QUALCHE ASTUZIA PRIMA DI INIZIARE: SUGGERIMENTI TECNICI SU WORKSPACE ONE

La forza lavoro mobile globale passerà da 1,32 miliardi nel 2014 a 1,75 miliardi nel 2020. I lavoratori mobili utilizzano sempre più spesso una gamma eterogenea di dispositivi e applicazioni, dai desktop agli smartphone, fino ai tablet o alle appliance IoT (Internet-of-Things) aziendali o le smart appliance, per svolgere le loro attività. Inoltre, vogliono poter accedere in modo flessibile alle mobile app e alle applicazioni legacy, desktop, Software-as-a-Service (SaaS) e cloud, in base all'attività o alla situazione e al tipo di interazione, utilizzando gli strumenti che preferiscono.

Per supportare queste interazioni, le aziende necessitano di un Digital Workspace con un'architettura IT integrata in grado di offrire agli utenti finali un'esperienza semplificata. L'esperienza dovrebbe essere legata all'identità del singolo e al contesto ogni volta che un utente accede a un'applicazione.

Nell'attuale mondo mobile, un'identità non è più vincolata a un singolo dispositivo o a una singola rete. Non è più sufficiente fornire a un utente un account per un unico dominio con privilegi per l'accesso completo, poiché i dipendenti moderni non lavorano più solo sulla rete aziendale. L'IT non può semplicemente limitarsi a proteggere il data center con un firewall. Le aziende devono creare un nuovo perimetro di sicurezza attorno all'utente per rimuovere gli ostacoli che non gli consentono di lavorare ovunque e in qualsiasi momento. Oggi, praticamente tutte le applicazioni e tutti i servizi potrebbero richiedere un'autenticazione univoca.

Spetta alle aziende soddisfare queste esigenze e adottare la digital transformation, che risulta vantaggiosa per gli utenti e per il business. Alla luce di quanto appena detto, di seguito sono riportati alcuni suggerimenti tecnici per rendere VMware Workspace ONE™ la piattaforma imprescindibile per il Digital Workspace definito in base all'identità:

1. Consentire un accesso continuo ad app e dati da qualsiasi dispositivo

È importante dare ai dipendenti la flessibilità necessaria per cogliere le opportunità offerte dalla mobility utilizzando il dispositivo che preferiscono. Ad esempio, per gli utenti Salesforce, offrire accesso Single Sign-on (SSO) all'applicazione web Salesforce sul desktop aziendale, sul laptop aziendale e sul PC personale tramite il portale web Workspace ONE.

Per offrire opzioni aggiuntive, è possibile consentire l'accesso SSO tramite un dispositivo mobile BYO (Bring Your Own) o gestito dall'azienda tramite la distribuzione e la configurazione dell'applicazione Salesforce nativa per i dispositivi mobili. Workspace ONE si integra senza difficoltà con i provider di identità esistenti dell'azienda, offrendo nel contempo un'esperienza d'uso semplice e coerente e rafforzando le regole di compliance.

Cos'è VMware Workspace ONE

VMware Workspace ONE™ integra funzionalità di gestione delle identità e della mobility per offrire ai dipendenti accesso semplice e sicuro alle applicazioni e ai dati richiesti tramite qualsiasi dispositivo, ovunque e in qualunque momento. Per maggiori informazioni su Workspace ONE, visitare il sito https://workspaceone.com.

2. Accertarsi che i dati nei dispositivi BYO siano sempre sicuri, indipendentemente dallo stato del dipendente

Gli utenti finali si aspettano che le aziende distribuiscano applicazioni, desktop e mobile app su qualsiasi dispositivo, inclusi dispositivi mobili BYO iOS e Android. Tuttavia, le aziende devono continuare a garantire la sicurezza dei dati presenti nei dispositivi mobili BYO degli utenti e avere la possibilità di cancellarli se il dipendente si dimette, viene licenziato o smarrisce il dispositivo.

Workspace ONE è in grado di gestire in modo adattivo e di supportare tutti i dispositivi necessari e di registrarli in base alle esigenze se l'utente finale richiede accessi aggiuntivi. Quando un utente finale ha bisogno di accedere alle applicazioni aziendali di base, non deve fare altro che accedervi tramite Workspace ONE e autenticarsi mediante il Single Sign-on. Quando è necessario un accesso più sicuro alle applicazioni, Workspace ONE può utilizzare i container nativi sul dispositivo e attivare un profilo se è richiesta una compliance più rigorosa dei dispositivi per un'applicazione specifica, in modo da garantire la sicurezza dei dati aziendali. In caso di smarrimento del dispositivo o di dimissioni/licenziamento del dipendente, il profilo può essere disattivato dall'utente o dall'IT aziendale senza altre conseguenze per il dispositivo mobile dell'utente finale.

3. Consentire agli utenti finali di accedere facilmente senza compromettere la sicurezza

Comprensibilmente, molti utenti finali non vedono di buon occhio configurazioni complesse e autenticazioni multi-touch quali RSA SecurID e altri metodi di autenticazione tramite token dai loro dispositivi mobili (inclusi laptop, tablet e smartphone). Grazie all'utilizzo delle funzioni di autenticazione sicura tramite token per applicazioni e a più fattori di VMware Identity Manager™ e di VMware Verify, Workspace ONE è in grado di fornire funzionalità SSO di facile utilizzo eventualmente integrabile con un'autenticazione a più fattori.

La funzione di autenticazione sicura tramite token per applicazioni utilizza diverse tecnologie per le varie piattaforme (ad esempio, Cloud KDC for iOS, Android for Work e Chrome Tabs for Android, Windows Account Provider e TBAUTH). Workspace ONE è compatibile con la maggior parte dei provider di autenticazione di terze parti e offre pertanto maggiore flessibilità.

4. Consolidare il numero di identità digitali mediante l'integrazione di provider di identità di terze parti

I provider di identità (IdP) di terze parti quali Ping possono essere configurati con VMware Identity Manager per autenticazioni degli utenti finali in cascata. Ad esempio, Ping può essere l'IdP per Salesforce, fungendo da provider di servizi. Per stabilire una concatenazione tramite VMware Identity Manager, Identity Manager diventa l'IdP per Ping e Ping funge da provider di servizi.

Workflow di esempio:

1. La richiesta di Salesforce viene inviata a Ping.
2. Ping prende una decisione relativa alle policy basata sull'utente, sull'app, sul tipo di dispositivo (desktop o mobile) e altro ancora.
3. L'adattatore Ping autentica l'utente desktop.
4. Ping inoltra la richiesta mobile a VMware Identity Manager.
5. VMware Identity Manager prende una decisione relativa alle policy.
6. Il dispositivo viene autenticato con un endpoint di autenticazione mobile.
7. Viene effettuato il reindirizzamento a Ping.
8. Ping invia un'asserzione SAML a Salesforce.
9. Operazione completata.

5. Agevolare le integrazioni dei sistemi aziendali esterni tramite connettori

Il connettore dei sistemi aziendali fornito con Workspace ONE facilita l'autenticazione Single Sign-on per gli utenti finali. Questo programma di installazione funge da pacchetto di connettori unificato per Workspace ONE, VMware AirWatch® e Identity Manager. I singoli connettori supportano numerose opzioni e le aziende possono scegliere i componenti che desiderano installare.

AirWatch Cloud Connector (ACC): l'uso di ACC è consigliato quando si utilizza un tenant Identity Manager SaaS oppure quando è necessario un accesso Single Sign-on ad applicazioni SaaS e web o a mobile app.

Gli utenti della Active Directory locale vengono sincronizzati nel tenant VMware AirWatch. Il tenant AirWatch sincronizza questi utenti e gruppi in VMware Identity Manager per l'autenticazione dell'utente in Workspace ONE. ACC richiede soltanto una connessione TCP 443 in uscita.

VMware Identity Manager Connector: l'uso di VMware Identity Manager Connector è consigliato quando si distribuisce VMware Identity Manager on-site oppure quando è necessario integrare il tenant Identity Manager SaaS con VMware Horizon®, VMware ThinApp® o ambienti Citrix XenApp e XenDesktop per il Single Sign-on in ambienti con app SaaS e/o basate su web.

Gli utenti della Active Directory locale vengono sincronizzati nel tenant VMware Identity Manager. Identity Manager Connector supporta un modello di comunicazione "solo in uscita" utilizzando solo una connessione TCP 443 in uscita per comunicare con l'Identity Manager SaaS quando si utilizzano i metodi di autenticazione della distribuzione cloud richiesti quali password, RSA Adaptive Authentication, RSA SecurID o Remote Authentication Dial-In User Service (RADIUS). Altri adattatori di autenticazione quali Kerberos (KerberosIdpAdapter) richiedono invece la connettività TCP 443 in uscita, che utilizza un indirizzo IP NAT (Network Address Translated) pubblico e un nome dominio completo (FQDN) pubblico per VMware Identity Manager Connector on-site. Inoltre, la soluzione on-site di VMware Identity Manager distribuisce automaticamente il connettore all'interno di una singola appliance virtuale (SVA).

Entrambe le applicazioni: se sono necessarie entrambe le mobile app (come pure l'integrazione con VMware Horizon, ThinApp o ambienti Citrix XenApp e XenDesktop), sono necessari sia VMware AirWatch Cloud Connector che VMware Identity Manager Connector.

Nota: Workspace ONE supporta tutte le configurazioni delle applicazioni SaaS e web.

Vantaggi offerti da un Digital Workspace definito in base all'identità

- Federazione dell'identità per i servizi on-site e cloud.
- Esperienza d'uso più fluida.
- Motore delle regole contestuale con sicurezza continua.
- Accesso per impostazione predefinita.
- Abilitazione di un singolo centro di raccolta per l'autorizzazione e l'autenticazione.
- Verifica dello stato dei dispositivi ai fini della compliance.

Conclusioni

Un Digital Workspace consente agli attuali dipendenti sempre più "mobili" di utilizzare qualsiasi desktop o dispositivo (BYO o di proprietà dell'azienda) in qualunque momento, mentre gli amministratori IT possono automatizzare in piena sicurezza la distribuzione di applicazioni e aggiornamenti in tempo reale. Le aziende che distribuiscono un Digital Workspace definito in base all'identità possono adottare tranquillamente un ecosistema eterogeneo, poiché l'accesso tramite l'identità e la personalizzazione non sono più legati alle singole applicazioni o a dispositivi specifici.

VMware Workspace ONE è una piattaforma che include soluzioni come VMware AirWatch®, VMware Socialcast®, VMware Horizon® Enterprise Edition, ThinApp, VMware User Environment Manager™, VMware App Volumes™ e VMware Identity Manager.

Di fatto, VMware Identity Manager costituisce il supporto sottostante per l'intera soluzione Workspace ONE e rappresenta il collante di tutti i prodotti e le soluzioni che operano nell'ambito di Workspace ONE. VMware Identity Manager fornisce inoltre agli utenti finali un'esperienza Single Sign-on per tutti i servizi remoti, desktop e applicazioni, incluse le applicazioni Windows legacy, le applicazioni e i desktop remoti e in hosting (incluso Citrix), le applicazioni SaaS e web, nonché mobile app, contenuti e gestione dei dispositivi.

INIZIA SUBITO

Inizia il test drive in un Hands-on Lab per scoprire quanto sia semplice gestire le applicazioni e l'accesso

Seguici online:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Inc. - Via Spadolini, 5 - Edificio A - 20141 Milano - Tel.: (+39) 02 3041 2700 Fax: (+39) 02 3041 2701 www.vmware.it