Realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale (“PSN”), di cui al comma 1 dell’articolo 33-septies del d.l. n. 179 del 2012

CUP: J51B21005710007

CIG: 9066973ECE

Manuale Utente - Managed Public Cloud Oracle

Data: 07/04/2025

PSN_Manuale Utente_v1.6

Ed. 7 - ver. 1.6

INTERNAL USE

QUESTA PAGINA È LASCIATA INTENZIONALMENTE BIANCA

INTERNAL USE

STATO DEL DOCUMENTO

TITOLO DEL DOCUMENTO			
Manuale Utente Managed Public Cloud Oracle			
EDIZ.	REV.	DATA	AGGIORNAMENTO
1	1.0	14/12/2023	Prima versione del documento
2	1.1	15/02/2024	Inserite nuove descrizioni in seguito ai feedback ricevuti dopo il collaudo di fase 1
3	1.2	26/02/2024	Aggiornate figure e introdotto capitolo 3
4	1.3	08/07/2024	Aggiornate modalità di accesso alla console OCI, modalità di configurazione network tramite Fastconnect, modalità di rotazione chiave e nuovo paragrafo 8 (Soluzione di DR)
5	1.4	09/10/2024	Aggiornata modalità richiesta nuova chiave EKM e par. 8
6	1.5	03/02/2025	Aggiornato par. 5.1.5 in merito alla modalità di rotazione di una chiave esterna su Autonomous DB e modalità creazione utenze secondarie. Aggiornato par. 5.1.3 ed eliminato par. 8
7	1.6	07/04/2025	Inserite note in merito alla creazione delle Fastconnect al par. 6.2.3, rinominato par. 5, ed inserita premessa. Inserito par. 9 Guida alla fatturazione

NUMERO TOTALE PAGINE:	41

AUTORE:	
Team di lavoro PSN	Unità operative Solution Development, Technology Hub e Sicurezza, Gruppo di lavoro PSN Managed – Oracle

REVISIONE:	
Referente del Servizio	Paolo Trevisan

INTERNAL USE

APPROVAZIONE:	
Direttore del Servizio	Antonio Garelli

INTERNAL USE

INDICE

INTERNAL USE

LISTA DELLE FIGURE

INTERNAL USE

LISTA DELLE TABELLE

INTERNAL USE

1. Definizioni e Acronimi

1.1 Definizioni

Definizione	Descrizione
PSN	È la nuova società che è stata costituita nell'ambito del progetto del Cloud Nazionale
TBC	Il tema è stato discusso ma è in attesa di conferma dalle parti coinvolte
TBD	Il tema non è ancora stato discusso

Tabella 1 – Glossario Definizioni

1.2 Acronimi

Acronimo	Descrizione
PSN	Polo Strategico Nazionale
VCN	Virtual Private Network
HA	Alta Affidabilità
VM	Virtual Machine
Baas	Backup As a Service
EKM	External Key Management
CSP	Cloud Service Provider
PA	Pubblica Amministrazione
OCI	Oracle Cloud Infrastructure
DWH	Datawarehouse
DRCC	Dedicated Region Cloud at Customer
IAM	Identity and Access Management
IDCS	Identity Cloud Service

Tabella 2 – Glossario Acronimi

INTERNAL USE

2. Executive Summary

2.1 Scopo del documento

Introduzione

Il presente documento contiene le principali istruzioni per svolgere attività di accesso e configurazione del servizio PSN Managed utilizzando la Console Oracle Cloud Infrastructure.

Prerequisiti

L'utente che vuole seguire le istruzioni di questo documento deve possedere una conoscenza e familiarità coi concetti Oracle Cloud.

Struttura del Documento

Le informazioni in questo documento riguardano:

- Accesso alla Console OCI
- Organizzazione risorse OCI
- Operazioni di accesso alle chiavi di cifratura
- Logging e Monitoring
- FAQ

3. Introduzione ai principali servizi di OCI

Oracle Cloud Infrastructure è una potente piattaforma cloud che offre una vasta gamma di funzionalità per supportare le aziende nel loro percorso verso la digitalizzazione. Essendo una piattaforma cloud, tutte le sue capacità sono accessibili attraverso internet, consentendo alle aziende di accedere e utilizzare risorse informatiche, come server, storage e servizi software, in modo flessibile e scalabile. Questo approccio cloud elimina la necessità di investimenti in hardware costoso e complesse operazioni di gestione, consentendo alle aziende di concentrarsi sullo sviluppo e l'innovazione dei loro prodotti e servizi.

Tra le sue capacità principali, spicca la scalabilità, che consente alle imprese di espandere o ridurre le risorse informatiche in base alle necessità del momento. La sicurezza è una priorità fondamentale, con misure avanzate di protezione dei dati e delle applicazioni. La flessibilità è

INTERNAL USE

un'altra caratteristica chiave di Oracle Cloud Infrastructure, che supporta una varietà di carichi di lavoro, dalle istanze di calcolo alle soluzioni di storage e database. Grazie alla sua architettura è in grado di integrarsi facilmente con le tecnologie esistenti e di supportare l'adozione di nuove soluzioni.

Inoltre, Oracle Cloud Infrastructure offre prestazioni elevate, grazie a un'infrastruttura avanzata e all'utilizzo di tecnologie all'avanguardia come il machine learning e l'intelligenza artificiale. Infine, la piattaforma è dotata di strumenti di monitoraggio e gestione avanzati, che consentono alle aziende di monitorare le prestazioni e ottimizzare l'utilizzo delle risorse in tempo reale.

Per ulteriori approfondimenti si rimanda alla documentazione ufficiale disponibile online.

3.1 Cloud Shell

Oracle Cloud Infrastructure (OCI) Cloud Shell è un terminale basato su browser Web accessibile da Oracle Cloud Console. Cloud Shell è gratuito (entro i limiti di tenant mensile) e fornisce l'accesso a una shell Linux, con una CLI Oracle Cloud Infrastructure pre-autenticata, un'installazione Ansible pre-autenticata e altri strumenti utili per eseguire svariate operazioni. Questa funzionalità è disponibile per tutti gli utenti OCI (che ovviamente dispongono dei permessi adeguati).

Cloud Shell crea:

- una macchina effimera da utilizzare come host per una shell Linux, preconfigurata con l'ultima versione di OCI Command Line Interface (CLI) e una serie di strumenti utili.
- 5 GB di spazio di archiviazione per propria home directory.
- Un frame persistente della Console che rimane attivo mentre si naviga tra le diverse pagine della Console.

RETE PRIVATA CLOUD SHELL
La rete privata Cloud Shell ti consente di connettere una sessione Cloud Shell a una rete privata in modo da poter accedere alle risorse in quella rete senza che il traffico fluisca sulle reti pubbliche. Esempi di casi in cui la rete privata può essere utile includono l'utilizzo su SSH in istanze di calcolo all'interno di una rete privata o la gestione di un cluster OKE privato.

Per accedere alla cloud shell cliccare sull'icona  in alto a destra e poi Cloud Shell, apparirà una finestra nella cloud console dove la shell sarà immediatamente disponibile.

Per ulteriori approfondimenti sulla vasta gamma di funzionalità della Cloud Shell si rimanda alla documentazione ufficiale Oracle.

INTERNAL USE

3.2 Immagini Compute

Un'immagine fornisce il sistema operativo e altro software per un'istanza di calcolo. L'immagine da utilizzare va specificata al momento della creazione di un'istanza di calcolo.

Di seguito sono elencati i tipi di immagini che si possono utilizzare per creare un'istanza di calcolo:

- Platform images: che include immagini Oracle Linux e Oracle Solaris. Queste immagini sono disponibili in ogni compartimento di ogni tenancy. Non è necessario scaricare o importare queste immagini per accedervi e creare un'istanza. Al momento della stesura della presente versione del manuale non sono disponibili immagini con licenze di terze parti (Windows, RH, ecc.). Per usufruire di server con tali immagini è possibile importare Custom Images. Consulta la documentazione per ulteriori dettagli.
- Custom images: in OCI è possibile creare un'immagine personalizzata del boot disk (disco di avvio) di un'istanza di calcolo e utilizzarla per creare altre istanze di calcolo. Le istanze create dalla custom image includono le personalizzazioni, la configurazione e il software installato al momento della creazione dell'immagine. Vedi gestione delle custom images.
- Bring your own image (BYOI): in OCI è possibile importare le proprie versioni di immagini purché l'hardware sottostante lo supporti. Consulta Bring Your Own Image (BYOI) per ulteriori dettagli.

Per un elenco dei sistemi operativi testati da Oracle, consulta Guest Operating Systems.

3.3 Exadata

Oracle Exadata è una piattaforma di database aziendale che esegue carichi di lavoro Oracle Database di qualsiasi dimensione e criticità con prestazioni, disponibilità e sicurezza elevate. Il design a scalabilità orizzontale di Exadata sfrutta ottimizzazioni uniche che permettono a elaborazione delle transazioni, analytics, machine learning e carichi di lavoro misti, di essere eseguiti in modo più rapido ed efficiente. Consolidare diversi carichi di lavoro di Oracle Database sulle piattaforme Exadata nei data center aziendali, in Oracle Cloud Infrastructure (OCI) e negli ambienti multi-cloud consente alle organizzazioni di aumentare l'efficienza operativa, ridurre l'amministrazione IT e abbassare i costi.

Dopo aver creato l'Exadata Infrastructure, in base alle risorse acquistate tramite PPFF, è possibile procedere alla creazione dei database, che possono basarsi su:

1. VM Cluster, database Oracle su VM cluster ritagliati a seconda dei workload. Per ulteriori dettagli fare riferimento alla documentazione relativa a Oracle Exadata Database Service on Dedicated Infrastructure.
2. Autonomous Database su infrastruttura dedicata.

INTERNAL USE

3.4 Fingerprint

Per recuperare il fingerprint associato ad una VM seguire i successivi step:

1. Accedere alla Cloud Shell, selezionare il relativo tasto in alto a sinistra dalla console di OCI e cliccare Cloud Shell.

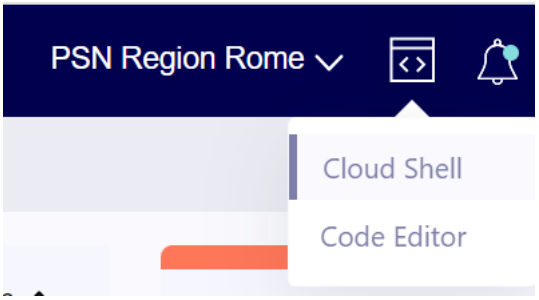

Figura 1 – Accesso Cloud Shell

2. Connettersi alla rete OCI dove si trova la VM in questione, nella finestra della cloud shell selezionare Network e poi Ephemeral private network setup.

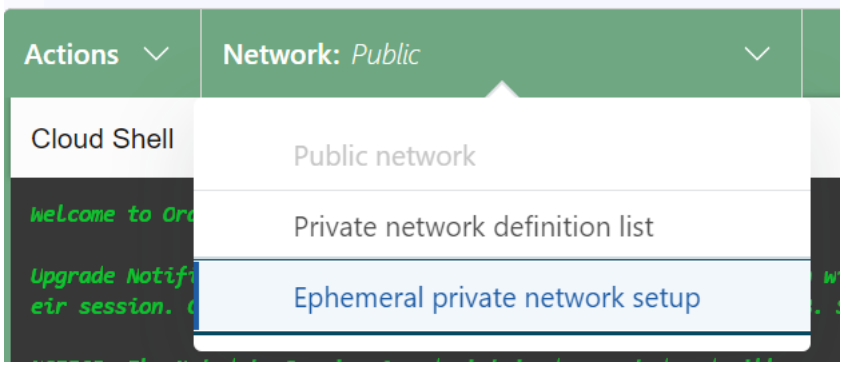

Figura 2 – Cloud Shell setup

A questo punto si aprirà una finestra dove occorre selezionare la vcn e la subnet dove si trova la VM in questione.

INTERNAL USE

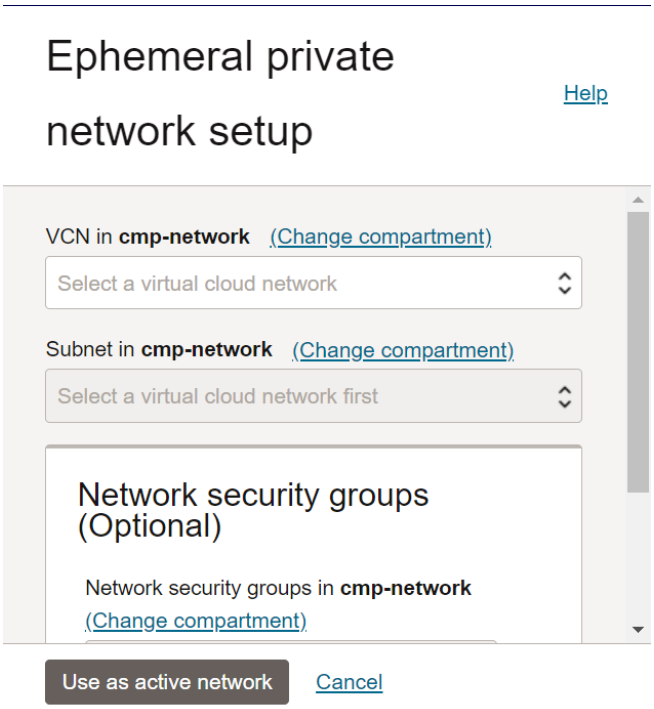

Figura 3 – Ephemeral private network setup Cloud Shell

3. Terminata la fase di caricamento della rete, recuperare l'IP della VM e lasciare il seguente comando:
   ssh opc@<IP-VM>
4. Verrà mostrato a video il fingerprint, che è verificato in quanto ci si sta collegando dalla VCN privata che sta direttamente nella rete di OCI.

INTERNAL USE

3.5 Auth token

I token di autenticazione sono stringhe token generate da Oracle che si possono utilizzare per eseguire l'autenticazione con API di terze parti che non supportano l'autenticazione basata sulla firma di Oracle Cloud Infrastructure. Ogni utente creato nel servizio IAM ha automaticamente la possibilità di creare, aggiornare ed eliminare i propri token di autenticazione nella console o tramite API. Non è necessario che un amministratore crei una policy per fornire a un utente tali permessi. Gli amministratori (o chiunque abbia l'autorizzazione per la tenancy) hanno anche la possibilità di gestire i token di autenticazione per altri utenti.

Non è possibile modificare il token di autenticazione in una stringa personalizzata poiché esso è sempre una stringa generata da Oracle.

I token di autenticazione non scadono. Ogni utente può avere fino a due token di autenticazione alla volta. Per ottenere un token di autenticazione dalla Console si rimanda alla documentazione ufficiale Oracle per la procedura di creazione di un Auth Token.

INTERNAL USE

4. Descrizione del servizio

4.1 Caratteristiche

Il servizio PSN Managed Oracle Cloud aiuta ad affrontare la sovranità digitale con le seguenti caratteristiche:

- Separazione fisica e/o logica dei workloads e dei rispettivi dati (Sovranità dei dati)
- Ispezionabilità per garantire i controlli di conformità (Trasparenza sui dati)
- Residenza dei dati e workload in EU/Italia (Residenza dei dati)
- Supporto locale con personale PSN

Nella figura seguente è rappresentata l'architettura complessiva del servizio PSN Managed Oracle Cloud.

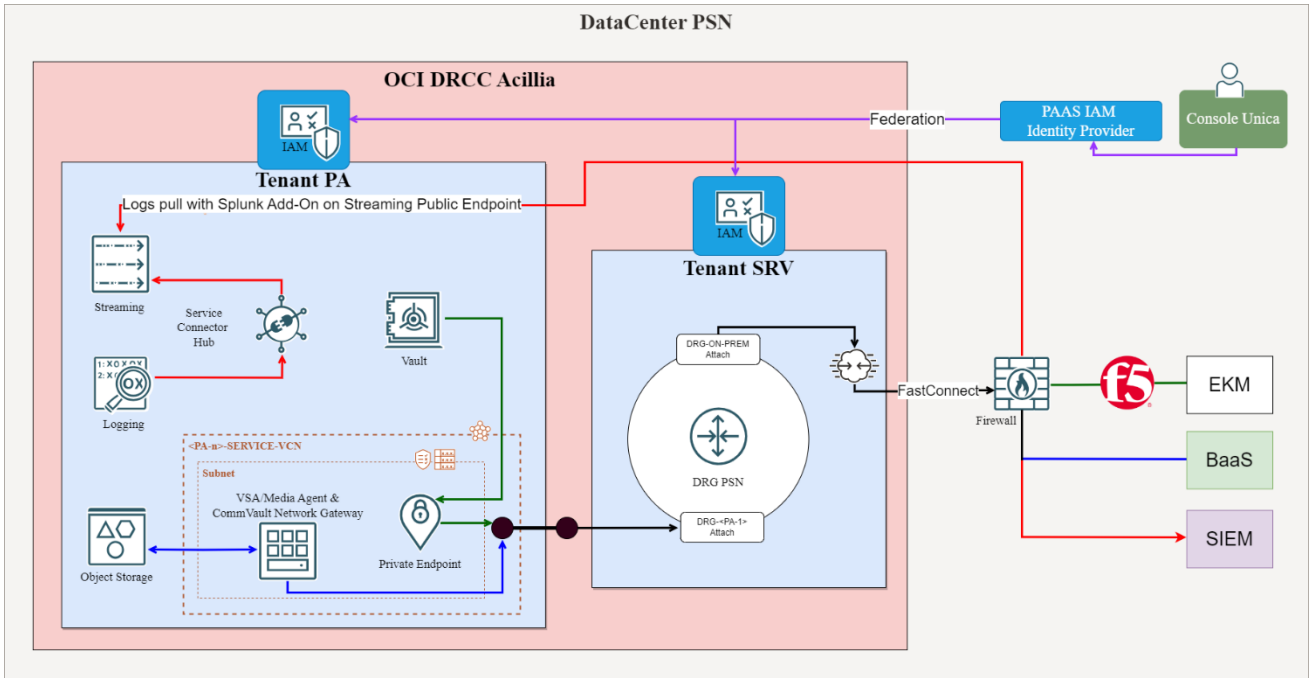

Figura 4 – Architettura generale

INTERNAL USE

4.2 Prerequisiti

Il rilascio dell'ambiente PSN Managed Oracle richiede al cliente di progettare e configurare, con l'eventuale supporto del Servizi Professionali, il proprio ambiente Cloud.

I servizi sotto riportati non richiedono particolari prerequisiti, in quanto gestiti interamente da PSN:

- Chiavi di crittografia dei dati at-rest (KMS)
- Gestione delle utenze con accesso al servizio (IDP)
- Monitoraggio dei log di sicurezza (SIEM)
- Configurazione del servizio BaaS CommVault (servizio opzionale)

I servizi e le risorse implementabili nel proprio ambiente Cloud sono pressocchè limitate (tramite Service Limits e size quote) ai servizi acquistati tramite PPFF. L'incremento di questi limiti può essere effettuato tramite variazione del PPFF.
Anche se al momento della pubblicazione del presente manuale non sono presenti a listino PSN tutti i servizi OCI (come ad esempio il servizio Compute), ne vengono comunque descritte alcune funzionalità e l'integrazione con i servizi PSN.

5. Guida all'utilizzo della console

Con riferimento all'utilizzo della console di cui al presente capitolo, in ragione dell'oggetto del Contratto di Utenza e dei relativi allegati, incluso il Progetto dei Piani dei Fabbisogni ("PPDF") ("Contratto"), l'Amministrazione Utente deve attivare esclusivamente quegli elementi presenti nel Listino pubblicato nell'area del sito istituzionale di Polo Strategico Nazionale e che trovano una corrispondenza nell'ambito dei Servizi oggetto di Contratto.

Resta inteso che, nel caso di violazione di quanto sopra, PSN:

- sarà legittimata, previa comunicazione all'Amministrazione Utente, alla disattivazione di quegli elementi indebitamente attivati, mettendosi a disposizione, per quanto possibile, per l'identificazione ed attivazione di soluzioni alternative.

- non sarà in alcun modo responsabile dell'utilizzo o del funzionamento di quegli elementi indebitamente attivati dall'Amministrazione Utente.

INTERNAL USE

5.1 Accesso alla console OCI

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

Per accedere alla console OCI del servizio PSN Managed Oracle Cloud è necessario connettersi al portale unico tramite le credenziali ricevute con la Welcom Letter:
https://console.polostrategiconazionale.it

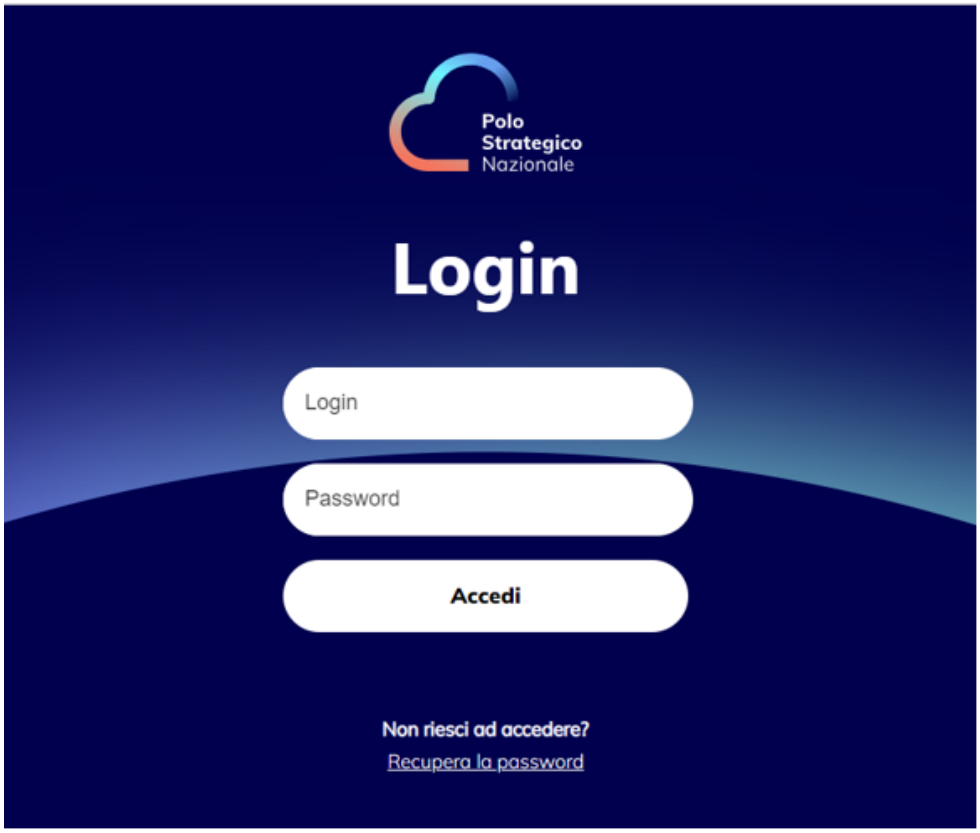

Figura 5 – Schermata login della cloud console

NB per accedere occorre inserire un PIN (MFA) ricevuto sull'utenza di posta associata alla propria utenza.

Dal portale è possibile cliccare su *Console OCI* ed accedere in modalità SSO senza dover reinserire le credenziali.

INTERNAL USE

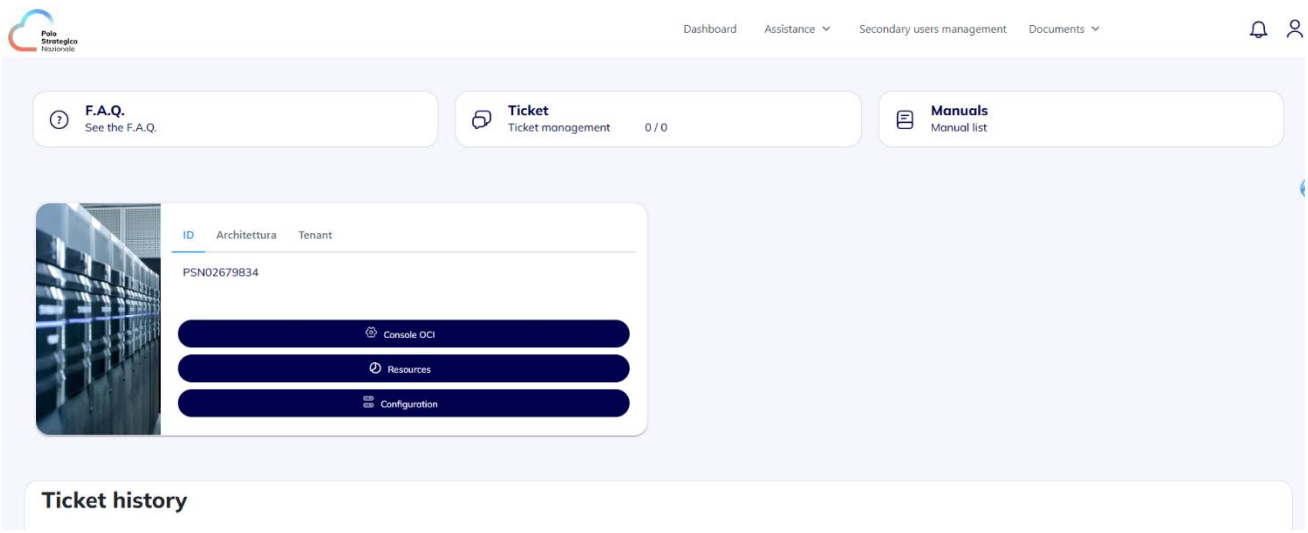

Figura 6 - Console PSN

Accesso alla console OCI:

1. inserire nome tenancy e cliccare Continua.

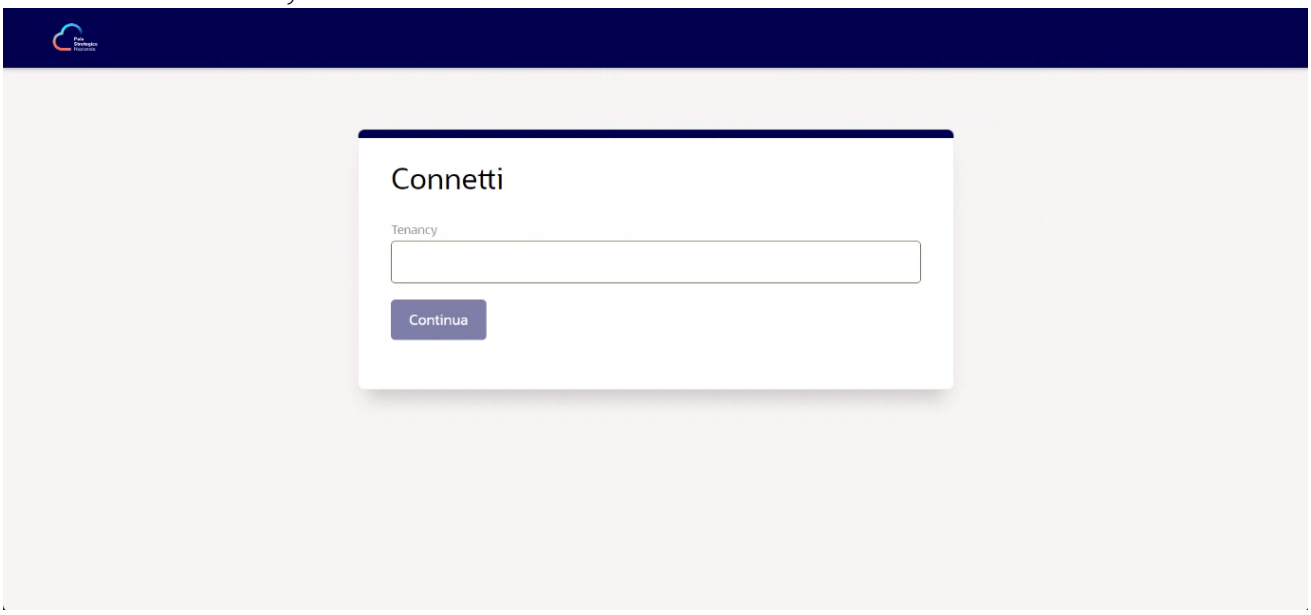

Figura 7 - Sign in inserimento Tenancy name

2. In Sign in with an identity domain selezionare il domain domain_psn e poi Next.

INTERNAL USE

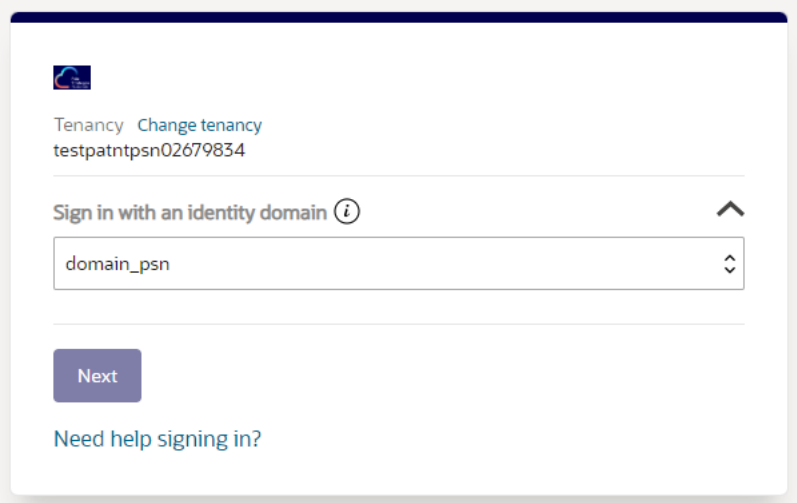

Figura 8 - Sign in selezione domain

A questo punto si arriverà sulla home page della console di OCI:

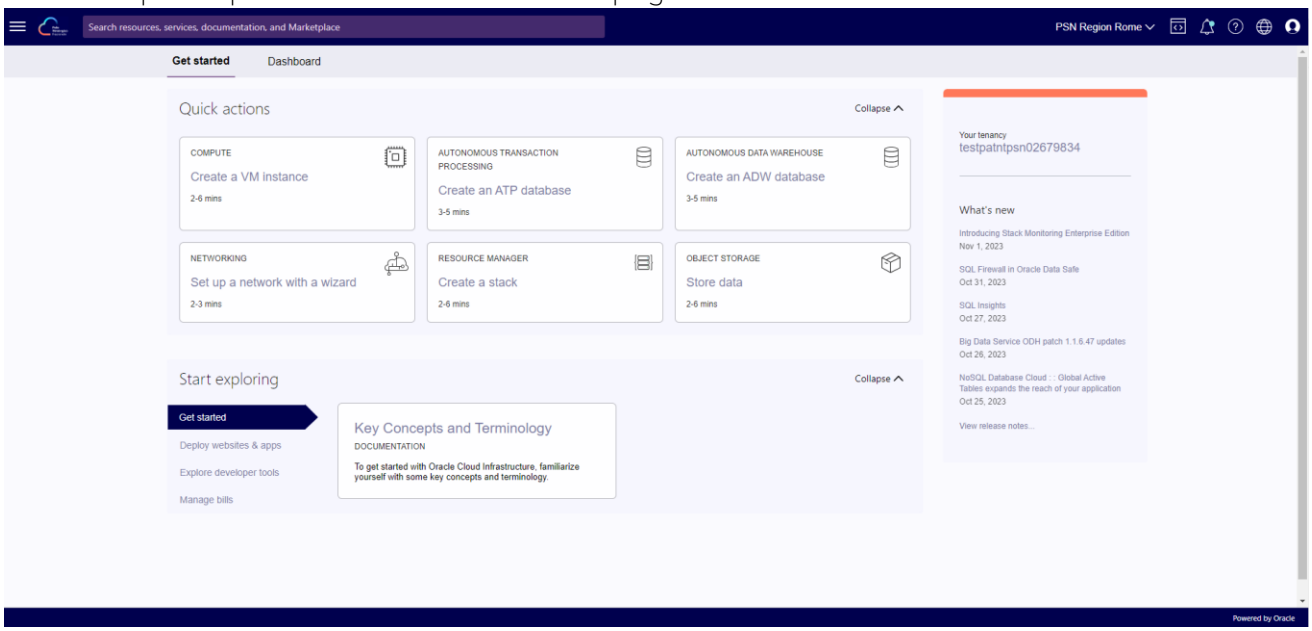

Figura 9 - Home Page Oracle Cloud console

Se non si ha necessità di accedere preventivamente alla console PSN, si può entrare tramite link diretto:

INTERNAL USE

https://cloud.psn-pco.it/

inserire come nel caso precedente il tenancy acquistato, selezionare il domain_psn ed inserire le credenziali nella home page della Console OCI dedicata:

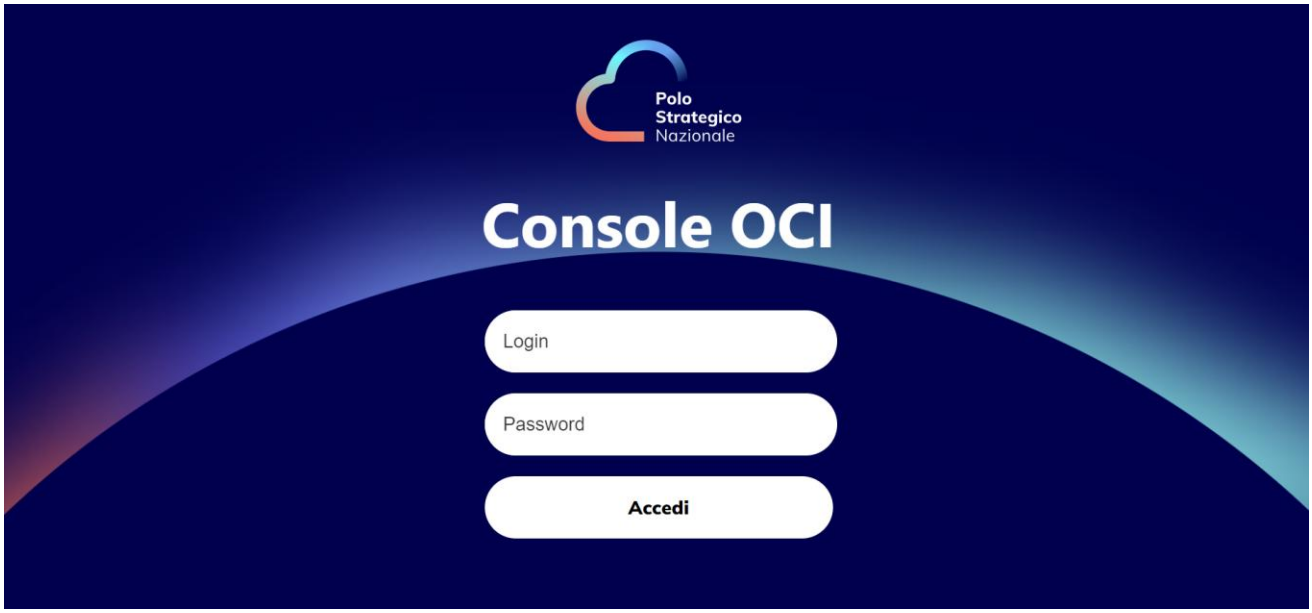

Figura 10 - Home Page PSN Oracle Cloud console

INTERNAL USE

6. Oracle Cloud Infrastructure

6.1 Organizzazione delle risorse

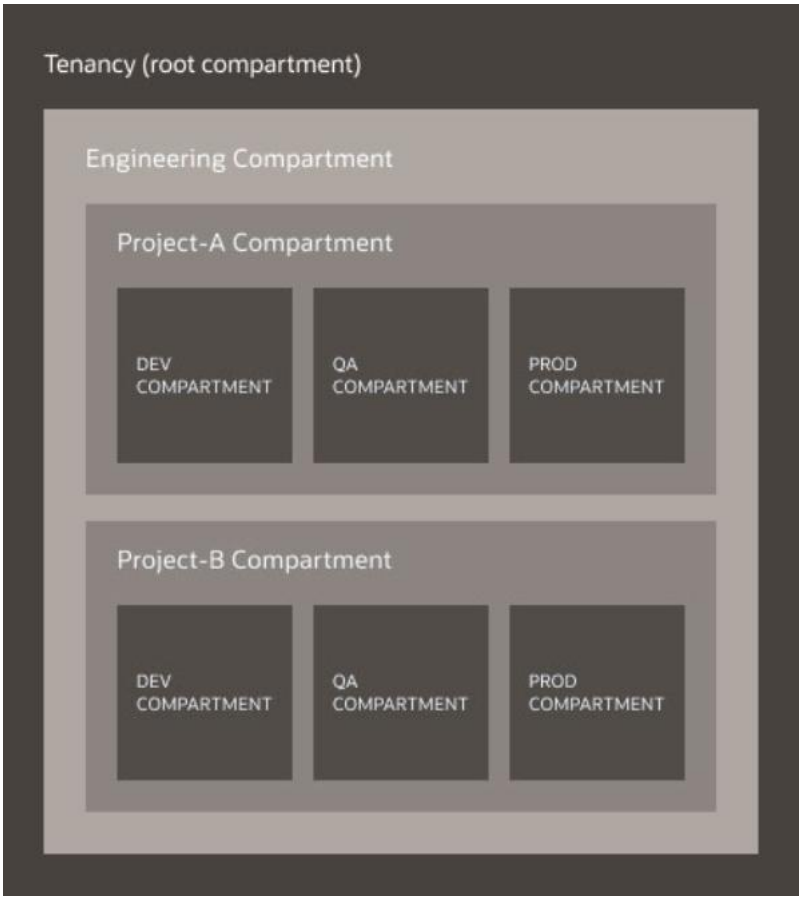

Figura 11 - Tenancy root

REGIONE

Oracle Cloud Infrastructure (OCI) è ospitato in regioni e domini di disponibilità (Availability Domain – AD). Una regione è un'area geografica localizzata, un dominio di disponibilità è costituito da uno o più data center situati all'interno di una regione.

I domini di disponibilità sono isolati gli uni dagli altri, tollerano gli errori ed è molto improbabile che si guastino simultaneamente. Poiché i domini di disponibilità non condividono infrastrutture quali alimentazione o raffreddamento oppure la rete interna, è improbabile che un guasto in un dominio di disponibilità all'interno di un'area influisca sulla disponibilità degli altri all'interno della stessa area. Le regioni sono indipendenti tra di loro e possono essere separate da grandi distanze – attraverso paesi o addirittura continenti. In genere, un'applicazione viene distribuita

INTERNAL USE

nell'area in cui viene utilizzata maggiormente. Tuttavia, puoi anche distribuire applicazioni in regioni diverse per i seguenti motivi:

- per mitigare il rischio di eventi a livello regionale come eventi meteorologici o terremoti.
- Per soddisfare i diversi requisiti di giurisdizioni legali, ambiti fiscali e altri criteri aziendali o sociali.

REGNO
Le regioni sono raggruppate in regni. Ciascun Tenancy esiste in un singolo regno e può accedere a tutte le regioni che appartengono a quel regno.

TENANCY
Una Tenancy è una partizione sicura e isolata all'interno dell'infrastruttura cloud. La tenancy è un concetto logico, la si può considerare come un container root in cui creare, organizzare e amministrare le risorse cloud.

COMPARTMENT
Il secondo concetto logico usato per organizzare e controllare l'accesso alle risorse cloud è il compartment. Un compartimento è una raccolta di risorse cloud correlate. La tenancy è anche il compartimento radice.

Si possono creare altri compartimenti all'interno della tenancy (fino a sei livelli di profondità) e usare i criteri (policy) corrispondenti per controllare l'accesso alle risorse in ogni compartimento. Ogni volta che viene creata una risorsa cloud, occorre specificare il compartimento in cui collocarla.

La figura sopra riportata mostra un compartimento denominato Engineering all'interno del compartimento radice. Il compartimento Engineering dispone di due compartimenti secondari (per Project-A e Project-B) e ognuno di questi compartimenti è ulteriormente separato in più compartimenti.

Questa struttura isola le risorse tra ambienti (sviluppo, garanzia di qualità, produzione) e progetti diversi. Attraverso i criteri (policy) è possibile definire gli amministratori per ogni compartimento. La creazione di criteri con filtro più avanzato garantisce agli utenti l'accesso ai compartimenti di cui hanno bisogno e che le risorse possano connettersi tra loro.

DOMINIO DI IDENTITÀ
Un dominio di identità è un contenitore per la gestione di utenti e ruoli, federazioni e provisioning di utenti, integrazione sicura delle applicazioni tramite la configurazione Oracle Single Sign-On (SSO) e l'amministrazione OAuth. Rappresenta una popolazione di utenti nell'infrastruttura Cloud e le relative configurazioni e impostazioni di sicurezza associate (come MFA).

RISORSA

INTERNAL USE

Una risorsa è un oggetto cloud creato e utilizzato durante l'interazione con i servizi Cloud. Ad esempio, istanze di calcolo, volumi di storage a blocchi, reti cloud virtuali (VCN), sottoreti, database, applicazioni di terze parti, applicazioni Software-as-a-Service (SaaS).

6.2 Tenant PA OCI

Accedendo al proprio tenant OCI, ciascuna PA potrà creare all'interno dell'ambiente cloud tutti i servizi che ha richiesto nel Piano dei Fabbisogni.

6.2.1 Compartment gestito da PSN

Ogni tenant reso disponibile alle PA, avrà preconfigurato un compartment chiamato "cmp-servicecompartment" all'interno del quale sono configurati i servizi gestiti dal PSN. In questo compartment sarà visibile ed accessibile solo un sotto-compartment dedicato alla sicurezza, chiamato "cmp-security"; nel quale sarà configurato il vault dell'EKM nella misura della creazione e rotazione delle chiavi secondo la normale prassi OCI; il ciclo di vita delle chiavi è gestito dal PSN. La configurazione dell'EKM è gestita esclusivamente da PSN, le PA potranno liberamente utilizzare le chiavi per crittografare qualsiasi risorsa OCI. Le PA potranno, invece, gestire in maniera autonoma i secret all'interno del vault (creazione/cancellazione).

6.2.2 Compartment gestiti dall'utente

Per raggiungere un alto livello di standardizzazione con attenzione alla sicurezza, nel Tenant viene utilizzata la configurazione di compartment e gruppi della "OCI Enterprise Landing Zone v2". Il Referente Tecnico, parte del gruppo TenancyAdministrators, potrà aggiungere gli utenti nei vari gruppi a seconda del loro ruolo, tramite console PSN.
Per questione di sicurezza è stata inibita la possibilità di creare nuove utenze e policy direttamente da console OCI. Per particolari esigenze (ad es. creazione di service account) il referente tecnico può aprire un ticket di nuova utenza specificandone la natura e le policy da impostare.

Nelle tabelle che seguono sono elencati i compartment e i gruppi preconfigurati e che potranno essere utilizzati dal cliente:

- *Compartment*

Parent Compartment	Compartment	Descrizione
Root	cmp-network	CIS Landing Zone compartment per tutte le risorse correlate alla rete: VCNs, subnets, network

INTERNAL USE

		gateways, security lists, NSGs, load balancers, VNICs, ecc.
Root	cmp-security	CIS Landing Zone compartment per tutte le risorse relative alla sicurezza: vault, topic, notifiche, logging, scanning, ecc.
Root	cmp-appdev	CIS Landing Zone compartment per tutte le risorse relative allo sviluppo di applicazioni: compute instances, storage, function, OKE, API Gateway, streaming, ecc.
Root	cmp-database	CIS Landing Zone compartment per tutte le risorse correlate ai database.
Root	cmp-exinfra	CIS Landing Zone compartment per l'infrastruttura Exadata Cloud Service.

Tabella 3 – Compartment Tenant PA

- *Gruppi*

Nome	Descrizione
_tenancyAdministrators	Gruppo di appartenenza del referente tecnico.
iam-admin-group	CIS Landing Zone gruppo per la gestione delle risorse IAM nel tenant.
cred-admin-group	CIS Landing Zone gruppo per la gestione delle credenziali degli utenti nel tenant.
network-admin-group	CIS Landing Zone gruppo per la gestione della rete.
security-admin-group	CIS Landing Zone gruppo per la gestione dei servizi di sicurezza.
appdev-admin-group	CIS Landing Zone gruppo per la gestione dei servizi correlati allo sviluppo di app.
database-admin-group	CIS Landing Zone gruppo per la gestione dei database.
exainfra-admin-group	CIS Landing Zone gruppo per la gestione dell'infrastruttura Exadata Cloud Service.

INTERNAL USE

storage-admin-group	CIS Landing Zone gruppo per la gestione dei servizi di storage.
auditor-group	CIS Landing Zone gruppo per l'auditing nel tenant.
announcement-reader-group	CIS Landing Zone gruppo per la lettura degli annunci della console.

Tabella 4 - Gruppi Tenant PA

6.2.3 *Gestione VCN e Network*

Nell'ambito dei propri compartment il Cliente ha la possibilità di creare tutti i servizi di rete e di sicurezza che ritiene opportuno implementare. L'erogazione dei propri servizi potrà avvenire sia su internet (con e senza VPN IP Sec) che su reti completamente private (MPLS/Fastconnect).

Per l'erogazione su internet il cliente è completamente autonomo, mentre nel caso abbia richiesto connettività privata occorre aprire un ticket di supporto verso gli operatori PSN per effettuare la configurazione necessaria.

Nota: la VCN di erogazione deve avere un indirizzamento compatibile con la VCN di servizio e la rete on-premises del PSN. Per evitare overlapping con le reti di servizio e management è indispensabile non utilizzare le seguenti classi riservate al PSN:

- 100.65.0.0/16
- 198.18.227.0/24
- 10.59.75.0/26
- 10.49.75.0/26

Di seguito gli step operativi per creare un collegamento Fastconnect:

In prima istanza occorre creare un DRG nel compartment di network come indicato nella figura seguente:

INTERNAL USE

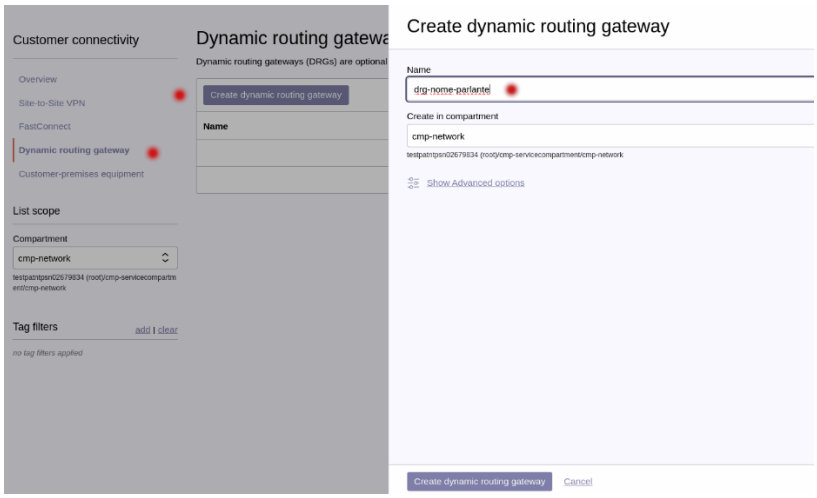

Figura 12 - Pannello creazione DRG

Creare una connessione tramite Fastconnect Partner (PSN_tim-noovle_private_erg)

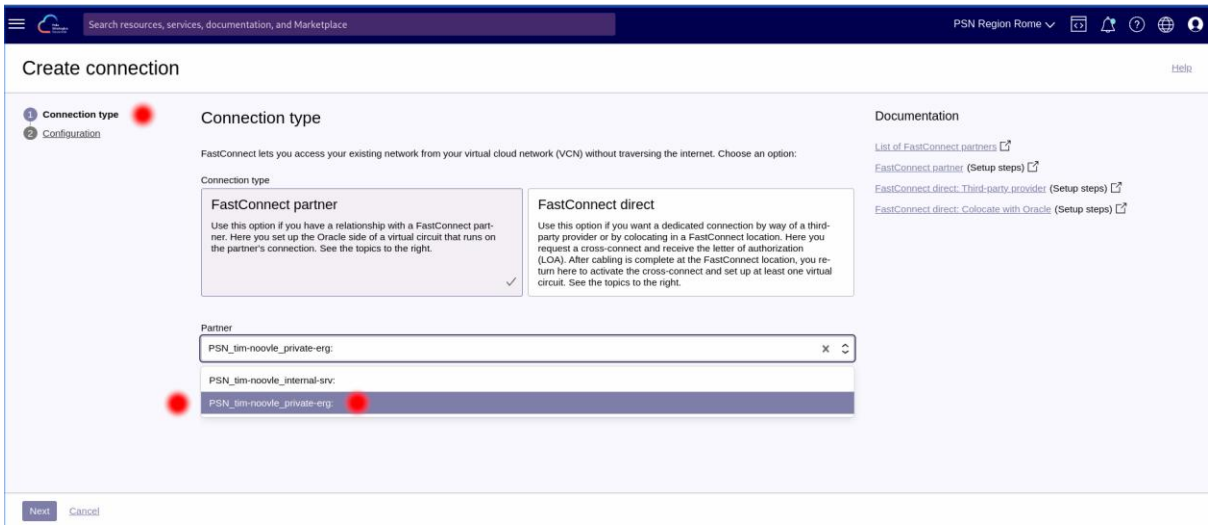

Figura 13 - Pannello creazione Connection Fastconnect (1/2)

Proseguire inserendo i parametri contrassegnati col pallino rosso

INTERNAL USE

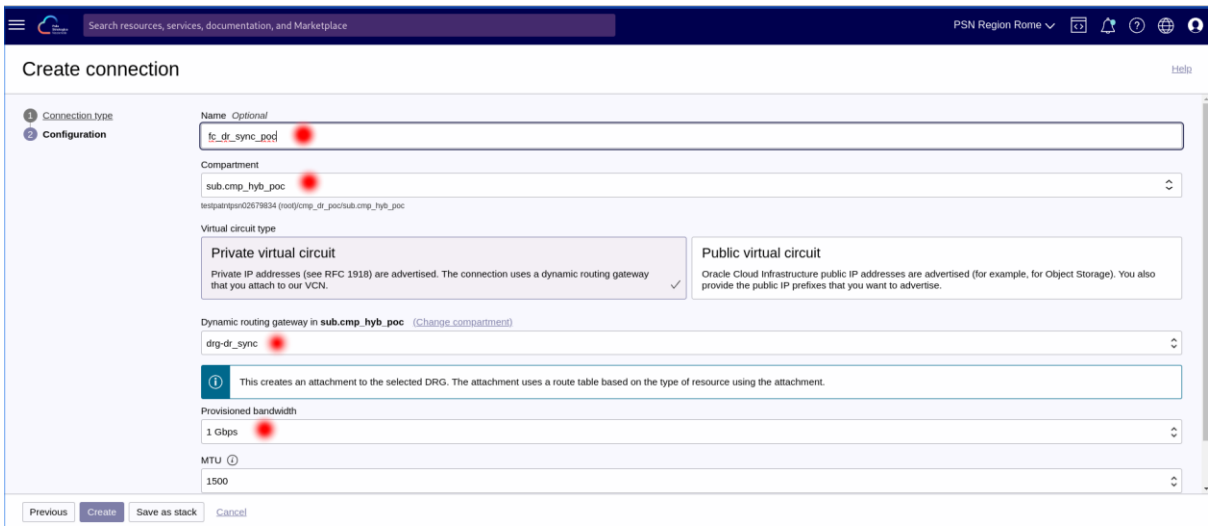

Figura 14 - Pannello creazione Connection Fastconnect (2/2)

NB: Si chiede di rispettare, per il nome della FastConnect, la seguente naming convention: fc-prv-<nomecliente>-psn<0xyzsp>
La bandwidth da inserire è quella contrattualizzata. Nel caso si inserisse una banda più elevata verrà comunque addebitata in fattura.

Alla fine della configurazione lo stato della connessione risulterà pending partner:

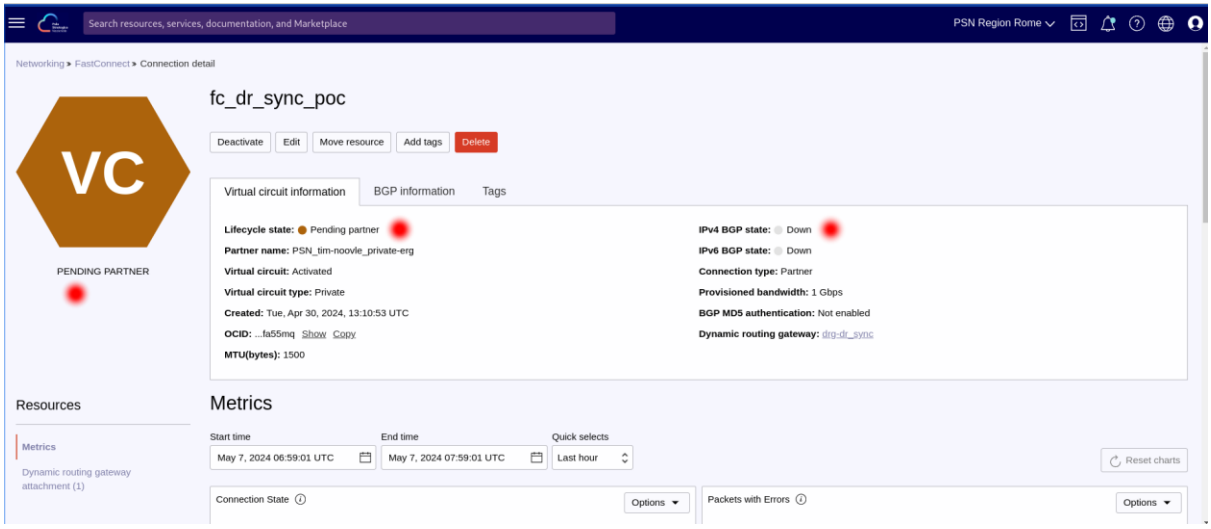

Figura 14 – Dettaglio Connessione

Per completare la configurazione occorrerà aprire una segnalazione al PMCA del servizio, dettagliando la configurazione effettuata, in modo che un operatore PSN possa completare la configurazione di rete richiesta.

INTERNAL USE

A valle dell'attivazione verificare tutti i collegamenti di rete (attachment, routing, security list) necessari ad instradare correttamente il traffico verso il collegamento Fastconnect/MPLS.
N.B. l'implementazione del collegamento Fastconnect non abilita automaticamente il traffico tra sorgenti e destinazioni, ma occorre verificare tutte le rotte sia lato OCI (come indicato in precedenza), ma anche all'altro estremo (IaaS, CaaS o onpremise)

Per l'implementazione di alcuni servizi, come ad esempio i DB su infrastruttura Exadata, o per utilizzare chiavi esterne, occorre prevedere all'interno della tabella di routing della VCN, la rotta verso un Service Gateway:

Figura 15 - Pannello configurazione Rotte

6.2.4 *Gestione Utenze*

Tutte le utenze sono gestite in modo centralizzato dal PSN realizzando una federazione tra lo IAM dell'Oracle Cloud e l'IdP del PSN. Le utenze non verranno create direttamente sullo IAM di OCI, bensì andranno create sulla console del PSN e, al primo accesso, queste vengono automaticamente create nello IAM di OCI. Tutti gli accessi alla console OCI avvengono tramite sistema di Multi Factor Authentication.
Quando il tenant viene consegnato alla PA, viene creata solo l'utenza del referente tecnico, il quale avrà il ruolo di admin del tenant ma con alcune limitazioni, sarà poi lui ad aggiungere le altre persone che dovranno accedere al tenant, queste saranno le utenze secondarie.

INTERNAL USE

- *Utenze secondarie*

Tutte le utenze secondarie vengono create dal referente tecnico direttamente dalla console del PSN seguendo la procedura che viene descritta di seguito.

1. Accedendo al portale del PSN, passare a Home > Gestione Utenze Secondarie e poi cliccare “Aggiungi nuovo utente”.

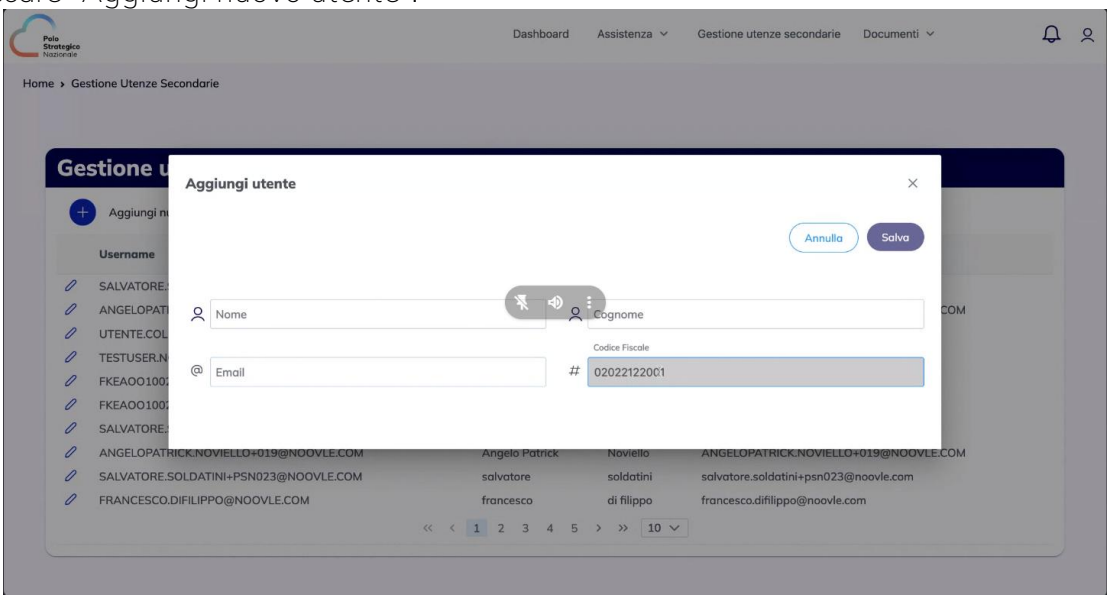

Figura 16 - Pannello Creazione Utenza Secondaria

Compilare i rispettivi campi con le informazioni necessarie e infine cliccare su “Salva”.

Da questo momento in poi, l’utenza secondaria sarà creata nell’IDP del PSN e l’utente riceve due mail:

i. la prima in cui viene notificata la creazione dell’utenza e indicato lo username a lui associato e che dovrà usare per accedere ai servizi del PSN.
ii. Una seconda mail contenente la password, che dovrà cambiare al primo accesso.

Se l’utente secondario appena creato accedesse dopo questo step, riuscirebbe ad accedere alla console di OCI ma non potrebbe fare nessun tipo di operazione, perché la sua utenza non è stata ancora abilitata ad accedere alla console OCI e associata ad alcun gruppo nello IAM di OCI.

Per richiedere l’abilitazione il Referente Tecnico dell’Amministrazione dovrà aprire un ticket di gestione utenze, indicando nel ticket l’utenza o le utenze secondarie create (ad es. 5EXXXX@PA.POLOSTRATEGICONAZIONALE.IT) e richiedere l’abilitazione ad accedere alla console OCI, il servizio contrattualizzato (ad es. PSN12345678), il nome del tenant a cui accedere (ad es. psn12345678), il ruolo da associare (ad es. TenancyAdministrator) e richiedere di inviare la richiesta al gruppo TI_IAM_HDI (IAM).

INTERNAL USE

INTERNAL USE

6.2.5 EKM

In ciascun tenant della PA è presente un Vault posizionato nel compartment cmp-servicecompartment:cmp-security. Al suo interno sono configurati gli end point delle chiavi generate dalla piattaforma Thales, che la PA utilizzerà per criptare tutte le risorse istanziate nel tenant.

In fase di onboarding del servizio, sono preconfigurate delle chiavi di crittografia, generate sugli apparati HSM del PSN e messe da subito a disposizione della PA per criptare i propri workload.

È comunque possibile, per la PA, richiedere tramite il servizio di ticketing dedicato del PSN, chiavi aggiuntive per specifici workload, indicando le caratteristiche della chiave da generare (nome, size, durata), nonché la destinazione d'uso. Il servizio base non prevede impostazioni di rotazione chiavi by design, ma deve essere espressamente richiesto dalla PA, con contestuale specifica dell'intervallo di rotazione ed il perimetro di chiavi impattato.

Nell'eventualità venga richiesta una nuova chiave tramite ticket, una volta che verranno ricevuti i valori della nuova chiave (*External Key ID*), questi andranno inseriti dalla PA navigando nella console OCI in Menù > Key Management & Secret Management > External Key Management > Vault Details e facendo click in basso sul bottone "Create key reference", all'interno del campo apposito, come da immagine seguente:

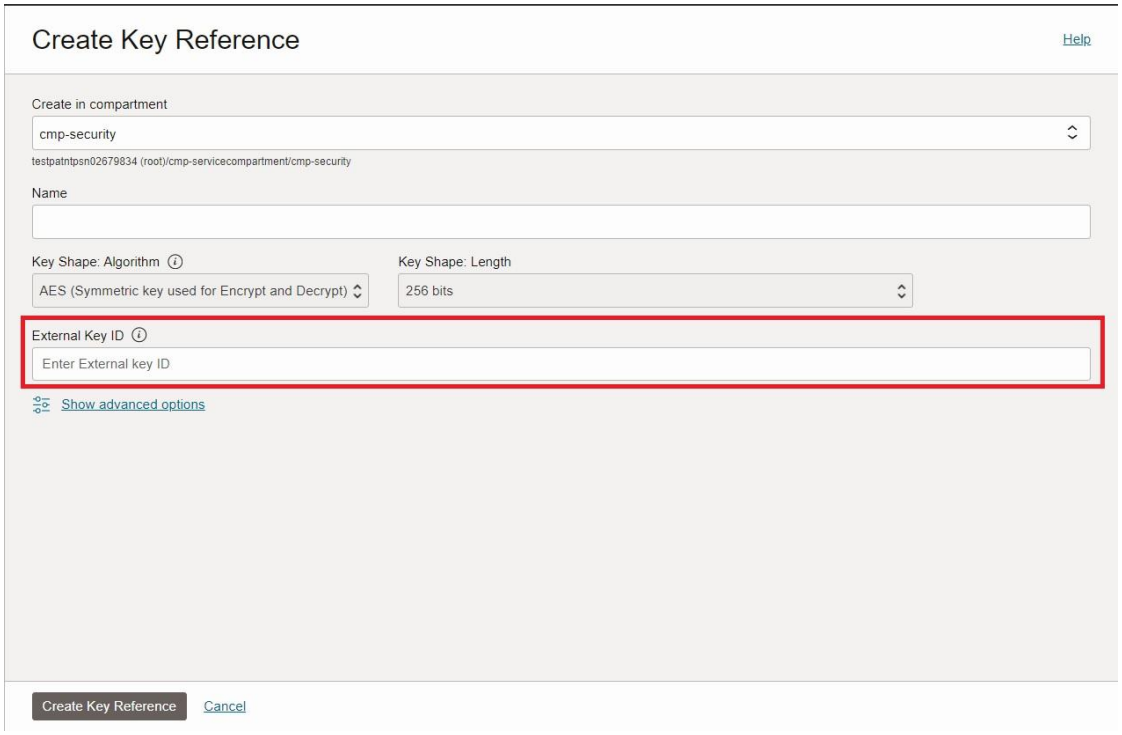

Figura 17 - Pannello Creazione Key Reference

INTERNAL USE

Il servizio offre le chiavi di crittografia tramite la tecnologia HYOK (Host You Own Key). Tali chiavi sono ospitate in un vault esterno (Thales CipherTrust Manager) e referenziate nel Vault di OCI. Tale modalità è quella suggerita per criptare qualsiasi dato ed è l'unica a garantire il livello di sicurezza necessario per i dati critici e strategici.
Ciò nonostante, la Pubblica Amministrazione può, a sua discrezione, responsabilità e completa gestione, utilizzare anche chiavi standard OCI o tramite la tecnologia BYOK, come di seguito:

- BYOK (Bring Your Own Key) – il cliente genera in autonomia la chiave sui suoi sistemi e la carica all'interno del Vault OCI.
- Chiave gestita da Oracle – in questo caso la risorsa viene criptata utilizzando delle chiavi gestite direttamente da Oracle.

Per questi metodi secondari si faccia riferimento alla documentazione ufficiale di Oracle Cloud Infrastructure.

Di seguito, a scopo esemplificativo, vengono descritte le procedure per utilizzare le chiavi HYOK gestite dal PSN per criptare un boot volume di una compute instance e di un DB (al momento della creazione), per tutte le altre risorse, la scelta della chiave di criptazione viene effettuata in modo analogo.

COMPUTE INSTANCE
Nella sezione "Boot volume" spuntare la casella "Encrypt this volume with a key that you manage" e scegliere il compartment cmp-servicecompartment:cmp-security, il vault "Vault_ekm" e la chiave che si vuole utilizzare.

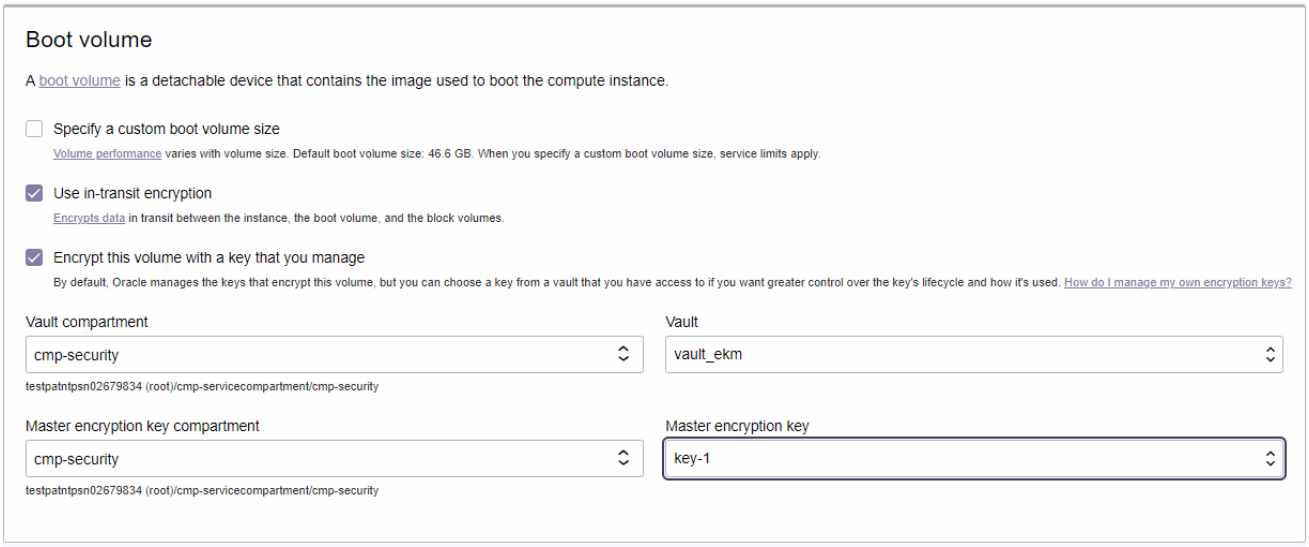

Figura 18 - Utilizzo chiave esterna per criptare il boot volume di una VM

INTERNAL USE

DATABASE

Per poter utilizzare una delle chiavi esterne per criptare i workload di un database, che sia un'istanza di Oracle Base Database Service oppure di Autonomous Database occorre prima aggiornare il gruppo dynamico che consente alle risorse precedentemente citate di poter utilizzare le chiavi esterne. Seguire i seguenti step:

1. Individuare l'OCID del compartment nel quale si vuole creare l'istanza database criptata con chiave esterna.
2. Navigare in Manu > Identity & Security > Domains selezionare il compartment cmp-servicecompartment ed entrare nel dominio domain_psn, questo è il dominio dove è definito il gruppo dynamico. Selezionare poi il tab Dynamic groups ed accedere al gruppo dynamico db-ekm.

Figura 19 - Dynamic Group

3. Cliccare su Edit all matching rules

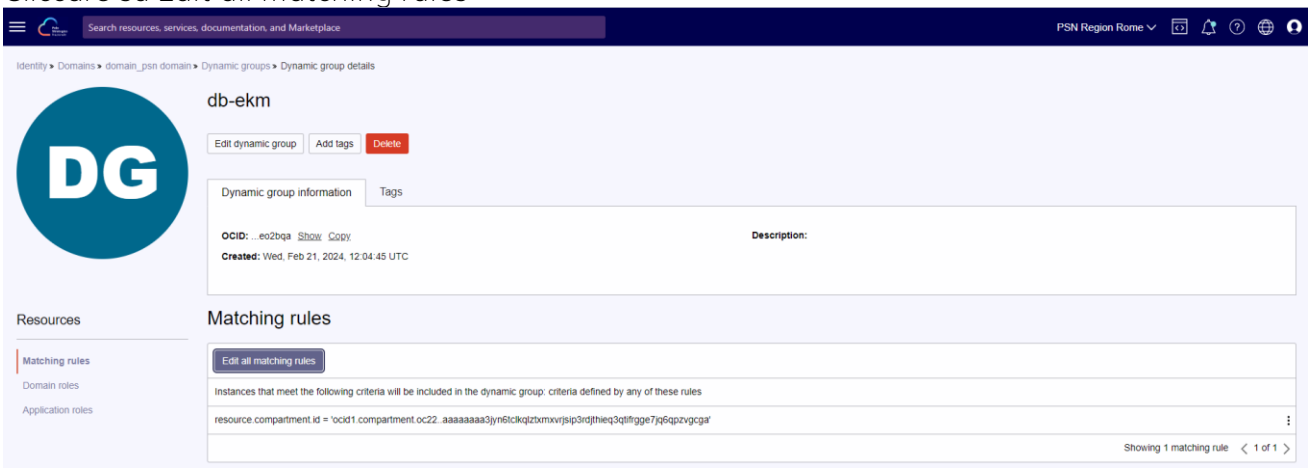

Figura 19 – Create Matching rules

Ed aggiungere una nuova riga con l'OCID del compartment in cui si vuole istanziare la risorsa database, come mostrato di seguito:
resource.compartment.id = '<OCID Compartment>

Da questo momento in poi in quel compartment è possibile creare qualsiasi risorsa DB criptata con la chiave esterna.

INTERNAL USE

Nota bene: Questo passaggio è indispensabile altrimenti il processo di creazione della risorsa fallisce.

ORACLE BASE DATABASE SERVICE
Nella scheda “Database information”, in fondo alla pagina cliccare su “Show advanced options” e nel tab “Encryption” selezionare “Use customer-managed keys” e scegliere il compartment cmp-servicecompartment:cmp-security, il vault “Vault_ekm” e la chiave che si vuole utilizzare.

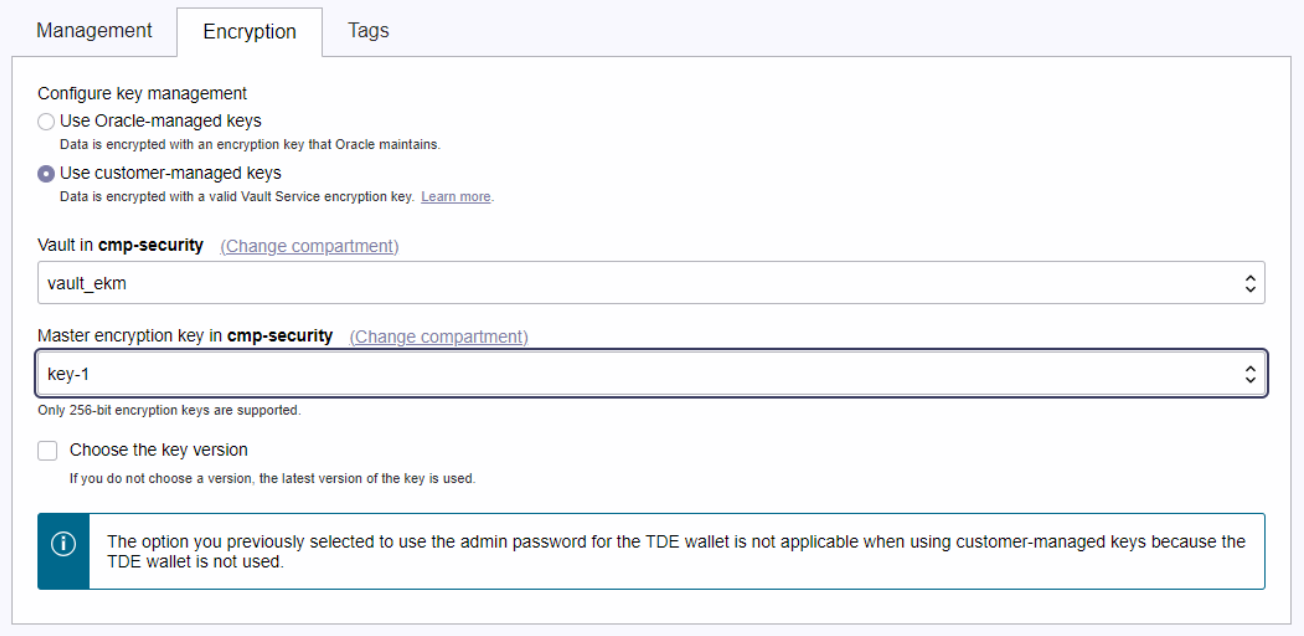

Figura 20 - Utilizzo chiave esterna per criptare Oracle Base Database

INTERNAL USE

- *Rotazione Chiave*

a. Object Storage

1. Il cliente richiede la rotazione della propria chiave tramite il servizio di ticketing dedicato del PSN.
2. Andare in Identity & Security, Key Management & Secret Management, External Key Management, entrare all'interno del proprio vault. Cliccare su Create Key Reference e inserire l'OCID della nuova chiave all'interno del campo. Cliccare su Create.
3. In seguito all'avvenuta assegnazione della nuova chiave all'interno dell'Object storage i nuovi oggetti creati utilizzeranno quest'ultima.

b. Block & Boot Volume

1. Il cliente richiede la rotazione della propria chiave tramite il servizio di ticketing dedicato del PSN.
2. Verrà creata una nuova chiave e fornito il nome e OCID.
3. Andare in Identity & Security, Key Management & Secret Management, External Key Management, entrare all'interno del proprio vault. Cliccare su Create Key Reference e inserire l'OCID della nuova chiave all'interno del campo. Cliccare su Create.
4. Per associare la nuova versione ad un Block volume seguire le azioni indicate nella documentazione ufficiale Oracle.
   Per associare la nuova versione ad un Boot volume seguire le azioni indicate nella documentazione ufficiale Oracle.

INTERNAL USE

c. BaseDB: Base Database

1. Il cliente richiede la rotazione della propria chiave tramite il servizio di ticketing dedicato del PSN.
2. Verrà creata una nuova versione della chiave e fornito l'OCID.
3. Andare in Identity & Security, Key Management & Secret Management, External Key Management, entrare all'interno del proprio vault. Cliccare su Create Key Reference e inserire l'OCID della nuova chiave all'interno del campo. Cliccare su Create.
4. Il cliente utilizzerà i seguenti comandi accedendo al Database via shell e tramite dbcli:

```
--Command to fetch the dbId:
dbcli list-databases

--Rotate key at the CDB level
dbcli update-tdekey -i <dbId> -r

--Rotate the key at the PDB level
dbcli update-tdekey -i <dbId> -n <pdbName> -no-r

--Assign a new key version to the CDB
export DEVMODE=true
dbcli set-keyversion -i <dbId> -n 'CDB$ROOT' -o <key version ocid>

--Assign a new key version to the PDB
export DEVMODE=true
dbcli set-keyversion -i <dbId> -n <pdb name> -o <key version ocid>
```

d. ADB-S: Autonomous Database on Shared Infrastructure

1. Il cliente richiede la rotazione della propria versione della chiave tramite il servizio di ticketing dedicato del PSN.
2. Verrà creata una nuova chiave e fornito il nome e OCID.
3. Andare in Identity & Security, Key Management & Secret Management, External Key Management, entrare all'interno del proprio vault e della propria chiave. Cliccare su Rotate Encryption Key e inserire l'OCID della nuova chiave all'interno del campo. Cliccare su Rotate.
4. Per associare la nuova versione ad un ADB-S seguire le azioni indicate nella documentazione ufficiale Oracle.

INTERNAL USE

e. ADB-D: Autonomous Database on Dedicated Infrastructure

1. Il cliente richiede la rotazione della propria versione della chiave tramite il servizio di ticketing dedicato del PSN.
2. Verrà creata una nuova chiave e fornito il nome e OCID.
3. Andare in Identity & Security, Key Management & Secret Management, External Key Management, entrare all'interno del proprio vault e della propria chiave. Cliccare su Rotate Key Reference e inserire l'OCID della nuova chiave all'interno del campo. Cliccare su Rotate.
4. Per associare la nuova versione ad un ADB-D (Container DataBase o Pluggable DataBase) seguire le azioni indicate nella documentazione ufficiale Oracle. E' necessario ruotare la chiave per entrambe le risorse Container DataBase e Pluggable DataBase: il Pluggable eredita la chiave utilizzata dal Cluster solamente in fase di deploy e non in fase di rotazione del Cluster.

N.B. quello che Oracle descrive nella documentazione pubblica come BYOK non è altro che il servizio HYOK offerto dal PSN Managed Oracle: chiavi ospitate in un vault esterno (Thales CipherTrust Manager) e referenziate nel Vault di OCI.

f. ExaCS: Exadata Database on Dedicated Infrastructure

1. Il cliente richiede la rotazione della propria chiave tramite il servizio di ticketing dedicato del PSN.
2. Verrà creata una nuova versione della chiave e fornito l'OCID.
3. Andare in Identity & Security, Key Management & Secret Management, External Key Management, entrare all'interno del proprio vault. Cliccare su Create Key Reference e inserire l'OCID della nuova chiave all'interno del campo. Cliccare su Create.
4. Il cliente utilizzerà i seguenti comandi accedendo al Database via shell e tramite dbaascli:

```
-- CDB
dbaascli tde setKeyVersion --dbname <db-name> --kmsKeyVersionOCID <ocid_key-version>
-- PDB
dbaascli tde setKeyVersion --dbname <db-name> --pdbName <pdb-name> --kmsKeyVersionOCID <ocid_key-version>
```


INTERNAL USE

6.2.6 Logging

Il cliente, dopo aver effettuato l'accesso alla console di OCI tramite la console del PSN, nella sezione "Logging" potrà visualizzare i log di accesso e quelli di servizio prodotti dalle varie risorse istanziate nel tenant. Una copia dei log relativi alla sicurezza, e quindi solamente quelli compatibili con il modello di shared-responsability, saranno inviati al SIEM del PSN.

6.2.7 Monitoring

Il rispetto del regime di compliance viene monitorato dal PSN sia tramite la Partner Console centrale che tramite il servizio Monitoring di OCI.

Il servizio Oracle Cloud Infrastructure Monitoring consente di monitorare attivamente e passivamente le risorse cloud attraverso metriche e allarmi. Tutte le risorse istanziate nel tenant di ciascun cliente, che si trovano nel compartment cmp-servicecompartment, e che consentono a ciascun tenant di integrarsi con i servizi del PSN, saranno attivamente monitorate dal PSN attraverso l'utilizzo di allarmi. Questi allarmi, quando scattano, vengono inviati direttamente ai sistemi di monitoraggio del PSN, alcuni di questi allarmi sono: CPU al 90% per la VM del BaaS, messaggi di errore sullo streaming, ecc. Sarà il PSN ad intervenire tempestivamente per assicurarsi che gli allarmi rientrino e che non causino disservizi.

La singola Amministrazione che voglia monitorare le risorse istanziate nel proprio compartment ha la possibilità di farlo installando appositi agenti che dialogano con strumenti proprietari o tramite opportuni Oracle Stream indirizzati a propri hub.

6.2.8 Backup as a Service

Il Backup as a Service del PSN è un servizio opzionale offerto alle PA, basato sulla tecnologia Commvault e che garantisce la disponibilità dei dati per la maggiorparte dei servizi OCI. Commvault Backup & Recovery offre protezione e ripristino di livello enterprise per macchine virtuali, container, database, applicazioni e file.

Il servizio copre al momento i seguenti servizi OCI

- Object Storage
- Compute Instance (Virtual Machine e Bare Metal).
- Oracle Base Database Service e Exadata (tramite agent installato sulla VM).
- Backup Applicativi (effettuato con agent installato sulla VM).

Altri servizi non elencati non sono al momento backuppabili tramite tecnologia CommVault, ma è sempre possibile utilizzare il backup nativo di OCI, anche per i servizi elencati.
Per usufruire del servizio BaaS offerto dal PSN in modalità agentless occorre semplicemente acquistare il servizio opzionale.

INTERNAL USE

Mentre, per i backup "applicativi" o che prevedano l'installazione di agent a bordo delle VM occorre aprire un ticket per richiedere la configurazione di tutte le risorse necessarie, in quanto occorre agire creando un peering tra il compartment del cliente e quello di servizio. Il set-up di questa configurazione verrà effettuato con il supporto di operatori del PSN.

Nel ticket aperto al PSN in cui viene richiesta questa configurazione occorre fornire due informazioni essenziali:

- CIDR Block della VCN di erogazione.
- OCID della VCN di erogazione della PA, quella in cui si trova la risorsa di cui si vuole eseguire il backup custom.
- OCID compartment dove si trova la VCN di erogazione della PA.

Per ulteriori dettagli si rimanda al Manuale Utente del servizio BaaS.

INTERNAL USE

7. Utilizzo API Tenant

Per poter utilizzare le API di OCI sono necessarie le seguenti informazioni:

- user OCID: <OCID user>.
- Tenancy OCID: <OCID Tenant>.
- Region: eu-dcc-rome-1.
- Chiave privata: API key caricata sul profilo dell'utente.

Oltre a queste informazioni, per accedere alla dedicated region, bisogna inserire in *~/.oci/* il *file regions-config.json* (in allegato), oppure utilizzando le variabili d'ambiente come documentato sul supporto Oracle (con i parametri impostati nel file allegato).

regions-config.json

8. Service Usage

8.1 Dashboard

Il monitoraggio dei consumi avviene accedendo alla Console PSN, cliccando il bottone Resources e collegandosi alla Dashboard predefinita, come mostrato nella seguente figura:

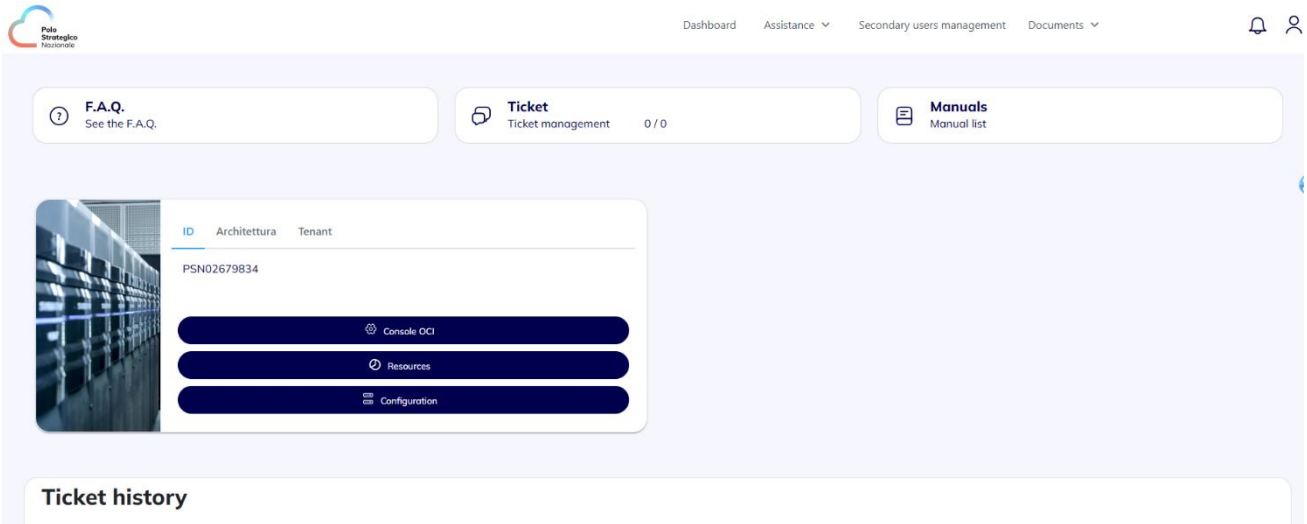

Figura 21 - Home Page Console PSN

INTERNAL USE

Figura 22 - Dashboard dei consumi sulla Console PSN

9. Guida alla fatturazione

I servizi Public Cloud PSN managed e Secure Public Cloud verranno fatturati bimestralmente a livello di "Famiglia di servizio" che è il risultato del campo "Macrotipologia" e "Tipo 1" del listino ufficiale pubblicato sul sito istituzionale di Polo Strategico Nazionale nell'area "Tutti i documenti per aderire a Polo Strategico Nazionale".

Per l'attivazione di risorse riservate o committate per 1 anno o 3 anni, in caso di recesso anticipato dal contratto o alla scadenza del contratto di utenza, al cliente verrà addebitata una fattura di consuntivo relativa agli importi non usufruiti per il periodo residuo di reservation/commitment.

10. FAQ

10.1 Documentazione OCI

- Oracle Cloud Infrastructure
  Oracle Cloud Infrastructure documentation

INTERNAL USE

10.2 Assistenza per il servizio

È possibile richiedere assistenza tramite:

- Console di Gestione Servizi: https://console.polostrategiconazionale.it;
- Numero verde 800.776.776 (utilizzando il PIN dedicato, comunicato nella welcome letter).

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.

INTERNAL USE