Sylvia Q

1. Types and differences of Update? Difference about security only/monthly roll up/CU.

Feature update:6月一次，每年3月和9月发布，仅适用Win10

Quality update:

Security Monthly Quality Rollup：2016年10月起微软每月发布一次累计更新，会把之前的所有的更新都集中起来到一起

Security-Only Update(2012R2,Win 7)：仅仅是当月的安全更新，体积较小

Preview of Monthly Rollup(Optional)：预览版，下一个月更新，可供用户选择安装

Cumulative update：累积更新是包含以前发布的更新的更新，它就像捆绑在一起的多个简单更新。

1. How to install update(dism/standalone/wsus etc)?

DISM:

Expand -f:\* C:\Temp\.... .msu C:\Temp;解压到C盘Temp文件夹

DISM /Online /Add-package /Packagepath:C:\Temp\..... .cab安装更新

DISM /Online /Get-PackageInfo /PackageName:<Package Identity>查看更新

DISM /Online /RemovePackage /PackageName:<Package Identity>卸载更新

Standalone

下载.msu文件安装Windows Update Standalone Installer按步骤安装

Wsus

指定Intranet Microsoft 更新服务位置，集中式自动化式更新管理

集中管理更新，可以更新一些长期没网隔离的计算机，只要WSUS主机有网就行。

1. 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chang 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)

1. Component states during installation?

Absent, Resolved, Staged, Installed.

1. 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

1. 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

重启：6005，6006，1074意外重启6008

Eventlog服务开启（开机）6005

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, UpdateSessionOrchestration.etl,Notification UxBroker.elt, CBS.log

checkSUR.log (SUR: System Update Readiness)

Location: C:%SYSTEMROOT%\logs\cbs

1. 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

1. 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

1. 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

1. How to check path level. How to check installed patches.

查看最新补丁

Winver或者hotfix

UI,dism

1. 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
3. 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。

1. 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. SSV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。

1. Update log
2. Component State corruption? Command/ tool 检查？失败日志？
3. Component store related registry location?

HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\CBS

1. 控制Windows Update behavior 的policy？
2. 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)