

Identità per Contoso Corporation

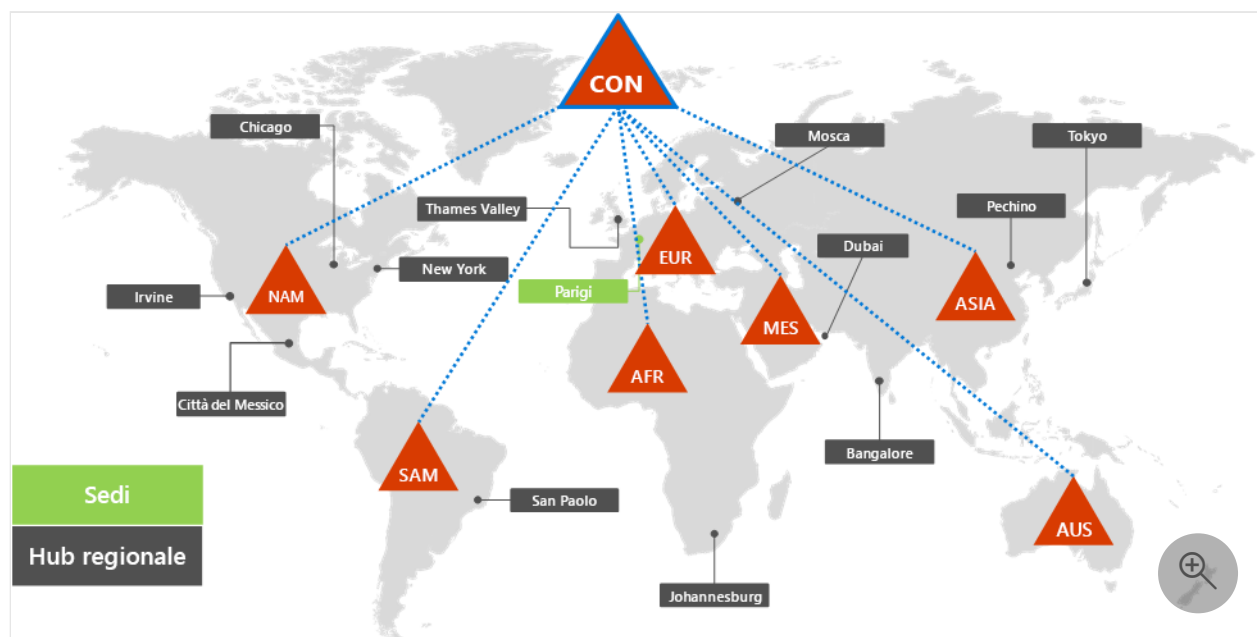
Articolo • 04/04/2023 • 2 minuti per la lettura

Microsoft fornisce Identity as a Service (IDaaS) nelle offerte cloud tramite Azure Active Directory (Azure AD). Per adottare Microsoft 365 per le aziende, la soluzione Contoso IDaaS doveva usare il provider di identità locale e includere l'autenticazione federata con i provider di identità di terze parti attendibili esistenti.

Foresta Active Directory Domain Services Contoso

Contoso usa una singola foresta Active Directory Domain Services (AD DS) per contoso.com con sette sottodomini, uno per ogni area del mondo. La sede principale, le sedi centrali regionali e le filiali contengono controller di dominio per l'autorizzazione e l'autenticazione locali.

Ecco la foresta Contoso con domini internazionali per le diverse parti del mondo che contengono hub regionali.



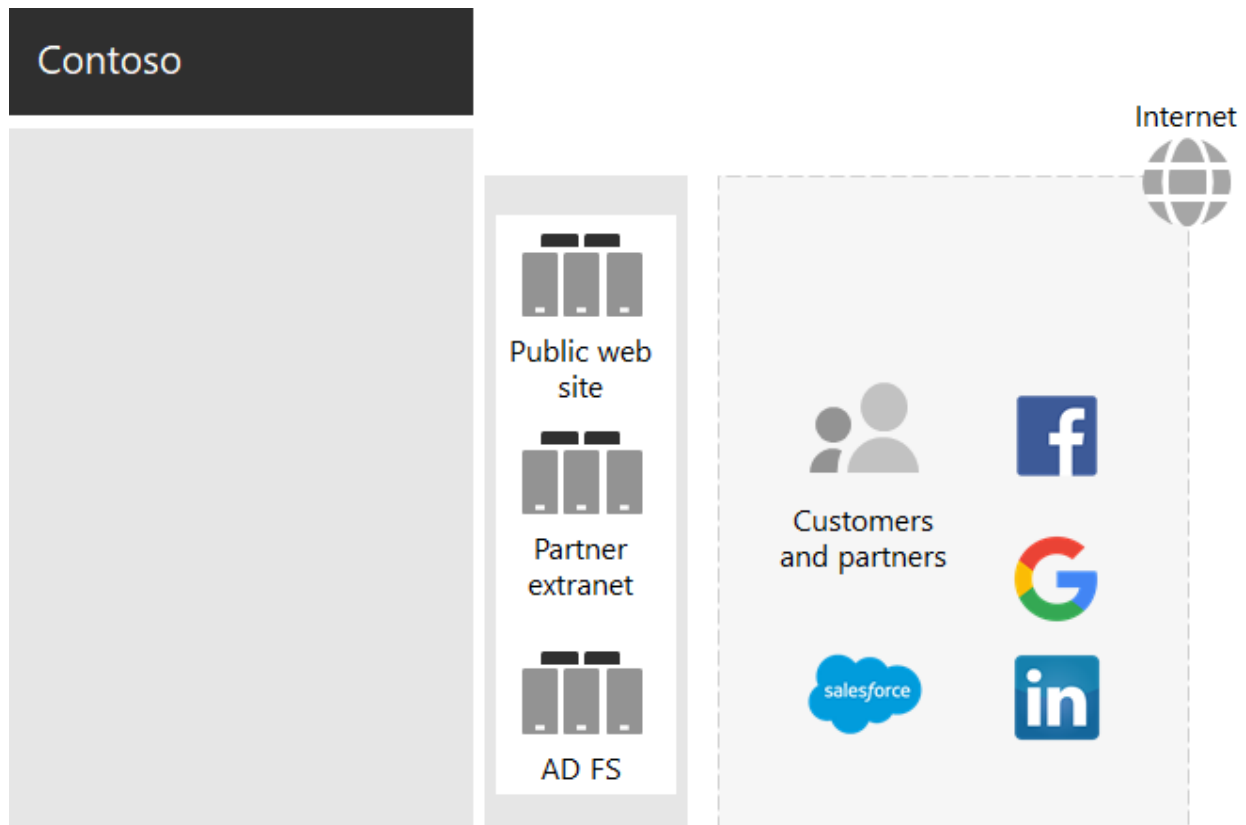
Contoso ha deciso di usare gli account e i gruppi nella foresta contoso.com per l'autenticazione e l'autorizzazione per i carichi di lavoro e i servizi di Microsoft 365.

Infrastruttura di autenticazione federata di Contoso

Contoso consente:

- I clienti devono usare i propri account Microsoft, Facebook o Google Mail per accedere al sito Web pubblico dell'azienda.
- Fornitori e partner possono usare i propri account LinkedIn, Salesforce o Google Mail per accedere all'extranet partner dell'azienda.

Ecco la rete perimetrale contoso contenente un sito Web pubblico, un'extranet partner e un set di server Active Directory Federation Services (AD FS). La rete perimetrale è connessa a Internet che contiene clienti, partner e servizi Internet.



I server AD FS nella rete perimetrale facilitano l'autenticazione delle credenziali dei clienti da parte dei provider di identità per l'accesso al sito Web pubblico e alle credenziali del partner per l'accesso all'extranet partner.

Contoso ha deciso di mantenere questa infrastruttura e dedicarla all'autenticazione dei clienti e dei partner. Gli architetti per le identità di Contoso stanno valutando la conversione di questa infrastruttura in soluzioni [B2B](#) e [B2C](#) di Azure AD.

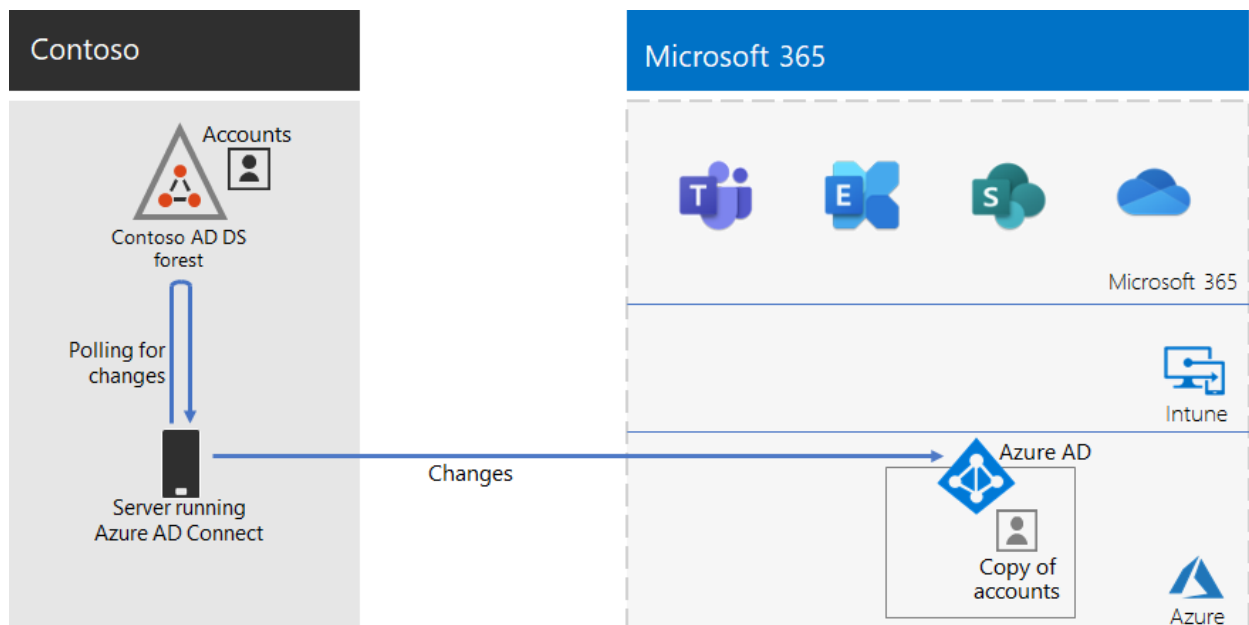
Identità ibrida con sincronizzazione dell'hash delle password per l'autenticazione basata su cloud

Contoso voleva usare la foresta di Servizi di dominio Active Directory locale per l'autenticazione alle risorse cloud di Microsoft 365. Ha deciso di usare la sincronizzazione dell'hash delle password (PHS).

PHS sincronizza la foresta di Active Directory Domain Services locale con il tenant di Azure AD della sottoscrizione di Microsoft 365 for enterprise, copiando account utente e gruppo e una versione con hash delle password degli account utente.

Per eseguire la sincronizzazione della directory, Contoso ha distribuito lo strumento Azure AD Connect in un server nel data center di Parigi.

Di seguito è riportato il server che esegue Azure AD Connect che esegue il polling della foresta Contoso AD DS per le modifiche e quindi la sincronizzazione di tali modifiche con il tenant di Azure AD.










Criteri di accesso condizionale per l'identità Zero Trust e l'accesso ai dispositivi

Contoso ha creato un insieme di [criteri di accesso condizionale](#) per Azure AD e Intune per tre livelli di protezione:

- *Le protezioni del punto di partenza* si applicano a tutti gli account utente.
- *Le protezioni aziendali* si applicano ai dirigenti senior e al personale esecutivo.
- *Le protezioni di sicurezza specializzate* si applicano a utenti specifici nei reparti finanziari, legali e di ricerca che hanno accesso a dati altamente regolamentati.

Ecco il set risultante di criteri di identità Contoso e accesso condizionale del dispositivo.

Livello di protezione	Tipo di dispositivo	Criteri di accesso condizionale di Azure AD			Criterio di rischio utente di Azure AD Identity Protection	Criteri di conformità dei dispositivi Intune	Criteri di protezione delle app di Intune
Di base: tutti gli account utente		È richiesta l'autenticazione a più fattori (MFA) quando il rischio di accesso è considerato medio o elevato	Sono richieste app approvate	Blocco dei client che non supportano l'autenticazione moderna	Sono richiesti PC conformi	Criteri di conformità per Windows, iOS e Android	Criteri di protezione delle app per iOS e Android
							
Avanzata: account utente dei dirigenti		È richiesta l'autenticazione a più fattori (MFA) quando il rischio di accesso è considerato basso, medio o elevato		Blocco dei client che non supportano l'autenticazione moderna	Sono richiesti PC e dispositivi mobili conformi	Gli utenti a rischio elevato devono modificare la password	
							
Per ambienti altamente regolamentati: account utente per posizioni legali, finanziarie e di ricerca		È richiesta sempre l'autenticazione a più fattori					
							

Passaggio successivo

Informazioni su come Contoso usa l'infrastruttura di microsoft endpoint Configuration Manager per [distribuire e mantenere aggiornati i Windows 10 Enterprise](#) nell'intera organizzazione.

Vedere anche

[Distribuire l'identità per Microsoft 365](#)

[Panoramica di Microsoft 365 per le aziende](#)

[Guide dei laboratori di testing](#)