Маркеєв Б.В., магістрант
Фальковський І.Г., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ МЕТОДІВ АВТОМАТИЗАЦІЇ РОЗГОРТАННЯ КОНТРОЛЕРІВ ДОМЕНУ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ACTIVE DIRECTORY

В умовах зростання складності та обсягу корпоративних мереж автоматизація процесів розгортання та налаштування інфраструктури Active Directory (AD) стає не лише бажаною, але й необхідною умовою для забезпечення масштабованості, оперативності й кібербезпеки. Метою цього дослідження є аналіз сучасних методів автоматизації для покращення ефективності IT-інфраструктури, зокрема шляхом використання PowerShell і Ansible.

Автоматизований підхід до налаштування контролерів домену охоплює інтегровану конфігурацію ключових компонентів мережі, зокрема служби DHCP для керування динамічним розподілом IP-адрес, впровадження статичної адресації серверів, а також централізоване створення й управління обліковими записами користувачів.[1] Важливу роль відіграє автоматизація організаційної структури через створення OU (Organizational Units) та застосування політик контролю доступу і групових політик (Group Policy). Ці заходи сприяють посиленню безпеки та уніфікації середовища, що є основою для сталого розвитку інформаційних систем. [2]

Реалізація автоматизації можлива завдяки потужним інструментам, зокрема PowerShell, який забезпечує розробку сценаріїв для виконання широкого спектра адміністративних завдань. За допомогою вбудованих модулів, PowerShell дозволяє автоматично налаштовувати AD, створювати користувачів, керувати OU та впроваджувати політики без необхідності втручання адміністратора.[2,3]

Іншим значущим інструментом у цій галузі є Ansible, що виступає як універсальний засіб оркестрації. Його можливості з централізованого управління конфігураціями та автоматизації за допомогою плейбуків дозволяють зменшити складність налаштувань у масштабних середовищах. Важливою перевагою Ansible є інтеграція з PowerShell, що розширює його функціональність у роботі з серверами на базі Windows.[5]

Окремо слід наголосити на необхідності резервного копіювання контролерів домену та тестування сценаріїв їх відновлення. Ці заходи є невід'ємною частиною стратегії забезпечення стійкості інфраструктури до збоїв, дозволяючи зберігати безперервність функціонування бізнес-процесів та мінімізувати наслідки потенційних атак чи апаратних відмов.

Отже, впровадження автоматизації у процеси розгортання та адміністрування контролерів домену на базі AD значно підвищує ефективність, надійність та кіберстійкість корпоративних мереж. Використання PowerShell у поєднанні з Ansible формує потужний інструментарій для побудови безпечного і керованого IT-середовища, що відповідає актуальним потребам цифрової трансформації та найкращим практикам у галузі інформаційних технологій.

Список використаних джерел

1. Active Directory Domain Services Overview [Електронний ресурс] / Microsoft Learn. – https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview – 17.08.2022..
2. What Is Active Directory and How Does It Work? [Електроний ресурс] / Lepide – https://www.lepide.com/blog/what-is-active-directory-and-how-does-it-work/– 24.04.2024.
3. Setting up Active Directory via PowerShell: [Електронний ресурс] / Microsoft – https://www.microsoft.com/en-gb/industry/blog/technetuk/2016/06/08/setting-up-active-directory-via-powershell/.
4. Powershell and domain controller: [Електронний ресурс] / Microsoft DevBlogs – https://devblogs.microsoft.com/scripting/use-powershell-to-deploy-a-new-active-directory-forest/ – Загол. з екрану.
5. Ansible: [Електронний ресурс] / Ansible – https://www.ansible.com/how-ansible-works/.