

## ALLEGATO N. 4

### PIANO DI SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

#### Premessa

Il presente piano di sicurezza, adottato ai sensi delle Linee guida AgID sul documento informatico, descrive le politiche adottate dal Comune di Fenestrelle affinché:

- i documenti e le informazioni trattati dall'Ente siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

A tali fini le Linee guida AgID individuano i requisiti minimi di sicurezza dei sistemi di protocollo informatico a cui il presente piano si conforma.

Il piano di sicurezza, in base ai rischi cui sono esposti i dati (personali e non) e/o i documenti trattati, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno del Comune di Fenestrelle;
- le modalità di accesso al Sistema di Gestione Informatica dei Documenti;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, al fine di garantire le misure di sicurezza necessarie alla tutela del patrimonio documentale dell'Ente e alla tutela e garanzia dei dati personali, sensibili o giudiziari;
- la formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Tale piano di sicurezza è soggetto a revisione con cadenza almeno biennale; a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche, potrà essere modificato anticipatamente.

#### Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel Sistema di Gestione Informatica dei Documenti

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'ausilio delle tecnologie informatiche sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al SGID o come accesso ai documenti, dati e unità archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati, includendo a tale proposito tutti i dati presenti sul Sistema di Gestione Informatica dei Documenti;
- perdita dei documenti e dei dati contenuti nel Sistema;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, il Comune di Fenestrelle adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

### Sicurezza della rete di accesso al servizio

Il Sistema di Gestione Informatica dei Documenti del Comune di Fenestrelle non è esposto all'accesso attraverso la rete internet, ma è installato in un server fisico, accessibile dalla rete intranet dell'Ente, ereditando dalla stessa tutti i meccanismi previsti per la sicurezza e la protezione. Il server fisico è ubicato in un locale chiuso a chiave il cui accesso è nell'esclusiva disponibilità dell'Ente; il locale dove è ubicato il server è provvisto di sistema di allarme, che è il sistema generale del municipio sempre attivo quando gli uffici sono chiusi.

### Procedure comportamentali degli operatori ai fini della protezione dei documenti informatici e dei dati in essi contenuti

Le postazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà del Comune di Fenestrelle a vario titolo messi a disposizione del personale, sono strumenti di lavoro e il loro utilizzo è finalizzato allo svolgimento delle attività professionali e istituzionali dell'Ente.

Ogni operatore adotta comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza dei sistemi informativi.

Gli operatori cui sono affidati i dispositivi informatici di proprietà del Comune sono tenuti ad avere le seguenti accortezze:

- l'accesso alle singole postazioni di lavoro avviene previa autenticazione dell'operatore tramite apposite credenziali di accesso personali, composte di almeno n. 8 caratteri, modificate con cadenza quadrimestrale; dopo n. 50 tentativi errati nell'immissione delle suddette credenziali il sistema blocca l'accesso dell'operatore;
- qualora nei dispositivi e nelle postazioni di lavoro siano memorizzati dati personali, sensibili o giudiziari, l'operatore che li utilizza deve porre in atto comportamenti idonei a garantire la protezione di detti dati;
- ciascun operatore è tenuto a segnalare immediatamente ai referenti informatici ogni sospetto utilizzo non autorizzato, violazione della sicurezza o malfunzionamento relativo ai dispositivi informatici a lui assegnati;
- al momento della cessazione del rapporto di lavoro, ciascun operatore deve restituire al Comune qualsiasi risorsa informatica a lui assegnata e mettere a disposizione ogni informazione di interesse istituzionale;

- non è consentito installare programmi non inerenti all'attività lavorativa;
- non è consentito copiare dati la cui titolarità sia del Comune di Fenestrelle su dispositivi esterni personali.

Ai fini della vigilanza nell'utilizzo degli strumenti informatici assegnati, ciascun operatore ha l'obbligo di impedire ad altri l'utilizzo non autorizzato della propria apparecchiatura informatica.

Le stazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, messi a disposizione del personale, non devono essere lasciati incustoditi. L'operatore è tenuto a bloccare o a spegnere il personal computer in caso di sospensione o termine dell'attività lavorativa e, comunque sempre, al termine dell'orario di servizio.

### Accesso al Sistema di Gestione Informatica dei Documenti e ai documenti e dati in esso contenuti da parte di utenti interni all'AOO

L'accesso al Sistema di Gestione Informatica dei Documenti, da parte degli utenti interni all'AOO, avviene attraverso l'utilizzo di credenziali di autenticazione; i profili di abilitazione alle funzionalità del Sistema stesso sono attribuiti a ciascun utente sulla base di quanto stabilito dall'allegato n. 2 al presente manuale. L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi.

Le credenziali di autenticazione consistono in un codice (*User-Id*), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (*Password*), conosciuta solamente dal medesimo; tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione, il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente, memorizzando, ai fini di controllo, l'*User-Id* corrispondente, ma non la *Password* dello stesso.

Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della *password*; quest'ultima è composta di almeno 8 caratteri (di cui almeno una lettera maiuscola, una lettera minuscola, un numero ed un simbolo non alfanumerico) e non contiene riferimenti agevolmente riconducibili al titolare. La *password* è modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza almeno semestrale; le credenziali di accesso saranno modificate con cadenza trimestrale per gli operatori che trattano dati personali, sensibili o giudiziari.

Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. I profili di accesso associati alle credenziali disattivate non vengono riattivati neppure successivamente.

Qualora il titolare delle credenziali di autenticazione dimenticasse la propria *password* si procederà all'assegnazione di una nuova chiave di accesso.

Le credenziali di accesso sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime.

## Accesso al trattamento di dati personali sensibili o giudiziari e politiche di sicurezza espressamente previste

L'accesso ai documenti contenenti dati personali, sensibili o giudiziari e ai dati medesimi avviene per mezzo dell'individuazione di specifici profili di autorizzazione, stabiliti sulla base del livello di riservatezza di ciascun documento, fascicolo, sottofascicolo o inserto, secondo quanto stabilito dall'art. 27 del presente manuale; tali profili, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento.

Periodicamente, e comunque con cadenza almeno annuale, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Gli incaricati del trattamento di dati personali, sensibili o giudiziari, come precedentemente indicato, non possono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento degli stessi.

Per quanto riguarda l'accesso al Sistema di Gestione Informatica dei Documenti, le credenziali di autenticazione di ciascun operatore vengono consegnate dai medesimi in busta chiusa e sigillata al Responsabile della propria UOR; in caso di prolungata assenza o impedimento del soggetto incaricato del trattamento dei dati personali, sensibili o giudiziari e, qualora si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Responsabile della UOR è autorizzato ad utilizzare le credenziali contenute nella suddetta busta per procedere al trattamento, comunicandolo al titolare. Il soggetto titolare delle credenziali provvederà, al momento del proprio rientro in servizio, alla sostituzione della *password*, provvedendo all'inserimento della stessa in altra busta sigillata da consegnare nuovamente al suddetto Responsabile.

## Trattamento dei dati personali, sensibili o giudiziari senza l'ausilio di strumenti elettronici

Analogamente al trattamento dei medesimi dati svolto per mezzo di strumenti elettronici, sarà verificato il sussistere delle condizioni per l'accesso e il trattamento dei suddetti dati, da parte di ciascun utente o gruppo di utenti, con cadenza almeno annuale.

I documenti, sono controllati e custoditi dagli incaricati del trattamento per tutto il tempo di svolgimento dei relativi compiti; nell'arco di tale periodo gli incaricati medesimi si assicureranno che a tali documenti non accedano persone prive di autorizzazione.

L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solo previa autorizzazione; le persone ammesse sono identificate e registrate.

## Formazione dei documenti

I documenti informatici del Comune di Fenestrelle sono prodotti utilizzando i formati previsti dall'allegato n. 6 del presente manuale.

L'apposizione della firma digitale, volta a garantire l'attribuzione certa della titolarità del documento e la sua integrità, avviene previa conversione in un formato, tra quelli previsti dalle Linee guida AgID, che garantisca la leggibilità, l'interscambiabilità, la non alterabilità,

l'immutabilità nel tempo del contenuto e della struttura del documento medesimo (ad esempio il PDF/A); l'acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati aventi le medesime caratteristiche.

L'apposizione della firma digitale o di altre eventuali sottoscrizioni elettroniche, nonché la validazione temporale del documento sottoscritto digitalmente avvengono in conformità di quanto sancito dalla vigente normativa in materia.

La sottoscrizione del documento con firma digitale avviene prima dell'effettuazione della registrazione di protocollo.

### **Sicurezza delle registrazioni di protocollo**

L'accesso al registro di protocollo al fine di effettuare le registrazioni o di apportare modifiche è consentito soltanto al personale abilitato.

Di norma i dipendenti che operano nell'ambito dei vari uffici dell'Ente sono abilitati ad accedere esclusivamente ai dati di protocollo dei documenti da essi prodotti, ad essi assegnati o, comunque, di competenza del proprio ufficio di riferimento.

Ogni registrazione di protocollo viene memorizzata dal Sistema di Gestione Informatica dei Documenti, unitamente all'identificativo univoco dell'autore che l'ha eseguita e alla data e all'ora della stessa.

Eventuali modifiche, autorizzate ai sensi dell'art. 28 del presente manuale, vengono registrate per mezzo di log di sistema che mantengono traccia dell'autore, della modifica effettuata, nonché della data e dell'ora; il Sistema mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione.

Il Sistema non consente la modifica del numero e della data di protocollo; in tal caso l'unica possibile modifica è l'annullamento della registrazione stessa di cui, analogamente al caso precedente, il Sistema manterrà traccia. L'annullamento di una registrazione di protocollo deve sempre essere accompagnato da autorizzazione scritta del Responsabile della gestione documentale e il SGID deve recare, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione.

L'impronta digitale del documento informatico, associata alla registrazione di protocollo del medesimo è generata utilizzando una funzione di hash, conforme a quanto previsto dalla normativa vigente.

Al fine di garantire l'immodificabilità delle registrazioni di protocollo, il Sistema permette, al termine della giornata lavorativa, la produzione del registro giornaliero delle registrazioni di protocollo, in formato digitale; tale registro, formato nel rispetto di quanto previsto nel manuale di conservazione, sarà trasferito nell'arco della giornata lavorativa successiva, alla struttura di conservazione accreditata di cui il Comune si serve, secondo quanto previsto dall'articolo 3 del presente manuale.

### **Gestione dei documenti e sicurezza logica del Sistema**

I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano immodificabili e non eliminabili; l'accesso ad essi, da parte degli utenti

interni all'AOO, avviene soltanto attraverso il Sistema medesimo, previa la suddetta procedura di identificazione informatica e nel rispetto dei profili di autorizzazione di ciascun utente.

Il Sistema consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il Sistema effettua, inoltre, il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni (log di sistema) sono protette al fine di non consentire modifiche non autorizzate. I dati registrati nei file di log sono raccolti, memorizzati e conservati dal sistema informatico in conformità alla normativa vigente. Le informazioni contenute nei file di log possono essere messe a disposizione dell'autorità giudiziaria, la quale può richiedere la non cancellazione e la conservazione di tali file per un periodo più lungo di quanto disposto dalla legge.

Il Sistema e tutti i documenti e dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici mediante l'attivazione di firewall gestito da Elnet e antivirus gestito da Alpmidia Communication mantenuti regolarmente aggiornati ogni qualvolta venga rilasciato un aggiornamento dal fornitore.

Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dall'AOO e il Sistema di Gestione Informatica dei Documenti, vengono tenuti costantemente aggiornati, per mezzo dell'installazione degli aggiornamenti periodici che i fornitori rendono disponibili.

### **Misure da adottare in caso di violazione dei dati personali**

Qualora si ravvisi un'avvenuta violazione dei dati personali, il responsabile del trattamento dei dati notifica, con le modalità previste dall'art. 33 del Regolamento Europeo sulla Protezione dei Dati n. 679 del 2016, la violazione all'Autorità di Controllo competente (il Garante per la Protezione dei Dati Personali) entro 72 ore da quando sia venuta a conoscenza della medesima. Qualora tale violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Ente comunica la violazione all'interessato, secondo le modalità previste dall'art. 34 del suddetto Regolamento Europeo (n.679/2016).

### **Backup e ripristino dell'accesso ai dati**

Il Backup dei dati contenuti nel Sistema di gestione informatica dei documenti avviene nelle modalità descritte nel piano di backup, DR e ripristino dell'Ente; il ripristino dei dati avviene nell'arco temporale massimo di 4 giorni comunque sempre nel rispetto dei tempi previsti dalla vigente normativa in materia.

Per i dettagli tecnici e le modalità operative si rimanda al suddetto piano backup, DR e ripristino dell'Ente, di cui si allega estratto al presente allegato.

Le copie di dati eseguite in locale sono custodite, sotto chiave, al fine di evitare accessi non autorizzati e trattamenti non consentiti.

Supporti riscrivibili, eventualmente utilizzati dal Comune, contenenti dati sensibili o giudiziari, possono venire cancellati e riutilizzati esclusivamente nel caso in cui le informazioni in essi contenute non siano intelligibili e in alcun modo ricostruibili.

Qualora dati sensibili e giudiziari vengano memorizzati su supporti rimovibili non riscrivibili, una volta che sia cessato lo scopo per cui tali dati sono stati memorizzati, i supporti vengono distrutti.

### **Trasmissione e interscambio dei documenti**

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno dell'AOO avviene esclusivamente per mezzo del Sistema di Gestione Informatica dei Documenti; nessun'altra modalità è consentita, al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati.

La trasmissione di documenti informatici al di fuori dell'Ente avviene tramite PEC o mediante i meccanismi dell'interoperabilità di cui al Sistema Pubblico di Connettività e Cooperazione (SPC), utilizzando le informazioni contenute nella segnatura di protocollo.

Le informazioni relative alla segnatura di protocollo sono strutturate in un file XML conforme alle specifiche contenute nelle Linee guida AgID relative alla produzione, gestione e conservazione del documento informatico.

### **Conservazione dei documenti**

I documenti informatici registrati sul SGID sono affidati per la conservazione digitale ad un soggetto conservatore accreditato dall'AgID, che svolge tale attività in conformità a quanto sancito dalle regole tecniche contenute nelle Linee guida AgID. Il trasferimento in conservazione avviene mediante la produzione di pacchetti di versamento, basati su uno schema XML conforme a quanto previsto nello stesso manuale di conservazione.

### **Disaster recovery e continuità operativa**

Il Comune di Fenestrelle si è dotato di un sistema di disaster recovery, gestito da un fornitore esterno, in grado di garantire il ritorno alla normale operatività in caso di eventi calamitosi, prevedendo il ripristino dei dati nell'arco temporale massimo di n. 4 giorni e comunque sempre nel rispetto dei tempi previsti dalla vigente normativa in materia.

Per i dettagli tecnici e le modalità operative si rimanda al piano di disaster recovery dell'Ente

### **Accesso di Utenti esterni al Sistema**

L'esercizio del diritto di accesso da parte di utenti esterni al Sistema viene effettuato nel rispetto di quanto sancito dalla legge 241/90 e s.m.i., dal D. Lgs. 196/03 e s.m.i. e dal Regolamento Europeo sulla Protezione dei Dati n. 679 del 2016.

Qualora l'utente esterno decida di esercitare il proprio diritto di accesso rivolgendosi direttamente all'URP o ad altro sportello allo scopo predisposto, la consultazione deve avvenire in modo che siano resi visibili soltanto dati o notizie che riguardino il soggetto interessato ed adottando gli opportuni accorgimenti (ad es. il posizionamento del monitor) volti ad evitare la diffusione di informazioni di carattere personale.

### **Piani formativi del personale**

Ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, il Comune predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo applicativi software per la gestione dei documenti informatici;
- utilizzo del Sistema di Gestione Informatica dei Documenti;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative al documento informatico, alla gestione documentale e alla conservazione digitale a norma;
- fascicolazione dei documenti informatici;
- gestione dei fascicoli informatici;
- aggiornamento sui temi suddetti.

### **Monitoraggio periodico del funzionamento del Sistema**

Il Responsabile della gestione documentale dell'Ente effettua periodiche verifiche sul corretto funzionamento del Sistema di Gestione Informatica dei Documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale. I log di sistema sono comunque conservati e protetti in modo da consentire successive verifiche che dovessero risultare necessarie sullo svolgimento di tutte le operazioni rilevanti al fine della sicurezza dei dati, effettuate sul sistema.

### **Misure di tutela e garanzia**

Qualora l'Ente adotti misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere all'esecuzione, riceverà dall'installatore una descrizione scritta dell'intervento che ne attesti la conformità ai criteri di protezione dei dati sensibili, personali e giudiziari previsti dalla normativa.

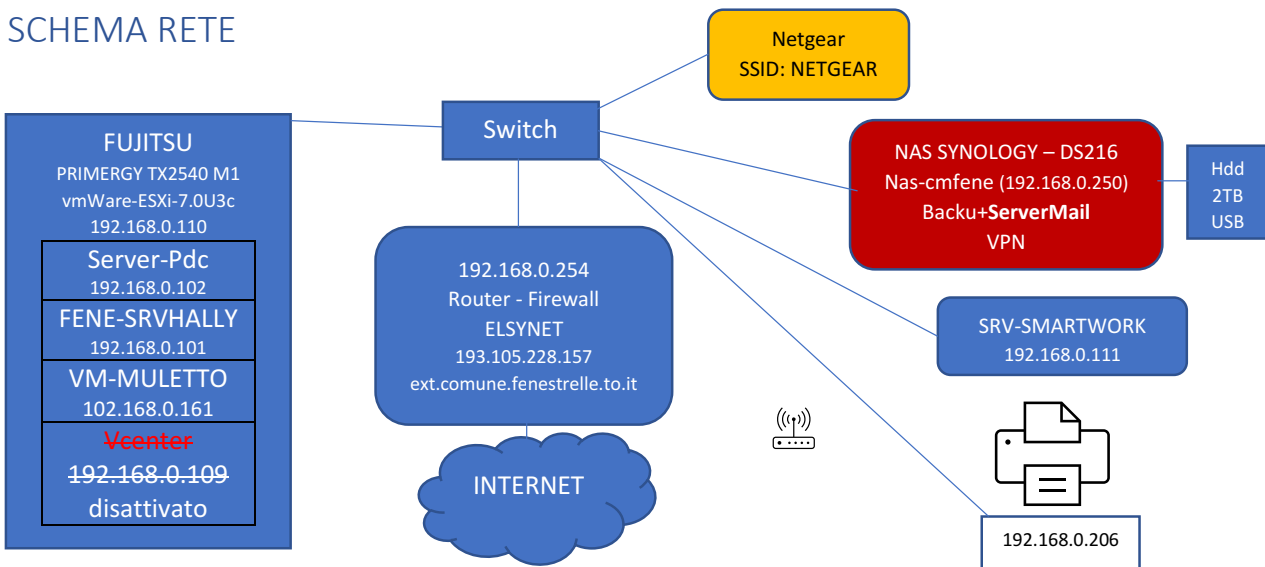
# Site Administrator Manual

## *ESTRATTO BACKUP, DR e Ripristino*

### Comune di Fenestrelle

Revisioni		
Aggiornamento	Tecnico Riferimento	Note
08.03.2022	DM	
14.04.2022	DM	
13.05.2022	SR	Aggiunta foto armadio
08.08.2022	DM	Descrizione dettagliata Piano Backup e Licenze
14.10.2022	DM	Estartto Backup, DR, Ripristino

# SCHEMA RETE



## PIANO DI BACKUP E RIPRISTINO

FASE 0a – [19:30 LMV] Copia dati (Server → NAS) con script robocopy

FASE 0b – [19:30 MGS] Copia dati (Server → NAS) con script robocopy

I singoli file presenti nelle cartelle condivise del server sono salvati con operazioni pianificate sul NAS synology nella condivisione <\\192.168.0.250\backup\SALVATAGGIO>.

Sono presenti due script schedulati rispettivamente LMV e MGS alle 19.30.

Utilità di pianificazione

Nome	Stato	Attivazione	Prossima esecuzione	Ultimi
Backup Dati ...	Pronto	Alle 19:30 ogni lunedì, mercoledì, venerdì di ogni settimana, a partire dal giorno 01/04/2019	08/08/2022 19:30:00	08/08/08/08
Backup Dati ...	Pronto	Alle 19:30 ogni martedì, giovedì, sabato di ogni settimana, a partire dal giorno 01/04/2019	09/08/2022 19:30:00	08/08/08/08
Optimize Sta...	Pronto	Quando il computer è inattivo		01/04/30/06
Optimize Sta...	Pronto	Quando il computer è inattivo		03/06/08/08
ShadowCop...	Pronto	Definite più attivazioni	09/08/2022 07:00:00	08/08/08/08
ShadowCop...	Pronto	Definite più attivazioni	09/08/2022 07:30:00	08/08/08/08

Quando si crea un'attività, è necessario specificare l'azione che dovrà essere eseguita al suo avvio. Per creare un'azione, fare clic su Nuova. Per modificare le azioni, aprire le pagine delle proprietà dell'attività tramite il comando Proprietà.

Operazione	Dettagli
Avvio programma	D:\salva_server_su_NAS_LMV.bat

```
@ECHO OFF
robocopy "D:\ClientsApps" "\\192.168.0.250\backup\SALVATAGGIO\LMV\ClientsApps" /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_LMV.log
robocopy "D:\Condivisi" "\\192.168.0.250\backup\SALVATAGGIO\LMV\Condivisi" /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_LMV.log
robocopy "D:\Delibere" "\\192.168.0.250\backup\SALVATAGGIO\LMV\Delibere" /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_LMV.log
robocopy "D:\Intranet" "\\192.168.0.250\backup\SALVATAGGIO\LMV\Intranet" /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_LMV.log
robocopy "D:\Modelli" "\\192.168.0.250\backup\SALVATAGGIO\LMV\Modelli" /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_LMV.log
robocopy "D:\Protocollo" "\\192.168.0.250\backup\SALVATAGGIO\LMV\Protocollo" /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_LMV.log
robocopy "D:\Tecnico" "\\192.168.0.250\backup\SALVATAGGIO\LMV\Tecnico" /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_LMV.log
robocopy "D:\Uffici" "\\192.168.0.250\backup\SALVATAGGIO\LMV\Uffici" /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_LMV.log
robocopy "D:\Users Shared Folders" "\\192.168.0.250\backup\SALVATAGGIO\LMV\Users Shared Folders" /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_LMV.log
```

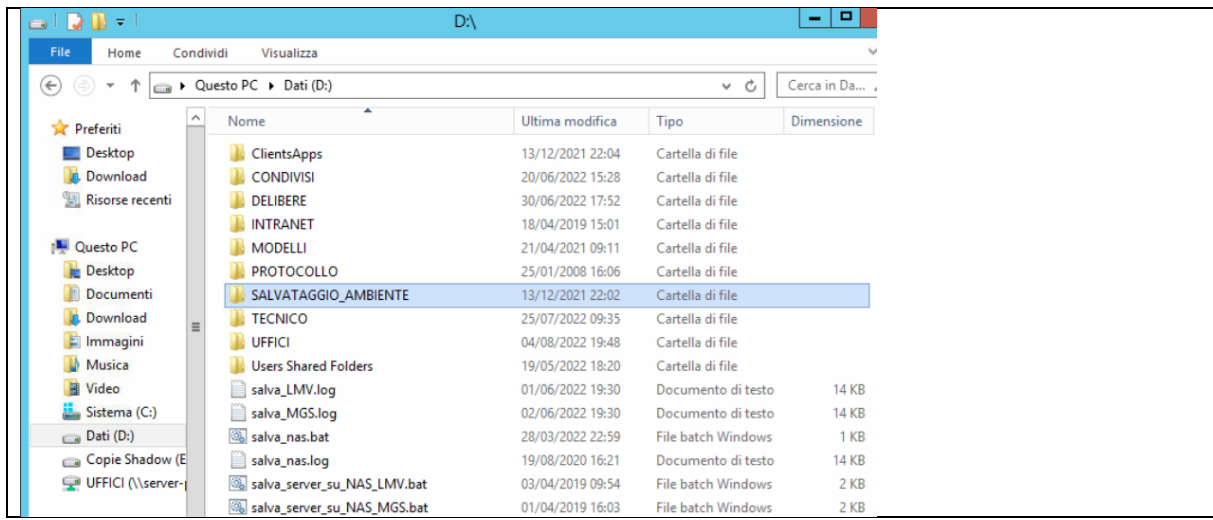
REM pause

Quando si crea un'attività, è necessario specificare l'azione che dovrà essere eseguita al suo avvio. Per creare un'azione, fare clic su Nuova. Per modificare le azioni, aprire le pagine delle proprietà dell'attività tramite il comando Proprietà.

Operazione	Dettagli
Avvio programma	D:\salva_server_su_NAS_MGS.bat

```
@ECHO OFF
robocopy "D:\Condivisi" "\\192.168.0.250\backup\SALVATAGGIO\MGS\Condivisi" /PURGE /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_MGS.log
robocopy "D:\Delibere" "\\192.168.0.250\backup\SALVATAGGIO\MGS\Delibere" /PURGE /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_MGS.log
robocopy "D:\Intranet" "\\192.168.0.250\backup\SALVATAGGIO\MGS\Intranet" /PURGE /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_MGS.log
robocopy "D:\Modelli" "\\192.168.0.250\backup\SALVATAGGIO\MGS\Modelli" /PURGE /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_MGS.log
robocopy "D:\Protocollo" "\\192.168.0.250\backup\SALVATAGGIO\MGS\Protocollo" /PURGE /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_MGS.log
robocopy "D:\Tecnico" "\\192.168.0.250\backup\SALVATAGGIO\MGS\Tecnico" /PURGE /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_MGS.log
robocopy "D:\Uffici" "\\192.168.0.250\backup\SALVATAGGIO\MGS\Uffici" /PURGE /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_MGS.log
robocopy "D:\Users Shared Folders" "\\192.168.0.250\backup\SALVATAGGIO\MGS\Users Shared Folders" /PURGE /NDL /E /TEE /NP /XO /R:0 /LOG+:d:\salva_MGS.log
```

REM pause



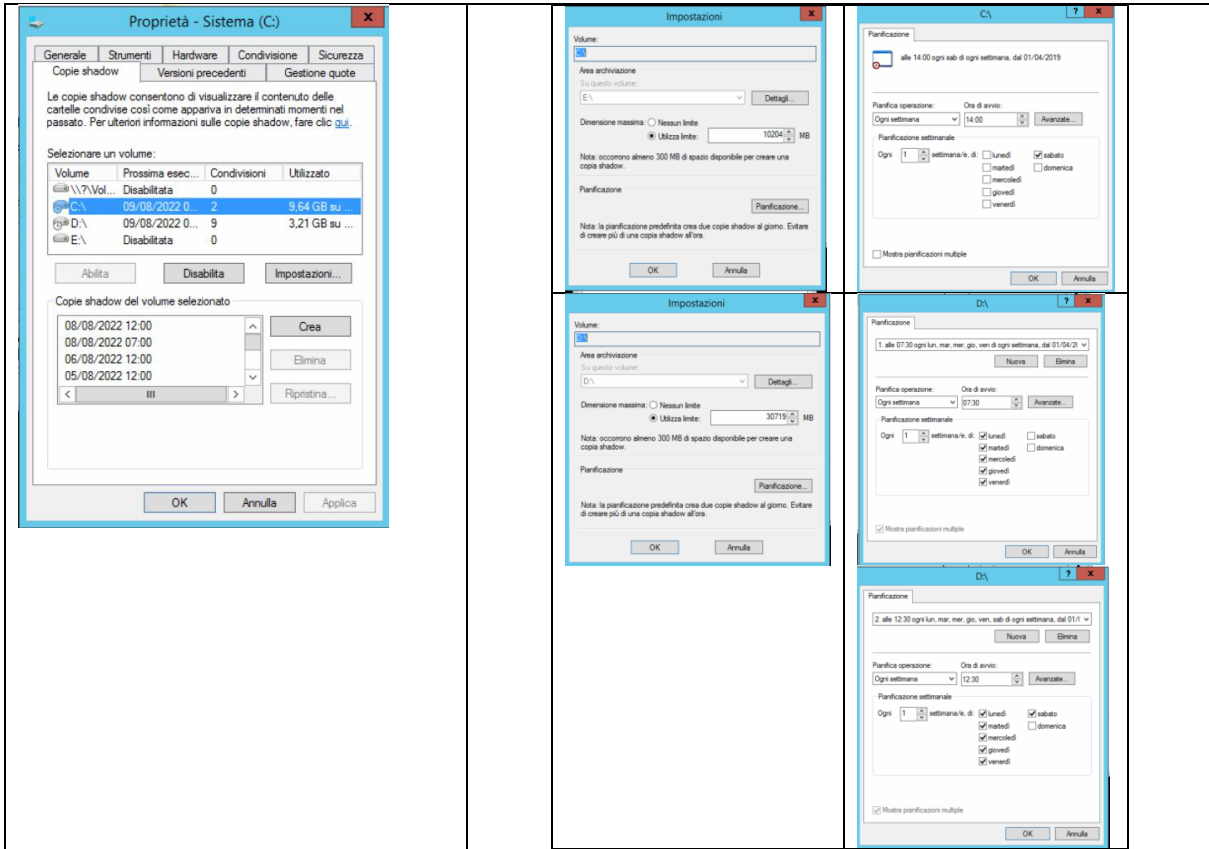
FASE 1a – [14:00 S] Shadow Copy (Versioni Precedenti) disco C:

FASE 1b – [7:30,12:30 L-V “D:”] Shadow Copy (Versioni Precedenti) disco D:

Le copie shadow sono attive sul disco C: e D:, entrambe sono eseguite sul disco E: e consentono di visualizzare il contenuto delle cartelle condivise così come appariva in determinati momenti nel passato.

I dettagli sono indicati nelle immagini seguenti.

Ogni utente può facilmente recuperare una versione precedente di qualsiasi file nelle cartelle condivise del server, semplicemente cliccando su di esso o sulla cartella superiore e selezionare dal menu contestuale la voce “versione precedenti”:



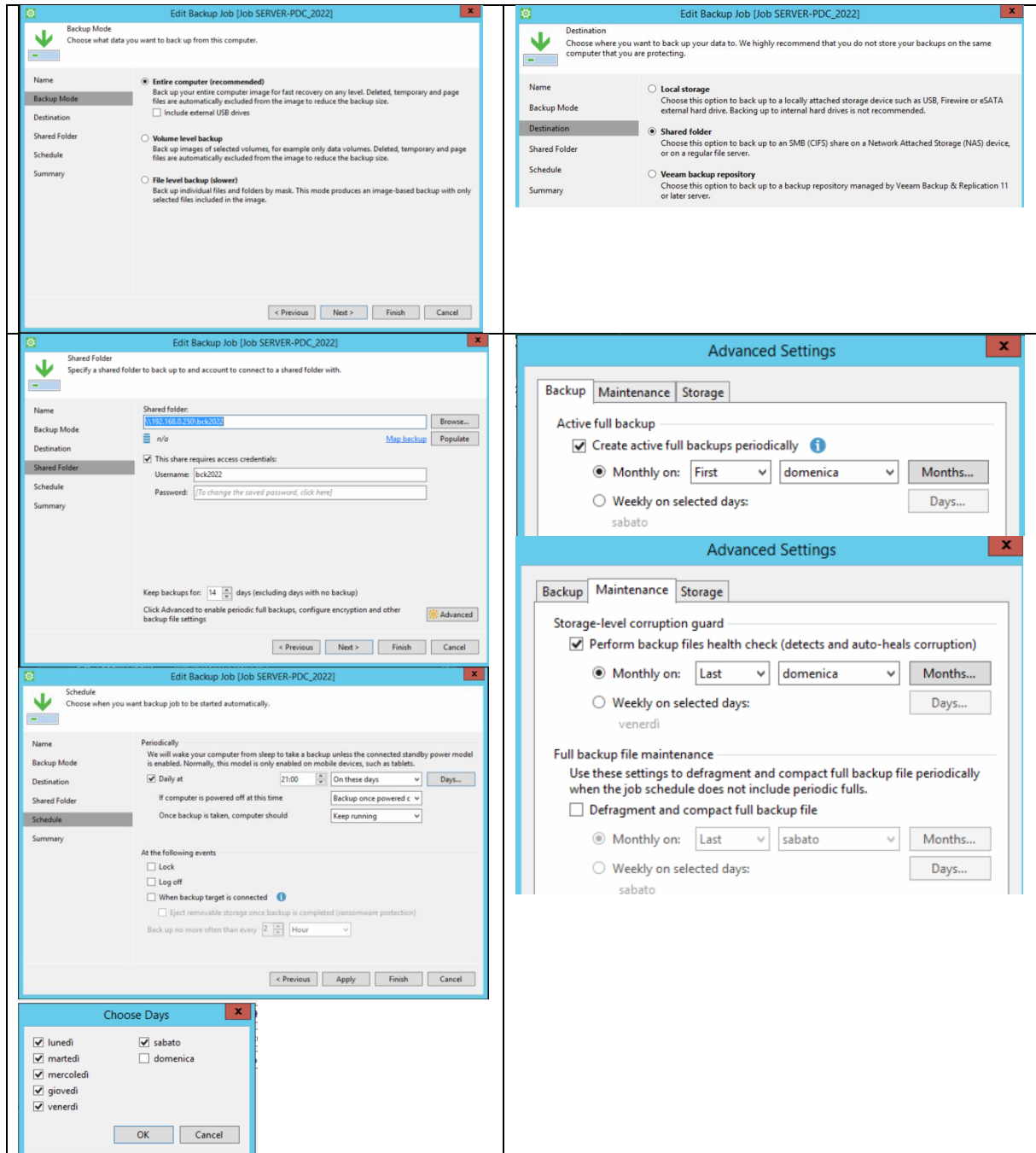
# FASE 2a – [21:00 L-S] Backup Server-PDC (Server→NAS) con Veeam Agent

Server-PDC	Win Srv 2012 R2 Std	Veeam Agent for Microsoft Windows 5.0.1.4584 Free Edition
------------	---------------------	---

La VM viene salvata interamente utilizzando il software Veeam Agent for Microsoft Windows. Il software è installato direttamente nel sistema operativo della VM.

La Pianificazione è: Lun-Sab 21:00.

La destinazione del backup è la condivisione bck2022 sul Nas Synology (\\192.168.0.250\bck2022). Per maggior sicurezza questa condivisione è accessibile solo all'utente bck2022 con la sua password configurata direttamente in Veeam. La Rotazione è di 14 giorni (esclusi i giorni senza backup).



# FASE 2b – [21:30 L-V] Backup FENE-SRVHALLEY (Server→NAS) con Veeam Agent

FENE-SRVHALLEY	Win Srv 2012 R2 Std	Veeam Agent for Microsoft Windows 5.0.3.4708 Free Edition
----------------	---------------------	---

La VM viene salvata interamente utilizzando il software Veeam Agent for Microsoft Windows. Il software è installato direttamente nel sistema operativo della VM.

La Pianificazione è: Lun-Ven 21:30.

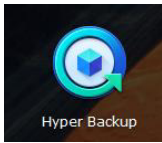
La destinazione del backup è la condivisione bck2022 sul Nas Synology (\\192.168.0.250\bck2022). Per maggior sicurezza questa condivisione è accessibile solo all'utente bck2022 con la sua password configurata direttamente in Veeam. La Rotazione è di 14 giorni (esclusi i giorni senza backup).

The screenshots illustrate the configuration steps for a Veeam backup job:

- Backup Mode:** Selected as "Entire computer (recommended)".
- Destination:** Selected as "Shared folder".
- Shared Folder:** Path is \\192.168.0.250\bck2022, Username is bck2022.
- Advanced Settings - Backup:** "Create active full backups periodically" is checked, set to "Monthly on: First" of the month on "domenica".
- Advanced Settings - Storage:** "Perform backup files health check" is checked, set to "Monthly on: Last" of the month on "domenica". "Full backup file maintenance" is also configured for "sabato".
- Schedule:** Set to "Periodically" with a "Daily at 21:30" on "On these days".
- Choose Days:** A dialog box showing days from lunedì to venerdì are selected.

## FASE 3 - Backup Caselle di posta (NAS → HDD USB 2TB) con Hyper Backup

Le cartelle e le applicazioni presenti sul NAS, indicate nelle immagini successive, sono salvate su un disco esterno da 2TB direttamente collegato al NAS Synology (usbshare1/BckFene\_1) con pianificazione giornaliera e 30 giorni di rotazione



The image displays four screenshots of the Hyper Backup configuration interface, arranged in a 2x2 grid.

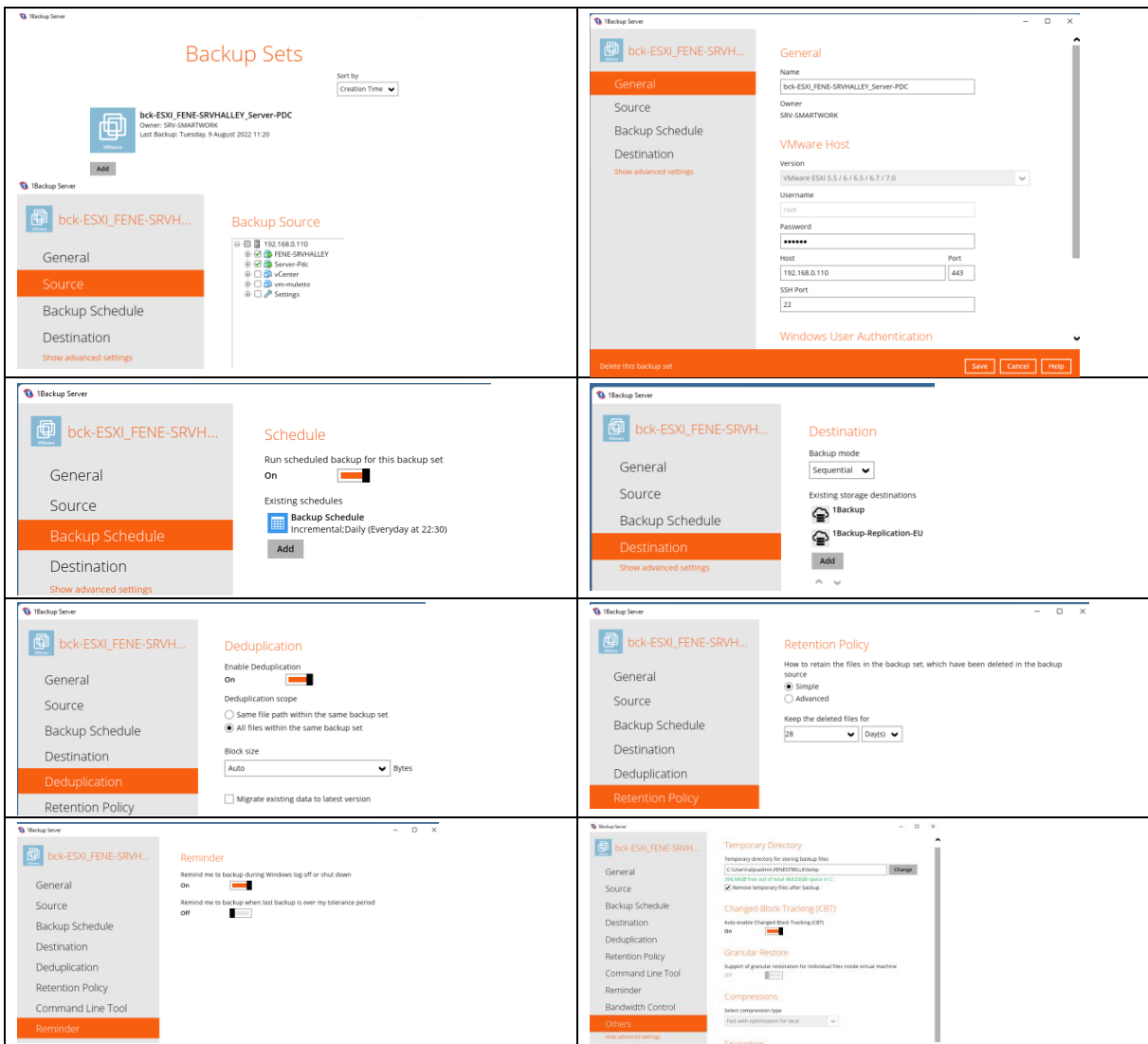
- Top Left:** "Impostazioni attività" - "Cartelle" tab. Shows a tree view for "Volume 1 (SHR)" with folders like Backup, BCK2022, CED, homes, web, and web\_packages selected. A "Suggerimento" (Suggestion) dialog box is open, suggesting to exclude subfolders. Buttons: "Annulla", "OK".
- Top Right:** "Impostazioni attività" - "Applicazione" tab. Lists applications: MariaDB 10, OAuth Service, Synology Mail Server, USB Copy, and Universal Search. Each has a checkbox and a description. A note at the bottom states: "Nota: Sono elencate solo le applicazioni supportate per il backup." Buttons: "Annulla", "OK".
- Bottom Left:** "Impostazioni attività" - "Programmazione" tab. Shows scheduling options: "Nessuna pianificazione", "Esegui nei giorni seguenti" (selected, "Giornaliero"), and "Esegui alla data seguente". Includes fields for start time (03:00), frequency (Ogni giorno), and end time (03:00). A "Controllo di integrità del backup" section is at the bottom. Buttons: "Annulla", "OK".
- Bottom Right:** "Impostazioni attività" - "Rotazione" tab. Shows "Attiva rotazione backup" checked. Options include "Dalle versioni più recenti" (selected), "Smart Recycle", and "Conservazione personalizzata". "Numero massimo di versioni conservate" is set to 30. A retention diagram shows a timeline with markers for "4 settimane più vicino" and "2 settimane più vicino". Buttons: "Annulla", "OK".

FASE 4 – [22:30 Daily] Backup VM FENE-SRVHALLEY e Server-PDC → CLOUD

Sul Srv-Smartwork (miniserver fisico) è installato l'agente di **1Backup l'infrastruttura certificata AGID**. L'Agente provvede ad eseguire il backup delle VM "SRV-HALLEY" e "Server-PDC", che ci sono sull'Hypervisor VMWARE ESXI collegandosi alla console stessa di VMWARE (192.168.0.110) tramite "indirizzo IP, root, password".

Viene inviata una mail con il risultato dell'operazione a daniele.martin@alpimedia.com.

Modalità	Macchina intera (deduplica)
Pianificazione	Daily 22:30
Posizione1	1Backup
Posizione2	1Backup-Replication-EU



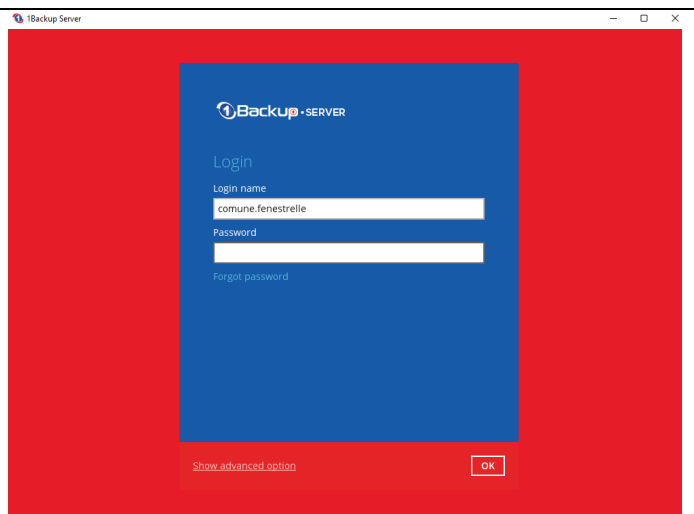
**Agents (1 risultato)**

Lista COMUNE.FENESTRELLE

Info	
Agent	comune.fenestrelle
Customer	
Server	backup@it.1backup.it
Administrator	alpimedia@
Agent	SERVER
Password	*****
Status	ENABLE
Type	PAID
Registration Date	19/05/2022
Expiration Date	never
Quota [GB]	800
Last Job	09/08/2022 11:20
Warning Jobs	0

**Contact info**

Name	comune.fenestrelle
Email	daniele.martin@alpimedia.com



Pwd: BckFene2022!#.

