应急响应模块 说明手册

一、背景信息

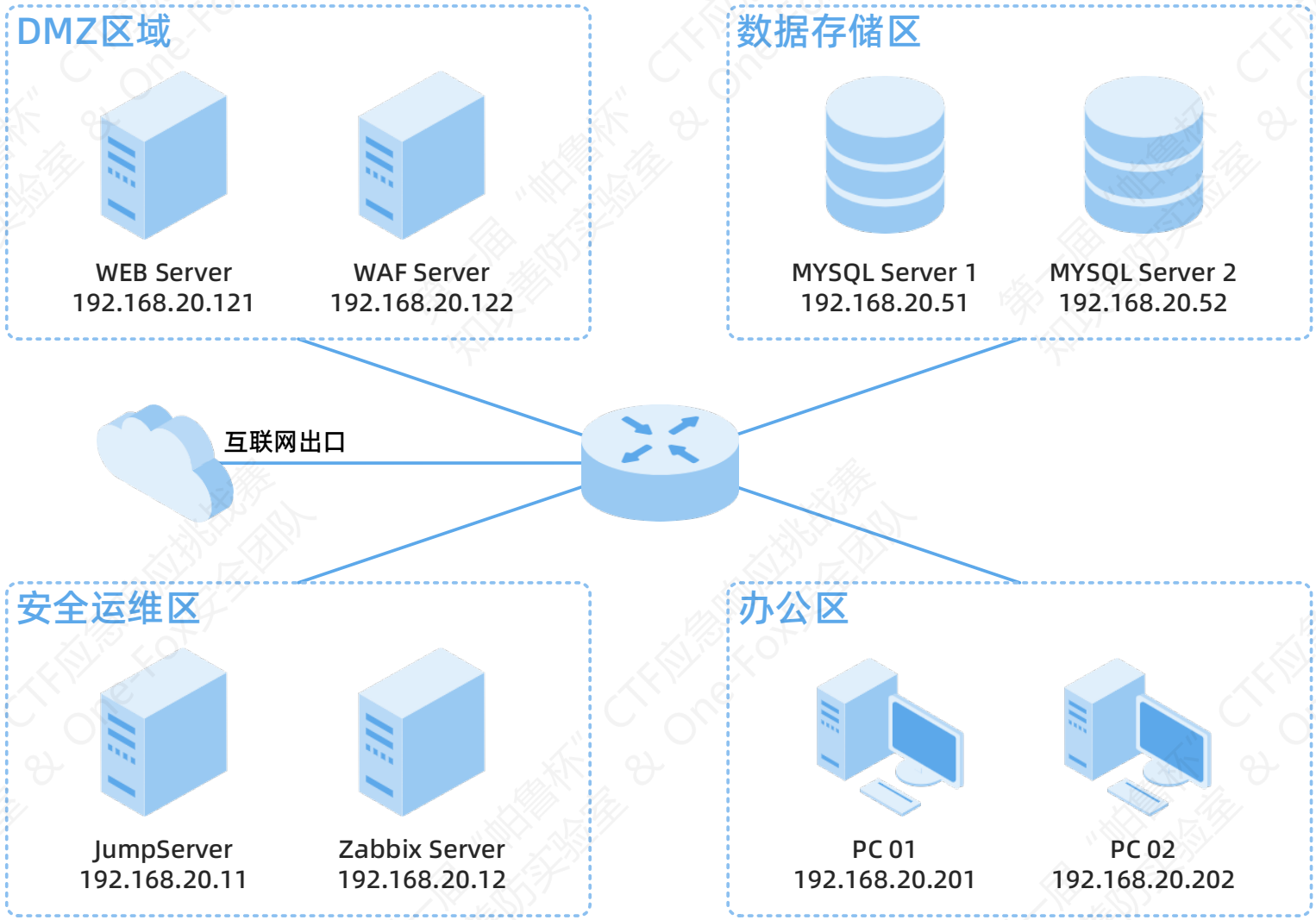
在这个跳跃的数字舞台上，数据安全成了政企单位稳航的重要压舱石。某政企单位，作为一艘驶向未来的巨轮，对数据的把控丝毫不敢松懈。眼下，我们即将启航一场无与伦比的探险——“信息安全探索之旅”。

这趟旅程的目的是遍访我们的信息系统每一个角落，探寻隐藏在暗处的风险海怪，提升船员们对数据宝藏的守护意识，确保我们的珍贵资讯宝藏不被外界窥见，不受损害，随时准备发挥其价值。在这场航旅中，某政企单位期望锻造一副更加坚不可摧的数据防护铠甲，增强面对意外风暴的航行能力。

你和你的团队，作为这次探险的领航员，将借助先进的应急响应罗盘，对我们的内部信息航道进行全域的安全梳理。从网络的海洋到系统的天空，从数据库的深渊到应用的岛屿，无一处不在你们的巡航范围之内。我们将特别防范那些潜伏的数据海盗——数据泄露、非法入侵、恶意攻击，以及物联网设备安全上的狂风骤雨。

让我们携手共航，把这次“信息安全探索之旅”变成一个传奇，确保我们的信息系统像最强大的舰队领航者一样，勇敢、可靠、无所畏惧。向着更安全的港湾，全速前进！

二、网络拓扑


DMZ区域
WEB Server
192.168.20.121
WAF Server
192.168.20.122
数据存储区
MYSQL Server 1
192.168.20.51
MYSQL Server 2
192.168.20.52
互联网出口
安全运维区
JumpServer
192.168.20.11
Zabbix Server
192.168.20.12
办公区
PC 01
192.168.20.201
PC 02
192.168.20.202

三、资产清单

区域	主机名	IP 地址	系统登录信息	服务登录信息
DMZ 区	WEB Server	192.168.20.121	未知	未知
	WAF Server	192.168.20.123	home/home1234!!!	https://192.168.20.123:9443/ admin/mQzm7LqF
安全运维区	JumpServer	192.168.20.11	home/home1234!!!	http://192.168.20.123:8080 admin/Network@2020
	Zabbix Server	192.168.20.12	home/home1234!!!	未知
数据存储区	MYSQL Server 1	192.168.20.51	mysql/mysql1234!!!	root/mysql1234
	MYSQL Server 2	192.168.20.52	mysql/mysql1234!!!	root/mysql1234
办公区	PC01	192.168.20.201	Administrator/Network@2020	未知
	PC02	192.168.20.202	Administrator/Network@2020	此靶机为"近源"对应靶机

四、答题说明

1.应急响应模块采用本地解题，线上提交的答题模式。

2.根据答题平台中应急响应题目的题目要求，在本地进行解题，获取到 flag 后，提交到答题平台。

3.CTF 模块与急响应模块都需提交 Writeup，请各参赛选手以战队为单位，在竞赛结束后 6 小时内在答题平台提交。

五、注意事项

1.应急响应环境为本地环境，需要提前在网盘进行下载。

2.本地环境的压缩包密码将会在开赛前一小时公布，选手需提前部署环境。

3.应急响应环境占用空间较大，需要为存放环境的目录至少预留 100G 的磁盘空间。

4.应急响应环境需要同时开启 8 台虚拟机，占用配置较高，推荐电脑配置至少 8 核 16G。

5.禁止在竞赛过程中对提供的账户密码进行修改，以免造成服务不可用。

6.推荐在环境部署完毕的情况下创建一次快照，出现意外可立即恢复快照以节省时间。

7.目前已知 PC01 和 PC01 两台 Windows 虚拟机网卡没有设置自动连接，需要在虚拟机设置中打开 nat 网卡的自动连接后再启动虚拟机。

六、部署流程

（一）安装 Vmware 虚拟机（如已安装可跳过）

1. 从以下链接 https://www.vmware.com/go/getworkstation-win 下载 VMware Workstation 17。
2. 按照安装提示安装 VMware Workstation。

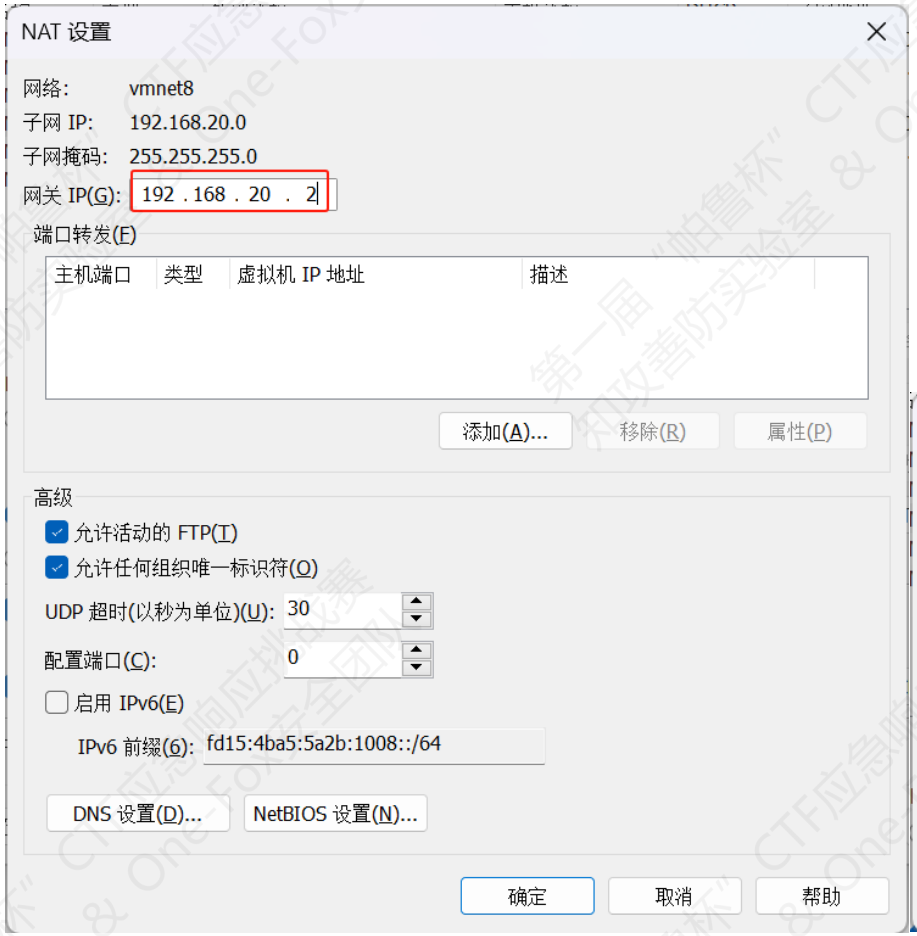
（二）虚拟机网络配置

1. 在 VMware 主界面右上角点击“编辑”，打开“虚拟网络编辑器”。

2. 在打开的界面中点击“更改设置”。

3. 选中“虚拟网络编辑器”中的 NAT 模式网卡，修改下方的子网 IP 和子网掩码。

4. 按照下方图片修改 NAT 模式网卡的“NAT 设置”和“DHCP 设置”。



5. 修改完成后点击“虚拟网络编辑器” 下方的确定完成网络配置。

（三）导入虚拟机

[提供 ovf 和 vmx 两种导入虚拟机的方式，可自行选择喜欢的方式导入，仅需下载一种方式的压缩包，使用一种方式部署即可]

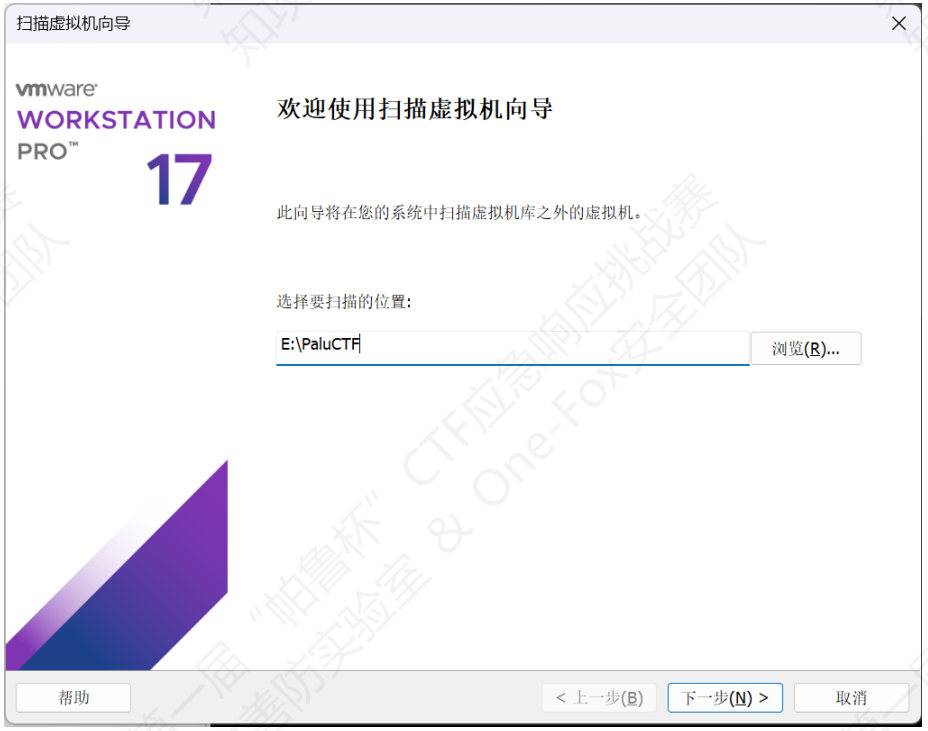
导入 vmx 虚拟机

1. 选择 vmx 格式的压缩包进行下载，下载完成后根据公布的压缩包密码进行解压，并将解压出来的所有虚拟机放置在同一目录中。

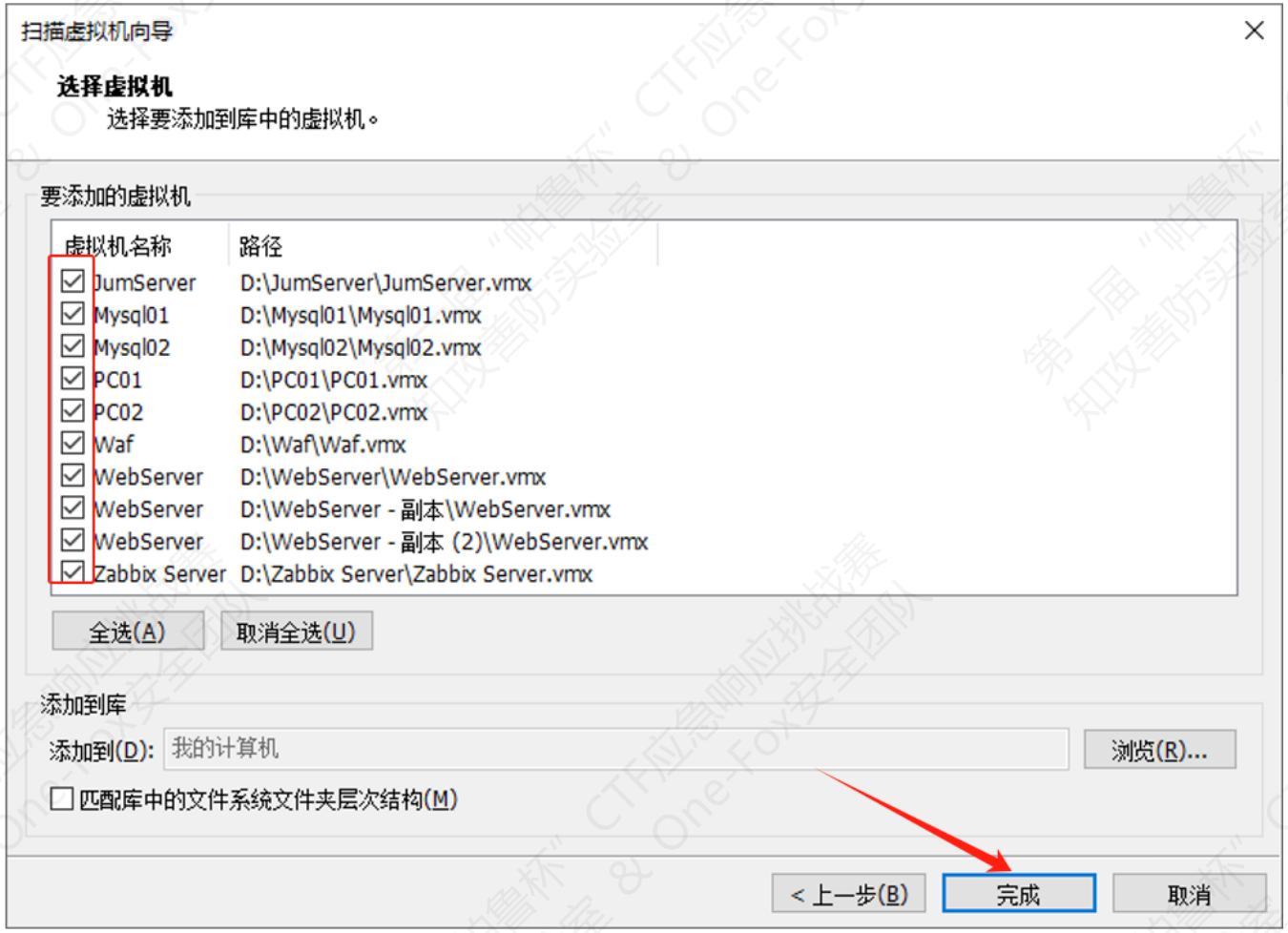
名称	修改日期	类型	大小
PC02.zip	2024/4/17 17:50	ZIP 文件	11,776,10...
JumServer.zip	2024/4/17 17:44	ZIP 文件	11,246,12...
Mysql01.zip	2024/4/17 17:36	ZIP 文件	1,673,476...
Mysql02.zip	2024/4/17 17:35	ZIP 文件	1,523,877...
Waf.zip	2024/4/17 17:33	ZIP 文件	2,085,996...
WebServer.zip	2024/4/17 17:31	ZIP 文件	3,250,763...
Zabbix Server.zip	2024/4/17 17:29	ZIP 文件	1,063,973...
JumServer	2024/4/17 18:58	文件夹	
PC01	2024/4/17 18:58	文件夹	
PC02	2024/4/17 18:58	文件夹	
Mysql01	2024/4/17 18:56	文件夹	
Mysql02	2024/4/17 18:56	文件夹	
WebServer	2024/4/17 18:56	文件夹	
Waf	2024/4/17 18:56	文件夹	
Zabbix Server	2024/4/17 18:55	文件夹	
vm	2024/4/17 18:54	文件夹	

2. 点击虚拟机主页面右上角“文件”，点击扫描虚拟机。

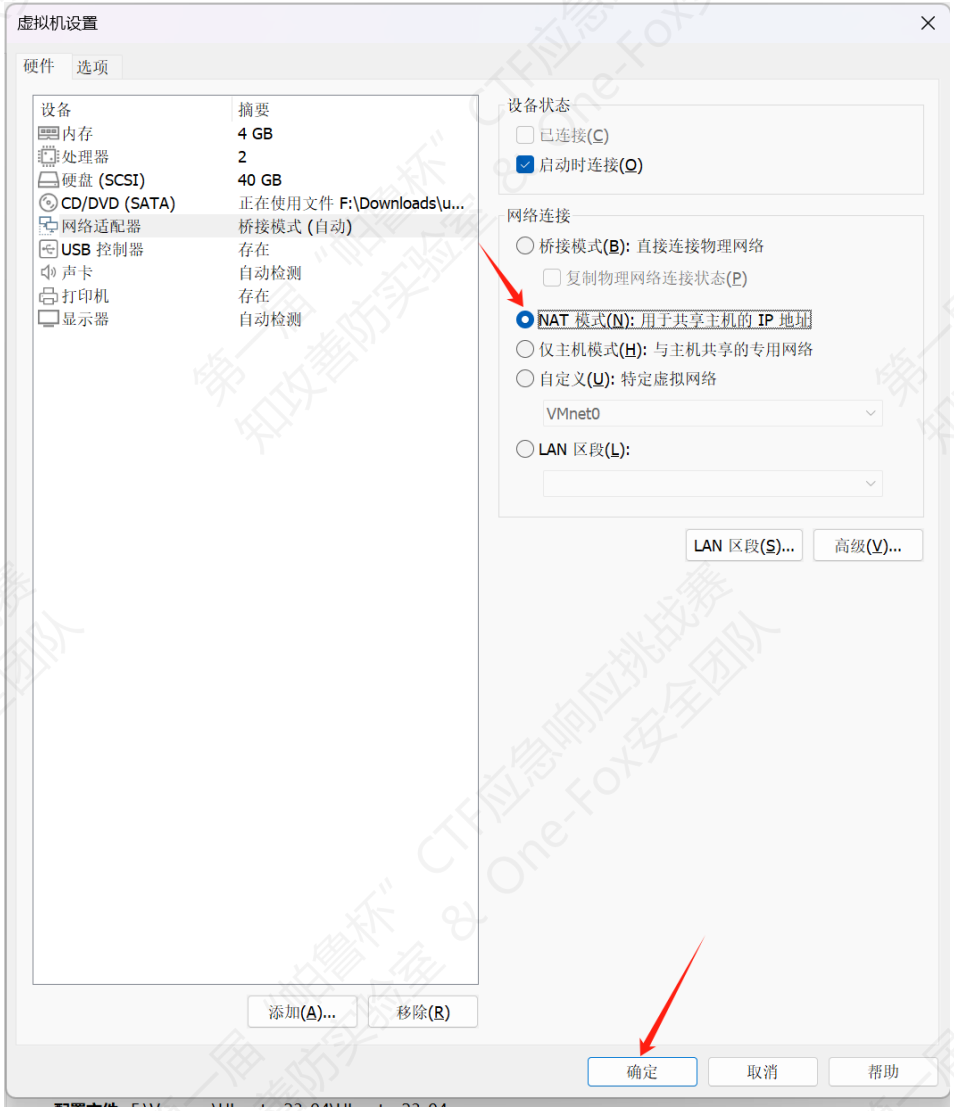
3. 在“扫描的位置”处选择解压出来的虚拟机文件目录。



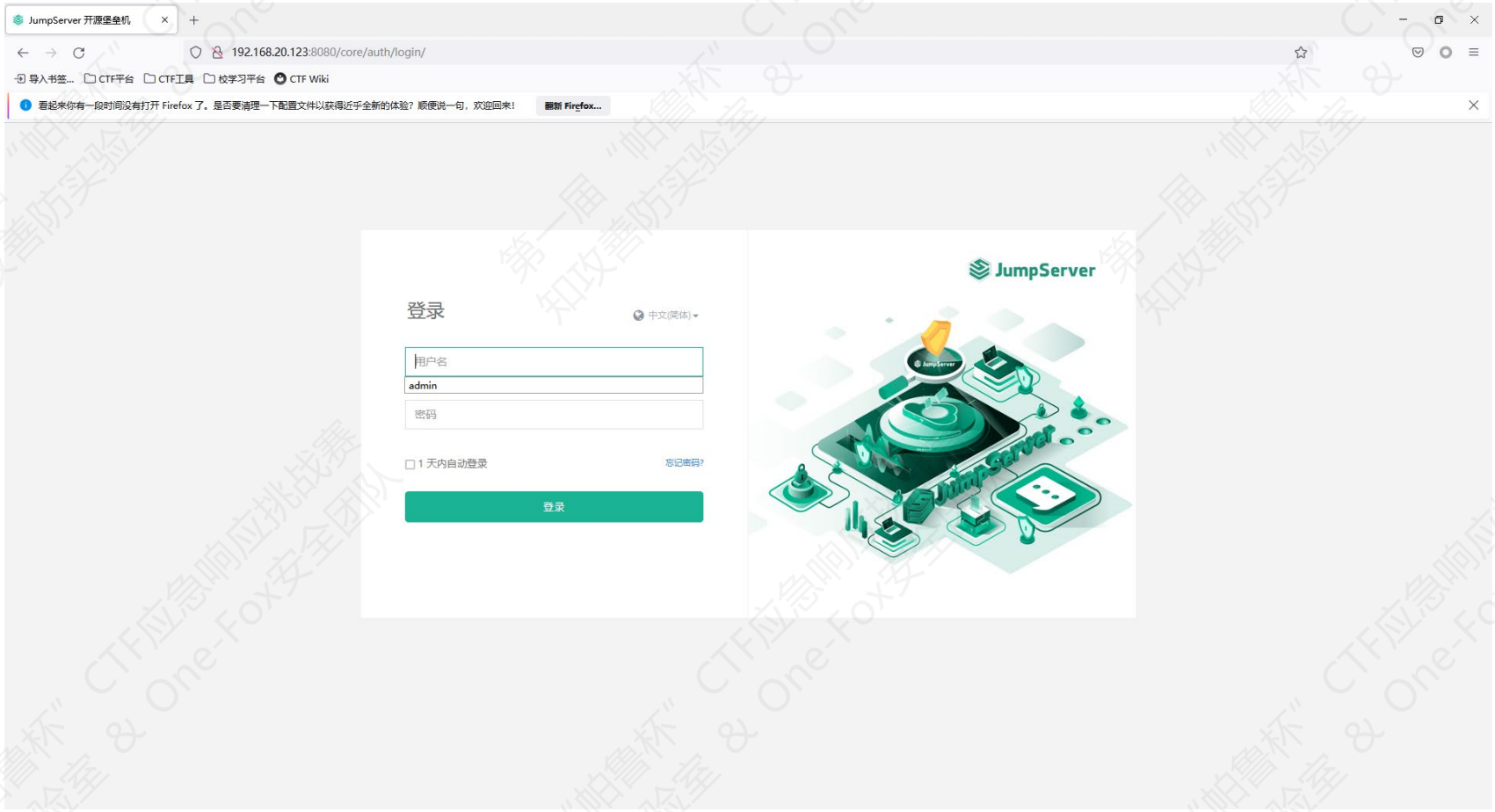
4. 点击下一步，在之后的界面选定环境所需要的 8 台虚拟机，点击完成创建。



5. 确保虚拟机设置当中网卡选择 NAT 模式，完成修改。

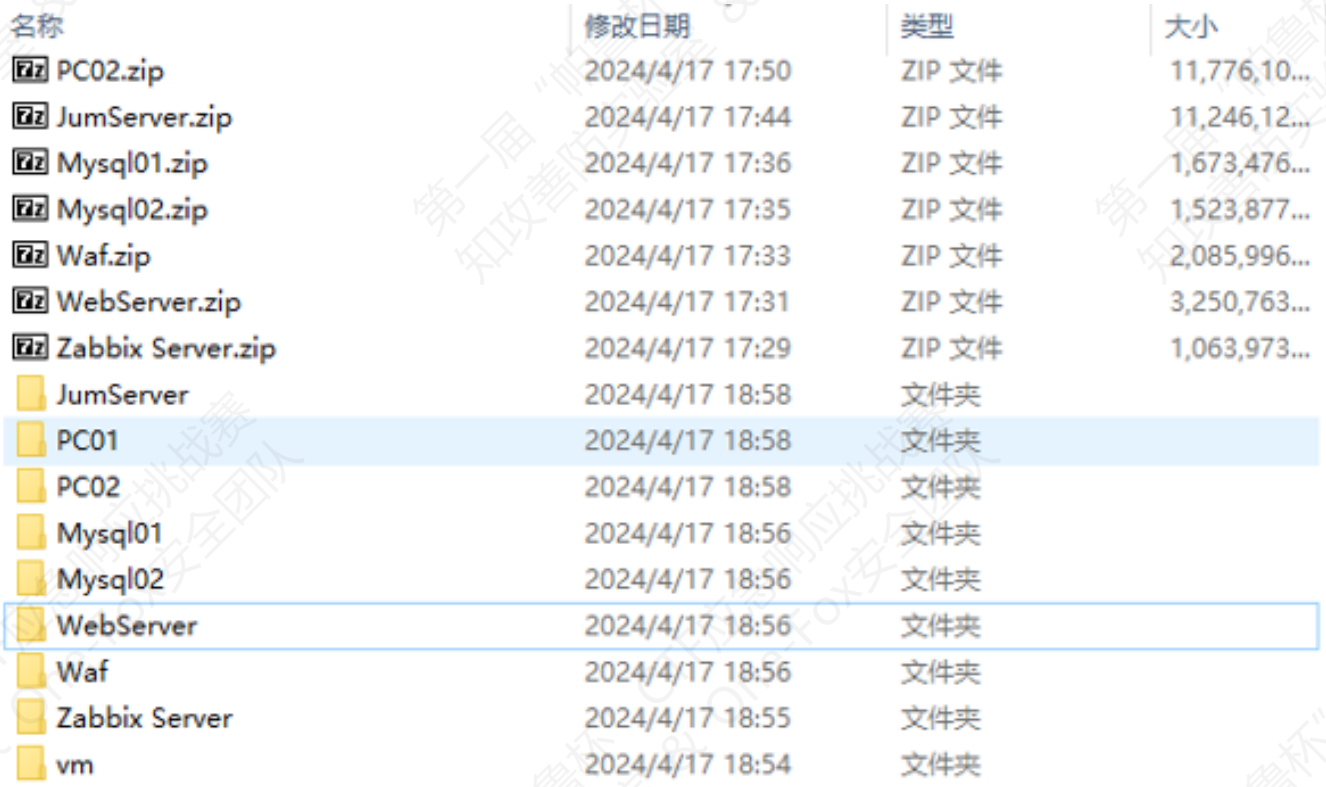


6. 启动环境中所需的全部虚拟机，测试连通性正常后完成配置。



导入 ovf 虚拟机

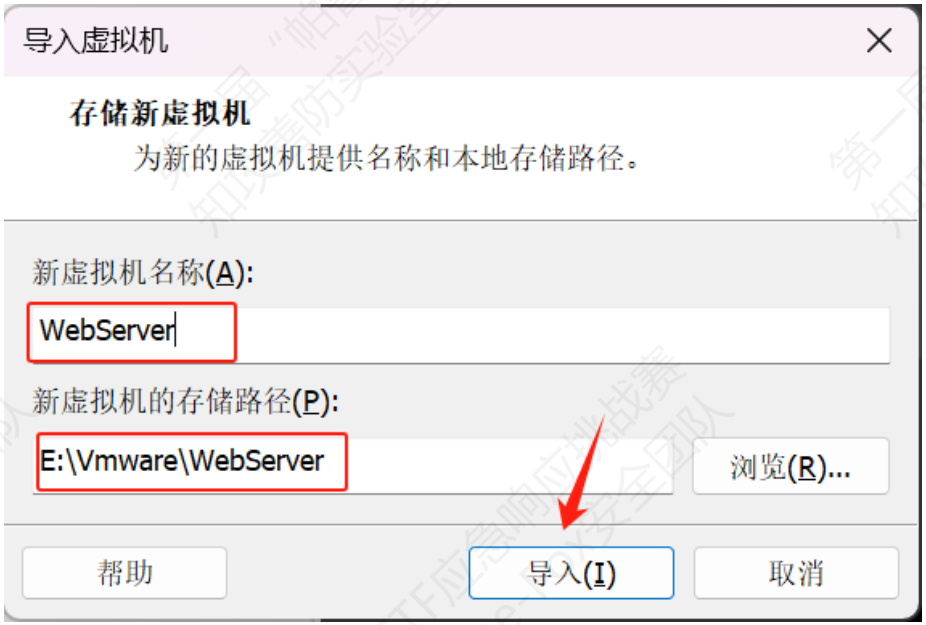
1. 选择 ovf 格式的环境压缩包进行下载，下载完成后根据公布的压缩包密码解压，将解压出来的所有虚拟机放置在同一目录中。



名称	修改日期	类型	大小
PC02.zip	2024/4/17 17:50	ZIP 文件	11,776,10...
JumServer.zip	2024/4/17 17:44	ZIP 文件	11,246,12...
Mysql01.zip	2024/4/17 17:36	ZIP 文件	1,673,476...
Mysql02.zip	2024/4/17 17:35	ZIP 文件	1,523,877...
Waf.zip	2024/4/17 17:33	ZIP 文件	2,085,996...
WebServer.zip	2024/4/17 17:31	ZIP 文件	3,250,763...
Zabbix Server.zip	2024/4/17 17:29	ZIP 文件	1,063,973...
JumServer	2024/4/17 18:58	文件夹	
PC01	2024/4/17 18:58	文件夹	
PC02	2024/4/17 18:58	文件夹	
Mysql01	2024/4/17 18:56	文件夹	
Mysql02	2024/4/17 18:56	文件夹	
WebServer	2024/4/17 18:56	文件夹	
Waf	2024/4/17 18:56	文件夹	
Zabbix Server	2024/4/17 18:55	文件夹	
vm	2024/4/17 18:54	文件夹	

2. 选择每台虚拟机目录中的.ovf 文件，双击或者拖入 Vmware 虚拟机中，出现“导入虚拟机”界面。

3. 在打开的“导入虚拟机”中输入正确的主机名，选择空间充足的存储路径，点击 “导入”完成导入操作。



4. 按照步骤 3 的方法，把环境中提供的 8 个虚拟机文件都进行导入。

5. 确保虚拟机设置当中网卡选择 NAT 模式，完成修改。

6. 启动环境中所需的全部虚拟机，测试连通性正常后完成配置。