

RAPPORTI TECNICI INGV

L'alta disponibilità (HA) nella
trasmissione e acquisizione del dato
sismico mediante soluzione ibrida
on-premise/cloud



ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA

486

Direttore Responsabile

Daniela VERSACE

Editor in Chief

Milena MORETTI (editorinchief.collane-editoriali@ingv.it)

Editorial Board

Laura ALFONSI (laura.alfonsi@ingv.it)
Raffaele AZZARO (raffaele.azzaro@ingv.it)
Christian BIGNAMI (christian.bignami@ingv.it)
Simona CARANNANTE (simona.carannante@ingv.it)
Viviana CASTELLI (viviana.castelli@ingv.it)
Luca COCCHI (luca.cocchi@ingv.it)
Rosa Anna CORSARO (rosanna.corsaro@ingv.it)
Luigi CUCCI (luigi.cucci@ingv.it)
Lorenzo CUGLIARI (lorenzo.cugliari@ingv.it)
Alessia DI CAPRIO (alessia.dicaprio@ingv.it)
Roberto DI MARTINO (roberto.dimartino@ingv.it)
Domenico DI MAURO (domenico.dimauro@ingv.it)
Domenico DORONZO (domenico.doronzio@ingv.it)
Filippo GRECO (filippo.greco@ingv.it)
Alessandro IAROCCI (alessandro.iarocci@ingv.it)
Marcello LIOTTA (marcello.liotta@ingv.it)
Mario MATTIA (mario.mattia@ingv.it)
Daniele MELINI (daniele.melini@ingv.it)
Anna NARDI (anna.nardi@ingv.it)
Lucia NARDONE (lucia.nardone@ingv.it)
Marco OLIVIERI (marco.olivieri@ingv.it)
Nicola PAGLIUCA (nicola.pagliuca@ingv.it)
Pierangelo ROMANO (pierangelo.romano@ingv.it)
Maurizio SOLDANI (maurizio.soldani@ingv.it)
Sara STOPPONI (sara.stopponi@ingv.it)
Umberto TAMMARO (umberto.tammaro@ingv.it)
Andrea TERTULLIANI (andrea.tertulliani@ingv.it)
Stefano URBINI (stefano.urbini@ingv.it)

Ufficio Editoriale

Francesca DI STEFANO - Coordinatore

Rossella CELI - Segreteria di Redazione

Produzione e grafica-redazionale

Barbara ANGIONI

Massimiliano CASCONI

Rossella CELI

Francesca DI STEFANO

Patrizia PANTANI

REGISTRAZIONE AL TRIBUNALE DI ROMA N.174 | 2014, 23 LUGLIO

© 2014 INGV Istituto Nazionale di Geofisica e Vulcanologia | Rappresentante legale: Carlo DOGLIONI

Sede: Via di Vigna Murata, 605 | Roma



ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA

RAPPORTI TECNICI INGV

L'alta disponibilità (HA) nella trasmissione e acquisizione del dato sismico mediante soluzione ibrida on-premise/cloud

High availability (HA) in the transmission and acquisition of seismic data through an on-premise/cloud hybrid solution

Luigi Falco¹, Ciriaco D'Ambrosio¹, Annamaria Vicari¹, Giovanni Scarpato²

¹INGV | Istituto Nazionale di Geofisica e Vulcanologia, Sezione Irpinia

²INGV | Istituto Nazionale di Geofisica e Vulcanologia, Amministrazione Centrale

Accettato 1 agosto 2024 | Accepted 1 August 2024

Come citare | How to cite L. Falco, D'Ambrosio C., Vicari A., Scarpato G., (2024). L'alta disponibilità (HA) nella trasmissione e acquisizione del dato sismico mediante soluzione ibrida on-premise/cloud. Rapp. Tec. INGV, 486: 1-22, <https://doi.org/10.13127/rpt/486>

In copertina | Cover AdobeStock_876124851

486

INDICE

Riassunto	7
<i>Abstract</i>	<i>7</i>
Introduzione	7
1. Dalla stazione remota al sistema di acquisizione	7
2. Sistemi di trasmissione dati delle stazioni di monitoraggio	8
2.1 Trasmissione 4G/LTE	8
2.2 Indirizzamento IP connettività 4G/LTE	9
2.3 Indirizzamento IP negli altri sistemi di trasmissione dati	10
3. Cosa sono le VPN	10
3.1 I protocolli VPN	10
4. Precedente infrastruttura di acquisizione e trasmissione dati	10
4.1 Limiti di questa infrastruttura e single points of failure	11
5. Nuova infrastruttura di acquisizione dati	12
5.1. Protocollo Wireguard	13
6. Hardware installato presso le stazioni	14
7. Cloud Azure	15
7.1 Servizi principali attivi sul cloud	15
7.2 Virtual Machine RouterOS on Azure	15
7.3 Virtual Machine SeedLink Server	16
7.4 IP pubblico statico	16
7.5 Servizio di archiviazione – Azure Container Storage	16
7.6 Dettaglio delle risorse allocate sul cloud	17
8. Costi	18
9. Conclusioni	18
Bibliografia	19
Sitografia	19

Riassunto

Il documento descrive l'infrastruttura informatica realizzata presso la sezione Irpinia e sul cloud Azure al fine di ridurre i single point of failure dell'attuale sistema di acquisizione e trasmissione dati delle stazioni sismiche e garantire un flusso dati sicuro e ad alta disponibilità verso la sala di sorveglianza sismica di Roma.

Saranno descritti i dispositivi hardware utilizzati presso le stazioni di monitoraggio, i layout di rete implementati, le configurazioni adottate e le risorse allocate sul cloud Azure di Microsoft.

Abstract

The document describes the IT infrastructure created at the Irpinia section and on the Azure cloud to reduce the single points of failure of the current data acquisition and transmission system of the seismic stations and guarantee a secure and highly available data flow towards the room of seismic surveillance of Rome. The hardware devices used at the monitoring stations, the network layouts implemented, the configurations adopted and the resources allocated to the Microsoft Azure cloud will be described.

Keywords Cloud; Alta disponibilità; Dato sismico | High availability; Seismic data

Introduzione

La RSN (Rete Sismica Nazionale) è un'importante infrastruttura dell'INGV che conta centinaia di stazioni di monitoraggio dislocate su tutto il territorio nazionale. L'efficienza del sistema di sorveglianza è fortemente dipendente dalla disponibilità dell'infrastruttura di acquisizione e trasmissione dati. Incrementarne il livello di disponibilità significa generalmente individuare i cosiddetti single point of failure e ridondare quelle componenti la cui singola rottura comprometterebbe l'intero funzionamento del sistema. La ridondanza ovviamente ha un costo e di conseguenza l'alta affidabilità di un servizio sarà tanto maggiore quanto maggiore sarà l'investimento che si intende dedicare. La sezione Irpinia è responsabile di 83 stazioni sismiche dislocate prevalentemente nel sud Italia e che contribuiscono fortemente alla sorveglianza sismica di quest'area. Il contenimento dei costi e la necessità di garantire un adeguato livello di efficienza della rete RSN ha portato a fare le scelte tecniche che saranno descritte in questo rapporto.

1. Dalla stazione remota al sistema di acquisizione

I segnali sismici vengono campionati e digitalizzati dagli strumenti installati presso i siti remoti e tramite differenti sistemi di trasmissione inviati ai centri di acquisizione. Si potrebbe semplificare la struttura del sistema schematizzandola in tre blocchi essenziali (Figura 1): il digitalizzatore, il sistema di trasmissione e il servizio di acquisizione in sede. Immaginando di avere a disposizione un budget infinito e volendo garantire la più alta disponibilità possibile del sistema si dovrebbero almeno duplicare (se non triplicare) i vari blocchi. Avere ad esempio due digitalizzatori sismici/ricevitori GNSS sullo stesso sito di monitoraggio, due sistemi di

trasmissione dati indipendenti (uno satellitare e l'altro UMTS/LTE ad esempio) e due servizi di acquisizione dati dislocati nella stessa sede (ma dotata di almeno due connettività indipendenti) o in luoghi separati. È chiaro che quanto si sta immaginando è altamente dispendioso e resta ovviamente una pura utopia considerando inoltre che su tutto il territorio nazionale ci sono circa 500 stazioni sismiche. È indubbio quindi che vanno fatte scelte tecniche in modo da ottenere un buon livello di servizio e una spesa sostenibile.

Figura 1 Schema a blocchi acquisizione dati sismici.

Figure 1 Seismic data acquisition block diagram.



2. Sistemi di trasmissione dati delle stazioni di monitoraggio

Le stazioni di monitoraggio sismico utilizzano diverse tecnologie di trasmissione dati. Sono attualmente attivi contratti con provider di servizi satellitari in banda KA-SAT, INTERNET, INTRANET, UMTS/LTE, WiFi/Hyperlan e recentemente StarLink. La dislocazione geografica di questi diversi sistemi sul territorio nazionale consente di attenuare eventuali conseguenze dovute alla compromissione di un determinato servizio su un'area ben specifica. L'obiettivo è quello di avere, in caso di malfunzionamento di un provider, una rete sismica a maglia più larga piuttosto che un'area del Paese non sorvegliata. Generalmente ogni sistema di trasmissione vanta delle sue caratteristiche in termini di banda disponibile, banda minima garantita, latenza, livello di disponibilità e piano di indirizzamento IP (statico o dinamico, privato o pubblico). È proprio quest'ultima caratteristica che è risultata determinante nella realizzazione dell'infrastruttura che ci si appresta a descrivere.

2.1 Trasmissione 4G/LTE

Una fetta importante dei sistemi di trasmissione dati utilizzati è rappresentata dalla connettività dati delle reti cellulari 4G/LTE. Presso la sezione Irpinia negli anni sono state implementate diverse soluzioni tecniche per la gestione dei siti di monitoraggio equipaggiati con questo sistema di connettività, maturando un'esperienza ultradecennale [Falco, 2008; Falco et al., 2015]. Con l'aumento delle prestazioni dovuto all'evoluzione tecnologica delle reti di trasmissione sono state adeguate anche le infrastrutture di acquisizione dati della sede.

È importante notare che nonostante le attuali reti 4G siano ampiamente diffuse nel nostro Paese con una buona copertura su gran parte del territorio, per un servizio critico quale la sorveglianza sismica, non è possibile affidarsi unicamente ad esse. La capacità dei collegamenti dati cellulare è prevalentemente determinata dal livello di saturazione delle celle dei vari operatori. Inoltre, durante eventi sismici è frequente la condizione in cui le linee cellulari e telefoniche subiscono disservizi. Per questo motivo presso la sezione Irpinia questa tecnologia è stata prevalentemente utilizzata per l'acquisizione di stazioni GNSS per le quali la disponibilità in tempo reale di dati non è al momento così critica come per le stazioni sismiche utilizzate ai fini della sorveglianza. Per le stazioni di monitoraggio sismico il collegamento 4G/LTE è spesso affiancato ad una connettività alternativa.

Ciò nonostante, oggi sono presenti un numero crescente di stazioni sismiche che utilizzano questo vettore di trasmissione siccome risulta facilmente installabile ma si utilizzano strategie di dislocazione sul territorio in modo da evitare eventuali disservizi localizzati in aree ben

circoscritte come in caso di eventi sismici. E i livelli di continuità forniti nella trasmissione dei dati si sono rivelati comparabili con quelli dei collegamenti terrestri.

2.2 Indirizzamento IP connettività 4G/LTE

Il piano di indirizzamento IP fornito dai provider per questo servizio è solitamente di tipo privato e dinamico. Spesso può anche capitare che l'indirizzo fornito sia di tipo pubblico ma comunque dinamico, un'eventualità che negli anni passati era più frequente. Oggi, infatti, al crescere dei dispositivi mobili in circolazione, la non completa applicazione del protocollo IPv6, ha portato i provider a continuare ad utilizzare ampiamente IPv4 ma rilasciando indirizzi IP privati gestiti tramite CGNAT (Carrier-grade NAT) per consentire l'accesso ad INTERNET a milioni di dispositivi. Ma a prescindere dal piano di indirizzamento privato o pubblico c'è un'altra componente fondamentale da considerare quando si utilizzano queste connettività, ovvero l'APN (Access Point Network). Si tratta di un gateway tra la rete cellulare ed INTERNET sul quale il provider applica particolari policy di firewalling in funzione dell'utilizzo a cui esso è riservato. Esistono infatti APN commerciali che hanno il compito principale di consentire la navigazione WEB ai propri clienti ma con forti limitazioni su determinati protocolli applicativi; altri APN, invece, dedicati ad una più ampia gamma di servizi come quelli utilizzati in caso di tethering (l'utilizzo del cellulare come hotspot). In entrambi i casi, per la tipologia di traffico trattato e soprattutto per questioni di sicurezza, questi APN consentono quindi un traffico di tipo unidirezionale. Più nel dettaglio, cioè, consentono ai terminali di effettuare connessioni verso INTERNET ma non di essere contattati da esso per via delle policy impostate a livello di APN. Per questo motivo, nella classica architettura dedicata all'acquisizione dei dati sismici di tipo client/server nella quale generalmente (a parte alcune eccezioni) la parte client risiede presso i centri di acquisizione mentre la parte server a bordo degli acquisitori sismici, risulterebbe praticamente impossibile inizializzare una connessione verso le stazioni remote. Ovviamente esistono alcuni tipi di APN denominati "machine to machine" (M2M) che si distinguono dai precedenti in quanto le policy di sicurezza applicate consentono, invece, di effettuare traffico dati bidirezionale e quindi di contattare, eventualmente, le stazioni remote. Il tipo di traffico che però viene generato su questi APN ha un costo decisamente superiore e nella stragrande maggioranza dei casi il piano di indirizzamento IP applicato dai provider è comunque di tipo dinamico. Questo comporta l'utilizzo di soluzioni di dDNS (dynamic DNS) per tenere di volta in volta aggiornato l'IP con un nome di dominio al quale i servizi di acquisizione potranno staticamente riferirsi nonostante i continui cambi di IP ai terminali remoti. Quest'ultima, però, è una soluzione da considerare non accettabile ai fini di un'acquisizione dati realtime stabile nel tempo, in quanto può produrre dei forti ritardi nel ripristino dell'acquisizione dati ogni qualvolta il dispositivo remoto dovesse cambiare IP. Questo fenomeno, infatti, produce una latenza tra la disconnessione e il ripristino del flusso dati verso i centri di acquisizione non dovuta soltanto al tempo che il dispositivo remoto impiega per aggiornare i DNS, come si potrebbe erroneamente pensare, ma soprattutto alla risoluzione nomi errata dovuta alla cache DNS che, se non scaduta, può non rispecchiare la reale associazione nome-IP.

Nei primi anni di utilizzo di queste connettività si è fatto ampio uso dei sistemi M2M e dei servizi dDNS, consapevoli che l'utilizzo della tecnologia VPN (Virtual Private Network) sarebbe stata la soluzione tecnica più ovvia. Sono state anche approcciate diverse soluzioni tecniche ma nessuna è risultata soddisfacente siccome vi era un limite a quei tempi invalicabile: la scarsa performance delle reti dati cellulari di seconda generazione nonostante qualche accenno di miglioramento in quelle di terza generazione. Il problema reale è che il mantenimento di un tunnel VPN introduce ulteriori costi in termini di occupazione di banda per via dell'overhead di informazioni necessario al mantenimento del tunnel stesso. E in uno scenario in cui la larghezza

di banda era già esigua questo avrebbe ulteriormente degradato le prestazioni di tutto il sistema. Oggi ci troviamo in uno scenario completamente diverso e le reti 4G/5G hanno consentito di rivalutare i collegamenti VPN con le stazioni remote consentendo di raggiungere elevati livelli di affidabilità nella trasmissione del dato sismico.

2.3 Indirizzamento IP negli altri sistemi di trasmissione dati

Ci sono poi gli altri sistemi di trasmissione dati i cui contratti prevedono l'assegnazione di indirizzi IP pubblici e statici. Questa, ovviamente, risulta essere la soluzione più agevole, in quanto la strumentazione remota è facilmente contattabile senza l'implementazione di alcun artificio tecnico seppure occorre proteggere i dispositivi remoti con un firewall affinché siano contattabili esclusivamente dai sistemi di acquisizione dell'INGV. Ad ogni modo, anche su questi tipi di collegamenti è preferibile l'implementazione di tunnel VPN, i quali introducono un elevato livello di sicurezza nella trasmissione del dato grazie a sofisticati protocolli di autenticazione e crittografia.

3. Cosa sono le VPN

Le Virtual Private Network (VPN) sono reti di telecomunicazioni private che utilizzano come tecnologia di trasporto infrastrutture di trasmissione pubbliche (INTERNET solitamente). Si pensi ad esempio ad una grande azienda che ha diverse sedi e la necessità di interconnetterle tra loro: può ricorrere a linee private dedicate (solitamente a noleggio) con costi decisamente alti oppure realizzare delle VPN con costi nettamente inferiori. È ovvio che, utilizzando reti pubbliche per il trasporto dei dati, le VPN devono assicurare dei canali di comunicazione estremamente sicuri, mediante la cifratura del traffico.

3.1 I protocolli VPN

Esistono svariati protocolli per l'implementazione di tunnel VPN su reti pubbliche (PPTP, IPSEC, OpenVPN, SSTP, ecc.). La scelta solitamente ricade sul tipo di infrastruttura da realizzare e dal livello di sicurezza che si vuole ottenere. Ci sono protocolli che meglio si prestano ad applicazioni di tipo "access VPN" in cui l'utente/dispositivo remoto ha necessità di connettersi ad una rete aziendale privata o applicazioni di tipo "site to site" in cui i tunnel VPN sono implementati per interconnettere in modo permanente diverse sottoreti private dislocate in aree geografiche ben distanti (come le sedi periferiche di un ente o azienda).

4. Precedente infrastruttura di acquisizione e trasmissione dati

La Figura 2 mostra la precedente infrastruttura di acquisizione e trasmissione dati.

Il SeedLink Server acquisisce il flusso dati sismico sia delle stazioni direttamente esposte su INTERNET che di quelle collegate tramite tunnel VPN.

Infatti, non tutte le stazioni di monitoraggio sono collegate alla sezione mediante tunnel VPN; alcune sono esposte direttamente su INTERNET e i relativi flussi dati sono direttamente instradati verso i server di acquisizione dati della sala di monitoraggio di Roma (HSL1 e HSL2). È inteso che anche per questo tipo di stazioni il tunnel VPN sarebbe realizzabile, anzi garantirebbe un elevato livello di sicurezza nella trasmissione del dato.

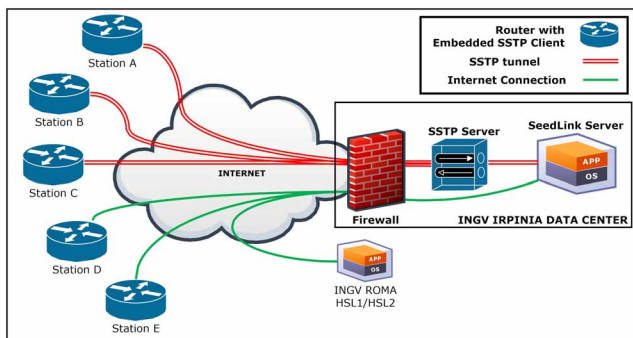


Figura 2 Layout della precedente infrastruttura di acquisizione e trasmissione dati.

Figure 2 Layout of the previous acquisition and transmission data infrastructure.

La funzione di concentratore o VPN Server è affidata ad un appliance Mikrotik (dispositivo che integra una serie di servizi di networking) e il protocollo utilizzato per l'implementazione del tunnel è SSTP. La scelta è ricaduta su questo protocollo perché consente facilmente di superare le limitazioni imposte dai firewall nel bloccare specifiche porte. Il server, infatti, è configurato per ricevere connessioni sulla porta TCP 443. È la stessa porta standard utilizzata dal protocollo applicativo HTTPS e siccome spesso alcune stazioni di monitoraggio sono ospitate presso enti terzi per i quali non si ha diretto controllo dei relativi sistemi di sicurezza informatica, si fa leva sul fatto che risulti poco probabile che venga limitata la navigazione WEB soprattutto se di tipo HTTPS. Si evita in questo modo di interagire con i referenti informatici delle organizzazioni e chiedere loro di impostare policy personalizzate di firewalling per consentire la trasmissione del dato. Anzi spesso per questioni di sicurezza la richiesta non viene avallata. SSTP, inoltre, utilizza SSL/TLS per garantire uno scambio di chiavi sicure e trasferimenti crittografati. Nello specifico la crittografia si basa sul protocollo AES a 256 bit considerato lo standard d'eccellenza nella crittografia a chiave simmetrica.

Il piano di indirizzamento IP dei dispositivi collegati tramite VPN è di tipo statico. Ogni stazione di monitoraggio si autentica con una propria coppia username/password e le viene assegnato sempre lo stesso indirizzo IP. Questo consente di evitare l'utilizzo di meccanismi come dDNS, ma soprattutto assicura una migliore continuità del flusso dati perché evita i problemi di caching DNS menzionati precedentemente.

La scelta di acquisire i dati della stazione di monitoraggio tramite tunnel VPN o direttamente tramite INTERNET dipende dalle caratteristiche della stessa, dai piani di indirizzamento IP discussi nei paragrafi precedenti, dal sistema di trasmissione adottato e dalla dotazione hardware della stazione (soprattutto router).

4.1 Limiti di questa infrastruttura e single points of failure

La sala di monitoraggio sismico dell'INGV di Roma garantisce il servizio di sorveglianza sismica dell'intero territorio nazionale grazie anche al contributo delle 83 stazioni sismiche di competenza della sezione Irpinia. Il flusso dati di queste stazioni viene acquisito dai sistemi di sala (HSL1 e HSL2) direttamente dal SeedLink Server della sezione Irpinia. È quindi di vitale importanza che questo flusso sia sempre garantito. Nello schema rappresentato in Figura 2 esistono evidenti single points of failure che possono pregiudicare il corretto instradamento del flusso dati dalla sezione Irpinia alla sala di monitoraggio di Roma.

I servizi SeedLink Server presso la sezione Irpinia sono ridondati; sono costituiti da macchine virtuali ospitate su un cluster VMware. L'alimentazione elettrica a questi ultimi è garantita da linee elettriche separate a monte delle quali vi sono due UPS distinti. Non per ultimo si riporta che anche gli appliance Mikrotik che implementano il concentratore VPN sono ridondati in configurazione MASTER/SLAVE così come i dispositivi di sicurezza perimetrali (firewall).

In questa configurazione appena descritta, sono ancora presenti alcune criticità. La sezione Irpinia, per esempio, è dotata di una singola connettività dati verso INTERNET fornita dal GARR tramite accesso in fibra ottica. L'interruzione di questo servizio rende inaccessibili i Seedlink Server di sezione alla sala sismica con un forte degrado del servizio di sorveglianza sismica. Questo rappresenta il single point of failure maggiormente critico.

Anche il singolo vettore di trasmissione dati presso il sito di monitoraggio rappresenta un'ulteriore criticità, sebbene il suo degrado comprometterebbe l'acquisizione di una singola stazione di monitoraggio anziché dell'intera rete.

A quanto sopra va aggiunta anche la possibilità di eventi avversi che potrebbero comunque produrre guasti in grado di isolare l'intera sezione. Negli anni, ad esempio, alcuni guasti in cabina elettrica o agli stessi UPS hanno portato ad un fermo dell'intero data center.

5. Nuova infrastruttura di acquisizione dati

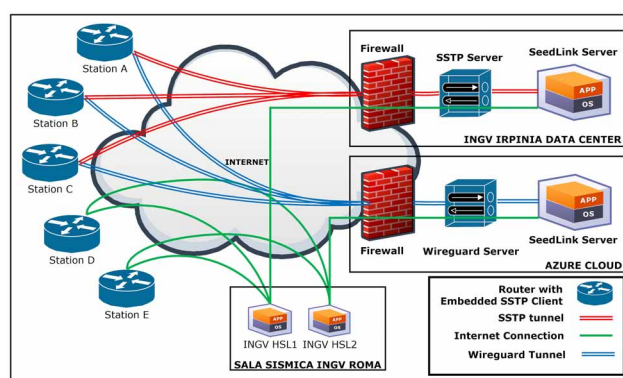
Come si diceva in precedenza, i limiti dell'infrastruttura appena descritta possono essere superati senza alcun impedimento tecnico, ma è un'attenta valutazione dei costi che ci ha portato a pianificare realmente quali servizi ridondare per eliminare i single points of failure più critici.

L'obiettivo principale è stato trovare un sito aggiuntivo ai servizi di acquisizione dati SeedLink e di conseguenza anche ai concentratori VPN per poter acquisire i dati delle stazioni di monitoraggio non direttamente esposte su INTERNET. In questo modo la sala sismica può contare su due servizi di acquisizione dati dislocati in due luoghi completamente differenti ognuno dei quali è in grado di acquisire autonomamente i dati delle stazioni di monitoraggio di competenza della sezione Irpinia.

Come secondo sito è stata scelta la soluzione cloud Azure di Microsoft approfittando di un contratto già in essere con l'INGV.

La Figura 3 illustra la nuova infrastruttura di acquisizione dati che si sviluppa in parte presso il datacenter della sezione Irpinia (on-premise) ed in parte presso la piattaforma cloud pubblica di Microsoft Azure.

Figura 3 Nuova infrastruttura acquisizione dati.
Figure 3 New data acquisition infrastructure.



I router installati presso le stazioni di monitoraggio sono stati configurati per implementare un doppio tunnel VPN: uno verso il concentratore dislocato presso la sezione Irpinia mediante l'utilizzo del protocollo SFTP, l'altro verso un concentratore installato sul cloud Azure e che utilizza il protocollo Wireguard. La scelta di utilizzare due protocolli VPN differenti è stata dettata unicamente dal concetto di diversificare quanto più possibile. Non è remota, infatti, la possibilità che vengano scoperte falle di sicurezza anche nei protocolli più accreditati. Di conseguenza la diversificazione ci consente di non essere completamente scoperti e di garantire il flusso dati sismico mediante l'altro concentratore mentre si sta applicando una patch di sicurezza al

concentratore affetto dal problema. Inoltre, si è volutamente scelto il protocollo Wireguard per una serie di caratteristiche che saranno descritte più avanti.

I servizi di acquisizione dati SeedLink Server installati presso la sezione Irpinia e sul cloud Azure acquisiscono i dati dalle stazioni sismiche in maniera del tutto indipendente l'uno dall'altro attraverso i relativi concentratori VPN. La sala di sorveglianza sismica di Roma, con i suoi due server di acquisizione dati HSL1 e HSL2, può contare sulla rete di stazioni sismiche della sezione Irpinia che risulta fruibile da 2 luoghi geografici distinti. In linea generale, il server HSL1 è configurato per prelevare i dati dal SeedLink Server ospitato nel data center della sezione Irpinia mentre HSL2 è configurato per acquisire i dati dal SeedLink server installato sul cloud Azure.

Il vantaggio di questa soluzione è evidente. L'eventuale irraggiungibilità della sezione Irpinia non comprometterebbe il servizio di sorveglianza sismica in quanto i flussi dati risulteranno disponibili mediante il server SeedLink ospitato sul cloud Azure. Stesso dicasi per un eventuale disservizio alla piattaforma cloud anche se questa eventualità risulterebbe attenuata dai meccanismi di replica tra zone che il cloud fornisce.

Le stazioni di monitoraggio che invece sono direttamente esposte su Internet ed accessibili senza la necessità di implementare tunnel VPN vengono acquisite direttamente dai server seedlink di sala HSL1 e HSL2.

La sezione Irpinia ha in gestione anche la rete sismica OTRIONS (codice rete OT) nata grazie ad un progetto congiunto tra INGV e Università degli studi di Bari "Aldo Moro" conclusosi nel 2013 [<http://www.otrions.uniba.it/>]. Le stazioni della rete OT sono oggi parte integrante del sistema di sorveglianza sismica nazionale soprattutto perché dislocate in un'area, quella garganica, dove la rete INGV (rete IV) è meno densa. Per l'acquisizione di queste stazioni si è scelto di utilizzare lo stesso paradigma descritto in questo rapporto tecnico. In pratica le stazioni sono acquisite in maniera indipendente sia sul cloud Azure che presso ReCas [<https://www.recas-bari.it/index.php/it/>], un data center realizzato dall'Università degli Studi di Bari "Aldo Moro" e dall'Istituto Nazionale di Fisica Nucleare (INFN).

5.1 Protocollo Wireguard

Per il collegamento VPN tra i siti remoti e l'appliance Mikrotik su cloud Azure si è scelto di utilizzare il protocollo Wireguard. Tra tutti i protocolli analizzati negli ultimi 10 anni è quello che si adatta meglio all'implementazione di tunnel VPN su connettività di tipo 4G/LTE (supporta infatti il roaming IP).

Si tratta di un protocollo molto semplice e veloce che utilizza i protocolli di crittografia più recenti. È stato progettato per essere snello, sicuro e performante, molto più di protocolli noti come IPSEC o OpenVPN. È un protocollo semplice da configurare e consente di effettuare connessioni VPN sicure attraverso il semplice scambio di chiavi pubbliche analogamente a quanto avviene per una sessione SSH. Si riporta un semplicissimo esempio di configurazione in ambiente RouterOS Mikrotik (Figura 4).

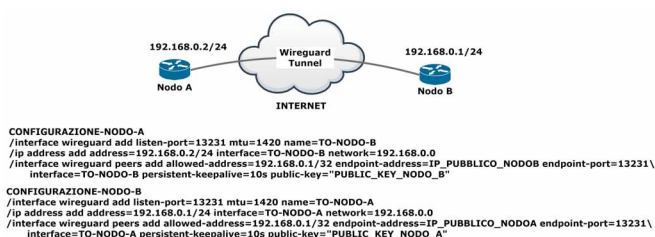


Figura 4 Esempio configurazione tunnel VPN Wireguard.
Figure 4 Wireguard VPN Tunnel configuration example.

Si considerino 2 nodi A e B che intendono instaurare un tunnel VPN con protocollo Wireguard su rete pubblica INTERNET; il primo comando consente di aggiungere a ciascun router un'interfaccia virtuale di tipo Wireguard in ascolto sulla porta UDP 13231 alla quale viene assegnato il nome mnemonico TO-NODO-A o TO-NODO-B. La creazione di una interfaccia crea automaticamente una coppia di chiavi (pubblica e privata). Va da sé che la chiave privata di ciascuna interfaccia deve essere accuratamente custodita.

Con il secondo comando vengono assegnati gli indirizzi IP privati da attribuire a ciascuna interfaccia Wireguard; nello specifico viene assegnato l'indirizzo IP 192.168.0.2/24 all'interfaccia TO-NODO-B del router NODO-A e l'indirizzo IP 192.168.0.1/24 all'interfaccia TO-NODO-A del router NODO-B.

Con il terzo comando si elencano per ciascun router i peer con i quali si intende instaurare il tunnel VPN. Nell'esempio riportato in figura NODO-A avrà come peer NODO-B e viceversa. La definizione di un peer prevede di specificare l'interfaccia Wireguard utilizzata per raggiungere quel peer (opzione interface), l'indirizzo IP pubblico sul quale il peer remoto accetterà la connessione VPN (opzione endpoint-address), la relativa porta UDP (opzione endpoint-port) e la sua chiave pubblica (opzione public-key). Una considerazione a parte va riservata al parametro allowed-address. Esso, infatti, ha un duplice scopo: per i pacchetti che giungono alla relativa interfaccia Wireguard funge da access control list consentendo nel caso di Nodo-A di accettare traffico solo dal peer avente IP 192.168.0.1. Allo stesso tempo il parametro viene utilizzato da Nodo-A per installare una rotta tramite la relativa interfaccia Wireguard per tutto il traffico diretto a 192.168.0.1. Discorso analogo per la configurazione relativa a NodoB.

Si noti che l'opzione endpoint-address non è tassativa su entrambi i nodi. Nel caso in cui non fosse specificata sul Nodo-B, quest'ultimo non inizializzerebbe mai una sessione VPN ma accetterebbe solo le richieste di connessione provenienti da Nodo-A.

Nello scenario reale questo è ciò che accade. Si consideri infatti NodoB il concentratore VPN on premise o su Azure. Esso è dotato di indirizzo IP pubblico statico al quale tutti i nodi remoti (le stazioni sismiche) possono riferirsi per instaurare tunnel VPN. Viceversa, NodoB non potrebbe mai instaurare di sua iniziativa connessioni VPN verso stazioni dotate di connettività LTE in quanto impossibilitato a raggiungerle per via dell'indirizzo IP privato dinamico che queste connettività ricevono dai rispettivi provider. Per questo motivo diventa indispensabile l'opzione persistent-keepalive in modo da assicurarsi che sia il router remoto della singola stazione ad inizializzare e mantenere sempre vivo il tunnel Wireguard verso il concentratore.

In ultimo, la caratteristica a nostro avviso più interessante del protocollo Wireguard è la capacità di roaming tra indirizzi IP consentendo di mantenere in piedi le connessioni anche al variare dell'IP lato WAN del device; è per questo particolare motivo che su connettività 4G/LTE abbiamo potuto apprezzarne fortemente le sue doti.

6. Hardware installato presso le stazioni

A prescindere dal tipo di trasmissione (satellitare, LTE, WiFi, ecc.) le stazioni di monitoraggio sono sempre dotate di un router grazie al quale possiamo realizzare funzionalità come firewalling, tunneling VPN, autenticazione, accounting, routing.

I router che si utilizzano sono prodotti dall'azienda lettone MikrotikLS e consentono di soddisfare una stragrande varietà di esigenze dal punto di vista delle connettività dati. L'azienda produce sia soluzioni embedded che router board da assemblare scegliendo tra diversi moduli dati (LTE, WiFi, ecc.). La scelta di utilizzare questi dispositivi proviene da almeno un decennio di esperienza nell'utilizzo del sistema operativo RouterOS (il sistema operativo di questi apparati), grazie a mirati percorsi di formazione e certificazione e al fatto che si sono rilevati molto affidabili nel funzionare in condizioni climatiche estreme a cui sono sottoposte molte delle stazioni di monitoraggio. Gli

apparati sono venduti sia in soluzioni integrate che in moduli da comporre in funzione delle proprie esigenze (ad esempio router board + modulo LTE + modulo WiFi + modulo GPS, ecc.).

7. Cloud Azure

L'infrastruttura individuata per ospitare in modalità ridondata i servizi di acquisizione dati ed il relativo concentratore VPN, come precedentemente affermato, è stata il cloud pubblico Azure di Microsoft. Il motivo principale è costituito dall'elevata disponibilità dei servizi erogati dai cloud service provider grazie ad architetture informatiche molto complesse e distribuite in "aree geografiche" molto ampie (Americhe, Europa, Asia, ecc.) e alla presenza di un contratto già in essere con l'INGV.

Su ognuna di queste aree insistono diverse "Region", ognuna delle quali presenta almeno 3 "zone di disponibilità" connesse tra loro da una rete ad alte prestazioni. Ogni "zona di disponibilità" è costituita da uno o più data center dotati di impianti indipendenti per l'alimentazione, il raffreddamento e la connettività di rete. Le zone di disponibilità sono progettate in modo che se una zona è interessata da un disservizio, i servizi sono garantiti dalle due zone rimanenti.

Inoltre, è possibile mettersi al riparo anche da eventi catastrofici che possano colpire un'intera "Region". In questo caso, infatti, è possibile utilizzare anche la Replica tra aree geografiche o "Region" differenti.

Lo stesso Dipartimento per la Trasformazione Digitale e l'Agenzia per la Cybersicurezza nazionale hanno definito una strategia denominata "Cloud First" che dovrebbe favorire l'adozione prioritaria da parte della Pubblica Amministrazione di strumenti e tecnologie di tipo cloud nello sviluppo di nuovi servizi. In questo modo si garantisce un'offerta di servizi digitali e infrastrutture tecnologiche sicure, efficienti, affidabili e autonome in linea con i principi di tutela della privacy. Per l'infrastruttura descritta nel presente rapporto tecnico si è scelto di utilizzare l'area geografica Europa ed in particolare la Region "Europa Occidentale".

I Service Level Agreement per le macchine virtuali su Azure sono i seguenti: 99,9% nel caso di Virtual Machine su singola istanza, 99,95% per le VM che hanno almeno 2 istanze nella stessa zona di disponibilità e 99,99% per VM con almeno 2 istanze su 2 differenti zone di disponibilità. Per la nostra infrastruttura abbiamo scelto macchine virtuali su singola istanza (con SLA del 99,9%) in quanto i servizi sono già replicati anche presso la sezione Irpinia.

7.1 Servizi principali attivi sul cloud

I servizi attivati sul cloud Azure descritti nell'infrastruttura di Figura 3 si possono sintetizzare in:

- Virtual Machine ospitante RouterOS con le funzioni di concentratore VPN, Firewall e gateway per tutta la rete virtuale sul cloud
- Virtual Machine ospitante il servizio di acquisizione dati SeedLink Server
- Indirizzo IP pubblico statico
- Servizio di archiviazione per ospitare le immagini delle VM, backup, ecc.

7.2 Virtual Machine RouterOS on Azure

Uno dei servizi più importanti che è stato attivato su Azure è un appliance virtuale col quale implementare i più comuni servizi di rete (Firewalling, Routing, Natting, VPN, ecc.) anziché ricorrere ai singoli servizi messi a disposizione, volendo, dal provider.

L'appliance è stato realizzato attraverso una macchina virtuale sulla quale è stato installato il

sistema operativo RouterOS di Mikrotik. L'azienda, infatti, consente previo pagamento di una licenza (dal costo di circa 50 euro) di installare il sistema operativo su ambienti X86.

Diversamente si sarebbero dovuti acquistare i singoli servizi messi a disposizione da Azure. A titolo esemplificativo: il servizio "Firewall di Azure" per implementare policy di firewalling avanzate oppure "Gateway VPN" per la realizzazione di tunnel VPN gestiti.

Si è scelto di gestire personalmente i vari servizi di rete ottenendo una forte riduzione del costo mensile dei servizi attivi sul cloud.

Le caratteristiche della Virtual Machine allocata per tale scopo sono: VM Standard B1s (1 cpu virtuale, 1 GiB memoria) + 1 GB HDD Standard con ridondanza locale.

7.3 Virtual Machine SeedLink Server

La seconda virtual machine implementata ospita il servizio di acquisizione dati SeedLink Server (il modulo di acquisizione del pacchetto software Seiscomp 4.0 [<https://www.seiscomp.de/>]) grazie al quale vengono acquisiti i flussi dei dati sismici delle stazioni di monitoraggio.

La VM è stata equipaggiata con sistema operativo Ubuntu Linux 20.04 e presenta le seguenti caratteristiche hardware virtuali: VM Standard B2s (2 cpu virtuali, 4 GiB memoria) + 30 GB SSD Premium con ridondanza locale.

7.4 IP pubblico statico

Per consentire l'instaurazione dei tunnel VPN dalle stazioni remote verso il concentratore dislocato su Azure lo stesso deve ovviamente essere raggiungibile tramite un indirizzo IP pubblico (meglio se statico). Per questo motivo l'ulteriore servizio Azure acquistato è stato "IP Pubblico di tipo statico" al quale è stato associato anche un nome DNS.

Tramite l'IP Pubblico viene distribuito il flusso dati delle stazioni di monitoraggio alla sala di sorveglianza sismica di Roma e a nessun altro. Tramite l'appliance Mikrotik e ai "Gruppi di sicurezza" (Paragrafo 7.6) si gestiscono le relative policy di firewalling. Si sarebbe potuto implementare un ulteriore link VPN tra la sala sismica e l'infrastruttura di acquisizione sul cloud ma si è preferito che lo scambio dati avvenisse direttamente su INTERNET. I motivi sono principalmente due: da un lato i dati trasmessi non richiedono particolari accorgimenti in termini di crittografia in quanto non ritenuti sensibili (basti pensare che tutti i dati sismici sono pubblicamente distribuiti tramite il portale Eida [<https://eida.ingv.it/it/>]), dall'altro in questo modo è possibile reindirizzare i flussi a qualsiasi altra sede dell'ente andando semplicemente ad agire sulle policy di firewalling senza dover preventivamente predisporre un nuovo tunnel VPN.

7.5 Servizio di archiviazione – Azure Container Storage

Esistono diversi servizi di archiviazione dati sul cloud Azure, ognuno rispondente a specifiche esigenze. Quello che è stato attivato è il servizio BLOB Storage. Si tratta di un servizio ad alta disponibilità che consente di archiviare enormi quantità di dati in maniera efficiente, sicura ed economica; è altamente scalabile e ottimizzato per la durabilità; è ideale per archiviare dati non strutturati che possono crescere senza limiti. Tale servizio è utilizzato per l'archiviazione delle immagini di boot dei dischi che compongono le macchine virtuali. Ma non solo. È utilizzato infatti per conservare i backup incrementali e snapshot che periodicamente vengono realizzati e dai quali è possibile ripristinare un'intera macchina virtuale; è utilizzato per l'archiviazione delle chiavi pubbliche utilizzate per l'accesso SSH alle VM e come disco virtuale per poter utilizzare il

servizio “Cloud Shell”, un terminale disponibile via web grazie al quale è possibile interagire con l'infrastruttura di Azure al fine di creare, avviare, eliminare e monitorare le risorse richieste.

7.6 Dettaglio delle risorse allocate sul cloud

La Figura 5 mostra in dettaglio tutte le risorse allocate sul cloud all'interno del gruppo di risorse assegnato alla sezione Irpinia. È evidente che quanto descritto fino ad ora in realtà si traduce in un numero di risorse/componenti maggiore. Nella figura, infatti, è possibile notare la granularità con la quale viene scomposta una semplice VM; sono infatti ben evidenti le sue interfacce di rete, i suoi dischi, le immagini dei dischi.

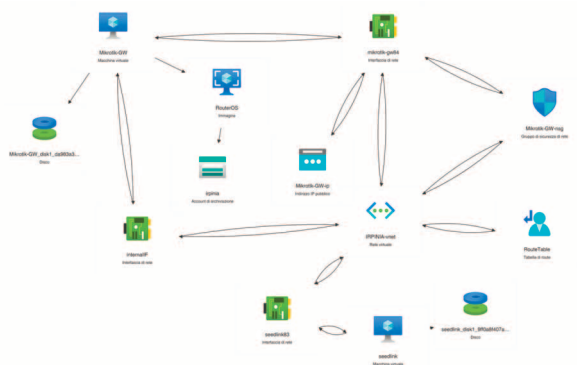


Figura 5 Visualizzazione grafica delle risorse attive sul cloud Azure.

Figure 5 Graphical view of Azure resources.

Come è evidente tutto ruota intorno alla rete virtuale denominata IRPINIA-VNET. Si tratta appunto di uno spazio di indirizzi IP privato grazie al quale le risorse (tramite le loro interfacce di rete) possono interagire tra di loro. Lo spazio di indirizzamento IP della IRPINIA-VNET è suddiviso in due sottoreti "/24": una privata non esposta su INTERNET e quindi completamente inaccessibile dall'esterno e l'altra riservata ai servizi che sono stati esposti pubblicamente (per esempio il gateway VPN).

Alle reti virtuali è possibile agganciare una “Tabella di routing” grazie alla quale vengono definite le rotte personalizzate per l’intera VNET. A tal proposito si ricorda che la modalità di instradamento definita nel cloud è di tipo Software-Defined. Ciò significa che ogni VNET presenta degli instradamenti di default definiti a livello centralizzato che è possibile ereditare e modificare proprio attraverso lo strumento messo a disposizione dalla “Tabella di Route”. Ad esempio, l’oggetto “Route Table” è stato utilizzato per far sì che tutta la sottorete privata venisse instradata verso INTERNET utilizzando la VM che ospita l’appliance virtuale RouterOS, in modo da poterne controllare tra le tante cose il NAT in uscita. Diversamente, l’instradamento verso INTERNET di default definito dal cloud Azure prevede l’accesso su INTERNET tramite un pool di indirizzi IP privati dinamici in modalità CGNAT.

Alla rete virtuale IRPINIA-VNET sono collegate le interfacce di rete delle VM implementate. Nello specifico l'interfaccia "seedlink83" della VM "seedlink" sulla quale gira il software Seiscomp e le interfacce "mikrotik-gw84" e "internalIF" della VM Mikrotik-GW che rappresentano rispettivamente le interfacce nella sottorete pubblica (mikrotik-gw84) e nella sottorete privata (internalIF).

Un componente di fondamentale importanza ai fini della sicurezza informatica è rappresentato dal “Gruppo di sicurezza di rete” che si materializza con l’oggetto “Mikrotik-GW-nsg”. Esso consente di filtrare il traffico di rete tra le risorse di Azure e può essere collegato sia alle reti virtuali VNET, sia alle singole interfacce di rete o ad entrambe. Esso agisce come un firewall di base sull’unica VNET disponibile (IRPINIA-VNET) e sull’unica interfaccia di rete presente nella

rete pubblica (mikrotik-gw-84). Questo oggetto può essere considerato come una sorta di firewall di livello base. Grazie ad esso, infatti, le risorse su rete privata non sono accessibili in alcun modo e l'unica risorsa su rete pubblica accessibile è invece la VM Mikrotik-GW, sulla quale però è implementato un firewall avanzato in modo da poter controllare con maggiore dettaglio il traffico da filtrare (l'intera infrastruttura sul cloud è accessibile solo dalle sedi di Roma e Grottaminarda dell'INGV). Si ricorda che le funzionalità avanzate di firewalling possono essere gestite anche dal servizio "Firewall di Azure" sostenendo un ulteriore costo per tale risorsa. Come specificato in paragrafi precedenti, invece, il firewall è totalmente autogestito tramite la VM Mikrotik-GW ottenendo quindi un importante risparmio in termini economici.

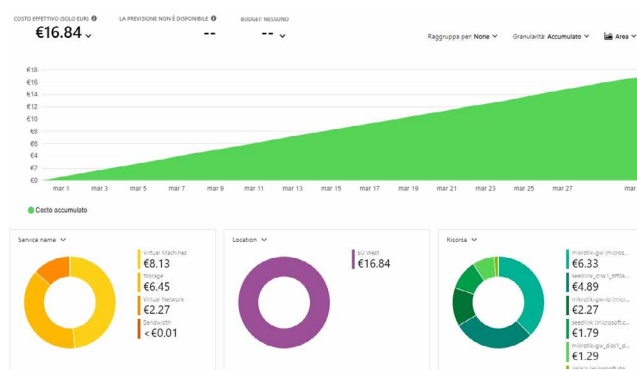
Gli ulteriori componenti presenti in Figura 3 sono l'oggetto "Mikrotik-gw-ip" agganciato all'interfaccia pubblica della VM Mikrotik-GW (mikrotik-gw-84), che rappresenta il leasing dell'IP pubblico statico con relativa associazione del nome DNS, l'immagine del sistema operativo RouterOS conservata nell'account di archiviazione "Irpinia" e i dischi delle singole VM. Si noti che non è presente l'immagine del sistema operativo Ubuntu 20.04 nell'account di archiviazione siccome è stato utilizzato direttamente quello messo a disposizione dal repository di Azure.

8. Costi

Uno degli aspetti più importanti nell'utilizzo di risorse cloud è proprio la razionalizzazione dei costi. Si consideri che nella fattispecie di quanto realizzato e descritto in tale lavoro i costi ricadono prevalentemente sulle macchine virtuali istanziate, sull'occupazione di spazio nell'account di archiviazione, sul lease dell'indirizzo IP pubblico statico. Le risorse, al momento, vengono contabilizzate per ogni minuto di utilizzo e nel caso specifico 24 ore su 24 per 365 giorni all'anno. Pre-allocando le risorse si potrebbero eventualmente ottenere delle forti riduzioni di prezzo. Detto ciò, il costo che mensilmente si sta sostenendo per il mantenimento in esercizio dei servizi descritti in questo rapporto tecnico sul cloud Azure ammonta a circa 15 euro mensili (vedi Figura 6).

Figura 6 Dettaglio dei costi sostenuti nel mese di Marzo 2024.

Figure 6 March 2024 cost details.



9. Conclusioni

In quasi due anni di utilizzo l'infrastruttura realizzata si è rilevata molto affidabile. Le risorse dislocate sul cloud Azure hanno registrato una disponibilità del 100%, valore maggiore di quanto previsto dal Service Level Agreement (SLA) per le VM su singola istanza presente nel contratto Microsoft (99,9%). Quelle allocate in sezione si sono attestate ad una percentuale più bassa a causa di alcuni disservizi verificatisi sull'impianto elettrico della sede. In ogni caso il flusso dei dati verso la sala di sorveglianza sismica, per quelle stazioni di monitoraggio alle quali è stata

applicata la configurazione del doppio tunnel VPN, non si è mai arrestato. Ad oggi sono circa 40 su 83 le stazioni di monitoraggio di competenza della sezione Irpinia che utilizzano il doppio tunnel VPN. La restante parte di stazioni è direttamente connessa ai sistemi di sala HSL1 e HSL2 perché raggiungibili direttamente su INTERNET o perché collegate in VPN direttamente alla sala.

Bibliografia

Falco L., (2008). *Implementazione e gestione di una rete di monitoraggio GPS e sismica mediante tecnologie GPRS/EDGE/UMTS/HSDPA*. Rapp. Tec. INGV, 69: 1-21. <http://hdl.handle.net/2122/4191>

Falco L., Cecere G., D'Ambrosio C., (2015). *Acquisizione dati sismici e GPS mediante implementazione di un cloud privato su rete dati cellulare ad integrazione della rete informatica della sede Irpinia*. Rapp. Tec. INGV, 301: 1-22. <https://doi.org/10.13127/rpt/301>

Sitografia

RouterOS Documentation <https://help.mikrotik.com/docs/>
Azure Documentation <https://learn.microsoft.com/it-it/azure/>
Seiscomp 4.0 Documentation <https://www.seiscomp.de/doc/>
Wireguard Documentation <https://www.wireguard.com/>
Rete Sismica OTRIONS <http://www.otrions.uniba.it/>
DataCenter RECAS <https://www.recas-bari.it/index.php/it/>
Seiscomp 4.0 <https://www.seiscomp.de>

QUADERNI di GEOFISICA

ISSN 1590-2595

<https://istituto.ingv.it/it/le-collane-editoriali-ingv/quaderni-di-geofisica.html/>

I QUADERNI DI GEOFISICA (QUAD. GEOFIS.) accolgono lavori, sia in italiano che in inglese, che diano particolare risalto alla pubblicazione di dati, misure, osservazioni e loro elaborazioni anche preliminari che necessitano di rapida diffusione nella comunità scientifica nazionale ed internazionale. Per questo scopo la pubblicazione on-line è particolarmente utile e fornisce accesso immediato a tutti i possibili utenti. Un Editorial Board multidisciplinare ed un accurato processo di peer-review garantiscono i requisiti di qualità per la pubblicazione dei contributi. I QUADERNI DI GEOFISICA sono presenti in "Emerging Sources Citation Index" di Clarivate Analytics, e in "Open Access Journals" di Scopus.

QUADERNI DI GEOFISICA (QUAD. GEOFIS.) welcome contributions, in Italian and/or in English, with special emphasis on preliminary elaborations of data, measures, and observations that need rapid and widespread diffusion in the scientific community. The on-line publication is particularly useful for this purpose, and a multidisciplinary Editorial Board with an accurate peer-review process provides the quality standard for the publication of the manuscripts. QUADERNI DI GEOFISICA are present in "Emerging Sources Citation Index" of Clarivate Analytics, and in "Open Access Journals" of Scopus.

RAPPORTI TECNICI INGV

ISSN 2039-7941

<https://istituto.ingv.it/it/le-collane-editoriali-ingv/rapporti-tecnici-ingv.html/>

I RAPPORTI TECNICI INGV (RAPP. TEC. INGV) pubblicano contributi, sia in italiano che in inglese, di tipo tecnologico come manuali, software, applicazioni ed innovazioni di strumentazioni, tecniche di raccolta dati di rilevante interesse tecnico-scientifico. I RAPPORTI TECNICI INGV sono pubblicati esclusivamente on-line per garantire agli autori rapidità di diffusione e agli utenti accesso immediato ai dati pubblicati. Un Editorial Board multidisciplinare ed un accurato processo di peer-review garantiscono i requisiti di qualità per la pubblicazione dei contributi.

RAPPORTI TECNICI INGV (RAPP. TEC. INGV) publish technological contributions (in Italian and/or in English) such as manuals, software, applications and implementations of instruments, and techniques of data collection. RAPPORTI TECNICI INGV are published online to guarantee celerity of diffusion and a prompt access to published data. A multidisciplinary Editorial Board and an accurate peer-review process provide the quality standard for the publication of the contributions.

MISCELLANEA INGV

ISSN 2039-6651

https://istituto.ingv.it/it/le-collane-editoriali-ingv/miscellanea-ingv.html

MISCELLANEA INGV (MISC. INGV) favorisce la pubblicazione di contributi scientifici riguardanti le attività svolte dall'INGV. In particolare, MISCELLANEA INGV raccoglie reports di progetti scientifici, proceedings di convegni, manuali, monografie di rilevante interesse, raccolte di articoli, ecc. La pubblicazione è esclusivamente on-line, completamente gratuita e garantisce tempi rapidi e grande diffusione sul web. L'Editorial Board INGV, grazie al suo carattere multidisciplinare, assicura i requisiti di qualità per la pubblicazione dei contributi sottomessi.

MISCELLANEA INGV (MISC. INGV) favours the publication of scientific contributions regarding the main activities carried out at INGV. In particular, MISCELLANEA INGV gathers reports of scientific projects, proceedings of meetings, manuals, relevant monographs, collections of articles etc. The journal is published online to guarantee celerity of diffusion on the internet. A multidisciplinary Editorial Board and an accurate peer-review process provide the quality standard for the publication of the contributions.

Coordinamento editoriale

Francesca DI STEFANO
Istituto Nazionale di Geofisica e Vulcanologia

Progetto grafico

Barbara ANGIONI
Istituto Nazionale di Geofisica e Vulcanologia

Impaginazione

Barbara ANGIONI
Patrizia PANTANI
Massimiliano CASCONI
Istituto Nazionale di Geofisica e Vulcanologia

©2024

Istituto Nazionale di Geofisica e Vulcanologia
Via di Vigna Murata, 605
00143 Roma
tel. +39 06518601

www.ingv.it



Creative Commons Attribution 4.0 International (CC BY 4.0)



ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA