Department for Levelling Up,
Housing & Communities

Active Directory: Password policies, M365 integration & DC 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.

LOCAL DIGITAL Cyber

Concepts for account security

Key areas for consideration for 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

LOCAL DIGITAL Cyber

Why are these practices important?

Password Policies:

- Secure password and more educated users lower the risk of an account breach.

M365 Integration:

- 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. Only a single Connector per domain is allowed by Microsoft so staging mode is the best that is currently possible.

Domain Controller Placement:

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

LOCAL DIGITAL Cyber

Considerations for password policies

Having password complexity set is probably not enough!

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

- Are a way to enforce a tiered level of security, and not over complicate non-privileged accounts.

LOCAL DIGITAL Cyber

Considerations for password policies (cont…)

Password Auditing

- Completed on a regular basis will help identify users who need education on the importance of account security.

LOCAL DIGITAL Cyber

Password policies

Password Requirements

- Maintain at least an 8-character minimum length requirement, ideally 12 characters with no maximum length.
- Follow the NCSC Guidance for ‘3 random words’.
- 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’.

LOCAL DIGITAL Cyber

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 favourite bands, and phrases you like to use.
- Educate your users to not re-use their organisation 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

LOCAL DIGITAL Cyber

Password policies (cont…)

Fine grained policies*

- 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 synchronised with other data sources.

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

LOCAL DIGITAL Cyber

Password policies (cont…)

Password auditing

- Password security audits help you test the strength of your users' passwords and your resiliency against password attacks.
- Provide an opportunity to educate your employees on proper password utilisation.

LOCAL DIGITAL Cyber

Microsoft 365 integration

- 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. Only a single Connector per domain is allowed by Microsoft 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.

LOCAL DIGITAL Cyber

Microsoft 365 integration (cont…)

Additional recommendations

- Keep a documented set of the configuration settings in a secure location.
- 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.

LOCAL DIGITAL Cyber

Domain controller placement

- It is best practice to ensure the physical security of domain controllers in hub and satellite locations so that unauthorised personnel cannot access them, so consider this when selecting locations for offsite domain controller placement.

LOCAL DIGITAL Cyber

Further considerations

Multi Factor Authentication

- Provides 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

- Password storage products 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

LOCAL DIGITAL Cyber

Staying in touch - cyber support sessions

Cyber treatment plan & implementation support session available to book using this link: https://calendly.com/andrea-baron/ad-hoc-call-with-council .
These are longer 1:1 sessions between DLUHC cyber team and a council, available for any support, guidance or hands on help for the implementation of your cyber treatment plan.

Cyber support drop in sessions every Wednesday for 30 minute session between 2pm - 4pm. These regular 1:1 sessions are available for you to book anytime using the Calendly link: https://calendly.com/andrea-baron/drop-in-support-session.

Cyber clinics are occurring on the 3rd Thursday of the month between 11.30am - 12.30pm where a targeted cyber focus area will be presented, tool sets demonstrated and will be open to questions. Support, guidance and hands-on help is available to assist you in adoption and implementation.

LOCAL DIGITAL Cyber

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on Medium
- Follow LDCU on Twitter (@LDgovUK)
- Subscribe to our Cyber newsletter for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the DLUHC Digital blog

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please email cybersupport@localdigital.gov.uk.

LOCAL DIGITAL Cyber

Department for Levelling Up,
Housing & Communities

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber