White Paper

Everpure

Why Use LDAP for Everpure Fusion?

Adding “just enough” identity pays off for storage teams

Everpure

Contents

Introduction 3

Why identity becomes critical with Everpure Fusion 3

LDAP as a foundation for consistency 4

What LDAP + Everpure Fusion gives storage teams 4

The concerns over LDAP 5

The "minimal blast radius" LDAP model for Everpure Fusion 6

- What this looks like in practice 6
- How this setup is a "win-win" for IT teams 6
- What you gain with this approach 6
- The trade-offs 7

Conclusion 8

Introduction

For IT teams, especially those working day-to-day to manage their organization's data, Everpure Fusion™ presents immediate and compelling value: fleet-level management, policy-driven provisioning, and a unified control plane in place of individually managed arrays.

However, adoption of Everpure Fusion can stall over a possible IT team concern: Everpure Fusion requires Lightweight Directory Access Protocol (LDAP) and a directory service such as Active Directory or identity provider (IdP) such as Okta. And if they're not already using LDAP, why should IT teams start now just to enable Everpure Fusion?

Directory services can be perceived as additional infrastructure, a potential security risk, or the beginning of a broader identity and access management (IAM) overhaul. However, a lack of LDAP is not the roadblock it may appear to be at first.

With the right design approach, the benefits of both LDAP and Everpure Fusion—consistent access control, automation, and governance across the storage fleet—can be realized without expanding into a large-scale identity transformation.

Why identity becomes critical with Everpure Fusion

Traditional Everpure™ FlashArray™ and FlashBlade® environments are often managed at the individual array level. In this scenario, local user accounts are typically sufficient. A small number of administrators, limited scope, and some scripting can keep operations manageable.

Everpure Fusion changes this operating model in several important ways:

- Management shifts from individual arrays to fleets.
- Policies are applied across multiple arrays and locations.
- Automation replaces manual configuration tasks, allowing far more scale and consistency.
- Governance becomes even more important as environments scale.

In this model, local user accounts no longer provide the necessary consistency or scalability. The remote operations of Everpure Fusion require more robust, centralized identities.

Everpure Fusion depends on a centralized system to answer two fundamental questions across all arrays in the fleet:

- Who is the user?
- What actions is the user authorized to perform?

To ensure consistent answers, all participating arrays must share a common user directory configuration. This is the role LDAP plays in an Everpure Fusion environment.

LDAP as a foundation for consistency

A key point to understand is that LDAP is not, by itself, an identity strategy. It is a widely adopted protocol and directory interface that supports existing identity systems.

LDAP doesn't replace your existing identity system (even if it's informal). It enables several core capabilities:

- Centralized authentication using directory-managed credentials
- Group-based authorization, where roles are assigned through directory groups
- Consistent access control across systems and environments

Within Everpure Fusion, these capabilities allow storage administration to become more predictable, auditable, and scalable across the entire fleet.

Importantly, adopting LDAP for Everpure Fusion does not require building a new, dedicated identity platform just for your data management. In many environments, directory services (for example, Active Directory on Windows systems) or an IdP are already in place for file services or other infrastructure, and Everpure Fusion can integrate directly with them. Cloud-focused organizations may use managed directory services or Secure LDAP (LDAPS) endpoints to provide compatibility without operating their own directory infrastructure.

It is important to recognize that directory services become a foundational dependency for the Everpure Fusion control plane. Treating them as a Tier 0 component is a deliberate architectural decision that supports reliable and consistent fleet-wide operations.

What LDAP + Everpure Fusion gives storage teams

The following table provides a storage-focused perspective on the advantages of LDAP and Everpure Fusion, specifically illustrating how Everpure Fusion and Purity leverage LDAP.

Everpure Fusion + LDAP benefit	Why it matters day-to-day
Centralized access control	No more managing local users on every array; add or remove admins in one place instead of per-box sprawl.
Group-based Role-Based Access Control (RBAC)	Grant access once (for example, to array_admins group) and apply everywhere in the fleet via group-to-role mappings.
Cleaner offboarding	Remove a user from the right group and admin rights disappear across all Everpure Fusion-enabled arrays on the next auth.
Fleet-level consistency	Maintain the same roles, permissions, and policy mappings on every member array with less configuration drift.
Better auditability	"Who can manage storage?" has a real, directory-backed answer; actions are tied to identity and role.
Required enabler for Everpure Fusion	Unlock fleet management, remote provisioning, and policy-driven automation; Everpure Fusion does not currently perform cross-array operations without LDAP.
Works with existing identity	In Active Directory-heavy environments, you're using the directory you already own; in others, a managed LDAP endpoint can bridge existing IAM to Everpure Fusion.
Designed for read-heavy auth	Directories are optimized for fast, read-heavy lookup workloads (auth and group resolution), which matches Everpure Fusion usage well.
Secure, scalable management	Once you stop managing arrays individually, having a central source of truth for admin identity and role is an essential, not a nice-to-have.

In short, LDAP removes friction from storage operations once you move beyond single-array thinking and want Everpure Fusion fleet-level benefits.

All of this assumes a consistent LDAP configuration across every array in the Everpure Fusion fleet—uniform resource locator/uniform resource identifier (URL/URI), base distinguished name (base DN), group names, and role mappings must match. That level of consistency is a requirement for Everpure Fusion.

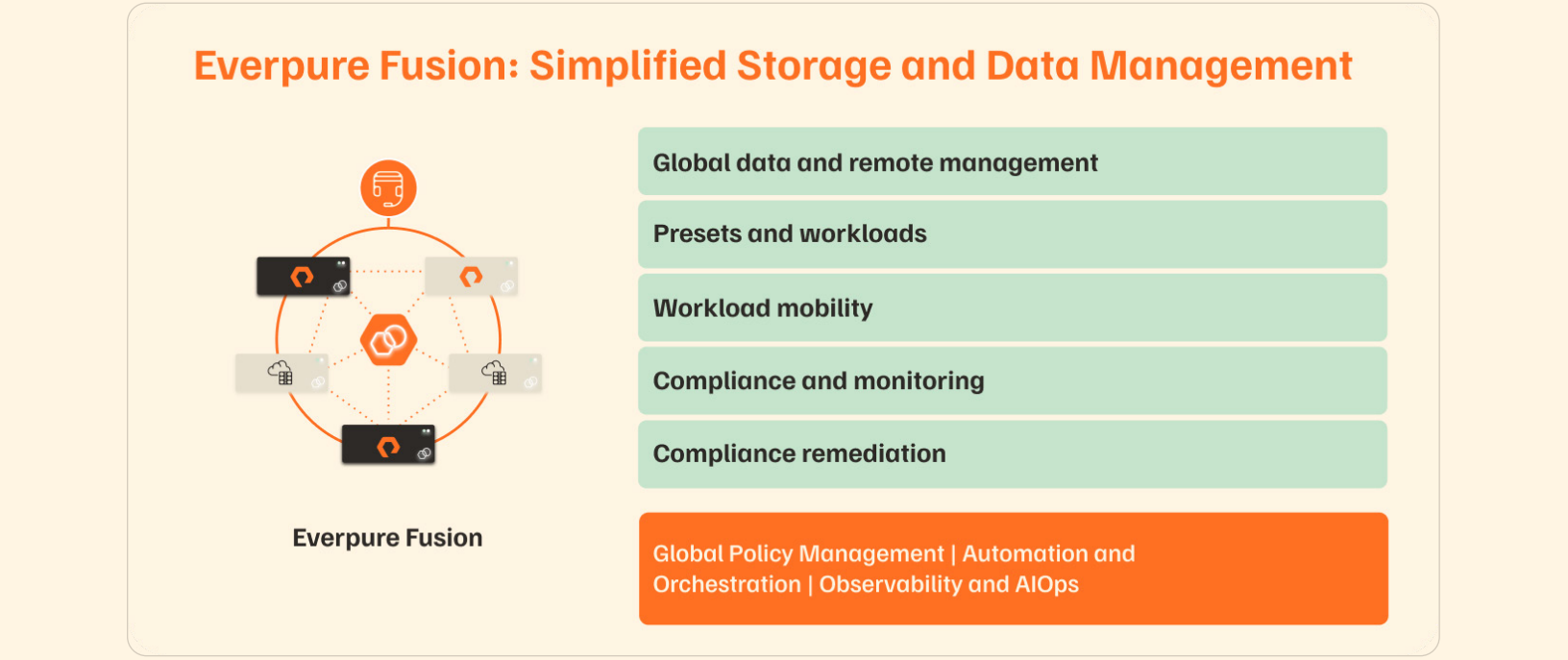
The concerns over LDAP

LDAP does have a bit of a reputation—and not all of it is undeserved. The key to overcoming these concerns lies in how you deploy and scope it and how honest you are about the operational and security work involved for the teams responsible for it.

Concerns about LDAP	Why teams worry
Additional infrastructure to manage	Fear of running a directory just for storage, plus any overhead for high availability, backups, monitoring, and so on
Potential security risks	Managing additional credentials, increasing attack surface, misconfigurations around LDAP and channel binding
Availability dependency	Concerns around the availability risk introduced if LDAP goes down and Everpure Fusion can't authenticate admins
IAM scope creep	Potentially creating a much larger, cross-team project (storage + security + IAM)
Legacy baggage	LDAP can feel old compared to SAML or OpenID Connect single sign-on and modern identity as a service

These can become real issues if LDAP is treated as a core identity authority and then operated casually.

The good news: that's **not** what Everpure Fusion requires. If you can plug into a directory that your security and IAM teams consider Tier 0 and properly hardened, you're all set. And there's a simpler way of achieving this goal than you might have imagined.



The "minimal blast radius" LDAP model for Everpure Fusion

The reality is that you don't need to launch a massive new LDAP or IAM project just to lay the groundwork and take advantage of Everpure Fusion. The winning setup for many Everpure customers is simple:

Use LDAP as a read-only, scoped integration into your existing identity world—and nothing more.

What this looks like in practice

- **Read-only LDAP access:** Everpure Fusion authenticates users against the directory and resolves group membership; it does not perform writes, schema changes, or lifecycle operations back into the directory.
- **Dedicated groups for Everpure Fusion/admin roles:** Create dedicated groups such as `PF_Admin`, `PF_Operator`, and `PF_ReadOnly`, or use whatever naming aligns to your standards. Each group maps cleanly to a Purity role (`array_admin`, `storage_admin`, `ops_admin`, `readonly`) on every array.
- **Low-privilege service account (bind user):** A dedicated service account is scoped to a specific organizational unit or search base that contains only the relevant groups and users; it is a member of the Domain Users group only and is limited to read-only directory lookups with no elevated rights.
- **TLS-only (LDAPS/StartTLS) connections using proper certificates:** Everpure uses LDAPS only for querying your directory service. You plan for certificate issuance, rotation, and troubleshooting as an ongoing responsibility, not an afterthought.
- **Upstream identity life cycle:** Joiners, movers, and leavers are handled by your existing IAM and HR processes. LDAP simply reflects the current state, and Everpure Fusion consumes that via read-only queries.
- **Consistent configuration across all Everpure Fusion arrays:** Every fleet member is configured with the same LDAP base DN, and you validate with `pureds` tests on FlashArray or FlashBlade.

How this setup is a "win-win" for IT teams

- **Any LDAP outages only affect Everpure Fusion management plane access and do not block I/O to existing volumes.** Your applications keep running as normal, but administrators may be temporarily blocked from logging in or performing remote operations until the directory recovers.[1]
- **Everpure Fusion doesn't become an IAM authority;** it delegates identity to LDAP and sticks to RBAC on the storage side.
- **Security and IAM teams are more comfortable** because the integration is read-only, TLS-protected, and scoped.
- **Storage teams get the fleet-level control plane they need** without reinventing identity or taking on a massive new project.

What you gain with this approach

With a minimal, read-only LDAP integration, your Everpure Fusion capabilities remain intact. These include:

- Fleet-wide provisioning of block, file, and object resources across supported arrays
- Storage-as-code workflows via API/CLI using `--context` for remote operations
- Policy-based governance via presets, workloads, protection policies, and quality of service templates
- A centralized control plane view (Fleet View) for resources and operations
- Auditability of admin access and actions tied back to directory-backed identities

LDAP simply gates **who** can use Everpure Fusion, not **whether** Everpure Fusion can do these things with today's feature set. **The constraints are in who may act, not in what Everpure Fusion is capable of.**

The only potential limitation would be with any future Everpure Fusion capabilities that are more identity-native (for example, attribute-based policies). Those features may require more than just "user is in group X" identity management.

The trade-offs

While a minimal LDAP approach does come with some caveats that should be understood, none of these trade-offs should be considered deal-breakers.

Trade-off	Impact
Less dynamic RBAC	Access is explicit, not autogenerated from rich organizational attributes; you rely on a small set of admin groups rather than policies that rely on Attribute-Based Access Control (ABAC).
No identity writes from Everpure Fusion	Life cycle stays outside storage; IAM/HR systems remain the source of truth for user accounts and group membership.
Slightly slower access changes	Group updates propagate on next auth/sync; storage teams may need to coordinate with IAM instead of flipping roles locally.
Less future ABAC flexibility	You're prioritizing today's Everpure Fusion value over hypothetical future identity-native features; you may need to evolve your model later if you want deep ABAC/JIT integration.
Some upfront IAM coordination	Storage can't unilaterally define roles; group naming/ownership and LDAPS hardening involve working with security and directory teams.

The honest take on these trade-offs? For storage administration, **many of these are actually features, not bugs**:

- Explicit access is always preferred over accidental privilege expansion.
- Keeping lifecycle and identity writes out of the storage plane reduces blast radius.
- Cross-team discipline around who is in **PF_Admin** is a good thing.

Making sure that your security and IAM partners are familiar with these trade-offs can help ease any concerns that they might have around adopting this minimal, Everpure Fusion-centric LDAP setup.

Conclusion

Everpure Fusion utilizes LDAP and your directory service or IdP to handle access rights across your data estate to deliver safe, secure, and useful data management at scale. This combination has several advantages for IT teams.

- Everpure Fusion delivers its biggest value when identity is centralized through LDAP, not scattered local accounts.
- LDAP integration doesn't have to be a big, scary IAM rearchitecture—but it is a Tier 0 dependency that deserves real design and security attention.
- A scoped, read-only LDAP layer, wired consistently across your fleet, unlocks Everpure Fusion safely and predictably.
- The operational gains—fleet automation, policy consistency, and simplified audits—outweigh the overhead for most environments that are already on a growth path beyond one or two arrays.

LDAP isn't a cost of Everpure Fusion—it's the multiplier for taking Everpure Fusion from "neat feature on a single box" to a real, fleet-scale storage platform.

The key is to approach your Everpure Fusion-focused LDAP environment deliberately:

- Start with a minimal, read-only integration.
- Design groups and role mappings like a product.
- Treat your directory as the Tier 0 service it already is.

If your storage environment is growing or spanning multiple arrays, or you'd love to automate more and eliminate storage headaches, "just enough LDAP" is often the missing piece that makes Everpure Fusion practical, not theoretical.

For more information on Everpure Fusion:

- Watch the video
- Take a test drive
- Visit the webpage

Review:

- The Everpure Fusion Quick Start Guide
- The Everpure Community forums

1 | If you already use LDAP for SMB/NFS or multiprotocol file services, directory outages can impact data-path authentication for those workloads independent of Everpure Fusion.

ID19414-01-en-04/26