云计算与虚拟化技术

第11章：Data Center Management

https://internet.hactcm.edu.cn

河南中医药大学信息技术学院（智能医疗行业学院）智能医疗教研室
河南中医药大学医疗健康信息工程技术研究所

2025年2月

讨论提纲

- **系统配置**
  - 配置 VM
  - 配置 ESXi Host
  - 配置 vCenter Server
- **升级维护**
  - vSphere 升级管理
  - VUM
  - vCSA 升级
- **安全管理**
  - vSphere 安全体系
  - 安全加固

1. 系统配置

vSphere 配置对象与配置方式

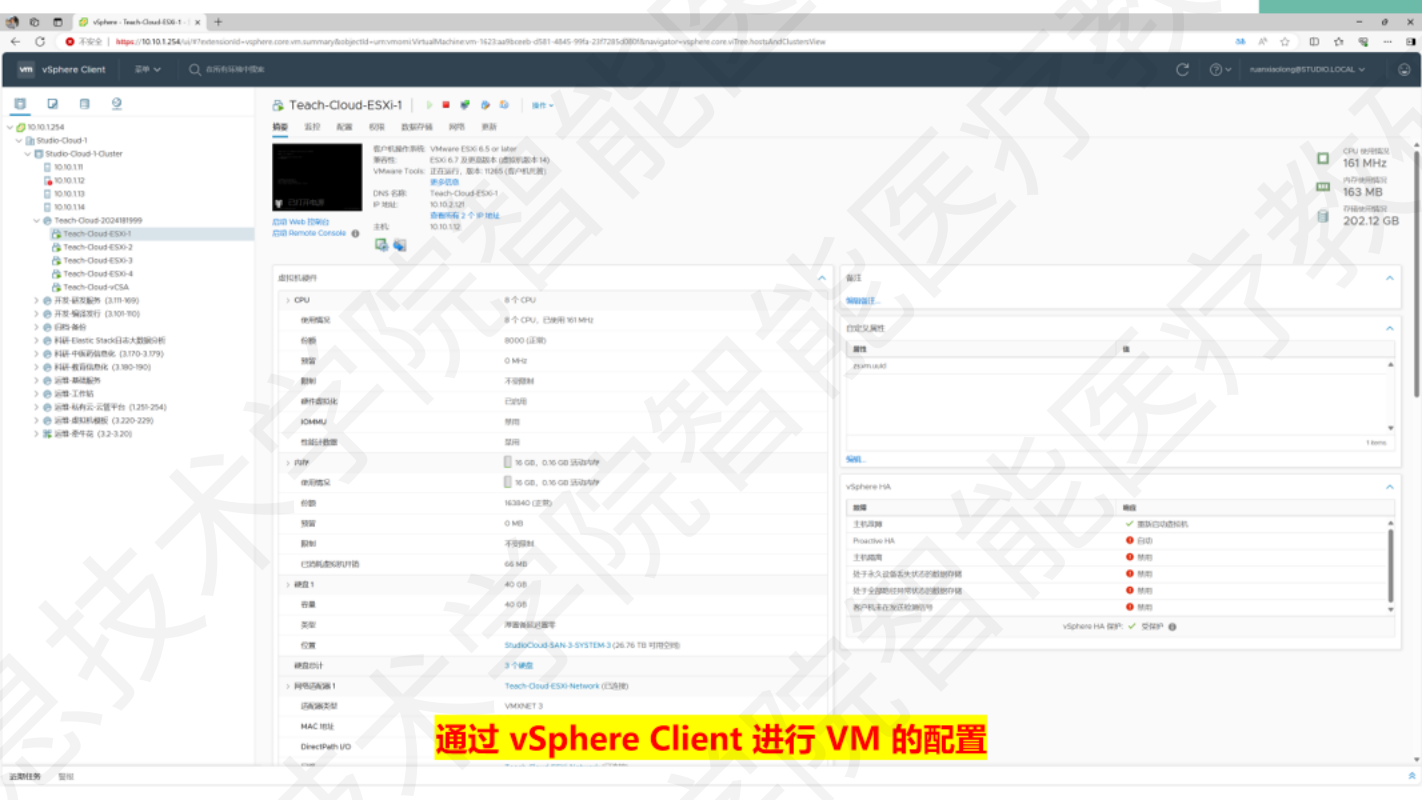
1. 系统配置

vSphere 配置对象与配置方式

VM	ESXi Host	vCenter Server
vSphere Host Client vSphere Client	vSphere Host Client vSphere Client ESXi DCUI ESXCLI	vSphere Client VMware Appliance Management Administration (VAMI)

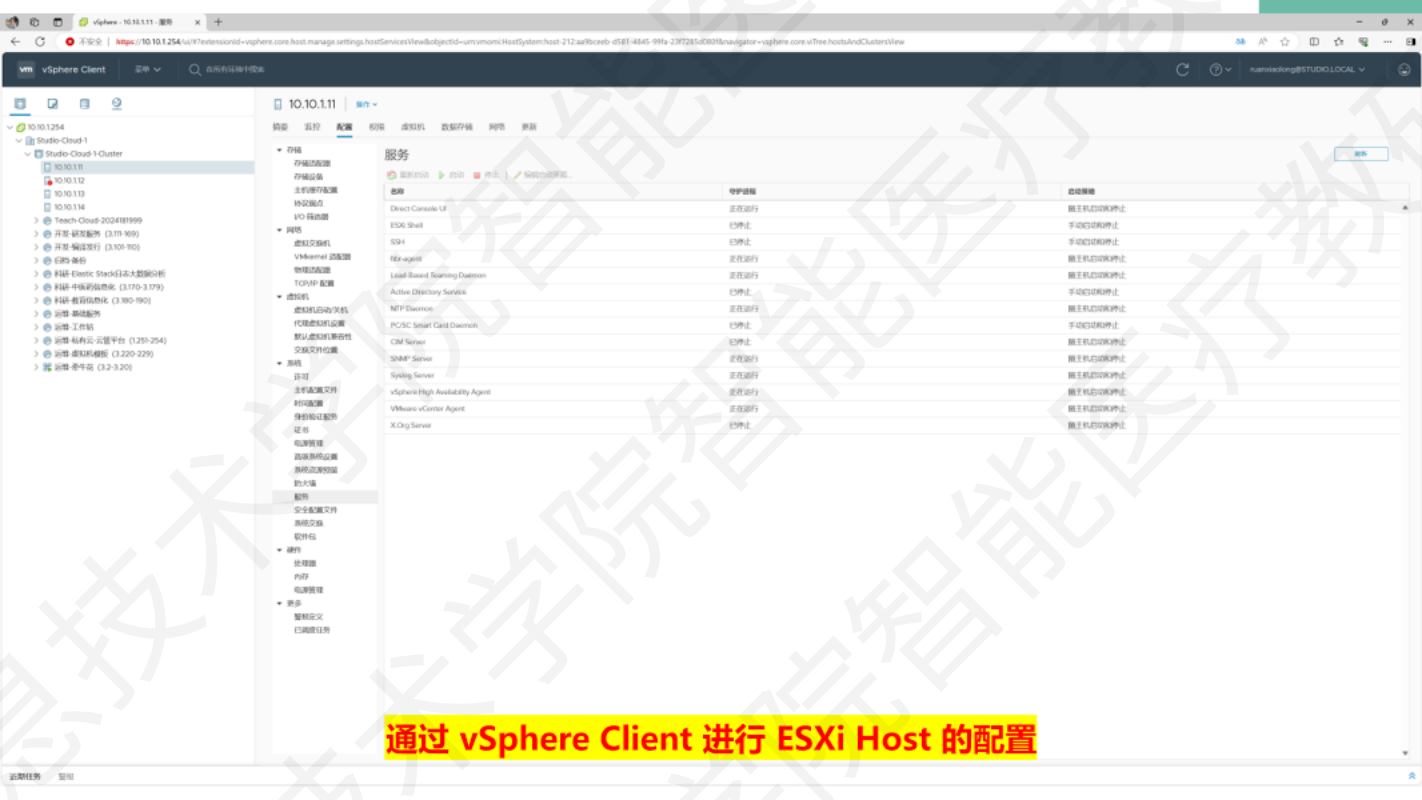
1. 系统配置

- 对 VM 的配置主要有三类。
  - 对 VM 的硬件资源配置
    - 例如：CPU、内存、网络、存储、磁盘等，以及虚拟机的版本与兼容性等配置。
  - 对 VM 的操作应用配置
    - 例如：操作系统启动选项、虚拟机安全等配置。
  - 对 VM 的管理维护配置
    - 例如：虚拟机名称与描述、电源、备份与恢复策略、迁移设置、资源使用等配置。


vSphere Client
Teach-Cloud-ESXi-1
通过 vSphere Client 进行 VM 的配置

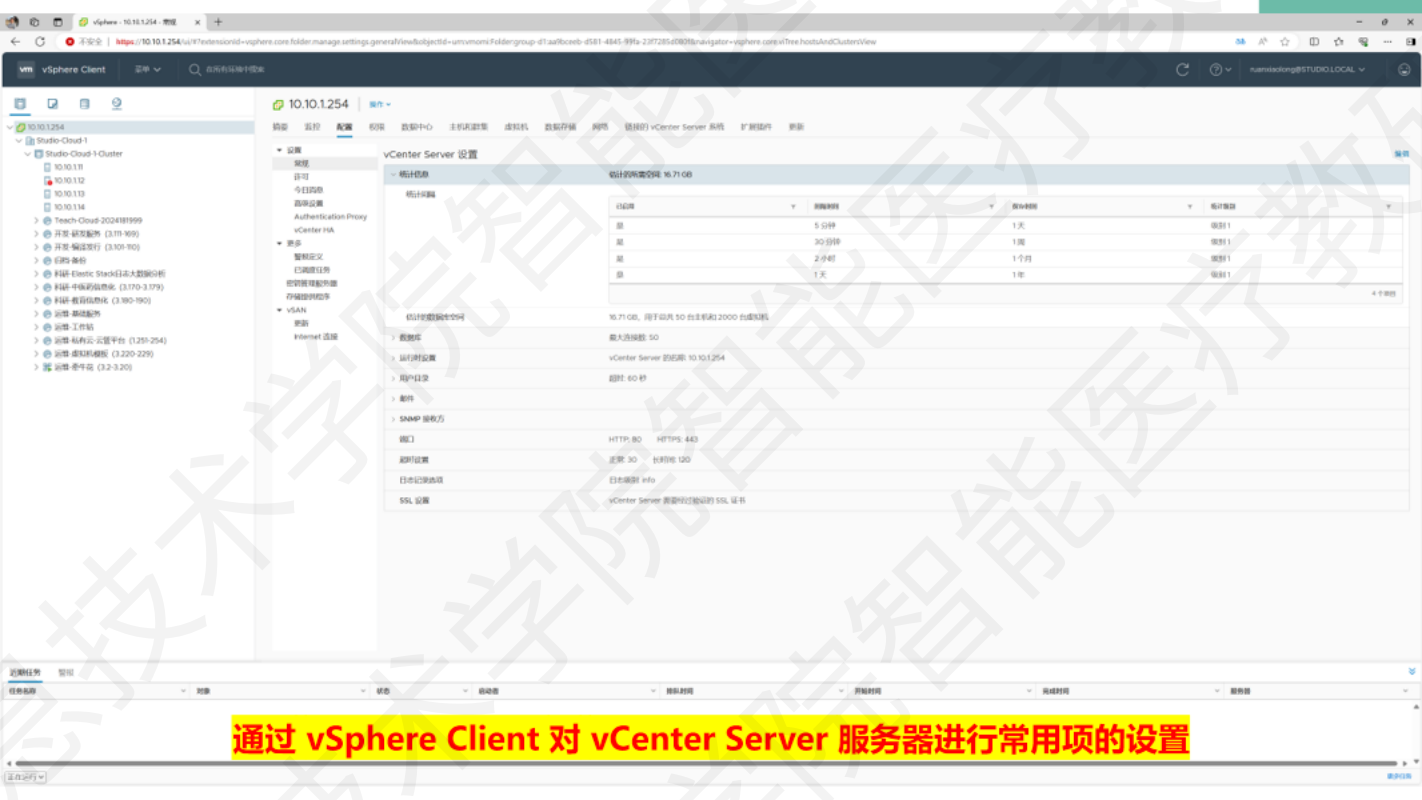
1. 系统配置

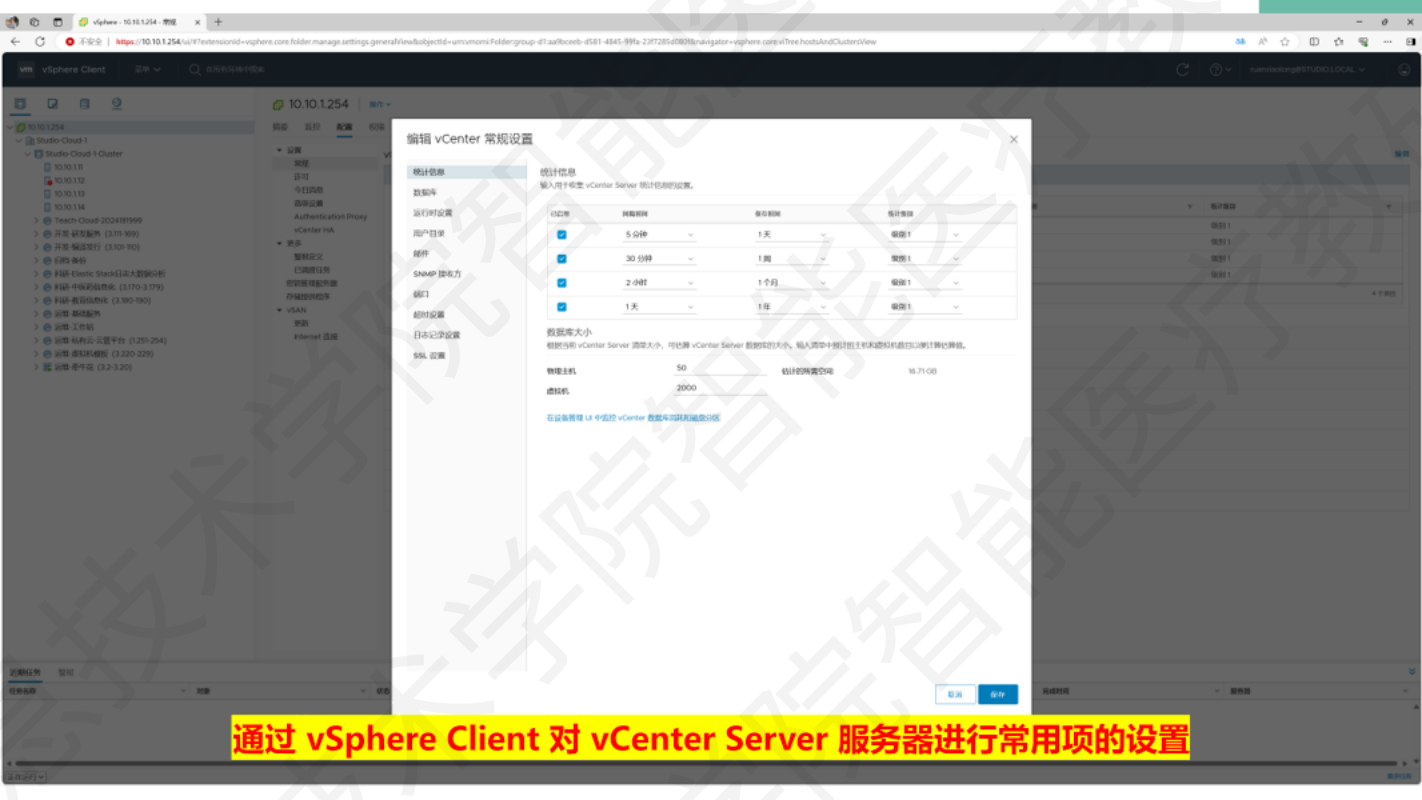
- 对 ESXi Host 的配置主要是四类：
  - 对 ESXi Host 的系统配置
    - 例如：系统信息（主机名、域名、时间同步设置等）、管理网络等配置。
  - 对 ESXi Host 的硬件配置
    - 例如：CPU、内存、电源管理等配置。
  - 对 ESXi Host 的服务配置
    - 例如：进程服务、存储、网络、虚拟机、系统资源预留等配置
  - 对 ESXi Host 的安全配置
    - 例如：身份验证服务、防火墙、安全配置文件等配置。

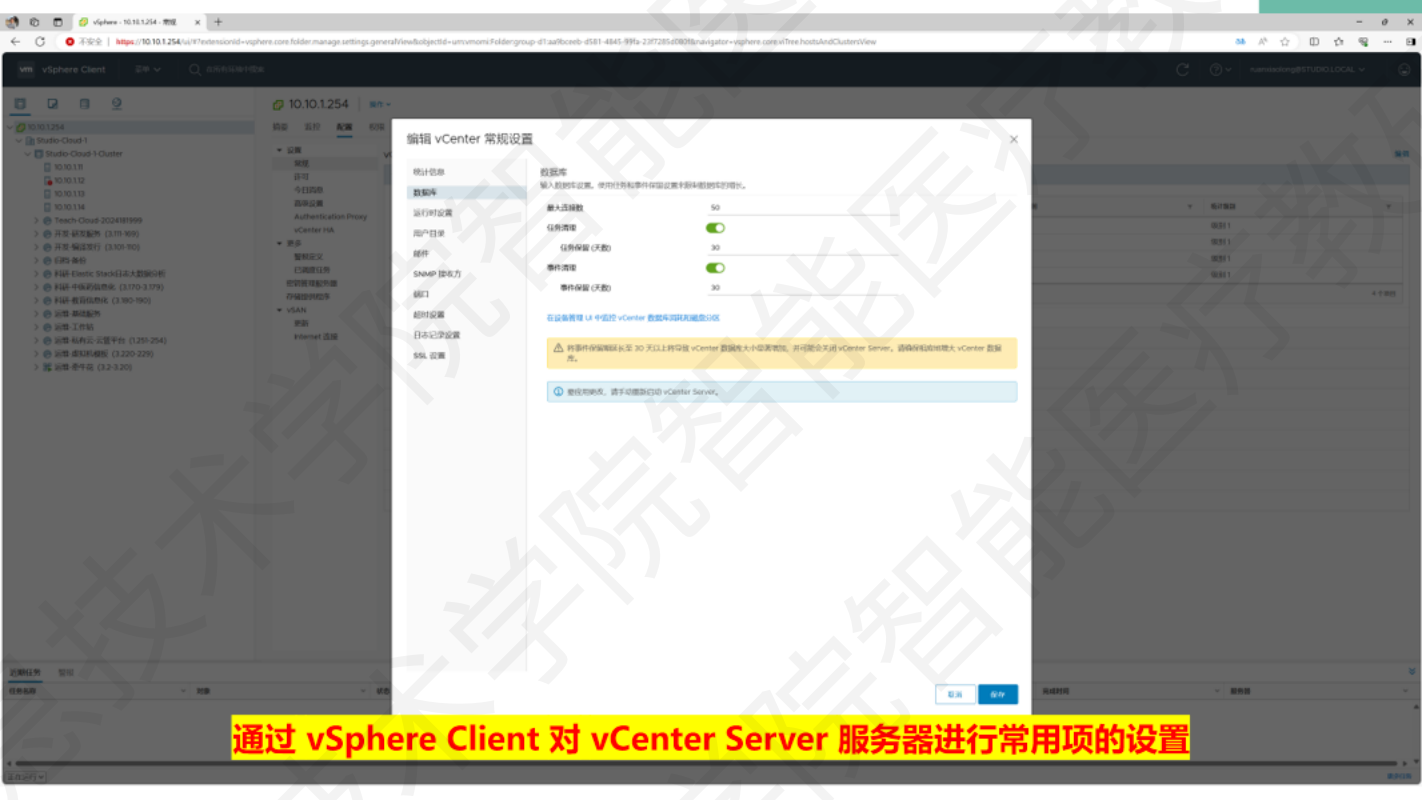

vSphere Client
10.10.1.11
服务
通过 vSphere Client 进行 ESXi Host 的配置

1. 系统配置

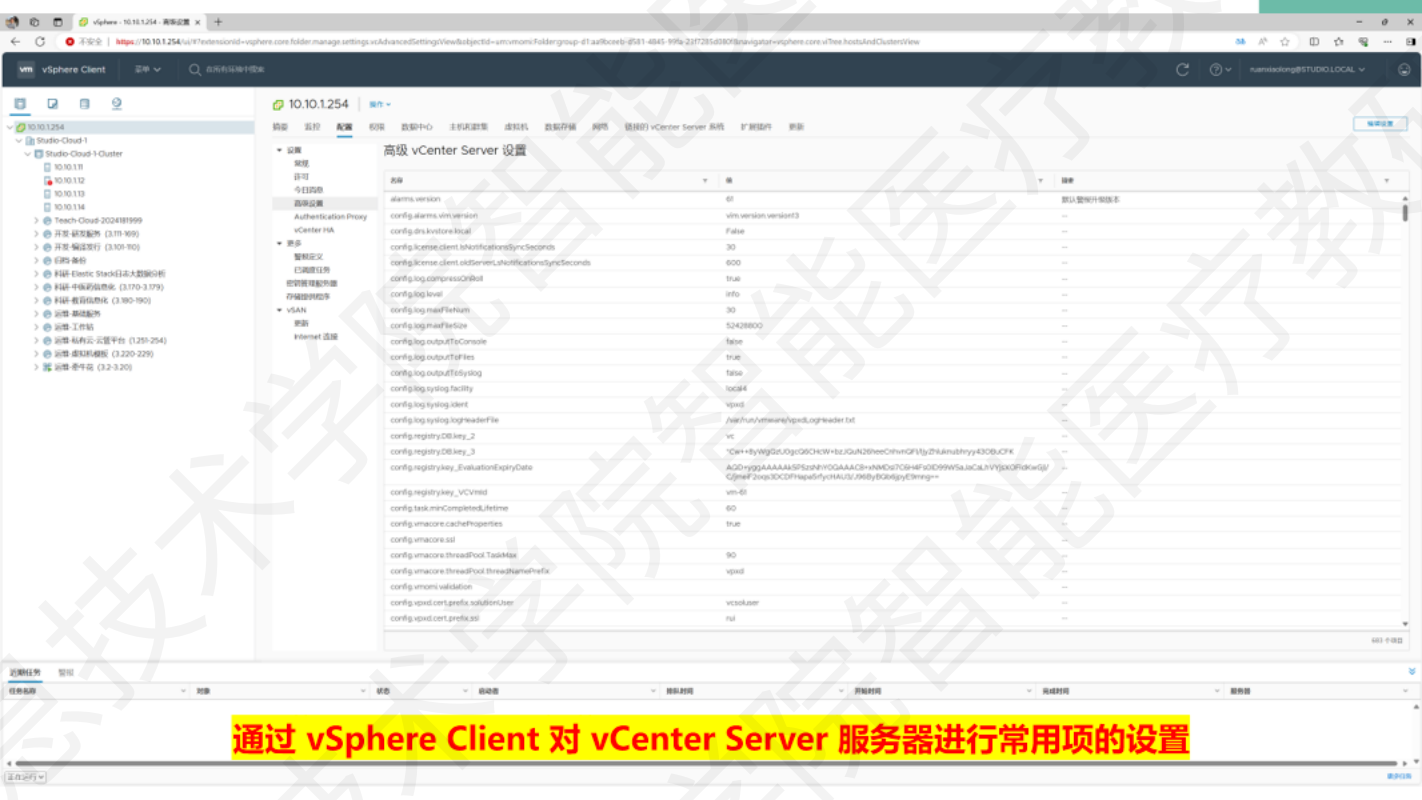
- 对 vCenter Server 的配置有三个主要内容。
  - 通过 vSphere Client 对 vCenter Server 服务器进行常用项的设置。
    - 在 vSphere Client 中选择 vCenter Server 时，可在“配置”选项卡上查看到“设置”。
    - 可以配置的项目有：
      - 常规：
        - 统计信息、数据库、运行时 设置、用户目录、邮件、SNMP 接收方、端口
        - 超时设置、日志记录选项、SSL 设置
      - 许可：许可证信息
      - 今日消息
      - 高级设置：vCenter Server 的所有配置项
      - Authentication Proxy：身份验证代理是为自动化运维设置账号
      - vCenter HA：设置 VCSA 的高可用。


vSphere Client
10.10.1.254
vCenter Server 设置
通过 vSphere Client 对 vCenter Server 服务器进行常用项的设置


编辑 vCenter 常规设置
统计信息
数据库
运行时设置
用户目录
邮件
SNMP 接收方
端口
超时设置
日志记录设置
SSL 设置
统计信息
输入用于收集 vCenter Server 统计信息的设置。
间隔时间
保存期限
统计级别
5 分钟
1 天
级别 1
30 分钟
1 周
级别 1
2 小时
1 个月
级别 1
1 天
1 年
级别 1
数据库大小
物理主机
50
虚拟机
2000
估计的所需空间
16.71 GB
取消
保存
通过 vSphere Client 对 vCenter Server 服务器进行常用项的设置



通过 vSphere Client 对 vCenter Server 服务器进行常用项的设置


vSphere Client
10.10.1.254
高级 vCenter Server 设置
通过 vSphere Client 对 vCenter Server 服务器进行常用项的设置

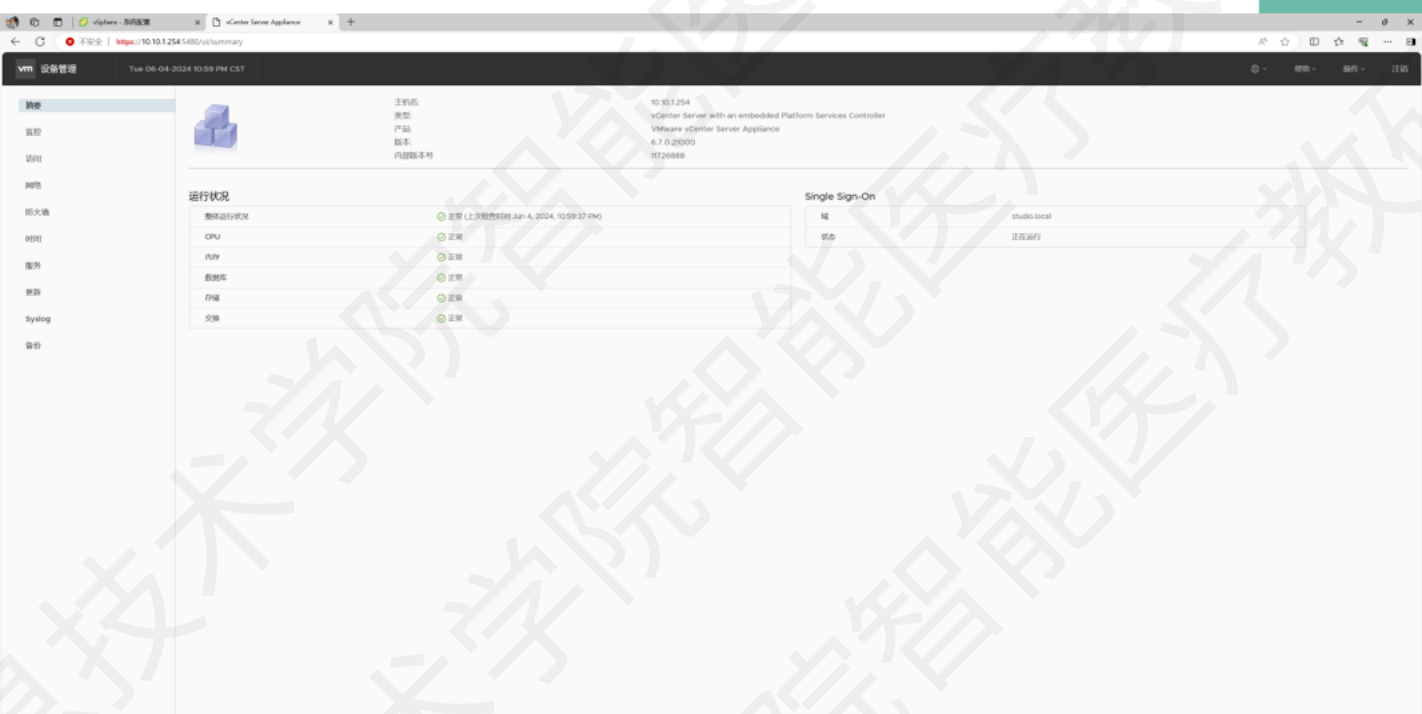
1. 系统配置

- 对 vCenter Server 的配置有三个主要内容。
  - 通过 vSphere Client 进行系统管理。
    - 在 vSphere Client 的“菜单”中，选择“系统配置”进行常用管理。
    - 该管理与 VAMI 的管理有一些重叠，但集成到 vSphere Client 中会更方便使用。
    - 系统配置的内容有：
      - 访问控制：包含角色、全局权限。
      - 许可：vSphere 的许可证管理。
      - 解决方案：包含客户端插件、vCenter Server 扩展的集中管理。
      - 部署：包含系统配置，可以导出 vCenter Server 支持包，以及重启 vCenter Server 操作。
      - 支持：将服务的详细信息提交给 VMware 官方。
      - SSO：配置用户、用户组等。
      - 证书：启用第三方证书管理。

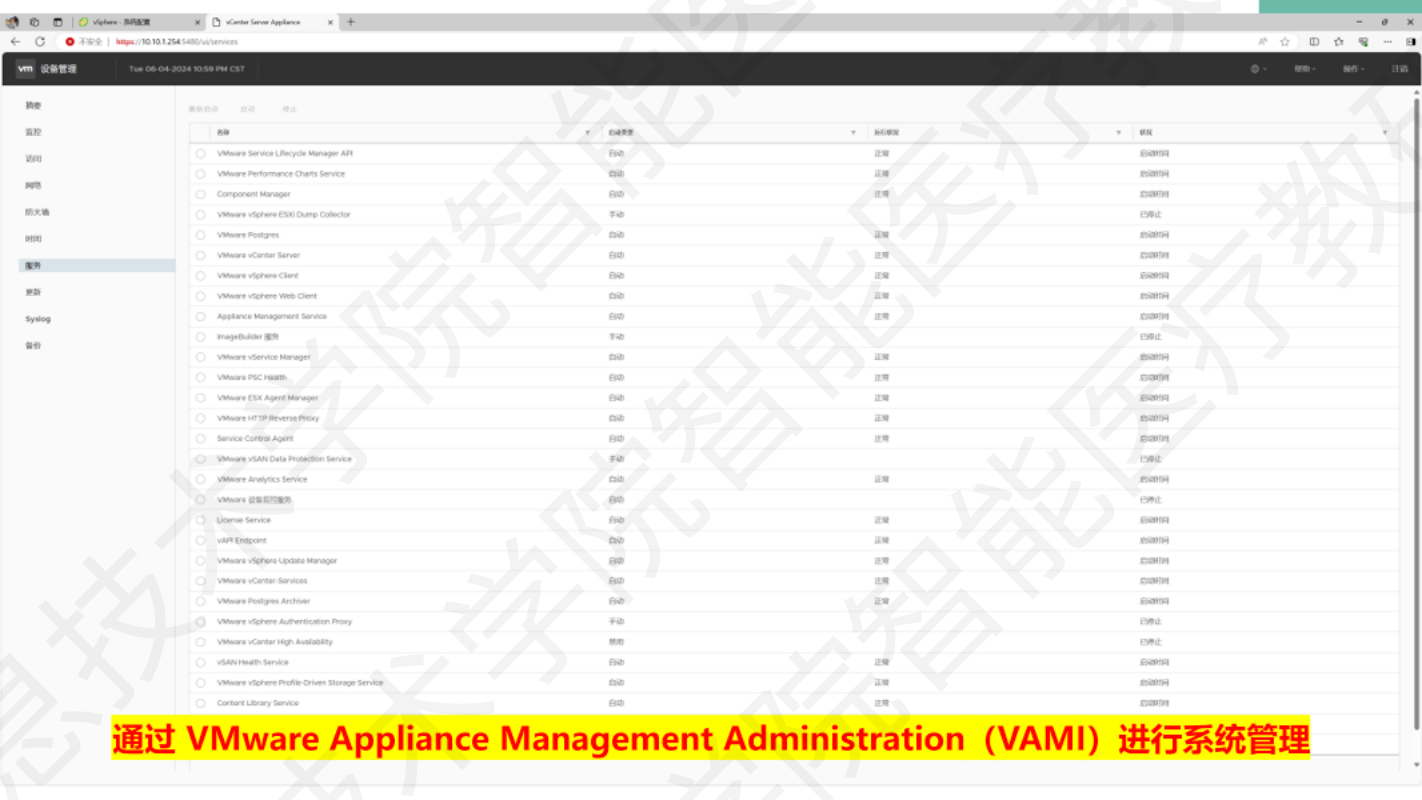

vSphere Client
系统配置
通过 vSphere Client 进行系统管理

1. 系统配置

- 对 vCenter Server 的配置有三个主要内容。
  - 通过 VMware Appliance Management Administration（VAMI）进行系统管理。
    - VAMI 是 VMware 产品的通用管理系统，相当于基于 Web 的操作系统管理界面。
      - 可以不恰当的理解为：为 Linux 服务器安装的 Cockpit。
      - 访问地址是：https://<server.domain.com>:5480
    - 通过 VAMI 可以进行的配置有：
      - 摘要：显示系统的运行状况。
      - 监控：vCenter Server 服务器的运行情况。
      - 访问：vCenter Server 访问设置。
      - 网络：网络基本配置，主机的网络设置。
      - 防火墙：防火墙策略。
      - 时间：时区、时间同步的设置。
      - 服务：vCenter Server 的服务配置。
      - 更新：vCenter Server 的升级。
      - Syslog：日志转发，支持转发到3台服务器。
      - 备份：vCenter Server 的配置信息的备份。
    - 通过 VAMI 的“操作”菜单可以重启和关机操作。



通过 VMware Appliance Management Administration（VAMI）进行系统管理



通过 VMware Appliance Management Administration（VAMI）进行系统管理

1. 系统配置

对 VM、ESXi Host、vCenter Server 进行配置
讨论各配置项目的内涵，总结 vSphere 配置功能的规律

2. 升级维护

vSphere 升级、修补、更新和迁移之间的差异

版本升级

对软件进行重大更改
新功能，性能与安全增强
vSphere 6.7 -> 7.0

修补更新

对软件进行较小更改
修复已知的问题和漏洞
vSphere 6.7 U2 -> U3

平台迁移

对软件平台进行更改
如 Windows vCenter Server 转换为VCSA

2. 升级维护

vSphere 升级、修补、更新和迁移之间的差异

版本升级

对软件进行重大更改
新功能，性能与安全增强
vSphere 6.7 -> 7.0

Upgrades

修补更新

对软件进行较小更改
修复已知的问题和漏洞
vSphere 6.7 U2 -> U3

Patches, Updates

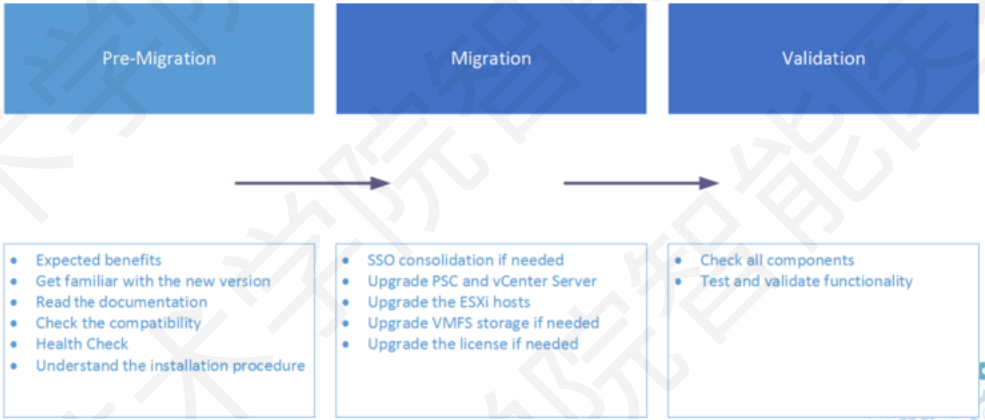
平台迁移

对软件平台进行更改
如 Windows vCenter Server 转换为VCSA

Migrations

2. 升级维护

- 为了成功迁移到新版本，必须精准设计工作流，并按照流程执行。
  - 避免潜在的问题，如服务中断或运行组件的兼容性问题。
- 迁移过程计划可分为三个主要步骤：



2. 升级维护

- 为了成功迁移到新版本，必须精准设计工作流，并按照流程执行。
  - 避免潜在的问题，如服务中断或运行组件的兼容性问题。
- 迁移过程计划可分为三个主要步骤：

2. 升级维护

- 为了成功迁移到新版本，必须精准设计工作流，并按照流程执行。
  - 避免潜在的问题，如服务中断或运行组件的兼容性问题。
- 迁移过程计划可分为三个主要步骤：

2. 升级维护

- 为了成功迁移到新版本，必须精准设计工作流，并按照流程执行。
  - 避免潜在的问题，如服务中断或运行组件的兼容性问题。
- 迁移过程计划可分为三个主要步骤：

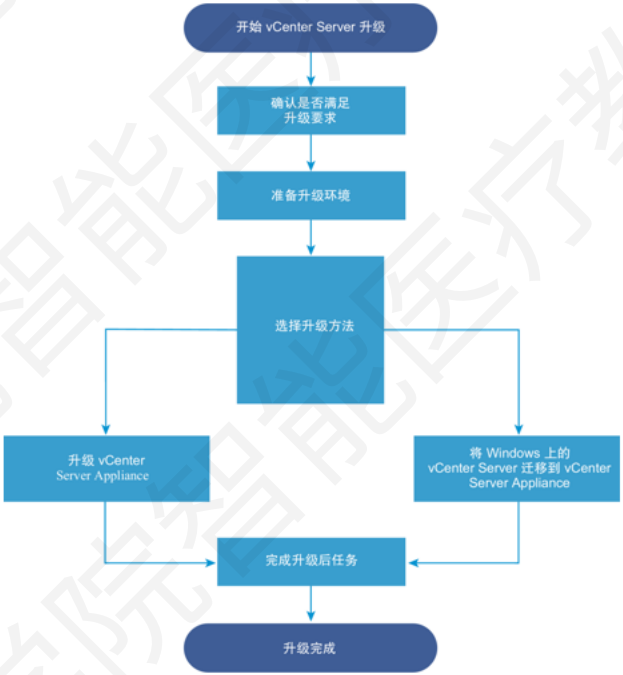
能不迁移不迁移、先做备份后迁移、反复演练再迁移

2. 升级维护

- vSphere 是一款复杂的软件，版本升级涉及多个组件需要升级。
  - vSphere 升级任务
    - 第1步：阅读 vSphere 发行说明。
    - 第2步：验证是否已备份配置。
    - 第3步：如果 vSphere 系统包括 VMware 解决方案或插件，验证是否与要升级到的 vCenter Server Appliance 版本兼容。
    - 第4步：升级 vCenter Server。
    - 第5步：要确保有足够的磁盘存储来存储日志文件，优先用远程 syslog 服务器。
    - 第6步：通过手动或使用 vSphere Lifecycle Manager 升级虚拟机。
  - vSphere 每个版本都提供明确的升级指南，务必依据指南制定升级方案。
    - 升级的本质，就是迁移，非不要不做版本升级。

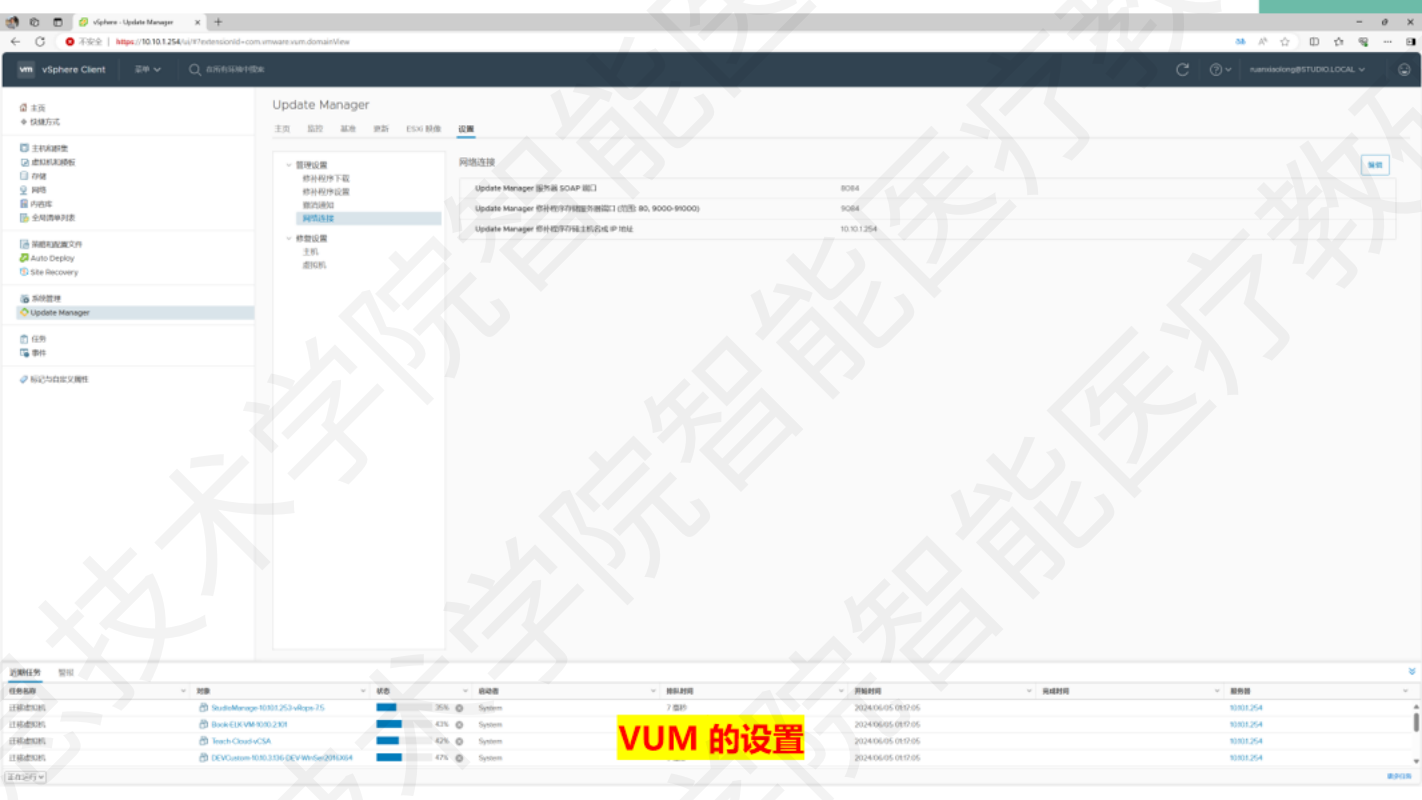
vSphere 升级任务

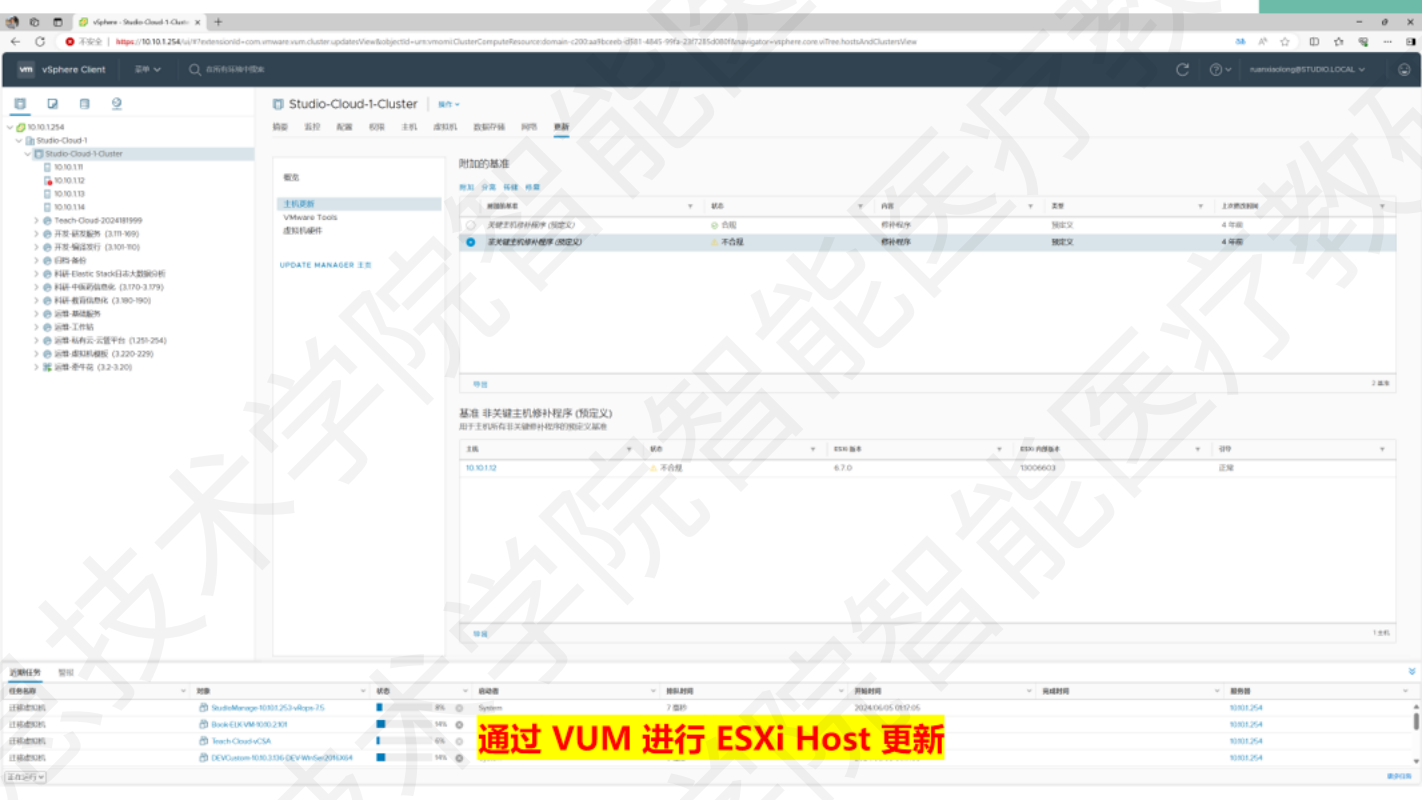
vCenter Server 升级任务

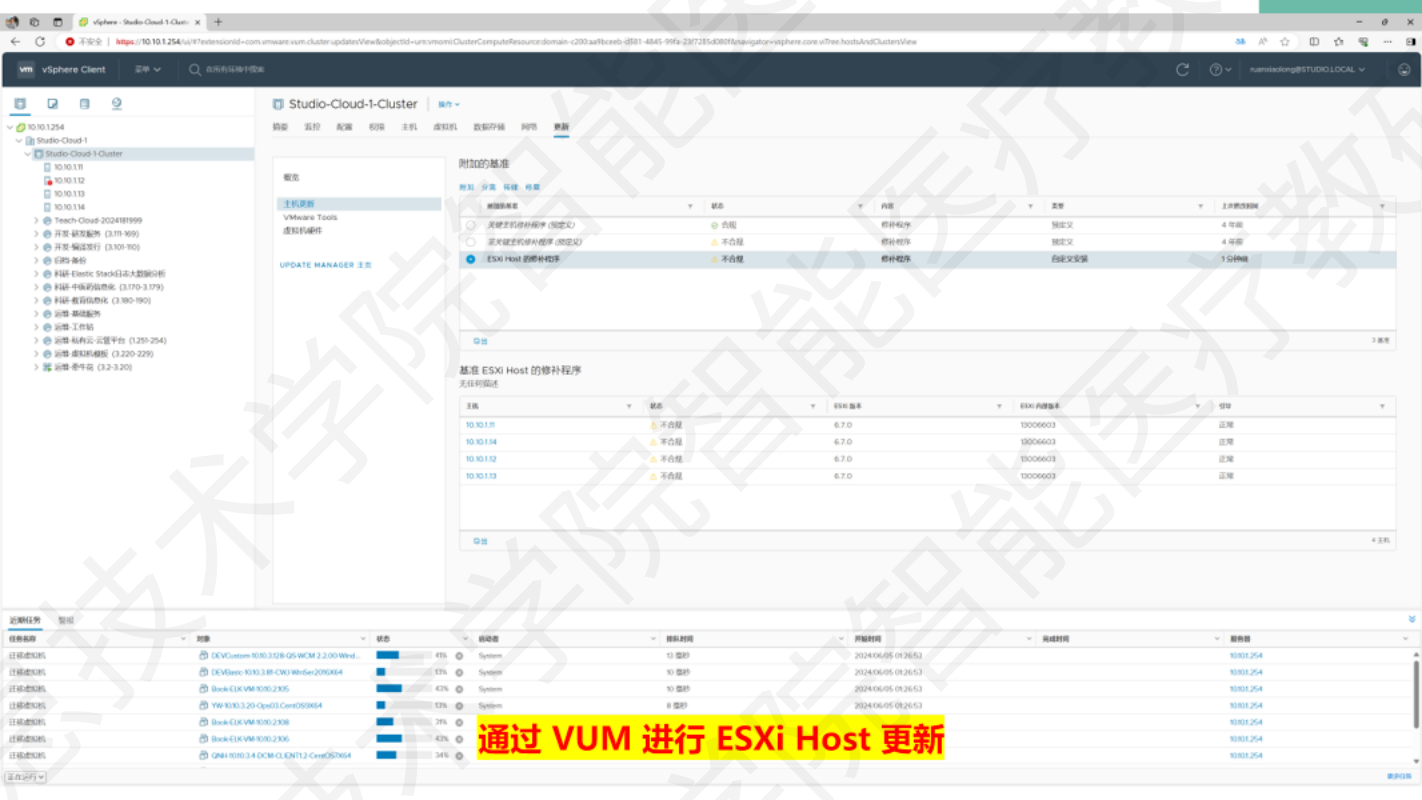


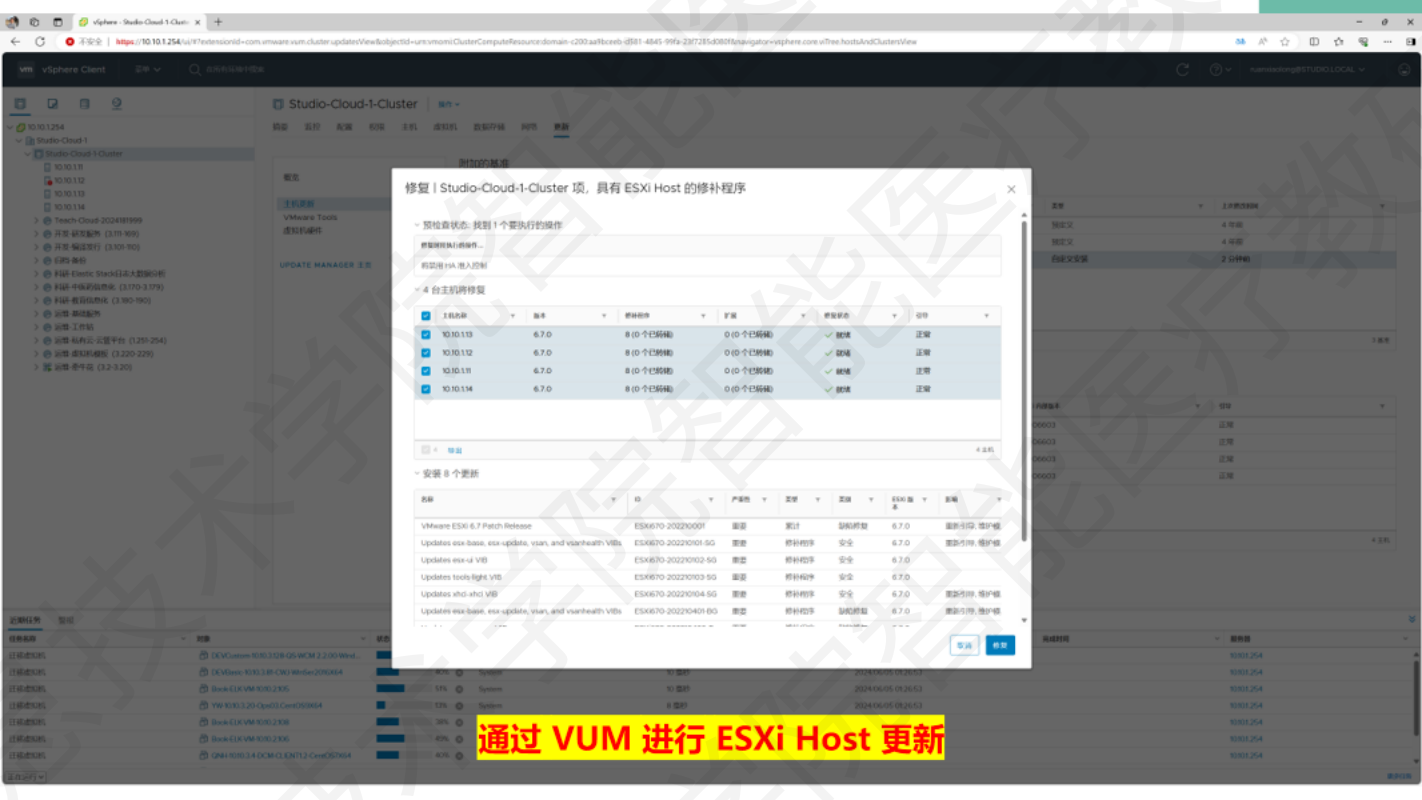
2. 升级维护

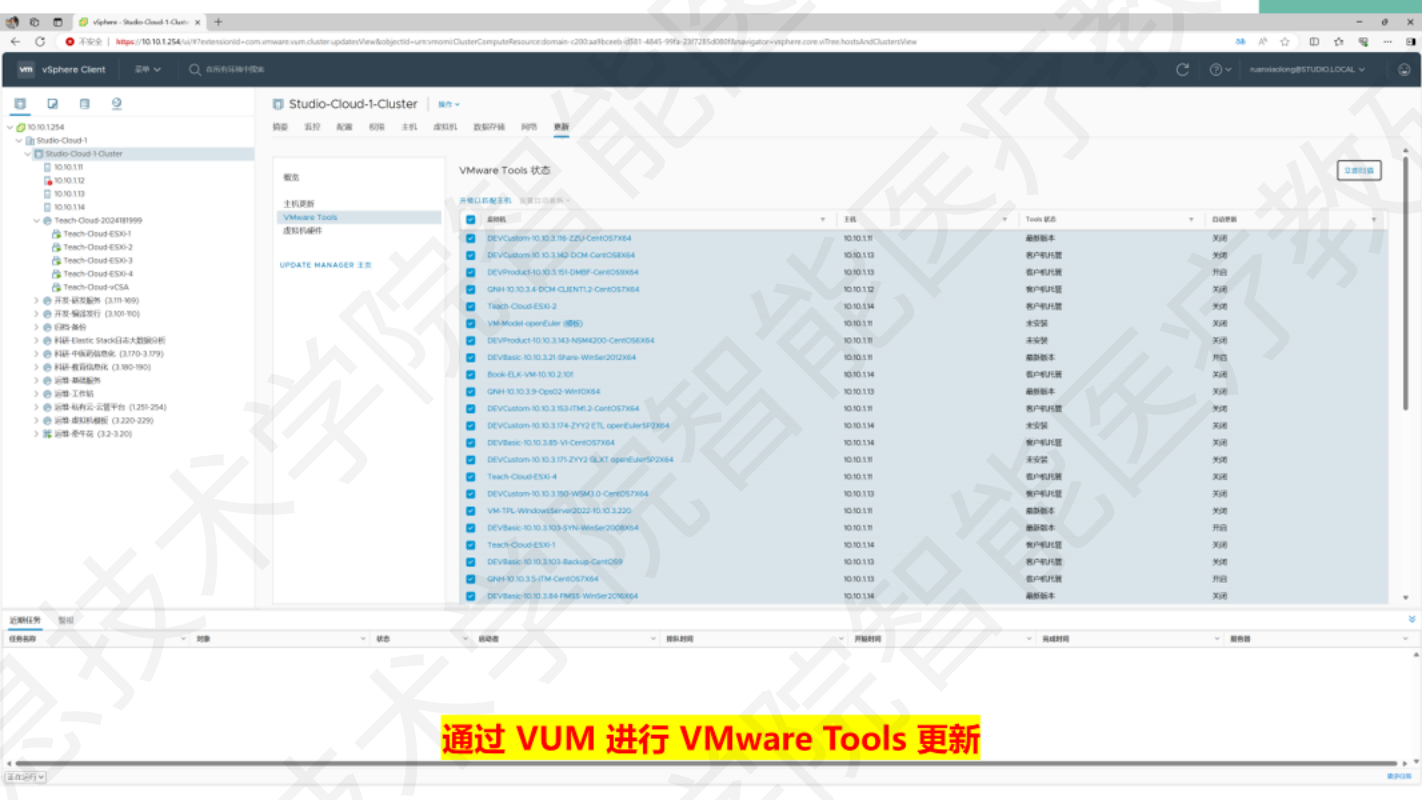
- vSphere Update Manager，VUM
  - VUM 是一个工具，能够有效地管理在虚拟环境中安装的 VM、ESXi Host 和 vAPP 的补丁和更新。
  - VUM 是 vCSA 的一个组件，默认是启用的。
  - 使用 VUM 可以：
    - 升级和修补 ESXi Host。
    - 在 ESXi Host 上安装和更新第三方软件。
    - 升级 VM 硬件。
    - 升级 VM 的 VMware Tools。

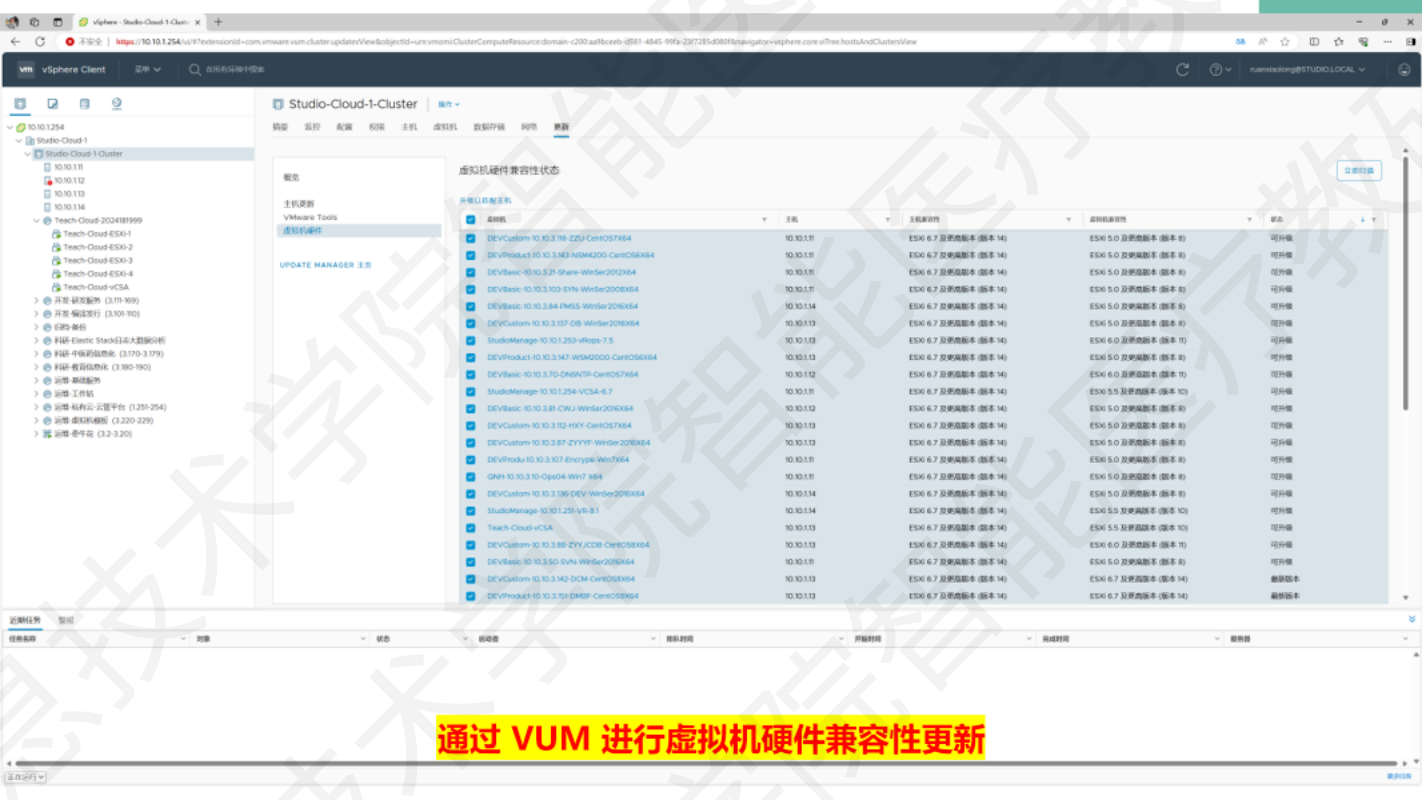

vSphere - Update Manager
不安全 | https://10.10.1.254/ui/#?extensionId=com.vmware.vum.domainView
vSphere Client
菜单
在所有环境中搜索
ruanxiaolong@STUDIO.LOCAL
主页
快捷方式
主机和群集
虚拟机和模板
存储
网络
内容库
全局清单列表
策略和配置文件
Auto Deploy
Site Recovery
系统管理
Update Manager
任务
事件
标记与自定义属性
Update Manager
主页
监控
基准
更新
ESXi 映像
设置
管理设置
修补程序下载
修补程序设置
警告通知
网络连接
修复设置
主机
虚拟机
网络连接
编辑
Update Manager 服务器 SOAP 端口
8084
Update Manager 修补程序存储服务器端口 (范围: 80, 9000-91000)
9084
Update Manager 修补程序存储主机名或 IP 地址
10.10.1.254
近期任务
警报
任务名称
对象
状态
启动者
排队时间
开始时间
完成时间
服务器
迁移虚拟机
StudioManager-10.10.1.253-vRops-7.5
35%
System
7 毫秒
2024/06/05 01:17:05
10.10.1.254
迁移虚拟机
Book-ELK-VM-10.10.2.101
43%
System
2024/06/05 01:17:05
10.10.1.254
迁移虚拟机
Teach-Cloud-vCSA
42%
System
2024/06/05 01:17:05
10.10.1.254
迁移虚拟机
DEVCustom-10.10.3.136-DEVWinSer2019X64
47%
System
2024/06/05 01:17:05
10.10.1.254
正在运行
VUM 的设置


vSphere - Studio-Cloud-1-Cluster
vSphere Client
Studio-Cloud-1-Cluster
通过 VUM 进行 ESXi Host 更新


vSphere Client
Studio-Cloud-1-Cluster
通过 VUM 进行 ESXi Host 更新


修复 | Studio-Cloud-1-Cluster 项，具有 ESXi Host 的修补程序
预检查状态：找到 1 个要执行的操作
4 台主机将修复
安装 8 个更新
通过 VUM 进行 ESXi Host 更新


vSphere Client
Studio-Cloud-1-Cluster
VMware Tools 状态
通过 VUM 进行 VMware Tools 更新


vSphere Client
Studio-Cloud-1-Cluster
通过 VUM 进行虚拟机硬件兼容性更新

2. 升级维护

使用 VUM：配置基准、扫描、升级

2. 升级维护

- VCSA 的更新升级有两种方法。
  - 使用 VAMI
    - 推荐此方案
  - 通过命令行
    - 通过 VMware 网站下载 ISO 格式的 vCenter Server 更新程序。
    - 将 ISO 挂载到 VCSA 服务器上。
    - 通过命令行管理 VCSA，并执行升级。

通过 VAMI 进行 vCenter Server 更新

3. 安全管理

- 安全是一个完整流程，涵盖整个生命周期，确保全面保护。
- vSphere 安全保护的对象：
  - ESXi Host
  - vCenter Server
  - virtual machines (VM)
  - The Applications running in the VM
- vSphere 安全保护的建议（AAA安全认证）：
  - 认证：Authentication
    - 对用户的身份进行验证，判断其是否为合法用户。
  - 授权：Authorization
    - 对通过认证的用户，授权其可以使用哪些服务。
  - 审计：Accounting
    - 记录用户使用网络服务的资源情况，这些信息将作为审计的依据。

3. 安全管理

- 在确保信息安全方面，VMware 采取一系列策略来强化其安全架构。
  - 权限最小化原则：Least Privilege
    - 核心原则，适用于所有用户账户、服务账户以及服务操作。
    - 仅授予完成特定任务所需的最低权限，降低潜在的安全风险。
  - 微分段：Micro-segmentation
    - 通过 NSX 技术，能够在虚拟机层面实现网络控制的精细化管理。
    - 结合 VMware AppDefense，在网络和应用层面提供更严格的虚拟机安全保障。
  - 数据加密：Encryption
    - 为了在不同层面上保护数据安全，加密技术是关键，特别是在物理层面，为数据提供了坚固的安全防护。

3. 安全管理

- 在确保信息安全方面，VMware 采取了一系列策略来强化其安全架构。
  - 多因素认证：Multi-factor Authentication (MFA)
    - 身份验证环节常常是安全体系中的薄弱点。
    - 多因素认证可以有效提升安全性，降低因密码简单或长时间未更新的风险。
  - 及时更新补丁：Patching
    - 保持更新对于维护系统安全至关重要，也是引入新功能和保障系统稳定性的基础。

3. 安全管理

- vCenter Single Sign-On (SSO)
  - 是 vSphere 使用的用户管理、服务管理及认证系统。
  - vCenter SSO 支持的认证模式有：
    - Local SSO Domain：本地单点登录域：
      - 在部署PSC过程中，系统默认创建了一个单点登录域，它充当了身份验证的默认来源。
    - Active Directory（Native）：
      - 当PSC与活动目录域集成时，可以利用Kerberos认证机制，将该域作为认证源。
    - LDAP（Active Directory）：
      - 若不希望将 PSC 加入到活动目录域中，或者正在采用一个简化版的活动目录，此选项将十分适用。
    - LDAP（OpenLDAP）：
      - 对于拥有开源LDAP服务器，例如 OpenLDAP 的用户，此选项提供了一个合适的选择。
    - 本地操作系统：
      - 可以在安全账户管理器（SAM）中定义账户，或者在 /etc/passwd 和 /etc/shadow 文件中定义账户。


vSphere Client
配置
Active Directory 域
10.10.1.254
节点未加入任何 Active Directory。
vCenter SSO 支持的认证模式

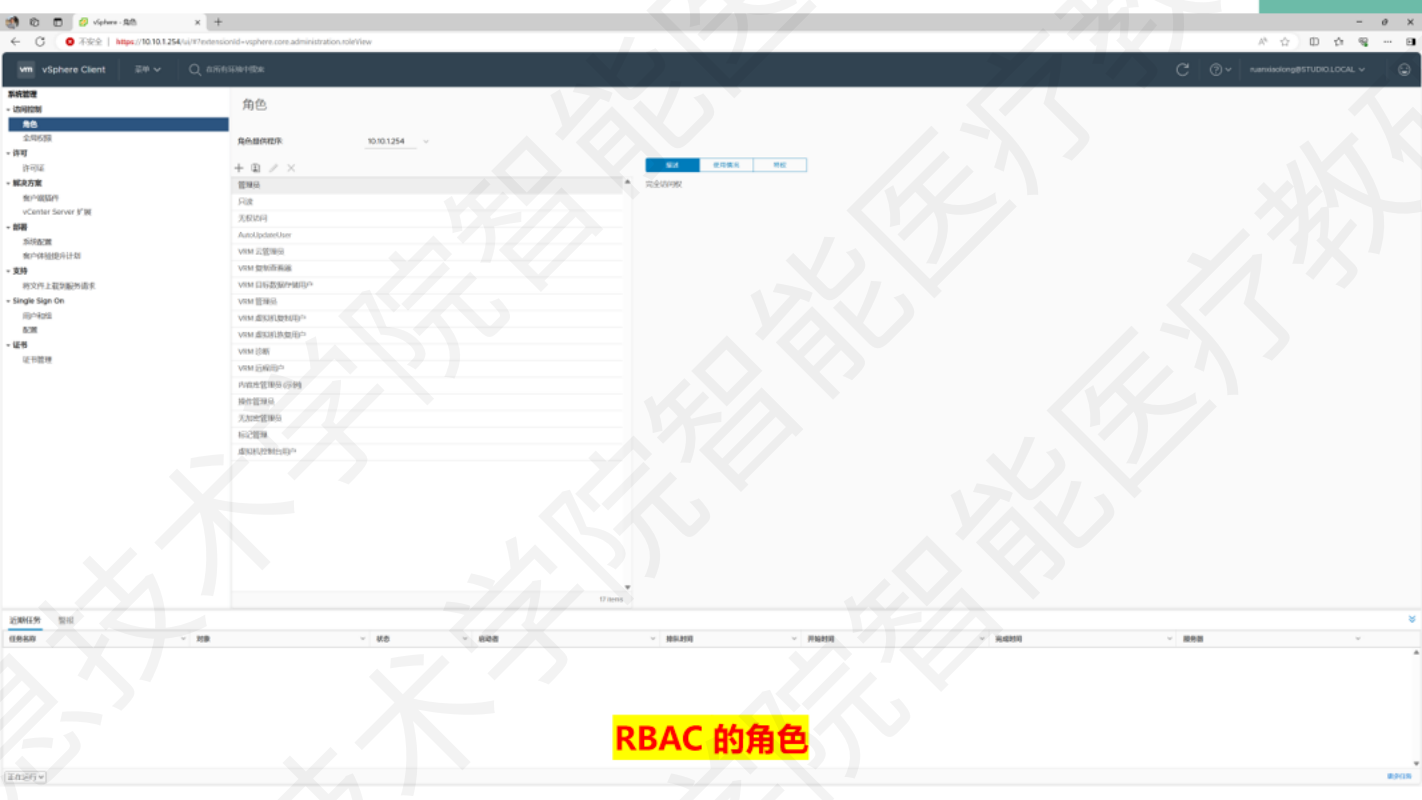
3. 安全管理

- vCenter Single Sign-On (SSO)
  - 密码管理的基本原则
    - Strength and complexity：强度和复杂度，通过 pam_passwdqc.so 实现。
    - Lockout：锁定账户，可以在错误尝试后锁定，并根据规则自动解锁。
    - Policies：密码策略，密码格式和使用的规则。
  - vCenter SSO 的密码管理的策略分为三类：
    - PASSWORD POLICY：强制密码策略。
      - 最长生命周期、限制重用、最大长度、最小长度、字符要求
    - LOCKOUT POLICY：锁定账户策略。
      - 最多失败登录尝试次数、两次失败之间的时间间隔、解除锁定时间
    - TOKEN POLICY：会话令牌策略。
      - 时钟容错、最大令牌续订计数、最大令牌委派计数
      - 持有者令牌的最长生命周期、密钥所有者令牌的最长生命周期

vCenter SSO 的密码管理策略

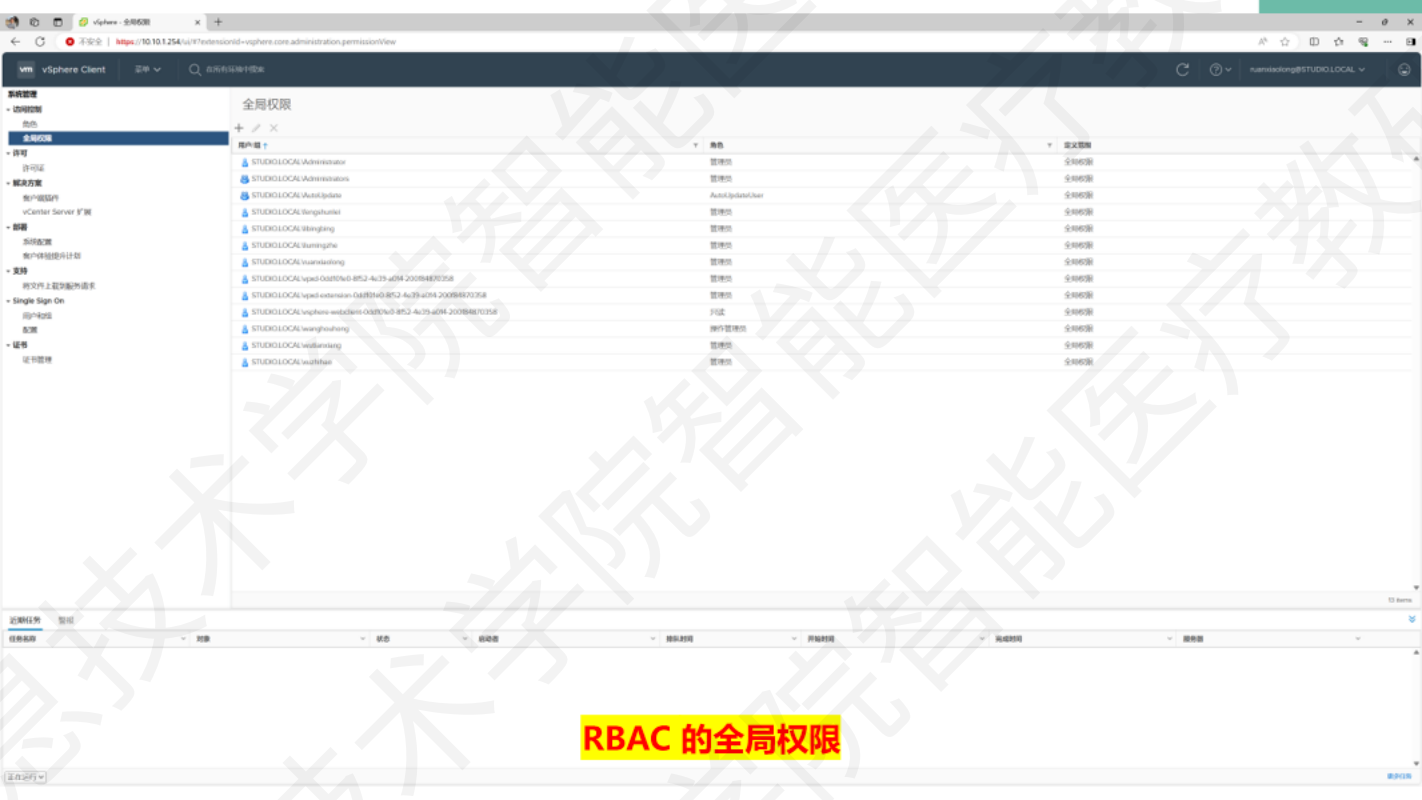
3. 安全管理

- Role-Based Access Control (RBAC)：基于角色的访问控制
  - 权限与角色相关联，用户通过成为某角色成员而得到角色对应权限。
    - 简化了权限管理。权限赋给角色，角色赋予用户。
    - 权限设计很清楚，权限管理很方便。
  - vSphere 实现 RBAC 的 3 个核心组件：Who 对 What 进行 How 的操作
    - 角色 Roles：What
      - 角色代表了一组特定权限，这些权限是用户操作中不可或缺的一部分。
    - 权限 Permissions：How
      - 权限是执行特定任务所必需的，如关闭虚拟机操作就需要相应权限。
      - 多个权限集合构成了一个角色。
    - 用户与组 Users and Groups：Who
      - 角色被分配给特定的用户和 vSphere 的特定对象，如数据中心、群集或单独的虚拟机。


vSphere Client
角色
RBAC 的角色

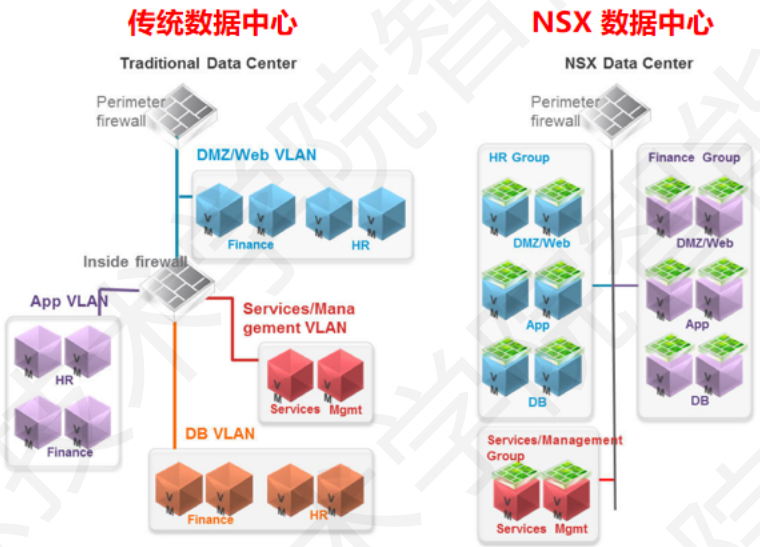
3. 安全管理

- vSphere 定义了两类用户和组：
  - 对象级别权限：
    - 传统的权限添加方式。
    - 将用户或组与 vSphere 中的特定对象关联，并赋予相应的角色。
  - 全局级别权限：
    - 允许在基础设施的整个范围内（在PSC级别）定义全局权限。
    - 权限将通过特定的角色应用到所有与 PSC 连接的 vCenter 服务器上。


vSphere - 全局权限
不安全 | https://10.10.1.254/ui/#?extensionId=vsphere.core.administration.permissionView
vSphere Client
菜单
在所有环境中搜索
ruanxiaolong@STUDIO.LOCAL
系统管理
访问控制
角色
全局权限
许可
许可证
解决方案
客户端插件
vCenter Server 扩展
部署
系统配置
客户体验提升计划
支持
将文件上载到服务请求
Single Sign On
用户和组
配置
证书
证书管理
全局权限
用户/组
角色
定义范围
STUDIO.LOCAL\Administrator 管理员 全局权限
STUDIO.LOCAL\Administrators 管理员 全局权限
STUDIO.LOCAL\AutoUpdate AutoUpdateUser 全局权限
STUDIO.LOCAL\bingshuitai 管理员 全局权限
STUDIO.LOCAL\bingbing 管理员 全局权限
STUDIO.LOCAL\liumingzhe 管理员 全局权限
STUDIO.LOCAL\ruanxiaolong 管理员 全局权限
STUDIO.LOCAL\vpxd-0dd1f0e0-8f52-4c39-a0f4-2009f4870358 管理员 全局权限
STUDIO.LOCAL\vpxd-extension-0dd1f0e0-8f52-4c39-a0f4-2009f4870358 管理员 全局权限
STUDIO.LOCAL\vsphere-webclient-0dd1f0e0-8f52-4c39-a0f4-2009f4870358 只读 全局权限
STUDIO.LOCAL\wanghouheng 操作管理员 全局权限
STUDIO.LOCAL\weibanniang 管理员 全局权限
STUDIO.LOCAL\wuhihao 管理员 全局权限
53 items
近期任务
警报
任务名称
对象
状态
启动者
排队时间
开始时间
完成时间
服务器
正在运行

RBAC 的全局权限

3. 安全管理



微分段(Micro-segmentation)

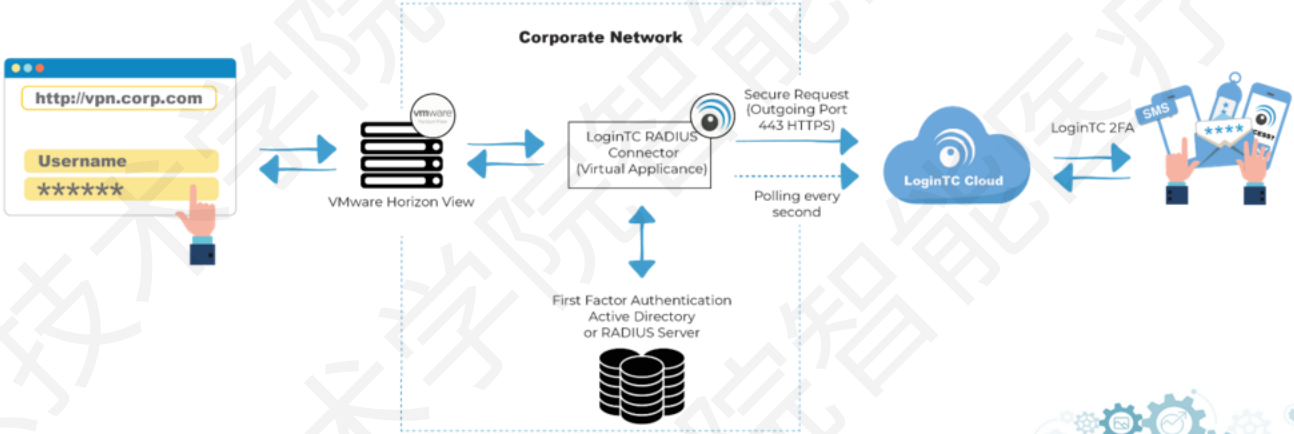
- 是网络虚拟化提出的安全技术。
- 能够提供工作负载级别上的精细安全策略控制来保障用户业务安全。
- 无须硬件设备(硬件防火墙）介入，
- 安全策略集成到虚拟网络(virtual network)、虚拟主机(VM)、操作系统及其他虚拟安全实例。

3. 安全管理

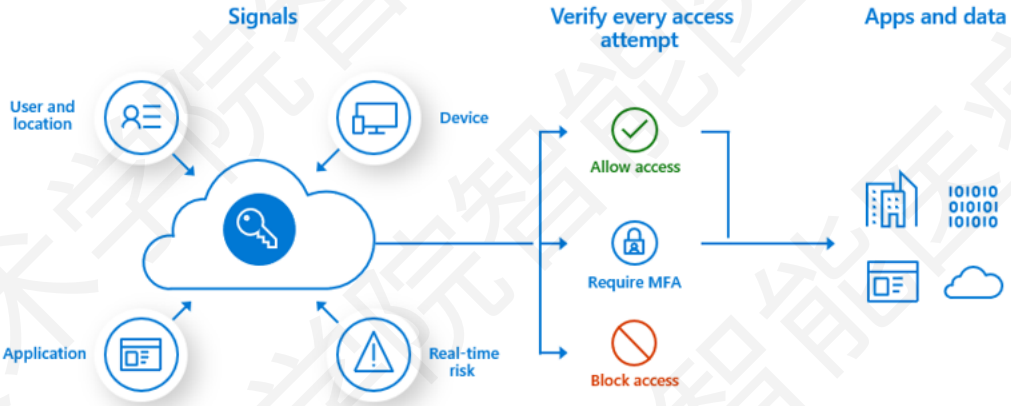
- 多重身份验证（Multi-Factor Authentication）
  - 是一种增强身份验证安全性的方法。
  - 要求用户提供两种或更多种不同类型的身份验证因素来确认其身份。
- 双因素身份验证（2FA）
  - 是一种只使用两个组件的 MFA 类型。
  - 从vSphere 6.0 Update 2 开始，可以使用以下方式使用 2个 FA：
    - 智能卡 Smart Cards（ UPN-based Common Access Card，CAC ）
    - RSA SecurID 令牌

3. 安全管理

vSphere 2FA



MFA



什么是 MFA？
https://docs.microsoft.com/zh-CN/azure/active-directory/authentication/concept-mfa-howitworks

3. 安全管理

- vSphere 提供两种方式的数据加密：
  - 存储加密：Encryption at rest
    - 数据加密后存储在存储设备上。
    - 换句话说，就是存储的数据是加密后的数据。
  - 传输加密：Encryption during transit
    - 数据在通过不安全的通道传输时会被加密。
    - 数据加密后传输，确保在不可靠的通信时保护数据安全。

3. 安全管理

- vSphere 提供的存储加密方式：
  - Encryption at storage physical level
    - 使用具有 self-encrypting drives (SEDs) 功能的设备，也称为基于硬件的全磁盘加密技术 full-disk encryption (FDE)。
    - 此种方式需要存储设备具体实现加密。
  - Encryption at storage logic level
    - 针对 vSAN，使用 AES 256 算法进行加密，比购买 SEDs 成本更低。
    - 实现了 vSAN 的全磁盘加密。
  - Encryption at VM level *
    - 虚拟机的虚拟磁盘进行加密。
  - Encryption inside the VM
    - 支持 VM 安装的 Guest OS 开启磁盘分区加密功能。
    - 例如 Windows 的 BitLocker 驱动器加密功能。

3. 安全管理

- VM encryption
  - 是 vSphere 6.5 之后的新功能，实现对整个 VMDK virtual disks 的加密。
  - VM encryption 的实现需要三个组件：
    - KMS:
      - 生成并存储传递给 vCenter 服务器以对虚拟机进行加密和解密的密钥。
    - vCenter Server:
      - 是唯一能登录 KMS 并获取密钥，并将密钥推送到 ESXi Host，确保密钥的安全性和有效分发。
      - vCenter Server 不存储密钥，仅维护密钥 ID 列表，以便于管理和追踪。
    - ESXi Host：
      - 通过密钥管理协议 KMIP，获取密钥实现对 VM 的加密和解密。

3. 安全管理

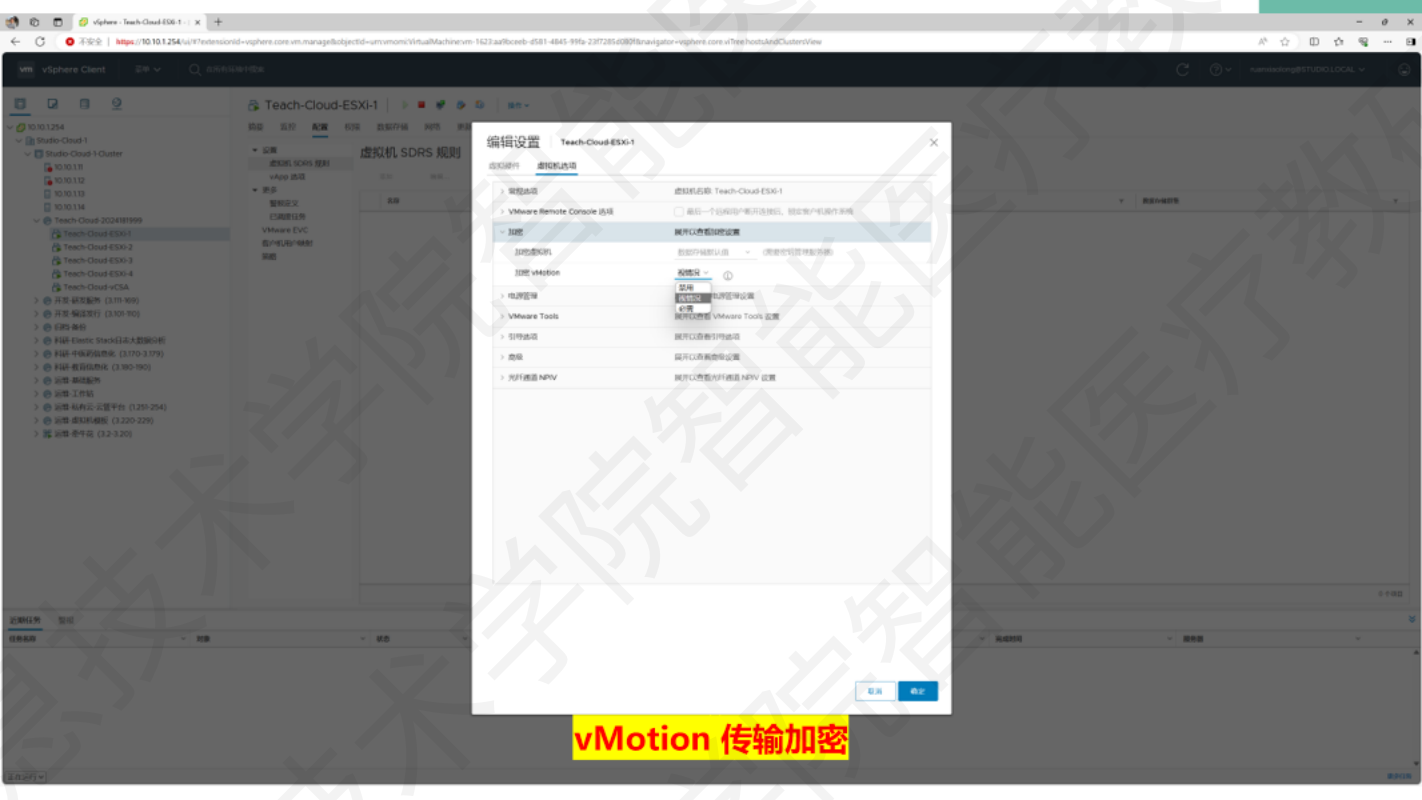
虚拟机加密：How vSphere Virtual Machine Encryption Protects Your Environment
https://docs.vmware.com/cn/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-E6C5CE29-CD1D-4555-859C-A0492E7CB45D.html

3. 安全管理

- 传输加密 Encryption during transit
  - Protecting data in motion，旨在保护传输中的数据。
  - 已经加密传输的数据
    - vSphere Client
    - vSphere Host Client
    - vMonitor（vSphere 6.5 及以后版本支持）
  - 没有加密传输的数据
    - FT Logging
    - storage traffic based on IP, such as iSCSI or NFS traffic.
    - 如果由必要可以使用：MACsec 、IPsec

3. 安全管理

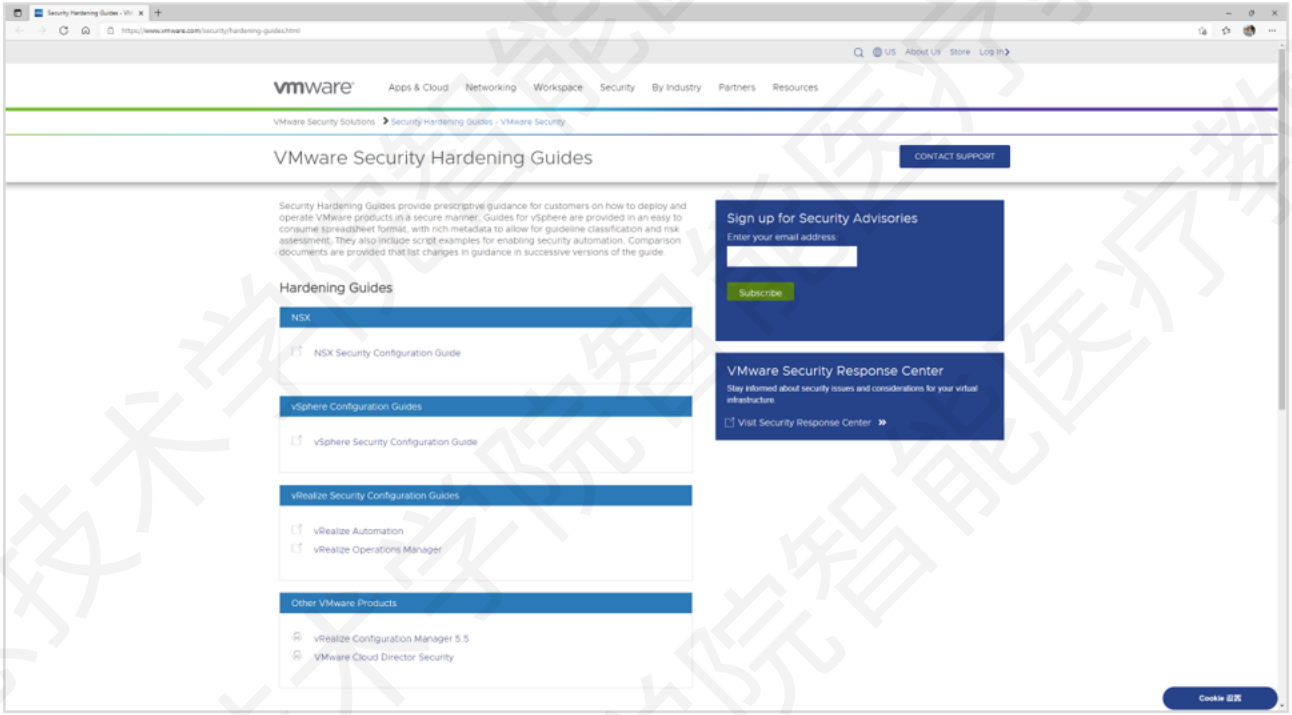
- 传输加密 Encryption during transit
  - 在执行 vMotion 操作时，采用三种不同的策略来确保数据传输的安全性。
    - 视情况：Opportunistic
      - 当源和目标 ESXi Host 都支持加密 vMotion 时，将使用加密 vMotion。
      - 如果任一主机不支持加密 vMotion，则将使用常规的未加密 vMotion。
    - 必须：Required
      - 此策略要求源和目标 ESXi Host 都必须能够执行加密 vMotion。
      - 如果任一主机不符合要求，vMotion 配置将失败。
    - 禁用：Disabled
      - 在此选项下，完全不使用加密 vMotion，只会使用常规的未加密 vMotion。

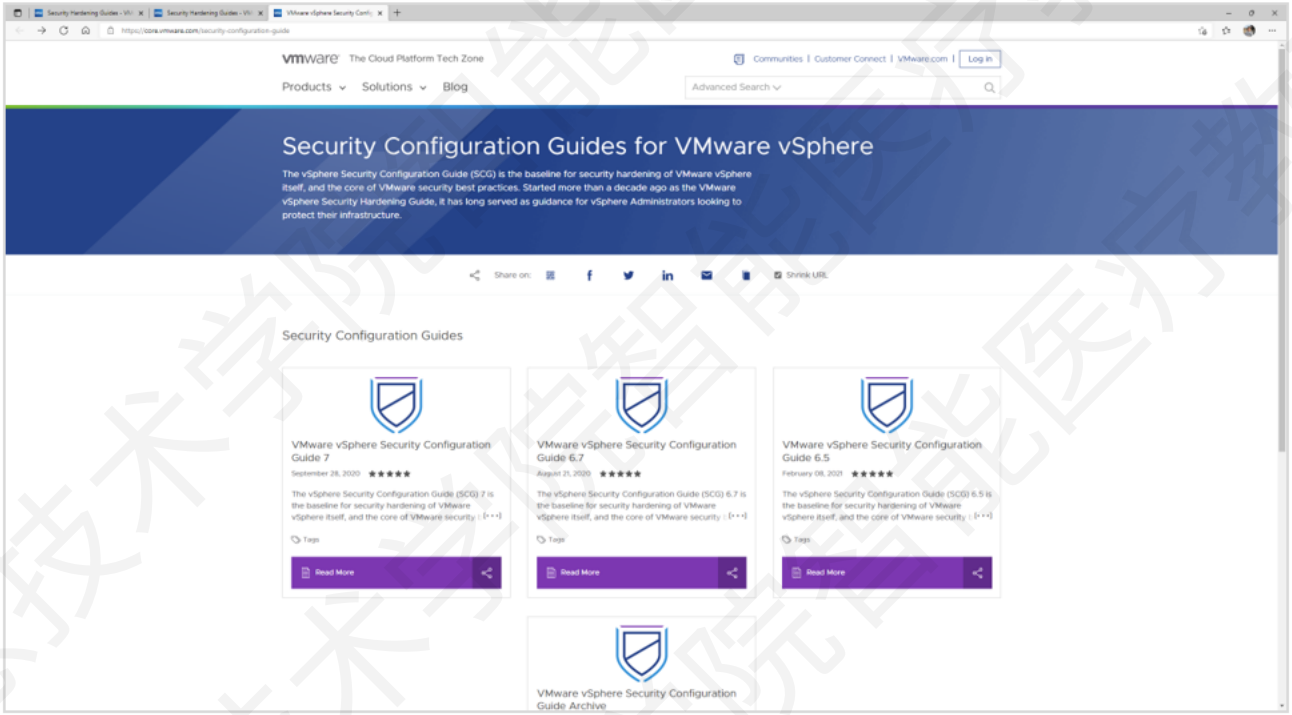

编辑设置
Teach-Cloud-ESXi-1
虚拟硬件
虚拟机选项
常规选项
虚拟机名称: Teach-Cloud-ESXi-1
VMware Remote Console 选项
加密
展开以查看加密设置
加密虚拟机
加密 vMotion
禁用
机会性
必需
电源管理
VMware Tools
展开以查看 VMware Tools 设置
引导选项
展开以查看引导选项
高级
展开以查看高级设置
光纤通道 NPIV
展开以查看光纤通道 NPIV 设置
取消
确定
vMotion 传输加密

3. 安全管理

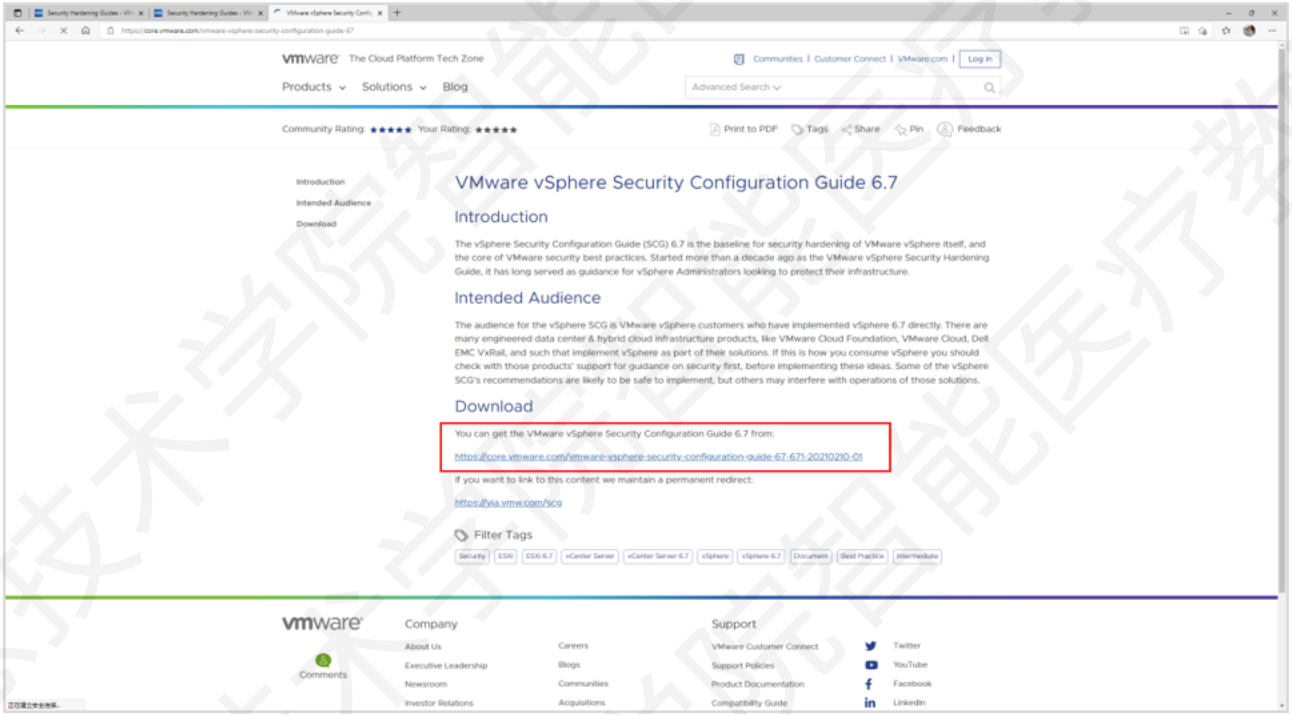
- 安全加固是保护系统、服务、基础设计的过程。

Security Hardening Guides

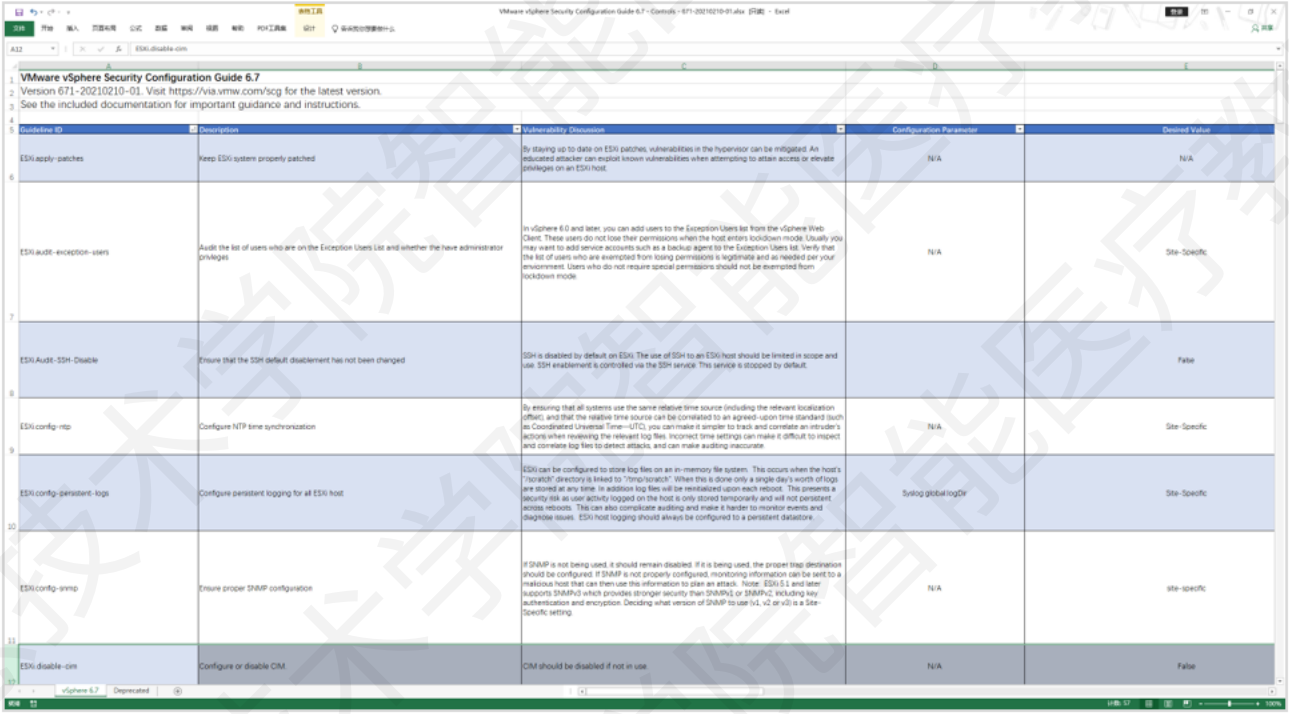

Security Hardening Guides - VM
https://www.vmware.com/security/hardening-guides.html
US
About Us
Store
Log In
vmware
Apps & Cloud
Networking
Workspace
Security
By Industry
Partners
Resources
VMware Security Solutions
Security Hardening Guides - VMware Security
VMware Security Hardening Guides
CONTACT SUPPORT
Security Hardening Guides provide prescriptive guidance for customers on how to deploy and operate VMware products in a secure manner. Guides for vSphere are provided in an easy to consume spreadsheet format, with rich metadata to allow for guideline classification and risk assessment. They also include script examples for enabling security automation. Comparison documents are provided that list changes in guidance in successive versions of the guide.
Hardening Guides
NSX
NSX Security Configuration Guide
vSphere Configuration Guides
vSphere Security Configuration Guide
vRealize Security Configuration Guides
vRealize Automation
vRealize Operations Manager
Other VMware Products
vRealize Configuration Manager 5.5
VMware Cloud Director Security
Sign up for Security Advisories
Enter your email address:
Subscribe
VMware Security Response Center
Stay informed about security issues and considerations for your virtual infrastructure.
Visit Security Response Center
Cookie 设置


vmware The Cloud Platform Tech Zone
Communities | Customer Connect | vmware.com | Log in
Products Solutions Blog
Advanced Search
Security Configuration Guides for VMware vSphere
The vSphere Security Configuration Guide (SCG) is the baseline for security hardening of VMware vSphere itself, and the core of VMware security best practices. Started more than a decade ago as the VMware vSphere Security Hardening Guide, it has long served as guidance for vSphere Administrators looking to protect their infrastructure.
Share on:
Shrink URL
Security Configuration Guides
VMware vSphere Security Configuration Guide 7
September 28, 2020
The vSphere Security Configuration Guide (SCG) 7 is the baseline for security hardening of VMware vSphere itself, and the core of VMware security
Tags
Read More
VMware vSphere Security Configuration Guide 6.7
August 21, 2020
The vSphere Security Configuration Guide (SCG) 6.7 is the baseline for security hardening of VMware vSphere itself, and the core of VMware security
Tags
Read More
VMware vSphere Security Configuration Guide 6.5
February 08, 2021
The vSphere Security Configuration Guide (SCG) 6.5 is the baseline for security hardening of VMware vSphere itself, and the core of VMware security
Tags
Read More
VMware vSphere Security Configuration Guide Archive

安全指南是个电子表格，对安全风险进行分类，并给出配置指南。



安全指南是个电子表格，对安全风险进行分类，并给出配置指南。



VMware vSphere Security Configuration Guide 6.7

Version 671-20210210-01. Visit https://via.vmw.com/scg for the latest version.

See the included documentation for important guidance and instructions.

Guideline ID	Description	Vulnerability Discussion	Configuration Parameter	Desired Value
ESXi-apply-patches	Keep ESXi system properly patched	By staying up to date on ESXi patches, vulnerabilities in the hypervisor can be mitigated. An educated attacker can exploit known vulnerabilities when attempting to attain access or elevate privileges on an ESXi host.	N/A	N/A
ESXi-audit-exception-users	Audit the list of users who are on the Exception Users List and whether the have administrator privileges	In vSphere 6.0 and later, you can add users to the Exception Users list from the vSphere Web Client. These users do not lose their permissions when the host enters lockdown mode. Usually you may want to add service accounts such as a backup agent to the Exception Users list. Verify that the list of users who are exempted from losing permissions is legitimate and as needed per your environment. Users who do not require special permissions should not be exempted from lockdown mode.	N/A	Site-Specific
ESXi-Audit-SSH-Disable	Ensure that the SSH default disablement has not been changed	SSH is disabled by default on ESXi. The use of SSH to an ESXi host should be limited in scope and use. SSH enablement is controlled via the SSH service. This service is stopped by default.		False
ESXi-config-ntp	Configure NTP time synchronization	By ensuring that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time--UTC), you can make it simpler to track and correlate an intruder's actions when reviewing the relevant log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate.	N/A	Site-Specific
ESXi-config-persistent-logs	Configure persistent logging for all ESXi host	ESXi can be configured to store log files on an in-memory file system. This occurs when the host's "/scratch" directory is linked to "/tmp/scratch". When this is done only a single day's worth of logs are stored at any time. In addition log files will be reinitialized upon each reboot. This presents a security risk as user activity logged on the host is only stored temporarily and will not persistent across reboots. This can also complicate auditing and make it harder to monitor events and diagnose issues. ESXi host logging should always be configured to a persistent datastore.	Syslog.global.logDir	Site-Specific
ESXi-config-snmp	Ensure proper SNMP configuration	If SNMP is not being used, it should remain disabled. If it is being used, the proper trap destination should be configured. If SNMP is not properly configured, monitoring information can be sent to a malicious host that can then use this information to plan an attack. Note: ESXi 5.1 and later supports SNMPv3 which provides stronger security than SNMPv1 or SNMPv2, including key authentication and encryption. Deciding what version of SNMP to use (v1, v2 or v3) is a Site-Specific setting.	N/A	site-specific
ESXi-disable-cim	Configure or disable CIM.	CIM should be disabled if not in use.	N/A	False

3. 安全管理

vSphere 安全加固的体系

vCenter Server

PSC
SSO
NTP

ESXi Host

Limit
Lockdown Mode
Networking
Transparent Page Sharing
VIB Acceptance Level
Host Encryption Mode
ESXi Secure Boot

VM

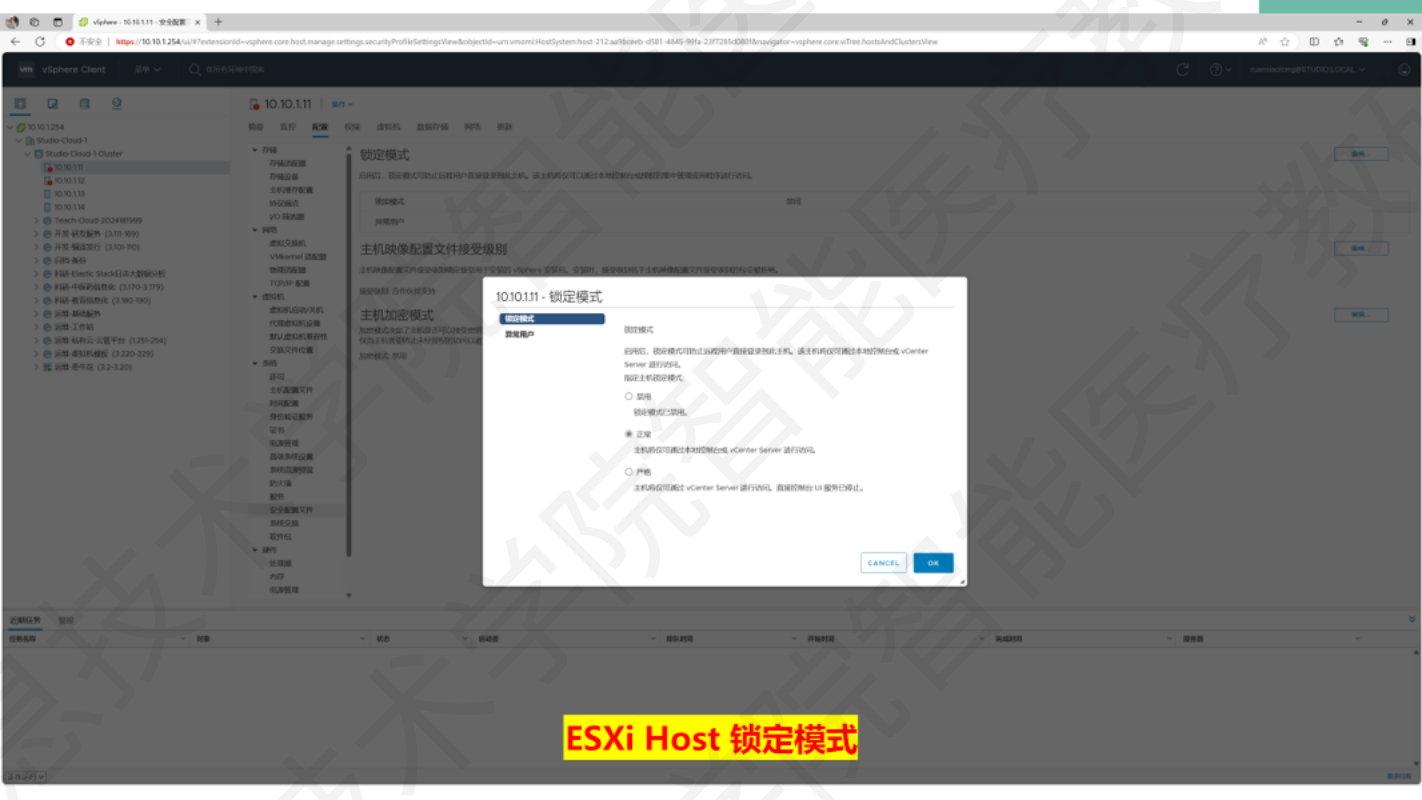
Templates
Minimize use of VM Console
Prevent VMs from taking over resources
Disable unnecessary functions
VM Secure Boot

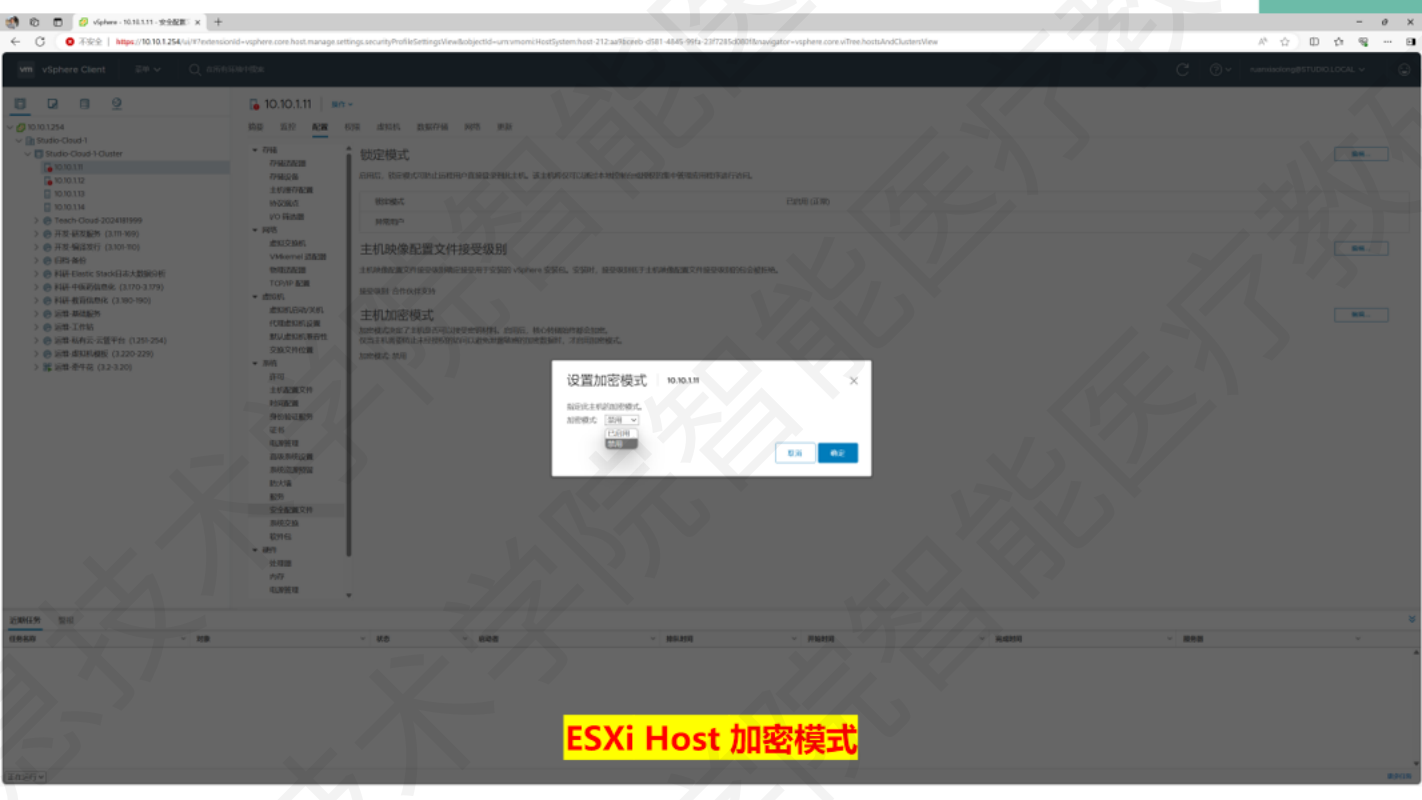
3. 安全管理

- vCenter Server 就是 Linux 应用服务器。不讨论基于 Windows 的部署模式
  - ESXi Host 的安全措施同样适用于 VCSA。
  - VCSA 的安全还要考虑到 PSC：
    - Check password expiration:
      - 默认的 vCenter SSO 密码有效期是 90 天。
    - Configure NTP:
      - 确保所有系统使用相同的相对时间源（包括相关的本地化偏移量）。
      - 同步的系统对于 vCenter SSO 证书有效性以及其他 vSphere 证书的有效性是至关重要的。
      - 证书有效性直接决定于 NTP。

3. 安全管理

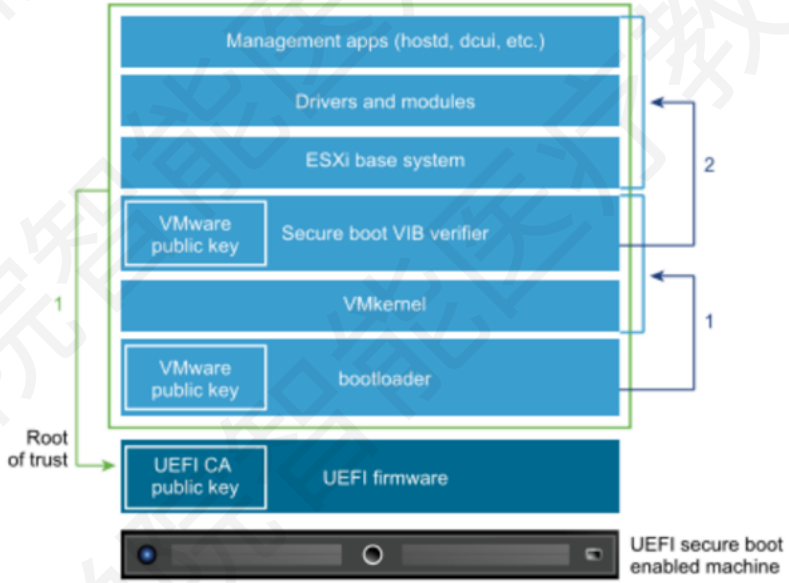
- 为了保护 ESXi Host 免受未经授权的入侵和误用，提高基础设施安全性，推荐配置选项：
  - Limit user access: 限制对 ESXi Host 的直接访问
    - Lockdown mode could be used to limit access to the hosts to all users.
  - Limit shell access: 限制 Shell 或 SSH 的访问方式
  - Limit services: 限制为最小服务
  - Limit network connections: 通过防火墙限制网络访问
  - Use secure connections: 使用安全链接访问
    - Starting with vSphere 6.5, the Transport Layer Security (TLS) protocol versions 1.0, 1.1, and 1.2 are enabled by default.
  - Patch your hosts: 从 VMware 官方途径升级
    - Use only VMware sources to upgrade or patch ESXi hosts.


10.10.1.11 - 锁定模式
锁定模式
异常用户
锁定模式
启用后，锁定模式可防止远程用户直接登录到此主机。该主机将仅可通过本地控制台或 vCenter Server 进行访问。
指定主机的锁定模式：
禁用
锁定模式已禁用。
正常
主机将仅可通过本地控制台或 vCenter Server 进行访问。
严格
主机将仅可通过 vCenter Server 进行访问。直接控制台 UI 服务已停止。
CANCEL
OK
ESXi Host 锁定模式


设置加密模式
10.10.1.11
加密模式
已启用
取消
确定
ESXi Host 加密模式

3. 安全管理

- ESXi Secure Boot
  - ESXi Host 的安全启动支持所有的 VIB 选项，例如启动时加密等。
  - 通过 UEFI，启动时只有通过安全审核的 ESXi VMkernel 才能够启动。



3. 安全管理

- 为了提升 VM 的安全性：
  - vSphere 6.0 及以后版本，VM 默认配置参数参照安全加固指南进行的。
  - 使用默认值，就可以做到较高安全性。
    - 关于 VM 默认值的配置信息，可以阅读：
    - https://blogs.vmware.com/vsphere/2017/06/secure-default-vm-disable-unexposed-features.html

3. 安全管理

- 虚拟机安全性最佳做法：
  - 虚拟机常规保护
    - 虚拟机在大多数情况下等同于物理服务器。
    - 在虚拟机中采用与物理系统相同的安全措施。
  - 使用模板来部署虚拟机
    - 在虚拟机上手动安装客户机操作系统和应用程序时，会带来配置错误的风险。
    - 通过使用模板捕捉未安装任何应用程序的强化基础操作系统映像，可以确保通过已知的安全基准级别创建所有虚拟机。
  - 尽量少用虚拟机控制台
    - 虚拟机控制台为虚拟机提供的功能与物理服务器上的监视器相同。
    - 具有虚拟机控制台访问权限的用户可以访问虚拟机电源管理和可移除的设备连接控制。
    - 因此，控制台访问权限可能造成对虚拟机的恶意攻击。

3. 安全管理

- 虚拟机安全性最佳做法：
  - 防止虚拟机取代资源
    - 当一个虚拟机消耗过多主机资源而使主机上的其他虚拟机无法执行其预期功能时，可能会出现拒绝服务 (DoS)。
    - 为防止虚拟机造成 DoS 问题，请使用主机资源管理功能（例如设置份额和使用资源池）。
  - 禁用虚拟机中不必要的功能
    - 虚拟机中运行的任何服务都有可能引发攻击。
    - 通过禁用支持系统上运行的应用程序或服务非必需的系统组件，可以降低这种风险。

3. 安全管理

虚拟机安全性最佳做法
https://docs.vmware.com/cn/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-14CCC8CD-D90D-4227-B2C3-0A93D3C023BA.html

3. 安全管理

- 与物理服务器相同的安全原则，同样适用于虚拟机：
  - 使用密码保护 BIOS
  - 为操作系统和应用程序及时升级补丁程序
  - 启用 Secure Boot
  - 开启防火墙
- VM Secure Boot 的基本要求：
  - Virtual hardware version 13 or later
  - EFI firmware in the VM boot options
  - Guest OS that supports UEFI Secure Boot
    - Windows 8 and Windows Server 2012 +
    - RHEL/Centos 7.0 +
    - Ubuntu 14.04 +

Backup is not security

Snapshot is not backup

智能运维课程体系


棒棒堂智能运维
UID: 510401430
抖音
@棒棒堂智能运维
抖音号：ID2003079563
只要思想不滑坡，办法总比困难多。
保存图片到相册
打开抖音搜索页扫一扫