DELL Technologies

APEX Data Storage Services - Best practice di sicurezza

Organizzazione per la Resilienza e la Sicurezza aziendale di Dell • Versione 1.1 • Ultimo aggiornamento 18-08-2022

Executive Summary

Le organizzazioni IT continuano ad affrontare sfide nei loro percorsi di trasformazione tecnologica, come ad esempio:

- Overprovisioning/underprovisioning
- Vincoli sugli investimenti di capitale
- Lunghi cicli di approvvigionamento
- Complessità nella migrazione dell'infrastruttura
- Ritmo sostenuto dei cambiamenti tecnologici
- Risorse e set di competenze del personale IT limitati

I leader IT cercano esperienze molto più semplici e agili. APEX Data Storage Services è un portafoglio as-a-Service di risorse di storage scalabili ed elastiche progettate per il trattamento OpEx.[1] Grazie a questa offerta è possibile ottimizzare per semplicità, riducendo l'overprovisioning e l'underprovisioning nonché i complessi cicli di approvvigionamento e migrazione. È possibile gestire senza problemi l'esperienza as-a-Service tramite l'unica interfaccia costituita dalla console APEX.

Il presente documento si basa su strategie di sviluppo protette, fondamentali per la progettazione e lo sviluppo di applicazioni e programmi presso Dell. Il white paper è incentrato su uno scenario di deployment on-premise di APEX Data Storage Services.

Il white paper analizza:

1. I rischi per la sicurezza che è bene che le organizzazioni prendano in considerazione.
2. Le responsabilità associate alla protezione delle informazioni tramite la Matrice di responsabilità condivisa.
3. In che modo le strategie e le misure di sicurezza di APEX Data Storage Services proteggono la sicurezza e l'integrità dei dati.

Considerazioni sulla sicurezza di APEX Data Storage Services

Le organizzazioni devono assicurarsi di considerare i potenziali rischi associati all'integrazione dell'infrastruttura di terze parti nell'ambiente del data center. Tra le considerazioni chiave sulla sicurezza per le organizzazioni che oggi utilizzano o prevedono di utilizzare lo storage fornito in un modello as-a-Service figurano:

- **Governance della sicurezza:** La governance della sicurezza è cruciale poiché delinea le rispettive responsabilità del fornitore di servizi e del cliente. Dell dispone di una propria governance della sicurezza mappata su diversi framework e controlli importanti del settore. Sono riportati più avanti in questo documento nella sezione Sicurezza e conformità.
- **Considerazioni sulla protezione dei dati:** L'archiviazione di dati e informazioni altamente sensibili su sistemi di storage di terze parti rappresenta un rischio aggiuntivo per i clienti. Una violazione dei dati sensibili potrebbe causare perdite tangibili e non tangibili, come la reputazione dell'azienda, che potrebbe avere un impatto diretto sulla redditività dell'organizzazione e anche tradursi in potenziali problemi normativi. Pertanto, i clienti as-a-Service hanno bisogno della sicurezza della protezione dei dati, che comprende, a titolo esemplificativo, la certezza che il fornitore di servizi attui controlli per la riduzione dei rischi.
- **Legale/conformità:** Le organizzazioni che stanno prendendo in considerazione servizi di storage privato o pubblico devono essere sicure di comprendere le implicazioni legali associate ai tipi di dati che

[1] Il trattamento OpEx è soggetto alle policy e alla revisione contabile interna del cliente.

è possibile archiviare con il fornitore di storage. Tra le altre cose, le normative applicabili (ad esempio, il GDPR e il CCPA) e la sensibilità dei dati archiviati possono avere un impatto significativo sui rischi implicati associati all'approccio allo storage dei dati.

I rischi che Dell attenua sono associati alla sicurezza dell'offerta di servizi e dell'infrastruttura di supporto. È responsabilità del cliente gestire i rischi correlati al funzionamento dei dati, dei sistemi e delle applicazioni all'interno del cloud.

Responsabilità del cliente e di Dell riguardo ad APEX Data Storage Services

Oltre all'opzione dei servizi per blocchi e file gestiti da Dell, i clienti hanno la flessibilità e il controllo per scegliere chi esegue le operazioni di gestione quotidiane. La gestione di Dell consente di mantenere il controllo operativo dei carichi di lavoro e delle applicazioni mentre Dell gestisce l'infrastruttura on-premise e si occupa della manutenzione. In alternativa, le organizzazioni IT che desiderano un controllo ancora maggiore sull'esperienza as-a-Service possono scegliere l'opzione gestita dal cliente, concepita per affidare al cliente la responsabilità di attività come il monitoraggio dell'utilizzo della capacità, la gestione dell'infrastruttura e l'ottimizzazione delle risorse.

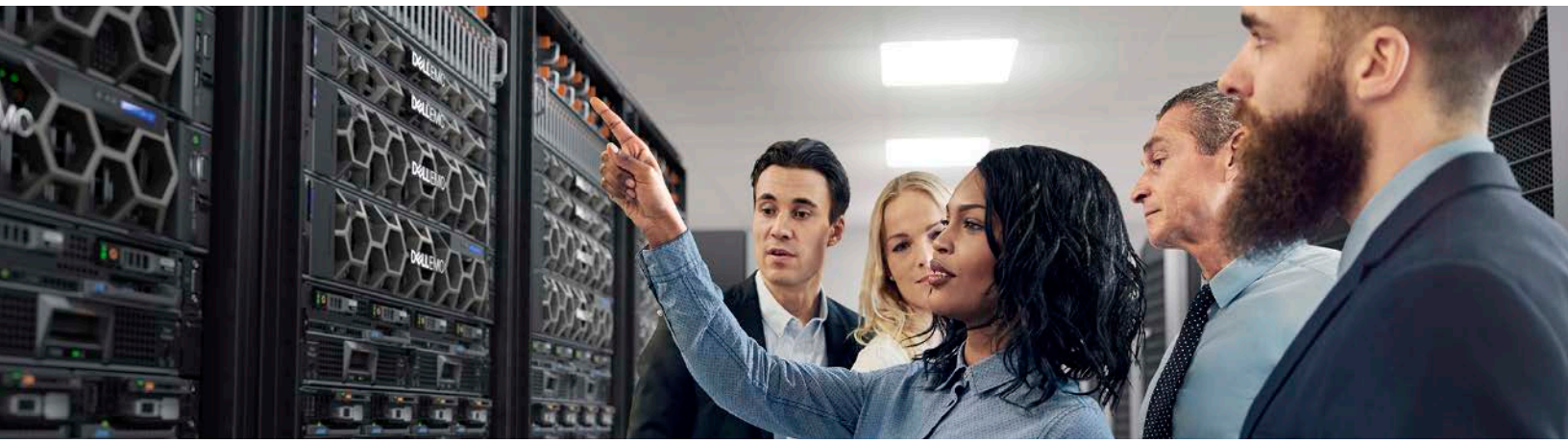
È stato sviluppato un modello di responsabilità condivise che delinea chiaramente i rispettivi ruoli tra il cliente e Dell in base alla funzione, nonché livelli di responsabilità condivisi. Evidenzia una strategia di distribuzione delle applicazioni che consente ai team dei clienti di concentrarsi sulle operazioni quotidiane senza preoccuparsi dell'infrastruttura sottostante per il servizio.

Per una panoramica dettagliata dei ruoli e delle responsabilità, consulta la documentazione disponibile qui: https://www.dell.com/support/home/it-it/product-support/product/apex-data-storage-service/docs

Categoria	Attività di assistenza	Gestione a cura del cliente		Gestione a cura di Dell	
		Cliente	Dell	Cliente	Dell
Deployment	Elettricità, spazio, HVAC, accesso alla rete di gestione e ai dati del cliente*	✓		✓	
	Connettività remota: accesso alla telemetria per il monitoraggio dell'utilizzo e dell'integrità*	✓	✓	✓	✓
	Installazione e provisioning iniziale		✓		✓
Monitoraggio	Prestazioni, capacità e disponibilità del sistema	✓			✓
	Modifiche alla configurazione per mantenere l'impegno in termini di prestazioni e uptime	✓			✓
Gestione	Implementazione degli aggiornamenti del firmware e del software di sistema (manutenzione del sistema)**	✓			✓
	Definizione e gestione delle policy relative a istantanee, sincronizzazione e protezione dei dati	✓		✓	
	Gestione dell'accesso ai dati: volumi, esportazioni NFS e condivisioni di file SMB	✓		✓	
Ottimizzazione	Consigli su prestazioni e configurazione	✓			✓
	Espansione proattiva della capacità e gestione del buffer	✓			✓
Supporto	Supporto proattivo 24x7 per hardware e software di sistema e sostituzione dei componenti on-site		✓		✓
	Indicazioni operative per le procedure		✓		✓
Dismissione	Sanificazione dei dati on-site e recupero degli asset con coordinamento del cliente		✓		✓

*Per le strutture di colocation gestite da Dell, Dell è la principale responsabile di tali attività

**Per l'opzione gestita dal cliente, è responsabilità del cliente avviare la manutenzione semestrale del sistema. Per l'opzione gestita da Dell, la manutenzione del sistema viene fornita costantemente in base alle esigenze



In che modo le informazioni sono protette

Per le soluzioni gestite dal cliente è responsabilità del cliente implementare, effettuare la manutenzione e supportare tutte le configurazioni e le attività per la sicurezza che interessano l'infrastruttura implementata presso la sede del cliente per ragioni di sicurezza e conformità, controllo degli accessi, gestione delle minacce e delle vulnerabilità, crittografia dei dati e risposta agli incidenti.

APEX Console

La console di gestione IT self-service riduce la complessità per facilitare l'identificazione, il deployment, il monitoraggio e l'espansione delle soluzioni in modo rapido, nell'ottica di soddisfare i requisiti aziendali, riducendo al contempo i rischi operativi. La riduzione delle complessità e dei rischi operativi tramite la console offre un modo semplice ma sicuro di gestire i servizi.

Sicurezza e adempienza alle norme

APEX Data Storage Services protegge i dati Dell e dei clienti utilizzando policy e strategie da framework stabiliti. In questo modo i clienti soddisfano i relativi requisiti del programma di conformità. Ove possibile, lo sviluppo di applicazioni e prodotti presso Dell utilizza mapping per framework stabiliti e normative per garantire che l'integrazione di principi e requisiti di sicurezza appropriati nel ciclo di vita dello sviluppo. Le misure di sicurezza che proteggono APEX sono ispirate da standard, normative e framework di controllo CCM, ISO e NIST per garantire la sicurezza.

- NIST - Controlli di sicurezza e privacy per sistemi informativi e organizzazioni federali
- ISO 27000 - Sistemi di gestione della sicurezza delle informazioni
- CCM - Cloud Control Matrix

Controllo degli accessi

È necessario proteggere l'accesso alle informazioni archiviate nell'infrastruttura sottostante di APEX Data Storage Services da accesso, divulgazione e modifiche non autorizzati. Le seguenti procedure di controllo degli accessi consentono di mantenere la sicurezza per l'accesso ai dati:

- Considerazioni sul business case per livelli di sicurezza più elevati
- Verifica dell'affidabilità dell'identità e interoperabilità dell'elaborazione delle informazioni (ad es., SSO)
- Autorizzazioni e funzionalità di supporto per i controlli dei clienti su regole di autenticazione, autorizzazione e accounting (AAA) per l'accesso a dati e sessioni

Gestione delle minacce e delle vulnerabilità

APEX Data Storage Services supporta strategie di gestione delle minacce e delle vulnerabilità per garantire che l'infrastruttura sia protetta da rischi e vulnerabilità identificati. Queste strategie di gestione delle minacce e delle vulnerabilità sono mutuate da metodologie utilizzate nel ciclo di vita di sviluppo sicuro di Dell, tra cui:

1. La coerenza nell'applicazione di patch all'infrastruttura sottostante garantisce l'implementazione delle funzionalità più recenti e aggiornate e delle lacune di sicurezza. Dell utilizza una metodologia regolamentata per la scansione dell'infrastruttura sottostante per APEX Data Storage Services.
2. I metodi per identificare le vulnerabilità o i rischi per la sicurezza sono implementati come parte integrante di APEX Data Storage Systems. Questi metodi includono sia scansioni che test della sicurezza.

Nota: i clienti si assumono la responsabilità di garantire che le applicazioni connesse all'infrastruttura di APEX Data Storage Services siano gestite e aggiornate in modo coerente per evitarne l'uso come vettori di attacco.

Crittografia

APEX Data Storage Services è in grado di crittografare i dati utilizzando algoritmi approvati dal NIST definiti secondo le NIST Special Publications 800-131Ar2. Il Crypto Algorithms del NIST definisce l'utilizzo di algoritmi crittografici e le lunghezze delle chiavi. Di seguito sono riportati gli standard utilizzati da Dell per l'infrastruttura a chiave pubblica per proteggere asset e informazioni:

- Gli algoritmi di crittografia obsoleti sono disabilitati per impostazione predefinita
- I dati classificati come sensibili durante il transito e at-rest possono e devono essere crittografati
- La lunghezza delle chiavi simmetriche deve essere di almeno 256 bit
- La lunghezza delle chiavi asimmetriche deve essere di almeno 2048 bit per RSA e DSA e di 256 bit per algoritmi a curva ellittica
- Occorre rafforzare il TRIPLE DES (3DES) alla baseline AES a 256 bit per tutte le applicazioni

Risposta agli incidenti

Dell si occupa degli incidenti e degli eventi di sicurezza sulla base di una metodologia documentata per il reporting e la gestione. Questo processo garantisce l'avviso tempestivo dei clienti e, se necessario, l'adozione di misure appropriate per risolvere l'incidente.

Dell segue la seguente procedura per la risposta agli incidenti:

- Preparazione
- Rilevamento/analisi
- Contenimento/eliminazione
- Ripristino
- Report

Responsabilità e verifica del sistema

APEX Data Storage Services sfrutta i processi di conformità e protezione per valutare continuamente l'efficacia dei controlli di sicurezza in atto per proteggere i dati e le informazioni sulla piattaforma. Questo comporta audit e valutazioni periodici per identificare e risolvere la mancata conformità.

Dell effettua revisioni e valutazioni indipendenti al fine di garantire che APEX, che si basa su framework stabiliti come il CCM di Cloud Security Alliance, sia conforme alle policy e agli standard definiti del settore.

La valutazione includerà:

- Valutazione dell'host
- Valutazione delle applicazioni web
- Valutazione dei servizi web
- Valutazione dispositivi mobili
- Valutazioni binarie (ove applicabile)

Gateway con connessione sicura

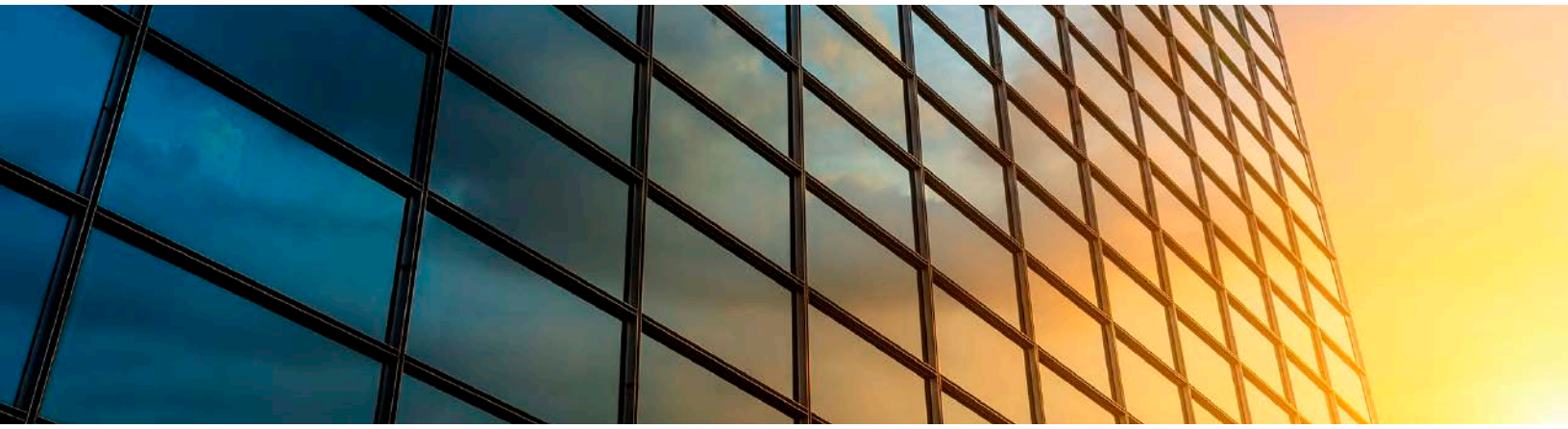
Gateway con connessione sicura è la connessione bidirezionale sicura tra APEX Data Storage Services e l'infrastruttura del cliente. L'introduzione dello strumento gateway con connessione sicura garantisce il trasferimento protetto dei dati e l'utilizzo solo da parte di utenti/dispositivi autorizzati. Questa soluzione fornisce monitoraggio proattivo dell'integrità e prevenzione dei problemi.

Il cliente è responsabile della manutenzione degli utenti, dei corrispondenti attributi e della creazione delle connessioni all'interno della propria infrastruttura. Dell sarà responsabile della gestione dei server e delle reti di sostegno che supporteranno la comunicazione. I servizi richiedono protocolli altamente protetti da Dell e dal cliente per tutte le comunicazioni. Dell fornirà inoltre guide alla configurazione durante l'implementazione.

Conclusioni

APEX Data Storage Services guiderà i tuoi percorsi di trasformazione, offrendo la capacità di chiedere e rispondere alle esigenze di storage scalabile con questa potente soluzione di Storage as-a-Service. I clienti hanno la garanzia dell'impegno di Dell a fornire un'esperienza affidabile, privata e sicura per la raccolta, la comunicazione, il trasporto, l'utilizzo e lo storage dei dati all'interno dell'infrastruttura di APEX Data Storage Services.

Per ulteriori informazioni su APEX Data Storage Services, visita Dell.com/APEX-Storage



Glossario

Termini	Definizione
APEX	APEX è il portafoglio delle offerte as-a-Service di Dell Technologies che semplificano la Digital Transformation aumentando l'agilità e il controllo dell'IT.
NIST	National Institute of Standards and Technology
EC	curva ellittica
RSA	Rivest–Shamir–Adleman
AAA	Authentication, Authorization and Accounting, ossia autenticazione, autorizzazione e contabilità
CCM	Cloud Control Matrix
DSA	Digital Signature Algorithm, algoritmo della firma digitale
SSO	Single Sign-On
OpEx	Spese operative
GDPR	General Data Protection Regulation, il regolamento generale sulla protezione dei dati dell'UE
CCPA	California Consumer Privacy Act
AICPA	American Institute of Certified Public Accountants
PCI DSS	Payment Card Industry Data Security Standard
CSP	Cloud Service Provider, fornitore di servizi di cloud

AVVISO
Il presente white paper è solo a scopo informativo e rappresenta le attuali pratiche Dell soggette a modifiche senza preavviso. Non crea alcun impegno o garanzia da parte di Dell e delle sue affiliate, dei suoi fornitori o licenziatari. Le responsabilità di Dell nei confronti dei propri clienti sono gestite da contratti Dell che non fanno parte di, né sono modificati dal presente white paper. I clienti sono gli unici responsabili della valutazione indipendente delle informazioni fornite nel white paper in questione.