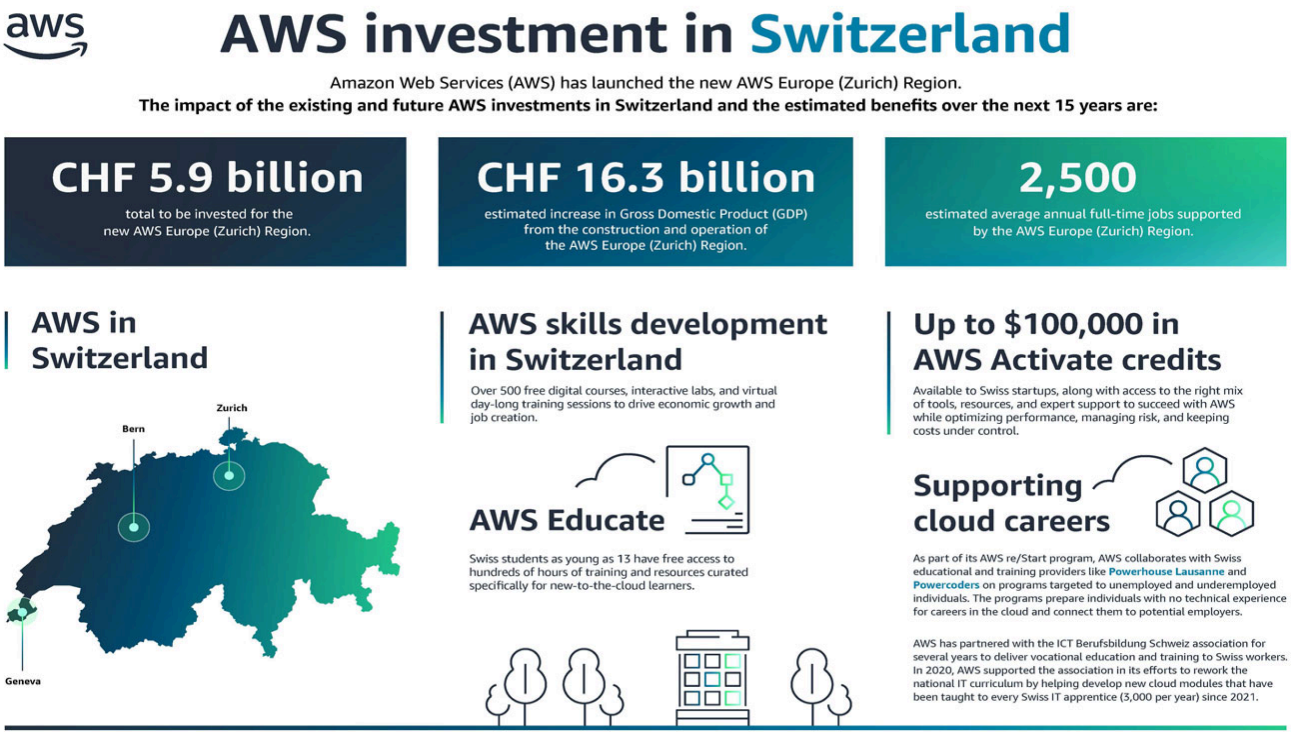
Overview infrastruttura tecnologica per l'erogazione dei servizi

AWS - Amazon Web Services (Cloud)

Svizzera (Zurigo)



La Regione AWS Europa (Zurigo) è diventata operativa il 9 novembre 2022, eroga servizi a sviluppatori, startup, imprenditori e imprese, nonché organizzazioni governative, educative e senza scopo di lucro, per eseguire le proprie applicazioni e servire gli utenti finali dai data center situati in Svizzera, utilizzando tecnologie AWS avanzate per promuovere l'innovazione.

APPING S.r.l.
Sede legale: Via Albano Zanella, 23 - 25030 Erbusco (BS)
+39 030 7724111 amministrazione@apping.it www.apping.it
C.F./ Reg.Imp e P. IVA 04118550989 - REA: BS - 589870, Capitale Sociale: € 10.000,00 i.v.
Apping - Startup innovativa - Gruppo smeup

SICUREZZA

La sicurezza in AWS inizia dalla infrastruttura centrale. Personalizzata per il cloud e progettata per rispondere ai requisiti di sicurezza più severi al mondo, l'infrastruttura è monitorata 24/7 per assicurare la riservatezza, l'integrità e la disponibilità dei dati dei clienti finali. Tutti i dati che passano attraverso la rete globale AWS che collega i centri dati e le regioni vengono automaticamente crittografati a livello fisico prima di lasciare le strutture sicure. I clienti AWS possono costruire soluzioni sull'infrastruttura globale più sicura, sapendo che i loro dati rimangono di loro proprietà, e hanno anche la possibilità di crittografarli, spostarli e gestirne la retention.

DISPONIBILITA'

AWS offre la più alta disponibilità di rete di qualsiasi altro provider cloud. Ogni regione è completamente isolata e composta da più zone di disponibilità, che sono partizioni completamente isolate della nostra infrastruttura. Per isolare in modo più efficace ogni problematica e giungere ad una maggiore disponibilità, è possibile suddividere le applicazioni in più zone di disponibilità all'interno della stessa regione. Inoltre, i piani di controllo AWS e la console di gestione AWS sono distribuiti su più regioni e includono endpoint API regionali, progettati per funzionare in sicurezza per almeno 24 ore se isolati dalle funzioni del piano di controllo globale senza richiedere ai clienti di accedere alla regione o ai propri endpoint API tramite reti esterne durante qualsiasi isolamento.

PRESTAZIONI

L'infrastruttura globale di AWS è progettata per le prestazioni. Le regioni AWS offrono bassa latenza, perdite di pacchetti minime e alta qualità della rete. Tutto questo grazie a una rete completa su fibra da 100 GbE in grado di erogare molti terabit di capacità tra regioni. AWS Local Zones e AWS Wavelength, con i provider telco, forniscono prestazioni per le applicazioni che richiedono latenze di pochi millisecondi consegnando un'infrastruttura e dei servizi AWS più vicini agli utenti finali e dispositivi connessi in 5G. Grazie al cloud puoi aumentare velocemente le risorse quando necessario, implementando centinaia o persino migliaia di server in pochi minuti.

APPING S.r.l.
Sede legale: Via Albano Zanella, 23 - 25030 Erbusco (BS)
+39 030 7724111 amministrazione@apping.it www.apping.it

C.F./ Reg.Imp e P. IVA 04118550989 - REA: BS - 589870, Capitale Sociale: € 10.000,00 i.v.
Apping - Startup innovativa - Gruppo smeup

PROGETTAZIONE SICURA

SELEZIONE DEL SITO

Prima di scegliere una sede, AWS esegue valutazioni preliminari di natura ambientale e geografica. AWS sceglie attentamente la sede dei propri data center per limitare il rischio di danni di natura ambientale, come alluvioni, condizioni climatiche estreme e attività sismiche. Le zone di disponibilità sono costruite in modo da essere indipendenti e fisicamente separate le une dalle altre.

RIDONDANZA

I data center sono stati progettati per anticipare e tollerare i guasti mantenendo gli stessi livelli di servizio. In caso di problemi, i processi automatizzati spostano il traffico dall'area colpita. Le applicazioni strategiche sono distribuite seguendo una configurazione N+1 standard; in questo modo, in caso di problemi al data center, viene garantita una capacità sufficiente per permettere al traffico di essere distribuito sui siti rimanenti.

DISPONIBILITÀ

AWS ha identificato i componenti di sistema essenziali, necessari per il mantenimento della disponibilità del sistema e il ripristino del servizio in caso di interruzione. Il backup dei componenti di sistema essenziali viene effettuato in più posizioni isolate note come zone di disponibilità. Ogni zona di disponibilità è stata progettata per operare in modo indipendente e garantire la massima affidabilità. Le zone di disponibilità sono collegate tra loro per consentire ai clienti di progettare applicazioni che gestiscano il failover su diverse zone senza provocare interruzioni. Sistemi altamente resilienti e, di conseguenza, la disponibilità dei servizi sono funzioni integrate nella progettazione. Grazie all'uso di zone di disponibilità e di replica dei dati, i clienti AWS possono raggiungere obiettivi molto ambiziosi in termini di tempi brevi di ripristino e punti di ripristino, oltre a una disponibilità del servizio molto elevata.

PIANIFICAZIONE DELLA CAPACITÀ

AWS monitora costantemente l'utilizzo dei servizi per distribuire un'infrastruttura in grado di garantire impegni e requisiti di disponibilità. AWS offre un modello di pianificazione delle capacità in grado di valutare almeno mensilmente utilizzo e richieste della nostra infrastruttura. Grazie a questo modello è possibile pianificare le richieste future e includere considerazioni sull'elaborazione delle informazioni, sulle telecomunicazioni e sullo storage di registri di controllo.

CONTINUITÀ AZIENDALE E DISASTER RECOVERY

PIANO DI CONTINUITÀ AZIENDALE

Il Piano di continuità aziendale AWS illustra le misure da adottare per evitare e ridurre l'impatto di eventi ambientali. Descrive inoltre nel dettaglio le diverse fasi da seguire prima, durante o dopo il verificarsi di un evento. Il Piano di continuità aziendale prevede dei test, tra cui la simulazione di scenari diversi. Durante e in seguito a tali test, AWS documenta le prestazioni di persone e processi, le azioni correttive e le lezioni apprese, con l'obiettivo di migliorare continuamente la nostra reazione.

RISPOSTA PANDEMICA

Nella propria pianificazione di disaster recovery AWS integra policy e procedure di risposta pandemica per reagire rapidamente a minacce di epidemie di malattie infettive. Le strategie di mitigazione dei rischi prevedono modelli alternativi di gestione del personale per trasferire processi strategici in altre regioni e l'attivazione di un piano di gestione della crisi a supporto di operazioni aziendali critiche. Nei piani pandemici si fa riferimento ad agenzie e normative sanitarie internazionali, nonché a punti di contatto di agenzie internazionali.

APPING S.r.l.
Sede legale: Via Albano Zanella, 23 - 25030 Erbusco (BS)
+39 030 7724111 amministrazione@apping.it www.apping.it

C.F./ Reg.Imp e P. IVA 04118550989 - REA: BS - 589870, Capitale Sociale: € 10.000,00 i.v.
Apping - Startup innovativa - Gruppo smeup

ACCESSO FISICO

ACCESSO AI DATA CENTER DEI DIPENDENTI

AWS offre l'accesso fisico ai data center solo ai dipendenti autorizzati. Tutti i dipendenti che devono accedere al data center devono prima richiedere l'autorizzazione all'accesso e fornire una motivazione aziendale valida. L'autorizzazione di tali richieste viene fatta sulla base del principio del privilegio minimo, secondo cui è necessario specificare il layer del data center a cui il dipendente deve accedere, e ha una durata limitata nel tempo. Le richieste vengono vagliate e approvate da personale autorizzato e l'accesso viene revocato alla sua scadenza. Una volta ottenuta l'autorizzazione, le persone possono accedere solo alle aree consentite.

ACCESSO AL DATA CENTER DI TERZI

L'accesso di terzi deve essere richiesto da dipendenti AWS designati che devono chiedere l'autorizzazione e fornire una motivazione aziendale valida. L'autorizzazione di tali richieste viene fatta sulla base del principio del privilegio minimo, secondo cui è necessario specificare il layer del data center a cui il dipendente deve accedere, e ha una durata limitata nel tempo. Tali richieste vengono approvate da personale autorizzato e l'accesso viene revocato alla sua scadenza. Una volta ottenuta l'autorizzazione, le persone possono accedere solo alle aree consentite. Tutti coloro che sono autorizzati all'accesso con il badge visitatore devono presentare al proprio arrivo un documento d'identità, firmare al momento dell'ingresso ed essere scortati dal personale autorizzato.

ACCESSO AI DATA CENTER AWS GOVCLOUD

L'accesso fisico ai data center nelle specifiche regioni AWS è consentito solo ai dipendenti che hanno dimostrato di essere in possesso della relativa cittadinanza.

MONITORAGGIO E REGISTRAZIONE DI LOG

REVISIONE DEGLI ACCESSI AL DATA CENTER

Gli accessi ai data center vengono regolarmente rivisti. L'accesso è revocato automaticamente quando il profilo di un dipendente viene eliminato dal sistema delle risorse umane di Amazon. Inoltre, quando l'accesso di un dipendente o di un appaltatore scade in base alla richiesta di durata approvata, alla persona viene revocato l'accesso, anche se continua a essere alle dipendenze di Amazon.

LOG DEGLI ACCESSI AI DATA CENTER

Ogni accesso fisico ai data center AWS è registrato, controllato e archiviato. In base alle esigenze, AWS mette in relazione le informazioni ottenute da sistemi logici e fisici di monitoraggio per migliorare la sicurezza.

MONITORAGGIO DEGLI ACCESSI AI DATA CENTER

Monitoriamo i data center grazie ai nostri Security Operations Center (SOC) globali che monitorano, valutano e mettono in pratica programmi di sicurezza. Tali centri offrono un supporto globale 24 ore su 24, 7 giorni su 7, gestendo e monitorando le attività di accesso ai data center e offrendo ai team locali e ad altri team di supporto gli strumenti per reagire a incidenti di sicurezza e valutare, analizzare, consultarsi e fornire una risposta.

APPING S.r.l.
Sede legale: Via Albano Zanella, 23 - 25030 Erbusco (BS)
+39 030 7724111 amministrazione@apping.it www.apping.it

C.F./ Reg.Imp e P. IVA 04118550989 - REA: BS - 589870, Capitale Sociale: € 10.000,00 i.v.
Apping - Startup innovativa - Gruppo smeup

SORVEGLIANZA E RILEVAMENTO

VIDEOCAMERE A CIRCUITO CHIUSO (CCTV)

I punti di accesso fisico alle sale server sono controllati da videocamere a circuito chiuso (CCTV). Le immagini vengono archiviate in base a requisiti legali e di conformità.

PUNTI DI ACCESSO AI DATA CENTER

L'accesso fisico viene controllato presso i punti di ingresso dell'edificio dal personale addetto alla sicurezza che si avvale di sistemi di sorveglianza, di rilevamento delle intrusioni e di altri dispositivi elettronici. Per accedere ai data center il personale autorizzato utilizza meccanismi di autenticazione a più fattori. Gli ingressi alle sale server sono protetti da dispositivi che attivano un allarme e una risposta agli incidenti nel caso in cui la porta rimanga aperta o venga forzata.

RILEVAMENTO DELLE INTRUSIONI

Nel layer dei dati vengono installati sistemi elettronici di rilevamento delle intrusioni che monitorano, rilevano e avvisano automaticamente il personale preposto della presenza di incidenti di sicurezza. I punti di ingresso e di uscita delle sale server sono protetti da dispositivi che richiedono a ogni persona l'autenticazione a più fattori prima di autorizzare l'entrata o l'uscita. Tali dispositivi attivano un allarme nel caso in cui la porta rimanga aperta o venga forzata senza autenticazione. I dispositivi di allarme delle porte sono anche configurati per rilevare i casi in cui una persona entra o esce dal layer di dati senza fornire l'autenticazione a più fattori. Gli allarmi vengono immediatamente inviati ai Security Operations Center di AWS 24 ore su 24, 7 giorni su 7, per registrazione, analisi e risposta immediate.

GESTIONE DEI DISPOSITIVI

GESTIONE ASSET

Gli asset di AWS vengono gestiti centralmente attraverso un sistema di inventario che archivia e traccia proprietario, sede, stato, manutenzione e informazioni descrittive degli asset di proprietà AWS. Nella fase successiva all'acquisizione, gli asset vengono esaminati e tracciati, mentre gli asset sottoposti a manutenzione vengono verificati e monitorati per definirne proprietà, stato e risoluzione.

DISTRUZIONE DEI SUPPORTI MULTIMEDIALI

I dispositivi di storage multimediali utilizzati per archiviare i dati dei clienti sono classificati da AWS come Critici e ad alto impatto e devono essere trattati come tali per tutto il loro ciclo di vita. AWS segue standard rigorosi per l'installazione, l'utilizzo e infine lo smaltimento dei dispositivi quando non sono più utili. Quando un dispositivo di storage è alla fine del proprio ciclo utile di vita, AWS si occupa del suo smaltimento, utilizzando le tecniche illustrate nel dettaglio in NIST 800-88. I supporti multimediali in cui sono archiviati i dati dei clienti continuano a essere sotto il controllo di AWS fino al loro totale smaltimento.

APPING S.r.l.
Sede legale: Via Albano Zanella, 23 - 25030 Erbusco (BS)
+39 030 7724111 amministrazione@apping.it www.apping.it

C.F./ Reg.Imp e P. IVA 04118550989 - REA: BS - 589870, Capitale Sociale: € 10.000,00 i.v.
Apping - Startup innovativa - Gruppo smeup

SISTEMI OPERATIVI DI SUPPORTO

ALIMENTAZIONE

I sistemi di energia elettrica che alimentano i nostri data center sono completamente ridondanti e la loro manutenzione può essere eseguita senza alcun impatto sull'operatività, 24 ore al giorno. AWS garantisce che i propri data center sono dotati di generatori di backup per non interrompere le operazioni di carichi strategici e critici in caso di interruzione dell'energia elettrica presso la struttura.

CLIMA E TEMPERATURA

I data center AWS utilizzano meccanismi di controllo del clima e della temperatura per garantire le condizioni ottimali per server e altro hardware, evitare eventuali surriscaldamenti e ridurre al minimo possibili disservizi. Il personale e i sistemi monitorano e verificano che umidità e temperatura rimangano entro i limiti stabiliti.

RILEVAMENTO ED ESTINZIONE DEL FUOCO

I data center AWS sono dotati di attrezzature automatiche per il rilevamento e l'estinzione delle fiamme. Tali sistemi utilizzano sensori di rilevamento del fumo all'interno di spazi dedicati alla rete, alle infrastrutture e a componenti meccanici. Tali aree sono anche protette da sistemi di estinzione delle fiamme.

RILEVAMENTO DI PERDITE

Per individuare la presenza di perdite, AWS installa presso i propri data center sistemi in grado di rilevare la comparsa di acqua. In questo caso, si attivano meccanismi in grado di rimuovere l'acqua per evitare eventuali danni aggiuntivi.

MANUTENZIONE DELL'INFRASTRUTTURA

MANUTENZIONE DELLE APPARECCHIATURE

AWS monitora le apparecchiature meccaniche e tecniche ed esegue manutenzioni di prevenzione per garantire la continuità dei sistemi presenti all'interno del data center AWS. Personale qualificato esegue e porta a compimento procedure di manutenzione delle apparecchiature secondo un piano definito e documentato.

GESTIONE DELL'AMBIENTE

AWS monitora i sistemi meccanici ed elettrici e le relative attrezzature per consentire un'identificazione immediata delle problematiche. Tale obiettivo viene raggiunto attraverso il continuo utilizzo di strumenti di controllo e di informazioni fornite da sistemi di monitoraggio delle componenti elettriche e di gestione degli edifici. La manutenzione di prevenzione viene eseguita per garantire un'operatività senza interruzioni delle apparecchiature.

GOVERNANCE E RISCHI

GESTIONE CONTINUA DEI RISCHI DEI DATA CENTER

Il Security Operations Center di AWS esegue con regolarità analisi delle minacce e delle vulnerabilità dei data center. Il monitoraggio continuo e la mitigazione di vulnerabilità potenziali vengono eseguite attraverso attività di valutazione dei rischi del data center. Tali operazioni si aggiungono al processo di valutazione dei rischi di livello Enterprise che ha lo scopo di individuare e gestire eventuali rischi del business nella sua interezza. Di questo processo fanno parte anche rischi normativi e ambientali a livello regionale.

ATTESTAZIONE DI SICUREZZA DI TERZI

I test dei data center AWS eseguiti da terze parti e documentati in report garantiscono la corretta implementazione delle misure di sicurezza, in linea con regole condivise, il cui rispetto è necessario per ottenere le relative certificazioni. A seconda del programma di conformità e dei relativi requisiti, revisori esterni possono eseguire test delle procedure di smaltimento di supporti multimediali, analizzare i filmati delle videocamere di sicurezza, osservare ingressi e corridoi del data center, verificare i dispositivi elettronici di controllo degli accessi ed esaminare le apparecchiature.

APPING S.r.l.
Sede legale: Via Albano Zanella, 23 - 25030 Erbusco (BS)
+39 030 7724111 amministrazione@apping.it www.apping.it

C.F./ Reg.Imp e P. IVA 04118550989 - REA: BS - 589870, Capitale Sociale: € 10.000,00 i.v.
Apping - Startup innovativa - Gruppo smeup

Server Plan / IT.net

Italia (Milano e Roma)



DATA CENTER

Tutta l'infrastruttura è realizzata con prodotti di fascia enterprise e tecnologia certificata. Server Plan / IT.net implementa le migliori soluzioni disponibili sul mercato per garantire sempre le prestazioni più alte per velocità, stabilità e sicurezza.

- Sistema di rilevamento anti-intrusione;
- Presidio con agenti di vigilanza 24 ore su 24, per sette giorni su sette;
- Telecamere a circuito chiuso e archiviazione digitale delle riprese;
- Sistemi di rilevamento anti-fumo, anti-incendio e anti-allagamento;
- Alimentazioni multiple e indipendenti con percorsi diversificati;
- Sistema di raffreddamento a doppio circuito di alimentazione;
- 2 Gruppi elettrogeni in ambienti separati;
- Connettività verso internet 100Gbps multi operatore.

Tutti i server dedicati sono collocati presso la web farm di IT.net di Milano e Roma che che prevede l'ospitalità dei server dei clienti in una struttura appositamente attrezzata contraddistinta da massimi livelli di sicurezza, assistenza a ciclo continuo e con capacità di connessione praticamente illimitata.

I Data Center di Milano e Roma sono pensati per soddisfare le necessità di affidabilità, flessibilità e performance dei clienti business e favorire:

- Ridondanza e Uptime garantito secondo gli standard TIER IV/RATING 4 "FAULT TOLLERANT";
- Data Center carrier independent e collegati ai principali carrier nazionali e internazionali;
- Protezione e sicurezza attiva attraverso sistemi di controllo accessi e monitoraggio H.24X365;
- Control Room e personale tecnico e di sicurezza presente H.24×365 in tutti i data center;
- Garanzia del servizio attraverso SLA definiti e procedure di service management (delivery, change, incident management).

Ai locali è ammesso solo personale autorizzato tramite badge e codici numerici a più livelli; tutti i Data Center sono forniti di sistemi di rilevamento attivi H.24×365, telecamere ad archiviazione digitale, sistemi di rilevamento anti fumo, anti incendio e anti allagamento.

APPING S.r.l.
Sede legale: Via Albano Zanella, 23 - 25030 Erbusco (BS)
+39 030 7724111 amministrazione@apping.it www.apping.it

C.F./ Reg.Imp e P. IVA 04118550989 - REA: BS - 589870, Capitale Sociale: € 10.000,00 i.v.
Apping - Startup innovativa - Gruppo smeup

CERTIFICAZIONI

ISO 9001:2015
Sistemi di gestione per la qualità
Servizi di Web Hosting e servizi di registrazione domini, cloud storage, cloud computing, backup e disaster recovery. Servizi di posta e fatturazione elettronica, gestione e conservazione elettronica dei documenti e servizi informatici correlati.

ISO 27001:2013
Sistemi di gestione della sicurezza delle informazioni
Servizi di Web Hosting e servizi di registrazione domini, cloud storage, cloud computing, backup e disaster recovery. Servizi di posta e fatturazione elettronica, gestione e conservazione elettronica dei documenti e servizi informatici correlati.

ISO 14001:2015
Hosting, domini e cloud
Server Plan è conforme allo standard ISO 14001:2015 per i servizi di Web Hosting e servizi di registrazione domini, cloud storage, cloud computing, backup e disaster recovery. Servizi di posta e fatturazione elettronica, gestione e conservazione elettronica dei documenti e servizi informatici correlati.

ISO 27017:2015
Controlli di sicurezza per servizi cloud
I servizi cloud Server Plan hanno ottenuto la certificazione ISO/IEC 27017, che prevede misure di sicurezza rafforzati e controlli aggiuntivi sulle informazioni gestite.

ISO 27018:2019
Protezione dei dati personali nei servizi Public Cloud
I servizi cloud Server Plan hanno ottenuto la certificazione ISO/IEC 27018 (che è un'espansione della Norma ISO 27001) con particolare riferimento alla gestione dei dati personali, ritenuta conforme agli standard internazionali.

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
Servizi IaaS per la PA
Server Plan ha superato i controlli e le verifiche per essere parte del gruppo di fornitori cloud IaaS per la pubblica amministrazione.

ACCREDITAMENTI

Server Plan è tra i pochi provider italiani a poter garantire il controllo diretto delle registrazioni dei domini ed il mantenimento senza alcuna dipendenza da aziende esterne. Grazie all'accreditamento presso Eurid, ICANN, Nic e tutti i Registri che forniscono le nuove estensioni, offriamo ai clienti la totale trasparenza nella registrazione dei domini. Inoltre, siamo presenti sul MEPA per poter fornire i servizi anche alle pubbliche amministrazioni ed iscritti al Registro degli Operatori di Comunicazione disponibile al seguente link http://www.elencopubblico.roc.agcom.it.

I servizi Cloud di Server Plan hanno superato positivamente tutti i test qualitativi previsti e sono ora identificati dal marchio di garanzia del CISPE (Cloud Infrastructure Services Providers in Europe).

APPING S.r.l.
Sede legale: Via Albano Zanella, 23 - 25030 Erbusco (BS)
+39 030 7724111 amministrazione@apping.it www.apping.it

C.F./ Reg.Imp e P. IVA 04118550989 - REA: BS - 589870, Capitale Sociale: € 10.000,00 i.v.
Apping - Startup innovativa - Gruppo smeup

ARCHITETTURA

Affidabilità e performance sono i valori che caratterizzano i Data Center di Roma e Milano, valori che si traducono in infrastrutture e servizi di altissima qualità:

- Ridondanza dei critical system: 2N a fronte di qualsiasi fault;
- Sistemi e distribuzione duplicati e fisicamente separati;
- Manutenzione di tutti i sistemi continua e regolare senza impatti sull'operatività;
- Personale tecnico e addetto alla sicurezza presente nei data center H.24×365.

CONNETTIVITA'

I Data Center sono dotati di collegamenti con i principali carrier nazionali, internazionali ed al Mix attraverso percorsi di accesso alla facility diversificati:

- Velocità di porta Ethernet personalizzabili (FastE, GigE e 10GigE);
- Assegnazione degli indirizzi IPv4 e IPv6;
- Routing Statico e dinamico (BGP);
- DDoS Platform;
- Collegamenti Layer2 e Dark Fiber per raggiungere le sedi del cliente;
- Doppia Carrier Room e doppia Meet-Me-Room;
- Collegamenti diretti alle piattaforme di Public Cloud (AWS, Azure, Google,…);
- SLA definiti in base alle necessità dei clienti.

APPING S.r.l.
Sede legale: Via Albano Zanella, 23 - 25030 Erbusco (BS)
+39 030 7724111 amministrazione@apping.it www.apping.it

C.F./ Reg.Imp e P. IVA 04118550989 - REA: BS - 589870, Capitale Sociale: € 10.000,00 i.v.
Apping - Startup innovativa - Gruppo smeup