Disaster Recovery as a Service

| CARATTERISTICHE DEL SERVIZIO |

Il servizio di **Disaster Recovery as a Service (DRaaS**) permette di proteggere rapidamente la propria infrastruttura Private Cloud Aruba **con un servizio di Disaster Recovery professionale, semplice e sicuro**.

Attraverso un pannello web self-service su connessione sicura, il cliente può autonomamente creare direttive e politiche di Disaster Recovery, selezionando sorgente e destinazione a scelta tra proprie **infrastrutture virtuale VMware on-premise e/o Data Center Aruba abilitati al servizio Private Cloud**. In pochi minuti si possono creare repliche autoconsistenti tra siti remoti ed essere in grado di attivare una procedura di DR perfettamente funzionante.

Durante la definizione di una soluzione di Disaster Recovery, fondamentale importanza rivestono due parametri di misurazione: l'**RPO** e l'**RTO.**

- **RPO (Recovery Point Objective)**: rappresenta il disallineamento massimo che si è disposti a tollerare tra l'ambiente di produzione e ambiente replicato. Descrive quindi a tutti gli effetti la quantità di dati rimasti non sincronizzati in caso di disastro.
- **RTO (Recovery Time Objective)**: rappresenta il tempo necessario al ripristino operativo dei servizi sul sito secondario, a seguito di disastro. Descrive quindi il tempo necessario per completare operativamente la procedura di Disaster Recovery necessaria a rendere i propri servizi nuovamente attivi.

Il meccanismo di replica adottato dal servizio è basato sulla tecnologia Zerto (stato dell'arte nelle soluzioni Disaster Recovery virtualizzate VMware) che ottimizza, deduplica e comprime i dati da salvaguardare garantendo il minimo impatto sulla banda necessaria, minimizzando di conseguenza l'RPO conseguibile. In particolare il sistema riduce l'RPO a valori che mediamente possono variare da pochi secondi a pochi minuti anche su distanze internazionali.
Il basso RTO viene invece garantito da una semplicità di utilizzo estrema, garantita da un semplice pannello web self-service sicuro che, con un solo tasto, permette di dare inizio alla procedura, completamente automatizzata, di ripristino. In pochi secondi il sistema è in grado di effettuare il passaggio dei workload di produzione nel sito di Disaster Recovery.
Per garantire la bontà della soluzione e verificare il funzionamento della propria procedura di Disaster Recovery, **il cliente può lanciare test DR in qualsiasi momento e in modo completamente autonomo**. Il test effettua a tutti gli effetti un tentativo di recupero da disastro, attivando le macchine nel sito secondario, senza andare in alcun modo a interferire con le macchine di produzione, operazione che permette di verificare che le repliche e le procedure di Disaster Recovery funzionino correttamente.
Come per tutti i servizi Aruba è disponibile **l'opzione "Managed"** che **permette di dare in gestione a personale tecnico qualificato Aruba l'intero ciclo di vita della propria soluzione di Disaster Recovery**.

| Assistenza e SLA |

A disposizione dei clienti due differenti canali di assistenza: assistenza telefonica e assistenza via Ticketing System.

Assistenza Tecnica	
Orario	Tempo medio presa in carico segnalazione
365 giorni 24h	15 minuti

Assistenza Amministrativa	
Orario	Tempo medio presa in carico segnalazione
Lun-Ven 8.30-18.00	15 minuti

Uptime garantito: 99,95% su base annuale

Disaster Recovery as a Service

Caratteristiche generali del servizio	Specifiche tecniche
Service Level Agreement - Uptime	99,95% su base annuale relativo alla disponibilità del sistema DRaaS. Il sistema DRaaS è considerato disponibile quando è disponibile il pannello di controllo e la possibilità di effettuare la procedura di ripristino da disastro
Service Level Agreement - Penali	5% del canone mensile del servizio per ogni frazione completa di 15 minuti di downtime oltre i limiti previsti dall'uptime del servizio, fino a un massimo di 300 minuti al mese
Assistenza	Inclusa attraverso il canale ticketing e telefonico
Periodo di fatturazione	Mensile
Durata minima contratto	1 mensilità
Data center su cui è attivabile il servizio	IT1, IT3, CZ1, FR1, PL1 (https://www.cloud.it/infrastrutture.aspx), on premise
Certificazioni disponibili sul servizio	ISO 9001:2015, ISO 27001:2013 (http://www.aruba.it/certificazioni.aspx)

Caratteristiche software	Specifiche tecniche
Software utilizzato per la replica	Zerto (www.zerto.com)
Meccanismo di controllo	Pannello web HTTPS presente in ogni data center abilitato al servizio
WAN Optimization	Attraverso tecniche di deduplica e compressione
Visibilità dell'RPO istantanea	In secondi e minuti
Funzionalità di test DR non distruttivo	Il cliente ha la possibilità di testare il proprio DR in qualunque momento senza impattare sulla produzione
Funzionalità di sincronia inversa	Permette di invertire il flusso di replica per il ritorno da Disaster Recovery a produzione
Numero massimo di VM gestibili	Illimitato
Possibilità di personalizzare le reti di DR	Per ciascuna macchina. Possono essere definite reti diverse per test e reale disastro
Possibilità di personalizzare i datastore di DR	Per ciascuna macchina
Possibilità di replicare infrastrutture on-premise	Sia come sorgente che come destinazione di replica
Opzione "Managed"	Opzionale. Il servizio può essere dato interamente in gestione a personale tecnico qualificato Aruba

Caratteristiche assistenza tecnica	Specifiche tecniche
Ticket inclusi	Illimitati
Telefonate incluse	Illimitate
Orario servizio di assistenza tecnica	24h/24h 365 giorni l'anno con tempo medio di presa in carico di 15 minuti

| Misure tecniche di sicurezza |

Questo capitolo descrive le misure tecniche di sicurezza che Aruba ha implementato per il servizio Disaster Recovery as a Service (DRaaS).

Disponibilità del servizio
Il sistema di erogazione della replica è una componente infrastrutturale presente sullo stesso cluster di calcolo, in grado di replicarne il contenuto verso un altro sito abilitato. Il cluster stesso, configurato in HA, garantisce l'alta affidabilità in caso di guasto. La replica viene mantenuta attiva anche in caso di movimentazione della VM a seguito di bilanciamento del carico o failover del nodo di erogazione e ne viene gestita automaticamente e in modo totalmente trasparente la continuità. Il sistema di pannello necessario a gestire il processo da parte del cliente è protetto da un sistema di virtualizzazione basato su VMware configurato in alta affidabilità.

Ogni sito di erogazione è gestito in modo indipendente. In questo modo, in caso di disastro il cliente può operare in modo self-service sul sito di ripartenza scelto e configurato e applicare le proprie politiche di recupero da disastro.

Integrità del servizio
La persistenza e l'integrità del servizio sono garantite da un sistema storage con dischi aggregati in RAID in grado di resistere al guasto di uno qualunque di essi. Il sistema storage contiene dischi di spare in grado di ricostruire un disco divenuto guasto mantenendo la disponibilità del dato.

Lo storage relativo all'erogazione del sistema di replica viene mantenuto esso stesso replicato in modalità semi-sincrona (RPO ~ 0) su uno storage gemello, anch'esso dotato dello stesso livello di ridondanza dello storage primario su un rack differente all'interno dello stesso data center.

Protezione e accessibilità del servizio
Il dato viene protetto con differenti livelli di sicurezza perimetrale. In particolare:

Il pannello di controllo del sistema DRaaS è protetto da un firewall perimetrale e da credenziali personali (utente e password) e rilasciate al cliente.

- La rete di gestione dell'infrastruttura è segregata e non accessibile da rete pubblica, rimanendo sotto il diretto controllo e supervisione del personale Aruba.
- La connessione tra i siti posti in replica, sia che siano la sede del cliente sia che sia uno dei Data Center Aruba, sono protetti da una connettività privata grazie a una VPN IPSEC cifrata con protocollo AES (instaurata in fase di setup).
- Il pannello di controllo del sistema DRaaS è protetto da un firewall perimetrale e da credenziali personali (utente e password) e rilasciate al cliente ed erogato tramite canale cifrato (HTTPS).