

## 《网络系统管理与维护》

### 单选 (266) —

- 1.0 常见的备份工具有 ( )。-->[Ghost](#)
2. AH 的 IP 协议号为 ( )，提供数据的完整性 (MD5、SHA-1) 和数据源身份验证，但是不能提供数据保密性功能，所有数据均以明文进行传输。-->[A. 51](#)
3. CA 默认会每隔 ( ) 天自动发布一次 CRL。-->[7](#)
4. CA 默认会每隔 ( ) 天自动发布一次增量 CRL。-->[1](#)
5. CRL 是如下 ( ) 功能的英文缩写。-->[证书吊销列表](#)
6. DNS 服务器中的 ( ) 记录表示一条邮件交换记录。-->[MX](#)
7. DNS 服务器中的 ( ) 记录表示一条主机记录。-->[A](#)
8. FTP 授权规则设置中，可以特殊指定 ( ) 访问站点内容-->[所有用户、所有匿名用户、指定的角色或用户组、指定的用户](#)
9. FTP 在 Internet 中的作用是 ( ) -->[用来传送文件的一种服务](#)
10. FTP 在 Internet 中的作用是 ( )。-->[用来传送文件的一种服务](#)
11. HTTP 协议的端口号是 ( ) -->[80](#)
12. IIS 在一台计算机上可以通过如下哪些方式同时建立多个网站 ( )。-->[使用主机头名称来建立多个网站、使用多个 IP 地址建立多个网站、使用 TCP 连接端口来创建多个网站](#)
13. IIS 中无法对 FTP 站点执行 ( ) 操作。-->[挂起](#)
14. IIS 中无法对网站执行 ( ) 操作。-->[挂起](#)
15. IMAP4 协议的端口号是 ( )。-->[143](#)
16. IPsec 是开放标准的一个框架，包括两个主要协议：( )。-->[AH、ESP](#)
17. IPsec 有两种工作模式：( ) 模式和隧道模式。-->[C. 传输](#)

18. ISO 的网络安全体系结构中定义了五类安全服务：鉴别服务、访问控制服务、( )、数据完整性服务、抗抵赖性服务。-->[数据保密性服务](#)
19. MD5 在本质上是简单的二进制操作 (如异或运算) 的一个复杂序列，被用于在输入数据上执行，生成一个 ( ) 位的报文摘要值。-->[B. 128](#)
20. NetFlow 通过将数据包中的多个关键字段相结合来定义一个“流”，最初定义了 ( ) 个关键字段。-->[C. 七](#)
21. Netscape 公司推出了一个名为 ( ) 的传输层安全协议，用以保障在 Internet 上数据传输的安全。-->[D. SSL](#)
22. PKI 提供的安全服务包括 ( )。-->[信息保密、身份验证、抗否认、完整性控制](#)
23. POP3 (PostOfficeProtocol-Version3，邮局协议版本 3) 在使用 TLS 保护后，被称为 ( )。-->[A. POP3S](#)
24. POP3 协议的端口号是 ( )。-->[110](#)
25. PPP 身份验证方法包括 ( )。-->[PAP、CHAP](#)
26. PPP 协议使用 LCP 来建立和维护数据链路连接。借助 ( ) 在同一条点到点连接上使用多种网络层协议。-->[C. NCP](#)
27. RAID1+0-->[. PFX](#)
28. RAID1、RAID5、RAID1+0-->[. PFX](#)
29. RSA 密钥的长度可以是：( )。-->[512 位、1024 位、2048 位](#)
30. SHA-1) 和数据源身份验证，但是不能提供数据保密性功能，所有数据均以明文进行传输。-->[A. 51](#)
31. SMTP 服务器出站安全设置中，支持的身份验证包括 ( )。-->[匿名访问、基本身份验证、集成 Windows 身份验证](#)
32. SMTP 服务器默认连接超时设置为 ( ) 分钟。-->[10](#)
33. SMTP 服务器默认限制连接数不超过 ( )。-->[100](#)
34. SMTP 协议的端口号是 ( )。-->[25](#)
35. SNMP 报文主要包括：( ) 报文、GetNextRequest 报文、SetRequest 报文、GetResponse 报文和 Trap 报文。-->[D. GetRequest](#)
36. SNMP 管理系统通常由 SNMP 管理站、SNMP 代理和 ( ) 组成。-->[C. 管理信息库 \(MIB\)](#)
37. SNMP 协议提供了三类操作，包括：Get、Set 和 ( )。-->[D. Trap](#)
38. SO 的网络安全体系结构中定义了五类安全服务，包括：认证服务、访问控制服务、数据完整性服务、抗抵赖性服务和 ( )。-->[数据保密性服务](#)
39. TCP 连接的建立与断开采用 ( ) 的方式。-->[B. “三次握手+四次断开”](#)
40. Windows 备份工具支持的备份类型主要有：( ) 备份、差别备份、增量备份、每日备份等。-->[正常](#)
41. Windows 备份工具支持的备份类型主要有：正常备份、( ) 备份、增量备份、每日备份等。-->[A. 差别](#)
42. Windows 操作系统内置的 Users 组帐户的成员属于 ( ) 帐户。-->[B. 标准帐户](#)
43. Windows 操作系统内置的 ( ) 组帐户的成员就属于标准帐户。-->[Users](#)
44. Windows 操作系统中的密码必须符合复杂性要求，定义的帐户密码至少有 ( ) 个字符的长度。-->[C. 6](#)
45. Windows 系统内置的 ( ) 用户帐户属于管理员帐户。-->[A. Administrator](#)

46. Windows 系统内置的 ( ) 用户帐户属于管理员帐户。-->[Administrator](#)
47. ( ) FTP 为已在 FTP 服务器上建立了特定帐号的用户使用，必须以用户名和密码登录。-->[用户](#)
48. ( ) 安全是指对信息在数据处理、存储、传输、显示等使用过程中的保护，主要关注的是数据信息本身的安全，保障数据依据授权使用，而不会被窃取、篡改、冒充、抵赖。其主要涉及数据的保密性、完整性、真实性、不可抵赖性等。-->[B. 数据层](#)
49. ( ) 病毒是一种寄生在磁盘引导区的计算机病毒，它用病毒的全部或部分取代正常的引导记录，而将正常的引导记录隐藏在磁盘的其它地方-->[A. 引导型](#)
50. ( ) 的计费是根据用户在一段时间内所使用的全部网络流量 (发送和接收) 统计数据来收取用户费用的一种计费方式。-->[D. 基于网络流量](#)
51. ( ) 负责向被管理对象发出管理操作指令，并接收来自代理的通告信息。-->[A. 管理站](#)
52. ( ) 函数被设计用来验证和确保数据完整性。-->[C. 密码散列](#)
53. ( ) 会向网络中发送特定的探测数据包，网络系统管理员通过对探测数据包所受网络影响而发生特性变化的分析，得到网络状态和性能参数。-->[B. 主动测量](#)
54. ( ) 可实现用户访问 SMTP 服务器，不需要提供用户名和密码。-->[匿名访问](#)
55. ( ) 可实现用户访问 SMTP 服务器，需要提供用户名和密码，而且密码会被加密。-->[集成 Windows 身份验证](#)
56. ( ) 可实现用户访问 SMTP 服务器，需要提供用户名和密码，而且密码是以不加密的明文方式来发送。-->[基本身份验证](#)
57. ( ) 可以通过软件或硬件来实现，它把存储的文件切成小块，再比较每个小块的区别，然后对重复的数据块只保留一个副本。-->[A. 重复数据删除](#)
58. ( ) 命令用来跟踪源与目标节点之间的所有路由器。-->[C. tracert](#)
59. ( ) 是 Internet 传统的服务之一，用来在远程计算机之间进行文件传输。-->[FTP](#)
60. ( ) 是 Windows 操作系统中的一个系统命令，用于显示本机的 TCP/IP 网络配置值。-->[C. ipconfig](#)
61. ( ) 是把自己伪装成善意应用程序 (进程) 的恶意软件程序。-->[D. 特洛伊木马](#)
62. ( ) 是建立在 SAN 基础上的解决方案，是指数据无须通过局域网而直接进行备份。-->[A. 不依赖局域网 \(LAN-Free\) 结构](#)
63. ( ) 是微软公司推出的用于局域网内计算机有关操作系统、应用软件等补丁管理的一种服务器软件，它可以快速、方便地为网络中每台运行 Windows 操作系统的计算机分发操作系统和应用软件的补丁。-->[D. WSUS](#)
64. ( ) 是小型办公环境最常用的备份组网方式。在这种结构中，预先配置一台服务器作为备份管理服务器，它负责整个企业系统的备份操作。备份介质接在某台服务器上，当需要备份数据时，备份对象把数据通过网络传输到备份介质中。-->[D. 基于局域网结构](#)
65. ( ) 是一个存储网络管理信息的数据库，由被管理对象组成。-->[C. 管理信息库](#)

66、()是一系列网络管理规范的集合,包括:协议、数据结构的定义和一些相关概念,目前已成为网络管理领域中事实上的工业标准。-->[C. SNMP](#)

67、()是一种插入到软件中并能对运行中出现的软件错误进行修改的程序编码,往往是在漏洞被发现后由软件开发商开发和发布的。-->[D. 软件补丁](#)

68、()是一种电子设备,用来测量并连续显示信号的电压及信号的波形。-->[B. 示波器](#)

69、()是一种基于票据(Ticket)的认证方式,其设计目标是通过使用一台中央服务器提供“票据”,而网络中提供资源的服务器和访问资源的客户端之间使用这个“票据”相互识别。-->[D. Kerberos](#)

70、()是一种可以对域中的某一部分对象进行单独管理的容器。-->[B. 组织单位](#)

71、()是一种网络监测功能,可以收集流入和流出网络接口的IP数据包。-->[NetFlow](#)

72、()是以最近一次备份为基准,对最近一次备份后到进行此种备份的这段时间内,发生变化的数据进行备份。-->[D. 增量备份](#)

73、()是以最近一次完全备份为基准,对最近一次完全备份后到进行此种备份的这段时间内,发生变化的数据进行备份。-->[B. 差异备份](#)

74、()是针对OSI模型的第1层设计的,它只能用来测试电缆而不能测试网络的其它设备。-->[D. 电缆测试仪](#)

75、()是指入侵者伪装成某个受信任的网站,如把自己伪装成用户使用的网上银行页面,要求用户更新自己的财务信息,如登录用户名、信用卡号码、消费密码等,进而获得用户的私人数据。-->[D. 钓鱼式攻击](#)

76、()是最简单实用的服务器监视工具。利用它,管理员可以迅速获得简要的系统信息,例如:应用程序、进程、性能、联网和用户等。-->[B. 任务管理器](#)

77、()数据主要是指业务系统的所有业务数据,对数据的安全性、准确性、完整性、一致性要求很高,而且变化频繁。-->[B. 应用](#)

78、()通常采用便携式测量仪表,在网络中的某个节点上安置测量系统或测量仪表进行测量。-->[D. 单点测量](#)

79、()通常设置在企业内部网络中客户端与外部网络中服务器之间,它会暂存客户端发来的请求,并由自己发出这些请求。-->[B. 代理服务器](#)

80、()通常适用于数据量大,对备份设备的性能和可靠性要求很高的场景。-->[硬盘](#)

81、()位于被管理对象中,被管理对象可以是计算机、网络设备、应用程序等。-->[B. 代理](#)

82、()协议是一种广泛应用于无线网络的基于端口的网络访问控制协议。它具有完备的用户认证、管理功能,可以很好地支撑宽频网络的计费、安全访问、日常运营和管理要求。-->[B. 802.1X](#)

83、()协议用于发送电子邮件。-->[SMTP](#)

84、()允许用户在指定的时间段内以数据包为单位查看指定协议的数据,对这些数据包的原始数据位和字节解码,并能依据其对该数据包所用协议的理解提供综合信息。-->[A. 协议分析仪](#)

85、《信息安全技术信息系统灾难恢复规范》(GB/T20988—2007)中定义的灾难恢复能力分为()个等级。-->[C. 六](#)

86、安全管理的主要功能包括:身份验证、密钥管理、()、访问控制。-->[安全控制](#)

87、按照防火墙实现的技术不同,可以分为包过滤防火墙、()防火墙、电路层防火墙、状态检测防火墙。-->[B. 应用层](#)

88、按照网络测量点的位置,可以分为端系统测量和()。-->[D. 中间系统测量](#)

89、把电子邮件发送到收件人的电子邮箱中,所采用的邮件传输协议是()。-->[SMTP](#)

90、备份管理系统,主要包含()和备份管理服务器,负责备份策略管理和备份作业监控,以及读取备份客户端的数据并把数据写入备份介质。-->[B. 备份软件](#)

91、备份介质是指备份数据存储的媒介,一般为磁盘阵列、物理磁带库或者虚拟磁带库、光盘塔、()。-->[B. 云存储](#)

92、备份客户端是指需要备份数据的业务主机,它负责提供要备份的数据,一般需安装()。-->[C. 备份软件客户端代理程序](#)

93、备份系统的组件包括:备份管理系统、备份客户端、()和备份介质。-->[C. 备份网络](#)

94、必须在拥有AD的企业环境中才可以部署的CA类型是()。-->[企业CA](#)

95、边缘网络也称为(),位于内部防火墙与外部防火墙之间,受保护强度较低,一般用于放置面向Internet的服务设备,这些设备需要接受来自互联网的用户访问。-->[D. DMZ](#)

96、常见的RAID类型包括()。-->[RAIDO、RAIDI、RAID5、RAID1+0](#)

97、常见的备份工具有()。-->[Ghost](#)

98、常见的备份工具有()。-->[Windows 备份工具](#)

99、常见的备份工具有()。-->[A. Ghost](#)

100、常用的数据备份方式有完全备份、差异备份以及()。-->[D. 增量备份](#)

101、从宏观角度来看,在使用Kerberos时,一个客户端需要经过()个步骤来获取服务。-->[B. 3](#)

102、从数据用途角度来说,一般可将需要备份的数据分为系统数据、基本数据、应用数据、()数据。-->[A. 临时](#)

103、从网络测量系统的功能角度,网络测量系统的体系结构从底层到高层分别为数据采集层、数据管理层、()和数据表示层。-->[A. 数据分析层](#)

104、大部分的网络是基于()构建的,网络系统管理员在网络故障排除时,可以参考它的分层思想。-->[TCP/IP 协议](#)

105、代理服务器通常设置在企业内部网络中客户端与()之间。-->[外部网络中服务器](#)

106、带有私钥的证书文件格式是()。-->[. PFX](#)

107、当故障转移群集的节点数为奇数时,建议仲裁模式配置为()。-->[多数节点](#)

108、当故障转移群集希望仲裁磁盘拥有唯一投票权时,建议仲裁模式配置为()。-->[仅磁盘](#)

109、当前,在机场候机厅提供的免费无线Wi-Fi服务,属于基于使用()的计费方式。-->[时间](#)

110、当前许多计费系统采用三层体系结构,分别对应表示层、()和数据层。-->[应用层](#)

111、当群集网络接口状态为()时,代表了当前网络已经故障,无法正常工作。-->[Down](#)

112、当群集网络接口状态为()时,群集网络的工作完全正常。-->[Up](#)

113、当群集网络接口状态为()时,意味着一个或多个节点的通信有问题,或最近故障了。-->[Partitioned](#)

114、电缆测试仪是针对OSI模型的第()层设计的。-->[D. 一层](#)

115、电子邮件从发送到接收的过程中,需要使用哪些协议方可完成()。-->[SMTP、POP3](#)

116、防火墙的处理方式主要包括:Accept、Drop和()。-->[C. Reject](#)

117、防火墙客户端不能安装在()操作系统上。-->[D. UNIX](#)

118、防火墙客户端能够安装在()操作系统上。-->[A. WindowsServer2003](#)

119、访问控制服务,与()相关。-->[C. 访问控制机制](#)

120、根据检测对象分类,可以将入侵检测系统分为:基于主机的入侵检测系统、()和混合型入侵检测系统。-->[A. 基于网络的入侵检测系统](#)

121、故障管理包括()、隔离故障和纠正故障3个方面。-->[D. 故障检测](#)

122、故障转移群集的仲裁模式包含哪几种()。-->[节点多数、节点和磁盘多数、多数节点和文件共享、仅磁盘](#)

123、故障转移群集网络接口状态包括()。-->[UP、Unavailable、Partitioned、Down](#)

124、故障转移群集中最多可以包含多少个节点()。-->[8](#)

125、国际标准Share78对灾难恢复解决方案从低到高分为()种不同层次。-->[C. 七](#)

126、国际标准Share78对灾难恢复解决方案从低到高分为多个不同层次,针对每个层次都有相应的容灾方案。其中(0)级是成本最低的灾难恢复方案()。-->[无异地备份](#)

127、国际标准Share78对灾难恢复解决方案从低到高分为多个不同层次,针对每个层次都有相应的容灾方案。其中()级是成本最低的灾难恢复方案(无异地备份)。-->[A. 0](#)

128、国际标准Share78对灾难恢复解决方案从低到高分为多个不同层次,针对每个层次都有相应的容灾方案。其中()级是最高级别的灾难恢复方案(零数据丢失)。-->[C. 6](#)

129、国际标准化组织于1989年发布了《信息处理系统-开放系统互连-基本参考模型第2部分:安全体系结构》来定义网络安全体系结构。在该体系结构中提出了以下()类。-->[安全服务](#)

130、国际标准化组织于1989年发布了《信息处理系统-开放系统互连-基本参考模型第2部分:安全体系结构》来定义网络安全体系结构。在该体系结构中提出了以下()类安全服务。-->[C. 五](#)

131、活动目录的优点是:()。-->[降低总体拥有成本、单一用户登录](#)

132、活动目录的主要特点有:()等。-->[集中管理与分散管理相结合](#)

133、基础数据分析包括三方面功能:基本统计功能、()和数据关联分析。-->[C. 性能趋势预测](#)

134、基于流量计费是根据用户在一段时间内所使用的全部网络流量(发送和接收)统计数-->[D. NetFlow](#)

135、基于数据库的复制方式可将远程数据库复制分为实时复制、()和存储转发复制。-->[B. 定时复制](#)

136、计费管理的组件包括：计费数据的采集和存储（）与用户、管理员之间的人机交互界面。-->[数据的分析和统计](#)

137、计费管理的组件包括：计费数据的采集和存储（）；与用户、管理员之间的人机交互界面。-->[B. 数据的分析和统计](#)

138、计费管理可以用来确定网络中每一种服务的价值，包括（）类服务、软件类服务和人工服务。-->[A. 硬件](#)

139、计费管理可以用来确定网络中每一种服务的价值，包括硬件类服务、软件类服务和（）服务。-->[人工](#)

140、计算机病毒的特征为：隐蔽性、（）、潜伏性、破坏性、针对性。-->[传染性](#)

141、计算机病毒的生命周期一般由四个阶段组成，包括：潜伏阶段、传播阶段、（）和发作阶段。-->[C. 触发阶段](#)

142、接收电子邮件的协议是（）。-->[POP3](#)

143、经典的加密方法，主要包括：替换加密、换位加密和（）。-->[A. 一次性填充](#)

144、可以使用（）组合键，打开 Windows 任务管理器。-->[A. Ctrl+Shift+Esc](#)

145、可以在无 AD 的企业环境中部署的 CA 类型是（）。-->[独立 CA](#)

146、可以自动颁发证书的 CA 类型是（）。-->[企业 CA](#)

147、类似于用户的增减、设备的维修或更新、新技术的应用等事件，属于（）范畴。-->[C. 配置管理](#)

148、每年 99.95% 的服务可用性意味着数据和服务每年的计划外停机时间不得超过 0.05%，以一年 365 天，每天 24 小时为例，一年的停机时间不得超过（）。-->[C. 4.38 小时](#)

149、每年 99.9% 的服务可用性意味着数据和服务每年的计划外停机时间不得超过 0.1%，以一年 365 天，每天 24 小时为例，一年的停机时间不得超过（）。-->[A. 8.76 小时](#)

150、每年 99% 的服务可用性意味着数据和服务每年的计划外停机时间不得超过-->[76 小时](#)

151、每年 99.9% 的服务可用性意味着数据和服务每年的计划外停机时间不得超过（）。-->[0.1%](#)

152、美国国防部高级研究计划局提出的通用入侵检测框架将入侵检测系统分为四个组件，包括：事件产生器、事件分析器、（）和响应单元。-->[B. 事件数据库](#)

153、默认情况下，FTP 服务中文件传输所使用的 TCP 端口号为（）。-->[21](#)

154、默认情况下，Web 服务所使用的 TCP 端口号为（）。-->[80](#)

155、认证服务能够确保某个实体身份的可靠性，可分为两种类型。一种认证服务类型是认证实体本身的身份，确保其真实性，称为实体认证。另一种认证服务类型是证明某个信息是否来自某个特定的实体，这种认证称为（）。-->[D. 数据源认证](#)

156、如果安装了错误的调制解调器驱动程序，Windows 操作系统无法正常启动，那么应该进入（）进行恢复。-->[D. 安全模式](#)

157、如果继续使用厂商不再支持的操作系统，就会存在非常严重的安全风险。以微软的 Windows 生命周期为例，客户端操作系统的生命周期一般为（）年。-->[B. 十](#)

158、如果企业将 RPO 设置为 3 小时，则必须每 3 小时至少执行（）备份。-->[一次](#)

159、如果向网络发送数据包并不断提高发送速度直至网络饱和，就可以测量网络的最大负载能力，这种测量方式属于（）。-->[主动测量](#)

160、如下 RAID 类型中，不提供数据保护功能的是（）-->[RAID0](#)

161、如下（）功能可以使用故障转移群集功能实现高可用性。-->[FTP 服务器、SQLServer、文件服务器](#)

162、如下浏览器属于谷歌公司的是（）-->[Chrome](#)

163、如下浏览器属于苹果公司的是（）。-->[Safari](#)

164、如下浏览器属于微软公司的是（）。-->[Internet Explorer](#)

165、如下哪个服务为 Windows Server 2016 默认已安装服务，无需另行安装（）。-->[IIS、DNS、DHCP](#)

166、如下哪类 CA，可以部署在非 AD 环境中（）。-->[独立根 CA、独立从属 CA](#)

167、入侵者可以拦截网络中正常的通信数据，并修改和控制通信双方的 TCP 会话，而通信的双方却毫不知情，入侵者就可以使用抓包软件查看双方的通信内容。此种入侵手段被称为（）。-->[C. 中间人攻击](#)

168、入侵者试图通过将数据包的源 IP 伪装成为一个受信任计算机的 IP 地址，并借此访问企业内部网络中的资源。此种入侵手段被称为（）。-->[A. IP 欺骗](#)

169、上网行为管理的主要功能包含：（）、网络应用控制、带宽流量管理、信息收发审计、用户行为分析、上网人员管理。-->[B. 网页访问过滤](#)

170、输入 netstat (-n) 命令，则显示活动的 TCP 连接、地址和端口号（）。-->[以数字形式表示](#)

171、输入 netstat ( ) 命令，则显示活动的 TCP 连接、地址和端口号（以数字形式表示）。-->[C. -n](#)

172、数据管理功能包括基于数据管理和（）管理。-->[B. 事件](#)

173、数据链路层的故障主要表现在通信双方的（）封装协议是否一致。-->[C. 二层](#)

174、提供认证、授权和计费功能的标准，包括：（）。-->[RADIUS、TACACS](#)

175、通常可以把网络信息安全的问题划分为物理层、网络层、数据层和（）这 4 个层面-->[A. 内容层](#)

176、通过发送（）数据包，可以获得网络往返时延、丢包率与连通性等参数。-->[A. ICMP](#)

177、通过上网行为管理产品，网络系统管理员可以实时掌握已连接到网络的设备、用户及位置，为网络资源的合规使用提供支持。具体包括：上网身份管理、上网终端管理、（）和上网地点管理。-->[D. 移动终端管理](#)

178、通过上网行为管理产品，网络系统管理员可以制定全面的信息收发监控策略，有效控制关键信息的传播范围，避免可能引起的法律风险。具体包括：普通邮件管理、Web 邮件管理、网页发帖管理、（）和其他外发管理。-->[C. 即时通信管理](#)

179、网络测量的功能按照测量对象，可分为三大类：网络性能测量、业务性能测量、（）。-->[网络流量测量](#)

180、网络测量技术的基本要求是有效性、高速测量、准确性和（）。-->[C. 实时性](#)

181、网络服务故障主要包括 3 个方面：服务器硬件故障、网络操作系统故障和（）。-->[C. 网络服务故障](#)

182、网络负载均衡群集端口规则设置中，可以选择的筛选模式包括（）。-->[多个主机、单一主机、禁用此端口范围](#)

183、网络负载均衡群集端口规则支持最大端口号为（）。-->[65535](#)

184、网络负载均衡群集节点优先级最低的使用（）表示。-->[32](#)

185、网络负载均衡群集节点优先级最高的使用（）表示。-->[1](#)

186、网络负载均衡群集可以选择的群集操作模式包括（）。-->[单播、多播、IGMP 多播](#)

187、网络故障排查流程：描述网络故障现象、收集可能的网络故障原因信息、（）、网络故障分析、事后记录和总结。-->[B. 建立诊断计划](#)

188、网络管理包括五大功能：故障管理、配置管理、计费管理、（）和安全管理。-->[性能管理](#)

189、网络系统管理人员应该针对不同（）对不同资源分配不同的访问权-->[用户](#)

190、网页中可以包含如下哪个内容（）。-->[文字、音频、视频](#)

191、网站中的内容（如网页）最好存储在（）格式的磁盘分区中。-->[NTFS](#)

192、微软产品系列中，用户实现电子邮件功能的服务器产品是（）。-->[Exchange](#)

193、微软的 POP3 服务支持以下三种用来验证用户身份的方式包括（）。-->[本地 Windows 账户验证、ActiveDirectory 集成验证、已加密的密码文件验证](#)

194、微软的证书颁发机构包括如下哪几种类型（）。-->[企业根 CA、企业从属 CA、独立根 CA、独立从属 CA](#)

195、为了支持《信息处理系统-开放系统互联-基本参考模型第 2 部分：安全体系结构》定义的安全服务，ISO 的网络安全体系结构定义了（）类安全机制。-->[A. 八](#)

196、无法管理证书模板的 CA 类型是（）。-->[独立 CA](#)

197、下列哪个不是电子邮件提供的功能（）-->[将附件内容自动写入邮件正文](#)

198、下列哪个不是电子邮件提供的功能（）。-->[通知电子邮件到达](#)

199、下列能够建立 Web 服务器的功能是：（）。-->[IIS](#)

200、下列主要用于电子邮件收发和管理的软件是（）。-->[Outlook Express](#)

201、下面关于 FTP 的叙述中，错误的是（）。-->[目前大多数 FTP 匿名服务允许用户上传和下载文件](#)

202、性能管理的主要功能包括：性能测量、（）、性能管理控制和提供性能指标。-->[B. 性能分析](#)

203、一旦把内部网络中的计算机配置成为 Web 代理客户端，它们将只能把本地用户访问 Internet 的（）对象的请求提交给 ISAServer，由 ISAServer 代为转发。-->[A. HTTP](#)

204、用户将文件从 FTP 服务器复制到自己计算机的过程，称为（）。-->[下载](#)

205、用户将文件从个人计算机复制到 FTP 服务器的过程，称为（）。-->[上传](#)

206、用于从 Web 网站服务器传输超文本到本地浏览器的传输协议是（）。-->[HTTP](#)

207、用于给内部网络或网络服务供应商自动分配 IP 地址的协议是（）。-->[DHCP](#)

208、用于解析域名的协议是（）。-->[DNS](#)

209、用于支持使用客户端远程管理在服务器上的电子邮件的协议是（）。-->[POP3](#)

210、有效性、高速测量、准确性和（）是对网络测量技术的基本要求。-->[实时性](#)

211、与带宽相关的参数有：链路带宽、瓶颈带宽、（）等。-->[B. 可用带宽](#)

212、域管理员可以使用（）对域中的某一部分对象进行单独的管理。-->[B. 组织单位](#)

213、灾难恢复体系规划设计包括灾难恢复需求分析、策略制定、技术体系规划、（）等方面。-->[B. 资源规划](#)

214、灾难恢复需求分析能力包括对风险分析、（）和灾难恢复目标制定3个方面，对其分析结果进行评估，以确保企业灾难恢复需求分析的结论符合企业业务恢复要求。-->[C. 业务影响分析](#)

215、在FTP服务器中，授予用户如下（）权限，可以获得上传文档的权限。为了防止权限过大情况发生，请选择可以授予的最小权限。-->[写入](#)

216、在FTP服务器中，授予用户如下（）权限，只能获得下载文档的权限。-->[读取](#)

217、在IIS中，使用同一个IP地址实现多个站点的方法是（）。-->[主机头名方式](#)

218、在TCP/IP参考模型中，属于传输层协议的包括（）。-->[TCP、UDP](#)

219、在TCP/IP参考模型中，属于应用层协议的包括（）。-->[FTP、DNS、SMTP](#)

220、在WindowsServer2016中，证书服务必须发布基于（）协议的证书申请网站。-->[HTTPS](#)

221、在WindowsServer2016中，证书服务已不再支持发布基于（）协议的证书申请网站。-->[HTTP](#)

222、在WindowsServer服务器上的命令提示符窗口中，输入（），打开“高级安全Windows防火墙”窗口。-->[D. wf.msc](#)

223、在WindowsServer中，FTP服务内置于哪个功能之中（）。-->[IIS](#)

224、在WindowsServer中，SMTP服务依托于如下哪个功能之中（）。-->[IIS](#)

225、在WindowsServer中，网络负载均衡适用于如下哪些应用功能（）。-->[IIS](#)

226、在Windows操作系统的计算机上运行的ping命令会发送4个ICMP回送请求数据包，每个数据包为（）。-->[B. 32字节](#)

227、在Windows操作系统中，（）能够支持的密码必须符合复杂性要求。-->[B. P@s0rd](#)

228、在Windows操作系统中，（）能够满足密码的复杂性要求。-->[B. P@s0rd](#)

229、在（）体系中，测量节点是完整的测量系统，它们分布在网络中的多个位置，既可以独立地进行网络测量，也可以将测量数据发送到测量中央服务器。-->[B. 分布式测量](#)

230、在（）中，备份服务器仍参与备份过程，但负担大大减轻，因为它的作用只是指挥，而且不涉及数据的装载和运输，不是主要的备份数据通道。-->[不依赖服务器 \(Server-Free\) 结构](#)

231、在（）中，备份服务器仍参与备份过程，但负担大大减轻，因为它的作用只是指挥，而且不涉及数据的装载和运输，不是主要的备份数据通道。-->[C. 不依赖服务器 \(Server-Free\) 结构](#)

232、在安装防火墙时，需要安装（）软件。-->[A. 防火墙客户端](#)

233、在创建故障转移群集之前，应该进行验证测试，（）可以测试出服务器上可用的所有磁盘。-->[存储设备测试](#)

234、在创建故障转移群集之前，应该进行验证测试，（）用于记录服务器硬件每个重要组成的配置信息。-->[清单测试](#)

235、在创建故障转移群集之前，应该进行验证测试，（）用于实现群集的网络拓扑、IP地址和Windows防火墙的配置情况。-->[网络测试](#)

236、在创建故障转移群集之前，应该进行验证测试，（）用于验证系统的配置情况。-->[系统配置测试](#)

237、在工作组环境中的Windows操作系统，可以使用（）管理器来配置本地计算机的安全策略。-->[A. 本地安全策略](#)

238、在活动目录中，所有被管理的资源信息，例如：用户账户、组账户、计算机账户、甚至是域、域树、域森林等，统称为（）。-->[A. 活动目录对象](#)

239、在没有AD的前提下，部署微软证书服务可以选择如下哪几种类型（）。-->[独立CA](#)

240、在默认情况下，IIS默认文档中哪种文档的优先级最低（）。-->[iisstart.htm](#)

241、在默认情况下，IIS默认文档中哪种文档的优先级最高（）。-->[Default.htm](#)

242、在配置IIS时，如果想禁止某些IP地址访问Web服务器，应在“默认Web站点”属性对话框中的（）选项卡中进行配置。-->[目录安全性](#)

243、在事件查看器中，（）日志记录Windows操作系统自身产生的错误、警告或者提示。例如：当驱动程序发生错误时，这些事件将被记录到上述日志中。-->[系统](#)

244、在事件查看器中，（）日志记录应用程序所产生的错误、警告或者提示。例如：如果应用程序执行非法操作，系统会停止运行该应用程序，并把相应的事件记录到相应的日志中。-->[B. 应用程序](#)

245、在事件查看器中，（）日志用来记录与网络安全有关的事情。例如：用户登录成功或失败、用户访问NTFS资源成功或失败等。-->[C. 安全性](#)

246、在网络负载均衡配置中，当群集节点主机之间不需要单独建立通信时，最佳实践为（）。-->[节点计算机配置一个网卡](#)

247、在网络负载均衡配置中，当群集中没有任何节点需要和外部网络其他计算机进行通信时，最佳实践为（）。-->[网络负载均衡设置为单播模式](#)

248、在网络负载均衡群集中，可以对主机进行如下哪些操作（）。-->[停止、挂起、继续、开始](#)

249、在一般的保密通信模型中，在发送端将明文P用加密算法E和密钥K加密，变换成密文C，即C=E(K, P)，在接收端利用解密算法D和密钥K，对C进行解密，得到明文P，即（）。-->[D. P=D\(K, C\)](#)

250、在一个Windows域中，成员服务器的数量为（）。-->[D. 可有可无](#)

251、在一个Windows域中，更新组策略的命令为（）。-->[A. Gpupdate.exe](#)

252、在一个Windows域中，域控制器的数量为（）。-->[A. 至少1台](#)

253、在一个Windows域中，至少需要（）台域控制器。-->[A. 1台](#)

254、在一些大型的备份管理系统中，备份服务管理服务器通常由备份服务器和（）组成。-->[A. 介质服务器](#)

255、在运行窗口中输入（），可以打开管理控制台界面。-->[mmc](#)

256、在运行窗口中输入（），可以打开命令提示符界面。-->[cmd](#)

257、在运行窗口中输入（），可以打开注册表管理界面。-->[regedit](#)

258、在制定组策略时，可以把组策略对象链接到（）上。-->[C. 组织单位](#)

259、在组策略中，计算机策略仅对（）生效。-->[D. 计算机账户](#)

260、在组策略中，用户策略仅对（）生效。-->[C. 用户账户](#)

261、帐户锁定策略用来设置锁定用户帐户的方式，如（）、帐户锁定的持续时间以及解锁帐户的方法。-->[D. 帐户锁定阈值](#)

262、指定网络负载均衡不需要将同一客户端的多个请求定向到同一台服务器，应将客户端相关性设置为（）。-->[无](#)

263、指定网络负载均衡将同一C类地址范围的多个请求定向到同一台服务器，应将客户端相关性设置为（）。-->[网络](#)

264、主动测量方法可以利用TCP/IP协议中的（）、TCP、UDP等协议来发送探测数据包进行测量。-->[A. ICMP](#)

265、住宅的宽带接入服务，当用户订购服务之后，可以按月或按年支付费用，并随意访问Internet。这种计费方式属于（）的计费。-->[C. 统一费用](#)

266、最常见的网络数据备份系统按其架构不同可以分为：（）结构、基于局域网(LAN-Base)结构、不依赖局域网(LAN-Free)结构和不依赖服务器(Server-Free)结构。-->[C. 基于主机](#)

**多选(50)一**

1、IPsec是开放标准的一个框架，包括两个主要协议：（）  
-->[\(B. AH.C. ESP\)](#)

2、PPP身份验证方法包括（）。-->[\(B. PAPD. CHAP\)](#)

3、RSA密钥的长度可以是：（）。-->[\(C. 512位 D. 1024位 E. 2048位\)](#)

4、SNMP使用（）和（）端口。-->[\(A. UDP161C. UDP162\)](#)

5、TCP/IP网络性能指标可以从物理层、数据链路层、（）、传输层和（）5个层次来分析。-->[\(D. 网络层 E. 应用层\)](#)

6、WindowsServerBackup是WindowsServer2016操作系统提供的一项备份功能，它提供的操作接口包括：管理控制台和（）。  
-->[\(B. wbadmin命令 C. WindowsPowerShell命令\)](#)

7、（）的计费是根据用户在一段时间内所使用的全部网络流量（）统计数据来收取用户费用的一种计费方式。-->[\(基于网络流量；发送和接收\)](#)

8、常见的加密算法包括哪些：（）。-->[\(A. 3DESC. AESE. RSA\)](#)

9、常见的证书格式包括（）-->[\(PFX; P12; P7B; CER\)](#)

10、当前许多计费系统采用三层体系结构，分别对应表示层、（）和（）。-->[\(D. 应用层 E. 数据层\)](#)

11、电子邮件从发送到接收的过程中，需要使用哪些协议方可完成（）-->[\(SMTP; POP3\)](#)

12、防火墙的部署方案主要有：（）、（）和（）。-->[\(B. 边缘防火墙 C. 三向防火墙 D. 背对背防火墙\)](#)

13、故障转移群集适配器接口状态包括()-->(UP; Unavailable; Failed; Unreachable)

14、活动目录的优点是()和()。-->(B.降低总体拥有成本 C.单一用户登录)

15、活动目录的优点是:()。-->(降低总体拥有成本单一用户登录)

16、活动目录的主要特点有:()、()、()等。-->(A.动态的组织形式 B.集中管理与分散管理相结合 C.资源访问的分级管理)

17、计算机病毒的特征有:()、()和()。-->(A.可执行性 C.隐蔽性 D.传染性)

18、计算机病毒的危害主要表现为:()、()和()等。-->(A.破坏计算机的数据 B.占用磁盘空间 C.影响计算机运行速度)

19、计算机病毒具有的特征包括:传染性、隐蔽性、潜伏性、()和()。-->(破坏性; 针对性)

20、抗抵赖性服务,主要涉及:数字签名机制、()和()。-->(B.数据完整性机制 D.公证机制)

21、可以基于()等网络设备来实现基于流量的计费。-->(B.路由器 C.防火墙 E.代理服务器)

22、密码策略可以定义()。-->(密码必须符合复杂性要求; 密码最长使用期限; 密码最短使用期限; 密码长度最小值)

23、目前流行的浏览器产品包括()-->(微软 IE 浏览器 (Internet Explorer); 谷歌浏览器 (Chrome); 火狐浏览器 (Firefox); 苹果浏览器 (Safari) )。

24、目前网络存在的威胁主要表现:非授权访问、信息泄漏、破坏数据完整性、()和()。-->(A.拒绝服务攻击 C.利用网络传播病毒)

25、目前最常用的网络管理协议包括()、()和(),它们广泛地应用于网络管理解决方案中。-->(A. CMIPB. CMISD. SNMP)

26、认证服务,与加密机制、()和()相关。-->(D.数字签名机制 E.认证机制)

27、如果用户希望使用完全合格域名()来访问网站,则必须配合()服务完成名称解析。-->(FQDN; DNS)

28、如下产品可以使用微软证书服务进行信息加密的有()  
-->(Exchange Server; SharePoint Server; SQL Server; Office)

29、如下哪类 CA,可以部署在非 AD 环境中()-->(独立根 CA; 独立从属 CA)

30、数据保密性服务,主要涉及:加密机制、()和()。-->(B.路由控制机制 E.业务流填充机制)

31、数据完整性服务,主要涉及:数字签名机制、()和()。-->(A.加密机制 B.数据完整性机制)

32、数据帧封装格式包括:HDLC、()和()等。-->(D. PPPE. Frame-Relay)

33、提供认证、授权和计费功能的标准,包括:()。-->(A. RADIUS E. TACACS)

34、通常可以把网络信息安全的问题划分为物理层、网络层、()和()4个层面。-->(数据层; 内容层)

35、通过上网行为管理产品,网络系统管理员可以实时了解、统计、分析 Internet 使用状况,并根据分析结果对管理策略做出调整和优化,具体包括()。-->(A. 上网行为实时监控 C. 上网行为日志查询 E. 上网应用累计时长限额)

36、网络测量的功能按照测量对象,可分为三大类:()、()、()。-->(A.网络性能测量 B.业务性能测量 E.网络流量测量)

37、网络故障大致可以分为4类,即链路故障、协议故障、()和()。-->(A.配置故障 C.服务故障)

38、网络管理包括五大功能:故障管理、配置管理、计费管理、()和()。-->(B.性能管理 D.安全管理)

39、网络系统管理与维护的基本功能有:()、()、()。-->(A.故障管理 B.配置管理 C.性能管理)

40、网络系统管理员可以使用 Windows Server Backup 备份:完整服务器、系统状态、()和()等。-->(C.仅单个文件和文件夹 D.仅 Hyper-V 主机上的单个虚拟机)

41、微软的 POP3 服务支持以下三种用来验证用户身份的方式包括()-->(本地 Windows 账户验证; Active Directory 集成验证; 加密的密码文件验证)

42、灾难恢复的重要指标包括:服务可用性、恢复点目标、()等。-->(A.恢复时间目标 B.保留目标)

43、在 IIS 中可以配置如下哪些功能()。-->(网站、FTP 网站、SMTP 网站、网络新闻传输协议 (NNTP) 站点)

44、在 ISO 的网络安全体系结构中定义的安全服务有:()、()和()。-->(A.访问控制服务 C.数据机密性服务 D.数据完整性服务)

45、在 ISO 的网络安全体系结构中定义了5类安全服务,包括:认证服务、访问控制服务、数据保密性服务、()和()。-->(B.数据完整性服务 D.抗抵赖性服务)

46、在 ISO 的网络安全体系结构中定义了5类安全服务,包括:认证服务、访问控制服务、数据保密性服务、()和()。-->(B.数据完整性服务 D.抗抵赖性服务)

47、在 TCP/IP 参考模型中,属于应用层协议的包括()。-->(FTP; DNS; SMTP)

48、在 Windows 资源监视器中,可以查看到的选项卡包括:()、()、内存、磁盘、()。-->(A.概述 C. CPU D. 网络)

49、在基于 Windows 操作系统的计算机上,可以将帐户大体划分为哪三种类型?()-->(A.管理员帐户 B.标准帐户 C.来宾帐户)

50、在一个域中,计算机的角色有:()、()和()。-->(B.域控制器 C.成员服务器 D.工作站)

判断(240)一

1、“黑客”一词是由英语单词“Cracker”音译而来的,是指专门研究、搜寻计算机漏洞和网络漏洞的计算机爱好者。-->错

2、arp 命令用于显示和修改地址解析协议 (Address Resolution Protocol, ARP) 缓存表的内容。-->对

3、CA 必须部署在拥有 AD 的企业环境中。-->错

4、CHAP 不会在网络上直接传输用户的密码,因此比 PAP 更安全。-->对

5、CIDF 体系结构中的事件产生器可以是来自网络的数据包,也可以是从系统日志等其他途径得到的信息。-->对

6、CIH 病毒是一种危害性很小的病毒。-->错

7、DES (Data Encryption Standard, 数据加密标准) 制定于 1977 年,它将明文分成 64 位的块,对每个块进行变换(替换和换位)。-->对

8、FTP 服务器无法单独控制文件的下载权限。-->对

9、FTP 服务只能使用 TCP 端口 21。-->错

10、IIS 建立的网站只能通过 80 端口进行访问。-->错

11、IIS 可以建立支持 80 和 443 端口协议的网站。-->对

12、IIS 默认站点中的默认文档名称包括:Default.asp。-->对

13、IIS 默认站点中的默认文档名称包括:Default.html。-->错

14、IIS 默认站点中的默认文档名称包括:Default.htm。-->对

15、IIS 默认站点中的默认文档名称包括:iisstart.html。-->错

16、IIS 默认站点中的默认文档名称包括:index.htm。-->对

17、IIS 站点中的默认文档顺序可以手动调整优先级。-->对

18、IIS 站点中的默认文档顺序无法调整优先级。-->错

19、Internet 提供的主要信息服务有:WWW 服务、FTP 服务、E-mail 服务、Telnet 服务、信息讨论与公布服务、娱乐与会话服务等。-->对

20、ipconfig 命令是个使用频率极高的测试命令,其主要功能是使用 ICMP (Internet Control Message Protocol, 网络控制报文协议) 数据包来测试从源端到目的端网络的连通性,它可以快速准确地判断网络故障。-->错

21、IPsec 是一个建立在网络层之上的企业私有协议。-->错

22、IPsec 有两种工作模式:传输模式和隧道模式。-->对

23、ISO 的网络安全体系结构定义了六类安全机制。-->错

24、MD5 和 SHA 属于数据完整性检测方法。-->对

25、MIB 定义了如何识别被管理对象,以及如何组织被管理对象的信息结构。MIB 中的对象按层次进行分类和命名。-->对

26、netstat 命令用于显示 TCP 连接、当前计算机正在监听的端口、以太网统计信息、IP 路由表、IPv4 统计信息、IPv6 统计信息等。-->对

27、ping 命令还能显示 TTL (Time To Live, 生存期) 值,该值是由发送端主机设置的,它的作用是防止数据包在 IP 网络中永无止境地转发下去。-->对

28、ping 扫描,也称为 TCP 扫描,它可以确定网络中某些设备(如计算机、路由器)是否在线.ping 扫描通常在攻击初期使用。-->错

29、POP3 协议的端口号是 110。-->对

30、PPP 协议是一种传输层协议,被设计用于点对点连接中传递数据,使用用户名和密码进行验证,并协调两个设备使用的网络协议。-->错

31、RC4 属于非对称加密算法。-->错

32、Rivest、Shamir 和 Adleman 对 Diffie-Hellman 的公钥加密算法进行了改进,于 1977 年发明了 RSA 算法。-->对

33、SecureNAT 客户端支持身份验证。-->错

34、SMTP 协议的端口号是 25。-->对

35、SMTP 协议使用的端口号为 25。-->对

36、SNMP 的 Trap 报文用于代理主动向管理站通告重要事件。-->对

37、SNMP 的 Trap 报文由代理主动发给管理站,并且需要管理站的响应。-->错

38、tracert 命令用来跟踪源与目标节点之间的所有路由器。-->对

39、VPN 服务器可以作为 RADIUS 体系中的网络接入服务器。-->对

40、Web 代理客户端不支持 DNS 转发功能。-->错

41、Web 代理客户端支持 DNS 转发功能。-->对

42、Web 代理客户端支持身份验证。-->对

43、Web 网站中的所有资源都必须存储在主目录中，用户无法访问位于主目录之外的网页资源。-->错

44、WindowsServerBackup 是单服务器备份解决方案。不能使用一个服务器上的 WindowsServerBackup 备份多个服务器上的数据。-->对

45、Windows 操作系统内置的 Administrator 用户帐户，可以执行本台计算机的所有管理工作，如创建/更改/删除用户帐户、设置用户帐户的权限和权利、更改计算机名称、设置安全策略、管理硬件设备、管理文件系统等。-->对

46、Windows 操作系统内置的 Guest 用户帐户，主要针对临时使用计算机的用户，对操作系统拥有极为有限的访问权限和权利。-->对

47、Windows 操作系统内置了“本地安全策略”功能，可以针对本地主机配置安全策略，管理员使用 secpol.cpl 命令，来打开“本地安全策略”窗口。-->错

48、Windows 操作系统内置了“本地安全策略”功能，可以针对本地主机配置安全策略。-->对

49、Windows 自带的备份工具既可以备份本机的系统状态也可以备份远程计算机的系统状态。-->错

50、WSUS 服务的部署方案主要有：单服务器方案和链式方案。-->对

51、WWW 主要通过超文本向用户提供网页信息。-->对

52、() 是一种网络监测功能，可以收集流入和流出网络接口的 IP 数据包。-->错

53、按照防火墙实现的技术不同，可以分为硬件防火墙和软件防火墙。-->错

54、包过滤防火墙，通常是在网络的入口对通过的数据包进行选择，只有满足条件的数据包才能通过（进入企业内部网络），否则被抛弃。-->对

55、备份的主要目标是保证数据安全性，保存的是历史数据，恢复时间相对长；而容灾的主要目标是防止生产数据丢失或数据中心遭受毁灭性灾难，快速恢复，保证业务连续性。-->对

56、备份软件是备份系统的核心，负责维护所有的备份配置信息（涉及客户端、介质代理、备份设备等）。-->错

57、备份系统的组件包括备份管理系统、备份客户端、备份软件和备份介质。-->错

58、被动测量会向网络中注入额外的数据包，从而对网络的实际行为造成影响，可能会遮盖网络行为的本来面目，因此，测量结果也会造成一定的偏差。-->错

59、标准帐户通常分配给最终用户使用，适用于日常工作，对操作系统拥有一些基本的权限和权利。-->对

60、病毒是通过磁盘、网络等媒介传播扩散并能够“传染”其他程序的程序。-->对

61、不可以匿名访问 IIS 网站。-->错

62、部署五节点的故障转移群集后，其中四节点故障，群集依然可以正常使用。-->错

63、常见的网络数据备份系统，按其架构不同可以分为 7 种备份组网方式。-->错

64、常用的加密算法有对称加密算法和非对称加密算法。-->对

65、传输控制协议 (TransmissionControlProtocol, TCP) 是面向数据报文的传输层协议。在基于 TCP 的主动测量过程中，测量主机需要向被测量主机发送探测数据包，但通信双方之间的传输没有明确的连接（类似于邮件传输），通信双方是对等的，单次传输的最大数据量取决于具体的网络。-->错

66、传统的加密系统是以密钥为基础的，这是一种对称加密方法，也就是说，用户使用同一个密钥加密和解密。-->对

67、从 Windows7 开始，Windows 操作系统才内置了软件防火墙功能。-->错

68、大部分的网络是基于 TCP/IP 协议构建的，网络系统管理员在排除网络故障时，可以参考 TCP/IP 协议的分层思想。-->对

69、代理服务器能够记录用户的 IP 地址、帐户、请求时间、访问地址、信息长度等详细数据，可以进行分类统计和记账。-->对

70、代理服务器通常设置在企业内部网络中客户端与外部网络中服务器之间，它会暂存客户端发来的请求，并由自己发出这些请求。-->对

71、带宽通常表示网络传输路径或链路的传输容量，即数据包的传输速度。-->对

72、当用户访问计算机系统、应用程序、网络资源时，无需进行身份凭据的验证。-->错

73、当员工离职后，为了避免员工继续访问工作资源，企业可以选择将证书进行吊销操作。-->对

74、丢包率是单位时间内传输中丢失的数据包与所有数据包的比值。数据包丢失一般是由网络拥塞引起的，当丢包率超过 15% 时，可能会导致网络不可用。-->对

75、独立 CA 无法部署在 AD 环境内。-->错

76、发起 PPP 连接后，链路将经过 4 个会话建立阶段。-->错

77、防火墙不能防止被病毒感染过的程序和文件进出网络。-->对

78、防火墙不能完全消除来自内部网络的威胁，但防火墙能够防止被病毒感染过的程序和文件进出网络。-->错

79、防火墙客户端不支持身份验证。-->错

80、防火墙客户端支持 DNS 转发。-->对

81、防火墙客户端支持身份验证。-->对

82、访问 FTP 服务器不可以匿名访问。-->错

83、访问 FTP 服务器可以匿名访问。-->对

84、服务可用性是指用户可使用数据和服务的时间百分比（通常以周作为单位）。-->错

85、根据测量点的位置，可以分为端系统测量和中间系统测量。-->对

86、根据测量过程中是否向网络系统中注入探测数据包，可以将测量方式分为主动测量和被动测量。-->对

87、根据防火墙的功能，网络系统管理员不可以基于数据包的源端口、目标端口，来阻止或允许进出企业内部网络的数据包。-->错

88、根据防火墙的功能，网络系统管理员可以基于数据包的源地址、目标地址，来阻止或允许进出企业内部网络的数据包。-->对

89、故障管理 (FaultManagement) 的主要任务是创建、检测和控制网络的配置状态。-->错

90、故障管理 (FaultManagement) 的主要任务是当网络运行出现异常（故障）时，能够迅速找到故障的位置和原因，对故障进行检测、诊断、隔离和纠正，以恢复网络的正常运行。-->对

91、故障管理 (FaultManagement) 的主要任务是当网络运行出现异常（故障）时，能够迅速找到故障的位置和原因，对故障进行检测、诊断、隔离和纠正，以恢复网络的正常运行。-->对

92、故障转移群集的节点数必须为偶数，否则群集无法正常使用。-->错

93、故障转移群集的节点数必须为奇数，否则群集无法正常使用。-->错

94、故障转移群集的所有节点 IP 地址必须位于同一个子网络。-->错

95、故障转移群集的所有节点 IP 地址不必位于同一个子网络。-->对

96、故障转移群集节点故障可以实现自动切换到其他节点，也可以手动切换到其他节点。-->对

97、故障转移群集无法实现单节点工作。-->错

98、故障转移群集中的每个节点必须独立存储设备。-->错

99、故障转移群集中的所有节点共享存储设备。-->对

100、管理信息库 (ManagementInformationBase, MIB) 是一个存储网络管理信息的数据库，由被管理对象组成。-->错

101、管理信息库 (MIB, ManagementInformationBase) 是一个存储网络管理信息的数据库，由被管理对象组成。-->对

102、管理员可以设置让 FTP 站点允许或拒绝某台特定计算机或某一组计算机来访问该 FTP 站点中的文件。-->对

103、管理员审批补丁的方式有：手动审批和自动审批。-->对

104、宏病毒，是一种寄生于文档或模板的宏中的计算机病毒。-->对

105、缓冲区是指应用程序或操作系统用来保存数据的临时区域。-->对

106、恢复点目标 (RecoveryPointObject, RPO) 是指故障后恢复数据和服务上线所需的时间量。-->错

107、恢复时间目标 (RecoveryTimeObject, RTO) 是指故障后恢复数据和服务上线所需的时间量。-->对

108、基本的网络测试命令有：Ping 命令、Tracert 命令、Show 命令和 Debug 命令等。-->对

109、基于访问日志的数据采集方式既可以对 IP 地址进行流量计费，又可以对用户流量计费。-->错

110、基于计算机病毒的感染途径，可以将计算机病毒分为文件型计算机病毒、引导型计算机病毒和宏病毒。-->对

111、基于局域网 (LAN-Base) 结构是最简单的备份组网方式。在大多数情况下，这种备份是使用服务器主机上自带的备份介质，而备份操作往往也是通过手工操作的方式进行的。-->错

112、基于流量计费是根据用户在一段时间内所使用的全部网络流量（发送和接收）统计数据来收取用户费用的一种计费方式。-->对

113、基于使用时间的计费最早应用于传统电话，它是根据用户使用网络的时间长短来收取用户费用的一种计费方法。-->对

114、基于主机的入侵检测系统是针对整个网络的入侵检测系统，包括对网络中的所有主机、网络设备进行入侵行为的监测和响应。-->错

115、基于主机的入侵检测系统只关注主机上发生的入侵事件，而不会监测网络上的情况。-->对

116、计费管理的组件包括：计费数据的采集和存储；数据的分析和统计；与用户、管理员之间的人机交互界面。-->对

117、计费管理为网络资源成本计算和收费提供依据，它记录网络资源的使用情况、提出计费报告、为网络资源的使用核算成本和提供收费依据。-->对

118、计费管理为网络资源成本计算和收费提供依据，它记录网络资源的使用情况、提出计费报告、为网络资源的使用核算成本和提供收费依据。-->对

119、计算机病毒的整个生命周期一般由四个阶段组成，即：潜伏阶段、传播阶段、发作阶段和破坏阶段。-->错

120、计算机病毒是一种人为制造的程序，它不会自然产生，而是由精通编程的人精心编制的。-->对

121、计算机病毒危害的“宿主”通常是指正常工作的计算机和网络。-->对

122、加密技术的基本思想是伪装信息，使未授权者不能理解它的真实含义。-->对

123、简单来说，云存储就是将数据资源放到云计算平台上供人读写的一种方案。-->对

124、将某种业务的 RPO 设置为 6 小时，表示该业务能容忍最多 6 小时的数据丢失，所以必须每 6 小时至少执行一次备份，同时还要考虑执行备份所需的时间。-->对

125、经典的加密方法，主要使用了 3 种加密技术：替换加密、换位加密和一次性填充。-->对

126、拒绝服务攻击会不断对网络服务系统进行干扰，改变其正常的运行流程，执行无关应用程序，大量消耗硬件资源，使系统响应减慢，甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能得到已经授权的服务。-->对

127、据来收取用户费用的一种计费方式。-->对

128、抗抵赖性服务可防止发送方与接收方在执行各自操作后，否认各自所做的操作。-->对

129、可以匿名访问 IIS 网站。-->对

130、可以在 Windows 操作系统内置的“高级安全 Windows 防火墙”窗口中配置防火墙的进站规则和出站规则。-->对

131、链路带宽是指源节点到目的节点之间性能最低的链路所能达到的最大传输速度，也就是该传输路径所能提供给一个业务流的最大传输速度。-->错

132、密码策略用来设置帐户密码的安全性要求，如用户名的使用期限、长度和复杂性。-->错

133、默认时，Web 网站不允许任何计算机来访问它。-->错

134、默认时，当父容器的组策略设置与子容器的组策略设置发生冲突时，父容器的组策略设置最终生效。-->错

135、目标端重复数据删除是先将数据从业务中心传到备份中心，在备份中心存储时再删除重复数据。这种方法不会占用源端资源，但也不能节省传输带宽。-->对

136、目录服务恢复模式仅在域控制器上使用。-->对

137、目录服务恢复模式可以在域中任何一台计算机上使用。-->错

138、目录服务恢复模式只能在域控制器上使用。-->对

139、目前，EAP 主要应用在有线局域网方面。-->错

140、目前，EAP 主要应用在有线局域网方面。-->错

141、目前，最常用的备份介质有磁带、硬盘、光盘、云存储等。-->对

142、配置管理主要负责创建、检测和控制网络的配置状态。-->对

143、企业 CA 和独立 CA 均可以对证书模板进行自定义。-->错

144、企业从属 CA 只能部署在企业根 CA 之下。-->错

145、企业环境可以直接部署从属 CA，无需部署根 CA。-->错

146、认证（Authentication）是对用户的身份进行验证，判断其是否为合法用户。授权（Authorization）是对通过认证的用户，授权其可以使用哪些服务。计费（Accounting）是记录用户使用网络服务的资源情况，这些信息将作为计费的依据。-->对

147、认证服务器和票据授予服务器构成了密钥分发中心。-->对

148、任意 CA 颁发的证书均可安装并使用。-->错

149、容灾可认为是低级别的备份，容灾是备份的基础。-->错

150、如果 KDC 出现故障，那么客户端将无法请求票据并访问网络资源。-->对

151、如果没有预先经过同意就擅自使用网络或计算机资源，则被看作非授权访问。-->对

152、如果希望网络负载均衡群集中的节点之间可以互相通信，而节点主机均为单网络适配器，则群集操作模式应该选择多播模式。-->对

153、如果希望网络负载均衡群集中的节点之间可以互相通信，而节点主机均为单网络适配器则群集操作模式应该选择单播模式。-->错

154、如果由于安装了错误的显卡驱动程序或者设置了错误的分辨率而导致无法正常显示的话，则可以选择“启用 VGA 模式”进行修复。-->对

155、入侵检测就是对各种入侵行为的发现与报警，是一种通过观察通信行为，根据安全日志或审计数据来检测入侵的技术。-->对

156、软件防火墙（也称为基于主机的防火墙）一般是安装在计算机上的软件，执行与硬件防火墙相同或类似的功能。-->对

157、三节点故障转移群集的仲裁模式只能选择多数节点模式。-->错

158、散列值只被用于提供数据完整性。-->对

159、上网行为管理是指控制和管理用户对网络的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析、上网人员管理等。-->对

160、身份验证，属于配置管理的主要功能。-->错

161、审核技术能够记录用户使用计算机网络系统进行各种活动的过程，记录系统产生的各类事件。-->对

162、数据包分析工具是一种可以捕获和记录网络数据包的工具，可以帮助网络系统管理员解决网络问题、检查网络安全隐患、显示数据包传输状态、学习网络传输协议。-->对

163、数据保密性服务可防止未授权的对数据的修改操作。-->错

164、数据保密性服务与公证机制具有相关性。-->错

165、数据的备份是整个灾备系统的基础。通常可以将灾难恢复方案分为离线灾难恢复和在线灾难恢复。-->对

166、数据的预处理是要对采集到的数据包进行分类、过滤、计数和归并。-->对

167、数据分析结果通常有两种交付形式：一是统计报表，二是可视化图形。-->对

168、数据链路层负责在网络层与传输层之间进行信息传输，数据帧的封装、解封装、差错校验等。-->错

169、数据完整性的检测方法是基于一种单向的数学函数（散列函数），这种函数相对来说易于计算，而且也容易作逆运算。-->错

170、数字电压表的工作方式是通过电缆定时发送脉冲，监听反射回来的信号。-->错

171、数字签名是保证数据完整性和抗抵赖性的一种重要手段。-->对

172、特洛伊木马是把自己伪装成为善意应用程序（进程）的恶意软件程序。-->对

173、通常可以把网络信息安全的问题划分为物理层、网络层、数据层和内容层 4 个层面。-->对

174、通常可以将网络管理系统分为管理站（Manager）和服务器（Server）两部分。-->错

175、通常情况下，代理服务有利于保障网络终端的隐私或安全，防止源自内部的攻击。-->错

176、通过启动病毒实时监控系统并且及时升级病毒库，可以有效保护计算机的安全。-->对

177、通过上网行为管理产品，网络系统管理员可以制定精细的带宽管理策略，对不同岗位的员工、不同网络应用划分带宽通道，并设定优先级，合理利用有限的带宽资源，确保网页下载文件的合法性。-->错

178、通过上网行为管理产品，网络系统管理员可以制定精细的带宽管理策略。-->对

179、同步远程复制能够向异地提供最新的数据，但应用程序会因等待写入完成指示而被延迟一段时间。-->对

180、吞吐量是描述网络设备转发速度的性能指标。其度量单位通常是字节/秒（Byte/s）。-->错

181、完成 IIS 安装后，可以使用一个默认网站，该网站没有任何内容，无法浏览。-->错

182、完全备份是在某一个时间点上对所有数据的一个完全复制。这种备份方式的优点是备份速度快，备份数据量较少，没有重复的备份数据。-->错

183、网卡硬件故障属于链路故障。-->对

184、网络测量是利用测量工具检测网络设备或网络系统运行状态、获取网络性能参数的过程。-->对

185、网络层提供用户服务，如网页服务、电子邮件服务、文件传输服务、域名查询服务等。-->错

186、网络负载均衡群集的所有节点 IP 地址必须位于同一个子网络。-->对

187、网络负载均衡群集的所有节点 IP 地址不必位于同一个子网络。-->错

188、网络负载均衡群集最多可以配置 32 个节点。-->对

189、网络负载均衡群集最多可以配置 64 个节点。-->错

190、网络故障大致可以分为 4 类，即应用故障、协议故障、操作故障和服务故障。-->错

191、网络故障诊断是以网络原理、网络配置和网络运行的知识为基础，从故障现象入手，以网络诊断工具为手段获取诊断信息，

确定网络故障点，查找问题的根源并排除故障，恢复网络正常运行的过程。-->对

192、网络管理包括五大功能：故障管理、配置管理、计费管理、性能管理和服务管理，简称为 FCAPS。-->错

193、网络管理员不需要经常对网络系统的各方面性能进行监视。-->错

194、网络链路的问题通常是由网卡、跳线、信息插座、交换机、UPS 等设备和服务配置引起的。-->错

195、网络系统管理是指对网络的运行状态进行监测和控制，使其能够安全、可靠、高效、经济地为客户提供服务。-->对

196、伪装前的原始数据称为密文，伪装后的数据称为密钥，伪装的过程称为加密，加密在加密密钥的控制下进行。-->错

197、物理层安全是指对网络与信息系统的运行状态的保护，主要关注的是信息系统的安全。-->错

198、系统内置的 Administrator 用户帐户和 Administrators 组帐户的成员就属于管理员帐户。-->对

199、系统数据主要是指操作系统、数据库系统安装的各类软件包和应用系统执行程序。-->对

200、性能管理的主要内容是对网络系统资源的吞吐量、使用率、时延、拥塞等系统性能进行分析，实现网络性能的监控和优化。-->对

201、需要经过 4 个会话阶段，才能建立一条完整的 PPP 链路。-->错

202、一般的网络管理系统分为管理站 (Manager) 和代理 (Agent) 两部分。-->对

203、一个 GPO 可以同时被链接到多个组织单位上。-->对

204、异步远程复制对应用程序性能的影响最小，而且异地磁盘系统在数据的更新程度也不会有任何延迟。-->错

205、因为 TCP 协议是面向连接的，所以通过测试 TCP 的性能反映发送端与接收端之间的性能参数。-->对

206、引导型计算机病毒会影响计算机系统中的可执行文件 (.exe) 和命令文件 (.com)。-->错

207、应用层防火墙，也称为代理。它接受来自内部网络用户的通信，然后与外部网络服务器建立单独连接，而不允许内部网络与外部网络直接通信，它在应用层的通信中扮演着一个消息传递者的角色。-->对

208、应用数据主要是指保证业务系统正常运行所使用的系统目录、用户目录、系统配置文件、网络配置文件、应用配置文件、存取权限控制等。-->错

209、用户在客户端计算机上可以使用浏览器浏览 Web 服务器上的信息。-->对

210、用于发送电子邮件的 TCP/IP 协议是 SMTP 协议。-->对

211、与 LAN-Base 结构相比，LAN-Free 结构让多台服务器共享备份介质，备份数据不再经过局域网，而直接从磁盘阵列传到备份介质内。-->对

212、灾难恢复工作包括灾难发生后的应急响应与处置、信息系统在灾难备份中心的恢复和重新运行、业务系统的灾后重建和回退工作。-->对

213、灾难恢复是指将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。-->对

214、在 Cisco 公司的交换机上，可以使用 showvlan 命令查看交换机配置的 VLAN 相关信息。-->对

215、在 IIS 中创建站点使用的物理路径必须保存在 C 盘目录下。-->错

216、在 Windows Server 操作系统中，网络负载均衡群集是实现高可用性的重要功能之一。-->对

217、在 Windows Server 中，FTP 服务功能可以独立安装，不依赖于其他功能。-->错

218、在 Windows 操作系统的命令提示符窗口中输入“ping127.0.0.1”，能够根据响应结果，判断本机的 TCP/IP 协议设置是否正常。-->对

219、在 Windows 操作系统的命令提示符窗口中输入“ping127.0.0.1”，能够判断本机的 TCP/IP 协议设置是否正常。-->错

220、在 Windows 操作系统的命令提示符窗口中输入 arp-a 命令，会显示所有网卡接口的 ARP 缓存表。-->对

221、在 Windows 操作系统中，FTP 客户端必须使用第三方工具。-->错

222、在测量单向时延时，首先应该使测量节点 A 和测量节点 B 的时间同步，然后在节点 A 形成一个 64 字节的 UDP 数据包，获取节点 A 的时间后在包头部加载一个时间戳 (A) 并立即发出，当节点

B 完整地接收到这个数据包后，立即获取接收时间 (B)，则“B 减 A”的值即为该链路的单向时延。-->对

223、在防火墙的处理方式中，Drop 是指丢弃数据包，并且不通告数据源。-->对

224、在防火墙的处理方式中，Receive 是指允许数据包通过。-->错

225、在计费系统的三层体系结构中，数据层通常作为用户输入和获取数据的接口，通常由 Web 浏览器 (或计费软件控制台) 和处理请求的模块组成。-->错

226、在计算机上安装防病毒软件是一项必不可少的安全措施。-->对

227、在设置组策略时，当父容器的组策略设置与子容器的组策略设置没有冲突时，子容器会继承父容器的组策略设置。-->对

228、在网络负载均衡群集中，所有节点会随机接收访问请求，无法控制优先级。-->错

229、在一个 Windows 域中，可以把链接在一个组织单位上的 GPO 链接到另一个组织单位上。-->对

230、在一个域上可以同时链接多个 GPO。-->对

231、在一个域中不能包含组织单位。-->错

232、在一个组织单位上可以同时链接多个 GPO。-->错

233、在一个组织单位上可以同时链接多个 GPO。-->对

234、在一个组织单位中可以包含多个域。-->错

235、帐户锁定时间，用于指定已锁定的帐户在自动解锁之前保持锁定状态的时长。-->对

236、帐户锁定时间设置，用于指定已锁定的帐户在手动解锁之前保持锁定状态的时长。-->错

237、证书只要未到期就可以正常使用。-->错

238、只有企业 CA 才能对证书模板进行自定义。-->对

239、主动测量方法的优点包括：不依赖于被测量对象的测量能力，能直接测量和分析网络性能；适合端到端的网络性能测量，对于所关注的内容只要在本地发送测试数据包，然后观察网络的响应即可；测量方式不涉及用户的网络信息，所以对用户而言安全性好。-->对

240、状态检测防火墙，又称自动包过滤防火墙。-->错

名词配伍题(18)一

1、①ICMP; ②Frame-Realy; ③TCP; ④SNMP; ⑤ipconfig

①	ICMP	a	采用“三次握手+四次断开”的方式来建立与断开连接。
②	Frame-Realy	b	是TCP/IP协议族中的网络管理协议,定义了传送管理信息的协议消息格式、管理站和代理之间进行消息传送的规则,能对IP网络中不同类型的设备进行监控和管理。
③	TCP	c	用于显示本机的TCP/IP网络配置值。
④	SNMP	d	是TCP/IP协议族中IP层的一个重要协议,提供了差错报告和IP设备间重要信息交换的机制,被广泛应用于网络的管理和主动测量方法之中。
⑤	ipconfig	e	一种二层数据帧的封装格式。

正确答案: 1、d2、e3、a4、b5、c

2、①MD5; ②NCP; ③PAP; ④TACACS+; ⑤SSL记录协议

①	MD5	a	用于封装多种网络层协议(如IP、IPX、AppleTalk)报文并通过同一条PPP数据链路发送它们。
②	NCP	b	以明文方式发送密码,也就是没有经过加密,因此如果在传输进程中被拦截,密码有可能外泄,比较不安全。
③	PAP	c	默认使用TCP49端口,并且对不同的设备采用不同的授权、认证和记账方法。
④	TACACS+	d	是一种单向函数,这使得从给定输入数据计算出散列值很容易,但要从散列值反向计算出输入数据则不可行。
⑤	SSL记录协议	e	建立在可靠的传输协议(如TCP)之上,为高层协议提供数据封装、压缩、加密等基本功能的支持。

正确答案: 1、d2、a3、b4、c5、e

3、①MIB②Kerberos③DES④IPSec⑤SSL

①	MIB	a	是一种对称密钥算法。
②	Kerberos	b	建立在网络层之上,可以保护网关之间、主机之间或网关与主机之间的路径安全。
③	DES	c	是Netscape公司首先提出了一个标准,一个传输层安全协议,用以保障在Internet上数据传输的安全。
④	IPSec	d	是一个存储网络管理信息的数据库,由被管理对象组成。
⑤	SSL	e	是一种基于票据(Ticket)的认证方式,其设计目标是通过使用一台中央服务器提供“票据”,而网络中提供资源的服务器和访问资源的客户端之间使用这个“票据”相互识别。

正确答案: 1、d2、e3、a4、b5、c

4、①SNMP的Trap报文; ②数据加密; ③管理员帐户; ④MD5; ⑤应用数据

①	SNMP的Trap报文	a	拥有管理本台计算机的所有权限和权利。
②	数据加密	b	是一种单向函数,这使得从给定输入数据计算出散列值很容易,但要从散列值反向计算出输入数据则不可行。
③	管理员帐户	c	用于代理主动向管理站通告重要事件的报文。
④	MD5	d	主要是指业务系统的所有业务数据,对数据的安全性、准确性、完整性、一致性要求很高,而且变化频繁。
⑤	应用数据	e	是防止未经授权的用户访问敏感信息的手段,这就是人们通常理解的安全措施,也是其他安全方法的基础。

正确答案: 1、c2、e3、a4、b5、d

5、①TLS; ②IPsec; ③ProxyServer; ④CIDF; ⑤RTO

①	TLS	a	提供代理服务的计算机或其他网络设备。
②	IPsec	b	是指故障后恢复数据和服务上线所需的时间量。
③	Proxy Server	c	对SSL进行了改进,用于保证Web通信以及其他流行协议的安全。
④	CIDF	d	将入侵检测系统分为4个组件:事件产生器、事件分析器、事件数据库、响应单元。
⑤	RTO	e	提供的安全功能包括:保密性、完整性、身份验证和安全密钥交换。

正确答案: 1、c2、e3、a4、d5、b

6、①备份客户端; ②云存储; ③CMIP; ④帐户锁定时间; ⑤认证服务

①	备份客户端	a	用于指定已锁定的帐户在自动解锁之前保持锁定状态的时长。
②	云存储	b	能够确保某个实体身份的可靠性,可分为两种类型。
③	CMIP	c	指一个以数据存储和管理为核心的云计算系统。
④	帐户锁定时间	d	是构建于OSI参考模型上的网络管理协议,与之相关的CMIS(Common Management Information Service,通用管理信息服务)定义了获取、控制和接收有关被管理对象运行状态的服务。
⑤	认证服务	e	是需要备份数据的业务主机,它负责提供要备份的数据,一般需安装备份软件客户端代理程序。

正确答案: 1、e2、c3、d4、a5、b

7、①差异备份; ②认证服务; ③缓冲区; ④宏病毒; ⑤包过滤防火墙

①	差异备份	a	通常是在网络的入口对通过的数据包进行选择,只有满足条件的数据包才能通过(进入企业内部网络),否则被抛弃。
②	认证服务	b	提供对通信中对等实体和数据来源的鉴别。
③	缓冲区	c	是一种寄存于文档或模板的宏中的计算机病毒。
④	宏病毒	d	是指应用程序或操作系统用来保存数据的临时区域。
⑤	包过滤防火墙	e	是以最近一次完全备份为基准,对最近一次完全备份后到进行差异备份的这段时间内,发生变化的数据进行备份。

正确答案: 1、e2、b3、d4、c5、a

8、①访问控制服务; ②基于主机的入侵检测系统; ③RSA; ④中间人攻击; ⑤代理

①	访问控制服务	a	入侵者可以拦截网络中正常的通信数据,并修改和控制通信双方的TCP会话,而通信的双方却毫不知情,入侵者就可以使用抓包软件查看双方的通信内容。
②	基于主机的入侵检测系统	b	是使用不同的密钥进行加密和解密的一种加密算法。
③	RSA	c	对资源提供保护,防止非授权的访问和操纵。
④	中间人攻击	d	是一种网络服务,允许一个网络终端(如客户端计算机)通过这个服务与另一个网络终端(如Web服务器、邮件服务器、DNS服务器)进行非直接连接。
⑤	代理	e	运行在受保护设备上(如计算机)的,用于监测主机操作系统和系统本地用户的状况。

正确答案: 1、c2、e3、b4、a5、d

9、①蠕虫; ②特洛伊木马; ③中间人攻击; ④泛洪; ⑤社会工程攻击

①	蠕虫	a	入侵者可以拦截网络中正常的通信数据,并修改和控制通信双方的TCP会话,而通信的双方却毫不知情,入侵者就可以使用抓包软件查看双方的通信内容。
②	特洛伊木马	b	把自己伪装成善意应用程序(进程)的恶意软件程序。
③	中间人攻击	c	是指入侵者可以向网络中发送大量的无用数据包,使网络设备

			(如交换机)满负荷或超负荷运行,导致网络性能下降,甚至瘫痪。
④	泛洪	d	入侵者利用或操控企业内部人员,获取他们所需要的信息,包括电话诈骗;试图套出公司员工的名字和口令;伪装成为合法人员。
⑤	社会工程攻击	e	可以占领计算机的内存空间,以自我复制的方式从一台计算机通过网络蔓延到另一台计算机。

正确答案: 1、e2、b3、a4、c5、d

10、①事件数据库; ②端口认证; ③备份网络; ④服务可用性; ⑤中间系统测量

①	事件数据库	a	是指备份数据由备份客户端到备份服务器的传输路径。
②	端口认证	b	是指用户可使用数据和服务的时间百分比(通常以年作为单位)。
③	备份网络	c	是指在网络设备(如路由器、交换机)上进行的测量。
④	服务可用性	d	是指允许远程用户通过某个进入点(端口)访问另一个网络。
⑤	中间系统测量	e	负责存放有关事件的各种中间过程数据和最终数据,它可以是面向对象的复杂数据库,也可以是简单的文本文件。

正确答案: 1、e2、d3、a4、b5、c

11、①数据保密性服务; ②数据完整性服务; ③访问控制服务; ④认证服务; ⑤路由控制机制

①	数据保密性服务	a	可以防止对任何资源的非授权访问,确保只有经过授权的实体才能访问相应的资源。
②	数据完整性服务	b	采用加密手段,防止数据被破解后泄露。
③	访问控制服务	c	能够确保某个实体身份的可靠性。
④	认证服务	d	为数据发送方选择安全的网络通信路径,避免发送方使用不安全路径发送数据而受到攻击,以提高数据的安全性。
⑤	路由控制机制	e	可防止未授权的对数据的修改操作。

正确答案: 1、b2、e3、a4、c5、d

12、①数字电压表; ②时域反射计; ③电缆测试仪; ④协议分析仪; ⑤网络管理软件

①	数字电压表	a	可以在网络中的每一帧中提供应用层、传输层、网络层和数据链路层信息。
②	时域反射计	b	可用于进行链路连通性测试,可以测量诸如交直流电压、电流、电阻、电容以及电缆连续性等参数,利用这些参数可以检测物理连通性。
③	电缆测试仪	c	可以对所连接的网络进行网络监视,判断网络运行是否正常,还可以进行协议分析,能够对网络上的协议或者通信问题进行故障诊断。
④	协议分析仪	d	可用于确定电缆断开的具体位置。通过电缆定时发送脉冲,监听反射回来的信号。
⑤	网络管理软件	e	针对 OSI 模型的第一层设计的,它只能用来测试电缆而不能测试网络的其他设备。

正确答案: 1、b2、d3、e4、a5、c

13、①替换加密; ②换位加密; ③一次性填充; ④DES; ⑤RSA

①	替换加密	a	把明文变为一种编码(如 ASCII 编码),选择一个等长的随机字符串作为密钥,对二者进行逐位异或运算(两个值不相同,则异或结果为 1,否则异或结果为 0)得到密文。
---	------	---	------------------------------------------------------------------------------------

②	换位加密	b	将明文分成 64 位的块,对每个块进行 19 次变换(替换和换位),其中 16 次变换由 56 位的密钥的不同排列形式控制,最后产生 64 位的密文块。
③	一次性填充	c	用一个字母替换另一个字母。
④	DES	d	按照一定的规律重排字母的顺序。
⑤	RSA	e	其密钥的长度通常是 512 位~2 048 位,它的安全性基于大素数分解的困难性。

正确答案: 1、c2、d3、a4、b5、e

14、①完全备份; ②故障管理; ③业务流填充机制; ④特洛伊木马; ⑤硬件防火墙

①	完全备份	a	是指通过网络系统管理员快速地检查问题并启动恢复过程的工具,使得网络服务的可靠性得到增强。
②	故障管理	b	通常是位于企业网络边界上的一个小盒子,通过硬件和软件的结合达到隔离内外网络的目的。
③	业务流填充机制	c	是在某一个时间点上对所有数据的一个完全复制。
④	特洛伊木马	d	是把自己伪装成为善意应用程序(进程)的恶意软件程序。
⑤	硬件防火墙	e	通过在数据传输过程中传递随机数的方式,混淆真实的数据,加大数据破解的难度,提高数据的保密性。

正确答案: 1、c2、a3、e4、d5、b

15、①网络管理; ②性能分析; ③SNMP; ④防火墙; ⑤计算机病毒

①	网络管理	a	负责分析和统计历史数据,建立性能基线和性能分析的模型,预测网络性能的长期趋势。
②	性能分析	b	是指对网络的运行状态进行监测和控制,使其能够安全、可靠、高效、经济地为客户提供服务。
③	SNMP	c	是一种将企业内部网络与外部网络分离的方法,是在企业内部网络和外部网络之间所施加的安全防范系统。
④	防火墙	d	是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用,并且能自我复制的一组计算机指令或者程序代码。
⑤	计算机病毒	e	定义了一系列网络管理规范标准,提供了一个用来监测网络状态、管理配置文件、收集网络数据和检测网络行为的工具。

正确答案: 1、b2、a3、e4、c5、d

16、①硬件防火墙; ②应用层防火墙; ③状态检测防火墙; ④电路层防火墙; ⑤入侵检测系统

①	硬件防火墙	a	接受来自内部网络用户的通信,然后与外部网络服务器建立单独连接,而不允许内部网络与外部网络直接通信,它在应用层的通信中扮演着一个消息传递者的角色。
②	应用层防火墙	b	负责数据转发的独立系统,它由网关路由器建立通信双方的两个 TCP 连接,即一个连接网关与内部网络,另一个连接网关与外部网络。
③	状态检测防火墙	c	监视、分析用户及系统活动,查找非法用户和合法用户的越权操作。
④	电路层防火墙	d	又称动态包过滤防火墙,是包过滤的功能扩展
⑤	入侵检测系统	e	通常是位于企业网络边界上的一个小盒子,通过硬件和软件的结合达到隔离内外网络的目的。

正确答案: 1、e2、a3、d4、b5、c

17、①增量备份; ②抗抵赖性服务; ③一次性填充加密; ④密码散列(Hash)函数; ⑤PPP

①	增量备份	a	防止参与某次通信的任何一方事后否认本次通信或通信内容。
②	抗抵赖性服务	b	把明文变为一种编码(如 ASCII 编码), 选择一个等长的随机字符串作为密钥, 对二者进行逐位异或运算得到密文。
③	一次性填充加密	c	是一种数据链路层协议, 被设计用于点对点连接中传递数据, 使用用户名和密码进行验证, 并协调两个设备使用的网络协议。
④	密码散列 (Hash) 函数	d	是以最近一次备份(包括完全备份、差异备份、增量备份)为基准, 对最近一次备份后到进行增量备份的这段时间内, 发生变化的数据进行备份。
⑤	PPP	e	被设计用来验证和确保数据完整性。

正确答案: 1、d2、a3、b4、e5、c

18、①帐户锁定阈值; ②泛洪; ③流加密; ④基础数据; ⑤基于网络的入侵检测系统

①	帐户锁定阈值	a	是针对整个网络的入侵检测系统, 包括对网络中的所有主机、网络设备进行入侵行为的监测和响应。
②	泛洪	b	用于指定在用户帐户被锁定之前允许登录失败的次数。
③	流加密	c	主要是指保证业务系统正常运行所使用的系统目录、用户目录、系统配置文件、网络配置文件、应用配置文件、存取权限控制等。
④	基础数据	d	是将数据包与密钥生成二进制比特流进行异或运算的加密过程。
⑤	基于网络的入侵检测系统	e	是指入侵者可以向网络中发送大量的无用数据包, 使网络设备(如交换机)满负荷或超负荷运行, 导致网络性能下降, 甚至瘫痪。

正确答案: 1、b2、e3、d4、c5、a

操作题(66)一

- 1、在 ISA Server 上, 管理员需要创建发布规则, 把...
- 2、在 ISA Server 上创建“允许传出的 Ping 流量...”
- 3、在一台安装了 Windows 操作系统的服务器 Ser...
- 4、在一台安装了 Windows 操作系统的域控制器...
- 5、[请对应选择描述正确的一项]用于接收电子邮...
- 6、安装 FTP 的操作步骤:
- 7、安装 IIS 的操作步骤:
- 8、安装 SMTP 服务的操作步骤:
- 9、安装 SMTP 服务的操作步骤:
- 10、安装故障转移群集功能的操作步骤: ...
- 11、安装网络负载均衡功能的操作步骤: ...
- 12、安装证书服务的操作步骤:
- 13、把你的计算机配置为一台 SyGate 服务器, ...
- 14、备份计算机上 C:\movie 文件夹中的内容, 备份...
- 15、调整 IIS 网站的默认文档, 包括优先级调整、添...
- 16、调整网络负载均衡群集中指定节点的优先级操...
- 17、换位加密能够按照一定的规律重排字母的顺序...
- 18、换位加密能够按照一定的规律重排字母的顺序...
- 19、假设在域 abc.com 中有一个“研发部”OU, 在该 O...
- 20、将计算机上的备份文件 C:\movie bk.bkf 还原...
- 21、请对应选择描述正确的一项。
- 22、设置访问 FTP 服务器的 IP 地址限制...
- 23、使用 Windows 的 POP3 管理工具把你的计算机配...

- 24、使用 Winmail 在计算机上创建一个电子邮件域, ...
- 25、在一台安装了 Windows Server 操作系统的服务器 Se...
- 26、完成 CA 备份和还原的操作步骤: ...
- 27、为了允许普通的域用户账户能够在 DC 上登录到...
- 28、向故障转移群集中添加节点的操作步骤: ...
- 29、修改“Default Domain Controllers Policy...
- 30、在 ISA Server 上, 管理员需要创建发布规则, 以允...
- 31、在计算机上利用 IIS 创建一个 Web 网站: ...
- 32、在计算机上使用 Serv-U 创建一个 FTP 站点: ...
- 33、在计算机上使用 WindowsMediaServices 创建点...
- 34、在一台安装了 Windows Server 操作系统的服务...
- 35、在一台安装了 Windows Server 操作系统的服务...
- 36、在一台安装了 Windows Server 操作系统的服务...
- 37、在一台安装了 WindowsServer 操作系统的服务...
- 38、在一台安装了 WindowsServer 操作系统的服务...
- 39、在一台安装了 WindowsServer 操作系统的服务...
- 40、在一台安装了 WindowsServer 操作系统的服务...
- 41、在一台安装了 Windows 操作系统的服务器 Serve...
- 42、在一台安装了 Windows 操作系统的服务器 Serve...
- 43、在一台安装了 Windows 操作系统的服务器 Serve...
- 44、在一台安装了 Windows 操作系统的服务器 Serve...
- 45、在一台安装了 Windows 操作系统的服务器 Serve...
- 46、在一台安装了 Windows 操作系统的服务器 Serve...
- 47、在一台安装了 Windows 操作系统的服务器 Serve...
- 48、在一台安装了 Windows 操作系统的服务器 Serve...
- 49、在一台安装了 Windows 操作系统的服务器 Serve...
- 50、在一台安装了 Windows 操作系统的服务器 Serve...
- 51、在一台安装了 Windows 操作系统的服务器 Serve...
- 52、在一台安装了 Windows 操作系统的服务器 Serve...
- 53、在一台安装了 Windows 操作系统的服务器 Serve...
- 54、在一台安装了 Windows 操作系统的服务器 Serve...
- 55、在一台安装了 Windows 操作系统的服务器 Serve...
- 56、在一台安装了 Windows 操作系统的服务器 Serve...
- 57、在一台安装了 Windows 操作系统的服务器 Serve...
- 58、在一台安装了 Windows 操作系统的服务器 Serve...
- 59、在一台安装了 Windows 操作系统的服务器 Serve...
- 60、在一台安装了 Windows 操作系统的服务器 Serve...
- 61、在一台安装了 Windows 操作系统的服务器 Serve...
- 62、在一台安装了 Windows 操作系统的域控制器服...
- 63、在一台安装了 Windows 操作系统的域控制器服...
- 64、在一台安装了 Windows 操作系统的域控制器服...
- 65、在一台安装了 Windows 操作系统的域控制器服...
- 66、在一台安装了 Windows 操作系统的域控制器服...

1、在 ISA Server 上, 管理员需要创建发布规则, 把内部的 Web 服务器发布出来, 以允许外部用户访问。其中, 内部的 Web 服务器安装在计算机 PC1 (IP 地址: 192.168.1.1) 上; ISA Server 连接内部的网卡 IP 地址为: 192.168.1.200, 连接外部的网卡 IP 地址为: 131.107.1.200。

在 ISA Server 上, 管理员需要创建发布规则, 把内部的 Web 服务器发布出来, 以允许外部用户访问。其中, 内部的 Web 服务器安装在计算机 PC1 (IP 地址: 192.168.1.1) 上; ISA Server 连接内部的网卡 IP 地址为: 192.168.1.200, 连接外部的网卡 IP 地址为: 131.107.1.200。要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

步骤 1: \_\_\_\_\_ ①  
步骤 2: 在“欢迎使用新建 Web 发布规则向导”画面中输入发布规则的名称, 例如: 发布内部 Web 服务器, 然后单击【下一步】。  
步骤 3: \_\_\_\_\_ ②  
步骤 4: 由于只发布一个 Web 网站, 所以选择“发布单个网站或负载平衡器”, 然后单击【下一步】。  
步骤 5: 在弹出的窗口中, 选择 HTTP 方式, 然后单击【下一步】。 步骤 6: \_\_\_\_\_ ③  
步骤 7: 在弹出的窗口中, 在“路径”一项保留为空白, 即: 发布整个网站。然后, 单击【下一步】。  
步骤 8: \_\_\_\_\_ ④ 步骤 9: 在弹出的窗口中选择合适的 Web 侦听器, 以便通过此侦听器来侦听 Internet 用户的访问请求。  
步骤 10: 由于不需要身份验证, 因此选择“无委派, 客户端无法直接进行身份验证”, 然后单击【下一步】。

步骤 11: 在弹出的窗口中, 保留默认的“所有用户”, 然后单击【下一步】。 步骤 12: 出现“正在完成新建 Web 发布规则向导”画面时, 单击【完成】按钮。

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: D. 在 ISA Server 的管理控制台中, 单击左窗格中的“防火墙策略”, 然后单击任务窗格的“任务”选项卡, 接着单击“发布网站”。 ②: B. 在“规则操作”窗口中, 选择“允许”, 然后单击【下一步】。 ③: C. 在弹出的窗口中输入 PC1 的 IP 地址: 192.168.1.1。然后, 单击【下一步】。 ④: A. 在弹出的窗口中的“公用名称”中输入: 131.107.1.200, 以便让外部用户通过此 IP 地址来访问内部网站。然后, 单击【下一步】。

## 2、在 ISA Server 上创建“允许传出的 Ping 流量”的访问规则, 从而允许内部网中的用户可以使用 Ping 命令去访问外部网中的计算机。

在 ISA Server 上创建“允许传出的 Ping 流量”的访问规则, 从而允许内部网中的用户可以使用 Ping 命令去访问外部网中的计算机。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

步骤 1: \_\_\_\_\_ ①  
步骤 2: 在“欢迎使用新建访问规则向导”画面中输入访问规则的名称, 例如: 允许传出的 Ping 流量, 然后单击【下一步】。  
步骤 3: \_\_\_\_\_ ②  
步骤 4: 在“协议”窗口中, 单击下拉式箭头, 选择“所选的协议”。  
步骤 5: \_\_\_\_\_ ③  
步骤 6: \_\_\_\_\_ ④  
步骤 7: \_\_\_\_\_ ⑤  
步骤 8: 在“用户集”的画面中, 选择“所有用户”。接着, 单击【下一步】。  
步骤 9: 在“正在完成新建访问规则向导”画面中, 单击【完成】。  
步骤 10: 在弹出的警告窗口中, 单击【应用】按钮, 使该访问规则生效。

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( ) ⑤: ( )

答案: ①: C. 在 ISA Server 的管理控制台中, 单击左窗格中的“防火墙策略”, 然后单击任务窗格的“任务”选项卡, 接着单击“创建访问规则”。 ②: A. 在“规则操作”窗口中, 选择“允许”, 然后单击【下一步】。 ③: B. 单击【添加】按钮来添加协议, 单击“通用协议”, 从中选择“PING”, 然后单击【添加】按钮。接着, 单击【下一步】。 ④: D. 在“访问规则目标”的画面中, 单击“网络”, 从中选择“外部”, 然后单击【添加】按钮。接着, 在左图中单击【下一步】。

## 3、在一台安装了 Windows 操作系统的服务器 Server8 上, 管理员需要创建一个防火墙规则: 拒绝此服务器 (Server8) 访问任何远程计算机的 443 端口的访问。

在一台安装了 Windows 操作系统的服务器 Server8 上, 管理员需要创建一个防火墙规则: 拒绝此服务器 (Server8) 访问任何远程计算机的 443 端口的访问。要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

步骤 1: \_\_\_\_\_ ①

步骤 2: 在左侧导航栏中, 右击“出站规则”并单击“新建规则”。在“规则类型”对话框中, 选择“自定义”选项, 单击“下一步”。

步骤 3: 在“程序”对话框中, 单击“下一步”。 步骤 4: \_\_\_\_\_ ②

步骤 5: 在“作用域”对话框中, 单击“下一步”。 步骤 6: \_\_\_\_\_ ③

步骤 7: 在“配置文件”对话框中, 单击“下一步”。

步骤 8: \_\_\_\_\_ ④

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: D. 登录服务器 Server8, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 wf.msc, 单击“确定”。 ②: F. 在“协议和端口”对话框中, 选择“协议类型: TCP”、“远程端口: 特定端口、443”, 单击“下一步”。 ③: A. 在“操作”对话框中, 选中“阻止连接”选项, 单击“下一步”。 ④: B. 在“名称”对话框中, 输入规则名称后, 单击“下一步”。

## 4、在一台安装了 Windows 操作系统的域控制器服务器 Server9 上, 管理员需要设置 Windows 防火墙属性: 记录被丢弃的数据包。

在一台安装了 Windows 操作系统的域控制器服务器 Server9 上, 管理员需要设置 Windows 防火墙属性: 记录被丢弃的数据包。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

步骤 1: \_\_\_\_\_ ①

步骤 2: 在左侧导航栏中, 右击“本地计算机上的高级安全 Windows 防火墙”并单击\_\_\_\_\_ ②

步骤 3: 在弹出的对话框中, 单击\_\_\_\_\_ ③ 右侧的“自定义”。

步骤 4: 在弹出的对话框中, 在\_\_\_\_\_ ④ 右侧的列表框中, 选择“是”, 然后单击“确定”。

步骤 5: 返回上一级对话框, 单击“确定”。

步骤 6: 关闭“高级安全 Windows 防火墙”窗口。

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: D. 登录服务器 Server9, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 wf.msc, 单击“确定”。 ②: F. 属性 ③: A. 日志 ④: B. 记录被丢弃的数据包

## 5、[请对应选择描述正确的一项]用于接收电子邮件。

用于接收电子邮件。(POP3 协议)

默认时, 网站中所有资源存储的文件夹。(主目录) 接收并转发用户电子邮件的服务器。(邮件服务器)

将文件从 FTP 等服务器中复制到用户自己的计算机上。(下载,)

建立 Web 站点的工具。(Is)

## 6、安装 FTP 的操作步骤:

步骤 1: 登录 WindowsServer2016, 打开服务器管理器工具。

步骤 2: 单击添加角色和功能按钮, 进入添加角色和功能向导。

步骤 3: 依次点击下一步, 在“服务器角色”界面中, 勾选安装 Web 服务器 (IIS) 角色。

步骤 4: 在“角色服务器”界面中, 勾选安装 FTP 服务器角色。

步骤 5: 依次点击下一步, 完成 FTP 的安装。

## 7、安装 IIS 的操作步骤。

步骤 1: 登录 WindowsServer2016, 打开服务器管理器工具。

步骤 2: 单击添加角色和功能 1 按钮, 进入添加角色和功能 2 向导。

步骤 3: 依次点击下一步, 在“服务器角色”界面中, 勾选安装 Web 服务器 (IIS) 角色。

步骤 4: 依次点击下一步, 完成 IIS 的安装。

## 8、安装 SMTP 服务的操作步骤:

步骤 1: 登录 WindowsServer2016, 打开服务器管理器工具。

步骤 2: 单击添加角色和功能按钮, 进入添加角色和功能向导。

步骤 3: 依次单击下一步, 在“功能”界面中, 勾选安装 SMTP 服务器功能。

步骤 4: 依次单击下一步, 完成 IIS 的安装。

## 9、安装 SMTP 服务的操作步骤:

步骤 1: 登录 WindowsServer2016, 打开服务器管理器工具。

步骤 2: 单击**添加角色和功能 1**按钮, 进入**添加角色和功能 2**向导。  
步骤 3: 依次点击下一步, 在“**功能**”界面中, 勾选安装 **SMTP 服务器** 功能。  
步骤 4: 依次点击下一步, 完成 IIS 的安装。

#### 10、安装故障转移群集功能的操作步骤:

步骤 1: 登录 WindowsServer2016, 打开**服务器管理器**工具。  
步骤 2: 单击**添加角色和功能 1**按钮, 进入**添加角色和功能 2**向导。  
步骤 3: 依次点击下一步, 在“**功能**”界面中, 勾选**安装故障转移群集**功能。  
步骤 4: 依次点击下一步, 完成 IIS 的安装。

#### 11、安装网络负载均衡功能的操作步骤:

步骤 1: 登录 WindowsServer2016, 打开**服务器管理器**工具。  
步骤 2: 单击**添加角色和功能 1**按钮, 进入**添加角色和功能 2**向导。  
步骤 3: 依次点击下一步, 在“**功能**”界面中, 勾选安装**网络负载均衡**功能。  
步骤 4: 依次点击下一步, 完成 IIS 的安装。

#### 12、安装证书服务的操作步骤:

步骤 1: 登录 WindowsServer2016, 打开**服务器管理器**工具。  
步骤 2: 单击**添加角色和功能 1**按钮, 进入**添加角色和功能 2**向导。  
步骤 3: 依次点击下一步, 在“**服务器角色**”界面中, 勾选安装 **ActiveDirectory 证书服务**角色。

步骤 4: 依次点击下一步, 完成 IIS 的安装。

#### 13、把你的计算机配置为一台 SyGate 服务器,

它使用 ADSL 或以太网宽带接入 Internet, 使用一个网卡连接内部局域网 (IP 地址为: 192.168.1.100)。

##### 【操作步骤】

步骤 1: **C. 把这台计算机的网卡的 IP 地址设置为: 192.168.1.100, 然后使用宽带连接将这台计算机连接到 Internet**

步骤 2: **B. 双击 SyGate 软件的安装文件, 它会启动安装程序, 然后单击【下一步】按钮**

步骤 3: 在“许可证协议”窗口中, 浏览一下授权协议书, 如果可以接受这个协议书的话, 单击【是】按钮。必须接受这个授权协议书才能安装 SyGate 软件, 否则会终止程序的安装。

步骤 4: **D. 在“选择目的地位置”窗口中指定程序的安装路径, 单击【下一步】按钮**

步骤 5: 在“选择程序文件夹”对话框中设定安装程序将要在【开始】菜单中创建的程序组的名称, 安装者可以在这里自行设定一个名称, 然后单击【下一步】按钮, 便开始程序的安装。

步骤 6: **A. 在分页籍设置”窗口中选择安装模式。在这里, 应该选择【服务器模式】, 从而把这台计算机配置为 SyGate 服务器。另外, 还需要给这台计算机起一个名称, 以在网络中表示这台服务器, 当上述项目都设置完毕后, 单击【确定】按钮**

步骤 7: 将计算机连接到 Internet 上, 然后回到安装过程。SyGate 安装程序将验证 Internet 连接和 TCP/IP 协议设定。

步骤 8: 如果验证成功, 将会出现完成诊断网络的画面。

步骤 9: 接下来出现的就是完成画面。为了使安装生效, 必须重启计算机。当计算机重启的时候, SyGate 共享服务将自动启动, 而客户机将能够通过这个服务连接到 Internet 上。当系统重新启动后, SyGate 软件将自动运行。

#### 14、备份计算机上 C:\movie 文件夹中的内容, 备份类型为: 正常备份, 备份文件存储在:

C:\movie\_bk.bkf。

备份计算机上 C:\movie 文件夹中的内容, 备份类型为: 正常备份, 备份文件存储在:

C:\movie\_bk.bkf。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的步骤中, 从而把步骤补充完整。

##### 【操作步骤】:

步骤 1: 单击“开始”→“程序”→“附件”→“系统工具”→“备份”。

步骤 2: 在图中, 清除“总是以向导模式启动”复选框, 然后单击“高级模式”。步骤 3: 在弹出的对话框中, 单击【备份向导 (高级)】按钮, 然后在弹出的“欢迎使用备份向导”窗口中单击【下一步】。

步骤 4: \_\_\_\_\_ ① \_\_\_\_\_

步骤 5: \_\_\_\_\_ ② \_\_\_\_\_

步骤 6: 在弹出的窗口中, 单击【浏览】按钮, 设置备份文件的名称和存储地点。

步骤 7: \_\_\_\_\_ ③ \_\_\_\_\_

步骤 8: 在弹出的窗口中, 可以看到备份文件的名称和存储地点。如果没有问题, 单击【下一步】。

步骤 9: 在弹出的窗口, 单击【高级】按钮。

步骤 10: \_\_\_\_\_ ④ \_\_\_\_\_

步骤 11: 为了保证备份数据的可靠性, 可以选中“备份后验证数据”。然后, 单击【下一步】。

步骤 12: 在这里, 选择“替换现有备份”。然后, 单击【下一步】。

步骤 13: 在这里, 选择“现在”。然后, 单击【下一步】。

步骤 14: 在“完成向导”画面中, 如果确认没有问题, 则单击【完成】按钮。

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: D. 在弹出的对话框中, 选择“备份选定的文件、驱动器或网络数据”, 然后单击【下一步】。②: B. 在弹出的窗口中, 选择要备份的 C:\movie 文件夹, 然后单击【下一步】。③: C. 在弹出的对话框中, 选择存储地点, 然后指定备份文件名。在这里, 把文件备份到 C:\movie\_bk.bkf 文件中。然后, 单击【保存】。④: A. 在“选择要备份的类型”处, 单击下拉式箭头, 选择备份类型。在这里, 选择“正常”备份。然后, 单击【下一步】。

#### 15、调整 IIS 网站的默认文档, 包括优先级调整、添加以及删除。

步骤 1: 在 **IIS 管理器**工具中, 选择 IIS 站点。

步骤 2: 选择进入**默认文档**界面。

步骤 3: 完成添加默认文档操作, 需点击右侧**添加**按钮。

步骤 4: 完成删除默认文档操作, 需选中指定文档, 点击右侧**删除**按钮。

步骤 5: 完成优先级调整操作, 需选中指定文档, 点击右侧**上移**或**下移**按钮。

#### 16、调整网络负载均衡群集中指定节点的优先级操作步骤。

步骤 1: 在**网络负载均衡管理器**工具中, 选择指定节点。

步骤 2: 右键单击节点, 选择**主机属性**命令。

步骤 3: 在节点属性窗口中, 调整**主机参数**选项卡下的**优先级**。

步骤 4: 单击确定按钮完成设置。

#### 17、换位加密能够按照一定的规律重排字母的顺序。例如, 以 LUCKY 作为密钥 (在字母表中的出现顺序为 34125), 对明文 HELLOWORLD 进行加密, 会得到密文 LRLHWEOD, 如下表所示。

	L	U	C	K	Y
密钥					
字母表中的顺序	3	4	1	2	5
明文	H	E	L	L	O
	W	O	R	L	D
密文	LR (C 列) LL (K 列) HW (L 列) EO (U 列) OD (Y 列)				

请参考上述加密方法, 以 TONY 作为密钥, 将明文 HAPPYNEWYEAR 转换为密文:

P \_\_\_\_\_ A \_\_\_\_\_ H \_\_\_\_\_ P \_\_\_\_\_

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

##### 【答案选项】

A. YY。

B. WR。

C. WY。

D. EA。

E. EN。

F. NE。

正确答案: 1、D 2、F 3、A 4、B

#### 18、换位加密能够按照一定的规律重排字母的顺序。例如, 以 LUCKY 作为密钥 (在字母表中的出现顺序为 34125), 对明文 HELLOWORLD 进行加密, 会得到密文 LRLHWEOD, 如下表所示。

1.

	L	U	C	K	Y
密钥					
字母表中的顺序	3	4	1	2	5
明文	H	E	L	L	O
	W	O	R	L	D
密文	LR (C 列) LL (K 列) HW (L 列) EO (U 列) OD (Y 列)				

请参考上述加密方法，以 CAT 作为密钥，将明文 HOWAREYOU 转换为密文：

0    O    A    W    U

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【答案选项】

A.Y.   B.E.   C.C.   D.R.   E.T.   .H.

正确答案： 1、D 2、F 3、A 4、B

19、假设在域 abc.com 中有一个“研发部”OU，在该 OU 中有 5 个用户账户：user1、user2、user3、user4 和 user5。域管理员需要设置一条组策略，使得“研发部”OU 中的所有用户登录到域以后，在自己的“开始”菜单中找不到“运行”命令。

假设在域 abc.com 中有一个“研发部”OU，在该 OU 中有 5 个用户账户：user1、user2、user3、user4 和 user5。域管理员需要设置一条组策略，使得“研发部”OU 中的所有用户登录到域以后，在自己的“开始”菜单中找不到“运行”命令。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

步骤 1：\_\_\_\_\_①\_\_\_\_\_

步骤 2：\_\_\_\_\_②\_\_\_\_\_

步骤 3：\_\_\_\_\_③\_\_\_\_\_ 步骤 4：右击刚刚创建的 GPO，然后在快捷菜单中单击“编辑”。

步骤 5：\_\_\_\_\_④\_\_\_\_\_ 步骤 6：在对话框中，选中“已启用”，然后单击【确定】。

请填写：①：( ) ②：( ) ③：( ) ④：( )

答案：①：D. 单击“开始”→“程序”→“管理工具”→“组策略管理”。②：A. 右击“研发部”OU，然后在快捷菜单中单击“创建并链接 GPO”。③：C. 在“新建 GPO”画面的“名称”处，为该 GPO 命名，例如：“研发部”OU 的 GPO，然后单击【确定】。④：B. 在组策略编辑窗口中，单击“用户配置”→“管理模板”→“任务栏和[开始]菜单”→双击“从[开始]菜单中删除‘运行’菜单”组策略。

20、将计算机上的备份文件 C:\movie\_bk.bkf 还原到本地 C:\123 文件夹中。

将计算机上的备份文件 C:\movie\_bk.bkf 还原到本地 C:\123 文件夹中。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的步骤中，从而把步骤补充完整。

【操作步骤】

步骤 1：在还原向导的对话框中，单击【还原向导（高级）】按钮。

步骤 2：在“欢迎使用还原向导”画面中，单击【下一步】。

步骤 3：\_\_\_\_\_①\_\_\_\_\_

步骤 4：在还原向导的窗口，单击【高级】按钮。

步骤 5：\_\_\_\_\_②\_\_\_\_\_

步骤 6：\_\_\_\_\_③\_\_\_\_\_

步骤 7：在“高级还原选项”对话框中，保留默认项，单击【下一步】。

步骤 8：在“完成向导”画面中，如果确认没有问题，则单击【完成】按钮。

请填写：①：( ) ②：( ) ③：( )

答案：①：B. 在“还原项目”窗口中左窗格的“要还原的项目”处，选中希望还原的备份文件 movie\_bk.bkf，然后单击【下一步】。②：C. 在“还原位置”窗口中，选择将文件还原到“备用位置”，然后在“备用位置”处输入一个还原位置，即：C:\123 文件夹，然后单击【下一步】。③A.

在“如何还原”窗口中，选择“替换现有文件”，即：只要在还原位置处存在其它文件，一律覆盖。然后，单击【下一步】。

21、请对应选择描述正确的一项。

提供 SMTP 服务的计算机。(SMTP 服务器)

在网站上设置的一个默认网页，便于用户访问网站时使用。(网站首页)

可缩写为 w3 或 Web，是目前 Internet 上最为流行、最受欢迎的一种信息浏览服务。(万维网)

用于将远程计算机上的文件下载到自己计算机的磁盘中，也可以将本机上的文件上传到远程计算机上。

(FTP 协议) 利用计算机网络来发送或接收的邮件。(电子邮件)

22、设置访问 FTP 服务器的 IP 地址限制

步骤 1：在 IIS 管理器工具中，选择 FTP 站点。

步骤 2：选择进入 FTPIP 地址和限制界面。

步骤 3：完成添加 IP 地址限制条目操作，需右键选择添加允许条目命令。

步骤 4：完成删除 IP 地址限制条目操作，需右键选择删除允许条目命令。

23、使用 Windows 的 POP3 管理工具把你的计算机配置为电子邮件服务器。

选择验证方法为“本地 Windows 帐户”；建立电子邮件域“abc.com”；建立一个电子邮箱“john@abc.com”，设置密码“123”。

操作步骤：

步骤 1：把 POP3 服务器的验证身份方法设置为 D. 本地 Windows 帐户。

步骤 2：在“POP3 服务”管理工具中，单击【新域】，然后输入域的名称：A. abc.com，单击【确定】按钮。

步骤 3：选择所建立的域：A. abc.com，单击【添加邮箱】，然后，输入邮箱名称：B. john，并且为邮箱设置密码：123，其它使用默认设置。

步骤 4：按【确定】按钮。

24、使用 Winmail 在计算机上创建一个电子邮件域，域名为“efg.com”，采用默认设置。

然后在域创建一个电子邮箱，邮箱名称为 john@efg.com，采用默认设置。

操作步骤：

步骤 1：在 Winmail 管理工具中，单击【域名设置】—【域名管理】—【新增】。

步骤 2：在“域名”的“基本参数”选项卡中的【域名】处输入该域的名称：B. efg.com，其余项目保留默认选项。

步骤 3：单击【确定】按钮。

步骤 4：再单击【用户和组】—【用户管理】，在右侧窗口中的【域名】中选择希望建立邮箱的电子邮件域名：B. efg.com，然后单击【新增】按钮。

步骤 5：在“基本设置”对话框中的【用户名】处输入邮箱的名称：A. john，在【真实姓名】处输入使用者的真实姓名，在【密码】处设定该邮箱的密码，其它项目保留默认选项，然后单击【下一步】按钮。

步骤 6：单击【完成】按钮。

25、台安装了 Windows Server 操作系统的服务器 Server18 上，管理员需要立即备份一次系统状态数据。

在一台安装了 Windows Server 操作系统的服务器 Server18 上，管理员需要立即备份一次系统状态数据。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

步骤 1：登录服务器 Server18，在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”，打开“wbadmin”控制台窗口。

步骤 2：\_\_\_\_\_①\_\_\_\_\_

步骤 3：在“备份选项”对话框中，单击“下一步”。

步骤 4：在“选择备份配置”对话框中，选中“自定义”选项，然后单击“下一步”。

步骤 5：\_\_\_\_\_②\_\_\_\_\_

步骤 6：返回上一级对话框，单击“下一步”。

步骤 7: 在“指定目标类型”对话框中,单击“下一步”。

步骤 9: ③

步骤 10: 在“确认”对话框中,单击“备份”。

步骤 11: ④ 请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: C. 在“wbadmin”控制台窗口左侧导航栏中,右击“本地备份”,并单击“一次性备份...”。②: A. 在“选择要备份的项”对话框中,单击“添加项目”,并勾选“系统状态”选项,然后单击“确定”。③: B. 在“选择备份目标”对话框中,选择备份目标,再单击“下一步”。④: E. 在“备份进度”对话框中,单击“关闭”。

## 26、完成 CA 备份和还原的操作步骤:

步骤 1: 打开证书颁发机构工具。

步骤 2: 右键单击证书颁发机构,依次选择所有任务 1--备份 CA命令,完成备份 CA 操作。

步骤 3: 右键单击证书颁发机构,依次选择所有任务 2--还原 CA命令,完成还原 CA 操作。

## 27、为了允许普通的域用户账户能够在 DC 上登录到域,管理员需要修改“Default Domain Controllers Policy”GPO 中的“允许在本地登录”组策略,以便让“Domain Users”组的所有成员都具有在 DC 上登录到域的权利。

为了允许普通的域用户账户能够在 DC 上登录到域,管理员需要修改“Default Domain Controllers Policy”GPO 中的“允许在本地登录”组策略,以便让“Domain Users”组的所有成员都具有在 DC 上登录到域的权利。

要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。【操作步骤】:步骤 1: ① 步骤 2: 在打开的窗口中,右击“Default Domain Controllers Policy”→在快捷菜单中单击“编辑”,打开“组策略编辑器”。

步骤 3: ② 步骤 4: 单击【添加用户或组】按钮,选择该域的 Domain Users 组,然后单击【确定】。

步骤 5: ③ 请填写: ①: ( ) ②: ( ) ③: ( )

答案: ①: C. 单击“开始”→“程序”→“管理工具”→“组策略管理”。②: A. 单击“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”→双击“允许本地登录”组策略。③: B. 在域控制器上,运行“gpupdate”命令,使这条组策略立即生效。

## 28、向故障转移群集中添加节点的操作步骤:

步骤 1: 登录 Windows Server 2016,打开故障转移群集工具。

步骤 2: 单击右侧添加节点命令。

步骤 3: 在选择服务器界面中,输入服务器名称。

步骤 4: 依次单击下一步,完成操作。

## 29、修改“Default Domain Controllers Policy”GPO 中的组策略,使得 Domain Users 组中的所有成员都具有在域控制器上登录到域的权利。

修改“Default Domain Controllers Policy”GPO 中的组策略,使得 Domain Users 组中的所有成员都具有在域控制器上登录到域的权利。要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤 1: 单击“开始”→“程序”→“管理工具”→“组策略管理”。

步骤 2: ①

步骤 3: ②

步骤 4: ③

步骤 5: 在域控制器上,运行“gpupdate”命令,使这条组策略立即生效。

请填写: ①: ( ) ②: ( ) ③: ( )

答案: ①: B. 在弹出的窗口中,右击“Default Domain Controllers Policy”→在快捷菜单中单击“编辑”,打开“组策略编辑器”。②: C. 在弹出的窗口中,单击“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”→双击“允许本地登录”组策略。③: A. 在弹出的窗口中,单击【添加用户或组】按钮,选择该域的 Domain Users 组,然后单击【确定】。

## 30、在 ISA Server 上,管理员需要创建发布规则,以允许外部用户访问内部的电子邮件服务器,执行收发邮件的工作。其中,内部的邮件服务器安装在计算机 PC1 (IP 地址: 192.168.1.1); ISA Server 连接内部的网卡 IP 地址为: 192.168.1.200,连接外部的网卡 IP 地址为: 131.107.1.200。

在 ISA Server 上,管理员需要创建发布规则,以允许外部用户访问内部的电子邮件服务器,执行收发邮件的工作。其中,内部的邮件服务器安装在计算机 PC1 (IP 地址: 192.168.1.1); ISA Server 连接内部的网卡 IP 地址为: 192.168.1.200,连接外部的网卡 IP 地址为: 131.107.1.200。要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤 1: ①

步骤 2: 在“欢迎使用新建邮件服务器发布规则向导”画面中输入发布规则的名称,例如:发布内部邮件服务器,然后单击【下一步】。

步骤 3: ②

步骤 4: ③

步骤 5: 在弹出的窗口中指定内部邮件服务器的 IP 地址,这里应该输入 PC1 的 IP 地址: 192.168.1.1,然后单击【下一步】。

步骤 6: ④

步骤 7: 出现“正在完成新建邮件服务器发布规则向导”画面时,单击【完成】。

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: D. 在 ISA Server 的管理控制台中,单击左窗格中的“防火墙策略”,然后单击任务窗格的“任务”选项卡,接着单击“发布邮件服务器”。②: C. 由于希望外部的客户端(而非外部的邮件服务器)来访问内部邮件服务器,所以在弹出的窗口中选择“客户端访问: RPC、IMAP、POP3、SMTP”,然后单击【下一步】。③: A. 由于希望外部的客户端通过 SMTP 和 POP3 的标准端口来访问内部邮件服务器,所以在弹出的窗口中选择“POP3 (standard port)”和“SMTP (standard port)”,然后单击【下一步】。④: B. 在弹出的窗口中,选择“外部”网络,然后单击【地址】按钮。然后,在弹出的窗口中选择“在此网络上选择的 IP 地址”,从“可用的 IP 地址”中选择一个 IP 地址(即: 131.107.1.200),然后单击【添加】按钮,将该地址添加到右侧的“选择的 IP 地址”栏中,再按【确定】按钮即可。

## 31、在计算机上利用 IIS 创建一个 Web 网站。

其中,网站名称为“web1”;网站使用的 IP 地址为: 192.168.0.1 端口号为: 9000、没有主机头;使用 D 分区的“resource”文件夹作为该站点的主目录、允许匿名访问并且分配“浏览”的访问权限。

操作步骤:

步骤 1: 在计算机上启动“IIS 管理器”,展开本地计算机,右键单击【网站】,在快捷菜单中单击【新建】C. 网站。

步骤 2: 在出现“欢迎使用网站创建向导”画面时,单击【下一步】按钮。步骤 3: 在“网站描述”对话框中输入: B. web1,然后单击【下一步】按钮。

步骤 4: 在“IP 地址和端口设置”中的【网站 IP 地址】处输入: E. 192.168.0.1,在【网站 TCP 端口(默认值: 80)】

处输入: A. 9000,然后单击【下一步】按钮。

步骤 5: 在“网站主目录”对话框中输入: F. D:\resource,选中【允许匿名访问网站】复选框,然后单击【下一步】按钮。

步骤 6: 在“网站访问权限”对话框中,除了保留默认的权限外,还需要选择 D. 浏览 权限,然后单击【下一步】按钮。

步骤 7: 在出现“已成功完成网站创建向导”画面时,单击【完成】按钮。

## 32、在计算机上使用 Serv-U 创建一个 FTP 站点。

其中,该站点的名称为“ftp.efg.com”,使用的 IP 地址: 192.168.0.100,使用端口号: 10000,该域被存储在【.INI 文件】中。

操作步骤:

步骤 1: 在“Serv-U 管理员”控制台中右键单击【域】,在快捷菜单中选择【新建域】。

步骤 2: 在“添加新建域—第一步”对话框中,选择该域希望使用的 IP 地址: D. 192.168.0.-100,然后单击【下一步】

按钮。

步骤 3: 在“添加新建域—第二步”对话框中,为该域指定一个完全合格域名: C. ftp.efg.cam,

然后单击【下一步】按钮。

步骤4: 在“添加新建域一第三步”对话框中,为该域所对应的站点指定一个端口号: A. 10000, 然后单击

【下一步】按钮。

步骤5: 在“添加新建域一第四步”对话框中,选择存储于 B. INI 文件, 然后单击【下一步】按钮。

33、在计算机上使用 WindowsMediaServices 创建点播发布点。

其中,发布点名称为“video”;在内容类型中选择【目录中的文件】,并且指向“d:\video”文件夹;在内容播放方式中选择【循环播放】;完成向导后不要创建公告文件。

操作步骤:

步骤1: 单击【开始】—【程序】—【管理工具】—\*[WindowsMediaServices], 进入 WindowsMediaServices 管理窗口。

步骤2: 右键单击【发布点】, 然后选择【添加发布点(向导)】。

步骤4: 在“发布点名称”对话框中,为这个发布点设置名称: C. video。然后,单击【下一步】按钮。

步骤5: 在“内容类型”窗口中选择要传输的内容类型,所以选择 A. 目录中的文件复选框。然后,单击【下一步】按钮。

步骤6: 在“发布点类型”对话框中,选择 B. 点播发布点, 然后单击【下一步】按钮。

步骤7: 在“目录位置”文本框中输入: E. d:\video。

步骤8: 在“内容播放”对话框中,设置点播文件目录中的文件的播放方式: D. 循环播放, 然后单击【下一步】按钮。

步骤10: 在“发布点摘要”窗口中,对照显示的摘要内容进行确认。

步骤11: 单击【下一步】按钮,选择不要设置公告内容。然后,单击【完成】按钮。】

34、在一台安装了 Windows Server 操作系统的服务器 Server17 上,管理员需要创建一个备份计划: 每天 23 点备份一次服务器上的所有数据(包括应用程序和系统状态)。

在一台安装了 Windows Server 操作系统的服务器 Server17 上,管理员需要创建一个备份计划: 每天 23 点备份一次服务器上的所有数据(包括应用程序和系统状态)。

要求: 从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤1: 登录服务器 Server17, 在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”, 打开“wbadmin”控制台窗口。

步骤2: ①

步骤3: 在“开始”对话框中,单击“下一步”。

步骤4: 在“选择备份配置”对话框中,选中“整个服务器”选项,然后单击“下一步”。

步骤5: ②

步骤6: 在“指定目标类型”对话框中,单击“下一步”。

步骤7: ③

步骤8: 在弹出的对话框中,勾选可用的联机磁盘,然后单击“确定”。返回上一级对话框,勾选添加的磁盘,再单击“下一步”。

步骤9: ④ 步骤10: 在“确认”对话框中,单击“完成”。

步骤11: ⑤

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( ) ⑤: ( )

答案: ①: C. 在“wbadmin”控制台窗口左侧导航栏中,右击“本地备份”,并单击“备份计划...”。②: A. 在“指定备份时间”对话框中,选中“每日一次”,并设置“选择时间”为 23:00,然后单击“下一步”。③: B. 在“选择目标磁盘”对话框中,单击“显示所有可用磁盘”。④: E. 弹出警告对话框,单击“是”。⑤: D. 在“摘要”对话框中,单击“关闭”。

35、在一台安装了 Windows Server 操作系统的服务器 Server19 上,管理员需要创建一个备份计划: 每天 22 点备份一次服务器的本地磁盘 C: 上的数据。

在一台安装了 Windows Server 操作系统的服务器 Server19 上,管理员需要创建一个备份计划: 每天 22 点备份一次服务器的本地磁盘 C: 上的数据。

要求: 从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤1: 登录服务器 Server19, 在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”, 打开“wbadmin”控制台窗口。

步骤2: ①

步骤3: 在“开始”对话框中,单击“下一步”。

步骤4: 在“选择备份配置”对话框中,选中“自定义”选项,然后单击“下一步”。

步骤5: ② 步骤6: 在“指定备份时间”对话框中,选中“每日一次”,并设置“选择时间”为 22:00, 然后单击“下一步”。

步骤7: 在“指定目标类型”对话框中,单击“下一步”。

步骤8: ③

步骤9: 在弹出的对话框中,勾选可用的联机磁盘,然后单击“确定”。返回上一级对话框,勾选添加的磁盘,再单击“下一步”。

步骤10: 步骤11: 在“确认”对话框中,单击“完成”。

步骤12: ④

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: C. 在“wbadmin”控制台窗口左侧导航栏中,右击“本地备份”,并单击“备份计划...”。②: F. 在“选择要备份的项”对话框中,单击“添加项目”,然后勾选“本地磁盘(C:)”选项,并单击“确定”,返回上一级对话框,单击“下一步”。③: B. 在“选择目标磁盘”对话框中,单击“显示所有可用磁盘”。④: D. 在“摘要”对话框中,单击“关闭”。

36、在一台安装了 Windows Server 操作系统的服务器 Server20 上,管理员需要立即备份一次系统状态数据到远程共享文件夹\\w2016\bak。

在一台安装了 Windows Server 操作系统的服务器 Server20 上,管理员需要立即备份一次系统状态数据到远程共享文件夹\\w2016\bak。

要求: 从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤1: 登录服务器 Server20, 在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”, 打开“wbadmin”控制台窗口。

步骤2: ①

步骤3: 在“备份选项”对话框中,单击“下一步”。

步骤4: 在“选择备份配置”对话框中,选中“自定义”选项,然后单击“下一步”。

步骤5: ②

步骤6: 返回上一级对话框,单击“下一步”。

步骤7: ③

步骤8: 在“指定远程文件夹”对话框中,“位置”下方的文本框中输入“\\w2016\bak”, 再单击“下一步”。步骤9: 在“确认”对话框中,单击“备份”。

步骤10: ④ 请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: C. 在“wbadmin”控制台窗口左侧导航栏中,右击“本地备份”,并单击“一次性备份...”。②: A. 在“选择要备份的项”对话框中,单击“添加项目”,并勾选“系统状态”选项,然后单击“确定”。③: B. 在“指定目标类型”对话框中,选择“远程共享文件夹”选项,然后单击“下一步”。④: E. 在“备份进度”对话框中,单击“关闭”。

37、在一台安装了 Windows Server 操作系统的服务器 Server17 上,管理员需要创建一个备份计划: 每天 23 点备份一次服务器上的所有数据(包括应用程序和系统状态)。

要求: 从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤1: 登录服务器 Server17, 在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”, 打开“wbadmin”控制台窗口。

步骤2: ( )

- 步骤 3: 在“开始”对话框中,单击“下一步”。
- 步骤 4: 在“选择备份配置”对话框中,选中“整个服务器”选项,然后单击“下一步”。
- 步骤 5: ( )
- 步骤 6: 在“指定目标类型”对话框中,单击“下一步”。
- 步骤 7: ( )
- 步骤 8: 在弹出的对话框中,勾选可用的联机磁盘,然后单击“确定”。返回上一级对话框,勾选添加的磁盘,再单击“下一步”。
- 步骤 9: ( )
- 步骤 10: 在“确认”对话框中,单击“完成”。
- 步骤 11: ( )

**【答案选项】**

- A. 在“指定备份时间”对话框中,选中“每日一次”,并设置“选择时间”为 23:00,然后单击“下一步”。
- B. 在“选择目标磁盘”对话框中,单击“显示所有可用磁盘”。
- C. 在“wbadmin”控制台窗口左侧导航栏中,右击“本地备份”,并单击“备份计划...”。
- D. 在“摘要”对话框中,单击“关闭”。
- E. 弹出警告对话框,单击“是”。
- F. 在“指定备份时间”对话框中,选中“每日多次”,然后单击“下一步”。

正确答案: 1、C 2、A 3、B 4、E 5、D

**38、在一台安装了 WindowsServer 操作系统的服务器 Server18 上,管理员需要立即备份一次系统状态数据。**

要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

**【操作步骤】:**

- 步骤 1: 登录服务器 Server18,在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”,打开“wbadmin”控制台窗口。
- 步骤 2: ( )
- 步骤 3: 在“备份选项”对话框中,单击“下一步”。
- 步骤 4: 在“选择备份配置”对话框中,选中“自定义”选项,然后单击“下一步”。
- 步骤 5: ( )
- 步骤 6: 返回上一级对话框,单击“下一步”。
- 步骤 7: 在“指定目标类型”对话框中,单击“下一步”。
- 步骤 9: ( )
- 步骤 10: 在“确认”对话框中,单击“备份”。
- 步骤 11: ( )

**【答案选项】**

- A. 在“选择要备份的项”对话框中,单击“添加项目”,并勾选“系统状态”选项,然后单击“确定”。
- B. 在“选择备份目标”对话框中,选择备份目标,再单击“下一步”。
- C. 在“wbadmin”控制台窗口左侧导航栏中,右击“本地备份”,并单击“一次性备份...”。
- D. 在“摘要”对话框中,单击“关闭”。
- E. 在“备份进度”对话框中,单击“关闭”。
- F. 在“指定备份时间”对话框中,选中“每日多次”,然后单击“下一步”。

正确答案: 1、C 2、A 3、B 4、E

**39、在一台安装了 WindowsServer 操作系统的服务器 Server19 上,管理员需要创建一个备份计划:每天 22 点备份一次服务器的本地磁盘 C: 上的数据。**

要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

**【操作步骤】:**

- 步骤 1: 登录服务器 Server19,在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”,打开“wbadmin”控制台窗口。
- 步骤 2: ( )

- 步骤 3: 在“开始”对话框中,单击“下一步”。
- 步骤 4: 在“选择备份配置”对话框中,选中“自定义”选项,然后单击“下一步”。
- 步骤 5: ( )
- 步骤 6: 在“指定备份时间”对话框中,选中“每日一次”,并设置“选择时间”为 22:00,然后单击“下一步”。
- 步骤 7: 在“指定目标类型”对话框中,单击“下一步”。
- 步骤 8: ( )
- 步骤 9: 在弹出的对话框中,勾选可用的联机磁盘,然后单击“确定”。返回上一级对话框,勾选添加的磁盘,再单击“下一步”。
- 步骤 10: ( )
- 步骤 11: 在“确认”对话框中,单击“完成”。
- 步骤 12: ( )

**【答案选项】**

- A. 在“指定备份时间”对话框中,选中“每日一次”,并设置“选择时间”为 24:00,然后单击“下一步”。
- B. 在“选择目标磁盘”对话框中,单击“显示所有可用磁盘”。
- C. 在“wbadmin”控制台窗口左侧导航栏中,右击“本地备份”,并单击“备份计划...”。
- D. 在“摘要”对话框中,单击“关闭”。
- E. 弹出警告对话框,单击“是”。
- F. 在“选择要备份的项”对话框中,单击“添加项目”,然后勾选“本地磁盘 (C:)”选项,并单击“确定”,返回上一级对话框,单击“下一步”。

正确答案: 1、C 2、F 3、B 4、E 5、D

**40、在一台安装了 WindowsServer 操作系统的服务器 Server20 上,管理员需要立即备份一次系统状态数据到远程共享文件夹\\w2016\bak。**

要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

**【操作步骤】:**

- 步骤 1: 登录服务器 Server20,在“服务器管理器”窗口右上角单击“工具”→“Windows Server Backup”,打开“wbadmin”控制台窗口。
- 步骤 2: ( )
- 步骤 3: 在“备份选项”对话框中,单击“下一步”。
- 步骤 4: 在“选择备份配置”对话框中,选中“自定义”选项,然后单击“下一步”。
- 步骤 5: ( )
- 步骤 6: 返回上一级对话框,单击“下一步”。
- 步骤 7: ( )
- 步骤 8: 在“指定远程文件夹”对话框中,“位置”下方的文本框中输入“\\w2016\bak”,再单击“下一步”。
- 步骤 9: 在“确认”对话框中,单击“备份”。
- 步骤 10: ( )

**【答案选项】**

- A. 在“选择要备份的项”对话框中,单击“添加项目”,并勾选“系统状态”选项,然后单击“确定”。
- B. 在“指定目标类型”对话框中,选择“远程共享文件夹”选项,然后单击“下一步”。
- C. 在“wbadmin”控制台窗口左侧导航栏中,右击“本地备份”,并单击“一次性备份...”。
- D. 在“摘要”对话框中,单击“关闭”。
- E. 在“备份进度”对话框中,单击“关闭”。
- F. 在“指定备份时间”对话框中,选中“每日多次”,然后单击“下一步”。

正确答案: 1、C 2、A 3、B 4、E

**41、在一台安装了 Windows 操作系统的服务器 Server12 上,管理员需要创建一个防火墙规则:拒绝任何远程计算机访问此服务器 (Server12) 上的 iSCSI 服务。**

在一台安装了 Windows 操作系统的服务器 Server12 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server12）上的 iSCSI 服务。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

- 步骤 1: \_\_\_\_\_ ① \_\_\_\_\_  
步骤 2: 在左侧导航栏中，右击“入站规则”并单击“新建规则”。  
步骤 3: 在“规则类型”对话框中，选择\_\_\_\_\_ ② \_\_\_\_\_选项，并在列表框中选择“iSCSI 服务”，单击“下一步”。  
步骤 4: 在“规则”对话框中，勾选\_\_\_\_\_ ③ \_\_\_\_\_选项，然后单击“下一步”。 步骤 5:

\_\_\_\_\_ ④ \_\_\_\_\_  
请填写：①：（） ②：（） ③：（） ④：（）

答案：①：E. 登录服务器 Server12，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。②：C. 预定义 ③：F. iSCSI 服务 ④：A. 在“操作”对话框中，选中“阻止连接”选项，单击“完成”。

42、在一台安装了 Windows 操作系统的服务器 Server12 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server12）上的 iSCSI 服务。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

- 步骤 1: （）  
步骤 2: 在左侧导航栏中，右击“入站规则”并单击“新建规则”。  
步骤 3: 在“规则类型”对话框中，选择（）选项，并在列表框中选择“iSCSI 服务”，单击“下一步”。  
步骤 4: 在“规则”对话框中，勾选（）选项，然后单击“下一步”。  
步骤 5: （）

【答案选项】

- A. 在“操作”对话框中，选中“阻止连接”选项，单击“完成”。  
B. 在“名称”对话框中，输入规则名称后，单击“完成”。  
C. 预定义。  
D. 登录服务器 Server12，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。  
E. 登录服务器 Server12，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。  
F. iSCSI 服务。

正确答案： 1、E 2、C 3、F 4、A

43、在一台安装了 Windows 操作系统的服务器 Server13 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server13）上的所有程序。

在一台安装了 Windows 操作系统的服务器 Server13 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server13）上的所有程序。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

- 步骤 1: \_\_\_\_\_ ① \_\_\_\_\_  
步骤 2: 在左侧导航栏中，右击“入站规则”并单击“新建规则”。  
步骤 3: 在“规则类型”对话框中，选择\_\_\_\_\_ ② \_\_\_\_\_选项，然后单击“下一步”。  
步骤 4: 在“程序”对话框中，选择\_\_\_\_\_ ③ \_\_\_\_\_选项，然后单击“下一步”。  
步骤 5: \_\_\_\_\_ ④ \_\_\_\_\_  
步骤 6: 在“配置文件”对话框中，单击“下一步”。  
步骤 8: 在“名称”对话框中，输入规则名称后，单击“完成”。

请填写：①：（） ②：（） ③：（） ④：（）

答案： ①：E. 登录服务器 Server13，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。②：C. 程序 ③：F. 所有程序④：A. 在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。

44、在一台安装了 Windows 操作系统的服务器 Server13 上，管理员需要创建一个防火墙规则：拒绝任何远程计算机访问此服务器（Server13）上的所有程序。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

- 步骤 1: （）  
步骤 2: 在左侧导航栏中，右击“入站规则”并单击“新建规则”。  
步骤 3: 在“规则类型”对话框中，选择（）选项，然后单击“下一步”。  
步骤 4: 在“程序”对话框中，选择（）选项，然后单击“下一步”。  
步骤 5: （）  
步骤 6: 在“配置文件”对话框中，单击“下一步”。  
步骤 8: 在“名称”对话框中，输入规则名称后，单击“完成”。

【答案选项】

- A. 在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。  
B. 在“名称”对话框中，输入规则名称后，单击“完成”。  
C. 程序。  
D. 登录服务器 Server13，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。  
E. 登录服务器 Server13，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。  
F. 所有程序。

正确答案： 1、E 2、C 3、F 4、A

45、在一台安装了 Windows 操作系统的服务器 Server14 上，管理员需要创建一个防火墙规则：仅拒绝此服务器（Server14）访问任何远程计算机的 TCP53 端口。

在一台安装了 Windows 操作系统的服务器 Server14 上，管理员需要创建一个防火墙规则：仅拒绝此服务器（Server14）访问任何远程计算机的 TCP53 端口。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

- 步骤 1: \_\_\_\_\_ ① \_\_\_\_\_  
步骤 2: 在左侧导航栏中，右击“出站规则”并单击“新建规则”。  
步骤 3: 在“规则类型”对话框中，选择\_\_\_\_\_ ② \_\_\_\_\_选项，单击“下一步”。  
步骤 3: 在“协议和端口”对话框中，选择“TCP”，在\_\_\_\_\_ ③ \_\_\_\_\_右侧的文本框中输入 53，然后单击“下一步”。 步骤 4: 在“操作”对话框中，选中“阻止连接”选项，单击“下一步”。 步骤 5: 在“配置文件”对话框中，单击“下一步”。  
步骤 6: \_\_\_\_\_ ④ \_\_\_\_\_

请填写：①：（） ②：（） ③：（） ④：（）

答案：①：D. 登录服务器 Server14，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。②：F. 端口 ③：A. 特定远程端口 ④：B. 在“名称”对话框中，输入规则名称后，单击“下一步”。

46、在一台安装了 Windows 操作系统的服务器 Server14 上，管理员需要创建一个防火墙规则：仅拒绝此服务器（Server14）访问任何远程计算机的 TCP53 端口。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

- 步骤 1: （）  
步骤 2: 在左侧导航栏中，右击“出站规则”并单击“新建规则”。  
步骤 3: 在“规则类型”对话框中，选择（）选项，单击“下一步”。  
步骤 3: 在“协议和端口”对话框中，选择“TCP”，在（）右侧的文本框中输入 53，然后单击“下

一步”。

步骤4: 在“操作”对话框中,选中“阻止连接”选项,单击“下一步”。

步骤5: 在“配置文件”对话框中,单击“下一步”。

步骤6: ( )

【答案选项】

A. 特定远程端口。

B. 在“名称”对话框中,输入规则名称后,单击“下一步”。

C. 所有远程端口。

D. 登录服务器 Server14,在桌面左下角右击“Win 图标”→“运行”,在弹出的“运行”对话框中输入 wf.msc,单击“确定”。

E. 登录服务器 Server14,在桌面左下角右击“Win 图标”→“运行”,在弹出的“运行”对话框中输入 firewall.cpl,单击“确定”。

F. 端口。

正确答案: 1、D 2、F 3、A 4、B

47、在一台安装了 Windows 操作系统的服务器 Server1 上,管理员需要创建一个帐户策略,以确保用户必须使用复杂的密码。

要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤1: ( )

步骤2: 在左侧导航栏中,展开“帐户密码”->( )

步骤3: 在右侧窗格中,右击( ),并单击“属性”

步骤4: 在弹出的对话框中,选中( )选项,然后单击“确定”。

步骤5: 关闭“本地安全策略”窗口。

【答案选项】

A. 密码必须符合复杂性要求。

B. 登录服务器 Server1,在桌面左下角右击“Win 图标”→“运行”,在弹出的“运行”对话框中输入 secpol.msc,单击“确定”。

C. 密码策略。

D. 已禁用。

E. 密码长度最小值。

F. 已启用。

正确答案: 1、B 2、C 3、A 4、F

48、在一台安装了 Windows 操作系统的服务器 Server1 上,管理员需要创建一个帐户策略,以确保用户必须使用复杂的密码。要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

在一台安装了 Windows 操作系统的服务器 Server1 上,管理员需要创建一个帐户策略,以确保用户必须使用复杂的密码。

要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤1: \_\_\_\_\_①\_\_\_\_\_

步骤2: 在左侧导航栏中,展开“帐户密码”->\_\_\_\_\_②\_\_\_\_\_

步骤3: 在右侧窗格中,右击\_\_\_\_\_③\_\_\_\_\_,并单击“属性” 步骤4: 在弹出的对话框中,选中\_\_\_\_\_④\_\_\_\_\_选项,然后单击“确定”。 步骤5: 关闭“本地安全策略”窗口。

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: B. 登录服务器 Server1,在桌面左下角右击“Win 图标”→“运行”,在弹出的“运行”对话框中输入 secpol.msc,单击“确定”。 ②: C. 密码策略 ③: A. 密码必须符合复杂性要求。 ④: F. 已启用

49、在一台安装了 Windows 操作系统的服务器 Server2 上,管理员需要创建一个帐户策略,以确保用户密码长度最小值为 8 字符。

要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤1: ( )

步骤2: 在左侧导航栏中,展开“帐户密码”->( )

步骤3: 在右侧窗格中,右击( ),并单击“属性”

步骤4: 在弹出的对话框中,在文本框中输入( ),然后单击“确定”。

步骤5: 关闭“本地安全策略”窗口。

【答案选项】

A. 密码长度最小值。

B. 登录服务器 Server2,在桌面左下角右击“Win 图标”→“运行”,在弹出的“运行”对话框中输入 secpol.msc,单击“确定”。

C. 密码策略。

D. 已启用。

E. 密码必须符合复杂性要求。

F. 8。

正确答案: 1、B 2、C 3、A 4、F

50、在一台安装了 Windows 操作系统的服务器 Server2 上,管理员需要创建一个帐户策略,以确保用户密码长度最小值为 8 字符。要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

在一台安装了 Windows 操作系统的服务器 Server2 上,管理员需要创建一个帐户策略,以确保用户密码长度最小值为 8 字符。要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤1: \_\_\_\_\_①\_\_\_\_\_

步骤2: 在左侧导航栏中,展开“帐户密码”->\_\_\_\_\_②\_\_\_\_\_

步骤3: 在右侧窗格中,右击\_\_\_\_\_③\_\_\_\_\_,并单击“属性”

步骤4: 在弹出的对话框中,在文本框中输入\_\_\_\_\_④\_\_\_\_\_,然后单击“确定”。

步骤5: 关闭“本地安全策略”窗口。

【答案选项】 A. 密码长度最小值 B. 登录服务器 Server2,在桌面左下角右击“Win 图标”→“运行”,在弹出的“运行”对话框中输入 secpol.msc,单击“确定”。 C. 密码策略 D. 已启用 E. 密码必须符合复杂性要求 F. 8

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案:

①: B. 登录服务器 Server2,在桌面左下角右击“Win 图标”→“运行”,在弹出的“运行”对话框中输入 secpol.msc,单击“确定”。

②: C. 密码策略

③: A. 密码长度最小值

④: F. 8

51、在一台安装了 Windows 操作系统的服务器 Server3 上,管理员需要创建一个帐户策略,以确保用户密码最长使用期限为 30 天。

在一台安装了 Windows 操作系统的服务器 Server3 上,管理员需要创建一个帐户策略,以确保用户密码最长使用期限为 30 天。

要求:从答案选项中选择正确的选项,将其对应的字母填写在空白的操作步骤中,从而把步骤补充完整。

【操作步骤】:

步骤1: \_\_\_\_\_①\_\_\_\_\_

步骤2: 在左侧导航栏中,展开“帐户密码”,然后单击\_\_\_\_\_②\_\_\_\_\_

步骤3: 在右侧窗格中,右击\_\_\_\_\_③\_\_\_\_\_,并单击“属性”

步骤4: 在弹出的对话框中,在文本框中输入\_\_\_\_\_④\_\_\_\_\_,然后单击“确定”。

步骤5: 关闭“本地安全策略”窗口。请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: B. 登录服务器 Server3, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 secpol.msc, 单击“确定”。 ②: C. 密码策略 ③: A. 密码最长使用期限④: F. 30  
52、在一台安装了 Windows 操作系统的服务器 Server3 上, 管理员需要创建一个帐户策略, 以确保用户密码最长使用期限为 30 天。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

- 步骤 1: ()  
步骤 2: 在左侧导航栏中, 展开“帐户密码”, 然后单击 ()  
步骤 3: 在右侧窗格中, 右击 (), 并单击“属性”  
步骤 4: 在弹出的对话框中, 在文本框中输入 (), 然后单击“确定”。  
步骤 5: 关闭“本地安全策略”窗口。

【答案选项】:

- A. 密码最长使用期限。  
B. 登录服务器 Server3, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 secpol.msc, 单击“确定”。  
C. 密码策略。  
D. 已启用。  
E. 密码长度最小值。  
F. 30。

正确答案: 1、B 2、C 3、A 4、F

53、在一台安装了 Windows 操作系统的服务器 Server4 上, 管理员需要创建一个帐户策略, 以确保用户密码最短使用期限为 1 天。

在一台安装了 Windows 操作系统的服务器 Server4 上, 管理员需要创建一个帐户策略, 以确保用户密码最短使用期限为 1 天。要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

- 步骤 1: ①  
步骤 2: 在左侧导航栏中, 展开“帐户密码”, 然后单击 ②  
步骤 3: 在右侧窗格中, 右击 ③, 并单击“属性”  
步骤 4: 在弹出的对话框中, 在文本框中输入 ④, 然后单击“确定”。  
步骤 5: 关闭“本地安全策略”窗口。

请填写: ①: () ②: () ③: () ④: ()

答案: ①: B. 登录服务器 Server4, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 secpol.msc, 单击“确定” ②: C. 密码策略 ③: A. 密码最短使用期限 ④: F. 1

54、在一台安装了 Windows 操作系统的服务器 Server4 上, 管理员需要创建一个帐户策略, 以确保用户密码最短使用期限为 1 天。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

- 步骤 1: ()  
步骤 2: 在左侧导航栏中, 展开“帐户密码”, 然后单击 ()  
步骤 3: 在右侧窗格中, 右击 (), 并单击“属性”  
步骤 4: 在弹出的对话框中, 在文本框中输入 (), 然后单击“确定”。  
步骤 5: 关闭“本地安全策略”窗口。

【答案选项】:

- A. 密码最短使用期限。  
B. 登录服务器 Server4, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 secpol.msc, 单击“确定”。  
C. 密码策略。  
D. 已启用。

E. 密码长度最小值。

F. 1。

正确答案: 1、B 2、C 3、A 4、F

55、在一台安装了 Windows 操作系统的服务器 Server5 上, 管理员需要创建一个帐户策略, 以实现用户在 30 分钟内输错 5 次密码后, 其帐户被自动锁定 30 分钟。

在一台安装了 Windows 操作系统的服务器 Server5 上, 管理员需要创建一个帐户策略, 以实现用户在 30 分钟内输错 5 次密码后, 其帐户被自动锁定 30 分钟。要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

- 步骤 1: ①  
步骤 2: 在左侧导航栏中, 展开“帐户密码”, 然后单击 ②  
步骤 3: 在右侧窗格中, 右击 ③, 并单击“属性”  
步骤 4: 在弹出的对话框中, 在文本框中输入 ④, 然后单击“确定”。在“建议的数值改动”对话框中, 单击“确定”。  
步骤 5: 关闭“本地安全策略”窗口。

请填写: ①: () ②: () ③: () ④: ()

答案: ①: D. 登录服务器 Server5, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 secpol.msc, 单击“确定”。 ②: C. 帐户锁定策略 ③: A. 帐户锁定阈值④: E. 5

56、在一台安装了 Windows 操作系统的服务器 Server5 上, 管理员需要创建一个帐户策略, 以实现用户在 30 分钟内输错 5 次密码后, 其帐户被自动锁定 30 分钟。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

- 步骤 1: ()  
步骤 2: 在左侧导航栏中, 展开“帐户密码”, 然后单击 ()  
步骤 3: 在右侧窗格中, 右击 (), 并单击“属性”  
步骤 4: 在弹出的对话框中, 在文本框中输入 (), 然后单击“确定”。在“建议的数值改动”对话框中, 单击“确定”。  
步骤 5: 关闭“本地安全策略”窗口。

【答案选项】:

- A. 帐户锁定阈值。  
B. 30。  
C. 帐户锁定策略。  
D. 登录服务器 Server5, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 secpol.msc, 单击“确定”。  
E. 5。  
F. 帐户锁定时间。

正确答案: 1、D 2、C 3、A 4、E

57、在一台安装了 Windows 操作系统的服务器 Server6 上, 管理员需要创建一个帐户策略, 以实现用户在 20 分钟内输错 7 次密码后, 其帐户被自动锁定 20 分钟。

在一台安装了 Windows 操作系统的服务器 Server6 上, 管理员需要创建一个帐户策略, 以实现用户在 20 分钟内输错 7 次密码后, 其帐户被自动锁定 20 分钟。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

- 步骤 1: 登录服务器 Server6, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 secpol.msc, 单击“确定”。  
步骤 2: 在左侧导航栏中, 展开“帐户密码”, 然后单击“帐户锁定阈值”。  
步骤 3: 在右侧窗格中, 右击 ①, 并单击“属性”  
步骤 4: 在弹出的对话框中, 在文本框中输入 ②, 然后单击“确定”。在“建议的数值改动”对话框中, 单击“确定”。

步骤 5: 在右侧窗格中, 右击 ③, 并单击“属性”。步骤 6: 在弹出的对话框中, 在文本框中输入 ④, 然后单击“确定”。在“建议的数值改动”对话框中, 单击“确定”。

步骤 7: 关闭“本地安全策略”窗口。请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: A. 帐户锁定阈值 ②: E. 7 ③: F. 帐户锁定时间 ④: B. 20

58、在一台安装了 Windows 操作系统的服务器 Server6 上, 管理员需要创建一个帐户策略, 以实现用户在 20 分钟内输错 7 次密码后, 其帐户被自动锁定 20 分钟。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

步骤 1: 登录服务器 Server6, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 secpol.msc, 单击“确定”。

步骤 2: 在左侧导航栏中, 展开“帐户密码”, 然后单击“帐户锁定阈值”。

步骤 3: 在右侧窗格中, 右击 ( ), 并单击“属性”。

步骤 4: 在弹出的对话框中, 在文本框中输入 ( ), 然后单击“确定”。在“建议的数值改动”对话框中, 单击“确定”。

步骤 5: 在右侧窗格中, 右击 ( ), 并单击“属性”。

步骤 6: 在弹出的对话框中, 在文本框中输入 ( ), 然后单击“确定”。在“建议的数值改动”对话框中, 单击“确定”。

步骤 7: 关闭“本地安全策略”窗口。

【答案选项】:

A. 帐户锁定阈值。

B. 20。

C. 帐户锁定策略。

D. 登录服务器 Server6, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 secpol.msc, 单击“确定”。

E. 7。

F. 帐户锁定时间。

正确答案: 1、A 2、E 3、F 4、B

59、在一台安装了 Windows 操作系统的服务器 Server7 上, 管理员需要创建一个防火墙规则: 拒绝任何远程计算机访问此服务器 (Server7) 的 80 端口。

在一台安装了 Windows 操作系统的服务器 Server7 上, 管理员需要创建一个防火墙规则: 拒绝任何远程计算机访问此服务器 (Server7) 的 80 端口。要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

步骤 1: ①

步骤 2: 在左侧导航栏中, 右击“入站规则”并单击“新建规则”。在“规则类型”对话框中, 选择“自定义”选项, 单击“下一步”。

步骤 3: 在“程序”对话框中, 单击“下一步”。步骤 4: ②

步骤 5: 在“作用域”对话框中, 在“此规则应用于哪些本地 IP 地址”选项下方, 选中“下列 IP 地址”选项, 在下方文本框中输入服务器 Server7 的 IP 地址, 然后单击“添加”; 在“此规则应用于哪些远程 IP 地址”选项下方, 选中“任何 IP 地址”选项, 然后单击“下一步”。

步骤 6: ③

步骤 7: 在“配置文件”对话框中, 单击“下一步”。

步骤 8: ④

请填写: ①: ( ) ②: ( ) ③: ( ) ④: ( )

答案: ①: E. 登录服务器 Server7, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 wf.msc, 单击“确定”。②: C. 在“协议和端口”对话框中, 选择“协议类型: TCP”、“本地端口: 特定端口、80”, 单击“下一步”。③: A. 在“操作”对话框中, 选中“阻止连接”选项, 单击“下一步”。④: B. 在“名称”对话框中, 输入规则名称后, 单击“下一步”。

60、在一台安装了 Windows 操作系统的服务器 Server7 上, 管理员需要创建一个防火墙规则: 拒绝任何远程计算机访问此服务器 (Server7) 的 80 端口。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

步骤 1: ( )

步骤 2: 在左侧导航栏中, 右击“入站规则”并单击“新建规则”。在“规则类型”对话框中, 选择“自定义”选项, 单击“下一步”。

步骤 3: 在“程序”对话框中, 单击“下一步”。

步骤 4: ( )

步骤 5: 在“作用域”对话框中, 在“此规则应用于哪些本地 IP 地址”选项下方, 选中“下列 IP 地址”选项, 在下方文本框中输入服务器 Server7 的 IP 地址, 然后单击“添加”; 在“此规则应用于哪些远程 IP 地址”选项下方, 选中“任何 IP 地址”选项, 然后单击“下一步”。

步骤 6: ( )

步骤 7: 在“配置文件”对话框中, 单击“下一步”。

步骤 8: ( )

【答案选项】:

A. 在“操作”对话框中, 选中“阻止连接”选项, 单击“下一步”。

B. 在“名称”对话框中, 输入规则名称后, 单击“下一步”。

C. 在“协议和端口”对话框中, 选择“协议类型: TCP”、“本地端口: 特定端口、80”, 单击“下一步”。

D. 登录服务器 Server7, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 firewall.cpl, 单击“确定”。

E. 登录服务器 Server7, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 wf.msc, 单击“确定”。

F. 在“协议和端口”对话框中, 选择“协议类型: TCP”、“远程端口: 特定端口、80”, 单击“下一步”。

正确答案: 1、E 2、C 3、A 4、B

61、在一台安装了 Windows 操作系统的服务器 Server8 上, 管理员需要创建一个防火墙规则: 拒绝此服务器 (Server8) 访问任何远程计算机的 443 端口的访问。

要求: 从答案选项中选择正确的选项, 将其对应的字母填写在空白的操作步骤中, 从而把步骤补充完整。

【操作步骤】:

步骤 1: ( )

步骤 2: 在左侧导航栏中, 右击“出站规则”并单击“新建规则”。在“规则类型”对话框中, 选择“自定义”选项, 单击“下一步”。

步骤 3: 在“程序”对话框中, 单击“下一步”。

步骤 4: ( )

步骤 5: 在“作用域”对话框中, 单击“下一步”。

步骤 6: ( )

步骤 7: 在“配置文件”对话框中, 单击“下一步”。

步骤 8: ( )

【答案选项】:

A. 在“操作”对话框中, 选中“阻止连接”选项, 单击“下一步”。

B. 在“名称”对话框中, 输入规则名称后, 单击“下一步”。

C. 在“协议和端口”对话框中, 选择“协议类型: TCP”、“本地端口: 特定端口、443”, 单击“下一步”。

D. 登录服务器 Server8, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 wf.msc, 单击“确定”。

E. 登录服务器 Server8, 在桌面左下角右击“Win 图标”→“运行”, 在弹出的“运行”对话框中输入 firewall.cpl, 单击“确定”。

F. 在“协议和端口”对话框中, 选择“协议类型: TCP”、“远程端口: 特定端口、443”, 单击“下一步”。

正确答案： 1、D 2、F 3、A 4、B

62、在一台安装了 Windows 操作系统的域控制器服务器 Server10 上，管理员需要设置 Windows 防火墙属性：将日志文件的保存路径设置为 D:\fw\fw.log。

在一台安装了 Windows 操作系统的域控制器服务器 Server10 上，管理员需要设置 Windows 防火墙属性：将日志文件的保存路径设置为 D:\fw\fw.log。要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

步骤 1：\_\_\_\_\_①\_\_\_\_\_。  
步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击\_\_\_\_\_②\_\_\_\_\_。  
步骤 3：在弹出的对话框中，单击\_\_\_\_\_③\_\_\_\_\_右侧的“自定义”。  
步骤 4：在弹出的对话框中，在\_\_\_\_\_④\_\_\_\_\_右侧的文本框中输入“D:\fw\fw.log”，然后单击“确定”。

步骤 5：返回上一级对话框，单击“确定”。步骤 6：关闭“高级安全 Windows 防火墙”窗口。

请填写：①：( ) ②：( ) ③：( ) ④：( )

答案：①：D. 登录服务器 Server10，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。②：F. 属性③：A. 日志④：B. 名称

63、在一台安装了 Windows 操作系统的域控制器服务器 Server10 上，管理员需要设置 Windows 防火墙属性：将日志文件的保存路径设置为 D:\fw\fw.log。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

步骤 1：( )  
步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击( )。  
步骤 3：在弹出的对话框中，单击( )右侧的“自定义”。  
步骤 4：在弹出的对话框中，在( )右侧的文本框中输入“D:\fw\fw.log”，然后单击“确定”。  
步骤 5：返回上一级对话框，单击“确定”。  
步骤 6：关闭“高级安全 Windows 防火墙”窗口。

【答案选项】

- A. 日志。
- B. 名称。
- C. 设置。
- D. 登录服务器 Server10，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
- E. 登录服务器 Server10，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
- F. 属性。

正确答案： 1、D 2、F 3、A 4、B

64、在一台安装了 Windows 操作系统的域控制器服务器 Server11 上，管理员需要设置 Windows 防火墙属性：将防火墙状态设置为：关闭。

在一台安装了 Windows 操作系统的域控制器服务器 Server11 上，管理员需要设置 Windows 防火墙属性：将防火墙状态设置为：关闭。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

步骤 1：\_\_\_\_\_①\_\_\_\_\_。  
步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击\_\_\_\_\_②\_\_\_\_\_。  
步骤 3：在弹出的对话框中，在\_\_\_\_\_③\_\_\_\_\_右侧的列表框中，选择\_\_\_\_\_④\_\_\_\_\_，然后单击“确定”。  
步骤 4：关闭“高级安全 Windows 防火墙”窗口。

请填写：①：( ) ②：( ) ③：( ) ④：( )

答案：①：D. 登录服务器 Server11，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。②：F. 属性③：A. 防火墙状态 ④：C. 关闭

65、在一台安装了 Windows 操作系统的域控制器服务器 Server11 上，管理员需要设置 Windows 防火墙属性：将防火墙状态设置为：关闭。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

步骤 1：( )  
步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击( )。  
步骤 3：在弹出的对话框中，在( )右侧的列表框中，选择( )，然后单击“确定”。  
步骤 4：关闭“高级安全 Windows 防火墙”窗口。

【答案选项】

- A. 防火墙状态。
- B. 阻止。
- C. 关闭。
- D. 登录服务器 Server11，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
- E. 登录服务器 Server11，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
- F. 属性。

正确答案： 1、D 2、F 3、A 4、C

66、在一台安装了 Windows 操作系统的域控制器服务器 Server9 上，管理员需要设置 Windows 防火墙属性：记录被丢弃的数据包。

要求：从答案选项中选择正确的选项，将其对应的字母填写在空白的操作步骤中，从而把步骤补充完整。

【操作步骤】：

步骤 1：( )  
步骤 2：在左侧导航栏中，右击“本地计算机上的高级安全 Windows 防火墙”并单击( )。  
步骤 3：在弹出的对话框中，单击( )右侧的“自定义”。  
步骤 4：在弹出的对话框中，在( )右侧的列表框中，选择“是”，然后单击“确定”。  
步骤 5：返回上一级对话框，单击“确定”。  
步骤 6：关闭“高级安全 Windows 防火墙”窗口。

【答案选项】

- A. 日志。
- B. 记录被丢弃的数据包。
- C. 设置。
- D. 登录服务器 Server9，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 wf.msc，单击“确定”。
- E. 登录服务器 Server9，在桌面左下角右击“Win 图标”→“运行”，在弹出的“运行”对话框中输入 firewall.cpl，单击“确定”。
- F. 属性。

正确答案： 1、D 2、F 3、A 4、B