Essential Eight on Linux, Part 4 of 8: Restrict Administrative Privileges on Ubuntu 26.04 LTS

April 29, 2026 / Gavin Jackson

essential-eight asd ism ubuntu linux teleport active-directory entra-id sudo security

If I had to pick one Essential Eight mitigation that most clearly benefits from identity-aware tooling on Linux, this would be it.

Ubuntu gives you the core primitives. **sudo**, **SSH**, **PAM**, **SSSD**, and **polkit** are all there. But if you want something that feels closer to modern privileged identity management rather than old-school shared admin habits, you need to combine the native platform with stronger brokering and approval workflows.

That is where **Teleport** becomes genuinely useful.

What ASD is trying to achieve

The goal is not just "fewer admins."

It is:

- no routine use of privileged accounts
- no standing access where avoidable
- control over who can elevate, to what, and when
- traceability for administrative actions

On Linux, that means you should be deeply suspicious of:

- direct root SSH
- shared local admin accounts
- always-on sudo access for broad teams
- unmanaged SSH keys
- local emergency accounts that quietly became permanent

Ubuntu 26.04 LTS reference implementation

Resolute Raccoon highlights

Ubuntu 26.04 LTS adds a genuinely useful new option here: **authd** is available from the official Ubuntu repositories and supports **Microsoft Entra ID**, **Google IAM**, and standard **OIDC** providers.

That does not replace Teleport for just-in-time privileged brokering, approvals, or session recording. What it does do is give Ubuntu a stronger first-party story for cloud-backed identity on both desktops and servers.

1. Separate user identity from administrative identity

Every administrator should have:

- a standard user identity for day-to-day work
- a separate privileged path for approved administrative activity

Even before you add Teleport, that means:

- disable direct root login over SSH
- require named accounts
- use `sudo` instead of routine root shells
- scope `sudoers` rules to roles and commands where possible

2. Use AD or Entra-backed identity as the source of truth

For on-premises Active Directory, Ubuntu 26.04 can integrate cleanly with:

- `realmd`
- `sssd`
- Kerberos
- AD-backed group membership

If you are deeper in the Microsoft cloud, Entra ID often makes more sense as the administrative identity layer, especially when paired with a zero-trust access broker.

This is where I think the split becomes useful:

- **Active Directory** for traditional domain integration and host identity on enterprise internal networks
- **Entra ID** for SSO, MFA, conditional access, and stronger central identity policy

3. Use Teleport for privileged access brokering

Teleport is not the only option, but it is a strong Linux-native fit for this mitigation because it gives you:

- short-lived certificates instead of unmanaged long-lived SSH keys
- role-based access control
- access requests and approvals
- session recording
- central audit trails
- SSO integration with Entra ID and other identity providers

That makes it a very practical way to implement a Linux-flavoured PIM model.

I would treat Teleport as the privileged front door to high-value Linux resources:

- bastions
- production servers
- Kubernetes admin paths
- databases
- internal web consoles

> ***A note on Teleport Community Edition vs commercial Teleport***
>
> *There is an important nuance here: when people say "Teleport is open source," they are usually talking about the **open source core** and **Community Edition**, not the full commercial feature set.*
>
> *The Community Edition is useful, especially for labs, small teams, and learning the platform. You still get a lot of the fundamentals:*
>
> - *certificate-based access*
> - *RBAC*
> - *audit logs*
> - *session recording*
> - *self-hosted deployment*
>
> *But some of the things that make Teleport especially attractive as a Linux-flavoured PIM platform are tied to the commercial editions rather than the community binaries. The current Teleport feature matrix shows that advanced identity-governance capabilities such as richer **access reviews**, **automatic approvals**, broader **SSO and directory integrations**, and stronger enterprise governance features sit on the enterprise side of the fence.*
>
> *That matters because the more this article leans into **Entra ID integration**, **approval workflows**, and a polished **just-in-time privileged access** experience, the more likely you are to end up needing commercial Teleport rather than just Community Edition.*
>
> *There is also a licensing nuance. Teleport's **Community Edition binaries** now carry commercial-use restrictions for larger companies, while the source code in GitHub remains available under **AGPLv3**. In practice, that means there is a difference between:*
>
> - *using the officially distributed Community Edition binaries or images*
> - *compiling Teleport yourself from source under the AGPL terms*
>
> *For small organisations and home labs, the official community binaries may still be perfectly fine. For larger enterprises, it is worth reading the licensing terms carefully and not assuming that "community edition" means the same thing it used to.*

> *On cost, Teleport's official pricing is now **quote-based and usage-based**, not a simple public per-user price list. That makes it hard to pin to a neat number in an article, but it is fair to say that commercial Teleport can become a **significant investment** once you move beyond hobby or small-team use. The product can absolutely be worth it, but it is not a trivial line item.*

4. Build a just-in-time pattern instead of standing sudo

The strong pattern looks like this:

1. User signs in with SSO and MFA.
2. User requests elevated access to a Linux role or target set.
3. Approval is granted for a short window.
4. Teleport issues short-lived credentials and records the session.
5. Host-level sudo is available only through the approved role mapping.

That is not identical to Microsoft Entra PIM, but it gets you to a very similar control outcome for Linux resources.

5. Map identity groups to narrow Linux roles

Avoid giant "linux-admins" groups with universal reach.

Instead, use environment or function-based roles such as:

- `prod-web-admin`
- `prod-db-breakglass`
- `devops-nonprod`
- `landscape-platform-admin`

On the host side, keep `sudoers` aligned to those roles. On the identity side, map AD or Entra groups into Teleport roles with short expiry and approval requirements.

ISM control mapping

The October 2024 Essential Eight to ISM mapping links this mitigation to the following controls:

ISM control	Linux implementation on Ubuntu 26.04 LTS
ISM-1507	Restrict privileged access to systems and applications through named admin paths and role mapping.
ISM-1647	Limit administrative privileges to users with an established business need.
ISM-1648	Use separate privileged accounts or access paths rather than routine elevation from general-purpose sessions.
ISM-0445	Prevent direct or shared privileged account use where accountable named access is possible.
ISM-1175	Review privileged access regularly and remove stale entitlements.
ISM-1883	Ensure privileged access is tightly controlled for high-value or sensitive systems.
ISM-1380	Use approval workflows or additional controls for privileged operations where feasible.
ISM-1687	Avoid broad standing administrative privileges across the fleet.
ISM-1688	Constrain the scope of privileged access to the minimum systems and functions required.
ISM-1689	Review and revalidate privileged assignments on a recurring basis.
ISM-1387	Monitor and log privileged activity for accountability and incident response.
ISM-1685	Ensure privileged users use dedicated administrative mechanisms rather than unmanaged workarounds.
ISM-1509	Protect credentials and authentication material used for privileged access.
ISM-1650	Enforce additional controls around privileged access, including stronger authentication and approvals.
ISM-1815	Apply stronger controls and governance to privileged access at higher maturity levels.
ISM-1906	Align privileged access restrictions with uplift controls across the environment.
ISM-1228	Use logging and monitoring to detect privileged misuse or anomalous administrative behaviour.
ISM-0123	Protect administrative event logs from tampering.
ISM-0140	Retain sufficient records for security monitoring and investigation.
ISM-1819	Review and strengthen administrative controls over time rather than treating them as static.

Active Directory and Entra ID: where each fits

This is the model I think makes the most sense for many Ubuntu shops:

- use **AD integration on Ubuntu** where you need traditional domain-backed account management and policy
- use **Entra ID** as the identity provider for SSO and MFA
- use **Teleport** as the brokering layer for privileged Linux access

That gives you a cleaner answer than trying to force every Linux administrative pattern directly into native Microsoft tooling.

It also keeps the control portable. Teleport can front SSH, Kubernetes, databases, and internal apps using the same approval and audit model.

Where native Ubuntu falls short

Ubuntu has the local mechanics for privilege separation, but it does not natively provide a first-party PIM workflow with:

- access requests
- time-bound elevation
- central approval chains
- session recording

That is the gap Teleport closes very well.

Commercial alternatives

Teleport is the first product I would look at for this control in Linux-heavy estates, especially where you want PIM-like behaviour without turning Linux administration into a collection of brittle bastions and static keys.

Other PAM or PIM platforms can also play here, but Teleport has the advantage of fitting the Linux operating model naturally instead of feeling like a Windows control awkwardly pasted onto SSH. I would just go into it with clear eyes about which features live in Community Edition and which ones push you into enterprise licensing.

The bottom line

Restricting administrative privileges on Ubuntu 26.04 LTS is not mainly a `sudoers` problem. It is an identity, approval, and audit problem.

Use Ubuntu's native privilege controls as the base layer, then add **AD or Entra-backed identity** and **Teleport** for short-lived, approved, and recorded administrative access. Resolute Raccoon's packaged **authd** capability makes Entra and OIDC-backed Linux identity more interesting than it was on Ubuntu 24.04, but Teleport is still the stronger answer for PIM-like control.

References

- ASD Essential Eight maturity model and ISM mapping (October 2024)
- Ubuntu Active Directory integration
- ADSys for Ubuntu and Active Directory
- Teleport Access Requests
- Teleport Microsoft Entra ID SSO
- authd documentation
- Teleport core concepts and editions

- Teleport feature matrix
- Teleport pricing
- Teleport Community Edition licensing change

Downloaded from https://www.gavinj.net/post/essential-eight-linux-restrict-administrative-privileges
Generated November 14, 2026. Copyright Gavin Jackson. All rights reserved.