

La ridefinizione di resilienza nell'Edge Computing

White Paper 256

Revisione 0

di Kevin Brown e Wendy Torell

Riepilogo

L'uso del cloud computing nelle grosse imprese si sta diffondendo sempre più rapidamente. L'aumento della dipendenza da applicazioni basate sul cloud impone alle imprese una ridefinizione del livello di ridondanza delle apparecchiature dell'infrastruttura fisica (alimentazione, raffreddamento, rete) che restano all'interno in strutture periferiche ("edge"). Questo white paper descrive e valuta criticamente gli attuali standard adottati per l'infrastruttura fisica, propone un metodo di analisi dei requisiti di resilienza e descrive gli standard ottimali che garantiscono ai dipendenti una connessione ininterrotta alle applicazioni critiche.

Introduzione

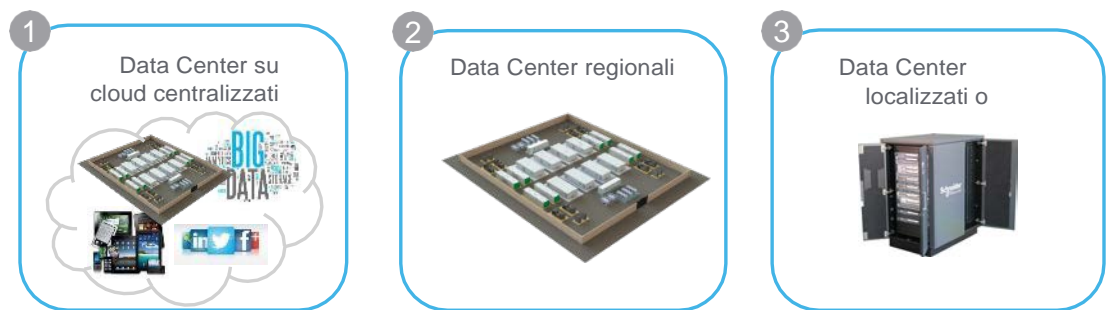
La continua crescita dell'IoT (Internet of Things), l'aumento del volume di traffico digitale e l'adozione sempre più diffusa di applicazioni basate sul cloud sono tendenze tecnologiche che stanno rimodellando il panorama dei Data Center.

Migliaia di applicazioni aziendali critiche che prima risiedevano nei Data Center interni ora sono ospitate in Data Center su cloud di vaste o vastissime proporzioni. Non tutte le applicazioni sono passate sul cloud per vari motivi, ad esempio le normative, la cultura aziendale, le applicazioni proprietarie e la latenza.

Di conseguenza, gli ambienti dei Data Center possono essere definiti "ibridi", ossia: 1) Data Center su cloud centralizzati, 2) Data Center regionali di medie-grosse dimensioni, 3) Data Center interni, localizzati, di dimensioni inferiori. Si veda la Figura 1. Ciò che era un Data Center interno da 1 MW in una filiale aziendale ora può essere costituito da un paio di rack di apparecchiature informatiche che eseguono applicazioni critiche e/o forniscono la connettività di rete al cloud. La riduzione dell'ingombro e della capacità del Data Center interno, però, non dovrebbe comportare anche una riduzione della criticità, dal momento in che in alcuni casi le apparecchiature che rimangono all'interno acquisiscono un'importanza ancora maggiore.

Questo white paper descrive i comuni standard nei tre tipi di Data Center indicati e le nuove aspettative di disponibilità, propone un metodo per la valutazione dei requisiti di resilienza dei Data Center periferici (interni) per garantire l'adempimento degli obiettivi aziendali e descrive gli standard ottimali per l'implementazione di micro Data Center periferici.

Figura 1
I Data Center possono essere di tre tipi. Questo white paper è dedicato ai Data Center periferici.



Tipi di Data Center

Originariamente, il cloud centralizzato fu concepito per determinati tipi di applicazioni, ossia

i.e. posta elettronica, libri paga e social media, le cui tempistiche non rappresentavano una priorità fondamentale. Mano a mano che nel cloud sono state trasferite applicazioni critiche, la latenza, le limitazioni della larghezza di banda, la sicurezza e altri requisiti normativi sono diventati veri e propri problemi da risolvere. Si pensi all'applicazione per le automobili a guida autonoma, la quale richiede un'enorme mole di calcoli e non tollera la latenza, altrimenti può causare incidenti. Altre applicazioni vitali sono quelle mediche: sensori che acquisiscono dati sui pazienti o strumenti chirurgici che devono garantire la massima reattività durante gli interventi. La necessità di avvicinare il calcolo al punto di fruizione è diventata evidente.

La distribuzione di contenuti ad elevata larghezza di banda è un'altra applicazione che si avvantaggia dell'avvicinamento al punto di fruizione, allo scopo di migliorare lo streaming e ridurre i costi della larghezza di banda.

Molte aziende sono propense oppure obbligate a gestire internamente alcune applicazioni aziendali, allo scopo di migliorare il controllo e adempiere a requisiti normativi e disponibilità. A volte queste applicazioni sono replicate in maniera ridondante sul cloud.

Il white paper 226 di Schneider Electric, [Fattori di scelta e vantaggi dell'edge computing](#), spiega più dettagliatamente queste applicazioni da cui nasce un ecosistema di Data Center più regionali e localizzati. Questa sezione descrive ognuno di questi tipi di Data Center e i tipici standard dell'infrastruttura fisica implementati in questi Data Center.

Data Center centralizzato

I grossi Data Center centralizzati (da parecchi megawatt), sia nel cloud sia di proprietà delle aziende, generalmente sono ritenuti fondamentali, per cui sono progettati ottimizzandone la disponibilità. Per garantire la continuità di questi Data Center, sono stati implementati standard ottimali che nel corso degli anni si sono ampiamente consolidati. Le strutture e il personale informatico gestiscono queste sedi perseguendo un unico obiettivo ineludibile: la continuità 24/7 di tutti i sistemi. Generalmente, queste sedi sono progettate e talvolta certificate in base agli standard Tier 3 o Tier 4 dell'Uptime Institute. I fornitori di cloud e colocation spesso pubblicizzano queste caratteristiche progettuali di alta disponibilità per incentivare le vendite dei loro Data Center.

Standard ottimali comuni:

- **Ridondanza dei sistemi critici:** gli impianti di alimentazione e raffreddamento critici spesso sono progettati con ridondanza 2N per evitare interruzioni causate da guasti o interventi di manutenzione.
- **Sicurezza fisica di alto livello:** soluzioni come i sensori biometrici ai varchi, i varchi di ingresso a bussola, la videosorveglianza e le guardie giurate 24/7 sono ampiamente diffuse per garantire la sicurezza dei sistemi e limitare l'accesso solo al personale autorizzato.
- **File e rack organizzati:** oltre al blocco dei rack, i cavi di alimentazione e di rete sono organizzati per ridurre il rischio di errori umani (ad es. il rischio che vengano tirati i cavi sbagliati o che vengano collegati due alimentatori allo stesso circuito elettrico); viene pianificata, inoltre, la distribuzione dell'aria e vengono utilizzati vari dispositivi (ad es. strisce a spazzola e pannelli ciechi) per ridurre i punti caldi.
- **Monitoraggio:** per la gestione, il controllo e l'ottimizzazione di tutti i sistemi del Data Center vengono implementati sensori e misuratori per sistemi BMS (Building Management Systems) e DCIM (Data Center Infrastructure Management).

Figura 2
Standard sicurezza comuni nei Data Center centralizzati su cloud e in colocation

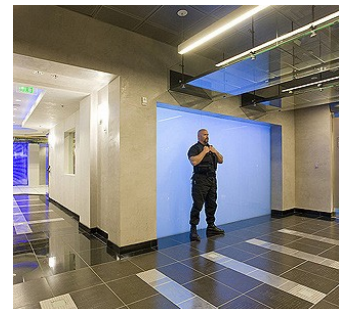
La Figura 2 illustra alcuni standard di sicurezza comuni in questi Data Center:



Sensori biometrici



Varchi di ingresso a bussola



Guardie giurate

Data Center regionali

I Data Center regionali sono più vicini ai punti di fruizione (ossia dove i dati vengono creati e utilizzati) e sono di dimensioni inferiori rispetto a quelli centralizzati. Come già detto, questi Data Center hanno la funzione di avvicinare ai punti di fruizione le applicazioni sensibili alla latenza e alla larghezza di banda e generalmente occupano una posizione strategica per la gestione di elevati volumi di dati. Questi Data Center possono essere ritenuti una sorta di "ponte" tra i Data Center centrali e quelli ubicati all'interno delle aziende.

Analogamente ai grossi Data Center centralizzati, i Data Center regionali generalmente sono progettati per ottimizzare la sicurezza e la disponibilità, per cui i progetti Tier 3 non sono rari in questo tipo di strutture. A volte per questi usi vengono scelti e implementati approcci progettuali prefabbricati, sfruttando anche i progetti di riferimento come punto di partenza (v. esempio in Figura 3).

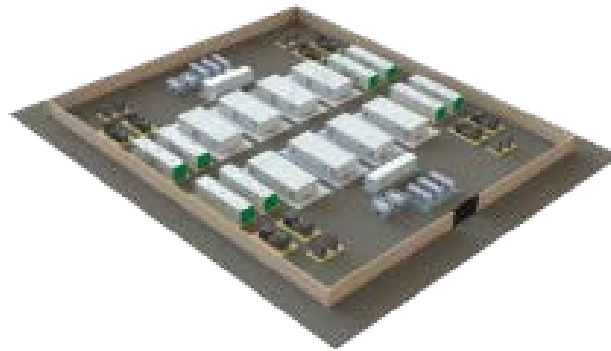


Figura 3
Esempio di progetto di riferimento come punto di partenza per la realizzazione di Data Center regionali o centralizzati

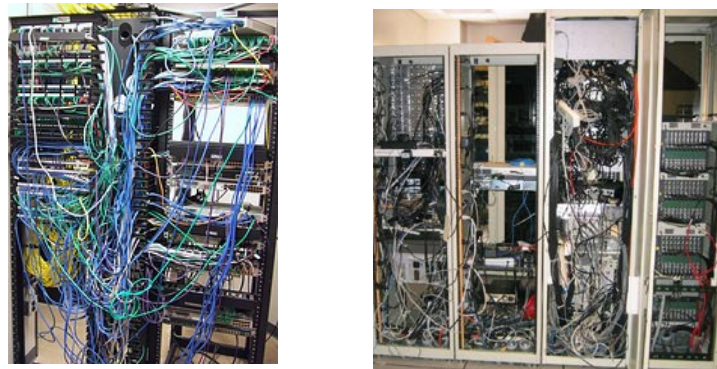
Data Center localizzato

Un Data Center localizzato è quello gestito in colocation dagli utenti. Per descrivere questi Data Center si utilizzano vari termini, ad esempio "interni", "on-premise" o "micro". La potenza dei Data Center localizzati può variare da 1-2 MW fino ad appena 10-20 kW. Dal momento che sono sempre di più le imprese che scelgono l'esternalizzazione delle applicazioni aziendali affidandosi a fornitori di cloud e colocation, le dimensioni di questi Data Center tendono a restringersi fino a un paio di rack sistemati in armadi o piccoli ambienti.

Per molti di questi moderni Data Center sottodimensionati i progetti sono Tier 1, senza particolare attenzione alla ridondanza o alla disponibilità. Non è infrequente constatare vari problemi di questi piccoli Data Center interni:

- Assenza di sicurezza: gli ambienti spesso non sono protetti e i rack vengono lasciati aperti (senza sportelli).
- Assenza di organizzazione dei rack: la gestione dei cavi non è curata, per cui i cavi si aggrovigliano, ostacolano il flusso d'aria nei rack e aumentano gli errori umani in occasione di aggiunte, spostamenti e cambiamenti. Si veda la Figura 4.
- Assenza di ridondanza: i sistemi di alimentazione (UPS, distribuzione) spesso sono 1N, riducendo la disponibilità e la continuità dei sistemi durante la manutenzione.
- Assenza di raffreddamento dedicato: il raffreddamento di questi piccoli ambienti e armadi spesso è affidato unicamente ai condizionatori presenti nell'edificio, per cui le apparecchiature sono soggette a surriscaldamenti.
- Assenza di monitoraggio DCIM: questi ambienti spesso non vengono affatto gestiti, per cui non esiste una gestione delle risorse e della continuità tramite strumenti software o personale dedicato.

Figura 4 Esempi di piccoli Data Center interni dove i cavi non vengono gestiti e la sicurezza è scarsa.



Le sedi spesso finiscono per assomigliare a questi esempi, dal momento che le aziende passano al cloud o alla colocation, questi piccoli rack che restano all'interno sono poco considerati e tutta l'attenzione è concentrata sulla disponibilità dei Data Center di maggiori dimensioni. Questa logica, tuttavia, è fallace in quanto i rack che restano all'interno acquisiscono un'importanza ancora maggiore.

Si consideri le risorse che generalmente rimangono interne: 1) applicazioni critiche e proprietarie; 2) connettività di rete al cloud. Quali sono le implicazioni sulla produttività se non è possibile accedere alle applicazioni? Presupponendo che in una determinata sede rimanga lo stesso numero di persone, la disponibilità di appena un paio di rack interni ne aumenta la singola importanza, dal momento che apparecchiature locali sono fondamentali per la connettività alle applicazioni aziendali quotidiane; visto l'aumento dell'uso del cloud, quindi, è evidente che se il punto di accesso è fuori uso i dipendenti non possono lavorare.

Tutto ciò suggerisce la necessità di un cambiamento nella modalità di progettazione di questi piccoli Data Center interni. Non è più possibile concentrarsi esclusivamente sui Data Center centrali o regionali, ma occorre senza dubbio considerare adeguatamente le sedi localizzate perché attualmente rappresentano gli anelli deboli. Nel prosieguo di questo white paper verranno descritti gli standard ottimali da implementare in queste sedi per garantire la continuità della connettività e della produttività.

Una metrica della disponibilità più comprensibile

Considerando questi ambienti ibridi interconnessi, occorre rispondere a una domanda importante: è necessario riconsiderare i problemi di criticità e ridondanza? Gli strumenti utilizzati attualmente nel settore dei Data Center sono finalizzati a garantire la massima solidità di un singolo Data Center. I livelli Tier facilitano la progettazione di una singola sede per ottenere un determinato livello di disponibilità (il numero di 9). Per guasto generalmente si intende la rottura di un'apparecchiatura informatica in un determinato Data Center.

Gli strumenti e le metriche non contemplano la dipendenza da più Data Center, dall'elevato numero di utenti interessati dal guasto, dalla criticità delle funzioni aziendali interessate o dal failover di un'applicazione (software). Per tale motivo, è ovvio che occorre fare un passo avanti.

Il cambiamento delle aspettative in termini di disponibilità

Le aspettative dei dipendenti attualmente sono diverse da quelle delle generazioni precedenti. Siccome la forza lavoro invecchia e la percentuale di millennial cresce, le aspettative sono molto diverse. Questa generazione è cresciuta fruendo costantemente di dispositivi e sistemi informatici connessi e pretende che funzionino continuamente. La tolleranza ai problemi del servizio è molto bassa. Per questa generazione, la tecnologia è importante sia per il lavoro

che per la vita quotidiana; l'82% dei millennial, infatti, ritiene che il livello tecnologico del luogo di lavoro sarà un fattore discriminante nella scelta di una nuova occupazione.¹

Se questa tendenza continuerà, sarà indispensabile considerare altri sistemi olistici che valutino la resilienza dei Data Center e che forniscano la visibilità necessaria per modificare le strategie progettuali. "Non si può gestire ciò che non si misura", per cui le metriche sulla resilienza devono evolversi per adattarsi ai moderni requisiti delle aziende.

Un approccio diverso

Considerando la disponibilità da un punto di vista diverso, anche le iniziative cambiano. La Tabella 1 illustra il confronto tra il vecchio paradigma odierno e il nuovo paradigma alla base di iniziative indispensabili.

Tabella
1
Un nuovo paradigma per i guasti dei Data Center

Vecchio paradigma	Nuovo paradigma
Incentrato sul Data Center centralizzato	Incentrato su un ambiente ibrido
Un guasto è tale se coinvolge un'apparecchiatura informatica nel rack.	Un guasto è tale se coinvolge l'esperienza degli utenti.
Non riguarda sedi remote né persone o funzioni.	L'impatto sulla criticità dipende dal numero di dipendenti interessati e dal loro lavoro.

Si pensi a un'azienda elettrica e al problema della disponibilità: non basta considerare solo gli impianti che producono l'energia e le linee in alta tensione (i "Data Center centralizzati"), ma occorre valutare anche le diramazioni, i trasformatori su palo e così via, per cui l'efficienza in definitiva viene misurata in base all'energia fornita ai clienti (i "Data Center periferici"). Il settore dei Data Center deve considerare questo modello di servizio pubblico in cui le strutture periferiche hanno un'importanza pari o anche maggiore rispetto ai Data Center centralizzati.

La disponibilità di due sistemi in serie, vale a dire la dipendenza dalla disponibilità di entrambi, può essere calcolata:

$$\text{Disponibilità}_{\text{ sistema }} = \text{Disponibilità}_1 \times \text{Disponibilità}_2$$

Si può cominciare valutando un singolo utente la cui disponibilità e produttività dipende dal Data Center locale interno e dal Data Center centrale. Per calcolare la disponibilità dei Data Center dal punto di vista di questo utente, la formula precedente può essere utile. Ad esempio, se la disponibilità del Data Center centrale è pari al 99,98% (Data Center Tier 3 con 1,6 ore di interruzioni) e la disponibilità del Data Center interno è pari al 99,67% (Data Center Tier 1 con 28,8 ore di interruzioni), le interruzioni totali per tale utente saranno $99,98\% \times 99,67\% = 99,65\%$ (30,7 ore di interruzioni).

Considerando ora il punto di vista di un responsabile informatico, come si può valutare l'impatto dell'intero ecosistema di Data Center sulla connettività e sulla produttività? Non tutti i Data Center dipendono dall'operatività dagli altri Data Center per garantire

¹ <http://www.dell.com/learn/us/en/uscorp1/press-releases/2016-07-18-future-workforce-study-provides-key-insights> (ultimo accesso 31/10/2016)

l'operatività dei dipendenti. Ad esempio, una filiale a Londra non dipende da una filiale in California, ma entrambe possono dipendere dal Data Center centrale di New York.

Non tutti i Data Center hanno lo stesso impatto sull'efficienza. Uno dei fattori di impatto è dato dal numero di dipendenti; un Data Center interno con 1000 dipendenti, ad esempio, sarà più critico di uno con 10 dipendenti. La Tabella 2 riporta il numero di ore lavorative perdute in un esempio di ecosistema con un Data Center centrale Tier 3 e dieci Data Center localizzati Tier 1, ognuno con 100 dipendenti. Dalla tabella emerge chiaramente che l'entità totale delle interruzioni dipende dai Data Center periferici Tier 1 e maggiore è il numero di sedi periferiche, minore è il numero di ore senza interruzioni in altre sedi.

Tabella 2

Disponibilità di dieci Data Center periferici e un Data Center centrale, con la contabilizzazione del relativo impatto

Disponibilità Data Cente						
Descrizione	Disponibilità	Interruzioni interessate		Totale persone interessate		Ore lavorative annue perdute a causa delle interruzioni
		(ore)	N. sedi	N. persone/se de	interessate	
Data Center periferici Tier 1	99,67%	28,82	10	100	1.000	28.820
Data Center centrale Tier 3	99,98%	1,58	1	0	1.000	1.580
Totale ore lavorative annue perdute						30,400
Disponibilità						99,65%

La tabella precedente illustra uno scenario semplice con 2 livelli di Data Center e 1000 persone interessate da entrambi i livelli, ma quando aumenta il numero di Data Center, ognuno con diversi livelli di disponibilità e numero di persone interessate, il calcolo non è così semplice. Il risultato, inoltre, è incompleto perché non tiene conto del livello di importanza delle singole sedi; ad esempio, una sede dedicata all'assistenza clienti o alla produzione probabilmente è più importante di una sede occupata dagli amministratori che possono lavorare in remoto in caso di perdita della rete.

Un approccio ottimale per valutare olisticamente tutte le sedi consiste nell'indicazione di un punteggio, come l'esempio illustrato nella Tabella 3. Queste risorse semplificano ai responsabili informatici e dei Data Center l'identificazione delle sedi prioritarie su cui concentrare i miglioramenti. Il punteggio esprime la disponibilità e le interruzioni associate di ogni sede in un ambiente di Data Center ibrido (misura ideale), ma soprattutto il livello di criticità di ogni sede. Ulteriori informazioni sui punteggi di criticità² sono fornite di lato. Nel caso dei Data Center, la gravità delle conseguenze di un guasto in ogni sede si basa su alcuni fattori:

- Numero di persone interessate
- Funzioni

Comunemente si usa una scala da 1 a 5, dove 1 esprime l'impatto minimo in caso di interruzione e 5 si riferisce all'impatto massimo. Anche se la classificazione è qualitativa, questo sistema fornisce un approccio sistematico all'analisi di tutte le sedi nell'ecosistema dei Data Center. Tenere presente che i valori utilizzati qui vengono ricavati in vari modi dalle aziende; ciò che conta è la classificazione di tutte le sedi adoperando un metodo omogeneo.

² <http://www.weibull.com/hotwire/issue46/relbasics46.htm> (ultimo accesso 31/10/2016)

Analisi delle criticità

L'analisi qualitativa delle criticità, nota anche come FMECA (Failure Modes, Effects and Criticality Analysis) è un metodo ampiamente collaudato per valutare i rischi e definire le priorità degli interventi correttivi, ed è ben documentata nelle pubblicazioni tecniche inerenti all'affidabilità. Questa analisi include una classificazione della gravità delle conseguenze di un guasto con un numero RPN (Risk Priority Number) che descrive la priorità dei rischi. Il numero RPN si basa su 3 fattori: 1) gravità del guasto, 2) probabilità e 3) rilevamento².

In questo esempio, un ipotetico ecosistema conta cinque Data Center in cui le interruzioni annuali di ogni Data Center vengono moltiplicate in base al punteggio che definisce la "gravità delle conseguenze di un guasto" per ottenere il punteggio pesato.

In tal modo, basta ordinare le sedi in base al punteggio per scoprire quali sedi hanno più bisogno di un miglioramento del Data Center. È possibile anche calcolare la percentuale del punteggio per ogni sede (come indicato nell'esempio con l'"Impatto della sede sul punteggio"); a questo punto, le sedi con la percentuale più alta rappresentano quelle con la priorità più elevata.

Tabella 3

Esempio di punteggio che semplifica l'assegnazione delle priorità ai miglioramenti dei Data Center

Punteggio dei Data						
Sed	Nome	Disponibilità	annua Interruzioni (ore)	Gravità delle conseguenze di un guasto (1-5)*	Punteggio (pesato per la criticità)	Impatto della sede sul punteggio
1		99,98%	1,752	2	3,5	0,4%
2		99,20%	70,08	4	280,3	30,0%
3		99,60%	35,04	1	35,0	3,7%
4		98,60%	122,64	5	613,2	65,5%
5		99,98%	1,752	2	3,5	0,4%
Punteggio totale della criticità:					935,6	

Questo approccio è di tipo ripetitivo. In questo esempio, migliorando la disponibilità della sede 4, una nuova sede salirà di posizione tra le più importanti. Attuando questo ciclo di miglioramento continuo, verranno migliorate le sedi con l'impatto maggiore.

Con un metodo che indica correttamente la disponibilità, appare chiaro dove migliorare il progetto per ottimizzare la produttività e il ritorno degli investimenti. Nella maggior parte dei casi, questo esercizio dimostrerà che il funzionamento dei Data Center periferici, la cui disponibilità spesso è inferiore, si ripercuote in maniera maggiore sull'efficienza operativa.

I migliori standard nelle strutture periferiche

Le metriche e i metodi corretti evidenziano la necessità di rivalutare il progetto dei sistemi nei Data Center periferici. Come già detto, i tipici standard progettuali per le strutture periferiche sono inadeguati, vista la funzione indispensabile di queste sedi. Per migliorare occorre concentrarsi su determinate problematiche:

- Sicurezza fisica
- Standard operativi, monitoraggio (DCIM), monitoraggio remoto
- Alimentazione e raffreddamento ridondanti
- Reti a doppia connettività

Le sezioni seguenti illustrano i principali standard ottimali da implementare nelle strutture periferiche. Il white paper 174 di Schneider Electric, [Scelte pratiche per la distribuzione di piccole sale server e micro Data Center](#), descrive con maggiore dettaglio i metodi per apportare reali miglioramenti all'alimentazione, al raffreddamento, ai rack, alla sicurezza fisica e al monitoraggio nelle piccole sale server e nelle filiali con carico informatico fino a 10 kW.

Sicurezza ambientale

Alcuni Data Center locali spesso sono collocati in ambienti altamente accessibili, ad esempio spazi per uffici condivisi, e spesso non è previsto uno spazio dedicato ai rack, che rimangono aperti senza misure di sicurezza. Queste situazioni pongono seri rischi per la sicurezza, sia per l'intervento di malintenzionati sia per il rischio di incidenti.

Standard ottimali per ridurre tali rischi:

- Spostare le apparecchiature in ambienti o armadi chiusi a chiave.
- Predisporre un sistema di controllo accessi con tecnologie biometriche o altri metodi.
- In ambienti difficili, proteggere le apparecchiature in armadi a prova di incendi, allagamenti, umidità, atti vandalici e campi elettromagnetici.
- Implementare il monitoraggio 24/7 della sicurezza e dell'ambiente e la videosorveglianza.

Figura 5
Esempi di micro Data Center sviluppati da Schneider Electric

La Figura 5 illustra alcuni esempi di armadi protetti, che spesso sono prefabbricati e includono tutta l'infrastruttura di supporto necessaria.



Gestione dei Data Center

Il protocollo di gestione ed esercizio (ovvero esista) spesso varia da una sede periferica all'altra, per cui la gestione di centinaia o migliaia di sedi periferiche può essere lunga e costosa, e la disponibilità nelle sedi principali dipende da sistemi condivisi nella struttura, ad es. generatori, quadri elettrici e chiller.

Standard ottimali per ridurre tali rischi:

- Effettuare un inventario dei sistemi e dei metodi di gestione esistenti.
- Predisporre il consolidamento in una piattaforma di monitoraggio centralizzata per tutte le risorse nelle varie sedi.
- Implementare il monitoraggio remoto quando le risorse sono vincolate. Per ulteriori informazioni sull'importanza del monitoraggio per ridurre le interruzioni, consultare il white paper 237, [L'utilità del monitoraggio remoto digitale per la gestione e la manutenzione dei Data Center](#).

Alimentazione e raffreddamento

Gli impianti di alimentazione e raffreddamento (ad es. UPS e climatizzatori) nelle sedi periferiche generalmente sono distribuiti senza alcuna ridondanza, per cui si creano singoli punti di guasto con l'impossibilità di gestire simultaneamente gli impianti; in alcuni casi non esiste neppure un impianto di raffreddamento dedicato, per cui le apparecchiature si surriscaldano. Gli impianti spesso sono condivisi con il resto dell'edificio, per cui la disponibilità del Data Center periferico dipende dalla disponibilità di queste risorse condivise.

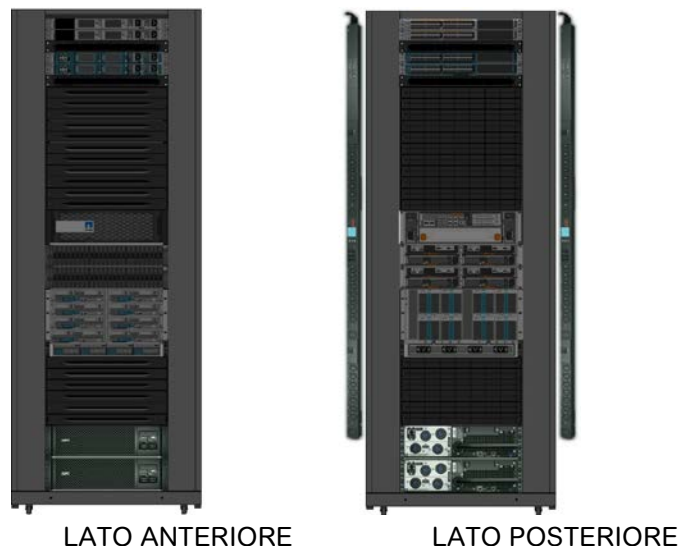
Standard ottimali per ridurre tali rischi:

- Misurare la temperatura e l'umidità per appurare il livello di raffreddamento necessario (flusso d'aria passivo, attivo o raffreddamento dedicato).
- Considerare percorsi di alimentazione ridondanti per la manutenzione simultanea nelle sedi critiche.
- Accertarsi che i circuiti critici siano collegati a un generatore di emergenza.

Figura 6

Esempio di micro Data Center con un solo rack che incorpora la ridondanza

La Figura 6 illustra un esempio di micro Data Center Tier 3 costituito da una soluzione integrata prefabbricata in un unico armadio 42U con UPS e distribuzione dell'alimentazione ridondanti.



Connettività di rete

Come già detto, la connettività al cloud è fondamentale per le sedi periferiche, anche se a volte è un singolo fornitore di servizi Internet a fornire tale connessione. Ciò rappresenta un singolo punto di guasto. Anche il caos dei cavi negli armadi di rete contribuisce agli errori umani.

Standard ottimali per ridurre tali rischi:

- Valutare l'opportunità di aggiungere un secondo fornitore di rete per le sedi critiche.
- Organizzare i cavi di rete con appositi dispositivi di gestione (canaline, sistemi di instradamento, fascette ecc.).
- Etichettare con una codifica a colori le linee di rete per evitare errori umani.

Conclusioni

L'adozione del cloud sta indirizzando un numero sempre maggiore di imprese verso ambienti ibridi con Data Center basati sul cloud e Data Center interni (periferici). Anche se le apparecchiature che rimangono all'interno delle sedi sono poco ingombranti, possono rivestire un'importanza ancora maggiore per i seguenti motivi:

- Con l'aumento della migrazione delle applicazioni sul cloud, la connettività al cloud è fondamentale per la continuità.
- Sono sempre di più i dipendenti che chiedono una connettività ininterrotta e non possono tollerare interruzioni.

In buona parte, però, i Data Center periferici attuali presentano vari problemi progettuali che causano costose interruzioni. Per ottimizzare il ritorno degli investimenti, per gli ambienti ibridi è indispensabile adottare un approccio sintomatico alla valutazione della disponibilità di tutti i Data Center.

Il metodo di valutazione tramite punteggi sopra illustrato consente ai dirigenti di ottenere un quadro olistico dell'ambiente, con la quantificazione del numero di persone e funzioni aziendali di ogni Data Center, e identifica le sedi che richiedono investimenti più urgenti.

I micro Data Center prefabbricati rappresentano una soluzione semplice per ottenere un ambiente periferico sicuro e altamente disponibile. I migliori standard, ad esempio gli UPS ridondanti, l'organizzazione sicura dei rack, un'adeguata gestione dei cavi e dei flussi d'aria, il monitoraggio remoto e la doppia connettività di rete, garantiscono l'adempimento dei requisiti di disponibilità nelle sedi più critiche.

Informazioni sugli autori

Kevin Brown è Direttore Tecnico della Divisione Data Center di Schneider Electric. È laureato in ingegneria meccanica alla Cornell University. Prima di assumere questo ruolo in Schneider Electric, è stato Direttore dello Sviluppo Marketing presso Airxchange, azienda produttrice di unità e componenti di ventilazione per il recupero energetico nel settore HVAC. Prima di entrare in Airxchange, ha ricoperto svariati ruoli gestionali in Schneider Electric, tra cui Direttore del Gruppo di Sviluppo Software e Senior VP del settore Soluzioni per Data Center.

Wendy Torell è Senior Research Analyst presso il Data Center Science Center di Schneider Electric. Nel ruolo che ricopre si occupa di ricerche sui migliori standard di progettazione e gestione dei Data Center, pubblica white paper e articoli, sviluppa tool TradeOff finalizzati all'ottimizzazione della disponibilità, dell'efficienza e dei costi dei Data Center dei clienti, e fornisce consulenze su standard progettuali e approcci scientifici alla disponibilità per l'attuazione degli obiettivi di rendimento dei Data Center. È laureata in ingegneria meccanica presso l'Union College di Schenectady (NY) ed è titolare di un Master in Business Administration ottenuto presso l'University of Rhode Island. Esercita la professione di ingegnere affidabilista certificato ASQ.



[Vantaggi dei micro Data Center in termini di costo](#)

White paper 223



[I benefici dell'edge computing](#)

White paper 226



[L'utilità del monitoraggio remoto digitale per la gestione e la manutenzione dei Data Center](#)

White paper 237



[Sfoggia tutti i white paper](#)

whitepapers.apc.com



[Sfoggia tutti i TradeOff Tools™](#)

tools.apc.com



Contatti

Per pareri e commenti sul contenuto di questo white paper:

Data Center Science Center
dcsc@schneider-electric.com

Per formulare richieste specifiche sulla progettazione del Data Center:

Rivolgersi a un rappresentante Schneider Electric all'indirizzo
www.apc.com/support/contact/index.cfm