

Backup PSN

Manuale d'uso del servizio

Guida Utente

Data: 24/03/2025

PSN_Backup_ManualeUtente_v5.7

Ed. 5 – ver. 5.7

QUESTA PAGINA È LASCIATA INTENZIONALMENTE
BIANCA

STATO DEL DOCUMENTO

TITOLO DEL DOCUMENTO			
HANDBOOK HIGH LEVEL DESIGN			
EDIZ.	REV.	DATA	AGGIORNAMENTO
1	1.0	22/12/2022	Prima versione del documento
2	2.0	05/05/2023	Aggiornamento configurazione del servizio di Backup.
3	3.0	18/05/2023	Aggiornamento immagini, Plans, Operazioni di backup
3	3.1	31/05/2023	Aggiornamento Cifratura, Regole FW, plugin vCloud
3	3.2	23/06/2023	Aggiunto Prerequisiti regole FW
3	3.3	23/06/2023	Aggiunta capitolo aggiornamento software
3	3.4	30/06/2023	Integrato nel capitolo 6 il tema del Backup con agent
3	3.5	04/07/2023	Modifiche Giustino
3	3.6	12/07/2023	Modificata sezione Job schedulazione di backup. Aggiunti dettagli Dashboard e Plan
4	4.0	09/2023	Aggiornamento configurazione Golden copy
5	5.0	02/2024	Aggiunta URL portale di backup Modalità di verifica dei logs
5	5.1	03/2024	Inserito dettaglio Reports <i>Utilizzo storage backup</i> . Inserito nuovo paragrafo con dettaglio cancellazione VM group e sospensione backup relativo ad un VM group
5	5.2	21/03/2024	Inserita frase capitolo 11 Operazioni di restore
5	5.3	02/07/2024	Inserito dettaglio per installazione client SPC
5	5.4	03/12/2024	Inserite specifiche per configurazione Hypervisor Oracle OCI

5	5.5	14/01/2025	Corrette imprecisioni descrizione dei servizi
5	5.6	12/02/2025	Aggiornamento subnet di backup con agent (per saturazione vlan precedenti)
5	5.7	24/03/2025	Corretto refuso al capitolo 7.1; Aggiunti paragrafi troubleshooting e Punti di Attenzione

NUMERO TOTALE PAGINE:	118
-----------------------	-----

AUTORE:	
Team di lavoro PSN	

REVISIONE:	
Referente del Servizio	

APPROVAZIONE:	
Direttore del Servizio	

INDICE

1	Definizioni e Acronimi.....	11
1.1	DEFINIZIONI	11
1.2	ACRONIMI	11
	Executive Summary	12
1.3	SCOPO DEL DOCUMENTO	12
2	Descrizione del servizio di Backup.....	13
3	Attività preliminari	15
3.1	ACCESSO ALLA CONSOLE DI AMMINISTRAZIONE DEL SERVIZIO.....	15
4	Console di amministrazione del servizio	17
4.1	DASHBOARD.....	17
4.2	PROTECT.....	18
4.2.1	<i>Virtualization</i>	19
4.2.2	<i>Servers</i>	19
4.2.3	<i>Databases</i>	20
4.3	JOB.....	20
4.4	REPORTS	22
4.4.1	<i>Utilizzo storage di backup</i>	24
4.5	MONITORING - ALERTS	25
4.6	MANAGE	26
4.7	WEB CONSOLE.....	27
4.8	PLUGIN VCLLOUD.....	27
5	Pianificazione schedulazione dei job di backup	30
5.1.1	<i>Modifica schedulazione jobs</i>	35
6	Configurazione dei client IaaS Industry Standard	37
6.1	PREREQUISITI PER BACKUP AGENT INDUSTRY STANDARD	37
6.1.1	<i>IMPORT subnet per backup con agent Industry standard</i>	37
6.1.2	<i>Personalizzazione VM per backup con agent</i>	37

6.2	INSTALLAZIONE DI UN SERVER CLIENT (TENANT ADMINISTRATOR)	39
6.2.1	<i>Client Windows</i>	39
6.2.2	<i>Client Linux</i>	44
6.3	AGGIORNAMENTO DEL CLIENT CON ULTERIORI AGENT	48
6.4	UPGRADE SOFTWARE DEL CLIENT GIÀ REGISTRATO	51
7	Configurazione dei client Secure Public Cloud	53
7.1	PREREQUISITI PER BACKUP AGENT SECURE PUBLIC CLOUD	53
7.2	INSTALLAZIONE DI UN SERVER CLIENT (TENANT ADMINISTRATOR)	53
7.2.1	<i>Client Windows</i>	54
7.2.2	<i>Client Linux</i>	59
7.3	AGGIORNAMENTO DEL CLIENT CON ULTERIORI AGENT	62
7.4	UPGRADE SOFTWARE DEL CLIENT GIÀ REGISTRATO	65
8	Configurazione dei client PSN MANAGED ORACLE CLOUD	67
8.1	PREREQUISITI PER BACKUP AGENT ORACLE CLOUD	67
8.2	INSTALLAZIONE DI UN SERVER CLIENT (TENANT ADMINISTRATOR)	67
8.2.1	<i>Client Linux su PSN Managed Oracle Cloud</i>	67
8.3	AGGIORNAMENTO DEL CLIENT CON ULTERIORI AGENT	71
8.4	UPGRADE SOFTWARE DEL CLIENT GIÀ REGISTRATO	75
9	Configurazione di un Hypervisor PSN MANAGED ORACLE CLOUD	77
10	Aggiunta e configurazione VM group	80
10.1	CANCELLAZIONE VM GROUP E SOSPENSIONE JOB DI BACKUP RELATIVO AL VM GROUP	85
11	Operazioni di backup	88
11.1	BACKUP DI TIPO FILE SYSTEM	88
11.2	BACKUP & RESTORE VIRTUAL MACHINE	90
11.3	BACKUP DATABASE	100
11.4	VERIFICA DEI LOG DEI JOB DI BACKUP	104
12	Backup Golden Copy	107

12.1	LIVELLI DI SICUREZZA GOLDEN COPY	107
12.2	EFFETTUARE BACKUP CON OPZIONE GOLDEN COPY.....	109
13	Operazioni di restore	110
14	Encryption	113
15	Best Practices & Troubleshooting	114
1.	VIRTUAL MACHINE WAS NOT FOUND.....	115
2.	[*] NO VIRTUAL MACHINES WERE DISCOVERED FOR [*]. CHECK THE CONTENT AND FILTERS. SOURCE: , PROCESS: VSDISCOVERY.....	115
3.	CAN NOT CREATE A SNAPSHOT WHEN ANOTHER TASK IS ALREADY RUNNING.....	115
4.	INSUFFICIENT FREE SPACE AVAILABLE TO CREATE A SNAPSHOT OF THE VIRTUAL MACHINE.....	115
5.	THE VIRTUAL MACHINE REPORTS THAT IT HAS VIRTUAL DISKS THAT NEED CONSOLIDATION AND THIS COULD NOT BE PERFORMED AUTOMATICALLY.....	116
6.	UNABLE TO CREATE A SNAPSHOT ON VIRTUAL MACHINE [*] BECAUSE ANOTHER TASK IS ALREADY RUNNING ON THE VIRTUAL MACHINE. THE JOB WILL GO TO PENDING AND BE RETRIED. SOURCE: PSNBCKCMSDCAC, PROCESS: JOBMANAGER**	116
7.	CLIENT IS ALREADY BEING BACKED UP BY JOB [*] FROM PARENT JOB [*]	116
16	Punti di attenzione	117
17	FAQ	117
17.1	È POSSIBILE CANCELLARE UN JOB DI BACKUP PER LIBERARE SPAZIO STORAGE? 117	
17.2	COME SI CANCELLANO I CLIENT?	117
17.3	È GARANTITA LA PRIVACY? COME VIENE SALVAGUARDATO L'ACCESSO AI DATI? 118	
17.4	COME POSSO RICHIEDERE ASSISTENZA PER IL SERVIZIO?.....	118

LISTA DELLE FIGURE

Figura 1 – Overview Servizio Backup.....	13
Figura 2 – Login Console Backup	15
Figura 3 – Home Dashboard Commvault.....	16
Figura 4 - Dashboard Commvault	18
Figura 5 - Sezione Protect.....	18
Figura 6 - Sezione Virtualization	19
Figura 7 - Sezione Servers	19
Figura 8 - Sezione Databases	20
Figura 9 - Sezione Jobs.....	20
Figura 10 - Sezione Virtualization e Actions.....	21
Figura 11 - Sezione Reports.....	22
Figura 12 - Reports – AUTHCODE.....	23
Figura 13 - Report PSN Utilizzo Storage backup.....	24
Figura 14 - Sezione Monitoring	25
Figura 15 - Sezione Manage – Active servers	26
Figura 16 - Sezione Manage - Blackout window	26
Figura 17 - Sezione Web Console.....	27
Figura 18 - Console di backup plugin vCloud	27
Figura 19 - Dashboard plugin vCloud	28
Figura 20 - VM protected	28
Figura 21 - VM unprotected	28
Figura 22 - Active jobs.....	29
Figura 23 - Advanced View Dashboard	29
Figura 24 - Modifica schedulazione job	35
Figura 25 - Modifica schedulazione job per VM group.....	35
Figura 26 - Modifica schedulazione job per server.....	36
Figura 27 – Interfaccia configurazione VM NICS.....	38
Figura 28 – Interfaccia modifica VM NICS.....	38
Figura 29 – Steps installazione client Windows on IaaS IND STD	39
Figura 30 – Steps installazione client Linux on IaaS IND STD.....	44
Figura 31 – Steps installazione altri agent su Client on IaaS IND STD	48
Figura 32 – Monitoraggio job di “Installazione nuovo agent di backup on IaaS IND STD”	50
Figura 33 – Steps aggiornamento client on IaaS IND STD	51
Figura 34 – Steps installazione client Windows on SPC	54
Figura 35 – Steps installazione client Linux on SPC.....	59
Figura 36 – Steps installazione altri agent su Client on SPC	62
Figura 37 – Steps aggiornamento client agent on SPC	65
Figura 38 – Steps installazione client Linux on Oracle_OCI	68
Figura 39 – Steps Installazione altri agent su Client on Oracle_OCI.....	71
Figura 40 – Steps aggiornamento client on Oracle_OCI.....	75
Figura 41 – Configurazione Hypervisor on Oracle_CLOUD	77
Figura 42 – Configurazione VM GROUP	80
Figura 43 – Cancellazione VM GROUP.....	85

Figura 44 – Sospensione backup di un VM GROUP	86
Figura 45 – Configurazione FS backup	88
Figura 46 – Backup & restore VM.....	90
Figura 47 – Backup VM	92
Figura 48 – Check configurazione server FLR per “guest files restore Linux” servizi CLOUD	94
Figura 49 – Restore.....	95
Figura 50 – Restore guest files	96
Figura 51 – Monitoraggio jobs restore.....	97
Figura 52 – Configurazione hypervisor e VMGroups.....	98
Figura 53 – Configurazione backup database	101
Figura 54 – Verifica logs jobs	104
Figura 55 – Configurazione backup con Golden Copy	109
Figura 56 – Procedura restore	110
Figura 57 – Overview Encyption	113
Figura 58 – Knowledgebase Job Error	116

LISTA DELLE TABELLE

Tabella 1: Glossario Definizioni	11
Tabella 2: Glossario Acronimi	11

1 Definizioni e Acronimi

1.1 Definizioni

Definizione	Descrizione

Tabella 1: Glossario Definizioni

1.2 Acronimi

Acronimo	Descrizione
GCP	Google Cloud Platform
AWS	Amazon Web Services
RPO	Recovery Point Objective
RTO	Recovery Time Objective
VSA	Virtual Service Agent
CPU	Central Processing Unit
SLA	Service Level Agreement
VM	Virtual Machine
FAQ	Frequently Asked Questions
PSN	Polo Strategico Nazionale
DC	Data Center
DCRZ	Data Center Rozzano
RN	Region Nord
DCSS	Data Center Santo Stefano
IaaS	Infrastructure as a Service

Tabella 2: Glossario Acronimi

Executive Summary

1.3 *Scopo del documento*

Introduzione

Il presente documento descrive la soluzione di data protection messa a disposizione dal servizio di backup as a service di PSN ed è indirizzato agli addetti IT dei clienti che dovranno effettuare operazioni di backup e restore dei dati.

Prerequisiti

Questo manuale può essere fruito dagli addetti IT dell'amministrazione in possesso di conoscenze sui concetti di backup e dataprotection, con particolare familiarità con la terminologia e le funzionalità base della tecnologia Commvault su cui è costruito il servizio.

Struttura del Documento

Le istruzioni riportate in questo documento sono strutturate in aree distinte che permettono di svolgere attività semplici di configurazione, backup e restore.

In particolare, le istruzioni principali sono ripartite tra le seguenti aree:

- Attività preliminari
- Console di amministrazione del servizio
- Configurazione dei Client
- Operazioni di Backup
- Operazioni di Restore
- Encryption
- Best Practices & Troubleshooting
- Punti di attenzione
- FAQ

Documentazione

Il servizio di Backup PSN si basa su tecnologia Commvault. Per approfondire istruzioni e concetti contenuti in queste linee guida si consiglia di consultare la documentazione ufficiale online di CommVault, con riferimento alla versione in esercizio rilevabile dalla console nella sezione Overview della dashboard.

ContentStore disponibile al seguente indirizzo web:

<https://documentation.commvault.com/>

2 Descrizione del servizio di Backup

Il servizio PSN Backup consente, tramite un'unica console centralizzata, la gestione in piena autonomia della protezione dei dati sia on premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio non offre la possibilità di effettuare backup dei Datacenter personali del cliente.

Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise (datacenter PSN) che su cloud provider (Google GCP, Azure, Oracle Cloud).

I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database).

I dati di backup possono essere storicizzati in repository disponibili sul servizio stesso.



Figura 1 – Overview Servizio Backup

Il servizio di backup/restore garantisce al cliente, attraverso una console web centralizzata, totale autonomia per il salvataggio dei propri dati e naturalmente il recupero degli stessi, in caso di perdita dovuta a guasti hardware o malfunzionamenti del software. Il ripristino può avvenire ad una certa data in relazione alle copie di backup effettuate.

Attraverso il servizio gli utenti potranno provvedere a:

- Conservazione e svecchiamento dei dati del backup secondo policy di retention predefinite (7 giorni, 1 mese, 2 mesi, 3 mesi, 6 mesi, 1 anno, 10 anni);
- Monitoring dei jobs di backup e restore;
- Reportistica all'interno della console.

Trattandosi di un servizio «self-managed» l'utente ha completa autonomia nella scelta della policy di backup. Per ogni servizio IaaS è disponibile backup standard che copre esigenze di backup fino a 100GB per istanza. Raggiunta la soglia relativa al totale storage backup 100GBxVM la funzionalità di backup viene disabilitata, tranne nel caso in cui è stato contrattualizzato il servizio di backup.

3 Attività preliminari

Le istruzioni contenute in questo capitolo riguardano operazioni di base come l'accesso alla console di amministrazione.

3.1 Accesso alla console di amministrazione del servizio

Per accedere alla console di amministrazione del servizio è necessario connettersi al portale unico.

Dal portale è possibile cliccare su *Console BaaS* ed effettuare il login.

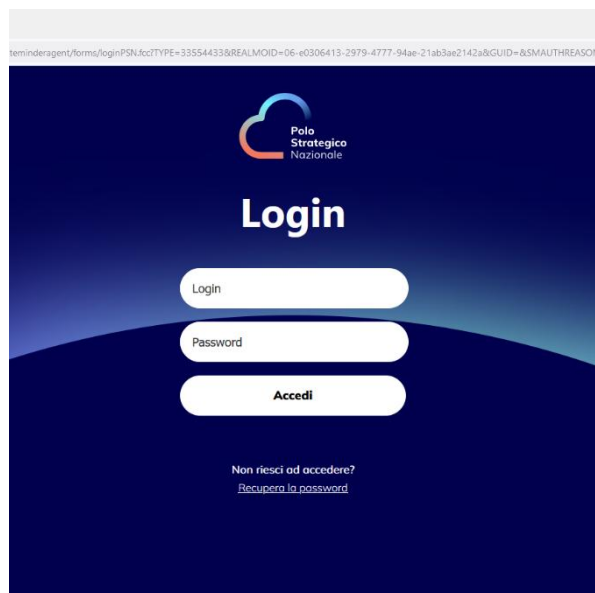


Figura 2 – Login Console Backup

In seguito al login si verrà indirizzati verso Region Nord o Region Sud.

Le due Region avranno URL di indirizzamento diversi. In base alla distribuzione geografica delle risorse, l'utente verrà indirizzato su una delle due region.

Una volta raggiunta la Console di Backup l'utente potrà navigare nella Home della Dashboard Commvault.

URL di connessione al portale di backup in caso di necessità:

<https://baas-nord.console.polostrategiconazionale.it>

<https://baas-sud.console.polostrategiconazionale.it>

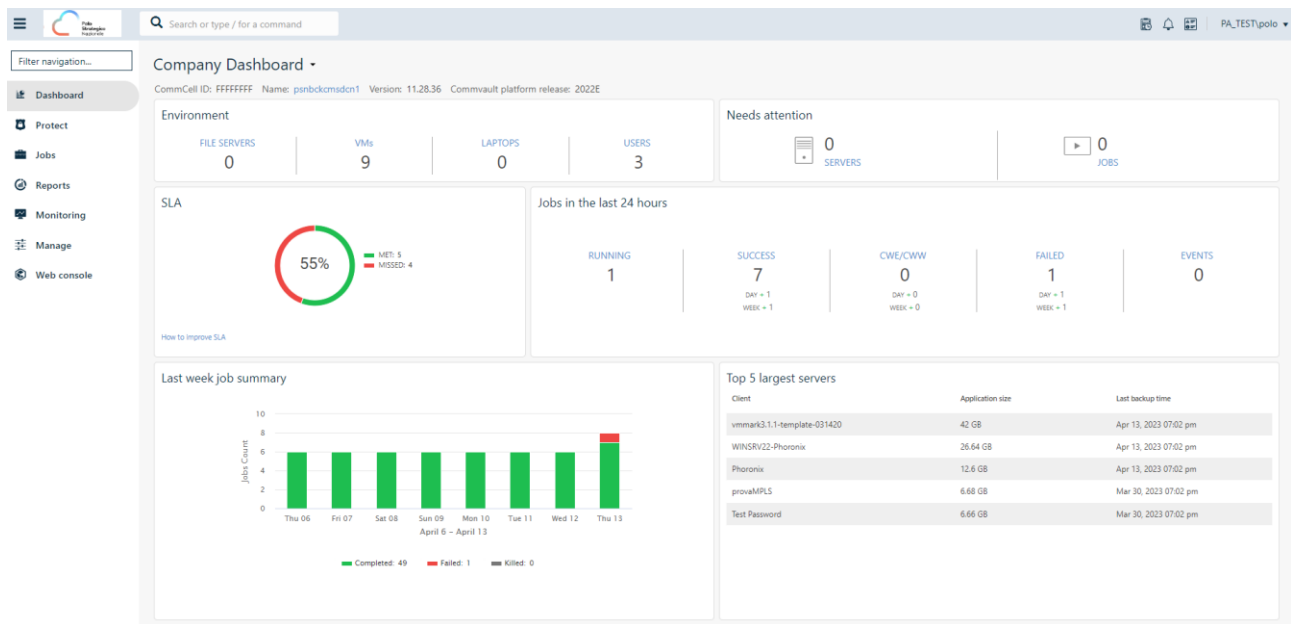


Figura 3 – Home Dashboard Commvault

4 Console di amministrazione del servizio

La console di amministrazione del servizio è l'interfaccia che consente l'utilizzo del servizio di backup attraverso cui è possibile:

- Configurare backup e restore, definire criteri di protezione dei dati, pianificare attività e monitorare le operazioni;
- Monitorare e gestire l'intero ambiente di data protection della propria infrastruttura IT in maniera centralizzata fornendo inoltre strumenti di analisi, reportistica e monitoring;
- Effettuare i backup (di server fisici, server virtuali, applicazioni, database, cloud system ed endpoint), stabilirne la frequenza in base ai requisiti di RPO e RTO;
- Raggruppare gli elementi oggetto di backup in diversi gruppi effettuando la segmentazione che si ritiene più opportuna (per unità di business, area geografica o altra classificazione).

All'interno è suddivisa in otto sezioni che è possibile selezionare attraverso il menu visualizzato sulla sinistra.

Le sezioni sono le seguenti:

- La Dashboard
- L'area di Protect
- La sezione di controllo dei Jobs
- L'area per l'accesso ai Reports
- La sezione di Monitoring
- L'area per la gestione (Manage) delle componenti per l'utilizzo del servizio
- La sezione per l'utilizzo dei Workflows per l'attivazione di ulteriori componenti di servizio
- La sezione di Web console per l'accesso al Download center

4.1 Dashboard

La Dashboard è la prima schermata che si presenta dopo aver effettuato il login al portale del servizio.

Essa visualizza un'anteprima delle informazioni più significative relativamente al servizio di backup che stiamo utilizzando.

Contiene le informazioni relative alle risorse oggetto di backup che abbiamo configurato (**Environment**) e contestualmente le risorse che necessitano di attenzione (**Needs attention**), ad esempio perché non più raggiungibili dal servizio di backup.

Inoltre, attraverso la Dashboard è possibile avere una panoramica istantanea in merito all'esecuzione dei jobs di backup (**Last week backup job summary** e **Jobs in the last 24 hours**) e ai principali server oggetto di backup (**Top 5 largest servers**).

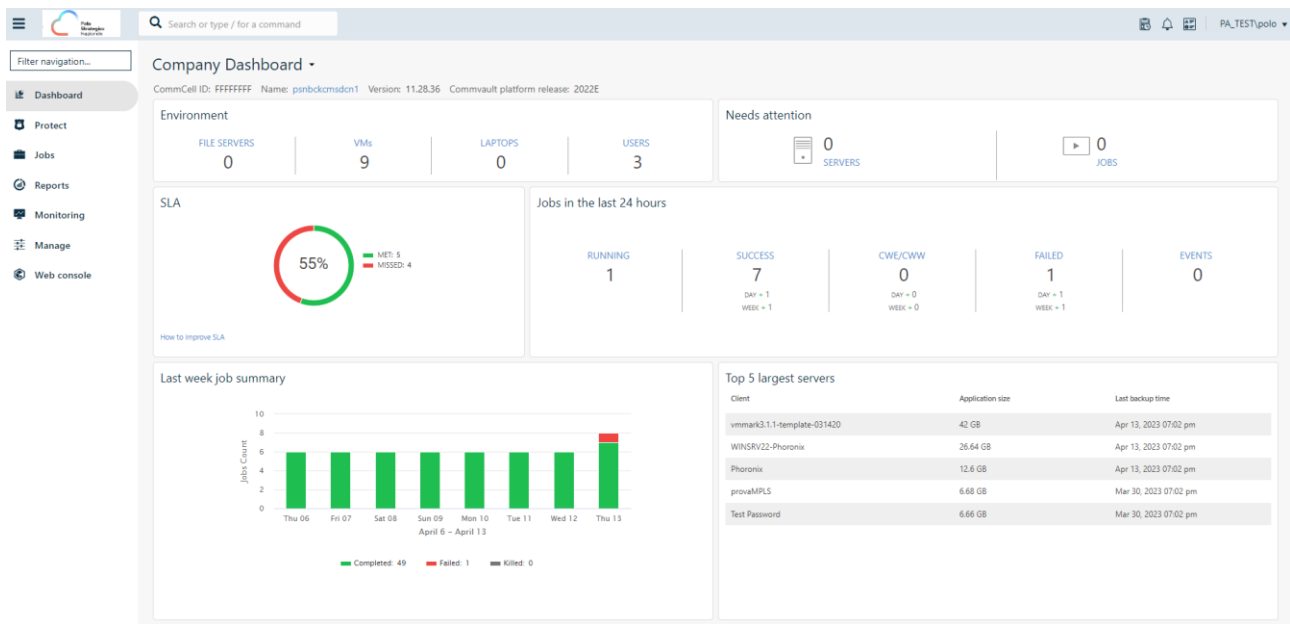
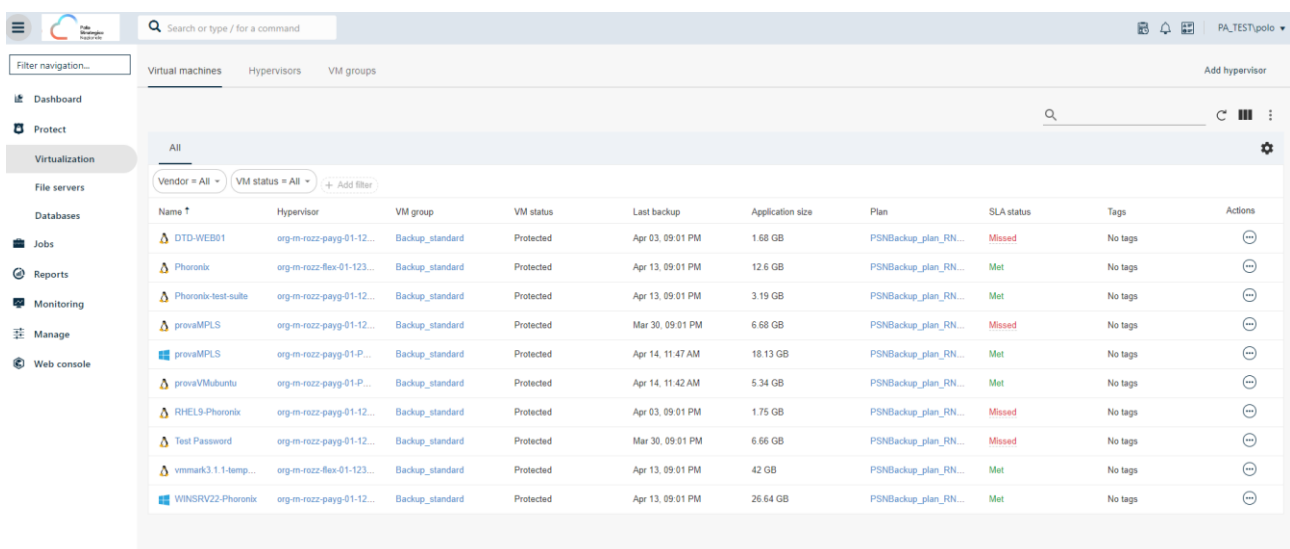


Figura 4 - Dashboard Commvault

4.2 Protect

L'area *Protect*, raggiungibile dal menu a sinistra della console, consente di gestire le risorse oggetto di backup. Da quest'area è comunque possibile accedere alle entità e quindi procedere alle operazioni di configurazione dei backup (descritte nei successivi capitoli). Le entità oggetto di backup sono le più svariate: file system dei server (fisici e virtuali), virtual machine, database, application, Object storage, Big Data, ecc.



Virtual machines

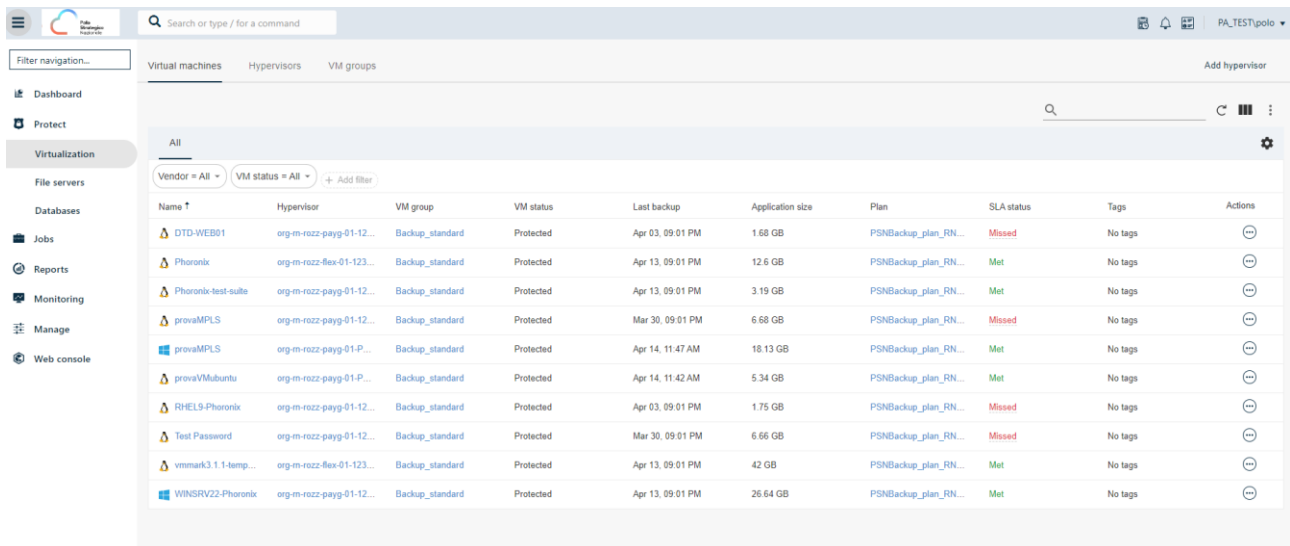
Vendor: All VM status: All

Name	Hypervisor	VM group	VM status	Last backup	Application size	Plan	SLA status	Tags	Actions
DTD-WEB01	org-m-rozz-payg-01-123...	Backup_standard	Protected	Apr 03, 09:01 PM	1.68 GB	PSNBackup_plan_RN...	Missed	No tags	
Phonix	org-m-rozz-flex-01-123...	Backup_standard	Protected	Apr 13, 09:01 PM	12.6 GB	PSNBackup_plan_RN...	Met	No tags	
Phonix-test-suite	org-m-rozz-payg-01-12...	Backup_standard	Protected	Apr 13, 09:01 PM	3.19 GB	PSNBackup_plan_RN...	Met	No tags	
provaMPLS	org-m-rozz-payg-01-12...	Backup_standard	Protected	Mar 30, 09:01 PM	6.68 GB	PSNBackup_plan_RN...	Missed	No tags	
provaMPLS	org-m-rozz-payg-01-P...	Backup_standard	Protected	Apr 14, 11:47 AM	18.13 GB	PSNBackup_plan_RN...	Met	No tags	
provaVMubuntu	org-m-rozz-payg-01-P...	Backup_standard	Protected	Apr 14, 11:42 AM	5.34 GB	PSNBackup_plan_RN...	Met	No tags	
RHEL9-Phonix	org-m-rozz-payg-01-12...	Backup_standard	Protected	Apr 03, 09:01 PM	1.75 GB	PSNBackup_plan_RN...	Missed	No tags	
Test Password	org-m-rozz-payg-01-12...	Backup_standard	Protected	Mar 30, 09:01 PM	6.66 GB	PSNBackup_plan_RN...	Missed	No tags	
vmmark3.1.1-temp...	org-m-rozz-flex-01-123...	Backup_standard	Protected	Apr 13, 09:01 PM	42 GB	PSNBackup_plan_RN...	Met	No tags	
WINSRV22-Phonix	org-m-rozz-payg-01-12...	Backup_standard	Protected	Apr 13, 09:01 PM	26.64 GB	PSNBackup_plan_RN...	Met	No tags	

Figura 5 - Sezione Protect

4.2.1 Virtualization

All'interno della sezione Protect, cliccando su Virtualization, è possibile selezionare Hypervisor, VM Group e Virtual Machine.

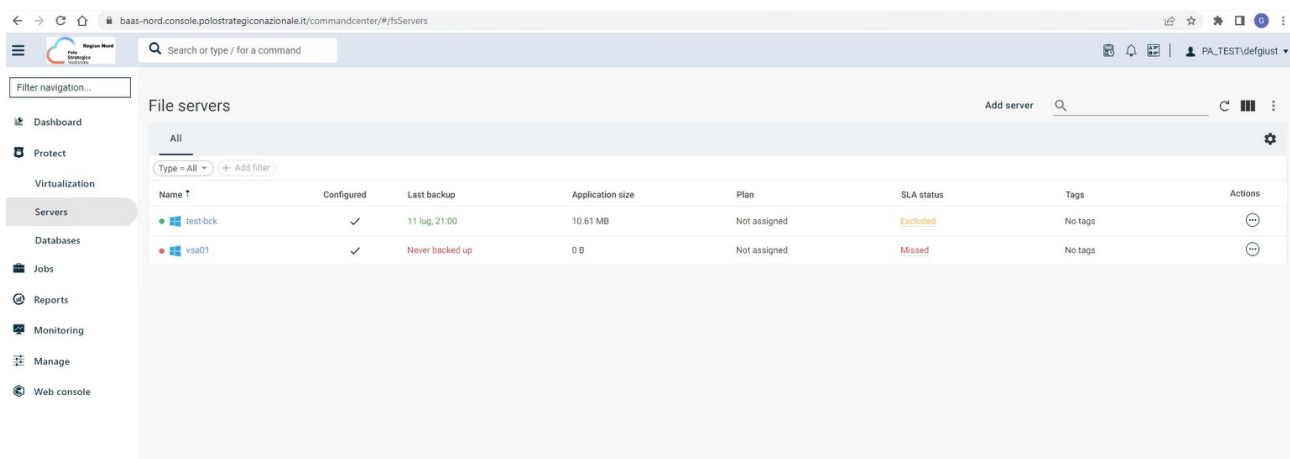


Name	Hypervisor	VM group	VM status	Last backup	Application size	Plan	SLA status	Tags	Actions
DTD-WEB01	org-m-rozz-payg-01-12...	Backup_standard	Protected	Apr 03, 09:01 PM	1.68 GB	PSNBackup_plan_RN...	Missed	No tags	⋮
Phonix	org-m-rozz-flex-01-123...	Backup_standard	Protected	Apr 13, 09:01 PM	12.6 GB	PSNBackup_plan_RN...	Met	No tags	⋮
Phonix-test-suite	org-m-rozz-payg-01-12...	Backup_standard	Protected	Apr 13, 09:01 PM	3.19 GB	PSNBackup_plan_RN...	Met	No tags	⋮
provaMPLS	org-m-rozz-payg-01-12...	Backup_standard	Protected	Mar 30, 09:01 PM	6.68 GB	PSNBackup_plan_RN...	Missed	No tags	⋮
provaMPLS	org-m-rozz-payg-01-P...	Backup_standard	Protected	Apr 14, 11:47 AM	18.13 GB	PSNBackup_plan_RN...	Met	No tags	⋮
provaVMubuntu	org-m-rozz-payg-01-P...	Backup_standard	Protected	Apr 14, 11:42 AM	5.34 GB	PSNBackup_plan_RN...	Met	No tags	⋮
RHEL9-Phonix	org-m-rozz-payg-01-12...	Backup_standard	Protected	Apr 03, 09:01 PM	1.75 GB	PSNBackup_plan_RN...	Missed	No tags	⋮
Test Password	org-m-rozz-payg-01-12...	Backup_standard	Protected	Mar 30, 09:01 PM	6.66 GB	PSNBackup_plan_RN...	Missed	No tags	⋮
vmmark3.1.1-temp...	org-m-rozz-flex-01-123...	Backup_standard	Protected	Apr 13, 09:01 PM	42 GB	PSNBackup_plan_RN...	Met	No tags	⋮
WINSRV22-Phonix	org-m-rozz-payg-01-12...	Backup_standard	Protected	Apr 13, 09:01 PM	26.64 GB	PSNBackup_plan_RN...	Met	No tags	⋮

Figura 6 - Sezione Virtualization

4.2.2 Servers

All'interno della sezione Protect, cliccando su Servers, è possibile selezionare i server su cui eseguire i backup.



Name	Configured	Last backup	Application size	Plan	SLA status	Tags	Actions
test-bck	✓	11 lug, 21:00	10.61 MB	Not assigned	Excluded	No tags	⋮
vsao1	✓	Never backed up	0 B	Not assigned	Missed	No tags	⋮

Figura 7 - Sezione Servers

4.2.3 Databases

All'interno della sezione *Protect*, cliccando su *Databases*, è possibile selezionare i database su cui eseguire i backup.

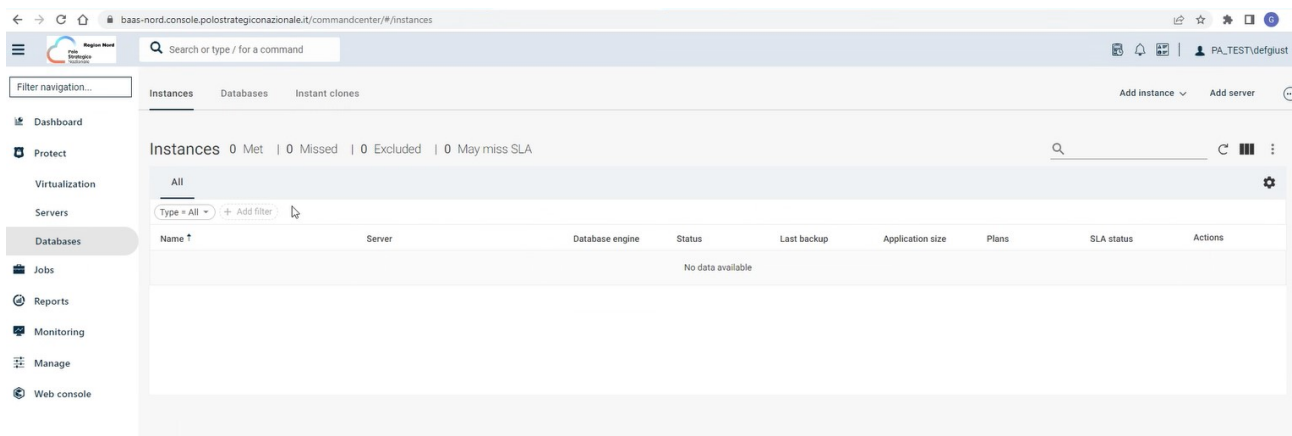


Figura 8 - Sezione Databases

4.3 Jobs

Jobs è la sezione della console attraverso cui è possibile visualizzare i jobs eseguiti o in esecuzione nell'ambito del servizio.

È possibile filtrare i jobs in esecuzione e selezionare il singolo job per verificarne i dettagli di esecuzione (messaggi, eventi correlati, stato, ecc.).

Selezionando il singolo job sarà inoltre possibile effettuare le operazioni di *suspend*, *resume*, *kill* e anche la visualizzazione dei log correlati.

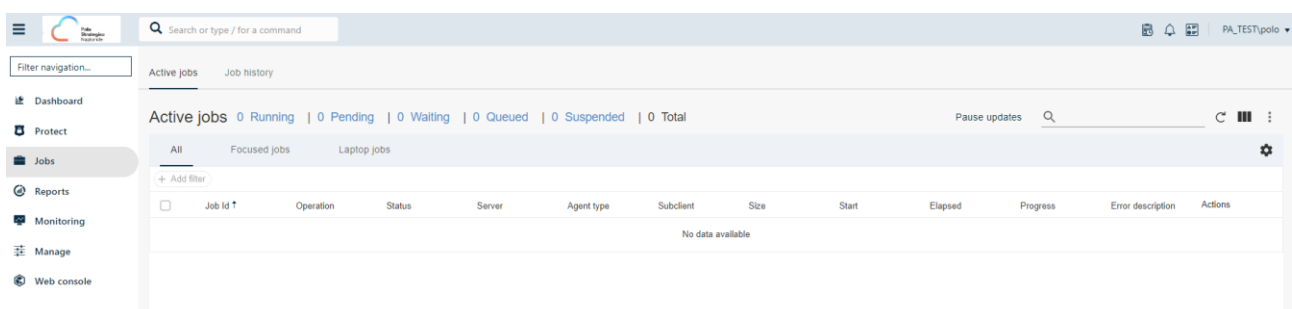
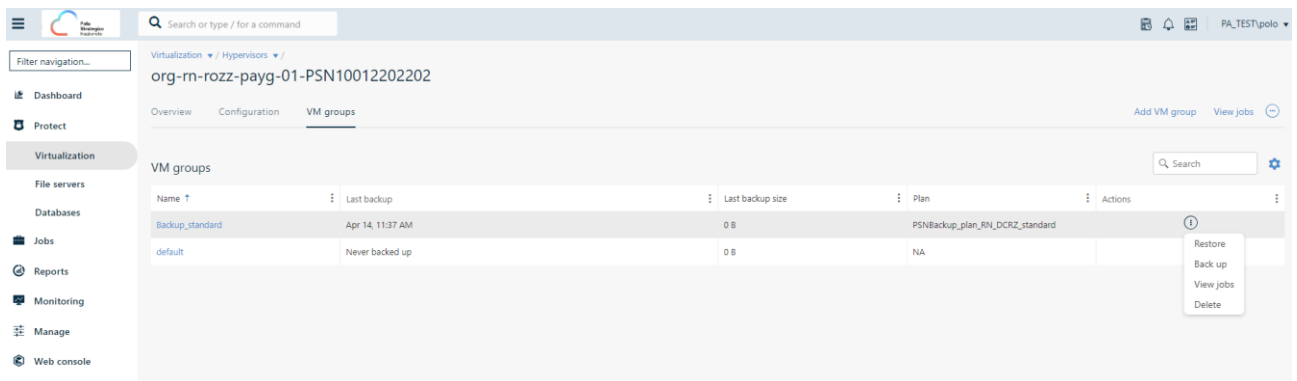


Figura 9 - Sezione Jobs

È possibile accedere direttamente alla sezione Jobs della console selezionando **View Jobs** dal menu a tendina della sezione *Protect* → *Virtualization* → *VM Groups* → **Actions**, per ognuna delle varie risorse presenti.



Virtualization ▾ / Hypervisors ▾ /

org-m-rozz-payg-01-PSN10012202202

Overview Configuration VM groups Add VM group View jobs

VM groups

Name ↑	Last backup	Last backup size	Plan	Actions
Backup_standard	Apr 14, 11:37 AM	0 B	PSNBackup_plan_RN_DCRZ_standard	ⓘ
default	Never backed up	0 B	NA	ⓘ Restore Back up View jobs Delete

Figura 10 - Sezione Virtualization e Actions

4.4 Reports

Attraverso questa sezione è possibile visualizzare la reportistica relativa al servizio. In particolare, è possibile eseguire i seguenti report:

1. Commcell Readiness: Report sullo stato delle component infrastrutturali proprietarie (MediaAgent, ecc.);
2. Infrastructure load: Report sui dati di carico (CPU, Memoria, ecc.) delle risorse infrastrutturali proprietarie;
3. Backup Job Summary: Report sui jobs di backup eseguiti;
4. Restore Job Summary: Report sui jobs di restore eseguiti;
5. SLA: Report con l'indicazione dei dati di sintesi in merito agli SLA di backup;
6. TIM Baas Uso Licenze: Report relative ai consumi giornalieri del servizio.

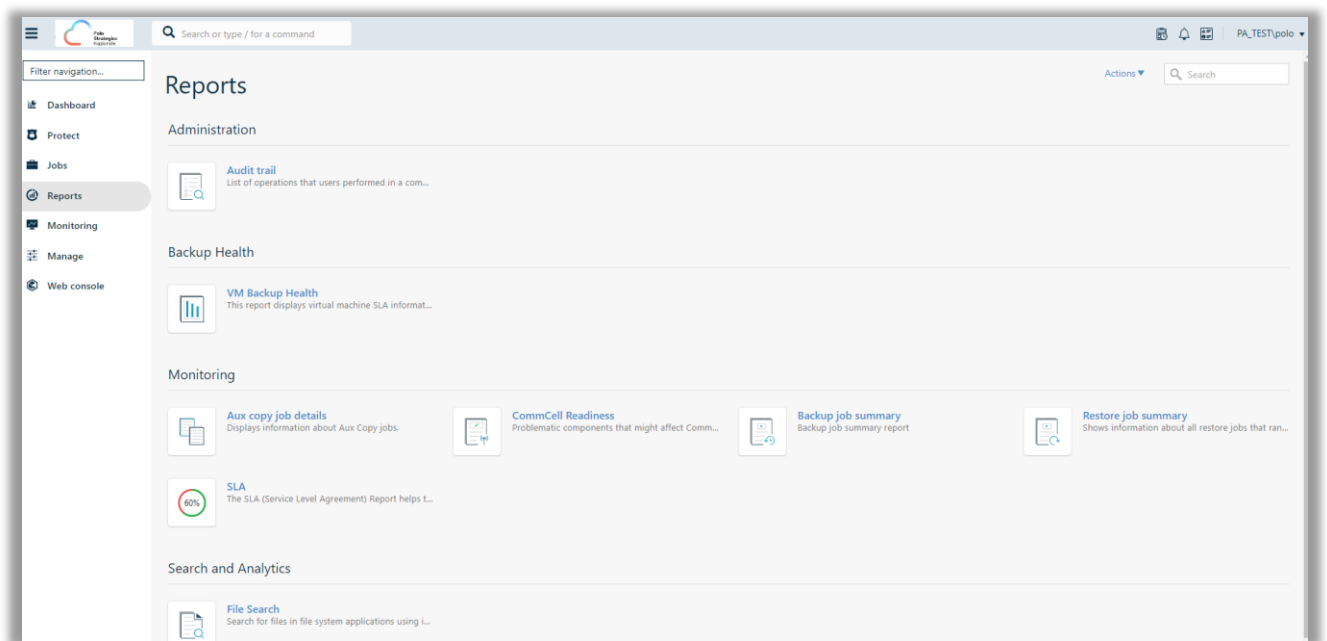


Figura 11 - Sezione Reports

Sotto PSN Utilizzo Storage Backup, in alto a destra, è possibile reperire l'AUTHCODENecessario per l'installazione degli agent ad esempio per il backup a livello filesystem (vedi sezione [#Installazione di un server client \(tenant administrator\)](#)).

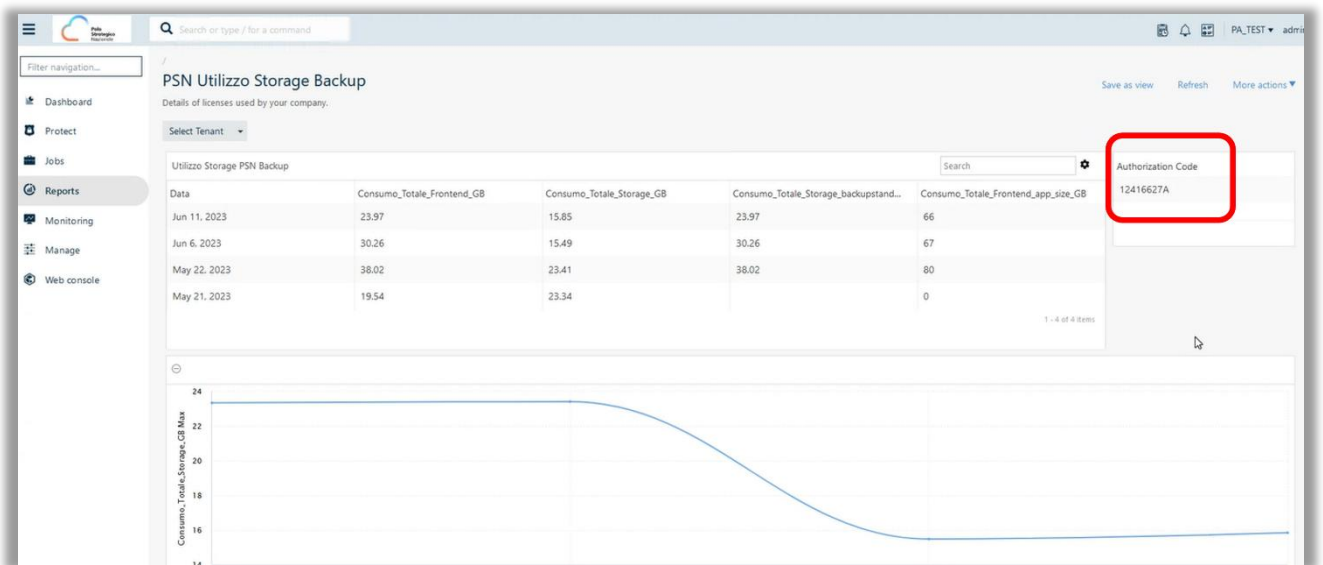
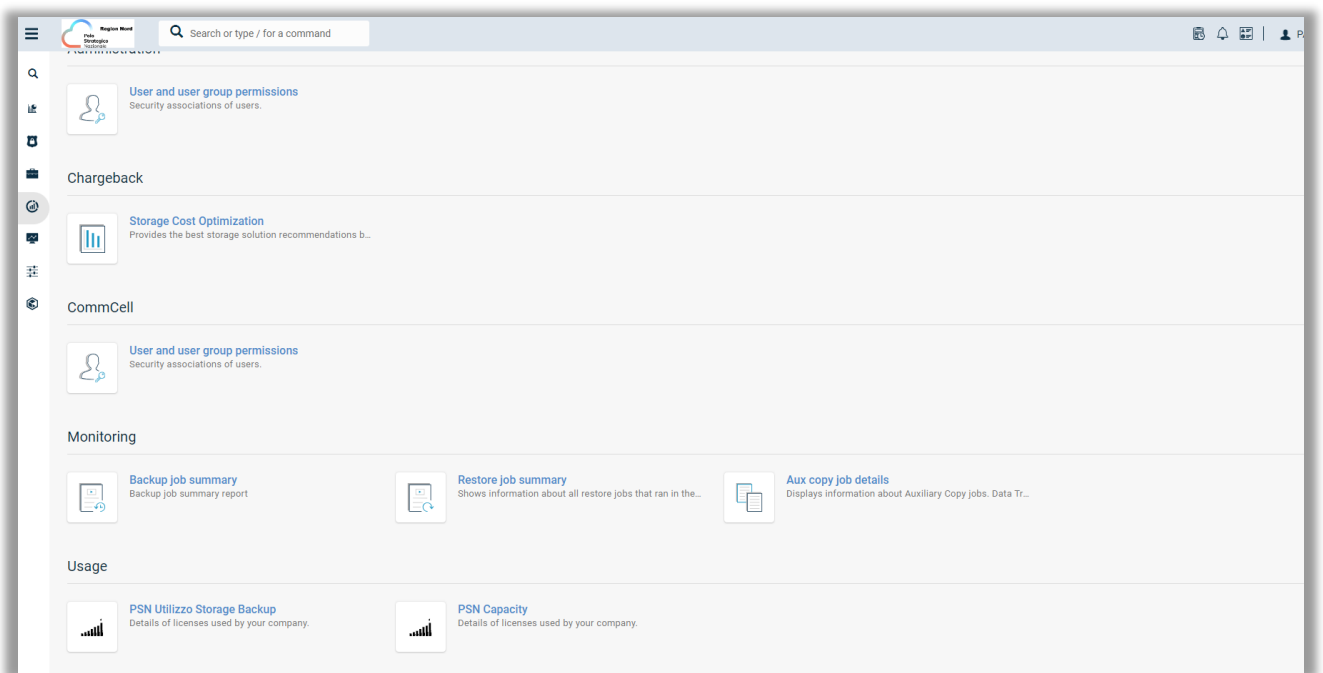


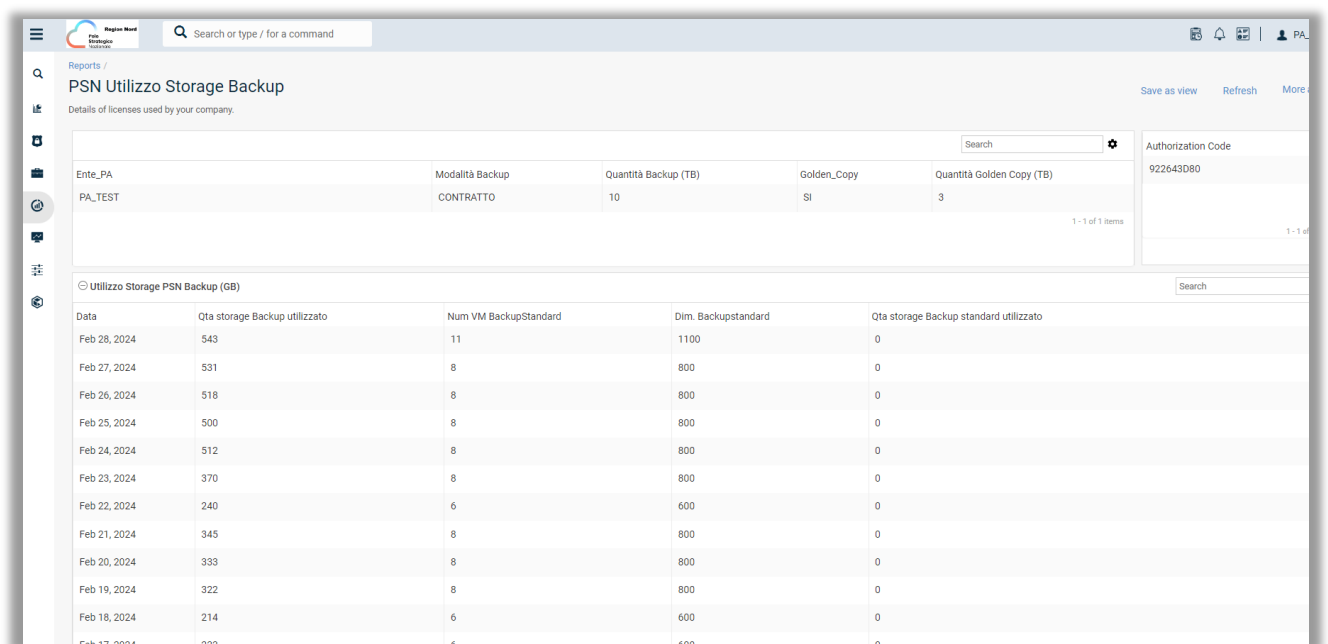
Figura 12 - Reports – AUTHCODE

4.4.1 Utilizzo storage di backup

Rimanendo nel report *Usage – PSN Utilizzo Storage Backup* si possono notare diverse colonne i cui dati presenti assumono un significato diverso a seconda della modalità di backup attiva.

Le modalità di backup possono essere due:

- Standard
- Contratto



Ente_PA	Modalità Backup	Quantità Backup (TB)	Golden_Copy	Quantità Golden Copy (TB)
PA_TEST	CONTRATTO	10	SI	3

Data	Qta storage Backup utilizzato	Num VM BackupStandard	Dim. Backupstandard	Qta storage Backup standard utilizzato
Feb 28, 2024	543	11	1100	0
Feb 27, 2024	531	8	800	0
Feb 26, 2024	518	8	800	0
Feb 25, 2024	500	8	800	0
Feb 24, 2024	512	8	800	0
Feb 23, 2024	370	8	800	0
Feb 22, 2024	240	6	600	0
Feb 21, 2024	345	8	800	0
Feb 20, 2024	333	8	800	0
Feb 19, 2024	322	8	800	0
Feb 18, 2024	214	6	600	0
Feb 17, 2024	233	6	600	0

Figura 13 - Report PSN Utilizzo Storage backup

- La colonna *Qta storage Backup utilizzato* indica la quantità di storage in uso che include la doppia copia di backup;
- La colonna *Num VM BackupStandard* indica il numero di virtual machine sotto backup standard;
- La colonna *Dim. BackupStandard* indica la dimensione massima del backup standard;
- La colonna *Qta storage Backup standard utilizzato* indica la quantità di storage in uso relativamente al backup standard;

Se la modalità di backup attiva è a contratto (come indicato nell'immagine sotto *Modalità backup*) non vanno prese in considerazione le ultime tre colonne del report (dove è specificata la dicitura standard) in quanto non risultano significative per la modalità a contratto.

4.5 Monitoring - Alerts

Monitoring è la sezione della console attraverso cui è possibile impostare gli allarmi che si intende ricevere in seguito all'esecuzione dei jobs di backup e restore.

In figura è mostrata la scheda degli *Alerts* che compare cliccando nella sezione *Monitoring*.

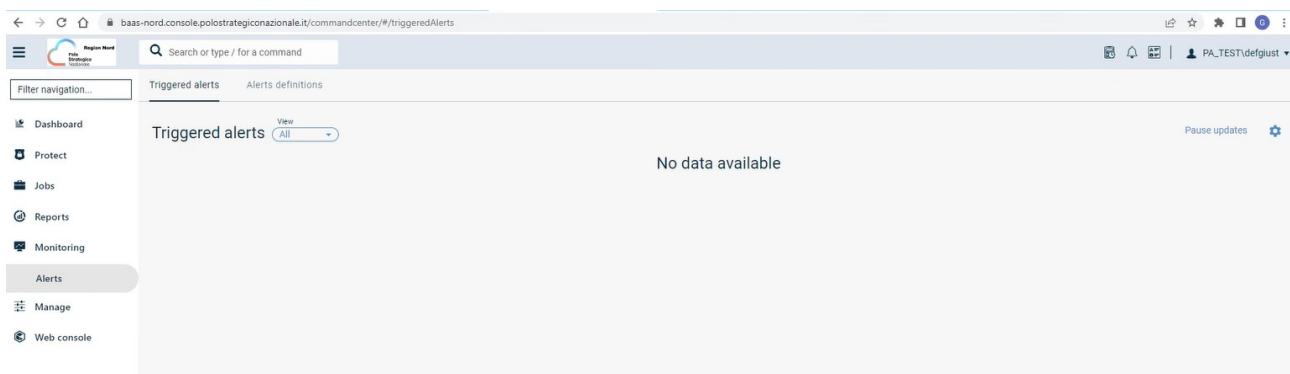


Figura 14 - Sezione Monitoring

Per impostare un allarme è necessario selezionarne il tipo tra quelli disponibili (*Backup/Restore jobs failed*, *Backup/Restore jobs succeeded*) e, sulla schermata successiva, attivare l'invio di un allarme attraverso il pulsante ***Send individual notification***.

È possibile, inoltre, inserire/modificare i destinatari delle mail di allarme e lo schema di mail da inviare digitando ***Edit Template***.

4.6 Manage

L'area **Manage** consente di gestire le risorse di backup.
In particolare, è possibile controllare e modificare:

- **Servers** su cui sono installati i vari agent di backup;
- **Servers Group** con cui raggruppare logicamente i **Servers**;
- **Blackout window**;
- **Plans** per definire i requisiti da applicare ai backup in termini di cosa, dove e quando effettuare i backup (ad esempio, è possibile modificare lo Start Time di un job di backup già implementato);

La sezione Manage comprende a sua volta *Active Servers* e *Blackout window*.

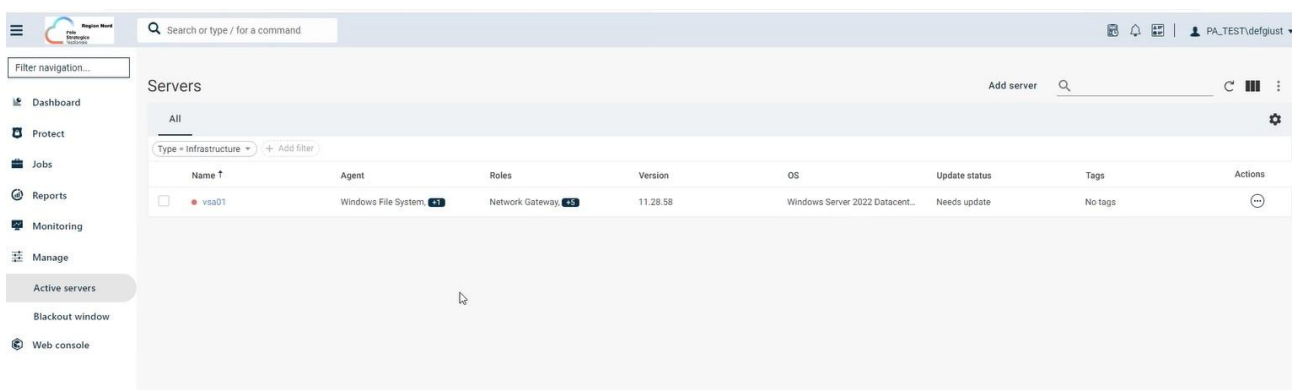


Figura 15 - Sezione Manage – Active servers

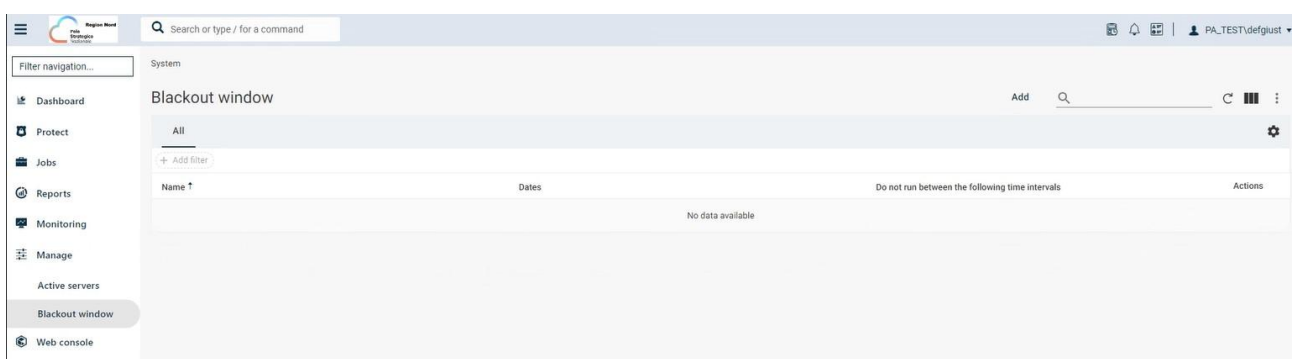


Figura 16 - Sezione Manage - Blackout window

4.7 Web console

Dalla sezione *Web Console* si accede all'area di **Download Manager** da cui sarà possibile scaricare sia la documentazione relativa al servizio che i pacchetti di installazione per configurare i client sul servizio.

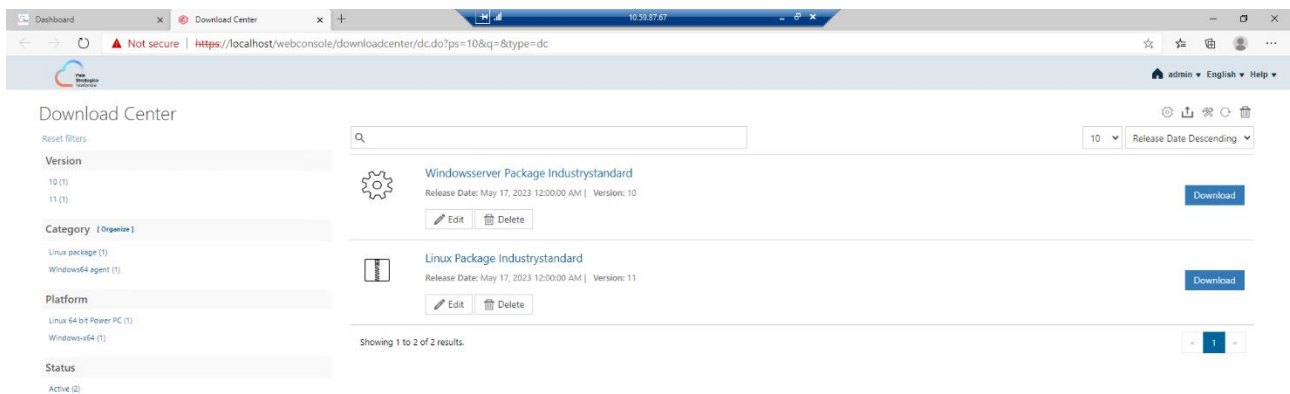


Figura 17 - Sezione Web Console

4.8 Plugin vCloud

Tramite l'integrazione con il plugin vCloud è possibile accedere alla console di Backup PSN secondo la procedura descritta di seguito:

- Accedere alla console IaaS;
- Dal menù in alto, alla sezione *Altro* cliccare su *Commvault Data Protection*

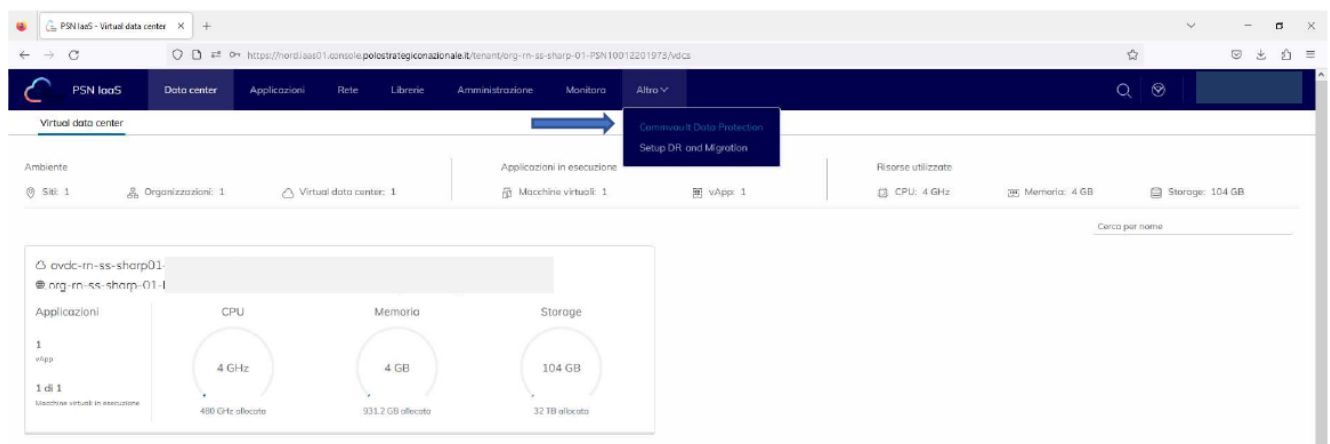


Figura 18 - Console di backup plugin vCloud

- Cliccando su *Commvault Data Protection* si ha accesso diretto alla Dashboard.

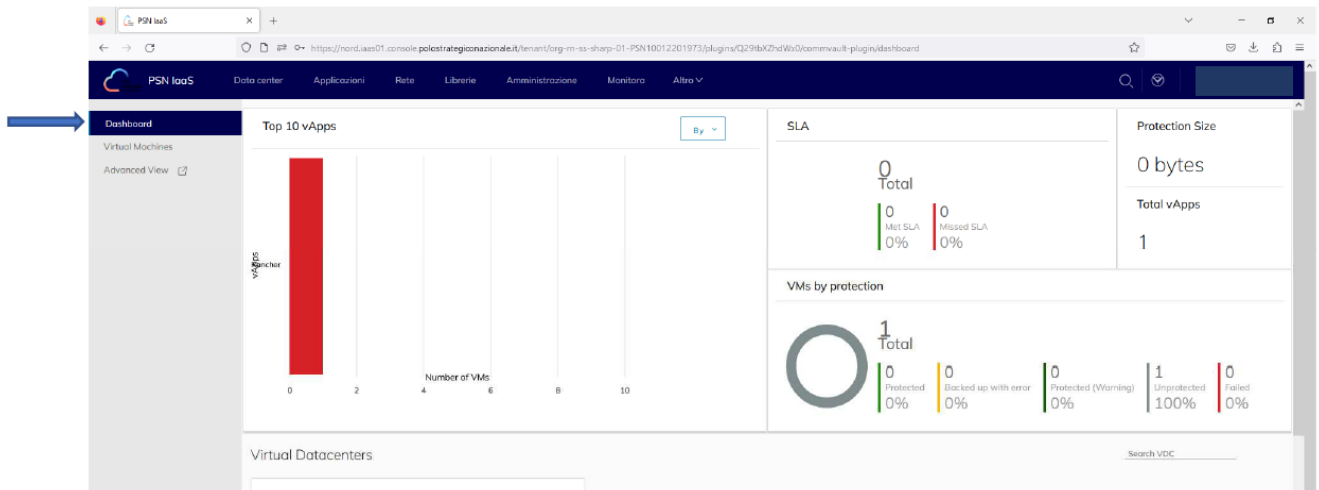


Figura 19 - Dashboard plugin vCloud

- Appena sotto *Dashboard*, è presente la sezione *Virtual Machines*, nella quale è possibile controllare lo stato delle VM relativamente al backup.

Elenco VM protette

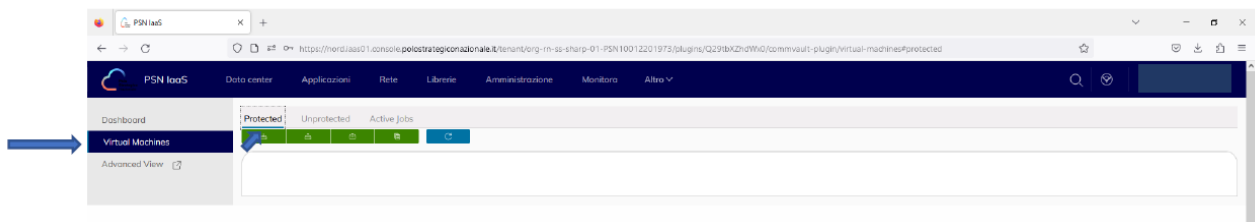


Figura 20 - VM protected

Elenco VM non protette

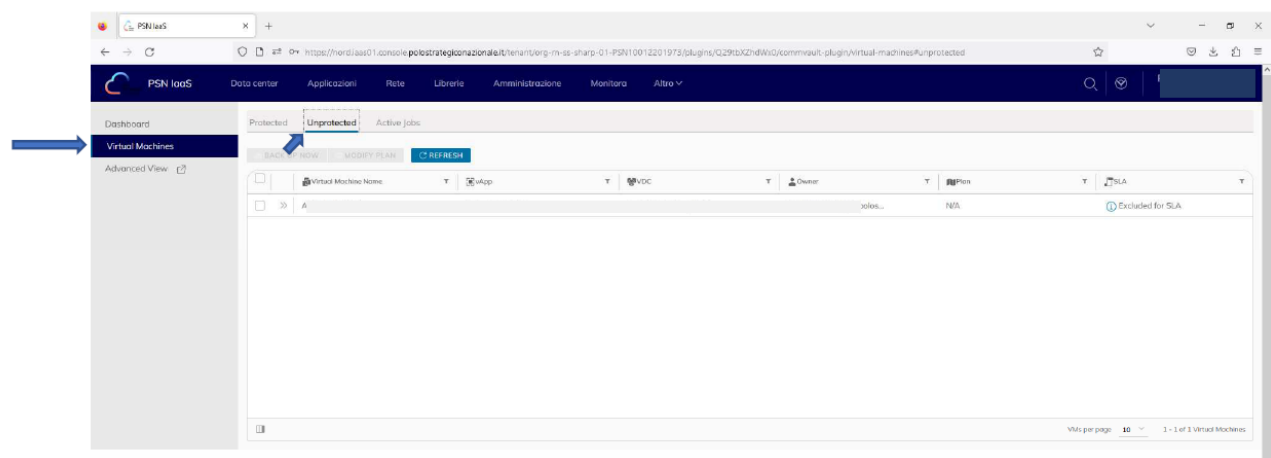


Figura 21 - VM unprotected

Elenco job in corso

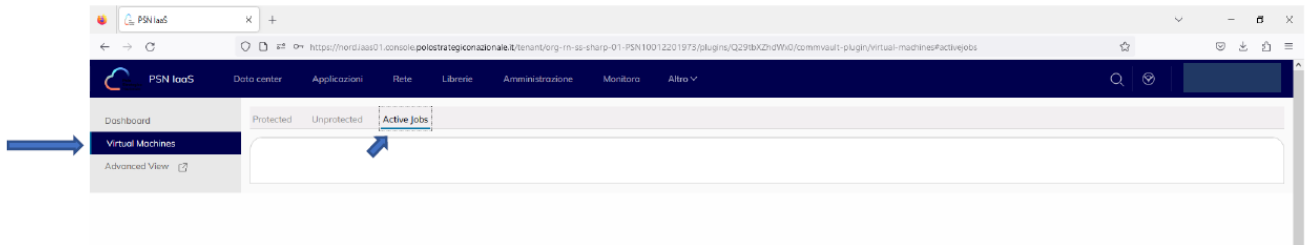


Figura 22 - Active jobs

- Appena sotto *Virtual Machines*, è presente la sezione *Advanced View*, nella quale è possibile accedere ad una vista più dettagliata della console di backup.

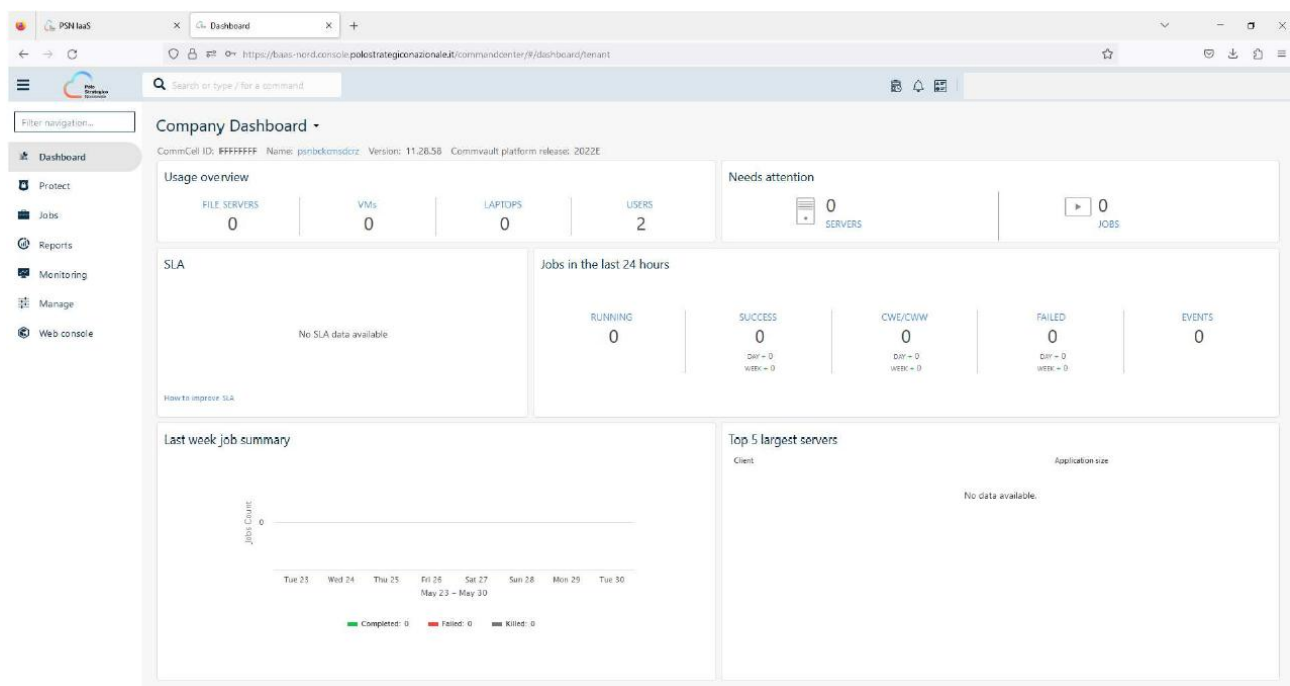


Figura 23 - Advanced View Dashboard

5 Pianificazione schedulazione dei job di backup

Sulla piattaforma sono disponibili alcuni plan di backup predefiniti, il cui dettaglio è mostrato di seguito.

Sarà possibile avere tre tipologie differenti di servizio di backup:

1. Come servizio di base sarà possibile avere un solo plan di backup standard per Data Center all'interno della singola region che prevede retention 2 settimane + backup full settimanale.
2. Nel caso in cui venga acquistato solo il servizio BaaS, senza Goldencopy, i plan selezionabili nella fase iniziale saranno 7 per Data Center all'interno della singola Region.
3. Nel caso in cui venga acquistato il servizio BaaS e il servizio di Goldencopy, i plan selezionabili nella fase iniziale saranno quattordici, 7 plan per Data Center all'interno della singola Region e 7 plan per Data Center con la possibilità di attivare la Golden Copy su altra Region rispetto a quella di appartenenza (Goldencopy su Region Sud se il servizio di backup è attivo su Region Nord, Goldencopy su Region Nord se il servizio di backup è attivo su Region Sud).

REGION NORD

Tutti i plan descritti prevedono un backup full e un backup incrementale giornaliero.

Tutti i backup full relativi al Data Center di Rozzano sono settimanali e schedulati per il sabato alle ore 3:00 PM (15:00), ad eccezione del plan *PSNBackup_plan_RN_DCRZ_7_giorni* il cui backup full è schedulato per ogni domenica alle ore 3:00 PM (15:00) e del plan *PSNBackup_plan_RN_DCRZ_10_anni* che prevede backup full mensile il primo sabato di ogni mese alle ore 3:00 PM (15:00).

Tutti i backup incrementali di Rozzano sono giornalieri e previsti per le ore 6:00 PM (18:00).

Tutti i backup full relativi al Data Center di Santo Stefano sono settimanali e schedulati per la domenica alle ore 3:00 PM (15:00), ad eccezione del plan *PSNBackup_plan_RN_DCSS_10_anni* che prevede backup full mensile la prima domenica di ogni mese alle ore 3:00 PM (15:00).

Tutti i backup incrementali di Santo Stefano sono giornalieri e previsti per le ore 6:00 PM (18:00).

Plan backup standard:

- PSNBackup_plan_RN_DCRZ_standard (riferito al DC di Rozzano)
- PSNBackup_plan_RN_DCSS_standard (riferito al DC di Santo Stefano)

Di seguito il dettaglio dei plan backup del DC di Rozzano:

- PSNBackup_plan_RN_DCRZ_7_giorni

-
- PSNBackup_plan_RN_DCRZ_1_mese
 - PSNBackup_plan_RN_DCRZ_2_mesi
 - PSNBackup_plan_RN_DCRZ_3_mesi
 - PSNBackup_plan_RN_DCRZ_6_mesi
 - PSNBackup_plan_RN_DCRZ_1_anno
 - PSNBackup_plan_RN_DCRZ_10_anni

Di seguito il dettaglio dei plan del DC di Santo Stefano:

- PSNBackup_plan_RN_DCSS_7_giorni
- PSNBackup_plan_RN_DCSS_1_mese
- PSNBackup_plan_RN_DCSS_2_mesi
- PSNBackup_plan_RN_DCSS_3_mesi
- PSNBackup_plan_RN_DCSS_6_mesi
- PSNBackup_plan_RN_DCSS_1_anno
- PSNBackup_plan_RN_DCSS_10_anni

Qualora il servizio di Golden Copy sia stato configurato, con caratteristiche di write once, ready many (WORM) su storage distinto privo di ogni accesso fisico e logico, sarà possibile inoltre implementare i seguenti plan. La Goldencopy sarà attiva su Region Sud.

Di seguito il dettaglio dei plan del DC di Rozzano:

- PSNGoldenCopy_plan_RN_DCRZtoDCAC_7_giorni
- PSNGoldenCopy_plan_RN_DCRZtoDCAC_1_mese
- PSNGoldenCopy_plan_RN_DCRZtoDCAC_2_mesi
- PSNGoldenCopy_plan_RN_DCRZtoDCAC_3_mesi
- PSNGoldenCopy_plan_RN_DCRZtoDCAC_6_mesi
- PSNGoldenCopy_plan_RN_DCRZtoDCAC_1_anno
- PSNGoldenCopy_plan_RN_DCRZtoDCAC_10_anni

Di seguito il dettaglio dei plan del DC di Santo Stefano:

- PSNGoldenCopy_plan_RN_DCSStoDCPM_7_giorni
- PSNGoldenCopy_plan_RN_DCSStoDCPM_1_mese
- PSNGoldenCopy_plan_RN_DCSStoDCPM_2_mes1
- PSNGoldenCopy_plan_RN_DCSStoDCPM_3_mesi
- PSNGoldenCopy_plan_RN_DCSStoDCPM_6_mesi
- PSNGoldenCopy_plan_RN_DCSStoDCPM_1_anno
- PSNGoldenCopy_plan_RN_DCSStoDCPM_10_anni

REGION SUD

Tutti i plan descritti prevedono un backup full e un backup incrementale giornaliero.

Tutti i backup full relativi al Data Center di Acilia sono settimanali e schedulati per il sabato alle ore 3:00 PM (15:00), ad eccezione del plan *PSNBackup_plan_RS_DCAC_7_giorni* il cui backup full è schedulato per ogni domenica alle ore 3:00 PM (15:00) e del plan *PSNBackup_plan_RS_DCAC_10_anni* che prevede backup full mensile il primo sabato di ogni mese alle ore 3:00 PM (15:00).

Tutti i backup incrementali di Acilia sono giornalieri e previsti per le ore 6:00 PM (18:00).

Tutti i backup full relativi al Data Center di Pomezia sono settimanali e schedulati per la domenica alle ore 3:00 PM (15:00), ad eccezione del plan *PSNBackup_plan_RS_DCPM_10_anni* che prevede backup full mensile la prima domenica di ogni mese alle ore 3:00 PM (15:00).

Tutti i backup incrementali di Pomezia sono giornalieri e previsti per le ore 6:00 PM (18:00).

Plan backup standard:

- PSNBackup_plan_RS_DCAC_standard (riferito al DC di Acilia)
- PSNBackup_plan_RS_DCPM_standard (riferito al DC di Pomezia)

Di seguito il dettaglio dei plan backup del DC di Acilia:

- PSNBackup_plan_RS_DCAC_7_giorni
- PSNBackup_plan_RS_DCAC_1_mese
- PSNBackup_plan_RS_DCAC_2_mesi
- PSNBackup_plan_RS_DCAC_3_mesi
- PSNBackup_plan_RS_DCAC_6_mesi
- PSNBackup_plan_RS_DCAC_1_anno
- PSNBackup_plan_RS_DCAC_10_anni

Di seguito il dettaglio dei plan del DC di Pomezia:

- PSNBackup_plan_RS_DCPM_7_giorni
- PSNBackup_plan_RS_DCPM_1_mese
- PSNBackup_plan_RS_DCPM_2_mesi
- PSNBackup_plan_RS_DCPM_3_mesi
- PSNBackup_plan_RS_DCPM_6_mesi
- PSNBackup_plan_RS_DCPM_1_anno
- PSNBackup_plan_RS_DCPM_10_anni

Qualora il servizio di Golden Copy sia stato configurato, con caratteristiche di write once, ready many (WORM) su storage distinto privo di ogni accesso fisico e logico, sarà possibile inoltre implementare i seguenti plan. La Goldencopy sarà attiva su Region Nord.

Di seguito il dettaglio dei plan del DC di Acilia:

- PSNGoldenCopy_plan_RS_DCACtoDCRZ_7_giorni
- PSNGoldenCopy_plan_RS_DCACtoDCRZ_1_mese
- PSNGoldenCopy_plan_RS_DCACtoDCRZ_2_mesi
- PSNGoldenCopy_plan_RS_DCACtoDCRZ_3_mesi
- PSNGoldenCopy_plan_RS_DCACtoDCRZ_6_mesi
- PSNGoldenCopy_plan_RS_DCACtoDCRZ_1_anno
- PSNGoldenCopy_plan_RS_DCACtoDCRZ_10_anni

Di seguito il dettaglio dei plan del DC di Pomezia:

- PSNGoldenCopy_plan_RN_DCPMtoDCSS_7_giorni
- PSNGoldenCopy_plan_RN_DCPMtoDCSS_1_mese
- PSNGoldenCopy_plan_RN_DCPMtoDCSS_2_mes1
- PSNGoldenCopy_plan_RN_DCPMtoDCSS_3_mesi
- PSNGoldenCopy_plan_RN_DCPMtoDCSS_6_mesi
- PSNGoldenCopy_plan_RN_DCPMtoDCSS_1_anno
- PSNGoldenCopy_plan_RN_DCPMtoDCSS_10_anni

Tali policy di backup, qualora utilizzate, consentiranno ai clienti di produrre una copia ausiliaria (golden copy) di backup al termine della copia primaria (Goldencopy su Region Sud se il servizio di backup è attivo su Region Nord, Goldencopy su Region Nord se il servizio di backup è attivo su Region Sud).

5.1.1 Modifica schedulazione jobs

All'interno della sezione *Protect* → *Virtualization* è possibile visualizzare il VM group o il subclient server. È possibile impostare lo *Start Time* del job che va a sovrascrivere quello del plan.

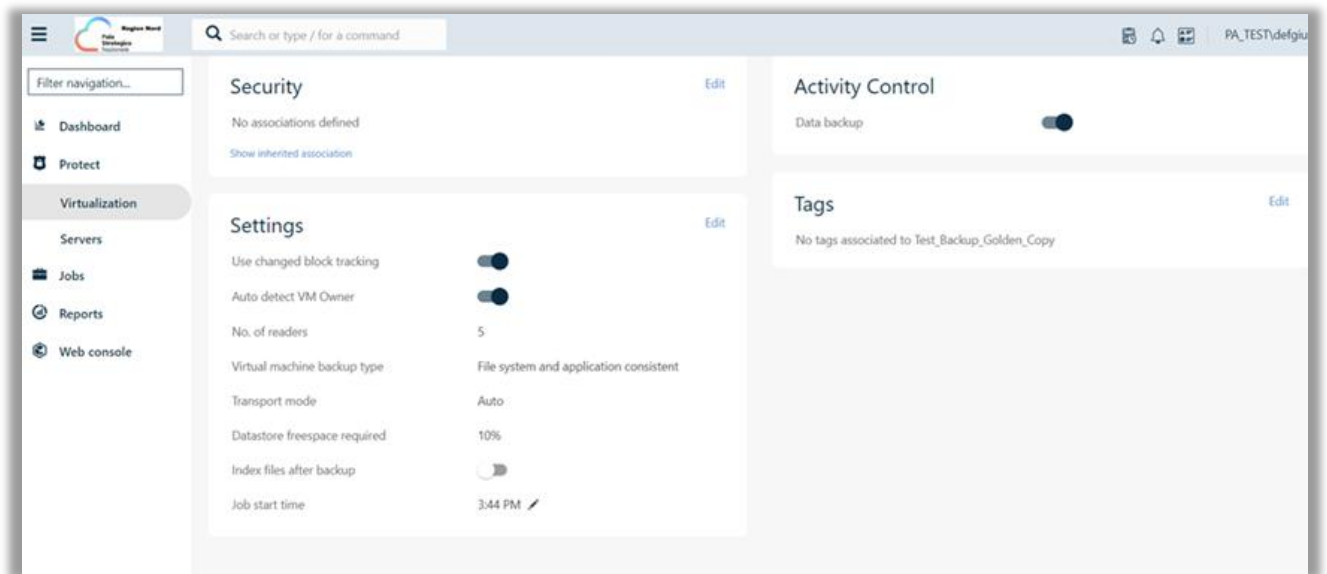


Figura 24 - Modifica schedulazione job

Lo *Start Time* si può impostare:

- a livello di VM group, nella sezione *Configuration*, per il backup a livello hypervisor (image copy delle VM).



Figura 25 - Modifica schedulazione job per VM group

- A livello di server (backup con agent) può essere impostato da *Manage* → *Active Servers* → *Overview* → Selezionare il server e impostare *Type=all*



Figura 26 - Modifica schedulazione job per server

6 Configurazione dei client IaaS Industry Standard

Le istruzioni contenute in questo capitolo si riferiscono alle operazioni relative alla installazione e configurazione dei client preliminari alle attività di schedulazione, backup e restore dei dati in tutti quei casi in cui è necessario predisporre il backup tramite agent.

6.1 *Prerequisiti per backup agent Industry standard*

Prima di effettuare l'installazione di un nuovo client è necessario verificare che la macchina sia dotata di un'adeguata connettività ai sistemi. Pertanto, è importante che le seguenti porte risultino aperte su tutti i firewall coinvolti fino alla raggiungibilità del servizio di backup:

- 8400
- 8401
- 8402
- 8403

Non è possibile avere nel proprio piano di indirizzamento IP le subnet 1916 (172.20.194.0/23 e 172.21.194.0/23) e 1914 (172.20.200.0/23 e 172.21.202.0/23).

6.1.1 *IMPORT subnet per backup con agent Industry standard*

Per poter effettuare un backup con agent è necessario prima aprire un ticket tramite la console di gestione dei servizi <https://console.polostrategiconazionale.it> per la richiesta di IMPORT della subnet di backup.

Sul ticket è necessario indicare:

1. la subnet di backup con agent di cui richiedere la import ossia:
 - a. per la region Nord la 1914 - 172.20.200.0/23
 - b. per la region Sud la 1914 - 172.21.202.0/23
2. la org su cui effettuare la import

6.1.2 *Personalizzazione VM per backup con agent*

Dopo l'avvenuta chiusura del ticket e la conseguente import della subnet di backup, per poter configurare correttamente il backup con agent è necessario seguire la procedura seguente.

- Entrare nella org in cui risiede la VM e cliccare sulla VM della quale si vuole effettuare il backup con agent, nella sezione *Virtual Machines*

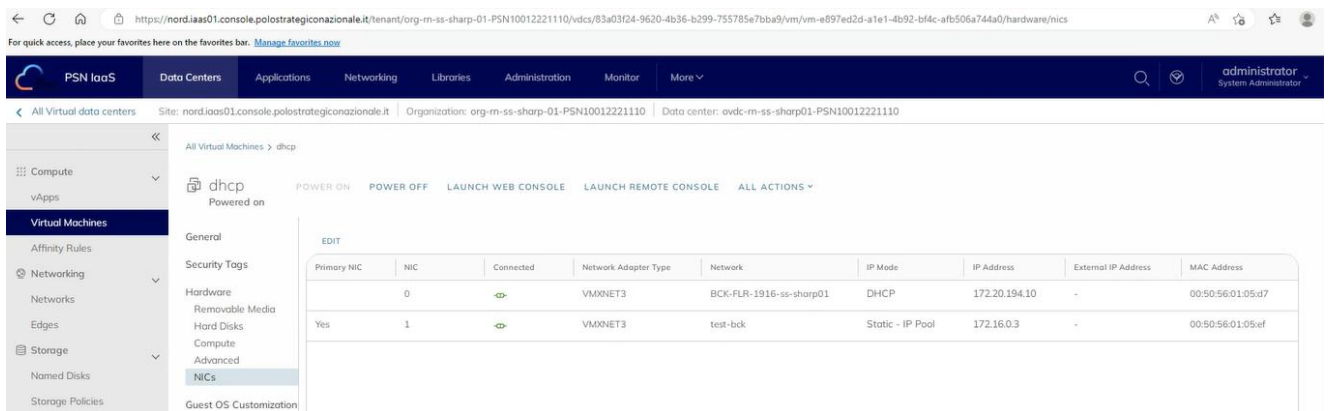


Figura 27 – Interfaccia configurazione VM NICS

- Cliccare su **NICs** → **EDIT** → **NEW** (selezionare **DHCP** per **IP Mode**)

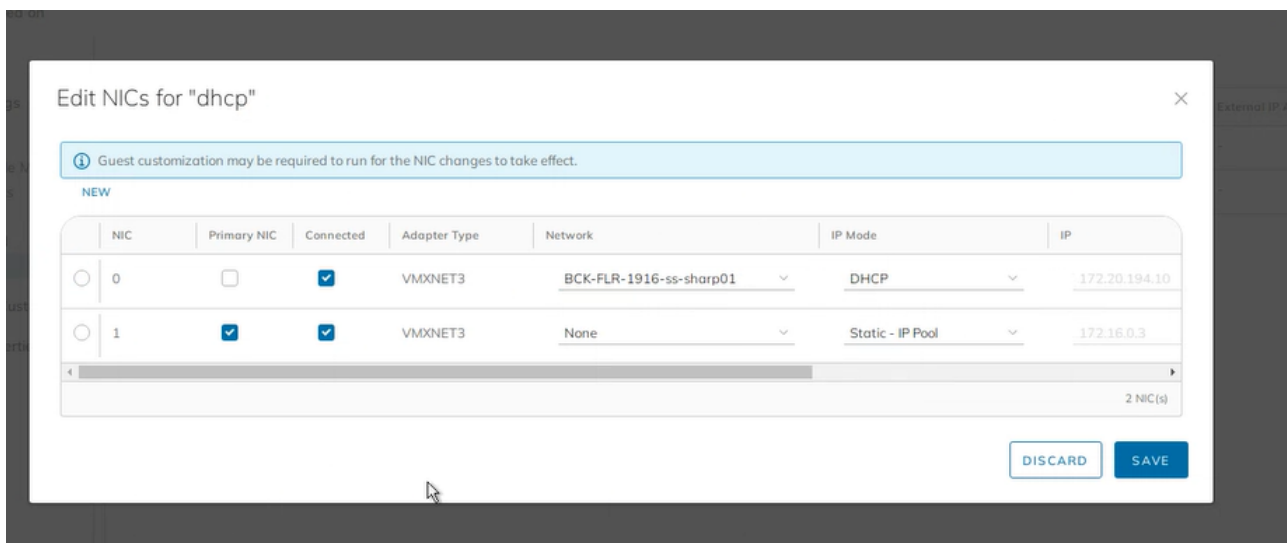


Figura 28 – Interfaccia modifica VM NICS

Una volta inserita la Network corretta, è necessario impostare alcune rotte sulla VM oggetto di backup con agent.

Le rotte da impostare sono le seguenti:

Region Nord:

- verso la network 172.20.193.0/24 attraverso il gateway 172.20.200.1
- verso la network 172.20.77.0/24 attraverso il gateway 172.20.200.1

Region Sud:

- verso la network 172.21.45.0/24 attraverso il gateway 172.21.202.1
- verso la network 172.21.77.0/24 attraverso il gateway 172.21.202.1

Ad esempio, per i sistemi windows i comandi sono i seguenti:

Region Nord:

```
route add 172.20.193.0 mask 255.255.255.0 172.20.200.1 -p
```

```
route add 172.20.77.0 mask 255.255.255.0 172.20.200.1 -p
```

Region Sud:

```
route add 172.21.45.0 mask 255.255.255.0 172.21.202.1 -p
```

```
route add 172.21.193.0 mask 255.255.255.0 172.21.202.1 -p
```

6.2 Installazione di un server client (tenant administrator)

Nel paragrafo successivo è descritta la procedura per installare un nuovo client nel servizio PSN Backup su Commvault, l'installazione va eseguita con un'utenza di sistema operativo dotata di diritti amministrativi.

6.2.1 Client Windows

Individuare il server con sistema operativo Windows sul quale si vorranno applicare le policy di backup o che sarà utilizzato per le varie funzionalità del servizio.

Scaricare, sul server in questione, il pacchetto di installazione relativo al sistema operativo Windows, selezionando dal menu della console la voce '**Web Console**' e quindi '**Download Center**'.

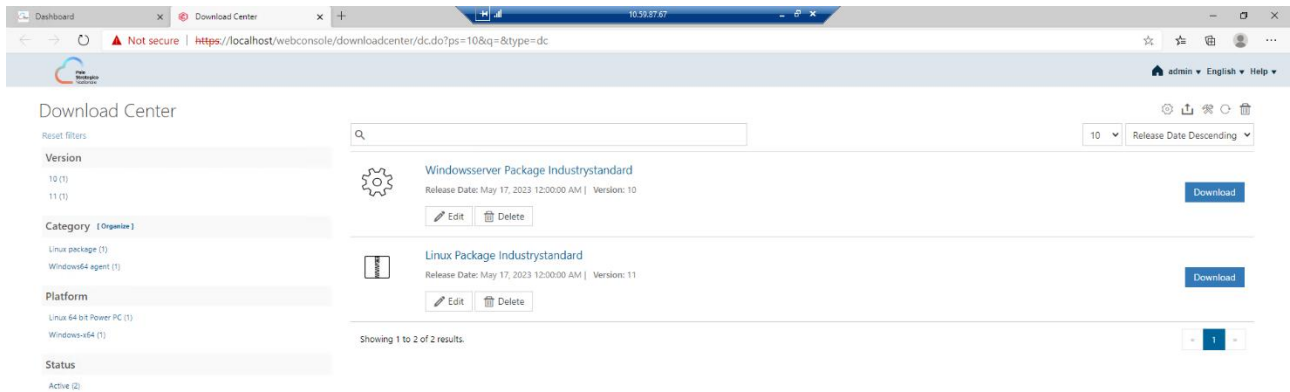
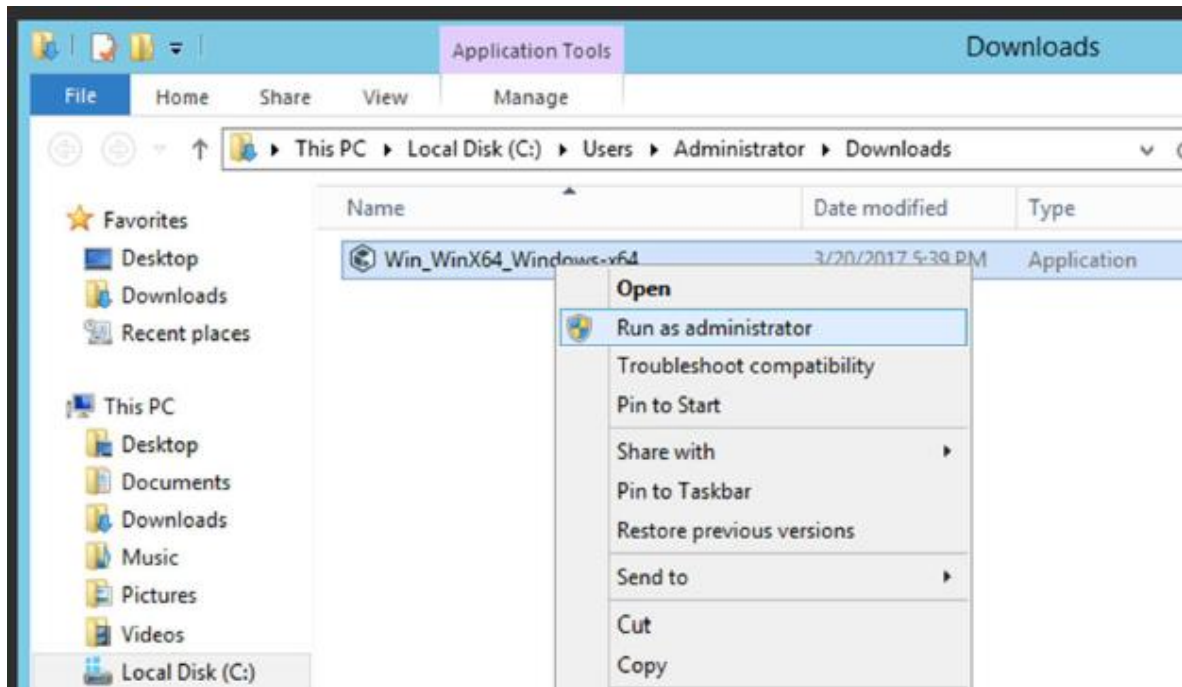


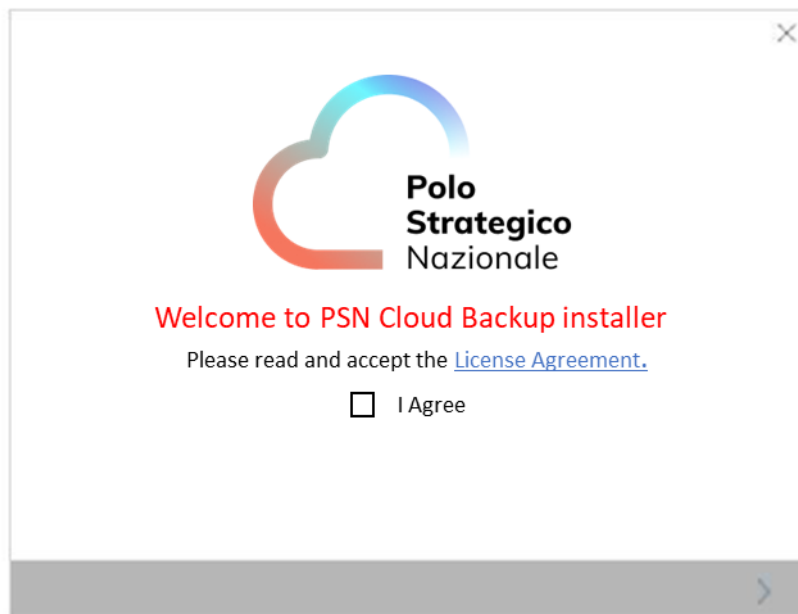
Figura 29 – Steps installazione client Windows on IaaS IND STD

Dopo aver scaricato il relativo pacchetto per il sistema operativo Windows, selezionare la voce "**Run as Administrator**" digitando con il tasto destro del mouse sul pacchetto appena scaricato.



Steps installazione client Windows on IaaS IND STD

Inserire il segno di spunta come indicato in figura e digitare il tasto in basso a destra per continuare l'installazione.



Steps installazione client Windows on IaaS IND STD

Quindi il software inizierà l'esecuzione.



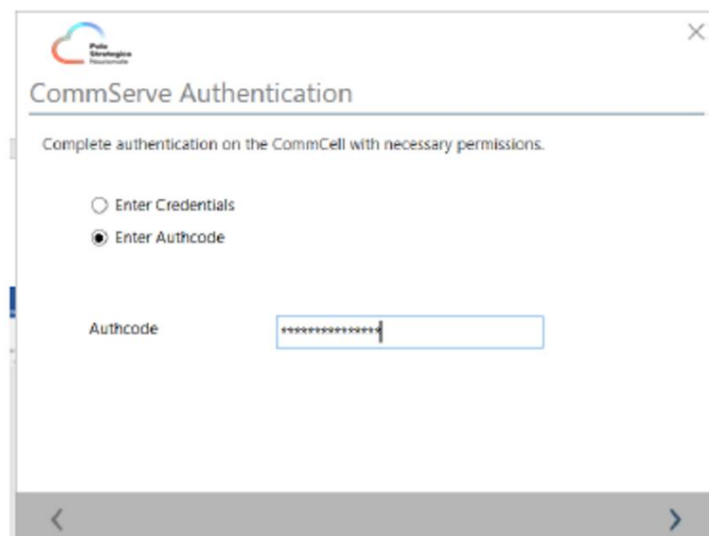
Steps installazione client Windows on IaaS IND STD

Al termine dell'installazione si avvierà il processo di registrazione del client sul servizio.



Steps installazione client Windows on IaaS IND STD

A tal fine sarà necessario inserire l'utenza e l'Authcode, quest'ultimo reperibile nella sezione *Reports*.

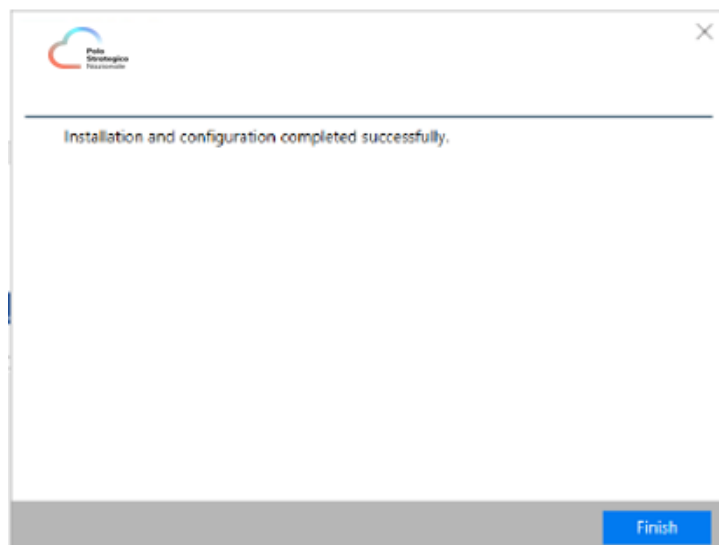


Steps installazione client Windows on IaaS IND STD



Steps installazione client Windows on IaaS IND STD

L'installazione risulterà completata alla visualizzazione della schermata successiva.



Steps installazione client Windows on IaaS IND STD

Digitare quindi 'Finish' per completare l'installazione.

6.2.2 Client Linux

Individuare il server con sistema operativo Linux sul quale si vorranno applicare le policy di backup o che sarà utilizzato per le varie funzionalità del servizio.

Scaricare, sul server in questione, il pacchetto di installazione relativo al sistema operativo Linux, selezionando dal menu della console la voce '**Web Console**' e quindi '**Download Center**'.

Quindi procedere a scompattare il file .tar entrando nella directory e digitando:

```
tar -xvf NOMEpacchetto.tar
```

(es. `tar -xvf linuxclientcvsp7.tar`)

Dopo aver completato la decompressione del file selezionare la directory `pkg` e avviare la procedura di installazione digitando

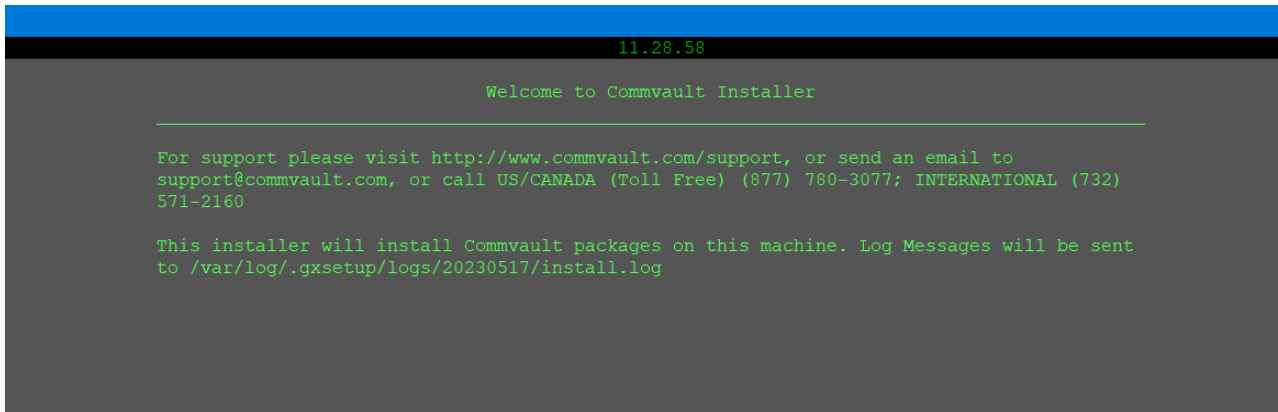
```
./cvpkgadd
```

La procedura di installazione richiede utenza root quindi se necessario utilizzare comando `sudo`.

```
bash: mkd: command not found
[root@psnbckfre101 tmp]# mkdir pkg
[root@psnbckfre101 tmp]# ll
total 54528
-rw-r--r-- 1 root root 0 Jun 14 10:57 bdinstaller.lock
drwxr-xr-x 2 root root 63 Jun 14 11:06 birdefender
-rw-r--r-- 1 root root 11335168 Jun 14 10:53 installer.tar
drwxr-xr-x 2 root root 6 Jun 5 21:55 locks
drwxr-xr-x 2 root root 6 Jun 21 14:19 pkg
-rwxr-xr-x 1 root root 44448413 Jun 16 16:11 splunkforwarder-9.0.5-e9494146ae5c.x86_64.rpm
drwx----- 3 root root 17 Jun 9 15:35 systemd-private-7c223981f01b433b804b99b30c44128c-chronyd.service-xd7Qth
drwxrwxrwx 3 root root 25 Jun 5 17:03 pkg
drwx----- 2 root root 6 Jun 5 09:15 vmware-root_938-2689078411
drwx----- 2 root root 6 Jun 5 12:18 vmware-root_940-2689209484
drwx----- 2 root root 6 Jun 5 15:12 vmware-root_941-4022177618
drwx----- 2 root root 6 Jun 5 10:38 vmware-root_942-2697663758
drwx----- 2 root root 6 Jun 5 14:36 vmware-root_943-4013723344
drwx----- 2 root root 6 Jun 5 14:43 vmware-root_952-2730562329
drwx----- 2 root root 6 Jun 9 15:35 vmware-root_966-2999001944
drwx----- 2 root root 6 Jun 5 18:16 vmware-root_967-4248221830
drwx----- 2 root root 6 Jun 9 15:25 vmware-root_968-2965448017
drwx----- 2 root root 6 Jun 5 18:09 vmware-root_972-2957124820
drwx----- 2 root root 6 Jun 6 05:17 vmware-root_979-4290625299
drwx----- 2 root root 6 Jun 9 14:56 vmware-root_980-2957518026
-rw-rw-rw- 1 root root 113 Jun 19 10:37 zabbix_agent.get_and_setup.err
-rw-rw-rw- 1 root root 538 Jun 19 10:37 zabbix_agent.get_and_setup.log
-rwxr-xr-x 1 root root 37394 May 23 16:32 zabbix_agent.get_and_setup.sh
[root@psnbckfre101 tmp]# cd pkg
[root@psnbckfre101 pkg]# sudo ./cvpkgadd
```

Figura 30 – Steps installazione client Linux on IaaS IND STD

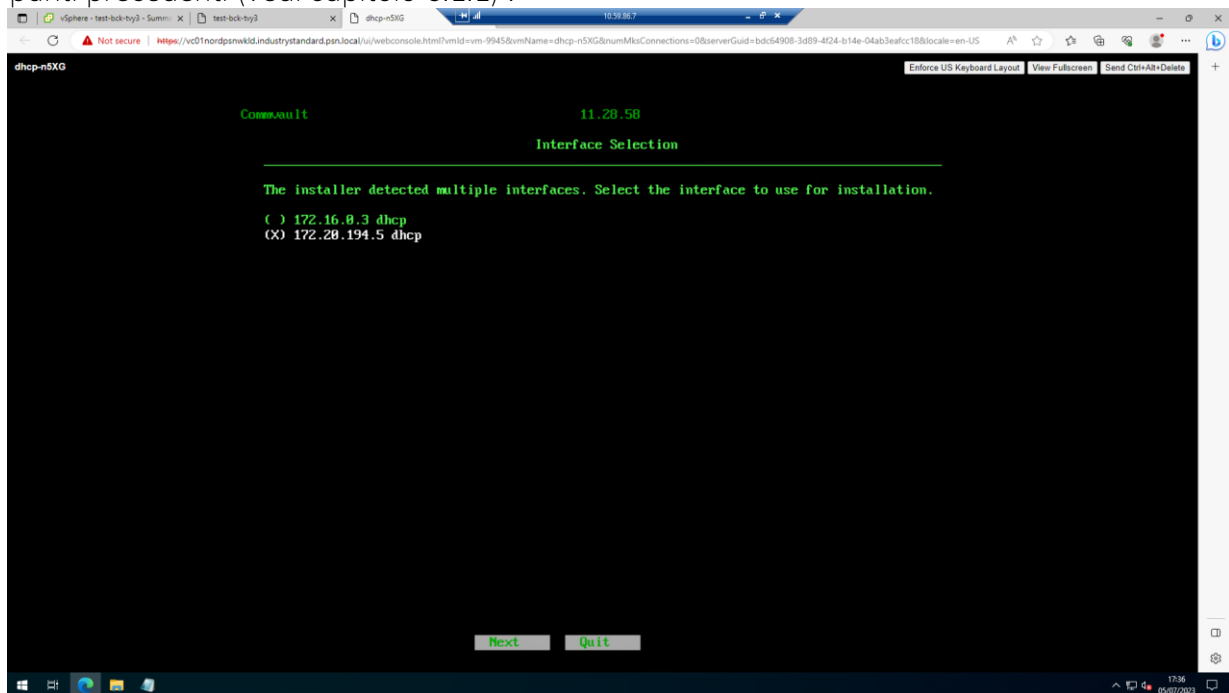
Alla schermata successiva selezionare **“Next”** per proseguire.



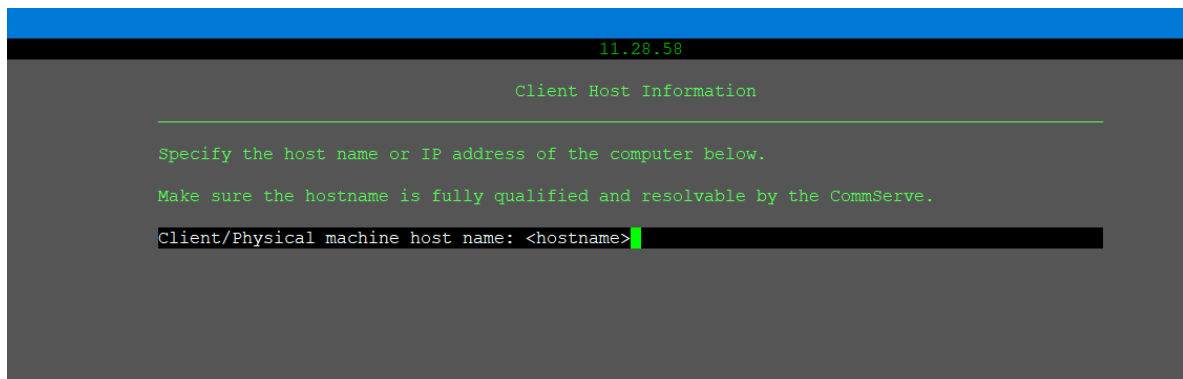
Steps installazione client Linux on IaaS IND STD

Quindi scegliere la directory di installazione (è preferibile non modificare la directory di default).

Selezionare l'interfaccia della subnet di backup (172.20.194.0/23 o 172.21.194.0/23) importata ai punti precedenti (vedi capitolo 6.1.1) :

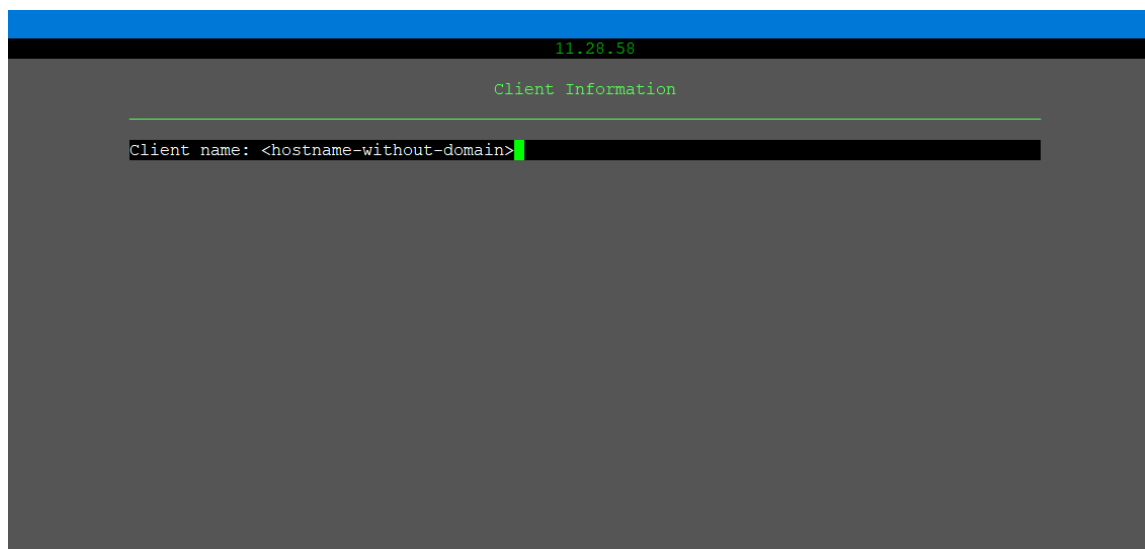


Steps installazione client Linux on IaaS IND STD



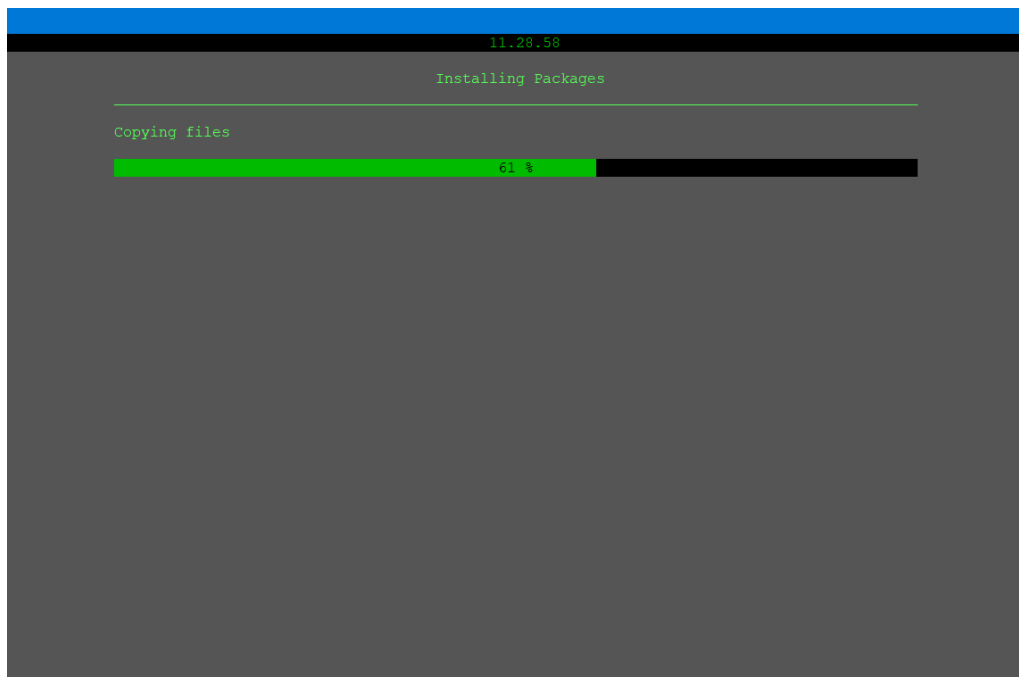
Steps installazione client Linux on IaaS IND STD

Digitare "Next" alle schermate successive relative ad hostname e clientname.

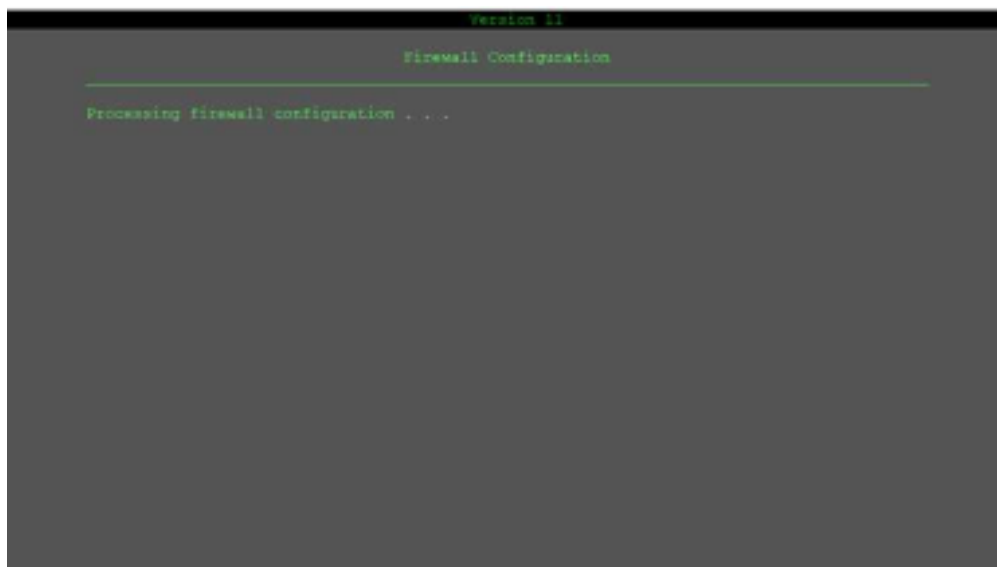


Steps installazione client Linux on IaaS IND STD

Quindi attendere il completamento della procedura di installazione.



Steps installazione client Linux on IaaS IND STD



Steps installazione client Linux on IaaS IND STD

6.3 Aggiornamento del client con ulteriori agent

Per poter installare ulteriori agent di backup (ad esempio per i Database Oracle, SQL Server, PostgreSQL, SAP for Oracle, SAP Hana, Sybase, ecc) è necessario che il server sia già registrato come client.

Accedere alla console di amministrazione del servizio e selezionare *Manage – Servers* dal menu di sinistra.

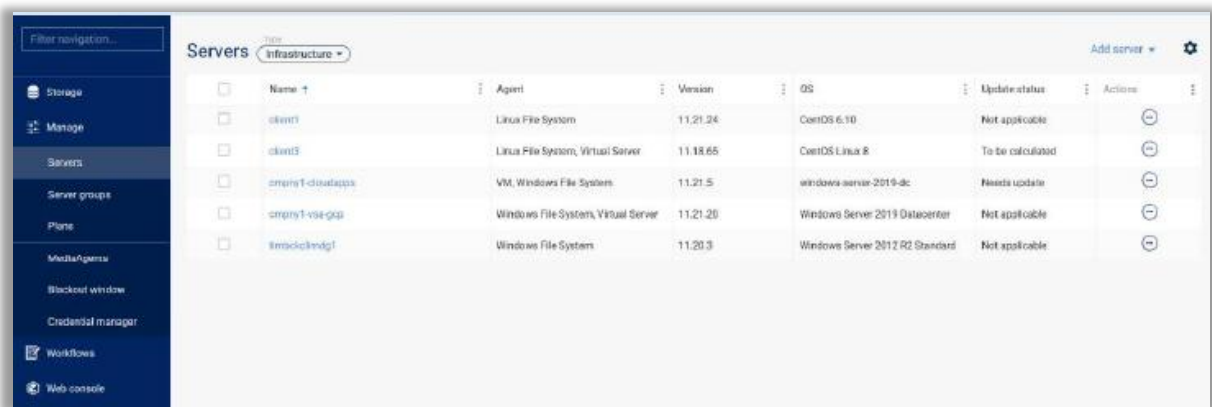
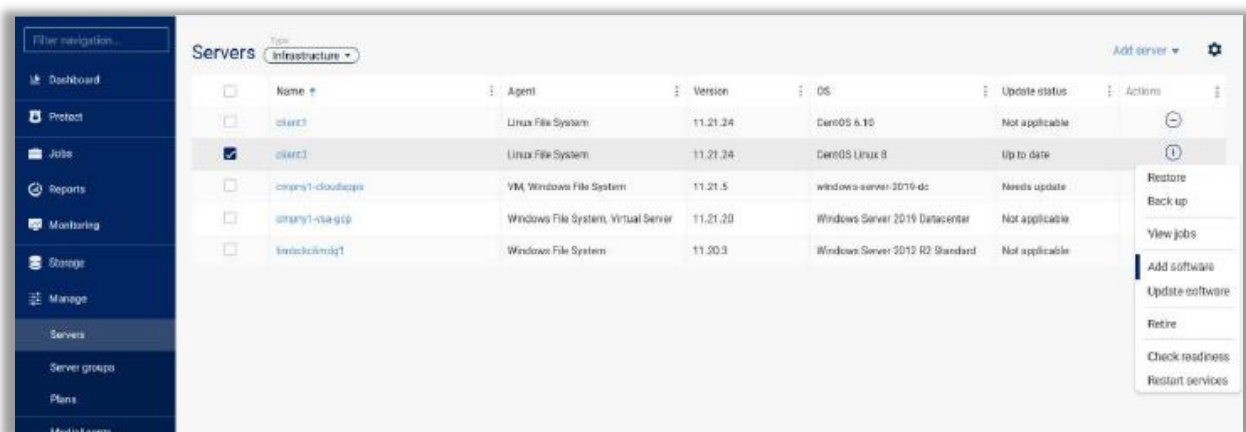


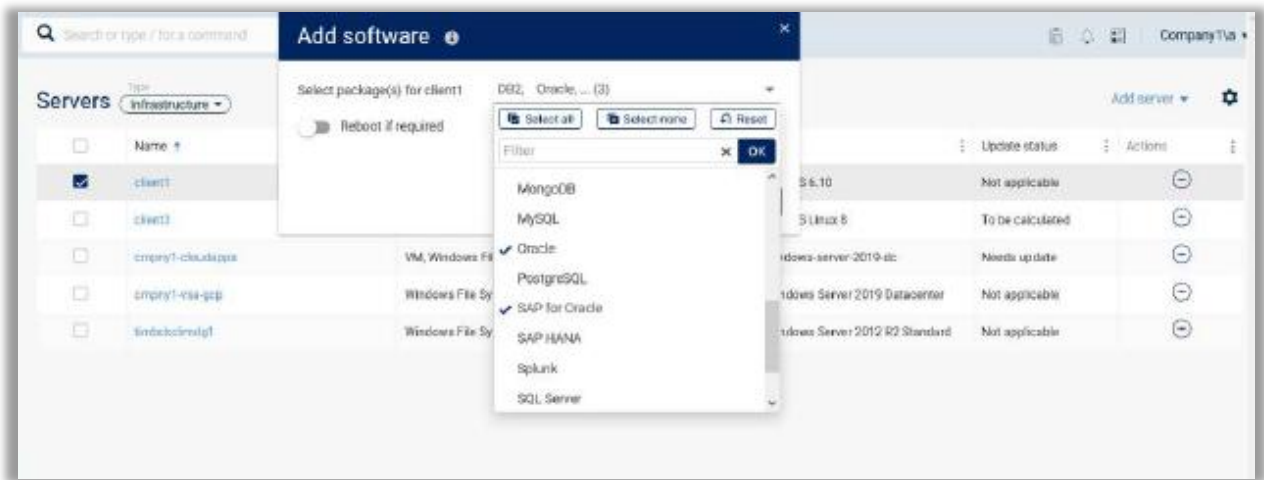
Figura 31 – Steps installazione altri agent su Client on IaaS IND STD

Individuare il client che si vuole aggiornare e attraverso il menù a tendina della colonna actions in corrispondenza del nome client individuato selezionare *Add Software*



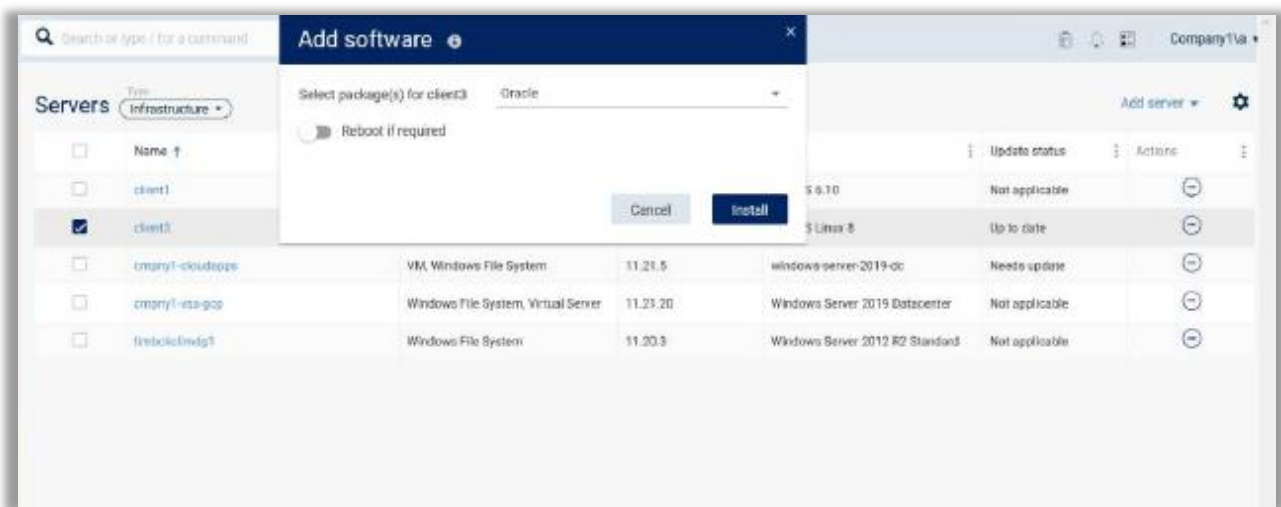
Steps Installazione nuovo agent di backup on IaaS IND STD

Selezionare gli agent software da installare (anche più di uno contemporaneamente) dal menu a tendina e premere il tasto *OK*



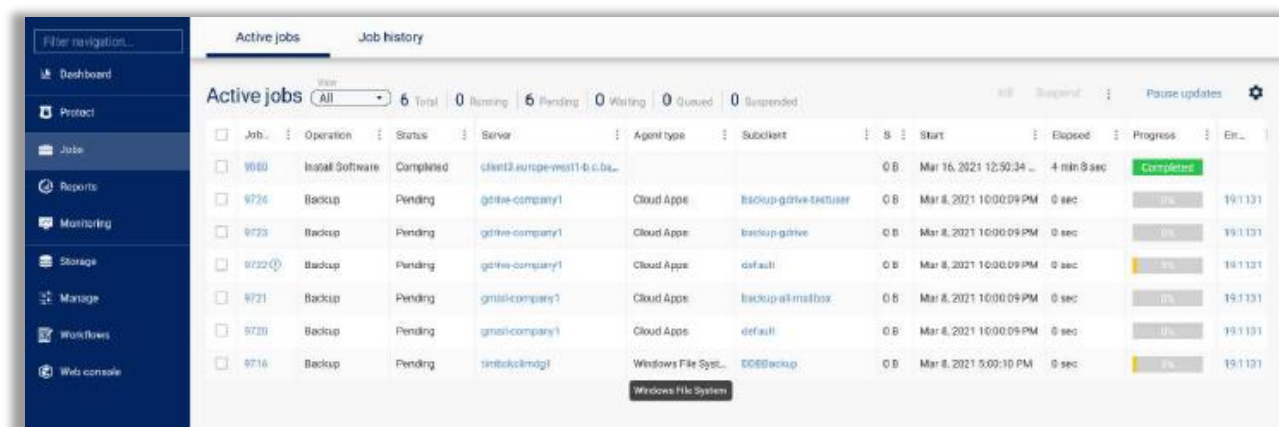
Steps Installazione nuovo agent di backup on IaaS IND STD

Quindi premere il tasto *Install*



Steps Installazione nuovo agent di backup on IaaS IND STD

Attendere la corretta esecuzione del job eseguito verificandone lo stato dalla sezione Jobs del menu a sinistra



Job ID	Operation	Status	Server	Agent type	Subclient	S	Start	Elapsed	Progress	Err.
9760	Install Software	Completed	client3.europe-west1-b.c.b...			0 B	Mar 8, 2021 12:50:34 ...	4 min 8 sec	Completed	
9726	Backup	Pending	gdrive-company1	Cloud Apps	Backup-gdrive-testuser	0 B	Mar 8, 2021 10:00:09 PM	0 sec	0%	19/11/31
9723	Backup	Pending	gdrive-company1	Cloud Apps	Backup-gdrive	0 B	Mar 8, 2021 10:00:09 PM	0 sec	0%	19/11/31
9722	Backup	Pending	gdrive-company1	Cloud Apps	default	0 B	Mar 8, 2021 10:00:09 PM	0 sec	0%	19/11/31
9721	Backup	Pending	gmail-company1	Cloud Apps	Backup-all-mailbox	0 B	Mar 8, 2021 10:00:09 PM	0 sec	0%	19/11/31
9720	Backup	Pending	gmail-company1	Cloud Apps	default	0 B	Mar 8, 2021 10:00:09 PM	0 sec	0%	19/11/31
9716	Backup	Pending	simbolsimdg1	Windows File Syst...	CCSDBackup	0 B	Mar 8, 2021 5:00:10 PM	0 sec	0%	19/11/31

Figura 32 – Monitoraggio job di “Installazione nuovo agent di backup on IaaS IND STD”

6.4 Upgrade software del client già registrato

Individuare il client che si vuole aggiornare e attraverso il menù a tendina della colonna *Actions*, in corrispondenza del client individuato, selezionare *Update software*.

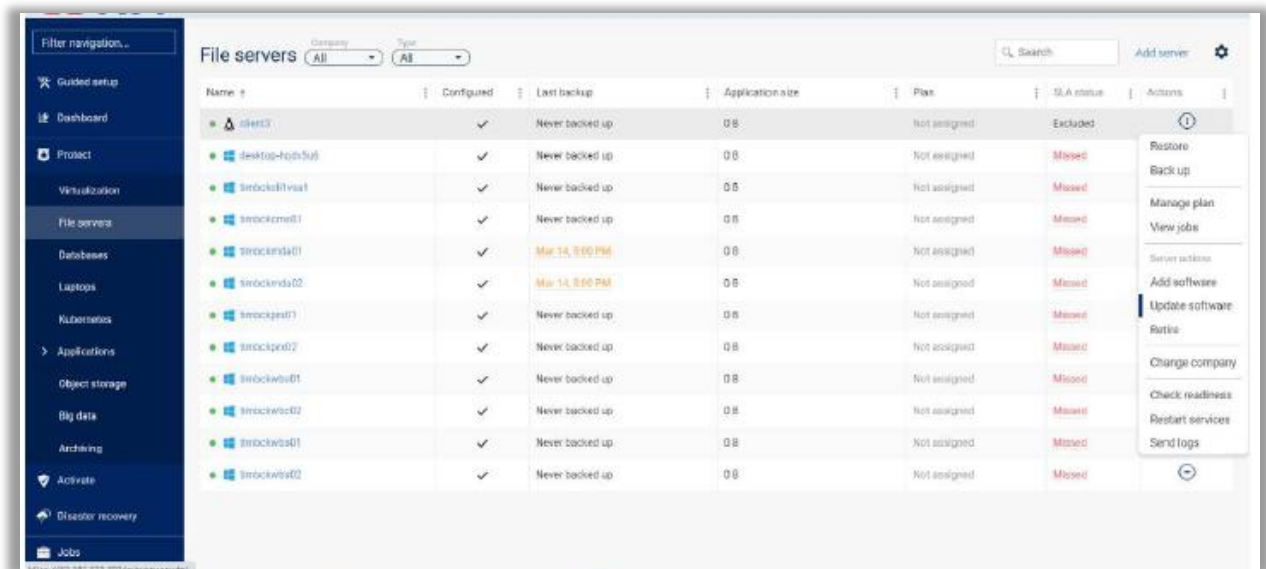
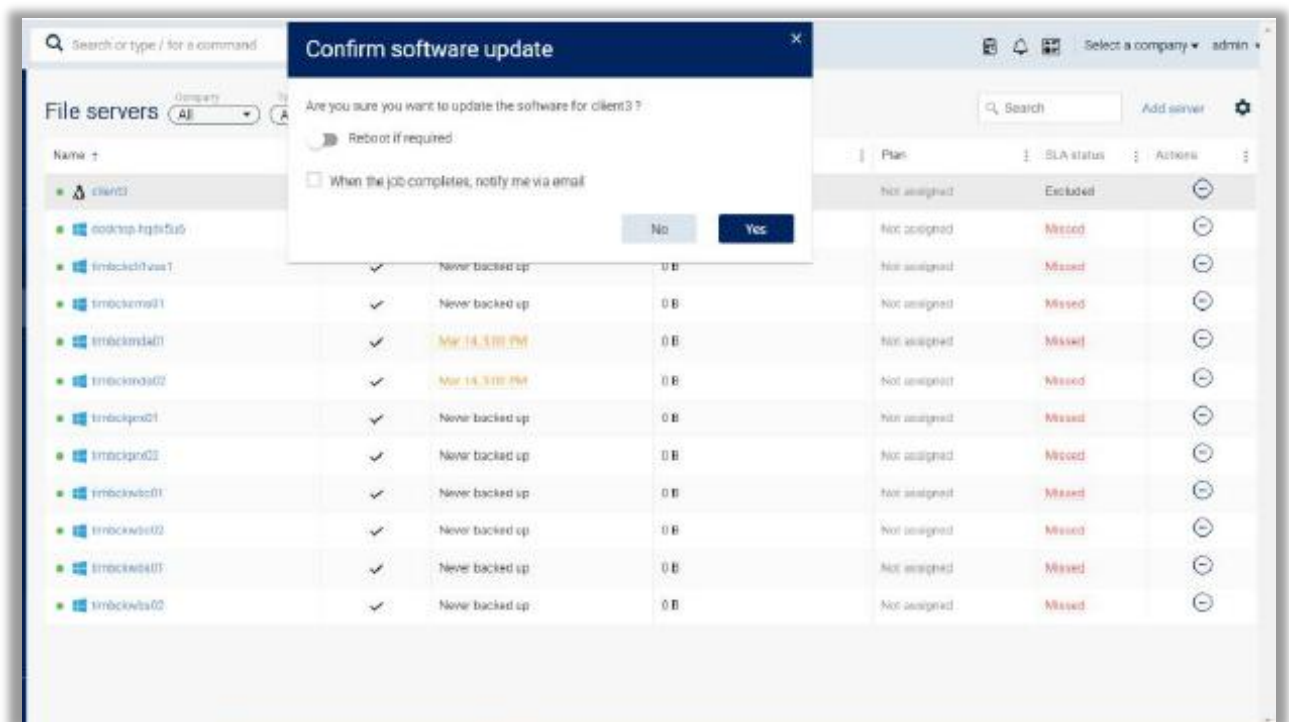


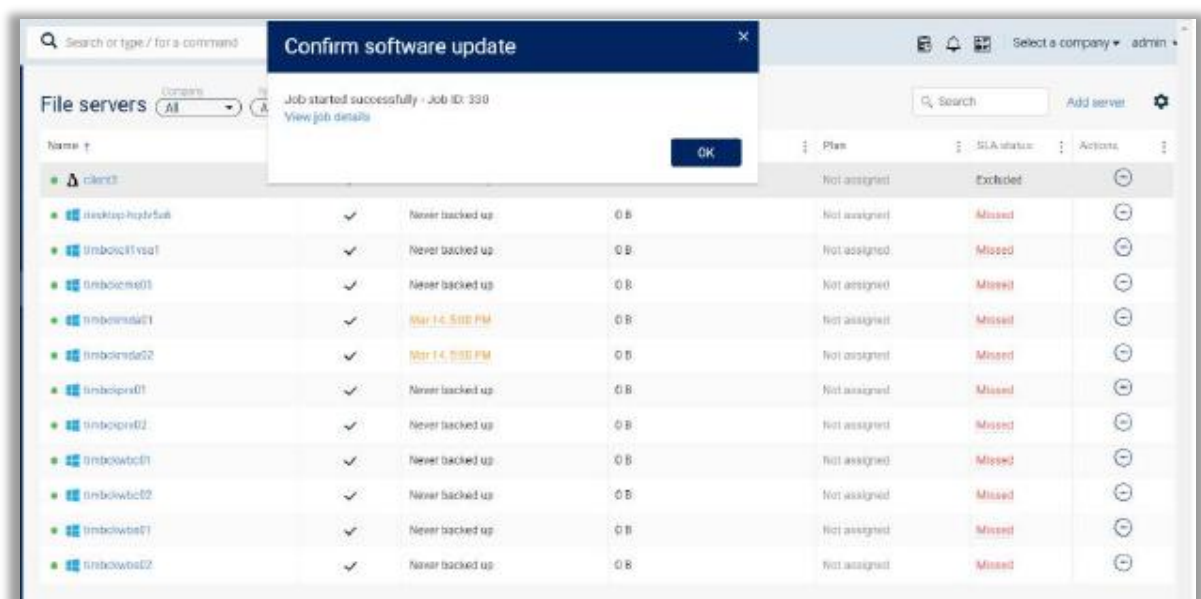
Figura 33 – Steps aggiornamento client on IaaS IND STD

Quindi scegliere se effettuare il reboot (l'aggiornamento non prevede un reboot del server target ma il solo eventuale riavvio automatico dei servizi Commvault) e ricevere notifica via e-mail al completamento del job di update e digitare il tasto Yes



Steps aggiornamento client on IaaS IND STD

Quindi digitare sul tasto OK relativo alla notifica della esecuzione del job. Attendere la corretta esecuzione del job eseguito.



Steps aggiornamento client on IaaS IND STD

7 Configurazione dei client Secure Public Cloud

Le istruzioni contenute in questo capitolo si riferiscono alle operazioni relative alla installazione e configurazione dei client preliminari alle attività di schedulazione, backup e restore dei dati in tutti quei casi in cui è necessario predisporre il backup tramite agent dei server Secure Public Cloud.

In particolare è necessario installare un agent di tipo File System se si vuole effettuare un restore di un *guest File* di un backup di una Virtual Machine altrimenti non sarà visibile alcuna VM utile su cui effettuare il restore.

7.1 *Prerequisiti per backup agent Secure Public Cloud*

Prima di effettuare l'installazione di un nuovo client è necessario verificare che la macchina sia dotata di un'adeguata connettività ai sistemi. Pertanto, è importante che le seguenti porte risultino aperte su tutti i firewall coinvolti fino alla raggiungibilità del servizio su Internet:

- 8400
- 8401
- 8402
- 8403

Il client dovrà raggiungere l'access node del servizio Secure Public Cloud.

7.2 *Installazione di un server client (tenant administrator)*

Nel paragrafo successivo è descritta la procedura per installare un nuovo client nel servizio PSN Backup su Commvault, l'installazione va eseguita con un'utenza di sistema operativo dotata di diritti amministrativi.

7.2.1 Client Windows

Individuare il server con sistema operativo Windows sul quale si vorranno applicare le policy di backup o che sarà utilizzato per le varie funzionalità del servizio.

Scaricare, sul server in questione, il pacchetto di installazione SPC relativo al sistema operativo Windows, selezionando dal menu della console la voce **'Web Console'** e quindi **'Download Center'**.

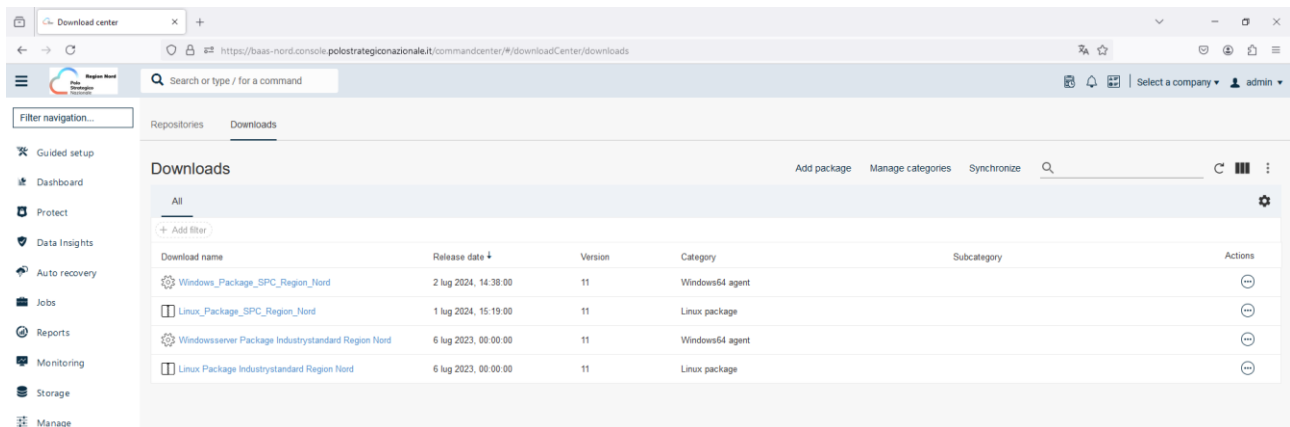
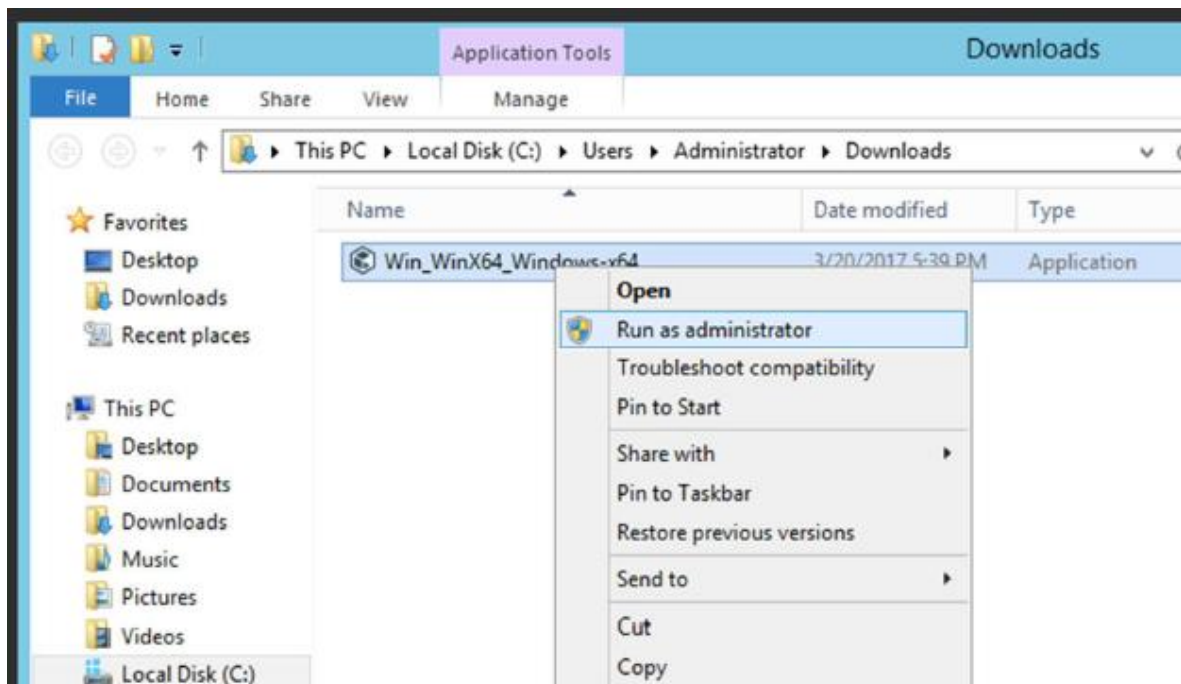


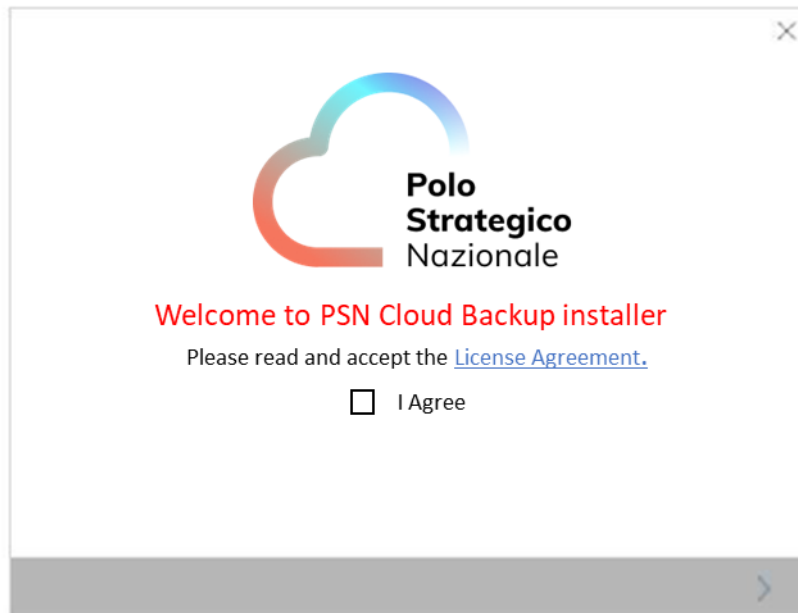
Figura 34 – Steps installazione client Windows on SPC

Dopo aver scaricato il relativo pacchetto per il sistema operativo Windows, selezionare la voce **"Run as Administrator"** digitando con il tasto destro del mouse sul pacchetto appena scaricato.



Steps installazione client Windows on SPC

Inserire il segno di spunta come indicato in figura e digitare il tasto in basso a destra per continuare l'installazione.



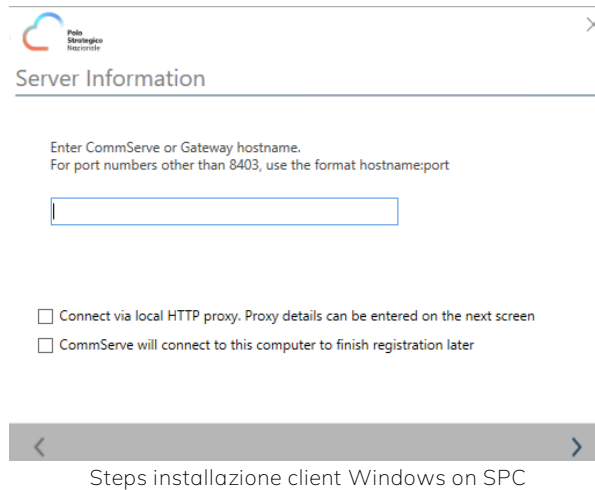
Steps installazione client Windows on SPC

Quindi il software inizierà l'esecuzione.



Steps installazione client Windows on SPC

Inserire il nome dell'access node (nome xxxxx-spcvsa01) SPC ricavabile dalla sezione Protect-Server del portale di backup.



Server Information

Enter CommServe or Gateway hostname.
For port numbers other than 8403, use the format hostname:port

☐ Connect via local HTTP proxy. Proxy details can be entered on the next screen
☐ CommServe will connect to this computer to finish registration later

< >

Steps installazione client Windows on SPC



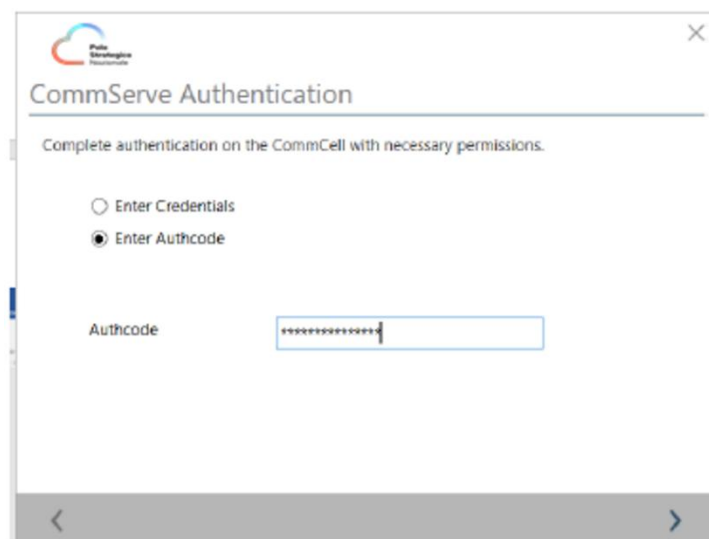
Steps installazione client Windows on SPC

Al termine dell'installazione si avvierà il processo di registrazione del client sul servizio.



Steps installazione client Windows on SPC

A tal fine sarà necessario inserire l'utenza e l'Authcode, quest'ultimo reperibile nella sezione *Reports*.

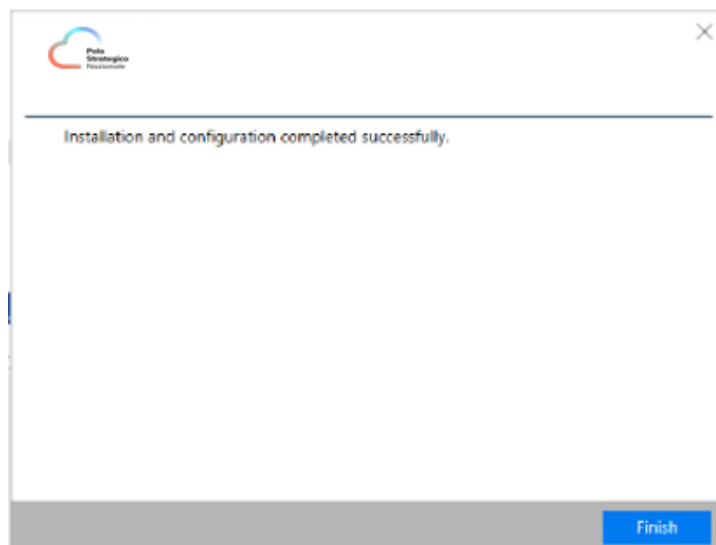


Steps installazione client Windows on SPC



Steps installazione client Windows on SPC

L'installazione risulterà completata alla visualizzazione della schermata successiva.



Steps installazione client Windows on SPC

Digitare quindi *'Finish'* per completare l'installazione.

7.2.2 Client Linux

Individuare il server con sistema operativo Linux sul quale si vorranno applicare le policy di backup o che sarà utilizzato per le varie funzionalità del servizio.

Scaricare, sul server in questione, il pacchetto di installazione SPC relativo al sistema operativo Linux, selezionando dal menu della console la voce '**Web Console**' e quindi '**Download Center**'.

Quindi procedere a scompattare il file .tar entrando nella directory e digitando:

```
tar -xvf NOMEPAcCHETTO.tar
(es. tar -xvf linuxclientcvsp7.tar)
```

Dopo aver completato la decompressione del file selezionare la directory `pkg` e avviare la procedura di installazione digitando

```
./cvpkgadd
```

La procedura di installazione richiede utenza root quindi se necessario utilizzare comando `sudo`.

```
bash: mkd: command not found
[root@psnbckfre101 tmp]# mkdir pkg
[root@psnbckfre101 tmp]# ll
total 54528
-rw-r--r-- 1 root root 0 Jun 14 10:57 bdiinstaller.lock
drwxr-xr-x 2 root root 63 Jun 14 11:06 bdi defender
-rw-r--r-- 1 root root 11335168 Jun 14 10:53 installer.tar
drwxr-xr-x 2 root root 6 Jun 5 21:55 locks
drwxr-xr-x 2 root root 6 Jun 21 14:19 pkg
-rwxr-xr-x 1 root root 44448413 Jun 16 16:11 splunkforwarder-9.0.5-e9494146ae5c.x86_64.rpm
drwx----- 3 root root 17 Jun 9 15:35 systemd-private-7c223981f01b433b804b99b30c44128c-chronyd.service-xd7Qth
drwxrwxrwx 3 root root 25 Jun 5 17:03 tmp
drwx----- 2 root root 6 Jun 5 09:15 vmware-root_938-2689078411
drwx----- 2 root root 6 Jun 5 12:18 vmware-root_940-2689209484
drwx----- 2 root root 6 Jun 5 15:12 vmware-root_941-4022177618
drwx----- 2 root root 6 Jun 5 10:38 vmware-root_942-2697663758
drwx----- 2 root root 6 Jun 5 14:36 vmware-root_943-4013723344
drwx----- 2 root root 6 Jun 5 14:43 vmware-root_952-2730562329
drwx----- 2 root root 6 Jun 9 15:35 vmware-root_966-2999001944
drwx----- 2 root root 6 Jun 5 18:16 vmware-root_967-4248221830
drwx----- 2 root root 6 Jun 9 15:25 vmware-root_968-2965448017
drwx----- 2 root root 6 Jun 5 18:09 vmware-root_972-2957124820
drwx----- 2 root root 6 Jun 6 05:17 vmware-root_979-4290625299
drwx----- 2 root root 6 Jun 9 14:56 vmware-root_980-2957518026
-rw-rw-rw- 1 root root 113 Jun 19 10:37 zabbix_agent.get_and_setup.err
-rw-rw-rw- 1 root root 538 Jun 19 10:37 zabbix_agent.get_and_setup.log
-rwxr-xr-x 1 root root 37394 May 23 16:32 zabbix_agent.get_and_setup.sh
[root@psnbckfre101 tmp]# cd pkg
[root@psnbckfre101 pkg]# sudo ./cvpkgadd
```

Figura 35 – Steps installazione client Linux on SPC

Alla schermata successiva selezionare "**Next**" per proseguire.

```
11.28.58
Welcome to Commvault Installer

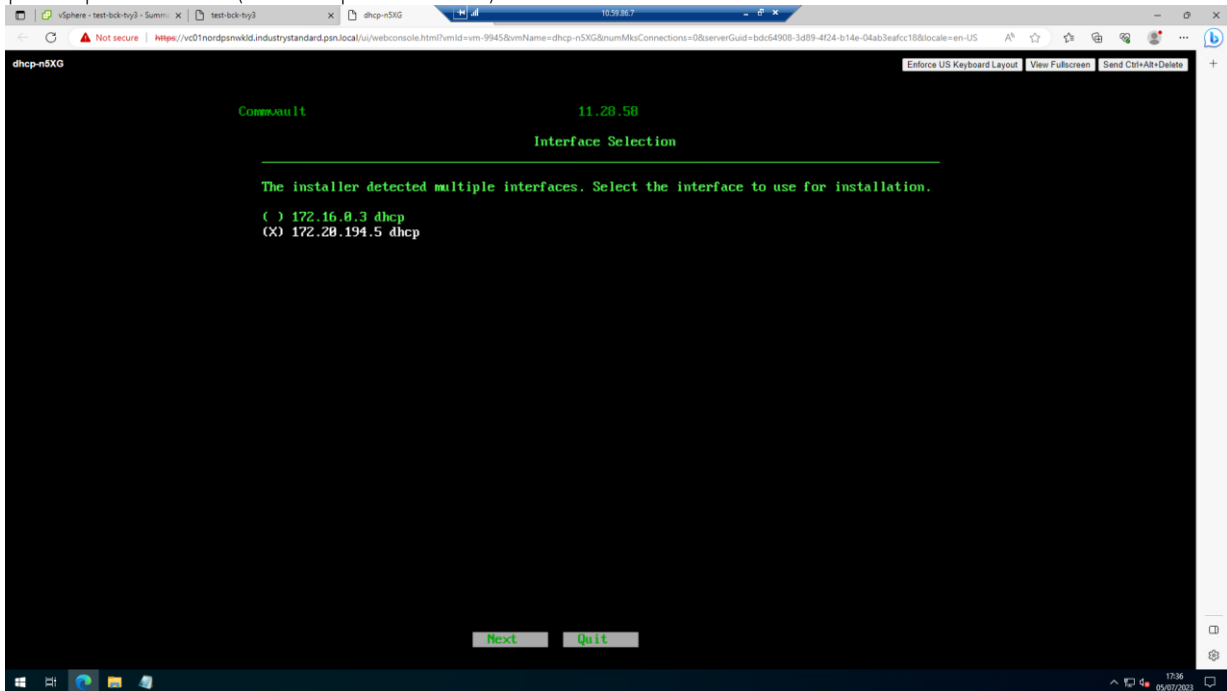
For support please visit http://www.commvault.com/support, or send an email to
support@commvault.com, or call US/CANADA (Toll Free) (877) 780-3077; INTERNATIONAL (732)
571-2160

This installer will install Commvault packages on this machine. Log Messages will be sent
to /var/log/.gxsetup/logs/20230517/install.log
```

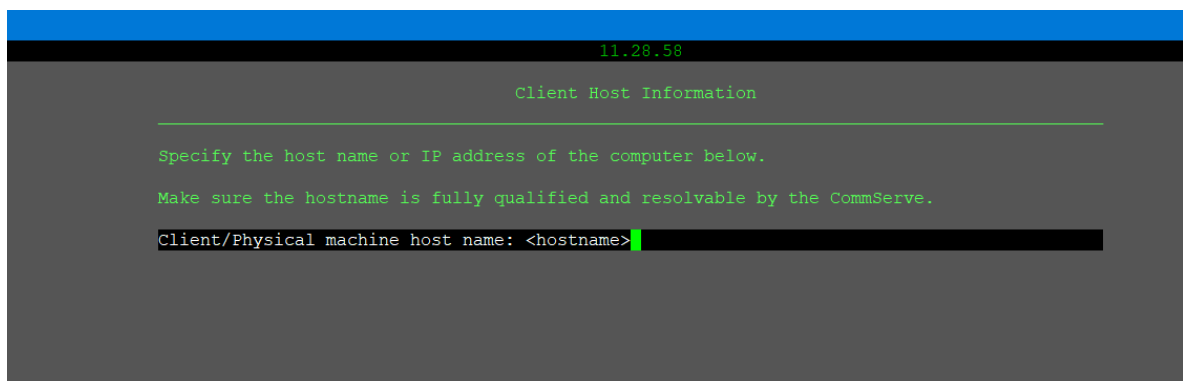
Steps installazione client Linux on SPC

Quindi scegliere la directory di installazione (è preferibile non modificare la directory di default).

Selezionare l'interfaccia della subnet di backup (172.20.194.0/23 o 172.21.194.0/23) importata ai punti precedenti (vedi capitolo 6.1.1) :

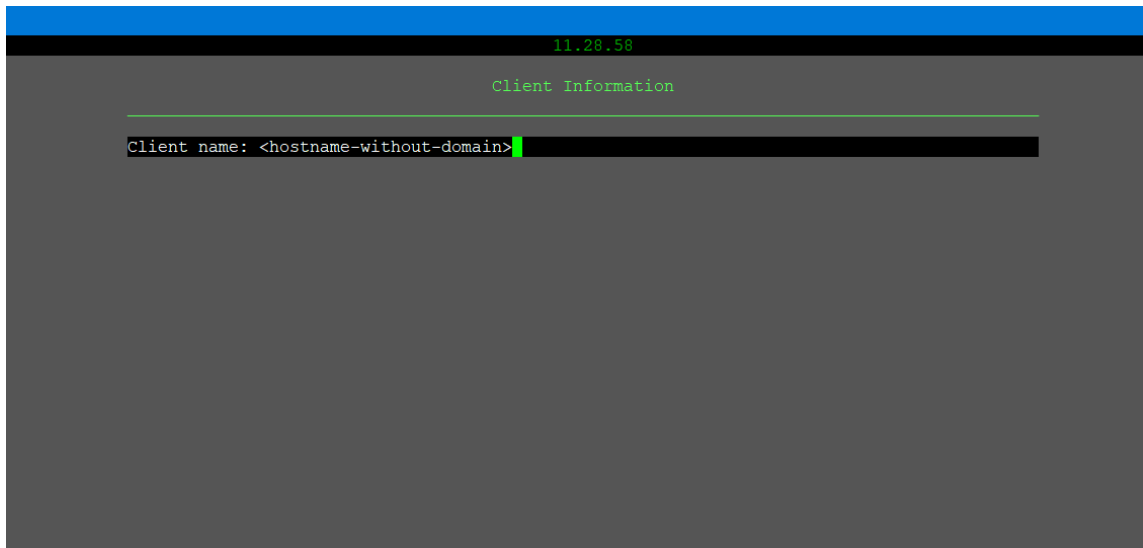


Steps installazione client Linux on SPC



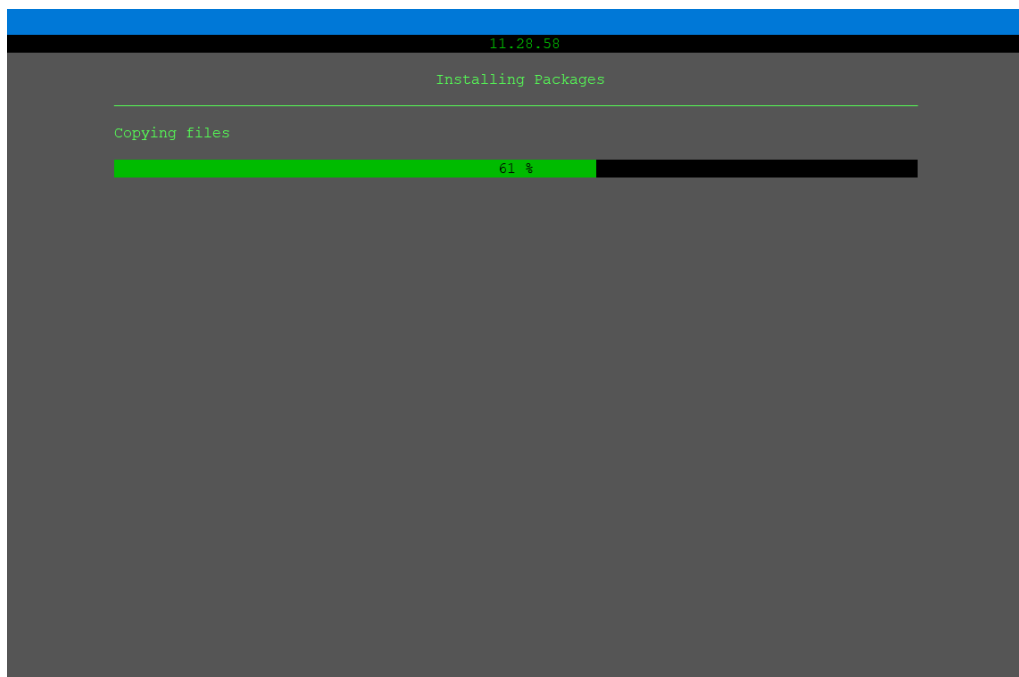
Steps installazione client Linux on SPC

Digitare "Next" alle schermate successive relative ad hostname e clientname.



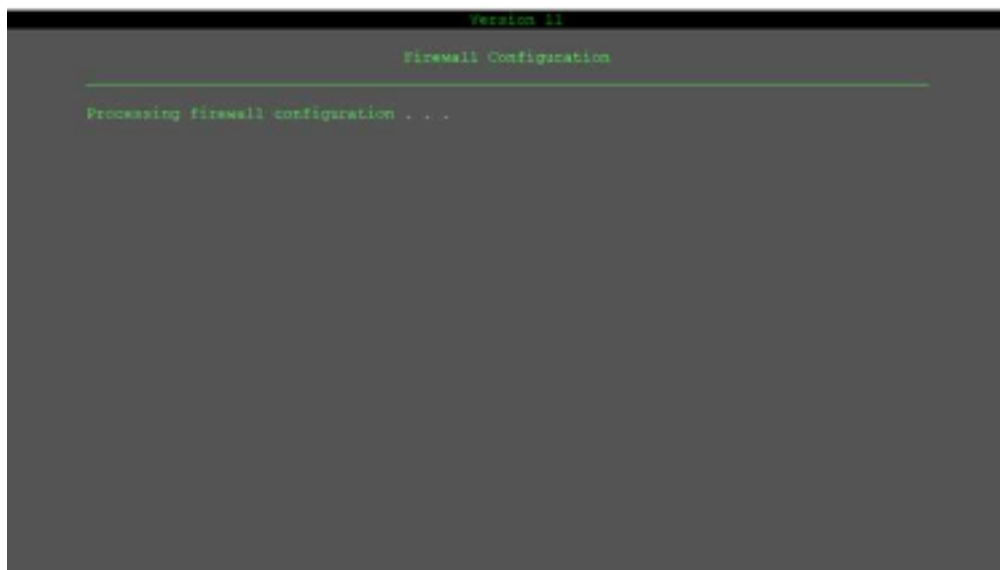
Steps installazione client Linux on SPC

Quindi attendere il completamento della procedura di installazione.



Steps installazione client Linux on SPC

Inserire il nome dell'access node (nome xxxxx-spcvsa01) SPC ricavabile dalla sezione Protect-Server del portale di backup.

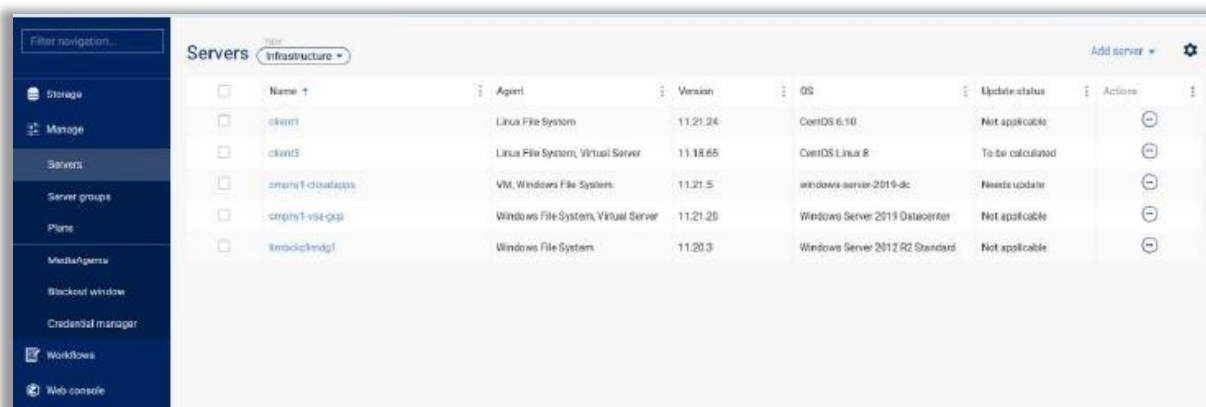


Steps installazione client Linux on SPC

7.3 Aggiornamento del client con ulteriori agent

Per poter installare ulteriori agent di backup (ad esempio per i Database Oracle, SQL Server, PostgreSQL, SAP for Oracle, SAP Hana, Sybase, ecc) è necessario che il server sia già registrato come client.

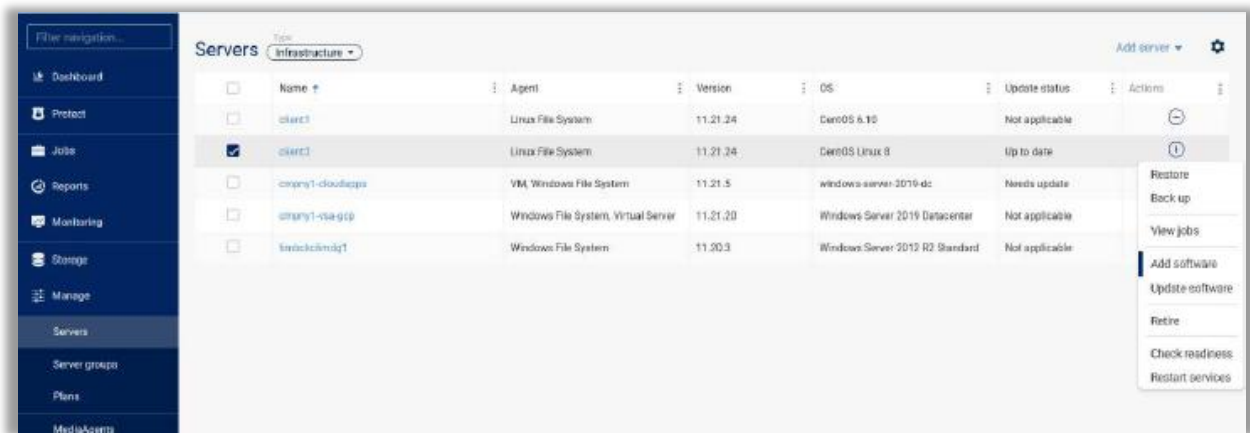
Accedere alla console di amministrazione del servizio e selezionare *Manage – Servers* dal menu di sinistra.



	Name ↑	Agent	Version	OS	Update status	Actions
☐	client1	Linux File System	11.21.24	CentOS 6.10	Not applicable	
☐	client5	Linux File System, Virtual Server	11.18.65	CentOS Linux 8	To be calculated	
☐	client1-cloudapp	VM, Windows File System	11.21.5	Windows Server 2019-DC	Needs update	
☐	client1-vse-gpu	Windows File System, Virtual Server	11.21.20	Windows Server 2019 Datacenter	Not applicable	
☐	client1-k8s	Windows File System	11.20.3	Windows Server 2012 R2 Standard	Not applicable	

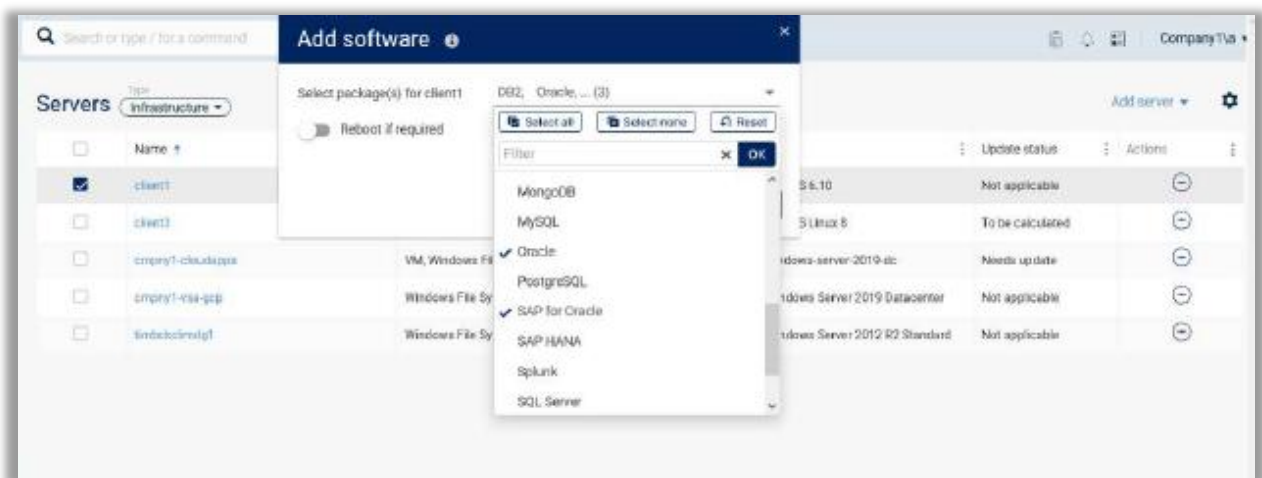
Figura 36 – Steps installazione altri agent su Client on SPC

Individuare il client che si vuole aggiornare e attraverso il menù a tendina della colonna actions in corrispondenza del nome client individuato selezionare *Add Software*



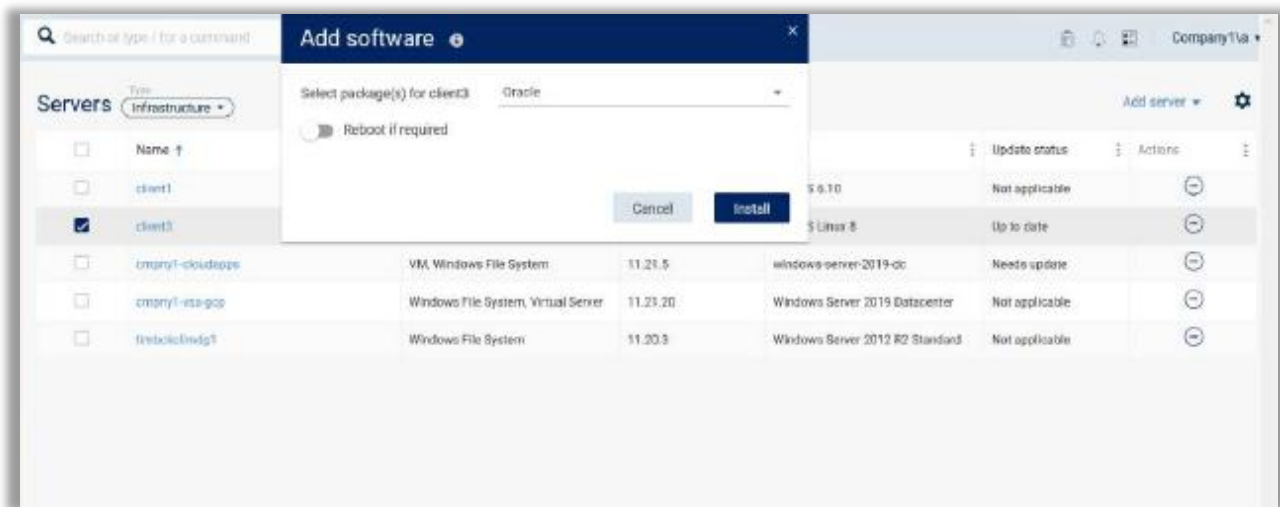
Steps installazione altri agent su Client on SPC

Selezionare gli agent software da installare (anche più di uno contemporaneamente) dal menu a tendina e premere il tasto OK



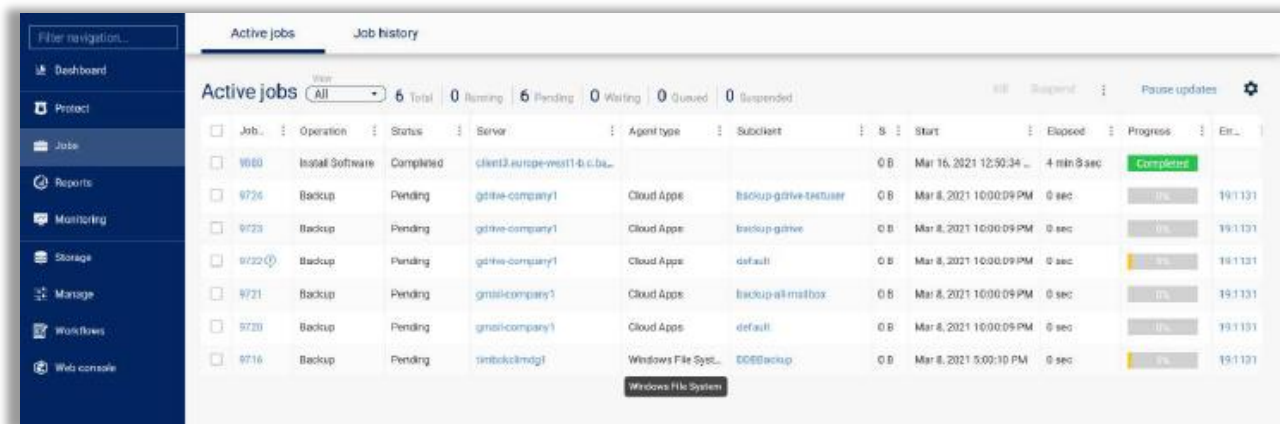
Steps installazione altri agent su Client on SPC

Quindi premere il tasto *Install*



Steps installazione altri agent su Client on SPC

Attendere la corretta esecuzione del job eseguito verificandone lo stato dalla sezione Jobs del menu a sinistra



Steps installazione altri agent su Client on SPC

7.4 Upgrade software del client già registrato

Individuare il client che si vuole aggiornare e attraverso il menù a tendina della colonna *Actions*, in corrispondenza del client individuato, selezionare *Update software*.

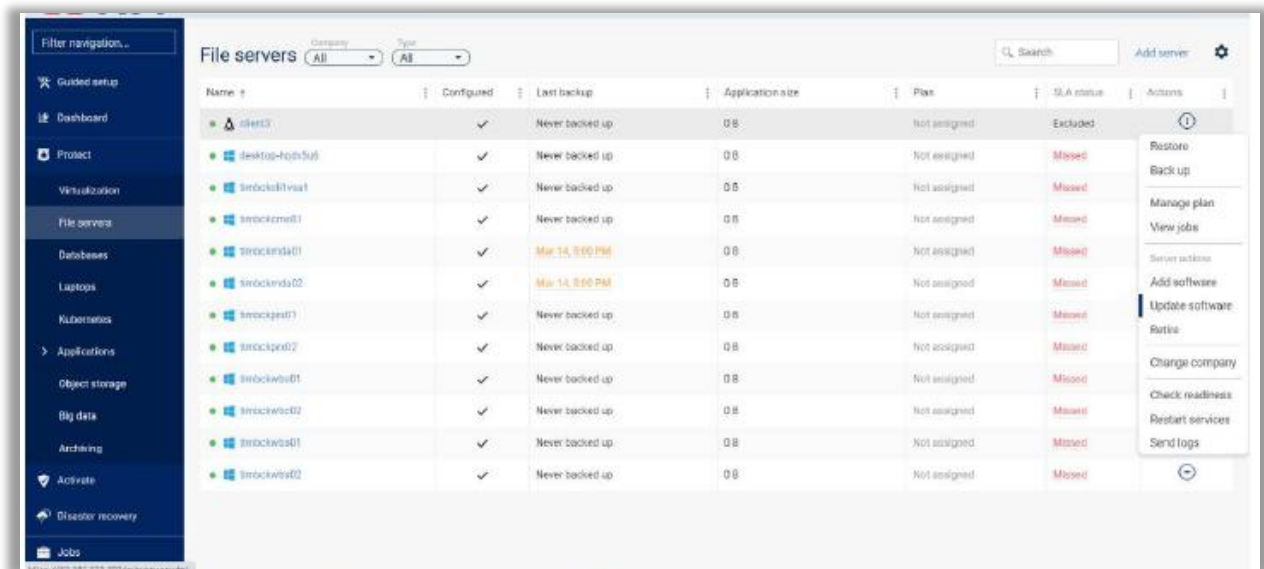
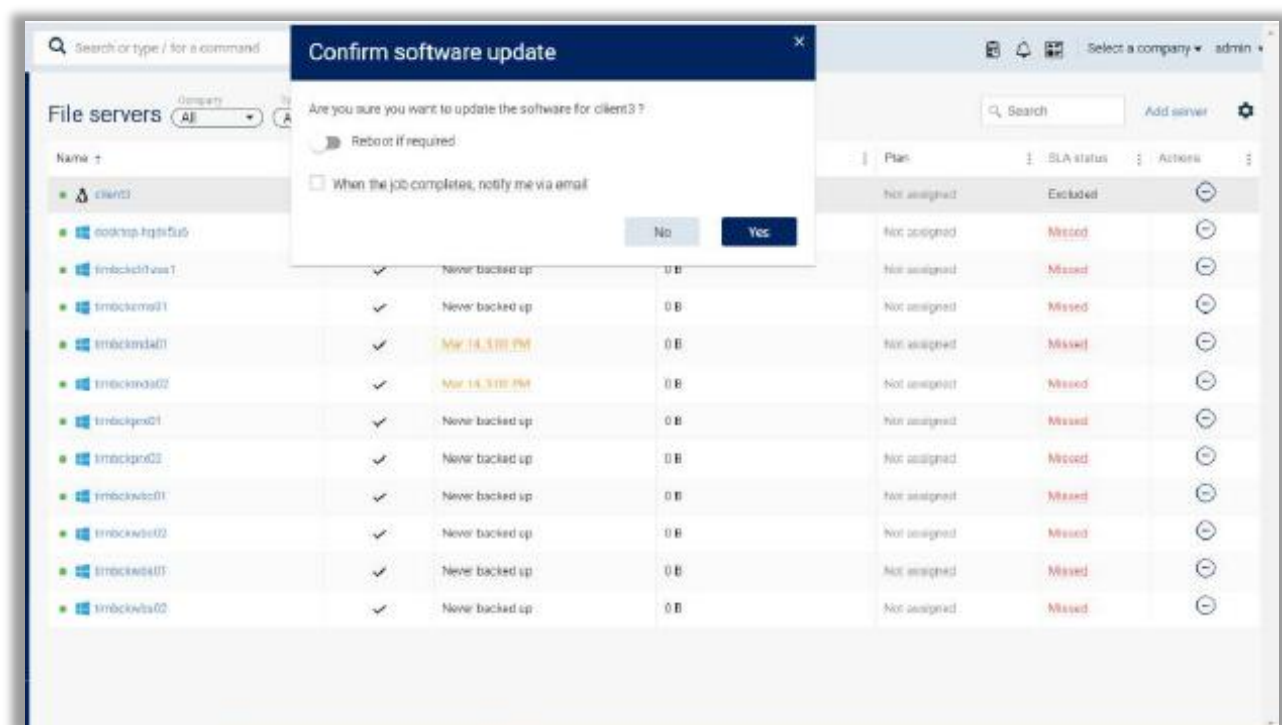


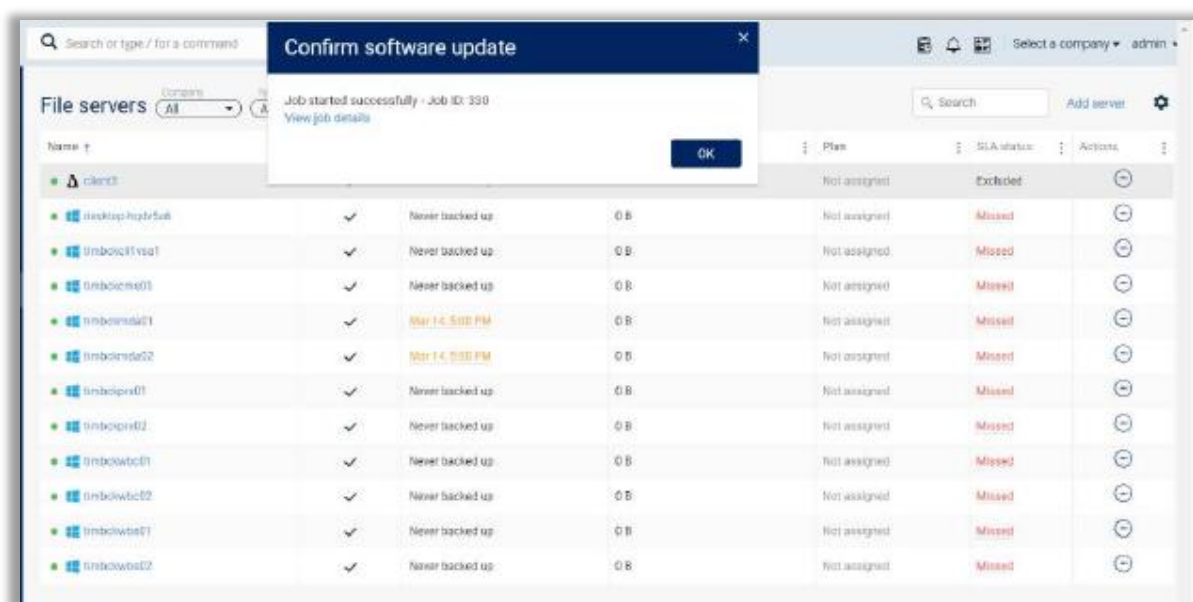
Figura 37 – Steps aggiornamento client agent on SPC

Quindi scegliere se effettuare il reboot (l'aggiornamento non prevede un reboot del server target ma il solo eventuale riavvio automatico dei servizi Commvault) e ricevere notifica via e-mail al completamento del job di update e digitare il tasto Yes



Steps aggiornamento client agent on SPC

Quindi digitare sul tasto OK relativo alla notifica della esecuzione del job. Attendere la corretta esecuzione del job eseguito.



Steps aggiornamento client agent on SPC

8 Configurazione dei client PSN MANAGED ORACLE CLOUD

Le istruzioni contenute in questo capitolo si riferiscono alle operazioni relative alla installazione e configurazione dei client preliminari alle attività di schedulazione, backup e restore dei dati in tutti quei casi in cui è necessario predisporre il backup tramite agent dei server PSN MANAGED ORACLE Cloud.

8.1 *Prerequisiti per backup agent Oracle cloud*

Prima di effettuare l'installazione di un nuovo client è necessario verificare che la macchina sia dotata di un'adeguata connettività ai sistemi. Pertanto, è importante che le seguenti porte risultino aperte su tutti i firewall coinvolti fino alla raggiungibilità del servizio di backup:

- 8400
- 8401
- 8402
- 8403

!!ATTENZIONE Il client dovrà raggiungere l'access node del servizio PSN Managed Oracle Cloud. A tal fine sarà necessario richiedere attraverso un ticket (tramite la console di gestione dei servizi <https://console.polostrategiconazionale.i>) l'abilitazione alla visibilità e raggiungibilità delle network tra l'agent e il compartimento di servizio.

8.2 *Installazione di un server client (tenant administrator)*

Nel paragrafo successivo è descritta la procedura per installare un nuovo client nel servizio PSN Backup su Commvault, l'installazione va eseguita con un'utenza di sistema operativo dotata di diritti amministrativi.

8.2.1 *Client Linux su PSN Managed Oracle Cloud*

Individuare il server con sistema operativo Linux sul quale si vorranno applicare le policy di backup o che sarà utilizzato per le varie funzionalità del servizio.

Scaricare, sul server in questione, il pacchetto di installazione `PSN_Managed_Oracle_OCI` relativo al sistema operativo Linux, selezionando dal menu della console la voce '**Web Console**' e quindi '**Download Center**' (`Linux_Package_PSN_Managed_Oracle_OCI_Region_Sud`).

Quindi procedere a scompattare il file .tar entrando nella directory e digitando:

```
tar -xvf NOMEpacchetto.tar  
(es. tar -xvf Linux_Package_PSN_Managed_Oracle_OCI_Region_Sud.tar)
```

Dopo aver completato la decompressione del file selezionare la directory `pkg` e avviare la procedura di installazione digitando con i diritti di root

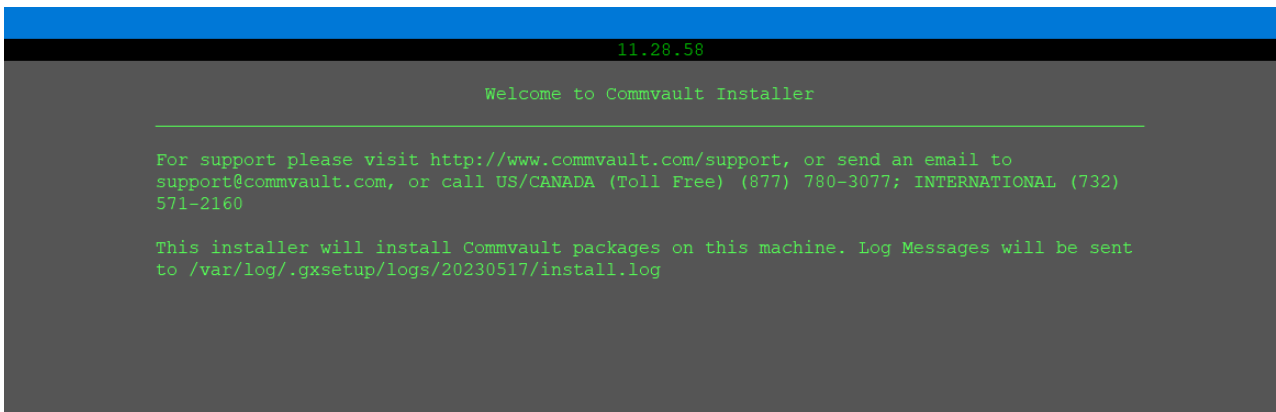
`./cvpkgadd`

La procedura di installazione richiede utenza root quindi se necessario utilizzare comando `sudo`.

```
-bash: mki: command not found
[root@psnbckfre101 tmp]# mkdir pkg
[root@psnbckfre101 tmp]# ll
total 54528
-rw-r--r-- 1 root root      0 Jun 14 10:57 bdinstaller.lock
drwxr-xr-x 2 root root    63 Jun 14 11:06 bitdefender
-rw-r--r-- 1 root root 11335168 Jun 14 10:53 installer.tar
drwxr-xr-x 2 root root      6 Jun 5 21:55 locks
drwxr-xr-x 2 root root      6 Jun 21 14:19 pkg
-rwxr-xr-x 1 root root 44448413 Jun 16 16:11 splunkforwarder-9.0.5-e9494146ae5c.x86_64.rpm
drwx----- 3 root root    17 Jun 9 15:35 systemd-private-7c223981f01b433b804b99b30c44128c-chronyd.service-xd7Qth
drwxrwxrwx 3 root root    25 Jun 5 17:03 [redacted]
drwx----- 2 root root      6 Jun 5 09:15 vmware-root_938-2689078411
drwx----- 2 root root      6 Jun 5 12:18 vmware-root_940-2689209484
drwx----- 2 root root      6 Jun 5 15:12 vmware-root_941-4022177618
drwx----- 2 root root      6 Jun 5 10:38 vmware-root_942-2697663758
drwx----- 2 root root      6 Jun 5 14:36 vmware-root_943-4013723344
drwx----- 2 root root      6 Jun 5 14:43 vmware-root_952-2730562329
drwx----- 2 root root      6 Jun 9 15:35 vmware-root_966-2999001944
drwx----- 2 root root      6 Jun 5 18:16 vmware-root_967-4248221830
drwx----- 2 root root      6 Jun 9 15:25 vmware-root_968-2965448017
drwx----- 2 root root      6 Jun 5 18:09 vmware-root_972-2957124820
drwx----- 2 root root      6 Jun 6 05:17 vmware-root_979-4290625299
drwx----- 2 root root      6 Jun 9 14:56 vmware-root_980-2957518026
-rw-rw-rw- 1 root root    113 Jun 19 10:37 zabbix_agent.get_and_setup.err
-rw-rw-rw- 1 root root    538 Jun 19 10:37 zabbix_agent.get_and_setup.log
-rwxr-xr-x 1 root root   37394 May 23 16:32 zabbix_agent.get_and_setup.sh
[root@psnbckfre101 tmp]# cd pkg
[root@psnbckfre101 pkg]# sudo ./cvpkgadd
```

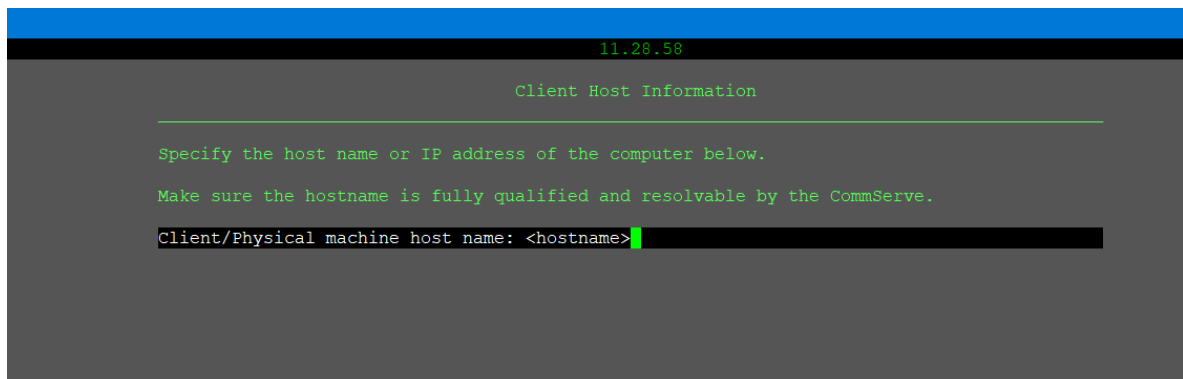
Figura 38 – Steps installazione client Linux on Oracle_OCI

Alla schermata successiva selezionare **“Next”** per proseguire.



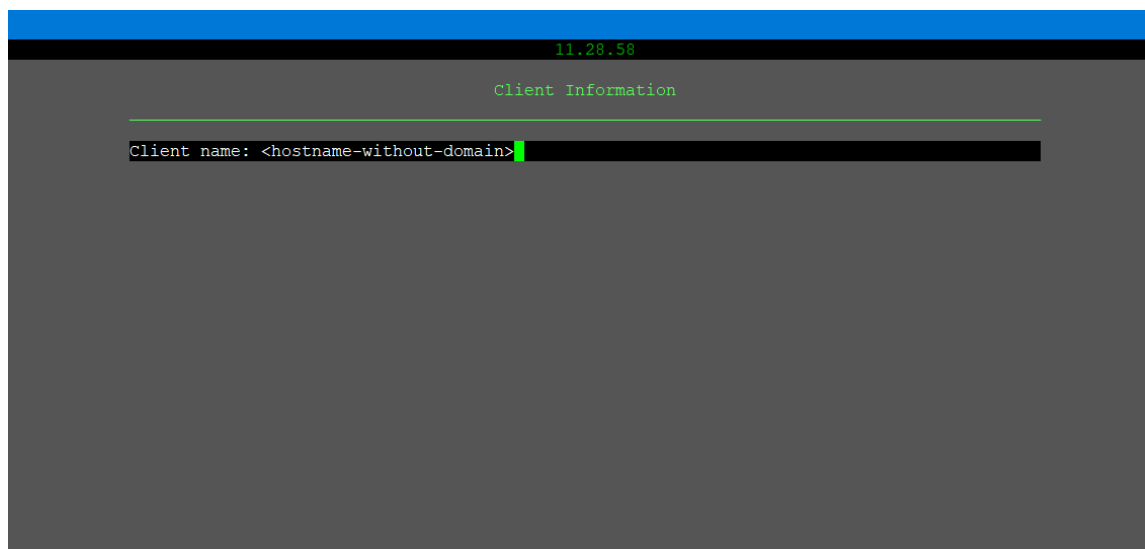
Steps installazione client Linux on Oracle_OCI

Se richiesto, scegliere la directory di installazione (è preferibile non modificare la directory di default).



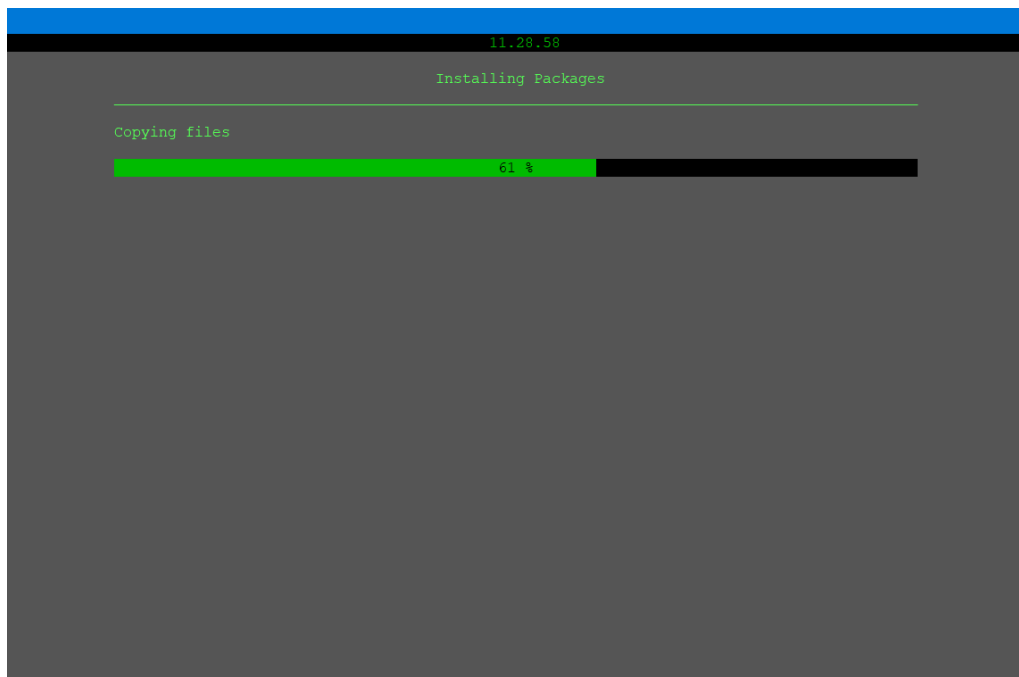
Steps installazione client Linux on Oracle_OCI

Digitare "Next" alle schermate successive relative ad hostname e clientname.



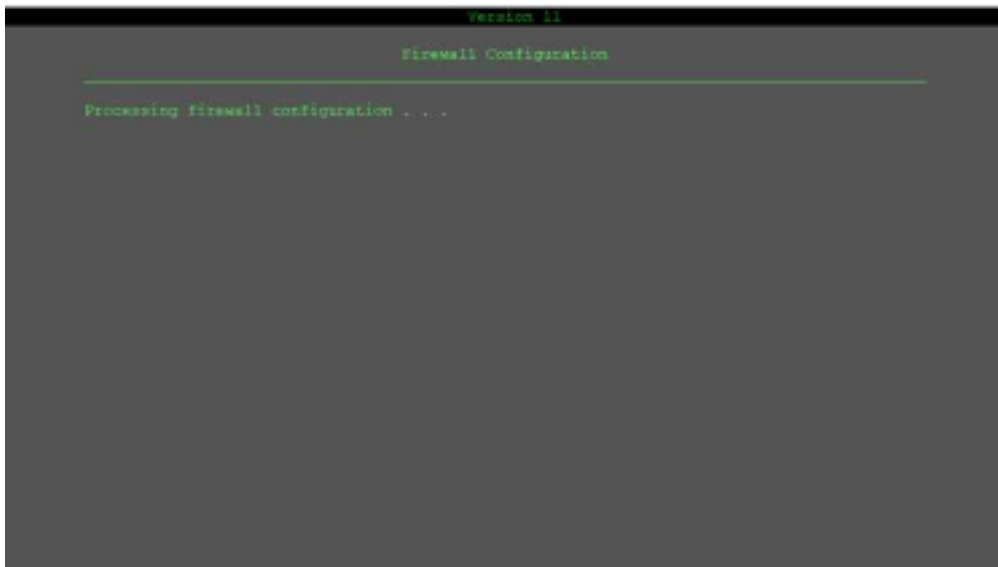
Steps installazione client Linux on Oracle_OCI

Quindi attendere il completamento della procedura di installazione.



Steps installazione client Linux on Oracle_OCI

Inserire il nome dell'access node (nome vm-xxxxxxx) PSN Managed ORACLE Cloud ricavabile dalla sezione Protect-Server del portale di backup.

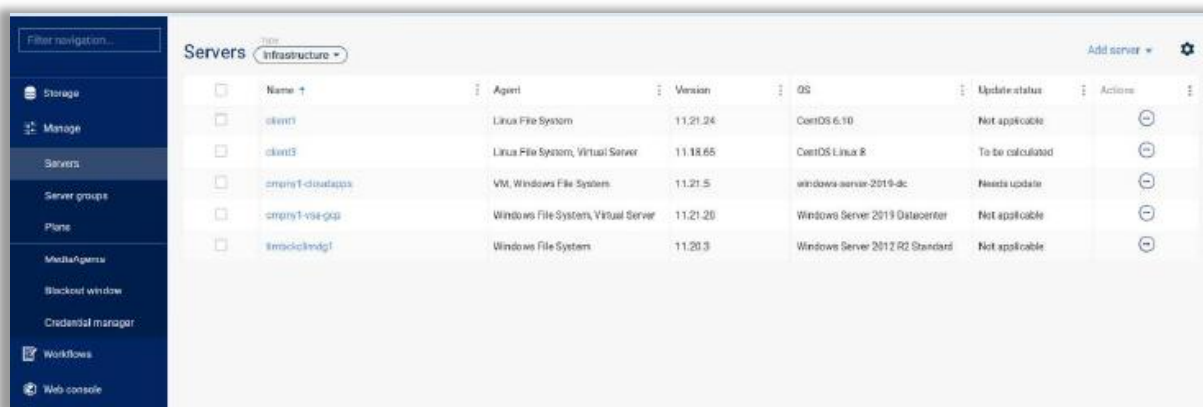


Steps installazione client Linux on Oracle_OCI

8.3 Aggiornamento del client con ulteriori agent

Per poter installare ulteriori agent di backup (ad esempio per i Database Oracle) è necessario che il server sia già registrato come client.

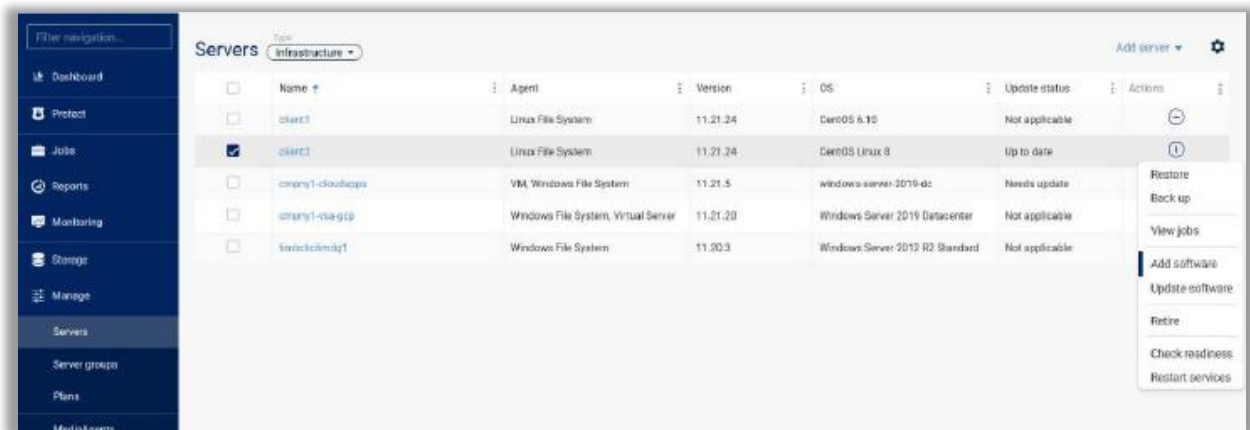
Accedere alla console di amministrazione del servizio e selezionare *Manage – Servers* dal menu di sinistra.



Name	Agent	Version	OS	Update status	Actions
client1	Linux File System	11.21.24	CentOS 6.10	Not applicable	⋮
client3	Linux File System, Virtual Server	11.18.65	CentOS Linux 8	To be calculated	⋮
empty1-cloudapp	VM, Windows File System	11.21.5	Windows Server 2019-DC	Needs update	⋮
empty1-vse-gp	Windows File System, Virtual Server	11.21.20	Windows Server 2019 Datacenter	Not applicable	⋮
ibackupmgr1	Windows File System	11.20.3	Windows Server 2012 R2 Standard	Not applicable	⋮

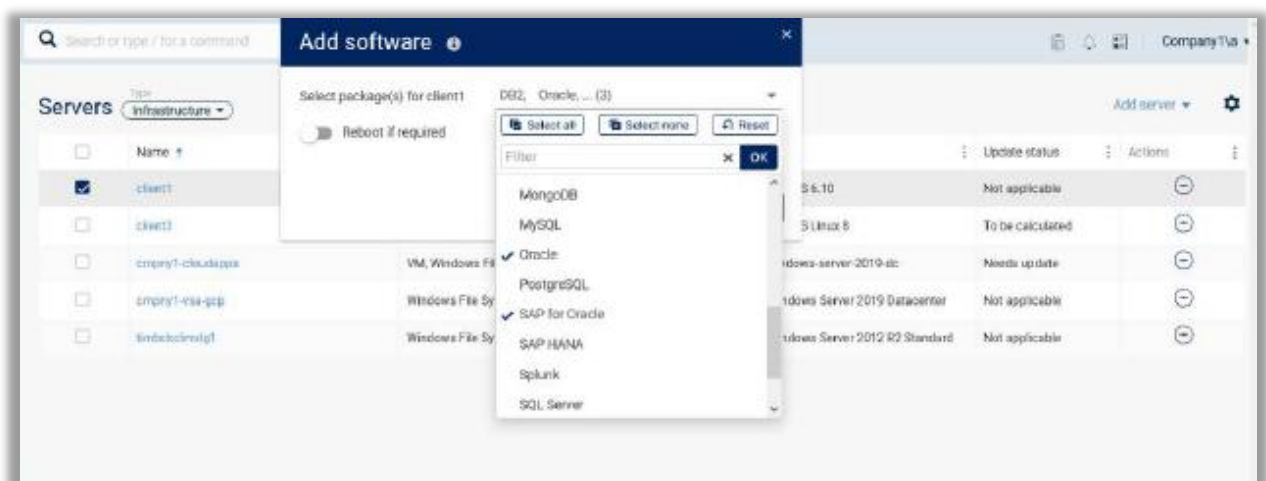
Figura 39 – Steps Installazione altri agent su Client on Oracle_OCI

Individuare il client che si vuole aggiornare e attraverso il menù a tendina della colonna actions in corrispondenza del nome client individuato selezionare *Add Software*



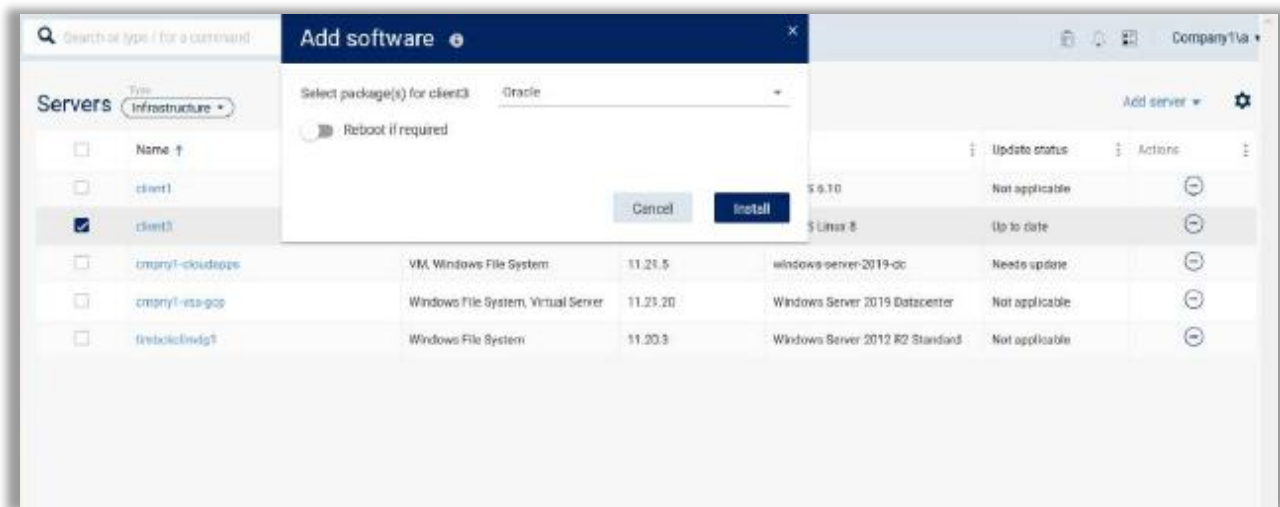
Steps Installazione altri agent su Client on Oracle_OCI

Selezionare gli agent software da installare (anche più di uno contemporaneamente) dal menu a tendina e premere il tasto OK



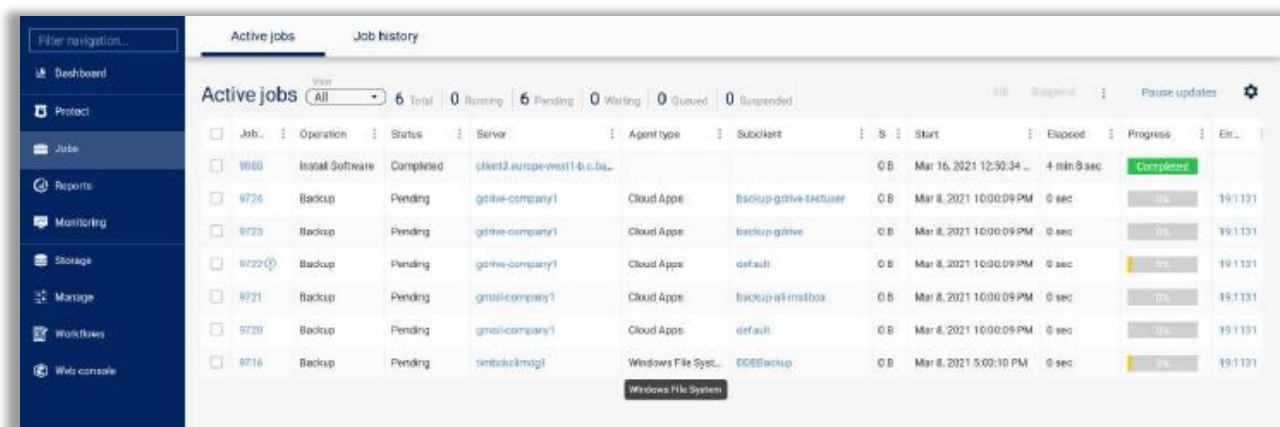
Steps Installazione altri agent su Client on Oracle_OCI

Quindi premere il tasto *Install*



Steps Installazione altri agent su Client on Oracle_OCI

Attendere la corretta esecuzione del job eseguito verificandone lo stato dalla sezione Jobs del menu a sinistra



Steps Installazione altri agent su Client on Oracle_OCI

8.4 Upgrade software del client già registrato

Individuare il client che si vuole aggiornare e attraverso il menù a tendina della colonna *Actions*, in corrispondenza del client individuato, selezionare *Update software*.

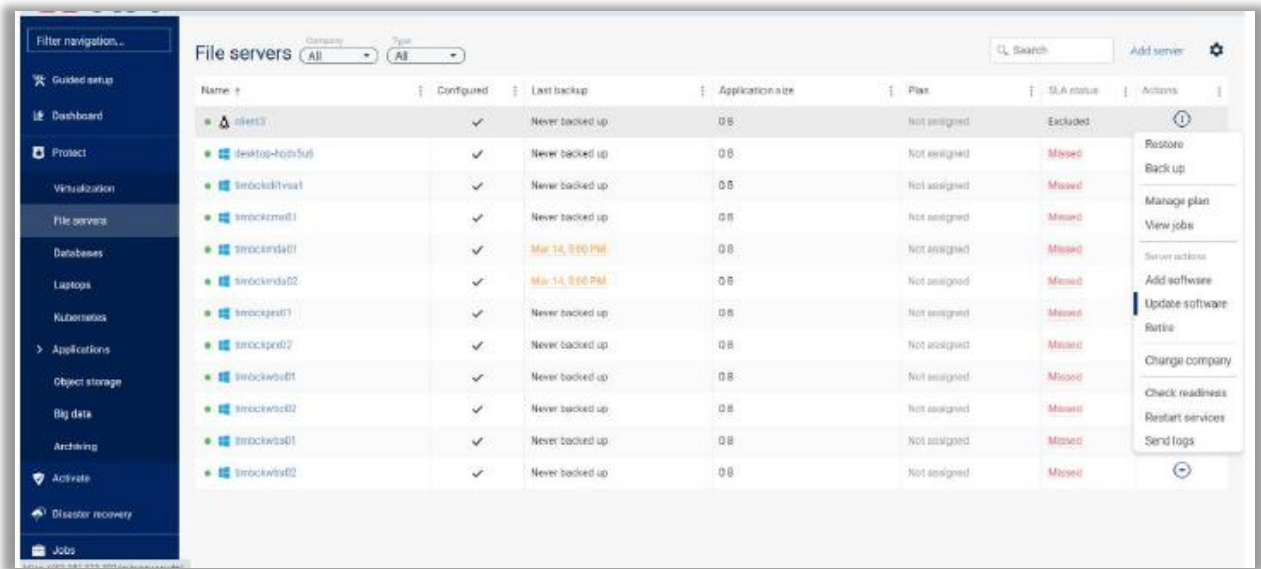
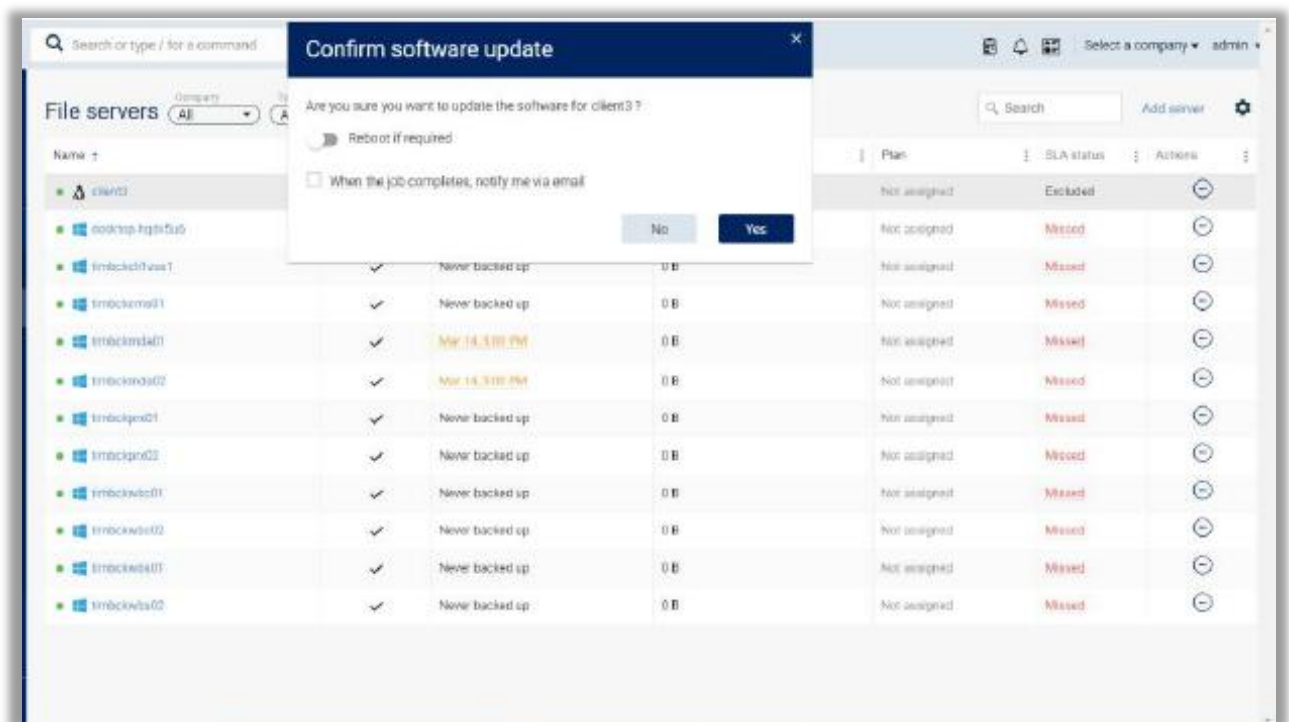


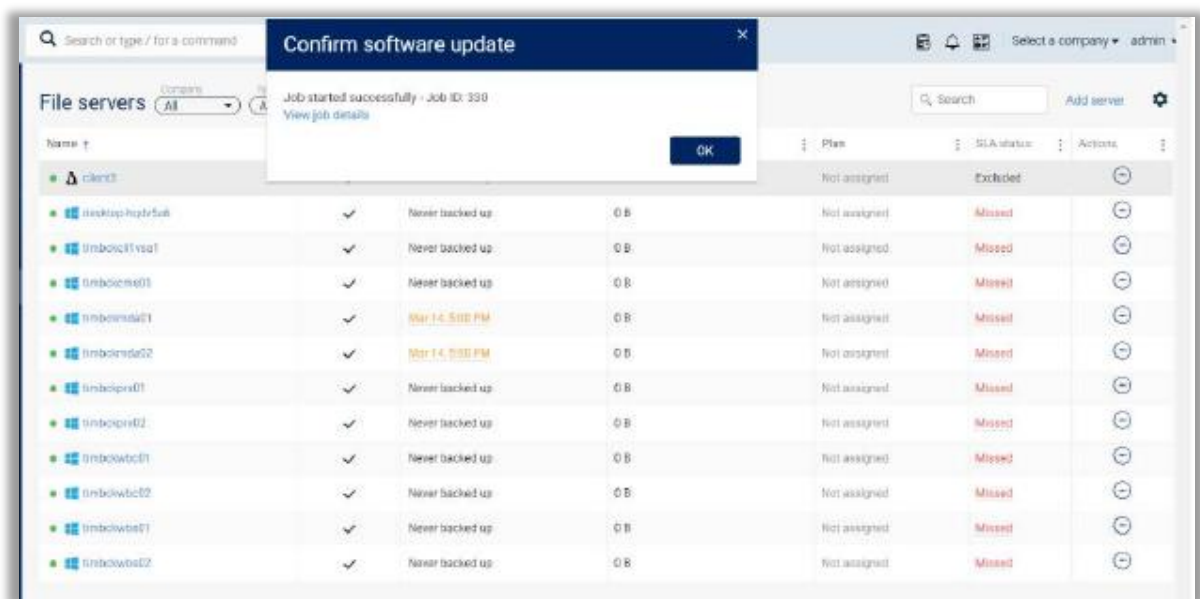
Figura 40 – Steps aggiornamento client on Oracle_OCI

Quindi scegliere se effettuare il reboot (l'aggiornamento non prevede un reboot del server target ma il solo eventuale riavvio automatico dei servizi Commvault) e ricevere notifica via e-mail al completamento del job di update e digitare il tasto Yes



Steps aggiornamento client on Oracle_OCI

Quindi digitare sul tasto OK relativo alla notifica della esecuzione del job. Attendere la corretta esecuzione del job eseguito.



Steps aggiornamento client on Oracle_OCI

9 Configurazione di un Hypervisor PSN MANAGED ORACLE CLOUD

Le istruzioni contenute in questo capitolo si riferiscono alle operazioni relative alla configurazione del client Hypervisor per un servizio PSN MANAGED ORACLE Cloud (ORACLE OCI) preliminare alle attività di schedulazione, backup e restore dei dati in ambito PSN MANAGED ORACLE OCI.

Dalla sezione Protect-Virtualization-Hypervisor selezionare in alto a destra Add Hypervisor:

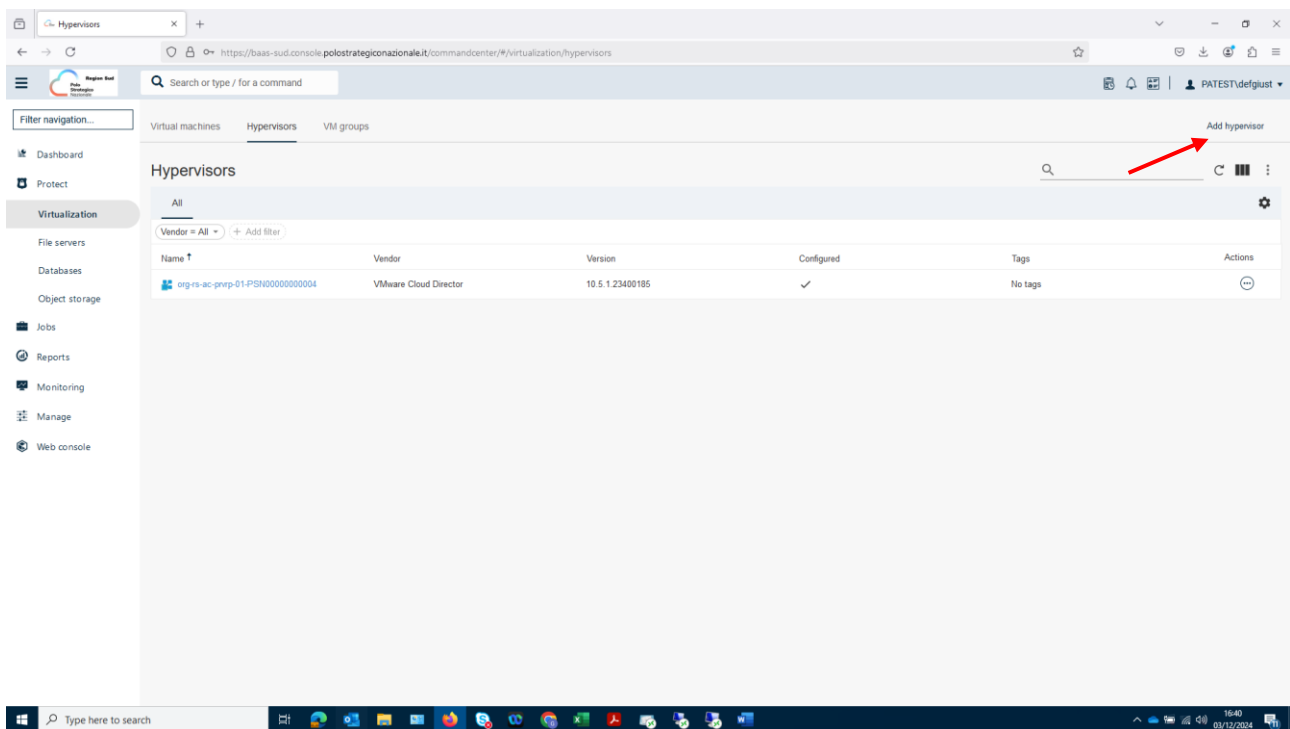
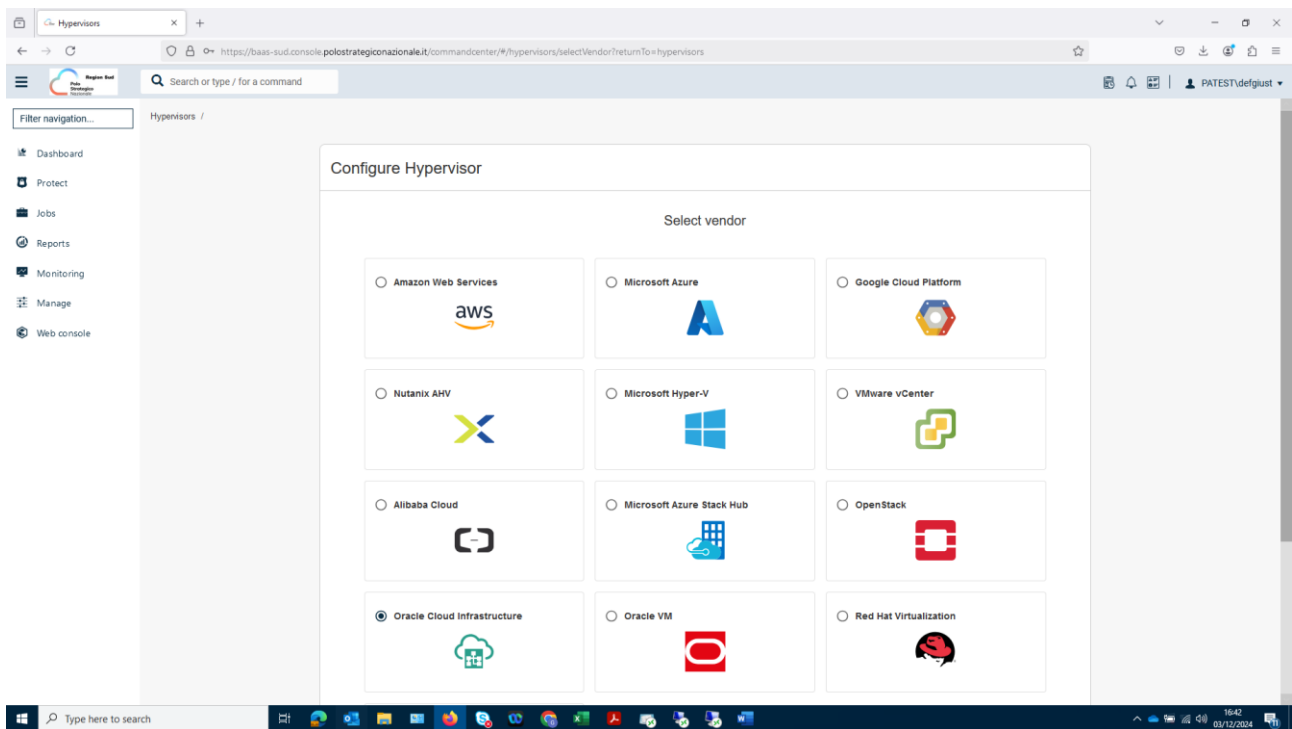


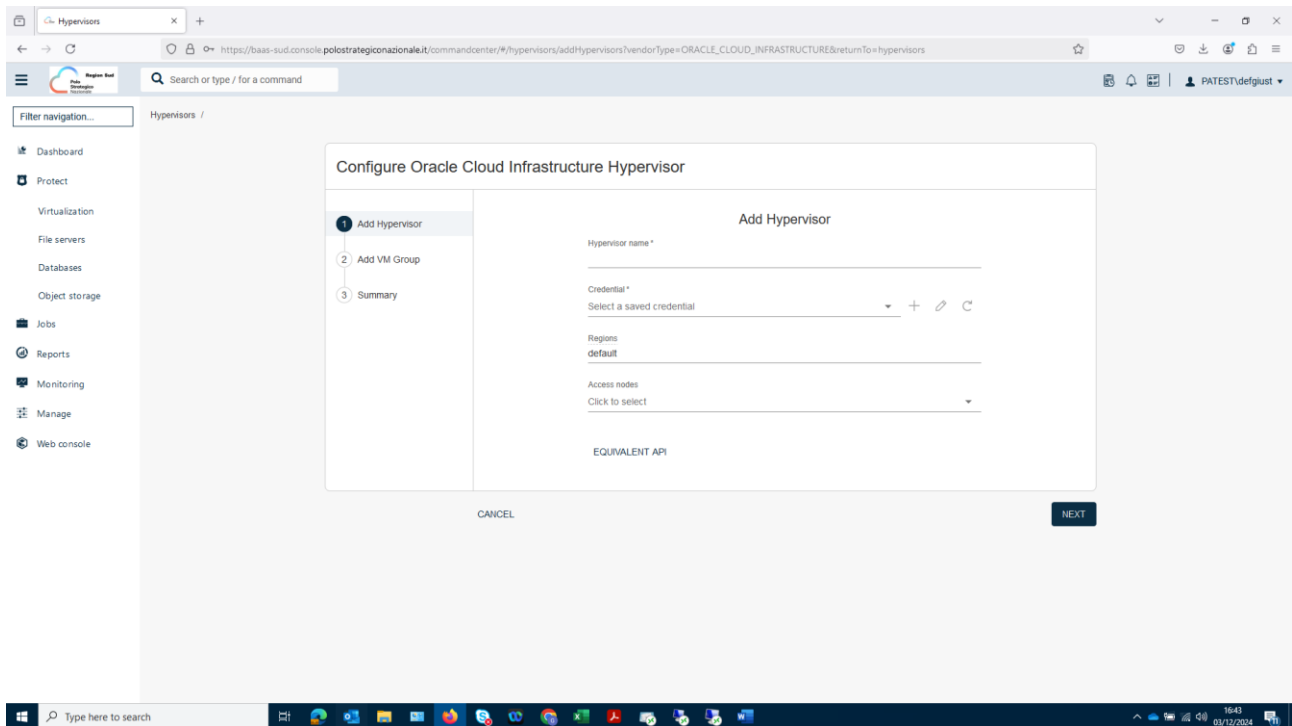
Figura 41 – Configurazione Hypervisor on Oracle_CLOUD

Selezionare quindi l'icona Oracle Cloud Infrastructure e premere il tasto next in basso a sinistra:



Configurazione Hypervisor on Oracle_CLOUD

Nella successiva schermata inserire le seguenti informazioni:



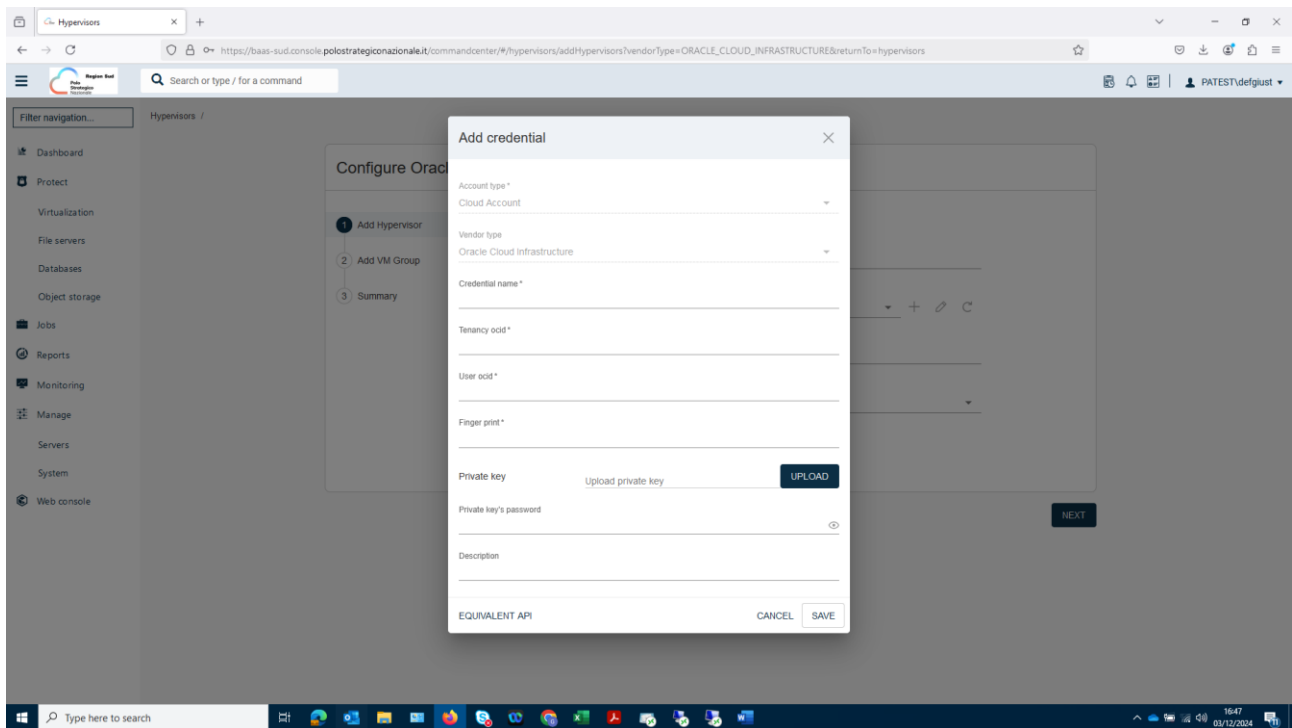
Configurazione Hypervisor on Oracle_CLOUD

Hypervisor Name: <nome con cui si vorrà identificare il client Oracle OCI in configurazione>

Regions: indicare il valore eu-dcc-rome-1

Access Nodes: Selezionare il nome dell'access node di riferimento (ad es. VM-xxxxx).

Credential: selezionare il tasto + e configurare le credenziali per l'accesso al tenant su PSN MANAGED ORACLE Cloud inserendo le seguenti informazioni:



Credential name: <nome con cui si vuole identificare le nuovi credenziali da creare>

Tenancy OcId: indicare il Tenancy OcId ricavabile dalla piattaforma PSN Managed Oracle (OCI)

User OcId: indicare l'User OcId ricavabile dalla piattaforma PSN Managed Oracle (OCI)

Finger Print: indicare il Finger print ricavabile dalla piattaforma PSN Managed Oracle (OCI)

Private Key: Effettuare l'upload della private Key scaricabile dalla piattaforma PSN Managed Oracle (OCI)

Description: Inserire una eventuale descrizione

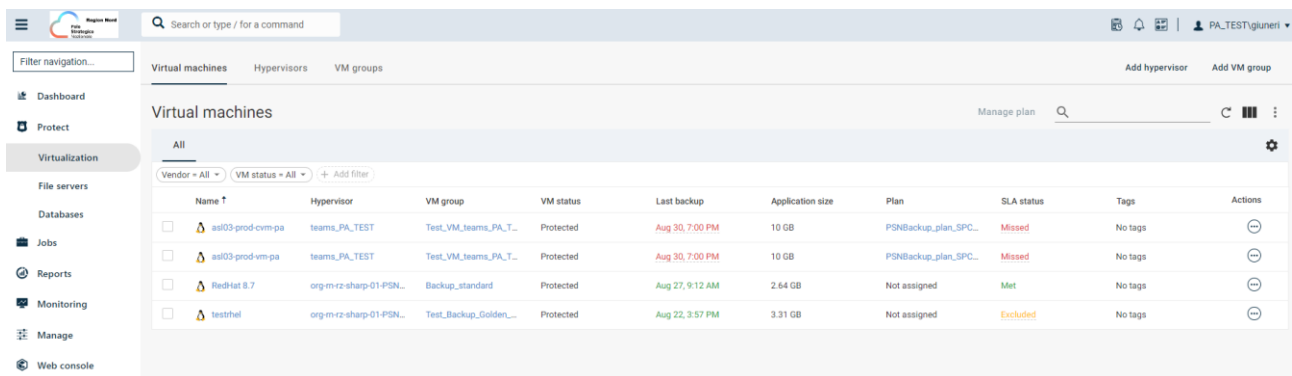
Premere il tasto Save

Quindi sulla schermata di Add Hypervisor selezionare Next e a seguire configurare i VM Groups (vedi capitolo Aggiunta e configurazione VM group).

10 Aggiunta e configurazione VM group

Una volta fatto accesso alla console di backup PSN (<https://baas-nord.console.polostrategiconazionale.it>), dal menù a sinistra, è possibile accedere alla sezione *Protect*. Si apriranno tre sottosezioni: *Virtualization*, *File servers* e *Databases*.

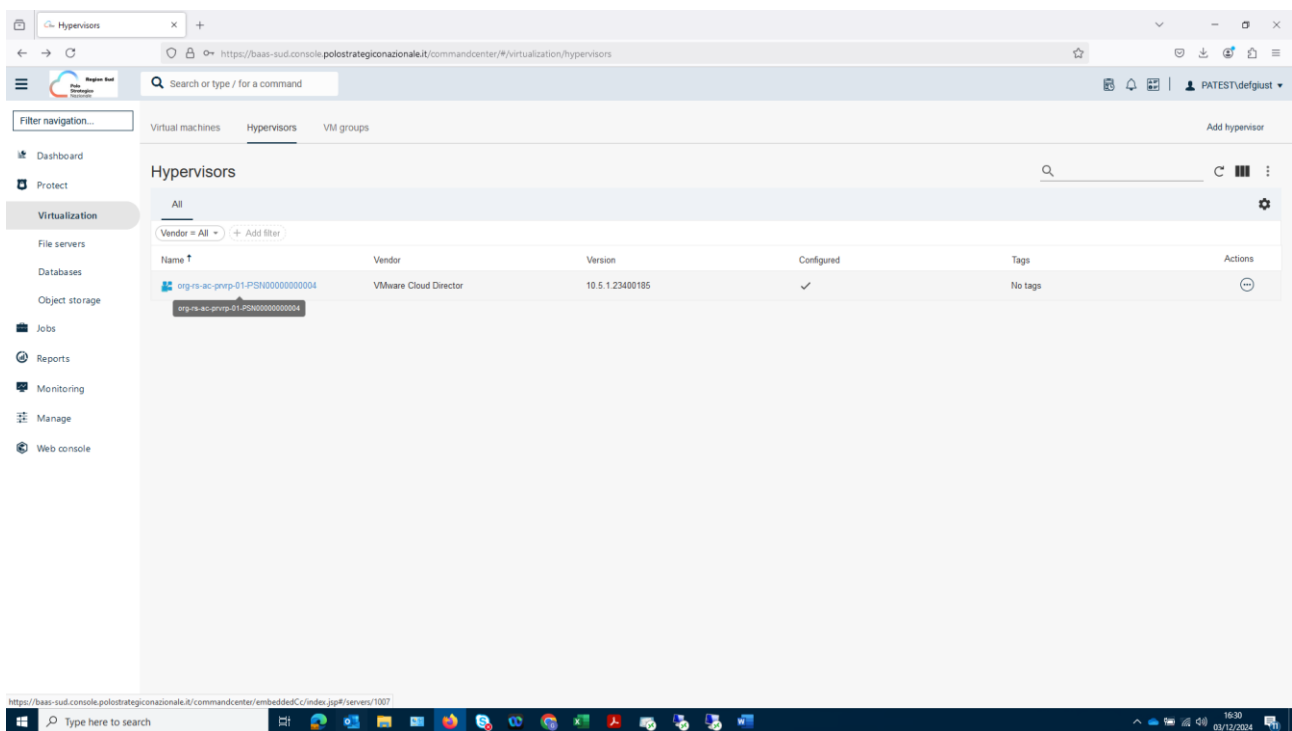
Cliccando su *Virtualization* compariranno le aree Virtual machines, Hypervisors e VM groups, come da immagine di seguito.



Name	Hypervisor	VM group	VM status	Last backup	Application size	Plan	SLA status	Tags	Actions
asi03-prod-cvm-pa	teams_PA_TEST	Test_VM_teams_PA_T...	Protected	Aug 30, 7:00 PM	10 GB	PSNBackup_plan_SPC...	Missed	No tags	⋮
asi03-prod-vm-pa	teams_PA_TEST	Test_VM_teams_PA_T...	Protected	Aug 30, 7:00 PM	10 GB	PSNBackup_plan_SPC...	Missed	No tags	⋮
RedHat 8.7	org-m-rz-sharp-01-PSN...	Backup_standard	Protected	Aug 27, 9:12 AM	2.64 GB	Not assigned	Met	No tags	⋮
testhel	org-m-rz-sharp-01-PSN...	Test_Backup_Golden...	Protected	Aug 22, 3:57 PM	3.31 GB	Not assigned	Excluded	No tags	⋮

Figura 42 – Configurazione VM GROUP

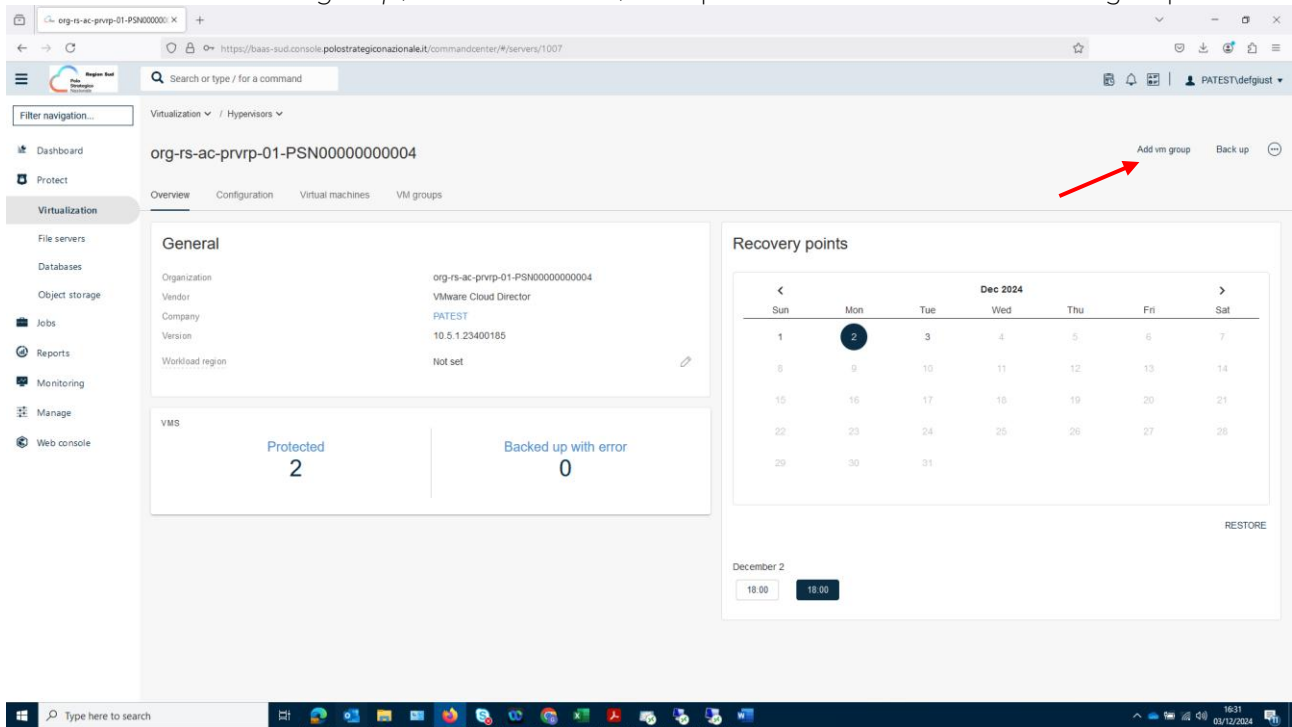
Selezionare l'Hypervisor su cui si vuole configurare un nuovo VM group:



Name	Vendor	Version	Configured	Tags	Actions
org-rs-ac-pnvp-01-PSN000000000004	VMware Cloud Director	10.5.1.23400185	✓	No tags	⋮

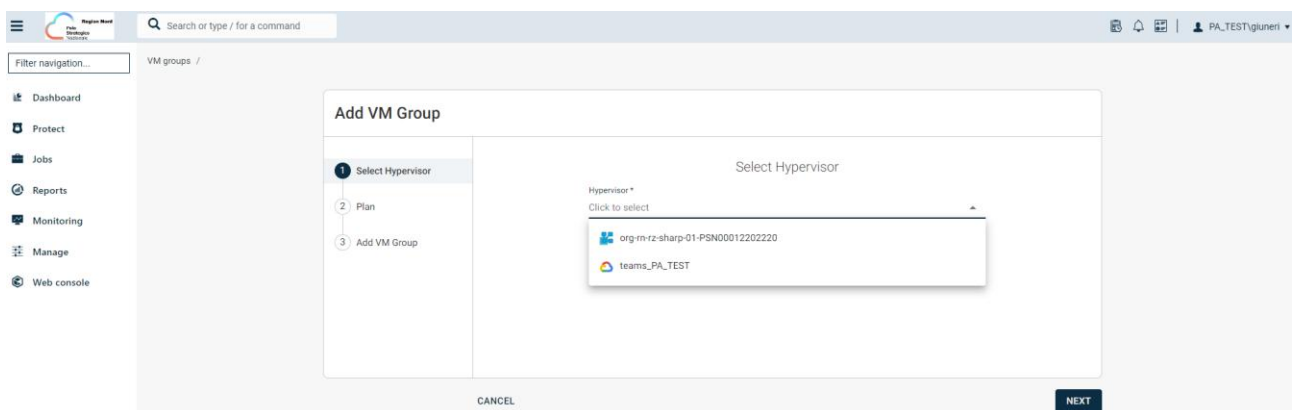
Configurazione VM GROUP

Selezionando *Add VM group*, in alto a destra, sarà possibile creare un nuovo VM group.



Configurazione VM GROUP

Come primo step per la creazione del VM Group è necessario selezionare l'Hypervisor, se non già indicato, e cliccare su *NEXT*, come da immagine di seguito.



Configurazione VM GROUP

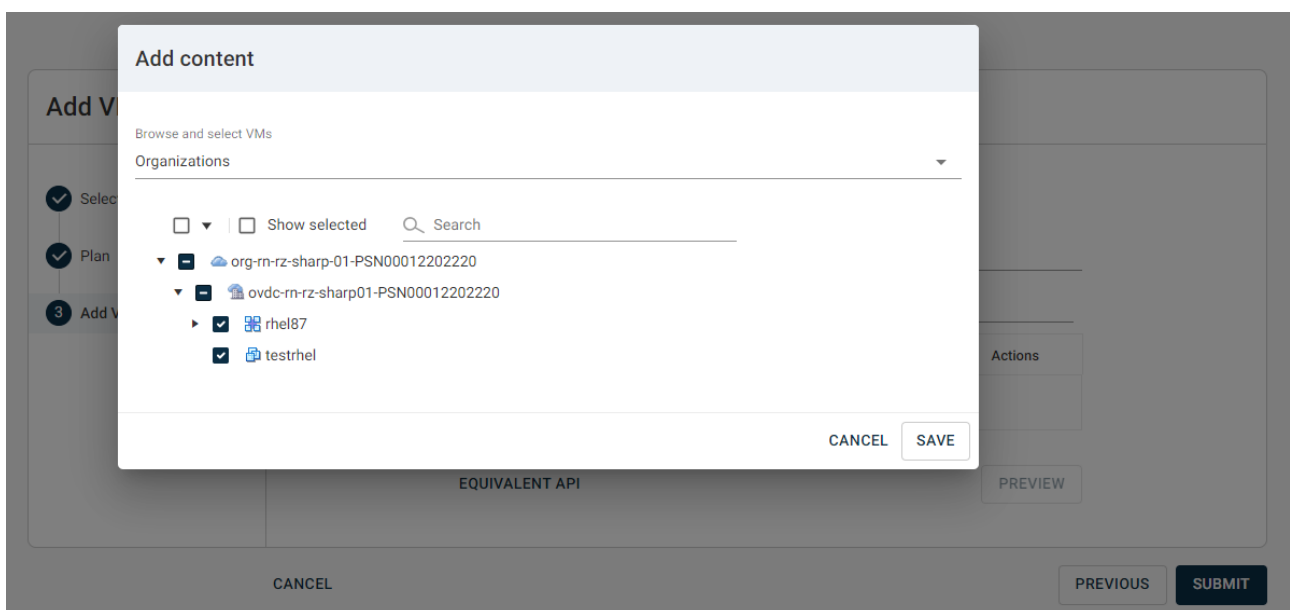
A questo punto va selezionato il Plan che si vuole associare al VM group su cui verrà effettuato il backup.

Si può scegliere tra quelli già presenti scorrendo il menù, come da immagine di seguito. Una volta scelto il plan, cliccarci sopra e poi cliccare su *NEXT*.

Selezionare le VM delle quali si vuole effettuare il backup e cliccare su **SAVE**.

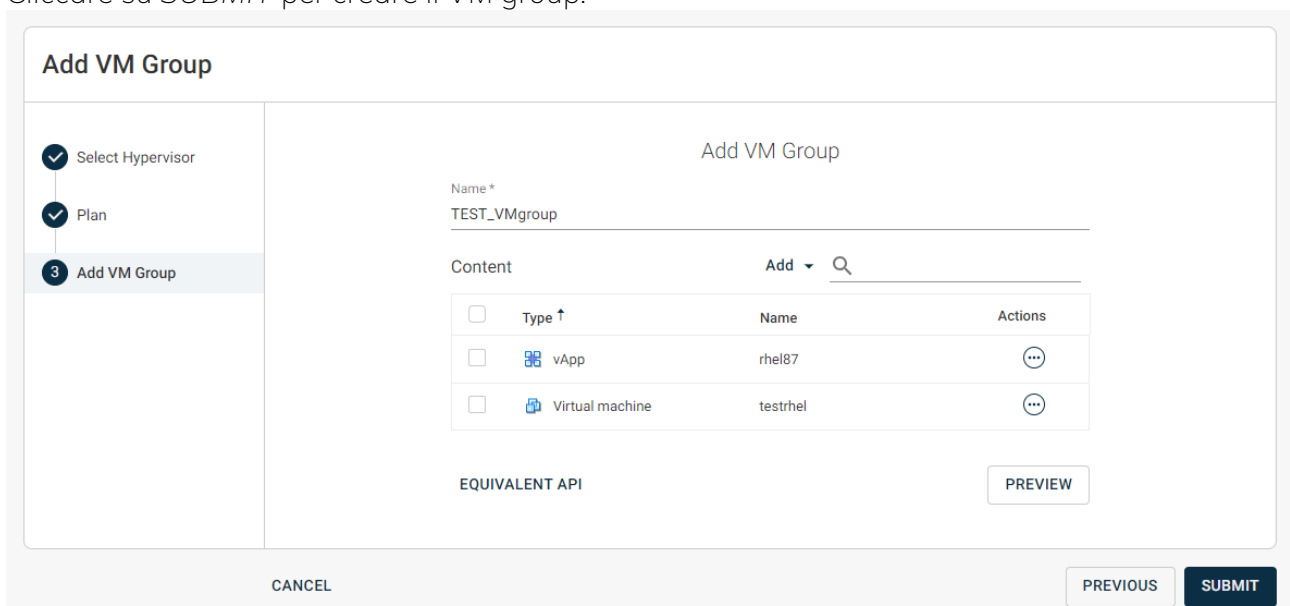
In alternativa è possibile utilizzare delle Rule per selezionare le VM appartenenti al gruppo in automatico ad esempio utilizzando Virtual machine name/pattern come criterio di match che consente l'uso di wildcards (per esempio Test* per identificare le VMs il cui VM name inizia con "Test"), è possibile inoltre definire un filtro (anche tramite rule) che rispetto al criterio di selezione escluda alcune VM.

Dopo aver configurato il Content di un VMGroup si consiglia sempre di utilizzare il tasto **PREVIEW** per controllare che il contenuto configurato corrisponda ai criteri.



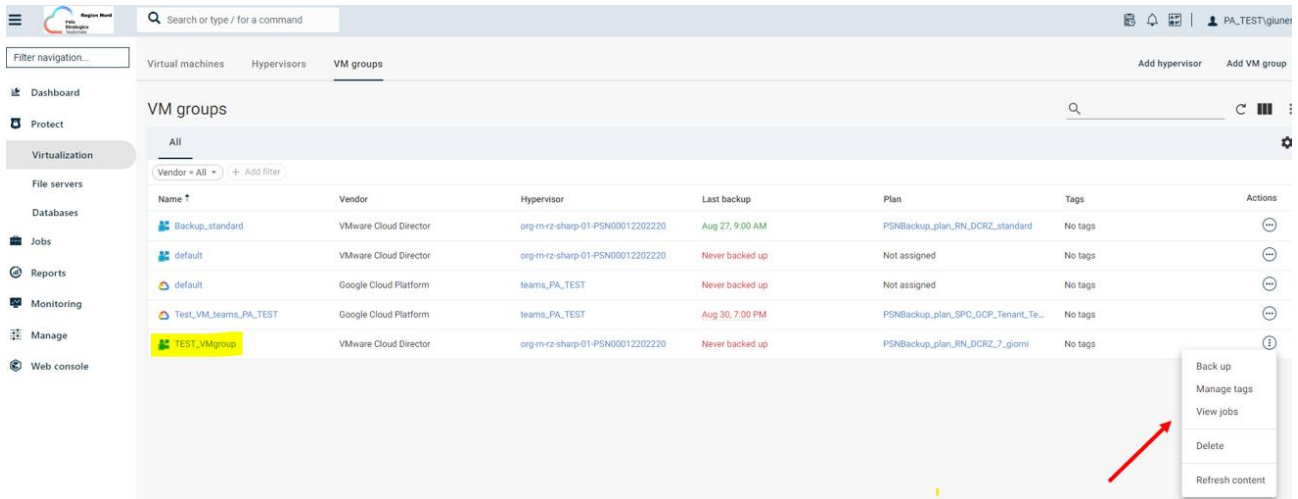
Configurazione VM GROUP

Cliccare su **SUBMIT** per creare il VM group.



Configurazione VM GROUP

Una volta creato il VM group è possibile effettuare delle Actions su di esso. Dal menu principale della console, passando per *Protect* → *Virtualization* → *VM groups*, in corrispondenza del VM group creato è possibile cliccare sui tre pallini a destra e visualizzare le actions.



The screenshot shows the PSN Backup console interface. The left sidebar contains navigation links: Dashboard, Protect, Virtualization (selected), File servers, Databases, Jobs, Reports, Monitoring, Manage, and Web console. The main area displays the 'VM groups' table. The table has columns: Name, Vendor, Hypervisor, Last backup, Plan, Tags, and Actions. The 'TEST_VMgroup' entry is highlighted in yellow. A red arrow points to the actions menu (three dots) for this entry, which contains the following options: Back up, Manage tags, View jobs, Delete, and Refresh content.

Name	Vendor	Hypervisor	Last backup	Plan	Tags	Actions
Backup_standard	VMware Cloud Director	org-mvz-sharp-01-PSN00012202220	Aug 27, 9:00 AM	PSNBackup_plan_RN_DCRZ_standard	No tags	⋮
default	VMware Cloud Director	org-mvz-sharp-01-PSN00012202220	Never backed up	Not assigned	No tags	⋮
default	Google Cloud Platform	teams_PA_TEST	Never backed up	Not assigned	No tags	⋮
Test_VM_teams_PA_TEST	Google Cloud Platform	teams_PA_TEST	Aug 30, 7:00 PM	PSNBackup_plan_SPC_GCP_Tenant_Te...	No tags	⋮
TEST_VMgroup	VMware Cloud Director	org-mvz-sharp-01-PSN00012202220	Never backed up	PSNBackup_plan_RN_DCRZ_7_giorni	No tags	⋮

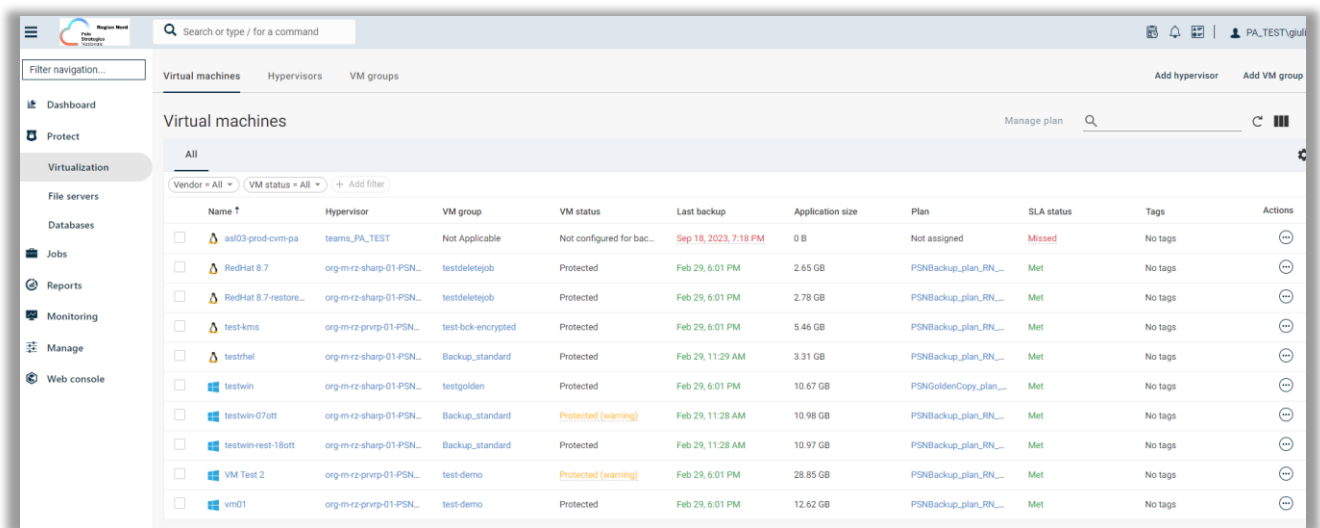
Configurazione VM GROUP

10.1 Cancellazione VM group e sospensione job di backup relativo al VM group

Nel seguente paragrafo verrà dettagliata la modalità di cancellazione dei VM group e la sospensione dei job di backup relativi ad un VM group.

Cancellazione VM group

Dal menu principale, all'interno della sezione Protect, cliccare su *Virtualization*.

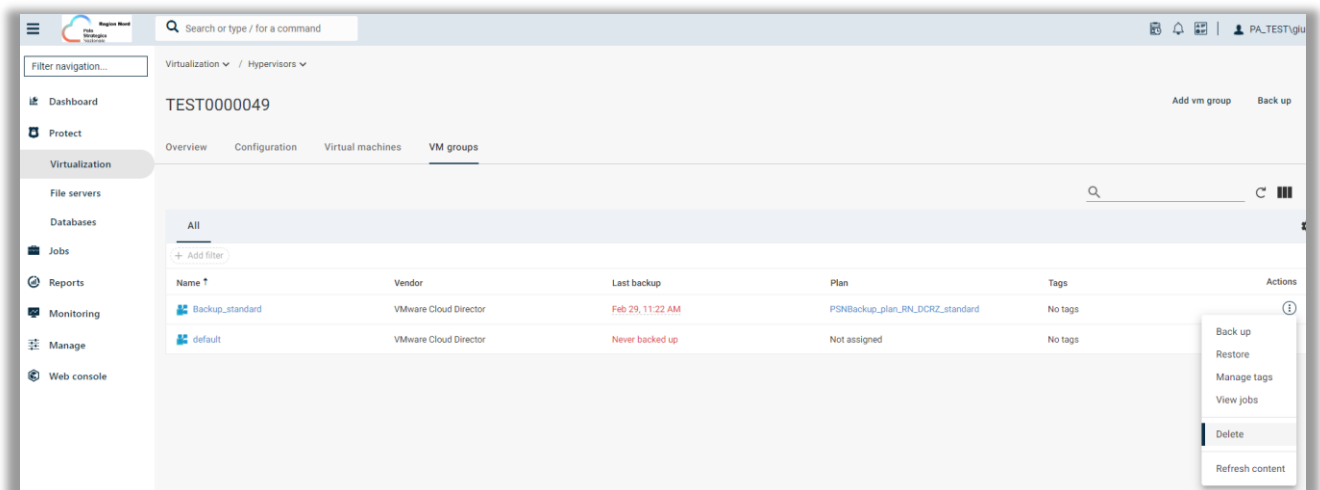


Name	Hypervisor	VM group	VM status	Last backup	Application size	Plan	SLA status	Tags	Actions
as03-prod-cvm-pa	teams_PA_TEST	Not Applicable	Not configured for bac...	Sep 18, 2023, 7:18 PM	0 B	Not assigned	Missed	No tags	⋮
RedHat 8.7	org-m-r2-sharp-01-PSN...	testdeletejob	Protected	Feb 29, 6:01 PM	2.65 GB	PSNBackup_plan_RN...	Met	No tags	⋮
RedHat 8.7-restore...	org-m-r2-sharp-01-PSN...	testdeletejob	Protected	Feb 29, 6:01 PM	2.78 GB	PSNBackup_plan_RN...	Met	No tags	⋮
test-kms	org-m-r2-prvrg-01-PSN...	test-bck-encrypted	Protected	Feb 29, 6:01 PM	5.46 GB	PSNBackup_plan_RN...	Met	No tags	⋮
testrhel	org-m-r2-sharp-01-PSN...	Backup_standard	Protected	Feb 29, 11:29 AM	3.31 GB	PSNBackup_plan_RN...	Met	No tags	⋮
testwin	org-m-r2-sharp-01-PSN...	testgolden	Protected	Feb 29, 6:01 PM	10.67 GB	PSNGoldenCopy_plan...	Met	No tags	⋮
testwin-07ott	org-m-r2-sharp-01-PSN...	Backup_standard	Protected (warning)	Feb 29, 11:28 AM	10.98 GB	PSNBackup_plan_RN...	Met	No tags	⋮
testwin-rest-18ott	org-m-r2-sharp-01-PSN...	Backup_standard	Protected	Feb 29, 11:28 AM	10.97 GB	PSNBackup_plan_RN...	Met	No tags	⋮
VM Test 2	org-m-r2-prvrg-01-PSN...	test-demo	Protected (warning)	Feb 29, 6:01 PM	28.85 GB	PSNBackup_plan_RN...	Met	No tags	⋮
vm01	org-m-r2-prvrg-01-PSN...	test-demo	Protected	Feb 29, 6:01 PM	12.62 GB	PSNBackup_plan_RN...	Met	No tags	⋮

Figura 43 – Cancellazione VM GROUP

Spostarsi nella sezione *Hypervisors* → *VM group*

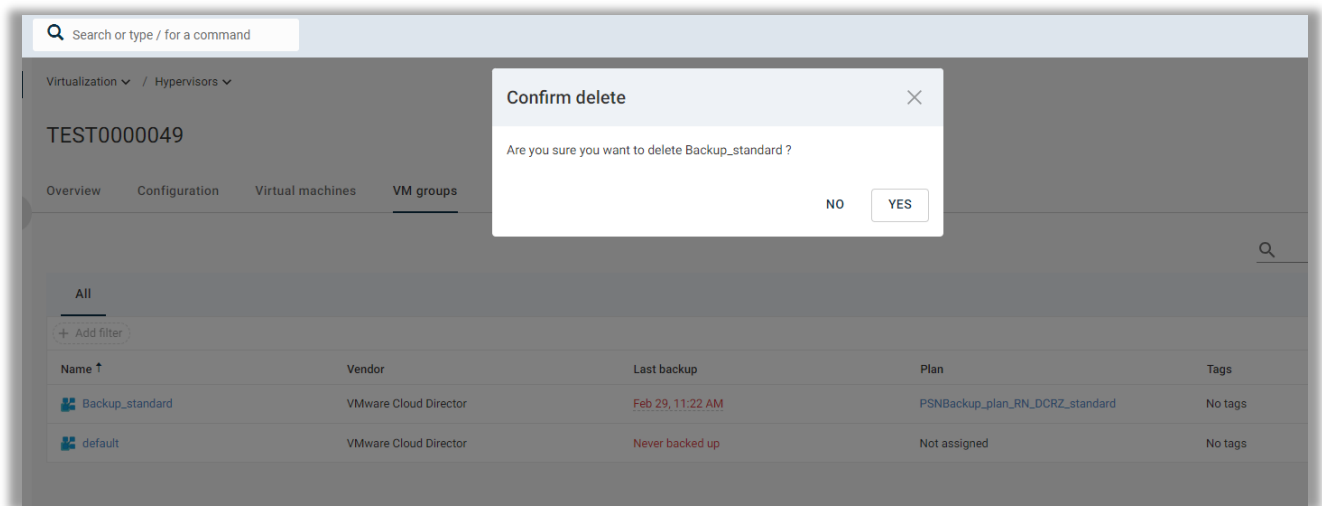
Scegliere il VM group da cancellare. Spostarsi verso i tre pallini in fondo sotto la colonna *Actions* e cliccare su *Delete*.



Name	Vendor	Last backup	Plan	Tags	Actions
Backup_standard	VMware Cloud Director	Feb 29, 11:22 AM	PSNBackup_plan_RN_DCRZ_standard	No tags	⋮
default	VMware Cloud Director	Never backed up	Not assigned	No tags	⋮

Cancellazione VM GROUP

Cliccare su YES nella finestra che comparirà.



Cancellazione VM GROUP

A questo punto il VM group è stato correttamente eliminato.
Il VM group viene eliminato anche se ci sono in corso job di backup attivi.

Sospensione job di backup relativo ad un VM group

È possibile anche sospendere l'esecuzione di un job di backup relativo ad un VM group. È sufficiente cliccare sul VM group, spostarsi sotto la sezione *Configuration* e cliccare sul pallino blu sotto *Activity control*.

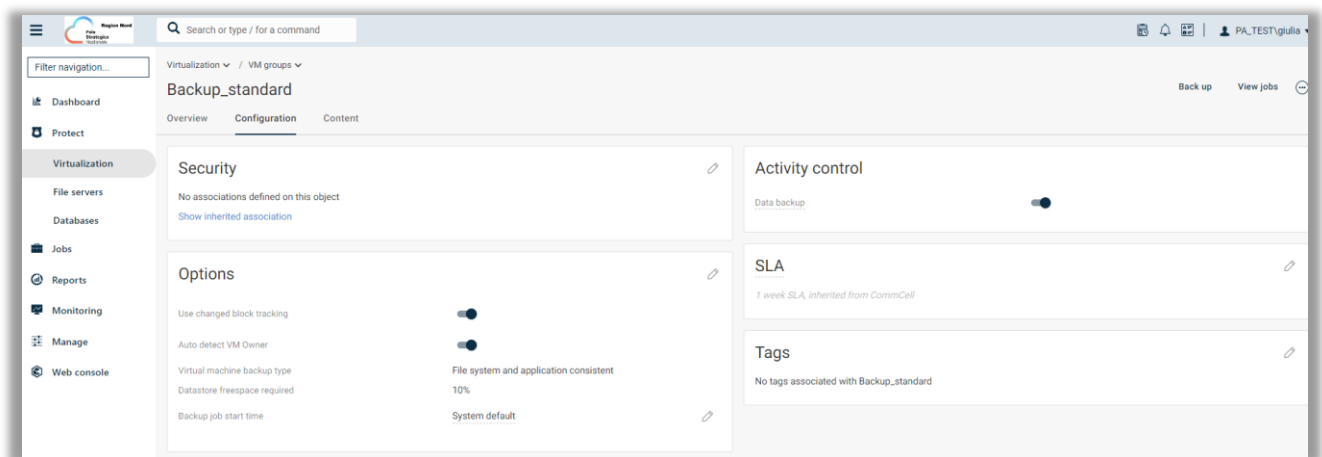
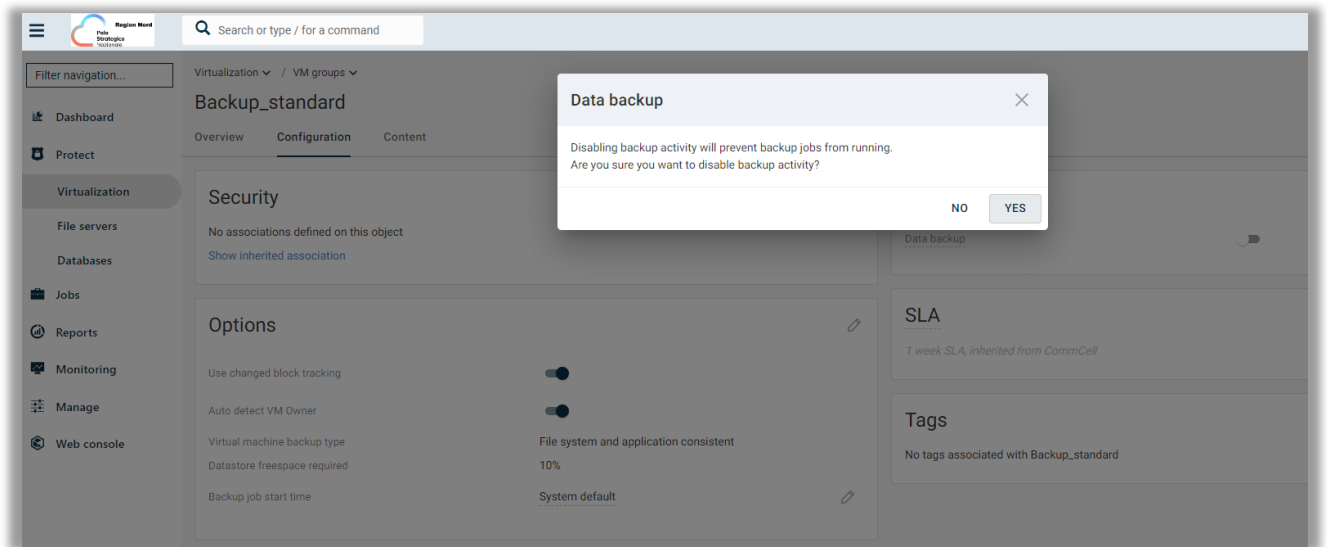


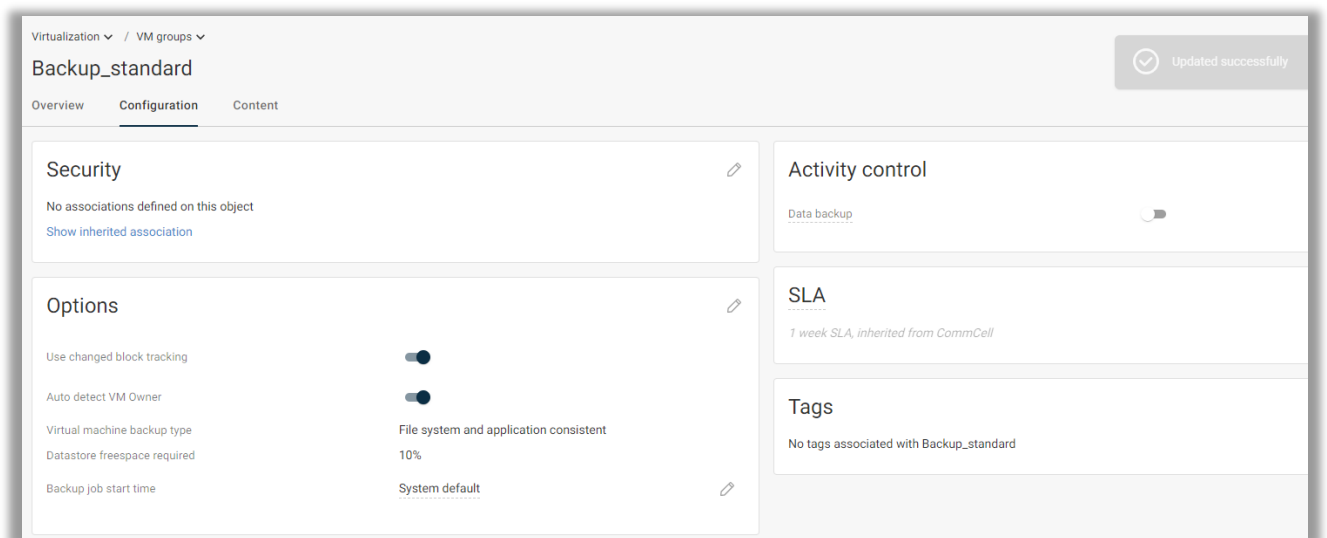
Figura 44 – Sospensione backup di un VM GROUP

Cliccare su YES nella finestra che si aprirà.



Sospensione backup di un VM GROUP

A questo punto l'esecuzione del job di backup relativo al VM group sarà correttamente disattivata. Il pallino blu diventerà grigio.



Sospensione backup di un VM GROUP

11 Operazioni di backup

Le istruzioni contenute in questa sezione sono relative alle operazioni di data protection. Nei successivi capitoli saranno descritte le attività da eseguire per effettuare il backup dei relativi contesti.

11.1 Backup di tipo file system

Accedere alla console di amministrazione del servizio e selezionare *Protect – File servers* dal menu di sinistra. Selezionare il server oggetto di backup tra quelli su cui precedentemente si è installato il client (vedi capitolo 5 *Configurazione dei client*) e scegliere la sezione *Overview* (già preimpostata).

Quindi selezionare *Add Subclient* in alto a destra nella sezione *Subclients* presente in fondo alla schermata.

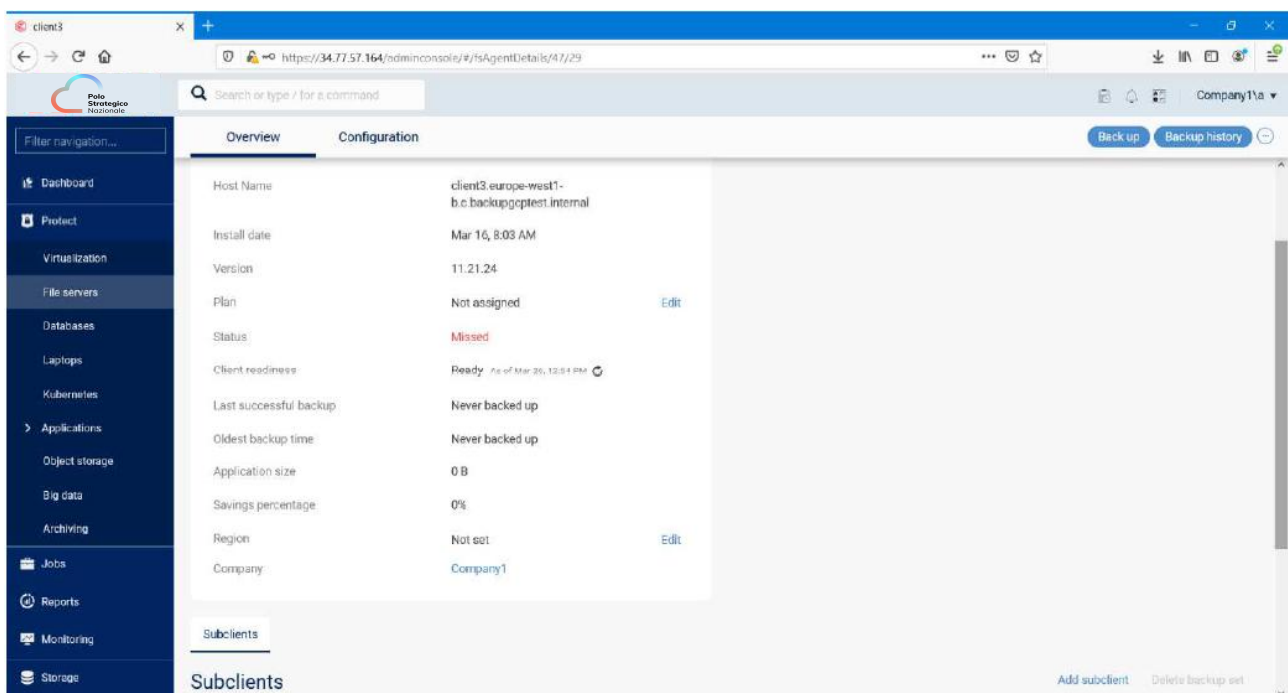


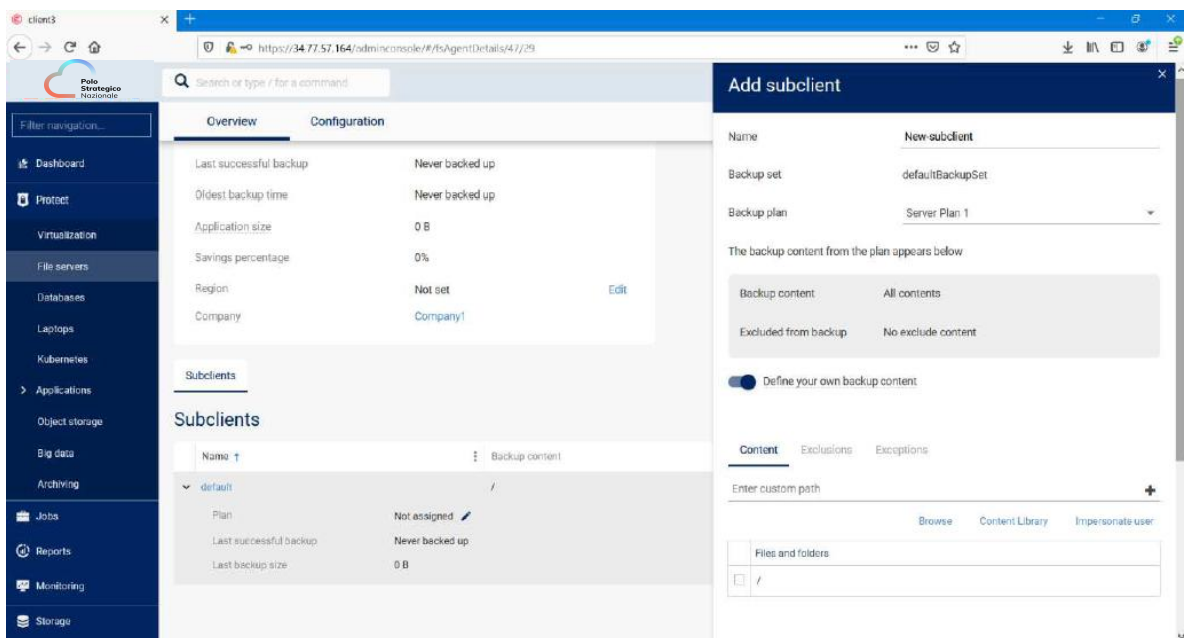
Figura 45 – Configurazione FS backup

Un subclient è una porzione di un client, e può contenere il puntamento a tutti i dati presenti sul sistema oppure a una porzione selezionata di quei dati. Ci sono due principali tipi di subclient: default e user-defined. Quando viene installato l'agent software, a seconda dell'agent selezionato, il programma di installazione crea automaticamente un subclient di default per quell'Agent, che comprenderà, nel caso del File System, tutte le risorse disco fisiche presenti (CDROM e drive di rete mappati vengono invece esclusi direttamente). È consigliabile creare ulteriori subclient personalizzati, detti anche user-defined, dove ognuno di questi contiene una porzione univoca dei dati del client (non è raccomandata la modifica di un Subclient di default).

Procedere a definire un *Name* per il subclient che si sta definendo e a selezionare uno dei *Plan* tra quelli disponibili (la lista dei *Plan* conterrà l'elenco dei *Plan* standard del servizio e l'elenco dei *Plan* proprietari precedentemente già definiti – vedi capitolo *0 Plans*).

Dopo aver scelto il *Plan* è possibile definire il contenuto di backup (file e/o cartelle) selezionando il tasto *Define your own backup content* oppure lasciare il backup content definito nel *Plan* selezionato.

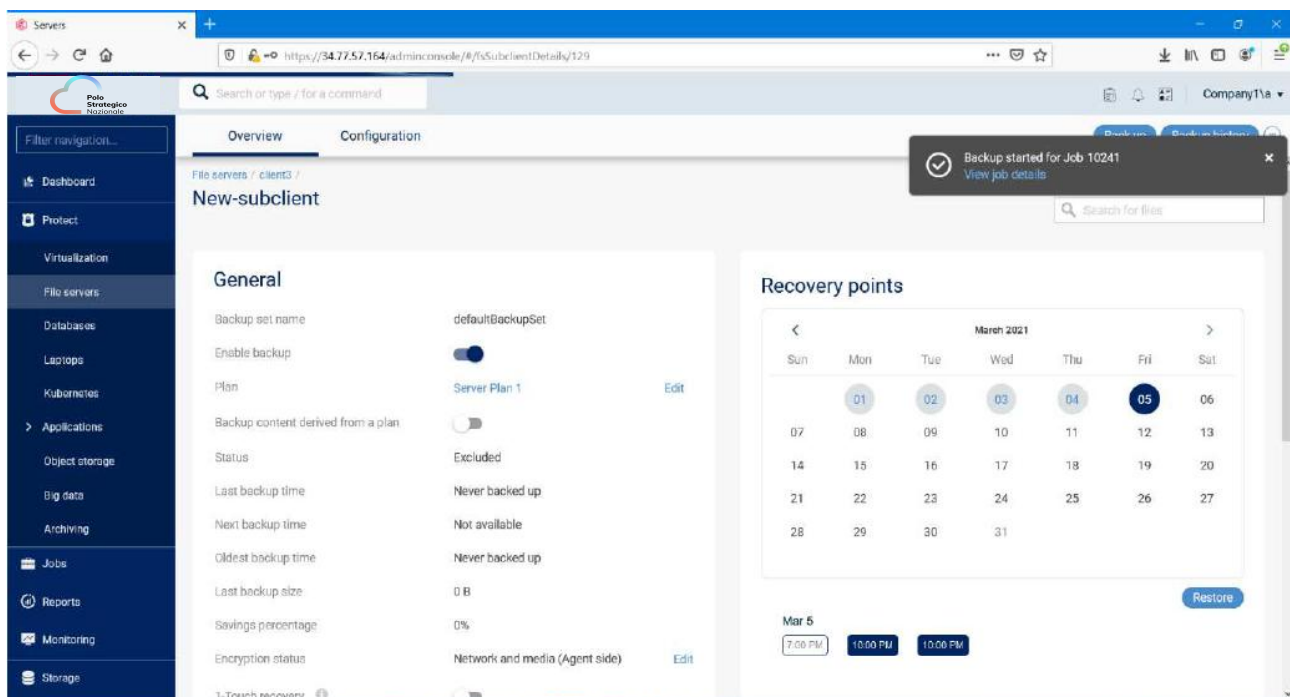
Se si definisce il proprio backup content allora sarà necessario definire il contenuto, le esclusioni e le eccezioni attraverso le sezioni *Content – Exclusions – Exceptions*. Quindi, opzionalmente si possono selezionare comandi di pre e post backup precedentemente definiti sul server della sezione *Backup process settings* e premere il tasto OK pre salvare il subclient.



Configurazione FS backup

A questo punto è possibile schedare manualmente un backup selezionando il subclient appena definito o un altro definito precedentemente o attendere la schedulazione impostata sul plan associato al subclient definito.

Se si vuole eseguire un backup manualmente allora si potrà digitare il tasto *Backup* in alto a destra e scegliere il tipo di backup da eseguire (*Full*, *Incremental*, *Synthetic Full*) nella sezione *Backup level* ed eventualmente impostare il flag per ricevere una mail al completamento del backup. Quindi dopo aver premuto il tasto *OK* si potrà controllare l'esito del relativo job di backup eseguito.



Configurazione FS backup

11.2 Backup & Restore Virtual Machine

Accedere alla console di amministrazione del servizio e selezionare *Protect – Virtualization* dal menu di sinistra e selezionare *Hypervisor*.

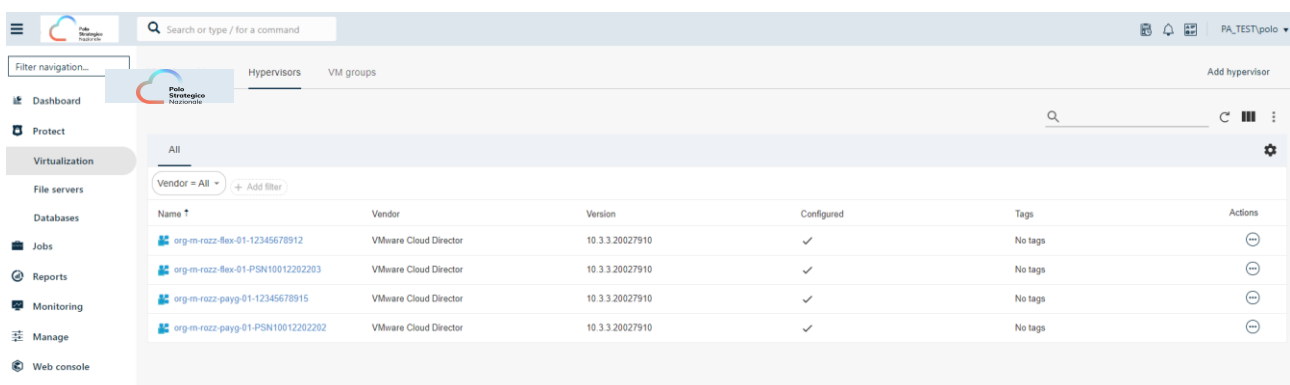
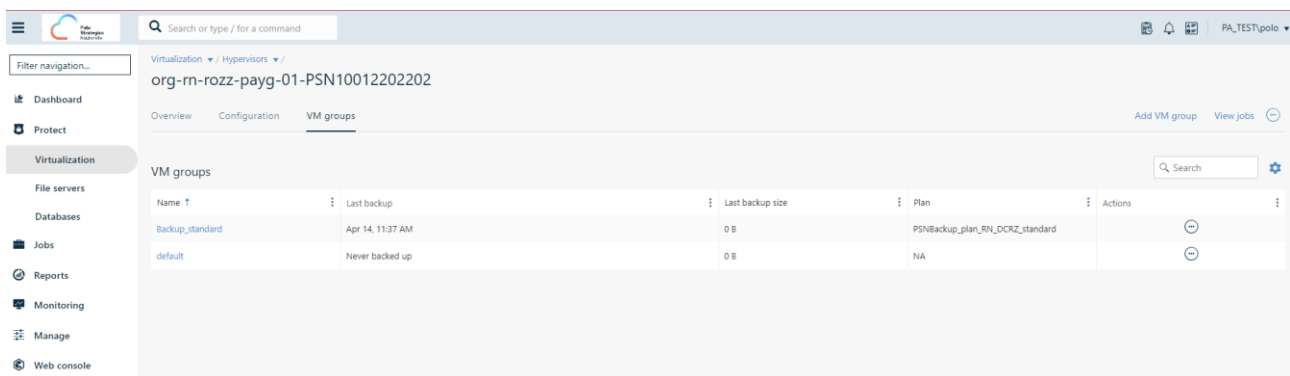


Figura 46 – Backup & restore VM

Ogni Company avrà un Hypervisor, al quale corrisponderà un solo VM Group con associato Plan standard (Retention 7 giorni + full settimanale).

VM Group e Plan standard del Backup_standard non dovranno essere modificati in alcun modo.



org-m-rozz-payg-01-PSN10012202202

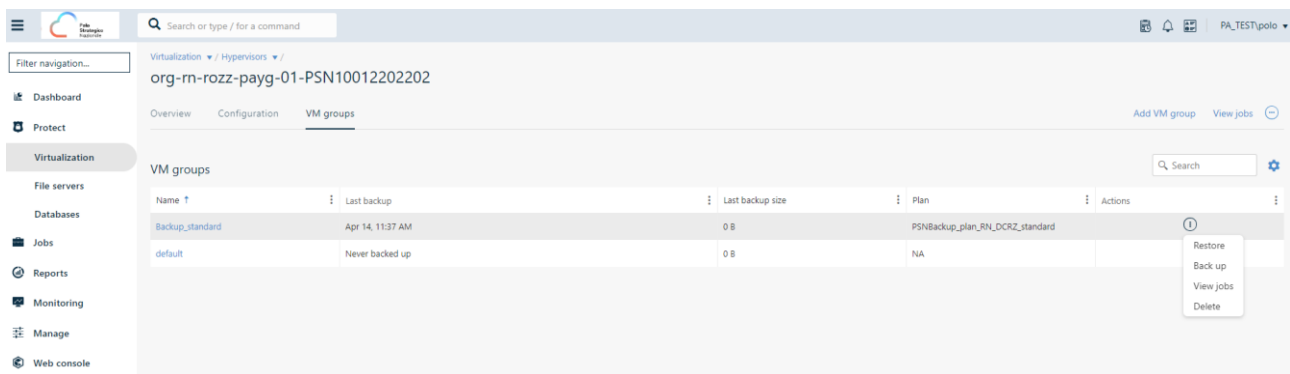
Overview Configuration **VM groups** Add VM group View jobs

VM groups

Name ↑	Last backup	Last backup size	Plan	Actions
Backup_standard	Apr 14, 11:37 AM	0 B	PSNBackup_plan_RN_DCRZ_standard	⌵
default	Never backed up	0 B	NA	⌵

Backup & restore VM

Dalla sezione *Actions* del Backup standard è possibile eseguire operazioni di backup e restore.



org-m-rozz-payg-01-PSN10012202202

Overview Configuration **VM groups** Add VM group View jobs

VM groups

Name ↑	Last backup	Last backup size	Plan	Actions
Backup_standard	Apr 14, 11:37 AM	0 B	PSNBackup_plan_RN_DCRZ_standard	⌵
default	Never backed up	0 B	NA	⌵

Backup & restore VM

BACKUP

Cliccando su *Backup* sarà possibile scegliere che tipo di backup effettuare. Selezionare quello più opportuno e cliccare su *OK*.

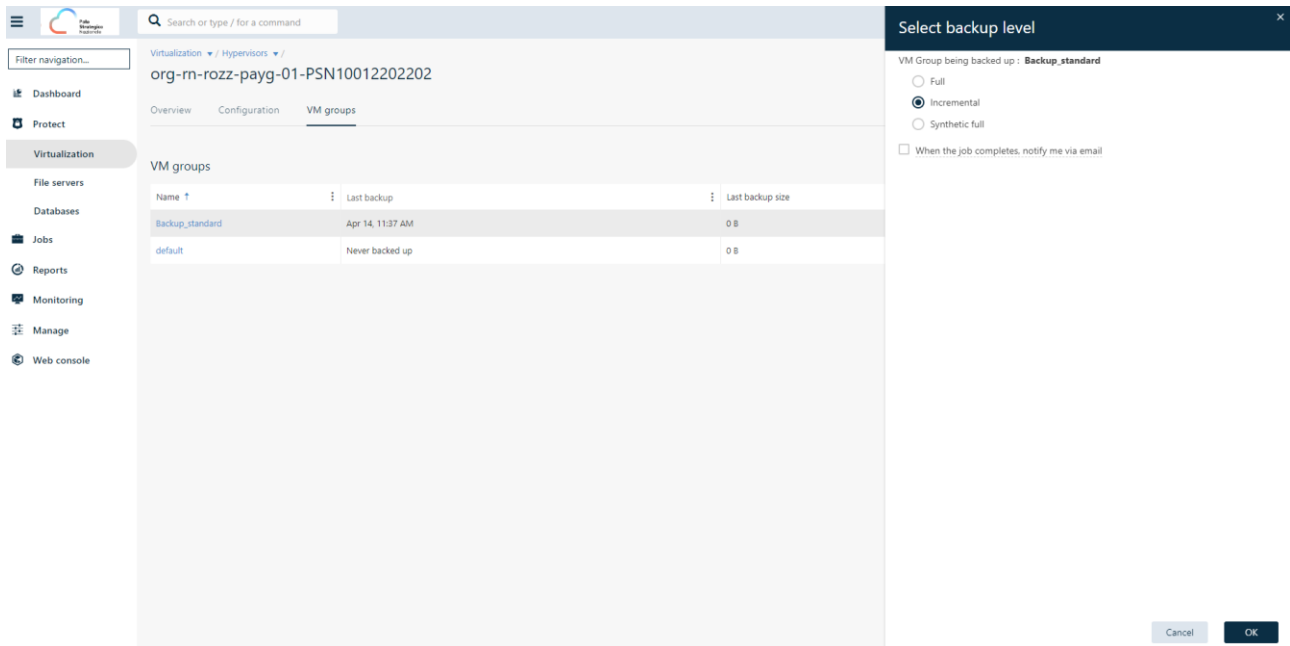
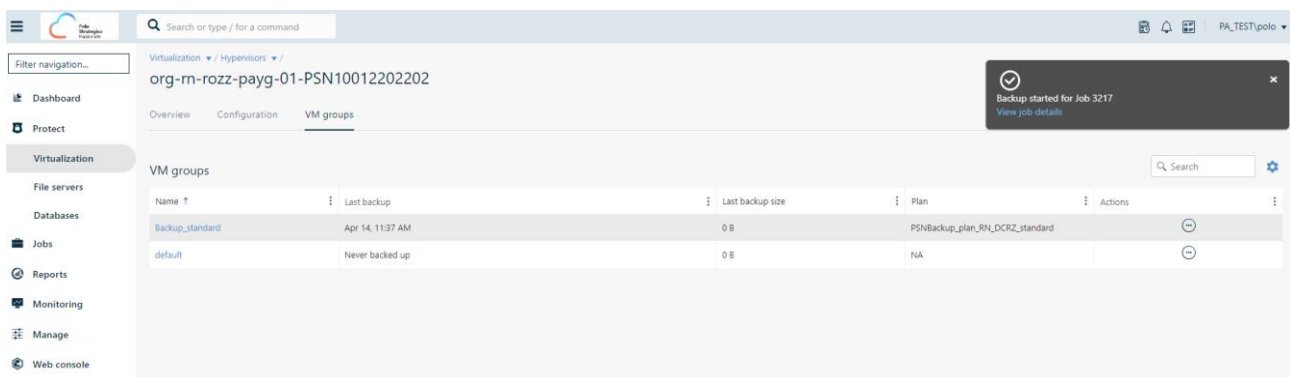
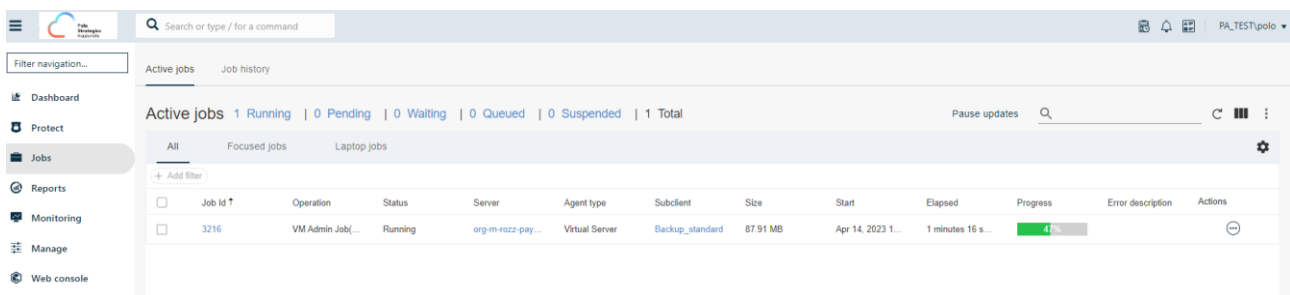


Figura 47 – Backup VM

È possibile seguire l'andamento del backup cliccando su *View job details* nella finestra che compare in alto a destra.



Backup VM



Search or type / for a command

Filter navigation...

Dashboard
Protect
Jobs
Reports
Monitoring
Manage
Web console

Active jobs Job history

Active jobs 1 Running | 0 Pending | 0 Waiting | 0 Queued | 0 Suspended | 1 Total

Pause updates

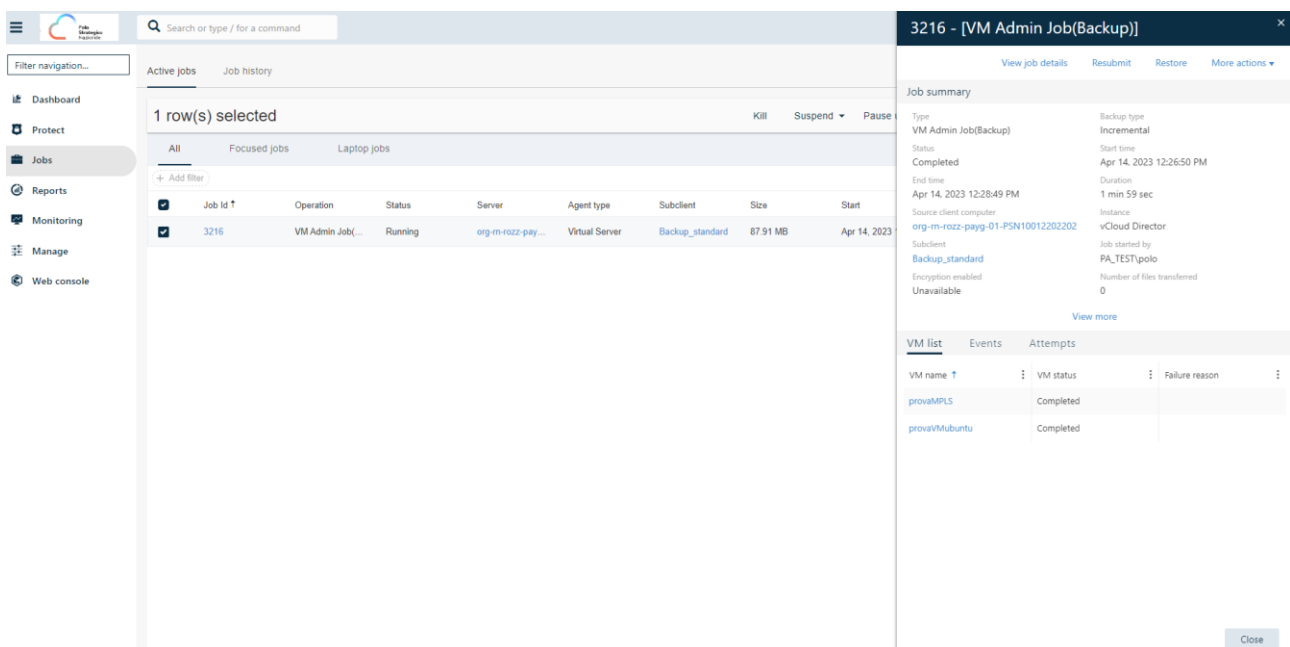
All Focused jobs Laptop jobs

+ Add filter

Job Id ↑	Operation	Status	Server	Agent type	Subclient	Size	Start	Elapsed	Progress	Error description	Actions
3216	VM Admin Job(...)	Running	org-m-rozz-pay...	Virtual Server	Backup_standard	87.91 MB	Apr 14, 2023 1...	1 minutes 16 s...	47%		

Backup VM

È possibile cliccare sul Job in oggetto per avere maggiori dettagli.



Search or type / for a command

Filter navigation...

Dashboard
Protect
Jobs
Reports
Monitoring
Manage
Web console

Active jobs Job history

1 row(s) selected Kill Suspend Pause

All Focused jobs Laptop jobs

+ Add filter

Job Id ↑	Operation	Status	Server	Agent type	Subclient	Size	Start
3216	VM Admin Job(...)	Running	org-m-rozz-pay...	Virtual Server	Backup_standard	87.91 MB	Apr 14, 2023

3216 - [VM Admin Job(Backup)]

View job details Resubmit Restore More actions

Job summary

Type	VM Admin Job(Backup)	Backup type	Incremental
Status	Completed	Start time	Apr 14, 2023 12:26:50 PM
End time	Apr 14, 2023 12:28:49 PM	Duration	1 min 59 sec
Source client computer	org-m-rozz-payg-01-PSN10012202202	Instance	vCloud Director
Subclient	Backup_standard	Job started by	PA_TEST\polo
Encryption enabled	Unavailable	Number of files transferred	0

View more

VM list	Events	Attempts
VM name ↑	VM status	Failure reason
provaiMPLS	Completed	
provaiVMubuntu	Completed	

Close

Backup VM

RESTORE

!! Attenzione nel caso di guest files restore Linux per i servizi CLOUD è necessario che sia configurato il server FLR da utilizzare, se la lista di tali sistemi è vuota contattare il supporto ([#Come posso richiedere assistenza per il servizio?](#))

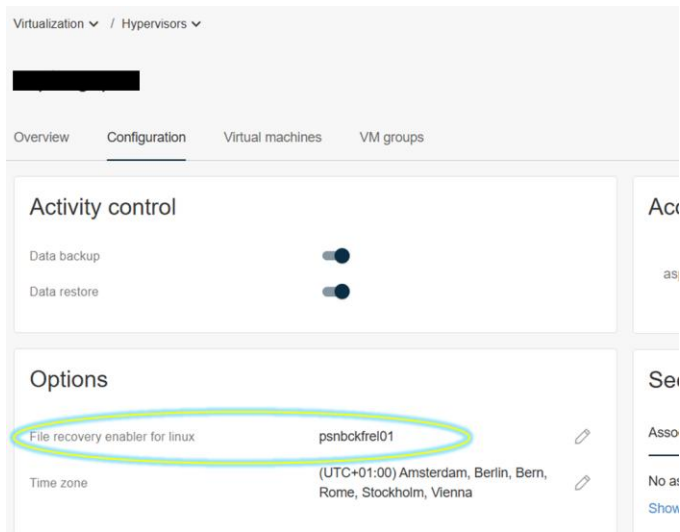


Figura 48 – Check configurazione server FLR per “guest files restore Linux” servizi CLOUD

Cliccando su *Restore* sarà possibile scegliere che tipo di restore effettuare: guest files o full virtual machine.

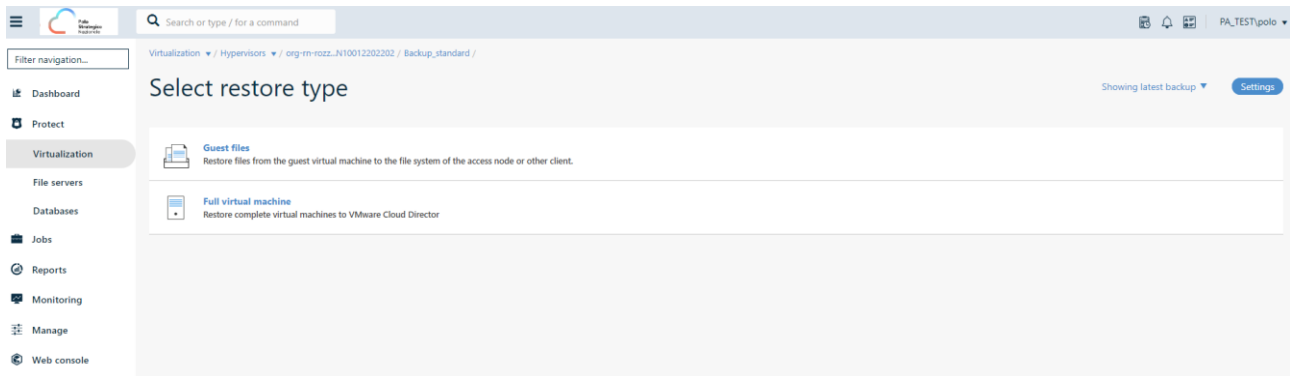


Figura 49 – Restore

Cliccando su *Guest files* vengono mostrate le VM sulle quali si può effettuare la restore dei file. Selezionando una VM vengono mostrate le relative cartelle/file.

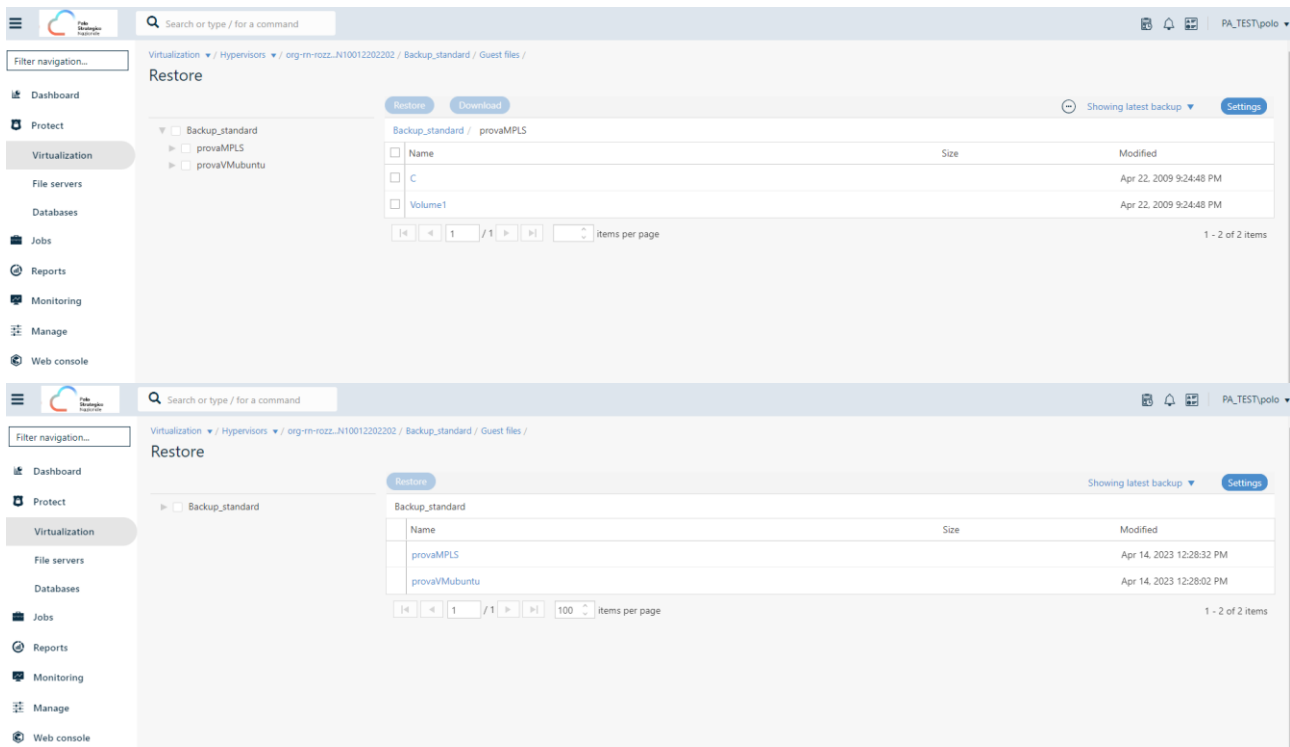
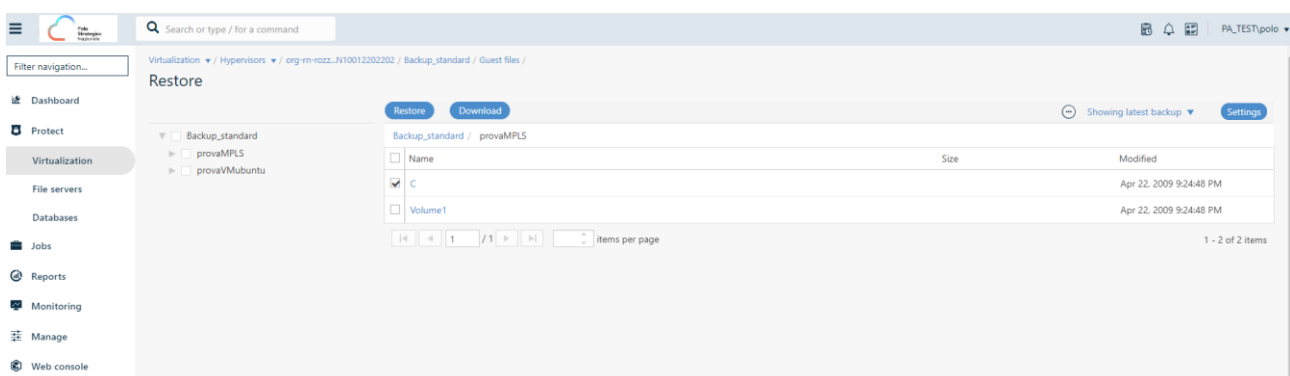


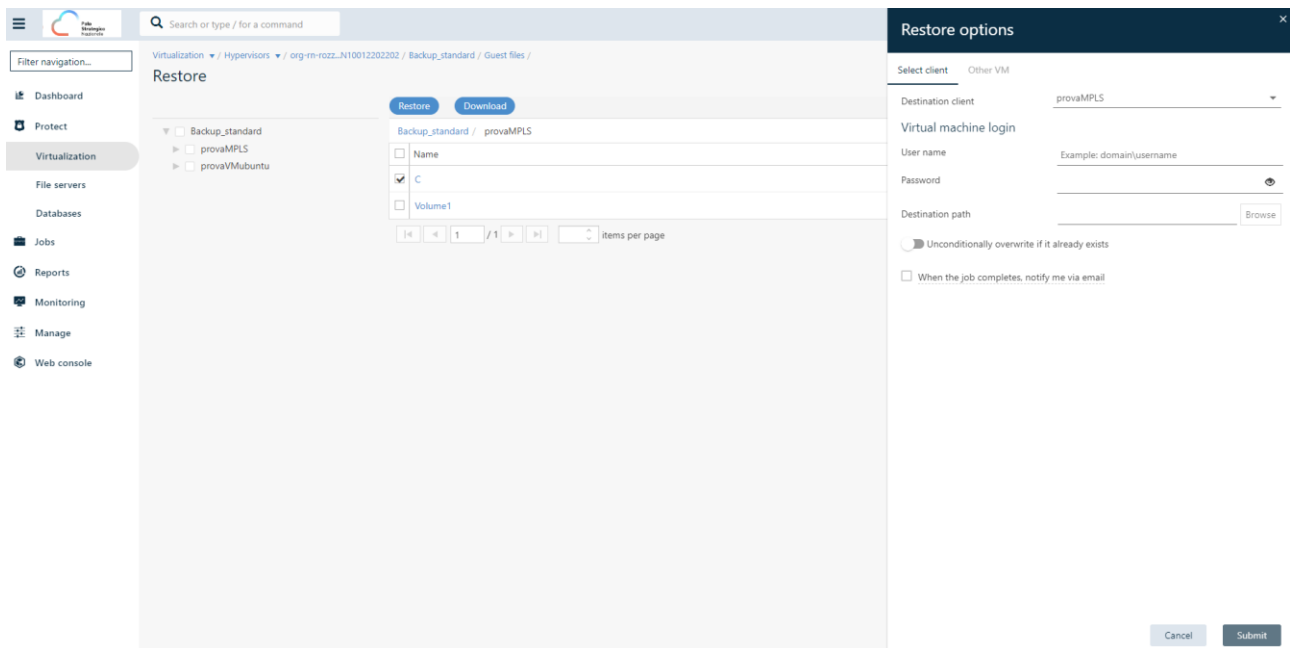
Figura 50 – Restore guest files

Selezionare la cartella/file di cui effettuare il restore e cliccare su *Restore*.



Restore guest files

Inserire i dettagli utili per la *Restore* e cliccare su *Submit*.



Restore guest files

È possibile vedere i progressi relativi alla restore cliccando su *View jobs* sulla finestrella che compare in alto a destra.

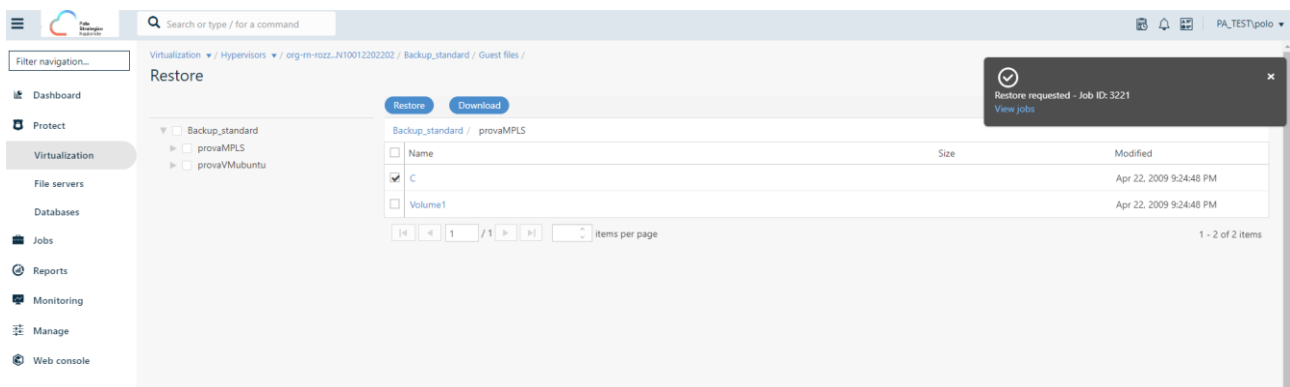
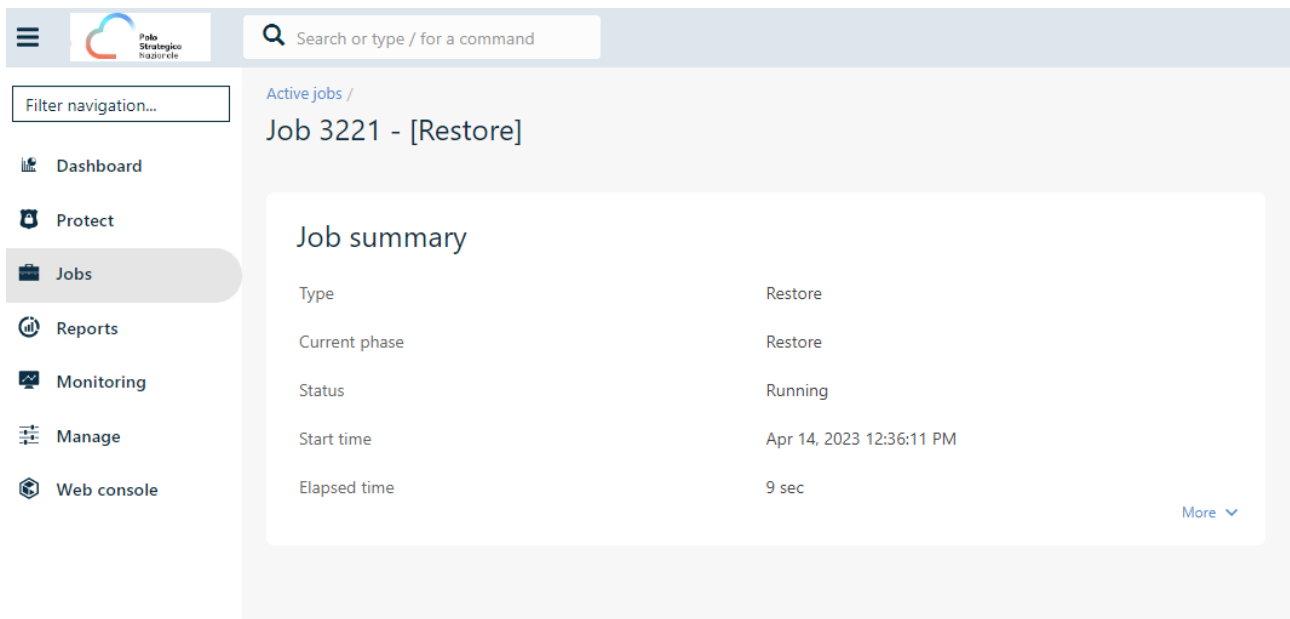


Figura 51 – Monitoraggio jobs restore



Filter navigation...

Dashboard

Protect

Jobs

Reports

Monitoring

Manage

Web console

Search or type / for a command

Active jobs /

Job 3221 - [Restore]

Job summary

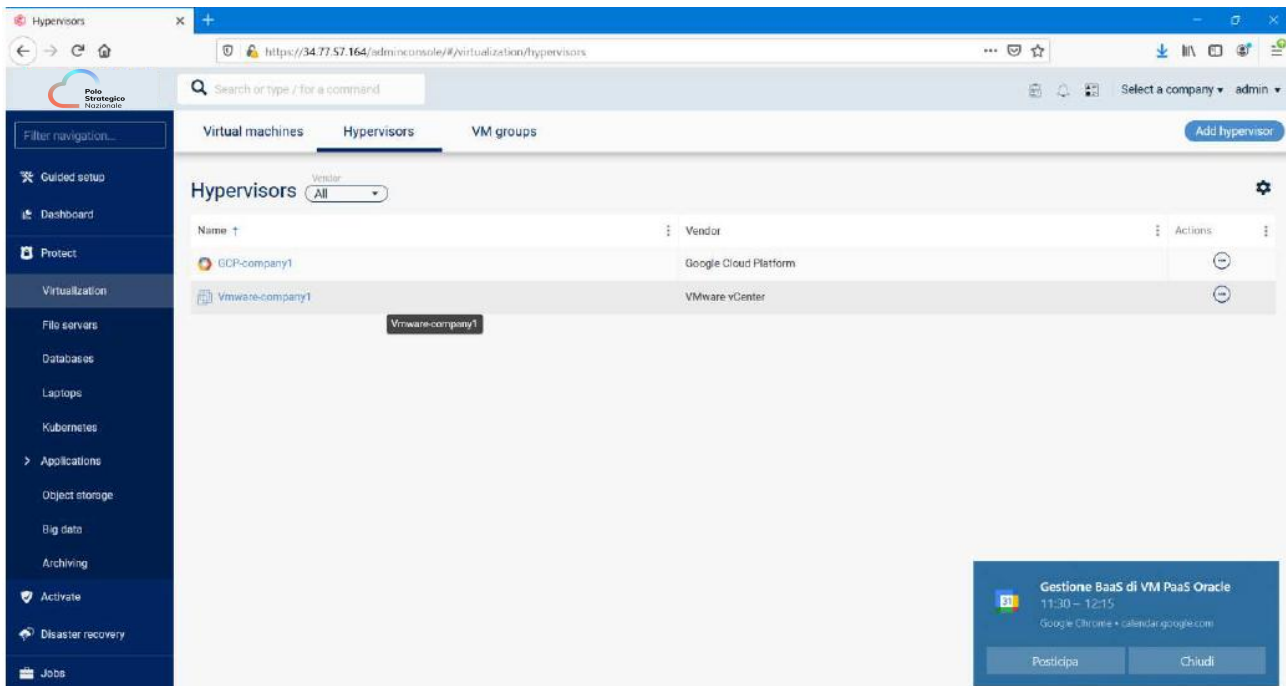
Type	Restore
Current phase	Restore
Status	Running
Start time	Apr 14, 2023 12:36:11 PM
Elapsed time	9 sec

More ▾

Monitoraggio jobs restore

Di seguito viene descritta la procedura generica per aggiungere e configurare Hypervisor e VM Group.

Dalla sezione *Protect – Virtualization - Hypervisor* selezionare l'Hypervisor.



Hypervisors

Search or type / for a command

Select a company ▾ admin ▾

Virtual machines Hypervisors VM groups

Add hypervisor

Hypervisors

Vendor: All ▾

Name ↑	Vendor	Actions
GCP-company1	Google Cloud Platform	⊖
VMware-company1	VMware vCenter	⊖

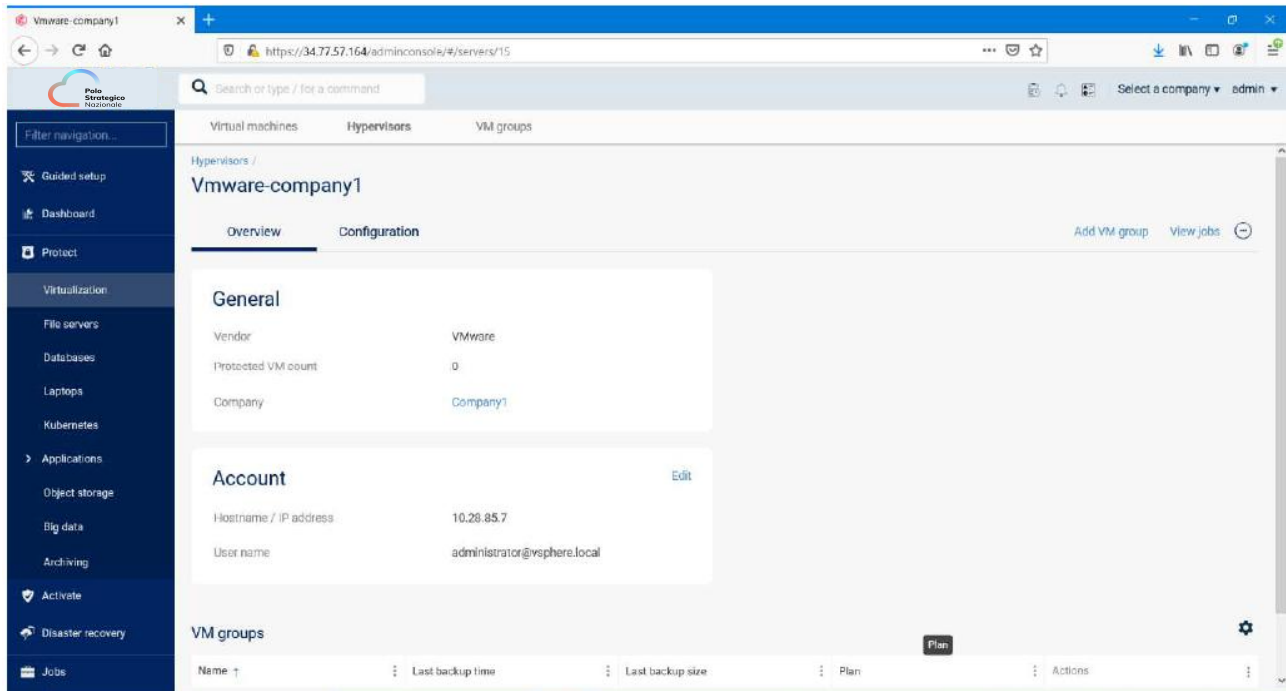
VMware-company1

Gestione BaaS di VM PaaS Oracle
11:30 - 12:15
Google Chrome - calendar.google.com

Partecipa Chiudi

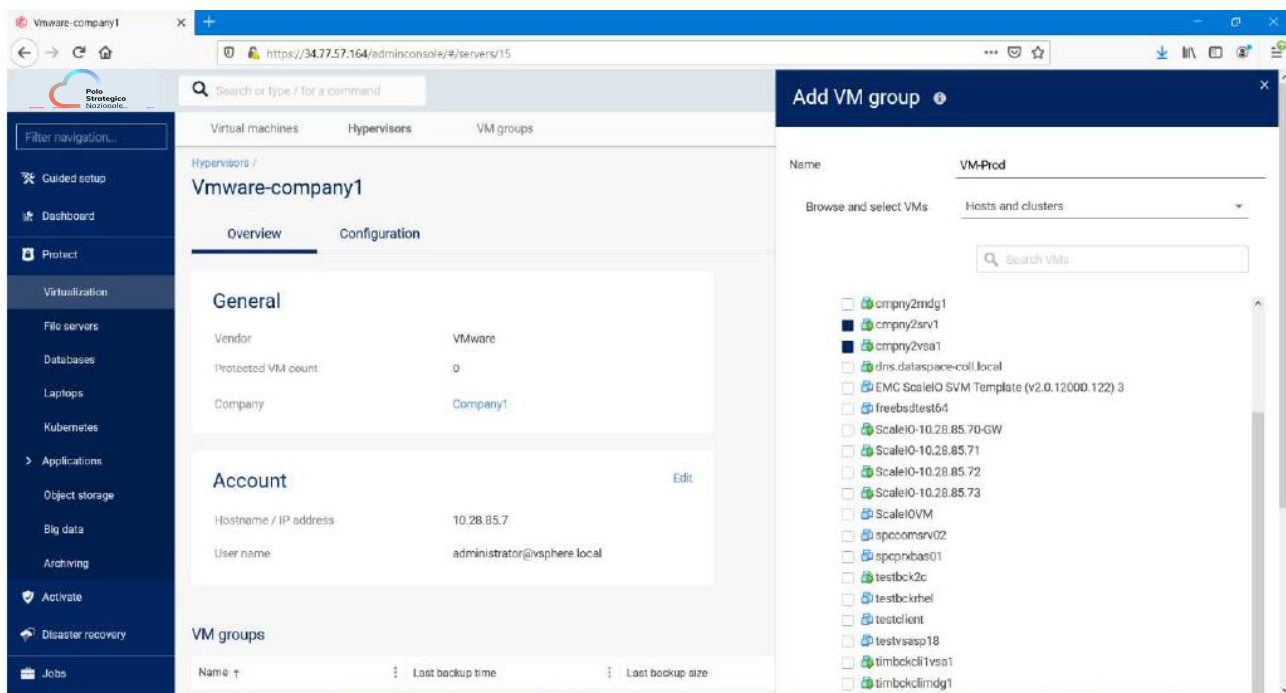
Figura 52 – Configurazione hypervisor e VMGroups

e premere il tasto *Add VM Groups* in alto a destra.



Configurazione hypervisor e VMGroups

Sulla schermata successiva indicare un *Name* per il VM group che si sta definendo, selezionare la modalità con cui si vuole effettuare il Browse delle VM (tra *Datastores* e *datastore cluster*, *Hosts and Cluster* e *VMs and template*) quindi selezionare le VM di cui si vuole effettuare il backup, indicare il *Plan* o la *Storage policy* e *schedule policy* associata al VM Group nella sezione *Backup configuration* e digitare il tasto *Save*.



Configurazione hypervisor e VMGroups

11.3 Backup Database

Accedere alla console di amministrazione del servizio e selezionare *Protect – Databases* dal menu di sinistra e selezionare l'istanza di cui si vuole effettuare backup selezionando backup dal menu a tendina a sinistra dell'istanza selezionata.

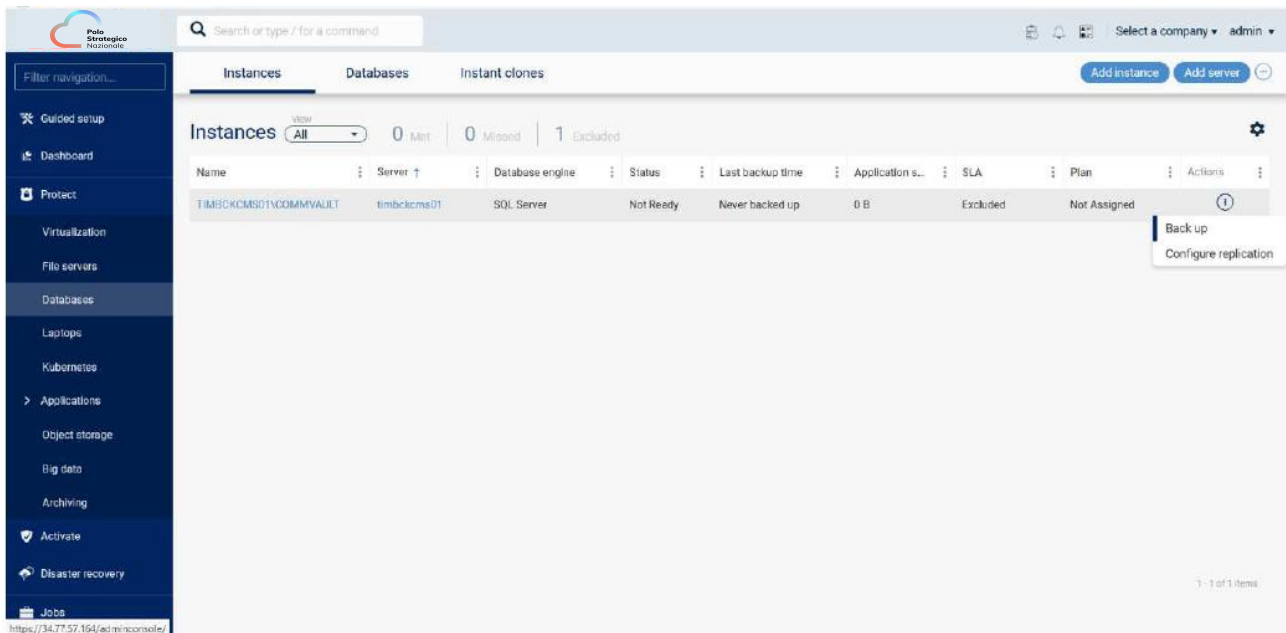
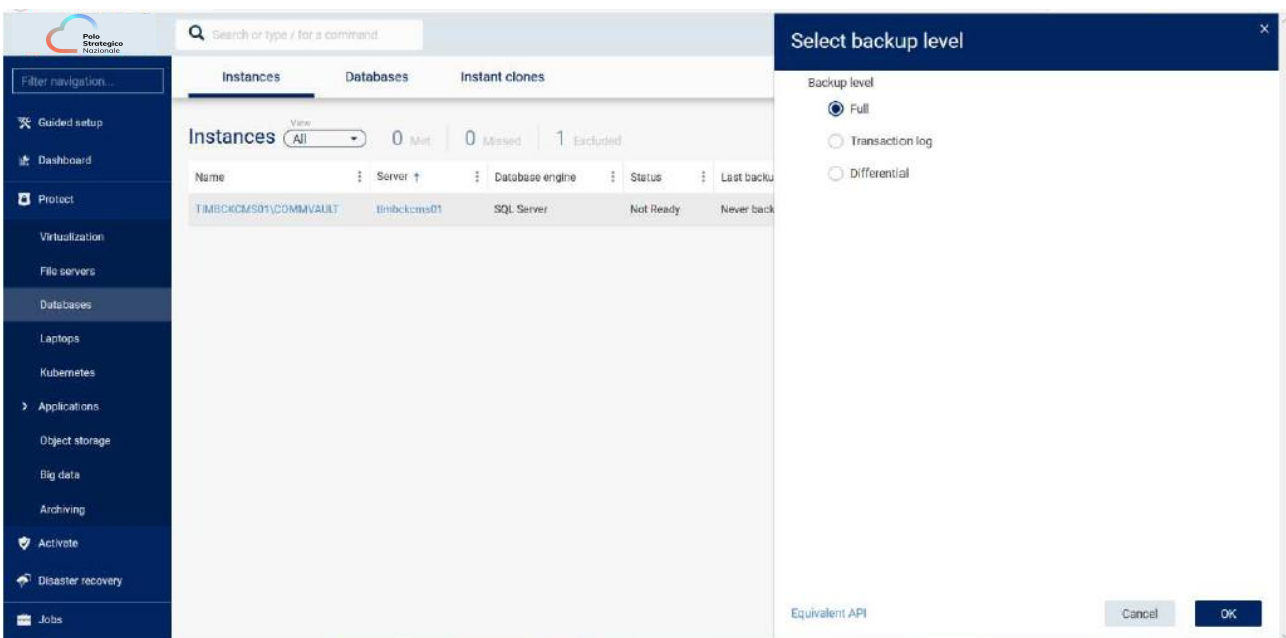


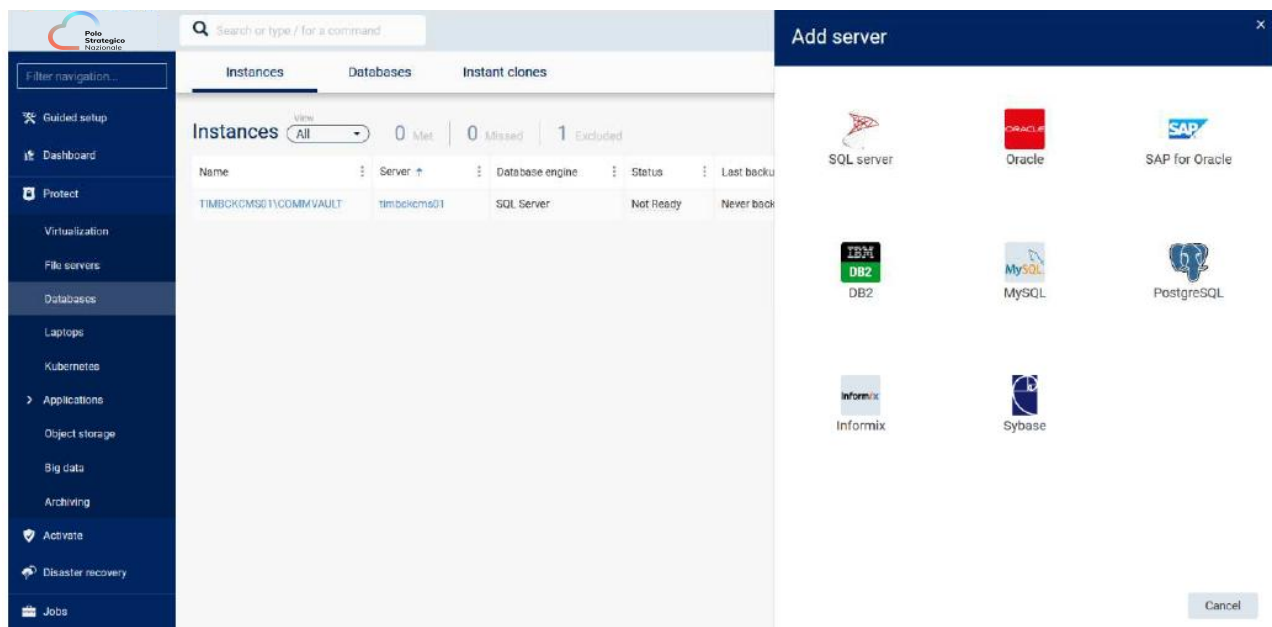
Figura 53 – Configurazione backup database

Sulla schermata successiva selezionare il tipo di backup (full, transaction log, Differential), premere il tasto OK e verificare la corretta esecuzione del job eseguito.



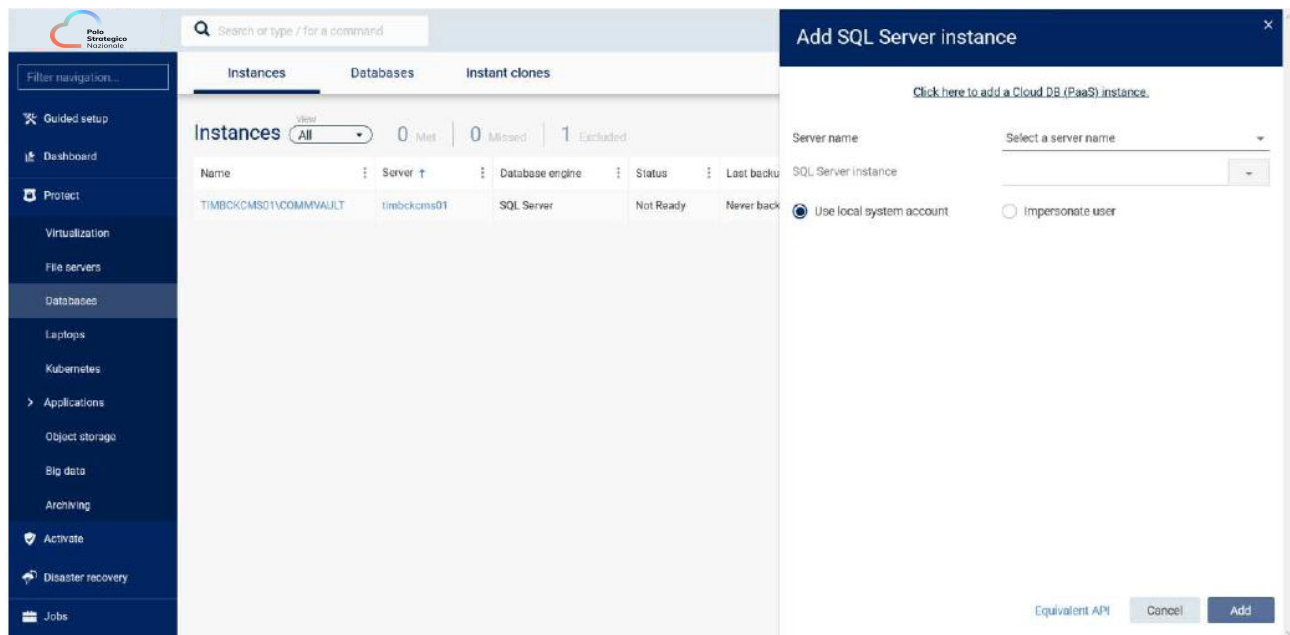
Configurazione backup database

Dalla sezione *Instances* del menù *Protect – Databases* è possibile configurare le istanze di DB su cui effettuare backup installando il relativo agent sul server già configurato al servizio (vedi [capitolo 5 Configurazione dei client](#)) digitando i tasti *Add server* e/o *Add Instance*. La stessa attività potrà comunque essere effettuata, come indicato nel capitolo 6 con gli ulteriori agent di backup.



Configurazione backup database

Sarà necessario selezionare il tipo di server/instance database da configurare e procedere con l'inserimento delle relative informazioni (tipicamente server su cui configurare l'istanza, utenze di accesso, ecc.).



The screenshot shows the Polo Strategico Nazionale management console. On the left is a navigation menu with options like Guided setup, Dashboard, Protect, Virtualization, File servers, Databases, Laptops, Kubernetes, Applications, Object storage, Big data, Archiving, Activate, Disaster recovery, and Jobs. The main area has tabs for Instances, Databases, and Instant clones. The 'Instances' tab is active, showing a table with one instance: 'TIMBCKCMS01VCOMMVAULT' on server 'timbckcms01', using 'SQL Server' engine, with status 'Not Ready' and 'Never back'. A modal window titled 'Add SQL Server instance' is open on the right. It includes a search bar, a dropdown for 'Server name', a text input for 'SQL Server instance', and radio buttons for 'Use local system account' (selected) and 'Impersonate user'. At the bottom of the modal are buttons for 'Equivalent API', 'Cancel', and 'Add'.

Configurazione backup database

11.4 Verifica dei log dei job di backup

Nel caso in cui un job di backup andasse in errore o in generale si volessero consultare i log relativi ai job di backup è possibile farlo nella sezione apposita, come mostrato di seguito.

Una volta fatto accesso alla console di backup, cliccare nella sezione Jobs (evidenziata in grigio), nel menù a sinistra. Nella sezione *Active jobs* è possibile visionare i job di backup in corso.

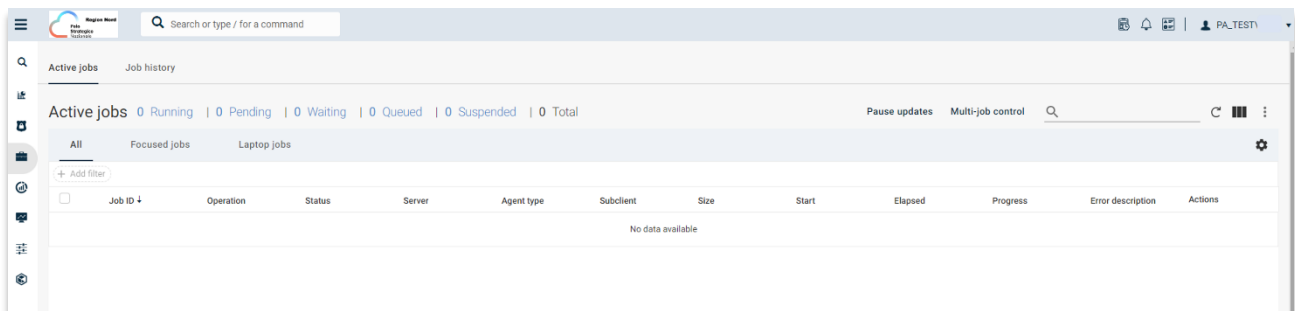
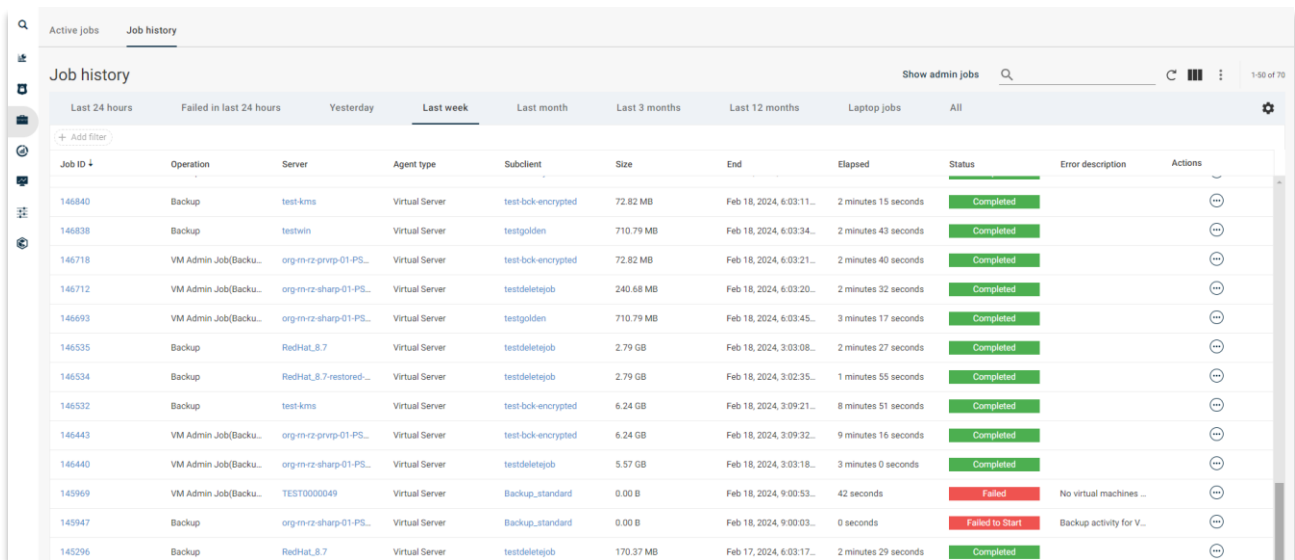


Figura 54 – Verifica logs jobs

Nella sezione *Job history* è possibile visionare i job di backup effettuati, anche quelli in *Failed* nel caso in cui ce ne siano stati.



Job ID	Operation	Server	Agent type	Subclient	Size	End	Elapsed	Status	Error description	Actions
146840	Backup	test-kms	Virtual Server	test-bck-encrypted	72.82 MB	Feb 18, 2024, 6:03:11...	2 minutes 15 seconds	Completed		
146838	Backup	testwin	Virtual Server	testgolden	710.79 MB	Feb 18, 2024, 6:03:34...	2 minutes 43 seconds	Completed		
146718	VM Admin Job(Backu...	org-m-rz-grwp-01-PS...	Virtual Server	test-bck-encrypted	72.82 MB	Feb 18, 2024, 6:03:21...	2 minutes 40 seconds	Completed		
146712	VM Admin Job(Backu...	org-m-rz-sharp-01-PS...	Virtual Server	testdeletejob	240.68 MB	Feb 18, 2024, 6:03:20...	2 minutes 32 seconds	Completed		
146693	VM Admin Job(Backu...	org-m-rz-sharp-01-PS...	Virtual Server	testgolden	710.79 MB	Feb 18, 2024, 6:03:45...	3 minutes 17 seconds	Completed		
146535	Backup	RedHat_8.7	Virtual Server	testdeletejob	2.79 GB	Feb 18, 2024, 3:03:08...	2 minutes 27 seconds	Completed		
146534	Backup	RedHat_8.7-restored...	Virtual Server	testdeletejob	2.79 GB	Feb 18, 2024, 3:02:35...	1 minutes 55 seconds	Completed		
146532	Backup	test-kms	Virtual Server	test-bck-encrypted	6.24 GB	Feb 18, 2024, 3:09:21...	8 minutes 51 seconds	Completed		
146443	VM Admin Job(Backu...	org-m-rz-grwp-01-PS...	Virtual Server	test-bck-encrypted	6.24 GB	Feb 18, 2024, 3:09:32...	9 minutes 16 seconds	Completed		
146440	VM Admin Job(Backu...	org-m-rz-sharp-01-PS...	Virtual Server	testdeletejob	5.57 GB	Feb 18, 2024, 3:03:18...	3 minutes 0 seconds	Completed		
145969	VM Admin Job(Backu...	TEST0000049	Virtual Server	Backup_standard	0.00 B	Feb 18, 2024, 9:00:53...	42 seconds	Failed	No virtual machines ...	
145947	Backup	org-m-rz-sharp-01-PS...	Virtual Server	Backup_standard	0.00 B	Feb 18, 2024, 9:00:03...	0 seconds	Failed to Start	Backup activity for V...	
145296	Backup	RedHat_8.7	Virtual Server	testdeletejob	170.37 MB	Feb 17, 2024, 6:03:17...	2 minutes 29 seconds	Completed		

Verifica logs jobs

Selezionare il job di cui si vogliono visionare i log, cliccando sul Job ID a sinistra.

Dalla schermata che compare si ha una *Overview* del job. Si possono anche visionare *Attempts* o *Events* cliccando sulle rispettive sezioni.

Jobs

Job 145969 - [VM Admin Job(Backup)]

Send logs View logs

Overview Attempts Events

General

Type	VM Admin Job(Backup)
Backup type	Full
Status	Failed
Job started by	master (Scheduled)
Encryption enabled	Yes
Storage Accelerator	No

Associations

Agent	Virtual Server
Backup set	defaultBackupSet
Source client computer	TEST000049
Instance	vCloud Director
Subclient	Backup_standard
Plan	PSNBackup_plan_RN_DCRZ_standard

Virtual Machine Count

Total	0
Successful	0
Partially Successful	0

Progress

Start time	Feb 18, 2024, 9:00:08 AM
Elapsed time	42 seconds
End time	Feb 18, 2024, 9:00:53 AM

Item status

Failures	0 Folders, 0 Files
Data transferred on network	0.00 B
Savings percentage	0.00 %

Error summary

Error code: [91.587]
Description: No virtual machines were discovered for [Backup_standard]. Check the content and filters.
Source: psnbckvsadorz02, Process: vdiscovery

Verifica logs jobs

Jobs

Job 145969 - [VM Admin Job(Backup)]

Send logs View logs

Overview Attempts Events

All

Phase	Status	Server started ↑	Server end	Elapsed time	No. of successes	No. of failures	No. of skipped	Size of application
Discover	Failed	Feb 18, 9:00 AM	Feb 18, 9:00 AM	42 seconds	0	0	0	0.00 B

Verifica logs jobs

Jobs

Job 145969 - [VM Admin Job(Backup)]

Send logs View logs

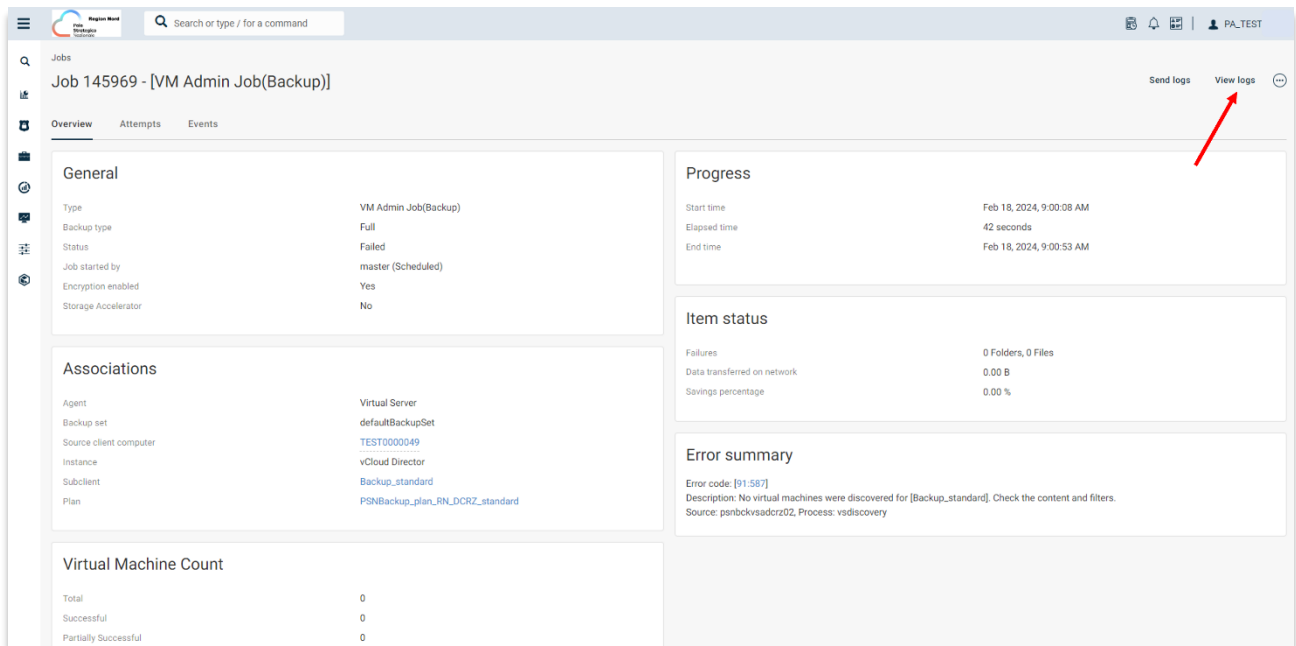
Overview Attempts Events

All

Severity	Event ID ↑	Date	Computer	Event code	Description
Minor	408849	Feb 18, 9:00 AM	psnbckmsdorz	19:122	Received failed message for job [145969], pha...

Verifica logs jobs

Per visionare i log relativi al job è necessario cliccare in alto a destra nella sezione *View logs*.



Jobs
Job 145969 - [VM Admin Job(Backup)]

Send logs View logs

Overview Attempts Events

General

Type	VM Admin Job(Backup)
Backup type	Full
Status	Failed
Job started by	master (Scheduled)
Encryption enabled	Yes
Storage Accelerator	No

Progress

Start time	Feb 18, 2024, 9:00:08 AM
Elapsed time	42 seconds
End time	Feb 18, 2024, 9:00:53 AM

Item status

Failures	0 Folders, 0 Files
Data transferred on network	0.00 B
Savings percentage	0.00 %

Associations

Agent	Virtual Server
Backup set	defaultBackupSet
Source client computer	TEST0000049
Instance	vCloud Director
Subclient	Backup_standard
Plan	PSNBackup_plan_RN_DCRZ_standard

Virtual Machine Count

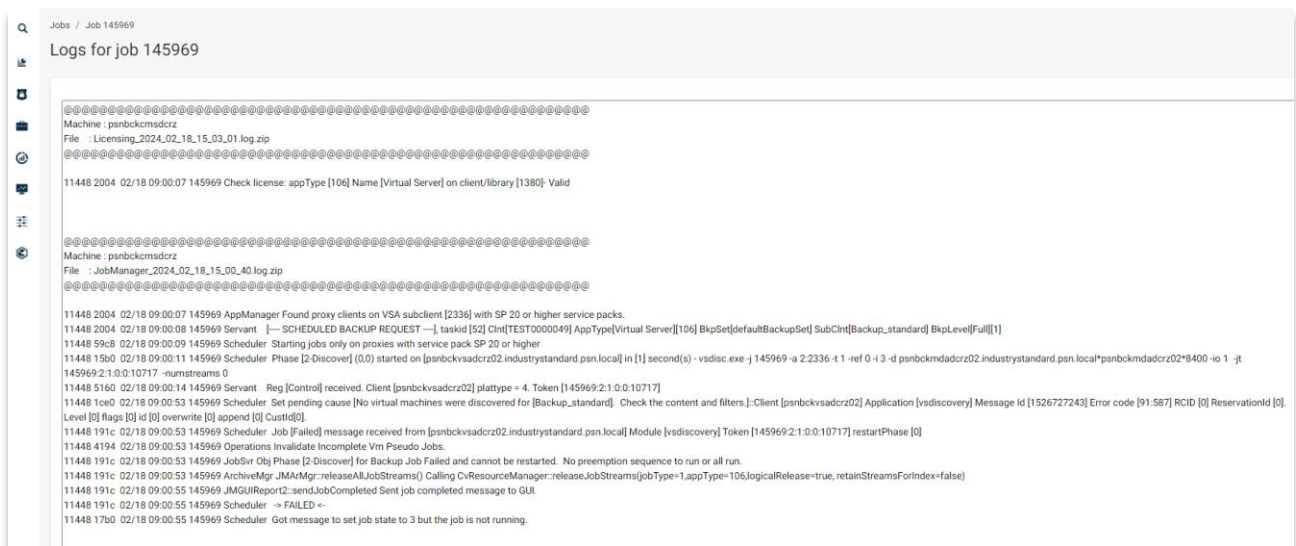
Total	0
Successful	0
Partially Successful	0

Error summary

Error code: [91.587]
Description: No virtual machines were discovered for [Backup_standard]. Check the content and filters.
Source: psnbckvsadcrz02, Process: vdiscovery

Verifica logs jobs

Dalla schermata che compare sarà possibile scorrere tra le righe di log.



Jobs / Job 145969
Logs for job 145969

```

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Machine : psnbckmsdcrz
File : Licensing_2024_02_18_15_03_01.log.zip
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

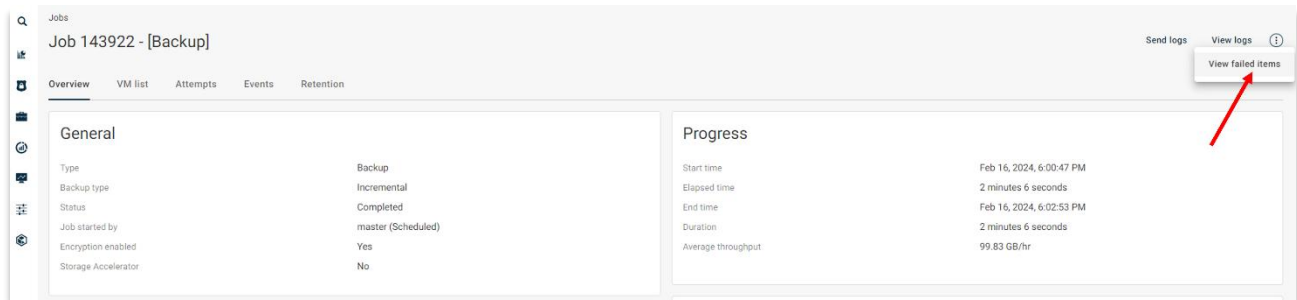
11448 2004 02/18 09:00:07 145969 Check license: appType [106] Name [Virtual Server] on client/library [1380]: Valid

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Machine : psnbckmsdcrz
File : JobManager_2024_02_18_15_00_40.log.zip
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

11448 2004 02/18 09:00:14 145969 Servant Reg [Control] received. Client [psnbckvsadcrz02] plattype = 4. Token [145969:2:1:0:0:10717]
11448 2004 02/18 09:00:08 145969 Servant [--- SCHEDULED BACKUP REQUEST ---], taskId [52] CInt[TEST0000049] AppType[Virtual Server][106] BkpSet[defaultBackupSet] SubCInt[Backup_standard] BkpLevel[Full][1]
11448 59c8 02/18 09:00:09 145969 Scheduler Starting jobs only on proxies with service pack SP.20 or higher
11448 15d0 02/18 09:00:11 145969 Scheduler Phase [2-Discover] (0,0) started on [psnbckvsadcrz02.industrystandard.psn.local] in [1] second(s) - vdiscovery 145969 -a 2.2336 -l 1 -ref 0 -l 3 -d psnbckmdadcrz02.industrystandard.psn.local*psnbckmdadcrz02*8400 -io 1 -jt 145969:2:1:0:0:10717 -numstreams 0
11448 5160 02/18 09:00:14 145969 Servant Reg [Control] received. Client [psnbckvsadcrz02] plattype = 4. Token [145969:2:1:0:0:10717]
11448 1ce0 02/18 09:00:53 145969 Scheduler Set pending cause [No virtual machines were discovered for [Backup_standard]. Check the content and filters.]-Client [psnbckvsadcrz02] Application [vdiscovery] Message Id [1526727243] Error code [91.587] RCID [0] ReservationId [0]. Level [0] flags [0] id [0] overwrite [0] append [0] CustId[0].
11448 191c 02/18 09:00:53 145969 Scheduler Job [Failed] message received from [psnbckvsadcrz02.industrystandard.psn.local] Module [vdiscovery] Token [145969:2:1:0:0:10717] restartPhase [0]
11448 4194 02/18 09:00:53 145969 Operations Invalidate Incomplete Vm Pseudo Jobs.
11448 191c 02/18 09:00:53 145969 ArchiveMgr JManMgr:releaseAllJobStreams() Calling CvResourceManager:releaseJobStreams(jobType=1,appType=106,logicalRelease=true, retainStreamsForIndex=false)
11448 191c 02/18 09:00:55 145969 JMGUReport2:sendJobCompleted Sent job completed message to GUI.
11448 191c 02/18 09:00:55 145969 Scheduler -> FAILED <-
11448 17b0 02/18 09:00:55 145969 Scheduler Got message to set job state to 3 but the job is not running.
  
```

Verifica logs jobs

Accanto alla sezione View logs sono presenti tre pallini in verticale dai quali, per alcuni job è possibile vedere gli oggetti in failed.



Verifica logs jobs

12 Backup Golden Copy

Quale ulteriore elemento di garanzia della protezione dei dati, oltre al backup standard, la soluzione di backup mette a disposizione un servizio opzionale aggiuntivo che analizza i backup mensili allo scopo di intercettare eventuali contaminazioni malware silenti che comprometterebbero la validità di un eventuale restore in produzione. Si tratta di una funzionalità completamente gestita ed opzionale, attivabile su richiesta, in aggiunta al servizio di Backup standard: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della golden copy; in particolare, quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum CRC per ogni blocco di dati sul sistema sorgente e queste signature vengono utilizzate per convalidare i dati del backup. Una volta validate, tali signature vengono memorizzate con il backup stesso: ciò permette di eseguire automaticamente la verifica della consistenza dei dati salvati nel backup, utilizzando le signature salvate.

12.1 Livelli di sicurezza Golden Copy

La soluzione implementata si basa sull'applicazione di tre livelli di protezione per limitare le minacce di attacco di tipo Ransomware/Malware alla golden copy di backup aumentando quindi la sicurezza dei dati di backup. Di seguito vengono descritti i tre livelli di protezione:

Livello	Descrizione
Air Gap	- Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato. - Replica dei dati con tunnel sicuro. - Tutto l'accesso ai dati isolati è bloccato. È consentito solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di

Livello	Descrizione
	riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).
WORM Protection	• Funzionalità della tecnologia di riferimento (Commvault) di WORM (Write Only Read Multiple) che si integra con le medesime funzionalità sullo storage di riferimento del repository • La tecnologia di riferimento (Commvault) blocca i dati di backup da modifiche casuali non autorizzate e previene la modifica o l'eliminazione dei dati di backup intenzionale (I dati di backup saranno cancellati solo quando saranno state raggiunte le retention applicate) • Nessun amministratore del backup potrà cancellare i dati di backup non scaduti • Inoltre, la tecnologia di riferimento (Commvault) convalida l'integrità dei dati durante il backup e durante le operazioni di copia dei dati. Quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum CRC per ogni blocco di dati sul client di origine e archiviati con il backup. Quando si copiano i dati, le firme (checksum CRC) vengono utilizzate per convalidare i blocchi di dati durante l'operazione di copia.
Ransomware Protection	• Funzionalità Commvault di Ransomware protection • I dati di backup sono bloccati e possono essere modificati solo dai processi della tecnologia di riferimento (Commvault). • Qualsiasi ransomware, applicazione o utente che tenti di eliminare, o modificare i dati di backup dal Media Agent (unico server che può accedere allo storage) riceverà una segnalazione di errore (catastrophic error dallo stack I/O del SO) a meno che non si tratti di un processo della tecnologia di riferimento (Commvault) autorizzato (modalità like SE-Linux).

12.2 Effettuare backup con opzione Golden Copy

In questo capitolo verrà mostrata la modalità di implementazione del backup con opzione Golden Copy.

In fase di attivazione del backup per una VM è possibile selezionare uno dei plan relativi alla Golden Copy, come mostrato in figura.

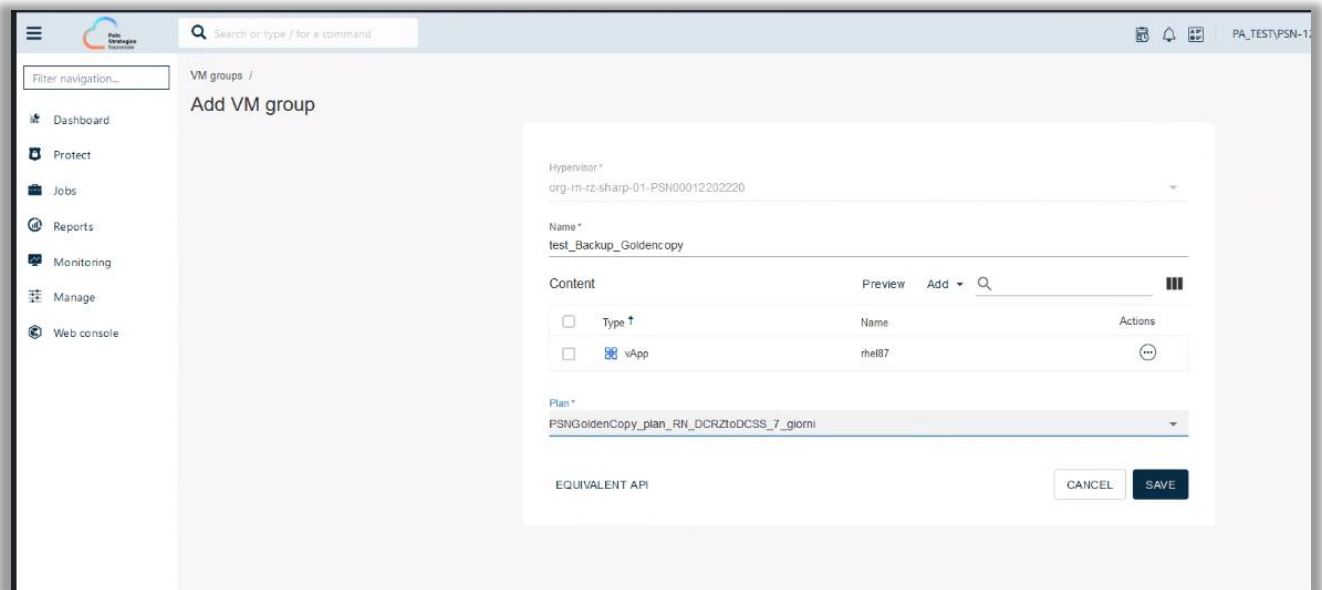
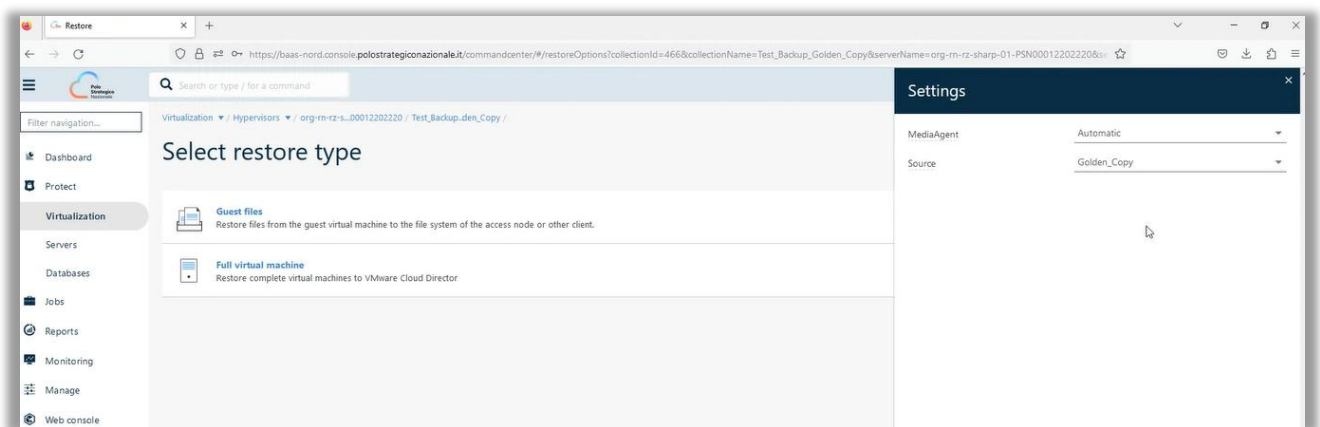


Figura 55 – Configurazione backup con Golden Copy

Una volta cliccato su **SAVE**, partirà il job di backup. Al suo completamento, visionabile nella sezione **Jobs** del menu, partirà la *auxiliary golden copy* in ambiente protetto di backup.

Nel caso si desideri effettuare una restore della VM in oggetto, avendo selezionato uno dei plan con opzione *golden copy*, sarà possibile ripristinare la auxiliary copy precedentemente creata, selezionando nei **Settings** l'opzione **Source** → **Golden_Copy**.



Configurazione backup con Golden Copy

13 Operazioni di restore

Le istruzioni contenute in questa sezione sono relative alle operazioni di restore dei dati. Per effettuare il restore di un dato che è stato sottoposto precedentemente a backup è necessario selezionare la risorsa (File Servers, Virtual machine, database, ecc.) su cui si vuole effettuare il restore e dal menu a sinistra selezionare l'opzione *Restore* dal menu a tendina.

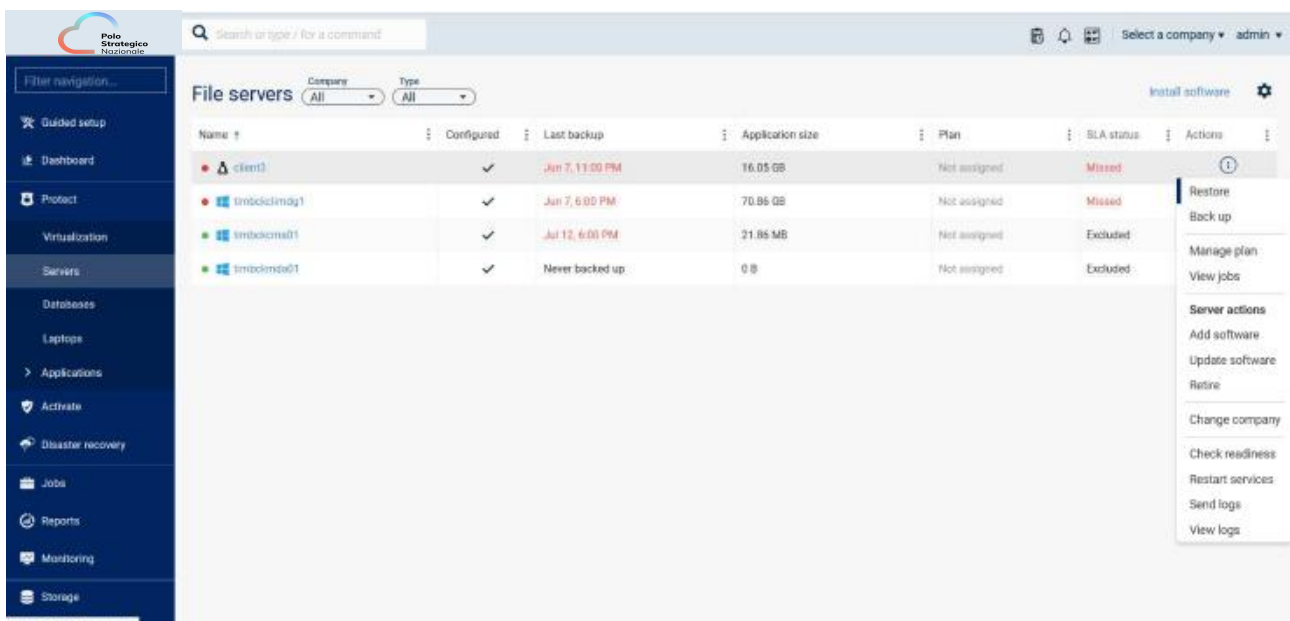
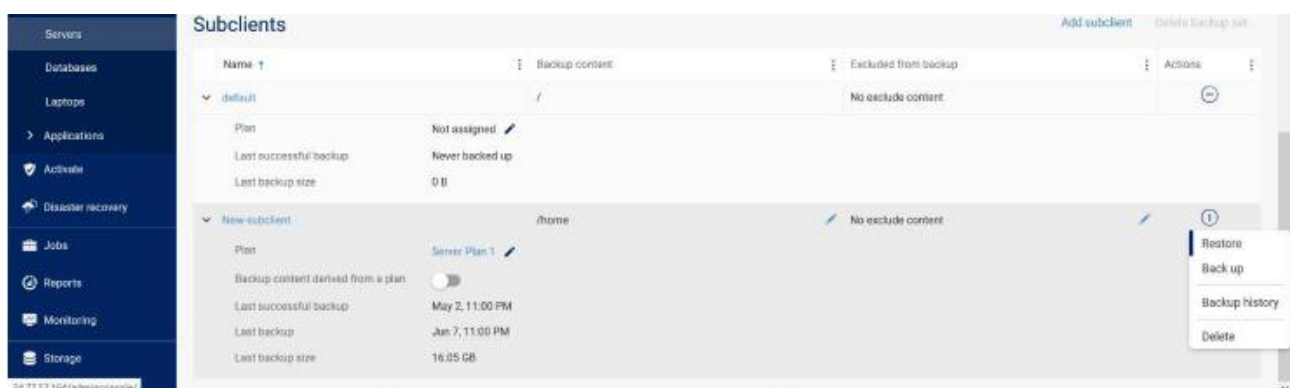


Figura 56 – Procedura restore

Oppure dopo aver selezionato la risorsa e il subclient, sempre dal menu a sinistra, selezionare l'opzione restore dal menu a tendina.



Procedura restore

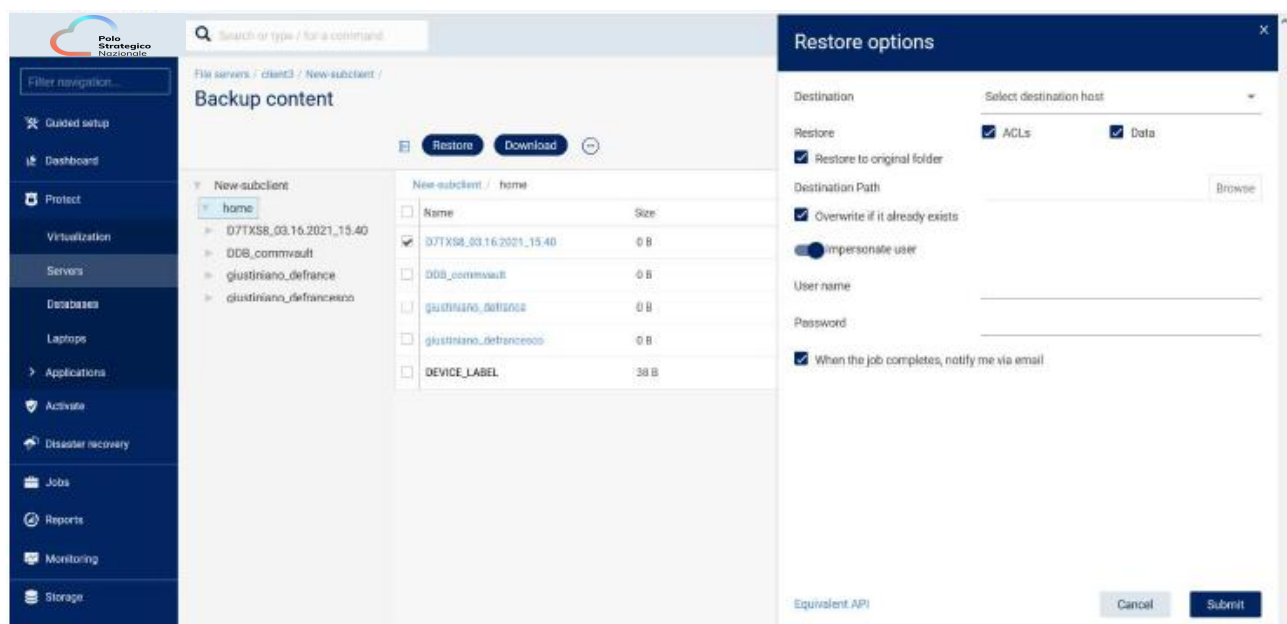
Quindi selezionare i dati che si vogliono *restorare* (si possono selezionare tutti i dati o solo alcuni dati puntuali a seconda del contesto oggetto di backup).



Procedura restore

Quindi è necessario selezionare le opzioni di restore ed in particolare scegliere se effettuare il restore sulla cartella originale, facendo attenzione al flag di overwrite a seconda se si vuole sovrascrivere i dati se già presenti, oppure effettuare un restore out-of-place e cioè su un'altra cartella rispetto a quella originaria e quindi scegliere la destination path dove effettuare il restore. È possibile anche scegliere un utente sulla macchina dove dovrà essere effettuato il restore con la relativa password. Infine, si può scegliere di ricevere una mail al completamento del job di restore.

Nel caso in cui si stia effettuando un restore di tipo Guest Files da un backup di una virtual machine Linux è necessario che la user da selezionare sia la User root della VM oggetto di restore.



Procedura restore

Dopo aver impostato i dati opzionali è necessario selezionare il tasto *submit* per eseguire il job di restore.

Le operazioni sono analoghe per gli altri contesti di dati (VM, database, ecc.) da sottoporre a backup.

14 Encryption

Il servizio di Backup PSN prevede, tramite software Commvault, l'encryption dei dati e si basa su due elementi principali:

1. Encryption dei dati a livello storage: i dati vengono crittografati a livello di storage policy (plan) tramite algoritmo AES-256.

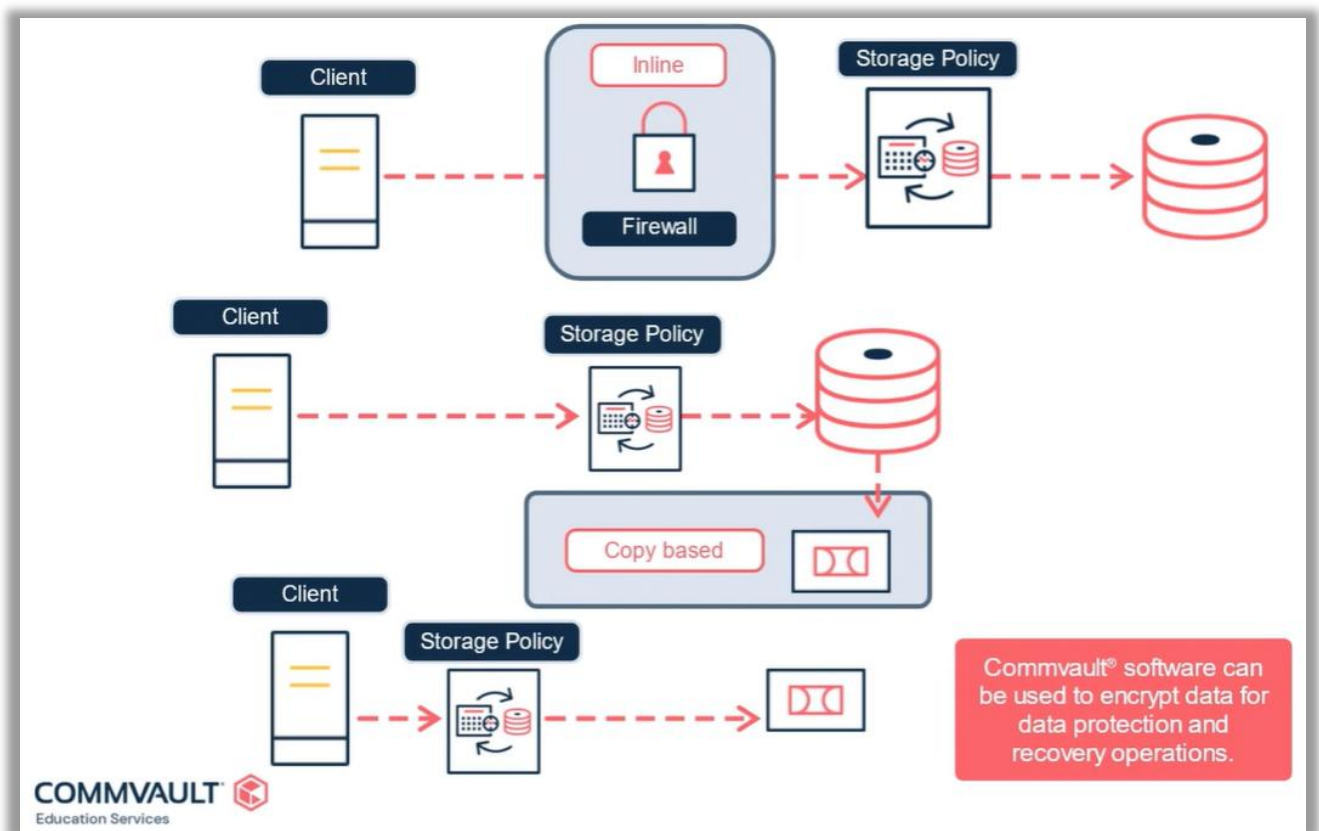


Figura 57 – Overview Encryption

2. Encryption dei dati in transito: sulle topology previste, i dati vengono trasmessi in maniera crittografata.

15 Best Practices & Troubleshooting

La protezione dati per i servizi IaaS Industry Standard (vOrg vCloud) prevede di default l'attivazione di una configurazione standard con una schedulazione di base preconfigurata per una quantità complessiva di 100GB di backup a VM (es. 2VM con 50GB e 150GB risultano entrambe protette con la schedulazione di base, in quanto la somma dei GB rientra dei 200GB garantiti).

In caso di Backup a CONTRATTO è necessario personalizzare il servizio configurando opportunamente cosa sottoporre a backup (virtual machine, filesystem, DB, ecc.) con specifici VMGROUP o SUBCLIENT ([#Aggiunta e configurazione VM group](#)) per raggruppare gli oggetti e organizzare la pianificazione a seconda delle esigenze di backup anche al fine di migliorare le prestazioni dei jobs (al capitolo [Pianificazione schedulazione dei job di backup](#) è descritta la modalità per modificare l'orario di partenza dei jobs di backup che è opportuno differenziare per ognuno dei VMGROUP/SUBCLIENT per evitare sovrapposizioni).

Una volta definito il proprio piano di dataprotection è consigliata la rimozione della schedulazione "backup standard" al fine di evitare sovrapposizioni.

Il servizio è unmanaged è quindi importante che il cliente segua le linee guida sotto riportate, per garantire la protezione dei propri dati in modo efficiente ed affidabile.

1. Eseguire controlli giornalieri sui log dei job di backup per individuare eventuali errori ricorrenti ed in caso di errore, procedere se necessario con una esecuzione manuale per recuperare il restore point fallito onde evitare la mancanza di punti di ripristino.
2. Verificare settimanalmente la disponibilità dei punti di ripristino attesi.
3. Mantenere aggiornati i filtri e i target di backup nei VM Group.
4. Verificare che le schedulazioni non si sovrappongano per evitare conflitti di esecuzione.
5. Per i backup Industry Standard, assicurarsi che i datastore abbiano sempre il 10% dello spazio disponibile per le snapshot.
6. Eseguire periodicamente la consolidazione dei dischi delle VM per evitare l'accumulo di snapshot obsolete.

Di seguito sono elencati i messaggi di errore (failure reason) più frequenti nel caso di insuccesso di backup su IaaS Industry, rilevabili dal report “Backup Job Summary”, la cui consultazione e schedulazione è disponibile dalla sezione Report della console.

Nel caso di fallimenti ricorrenti che non rientrano nelle casistiche sotto riportate e che compromettano più dell'80% dei job schedulati si prega di attivare il supporto (vedi FAQ [#Come posso richiedere assistenza per il servizio?](#)), diversamente si può fare riferimento alla documentazione commvault disponibile online prima di attivare il supporto (vedi riferimenti al paragrafo [2.1 Documentazione](#))

1. *Virtual Machine was not found*

- Causa: Il target backup inserito nel VM Group non è esistente.
- Risoluzione: Verificare il corretto contenuto del VM Group in quanto potrebbero essere configurate risorse non più esistenti.

2. *[*] No virtual machines were discovered for [*]. Check the content and filters. Source: , Process: vsdiscovery*

- Causa: Il VM Group è vuoto; non ci sono target di backup che rispondono ai criteri di filtro impostati per il VM Group (es. company appena deliverata senza VM create nell' organization).
- Risoluzione: Verificare la configurazione del VM Group inserendo i target di backup.

3. *Can not create a snapshot when another task is already running*

- Causa: Sovrapposizione delle schedulazioni per lo stesso target.
- Risoluzione: Verificare le corrette schedulazioni dei VM Group per evitare conflitti.

4. *Insufficient free space available to create a snapshot of the virtual machine*

- Causa: Il datastore non ha spazio sufficiente per effettuare la snapshot (10% deve essere riservato per snapshot).
- Risoluzione: per Industry Standard, assicurarsi che almeno il 10% dello spazio su datastore sia riservato agli snapshot per consentire il corretto funzionamento del backup.

5. The virtual machine reports that it has virtual disks that need consolidation and this could not be performed automatically

- Causa: Troppe snapshot richieste per i dischi della VM.
- Risoluzione: Forzare un disk consolidation sulla VM dalla console IaaS.

6. Unable to create a snapshot on virtual machine [*] because another task is already running on the virtual machine. The job will go to pending and be retried. Source: psnbckcmsdcac, Process: JobManager**

- Causa: Troppe snapshot richieste per i dischi della VM.
- Risoluzione: Verificare le snapshot attive sulle VM dalla console di IaaS ed eliminarle se necessario.

7. Client is already being backed up by job [*] from parent job [*]

- Causa: Il job precedente di backup è ancora in esecuzione.
- Risoluzione: Verificare il motivo della sovrapposizione dei job dipendenti e pianificare le schedulazioni in modo ottimale.

Durante l'attività di troubleshooting sui job Failed è utile accedere alla sezione "Error Summary" presente nella pagina di dettaglio del singolo job, in tale sezione è anche presente il link alla knowledge base di commvault.

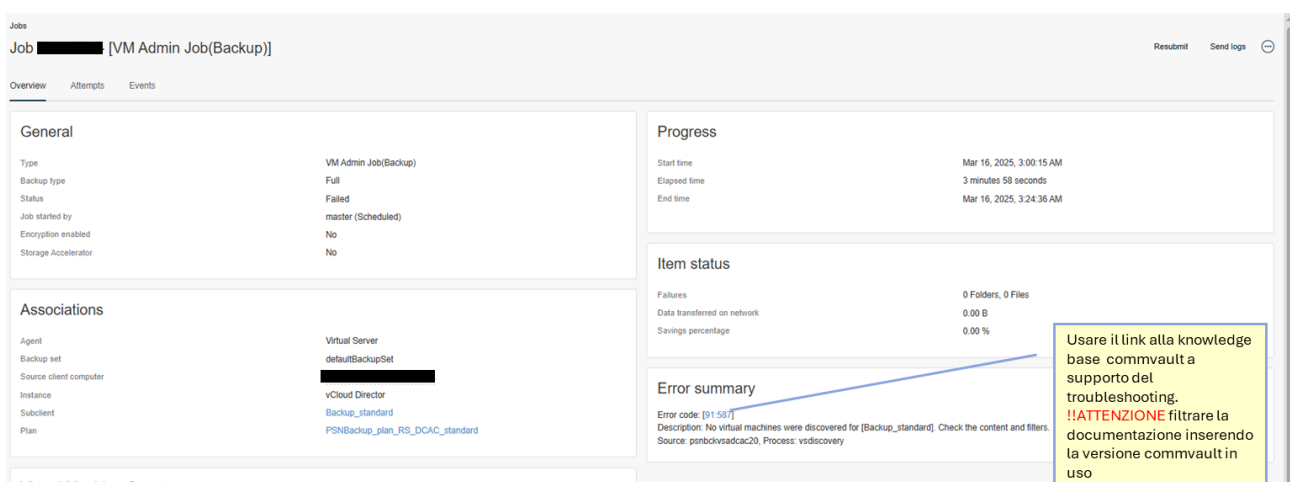


Figura 58 – Knowledgebase Job Error

16 Punti di attenzione

DB cluster non nativi: Non è possibile configurare backup a più nodi di postgres o più genericamente DB che non abbiano una gestione del cluster nativa. In presenza di qualsiasi middleware per la gestione del cluster (ad es. PGPOOL) non è certificata e possibile la configurazione del backup.

Vmware independent disks: Il backup tramite VMLImage di una VM non supporta i dischi independent per cui è necessario proteggere i dati presenti su tali dischi effettuando il backup dei dati tramite l'agent file server.

17 FAQ

17.1 *È possibile cancellare un job di backup per liberare spazio storage?*

Non è possibile cancellare i jobs di backup dalla console. Nel caso tale operazione dovesse essere comunque necessaria si può aprire un ticket al supporto con la richiesta di cancellazione fornendo tutti i dettagli in merito al/ai job/jobs da cancellare (job-id, data di esecuzione, ecc.).

17.2 *Come si cancellano i client?*

È possibile cancellare i client precedentemente configurati sulla console. La procedura per cancellare un client è la seguente:

1. Eseguire la Retire sul client (dal menu Protect a sinistra). Tale operazione effettuerà la disinstallazione del software sul client se il client risulta online altrimenti la disinstallazione dovrà essere effettuata manualmente direttamente sul Client da sistema operativo. Dopo la Retire il client sarà rimosso dalla scheda "Protect";
2. Selezionare il client ritirato dal menu Servers a sinistra (Selezionare "All" al posto di "Infrastructure" come filtro) e digitare "Delete" (Attenzione: il bottone "delete" è presente solo se tutto il software sul client è stato disinstallato con successo lato CommServe, altrimenti sarà presente l'opzione "Retire Client")

17.3 *È garantita la privacy? Come viene salvaguardato l'accesso ai dati?*

Il servizio garantisce la riservatezza dei dati non consentendo l'accesso e la visualizzazione dei dati dei clienti agli amministratori del servizio. In particolare, la visualizzazione e l'accesso ai dati è consentito solo all'utente amministratore del servizio che ha ricevuto le credenziali di accesso per l'utilizzo del servizio in fase di contrattualizzazione.

17.4 *Come posso richiedere assistenza per il servizio?*

È possibile richiedere assistenza tramite:

- Console di Gestione Servizi: <https://console.polostrategiconazionale.it>
- Numero verde 800776776

per segnalazioni riguardanti il malfunzionamento o il mancato raggiungimento della console di PSN Backup.

Trattandosi di un servizio *self-managed*, non sono invece inclusi nell'assistenza i servizi di configurazione del backup e di restore.