Instelligence

Essential 8 with Proxmox

Hardening Your Infrastructure for Essential 8 Compliance

Author: Stellios Williams
Email: stell (at) instelligence.io

February 2025

Contents

Disclaimer

The information provided in this document is based on best efforts at the time of writing. Cybersecurity practices and compliance requirements evolve, and while every attempt has been made to ensure accuracy, organisations should perform their own due diligence and consult relevant official sources for the most up-to-date information.

Security Liability Disclaimer

While every effort has been made to ensure the security recommendations in this document align with industry best practices, security risks evolve over time. Instelligence assumes no liability for any security incidents, misconfigurations, or vulnerabilities that may arise from implementing the guidance provided. Organisations are encouraged to conduct independent security assessments before applying any changes.

Regulatory Compliance Disclaimer

This document provides guidance for aligning Proxmox Virtual Environment with the Essential 8 framework as outlined by the Australian Cyber Security Centre (ACSC). However, compliance with Essential 8 does not imply compliance with other security frameworks such as ISO 27001, NIST, or GDPR. Organisations should consult legal and compliance experts to ensure full regulatory adherence.

Executive Summary

Cybersecurity threats are evolving rapidly, and organisations must take a proactive approach to hardening their IT infrastructure. The Essential 8, developed by the Australian Cyber Security Centre (ACSC), provides a structured framework for mitigating security risks and ensuring operational resilience. For organisations leveraging Proxmox Virtual Environment (PVE) as their virtualisation platform, or planning to migrate, aligning with the Essential 8 offers a cost-effective, open-source alternative while maintaining robust security.

This whitepaper explores how Proxmox can be configured to meet Essential 8 compliance, identifying its strengths, limitations, and necessary enhancements to ensure organisations achieve the highest security standards.

Key Takeaways

- ✓ Proxmox is a secure, flexible, and cost-efficient alternative to proprietary hypervisors but requires additional configurations to fully comply with Essential 8. Much like every other hypervisor.
- ✓ Multi-Factor Authentication (MFA) (MFA) is not built-in, requiring integration with OIDC, LDAP, or other identity providers. Much like every other hypervisor.
- ✓ Application Control is not native to Proxmox, but can be implemented using Debian's built-in security frameworks (SELinux, AppArmor, Systemd restrictions).
- ✓ Patch management requires careful planning - the Proxmox Enterprise Repository provides faster security updates but requires a subscription, whereas the No-Subscription Repository introduces a delay in critical patches.
- ✓ Backup and disaster recovery are crucial - Proxmox Backup Server (PBS) ensures fast recovery but must be complemented with offsite storage and regular disaster recovery testing.

As cyber threats intensify, ensuring Essential 8 compliance is no longer optional - it is a strategic necessity. Proxmox provides a scalable, enterprise-grade virtualisation platform that, when properly secured, enables organisations to reduce attack surfaces, ensure data resilience, and maintain compliance with Australian cyber security standards.

Instelligence offers expert platform audits, Proxmox hardening, and managed services to help organisations achieve Essential 8 compliance seamlessly. Contact us today to assess your private cloud posture and fortify your infrastructure with Proxmox.

Introduction

The growing sophistication of cyber threats demands that organisations move beyond reactive security measures and adopt structured, proactive strategies. The Essential 8, developed by the Australian Cyber Security Centre (ACSC), is designed to help organisations reduce their exposure to common cyber risks through a set of practical mitigation strategies.

As organisations explore modern virtualisation platforms such as Proxmox Virtual Environment (PVE), ensuring alignment with security best practices becomes essential. While Proxmox provides a feature-rich and cost-effective alternative to proprietary solutions, achieving compliance with Essential 8 requires deliberate planning and configuration.

This whitepaper examines how Proxmox can be optimised to meet Essential 8 security requirements, detailing its strengths, potential gaps, and the steps organisations can take to harden their infrastructure. By implementing these security measures, businesses can better safeguard their virtualised environments against evolving cyber threats while maintaining compliance with Australian security standards.

The Essential 8 Framework: An Overview

Cyber threats are one of the biggest challenges organisations face today. To mitigate these risks, the Australian Cyber Security Centre (ACSC) developed the Essential 8 - a set of proactive mitigation strategies aimed at reducing the likelihood and impact of cyber incidents. The Essential 8 focuses on preventing common attack vectors, limiting the extent of potential compromises, and ensuring rapid recovery in the event of a security breach.

The 8 Key Controls

These controls help organisations establish a structured and effective defence system against malicious activity. When properly implemented, the Essential 8 enhances an organisation's resilience against cyber threats by ensuring robust security measures are in place. The 8 Key Controls are:

1. **Application Control** – Prevents unauthorised applications from executing on systems.
2. **Patch Applications** – Ensures timely updates to eliminate security vulnerabilities.
3. **Configure Microsoft Office Macro Settings** – Restricts macro execution to prevent malware attacks.
4. **User Application Hardening** – Disables unnecessary features in applications to reduce exposure.
5. **Restrict Administrative Privileges** – Limits privileged access to only those who require it.
6. **Patch Operating Systems** – Ensures the underlying OS remains secure through regular updates.

7. **Multi-Factor Authentication (MFA)** – Adds an extra layer of security to user authentication.
8. **Regular Backups** – Ensures data resilience by creating and storing encrypted backups.

Each of the eight controls focuses on a critical area of IT security, such as application control, patching, access management, and data backup. Organisations can implement these controls at different maturity levels, ensuring a tailored approach to risk mitigation.

Maturity Levels of the Essential 8

The ACSC defines three maturity levels to measure how well organisations implement these controls:

- **Maturity Level 1**: Defends against opportunistic attacks using readily available exploits.
- **Maturity Level 2**: Protects against more sophisticated attackers who actively exploit vulnerabilities.
- **Maturity Level 3**: Ensures resilience against well-funded and persistent adversaries using advanced tactics.

The Essential 8 is designed to be adaptable, allowing organisations to incrementally improve their security posture based on their risk profile and operational requirements.

Applying the Essential 8 to Proxmox

Table 1 provides a breakdown of how each Essential 8 control can be implemented within Proxmox Virtual Environment (PVE). Each row outlines a specific control, the recommended implementation strategy for Proxmox, and the maturity level that can be achieved through proper application. This structured approach helps organisations assess their security posture and take necessary steps toward compliance.

	Essential 8 Control	Proxmox Implementation	Maturity Level Achieved
1	**Application Control**	Leverage Debian's built-in security frameworks (AppArmor, SELinux, and Systemd) to restrict application execution. Manual configuration is required.	Level 3 (with additional configuration)
2	**Patch Applications**	Establish a structured update management process to maintain security patches and prevent vulnerabilities.	Level 3
3	**Configure Microsoft Office Macro Settings**	Limit the execution of macros on connected workstations to reduce exposure to malicious scripts.	Level 2
4	**User Application Hardening**	Restrict unnecessary features and enforce secure access policies to minimise risk from user applications.	Level 2
5	**Restrict Administrative Privileges**	Apply role-based access controls to ensure users have only the minimum necessary permissions.	Level 3

	Essential 8 Control	Proxmox Implementation	Maturity Level Achieved
6	**Patch Operating Systems**	Maintain regular OS updates and monitor for security advisories to keep systems protected.	Level 3
7	**Multi-Factor Authentication**	Enforce strong authentication methods to safeguard against unauthorised access.	Level 2
8	**Regular Backups**	Implement a comprehensive backup strategy to ensure data integrity and rapid recovery.	Level 3

Table 1

The following section provides a comprehensive guide to hardening Proxmox, detailing the essential security measures required to align with the Essential 8 framework.

Hardening Proxmox for Essential 8 Compliance

1. Securing Your Proxmox Environment: A Layered Approach

Securing a Proxmox deployment requires a layered security approach that encompasses network segmentation, access controls, and proactive threat mitigation. By implementing strong security policies, organisations can significantly reduce attack surfaces and mitigate risks associated with unauthorised access or cyber threats.

At the foundation of a secure Proxmox deployment is network segmentation. Organisations should use an external firewall solution such as OPNsense to provide isolation and protection from non-Proxmox networks. Additionally, utilise Proxmox's built-in firewall to define rules that restrict traffic between virtual machines and external networks.

To prevent unauthorised system access, organisations must disable root SSH login and enforce key-based authentication. This ensures that privileged access is restricted to verified users only. Furthermore, SSH access should be limited to a management network or a dedicated VPN to prevent exposure to public networks, which significantly reduces the risk of brute-force attacks.

Proxmox, as a Debian-based system, provides security frameworks such as AppArmor, SELinux, and Systemd service restrictions. These must be manually configured to enforce application execution policies and limit unauthorised software.

The Proxmox web interface should also be hardened by changing default ports, enforcing strong authentication policies, and enabling TLS encryption. Intrusion detection and advanced filtering solutions should be used to detect and prevent attacks, in addition tools such as fail2ban should be deployed to monitor authentication attempts and block repeated failed login attempts, further reducing attack risks.

Summary

- **Disable** root SSH login and enforce key-based authentication. This ensures only authorised users can access administrative functions.
- **Restrict** SSH access to a secure management network or VPN. Exposing SSH to public networks increases the risk of brute-force attacks.
- **Change** the default Proxmox web UI ports to reduce exposure and mitigate common automated attack vectors.

- **Deploy** fail2ban to monitor login attempts and block repeated failed authentication attempts, reducing brute-force attack risks.
- **Enable** TLS encryption for all web-based and remote management connections. This ensures data remains secure while in transit.

2. Proactive Patch Management and System Updates

Keeping systems up to date is one of the most effective ways to protect against vulnerabilities and emerging threats. Patch management should be a continuous and structured process to minimise risks and maintain operational stability.

Proxmox offers two repository options for system updates: the Enterprise Repository (Paid) and the No-Subscription Repository (Free). The Enterprise Repository provides timely, thoroughly tested security updates, ensuring that critical patches are available immediately and reducing exposure to vulnerabilities. However, this requires a paid subscription. On the other hand, the No-Subscription Repository is free but delivers updates later, meaning systems using it may be exposed to known security vulnerabilities for a longer period. While the No-Subscription option offers cost savings, organisations with security-critical environments should carefully evaluate the trade-off between cost and risk when selecting a repository.

Using unattended-upgrades, IT teams can automate security patch deployment while reducing administrative overhead. However, major system updates should be scheduled within a controlled maintenance window to ensure minimal service disruption.

For environments requiring high availability, live patching solutions should be explored. These allow for security updates to be applied without requiring reboots, minimising downtime while keeping systems secure. Applying timely security updates is essential for maintaining a secure infrastructure.

Summary

- The Proxmox Enterprise Repository provides immediate access to security patches and thoroughly tested updates, reducing exposure to vulnerabilities, but comes at a financial **cost**.
- **Use** unattended-upgrades to ensure critical security patches are automatically applied.
- **Schedule** regular maintenance windows to apply kernel and software updates with minimal operational impact.
- **Implement** live patching solutions where possible to apply updates without system downtime.

3. Strengthening Identity and Access Controls

Enforcing strict identity and access management policies is critical to securing a Proxmox deployment. Role-Based Access Control (RBAC) should be configured to grant the least privilege necessary for each user, ensuring that administrative functions are only available to authorised personnel.

For authentication, organisations should integrate LDAP, Active Directory, or preferably OpenID Connect (OIDC) to centralise user authentication and maintain uniform identity management policies. To further enhance security, Multi-Factor Authentication (MFA) should be enforced (via authentication integration) for all privileged accounts, significantly reducing the risk of compromised credentials being used for unauthorised access.

Additionally, regular security audits should be conducted to review user access logs and identify anomalies or potential breaches. Implementing automated log analysis and alerts can provide early warnings for suspicious activity. Effective access control prevents unauthorised changes and restricts administrative access.

Summary

- **Integrate** OpenID Connect (OIDC) for centralised identity and access management.
- **Implement** Role-Based Access Control (RBAC) to assign the least privilege necessary to each user.
- **Require** Multi-Factor Authentication (MFA) for all administrator accounts. This adds a critical security layer, preventing credential-based attacks.
- **Audit** user activity logs regularly to detect anomalies or unauthorised access attempts.

4. Hardening Virtual Machines and Workloads

Securing virtual machines (VMs) is a crucial aspect of maintaining an overall secure Proxmox environment. The first step in workload security is removing unnecessary virtual hardware which improves virtualisation performance and reduces attack footprint.

All guest operating systems should be hardened by disabling unnecessary services, enforcing secure boot policies, and restricting inter-VM communication using Proxmox firewall rules. This minimises the risk of lateral movement in the event of a security breach.

Routine vulnerability scanning should be incorporated into security workflows using tools such as Lynis, OpenVAS, Rapid7, or another service. These tools help detect potential security weaknesses within virtualised workloads and provide actionable remediation steps. A properly hardened virtualisation environment reduces the attack surface of hosted workloads.

Summary

- Harden guest OS configurations by disabling unnecessary services, enforcing secure boot settings, and removing unnecessary virtual hardware.
- Restrict inter-VM communication using Proxmox firewall rules to prevent lateral movement in case of a compromise.
- Regularly scan virtual machines for vulnerabilities using tools like Lynis or OpenVAS.

5. Establishing a Robust Backup and Disaster Recovery Strategy

A comprehensive backup and disaster recovery plan is essential for ensuring business continuity in the event of a security breach, hardware failure, or catastrophic data loss. Organisations should deploy Proxmox Backup Server (PBS) to automate backup creation and maintain fast recovery capabilities.

Backups should be encrypted using AES-256 to protect sensitive data from unauthorised access. To enhance resilience, backups must be stored in geographically separate locations, mitigating risks associated with localised failures such as natural disasters or ransomware attacks.

A defined backup retention policy should be implemented to ensure historical snapshots are available for rollback or forensic analysis. Additionally, quarterly disaster recovery drills should be conducted to validate the effectiveness of backup strategies and restore procedures, ensuring minimal downtime in the event of an actual incident. A resilient backup strategy ensures that critical data is protected and can be restored in case of a cyber incident or failure.

Summary

- **Deploy** Proxmox Backup Server (PBS) to automate backups and enable fast recovery.
- **Ensure** all backups are encrypted using AES-256 to prevent data compromise in case of breach.
- **Store** backups in geographically separate locations to mitigate the risk of data loss due to localised failures.
- **Implement** a backup retention policy that ensures historical snapshots are available for forensic and rollback purposes.
- **Conduct** quarterly disaster recovery drills to validate the effectiveness of your backup and restore strategy.

Conclusion

By implementing the Essential 8 framework in your Proxmox Virtual Environment, you can build a resilient, secure, and compliant infrastructure that meets Australian cyber security standards. The combination of hardened security measures, access control policies, proactive patching, and robust backup strategies ensures that your organisation is protected against emerging cyber threats while maintaining operational efficiency.

How Instelligence Can Help

At Instelligence, we specialise in Proxmox security, implementation, and management to ensure your organisation is Essential 8 compliant. Our team of experts provides:

- ✓ **Proxmox Hardening & Private Cloud Audits** – We assess your Proxmox deployment, apply best practices, and eliminate vulnerabilities. Alternatively, we can assess your existing VMware environment and provide a pathway to Proxmox.
- ✓ **Patch Management & Continuous Monitoring** – We implement automated security updates and real-time monitoring to keep your infrastructure secure.
- ✓ **Access Control & Identity Management** – We help configure RBAC, MFA, and integration with LDAP/Active Directory to enforce strict access policies.
- ✓ **Backup & Disaster Recovery Planning** – Our team ensures that your Proxmox Backup Server (PBS) is properly configured, with encryption, redundancy, and tested restore processes.
- ✓ **Managed Proxmox Services** – Instelligence offers fully managed Proxmox environments on your hardware, ensuring you retain full control and data sovereignty. Our services allow you to focus on running your business while we handle security, compliance, and performance optimisation.

By partnering with Instelligence, you gain a secure, scalable, and fully managed Proxmox Private Cloud, giving you peace of mind and allowing you to meet federal compliance standards effortlessly.

References

1. Australian Cyber Security Centre (ACSC) – Essential 8 Framework
   https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
2. Proxmox Security Guide
   https://pve.proxmox.com/wiki/Security
3. Proxmox Package Repositories
   https://pve.proxmox.com/wiki/Package_Repositories
4. OPNsense Documentation
   https://docs.opnsense.org/

Copyright and Trademark Notices

Third-Party Software Disclaimer

This document includes references to third-party software solutions such as OPNsense, and OpenVAS. Instelligence does not develop, maintain, or support these third-party tools unless stated otherwise. Any issues, vulnerabilities, or changes in functionality related to these solutions should be addressed with their respective vendors.