GUÍA TÉCNICA

Guía: Arquitectura híbrida AD + Entra ID

Diseño de identidad híbrida para empresas con Active Directory on-premise y Microsoft 365.

Kwadrant Systems — Marzo 2026

La mayoría de empresas con más de 50 usuarios mantienen un Active Directory on-premise con años de configuración. Migrar a cloud no significa eliminarlo de golpe — significa integrarlo con Entra ID para obtener lo mejor de ambos mundos.

1. Opciones de sincronización

Opción	Descripción	Caso de uso
AD Connect	Servidor on-prem que sincroniza identidades con Entra ID. Soporta PHS, PTA y federation.	AD complejo, múltiples dominios o requisitos de autenticación específicos.
Cloud Sync	Agente ligero gestionado desde la nube. Más sencillo, menos funcionalidades.	AD simple, un solo dominio, sin requisitos de federation.
Solo cloud	Sin sincronización. Identidades solo en Entra ID.	Empresas nuevas sin AD o migración completa ya realizada.

2. Métodos de autenticación

Método	Descripción	Hash en cloud	Disponibilidad	Complejidad
PHS	El hash se sincroniza con Entra ID. Autenticación en la nube.	Sí	Alta	Baja
PTA	Autenticación validada contra AD on-prem en tiempo real.	No	Depende AD	Media
ADFS	Servidor de federación on-prem gestiona la autenticación.	No	Depende ADFS	Alta

Microsoft recomienda Password Hash Sync como baseline por su simplicidad y alta disponibilidad.

3. Exchange Hybrid

Si la empresa tiene Exchange Server on-premise, la coexistencia permite tener buzones en ambos entornos simultáneamente. La migración se hace por fases: se mueven buzones gradualmente, manteniendo la funcionalidad de libre/ocupado, delegaciones y reglas de transporte.

- ✓ Hybrid Configuration Wizard (HCW) ejecutado
- ✓ Certificado SSL válido en Exchange on-premise
- ✓ Conector de correo bidireccional configurado
- ✓ Autodiscover apuntando correctamente
- ✓ Migración por batches planificada con rollback

4. Decisiones de diseño

Antes de implementar, estas preguntas deben estar respondidas:

Source of authority: ¿AD on-prem o Entra ID será la fuente principal?

UPN: ¿Los usuarios tienen UPN correcto y routeable?

Grupos: ¿Se sincronizan todos los grupos o solo un subconjunto?

Dispositivos: ¿Hybrid Azure AD Join o Azure AD Join puro?

Apps legacy: ¿Hay aplicaciones que requieren Kerberos o NTLM?

DNS: ¿El dominio DNS público y el interno son el mismo?

Failover: ¿Qué pasa si AD Connect deja de funcionar 24 horas?

Contacto: kwadrant.es — Diseño de arquitectura híbrida sin coste inicial