SIT782

Cybersecurity Assessment Report

Essential Eight Maturity Model – Restrict Administrative Privileges (ML1-RA)
Assessment Scope: Redback Data Warehousing
Assessed by: Cybersecurity GRC Team, Redback Operations
Assessment Date: 17 May 2025

---

1. Introduction

This report presents the outcomes of the Essential Eight Maturity Level 1 (ML1) assessment focused on the "Restrict Administrative Privileges" control category (ML1-RA) for the Redback Data Warehousing environment. The Australian Cyber Security Centre's (ACSC) Essential Eight is a set of prioritized strategies to mitigate cybersecurity incidents, and ML1 establishes the foundational baseline for organizations to defend against common threats.
The objective of this assessment is to determine the extent to which administrative privilege management practices are implemented in the Redback data warehousing infrastructure and to identify opportunities to improve alignment with best practices in secure system administration.

---

2. System Overview and Scope

The target system is the Redback Data Warehousing Virtual Machine (VM), which serves as the core platform for storing and processing structured and semi-structured data across multiple internal Redback projects. The data warehouse:

- Hosts file upload services, MinIO object storage, and MongoDB for project-specific ingestion pipelines.
- Is used by different student project teams for data aggregation, visualization, and downstream analysis using Dremio, Streamlit dashboards, and Jupyter notebooks.
- Is a Deakin University-managed on-premises system, accessible only via VPN and internal network.
- Has no direct internet exposure and is provisioned and patched by Deakin IT Services, not Redback students.

While Redback students and mentors manage application-level services within the VM, the base operating system, patching, and privileged access controls fall partially within their administrative responsibility, particularly when creating new users, accessing Docker containers, and segmenting project environments.

S223090226 **SHREYAS VIVEK**

3. Assessment Methodology

The audit followed Redback's internal compliance testing workflow aligned to the ACSC Essential Eight Assessment Guide. For each ML1-RA test case, the following process was applied:

- Review of Active Directory (AD) roles and user groups
- Analysis of Group Policy Objects (GPOs) applied to privileged and unprivileged environments
- Interviews with mentors and infrastructure stakeholders (e.g., Ben Dang, Daezel Goyal)
- Inspection of logs from administrative sessions, credential provisioning, and container activity
- Manual validation of privilege escalation attempts using tools like runas, RDP, PowerShell Remoting (PSRemote)
- Examination of shared and segregated VM environments, credential reuse, and exception handling

---

4. Summary of Results

Test ID	Control Objective	Compliance Status
ML1-RA-01	Admin access granted only via approved requests	Implemented
ML1-RA-02	Admin accounts cannot access internet/web services	Implemented
ML1-RA-03	Admin accounts do not have email capabilities	Implemented
ML1-RA-04	Admin activities isolated from unprivileged environments	Implemented
ML1-RA-05	Standard users cannot access privileged environments	Implemented
ML1-RA-06	Standard users cannot elevate via PSRemote/RDP	Implemented
ML1-RA-07	Admin accounts restricted from unprivileged workstations	Partially Implemented
ML1-RA-08	Privilege elevation via tools like runas or remote management blocked	Implemented
ML1-RA-09	Quarterly review of administrative accounts	Partially Implemented
ML1-RA-10	Separate identities used for admin and user roles	Partially Implemented

---

5. Detailed Findings and Analysis

ML1-RA-01: Approved Justification for Admin Access

Administrative access to the data warehousing VM is provisioned via internal request and approval workflows managed through JIRA. All credential creation and elevated access is documented and stored in Confluence, allowing traceability. Each instance of admin access requires a new credential issued per session, ensuring that privilege is only granted when necessary. This control is **fully implemented**.

ML1-RA-02: Restricted Internet Access for Admin Accounts

Firewall rules and Squid proxy logs confirm that admin-level accounts are **blocked from accessing the public internet** from within the data warehouse VM environment. Administrative tasks must be performed within the internal network or using Deakin-managed bastion hosts. Users can only access external resources via personal endpoints connected to the Deakin VPN. This provides robust control over unauthorized data egress and ensures separation between privileged tasks and general web usage. **Fully implemented.**

ML1-RA-03: No Mail Capability for Admin Accounts

Mail server configurations enforce that **SMTP and IMAP are disabled** for all admin accounts. This restricts the risk of phishing or command-and-control callbacks being initiated from privileged accounts. A search of AD user objects and Exchange settings revealed no active mailboxes for administrator profiles. **Fully implemented.**

ML1-RA-04: Segregated Administrative Environments

Privileged activities occur in isolated container environments on the VM. VLAN-level separation and Linux container security measures are in place. The team validated that each Docker container has its own runtime environment and file system, providing logical segmentation between administrative and user-facing processes. Admin credentials are not used in user space. This satisfies the maturity level requirement for **logical separation**, and is **fully implemented**.

ML1-RA-05: Blocking Unprivileged Access to Admin Systems

Attempts to log into privileged environments from standard accounts were blocked by AD policies. Audit logs captured denied login attempts, and group membership enforcement aligned with expectations. Credential issuance is controlled and scoped per user, with privilege elevation only possible for approved accounts. This control is **fully implemented**.

ML1-RA-06: Blocking Remote Elevation (PSRemote, RDP)

Attempts to use PowerShell Remoting (Enter-PSSession, Invoke-Command) and RDP were unsuccessful when executed from unprivileged accounts. These actions triggered denied entries in the event log. This indicates that **remote elevation controls are working as intended**, and escalation paths from standard to admin privilege are blocked. **Fully implemented.**

ML1-RA-07: Restriction of Admin Logins on Unprivileged Systems

Group Policy Objects are applied to restrict admin accounts from logging into unprivileged environments. While technically enforced, the **user environments are hosted on shared containers**, meaning that home directories may still expose sensitive operations or config changes to other users. This undermines the strict separation expected under ML1. **Partially implemented.**

ML1-RA-08: Blocking Privilege Elevation via Tools

Elevation attempts using runas, Remote Desktop, and other tools are blocked. Logs show repeated failures when unprivileged users attempt to launch elevated sessions. This confirms that **privilege boundaries are technically enforced**, with appropriate policy application. **Fully implemented.**

ML1-RA-09: Quarterly Admin Account **Review**

While the GRC team conducts periodic reviews of admin accounts, the process is **manual** and relies on individuals such as Ben Dang to track credential creation and deprovisioning. AD membership is reviewed quarterly, but there is no automated alerting or deactivation policy for stale credentials. **Partially implemented.**

ML1-RA-10: Separate Identities for Admin and User Roles

The team uses a dual-identity model by assigning +admin suffixes to privileged accounts. This ensures traceability and accountability for administrative actions. However, shared credentials are still used for specific service-level administration (e.g., Dremio, backup scripts), which weakens role-based access control. **Partially implemented.**

---

6. Key Risks Identified

- Shared user environments (home directories) introduce risk of config leakage or accidental privilege overlap.
- Shared admin credentials for services reduce individual accountability.
- Manual tracking of admin accounts could lead to delays in deactivation or privilege revocation.

---

7. Recommendations

1. **Implement stricter isolation** between containers or user environments where privilege separation is required.
2. **Replace shared service-level admin credentials** with individual, auditable tokens or use secrets management platforms (e.g., AWS Secrets Manager, Vault).
3. **Automate quarterly admin account reviews** using AD group monitoring scripts and audit logs to flag inactive accounts.
4. **Establish a formal exception register** to document and manage any deviations from the default RBAC model.

---

8. Conclusion

Overall, the Redback Data Warehousing team demonstrates strong foundational compliance with the Restrict Administrative Privileges strategy under ACSC's Essential Eight Maturity Level One. The implemented controls ensure that elevated privileges are appropriately requested, restricted, and monitored. However, opportunities exist to enhance security posture through better credential hygiene, automation, and environment segmentation. Addressing the partially implemented controls will significantly improve resilience and reduce the risk of lateral movement or unauthorized administrative activity.

Acknowledgment

We acknowledge the support and contributions of the following entities and communities in the completion of this cybersecurity assessment:

Deakin University – We extend our sincere thanks to Deakin University and its IT Services division for providing the infrastructure, technical guidance, and learning environment that enabled this project. The Redback Operations initiative reflects Deakin's commitment to applied industry-focused education and innovation in cybersecurity.

OpenAI and ChatGPT – We gratefully acknowledge the use of OpenAI's ChatGPT technology, which assisted in drafting, reviewing, and refining audit documentation. This tool provided valuable language support and ensured that reports adhered to professional standards of clarity and consistency.

Traditional Owners of the Land – We acknowledge the Traditional Custodians of the land on which we study and work, the Wadawurrung people, and pay our respects to their Elders past and present. We recognize and honour the enduring connection Aboriginal and Torres Strait Islander peoples have to the land, waters, and culture.