An Internship Report on

System Administration

Submitted in accordance with the requirement for the degree of

B.A (HISTORY,ECONOMICS,POLITICAL SCIENCE)

Under the Faculty Guideship of

Sri. Dr.V.Surya narayana rao

Department of History

Dr. V. S. Krishna Government Degree & PG College (A),

Visakhapatnam

Submitted by:

KOTTHURU DHILLIRAO

Reg. No: *20121006*

Department of History

Dr. V. S. Krishna Government Degree & PG College (A),

Visakhapatnam.

SEMESTER INTERNSHIP

(On-Site / Virtual)

PROGRAM BOOKFOR

SEMESTERINTERNSHIP

Name of the Student: KOTTHURU DHILLIRAO

Name of the College: Dr. V. S. Krishna Government Degree & PG College (A), Visakhapatnam

Registration Number: 20121006

Period of Internship: 3 Months **From** 01.03.2023 **To** 31.05.2023

Name & Address of the Intern Organization:

IICTE Private Limited, Plot No. 24, Opposite Y. School,Srinivasa Nagar, GITAM College Road,Visakhapatnam, Andhra Pradesh

Dr. V. S. Krishna Government Degree & PG College (A), Visakhapatnam.

Andhra University

YEAR 2022-2023

Student's Declaration

I, KOTTHURU DHILLIRAO a student of B.A (HISTORY,ECONOMICS,POLITICAL SCIENCE) Program, Reg. No. 20121006 of the Department of English ,Dr. V. S. Krishna Government Degree & PG College (A), do hereby declare that I have completed the mandatory internship from 01.03.2023to 31.05.2023 in IICTE Private Limited, Visakhapatnam, under the Faculty Guideship of Sri. Dr.V.Surya narayana rao, Department of History , Dr. V. S. Krishna Government Degree & PG College (A), Visakhapatnam.

K. Dhillirao

(Signature and Date)

31/05/2023

Official Certification

This is to certify that [illegible] Reg. No. [illegible] has completed his/her Internship in [illegible] *Visakhapatnam* on [illegible] under my supervision as a part of partial fulfilment of the requirement for the Degree of [illegible] in the Department of *history*, *Dr. V. S. Krishna Government Degree & PG College (A), Visakhapatnam.*

This is accepted for evaluation.

(Signatory with Date and Seal)

Dr. A. LAKSHMI RUPA VANI
Lecturer in History
Dr.V.S.Krishna Govt Degree & P.G. College(A)
VISAKHAPATNAM

Endorsements

Faculty Guide

Head of the Department

Dr. A. LAKSHMI RUPA VANI
Lecturer in History
Dr.V.S.Krishna Govt Degree & P.G. College(A)
VISAKHAPATNAM

Principal

Certificate from Intern Organization

This is to certify that KOTTHURU DHILLIRAO Reg. No. 20121006 of *Dr. V. S. Krishna Government Degree & PG College (A), Visakhapatnam.* underwent internship in *IICTE Private Limited, Visakhapatnam* from 01.03.2023 to 31.05.2023.

The overall performance of the intern during his/her internship is found to be Satisfactory.

INDIAN INSTITUTE OF COMPUTER AND TECHNICAL EDUCATION PVT LTD

31/5/2023

Authorized Signatory with Date and Seal

Apprenticeship Completion Certificate

This is to certify that

KOTTHURU DHILLIRAO

Dr. V. S. Krishna Govt. Degree & P.G College

has successfully completed 12 weeks

SYSTEM ADMINISTRATION

During Mar-May 2023

Supported By IICTE

Dr. V. S. Krishna Govt.
Degree & P.G College

Director
IICTE PVT LTD

Acknowledgements

It gives me an immense pleasure and pride to express my sincere gratitude and respect for my teacher and guide Sri.Dr.V.Suryanarayanarao, Department of History , Dr. V. S. Krishna Government Degree & PG College (A) Visakhapatnam for his expert and inspiring guidance.

Also, I am very grateful to the head of the Department of History,and the other faculty members of the History Department for being a source of support during this project period.

I would like to extend my gratitude to my principal Sir Dr.I Vijaya Babu for providing me all the necessary facilities that were required for successful completion of this internship.

I also thank HCTE Private Limited, Visakhapatnam for providing internship opportunity.

My special thanks to the internship trainer Sri. E. Nageswararao for their constant support, encouragement and timely advice.

K. Dhillirao

Signature of the student

Contents

DETAILED INTERNSHIP PROJECT REPORT

a. Introduction.

b. Project specifications (area / background of the work assigned).

c. Problems taken up.

d. Analysis of the problem.

e. Recommendations and conclusions.

Introduction

COMPUTER ADMINSTRATION

System administration refers to the management of one or more hardware and software systems.

The task is performed by a system administrator who monitors system health, monitors and allocates system resources like disk space, performs backups, provides user access, manages user accounts, monitors system security and performs many other functions

System administration is a job done by IT experts for an organization. The job is to ensure that computer systems and all related services are working well. The duties in system administration are wide ranging and often vary depending on the type of computer systems being maintained, although most of them share some common tasks that may be executed in different ways.

Common tasks include installation of new hardware or software, creating and managing user accounts, maintaining computer systems such as servers and databases, and planning and properly responding to system outages and various other problems. Other responsibilities may include light programing or scripting to make the system workflows easier as well as training computer users and assistants.

specifications

- Managing Windows, Linux, or Mac systems
- Upgrading, installing, and configuring application software and computer hardware
- Troubleshooting and providing technical support to employees
- Creating and managing system permissions and user accounts
- Performing regular security tests and security monitoring
- Maintaining networks and network file systems

If you're using Windows 10, version 1803 and later, you can add security questions as you'll see in step 4 under **Create a local user account**. With answers to your security questions, you can reset your Windows 10 local account password. Not sure which version you have? You can check your version.

Create a local user account

1. Select **Start** > **Settings** > **Accounts** and then select **Family & other users.** (In some versions of Windows you'll see **Other users**.)
2. Select **Add someone else to this PC**.
3. Select **I don't have this person's sign-in information**, and on the next page, select **Add a user without a Microsoft account**.
4. Enter a user name, password, or password hint—or choose security questions—and then select **Next**.

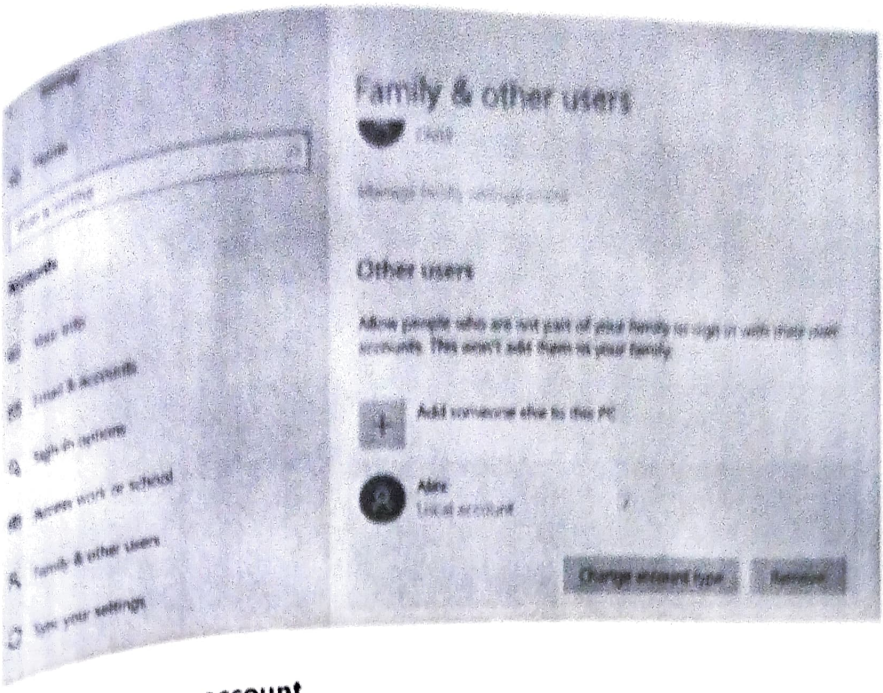
Open Settings and create another account

Change a local user account to an administrator account

1. Select **Start** > **Settings** > **Accounts** .
2. Under **Family & other users**, select the account owner name (you should see "Local Account" below the name), then select **Change account type**.

   Note: If you choose an account that shows an email address or doesn't say "Local account", then you're giving administrator permissions to a Microsoft account, not a local account.

3. Under **Account type**, select **Administrator**, and then select **OK**.
4. Sign in with the new administrator account.



Create a **local user account**

1. Select **Start** > **Settings** > **Accounts** and then select **Family & other users.** (In some versions of Windows you'll see **Other users**.)
2. Next to **Add other user**, select **Add account**.
3. Select **I don't have this person's sign-in information**, and on the next page, select **Add a user without a Microsoft account**.
4. Enter a user name, password, or password hint—or choose security questions—and then select **Next.**

Open Settings and create another account

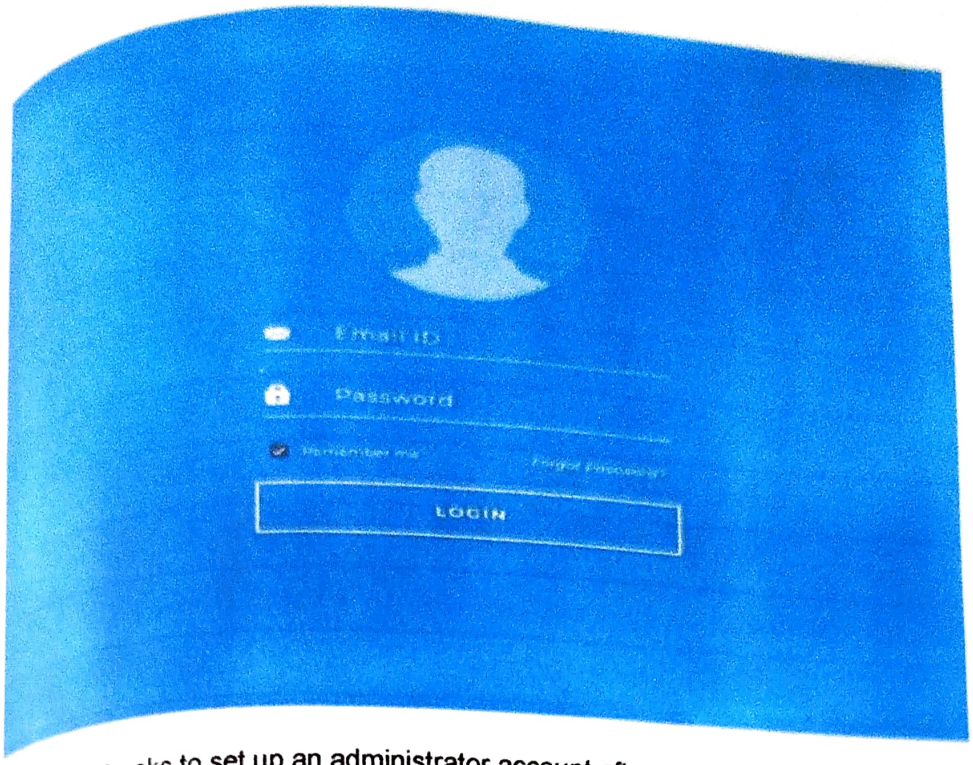
Change a local user account to an administrator account

1. Select **Start** > **Settings** > **Accounts** .
2. Under **Family & other users**, select the account owner name (you should see "Local account" below the name), then select **Change account type**.

   Note: If you choose an account that shows an email address or doesn't say "Local account", then you're giving administrator permissions to a Microsoft account, not a local account.

3. Under **Account type**, select **Administrator**, and then select **OK**.
4. Sign in with the new administrator account.

An administrator account in Windows 10 possesses all the privileges, such as changing security and configuration settings, installing and uninstalling applications, and allowing/limiting other users' access.



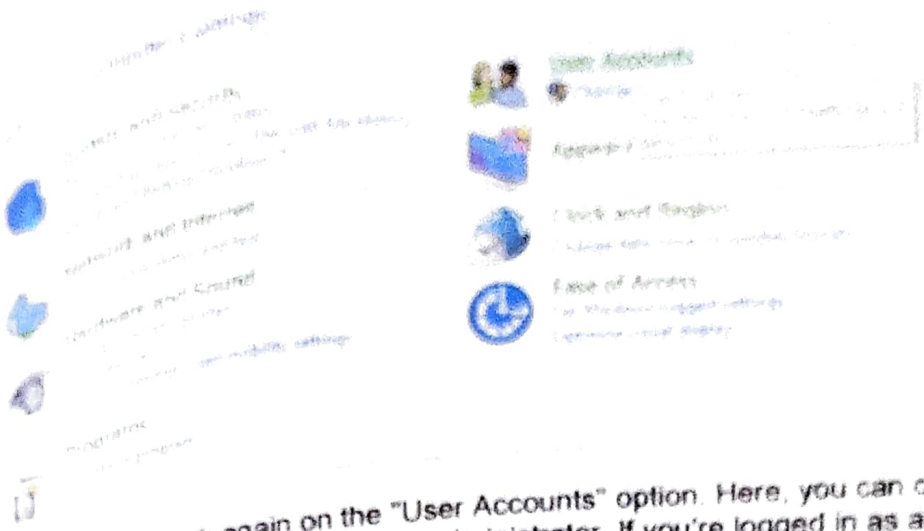
Windows 10 asks to set up an administrator account after a successful installation. After this, an administrator account can create more "administrator" or "standard" accounts. If you're using Windows 10, and want to log in as an administrator to make necessary changes, you're on the right page. This article will share how to log in as an administrator in Windows 10.

Login As an Administrator From Control Panel

The first way is to log in as an administrator from the Control Panel. Here's how to do it in five simple steps.

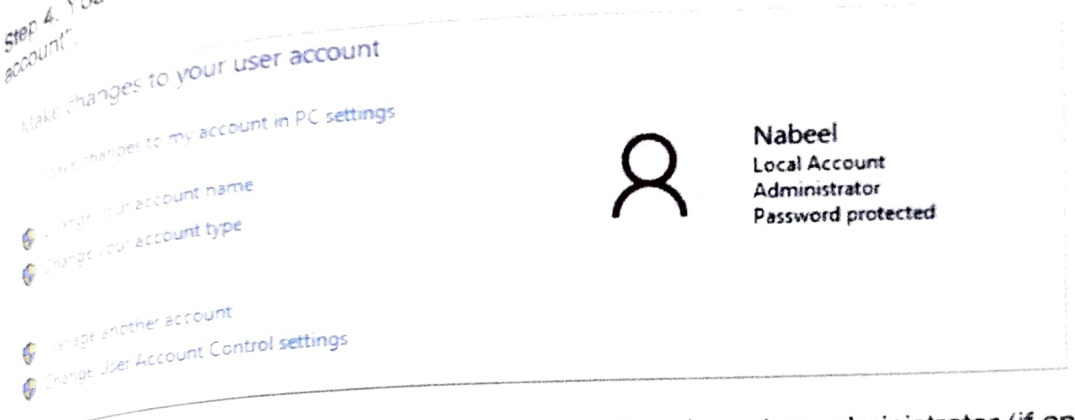
Step 1. Open Control Panel by typing "Control Panel" in the Windows 10 search bar.

Step 2. Click on the "User Accounts".



Step 3. After that, click again on the "User Accounts" option. Here, you can confirm whether you're already logged in as an administrator. If you're logged in as an administrator, it will be visible under your account name and account type.

Step 4. You can also confirm the status of other accounts by clicking "Manage another account".



Step 5. You can change the status of your account if you're not an administrator (if and only if you have the credentials of the administrator's account). To do so, apply the following operation:

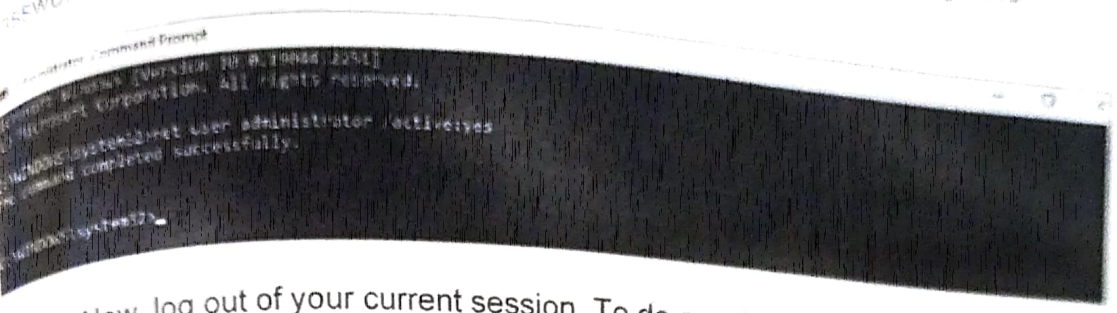
- Click on your current profile
- Select "Change the account type"
- Click the "Administrator option"
- Enter the admin password when prompted

gin As an Administrator From Command Prompt

econd option to log in as an administrator is from the command prompt. Follow the steps to complete the process.

1. Search for "cmd" in the search bar, then right-click the search result and click as Administrator". Also, allow this app to make changes to your system.

ep 2. Type net user administrator /active:yes in the cmd interface and press Enter. u'll see the message "The command completed successfully". By doing this, you ve successfully activated the default Windows 10 administrative account without ssword protection. You can also type net user administrator * to change the ssword.



Step 3. Now, log out of your current session. To do so, click on the Windows icon and then your profile picture icon. Here, click on the "Sign out" option.

Step 4. After the sign-out, click the Administrator user account.

Step 5. Type the password for the account (if you set up any) to log in as an administrator.

Conclusion

Windows 10 offers two different ways to create a user account. One is a Microsoft account, and the other is a local account. On top of this, you can either log in as an "administrator" or as a "standard user". There are two simple ways to log in as an administrator in Windows 10, which have been discussed in this article. Now, you can easily change a "standard user" to an "administrator" within a couple of steps.

About local user accounts

Local user accounts are stored locally on the device. These accounts can be assigned rights and permissions on a particular device, but on that device only. Local user accounts are security principals that are used to secure and manage access to the resources on a device, for services or users.

Default local user accounts

The *default local user accounts* are built-in accounts that are created automatically when the operating system is installed. The default local user accounts can't be removed or deleted and don't provide access to network resources.

Default local user accounts are used to manage access to the local device's resources based on the rights and permissions that are assigned to the account. The default local user accounts, and the local user accounts that you create, are located in the *Users* folder. The Users folder is located in the Local Users and Groups folder in the local *Computer Management* Microsoft Management Console (MMC). *Computer Management* is a collection of administrative tools that you can use to manage a local or remote device.

Default local user accounts are described in the following sections. Expand each section for more information.

DefaultAccount

Default local system accounts

SYSTEM

NETWORK SERVICE

LOCAL SERVICE

How to manage local user accounts

The default local user accounts, and the local user accounts you create, are located in the Users folder. The Users folder is located in Local Users and Groups. For more information about creating and managing local user accounts, see Manage Local Users.

You can use Local Users and Groups to assign rights and permissions on only the local server to limit the ability of local users and groups to perform certain actions. A right authorizes a user to perform certain actions on a server, such as backing up files and folders or shutting down a server. An access permission is a rule that is associated with an object, usually a file, folder, or printer. It regulates which users can have access to an object on the server and in what manner.

You can't use Local Users and Groups on a domain controller. However, you can use Local Users and Groups on a domain controller to target remote computers that aren't domain controllers on the network.

Security policy settings

- Article
- 02/17/2023
- 13 contributors
- Feedback

Applies to

- Windows 10
- Windows 11

This reference topic describes the common scenarios, architecture, and processes for security settings.

Security policy settings are rules that administrators configure on a computer or multiple devices for protecting resources on a device or network. The Security Settings extension of the Local Group Policy Editor snap-in allows you to define security configurations as part of a Group Policy Object (GPO). The GPOs are linked to Active Directory containers such as sites, domains, or organizational units, and they enable you to manage security settings for multiple devices from any device joined to the domain. Security settings policies are used as part of your overall security implementation to help secure domain controllers, servers, clients, and other resources in your organization.

Security settings can control:

- User authentication to a network or device.
- The resources that users are permitted to access.
- Whether to record a user's or group's actions in the event log.
- Membership in a group.

To manage security configurations for multiple devices, you can use one of the following options:

- Edit specific security settings in a GPO.
- Use the Security Templates snap-in to create a security template that contains the security policies you want to apply, and then import the security template into a Group Policy Object. A security template is a file that represents a security configuration, and it can be imported to a GPO, applied to a local device, or used to analyze security.

For more info about managing security configurations, see Administer security policy settings.

The Security Settings extension of the Local Group Policy Editor includes the following types of security policies:

- **Account Policies.** These policies are defined on devices; they affect how user accounts can interact with the computer or domain. Account policies include the following types of policies:
  - **Password Policy.** These policies determine settings for passwords, such as enforcement and lifetimes. Password policies are used for domain accounts.
  - **Account Lockout Policy.** These policies determine the conditions and length of time that an account will be locked out of the system. Account lockout policies are used for domain or local user accounts.
  - **Kerberos Policy.** These policies are used for domain user accounts; they determine Kerberos-related settings, such as ticket lifetimes and enforcement.
- **Local Policies.** These policies apply to a computer and include the following types of policy settings:
  - **Audit Policy.** Specify security settings that control the logging of security events into the Security log on the computer, and specifies what types of security events to log (success, failure, or both).

    Note

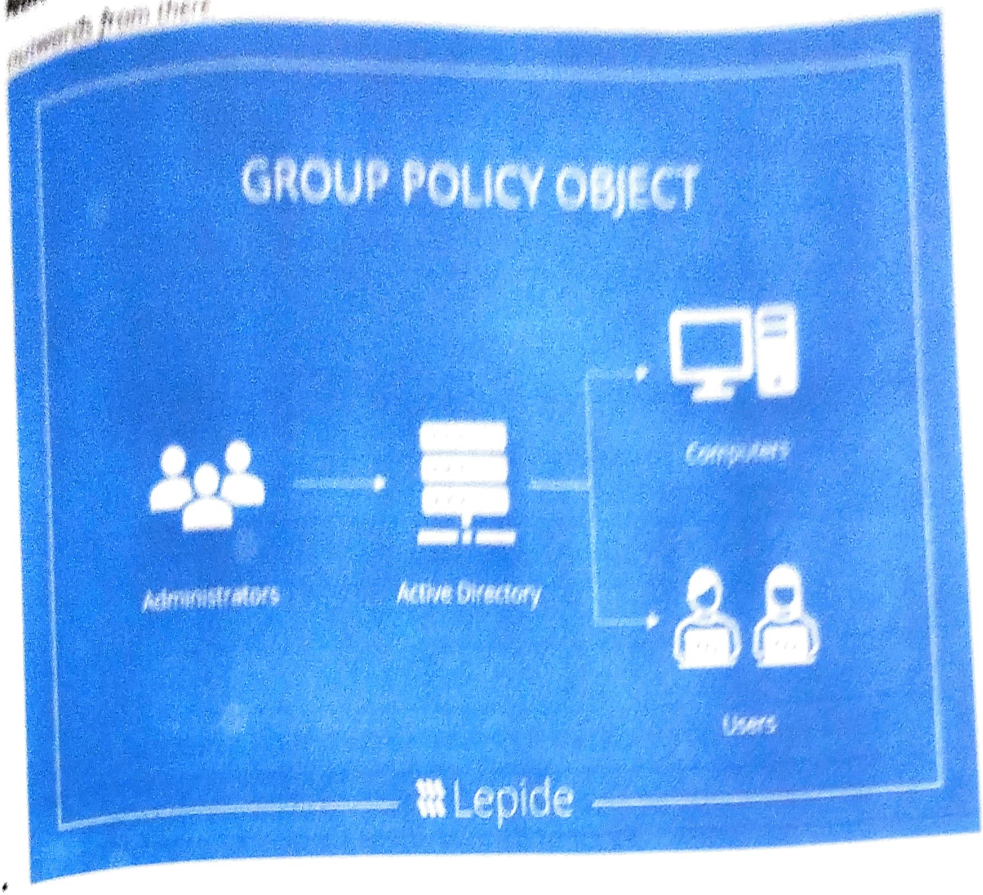
    For devices running Windows 7 and later, we recommend to use the settings under Advanced Audit Policy Configuration rather than the Audit Policy settings under Local Policies.

  - **User Rights Assignment.** Specify the users or groups that have sign-in rights or privileges on a device
  - **Security Options.** Specify security settings for the computer, such as Administrator and Guest Account names; access to floppy disk drives and CD-ROM drives; installation of drivers; sign-in prompts; and so on.

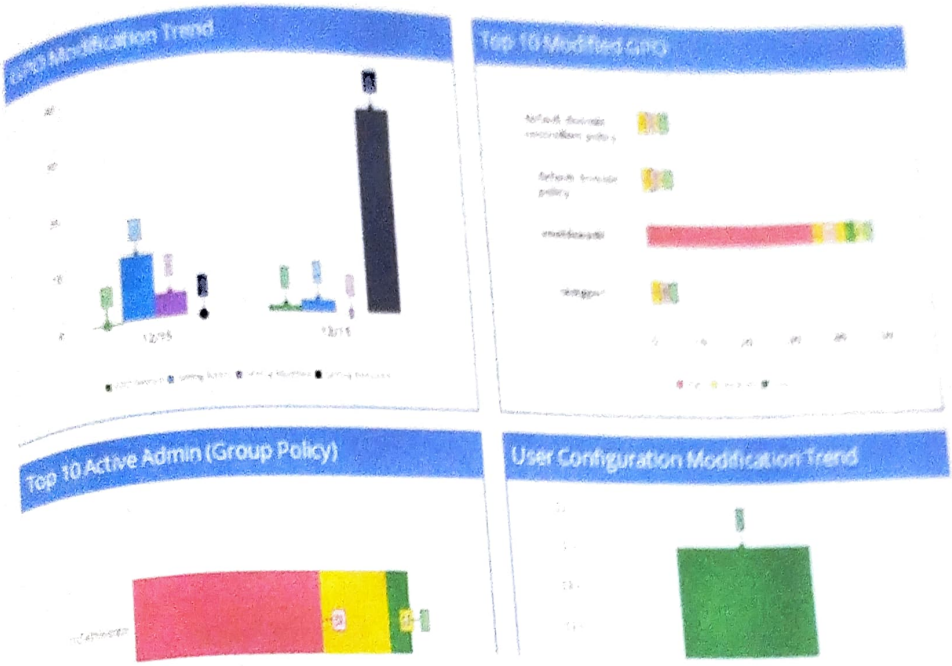
- A Group Policy Object (GPO) is a group of settings that are created using the Microsoft Management Console (MMC) Group Policy Editor. GPOs can be associated with single or numerous Active Directory containers, including sites, domains, or organizational units (OUs). The MMC allows users to create GPOs that define registry-based policies, security options, software installation, and much more.

- Active Directory applies GPOs in the same, logical order; local policies, site policies, domain policies and OU policies.

Note: GPOs that are in nested OUs work from the OU closest to the user first and outwards from there



- The Group Policy Auditing solution will help you to get more visibility over the changes being made to your Group Policy Objects. Every time a critical change is made, Lepide will send the admin a real-time alert and provide the option to roll back unwanted changes to their previous state; allowing admins to maintain a policy of least privilege and ensure the security policies of the organization remain intact.



While everything discussed in this chapter may seem like a lot of additional work that takes away from the "real" work of administering systems, actually the opposite is true; only by keeping this philosophy in mind will you give your users the service they deserve, and reach your full potential as a system administrator.

CHAPTER 4: OUTCOMES DESCRIPTION

Describe the work environment you have experienced *(in terms of people interactions, facilities available and maintenance, clarity of job roles, protocols, procedures, processes, discipline, time management, harmonious relationships, socialization, mutual support and teamwork, motivation, space and ventilation, etc.*

→ People interactions :- A supportive work environment fosters positive interactions promotes open communication

→ Facilities and Maintenance :- A well maintained and organised workspace is important for productivity

→ Clarity of Job Roles :- Clear job roles and help employees. goals.

→ Protocols, procedures, processes.

Describe the real time technical skills you have acquired (*in terms of the job- related skills and hands on experience)*

→ Programming and Software Development :- I an assist with programming languages such as python Java, C++, Java script.

→ Web Development :- HTML, CSS, Java script, as well as frame works and libraries like react angular.

→ Database Management

→ Networking and IT infrastructure.

Describe the managerial skills you have acquired (*in terms of planning, leadership, team work, behaviour, workmanship, productive use of time, weekly improvement in competencies, goal setting, decision making, performance analysis, etc.*)

→ Planning and organizing: Managers need to be skilled in creating strategic plans, setting goals, and organizing resources to achieve objectives.

→ Leadership:- Effective managers inspire and motivate their teams towards a common goals.

→ Teamwork and collaboration:- Managers should encourage teamwork and foster a collaborative work environment.

→ Behaviour and Professionalism

Describe how you could improve your communication skills (*in terms of improvement in oral communication, written communication, conversational abilities, confidence levels while communicating, anxiety management, understanding others, getting understood by others, extempore speech, ability to articulate the key points, closing the conversation, maintaining niceties and protocols, greeting, thanking and appreciating others, etc.,*)

→ Oral communication:-

Practice active listening:- pay attention to others, maintain eye contact, and show genuine interest in what they are saying.

* Speak clearly and concisely.
* Use effective body language seek feedback

→ Written communication → Conversational abilities

→ Confidence and anxiety Management.

Describe how you could enhance your abilities in group discussions, participation in teams, contribution as a team member, leading a team/activity

- Active Listening: Practice active listening by paying full attention to others during group discussions
- Empathy and respect: Cultivate empathy and respect for your team members, ideas, opinions, and contributions
- Time Management: Be mindful of time constraints during group discussion
- Problem-Solving Skills.

Describe the technological developments you have observed and relevant to the subject area of training *(focus on digital technologies relevant to your job role*

- Natural Language Processing: NLP has significantly advanced, enabling machines to understand
- Deep learning: Deep learning, a subset of machine, has experienced remarkable advancements.
- Generative Adversarial Networks (GANs) are a class of machine learning modules that are capable of generating synthetic data that closely resemble real data.
- Cloud computing
- Reinforcement learning.

Photographs