注册表

注册表保存到XXX目录

Win键+R: 调起运行窗口, 输入regedit

ľ	International and the second se Second second s	×
	Windows 将根据你所输入的名称,为你打开相应的程序、 文件夹、文档或 Internet 资源。	
	打开(<u>O</u>): regedit	~
	♥ 使用管理权限创建此任务。	
	确定 取消 浏览(<u>B</u>)	

右键导出所需要的键

➡ 注册表编辑器 文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H) 🗸 💻 计算机 HKEY_CLASSES_ROOT HKEY_CURRENT LICED 展开 > HKEY_LOCAL 新建(N) > > HKEY_USERS 查找(F)... > HKEY_CURREN 删除(D) 重命名(R) 导出(E) 权限(P)... 复制项名称(C)

截图示例:

🔬 wangguan.reg 属性 🛛 🕹 🗙						
常规 安全						
*	wangguan.reg					
文件类型:	注册表项 (.reg)					
打开方式:	1 注册表编辑器	更改(<u>C</u>)				
位置:	C:\inetpub	,				
大小:	5.68 MB (5,958,728 字节)					
占用空间:	5.68 MB (5,959,680 字节)					
创建时间:	2023年8月12日,9:19:43					
修改时间:	2023年8月12日,9:19:44					

本地策略

密码策略

Windows菜单——Windows管理工具——本地安全策略

或者

Win键+R:调起运行窗口,输入gpedit.msc



截图示例:

密码必须符合复杂性要求 属性

本地安全设置 说明
密码必须符合复杂性要求
● 已启用(E)
○ 已禁用(S)

账户锁定策略

文件(F) 操作(A) 查看(V) 帮助(H)						
🗇 🄿 🙋 📅 🗙 🖾 😼 🛛 🖬						
」 本地计算机 策略	▲ 策略 ^	安全设置				
✔ 👰 计算机配置	圆 帐户锁定时间	60 分钟				
> 🧰 软件设置		5 次无效登录				
✔ 🧰 Windows 设置	重置帐户锁定计数器	15 分钟之后				
> 🧮 域名解析策略						
🖹 脚本(启动/关机)						
> 🖶 已部署的打印机						
✔ 🚹 安全设置						
∨ 📴 帐户策略						
> 📴 密码策略						
> 📴 帐户锁定策略						



🧾 本地组策略编辑器			-	□ ×
文件(F) 操作(A) 查看(V) 帮助(H)				
🗢 🔿 🙍 📷 🗙 🗟 🚺 🖬				
📓 本地计算机 策略 🔷	策略 ^		安全设置	
✔ 擾 计算机配置	圆 审核策略更改		无审核	
	圆 审核登录事件		无审核	
✓ Windows 设直	圆 审核对象访问		无审核	
□ 烟本(启动/关机)	圖 审核进程跟踪		无审核	
> 扁 已部署的打印机	◎ □○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○		无审核	
▶ 🔓 安全设置	し、 軍核特权使用 の ・ ・ ・ ・		无审核	
> 🔀 帐户策略			大甲核	
∨ 📴 本地策略			元甲核	
> 强 审核策略			九甲核	
> 4 女主远视				
审核登录事件 属性	?	×		
本地安全设置 说明				
审核登录事件				
审核这些操作:				
☑成功(S)				
同生際の				

Part2

安全选项

帐户: 重命名来宾帐户 属性	?	×
本地安全设置 说明		
帐户: 重命名来宾帐户		
Guest]



2024/10/16 19:00		Part2		
关闭系统 属性			?	×
本地安全设置	说明			
×	闭系统			
Administrate Backup Ope WIN-TJA6L0	ors erators)KI6TE\manager			

防火墙策略

← → ~ ↑ 🔗 > 控制面板 > 系統	統和安全 → Windows 防火墙 → 允许的应用				√ Ö	搜索控制面板	Q
	允许应用通过 Windows 防火墙进行通信 若要添加、更改或删除所允许的应用和端口,请单击"更改设置"。				_		
	允许应用进行通信有哪些风险?		●更	改设置(N	1)		
	允许的应用和功能(A):						
	名称		专用	公用 ^			
	☑ 文件和打印机共享						
	□性能日志和警报						
	□虚拟机监控						
	□远程服务管理						
	□远程关机						
	□远程计划任务管理						
	☑远程卷管理						
	□远程事件监视器						
	□远程事件日志管理						
	☑ 远程桌面		◄				
		详细信息(L)	Ħ	】除(M)			
		4	~ 甘仲	立田(B)			
			AT SHIELD	<u>w</u> /m(i/)			
		72.00		HINS Y			

IIS

Windows管理工具——IIS管理器

服务器管理器

÷	E) 🔽 管理(M) <u>工具(T)</u> 视图(V) 帮助(H)
		DHCP
		DNS
		Internet Information Services (IIS) 6.0 管理器
		Internet Information Services (IIS)管理器
		iSCSI 发起程序
		Microsoft Azure 服务

端口配置

Na Internet Information Services (IIS)管理器 -	
← → ● → WIN-TJA6LOKI6TE → 网站 → Default Web Site → □	🕺 🟠 🔞 ·
文件(F) 视图(V) 報助(H)	
● Default Web Site 主页 ● Default Web Site 主页 ● ● ● <td< th=""><th>) </th></td<>)
就结	e ₁₁

目录浏览







错误页面

Internet Information Services (IIS)	5)管理器	
WIN-TJA6LOKI	5TE 🕨 网站 🕨 Defa	ult Web Site 🔸
文件(F) 视图(V) 帮助(H)		
主接 え・ □ 2 0 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		P 错误响应。错误响应可以是自定义错误页,也可以是包含故障排除信息的详细错误消息。
✓ · <mark>⑥</mark> 网站 ● Oefault Web Site	状态代码 ¹ 401	路径 %SystemDrive%\inetpub\custerr\ <language-t< th=""></language-t<>
> 😻 ftptest	403 404 405 406 412	%SystemDrive%\inetpub\custerr\ <language-tag>\403.htm %SystemDrive%\inetpub\custerr\<language-tag>\404.htm %SystemDrive%\inetpub\custerr\<language-tag>\405.htm %SystemDrive%\inetpub\custerr\<language-tag>\406.htm</language-tag></language-tag></language-tag></language-tag>
	500 501 502	%SystemDrive%\inetpub\custerr\ <language-tag>\500.htm %SystemDrive%\inetpub\custerr\<language-tag>\501.htm %SystemDrive%\inetpub\custerr\<language-tag>\502.htm</language-tag></language-tag></language-tag>

响应标头

000				
100 million	Internet	Information	Comison	
	Internet	information	Services	1113/BJ#68



日志滚动

W3C 日志记录字段	? ×
标准字段(S):	
☐ 接收的字节数(cs-bytes)	^
☑ 所用时间(time-taken)	
□ 协议版本(cs-version)	
□ 主机(cs-host)	
☑ 用户代理(cs(User-Agent))	
🗹 Cookie (cs(Cookie))	
☑ 引用网站(cs(Referer))	×

Internet Information Services (I	IS)管理器
← → WIN-TJA6L0KI	6TE → 网站 → Default Web Site →
文件(F) 视图(V) 帮助(H)	
连接 ▲	 ● 仅日志文件(L) ● 仅日志文件(L) ● 仅日志文件(A)
	日志文件滾动更新 洗掻 IIS 用来创建新的日志文件的方法. ● 计划(C): 毎小时 ✓ ● 取入文(+大小(チャ)(Z): ● 不创建新的日志文件(N) ■ 使用本地时间进行文件命名和滾动更新(U)
< >>	III 功能视图 III 内容视图

FTP

查看自己IP地址的方法:

Win键+R:调起运行窗口,输入cmd,然后在cmd当中输入ipconfig,查看10.3.4.xx的地址



•		
状态	类型	
已启用	内置	
已禁用	内置	
	已启用 已禁用	已启用 内置 已禁用 内置

请求筛选

	STP 🕽	青求筛选			
N-TJ	使用此功能可配置	FTP 服务的	筛选规则。		
	▶ 又件扩展者	◎◎◎ 隐藏段	ー ② 拒绝的 URL 序列	🎽 命令	
	文件扩展名	允许			
e	.bak	False]		
	.txt	True			

授权规则

Information Services (IIS)管埋器



地址限制

分组依据:不过	,添加拒绝限制规则	?	×
模式 ^	 拒绝访问以下 IP 地址或域名: ● 特定 IP 地址(S): 192.168.100.100 ○ IP 地址范围(R): 掩码(M): Ĺ 		





SMTP





首先需要开启SMTP服务器(可能会有卡死的情况,等卡死重新开启一次即可)

然后cmd输入telnet 10.3.4.x 25

🔤 管理员: C:\Windows\system32\cmd.exe



输入EHLO来检测当前SMTP服务器是否正常,输入ehlo server也有类似效果。



日志记录

右键SMTP服务器的属性,进行日志记录的配置

▲ Internet Information Services (IIS) 6.0 管理器

Part2

	文件(F)	操作(A)	查看(V)	窗口(W)	帮助(H)	
þ	۵ 🏟	TT E	0	?)⊧ ,∎ ,H	
h	Internet	Informatio	on Service	es	名称	COLUMN AND AND A

Internet Information Services 名称 WIN-TJA6L0KI6TE(本地计算机) 条 4	۲ ۲	[SMTP \	Virtual Se	erver #1] 属性			?	×
✓ [SMTP Virtual Server #1] 後域 ① 当前会话	w. 当前会	常规 デ テ WIN-T IP 地 (所有 正限 连接	访问 皖定的域名 JA6L0K16 止(P): 未分配) 制连接数: 御时(分钟)	邮件 3: TE 不超过(L) (0):	传递):	LDAP 路由	安全 ▼	高级(V) 10	
			启用日志 动日志格- 3C 扩展日 确定	记录(E)- ぜ∩)- 志文件析	計	应用(A	- 	属性(R) 帮助	

限制连接数

🐚 Internet Information Services (IIS) 6.0 管理器



限制邮件大小

🚺 Internet Information Services (IIS) 6.0	管理器	
🧐 文件(F) 操作(A) 查看(V) 窗口(W)	帮助(H)	
🗢 🌩 🙇 📊 🗐 🧕 🕞 🛛 🗊) ■ п	
 Internet Information Services WIN-TJA6L0KI6TE(本地计算机) 	名称	[SMTP Virtual Server #1] 属性
✓ SMTP Virtual Server #1]	≫ ^攻 ☑ 当前会	常规 访问 邮件 传递 LDAP
◎ ◎		请指定下列邮件传递信息。
		☑ 限制邮件大小不超过(KB)(L):
		☑ 限制会话大小不超过(KB) (S):
		☑ 限制每个连接的邮件数不超过(M):

名称	[SMTP Virtual Server #1] 届性 ? ×	
後域	常规 访问 邮件 传递 LDAP 路由 安全	
	市流 水川 火星 LOR Hall 火里 请指定下列邮件传递信息。 ✓ 限制邮件大小不超过(KB) (L): 10240 ✓ 限制每行连接的邮件数不超过(M): 10240 ✓ 限制每个连接的邮件数不超过(M): 20 ✓ 限制每封邮件的收件人数不超过(N): 100 将未送达报告的副本发送到(D): 工	
	C:\inetpub\mailroot\Badmail 测览(W) 确定 取消 应用(A) 帮助	

别名域



Part2

11 Internet Information Services (IIS) 6.0	管理器	
	帮助(H)	
🗢 🔿 🙋 📷 🗙 🖼 🙆 🛃 🖬		
Internet Information Services	域名	类型
✓ 劉 WIN-TJA6L0KI6TE(本地计算机)	🕾 WIN-TJA6L0KI6TE	本地(默认)
✓ (SMTP Virtual Server #1]	😵 wangluoanquan	本地(别名)

排除地址



DHCP





Part2

🕎 DHCP	
文件(F) 操作(A) 查看(V) 帮助(H)	新建作用域向导
	IP 地址范围 你通过确定一组连续的 IP 地址来定义作用域地址范围。
V iii win-tjabl0kibte	DHCP 服务器的配置设置
> 100 作用域 [192.168.95.0] dhcptest ● 服务器选项	输入此作用域分配的地址范围。
 □ 策略 > 觉 筛选器 	起始 IP 地址(S): 192 . 168 . 6 . 10
✓ Ⅰ IPv6 IB 服务器选项	结束 IP 地址(E): 192 . 168 . 6 . 250
	传播到 DHCP 客户端的配置设置
	长度(L): 24 ÷
	子网掩码(U): 255 . 255 . 0
	< 上一步(B) 下一步(N) > 取消

地址排除



Part2

🔷 🖄 📰 🙆 🚔 📔 📆 米			
DHCP	起始 IP 地址 \$□ 192.168.6.10 № 192.168.6.100 添加排除	结束 IP 地址 192.168.6.250 192.168.6.110	描述 地址分发范围 分发中不包括的 IP 地址 ? X
 □ 17/7342090 □ 第略 > □ 作用域 [192.168.95.0] dhcptest □ 服务器选项 □ 第略 > ☑ 筛选器 □ 介许 ∞ 介许 ∞ 指绝 ▼ IPv6 □ 服务器选项 	键入要排除的 IP 地中键入地址。 起始 IP 地址(S): 结束 IP 地址(E):	3地范围。如果要排除单个地 192 . 168 . 6 . 2 192 . 168 . 6 . 2 派	地,只需在"起始 IP 地址" 200 220 如(A) 关闭(C)

拒绝MAC地址

9 DHCP		
文件(F) 操作(A) 查看(V) 帮助(H)		
🗢 🌩 🛛 🚈 🗖 🗖 🔂 🕞 🖉 📻		
P DHCP	MAC 地址 描述	
 ✓ iii win-tja6l0ki6te ✓ iiii IPv4 > iiiiiiii 作用域 [192.168.6.0] 0812test 		这里没有任何项目。
> 📷 作用或 [192.108.95.0] dhcptest	新建筛选器	×
 □ 策略 ✓ <	提供不接收 DHCP 服务	的客户端的 MAC 地址。
○ 允许 送 拒绝	MAC 地址: f1-22	2-51-a2-3c-1f
📑 服务器选项	描述:	
		添加(A) 清除(E) 关闭(C)

允许MAC地址

文件(F) 操作(A) 查看(V) 帮助(H) ■ 🔿 📝 🔯 📴 🔀 📴		
Ž DHCP ✓] win-tja6l0ki6te ✓] IPv4 → ☐ 作用域 [192.168.6.0] 0812test	MAC 地址	描述这里没有任何项目。
 冷 作用域 [192.168.95.0] dhcptest 湯 服务器选项 ③ 策略 ⑦ 筛选器 ⑥ 允许 ※ 拒绝 	新建筛选器 提供将接收 DH MAC 地址:	XHCP 服务的客户端的 MAC 地址。
✓ Ⅰ IPv6 Ⅰ 服务器选项	描述:	添加(A) 清除(E) 关闭(C)

主机名称

		服务器洗项	?	×
文件(F) 操作(A) 查看(V) 帮助(H)			-	
🗢 🔿 📩 💽 🙆 🔢 📷 🗳		常规 高级		
 ◆ ● ② DHCP > ● ○ Win-tja6l0ki6te > ● ○ IPv4 > ● ○ 作用域 [192.168.6.0] 0812test ● ●<td> ・服务器选项是 DH</td><td>常规 高级 可用选项 □ 010 Impress 服务器 □ 011 後期位置限各案 □ 012 主机名称 □ 013 后动文件入小 □ 014 现场转储文件 □ 015 DNIC 结欠 < 文据项 字符串值(S): 网络</td><td>描述 Imagen Impress 服务器阵列 会优先顺度批列的子网上的 PF(客户端的主机名称,RFC 1035 后动映像文件的入小,以 5127 故障转储文件的路径名称 客户端部长的 DNIC 结合称</td><td>- - -</td>	 ・服务器选项是 DH	常规 高级 可用选项 □ 010 Impress 服务器 □ 011 後期位置限各案 □ 012 主机名称 □ 013 后动文件入小 □ 014 现场转储文件 □ 015 DNIC 结欠 < 文据项 字符串值(S): 网络	描述 Imagen Impress 服务器阵列 会优先顺度批列的子网上的 PF(客户端的主机名称,RFC 1035 后动映像文件的入小,以 5127 故障转储文件的路径名称 客户端部长的 DNIC 结合称	- - -

保留地址

• 🔿 🔁 📰 🗙 🗐 🙆 🗟 🗊 🦑			
DHCP	选项名	供应商	值
win-tja6l0ki6te	006 DNS 服务器	标准	223
✓ → IPv4	☐ 012 主机名称	标准	网络
✓ / 作用域 [192.168.6.0] 0812test			
✔ 📓 保留			
192.168.6.123] 123321			
作用域选项			
◎ 策略			
》 作用域 [192.168.95.0] dhcptest 3 肥久哭洗面			
·····································			
▶ 🖉 筛选器			
🔀 允许			
2 拒绝			
1000 服务稽达坝			
光神/见 留	2 ¥		
加建床曲			
为保留客户端输入信息。			
保留名称(R):			
192 . 168 . 6 . 122			
MAC ###H/M). 11-22-cc-33-44-55			
THAC SUST (IN).			
描述(E):			
描述(E):			
描述(E): ○ 西考(B)			
描述(E): -支持的类型 ○ 两者(B)			
描述(E): -支持的类型 (两者(B) C DHCP(D)			
描述(E): -支持的类型 ○ 两者(B) ○ DHCP(D) ○ BOOTP(O)			

DNS





培和 Internet → 网	🏺 以太网 2 状态	Q 以太网 2 居住	Internet 协议版本 4 (TCP/IPv4) 属性	×
着基本网络信息	常规	网络 共享	常规	
看活动网络		法按时使用.		
网络2 公用网络	连接 IPv4 连接: IPv6 连接: 无网络议	Realtek RTL8139C+ Fast Ethernet NIC	如果网络支持此功能,则可以获取自动指派的 IP 设置。否则,你需要从网络系统管理员处获得适当的 IP 设置。	
未识别的网络 公用网络 改网络设置 议置新的连续 设置宽带、到 议置宽带、到	煤体状态: 持续时间:	此连接使用下列项目(O):	 ● 自动获得 IP 地址(O) ● 使用下面的 IP 地址(S): IP 地址(I): ID · 3 · 4 · 42 子树掩码(U): 空55 · 255 · 252 · 0 默认网关(D): ID · 3 · 7 · 251 ● 自动获得 DNS 服务器地址(B) ● 使用下面的 DNS 服务器地址(E): 10.3.4.42 道选 DNS 服务器(P): 223 · 5 · 5 · 5 	
	字节: 30,558,994 178,	描述	备用 DNS 服务器(A):	
	◎属性(P) ◎禁用(D) 诊断(G)	传输控制协议/internet 协议,该协议是默认的广域网络 于在不同的相互连接的网络上通信。	□ 退出时验证设置(L)	
		确定	确定 取消	



刷新dns



hello world

反向区域

要标识反向查找	沤域,请键入网	网络 ID 或区域名称。	
● 网络 ID(E): 10 .3	.4 .		
网络记是	出了该区域 IP ;	也址的部分。用正常(2	下是反向的)顺序输入网络
如果在网络 10.in-addr	ID 中使用了一 .arpa 区域,网	个零 , 它会出现在区均 络 ID 10.0 会创建 0.	或名称中。例如,网络 II 10.in-addr.arpa 区域。
○反向查找区域	或名称(V):		
4.3.10.in-a	ddr.arpa		
a DNS 管理器			- 0
文件(F) 操作(A) 查看(V) 帮助	I(H) ■ == ■ == =■		
 ▲ ● ● ● ■ ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ●	名称 (与父文件夹相同) (与父文件夹相同)	类型 起始授权机构(SOA) 名称服务器(NS)	数据 [1], win-tja6l0ki6te., hos win-tja6l0ki6te.
 ◎ baidu.com ✓ ○ 反向查找区域 ◎ 4.3.10.in-addr.arpa > ○ 信仕京 > ○ 条件转发器) (更新服务器数据文件(U)	
/ <u> </u>		新建别名(CNAME)(A) 新建委派(G) 其他新记录(C) DNSSEC(D)	>

建资源记录		Part2	
		×	<
指针(PTR)			
主机 IP 地址(P):			
10.3.4.42			
完全限定的域名(FQDN)(F):			
42.4.3.10.in-addr.arpa			
主机名(H):			
wlaq.baidu.com		浏览(B)	
JDNS 管理器 ζ(件(F) 操作(A) 查看(V) 報問 ■ ● 2 〒 X III X III Q III	b(H)		
DNS	名称	类型 起始塔权机构(SOA)	数据
 ▼ 🚰 正向查找区域		包約服务器(N3)	win-gaolokiote.
 iii) zero.com iii) baidu.com iiii) 反向查找区域 iiiii) 4.3.10.in-addr.arpa iiii) 信任点 iii) 条件转发器 	10.3.4.42	指针(PTR)	wlaq.baidu.com
:\Users\Administrato 务器: UnKnown	m≻nslookup 10.3.4	4 . 42	
ldress: 10.3.4.42			
idress: 10.3.4.42 ⇔ UnKnown 找不到 10).3.4.42: Non-exis	stent domain	
idress: 10.3.4.42 ☞ UnKnown 找不到 10 \Users\Administrato 务器: wlaq.baidu.c Idress: 10.3.4.42).3.4.42: Non-exis pr>nslookup 10.3.4 com	stent domain 4.42	

 \times

2024/10/16) 19:00 1十(1) 漢(1-(4) 三相(1)	(II)(H447	Part2
	🔿 🖄 📰 🔛	ì 🔒 🛛 🖬 🕴 🗐 鬝	
े जिवस् र	DNS WIN-TJA6LOKI6TE Cip查找区域 Cip查找区域 Cip查找区域 Cip查找区域 Cip查找区域 Cip值任点	名称 配置 DNS 服务器(C) 新建区域(Z) 为所有区域设置老化/清理(S) 清除过时资源记录(N) 更新服务器数据文件(U) 清除缓存(E)	
	> 🔛 条件转发器	启动 nslookup (A) 所有任务(K) 查看(V)	>
		删除(D) 刷新(F) 导出列表(L)	
		雇性(R) 帮助(H)	

WIN-TJ	A6L0KI6T	E属性					?	×
接口	转发器	高级	根提示	调试日志	事件日志	盆视		
DNS 这个f	事件日志(1息用于分	保留 DNS	S服务器) 韵性能。	遇到的错误 、	警告和其他	也事件的记	录。你可]将
将下列	刘事件记录	到日志:						
〇没	有事件(N))						
O見	是错误(O))						
〇错	吴和警告(E)						
● 所有	有事件(V)							

监视

16 19:00							Part2	
WIN-TJA	A6L0KI6T	E属性					?	×
接口	转发器	高级	根提示	调试日志	事件日志	监视		
要验证	E服务器的	配置,你	可以进行	手动或自动	测试。			
选择一	一个测试类	型:						
□对□	比 DNS 服	资器的 简	前单查询(N	VI)				
☑刘	比 DNS 服	资器的 道	迴口查询((C)				
要立即	进行测试	, 请单击	"立即测试	đ"。			立即测试(T)
回以	下列间隔进	进行自动测	则试(P):]				
测	试间隔(E)):	30 5	4 (~			
测试结	ŧ果(S):							
日期		时间		简单查	询	递归查道	0	

调试日志

WIN-TJA6L0KI6TE 属性	? ×
接口 转发器 高级 根提示 调试日志 事件日志 监视	
为了帮助调试,你可以记录由 DNS 服务器发送和接收到一个日志 包。在默认情况下,调试日志为禁用的。	文件的数据
☑ 调试日志数据包(L)	
数据包方向: ☑ 传出(O) ☑ 传入(I)	至少选择— 个
数据包内容: 数据包类型: ☑ 查询/传送(Q)	至少选择—— 个
□ 通知(N)	
 □ 记录不匹配的传入响应数据包(G) ☑ 详细信息(D) ☑ 用 IP 地址筛选数据包(C) 篇选(F) 	
日志文件	
文件路径和名称(H):	
最大值(字节)(M): 50000000	
确定 取消 应用(A)	帮助

刷新间隔

	baidu.com 雇性	? ×
홃 DNS 管理器	常规 起始授权机构(SOA) 名称服务器 WINS 区域传送	
文件(F) 操作(A) 查看(V) 帮助(H)	序列号(S):	
a DNS 名称	1	增量(N)
✓ WIN-TJA6LOKI6TE ✓ □ 正向直找区域	主服务器(P):	
この この この この この この に の 、 に の 、 、 、 、 、 、 、 、 、 、 、 、 、	win-tja6l0ki6te.	浏览(B)
i baidu.com ✓ ○ 反向音找区域	负责人(R):	
🛐 4.3.10.in-addr.arpa	hostmaster.	浏览(O)
> 🛄 信任点 > 🛗 条件转发器	刷新间隔(E): 15 分钟 >	1
	最小(默认) TTL(M): 1 小时 ~	
	此记录的 TTL(T): 0 :1 :0 :0 (DDDDD	D:HH.MM.SS)
< >>		
	确定 取消 应用(A)	帮助

自动清理

WIN-TJA6L0KI6TE 属性			?	X
接口 转发器 高级 根提示	调试日志 事件日志	5 监视		
服务器版本号(S):				
10.0 14393 (0x3839)				
服务器选项(V):				
□禁用递归(也禁用转发器) □启用 BIND 辅助区域 □如果区域数据不正确,加载会失	败			
 ☑ 启用循环 ☑ 启用// Ⅲ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □				
凶保护缓存防止污染				
名称检查(N):	多字节(UTF8)			~
启动时加载区域数据(L):	从 Active Directo	ry 和注册表		~
☑ 启用过时记录自动清理(E)				٦
清理周期(C):	15	天		~
L		王王 王		۲
		里直内默	MIE(K)	

backup



备份、恢复



		^	操作	F	
		r	-		
		L	10	备份计划	
		Π	1	一次性备份	
以保护你的数据。	v l		1	恢复	
图 首切计划问号	*		<u> </u>	配置性能设置	
				查看	
省田 指定备份时	司		2	帮助	
开始	你希望以什么频率及何时运行备份?				
选择备份配置	● 每日一次(O)				
指定备份时间	选择时间(E): 21:00 ~				
指守目标兼刑	○ 每日多次(M)				
THE REPORT	单击可用的时间,然后单击"添加"将其添加到备份计划。				
如此人	可用时间: 计划时间:				
摘要	0:00				
	0:30				
	1:30				
	2:00				
	2:30 3:00 < 删除(R)				
	3:30				
	4:00				
	< 上一步(P) 下一步(N) > 完成F) 取満				
		_			
- 小村客心向	3				\sim
一人任用仍问	7				\sim
	40.416				
「 首	份进度				
友 /八注1百					
田切処坝	状念: 口元成。				
边拴首份配直					
	业大洋细信自				
远择要备份的项					
指定目标迷刑					
HALL WEEK	备份位置: F:				
<u>洪汉矣八日</u> 七					
加手用仍且你	传输的数据: 1 KB				
确认					
	火日				
备份进度		-	_		
	近日 米本 传输的数据				
	新加密(E:) 口元成。 1 KB/1 KB				

2024/10/16 19:00 恢复向导	Part2			×
开始 选择备份日期 选择恢复类型 选择要恢复的项目 指定恢复选项 确认	文件恢复进度: 状态: 已完成。 恢复详细信息(R): 项目	状态 B完成。 行。若要查看J 聪息。	传输的数据 1 KB/1 KB	

备份方式

				-	
				本地	的合分
				1	备份计划
				1	一次性备份
				20	抗复
🐌 优化备份性能		×	_		配置性能设置
如果备份包含整卷,则可以通过	选择下列设置之一管理以后的	性能。如果备		-	旦君
份似包含系统状态、又件或又件;	夹,则不适用这些设 <u>盂</u> 。			?	帮助
○ 普通會衍性胞(M) 创建各份的时间与更各份的粉	据大小成正比。				
	THE CLIMENT OF A				
④ 快速電历性能(2) 通过只跟踪上次备份和当前备	份之间的更改来提高备份速度	5。这可能会			
降低备份中包含的卷上的磁盘	春旺量。对于执行密集使用品	產操作的服			
回走X(0) 如果你拥有某些密集使用磁盘	;操作的卷,则分别配置每个卷	ž.			
卷	 备份选项				
系统保留	完整备份	~			
新加卷(F:)	完整备份	~			
本地磁盘(C:)	完整备份	~			
新加卷(E:)	完整备份 惯用备份				
	DEE HID				
	确定(0)	取消(C)			



CMD添加用户、用户组、修改密码、删除用户

C:\Users\Administrator>net user hzwg /add 命令成功完成。	添加用户hzwg
C:\Users\Administrator>net user hzwg 123456 命令成功完成。	修改hzwg的密码为123456
C:\Users\Administrator>net localgroup zhangzhou /add 命令成功完成。	添加用户组zhangzhou
C:\Users\Administrator>net localgroup zhangzhou hzwg 命令成功完成。	^{/add} 将hzwg添加到zhangzhou组
C:\Users\Administrator>net user hzwg /de1 🛛 🛗 命令成功完成。	除hzwg
C:\Users\Administrator>net localgroup zhangzhou /del 命令成功完成。	删除zhangzhou组

Ð C:\Users\Administrator> net user hzwg /add 1 2 命令成功完成。 3 4 5 C:\Users\Administrator> net user hzwg 123456 命令成功完成。 6 7 8 9 C:\Users\Administrator> net localgroup zhangzhou /add 命令成功完成。 10 11 12 C:\Users\Administrator> net localgroup zhangzhou hzwg /add 13 命令成功完成。 14 15 16 C:\Users\Administrator> net user hzwg /del 17 命令成功完成。 18 19 20 C:\Users\Administrator> net localgroup zhangzhou /del 21 22 命令成功完成。

用户文件权限、高级权限



全					
对象名称: (C:\ <mark>ftpsite</mark>				
组或用户名(G):					
CREATOR ON	WNER				
SYSTEM					
62 Administrate		OKIETE A	i i i di p	tors)	
👗 manager (W	N-TJA6L0KI6	TE\manager)			
Latin.					
Cocis (Will	DHOLOKIOTE	03013)			
Coers (Wile	DAGEORIOTE	Users)			
Users (WIN-	DAGEORIOTE	(Jacia)		10/20/00	
Users (WIII	DAOLOKIOTE	Users) 添加(D)		删除(R	()
manager 的权限(Users) 添加(D). 允	····	删除(R 拒绝	2)
manager 的权限(完全控制		(Jsers) 添加(D)。 允	···) 许	删除(R 拒绝	R)
manager 的权限(完全控制 修改	P)	(Users) 添加(D)。 允 []	···· 许 乙	删除(R 拒绝	2)
manager 的权限(完全控制 修改 读取和执行	P)	(Users) 添加(D) 允 〔	···· 许 乙 乙	删除(R 拒绝	()
manager 的权限(完全控制 修改 读取和执行 列出文件夹内容	P)	(Users) 添加(D). 允 [[[[[[[[[[[[[[[[[[···· 许 乙 乙 乙 乙	删除(R 拒绝 □ □	2)
manager 的权限(完全控制 修改 读取和执行 列出文件夹内容 读取	P)	(Users) 添加(D)。 允 〔 〔 〔 〔	···· 许 乙 乙 乙 乙 乙 乙 乙 乙	删除(R 拒绝 □ □	2)

×

		and a second		
ftpsite 的权限				
全				
动色夕彩.	Cliffondito			
AJ BRID PIN	Calipsite			
组或用户名(G):				
	OWNER			
SYSTEM				
STR A desired	OMINE TIAG	OKIETE A Jaciaint	ators)	
a manager (V	WIN-TJA6L0KI61	ΓE∖manager)		
amanager (V	WIN-TJA6L0KI61	FE∖manager) Jsers)		
a manager (V	WIN-TJA6L0KI6T	FE\manager) Users)		
a manager (V		(FE\manager)		
a manager (V		FE\manager) Jsers) 添加(D)	删除(R))
& manager (With Costra (With C		FE\manager) Jsers) 添加(D) 允许	删除(R) 拒绝)
A manager (With Costra (With C		FE\manager) Jsers) 添加(D) 允许	删除(R) 拒绝)
a manager (Wind Oscis (Wind Scars (Wind S		FE\manager) Jsers) 添加(D) 允许 ビ	删除(R) 拒绝)
a manager (Wind Users (Wind See 2000) manager 的权限 完全控制 修改 读取和执行		FE\manager) Ssers) 添加(D) 允许 ビ ビ	删除(R) 拒绝 □)
a manager (With Users (With See 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		FE\manager) SSETS) 添加(D) 允许 ビ ビ ビ	删除(R) 拒绝)
a manager (W Users (Wh Users (Wh Us	WIN-TJA6L0KI6T	FE\manager) SSETS) 添加(D) 允许 ビ ビ ビ ビ	删除(R) 拒绝 □ □)

ftpsite的電缆安全设置	×	
名称 C:\ftpsite 所有者: Administrators (WIN-TJA6L0KI6TE\Administrators)		
权限 审核 有效访问 如需其他信息,请双击权限项目。若要修改权限项目,请选择该项目并单击	Tipsite 部的制度	
収得条目: 使型 主体 访问 建 介许 Guests (WIN-TJAGLOKIGTE)Guests: 講家 2. 今许 manager OMIN TJAGLOKIGTE)の 学会計算	关型: 允许 > 应用于: 此文件类、子文件类和文件 >	
CFL Transaction (VIII-T AROLDADD EVITAL PLEIZER) FL 2014 FL 2014 FL 2014 FL 2014 Administrators (WIN-TJA6LOKI6TL. 先金控制 Administrators (WIN-TJA6LOKI6TE)Users) 逐隊視退行 法許 Users (WIN-TJA6LOKI6TE)Users) 逐隊視退行 法律 CREATOR OWNER 完全控制	 ・	
添加(D) 删除(P) 續欄(E) 算用證承(I) 〕使用可从此对象理承的权限项目替换所有子对象的权限项目(P)		

安装补丁

	最佳匹配	
ធ	Microsoft Azure 服务 桌面应用	
	服务器管理器 桌面应用	
	应用 >	
	🔍 服务	
	>>> 组件服务	
	设置	
	● 更改手动代理服务器设置	
	🗟 查看本地服务	
	🔁 配置代理服务器	
ŝ		
	服务	
	오 따 🤶 🥽 🖶	

	🔍 服务					-	- 🗆	×
_	文件(F) 操作(A) 重	查看(V) 帮助(H)						
_	() () () () () () () () () () () () () () 🗟 👔 📷 🕨 🔳 II ID						
	服务(本地)	0 服务(本地)						
		Windows Update	名称	描述	状态	启动类型	登录为	^
			Windows Font Cache Ser	通过	正在	自动	本地服务	
		描述:	🍓 Windows Image Acquisiti	为扫		手动	本地服务	
			Windows Installer	添加		手动	本地系统	
		用,这台计算机的用户将无法使用	Windows Management I	提供	正在	自动	本地系统	
		Windows 更新或其自动更新功能,	🖏 Windows Modules Install	启用		手动	本地系统	
		并且这些程序将无法使用 Windows	Windows Process Activati	Win	正在	手动	本地系统	
		更新代埋(WUA) API。	Windows Remote Manag	Win	正在	自动	网络服务	
			Windows Search	为文		禁用	本地系统	
			in windows Time	AR IN	正左	白土水油牛牛	大地印度	- L
			🦓 Windows Update	启用		禁用	本地系统	
		-	WINDOWS JELZIEALSHOURS	140/08	11.11	E AU	44403330	•
SI			Windows 推送通知用户服	此服		手动	本地系统	
			Windows 许可证管理器服务	为 W		手动(触发	本地服务	
			Q Windows 移动热点服务	提供		手动(触发	本地服务	
			🥋 Windows 预览体验服务	wisvc		手动	本地系统	
			WinHTTP Web Proxy Aut	Win	正在	手动	本地服务	- 6
			Wired AutoConfig	有线		手动	本地系统	
			WMI Performance Adapt	向网		手动	本地系统	
			Workstation	使用	正在	自动	网络服务	
			low World Wide Web 坐在肥友	(第)计	正左	ê əh	大吉公公	

取消禁用, 启动服务, 然后再安装更新包

Windows Search	为文		禁用	本地系统
🔍 Windows Time	维护	正在	自动(触发	本地服务
🎕 Windows Update 🛛 🥐			-	本地系统
🥋 Windows 推送通知系统服 B	启	动(S)		本地系统
🤐 Windows 推送通知用户服	停	止(0)		本地系统
Windows 许可证管理器服务	暂	停(U)		本地服务
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	恢	包(M)		

Part2 🚯 下载并安装更新 X 安装完成 关闭 🛐 程序 ~ (← 控制面板主页 程序和功能 0 卸载程序 | 🗣 启用或关闭 Windows 功能 | 查看已安装的更新 | 系统和安全 运行为以前版本的 Windows 编写的程序 | 如何安装程序 网络和 Internet 默认程序 硬件 更改媒体或设备的默认设置 / 始终使用指定的程序打开某种文件类型 / 设置默认程序 程序 用户帐户 外观和个性化 时钟、语言和区域 轻松使用 👒 已安装更新 \times → 🗸 🔷 🐝 > 控制面板 > 程序 > 程序和功能 > 已安装更新 ✓ X 搜索"已安装更新" P \leftarrow 控制面板主页 卸载更新 卸载程序 若要卸载更新,请从列表中将其选中,然后单击"卸载"或"更改"。 👎 启用或关闭 Windows 功能 = - ? 组织 -名称 程序 版本 发布者 安装时间 Microsoft Windows (3) ■ 用于 Microsoft Windows 的 安全更新(KB5016058) Microsoft Windows

Microsoft Windows

Microsoft Windows



用于 Microsoft Windows 的 安全更新(KB4048953)

用于 Microsoft Windows 的 更新(KB4049065)

2024/9/2

2018/2/3

2018/2/3

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

2024/10/16 19:00

115			
∎→ 此	电脑 > 新加卷 (E:)		✓ ひ 搜索"新
^	名称 ^	修改日期	类型 大小
	Poetry.txt	2022/6/21 10:37	文本文档 1 KB
×	Torttut	2022/8/3 15:26	文本文档 1 KB
*	share	2023/8/12 14:14	文件 ³ share 属性
×			
×			常规
			- the second s
.,			· · · · · · · · · · · · · · · · · · ·
			网络路径(N): 不共享
			共享(S)
			设置自定义权限,创建多个共享,并设置其他高级共享选项。
			♥ 高级共享(D)
;)			
D:)			- 密码保护
×			没有此计算机的用户帐户和密码的用户可以访问与所有人共享的
个坝日			
		44-43	
	Everyone		シ 法加(Δ)
	Administrator		7000H(N)
	Guest		
	quest003		-
	hacker		
	manager		
	Everyone		
	创建新用户		

文件隐藏、只读

0/10 19.00		Failz
I guest 属性		×
常规 共享	安全 以前的版本 自定义	
	guest	
类型:	文件夹	
位置:	E:\share	
大小:	0 字节	
占用空间:	0 字节	
包含:	0个文件,0个文件夹	
创建时间:	2023年8月12日,14:18:39	
属性:	属性: ✓ 只读(仅应用于文件夹中的文件)(R)	
	□隐藏(H) 高级(D)	
 qqq 属性 常规 共享 	安全 以前的版本 自定义	×
	999	
类型:	文件夹	
位置:	E:\	
大小:	0 字节	
占用空间:	0 字节	
包含:	0 个文件, 0 个文件夹	
创建时间:	2023年8月12日,14:30:39	
雇性:	 ■ 只读(仅应用于文件夹中的文件)(R) ☑ 隐藏(H) 高级(D) 	

火绒信任区、压缩包扫描、系统加固

💋 信任区					\times
以下文件已经被信任,	已被认为是安全的;如果发生误报,您也可以在此加入信任	£	文件	网址]
路径		~ 类型		Q	
C:\Users\Administr	ator\Desktop\whitelist\	文件夹			
🕖 设置			$\overline{\bigtriangledown}$		\times
 ⁽²⁾ 常规设置 基础设置 <u>查杀设置</u> 软件升级 ① 病毒防护 铅 系统防护 ① 网络防护 	全盘查杀配置 ✓ 深度查杀压缩包中的木马病毒,并跳过大于 10 MI 仅扫描 ∨ 指定扩展名文件 例知: exe;doct 月描网络驱动器 病毒处理方式 ● 询问我 自动处理	B的压缩包(20M-9999M :txt;.zip)		

火绒扫描

病毒类型

🤊 火鐵安全	病毒查杀		5 II _ >
	见险项目1个,建议立即处理	ŧ	部忽略立即处理
☑ 风险项目			状态
C:\tools\安全自热 ✓ 代码混淆器 Viri	🔿 风险详情	×	待处理 详情
	病毒类型: 代码混淆器 (VirTool/Obfuscator.fq)		
	病毒描述:通过代码变形、反跟踪、反虚拟机等技术手段,专门被病毒 安全软件进行技术对抗的恶意代码类型。	用来与	
	风险路径:C:\tools\安全自检工具.exe		
	处理建议: 立即处理		
	打开文件路径 信任文	(4	



MD5计算

C:\tools>certuti1 -hashfile 安全自检工具.exe md5 MD5 哈希(文件 安全自检工具.exe): 99342a4b5ce806ef4ab2a6d89ba8e99e CertUti1: -hashfile 命令成功完成。

certutil -hashfile 文件名 md5