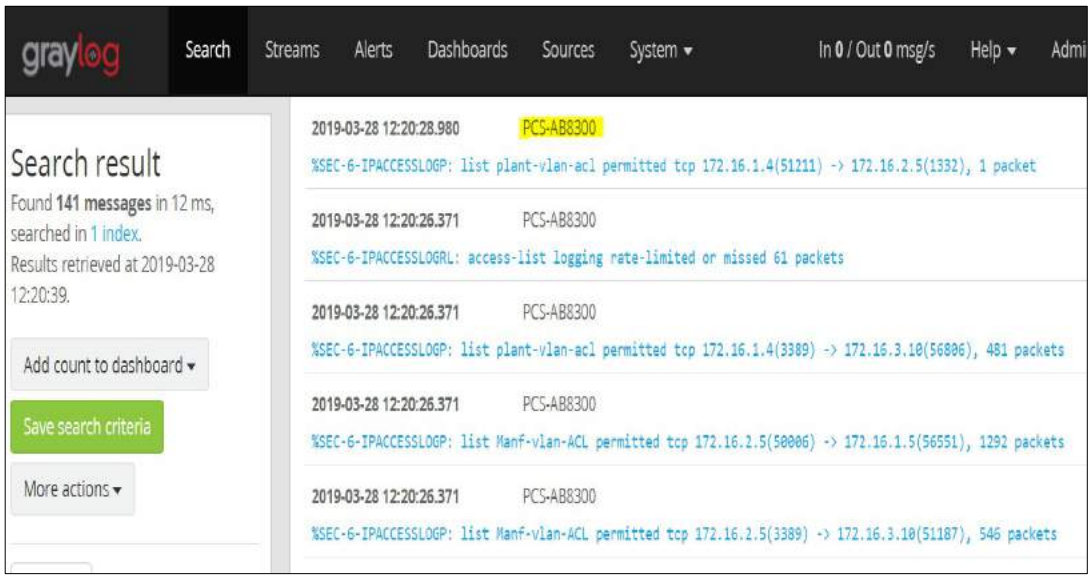


[119] http://docs.graylog.org/en/2.4/pages/pipelines.html

Rule source

```
1  rule "Correct PCS 8300Router Name"
2  when
3    has_field("source") AND contains(to_string($message.source), "10.100.0.40")
4  then
5     set_field("source", "PCS-AB8300");
6  end
```

【**Search**】（搜索）页面上显示的是主机名 PCS-AB8300，和规则中配置的一样。



配置告警邮件通知条件

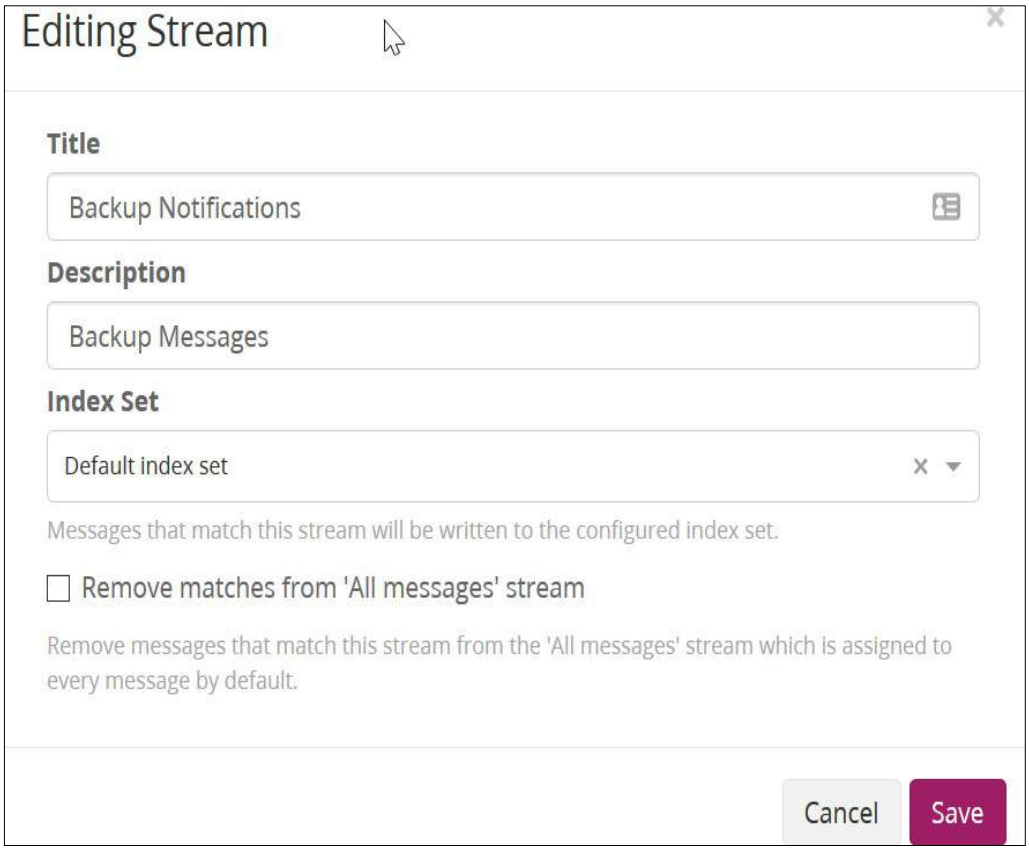
用户可为自定义事件设置邮件告警并配置告警条件。下文以从 Windows 客户端收到 Veeam 备份相关事件为例，介绍如何配置 Graylog 发送邮件通知。

用户可按照这个步骤定义自己的自定义告警条件。

要启用邮件通知，须进行如下配置：

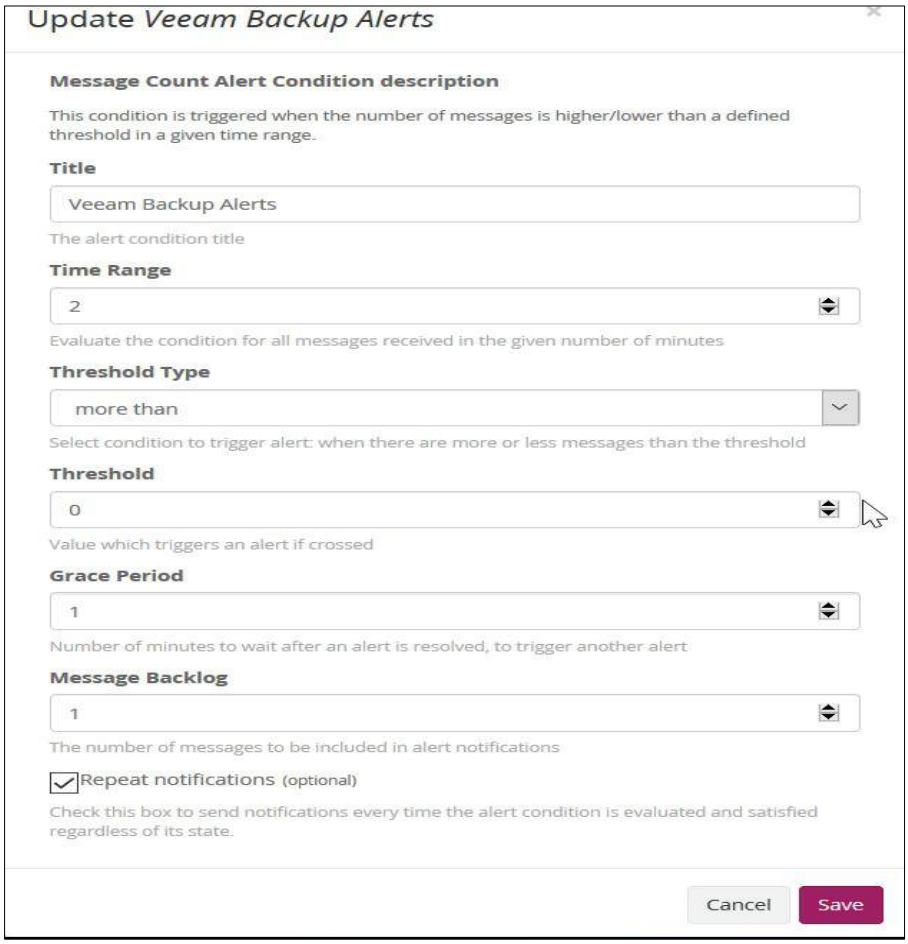
- 创建流（Steam）。
- 添加告警条件。
- 创建通知。

- 选择【**Streams**】菜单，单击【**Create a Stream**】（创建流），输入【**Title**】（标题）、【**Description**】（说明）和【**Index Set**】（索引集）（使用默认值 Default index set）。
- 单击【**Save**】（保存），保存设置。



- 选择【**Alerts**】（告警）菜单，单击 **Manage conditions > Add New Condition**（管理条件 > 新建条件）。
- 在【**Alert on stream**】（告警流）下拉列表中选择先前创建的流。在【**Condition type**】（条件类型）下拉列表中选择【**Message Count Alert Condition**】（消息计数告警条件）。

- 单击【**Add Alert Condition**】（添加告警条件），设置必配项。
- 单击【**Save**】（保存），完成配置（有关当前消息计数告警条件的示例，参见下文）。



- 创建通知，步骤如下：
  a. 单击右上角的【**Manage notifications**】（管理通知）。
  b. 单击【**Add New Notification**】（新建通知）。
  c. 从【**Notify on Stream**】（通知流）下拉列表中选择之前创建的通知。
  d. 从【**Notification Type**】（通知类型）下拉列表中选择【**Email Alert Callback**】（邮件告警回调）。
  e. 单击【**Add alert notification**】（新建邮件通知）按钮。
  f. 标题：<输入内容>，例如：**Veeam Backup Alerts**（Veeam备份告警）
  g. （供参考）邮件主题：“Veeam备份成功 源：${foreach backlog message}${message.source}${end}”，实际操作中去掉引号。当前回调信息样式，见下图。
  h. **发件人**：<发件人地址>
  i. 邮件内容：

告警描述：${check_result.resultDescription}

日期：${check_result.triggeredAt}

流 ID：${stream.id}

流标题：${stream.title}

流描述：${stream.description}

告警条件标题：${alertCondition.title}

${if backlog}本告警之前信息：

${foreach backlog message}${message}

j. **接收用户**：根据需要，选择Graylog用户。
k. **收件人**：接收告警的个人的邮件地址
l. 单击【**Save**】（保存）。

- 测试新流/告警/通知，确保配置正确。

补充信息

- 围绕特定厂商的技术、设备（如思科、Microsoft DNS、Bro IDS、Cacti、赛门铁克等），网上有许多内容包和插件可用[120]。
- 就管道创建，可参考相关指导资料[121]。

经验总结

谨慎配置各系统的日志级别。对于 Windows 客户端，用 nxlog.conf 文件过滤事件 ID，不要启用所有事件类别，以避免生成大量事件，进而影响 Graylog 中的搜索操作和 Graylog 服务器的整体性能。使用组策略启用审核时，只选择必要类别。进程创建（Process Creation）等类别会产生大量干扰信息。

4.16.6 对性能的主要影响

考虑到 Graylog 的典型安装位置和使用方式（在制造系统外），没有测试其对系统性能的影响。

4.16.7 性能测量数据集的相关链接

无

[120] https://marketplace.graylog.org
[121] https://jalogisch.de/2018/working-with-cisco-asa-nexus-on-graylog/

4.17 DBAN

4.17.1 技术方案概述

DBAN 是一个免费的开源数据清除实用程序，可清理硬盘，确保硬盘在准备淘汰并从本地移除时不会有任何数据留下。DBAN 等硬盘过滤工具仅适用于旋转硬盘。对于固态硬盘和其他闪存盘，在移除之前，请向厂商咨询有关媒体过滤事宜。

4.17.2 方案提供的技术能力

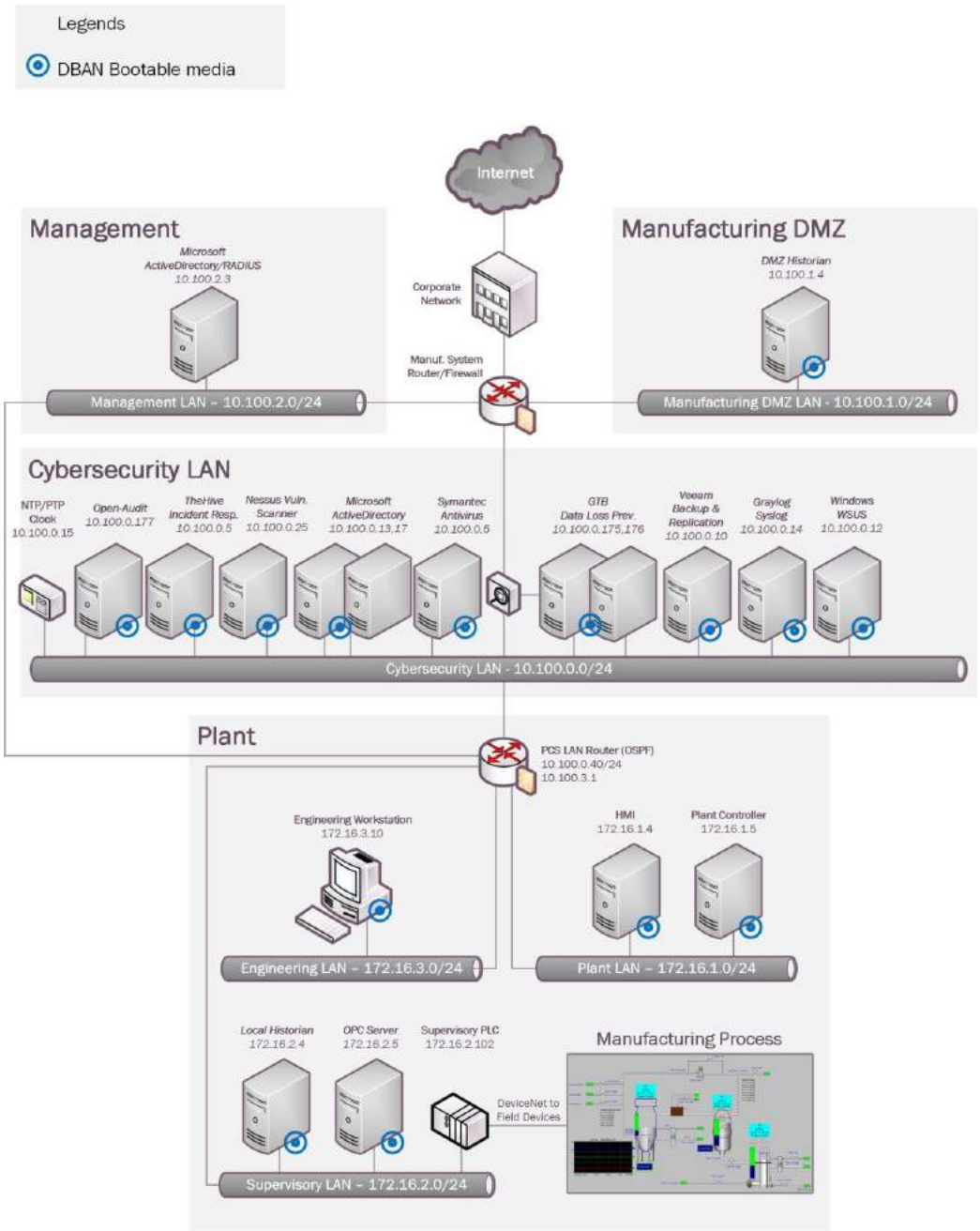
DBAN 提供以下技术能力（参见第 1 卷第 6 章）：

- 媒体过滤

4.17.3 方案实现的子类

PR.DS-3, PR.IP-6

4.17.4 方案实施架构图



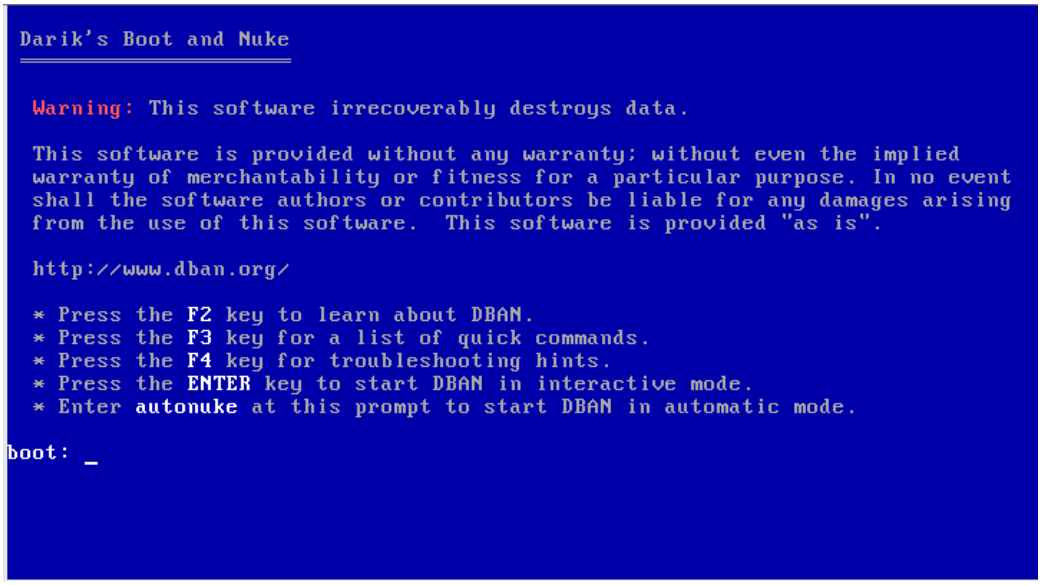
4.17.5 安装说明与配置

安装

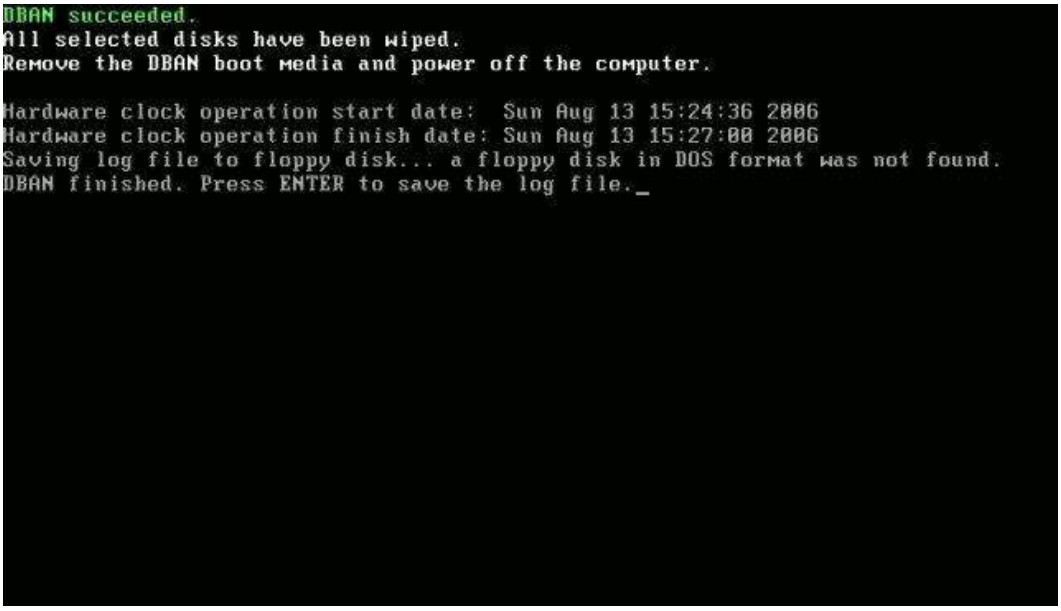
- 下载 DBAN ISO 文件[122]。
- 使用 ISO 引导程序将 ISO 文件刻录到 CD/DVD 或 U 盘中。

操作步骤

- 使用前面创建的引导盘启动需要清理的计算机。
- 启动后，选择媒体过滤模式。默认模式一般适用于大多数情况。



- 按回车键继续。默认过滤模式是“short DoD 5520.22-M”，可根据本公司安全计划规定的级别进行更改。
- 按照屏幕提示，启动清除程序。完成清除后，屏幕显示如下提示：



- 数据清除后，将物理硬盘从设备取出。这时，硬盘便可安全报废了。

[122] https://dban.org

补充信息

并非所有硬盘都可以用此方法清除。固态硬盘或闪存盘的写入方式与旋转硬盘不同，因此需要根据相关厂商的建议，进行妥善处理。

4.17.6 对性能的主要影响

鉴于 DBAN 项目的典型安装和使用位置（在制造系统外部），没有测试其对系统性能的影响。

4.17.7 性能测量数据集的相关链接

无

4.18 网络分段与隔离

4.18.1 技术方案概述

利用网络分段与隔离方案，制造商可将制造系统网络与其他网络（如企业网、访客网络）分隔，将内部制造系统网络分割成更小的网络，控制特定主机和服务之间的通信。

利用路由器的本机功能进行网络分段。

4.18.2 方案提供的技术能力

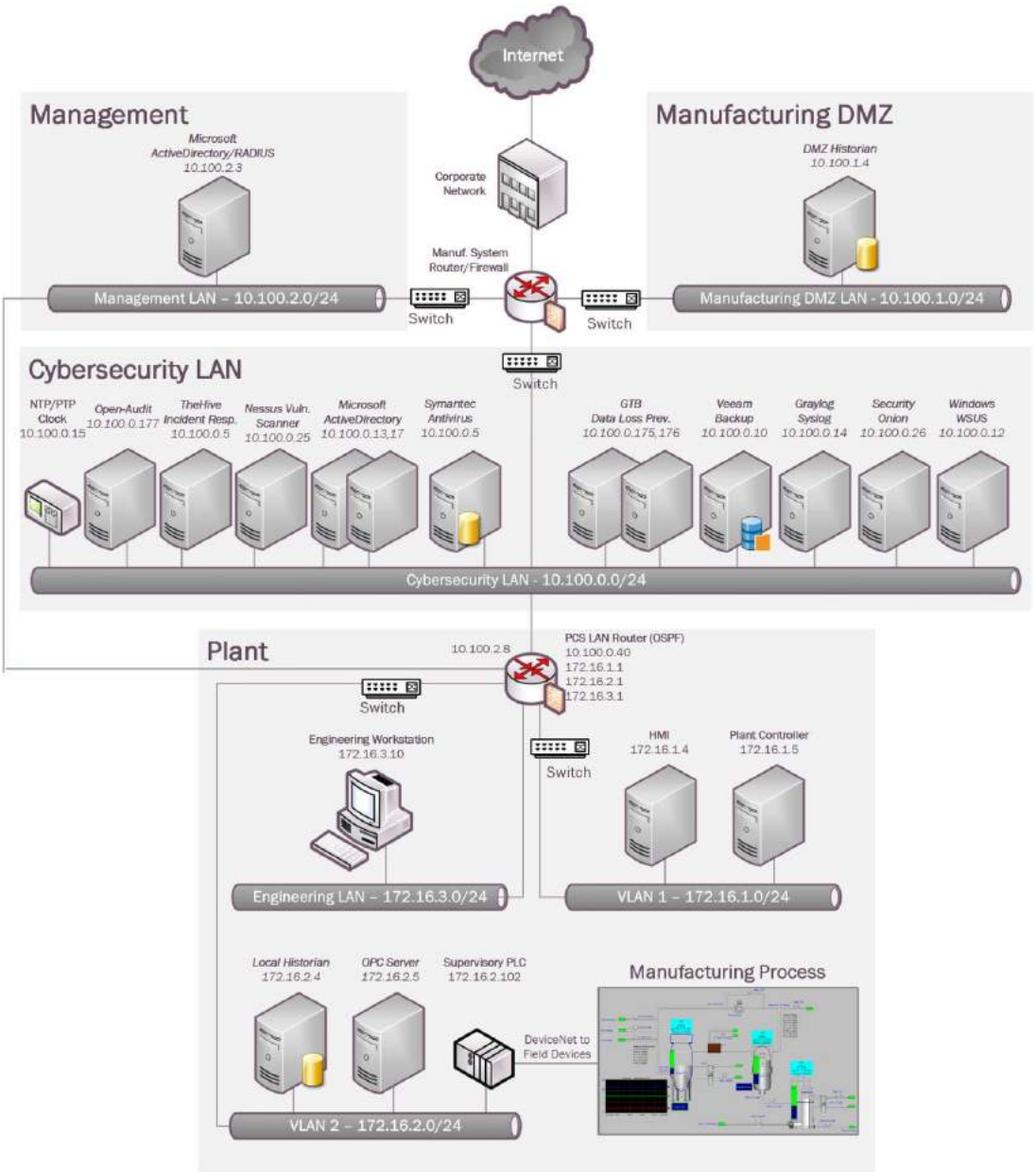
网络分段与隔离提供以下技术能力（参见第 1 卷第 6 章）：

- 网络分段与隔离

4.18.3 方案实现的子类

PR.AC-5

4.18.4 方案实施架构图



4.18.5 安装说明与配置

环境搭建

网络分段涉及如下设备：

设备	说明	位置
思科ASA 5512	运行Firepower Services FTD 6.2.3的下一代防火墙	制造系统
Allen Bradley Stratix 8300	防火墙、路由器	工作单元

S 网络安全局域网分段

下表列举了网络安全局域网中的边界路由器/防火墙思科 ASA 的接口：

接口	接口IP	子网	说明
GE 0/0	129.6.66.x	129.x.x.x/x	向上连接企业网
GE 0/1	10.100.0.1	10.100.0.0/24	网络安全局域网
GE 0/2	129.6.1.x	129.x.x.x/x	VPN用户
GE 0/3	10.100.2.1	10.100.2.0/24	管理局域网
GE 0/4	10.100.1.1	10.100.1.0/24	制造DMZ局域网

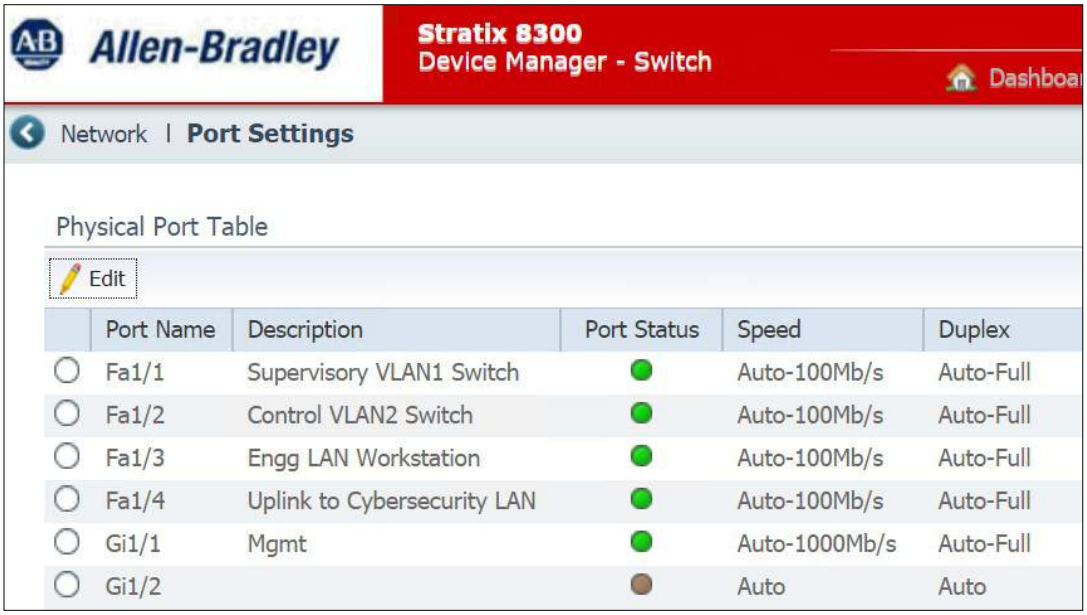
工厂网络分段

工作单元内有下列网络设备：

类型	说明
Allen Bradley Stratix 8300	边界防护防火墙、路由器
Allen Bradley Stratix 5700	控制网2层交换机
Allen Bradley Stratix 5700	监控网2层交换机

边界路由器 Allen Bradley 8300 上的接口如下表所列：

接口	接口IP	子网	说明
Fa 1/1	172.16.1.1	172.16.1.0/24	监控Vlan1
Fa 1/2	172.16.2.1	172.16.2.0/24	控制Vlan1
Fa 1/3	172.16.3.1	172.16.3.0/24	工程局域网
Fa 1/4	10.100.0.40		向上连接至网络安全局域网
Gi 1/1	10.100.2.8		管理口



其中一台 Stratix 5700 交换机连接至 8300 路由器的 Fa1/1 接口，属于监控（Vlan1）子网，与该交换机连接的设备的 IP 属于 172.16.1.0/24 子网。

另一台 Stratix 5700 交换机连接至路由器的 Fa1/2 接口，属于控制（Vlan2）子网，与该交换机连接的设备的 IP 属于 172.16.2.0/24 子网。

4.18.6 对性能的主要影响

鉴于网络分段在实施网络安全制造篇之前已在 PCS 上实现，因此没有测试其对网络性能的影响。

4.18.7 性能测量数据集的相关链接

无

4.19 网络边界防护

4.19.1 技术方案概述

边界防护设备用于监测、控制组织的外部边界和关键内部边界的连接和通信。边界防护机制包括路由器、防火墙、网关和数据二极管，将系统组件划分为多个逻辑上独立的网络或子网。

4.19.2 方案提供的技术能力

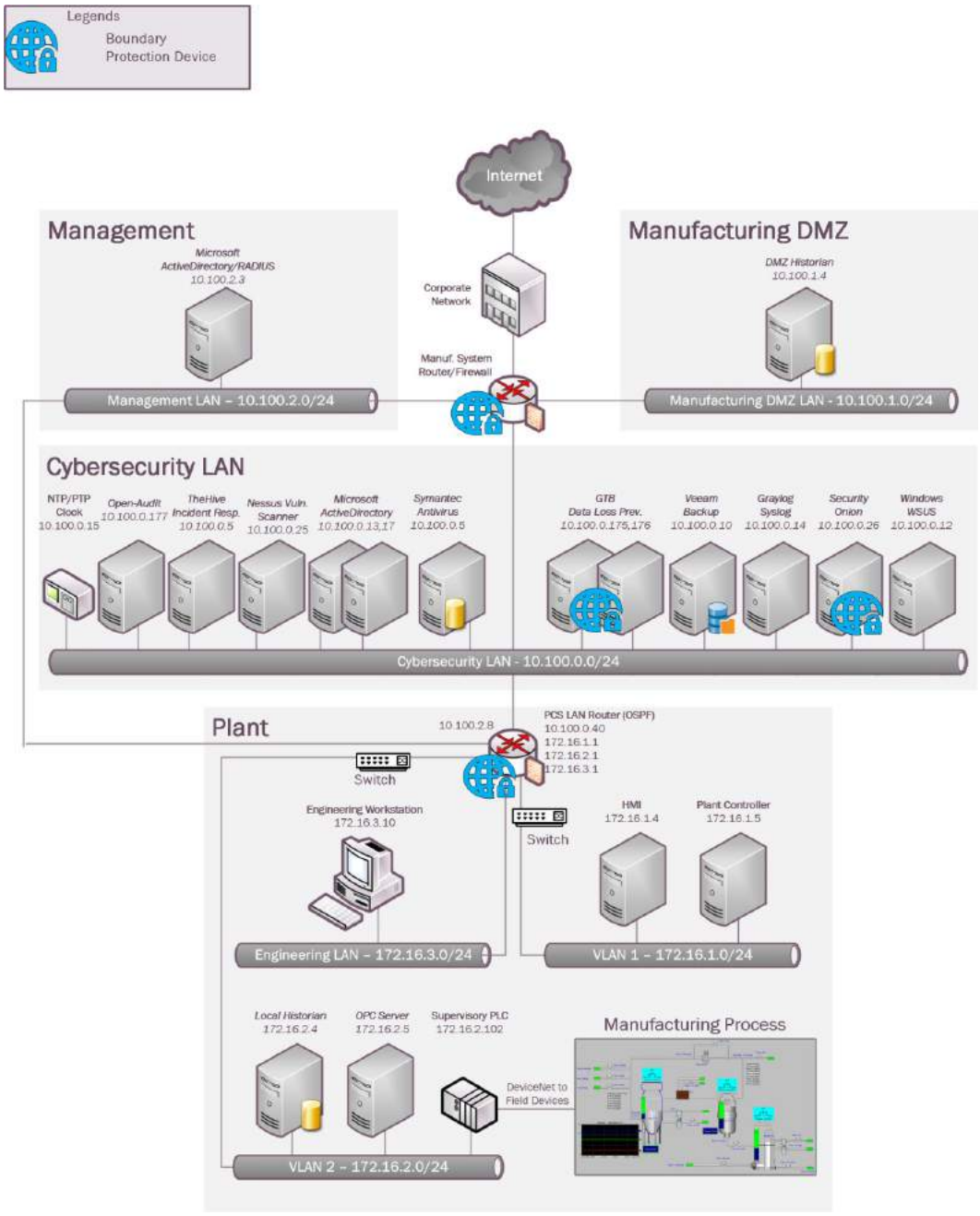
网络边界防护提供以下技术能力（参见第 1 卷第 6 章）：

- 网络边界防护

4.19.3 方案实现的子类

PR.AC-5, PR.PT-4, DE.CM-1

4.19.4 方案实施架构图



4.19.5 安装说明与配置

环境搭建

下表列举了边界防护设备：

设备	说明	位置
思科ASA 5512	运行Firepower Services FTD 6.2.3的下一代防火墙	制造系统
Allen Bradley Stratix 8300	防火墙、路由器	工作单元
GTB Inspector	数据泄露防护（DLP）虚拟设备	网络安全局域网
安全洋葱	运行Snort、BRO IDS	网络安全局域网

方案名	版本	硬件规格
Veeam备份与复制	9.5	VMware虚拟机： • 处理器：虚拟双核 • 内存：8 GB • 磁盘空间：4 TB • 网络：1个接口 • 操作系统：Windows 2012R2
Windows平台Veeam代理（免费版）	3.0.0.748	安装在工厂的所有物理设备（Windows计算机）上

思科 ASA 上的配置

在 ASA 防火墙上启用了以下功能和设置：

- 网络分段
- ACL 规则
- 互联网访问 NAT 策略
- Snort 检测
- DMZ 网络

网络分段

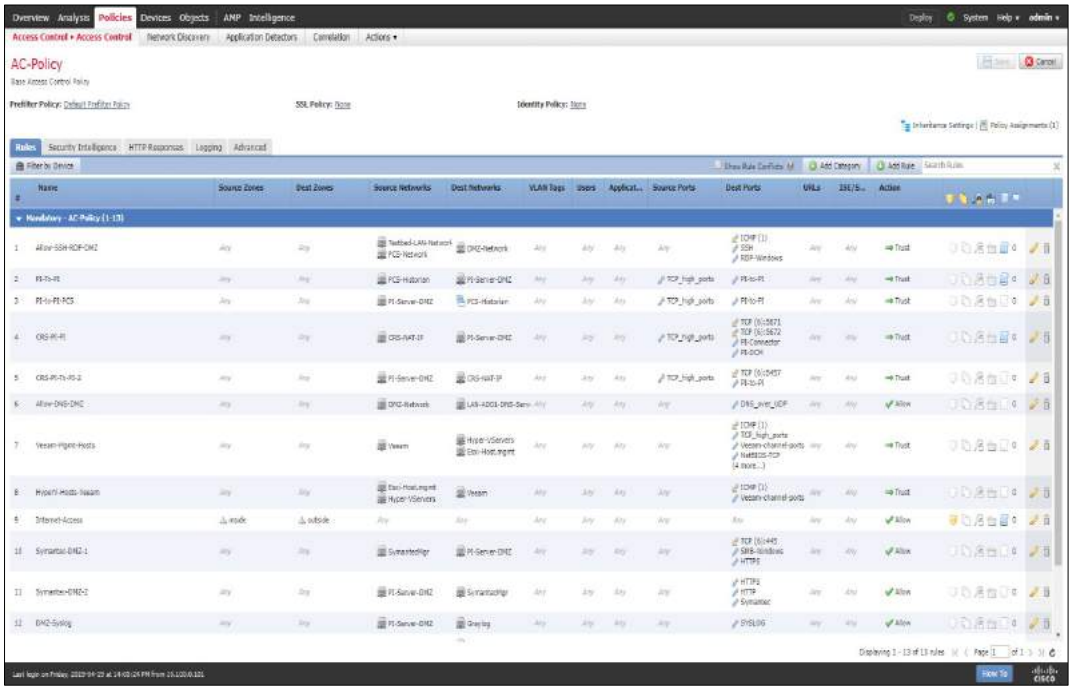
为不同的网段配置了不同的网络接口，如下所示：

- 内部接口（网络：10.100.0.0/24）
- DMZ 接口（网络：10.100.1.0/24）
- 外部接口（网络：129.6.91.x/24，连接至 NIST 企业网以访问外网）
- 公共接口（网络：129.6.1.x/24，供 VPN 用户使用）

访问控制列表（ACL）规则

ASA 上配置了如下 ACL 规则，默认动作为“Block all traffic”（拦截所有流量）。

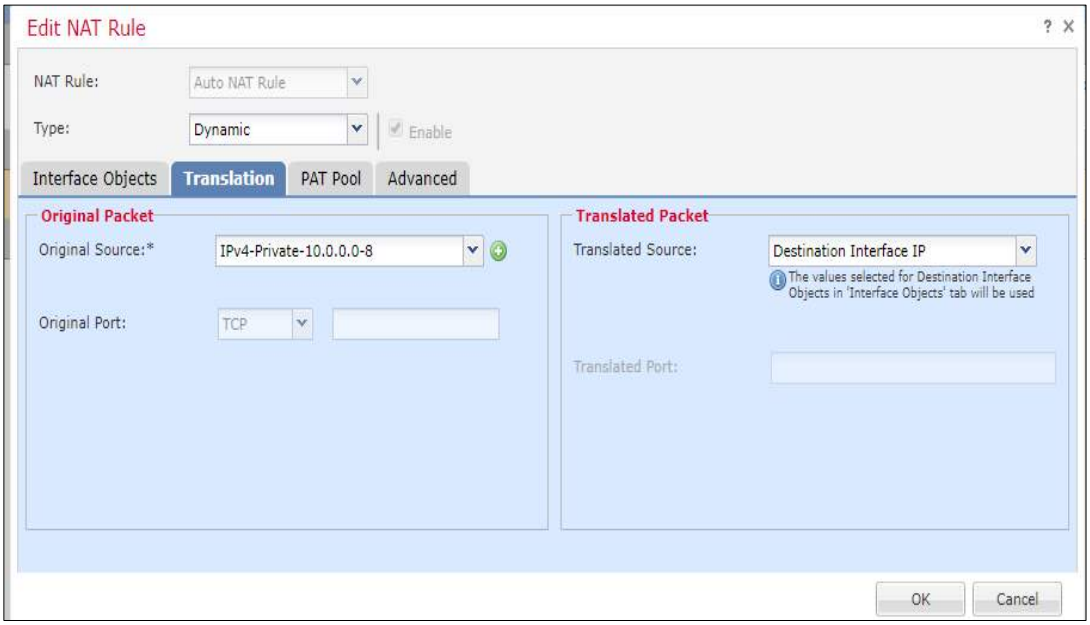
源	源端口	目的	目的端口	协议	动作
10.100.0.0/24、172.16.0.0/22	所有	DMZ网络	SSH、RDP、ICMP	TCP	信任
PCS-历史数据库（172.16.2.14）	TCP_高_端口	PCS-历史数据库	5450	TCP	信任
DMZ历史数据库	TCP_高_端口	DMZ-历史数据库	5450	TCP	信任
CRS-NAT（10.100.0.20）	TCP_高_端口	DMZ-历史数据库	5450、5460、5671、5672	TCP	信任
DMZ历史数据库	TCP_高_端口	CRS-NAT（10.100.0.20）	5457、5450	TCP	信任
DMZ历史数据库	所有	活动目录（10.100.0.17）	53	UDP	放行
Veeam服务器	所有	Hyper-V宿主服务器、Esxi宿主服务器	NETBIOS、ICMP、HTTPS、445、TCP_高_端口, 2500~5000、6160~6163	TCP	信任
Hyper-V宿主服务器、Esxi宿主服务器	所有	Veeam服务器	ICMP、2500~5000	TCP	信任
内部接口	所有	外部_接口	所有	所有	放行
DMZ历史数据库	所有	赛门铁克服务器	SMB (445)、HTTPS	TCP	信任
赛门铁克服务器	所有	DMZ历史数据库	HTTP、HTTPS、8014	TCP	信任
DMZ历史数据库	所有	Graylog服务器	514	UDP	信任
VPN_池（192.168.100.10~20）	所有	PCS-HMI-服务器、PCS-工作站	3389	TCP	放行



NAT 策略

配置了动态 NAT 策略，允许访问互联网：

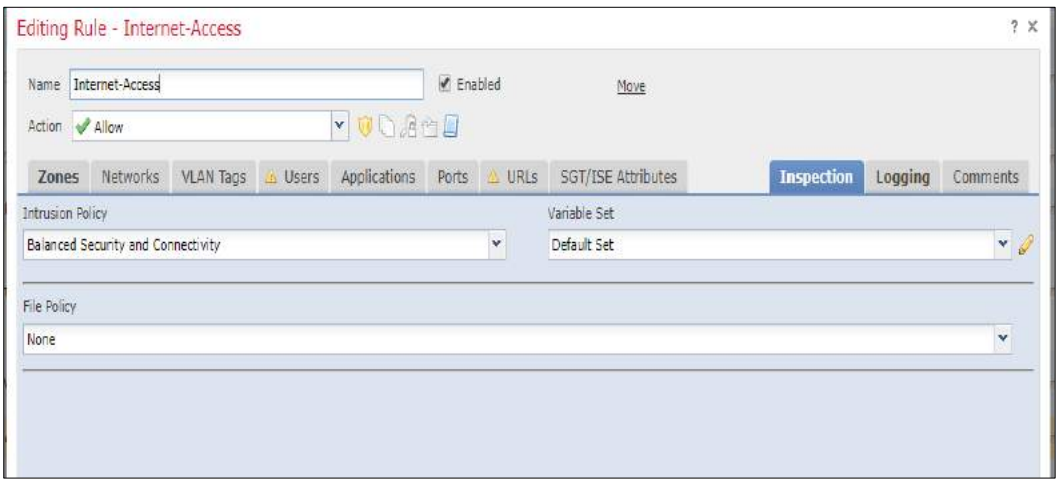
NAT规则类型	自动NAT
源接口	内部
目的接口	外部
转换前源地址	10.100.0.0/8
转换后源地址	目的接口IP
选项	转换匹配本规则的DNS应答：否



Snort 检测

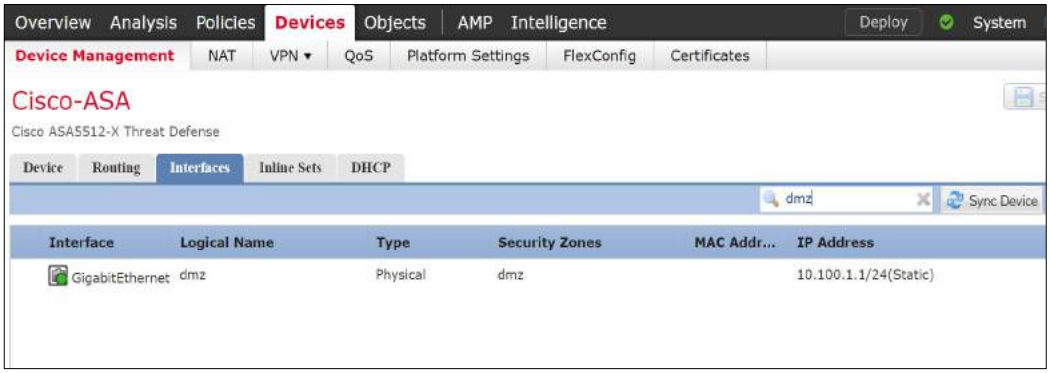
对下列 ACL 规则启用了 Snort 检测：

ACL规则名	入侵策略
放行-DNS-DMZ	均衡连接与安全
互联网访问规则	均衡连接与安全
VPN规则	均衡连接与安全



DMZ 网络

为制造 DMZ 局域网配置了单独的接口，用以托管 DMZ 历史数据库服务器。



Allen Bradley 防火墙配置

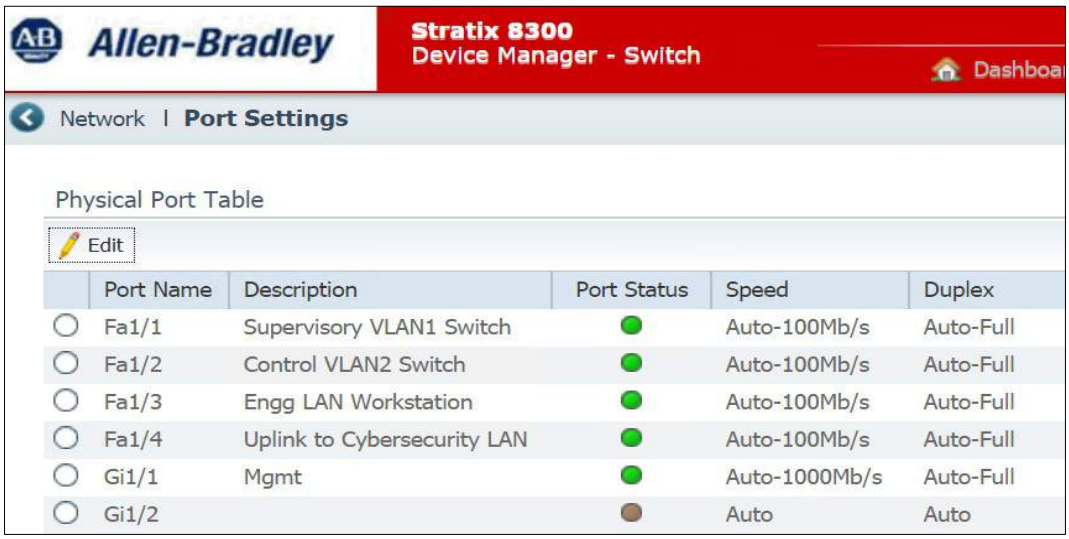
在 Allen Bradley 防火墙上启用了以下功能和设置：

- 网络分段
- ACL 规则

网络分段

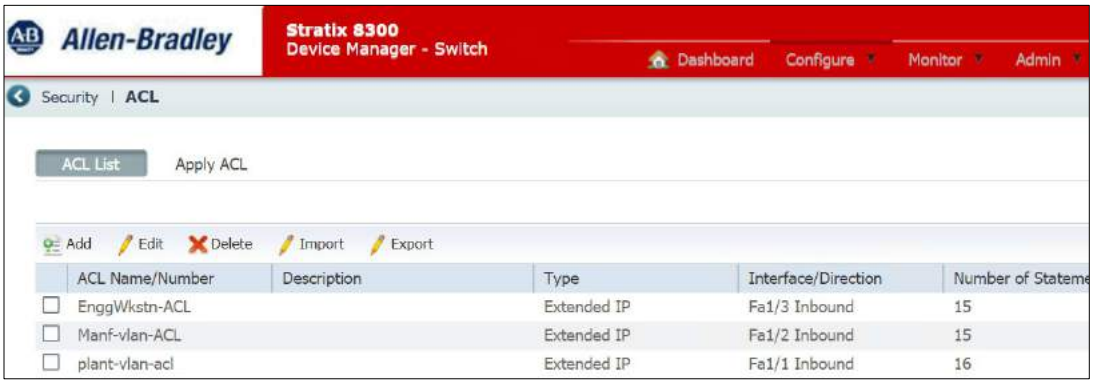
为不同的网段配置了不同的网络接口，如下所示：

- 监控 VLAN1（网络：172.16.1.0/24）
- 控制 VLAN2 接口（网络：172.16.2.0.0/24）
- 工程局域网（网络：172.16.3.0/24）
- 上行（IP 地址：10.100.0.40，向上连接至网络安全局域网）
- 管理接口（IP 地址：10.100.2.8）



访问控制列表（ACL）规则

创建了三条 Extended（扩展）类型的 ACL 规则，如下图所示。每条规则关联一个特定的网络接口，进行入向控制：



下图为防火墙的 running-config 文件中的部分 ACL：

```
ip access-list extended EnggWkstn-ACL
  permit ip host 172.16.3.10 10.100.0.0 0.0.0.255
  permit tcp host 172.16.3.10 172.16.1.0 0.0.0.15 eq 3389
  permit tcp host 172.16.3.10 172.16.2.0 0.0.0.15 eq 3389
  permit icmp host 172.16.3.10 any
  permit tcp host 172.16.3.10 host 172.16.2.102 eq 44818
  permit ip host 172.16.3.10 host 172.16.3.1
  permit ip host 172.16.3.10 host 172.16.2.2
  permit ip host 172.16.3.10 host 172.16.1.3
  permit tcp host 172.16.3.10 host 10.100.1.4 eq 3389
  permit tcp host 172.16.3.10 host 129.6.1.2 eq ftp
  permit tcp host 172.16.3.10 host 129.6.1.2 eq 22
  permit tcp host 172.16.3.10 host 129.6.1.2 eq www
  permit tcp host 172.16.3.10 host 172.16.2.102
  permit tcp 192.168.100.0 0.0.0.255 host 172.16.3.10 eq 3389
  permit tcp host 172.16.3.10 host 192.168.100.10 gt 49000
```

```
ip access-list extended Manf-vlan-ACL
 permit ip 172.16.2.0 0.0.0.15 172.16.1.0 0.0.0.15 log
 permit icmp 172.16.2.0 0.0.0.255 any log
 permit tcp 172.16.2.0 0.0.0.255 host 172.16.3.10 gt 49000 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.5 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.10 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.13 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.17 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.25 log
 permit ip 172.16.2.0 0.0.0.255 host 10.100.0.177 log
 permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.234 log
 permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq www log
 permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq 443 log
 permit tcp 172.16.2.0 0.0.0.255 host 10.100.0.12 eq 8530 log
 permit udp 172.16.2.0 0.0.0.255 host 10.100.0.14 eq syslog

ip access-list extended plant-vlan-acl
 permit ip 172.16.1.0 0.0.0.15 172.16.2.0 0.0.0.15 log
 permit icmp 172.16.1.0 0.0.0.255 any log
 permit tcp 172.16.1.0 0.0.0.255 host 172.16.3.10 gt 49000 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.5 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.10 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.13 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.17 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.25 log
 permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.234 log
 permit udp 172.16.1.0 0.0.0.255 host 10.100.0.14 eq syslog log
 permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq www log
 permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq 443 log
 permit tcp 172.16.1.0 0.0.0.255 host 10.100.0.12 eq 8530 log
 permit ip 172.16.1.0 0.0.0.255 host 10.100.0.177 log
 permit tcp 192.168.100.0 0.0.0.255 host 172.16.1.4 eq 3389 log
 permit tcp host 172.16.1.4 192.168.100.0 0.0.0.255 gt 49000
log
```

GTB Inspector 配置

详细信息，见 4.15 节。

安全洋葱配置

详细信息，见 4.7 节。

4.19.6 对性能的主要影响

在下面的实验中，我们测量了制造系统正常运行时网络边界防护对系统性能的影响：

实验 PL004.1– 在 PCS 边界防火墙上启用防火墙规则

启用防火墙规则时，没有观察到显著的性能影响。例如，防火墙规则启用前后，HMI 和 OPC 之间的报文往返时间基本一致。

应用规则需谨慎，深入了解系统很重要。防火墙规则一旦误配，可能会拦截合法连接，导致系统故障。

在 PCS 系统应用防火墙规则前，对网络连接进行了深入分析，找出了所有合法连接。有些网络连接是合法的，但不易分辨，有些连接时间很短。进行了验证测试，确保放过所有的合法网络连接，保证业务正常运行。实施和验证测试均在计划系统停机时间内完成。

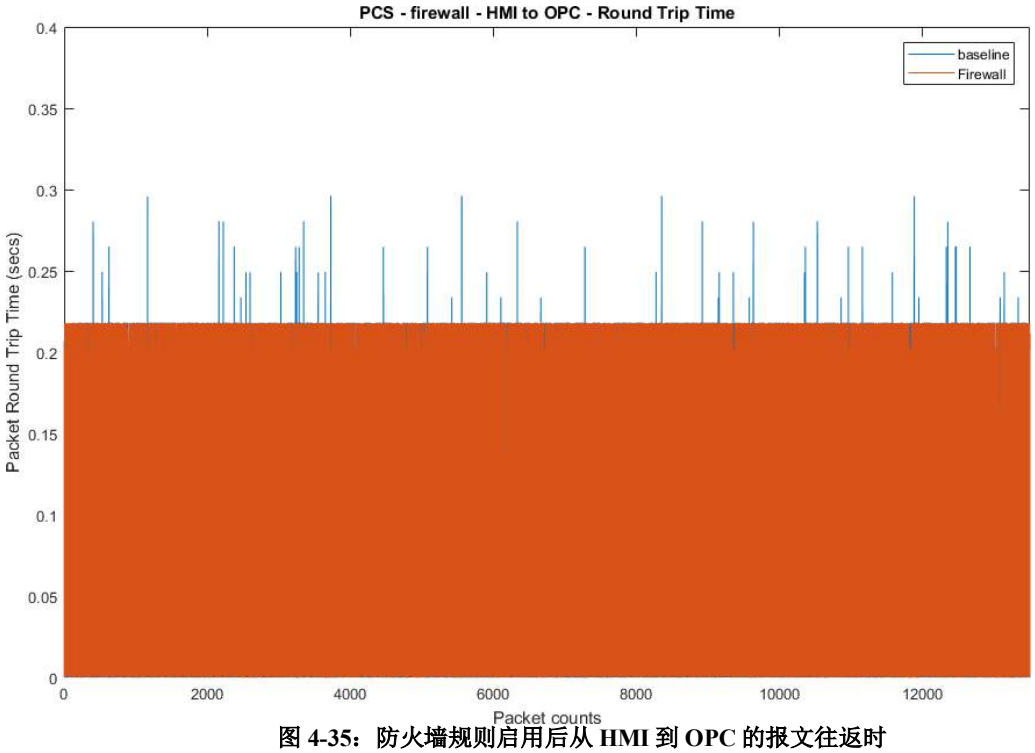


图 4-35：防火墙规则启用后从 HMI 到 OPC 的报文往返时

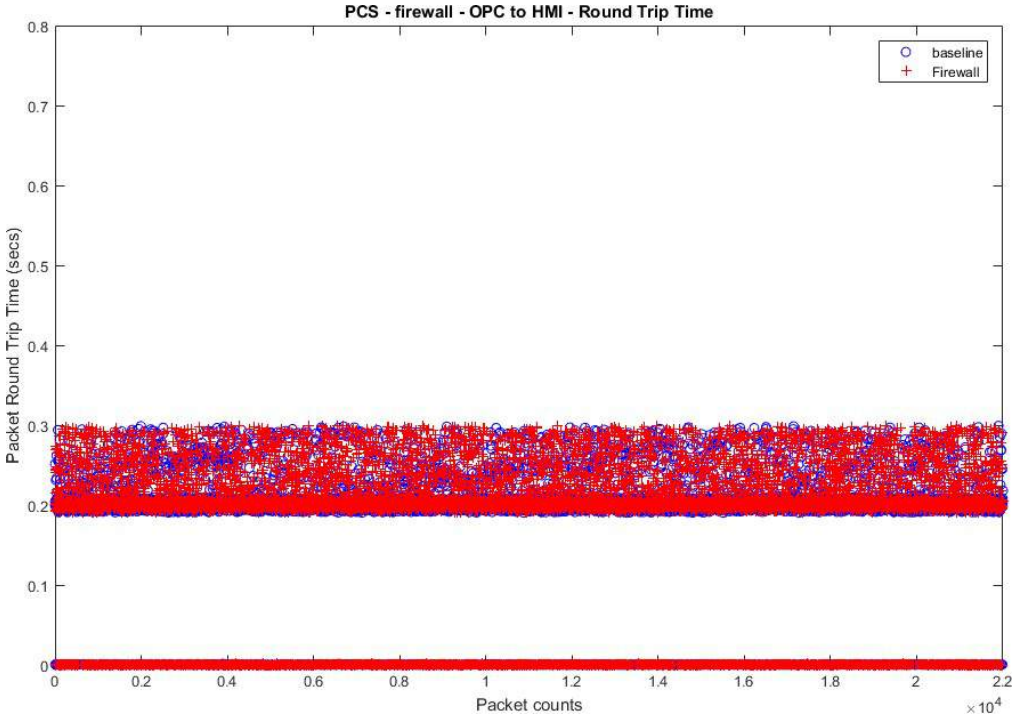


图 4-36：防火墙规则启用后从 OPC 到 HMI 的报文往返时间

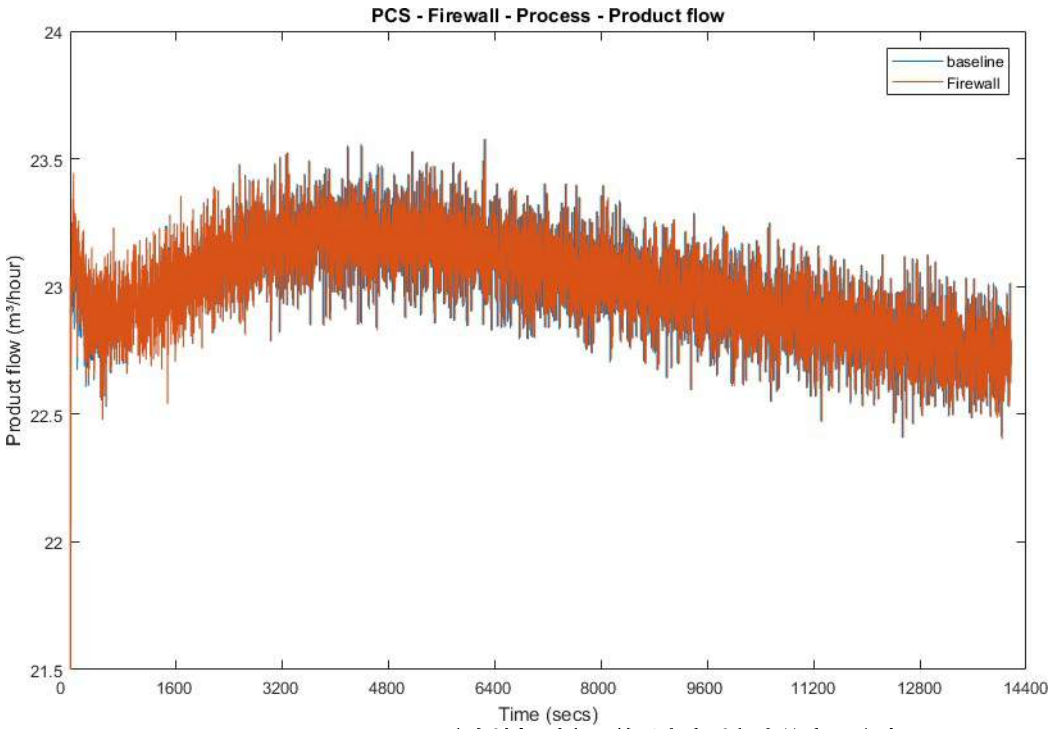


图 4-37：防火墙规则启用前后生产过程中的产品流速

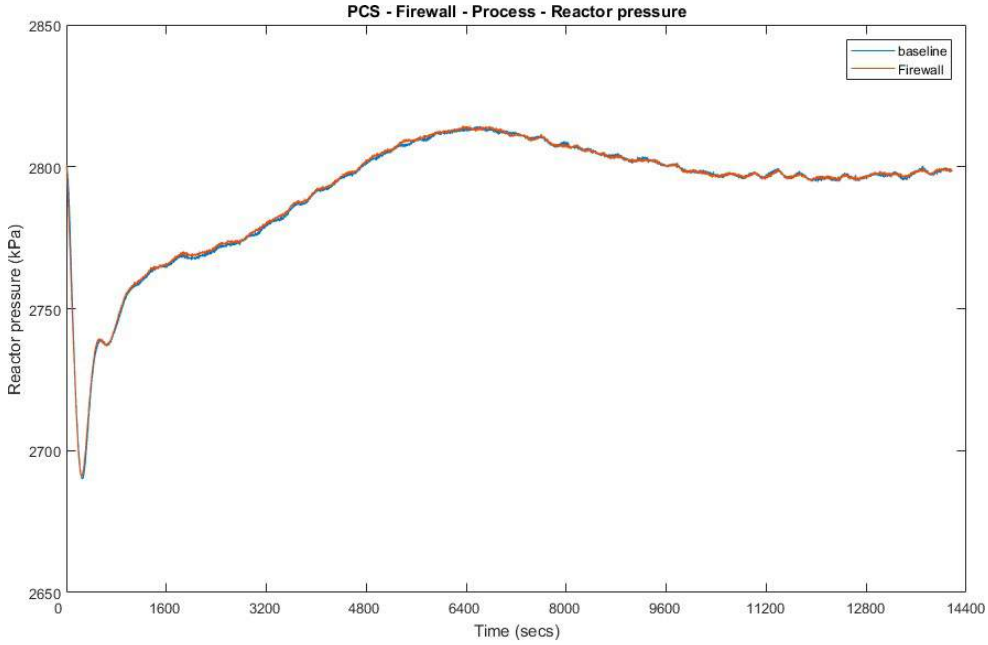


图 4-38：防火墙规则启用前后生产过程中的反应器压强

4.19.7 性能测量数据集的相关链接

- 防火墙 KPI 数据
- 防火墙测量数据

4.20 管理网络接口

4.20.1 技术方案概述

管理网络接口控制哪些网络设备可接入制造系统中的交换机，再根据连接的物理标签，对系统进行识别和分类。所有必要操作均直接在交换机外部进行。所使用的交换机端口将在交换机控制台进行逻辑标记，再加上相应网线，便于识别。所有网线均应贴上标签，说明哪一端连接交换机，哪一端连接其他设备。应配置交换机端口安全，仅允许预配置的授权媒体访问控制（MAC）地址设备访问交换机。

贴标签成本极低，且易于操作，但工作量会很大，要花费时间准确识别电缆连接。

多数交换机内置了端口安全，所以，不需要额外的实施成本。端口安全有详尽的配置文档，配置起来并不难。

4.20.2 方案提供的技术能力

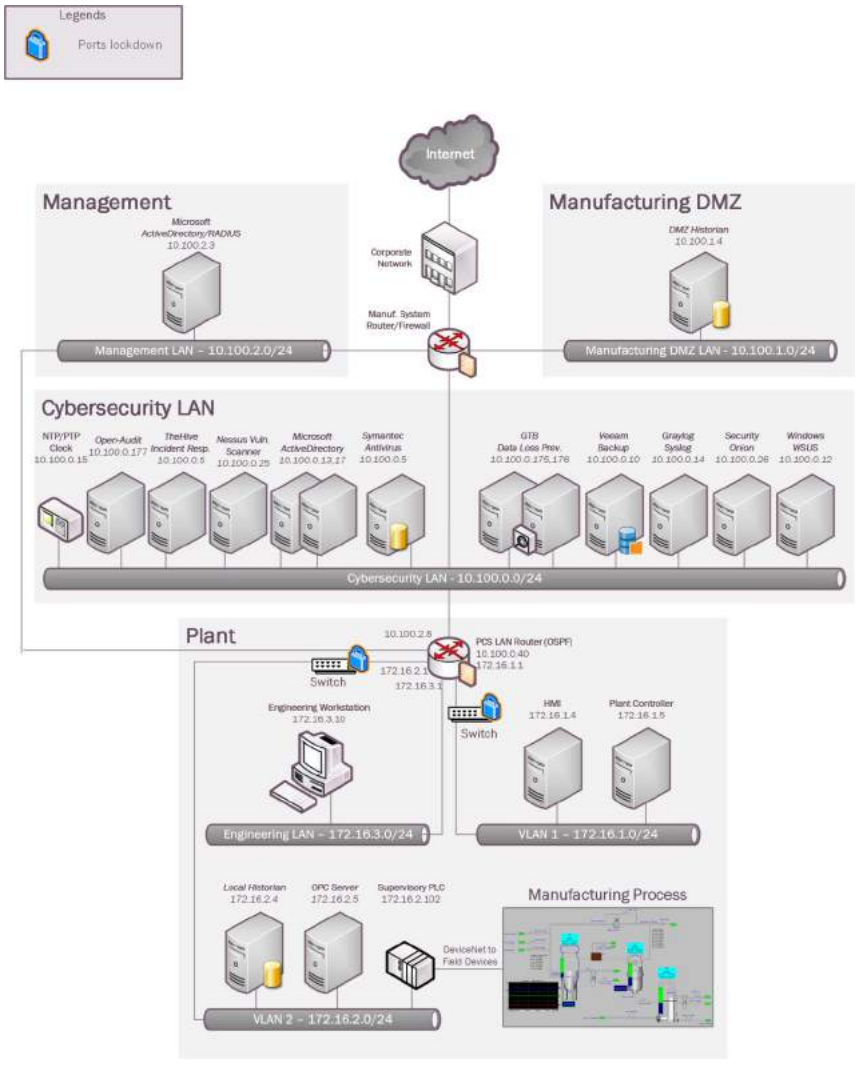
管理网络接口提供以下技术能力（参见第 1 卷第 6 章）：

- 管理网络接口

4.20.3 方案实现的子类

PR.AC-5

4.20.4 方案实施架构图



4.20.5 装说明与配置

管理网络接口按如下方式实现：

端口标记

端口标记方便其他人了解网络设备的位置。对交换机正确标记、分类可简化故障排除并提高网络安全性。

- 对 Allen Bradley 路由器和交换机进行端口标记：
  a. 通过Web浏览器登录交换机/路由器。
  b. 选择**Configure > Port Settings**（配置 > 端口设置）。
  c. 选择要标记的端口，单击【**Edit**】（编辑）。
  d. 在【**Description**】（说明）字段处输入标签。
  e. 单击【**OK**】，保存配置并退出。
- 也可在命令行窗口输入命令，标记端口：

```
#enable
#configure terminal (config)#Interface FastEthernet1/3
description <label>
(config)#end #wr mem
```

端口安全配置

端口安全或 MAC 地址过滤是用于控制访问的安全方法。使用这种方法，我们可以将设备的 MAC 地址加入黑名单或白名单，防止未经授权的设备接入网络交换机，获取敏感信息，将该等信息用于映射网络连接，最终泄漏数据。未经授权的设备接入受保护端口时，会记录告警日志并发送到 Syslog 服务器（若产品支持）。

- 对 Allen Bradley 路由器和交换机配置端口安全：
  a. 通过Web浏览器登录设备。
  b. 选择**Configure > Security > Port Security**（配置 > 安全 > 端口安全）。
  c. 选择需要配置安全措施的端口，单击【**Edit**】（编辑）按钮。
  d. 勾选【**Enable**】（启用）复选框，单击【**Add Learned MAC Addresses**】（添加学习到的MAC地址）或手动添加MAC地址。
  e. 添加MAC地址后，单击【**OK**】，保存设置。
  f. 若需要添加多个MAC地址，修改【**Maximum MAC Count**】（最大MAC地址数）为该端口所要求的MAC地址数。

工厂网络中的 Allen Bradley 边界路由器的部分配置如下：

```
Interface FastEthernet1/3 description Engg LAN
Workstation switchport mode access
switchport port-security mac-address 40a8.f03d.48aw
switchport port-security
ip access-group EnggWkstn-ACL in
```

工厂网络中的 Allen Bradley 边界交换机的部分配置如下：

```
Interface     FastEthernet1/1     Switchport
access vlan 102 switchport mode access
switchport port-security mac-address e490.693b.c2c7
switchport port-security
```

禁用无用端口

- 禁用 Allen-Bradley 路由器和交换机上的无用端口：
  a. 在主页上单击**Configure > Port Settings**（配置 > 端口设置）。
  b. 找出操作模式标记为“**down**”（关闭）的所有端口。
  c. 选中需要禁用的端口，单击**【Edit】**（编辑）。
  d. 在**【Edit Physical Port】**（编辑物理端口）窗口中，取消对**【Enable from Administrative】**（管理员启用）的勾选，单击**【OK】**。端口被禁用，任何设备插入此端口或其他禁用端口都无法正常工作。

Allen Bradley 交换机的禁用端口配置如下：

```
Interface FastEthernet1/2 shutdown

Interface FastEthernet1/8 shutdown
```

4.20.6 对性能的主要影响

鉴于管理网络接口的实现方法（在配置中手动禁用无用网络接口），未测试其对网络的性能影响。

4.20.7 性能测量数据集的相关链接

无

4.21 时间同步

4.21.1 技术方案概述

时间同步允许设备与可靠的时间源同步。时间同步对于系统登录、事件跟踪和制造系统中发生的其他时间敏感事件至关重要。

4.21.2 方案提供的技术能力

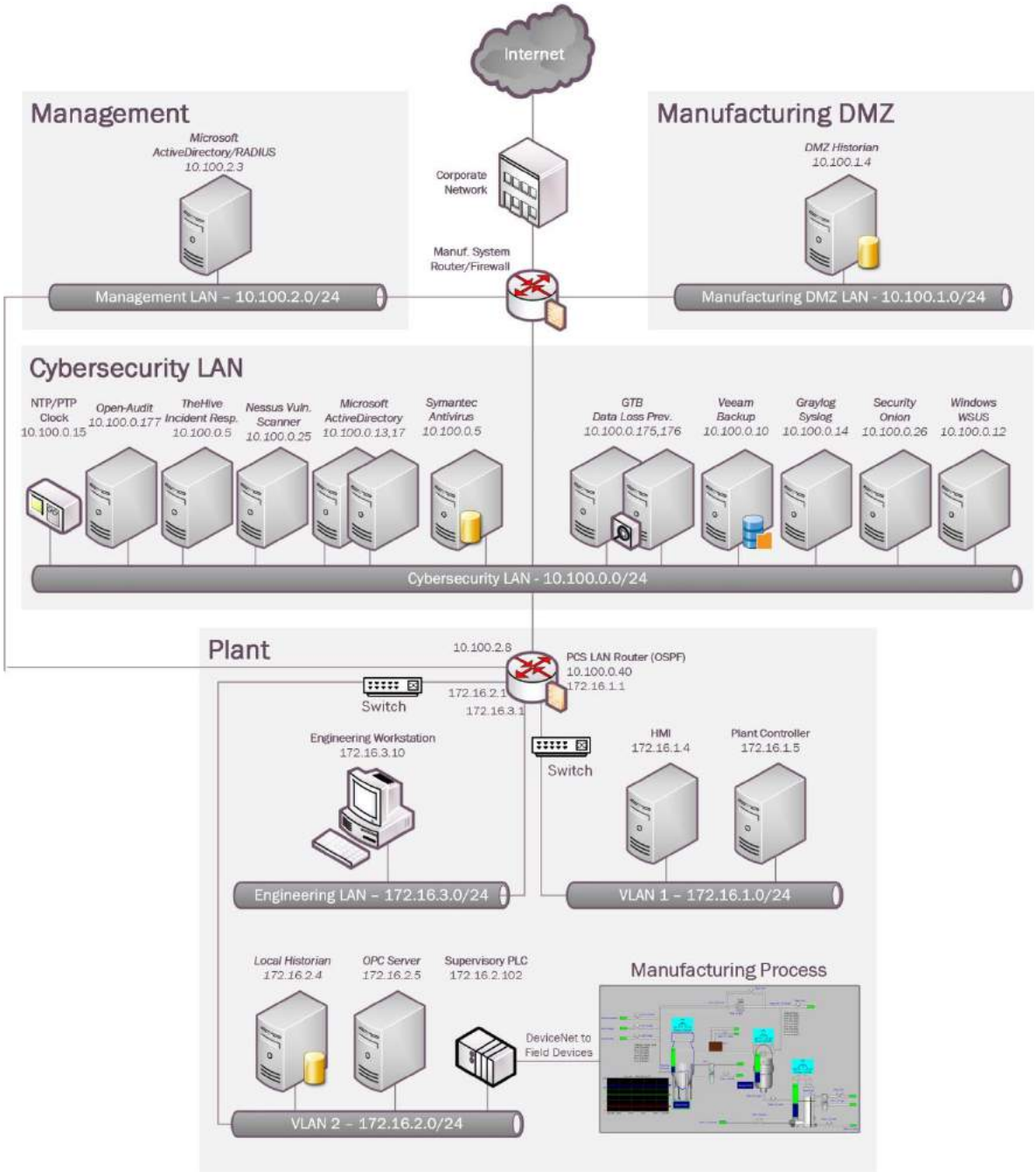
时间同步提供以下技术能力（参见第 1 卷第 6 章）：

- 时间同步

4.21.3 方案实现的子类

PR.PT-1

4.21.4 方案实施架构图



4.21.5 安装说明与配置

NTP 服务器详细实施信息如下：

工具名	IP地址	功能	硬件规格
Grandmaster	10.100.0.15	NTP/PTP时钟	型号：Meinberg Lantime M900

Meinberg M900 时间服务器

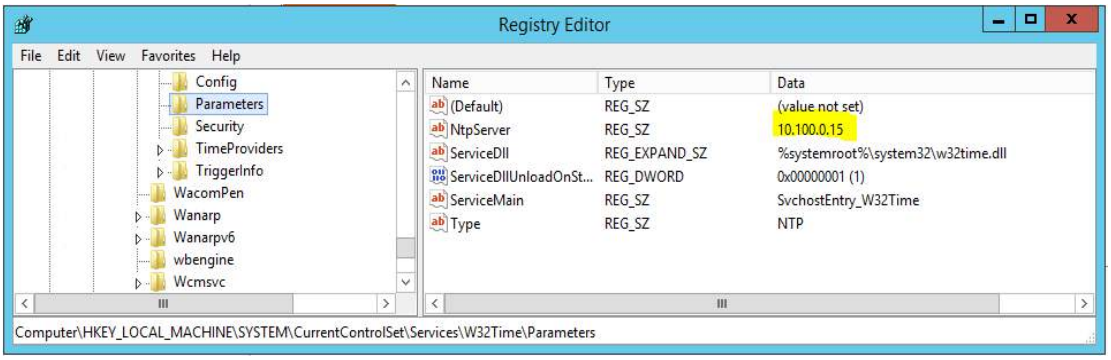
与典型 Windows 活动目录环境的默认功能相比，工业/制造环境通常需要更高的时间精度。考虑到这一点，使用了时间精度高达毫秒级的外部硬件时钟 Meinberg M900。配置该设备从上游的 NIST 时间服务器获取时间。

在域控制器上配置 NTP

对于在制造系统中承担 PDC 仿真器角色的活动目录域控制器[123]，将其配置为从 Meinberg Lantime M900 设备获取时间。

将域控制器上的以下注册表项更改为用 **w32Time.exe** 从外部源 IP 地址同步时间：

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Para meters\NtpServer**
- 下图中，域控制器指向 Meinberg Lantime M900 时钟的 IP 地址。



在成员服务器上配置 NTP

所有 Windows 计算机已加入活动目录域，这些机器自动连接本地域控制器（活动目录服务器），同步时间。

在网络设备上配置 NTP

制造系统中的所有其他设备如交换机、路由器等都配置为使用 NTP 与 Meinberg M900 同步时间。

对于 Allen Bradley 边界路由器和交换机，按如下步骤配置 NTP：

- 登录路由器/防火墙的 Web 界面。
- 选择 **Configure > NTP**（配置 > NTP）。
- 单击【**Add**】（添加）。

[123] https://support.microsoft.com/en-us/help/197132/active-directory-fsmo-roles-in-windows

- 输入时间源的 IP 地址。
- 单击【**Save**】（保存）。
- 完成后退出系统。

补充信息

选择的主时间参考应尽可能靠近设备的物理位置，以减少偏移量。

4.21.6 对性能的主要影响

鉴于时间同步在实施网络安全制造篇之前已在系统上实现，因此没有测试其对网络性能的影响。

4.21.7 性能测量数据集的相关链接

无

4.22 系统操作监控

4.22.1 技术方案概述

系统操作监控通过多种工具实现，利用数据外泄防护、系统加固和 Syslog 服务器进行监控、存储和审计，保护制造系统环境，使其免受恶意活动的影响。各种工具按要求为制造系统提供不同级别的保护。

实施系统操作监控，工作量不大，但需要了解 Linux 系统，具有虚拟机经验。

4.22.2 方案提供的技术能力

系统操作监控提供以下技术能力（参见第 1 卷第 6 章）：

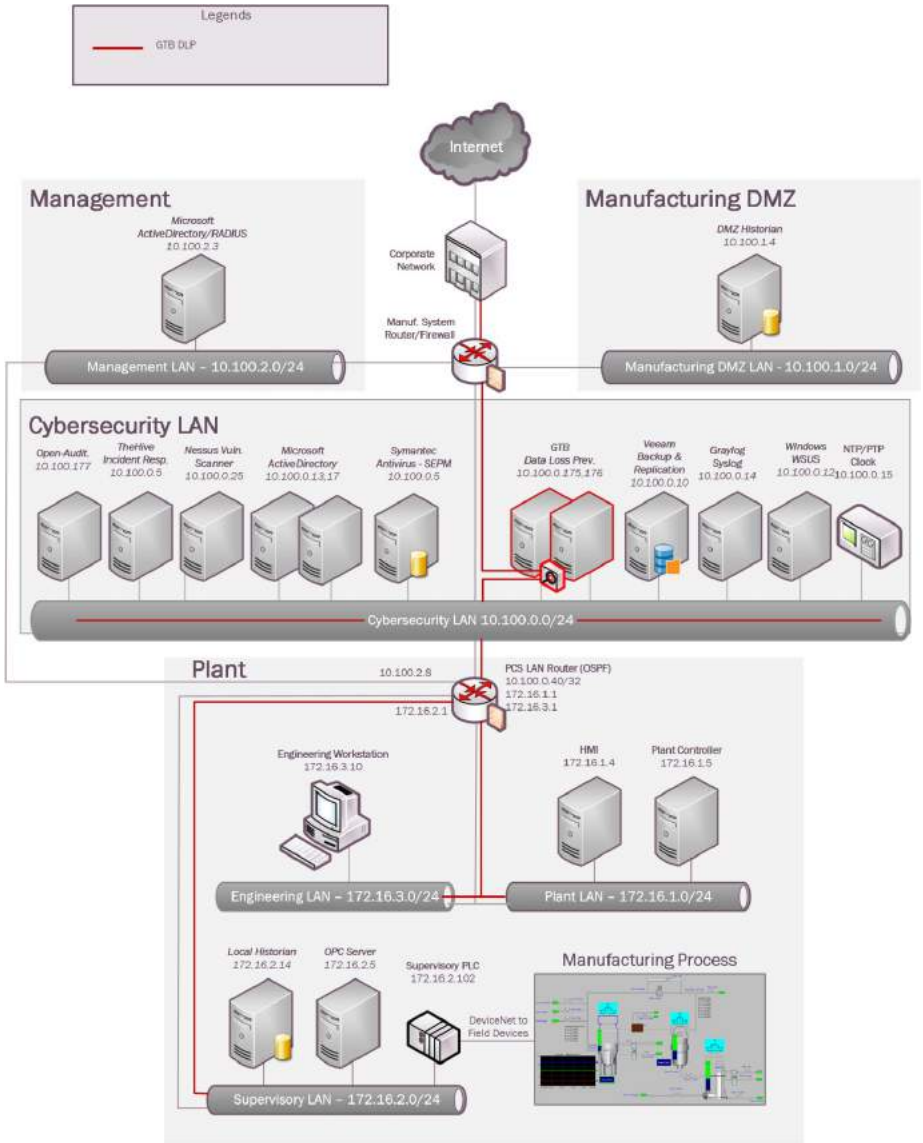
- 系统操作监控

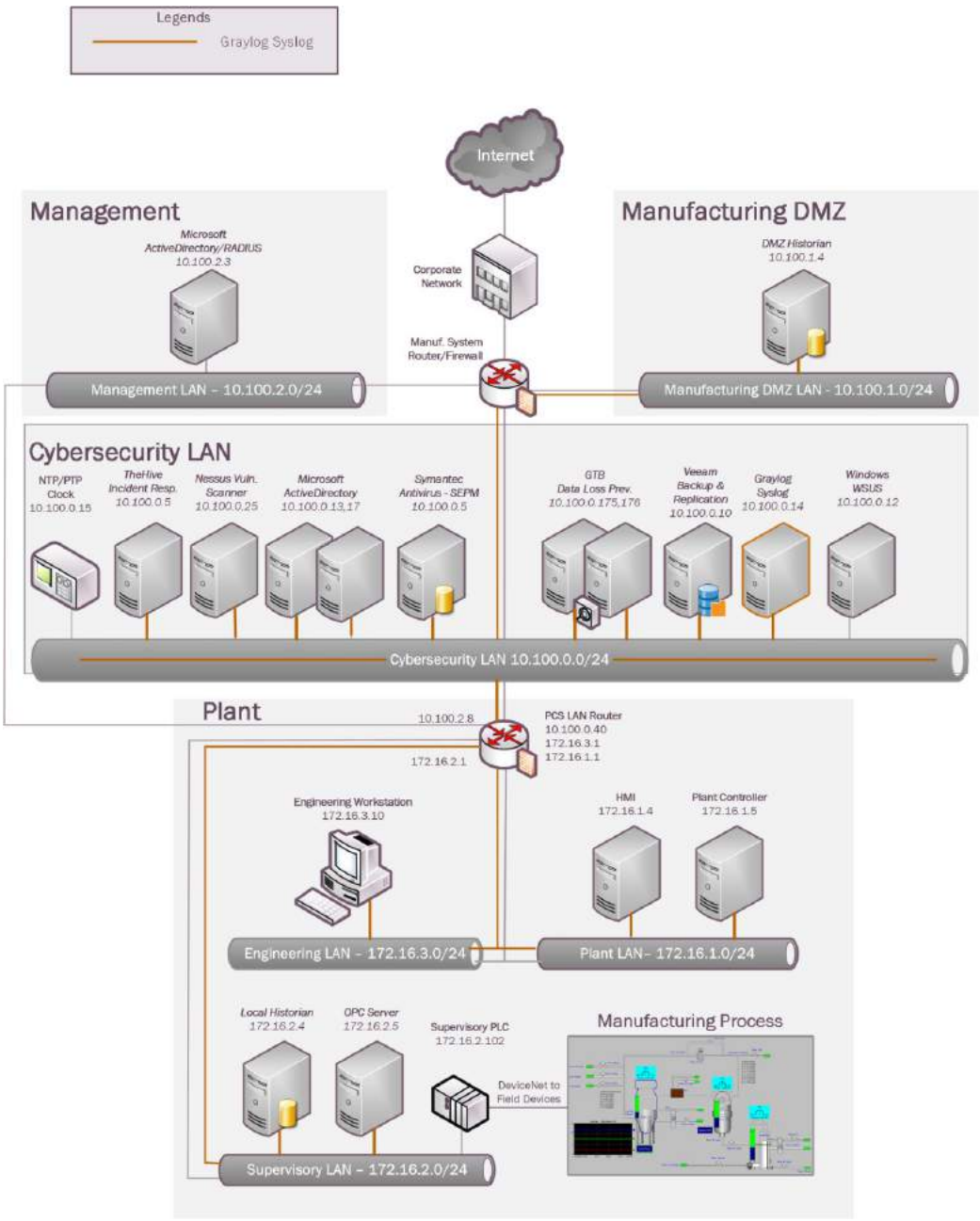
系统操作监控需要使用的工具包括 GTB Inspector、端口和服务锁定以及 Graylog。

4.22.3 方案实现的子类

PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3

4.22.4 方案实施架构图





4.22.5 安装说明与配置

系统操作监视通过多种工具实现，如 GTB Inspector、Graylog 和 Windows 服务器自带功能（如启用审核、限制管理用户帐户等）。

GTB DLP：具体安装配置，见 4.15.5 节。

Graylog：具体安装配置，见 4.16.5 节。

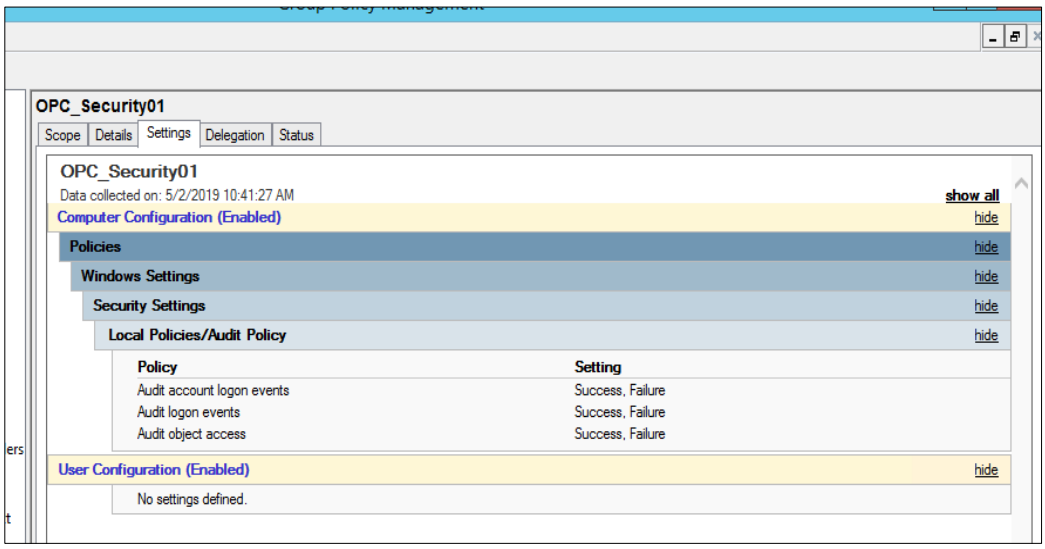
在 Windows 上启用审核

审核登录事件

- 运行 **gpedit.msc**，在域控制器上启动组策略管理器。
- 编辑【**Default Domain Controller Group Policy**】（默认域控制器组策略），或新建组策略对象，将其连接到对应服务器的 OU。
- 选择 **Computer Configuration > Polices > Windows Settings > Security Settings > Local Polices > Audit Policy**（计算机配置 > 策略 >

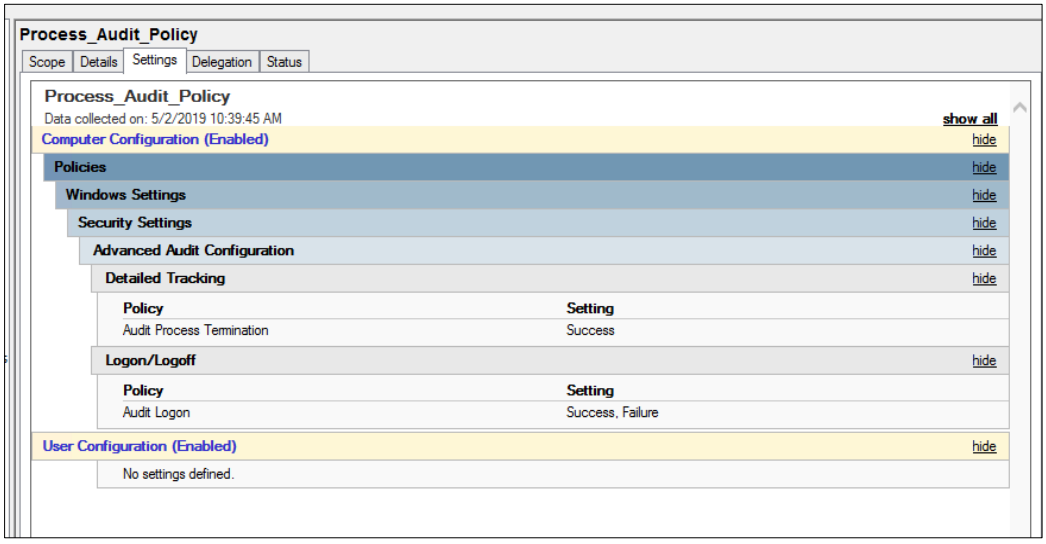
Windows 设置 > 安全设置 > 本地策略 > 审核策略）。

- 修改【**Audit Account logon events**】（审核账户登录事件）、【**Audit logon events**】（审核登录事件）和【**Audit Object access**】（审核对象访问）设置为【**Success, Failure**】，如下图所示。



审核进程终止

- 选择 **Computer Configuration > Polices > Windows Settings > Security Settings > Advanced Audit Configuration**（计算机配置 > 策略 > Windows 设置 > 安全设置 > 高级审核配置）。
- 将【**Detailed Tracking**】（详细跟踪）和【**Logon/Logoff**】（登录/注销）分别设置为 **Success 和 Success，Failure**（见下图）。



Windows – 限制管理用户

查看各系统上的本地管理员组，仅添加需要在系统上具有管理权限的帐户。

例如，创建了 AD 服务帐户 **opc-admin**，用以运行 OPC 服务器服务，对以下 2 台服务器具有管理权限：

- OPC 服务器
- 控制器服务器

限制对 PLC 的访问

PLC 的远程访问通过防火墙进行控制，仅允许从工程师站进行访问。

4.22.6 对性能的主要影响

鉴于 GTB 在网络拓扑中的位置，没有测量 PCS 中安装 GTB 后对网络的性能影响。在系统运行期间，生产过程中各组件均未频繁进行跨边界通信。

考虑到 Graylog 的典型安装位置和使用方式（在制造系统外部），没有测试其对系统性能的影响。

4.22.7 性能测量数据集的相关链接

无

4.23 端口和服务锁定

4.23.1 技术方案概述

利用端口和服务锁定方案，制造商能够发现并禁用非必要的逻辑网络端口及服务。逻辑端口是分配给“逻辑”连接的编号。每项服务分配一个端口号，这样，TCP/IP 就可以根据端口号发送流量。黑客使用端口扫描工具和漏洞扫描工具来识别服务器上的开放端口。通过这些端口，黑客可以确定服务器所提供的服务类型和运行的系统类型。将不必要的程序卸载，进而关闭不必要的端口，可以大大减少攻击面。这些操作需要手动执行。

使用了操作系统的自带功能、Open-AudIT 和 Nessus 扫描工具清点工厂所有设备上当前运行的端口和应用程序。

4.23.2 方案提供的技术能力

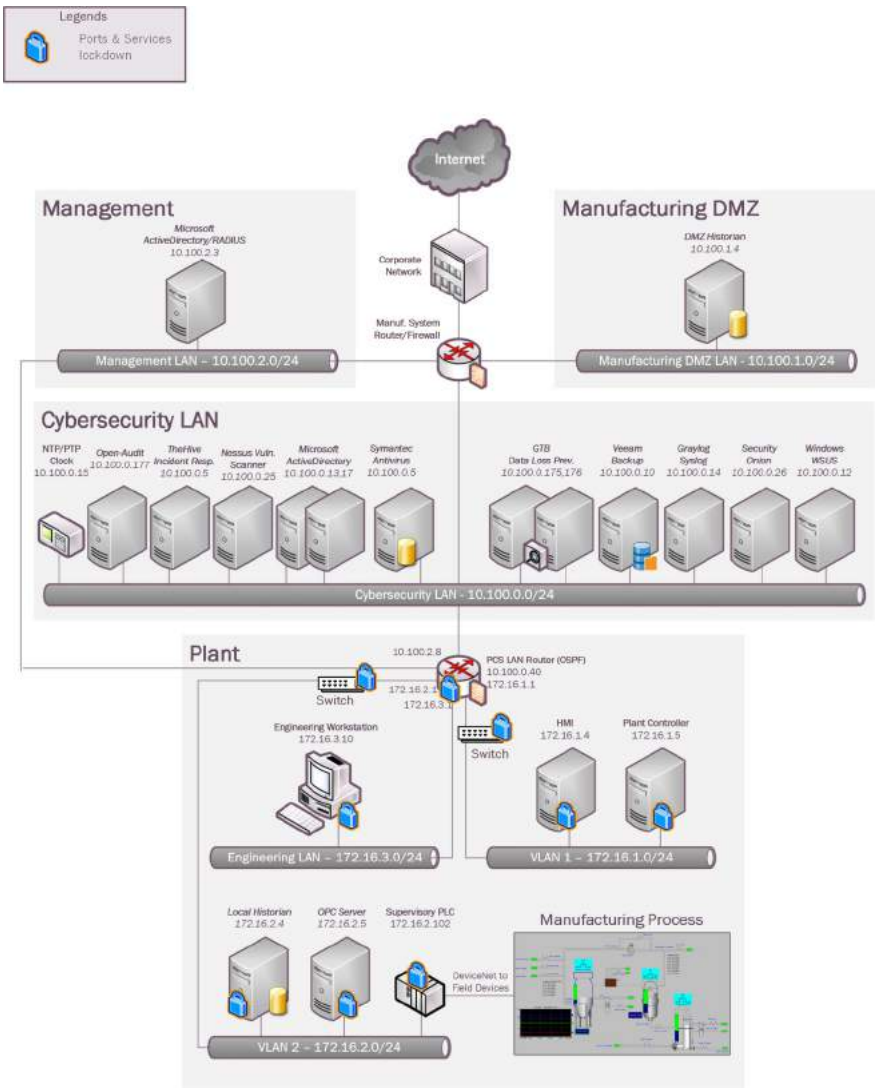
端口和服务锁定提供以下技术能力（参见第 1 卷第 6 章）：

- 端口和服务锁定

4.23.3 方案实现的子类

PR.IP-1, PR.PT-3

4.23.4 方案实施架构图



4.23.5 安装说明与配置

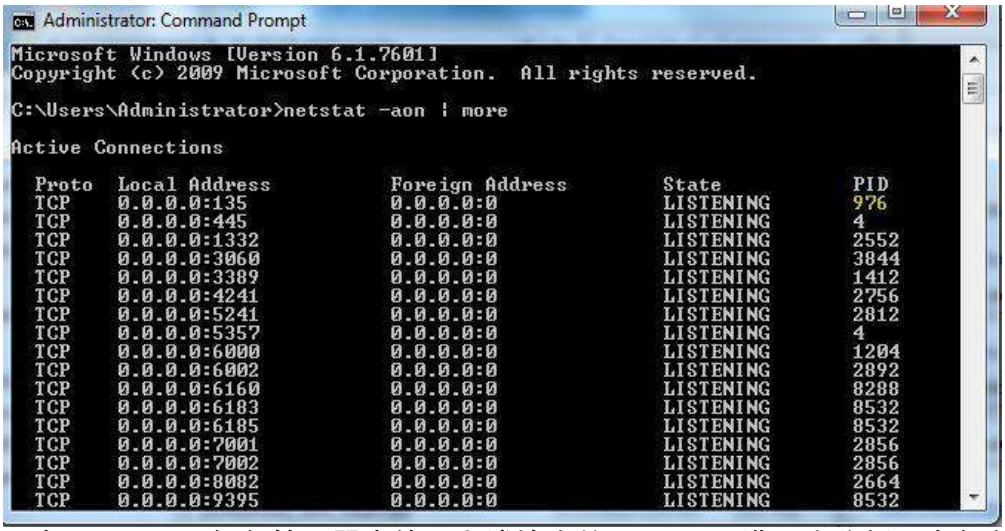
在工厂基础架构上执行如下操作进行端口和服务锁定。

从 Windows 系统中删除无用程序

按以下说明，找出系统中需要删除的无用程序：

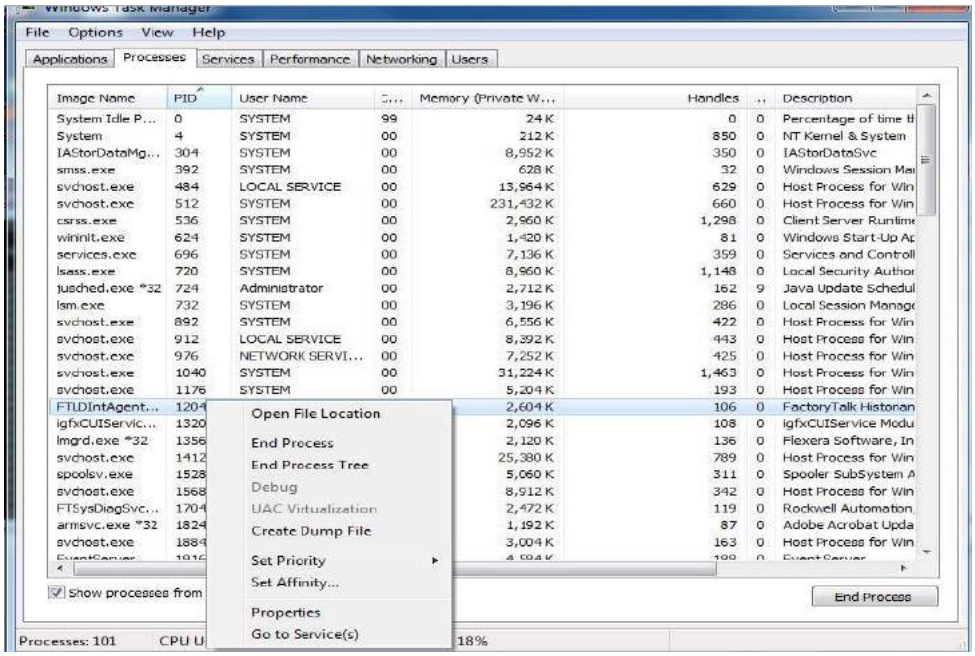
- 使用 Open-AudIT 清点各系统的软件。查看报告，找出并卸载无用程序，包括操作系统自带的一些软件。
- 使用 Netstat 实用程序收集各系统正在运行的应用程序或使用的 TCP/IP 端口信息。

  例如，运行 netstat -aon | more 命令列举进程和相关进程标识符（PID）。

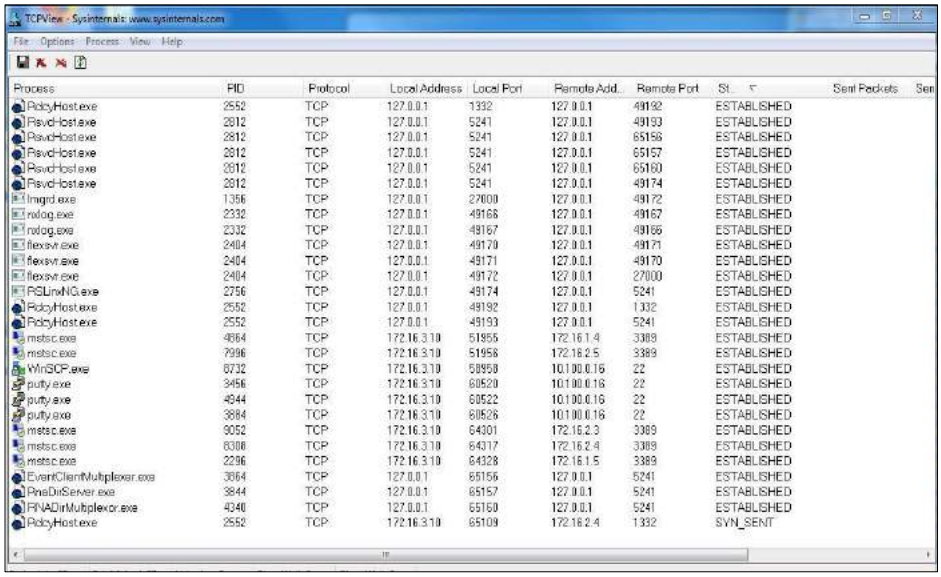


- 在 Windows 任务管理器中使用上述输出的 PID 展开进一步分析。在任务管理器（Windows 7）中，单击 **View > Select Columns**（查看 > 选择列），启用 PID 列。

- 勾选【**Show Processes for All Users**】（显示所有用户的进程），搜索列表中的 PID。要结束某进程，右键单击该进程，选择【**Open File Location**】（打开文件位置）或【**Go to Service(s)**】（转到服务），控制或终止该进程。



- 还可以使用 **Resource Monitor**（resmon.exe）（资源监视器）和 SysInternals 中的 TCPView。下图为 TCPView 示例。



禁用网络设备的不安全服务

按以下说明禁用工厂所有 Allen-Bradley 设备上的不安全服务：

- 禁用 Telnet、SNMP（v1 和 v2）等不安全服务。若需要使用 SNMP，须更改默认团体字或使用 SNMP v3。
- 运行下列命令（仅供参考），设置 enable 模式的密码。

```
#enable
#configure   terminal   (config)#enable
secret <password>
```

限制 SSH 访问

运行下列思科命令，限制指定网络的 SSH 访问：

```
 #enable
 #configure terminal
(config)#access-list 1 permit 172.16.0.0 0.0.255.255
(config)#line vty 0 15
(config)#access-class 1 in
```

加固 PLC

按以下步骤加固 PLC：

- 禁用 Telnet、SNMP、HTTP 等不安全服务。
- 使用防火墙规则限制访问，仅允许工程师站远程访问 PLC。

4.23.6 对性能的主要影响

鉴于管理网络接口的实现方法（手动禁用网络接口、删除无用的 Windows 程序和服务），未测试其对网络的性能影响。

4.23.7 性能测量数据集的相关链接

无

4.24 媒体防护

4.24.1 技术方案概述

硬件端口锁为保护 USB 端口提供了低成本的解决方案。该方案易于实施和使用，可快速安装、移除。USB 端口锁简单易行，可有效限制 USB 的使用。USB 端口锁插入并锁定后，除非使用钥匙，否则无法在不损坏 USB 端口的情况下卸下该锁。每个 USB 端口锁最多可锁住两个端口，根据挡片方向确定插入哪个端口。插入一个端口后，另一个端口被挡片遮挡，同时锁定。购买 USB 端口锁时可搭配一个锁环，以保护连接的 USB 鼠标和键盘，防止未经批准擅自移除。

4.24.2 方案提供的技术能力

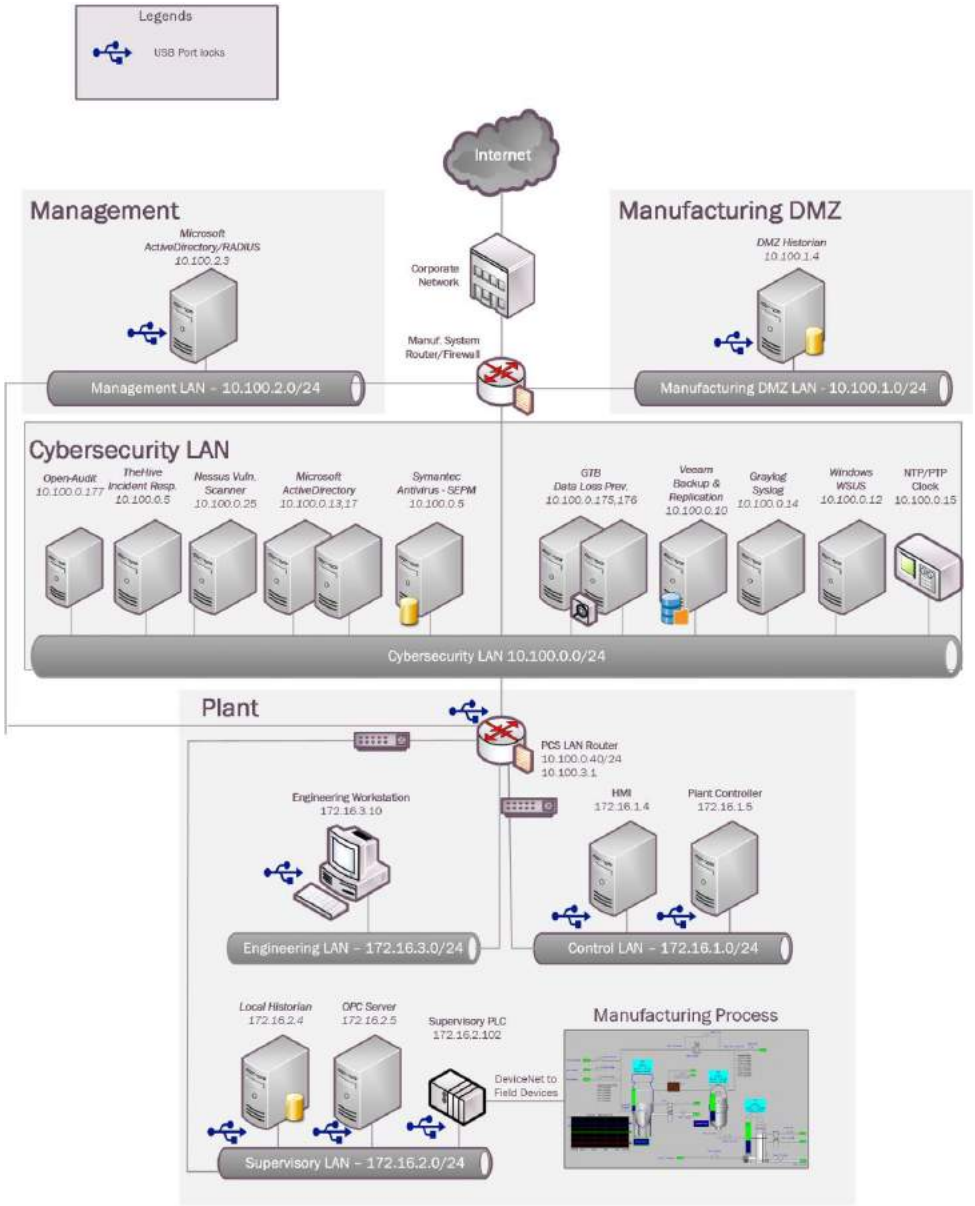
媒体防护提供以下技术能力（参见第 1 卷第 6 章）：

- 媒体防护

4.24.3 方案实现的子类

PR.PT-2

4.24.4 方案实施架构图



4.24.5 安装说明与配置

插入 USB 端口锁，按下按钮锁定。肯辛通（Kensington）提供多种插入式端口锁装置，包括 USB 键鼠保护锁。

使用本产品时需要耐心，避免不小心损坏了 USB 端口。

4.24.6 对性能的主要影响

鉴于 USB 端口锁的实现方法（物理限制对 USB 端口的访问），没有测试该锁对系统的性能影响。

4.24.7 性能测量数据集的相关链接

无

附录 A 缩略词

本文使用的缩略词列举如下：

AAA	Authentication, Authorization, and Accounting	认证、授权和计费
ACL	Access Control List	访问控制列表
AD	Active Directory	活动目录
API	Application Programming Interface	应用程序编程接口
ARP	Address Resolution Protocol	地址解析协议
AV	Anti-Virus	防病毒软件
CCN	Credit Card Number	信用卡号
CD	Compact Disk	光盘
CEO	Chief Executive Officer	首席执行官
COTS	Commercial Off-The-Shelf	商用现货
CSET	Cyber Security Evaluation Tool	网络安全评估工具
CSF	Cybersecurity Framework	网络安全框架
DC	Domain Controller	域控制器
DCS	Distributed Control System	分布式控制系统
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHS	Department of Homeland Security	国土安全部
DLP	Data Loss Prevention	数据泄露防护
DMZ	Demilitarized Zone	非军事区
DNS	Domain Name System	域名系统
DS	Domain Services	域服务
EFS	Encrypted File System	加密文件系统
FIPS	Federal Information Processing Standards	联邦信息处理标准
FTP	File Transfer Protocol	文件传输协议
GID	Generator ID	生成器 ID

HIDS	Host Intrusion Detection System	主机入侵检测系统
HMI	Human Machine Interface	人机界面
HR	Human Resources	人力资源
HTTP	Hypertext Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol Secure	超文本传输安全协议
HVAC	Heating, Ventilation, and Air Conditioning	供热、通风与空气调节（暖通）
ICMP	Internet Control Message Protocol	因特网控制消息协议
ICS	Industrial Control System	工业控制系统
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team	工控系统网络应急响应小组
ICSJWG	Industrial Control System Joint Working Group	工控系统联合工作组
IDE	Integrated Drive Electronics	集成驱动电子设备
IDS	Intrusion Detection System	入侵检测系统
IEEE	Institute of Electrical and Electronics Engineers	电气与电子工程师协会
IG	Implementation Guide	实施指南
IP	Internet Protocol	互联网协议
ISA	The International Society of Automation	国际自动化协会
ISE	Identity Services Engine	身份服务引擎
ISO	International Organization for Standardization	国际标准化组织
IT	Information Technology	信息技术
KPI	Key Performance Indicator	关键性能（绩效）指标
LAN	Local Area Network	局域网
LDAP	Lightweight Directory Access Protocol	轻量目录访问协议
LDAPS	Secure LDAP	安全 LDAP
MAC	Media Access Control	媒体访问控制
MFG	Manufacturing	制造业
MGMT	Management	管理
NAT	Network Address Translation	网络地址转换
NCCIC	National Cybersecurity and Communications Integration Center	国家网络安全与通信集成中心
NETBIOS	Network Basic Input/Output System	网络基本输入输出系统
NIDS	Network Intrusion Detection System	网络入侵检测系统

NIST	National Institute of Standards and Technology	国家标准与技术研究院
NISTIR	National Institute of Standards and Technology Internal Report	国家标准与技术研究院内部报告
NPS	Network Policy Server	网络策略服务器
NSA	National Security Agency	国家安全局
NTFS	New Technology File System	新技术文件系统
NTP	Network Time Protocol	网络时间协议
NVD	National Vulnerability Database	国家漏洞数据库
OPC	Open Platform Communications	开发平台通信
OS	Operating System	操作系统
OSSEC	Open Source HIDS SECurity	开源 HIDS 安全
OT	Operational Technology	运营技术
PC	Personal Computer	个人计算机
PCS	Process Control System	过程控制系统
PLC	Programmable Logic Controller	可编程逻辑控制器
PPD	Presidential Policy Directive	总统政策令
PPP	Point to Point protocol	点对点协议
PPTP	Point to Point tunneling protocol	点对点隧道协议
PTP	Precision Time Protocol	高精度时间同步协议
RDP	Remote Desktop Protocol	远程桌面协议
SCADA	Supervisory Control and Data Acquisition	数据采集与监视控制系统
SDLC	System Development Lifecycle	系统开发生命周期
SEC	Security	安全
SEPM	Symantec End-Point Protection Manager	赛门铁克端点保护管理器
SID	Signature ID	特征 ID
SIEM	Security Information and Event Management	安全信息和事件管理
SMB	Server Message Block	服务器消息块
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全外壳
SSL	Secure Socket Layer	安全套接层

SSN	Social Security Number	社保号
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全
UAC	User Access Control	用户访问控制
UI	User Interface	用户接口
UNC	Universal Naming Convention	通用命名规则
UPN	Universal Principal Name	通用主体名称
UPS	Uninterruptable Power Supply	不间断电源
USB	Universal Serial Bus	通用串行总线
US-CERT	United States Computer Emergency Readiness Team	美国计算机应急响应小组
VHD	Virtual Hard Drive	虚拟硬盘
VHDX	Hyper-V virtual hard disk	Hyper-V 虚拟硬盘
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网络
WAN	Wide Area Network	广域网
WMI	Windows Management Instrumentation	Windows 管理规范
XML	eXtensible Markup Language	可扩展标记语言

附录 B 词汇表

本附录列出了文中出现的部分术语的定义。

业务/任务目标 – 泛指业务目标，即对业务运营设置的目标结果。

产能规划 – 系统性地确定特定时间段内达到预计产量所需的资源。【businessdictionary.com】

大类 – 对功能的细分，体现为一个个的网络安全结果组，与计划性需求和特定活动密切相关。

关键基础设施 – 支撑美国社会的基础服务和相关资产，是国家经济、安全和健康的支柱。【DHS】

重要性评审 – 确定制造系统组件、服务、过程和输入的等级和优先级，以设置操作阈值和恢复目标。

关键服务 – 开展制造业务所需的基本服务的子集，是维持受控设备的健康、安全、环境和可用性的必要功能或能力。【62443】

网络风险 – 通过非法访问、使用、披露、中断、修改或破坏制造系统，用电子手段对制造系统中的信息和/或操作功能所使用的数字技术造成故障而引起的财务损失、运营中断或损害风险。

网络安全 – 通过预防、检测和响应攻击来保护信息的过程。【CSF】

纵深防御 – 分层或分步应用多种对抗措施来实现安全目标。该方法包括在常见攻击向量中分层构筑异构安全技术，这样，攻击在被某种技术漏防时会被另一种技术防住。【62443 1-1】

事件 – 制造系统中检测出的任何事件，包括可能会影响组织运营（包括使命、能力或信誉）的网络安全变化。【CSF】

固件 – 写入硬件设备闪存的软件程序或指令集，提供了设备与其他计算机硬件通信的必要指令。【Techterms.com】

框架 – 为保护关键基础设施而制定的网络安全框架，它提供了通用语言，方便组织内外理解、管理、描述网络安全风险，定义了活动，以实现特定的网络安全结果，并引用了一些指南，为实现这些结果提供指导。

功能 – 网络安全框架内的主要组成部分，描述最基本的网络安全活动。

安全事件 – 实际或潜在影响信息系统的、系统所处理、存储或传输的信息的机密性、完整性或可用性的事件，或违反或有可能违反安全政策、安全程序或可接受使用策略的事件。【CSF】

集成商 – 专注于工业控制和信息系统、制造实施系统和工厂自动化的增值工程组织，具有应用知识和技术专长，提供工程问题的集成解决方案。该方案包括最终项目工程、文档管理、硬件采购、定制软件开发、安装、测试和调试。【CSIA.com】

制造业务 – 与制造企业的设施运营、系统过程、材料输入/输出、维护、供应分配、健康安全、应急响应、人力资源、安全、信息技术等措施相关的活动。

网络访问 – 通过网络连接代替本地访问（用户直接接触设备）的任何访问。

运营技术 – 通过直接监视和/或控制企业的物理设备、过程和事件来检测或引起变化的硬件和软件。【Gartner.com】

可编程逻辑控制器 – 一种固态控制系统，具有用户可编程存储器，用于存储指令，以实现特定功能，如I/O控制、逻辑、定时、计数、三模（PID）控制、通信、算术、数据和文件处理。【800-82】

Profile – 特定系统或组织从框架大类和子类中选择的结果。【CSF】

目标Profile – 网络安全实施的目标结果或“未来”状态

当前Profile – 系统网络安全的“当前”状态

协议 – 用于实现和控制系统之间联系（如通信）的一组规则（格式和过程）。【800-82】

远程访问 – 用户（或信息系统）在信息系统安全边界外与系统进行通信。网络访问指通过网络连接代替本地访问（用户直接接触设备）的任何访问。【800-53】

恢复性要求 – 制造系统的可用性和可靠性特征，由业务驱动，明确了对中断和重大安全事件的恢复能力要求。

风险评估 – 通过确定发生概率、产生影响以及减轻这种影响的附加安全控制措施，识别机构运作（包括任务、职能、形象、声誉等）、机构资产或个人所面临风险的过程。风险评估属于风险管理，与风险分析同义，包含威胁和漏洞分析。【800-82】

风险承受能力 – 制造商在实现战略目标时愿意接受的风险水平。【800-53】

路由器 – 在OSI 3层的两个网络之间充当网关、转发数据包的计算机，路由器一般基于IP数据包运行。【800-82】

安全控制 – 针对系统制定的有关管理、运营和技术方面的控制措施（如防护措施或对策），以保护系统及其组件、进程和数据的保密性、完整性和可用性。【800-82】

子类 – 由大类细分成的具体技术及/或管理活动的结果，如“对外部信息系统进行了编目”、“对静态数据进行了保护”及“调查了检测系统发出的通知”。【CSF】

配套服务 – 通过各种消费者-生产者关系向制造商提供外部系统服务的供应商，这种关系包括但不限于 合资企业、商业伙伴关系、外包安排（通过合同、跨机构协议、业务线安排）、许可协议和/或供应链交换。配套服务包括电信、工程服务、电力、水、软件、技术支持和安全等。【800-53】

交**换机** – 一种设备，从多个输入端口选取一个端口，将其输入数据引导到特定的输出端口，再将数据转发至预期目的地址。【Whatis.com】

系统分类 – 评估可用性、完整性或机密性破坏后对组织运作、组织资产或个人的潜在影响，基于该评估，对制造系统及其组件和运营进行分类。【FIPS 199】

第三方关系 – 与外部实体的关系。外部实体包括服务提供商、厂商、供应方合作伙伴、需求方合作伙伴、联盟、企业集团和投资者，与这些实体的关系可能有合同约束，也可能没有。【国土安全部】

第三方提供商 – 制造系统运营组织的外部服务提供商、集成商、厂商、电信和基础设施支持。

阈值 – 用于确定具体决策点和运营控制限制的值，到达该阈值后会触发管理活动和响应升级。

附录 C 参考资料

1. 第13636号行政命令，提升键基础设施的网络安全，DCPD-201300091，20013年2月12日.
   https://www.govinfo.gov/app/details/FR-2013-02- 19/2013-03915

2. 国家标准与技术研究院（2014），提升关键基础设施网络安全框架，1.0版. （国家标准与技术研究院，马里兰州盖瑟斯堡），2014年2月12日. https://doi.org/10.6028/NIST.CSWP.02122014

3. Stouffer KA，Lightman S，Pillitteri VY，Abrams M，Hahn A（2015），工业控制系统（ICS）安全指南. （国家标准与技术研究院，马里兰州盖瑟斯堡），NIST特刊（SP）800-82，第二版. https://doi.org/10.6028/NIST.SP.800-82r2

4. Stouffer K，Zimmerman T，Tang CY，Lubell J，Cichonski J，McCarthy J（2019）网络安全框架制造篇. （国家标准与技术研究院，马里兰州盖瑟斯堡），NIST内部报告（NISTIR）8183，包含截至2019年5月20日的更新. https://doi.org/10.6028/NIST.IR.8183

小蜜蜂翻译公益译文项目，旨在分享国外先进网络安全理念、规划、框架、技术标准与实践，将网络安全战略性文档翻译为中文，为网络安全从业人员提供参考，促进国内安全组织在相关方面的思考和交流。

“安全加”社区

小蜜蜂公益翻译组