

智慧农业——环境监测系统服务器搭建与配置

🖉 引导案例

新中国成立以来,中国农业虽然实现了机械化生产的普及,节约了劳动力成本、 提高了生产效率,但是依然存在着缺陷。典型的缺陷是农产品质量参差不齐、附加值 低,需要通过精细化管理来改善。物联网技术能够为农产品的精细化管理提供强有力 的支撑,可以通过实时监控农产品的生长环境,及时采取调控措施,保障农产品顺利 生长,从而提高农产品质量和附加值,促进中国农业朝着精细化和智能化方向发展。

智慧农业——环境监测系统(见图 1-1-1)是基于物联网技术打造的农产品实时环 境监测系统,包括传感器、执行器、信号传输线路及服务器,其中服务器是整个系统 的核心组成部分。因此,正确完成服务器的操作系统安装、运行环境配置、安全策略 设置、Web 服务搭建对整个系统而言非常重要。



图 1-1-1 智慧农业——环境监测系统

任务 1 环境监测系统服务器操作系统安装及运行环境配置

🕷 职业能力目标

- 能根据现场的实际要求,完成虚拟机软件的选择、安装和配置。
- 能根据服务器配置,完成操作系统的选择、安装和配置。
- 能根据系统应用软件的需要,完成运行环境相关软件的安装和配置。

☑ 任务描述与要求

任务描述:

L公司长期深耕于物联网行业,业务涵盖物联网的设计、施工及运维等相关领域。近期,L公司承接了N农场的智慧农业——环境监测系统项目。N农场希望该系统能实现对其农产品生长过程的全程监测,对温湿度、光照等关键环境要素进行实时调整,以及通过后台服务器完成环境监测和调控。

L公司决定安排工程师LA负责服务器的搭建和配置。LA抵达现场后,通过合同约定、现场实际环境勘察及用户意见沟通,确定通过虚拟机搭载Windows Server 2019 操作系统,并安装.NET Framework 和 JDK 软件,从而完成服务器的操作系统 安装和运行环境配置。

任务要求:

- 选择虚拟机软件并完成安装和配置。
- 完成 Windows Server 2019 操作系统的安装。
- 完成.NET Framework 和 JDK 软件的安装。

🗳 知识储备

1.1.1 虚拟机介绍

虚拟机,英文全称为 Virtual Machine,是指通过软件来模拟出完整的计算机系统,模拟 的系统具备硬件系统功能,并运行在彻底隔离的环境中。简单的理解就是,虚拟机能够实 现实体计算机的功能,并完成各项工作任务。当虚拟机安装在实体计算机(宿主机)上时, 需要将宿主机的部分硬盘和内存容量作为虚拟机的硬盘和内存容量。每个虚拟机都有独立 的 CMOS、硬盘和操作系统,用户可以像使用实体计算机一样对虚拟机进行操作。

1. 虚拟机分类

(1) 系统虚拟机

系统虚拟机是一种安装在 Windows 计算机上的虚拟操作环境,其本质是宿主机上的文

件,而非真正意义上的操作系统。但是系统虚拟机可以实现与真实的操作系统一样的功能。 常见的系统虚拟机有 Linux 虚拟机、Microsoft 虚拟机、Mac 虚拟机、BM 虚拟机、HP 虚拟 机、SWsoft 虚拟机、SUN 虚拟机、Intel 虚拟机、AMD 虚拟机、BB 虚拟机等。

(2) 程序虚拟机

程序虚拟机可以在实体计算机上仿真模拟计算机的各种功能,是一个虚构出来的计算 机程序。程序虚拟机具有完善的硬件架构,如处理器、堆栈、寄存器等,以及相应的指令系 统。典型的程序虚拟机有 Java 虚拟机(简称 JVM)。

(3) 操作系统层虚拟化

操作系统层虚拟化是一种虚拟化技术,可以将操作系统内核虚拟化,允许用户将软件物件的空间分割成几个独立的单元并在内核中运行,而不只运行一个单一物件。软件物件通常也被称为容器(Container)、虚拟引擎(Virtualization Engine)、虚拟专用服务器(Virtual Private Server)或 Jail。典型的软件物体有 Docker 容器。

2. 主流虚拟机软件

(1) VMware Workstation

VMware 是 EMC 公司下属的一个独立软件公司,于 1998 年 1 月创立,主要研究在工业领域中应用的大型主机级的虚拟技术计算机,并于 1999 年发布了它的第一款产品:基于 主机模型的虚拟机 VMware Workstation。VMware 目前是虚拟机市场上的领航者,首先提出 并采用的气球驱动程序、影子页表、虚拟设备驱动程序等均被后来的其他虚拟机采用。在 VMware 中可以同时运行 Linux 各种发行版本、DOS、Windows 各种版本、UNIX 等。

(2) VirtualBox

VirtualBox 由德国 Innotek 公司开发,由 Sun Microsystems 公司出品,是一款开源的虚 拟机软件。在 Sun Microsystems 公司被 Oracle 公司收购之后,该软件正式更名为 Oracle VM VirtualBox。用户可以在 VirtualBox 上安装并执行 Solaris、Windows、DOS、Linux、OS/2 Warp、BSD 等系统,并将其作为客户端操作系统。

(3) Virtual PC

Virtual PC 是最新的 Microsoft 虚拟化技术。使用此技术可以在一台计算机上同时运行 多个操作系统。和其他虚拟机一样,Virtual PC 可以在一台计算机上同时模拟多台计算机, 虚拟的计算机使用起来与真实的计算机一样,还可以进行 BIOS 设定、硬盘进行分区、格式 化、操作系统安装等功能操作。

1.1.2 Windows Server 2019 介绍

根据不同的公司和操作系统内部结构划分,目前市面上主流的网络操作系统可以分为 Windows 类、Linux 类、UNIX 类等。归属 Windows 类的 Windows Server 系列是 Microsoft 公司在 2003 年 4 月 24 日推出的服务器操作系统,其核心是 Microsoft Windows Server

System,目前最新的服务版本是 Windows Server 2019。Windows 类的服务器操作系统在界面图形化、多用户、多任务、网络支持、硬件支持等方面都有良好表现。

1. Windows Server 2019 功能

(1) 混合云

Windows Server 2019 提供混合云服务,包括具有 Active Directory 的通用身份平台、基于 SQL Server 技术构建的通用数据平台,以及混合管理和安全服务。

① 混合管理

混合管理功能为 Windows Server 2019 的内置功能。Windows Admin Center(管理中心) 将传统的 Windows Server 管理工具整合到基于浏览器的现代远程管理应用中,该应用适用 于任何位置(包括物理环境、虚拟环境、本地环境、Azure 和托管环境)上运行的 Windows Server。

② Server Core

Windows Server 2019 中的 Server Core 按需应用兼容性功能,包含具有桌面体验图形环境的 Windows Server 的一部分二进制文件和组件,无须添加环境本身,因此显著提高了 Windows Server 核心安装选项的应用兼容性,增加了 Server Core 的功能,同时尽可能保持精简。

(2) 安全增强

Windows Server 2019 中的安全性方法包括 3 个方面:保护、检测和响应。

① Windows Defender 高级威胁检测

Windows Server 2019 集成的 Windows Defender 高级威胁检测可发现和解决安全漏洞, 攻击防护可帮助防止主机入侵。该功能会锁定设备以避免攻击媒介的攻击,并阻止恶意软 件攻击中常用的行为。而保护结构虚拟化功能适用于 Windows Server 或 Linux 工作负载的 受防护虚拟机,可保护虚拟机工作负载免受未经授权的访问。打开具有加密子网的交换机 的开关,即可保护网络流量。

2 Windows Defender ATP

Windows Server 2019 将 Windows Defender 高级威胁防护(ATP)嵌入到了操作系统中,可提供预防性保护,检测攻击、零日漏洞及其他功能。这使得用户可以访问深层内核和内存传感器,从而提高性能和防篡改,并在服务器计算机上启用响应操作。

(3) 容器改进

4

Windows Server 2019 的容器技术可帮助 IT 专业人员和开发人员进行协作,从而更快地 交付应用程序。通过将应用从虚拟机迁移到容器中,同时将容器优势转移到现有应用中, 且只需最少量的代码更改。 ① 容器支持

Windows Server 2019 可以借助容器更快地实现应用现代化。它提供更小的 Server Core 容器镜像,可加快下载速度,并为 Kubernetes 集群和 Red HatOpenShift 容器平台的计算、存储和网络连接提供更强大的支持。

② 工具支持

Windows Server 2019 改进了 Linux 操作,基于之前对并行 Linux 和 Windows 容器的支持,还可为开发人员提供对 Open SSH、Curl 和 Tar 等标准工具的支持,从而降低复杂性。

③ 应用程序兼容

Windows Server 2019 使基于 Windows 的应用程序容器化变得更加简单,提高了现有 Server Core 容器映像的应用兼容性。

④ 性能改进

Windows Server 2019 基本容器映像的安装包大小、本地文件的大小和启动时间都得到 了改善,从而加快了容器工作流。

(4) 超融合

Windows Server 2019 中的技术扩大了超融合基础架构(HCI)的规模,增强了性能和可靠性。通过具有成本效益的高性能软件定义的存储和网络使 HCI 民主化,它允许部署规模从两个节点扩展到多达 100 个节点。

Windows Server 2019 中的 Windows Admin Center 是一个基于轻量浏览器且部署在本地的 平台,可整合资源以增强可见性和可操作性,进而简化 HCI 部署的日常管理工作。

2. Windows Server 2019 版本介绍

(1) 许可版本

Windows Server 2019 目前包括 3 个许可版本,各个版本的应用场景如下。

① Datacenter Edition (数据中心版)

Datacenter Edition 适用于高虚拟化数据中心和云环境。

② Standard Edition (标准版)

Standard Edition 适用于物理或最低限度虚拟化环境。

③ Essentials Edition (基本版)

Essentials Edition 适用于最多 25 个用户或最多 50 台设备的小型企业。

(2) 版本区别

基本版目前应用较少,所以主要对标准版和数据中心版两个版本进行比较,如表 1-1-1 所示。其中,Hyper-V 是 Microsoft 提出的一种系统管理程序虚拟化技术,能够实现桌面虚 拟化,设计目的是为广泛的用户提供更为熟悉、成本效益更高的虚拟化基础设施软件,这 样可以降低运作成本、提高硬件利用率、优化基础设施并增强服务器的可用性。

功能	Windows Server 2019 Standard	Windows Server 2019 Datacenter		
可田作虐却化士机	支持,每个许可证允许运行两台虚拟	支持,每个许可证允许运行无限台虚拟		
可用作应弧化工机	机及一台 Hyper-V 主机	机及一台 Hyper-V 主机		
Hyper-V	支持	支持,包括受防护的虚拟机		
网络控制器	不支持	支持		
<u> </u>	支持(Windows 容器不受限制;	支持(Windows 容器和 Hyper-V 容器		
谷岙	Hyper-V 容器最多为两个)	均不受限制)		
主机保护对 Hyper-V 支持	不支持	支持		
方碑可未	支持(一种合作关系和一个具有单个	士快 王阳制		
计随副平	2TB 卷的资源组)	又持, 无限刑		
存储空间直通	不支持	支持		
继承激活	在托管于数据中心时作为访客	可以是主机或访客		

表 1-1-1 标准版和数据中心版两个版本比较

1.1.3 Microsoft. NET Framework 介绍

Microsoft.NET Framework(简称.NET Framework)是用于 Windows 的新托管代码编程 模型。其用于构建具有视觉上引人注目的用户体验的应用程序,能实现跨技术边界的无缝 通信,并且能支持各种业务流程。每台计算机上都需要安装 Microsoft.NET Framework,它 是开发框架的运行库。如果程序开始是使用.NET 开发的,则需要使用 Microsoft.NET Framework 作为底层框架。

Microsoft.NET Framework 支持生成和运行 Windows 应用及 Web 服务,旨在实现下列目标。

- 提供一个一致的、面向对象的编程环境,无论对象代码是在本地、Web 服务器中,还 是远程存储和执行。
- 提供一个将软件部署和版本控制冲突最小化的代码执行环境。
- 提供一个可提高代码(包括由未知的或不完全受信任的第三方创建的代码)执行安全 性的代码执行环境。
- 提供一个可消除脚本环境或解释环境的性能问题的代码执行环境。
- 使开发人员的经验在面对类型大不相同的应用(如基于 Windows 的应用和基于 Web 的应用)时保持一致。
- 按照工业标准生成所有通信,确保基于.NET Framework 生成的代码可与任何其他代码集成。

1.1.4 Java Development Kit介绍

Java 运行环境(Java Runtime Environment,简称 JRE)是一个软件,可以让计算机系统

运行 Java 应用程序(Application Program)。JRE 的内部有一个 Java 虚拟机(Java Virtual Machine,简称 JVM),以及一些标准的类别函数库(Class Library)。

Java Development Kit(简称 JDK)是 Java 语言的软件开发工具包,主要用于移动设备、嵌入式设备上的 Java 应用程序。JDK 是整个 Java 开发的核心,包含了 JRE 和 Java 工具。

没有 JDK 的话,无法编译 Java 程序(指 Java 源码.java 文件)。如果只想运行 Java 程序(指 class 或 jar 或其他归档文件),则要确保已安装相应的 JRE。JVM、JRE、JDK 之间的关系如图 1-1-2 所示。



图 1-1-2 JVM、JRE 和 JDK 之间的关系

■ 任务实施

1. 环境监测系统虚拟机安装

本任务选用 VirtualBox 作为虚拟机安装软件,具体操作如下。

(1) VirtualBox 软件下载

访问 VirtualBox 官方网站,根据本任务的宿主机使用的是 Windows 系统这一情况,选择 "Windows hosts"选项,如图 1-1-3 所示。

	VirtualBox Download VirtualBox
	Here you will find links to VirtualBox binaries and its source code.
About	VirtualBox binaries
Screenshots	By downloading, you agree to the terms and conditions of the respective license.
Downloads	If you're looking for the latest VirtualBox 6.0 packages, see VirtualBox 6.0 builds. Please also use version 6.0 if you need to run VMs with software
Documentation	virtualization, as this has been discontinued in 6.1. Version 6.0 will remain supported until July 2020.
End-user docs	If you're looking for the latest VirtualBox 5.2 packages, see VirtualBox 5.2 builds. Please also use version 5.2 if you still need support for 32-bit hosts, as
Technical docs	this has been discontinued in 6.0. Version 5.2 will remain supported until July 2020.
Contribute	VirtualBox 6.1.32 platform packages
Community	• ⊡Windows hosts
	• ©/OS X hosts Linux distributions
	Solaris hosts
	• 🖙 Solaris 11 IPS hosts



(2) VirtualBox 软件安装

软件安装过程极为简单,双击待安装软件,按照默认的提示安装即可。

2. 环境监测系统 Windows Server 2019 安装

(1) Windows Server 2019 下载

Microsoft 官方网站提供各种版本的 Windows 操作系统下载源,如下载 Windows Server 2019,只需到 Microsoft 官方网站,按照网页提示下载软件即可。

(2) Windows Server 2019 安装

在已经安装的虚拟机上进行 Windows Server 2019 操作系统的安装,具体操作如下。

① 虚拟电脑的创建

单击"新建"按钮,在"名称"文本框中输入虚拟电脑名称"Windows Server 2019", 在"版本"下拉列表中选择"Other Windows (64-bit)"选项,如图 1-1-14 所示。单击"下 一步"按钮,在弹出的对话框中设置内存容量,建议至少为 4096MB,并选择"现在创建虚 拟硬盘"选项。

② 虚拟硬盘的创建

将"虚拟硬盘文件类型"设置为"VDI(VirtualBox,磁盘映像)",将"硬盘空间使用" 设置为"动态分配",单击"下一步"按钮。选择文件存放的位置,设置硬盘大小,建议设 置为"30GB",如图 1-1-5 所示。

? ×
← 创建虚拟硬盘
文件位置和大小
请在下面的框中键入新建虚拟硬盘文件的名称,或单击文件夹图标来选择创建文件要保存到的文件夹。
alBox VMs\Windows Server 2019\Windows Server 2019. vdi 🛛 🗔
选择虚拟硬盘的大小。此大小为虚拟硬盘文件在实际硬盘中能用 的极限大小。
30.00 GB
4.00 MB 2.00 TB
创建 取消

图 1-1-4 新建虚拟电脑

图 1-1-5 创建虚拟硬盘

③ 虚拟电脑的启动

在 "Oracle VM VirtualBox 管理器"界面左侧列表中出现了"Windows Server 2019"选项,单击"启动"按钮,如图 1-1-6 所示。

🦸 Oracle VM VirtualBox 管理器					
管理(F) 控制(M) 帮助(H)					
	新建(N)	父 设置(S)	小清除	() 启动(T)	•
♥ ♥indows Serv 目目 ● 己关闭	_				

图 1-1-6 启动虚拟电脑

④ 启动盘的选择

在"选择启动盘"对话框中,选择 Windows Server 2019 的 ISO 文件,单击"启动"按钮,如图 1-1-7 所示。

注册(A) 创建(C) 刷新(R)	
名称	虚拟分配空间 ^
cn_windows_server_2019_x64_dvd_4de	e40f33.iso 4.74 GB
VBoxGuestAdditions.iso	57.82 MB ✓
2	>
按名称搜索 ▼	R R
选择	留空 取消
	注册(A) 创建(L) 和前(A) 名称

图 1-1-7 选择启动盘

⑤ Windows Server 2019 安装过程

按照安装程序向导的提示进行安装,在倒数第二个设置步骤之前都较为简单,这里只 做简要说明,具体操作如下。

- ▶"要安装的语言""时间和货币格式""键盘和输入方法"均选择默认,单击"下一步" 按钮。
- ▶ 在弹出的对话框中单击"现在安装"按钮。
- ▶ 在"激活 Windows"对话框中选择"我没有产品密钥"选项。
- ▶ 在"选择要安装的操作系统"对话框中选择"Windows Server 2019 Standard (桌面体验)"选项,单击"下一步"按钮。
- ▶在"适用的声明和条款"对话框中勾选"我接受许可条款"复选框,单击"下一步" 按钮。
- ▶在"你想执行哪种类型的安装"对话框中,勾选"自定义,仅安装 Windows (高级)" 复选框。
- ⑥ 磁盘空间的划分

磁盘空间的划分至关重要,当出现"你想将 Windows 安装在哪里"对话框时,需要创 建分区,如图 1-1-8 所示。单击"新建"按钮,输入磁盘大小,比如 15360MB(建议系统盘 大小至少为 10240MB,即 10GB),单击"应用"按钮,建议将硬盘至少划分为两个分区。

R想将 Windows	安装在哪里?			
名称		总大小	可用空间	类型
── 驱动器 0 分	☑ 1: 系统保留	549.0 MB	532.0 MB	系统分区
<>>> 驱动器 0 分	∑ 2	14.5 GB	14.5 GB	主分区
<>> 驱动器 0 分	⊠ 3	15.0 GB	15.0 GB	主分区
← 刷新(E)	★刪除(型))
》)加载驱动程序(L)	⊉扩展(⊻)			
				-

图 1-1-8 划分磁盘空间

⑦ 登录密码的设置

在操作系统自动安装完成之后,提示设置初始登录密码,初始登录密码的要求如下。 ▶不能包含用户的账户名。

▶至少有6个字符。

▶至少包含以下 4 类字符中的 3 类字符:英文大写字母(A~Z)、英文小写字母(a~z)、基本数字(0~9)、非字母字符(如!、\$、#、%)。

3. 环境监测系统 Windows Server 2019 网络配置

在虚拟机上完成 Windows Sever 2019 操作系统的安装工作之后,该操作系统还需要能够对 Internet 网络进行访问。因此,还要做相应的网络配置,具体操作如下。

(1) 设置 VirtualBox

在"Orade VM VirtualBox 管理器"界面中完成宿主机与虚拟机之间的网络设置。选择 "Windows Sever 2019"选项,单击"设置"按钮,在"Windows Server 2019-设置"界面中 选择"网络"选项,在对应的选项卡中将"连接方式"设置为"桥接网卡","界面名称"设 置为宿主机当前连接 Internet 使用的网卡,"混杂模式"设置为"全部允许",单击"OK"按 钮。设置界面如图 1-1-9 所示。

(2) 宿主机和虚拟机间的网络测试

在宿主机上通过"Win+R"组合键打开"运行"程序,在文本框中输入"cmd",单击"确定"按钮,打开命令提示符窗口。在打开的窗口中输入"ipconfig/all"命令,如图 1-1-10 所示,获取宿主机的 IP 地址,如 192.168.1.4。

智慧农业——环境监测系统服务器搭建与配置 项目1

🔋 Oracle VM VirtualBox 管理器			
管理(F) 控制(M) 帮助(H)			
TRY IA	新建(N) 设置(S)	→	
Tindors Server 2019	Windows Serv	er 2019 - 设置	? X
	二 常规	网络	
	■ 系统	网卡1 网卡2 网卡3 网卡4	
		✓ 启用网络连接(E)	
	▶ 存储	」连接方式(A): 桁接內卡 ▼ 奥而之称(N): Realtab RT18723RE Wireless IAN 802 11p PCT-E NTC	-
	● 声音	▼ 高級(d)	
	网络 网络	控制芯片(T): Intel PRO/1000 MT 桌面 (82540EM)	~
	☆ 串口		-
	DSB设备	mac. 19111 0m/. 00000 rbA1041 ☑ 接入网线(C)	e
	共享文件夹	端口转发 (P)	
	用户界面		
		下有	
		ОК	Cancel

图 1-1-9 VirtualBox 虚拟机网络设置

在虚拟机上同样通过"Win+R"组合键打开"运行"程序,在文本框中输入"cmd", 单击"确定"按钮,打开命令提示符窗口。使用"ping 宿主机 IP"命令,测试虚拟机与宿 主机间网络连接的通断,能 ping 通并且无任何丢包表明连接正常,如图 1-1-11 所示。



图 1-1-10 获取宿主机 IP 地址的命令

图 1-1-11 虚拟机与宿主机连接验证

(3) 虚拟机静态 IP 地址设置

日常中可能还会需要将虚拟机 IP 地址设置为固定值,这里也进行简单说明,具体操作如下。

① 服务器管理器

右击"此电脑",在弹出的快捷菜单中选择"管理"命令,如图 1-1-12 所示,弹出"服务器管理器"界面。

✔ ≱ 快速访问	> 文件夹 (7)
桌面	★ 3D 对象
➡ 下载	*
🔮 文档	* 图片
■ 图片	*
> 💷 此电脑	
	展开(A)
	♥ 管理(G)
	固定到"开始"屏幕(P)

图 1-1-12 打开服务器管理器

② 网络连接

在"服务器管理器"界面中选择"本地服务器"选项,单击"由 DHCP 分配的 IPv4 地 址, IPv6 已启用"文字链接, 双击"网络连接"界面中的"以太网"图标, 如图 1-1-13 所 示,弹出"以太网状态"对话框。

▶ 服务器管理器				🔮 网络连接	
(€) ● • • 本地	服务	器	• 🕝 🚩 管理(M) 工具(1	(→	> 网络连接
				组织 ▼	
■ 仪表板		用于 WIN-FU3PHCFA8	7M	以太网 网络 2	
本地服务器		计管机名	WIN-FU3PHCEA87M	Intel(R) PRO/1000 MT Deskto	
所有服务器		工作组	WORKGROUP		
🔹 文件和存储服务	⊳		レイイト	1.2	
			GIX IF		
		Windows Defender 防火墙	专用: 启用		
		远程管理	ビ启用 日本田		
		NIC 组合	已禁用		
		以太网	由 DHCP 分配的 IPv4 地址, IPv6 已启用		
		图 1	-1-13 打开网络连	接	

③ IP 地址设置

在"以太网状态"对话框中单击"属性"按钮,弹出"以太网属性"对话框,双击"Internet 协议版本 4 (TCP/IPv4)"选项,在弹出的"Internet 协议版本 4 (TCP/IPv4) 属性"对话框 中输入需要的 IP 地址、子网掩码、默认网关和 DNS 服务器地址,如图 1-1-14 所示。

🖗 以太网 状态	🖗 以太网 属性	Internet 协议版本 4 (TCP/IPv4) 雇性
常规	网络	常规
连接 IPv4 连接: ID-6 注注:	连接时使用:	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。
媒体状态: 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):
速度:	☑ 號 Microsoft 网络客户端 ☑ 號 Microsoft 网络的文件和打印机共享	IP 地址(I): 192 . 168 . 1 . 5
详细信息(E)		子网掩码(U): 255.255.255.0
	■ Internet 所成版本 4 (TCP/IPV4) ■ Microsoft 网络适配器多路传送器物	默认网关(D): 192.168.1.1
活动	 ☑ Microsoft LLDP 协议驱动程序 ☑ Internet 协议版本 6 (TCP/IPv6) ☑ 链路扁柘扑发现响应程序 	 自动获得 DNS 服务器地址(B) ● 使用下面的 DNS 服务器地址(E):
李节: 9,785,183 17	安装(N) 卸载(U) 描述	首选 DNS 服务器(P): 8 . 8 . 8 . 8 备用 DNS 服务器(A):
● 屬性(P) ● 禁用(D) 参断(G)	传输控制协议/Internet 协议。该协议是 于在不同的相互连接的网络上通信。	□退出时验证设置(L) 高级(V)

图 1-1-14 设置 IP 地址

4. 环境监测系统共享文件夹设置

本操作的目的是在环境监测系统服务器宿主机和虚拟机之间创建共享文件夹,以实现 两者之间的文件共享,具体操作如下。

(1) 宿主机共享文件夹创建及设置

在宿主机上创建名为"虚拟机共享"的文件夹,右击该文件夹,在弹出的快捷菜单中选择"属性"命令,在弹出的对话框中选择"共享"选项,在"共享"选项卡中单击"共享"按钮,在弹出的对话框中选择要与其共享的用户,比如"asus",单击"共享"按钮,如图 1-1-15 所示。在后续的对话框中单击"完成"按钮即可。

~	21 网络访问		
	选择要与其共享的用户		
	键入名称,然后单击"添加",或者单击箭头查找用户。		
	asus	~ 添加(A)	
	名称	权限级别	
	A asus 共享时有问题	Finate Finate	FIL
		♥共享(H) 取消	

图 1-1-15 设置共享文件夹

(2) VirtualBox 共享设置

在"Oracle VM VirtualBox 管理器"界面中单击"设置"按钮,在"Windows Server 2019-设置"界面中选择"共享文件夹"选项,单击右侧的 图标或者按"Insert"键,在弹出的 "添加共享文件夹"对话框中,将"共享文件夹路径"设置为宿主机创建的"虚拟机共享" 文件夹的路径,勾选"固定分配"复选框,单击"OK"按钮,如图 1-1-16 所示。

新建(JI) 新建(JI) ② Windows Serve	→ 清除 显示(H) er 2019 - 设置	•					?		×
 第規 系统 	共享文件夹 共享文件夹(F)								
□ □ □ □ □ □ □ □ □ □ □ □ □ □	名称 路径 固定分配 临时分配	添加共享文件 共享文件夹器径: 共享文件夹名称: 挂载点:	央 「星小以1sptho 「星沢秋1共享 」 只读分配(a) 自动挂載(b) 「国家分配(0) の版	? be9\虚拟机共5 Canc	×	访问权限	自动挂戴	Ŧ [
						OK	0	Cancel	

图 1-1-16 设置 VirtualBox 共享

(3) 虚拟机共享设置

① 增强功能安装

在虚拟机上单击"设备"按钮,在弹出的快捷菜单中选择"安装增强功能"命令, 如图 1-1-17 所示。

设备	F 帮助	
\odot	分配光驱	•
1	声音	•
P	网络	•
Ø	USB	•
	共享文件夹	•
	共享粘贴板	+
5	拖放	•
8	安装增强功能	

图 1-1-17 安装增强功能

② VBoxWindowsAdditions 安装

在"此电脑"界面中单击"CD驱动器"图标,双击"VBoxWindowsAdditions"应用程序,按照提示完成安装并重启。

③ 网络发现和文件共享设置

在"此电脑"界面中选择"网络"选项,出现提示"文件共享已关闭。看不到网络计算机 和设备,单击更改",选择"启动网络发现和文件共享"选项,如图 1-1-18 所示。

🖆 🖸 🛛 🔻	网络			-	
文件 网络	查看				
$\leftarrow \rightarrow \uparrow \uparrow$	💣 > 🕅	络》			∨ Ū 搜索"网
文件共享已关闭。	看不到网络	针算机和设备。单击更改…		络发现和文件共享(T)	1.
♪ 快速访问		∨ 计算机 (4)	打开网	络和共享中心(O)	-
📰 桌面	*	LAPTOP-PHIH	OBE9	WIN-F	U3PHCFA87M
➡ 下载	*				
	А.	DESKTOP-V55	SJI5A		P-OG822O38
📰 图片	1				
🖳 此电脑					
💣 网络					
	文件 网络 ← 个 文件共享已关闭。 # 快速访问 桌面 下载 圓 文档 ご 附出 歐 加出 政 四 丁 丁 丁 ○	文件 网络 查看 文件 网络 查看 ← 个 小 网 文件共享已关闭。看不到网络 # ● 桌面 * * 東面 * * 丁乾 * 〇 文档 * 〇 四日片 * 〇 山电脑 ●	文件 网络 查看 文件 网络 查看 ◆ 个 》、网络 > 文件共享已关闭。看不到网络计算机和设备、单主更改… > ★ 快速访问 > 桌面 * > ● 下载 * ● 文档 * ● 文档 * ● 文档 * ● 如片 * ● 此电脑 ● ● 网络 ●	文件 网络 查看 文件 网络 查看 文件 小 网络 文件 小 小 文件 小 小 文件 小 小 一 小 小 一 小 小 一 小 11 一 小 11 一 小 11 一 小 11 回 文档 小 回 文档 小 回 DESKTOP-V55315A 0 ● 山 山 小 田 1 ● 山 山 ● 山 日 ● 山 日 ● 小 日 ● 山 日 ● 山 日 ● □ □ ● <	文件 网络 文件 网络 文件 网络 女件 小 文件 小 · 小 · ·

图 1-1-18 启用网络发现和文件共享

随后出现"VBOXSVR"图标,单击该图标可以看到宿主机创建的共享文件夹,通过该 文件夹可以实现宿主机和虚拟机之间的文件互传,如图 1-1-19 所示。

💻 🖉 🛄 🖛 VBOXSVE	R
文件 主页 共享	查看
← → · ↑ 💻 › 🕅	络 > VBOXSVR
🧐 CD 驱动器 (D:) 🔦	\\Vboxsvr\虚拟机共享
🌧 网络	
DESKTOP-V5SJ	
LAPTOP-OG82	
LAPTOP-PHIHC	
VBOXSVR	
WIN-FU3PHCF/	

图 1-1-19 查看共享文件夹

5. 环境监测系统 JDK 安装

(1) JDK 软件下载

 \bigcirc

访问 Oracle 官方网站,选择"资源"→"Java 下载"选项,在 Java 软件列表中选择面 向开发人员的 Java (JDK),选择 Windows 版本的 64 位压缩包进行下载。

(2) JDK 软件安装

在虚拟机上安装已经下载的 JDK 压缩包, 整个安装过程非常简单, 按照提示安装即可。

(3) JDK 环境变量设置

① 环境变量设置界面

右击"此电脑",在弹出的快捷菜单中选择"属性"命令,在"系统"界面中选择"高级系统设置"选项,在"系统属性"对话框中选择"高级"选项,单击"环境变量"按钮,如图 1-1-20 所示,弹出"系统变量"对话框。



图 1-1-20 设置环境变量

② JAVA_HOME 环境变量设置

单击"新建"按钮,在"新建系统变量"对话框中,新建系统变量"JAVA_HOME", 设置变量值为 JDK 的安装路径,也可以通过单击"浏览目录"按钮选择,单击"确定"按 钮,如图 1-1-21 所示,返回"系统变量"对话框。

系统变量(S)			
新建系统变量			
变量名(N):	JAVA_HOME		
变量值(V):	C:\Program Files\Java		-
浏览目录(D)	浏览文件(F)	确定取	Ē
		新建(W) 编辑(I) 删除(L)	
		确定取消	

图 1-1-21 设置 JAVA_HOME 环境变量

③ CLASSPATH 环境变量设置

再次单击"新建"按钮,弹出"新建系统变量"对话框,将"变量名"设置为"CLASSPATH", "变量值"设置为".;%JAVA_HOME%\lib\dt.jar;%JAVA_HOME%\lib\tools.jar",单击"确定" 按钮,如图 1-1-22 所示。

系统变量(S)				
新建系统变量				
变量名(N):	CLASSPATH			
变量值(V):	.;%JAVA_HOME%\lib\dt.	jar;%JAVA_HOME%\lib\te	ools.jar	
浏览目录(D)	浏览文件(F)		确定	取消
		新建(W)	编辑(I)	删除(L)

图 1-1-22 设置 CLASSPATH 环境变量

④ Path 环境变量设置

在"系统变量"列表中选择"Path"变量,单击"编辑"按钮,在弹出的"编辑环境变量"对话框中单击"新建"按钮,在文本框中输入"%JAVA_HOME%\bin",单击"确定"按钮,如图 1-1-23 所示。

uministrator 的用户支重(0)		编辑环境变量	
变量	值		
Path	C:\Users\Administrator\AppData\Local\Microsoft	C:\Program Files (x86)\Common Files\Oracle\Java\javapath	新建()
TEMP	C:\Users\Administrator\AppData\Local\Temp	%SystemRoot%\system32	
TMP	C:\Users\Administrator\AppData\Local\Temp	%SystemRoot%	编辑(6
		%SystemRoot%\System32\Wbem	
		%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\	浏览(B
		%SYSTEMROOT%\System32\OpenSSH\	
		%JAVA_HOME%\bin	删除([
	新建(N) 编辑(E)		
			上移(
伝本县(0)			
5元文里(3)			下移(0
变量	值		
JAVA_HOIVIE	C:\Program Files\Java		
NUMBER_OF_PROCESSOR	C:\Program Files\Java S 1		编辑文本
NUMBER_OF_PROCESSOR OS	C:\Program Files\Java S 1 Windows_NT		编辑文本
NUMBER_OF_PROCESSOR OS Path	C:\Program Files\Java S 1 Windows_NT C:\Program Files (x86)\Common Files\Oracle\Java		编辑文本
NUMBER_OF_PROCESSOR OS Path PATHEXT	C:\Program Files\Java S 1 Windows_NT C:\Program Files (x86)\Common Files\Oracle\Java .COM; EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSF		编辑文本
NUMBER_OF_PROCESSOR OS Path PATHEXT PROCESSOR_ARCHITECT	C:\Program Files\Java S 1 Windows_NT C:\Program Files (x86)\Common Files\Oracle\Java .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSI AMD64		编辑文本
NUMBER_OF_PROCESSOR OS Path PATHEXT PROCESSOR_ARCHITECT PROCESSOR_IDENTIFIER	C:\Program Files\Java IS 1 Windows_NT C:\Program Files (x86)\Common Files\Oracle\Java .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSI AMD64 Intel64 Family 6 Model 142 Stepping 9, Genuinels		编辑文本
JAVA_HOME NUMBER_OF_PROCESSOR OS Path PATHEXT PROCESSOR_ARCHITECT PROCESSOR_IDENTIFIER	C:\Program Files\Java IS 1 Windows_NT C:\Program Files (x86)\Common Files\Oracle\Java .COM;.EXE;BAT;.CMD;.VBS;.VBE;JS;JSE;.WSF;.WS AMD64 Intel64 Family 6 Model 142 Stepping 9, Genuinels		编辑文本
JAVA_HOME NUMBER_OF_PROCESSOR OS Path PATHEXT PROCESSOR_ARCHITECT PROCESSOR_IDENTIFIER	C:\Program Files\Java S 1 Windows_NT C:\Program Files (x86)\Common Files\Oracle\Java .COM;EXE;BAT;.CMD;.VBS;.VBE;JS;JSE;.WSF;.WS AMD64 Intel64 Family 6 Model 142 Stepping 9, Genuinet		编辑文本

图 1-1-23 设置 Path 环境变量

在 JDK 环境变量都设置好之后,单击"确定"按钮,退出系统环境变量设置界面。

⑤ JDK 安装完成验证

在 JDK 环境变量设置完成之后,按"Win+R"组合键,打开"运行"程序,在文本框 中输入"cmd"并单击"确定"按钮,打开命令提示符窗口,输入"java-version"命令。如 果能够看到 JDK 的版本号,则说明 JDK 安装成功,如图 1-1-24 所示。

-0

管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.17763.107] (c) 2018 Microsoft Corporation。保留所有权利。
C:\Users\Administrator>java -version java version <u>"17.0.1"</u> 2021-10-19 LTS Java(TM) SE Runtime Environment (build 17.0.1+12-LTS-39) Java HotSpot(TM) 64-Bit Server VM (build 17.0.1+12-LTS-39, mixed mode, sharing)
C:\Users\Administrator>_

图 1-1-24 验证 JDK 安装完成

6. 环境监测系统 Microsoft.NET Framework 安装

(1) Microsoft.NET Framework 下载

访问 Microsoft 官方网站,下载.NET Framework。安装该软件的目的是使采用.NET Framework 开发的应用程序能够在服务器上正常运行,所以不需要下载用于应用程序开发的 Developer Pack 版本,选择包含运行库的 Runtime 版本即可。

(2) Microsoft.NET Framework 安装

在安装 Microsoft.NET Framework 时需要保持与 Internet 网络连接通畅,双击下载的安装文件,即可进行在线安装,整个安装过程按照提示进行即可。

▲ 任务小结

本任务介绍了虚拟机、Windows Sever 2019 操作系统、Microsoft.NET Framework 及 JDK 的相关理论知识和安装操作,以及宿主机与虚拟机之间设置共享文件夹的实践方法,让学 生能够理解和掌握 Windows 操作系统的安装及运行环境配置,并为后续各个项目的介绍和 实践做铺垫。

本任务的知识结构思维导图如图 1-1-25 所示。



图 1-1-25 知识结构思维导图

任务 2 环境监测系统服务器安全策略设置

希 职业能力目标

- 能根据用户管理的需要,完成服务器不同层级的用户和用户组设置。
- 能根据安全性和保密性的需要,完成服务器文件和文件夹权限设置。
- 能根据访问安全的需要,完成服务器本地安全策略和防火墙设置。

♥ 任务描述与要求

任务描述:

L 公司的工程师 LA 在完成服务器的操作系统安装和运行环境配置之后,项目 部根据用户需求,安排 LA 对 N 农场的维护人员 NA 进行一次有关服务器安全管理 的技能培训。

LA 通过当前的服务器指导 NA 现场进行实践。考虑到后期运行维护的需要,此次培训 NA 需要掌握的技能包括用户和用户组的设置、文件及文件夹权限的管理、 本地安全策略的设置,以及防火墙的设置。

任务要求:

- 完成 Windows Server 2019 服务器用户和用户组的设置。
- 完成 Windows Server 2019 服务器文件及文件夹权限管理。
- 完成 Windows Server 2019 服务器本地安全策略设置。
- 完成 Windows Server 2019 服务器防火墙设置。

🗳 知识储备

1.2.1 用户账户

用户账户是对计算机用户身份的标识,本地用户账户和密码只对本机有效,存储在本地安全账户数据库 SAM 中,文件路径为"C:\Windows\System32\config\SAM",对应的进程为 lsass.exe。

在 Windows 操作系统中,可以设置多个用户账户,这些用户账户除了具有区分不同用 户的作用,还可以分配不同的权限,从而起到保护系统安全的作用。

1. 用户账户的特征

用户账户具有以下3个典型特征。

(1) 权限

不同的用户账户可以拥有不同的权限。

(2) 名称与密码

每个用户账户都包含一个名称和一个密码。

(3) SID

每个用户账户都拥有一个唯一的安全标识符 SID(Secrurity Identifier)。

2. 系统内置账户

Windows Server 2019 标准版内置用户账户有 4 个。

(1) Administrator

Administrator 是管理本地计算机(域)的内置账户,默认密码永不过期。

(2) DefaultAccount

DefaultAccount 是系统管理的内置账户,默认密码永不过期、账号已禁用。

(3) Guest

Guest 是供来宾访问本地计算机或域的内置账户,默认用户不能修改密码、密码永不过 期、账户已禁用。

(4) WDAGUtilityAcount

WDAGUtilityAcount 是系统为 Windows Defender 应用程序防护方案管理和使用的账户,默认账户已禁用。

1.2.2 组账户

组账户是一些用户账户的集合,组账户内的用户账户自动具备该组账户被赋予的权限。 在 Windows 操作系统中,一个用户账户可以进入多个组,组和组之间可以有不同的权限。 合理利用组账户来管理用户权限,可以减轻网络管理的负担。

1. 本地内置组账户

Windows Server 2019 内置的本地组账户有很多,在这里主要关注以下 8 个组账户。

(1) Users

Users 组是普通用户组,该组的用户无法进行有意或无意的改动。因此,用户可以运行 经过验证的应用程序,但不可以运行大多数旧版应用程序。Users 组是最安全的组,因为分 配给该组的默认权限不允许用户修改操作系统的设置或用户资料。Users 组提供了一个最安 全的程序运行环境。在经过 NTFS 格式化的卷上,默认安全设置旨在禁止该组的用户执行 危及操作系统和已安装程序完整性的操作。用户不能修改系统注册表设置、操作系统文件 或程序文件。用户可以创建本地组,但只能修改自己创建的本地组。用户可以关闭工作站, 但不能关闭服务器。

(2) Power Users

Power Users 组是高级用户组,可以执行除了为 Administrators 组保留的任务的其他任何操作系统任务。分配给 Power Users 组的默认权限允许该组的用户修改整个计算机的设

置。但 Power Users 组不具有将自己添加到 Administrators 组中的权限。在权限设置中, Power Users 组的权限仅次于 Administrators 组。

(3) Administrators

Administrators 组是管理员组。在默认情况下,Administrators 组中的用户对计算机或域 有不受限制的完全访问权。分配给 Administrators 组的默认权限允许该组的用户对整个系统 进行完全控制。一般来说,应该把系统管理员或与其有着同样权限的用户设置为 Administrators 组的成员。

(4) Guests

Guests 组是来宾组, 跟 Users 组的用户有同等的访问权限, 但 Guests 组用户的限制更多。

(5) Backup Operators

Backup Operators 组的用户可以通过 Windows Server Backup 工具来备份与还原计算机 内的文件,不论他们是否有权限访问这些文件。

(6) Performance Monitor Users

Performance Monitor Users 组的用户可以监视本地计算机的运行性能。

(7) Remote Desktop Users

Remote Desktop Users 组的用户可以通过远程计算机的远程桌面服务进行登录。

(8) Network Configuration Operators

Network Configuration Operators 组的用户可以执行常规的网络配置工作,如更改 IP 地址;但是不能安装、删除驱动程序与服务,也不能执行与网络服务器配置有关的操作,如 DNS 服务器与 DHCP 服务器的设置。

2. 特殊组账户

除了前面介绍的组,Windows Server 2019 中还有一些特殊组,这些组的成员无法更改。 下面列出几个常见的特殊组。

(1) Everyone

所有用户都属于 Everyone 组。若 Guests 账户被启用的话,则在分配权限给 Everyone 组时要小心,因为如果某用户在计算机内没有账户,那么在通过网络登录计算机时,该计算机会自动允许该用户利用 Guests 账户来连接,因为 Guests 也属于 Everyone 组,所以该用户将具备 Everyone 组所拥有的权限。

(2) Authenticated Users

凡是利用有效的用户账户登录计算机的用户,都属于 Authenticated Users 组。

(3) Interactive

凡是在本地登录(通过按"Ctrl + Alt + Del"组合键的方式登录)的用户,都属于 Interactive 组。

(4) Network

凡是通过网络来登录计算机的用户,都属于 Network 组。

(5) Anonymous Logon

凡是未利用有效的用户账户登录计算机的用户(匿名用户),都属于 Anonymous Logon 组。Anonymous Logon 默认并不属于 Everyone 组。

1.2.3 文件及文件夹权限

用户在访问服务器资源时,需要具备相应的文件及文件夹权限。值得注意的是,这里 的权限仅适用于文件系统为 NTFS 或者 ReFS 的磁盘,其他的文件系统如 exFAT、FAT32 及 FAT 均不具备权限功能。

权限可划分为基本权限与特殊权限,其中基本权限已经可以满足日常需求,故本书针 社版权所有 对基本权限进行介绍。

1. 基本权限的种类

基本权限可以按文件和文件夹来分类。

(1) 文件基本权限的种类

① 读取

具备读取权限的用户可以读取文件内容、查看文件属性与权限等;还可以通过打开"文 件资源管理器"窗口,右击文件,在弹出的快捷菜单中选择"属性"命令的方法来查看只 读、隐藏等文件属性。

(2) 写入

具备写入权限的用户可以修改文件内容、在文件中追加数据与改变文件属性等(用户 至少具备读取权限和写入权限才可以修改文件内容)。

③ 读取和执行

具备读取和执行权限的用户除了具备读取的所有权限,还具备执行应用程序的权限。

④ 修改

具备修改权限的用户除了具备上述的所有权限,还可以删除文件。

⑤ 完全控制

具备完全控制权限的用户拥有上述的所有权限,以及可更改权限与取得所有权的特殊 权限。

(2) 文件夹基本权限的种类

① 读取

具备读取文件夹权限的用户可以查看文件夹中文件与子文件夹的名称、文件夹的属性 与权限等。

0

2 写入

具备写入文件夹权限的用户可以在文件夹中新建文件与子文件夹、改变文件夹的属性等。

③ 列出文件夹内容

除了拥有读取权限,还具备遍历文件夹的权限,即可以进出此文件夹的权限。

④ 读取和执行

读取和执行权限与列出文件夹内容权限相同。不过列出文件夹内容权限只会被文件夹 继承,而读取和执行权限会同时被文件夹与文件继承。

⑤ 修改

具备修改文件夹权限的用户除了拥有上述所有权限,还可以删除文件夹。

⑥ 完全控制

具备完全控制文件夹权限的用户拥有上述所有权限,以及可更改权限与取得所有权的特殊权限。

2. 用户最终有效权限

在实际操作中,用户可以归属不同的组,不同的组对某个文件或文件夹的权限并不一 定相同。由此,用户最终是否具备对某个文件或文件夹的权限,存在如下规则。

(1) 权限继承

在对文件夹设置权限之后,这个权限默认会被该文件夹的子文件夹与文件继承。

例如,设置用户 A 对甲文件夹拥有读取的权限,则用户 A 对甲文件夹内的文件也拥有 读取的权限。

(2) 权限累加

如果用户同时属于多个组,且该用户与这些组分别对某个文件或文件夹拥有不同的权限设置,则该用户对这个文件的最终有效权限是所有权限的总和。

例如, 若用户 A 本身具备对文件 F 的写入权限, 且该用户同时属于业务部组和经理组, 其中业务部组具备对文件 F 的读取权限, 经理组具备对文件 F 的执行权限;则用户 A 对文 件 F 的最终有效权限为所有权限的总和, 即写入+读取+执行。

(3)"拒绝"权限优先级更高

虽然用户对某个文件的有效权限是其所有权限的总和,但是如果其中有权限被设置为 拒绝,则用户将不会拥有任何访问权限。

例如,用户A本身具备对文件F的读取权限,该用户同时属于业务部组和经理组,且 其对于文件F的权限为拒绝读取和修改,则用户A的读取权限会被拒绝,即用户A无法读 取文件F。

1.2.4 本地安全策略

系统管理员通过组策略充分控制和管理用户的工作环境,可以确保用户拥有受控制的

工作环境,以及限制用户。从而让用户拥有适当的环境,同时减轻服务器管理人员的管理 负担。组策略可以通过本地安全策略和域组策略实现,其中域组策略优先级高于本地安全 策略,即如果设置了域组策略,那么本地安全策略将失效。考虑到本书面向学生群体,这 里只对本地安全策略进行讲解。

本地安全策略包含计算机配置与用户配置两部分,计算机配置只对计算机环境产生影 响,而用户配置只对用户环境产生影响。本地安全策略是用来设置本地单一计算机的策略, 该策略中的计算机配置只会被应用于这台计算机,而用户配置会被应用于这台计算机上登 录的所有用户。

本地安全策略用于提升本地服务器的安全性,包括账户策略(包括密码策略、账户锁 定策略)和本地策略(包括用户权限分配和安全选项策略)。

1. 密码策略

在 Windows Server 2019 操作系统中,密码策略有以下可供设置的选项,其详细功能及要求如下。

(1) 密码必须符合复杂性要求

用户的默认密码必须满足以下要求。

• 不能包含用户账户名称或全名。

• 长度至少要6个字符。

• 至少要包含 A~Z, a~z, 0~9, 特殊字符(如!、\$、#、%)等4 类字符中的3 类。

按照上述要求,111AAAaaa 是有效密码,而1234AAAA 是无效密码,因为它只使用了数字和大写字母两种字符组合。如果用户账户名称为 Mike,那么 123ABCMike 是无效密码,因为它包含了用户账户名称。

(2) 密码长度最小值

密码长度最小值用来设置用户的密码最少需要几个字符,它的取值范围为0~14,默认值为0,表示允许用户不设置密码。

(3) 密码最短使用期限

密码最短使用期限用来设置用户密码最短的使用期限,在期限未到之前,用户不能修 改密码。它的取值范围为 0~998 天,默认值为 0,表示允许用户随时更改密码。

(4) 密码最长使用期限

密码最长使用期限用来设置密码最长的使用期限,用户在登录时,如果密码已经到使 用期限,那么系统会要求用户更改密码。它的取值范围为 0~999 天,0 表示密码没有使用 期限限制,默认值是 42 天。

(5) 强制密码历史

强制密码历史用来设置是否保存用户曾经使用过的旧密码,并确定在用户修改密码时

是否允许重复使用旧密码,具体取值的含义如下。

1~24:表示要保存密码历史记录。如果设置为6,那么表示用户的新密码必须与前6次旧密码不同。

• 0: 为默认值, 表示不保存密码历史记录, 因此密码可以被重复使用。

(6) 用可还原的加密来储存密码

如果应用程序需要读取用户的密码,并用于验证用户身份,那么可以启用可还原的加 密功能来存储密码。不过在开启该功能之后,相当于用户没有进行密码加密,因此除非必 要,不要启用此功能。

2. 账户锁定策略

账户锁定策略有以下可供设置的选项,详细功能及要求如下。

(1) 账户锁定时间

账户锁定时间可以设置锁定账户的时间,时间过后自动解除锁定。它的取值范围为0~ 9999 分钟,0 表示永久锁定,不会自动解除锁定,在这种情况下,必须由系统管理员手动 解除锁定。

(2) 账户锁定阈值

账户锁定阈值可以设置在用户登录多次失败(密码输入错误)之后,锁定用户账户。 在未解除锁定之前,用户无法登录此账户。它的取值范围 0~999,默认值为 0,表示账户 永远不会被锁定。

(3) 账户锁定计数器

账户锁定计数器用来记录用户登录失败的次数,其初始值为0。如果用户登录失败,那 么计数器值加1;如果登录成功,那么计数器值重置为0。如果计数器的值达到账户锁定阈 值,那么账户将被锁定。

另外,在账户被锁定之前,从上一次登录失败开始计时,如果超过了该计数器所设置 的时间长度,那么计数器记录的次数将自动归零。

3. 用户权限分配

用户权限分配的功能是将权限分配给特定的用户或组。常见的用户权限如下。

(1) 允许本地登录

该权限允许用户直接在计算机上登录。

(2) 拒绝本地登录

该权限拒绝用户直接在计算机上登录,且优先于"允许本地登录"权限。

(3) 将工作站加入域

该权限允许用户将计算机加入域。

(4) 关闭系统

该权限允许用户对计算机进行关机操作。

(5) 从网络访问该计算机

该权限允许用户通过网络访问该计算机。

(6) 拒绝从网络访问该计算机

该权限拒绝用户通过网络访问该计算机,且优先于"从网络访问该计算机"权限。

(7) 从远程系统强制关机

该权限允许用户通过远程计算机来对该计算机进行关机操作。

(8) 备份文件和目录

该权限允许用户进行文件和文件夹备用操作。

(9) 还原文件和目录

该权限允许用户进行文件和文件夹还原操作。

(10)管理审核和安全日志

该权限允许用户定义待审核的事件,以及查询、清除安全日志。

(11) 更改系统时间

该权限允许用户更改该计算机的系统日期和时间。

(12) 加载和卸载设备驱动程序

该权限允许用户加载或卸载设备的驱动程序。

(13) 取得文件或其他对象的所有权

该权限允许用户夺取其他用户对所拥有的文件或其他对象的所有权。

4. 安全选项

安全选项可以用来启用一些安全设置,常用的安全选项如下。

(1) 交互式登录:无须按"Ctrl+Alt+Del"组合键

交互式登录是指直接在计算机上登录,而不通过网络登录。该选项可以使登录界面不显示类似在按"Ctrl+Alt+Del"组合键登录时显示的提示消息。

(2) 交互式登录: 不显示最后的用户名

在客户端登录界面上不显示上一个登录者的用户名。

(3) 交互式登录:提示用户在过期之前更改密码

设置后可以在用户密码过期的前几天提示用户更改密码。

(4) 交互式登录:之前登录到缓存的次数(域控制器不可用时)

在域用户登录成功后,相关账户信息将被存储到计算机的缓存区中,如果后面该计算机无法与域控制器连接,则该用户在登录时还可以通过缓存区的账户数据来验证身份并登录。通过此策略可以设置缓存区内账户信息的数量,默认记录 10 个登录用户的账户信息。

(5) 交互式登录: 试图登录的用户的消息文本、试图登录的用户的消息标题

在用户登录时,如果希望在其登录界面上显示提示信息,则需要设置这两个选项来实现,这两个选项分别对应信息内容和标题文字。

(6) 关机: 允许系统在未登录的情况下关闭

用户通过关机选项可以设置是否在登录界面的右下角显示关机图标,从而在未登录的 情况下直接通过此图标对计算机进行关机操作。

1.2.5 防火墙

1. 防火墙的功能

防火墙的功能主要是及时发现并处理在计算机网络运行时可能存在的安全风险、数据 传输等问题。防火墙对这些问题的处理措施包括隔离与保护,同时对计算机网络安全中的 各项操作实施记录与检测,以确保计算机网络运行的安全性,保障用户资料与信息的完整 性,为用户提供更好、更安全的计算机网络使用体验。

2. Windows Defender 防火墙

Windows Server 2019 系统内置的 Windows Defender 防火墙可以保护计算机避免遭受外 部恶意软件的攻击。系统默认已经启用 Windows Defender 防火墙。Windows Server 2019 系 统将网络位置分为专用网络、公用网络以及域网络,并且能够自动判断与设置计算机所在 的网络位置。不同网络位置的计算机有着不同的防火墙设置,安全要求也不同。例如,位 于公用网络的计算机,其 Windows Defender 防火墙的设置较为严格,而位于专用网络的计算机的防火墙设置则较为宽松。

Windows Defender 防火墙会阻拦大部分的入站连接,但是可以通过设置允许应用通过防火墙来解除对某些程序的阻拦。

■ 任务实施

1. 环境监测系统用户账户设置

环境监测系统用户账户设置主要涉及本地用户账户创建、本地用户账户修改及密码 修改。

(1) 本地用户账户创建

创建本地用户账户需要由系统管理员或者借助相应的管理员权限账户进行操作。假设 需要在环境监测系统服务器上添加一个本地用户账户,具体要求及相关操作步骤如下。

- 用户账户名为"监测 01"。
- 初始密码设置为 "HJJC_01"。
- 密码设置为"用户下次登录时须更改密码"。

单击"开始"按钮,选择"Windows管理工具"→"计算机管理"选项,打开"计算机

管理"界面,选择"系统工具"→"本地用户和组"→"用户"→"新用户"选项,按要求 完成用户名、密码及其他设置,勾选"用户下次登录时须更改密码"复选框,单击"创建" 按钮,如图 1-2-1 所示。

🌆 计算机管理(本地)	名称	
✔ 🕌 系统工具	用户	新用户 ? ×
> 🕘 任务计划程序	首组	
> 🔄 事件查看器		田白夕(山).
> 🔯 共享文件夹		
> 🐙 本地用户和组		全名(F)·
> 🔊 性能		±40).
Ⅰ 设备管理器		描述(D):
> 答請存储		
> 🐌 Windows Server 备份		
┏ 磁盘管理		
> 🔜 服务和应用程序		密码(P):
		确认密码(C):
		☑ 用户下次登录时须更改密码(M)
		□ 用户不能更改密码(S)
		密码永不过期(W)
		□ 帐户已禁用(B)
		帮助(H) 创建(E) 关闭(O)

图 1-2-1 环境监测系统本地用户账户创建

(2) 本地用户账户修改

修改本地用户账户同样需要由系统管理员或者借助相应的管理员权限账户进行操作, 包括修改用户账户密码、删除用户账户以及更改用户账户名等操作。

假设需要对新创建的"监测 01"账户进行修改,将密码修改为"HJJC_02",相关操作步骤如下。

进入"计算机管理"界面,选择"系统工具"→"本地用户和组"→"用户"选项,右击"监测 01"账户,在弹出的快捷菜单中选择"设置密码"命令,如图 1-2-2 所示,在弹出的对话框中完成新密码的设置。

100	🖣 计算机管理(本地)	名称	全名	描述	
1	✔ 🕌 系统工具	🖉 Administrat		管理计算机(均	姒的内置帐户
	> 🕑 任务计划程序	DefaultAcc		系统管理的用	户帐户。
	> 腰 事件查看器	Guest		供来宾访问计	·算机或访问域的内
	> 📓 共享文件夹	WDAGUtilit		系统为 Wind	ows Defender 应用
	✓ 🜆 本地用户和组	第 些测01	些测(01	30003 11110	
	🖺 用户		шкло-	设置密码(S)	1
	🖺 组				
	> 🔊 性能			所有任务(K) >	
	📲 设备管理器			删除(D)	
	🗸 📇 存储			重命勾(M)	
	> 🐌 Windows Server 备份			10 m	-
	📻 磁盘管理			属性(R)	
	🔉 🔜 服务和应用程序			帮助(H)	

图 1-2-2 环境监测系统本地用户账户修改

0

(3) 用户自行修改密码

假设"监测 01" 账户的用户需要自行更改密码为"a_12345678",注意事项和相关操作步骤如下。

注意:用户自行修改密码的前提是该账户被系统管理员在本地用户和组中设置为了"用 户下次登录时须更改密码"。

在登录界面中切换到监测 01 账户,使用原密码登录,按"Ctrl+Alt+Del"组合键,选择 "更改密码"选项并设置新密码。

2. 环境监测系统组账户设置

环境监测系统组账户设置主要涉及组账户创建、组账户成员添加,需要系统管理员权限。 (1)组账户创建

假设需要创建一个名为"监测"的组账户,相关操作步骤如下。

进入"计算机管理"界面,选择"系统工具"→"本地用户和组"选项,右击"组"选项,在弹出的快捷菜单中选择"新建组"命令,在弹出的"新建组"对话框中输入组名,单击"创建"按钮,如图 1-2-3 所示。



图 1-2-3 环境监测系统创建组账户

(2) 组账户成员添加

假设需要将"监测01"账户添加到"监测"组中,相关操作步骤如下。

进入"计算机管理"界面,选择"系统工具"→"本地用户和组"→"组"选项,右击 "监测"组,在弹出的快捷菜单中选择"添加到组"命令(这里也可以进行组的删除和重命 名操作),在"监测属性"对话框中单击"添加"按钮,在弹出的"选择用户"对话框中单 击"高级"按钮,将对象类型设置为"用户",单击"立即查找"按钮,在查找结果中选择 "监测 01"账户,单击"确定"按钮,如图 1-2-4 所示。

	监测 履性		选择用户	
書 计算机管理(本地) 名称 > № 系统工具 ▲	常规		选择此对 象 类型(S):	
> ④ 任务计划程序	d n		用户	对象类型(O)
> 圖 事件查看器 题 E	a 🧶 1	监测	春秋·位素(D)。	
> 図 共享文件突 唇(い あ 大地田白印)(2)	ie -			
● ####################################	2g	选择用户	WIN-FOSPHCFA87M	位置(L)
「相」の)e 描述(E):		一般性查询	
> ③ 性能 器	Dis	选择此对象类型(S):		
書 设备管理器 通び	.vi 成员(M):	用户或内置安全主体	名称(A): 起始为 ~	歹刂(C)
Y 留存储 、 Xh Windows Con 感日	ły			立即查
ディック Windows ser 日 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	IS	查找位童(F):	油(た()): 建加力 ~	110021
> 誌 服务和应用程序 题 图	٧e	WIN-FU3PHCFA87M	禁用的帐户(B)	停止
· · · · · · · · · · · · · · · · · · ·	'ei	输入对象名称来选择(示		
8월 F (전) -	?ei			6
28 H	°0		自上次登录后的天数(I):	79
्या । जिल्ला	20			
	2D			
	ND .		_	
· · · · · · · · · · · · · · · · · · ·	le	高級(A)	搜索结果(U):	确定 取深
eerer eer	le Treco	IDEG (D)	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
響用	te Rajju(D).		Administrat WIN-FU3PHC	
889	to		DefaultAcc WIN-FU3PHC	
ans 原1	Js	确定取	Guest WIN-FU3PHC	
	金则		BUWDAGUtilit WIN-FU3PHC	
			》监测01 WIN-FU3PHC	

图 1-2-4 环境监测系统添加组账户成员

3. 环境监测系统文件及文件夹权限设置

自行在 Windows Server 2019 上创建名为"环境监测系统"的文件夹,用于文件及文件 夹权限的设置演练。

假设需要对"环境监测系统"文件夹添加"监测"组的修改、读取和执行、列出文件夹 内容权限,相关操作步骤如下。

(1) 文件夹添加访问对象

右击"环境监测系统"文件夹,在弹出的快捷菜单中选择"属性"命令,在"环境监测 系统属性"对话框中选择"安全"选项,单击"编辑"按钮,在弹出的"环境监测系统的权 限"对话框中单击"添加"按钮,在弹出的"选择用户或组"对话框中,采用类似组账户成 员添加的操作添加"监测"组,单击"确定"按钮,如图 1-2-5 所示。

环境监测系统 属性			×
常规 共享 安全 以前的版本 自定义		安全	
对象名称: C:\环境监测系统		对象名称: C:\环境监测系统	
组或用户名(G):		组或用户名(G):	
SCREATOR OWNER		SECREATOR OWNER	
SYSTEM		AL SYSTEM	
Administrators (WIN-FU3PHCFA87M\Adm	ninistrators)	& Administrators (WIN-FU3PHCFA87M\Administrators	trators)
Sers (WIN-FU3PHCFA87M\Users)		& Users (WIN-FU3PHCFA87M\Users)	
要更改权限,请单击"编辑"。	编辑(E)		
Users 的权限(P) 允许	拒绝	添加(D)	删除(R)
完全控制	选择用户或组		×
修改			
读取和执行 🗸 🗸	选择此对象类型(S)	:	
列出文件夹内容	组		对象类型(O)
读取			,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
写入	查找位置(F):		
有关特殊权限或高级设置,请单击"高级"。	WIN-FU3PHCFA8	87M	位置(L)
	輸入对象名称来选	择(示例)(E):	
	WIN-FU3PHCFA8	87M\监测	检查名称(C)
确定 取消			
WIN-FU3PHCFA87	高级(A)	确定	取消

图 1-2-5 环境监测系统文件夹添加访问对象

智慧农业——环境监测系统服务器搭建与配置 项目1

(2) 文件夹访问对象权限设置

在"环境监测系统的权限"对话框中, 勾选"修改""读取和执行""列出文件夹内 容"3个复选框,如图1-2-6所示。

4. 环境监测系统本地安全策略设置

环境监测系统本地安全策略的设置包括 密码策略、账户锁定策略、本地策略的设置。

(1) 密码策略设置

环境监测系统密码策略设置的要求和相 关操作步骤如下。

- 用户必须设置密码。
- 密码长度最小值为8个字符。
- 密码最短使用期限为3天。
- 密码最长使用期限为 30 天。

单击"开始"按钮,选择"Windows管理工具"→"本地安全策略"选项,进入"本地 安全策略"界面,选择"账户策略"→"密码策略"选项,按照上述要求对各项进行设置, 如图 1-2-7 所示。

1 本地安全策略	K FIX	- 0
文件(F) 操作(A) 查看(V) 帮助(H)		
◆ ⇒ ≥ ≡ X B I I = \		
14 安全设置	策略 ^	安全设置
	闘 密码必须符合复杂性要求	已启用
> 密码策略	圆 密码长度最小值	8 个字符
> 🔂 帐户锁定策略	圆 密码最短使用期限	3 天
	🔜 密码最长使用期限	30天
局	闘 强制密码历史	0 个记住的密码
	圆 用可还原的加密来储存密码	已禁用
> 圖 高级审核策略配置		

图 1-2-7 环境监测系统密码策略设置

(2) 账户锁定策略设置

环境监测系统账户锁定策略设置的要求和相关操作步骤如下。

- 登录失败 5 次锁定账户。
- 被锁定账户 120 分钟后自动解锁。

进入"本地安全策略"界面,选择"账户策略"→"账户锁定策略"选项,先修改"账 户锁定阈值",再修改"账户锁定时间",如图 1-2-8 所示。

环接收测系统 的权阻			v
MARKING REAL			
安全			
对象名称: C:\坏境监测系统			
组或用户名(G):			
& CREATOR OWNER			
STEM SYSTEM			
▲监测 (WIN-FU3PHCFA87M\监	測)		
Administrators (WIN-FU3PHO	CFA87M\Adminis	trators)	
💐 Users (WIN-FU3PHCFA87M\I	Users)		
	添加(D)	删除(R)	
15-111 65#7/15(0)	44)T	垢佈	
22.80 D3DXPR(P)	70#	1E#5	
修改			
读取和执行			
列出文件夹内容			
读取			
写入	\checkmark		
		h.4	
And the lot of the		Ŷ	
An YEL LITLARY		v	
		· · ·	

图 1-2-6 环境监测系统文件夹访问对象权限设置

🗟 本地安全策略		-
文件(F) 操作(A) 查看(V) 帮助(H)		
🗢 🌩 🖄 🖬 🗟 🖬		
1 安全设置		安全设置
∨ 📑 帐户策略		120 分钟
> 🔂 密码策略	圆 帐户锁定阈值	5 次无效登录
> 🗋 帐户锁定策略	😡 重置帐户锁定计数器	30 分钟之后
> 📑 本地策略		
> 📄 高级安全 Windows Defender 防火坑		
📄 网络列表管理器策略		
> 🔛 公钥策略		
> 📄 软件限制策略		
> 📄 应用程序控制策略		
> 👵 IP 安全策略,在 本地计算机		
> 📄 高级审核策略配置		

图 1-2-8 环境监测系统账户锁定策略设置

(3) 用户权限分配设置

环境监测系统用户权限分配设置的要求和相关操作步骤如下。

- •为"监测"组添加备份目录和文件权限。
- 不允许"监测"组通过远程桌面服务登录服务器。

进入"本地安全策略"界面,选择"本地策略"→"用户权限分配"选项,双击"备份 文件和目录"选项,修改其安全设置,将其添加至"监测"组中,对"拒绝通过远程桌面 服务登录"选项执行同样的操作,将其也添加至"监测"组中,示例如图 1-2-9 所示。

五本地安全策略		
文件(F) 操作(A) 音看(V) 帮助(H)		
1. 安全设置	策略 ^	安全设置
✓ □ 帐户策略	·····································	WIN-FU3PHCEA87M\监测 Backup Operators Administrators
		Administrators
> 📠 帐户锁定策略		LOCAL SERVICE NETWORK SERVICE Administrators SERVICE
✓ □ 本地策略	(이 B)포크/이지 중 [] 쉐(神) 슈(神) 슈슈	LOCAL SERVICE, NETWORK SERVICE, Administrators, SERVICE
> 📑 审核策略		A durini at a star a s
> 二 用户权限分配		Administrators
> 🔝 安全选项		A desiriet est
> 📄 高级安全 Windows Defender 防火		Administrators
📄 网络列表管理器策略	(2) 从网络访问此计算机	Everyone, Administrators, Users, Backup Operators
> 🛄 公钥策略	瓜 从远程系统强制大机	Administrators
> iii 软件限制策略	夏秋时区	LOCAL SERVICE, Administrators
> 📋 应用程序控制策略	◎ 更改系统时间	LOCAL SERVICE, Administrators
> 慐 IP 安全策略,在 本地计算机	前 关闭系统	Administrators,Backup Operators
> 📄 高级审核策略配置	圖 管理审核和安全日志	Administrators
	◎ 还原文件和目录	Administrators,Backup Operators
	🖏 获取同一会话中另一个用户的模拟令牌	Administrators
	🖏 加载和卸载设备驱动程序	Administrators
	圆 将工作站添加到域	
	📓 拒绝本地登录	
	📓 拒绝从网络访问这台计算机	
	·····································	WIN-FU3PHCFA87M\监测
	圆 拒绝以服务身份登录	
	📗 拒绝作为批处理作业登录	

图 1-2-9 环境监测系统用户权限分配设置

(4) 安全选项设置

环境监测系统安全选项设置的要求和相关操作步骤如下。

- 密码过期前3天,提醒用户更改密码。
- 添加登录提示,标题为"注意:",内容为"非环境监测系统运维人员不得登录!"。
 进入"本地安全策略"界面,选择"本地策略"→"安全选项"选项,找到交互式登录

对应的选项,按照要求进行修改,如图 1-2-10 所示。

🖥 本地安全策略		
文件(F) 操作(A) 查看(V) 帮助(H)		
(+ +) (2) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2		
1 安全设置		安全设置
> 🖺 帐户策略	📓 交互式登录: 计算机不活动限制	没有定义
◇ □ 本地策略	圆 交互式登录: 计算机帐户锁定阈值	没有定义
	📓 交互式登录: 试图登录的用户的消息标题	注意:
	📓 交互式登录: 试图登录的用户的消息文本	非环境监测系统运维人员不得登录!
	🐻 交互式登录: 锁定会话时显示用户信息	没有定义
> 同級安主 Windows Defender 防火病 同級利率範囲制的数	🐻 交互式登录: 提示用户在过期之前更改密码	3天
	圆 交互式登录: 无须按 Ctrl+Alt+Del	已禁用
	交互式登录: 需要 Windows Hello 企业版或智能卡	已禁用
	📓 交互式登录: 需要域控制器身份验证以对工作站进行解锁	已禁用
> 圓 IP 安全策略,在本地计算机	📓 交互式登录: 之前登录到缓存的次数(域控制器不可用时)	10 登录
	🖫 交互式登录: 智能卡移除行为	无操作
	圆 设备: 防止用户安装打印机驱动程序	已启用

图 1-2-10 环境监测系统安全选项设置

5. 环境监测系统防火墙设置

管理网络用户对环境监测系统服务器的访问,要求和相关操作步骤如下。

- 不允许网络用户通过公用网络访问服务器的共享文件和打印机。
- 允许网络用户通过公用网络和专用网络查看服务器性能日志和警报。

单击"开始"按钮,选择"Windows 系统"→"控制面板"选项,进入"控制面板" 界面,选择"系统和安全"→"Windows Defender 防火墙"→"允许的应用"选项。在"允 许的应用"界面中,按照上述要求设置相关选项,单击"确定"按钮,如图 1-2-11 所示。

↑ 🔐 ≪ 系统和安全 → Windows Defender 防火墙 → 允许的应用	> ひ 搜索	控制面板
允许应用通过 Windows Defender 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)
允许的应用和功能(A):		
名称	专用	公用 ^
☑ 你的帐户		
☑ 强制网络门户流	\checkmark	
□ 软件负载平衡器		
☑ 网络发现	V	
☑ 文件和打印机共享	V	
✓性能日志和警报	V	
□ 虚拟机监控		
□远程服务管理		
□远程关机		
□远程计划任务管理		
□元程券管理		
详	细信息(L)	删除(M)
	允许其	地应用(R)
	确定	取消

图 1-2-11 环境监测系统防火墙设置

弊 任务小结

在本任务中,主要介绍了用户账户、组账户、文件及文件夹权限、本地安全策略以及 防火墙的相关理论知识。通过环境监测系统的用户账户、组账户、文件夹权限、本地安全 策略及防火墙任务实践,让学生在学习理论基础的同时掌握对应的实际应用。

本任务知识结构思维导图如图 1-2-12 所示。







任务 3 环境监测系统 Web 服务器搭建

希 职业能力目标

- 能根据文档资料,完成相应操作系统的 ⅡS 软件安装。
- 能根据网站建设要求,完成 Web 服务器网站的基本设置。
- 能根据安装及维护工作要求,完成 Web 服务器日志文件的查看。

🖸 任务描述与要求

任务描述:

L公司项目部在完成环境监测系统服务器操作系统安装、运行环境配置以及安全 策略设置之后,计划在服务器上完成 Web 服务器的搭建和部署。该工作仍然由工程 师 LA 负责。

根据与项目部和客户的沟通协调,LA决定在服务器上安装 IIS,完成网站的基本设置,并通过日志查看方式确认Web服务器是否成功部署。

任务要求:

- 完成 Windows Server 2019 服务器上的 IIS 软件安装。
- 完成 Windows Server 2019 服务器 IIS 网站的基本设置。
- 完成 Windows Server 2019 服务器 IIS 日志查看。

🖉 知识储备

1.3.1 Web 服务器介绍

Web 服务器也称为 WWW(World Wide Web)服务器、HTTP 服务器,其主要功能是提供网上信息浏览服务。

Windows NT/2000/2003 平台下最常用的服务器是 Microsoft 公司的 IIS (Internet Information Server)。而 UNIX 和 Linux 平台下的常用 Web 服务器有 Apache、Nginx、Tomcat、 IBM WebSphere、BEA Weblogic 等,其中应用最广泛的是 Apache。下面对常见 Web 服务器 进行简单介绍。

1. IIS 服务器

IIS 服务器是 Microsoft 公司的 Web 服务器产品。IIS 是允许在公共 Intranet 或 Internet 上发布信息的 Web 服务器,是目前最流行的 Web 服务器产品之一,很多著名的网站都是建 立在 IIS 平台上的。它提供了一个图形界面的管理工具,称为 Internet 服务管理器,可用于 监视配置和 Internet 服务控制。IIS 只能运行在 Microsoft Windows 平台上。

IIS 是一种 Web 服务组件,其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器,分别用于网页浏览、文件传输、新闻服务和邮件发送。它使得在网络(包括互联网和局域网)上发布信息成了一件很容易的事。它提供 ISAPI (Intranet Server API) 作为扩展 Web 服务器功能的编程接口,同时提供一个 Internet 数据库连接器,可以实现对数据库的查 询和更新。

2. Apache 服务器

Apache 仍然是世界上用得最多的 Web 服务器,市场占有率达 60%左右。它源于 NCSAhttpd 服务器,在 NCSA WWW 服务器项目停止之后,NCSA WWW 服务器的用户开 始交换用于此服务器的补丁,这也是 Apache 名称的由来 (pache,补丁)。世界上很多著名 的网站使用的都是 Apache,它的优势主要在于源代码开放、可移植性、有一支强大的开发 队伍、支持跨平台的应用 (几乎可以运行在所有的 UNIX、Windows、Linux 系统平台上) 等。Apache 的模块支持非常丰富,属于重量级产品,但在速度、性能上不及其他轻量级 Web 服务器,所消耗的内存也比其他 Web 服务器高。

3. Nginx 服务器

Nginx 是一个轻量级、高性能的 HTTP 和反向代理服务器,也是一个 IMAP/POP3/SMTP 代理服务器。Nginx 是由 Igor Sysoev 为俄罗斯访问量第二的 Rambler.ru 站点开发的,第一 个公开版本 0.1.0 发布于 2004 年 10 月 4 日,其源代码以类 BSD 许可证的形式发布。Nginx 以稳定性、丰富的功能集、示例配置文件和较低的系统资源消耗而闻名。2011 年 6 月 1 日, Nginx 1.0.4 发布。目前,中国大陆使用 Nginx 的网站用户有新浪、网易、腾讯等。

4. Tomcat 服务器

Tomcat 是一个开放源代码、运行 Servlet 和 JSP Web 应用软件,并基于 Java 的 Web 应 用软件容器。Tomcat 是根据 Servlet 和 JSP 规范执行的,因此也可以说它实行了 Apache-Jakarta 规范,且比绝大多数商业应用软件服务器要好。但是它对静态文件、高并发的处理 比较弱。

1.3.2 IIS 日志介绍

1. IIS 日志概要

IIS 日志就是 IIS 运行的记录。IIS 日志查看是所有 Web 服务器管理者都必须掌握的技能。服务器的异常状况和访问 IP 来源等信息都会记录在 IIS 日志中,所以 IIS 日志对 Web 服务器的运行、维护、管理非常重要。IIS 日志的存放路径、命名格式及文件后缀名称如下。

(1) 存放路径

IIS 日志在不同操作系统的服务器上的存放路径存在区别,它在 Windows Server 2019 服务器上的默认存放路径为"%systemroot%\inetpub\logs\LogFiles\"。假设操作系统安装在 C 盘,那么默认的 IIS 日志存放路径为"C:\inetpub\logs\LogFiles\"。

(2) 命名格式

IIS 日志支持以下日志命名格式: Microsoft IIS 日志命名格式、国家超级计算应用程序 (NCSA)的中心通用日志命名格式、万维网联合会(W3C)扩展日志命名格式以及 ODBC 日志文件格式(采用自定义格式,需要 Windows 版权支持,这里不做讨论)。

对于 Windows Server 2019 服务器,当 IIS 创建日志文件时,假设日志设置为按小时查询,命名格式如下。

① Microsoft IIS 日志命名格式

u in+年份的后两位数字+月份+日期+时段。

② 国家超级计算应用程序(NCSA)的中心通用日志命名格式

u_nc+年份的后两位数字+月份+日期+时段。

③ 万维网联合会(W3C)扩展日志命名格式

u ex+年份的后两位数字+月份+日期+时段。

IIS 日志查看还支持按月、周、天方式进行,此时生成的日志文件名称会相应简化。例如,按月份查询 W3C 扩展日志,生成的日志文件格式为"u ex+年份的后两位数字+月份"。

(3) 后缀名称

IIS 日志统一的后缀名称为"log"。例如,2021年9月30日生成的W3C日志文件是 "u ex210930.log"。

2. IIS 字段描述

(1) 日志开头注释的含义

IIS 日志会记录所有访问 Web 服务器的记录。打开日志,其开头几行的作用描述如下。

#Software: Microsoft Internet Information Services 10.0//IIS版本

#Version: 1.0//版本

#Date: 2021-12-16 08:58:50//创建时间

#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-taken//日志格式

(2) 日志格式中各字段的含义

对于日志格式,上述代码有部分字段未显示,所有字段的含义如下。

- date: 表示访问日期。
- time: 表示访问时间。
- s-sitename: 表示 Web 服务器的代称。
- s-ip: 表示 Web 服务器的 IP。
- cs-method: 表示访问方法,常见的有两种,一是 GET,相当于平常访问一个 URL 的动作;二是 POST,相当于提交表单的动作。
- cs-uri-stem: 表示访问哪一个文件。

- cs-uri-query: 表示访问地址的附带参数, 如 asp 文件后面的字符串 id=12 等, 如果没 有参数则用 "-" 表示。
- s-port: 表示服务器端口。
- cs-username: 表示访问者名称。
- c-ip: 表示访问者 IP。
- cs (User-Agent): 用户代理, 即用户所用的浏览器。
- sc-status: 表示协议状态, 200 表示成功, 403 表示没有权限, 404 表示找不到该页面, 500 表示程序有错。
- sc-substatus: 表示协议子状态。
- sc-bytes: 表示发送的字节数。
- cs-bytes: 表示接收的字节数。
- time-taken: 表示所用时间。
- 3. IIS 日志返回状态代码

IIS 日志返回状态代码对应日志中的 sc-status 字段,常见返回状态代码的含义如表 1-3-1 所示。

代码	代表含义
2××	成功
200	正常;请求已完成
201	正常;紧接 POST 命令
202	正常;已接受用于处理,但处理尚未完成
203	正常; 部分信息, 返回的信息只是一部分
204	正常;无响应(已接收请求,但不存在要回送的信息)
$3 \times \times$	重定向
301	已移动(请求的数据具有新的位置且更改是永久的)
302	已找到(请求的数据临时具有不同的 URI)
303	请参阅其他(可在另一 URI 下找到对请求的响应,且应使用 GET 方法检索此响应)
304	未修改(未按预期修改文档)
305	使用代理(必须通过位置字段中提供的代理来访问请求的资源)
306	未使用(不再使用);保留此代码以便将来使用
$4 \times \times$	客户机中出现的错误
400	错误请求(请求中有语法问题,或不能满足请求)
401	未授权(未授权客户机访问数据)
402	需要付款(表示计费系统已生效)
403	禁止(即使有授权也不需要访问)
404	找不到(服务器找不到给定的资源); 文档不存在

表 1-3-1 常见 IIS 日志返回状态代码

代	码	代表含义
407		代理认证请求(客户机首先必须使用代理认证本身)
410		请求的网页不存在(永久)
415		介质类型不受支持(因为不支持请求实体的格式,服务器拒绝服务请求)
$5 \times \times$		服务器中出现的错误
500		内部错误(因为意外情况,服务器不能完成请求)
501		未执行(服务器不支持请求的工具)
502		错误网关(服务器接收到来自上游服务器的无效响应)
503		无法获得服务(因为临时过载或维护,服务器无法处理请求)

■ 任务实施

1. 环境监测系统 IIS 服务器搭建

(1) IIS 安装



在环境监测系统的 Windows Server 2019 虚拟机上进行 IIS 的安装,操作步骤如下。 ① 在服务器管理器上添加 IIS 功能 右击"此电脑",在弹出的快捷菜单中选 择"管理"命令,打开"服务器管理器"界面, 选择"仪表板"选项,单击"管理"按钮,选 择"添加角色和功能"命令,如图 1-3-1 所示。 ② IIS 安装和设置

进入"添加角色和功能向导"界面,选择"服务器角色"选项,在"角色"列表中双击 "Web 服务器(IIS)"选项,在弹出的对话框中勾选"包括管理工具(如果适用)"复选框,单 击"添加功能"按钮,如图 1-3-2 所示。该过程除"服务器角色"选项外,均采用默认设置 即可完成 IIS 的安装和设置。

▲ 添加角色和功能向导			×
选择服务器角色		目标服务 WIN-FU3PHCFA87	器 M
开始之前 安装类型 展 务器集团 服务器集色 功能 确认 结果	法課要安装在所造服务器上的 角色 Active Directory 路信 Active Directory 路信 Active Directory 路信 Active Directory 部信 Active Directory 部信 Active Directory 部信 Active Directory 部信 Active Directory 部信 Active Directory 部信 Active Directory 部信 DISS 服务器 1DIRUX (#BS) 位置指示影器 设置指示功法服务者 1DIRUX (#BS) 位置指示影器 设置指示功法服务者 1DIRUX (#BS) 1DIRUX (#BS) 1DI	▲ 添加角色和功能向导 添加 Web 服务器(IIS) 所需的功能? 需要使用以下工具本管理此功能。但不需要安装在同一服务器上。 ▲ Web 服务器(IIS) ▲ 管理工具 (工具) IIS 管理控制会 ● 管理工具(工具)(IIS 管理控制会) 	×××
		<上一步(P) 下一步(N) > 安装(I) 取消	

图 1-3-2 服务器角色设置

续表

(2) IIS 网站基本设置

① IIS 网站默认主页访问

在 IIS 安装完成之后,在"服务器管理器"界面中会出现相关界面。右击新安装的 IIS 服务器,在弹出的快捷菜单中选择对应的 IIS 管理器,如图 1-3-3 所示。

€ → 服务器管	育理器・IIS ・② 🍢 🗺M エ風の 視園VV 幕助H
 正	
■■文件和存储服务 ▷	WIN-FU3PHCFA87M 192.168.1.11 ¥41 年についれるなども知識 2021 /12/20 1 / 22/20 2021 /12/20 1 / 22/20 2021 /12/20 1 / 2011 / 2011 / 22/20 2021 / 2011 / 2011 / 22/20 2021 / 2011 / 2011 / 22/20 2021 / 201 // ***********************

图 1-3-3 进入 IIS 管理器

在随后弹出的"Internet information Services(IIS)管理器"界面(以下简称"IIS管理器" 界面)中,可以查看 IIS 网站的默认主页。选择"Default Web Site"选项,单击"浏览*:80(http)" 按钮,弹出 IIS 默认主页,如图 1-3-4 和图 1-3-5 所示。

← → WIN-FU3PHCF	487M ► PAGAE	 Default V 	Veb Site 🕨						
文件(F) 视图(V) 帮助(H)									
连接	Do Do	fault Wo	h Sito =	۲Æ				操作	
G- [2] 8		lault we	b Site _					》 浏	览
2 起始页	(辞洗:		• 〒 开始(G) - 🖵 全部显	示(A) 分组体	据: 区域	-	编辑	損权限
✓ .€ WIN-FU3PHCFA87M (WIN-			P. J. Martin	/ %	3.0.9			编	眉网站
一 @ 应用程序池	115		0				^	绑刀	Ê
		124			404	- Th		[] 基2	本设置…
> Ste	HTTP 响应标	, MIME 类型	SSL 设置	处理程序映	错误页	模块	默认文档	查测	
	头			射				查测	看處拟目录
		2				A		管理网络	站
			*		影响				新启动
	日永刈見	宵水 啼匹	니죠	到四弦框	制山坂什	八正月月		▶ 启动	动
	会田							■ 停」	Ŀ
								30	的网站





图 1-3-5 IIS 默认主页

② IIS 网站默认主页修改

对于环境监测系统搭建的 IIS 服务器,显然只访问 IIS 默认主页并不合适。这里可以对 访问的主页进行简易修改。

在 Default Web Site 的主目录(路径为"%systemroot%\inetpub\wwwroot")下使用记事本新建一个"default.htm"空白网页文件,如图 1-3-6 所示。

共享	查看			
→ 此	电脑 > 本地磁盘(C:) > inetpub > w	rwwroot		
	名称 ^	修改日期	类型	大小
	🔊 default.htm	2021/12/16 17:05	HTML 文档	1 KB
	🔊 iisstart.htm	2021/12/20 14:36	HTML 文档	1 KB
*	iisstart.png	2021/12/20 14:36	PNG 文件	98 KB

图 1-3-6 新建 "default.htm" 文件

假设想要环境监测系统的网站主页上出现"欢迎访问环境监测系统"字样,则可以使 用记事本对该网页文件进行编辑和保存,如图 1-3-7 所示。

🗐 defa	ault.htm -	记事本			
文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)	
<h2 al<="" td=""><td>ign=ce</td><td>nter>欢</td><td>迎访问题</td><td>环境监测系统 <td>2></td></td></h2>	ign=ce	nter>欢	迎访问题	环境监测系统 <td>2></td>	2>

图 1-3-7 IIS 默认主页内容修改

在修改之后确认"default.htm"文件位于"iisstart.htm"文件的前面,再次单击"浏览*:80(http)"按钮,此时的 IIS 网站默认主页如图 1-3-8 所示。

					_	ð
() (http://localhost/			- C	搜索	- م	☆ ☆
@localhost	׼					
		欢迎访问	环境监测系统			

图 1-3-8 IIS 默认主页修改结果展示

2. 环境监测系统 IIS 服务器日志设置和查看

(1) 日志文件设置

环境监测系统的日志输出要求如下。

- 日志文件格式为 W3C。
- 日志文件存放路径采用默认路径。
- 仅将日志文件写入,不包括 ETW 事件。
- 每小时自动创建一个新的日志文件。
- 日志文件的字段除默认字段外,还需添加发送字节数和接收字节数两个字段。

进入"IIS管理器"界面,双击"日志"图标,弹出"日志"对话框,按照上述前4项 要求设置日志文件的格式、目录、事件目标、滚动更新,如图 1-3-9 所示。

● 日志	
使用此功能配置 IIS 在 Web 服务器上记录请求的方式。	
格式(M): W3C ~ 选择字段(S)	
目录(Y): %SystemDrive%\inetpub\logs\LogFiles	浏览(B)
编码(E):	
UTF8 V	
日志事件目标 选择 IIS 将写入日志事件的目标。 ④ 仅日志文件(L) ○ 仅 ETW 事件(T) ○ 日志文件和 ETW 事件(A)	
日志文件滚动更新 选择 IIS 用来创建新的日志文件的方法。	
 计划(C): 每小时 ~ 	

图 1-3-9 环境监测系统日志文件设置

最后一项要求的相关操作步骤如下。在"日志"对话框中单击"选择字段"按钮,弹出 "W3C 日志记录字段"对话框,勾选"发送的字节数(sc-bytes)""接收的字节数(cs-bytes)" 复选框,单击"确定"按钮,单击"应用"按钮,如图 1-3-10 所示,会提示已经保存更改。

电子丁	W3C 日志记录字段 (本集字段(S): (少 加32 状态(sc-substatus) (少 加32 状态(sc-substatus) (少 加32 状态(sc-substatus) (少 波波的子节放(co-bytes) (分 所用射周(time-taken) () 新用
	自定义于段(C):
	補定 取消

图 1-3-10 为日志文件添加字段

(2) 日志文件查看

此时日志文件的存放路径依然为默认路径"%systemroot%\inetpub\logs\LogFiles\"。由于操作系统安装在 C 盘,所以 IIS 日志存放路径为"C:\inetpub\logs\LogFiles\"。在访问网站之后,打开路径下生成的日志文件,可以看到新增了 sc-bytes、cs-bytes 两个字段以及新生成的访问记录,如图 1-3-11 所示。

/////////////////////////////////////	-		×
文件(F) 編辑(E) 格式(O) 查看(V) 帮助(H)			
#Software: Microsoft Internet Information Services 10.0			
#Version: 1.0			
#Date: 2021-12-20 08:21:28			
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c	-ip cs(User-	
Agent) cs(Referer) sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-	taken		
2021-12-20 08:21:28 ::1 GET / - 80 - ::1 Mozilla/5.0+(Windows+NT+10.0;+WOW6	4;		
+Trident/7.0;+rv:11.0)+like+Gecko - 304 0 0 142 349 113			

图 1-3-11 环境监测系统日志查看

弊 任务小结

在本任务中,主要介绍了 Web 服务器及 IIS 日志相关理论知识。通过环境监测系统的 IIS 服务器搭建、IIS 日志设置及查看的实践,使学生对 Web 服务器能够有一定的了解,并 且熟悉 IIS 相关理论知识,掌握 IIS 搭建、基本设置、日志查看等操作技能。

本任务知识结构思维导图如图 1-3-12 所示。



图 1-3-12 知识结构思维导图