Overview of active directory best practice:

Password policies, M365 integration & domain controller placement

V1.0

LOCAL DIGITAL Cyber

Objective

- Outline guidance and approach of considerations to be given to key elements of active directory.
- In particular, this pack covers the areas of password policies, M365 integration and domain controller placement.

Concepts for account security

Areas of security:

Key areas for consideration around password policies

- Password Requirements
- Fine Grained Policies
- Password Auditing

Microsoft 365 Integration

- Azure AD Connect Software

Active Directory Domain Controller Placement

- Local Redundancy
- Geographical Redundancy

Why are these practices important?

Password Policies:

- The more secure the password and the more educated your users, the lower the risk of an account breach.

M365 Integration:

- By having a second Azure AD Connector ready in staging mode will facilitate a speedy recovery from a failure of the primary Connector, and ensure the configuration is identical. Microsoft only allow for a single one per domain so staging mode is the best that is currently possible.

Domain Controller Placement:

- By having Domain Controllers in multiple locations logon speeds and availability will improve as well as providing a DR site Directory for aiding in recovery.

Considerations for password policies

“But we already have password complexity set, is that not enough ?”
The simple answer is - probably not

Password Requirements

- Using the standard domain policy for all accounts can mean privileged accounts may not be as secure as they could be.
- Domains that have ‘evolved’ may still have a weak level of requirements as the policies are not automatically upgraded with stronger settings.

Fine Grained Policies

- These are a great way to enforce a tiered level of security, and not over complicate non-privileged accounts

Considerations for password policies (cont.)

Password Auditing

- Auditing passwords on a regular basis will help identify users who need education on the importance of account security. It will also identify any passwords that have not been changed in a long time.

Password policies

Password Requirements

- Maintain at least an 8-character minimum length requirement
- Don't require character composition requirements. For example, *&(^%$ - but do require ‘special characters’ are used as part of the password
- Don't require mandatory periodic password resets for user accounts
- Don't use a single word, eg ‘password’ or a commonly-used phrase like ‘Iloveyou’

Password policies (cont.)

Password requirements

- Ban common passwords, to keep the most vulnerable passwords out of your system
- Make passwords hard to guess, even by those who know a lot about you, such as the names and birthdays of your friends and family, your favorite bands, and phrases you like to use
- Educate your users to not re-use their organization passwords for non-work related purposes

Review the latest guidance from the NCSC at:
https://www.ncsc.gov.uk/collection/passwords/updating-your-approach#tip5-password-collection

Password policies (cont.)

Fine grained policies*

- You can use fine-grained password policies to specify multiple password policies within a single domain and apply different restrictions for password and account lockout policies to different sets of users in a domain.
- For example, you can apply stricter settings to privileged accounts and less strict settings to the accounts of other users. In other cases, you might want to apply a special password policy for accounts whose passwords are synchronized with other data sources.

*You must use the Windows Server 2012 or newer version of Active Directory Administrative Center to administer fine-grained password policies through a graphical user interface.

Password policies (cont.)

Password auditing

- Password security audits help you test the strength of your users' passwords and your resiliency against password attacks. Not only can they help you uncover weak passwords, but they also provide an opportunity to educate your employees on proper password utilization.

Microsoft 365 integration

- Having a second Azure AD Connector ready in staging mode will facilitate a speedy recovery from a failure of the primary connector, and ensure the configuration is identical. Microsoft only allow for a single one per domain so staging mode is the best that is currently possible.

- If the connector (or the server it runs on) fails, then the selected options at the point of installation of the software would not be carried out until the server was rebuilt. Primarily these would be password synchronisation related, and new account synchronisation.

Microsoft 365 integration (cont.)

Additional recommendations

- Keep a documented set of the configuration settings elsewhere on your network
- Update your Azure AD Connect software on a regular basis to take advantage of enhancements in security and features
- Remember to update the standby staging server!

Domain controller placement

- Microsoft advise that it is best practice to ensure the physical security of domain controllers in hub and satellite locations so that unauthorized personnel cannot access them, so consider this when selecting locations for off site domain controller placement.

Further considerations

Multi Factor Authentication

- This gives you additional security on accounts in case username/password combinations are breached by requiring a 3rd (or more) level of authentication (examples : authentication apps, tokens, biometrics)

Password Storage Products

- There are plenty of password storage products on the market which keep your passwords securely, and you limit access to it with its own level of security. The passwords are not displayed, but you can copy them to use. Refer to the NCSC guidelines on using these systems: https://www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide

Ministry of Housing,
Communities &
Local Government

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL
DIGITAL
Cyber