激活的方法
个人:零售激活,OEM 激活
企业（批量激活）:MAK(永久激活),KMS(非永久，防盗版，提高激活效率）,ADBA（改进版的 KMS）
原理：设置一台机器为服务器（KMS 主机），用微软提供的 KMS 密钥（CSVLK）激活 KMS 主机，其他的电脑装好 KMS 客户端，用 GVLK 激活客户端，保证客户端和服务器在同一个网络中能够互相连通，KMS 服务器通过微软验证后（KMS 主机密钥）后，会在服务器上填写 SRV 记录，客户端通过 SRV 记录找到 KMS 服务器进行验证，达到阈值即可激活。
阈值：
KMS 客户端 OS 版本（Win10,Win8.1,Win7）>25 个
KMS 服务器 OS 版本（Win Server2019,2016,2012R2,2012）>5 个
KMS 密钥每 7 天续订一次，若 failed，client 每两小时重试一次
KMS 密钥最多可以安装在 6 个 KMS 主机上，同一主机用同一密钥可重新激活 9 次
ADBA:与 KMS 相似，只要在一个域内的机器就可以直接激活不需要激活阈值。

ADBA	KMS
无阈值，同一个域内任意计算机都可被激活	阈值，25 台计算机，5 台服务器
Win8, Win Server2012 等版本	Win7, Win Server2008R2 等版本
TCP/IP, 1688 端口， RPC	LDAP

部署 KMS 环境：

1. 用 VAT 批量激活工具，针对 server 版本，里面有个 server manage，在里面安装个角色 volume activation service，装了这个角色之后就会进入 VAT 界面，在这个界面上把 KMS host key 加入进去（UI 界面）
2. 激活方式：slmgr.vbs /ipk<KMS key>密钥激活, 电话激活，slmgr.vbs /ato<KMS key>在线激活（CMD 命令行）

ADBA 只能通过 UI 界面上，没有 CMD 命令，需要用到 KMS Host KEY, (CSVLK)
ADBA 原理：机器在同一个域中，通过设置一个 Activation Object 去激活
常见的 slmgr.vbs 命令
/CDNS 禁用 KMS 主机自动 DNS 发布，/SNDS 启用 KMS 主机自动 DNS 发布
/SKMS:禁用 KMS 客户端 /CKMS（默认）：启用 KMS 客户端自动寻找主机
/ato:在线激活
/dli /dlv:查看机器状态信息
订阅激活：专业版升级到企业版
前提条件：本身的 OS 就是要是激活的状态才能够实现升级/订阅激活
高版本的 KEY 可以激活本身以及低两个版本的 OS，例如 2019 的 KEY 可以激活 2012R2，前提条件：CU
ESU：扩展安全更新，2020.1.14 微软对 Win7, Server 2008R2 停止支持，微软提出了三种解决案，1.Move to Azure, 2.upgrade, 3.ESU
前提条件：Windows 7 SP1 和 Windows Server 2008 R2 SP1：
服务堆栈更新 （SSU） （KB4490628）
SHA-2 更新 （KB4474419）
Windows Server 2008 SP2：
服务堆栈更新 （SSU） （KB4493730）

最新的 SHA-2 更新 （KB4474419）
Licensing packing
激活 ESU：
1./ipk <ESU> key
2./dlv 获取 activation ID
3.配置防火墙白名单
4./ato <ESU Activation ID>
电话 atp:<confirmation id> 和<ESU key>和代理激活
VAMT:批量激活管理工具
KMS,MAK,ESU
激活方式：联机激活，代理激活，KMS 激活
(1).安装并运行 VAMT(2).配置防火墙白名单(3).运行 VAMT 数据库(4).寻找产品(AD,IP OR NAME 工作组，LDAP)(5).筛选排序计算机(6).收集计算机状态信息(7).添加密钥并监视计数(8).安装 KEY
(9).激活客户端
(10).代理激活 isolate 实验室,将 VAMT 数据导入.cilx 文件(11).VAMT 主机与微软确认 CID 并导入至.cilx 文件中(12).VAMT 主机将.cilx 文件分发给客户端(13).应用 CID 并激活计算
(14).KMS 激活前提条件，KMS 服务启用，VAMT 安装好并连接 DB(15).KMS 主机选择（DNS 自己寻找，手动指定，查找域中使用 DNS 的 KMS 主机）(16).筛选并选择产品(17).批量激活
Q1:电脑说他们的电脑没法激活？

1. 确认电脑数量规模
2. C/S 网络是否连通
3. PC 的 CMID 计数不唯一
4. 问客户是问题处在 Client 上还是 host 上（比如有多少台 client 出问题，可能是 kms client key 没加入进去），有可能很多台 client 出了问题，那么有可能是 host 问题
5. KEY 的版本是否正确，比如 key 是 2016 的但是环境是 2019 的
6. 向客户收集一下版本信息，日志信息

12290：激活所需的计数，CMID,许可证时间和状态到期时间
故障排除：（1）发生了网络中断（2）主机未解析或未在 DNS 中注册（3）防火墙禁用 TCP/IP 1688（4）事件日志已满
12293：主机未在 DNS 中发布所需的记录，会导致故障
因此在安装 KMS 主机之后并在部署客户端之前进行验证
12288：client 无法连接 host，主机无响应或客户端未收到响应
12289：激活标志，成功 1，失败 0，KMS 主机上计数 fail 可能是因为 client 计数不足
若机器达到阈值仍无法激活，观察 error code，阈值达到的时候，查询一下 count 计数问题，CID 不唯一无法正确计数，查询 dlv 可以查看有效 count，event log
UI 界面 Event Viewer 查看日志

Update
Feature Update:功能更新，每 6 月（3 月/9 月更新一次），仅适用于 Win10
Quality Update:质量更新

1. Security Monthly Quality Update：自 2016 年起，微软每月发布一次 CU,会把之前所有的更新都集中到一起。
2. Security Only:仅适用于 server 2016 之前，Win10 之前（如 Win7 或 server2012R2）
3. Preview of Monthly Rollup:用于测试特定软件，用户可选择地更新下个月预览更新

CU:累计更新是包含以前的发布过的更新，相当于捆绑在一起的多个简单更新。
2.how to install update(dism/standalone/wsus etc)?
DISM 方法:Expand -f* C:\Temp\... .msu C:\Temp;解压到 C 盘 Temp 文件夹
DISM /Oline /Add-package /Packagepath:C:\Temp\... .cab 安装更新
DISM /Online /Get-PackageInfo /PackageName:<Package Identity>查看更新
DISM /Online /RemovePackageName /PackageName:<Package Identity>卸载更新
Standalone 方法:下载.msu 文件安装 Windows Update Standalone Installer 按步骤更新
WSUS 方法:指定 Intranet Microsoft 更新服务位置，集中式自动化式更新管理，可以更新一些长期每网隔离的计算机，只要 WSUS 主机有网就行
3. Windows update Installation procedures and services.
WU installation procedures:当 update 可用时，会下载 Arbiter 和 metadata 元数据，完毕后 Arbiter 回去收集 device 信息和已下载的元数据比较去创建 action list,该 list 描述了所有人从 Windows update 所需的文件，以及什么 installer agent(CBS/SETUP)应该去做

Install update 时，点击 package 进行安装，则 servicing request call CBS,将文件投到目标 system 上，CBS 确认 System 上已安装的 file 和 staged file 的位置，将它们变成已安装并向 System 添加 registry value,CBS 读取 WinSxS/Manifest 中的文件确认安装内容和位置再确认所需的 package（C:/servicing/package 中）确认 install 顺序
CBS 完成之后 CALL CSI，生成 change list for system
CSI 在系统上生成 transaction，用 PI 和 AI 做组件安装
若有 POQ 且 No operation pending,则先执行 POQ 再 AIQ 在 CSI 之前完成
若有 operation pending.xml 则提示重启
重启中待做事项：C:\Windows\WinSxS\pending.xml
CSI CALL KTM 去维护事件隔离
APP call KTM 开始 transaction——要求 KTM 提交 transaction 同时保留 transaction log
一旦 KTM 完成所有操作回传 CSI SUCCESS OF FAIL
Success: CSI return to CBS 完成并提示用户 reboot
Fail: transaction rollback 显示失败信息
最后重启，staging 过程中，component，manifest，package 都被暂存，在 CBS Store 上面，便于 reboot 时将对应文件替换 C:\Windows\WinSxS

Service: Windows Module Installer Service 模块程序安装服务
Cryptographic Service 密码服务
Windows Update Service 更新服务
Background Intelligent Transfer Service 后台智能传输服务

1. What is manifest? Where does it exist? Extension name for manifest.
   应用程序清单是一个 XML 文件，描述各个 component 的安装

C:\Windows\WinsSxS\Manifest
(.manifest)

2. Component states during installation?
   Absent, Resolved, Staged, Installed.
3. What is staging? Where are components/manifests/packages stored for “staging” state.
   将更新文件添加到磁盘却不应用到系统的一种操作状态
   被暂存在 CBS STORE 上面，便于 reboot 时将对应文件进行替换。C:\Windows\WinSxS
4. During CBS troubleshooting, what log can be checked, location?
   CBS.log 分析关键词
   Operation Type: Appl, Plan Exec, Session, Startup, shutd
   System event log 一般要 filter:”Windows Update Client”记录安装开始，结束时间
   1074 意外重启 6008 （ctrl+alt+del）
   Eventlog 服务开启（开机）6005，关机 6006
   CBS verbose log 详细诊断日志
   Computer——Properties——Advanced System Setting——Environment Variables and add a new system variable called “Windows_Tracing_facility_Poq_Flags(10000)
   重复再复现问题然后 CBS log 中会有所有的 log
   TS 完成之后记得把环境变量删了!
   其他的 log 文件还有 Windows Update.log（检测下载）, UpdateSessionOrchestration.etl（深层问题）,Notification UxBroker.elt（异常通知）, CBS.log（更新安装）
   checkSUR.log (SUR: System Update Readiness)
   Location: C:%SYSTEMROOT%\logs\cbs
5. What is capability check? Possible reasons for “not applicable” error.
   在服务堆栈 Servicing Stack 中，CBS 从 top-level clients 获取下载 package，然后 CBS 评估该 package 是否适用于系统更新。如果适配的话，CBS 向 CSI 提供 component, generate appropriate installation state registry package with program and features
   更新被取代，更新组件将取代旧的组件，如收到报错，检查是否被新 package 取代
   已安装更新，若报错检查之前已安装 的更新
   32 or 64
   KB 版本
   Update 前提条件,例如 Monthly roll-up 需要提前下载 SSU
   Trust Installer Service 禁用
   Component Store
6. When will the rollback happen and what states of components during this phase?
   在 component level 确定 Install 是否完整，如果任何一个安装所需的操作失败，则认为 Component Install fail,则 Component（包括所有为了这个 component staging 的 file）都将在 rollback 期间从 System 中删除
   理想状态变成 absent，一些文件变成 staged 状态
7. How to check system healthiness status. Checksur logs and path.
   Check health: Dims.exe /Online/Cleanup-Image / CheckHealth,ScanHealth,RestoreHealth
   使用 CBS.log 去检查最后一次 update 安装失败
   修复在 CheckSUR 日志文件中发现的错误
   1. 打开 %SYSTEMROOT%\Logs\CBS\CheckSUR.log
   2. 确定该工具无法修复的包
   3. 下载程序包

4. 将包 （.msu） 复制到目录。默认情况下，此目录不存在，您需要创建它。%SYSTEMROOT%\CheckSUR\packages
5. 重新运行系统更新准备工具。

打开 %SYSTEMROOT%\Logs\CBS\CheckSUR.log

8. How to check path level. How to check installed patches.
   查看最新补丁，Winver 或者 hotfix，UI,dism
9. CBS auto clean task(winsxs folder 300GB).
   本身 CBS 是可以自动清理的
   1. Dism.exe /online /Cleanup-Image /StartComponentCleanup
   2. 设置 task 来清理
10. Why does system require reboot after update? What action will be done? Why? Actions be recorded in which file? (pending.xml)
    因为需要一些文件正在后台运行，如果不重启无法替换。
11. Group policy related to when restart? Group policy related to how updates offered?

Scenario1: If I installed the 2018 CUs and then I installed latest CU, what can we see in the control panel, get-hotfixes, dism get-package?
更新都可以看到，但是实际运行以最新版本为准
the control panel, get-hotfixes 看个大致 update 信息
dism get-package 看详细的 update 信息，以此为准
Scenario2:CX 客户 has installed an update successfully, the expected file versions are not updated accordingly. How to TS? What logs need to refer.
可能是 CX 的电脑已经装好了最新版本的 update，但是他本人不知道，这个时候查看一下电脑的 update，看看是否是此情况。Monthly roll-up 需要提前下载 SSU

Scenario3:only update with WSUS, automatic update at 11pm. On the third Tuesday of every month.
Q:How to configure group policy?
指定 intranet Microsoft
(Computer Configuration > Policies > Administrative Templates > Windows components > Windows Update > Windows Update for Business)
选择何时收到功能更新 Select when Feature Updates are received
Scenario4:If CX wants to block preview monthly roll-up with clicking check for update, is it available?
如果点击“检查更新”按钮，Microsoft 强制你下载并安装预览版，以便他们可以在正式更新之前查看其更新。唯一的解决方法是设置组策略以手动控制所有更新，直到看到常规更新而不是“预览”字样。然后才单击“下载”按钮，禁用手动更新，禁用预览版本
Scenario5:If only installed previously released updates, but scan results returning ”Your device is up to date”, what TS/logs should be checked.
可能是 CX 的电脑已经装好了最新版本的 update，但是他本人不知道，这个时候查看一下电脑的 update，看看是否是此情况。

1. SSU 是什么？
   服务堆栈更新提供对服务堆栈（安装 Windows 更新的组件）的修补程序。此外，它还包含“基于组件的服务堆栈”（CBS），它是 Windows 部署的多个元素（如 DISM、SFC、更改 Windows 功能或角色以及修复组件）的关键基础组件。CBS 是一个小组件，通常不会每月发布更新。
2. Update log
3. Component State corruption? Command/ tool 检查？失败日志？
4. Component store related registry location?
   HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\CBS
5. 控制 Windows Update behavior 的 policy？
6. 怎么看 Update 失败日志？event log——CBS

Windows 组件库,Windows SxS 文件夹

使用 Windows 更新安装新的组件版本。这样可以确保系统的安全性和最新状态。
启用或禁用 Windows 功能。
使用服务器管理器添加角色或功能。
在不同的 Windows 版本之间移动系统。
从损坏或启动故障中恢复系统
卸载有问题的更新
使用并行程序集运行程序

Servicing Layers

Client 层——提供 package，收集用户请求
CBS 层——将 Package/Update 解析为 Deployment
CSI 层——应用这些 deployment，解析为组件并对组件进行指控操作。

Prmitive Installer

使用 component change list 去生成每次变化所需的原始操作
File 和 registry change 是原始操作，所有的 PI 有的基本操作一起构成原始的操作队列
POQ 活动记录在%WinDIR%\WinSxS\Poqexec.log

Advance Installer

AI 不能执行文件建模更改 registry 的各种步骤操作，AIQ 是从组件更改生成的名单队列必须执行的操作事务顺序如下：

POQ 首先在 Kernel Transaction 中执行，执行 POQ 之后，将尽快运行 Advanced Installer，System 处于”torn state” util AIQ 完成，AIQ 失败需要复杂的 rollback。

Component State corruption

首先要有管理员权限

1．运行 SFC /scannow
若收到”Windows Resource Protection did not find any integrity violations.”进行 step02
若收到”Windows Resource Protection found corrupt files and successfully repaired them.查看 corruption 是否解决，如果还未解决进行 step02
2.运行 DISM 以查询并修复组件存储损坏
Dism.exe /Oline /cleanup-image /restorehealth(scanhealth,checkhealth)

1 Upgrade Process?

Down-Level: Online phase, SysCheck, App Driver and Device 遍历

Safe OS: Offline phase, migrate data from old OS to windows.old 文件夹 0-29%

First Boot: Offline phase, app driver data migration 30-75%

Second Boot: Offline phase, Remain of user settings, data 76-100%

2 Logs locations for upgrade process.

$ Windows. ~BT

Down-Level:\sources\Panther**Setupact.log** 和\Windows\Logs\Mosetup**Bluebox.log**

OOBE:\Source\Panther\UnattendGC**Setupact.log** 和\Windows\Panther**miglog.xml**

Rollback:\Sources\Rollback**Setupact.log**

3 How can Win 7 upgrade to Win 10? How old w10 upgrade to latest W10?

ISO 更新，Windows Feature Update，win10 更新助手。

Win10 的任何正式发布频道版本升级到更新，受支持的正式发布频道版本。

不支持 win7,win8.1 或 win10 正式发布频道到 Win10 LTSC 的就地升级

4 server 2008 to 2022, upgrade path.

可以逐级升级，这样不会删除用户的数据及设置，当然也可以卸载系统重装，这样数据就没了。

5 What is Dynamic Update? How to disable it?

系统后台和微软保持联系，使得组织和用户能够用到 **win10** 的最新功能

Setup DU, Safe OS DU, SSU, Latest CU, Language and feature on demand ,Driver Update

Unattend.xml 中默认时 true 开启，也可以 false 关闭；cmd 命令 setup /auto upgrade /DynamicUpdate disable

UI 界面，Task Sequence Editor 中选择开启 DU

6 WinPE VS WinRE? Differences and similarities

PE 是预安装，功能有限，用来部署修复 Windows 的迷你 OS

PE 无法加入网络域，文件服务器或终端服务器使用，远程桌面，IPv6 连接到 IPv4，.MSI 安装文件，非英文目录路径启动，32 位的 PE 上运行 64 位 APP，通过 DISM 添加.appxbundle 包

PE 技术原理就是把一个基本 OS 装到 image 中，然后启动时先在内存中创建一个虚拟盘符，然后把映像释放到虚拟盘中，最后实现系统启动。PE 对 PE 系统盘的任何修改都不被保存。

RE 就是一个特殊的 PE，进入 RE 后就默认进入系统恢复界面。

7 How to create WinPE. How to check WinPE versions. Win PE customization? How to add?

1.安装带有 WinPE 的 Windows ADK 后，以管理员身份启动部署和映像工具环境。

2.运行 copype 以创建 Windows PE 文件的工作副本。

Copype amd 64 C:\WinPE_amd64

Winpe file under C:\WinPE\media\sources\boot.wim

HLKM\Software\Microsoft\WindowsNT\CurrentVersion\WinPE 注册表项

设备驱动程序（.inf），软件包（.cab，也称 WinPE 可选组件）语言，添加文件和文件夹，DISM:使用更新的版本。当新版本的 Windows 需要最新版本的 DISM 的功能时，可以将 DISM 直接添加到 WinPE 中，启动脚本，应用程序，临时存储（暂存空间），背景图像，电源方案，WinPE 设置，Windows 更新。

1 装载 winPE

Dism/Mount/Image/ImageFile:D:\Sources\boot.wim/index:/MountDir:“C:\WinPE_amd64\Mount

2 添加自定义项，inf,更新，文件和文件夹，启动脚本，临时内存，替换背景图像

3.提交更改 Dism/Commit Image/MountDir:“C:\WinPE_amd64\mount”

8 What are unattended files? Where to find them? Search orders for answer files.

可用于在安装过程中修改 image 中的 Windows 设置。您还可以创建设置，以触发映像中的脚本，这些脚本在第一个用户创建其帐户并选择其默认语言后运行。

Windows\Panther

1.注册表 HKLM \System\Setup\UnattendFile。

2.Unattend.xml 或%WINDIR%\Panther\Unattend\下的 Autounattend.xml。

3.%WINDIR%\Panther 下的 Unattend.xml\

4.Autounattend.xml 位于可移动读/写介质的根目录，按驱动器号顺序排列。

5. Autounattend.xml 位于可移动只读介质根目录的，按驱动器号顺序排列。

6.windowsPE 和 offlineServicing 配置传递读取\Sources\Autounattend.xml。其他配置传递读取%WINDIR%\System32\Sysprep\Unattend.xml。

7.%SYSTEMDRIVE%下的 Unattend.xml 或 Autounattend.xml。

8.在运行 Windows Setup.exe 中，位于根目录下的 Unattend.xml 或 Autounattend.xml。

9 What is feature update? Frequency? Lifecycle?

每年两次，一般在 3 月，9 月更新，为 windows 添加新功能，仅适用于 win10.

10 How to upgrade OS from evaluation edition to permanent edition?

DISM 命令 Get-targetversion set-version

11 Can standard upgrade to datacenter? Yes

12 What is setupconfig.ini. What's the location and how to use it?

配置文件，改变文件中的参数来配置 Windows Setup.exe

Setup /No Reboot /Show OOBE None/ Telemetry Enable

用 ISO 时可以用 setupconfig.ini,但是当用 feature update 更新时这个就不哈用了，使用 WU 时，将 setupconfig.ini 放在%systemdriver%\Users\Default\AppData\Local\Microsoft\Windows\WSUS 中

13 What is Sysprep? Log Location

1. 从 Windows Image 中删除特定的信息包含 SID，使得将 image 应用到其他 PC
2. 从 image 中卸载特定的 PC 驱动
3. 通过设置 PC 启动到 OOBE，交付给 CX
4. 允许将 Answer File(unattend)settings 应用到现有安装中

Item	Log Path
Generalize 可移除 PC 特有信息如 Driver 和 SID	%WINDIR%\SYSTEM32\SYSPREP\PANTHER
Specialize	%WINDIR%\PANTHER
Unattended Windows Setup action(OOBE)	%WINDIR%\PANTHER\UnattendGC

14 How to rollback after upgrade has been done? What are included in windows.old? usage? Remaining period?

System setting – recovery – go back to Windows，旧的已安装的程序和设置的数据，保留旧系统的文件方便退回。Windows.old 文件夹 30 天后自动删除

15 Preparation before Win11 Upgrade?

硬件，设置 Microsoft Account 以传输文件和收藏夹，备份

16 Upgrade rollback scenarios and what's error details, key words, logs to check.

Sources\Panther\Setupact.log

Sources\Rollback\Setupact.log

检查数据备份并根据错误代码检查是否存在已知问题，更新 Windows, 以便安装所有可用的建议更新。

卸载第三方防病毒软件及任何不需要的软件，移除非基本外部硬件，检查并建议在系统制造商网站上安装更新的固件和驱动程序。