

Fornitura dei Servizi di Cloud Computing (IaaS, BaaS, SaaS) nell'ambito del Sistema Pubblico di Connettività e Cooperazione (SPC) per il CLIENTE REGIONE CAMPANIA

Contratto: 11980011990639005COEV3

Regione Campania

CIG: 882450323F



Collaudo parziale Infrastruttura Tecnologica

Codice Commessa: TLC21JV8

INDICE

0	REGISTRAZIONE MODIFICHE DOCUMENTO	3
1	INTRODUZIONE	4
2	DESCRIZIONE DEL PROGETTO.....	4
3	DETTAGLIO AVANZAMENTO LAVORI	7
3.1	SILF	7
4	ITER	19
4.1	iTer Mobile Configurazione nuova network.....	19
4.2	iTer V Configurazione nuova Network	19
4.3	iTer Base Configurazione nuova Network	19
4.4	iTer Supporto e Verifica applicativi IOT	20
4.5	iTer Supporto e verifica Portale.....	20
4.6	iTer Configurazione VPN.....	20
4.7	iTer monitoraggio	21
4.8	ITer - Supporto al moving	25
4.9	ITer – Supporto	25
4.10	ITer – Integrazione Monitoraggio	26
4.11	ITer – Integrazione pannello statistiche	26
5	RENDICONTAZIONE ATTIVITÀ	27

0 REGISTRAZIONE MODIFICHE DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

DESCRIZIONE MODIFICA	VERSIONE	DATA
Prima emissione	1	Marzo 2022

1 INTRODUZIONE

Scopo del presente documento è definire lo Stato Avanzamento Lavori concernenti le piattaforme SILF e ITER.

2 DESCRIZIONE DEL PROGETTO

La Regione Campania, nell'ambito del consolidamento e virtualizzazione dei Sistemi Informativi, ha migrato presso il Cloud di TIM gran parte del parco applicativo relativo ai Sistemi Informativi Lavoro.

Le applicazioni: Cliclavoro Campania, CO Campania, CR Campania, PID Campania e 5 SIL provinciali, Simona, Monitoraggio sono state trasferite in Cloud, aderendo alla convenzione SPC Lotto 1.

La piattaforma è fruibile per tutti gli utenti attraverso il classico collegamento internet sia per i cittadini che per gli operatori della Regione Campania. Tutti i sistemi della piattaforma comunicano tra loro all'interno del cloud.

I sistemi che sono stati oggetto della migrazione e nuova installazione in cloud sono i seguenti:

- Portale SILF
- Simona Accreditamento
- Simona Bandi
- Simona Monitoraggio

Per tale migrazione, il presente progetto specifica il fabbisogno delle risorse computazionali tramite i Servizi IaaS e PaaS e per il servizio di Backup tramite il servizio BaaS.

Infine, il progetto riporta l'effort e la pianificazione dei servizi professionali di Cloud Enabling, per supportare l'Amministrazione nella gestione della sicurezza, nella migrazione e nella fase di tuning dei Sistemi.

Con il contratto n. **1980011990639005COE** (cd SILF I) a scadenza 22 maggio 2021, in ottemperanza a quanto indicato nelle linee guida AGID, le soluzioni applicative sono state rilasciate per essere fruibili attraverso infrastrutture cloud;

Regione Campania ha richiesto un'estensione dei servizi fino a luglio 2022. Con riferimento all'estensione contrattuale n. **11980011990639005COEV3** i servizi vengono rinnovati ed integrati con nuove attività per il relativo periodo di riferimento.

A seguito della migrazione dei sistemi informativi lavoro della Regione Campania in ambiente Cloud sono inoltre emerse delle esigenze di ampliamento e consolidamento dell'infrastruttura oggi a disposizione dei sistemi informativi migrati. Si riporta di seguito una proposta di ampliamento dell'infrastruttura in essere per i 2 IaaS VDC attualmente presenti.

Ed in aggiunta un terzo VDC per sistema di gestione syslog.

Regione Campania ha inoltre richiesto di ricondurre all'interno di questo Progetto anche le risorse elaborative del contratto 1780011990639001COEV2 (cd ITER), lasciando inalterato il relativo tenant, senza attività di migrazione sui tenant del progetto SILF.

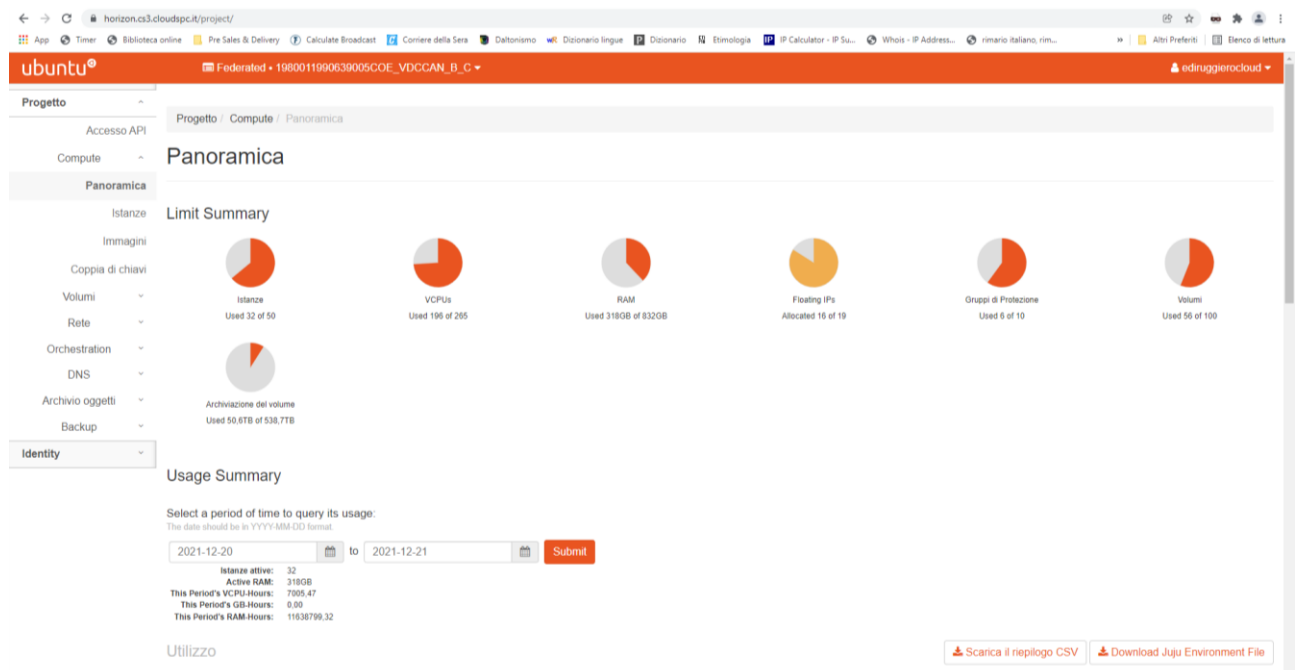
Per il sistema ITER è previsto un quarto VDC e sono richieste anche attività di Cloud Enabling per la configurazione di nuove componenti e network e per il monitoraggio di sistema.

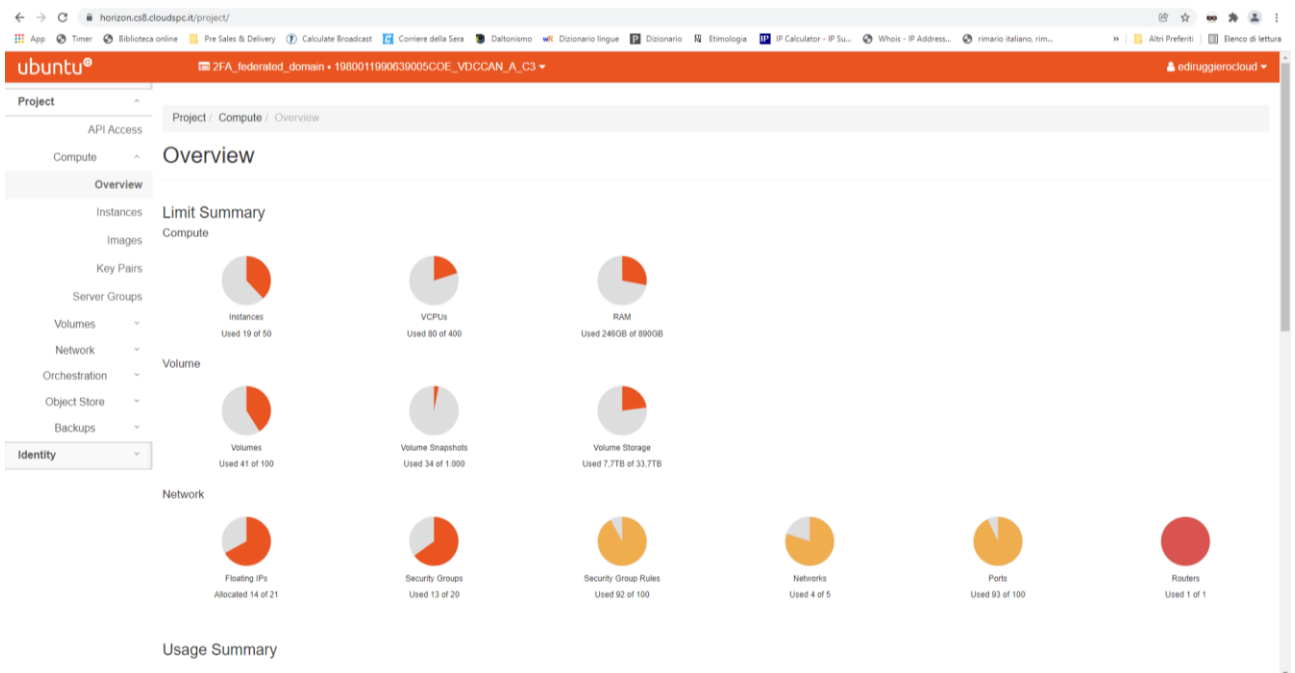
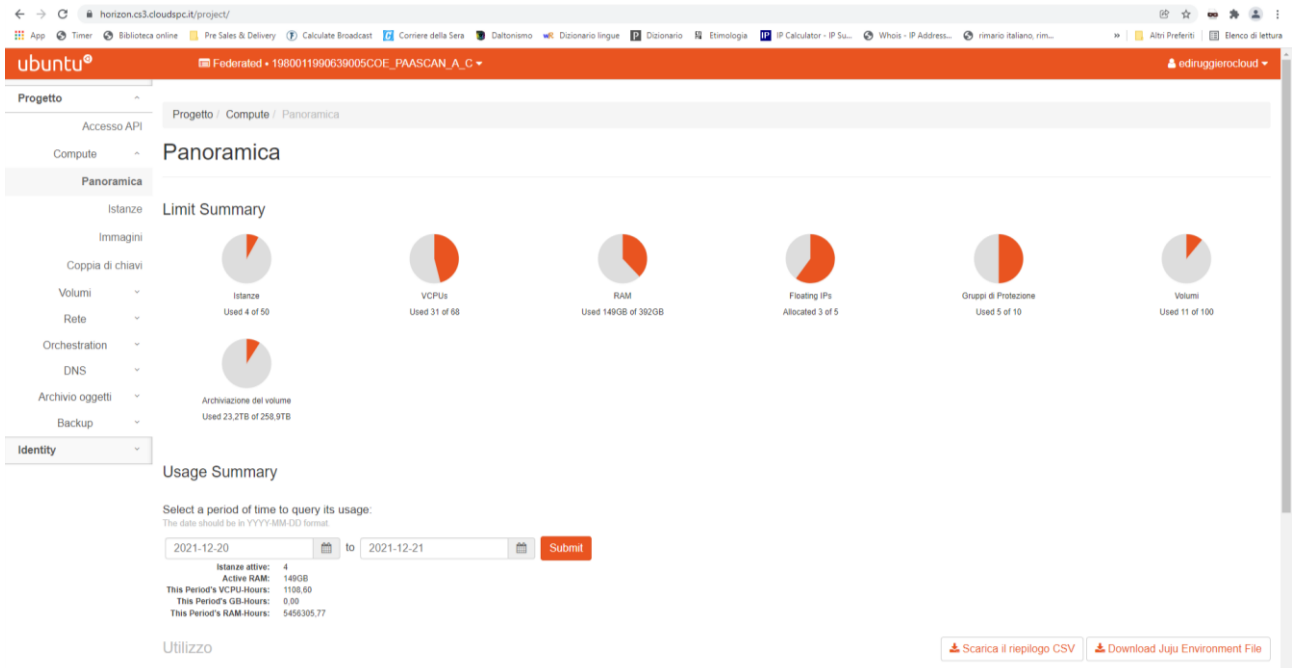
La tabella seguente sintetizza le risorse elaborative dei quattro Virtual Data Center.

	Total vCPUs	Total RAM (GB)	Total Volume Storage (TB)
Risorse aggiuntive per VDC A (SILF)	200	640	30
Risorse aggiuntive per VDC B (SILF)	50	512	2
Nuovo VDC per gestione syslog (SILF)	15	24	2,5
Nuovo VDC (VDC iTer)	676	886	7,5

Le risorse mostrate nella tabella precedente sono state rese disponibili il 20/12/2021. La loro fatturazione sarà gestita separatamente rispetto a quanto riportato in questo documento.

Di seguito alcuni screenshot della console per la verifica dell'avvenuto upgrade infrastrutturale





TIM in considerazione dei requisiti della Regione Campania ha aggiunto le seguenti ulteriori integrazioni per il progetto SILF:

- il servizio BaaS passa da un volume di 8 TB ad un volume di 28 TB
- viene introdotto il servizio PaaS Zabbix per monitorare la piattaforma

Si rende inoltre necessario disporre di un ambiente server di test (Istanza SQL Server di test), al fine di mantenere gli ambienti di produzione e pre-produzione allineati.

Al fine di migliorare la continuità dei servizi delle piattaforme PaaS SQL Server SE, si prevede di aggiungere, come indicato in precedenza, ulteriori risorse elaborative (VCPU, RAM, VNetwork, Storage) ad integrazione e un'architettura che prevede l'always-on dei PaaS SQL Server che ospitano il Data Base del SILF.

DETTAGLIO AVANZAMENTO LAVORI

3 SILF

3.1 Predisposizione ambiente di Staging e Update Produzione

Nel seguente capitolo illustreremo i lavori svolti per creare l'ambiente di Staging e gli update dei server Web inerenti all'ambiente di Produzione.

a. Ambiente di Staging

L'ambiente di Staging attualmente predisposto è legato all'istanza Sql server Sql2014 e l'host del server è stato chiamato TESTSQL01.

All'interno di tale ambiente sono stati ripristinati tutti i backup dei db attualmente in produzione.

Successivamente al ripristino sono stati effettuati i test di lettura e scrittura sui dischi collegati per valutarne le prestazioni di ogni singola unità rispetto all'attuale produzione.

È stata infine effettuata un'analisi di collegamento del server SQL con gli ambienti di prod e di cui si riporta un estratto nel paragrafo successivo.

b. Update Sistema Operativo Web Server di Produzione

Al termine delle operazioni indicate nel punto A sono stati creati 3 server Web Windows Server 2019 i quali andranno a sostituire in ambiente di produzione i server con sistema operativo Windows Server 2012.

I server sono stati nominati in base al servizio installato all'interno.

- HOST: WEBCO01
- HOST: WEBCLIC01
- HOST: WEBSIL01

I tre server sono stati installati con immagine Windows fornita da Telecom "Windows_Server_2019_Standard_Activated" ed è stata una prima copia delle cartelle e dati attualmente presenti sulla produzione al fine di poter effettuare i test di funzionamento degli applicativi.

I server che verranno dismessi da queste prime tre macchine saranno:

- HOST: WEBCO00
- HOST: WEB01
- HOST: WEB05

3.2 Analisi ambiente di Staging

Nel seguente capitolo illustreremo il server Staging Sql Server 2014 creato all'interno della sottoscrizione Telecom **1980011990639005COE PAASCAN A C3** e le relative prestazioni.

Il server è stato nominato TESTSQL01.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
TESTSQL01	WIN2012R2_MSSQL14_Activated	10.10.3.14, 156.54.34.76	4SOCKET_20CPU_64GB	mdaettkey	Active	nova	None	Running	1 mese, 2 settimane	Create Snapshot

I dischi sono stati montati sul server come Share all'interno del percorso C:\ShareDisk.

Prima di effettuare l'accensione del server sql abbiamo predisposto l'ambiente presente nella sottoscrizione Telecom e configurato come di seguito indicato:

Emesso da: EM-POS.PO/S

Codice doc.: TLC21JV8SAL

Versione:1

Data: 29/03/2022

- NETWORK

Abbiamo creato la network di Staging 10.10.3.0/24

<input type="checkbox"/> TESTNET	TEST-SUBNET 10.10.3.0/24	No	No	Active	UP	AZ3, AZ2, AZ1
----------------------------------	--------------------------	----	----	--------	----	---------------

- SECURITY GROUPS

Dopo la network è stato creato il Security Group dedicato alle porte Sql in ingresso.

<input type="checkbox"/> IN_Allow_SQLTEST	0d8e10f5-a71a-4b37-8b5b-28533a33bf4e
---	--------------------------------------

Nel gruppo sono stati inseriti gli ip abilitati ad accedere all’istanza con le seguenti porte (FILE SHARE, SQL):

- o TCP 135 – 139
- o TCP 161-162
- o TCP 167
- o TCP 445
- o TCP 1433
- o TCP 49152 - 65535
- o TCP 1024 – 5000

Dopo la configurazione di Base è stato creato il server TESTSQL01 con i seguenti settaggi:

- VOLUMI

Tramite il portale Volumes abbiamo creato i dischi impostandoli come da schermata sotto:

<input type="checkbox"/> Name	Description	Size	Status	Group	Type	Attached To
<input type="checkbox"/> TESTSQL01_data11	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdp on TESTSQL01
<input type="checkbox"/> TESTSQL01_data10	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdo on TESTSQL01
<input type="checkbox"/> TESTSQL01_data09	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdn on TESTSQL01
<input type="checkbox"/> TESTSQL01_data08	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdm on TESTSQL01
<input type="checkbox"/> TESTSQL01_temp00	Server Test Sql Server	200GiB	In-use	-	Prestazionale	/dev/vdl on TESTSQL01
<input type="checkbox"/> TESTSQL01_backup01	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdk on TESTSQL01
<input type="checkbox"/> TESTSQL01_backup00	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdj on TESTSQL01
<input type="checkbox"/> TESTSQL01_data07	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdi on TESTSQL01
<input type="checkbox"/> TESTSQL01_data06	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdh on TESTSQL01
<input type="checkbox"/> TESTSQL01_data05	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdg on TESTSQL01
<input type="checkbox"/> TESTSQL01_data04	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdf on TESTSQL01
<input type="checkbox"/> TESTSQL01_data03	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vde on TESTSQL01
<input type="checkbox"/> TESTSQL01_data02	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdd on TESTSQL01
<input type="checkbox"/> TESTSQL01_data01	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdc on TESTSQL01
<input type="checkbox"/> TESTSQL01_data00	Server Test Sql Server	500GiB	In-use	-	Prestazionale	/dev/vdb on TESTSQL01
<input type="checkbox"/> TESTSQL01_SO	Server Test Sql Server	128GiB	In-use	-	Prestazionale	/dev/vda on TESTSQL01

N.B. Il disco del Sistema Operativo TESTSQL01_SO è stato creato partendo dall’immagine fornita da Telecom “WIN2012R2_MSSQL14_Activated” e tutti i dischi sono di tipo prestazionale.

- IP NETWORK

Al server è stato assegnato l’ip statico 10.10.3.14 dentro la network TEST-NET e gli sono stati assegnati i Security Group “IN_Allow_SQLTEST” e “OUT_Allow_Internet”.

DNS Assignment

```

Hostname testsql01
IP Address 10.10.3.14
FQDN testsql01.cs8.cloudspc.it
    
```

Infine abbiamo assegnato l’ip pubblico 156.54.34.76 per poter raggiungere l’istanza, in base alle abilitazioni date in precedenza, anche dall’esterno.

Prestazioni dischi installati sul server TESTSQL01

Avviato il server e configurati i dischi i test hanno prodotto i seguenti report

TEMPDB:

PATH: C:\ShareDisk\temp00

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	177.84	234.88
RND4K Q1T1	1.85	1.65
RND4K (IOPS)	452.64	402.59
RND4K (µs)	2114.97	2471.78

DATA00: PATH: C:\ShareDisk\data00

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	206.34	311.17
RND4K Q1T1	2.06	1.65
RND4K (IOPS)	503.17	402.59
RND4K (µs)	1786.49	2473.37

DATA01: PATH: C:\ShareDisk\data01

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	243.27	264.05
RND4K Q1T1	2.22	1.65
RND4K (IOPS)	541.50	402.59
RND4K (µs)	1734.06	2473.61

DATA02: PATH: C:\ShareDisk\data02

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	341.38	340.37
RND4K Q1T1	1.98	1.75
RND4K (IOPS)	483.15	426.03
RND4K (µs)	2036.62	2336.20

DATA03: PATH: C:\ShareDisk\data03

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	338.09	291.71
RND4K Q1T1	2.46	1.65
RND4K (IOPS)	600.10	402.59
RND4K (µs)	1514.48	2473.61

DATA04: PATH: C:\ShareDisk\data04

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	304.13	239.70
RND4K Q1T1	2.25	1.65
RND4K (IOPS)	550.05	403.08
RND4K (µs)	1727.62	2470.10

DATA05: PATH: C:\ShareDisk\data05

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	288.59	232.12
RND4K Q1T1	1.81	2.14
RND4K (IOPS)	443.12	522.95
RND4K (µs)	2114.30	1901.59

DATA06: PATH: C:\ShareDisk\data06

DATA07:

C:\ShareDisk\data07

PATH:

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	253.91	278.26
RND4K Q1T1	2.01	1.98
RND4K (IOPS)	491.46	484.38
RND4K (µs)	1884.07	2054.38

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	155.60	300.93
RND4K Q1T1	2.87	2.43
RND4K (IOPS)	701.17	594.24
RND4K (µs)	1417.19	1672.58

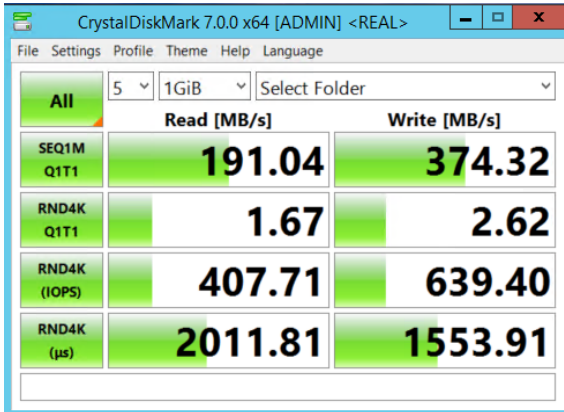
DATA09: PATH: C:\ShareDisk\data07

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	219.40	338.00
RND4K Q1T1	1.89	2.43
RND4K (IOPS)	460.69	593.75
RND4K (µs)	1721.00	1674.30

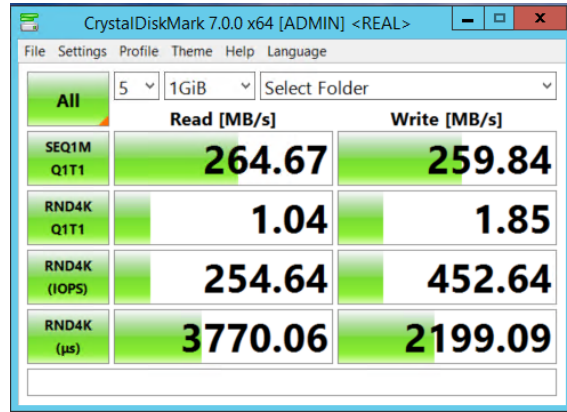
DATA08: PATH: C:\ShareDisk\data07

	Read [MB/s]	Write [MB/s]
SEQ1M Q1T1	348.12	305.34
RND4K Q1T1	2.29	1.65
RND4K (IOPS)	557.86	402.83
RND4K (µs)	1714.08	2472.62

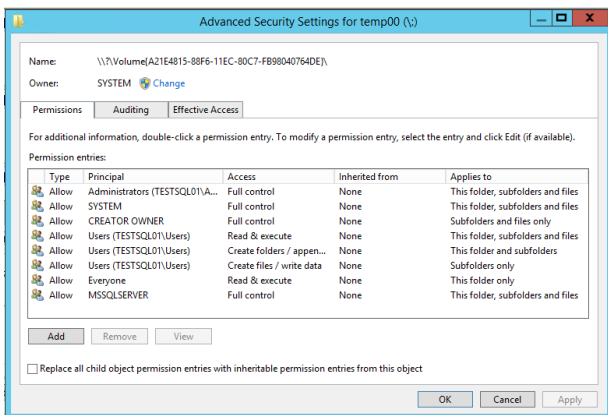
DATA10: PATH: C:\ShareDisk\data07



DATA11: PATH: C:\ShareDisk\data07



Nota Importante: Per Abilitare Sql Server ad accedere ai dischi montati sulla share C:\ShareDisk abbiamo inserito l'utenza NTSERVICE\MSSQLSERVER come "full control" dei dischi dati.



Ripristino Istanza dai Backup della produzione

Il ripristino operativo dell'istanza ha avuto i tempi sotto descritti.

N.B. Come da tabella allegata si evidenzia che il primo ripristino di tutti i database è durato circa 25 Ore e 32 Minuti.

DB NAME	TEMPO RIPRISTINO	TIPO	UNITA' MDF	UNITA' LDF
Campania_ColTemp	1H:54M	FULL	data00	data04
	2M	DIFF		
Campania_IDO	1S	FULL	data00	data04
	1S	DIFF		
Campania_IndiceRegional e	3M	FULL	data00	data04
	1S	DIFF		
Campania_Jump	8M	FULL	data01	data05
	27S	DIFF		
Campania_JumpBK	11M	FULL	data01	data05
	4S	DIFF		
Campania_Link	47M	FULL	data00	data04
	10M	DIFF		
Campania_Link_QM	45M	FULL	data02	data06
	3M	DIFF		
Campania_Link_Storico	10M	FULL	data02	data06
	2M	DIFF		
Campania_LinkBK	2M	FULL	data02	data06
	2S	DIFF		
Campania_PDDNET	18M	FULL	data03	data07
	3M	DIFF		
Campania_PDDNET_StoricoTrack er	1H	FULL	data02	data06
	7S	DIFF		
Campania_PDDNET_SAPReposito ry	20M	FULL	data02	data06
	35M	DIFF		
Campania_PDDNET_StatisticheSA P	18S	FULL	data03	data07

Al termine del ripristino i passaggi successivi sono stati quelli di creare i Server Web sotto descritti per effettuare i test operativi delle applicazioni.

3.3 Analisi procedura di creazione dei nuovi Web Server di produzione con i sistemi operativi upgradati a Windows 2019.

Nell'ambito delle attività di aggiornamento di sicurezza dei web server presenti, abbiamo creato i server sotto descritti per effettuare le prove operative degli applicativi ETT, presenti oggi su server Windows server 2012, sulla nuova piattaforma Windows server 2019.

c. SERVER WEBCO01:

Nel seguente capitolo illustreremo il server WEBCO01 creato all'interno della sottoscrizione Telecom **1980011990639005COE VDCCAN A C3**.

Il server è stato nominato WEBCO01 ed è il clone dati dell'attuale WEBCO00.

WEBCO01	Windows_Server_2019_Standard	VPN_NET 192.168.100.154 LAN_NEW 192.168.30.117 DMZ_NEW 172.16.3.165, 156.54.34.65	8CPU_32GBRAM	Active	all' nova	None	Running	2 mesi, 3 settimane	Create Snapshot
---------	------------------------------	---	--------------	--------	-----------	------	---------	---------------------	-----------------

I dischi montati sul server sono C: (Disco SO), E: (Disco Dati), F: (Disco Dati).

- VOLUMI

Tramite il portale Volumes abbiamo creato i seguenti dischi impostandoli come da schermata sotto

WEBCO01_data01	-	1000GiB	In-use	-	Prestazionale	/dev/vdc on WEBCO01
WEBCO01_data00	-	400GiB	In-use	-	Prestazionale	/dev/vdb on WEBCO01
WEBCO01_OS	-	150GiB	In-use	-	Prestazionale	/dev/vda on WEBCO01

- IP NETWORK

Al server sono stati assegnati gli ip statici 192.168.100.154, 192.168.30.117, 172.16.3.165 dentro le network VPN_NET, LAN_NEW, DMZ_NEW e gli sono stati assegnati i Security Group.

VPN_NET: "LAN_VPN_IPSec" e "VPN_NET".

LAN_NEW: "LAN" e "DomainController SG".

DMZ_NEW: "Internet_Access", "DMZ", "ETT_MANAGEMENT", "WEB_Servers".

IP Addresses

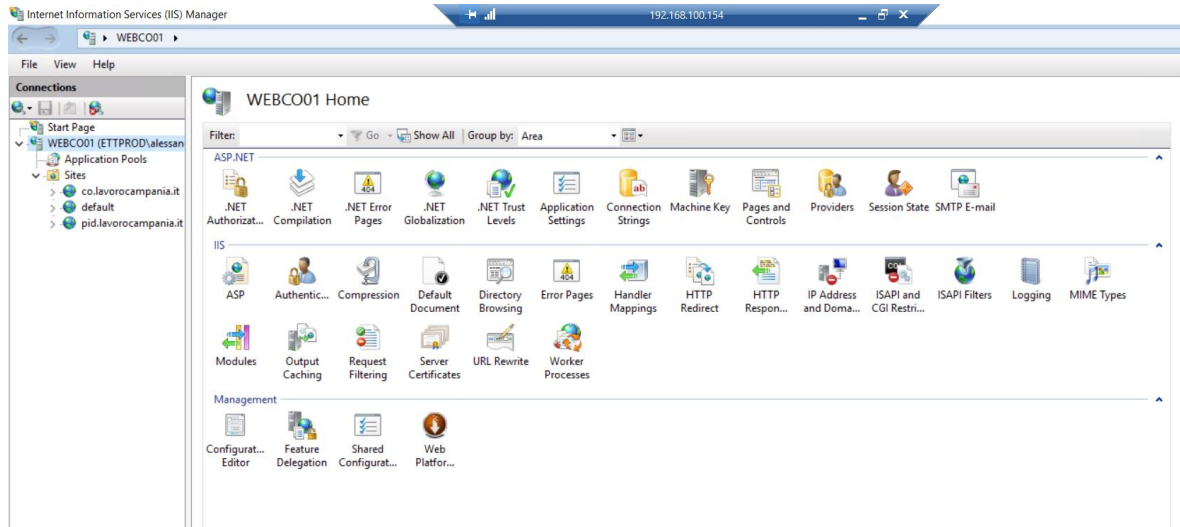
VPN_NET	192.168.100.154
LAN_NEW	192.168.30.117
DMZ_NEW	172.16.3.165, 156.54.34.65

Infine, abbiamo assegnato l'ip pubblico 156.54.34.65 per poter raggiungere l'istanza ed effettuare i test, in base alle abilitazioni date in precedenza, anche dall'esterno.

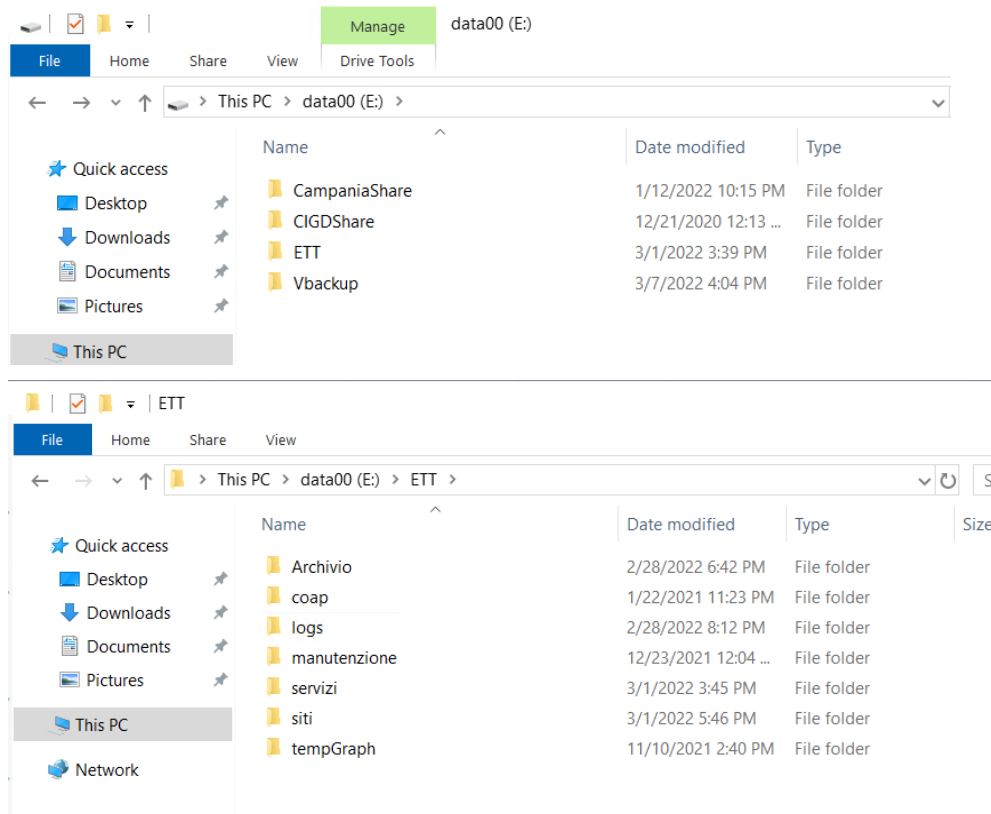
N.B. L'ip pubblico è solo temporaneo quando migreremo la produzione l'ip tornerà quello attuale di WEBCO00.

Di seguito le schermate della configurazione interna al Server:

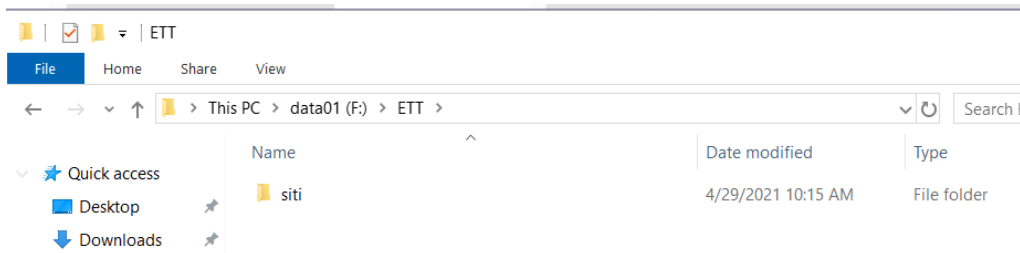
IIS:



DISCO DATA00 E:



DISCO DATA01 F:



d. SERVER WEBCLIC01

Nel seguente capitolo illustreremo il server WEBCLIC01 creato all’interno della sottoscrizione Telecom **1980011990639005COE VDCCAN A C3**.

Il server è stato nominato WEBCO01 ed è il clone dati dell’attuale WEBCO00.

<input type="checkbox"/> WEBCLIC01	Windows_Server_2019_Standard_Activated	LAN_NEW 192.168.30.170 VPN_NET 192.168.100.170 DMZ_NEW 172.16.3.170	4CPU_16GBRAM
------------------------------------	--	---	--------------

I dischi montati sul server sono C: (Disco SO), E: (Disco Dati).

- VOLUMI

Tramite il portale Volumes abbiamo creato i seguenti dischi impostandoli come da schermata sotto

<input type="checkbox"/> WEBCLIC01_data00	Server 01 Cliclavoro	100GiB	In-use	-	Prestazionale	/dev/vdb on WEBCLIC01	nova	No	No	Exit Volume
<input type="checkbox"/> WEBCLIC01_OS	Server 01 Cliclavoro	100GiB	In-use	-	Prestazionale	/dev/vda on WEBCLIC01	nova	SI	No	Exit Volume

- IP NETWORK

Al server sono stati assegnati gli ip statici 192.168.100.170, 192.168.30.170, 172.16.3.170 dentro le network VPN_NET, LAN_NEW, DMZ_NEW e gli sono stati assegnati i Security Group.
 VPN_NET: “LAN_VPN_IPSec” e “VPN_NET”.
 LAN_NEW: “LAN” e “DomainController SG”.
 DMZ_NEW: “Internet_Access”, “DMZ”, “ETT_MANAGEMENT”, “WEB_Servers”.

IP Addresses

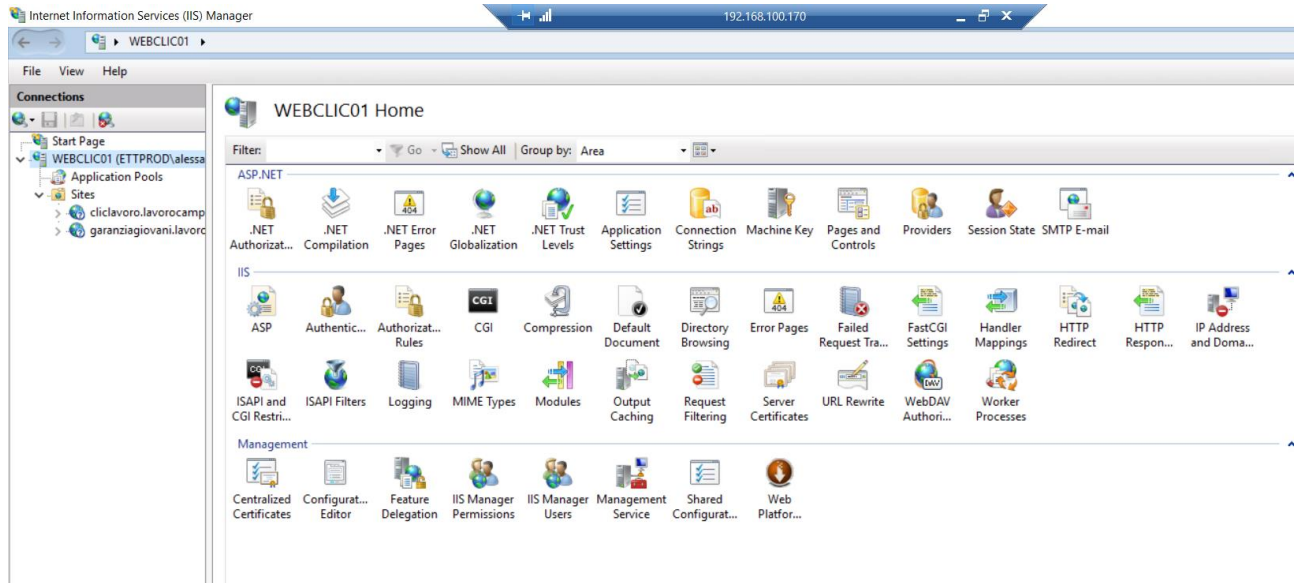
LAN_NEW	192.168.30.170
VPN_NET	192.168.100.170
DMZ_NEW	172.16.3.170

Infine, abbiamo assegnato l’ip pubblico 156.54.35.7 per poter raggiungere l’istanza ed effettuare i test, in base alle abilitazioni date in precedenza, anche dall’esterno.

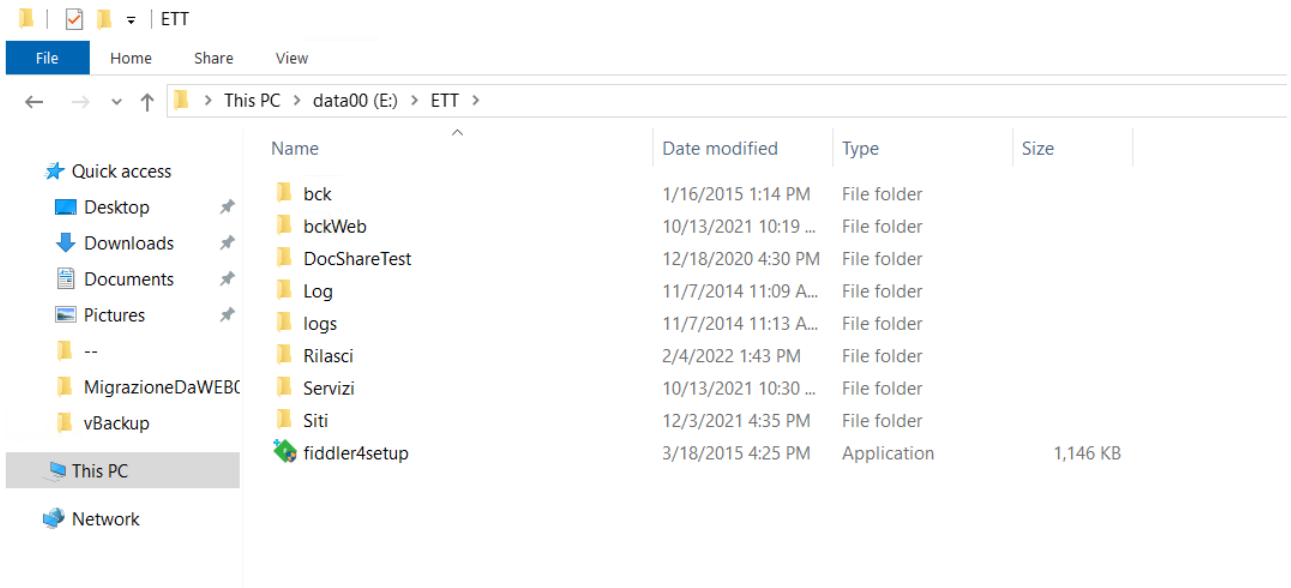
N.B. L’ip pubblico è solo temporaneo durante la migrazione delle attuali macchine di produzione alle nuove, l’ip tornerà quello attuale di WEB01.

Di seguito le schermate della configurazione interna al Server:

IIS:



DISCO DATA00 E:



e. SERVER WEBSIL01

Nel seguente capitolo illustreremo il server WEB01 creato all'interno della sottoscrizione Telecom **1980011990639005COE VDCCAN A C3**.

Il server è stato nominato WEBSIL01 ed è il clone dati dell'attuale WEB05.

<input type="checkbox"/> WEBSIL01	Windows_Server_2019_Standard_Activated	VPN_NEW 192.168.100.175 LAN_NEW 192.168.30.175 DMZ_NEW 172.16.3.175	4CPU_10GBRAM
-----------------------------------	--	---	--------------

I dischi montati sul server sono C: (Disco SO), E: (Disco Dati).

- VOLUMI

Tramite il portale Volumes abbiamo creato i seguenti dischi impostandoli come da schermata sotto

<input type="checkbox"/> WEBSIL01_OS	Server 01 Sil	100GB	In-use	-	Prestazionale	/dev/vda on WEBSIL01	nova	SI	No	Edit Volume
<input type="checkbox"/> WEBSIL01_Data00	Server 01 Sil	100GB	In-use	-	Prestazionale	/dev/vdb on WEBSIL01	nova	No	No	Edit Volume

- IP NETWORK

Al server sono stati assegnati gli ip statici 192.168.100.175, 192.168.30.175, 172.16.3.175 dentro le network VPN_NET, LAN_NEW, DMZ_NEW e gli sono stati assegnati i Security Group.

VPN_NET: “LAN_VPN_IPSec” e “VPN_NET”.

LAN_NEW: “LAN” e “DomainController SG”.

DMZ_NEW: “Internet_Access”, “DMZ”, “ETT_MANAGEMENT”, “WEB_Servers”.

IP Addresses

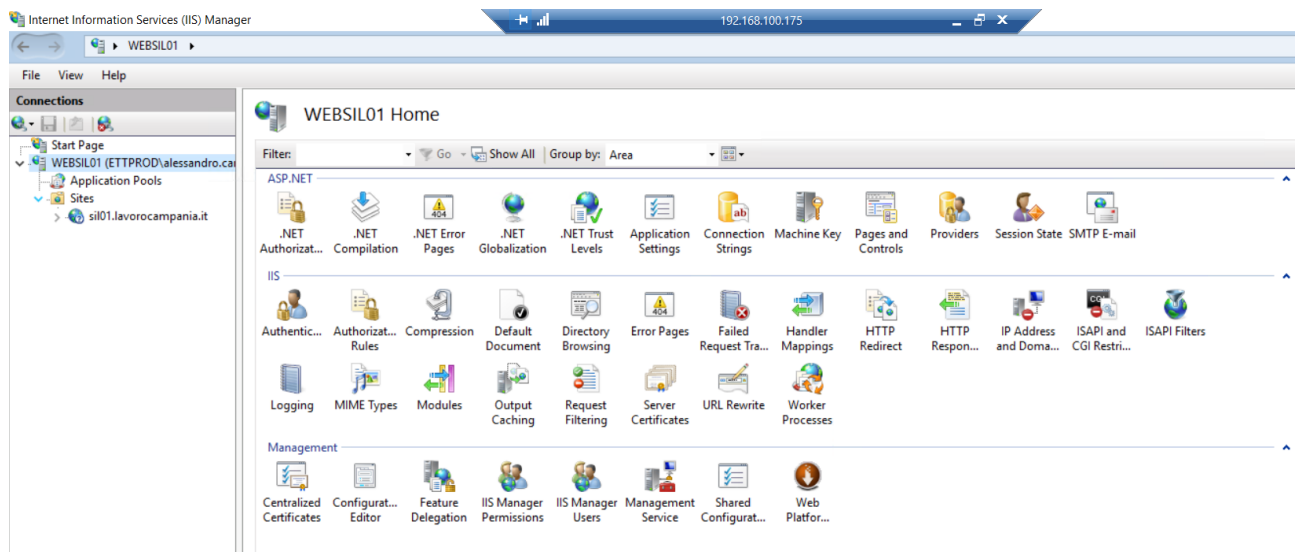
LAN_NEW	192.168.30.170
VPN_NET	192.168.100.170
DMZ_NEW	172.16.3.170

Infine abbiamo assegnato l’ip pubblico 156.54.34.95 per poter raggiungere l’istanza ed effettuare i test, in base alle abilitazioni date in precedenza, anche dall’esterno.

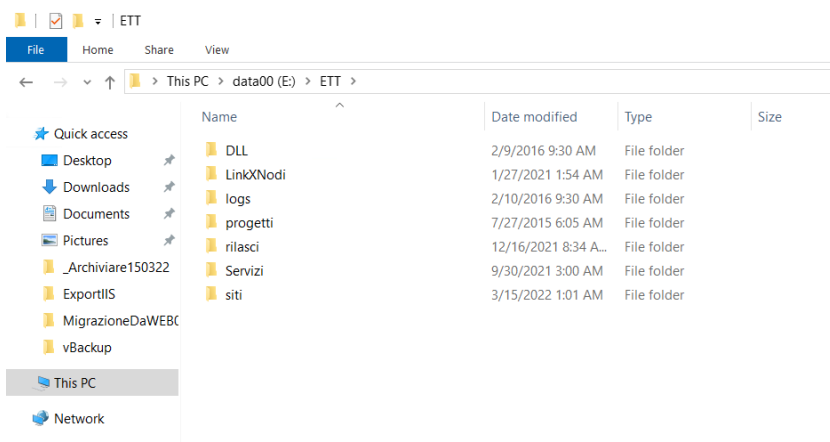
N.B. L’ip pubblico è solo temporaneo durante la migrazione delle attuali macchine di produzione alle nuove, l’ip tornerà quello attuale di WEB05.

Di seguito infine le schermate della configurazione interna al Server:

IIS:



DISCO DATA00 E:



3.4 Gestione sistemistica e conduzione operativa

Nell'ambito delle attività di conduzione operativa dei servizi sono state erogate e sono tutt'ora in corso di erogazione le seguenti attività.

- monitoraggio dei sistemi installati in produzione per la rilevazione e la risoluzione di malfunzionamenti hardware e software;
- configurazione e definizione delle modalità di utilizzo dello storage in termini di regole di allocazione e movimentazione dei dati;
- miglioramento delle prestazioni dei sistemi; la definizione, la realizzazione, la schedulazione e l'esecuzione delle procedure di gestione dei sistemi e dei collegamenti
- gestione dei backup dei dati di sistema attraverso gli strumenti di backup messi a disposizione dal servizio BAAS

4 ITER

4.1 iTer Mobile Configurazione nuova network

Per fronte alle esigenze del progetto si è reso necessario la creazione delle subnet in ambito cloud. La definizione delle stesse è derivata dallo studio delle esigenze progettuali, riunioni con il team di sviluppo, declinando il tutto in ambito cloud e concordando l'allocazione con Regione Campania, al fine di interconnettere l'ambiente, mediante connettività VPN, al Datacenter dell'Ente On-premise.

<input type="checkbox"/> Nome	Sottoreti Associate	Condiviso	Esterno	Stato	Stato Admin
<input type="checkbox"/> INTERNALB	• LAN00 10.244.10.0/23	No	No	Attivo	ATTIVO
<input type="checkbox"/> DMZ	• DMZ 10.244.12.0/24	No	No	Attivo	ATTIVO
<input type="checkbox"/> ext-net		No	Si	Attivo	ATTIVO

Mostrando 3 oggetti

4.2 iTer V Configurazione nuova Network

Per fronte alle esigenze del progetto si è reso necessario la creazione delle subnet in ambito cloud. La definizione delle stesse è derivata dallo studio delle esigenze progettuali, riunioni con il team di sviluppo, declinando il tutto in ambito cloud e concordando l'allocazione con Regione Campania, al fine di interconnettere l'ambiente, mediante connettività VPN, al Datacenter dell'Ente On-premise.

<input type="checkbox"/> Nome	Sottoreti Associate	Condiviso	Esterno	Stato	Stato Admin
<input type="checkbox"/> INTERNALB	• LAN00 10.244.10.0/23	No	No	Attivo	ATTIVO
<input type="checkbox"/> DMZ	• DMZ 10.244.12.0/24	No	No	Attivo	ATTIVO
<input type="checkbox"/> ext-net		No	Si	Attivo	ATTIVO

Mostrando 3 oggetti

4.3 iTer Base Configurazione nuova Network

Emesso da: EM-POS.PO/S

Codice doc.: TLC21JV8SAL

Versione:1

Data: 29/03/2022

<input type="checkbox"/>	Nome	Sottoreti Associate	Condiviso	Esterno	Stato	Stato Admin
<input type="checkbox"/>	SERVER_SPC	• INTERNAL-SERVER 10.244.6.0/23	No	No	Attivo	ATTIVO
<input type="checkbox"/>	DMZ_SPC	• DMZ_WEB 10.244.8.0/23	No	No	Attivo	ATTIVO
<input type="checkbox"/>	new-DMZ	• New-DMZ 10.244.14.0/24	No	No	Attivo	ATTIVO
<input type="checkbox"/>	ext-net		No	Sì	Attivo	ATTIVO

Mostrando 4 oggetti

4.4 iTer Supporto e Verifica applicativi IOT

Il gruppo di supporto iTer ha fornito pieno supporto durante la fase di implementazione e testing delle componenti IoT, partecipando attivamente alle varie riunioni operative indette, nel corso delle quali ha fornito anche suggerimenti e modifiche delle configurazioni necessari dalle specifiche emerse.

4.5 iTer Supporto e verifica Portale

Il gruppo di supporto iTer ha fornito pieno supporto durante la fase di implementazione e testing del portale, partecipando attivamente alle varie riunioni operative indette, nel corso delle quali ha fornito anche suggerimenti e modifiche delle configurazioni necessari dalle specifiche emerse.

4.6 iTer Configurazione VPN












A seguito della estinzione del progetto iTer, che ha coinvolto anche dispositivi di tipologia IoT/Mobile, ed al fine di preservare la sicurezza infrastrutturale, sia del progetto che delle infrastrutture coinvolte, si è reso necessario l'utilizzo di canali sicuri, mediante connettività VPN. Il fulcro di tali connettività risiede presso il Datacenter di Regione Campania ed è affidato ad una installazione in alta affidabilità di due appliance firewall OPnSense.

OPNsense è una distribuzione BSD Open Source, fork del progetto pfSense, creata con l'obiettivo di formare un kit di distribuzione completamente aperto al fine di avere funzionalità a livello di soluzioni commerciali per l'implementazione di firewall e gateway di rete. Tale soluzione presenta diverse caratteristiche peculiari dei firewall commerciali, anche di quelli più cari e performanti, con la sola differenza, come per gran parte del mondo Open Source, il supporto è offerto dalla community. Il focus è puntato sulla sicurezza e sulla qualità, con update settimanali in grado di fronteggiare le dinamiche minacce che si presentano quotidianamente in ogni azienda. Come per il progetto da cui nasce, pfSense, anche in OPNsense è possibile seguire una roadmap con gli obiettivi a breve e medio termine.

Nel caso specifico del progetto il prodotto è stato utilizzato prevalentemente al fine di gestire e veicolare il traffico VPN tra le seguenti direttrici:

- Datacenter Regione Campania
- Spc Cloud Tenant iTer
- Spc Cloud Tenant iTer Mobile/iTer V
- APN TIM, per Acamir, per i sistemi IoT
- APN TIM, per Acamir, per i sistemi di bordo

VPN: IPsec: Status Overview

Connection	Version	Local ID	Local IP	Remote ID	Remote IP	Local Auth	Remote Auth	Status
OPNCRED_HPEspc4 (con3)	IKEv2	109.115.186.40	192.168.1.191	131.1.231.54	131.1.231.54	pre-shared key	pre-shared key	  
OPNCRED_OPNSPC2 (con4)	IKEv2	109.115.186.40	192.168.1.191	131.1.252.237	131.1.252.237	pre-shared key	pre-shared key	  
OPNCRED_ACAMIR_SMR (con5)	IKEv2	109.115.186.40	192.168.1.191	131.1.254.146	131.1.254.146	pre-shared key	pre-shared key	  
OPNCRED_ACAMIR_TIM_APN (con1-000)	IKEv1	109.115.186.40	192.168.1.191	217.200.199.145	217.200.199.145	pre-shared key	pre-shared key	  

Tale sistema complesso sistema di rete in ambito VPN consente un'interconnessione sicura tra tutti gli elementi che costituiscono il servizio. La realizzazione di tali configurazioni di rete è stata possibile mediante sinergia del gruppo di gestione iTer, del NOC dislocato presso Regione Campania e del CNA di TIM.

4.7 iTer monitoraggio

L'intero ambiente, per quanto riguarda l'ambito di produzione, è stato inserito all'interno del sistema di monitoraggio presso il datacenter di Regione Campania.

Il sistema centralizzato è basato sul software Open Source Zabbix.

Il sistema Zabbix può essere usato sia per il monitoraggio basato su agenti che per il monitoraggio senza agenti. Gli agenti, installati sulle componenti IT, verificano le prestazioni ed effettuano la raccolta di dati. L'agente fa capo a un server di gestione centralizzato. Queste informazioni sono incluse nella reportistica o visualizzate tramite l'interfaccia utente grafica (GUI – Graphic User Interface). In caso di problemi, il sistema è in grado, oltre alla visualizzazione tramite la console web, di inviare notifiche agli utenti interessati. Il monitoraggio senza agente esegue un monitoraggio delle sole componenti raggiungibili via rete, ma non offre la possibilità del monitoraggio di quanto avviene sul server stesso. Normalmente un sistema monitorato tramite agente permette il monitoraggio di tutte le componenti infrastrutturali vitali per il sistema come ad esempio lo spazio disco, l'utilizzo di risorse come processore, memoria ed interfacce di rete ma anche lo stato dei processi di sistema. Essendo personalizzabile è possibile il monitoraggio di componenti applicative, anche complesse. Tale monitoraggio nasce da sinergia da parte delle componenti infrastrutturali ed applicative.

Emesso da: EM-POS.PO/S

Codice doc.: TLC21JV8SAL

Versione:1

Data: 29/03/2022

Nome	Applicazioni	Item	Trigger	Grafici	Discovery	Web	Interfaccia	Template	Stato	Disponibilità	Agent encryption	Info
zabbix-cloud.regione.campania.it: iter-item5.novalocal	Applicazioni 14	Item 46	Trigger 29	Grafici 9	Discovery 6	Web	10.244.10.33: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-web-01.novalocal	Applicazioni 14	Item 42	Trigger 23	Grafici 7	Discovery 5	Web	10.244.6.66: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-item2.novalocal	Applicazioni 14	Item 44	Trigger 27	Grafici 9	Discovery 6	Web	10.244.10.30: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-data3.novalocal	Applicazioni 14	Item 44	Trigger 27	Grafici 9	Discovery 6	Web	10.244.10.26: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-item1.novalocal	Applicazioni 14	Item 44	Trigger 27	Grafici 9	Discovery 6	Web	10.244.10.29: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-rfs.novalocal	Applicazioni 14	Item 77	Trigger 44	Grafici 14	Discovery 5	Web	10.244.6.118: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-hub5.novalocal	Applicazioni 14	Item 57	Trigger 32	Grafici 10	Discovery 5	Web	10.244.6.45: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-mq1.novalocal	Applicazioni 14	Item 58	Trigger 33	Grafici 10	Discovery 5	Web	10.244.6.71: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-com2.novalocal	Applicazioni 14	Item 57	Trigger 32	Grafici 10	Discovery 5	Web	10.244.6.70: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-mq2.novalocal	Applicazioni 14	Item 58	Trigger 33	Grafici 10	Discovery 5	Web	10.244.6.72: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-pg-service1.novalocal	Applicazioni 14	Item 59	Trigger 34	Grafici 10	Discovery 5	Web	10.244.6.59: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-mqt3.novalocal	Applicazioni 14	Item 44	Trigger 27	Grafici 9	Discovery 6	Web	10.244.10.16: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-gfnet-websocket-test	Applicazioni 14	Item 54	Trigger 33	Grafici 11	Discovery 6	Web	172.19.16.238: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-mqt3	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	10.200.17.70: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-mqt2	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	10.200.17.69: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-cep2	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	10.200.17.72: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-cep1	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	10.200.17.71: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-web1	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	192.168.10.126: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-form	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	10.200.17.62: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-mqt1	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	10.200.17.68: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter3-prod-redash-new	Applicazioni 14	Item 52	Trigger 29	Grafici 12	Discovery 6	Web	10.200.18.238: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-dep-box	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	10.200.17.60: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-dep-db	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	10.200.17.61: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
iter-pg-service2	Applicazioni 14	Item 53	Trigger 32	Grafici 11	Discovery 6	Web	10.200.17.64: 10050	Template OS Linux (Linux Security, Template App Zabbix Agent)	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-is.novalocal	Applicazioni 14	Item 54	Trigger 31	Grafici 9	Discovery 5	Web	10.244.6.49: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-ssd-mondrian.novalocal	Applicazioni 14	Item 57	Trigger 32	Grafici 10	Discovery 5	Web	10.244.6.64: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-gis2.novalocal	Applicazioni 14	Item 57	Trigger 32	Grafici 10	Discovery 5	Web	10.244.6.40: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	
zabbix-cloud.regione.campania.it: iter-hub8.novalocal	Applicazioni 14	Item 57	Trigger 32	Grafici 10	Discovery 5	Web	10.244.6.48: 10050	Template OS Linux CS2	Abilitato	ZBX SNMP JMX (PM)	NESSUNO	

Essendo tale sistema anche altamente scalabile si è deciso di dedicare un sistema satellite al progetto iTer per l'intera componente cloud. Tale scelta, oltre ad ottimizzare i flussi legati alla componente network, consente la distribuzione del carico elaborativo del monitoraggio. Tutti i sistemi, sia quelli rilasciati in ambito cloud, che quanto presso il datacenter Regionale, sono rilasciati con l'agente di monitoraggio installato.

Si è inoltre provveduto alla creazione di una vista legata al progetto, ed assegnare la stessa al gruppo dedicato al supporto del servizio.

Ora	Severity	Periodo di recovery	Stato	Info	Host	Problema	Ultimi valori	Durata	Ack	Azioni	Tag
18:22:02	Media	18:39:58			iter-mob-dns2	Zabbix agent on iter-mob-dns2 is unreachable for 10 minutes	Up (1)	17m 56s	No		
17:27:50	Media		PROBLEMA		iter-item5.novalocal	34 Lack of free swap space	0 %, 425.39 MB	1h 26m 34s	No		
05:17:54	Media		PROBLEMA		iter-giotto-data	Time not synced	2021-12-10 19:18:34	13h 36m 30s	No		
Oggi	Media		PROBLEMA		iter-data2.novalocal	34 Lack of free swap space	0 %, 166.03 MB	9d 16h 53m	No		
2021-12-01 02:00:59	Media		PROBLEMA		iter-gfnet-websocket-test	Time not synced	2021-12-10 18:50:49	23d 18h 44m	No		
2021-11-17 00:09:54	Media		PROBLEMA		iter-gfnet-mqt3-test	Time not synced	2021-12-10 18:50:40	24d 17h 35m	No		

Il sistema, per come configurato ed implementato, risulta funzionale non solo per quanto riguarda le problematiche, ma anche per l'eventuale troubleshooting dei sistemi gestiti. Tale modalità di utilizzo, oltre al miglioramento delle performance generali, risulta utile al fine di prevenire eventuali disservizi.

Dettagli scenario web: Iter Web

Passo	Velocità	Tempo di risposta	Codice risposta
Home	90.55 KBps	237.6ms	200
TOTALE		237.6ms	

In caso di problematica, l'operatore di turno viene attivato mediante allarme presente sul pannello di gestione oltre che via supporto E-mail.

Sebbene Zabbix sia lo strumento principale nella gestione delle problematiche legate al servizio, esistono altri canali per l'attivazione su eventuali problematiche di tipologia più complessa e non correttamente rilevata dal sistema di monitoraggio. Tali canali sono:

- Supporto di primo livello del servizio iTer
- Supporto di primo livello presso Regione Campania
- Notifica da parte del personale di gestione presso il datacenter Regionale
- Control Room TIM negli orari non presidiati

Di seguito i principali elementi monitorati:

CPU

itermobmqtt1	CPU (13 voci)			
<input type="checkbox"/>	10 Context switches per second	2021-12-10 19:16:52	170 sps	
<input type="checkbox"/>	10 Interrupts per second	2021-12-10 19:16:48	159 ips	-8 ips
<input type="checkbox"/>	11 Processor load (1 min x core)	2021-12-10 19:16:50	0	
<input type="checkbox"/>	11 Processor load (5 min average per core)	2021-12-10 19:16:51	0.0025	
<input type="checkbox"/>	11 Processor load (15 min average per core)	2021-12-10 19:16:49	0.0125	
<input type="checkbox"/>	12 CPU idle time	2021-12-10 19:16:53	99.9416 %	+0.0125 %
<input type="checkbox"/>	12 CPU interrupt time	2021-12-10 19:16:54	0 %	
<input type="checkbox"/>	12 CPU iowait time	2021-12-10 19:16:55	0 %	-0.0042 %
<input type="checkbox"/>	12 CPU nice time	2021-12-10 19:15:56	0 %	
<input type="checkbox"/>	12 CPU softirq time	2021-12-10 19:15:57	0 %	-0.0042 %
<input type="checkbox"/>	12 CPU steal time	2021-12-10 19:15:58	0 %	
<input type="checkbox"/>	12 CPU system time	2021-12-10 19:15:59	0.0459 %	+0.0126 %
<input type="checkbox"/>	12 CPU user time	2021-12-10 19:16:00	0.0208 %	+0.0041 %

Memoria

itermobmqtt1	Memory (5 voci)			
<input type="checkbox"/>	30 Total memory	2021-12-10 18:52:20	15.49 GB	
<input type="checkbox"/>	31 Free memory	2021-12-10 19:18:19	14.25 GB	+108 KB
<input type="checkbox"/>	32 Total swap space	2021-12-10 18:52:07	1.5 GB	
<input type="checkbox"/>	33 Free swap space	2021-12-10 19:18:05	1.5 GB	
<input type="checkbox"/>	34 Free swap space in %	2021-12-10 19:18:06	100 %	

Disco

Emesso da: EM-POS.POS

Codice doc.: TLC21JV8SAL

Versione:1

Data: 29/03/2022

itemobmqtt1		Filesystems (15 voci)		
20	Free Disk space on /	2021-12-10 19:18:38		24.54 GB
20	Free disk space on / (%)	2021-12-10 19:18:41		90.904 %
20	Free Disk space on /boot	2021-12-10 19:18:40		332.71 MB
20	Free disk space on /boot (%)	2021-12-10 19:18:43		66.9878 %
20	Free Disk space on /tmp	2021-12-10 19:18:39		981.74 MB
20	Free disk space on /tmp (%)	2021-12-10 19:18:42		96.8184 %
20	Free inodes on / (percentage)	2021-12-10 19:18:35		99.7488 %
20	Free inodes on /boot (percentage)	2021-12-10 19:18:37		99.9334 %
20	Free inodes on /tmp (percentage)	2021-12-10 19:18:36		99.9989 %
20	Total disk space on /	2021-12-10 19:18:34		26.99 GB
20	Total disk space on /boot	2021-12-10 19:18:36		496.67 MB
20	Total disk space on /tmp	2021-12-10 19:18:35		1014 MB
20	Used disk space on /	2021-12-10 19:18:47		2.46 GB
20	Used disk space on /boot	2021-12-10 19:18:49		163.96 MB
20	Used disk space on /tmp	2021-12-10 19:18:48		32.26 MB

Rete

itemobmqtt1		Network interfaces (2 voci)		
40	Incoming network traffic on ens192	2021-12-10 19:19:33	12.06 Kbps	-400 bps
40	Outgoing network traffic on ens192	2021-12-10 19:19:34	6.33 Kbps	+288 bps

Raggiungibilità

itemobmqtt2		PING (2 voci)		
	Performance Ping	2021-12-10 19:21:36	0.0004	-0.001
	Ping	2021-12-10 19:22:10	1	

itemobmqtt2		Processes (2 voci)		
-------------	--	--------------------	--	--

Servizi

itemobmqtt2		Services (1 voce)		
	Process Running java	2021-12-10 19:22:43	1	

4.8 ITer - Supporto al moving

A seguito di modifiche infrastrutturali apportate, derivate dal moving di alcuni servizi dall' ambito cloud a quello on premise, si è fornito pieno supporto per tutte le operazioni, di carattere infrastrutturale, necessarie al fine di armonizzare ed ottimare il sistema. In tale ambito si è provveduto, inoltre, alla riconfigurazione dell'intero ambiente di collaudo ospitato presso il CRED, al fine di inserire il medesimo nelle corrette Vlan dedicate a tale tipologia di servizio. Si è inoltre provveduto a predisporre le nuove Virtual Machine necessarie ed a fornire il supporto necessario. In tale revisione si è provveduto anche a realizzare dei bilanciatori software, uno in ambito CRED ed uno in cloud, al fine di bilanciare il traffico in ingresso.

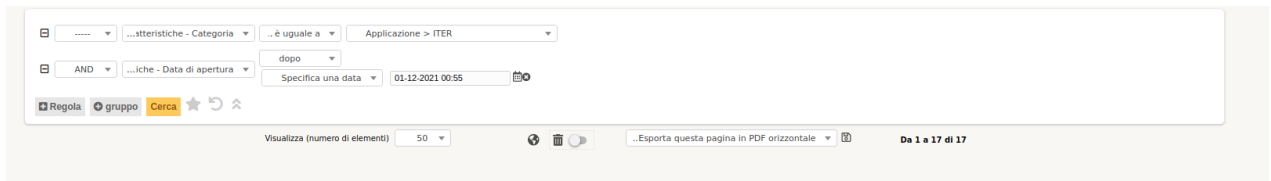
4.9 ITer – Supporto

Il gruppo di supporto iTer fornisce pieno supporto sulla componente infrastrutturale. Sebbene molte delle problematiche siano ancora incanalate mediante mail e/o telefonate, si sta provando a far transitare tutte le problematiche mediante il software di ticketing di Regione Campania GLPI

ID	Titolo	Entità	Stato	Ultima modifica	Ultima modifica di	Data di apertura	Data di risoluzione	Richiedente - Richiedente	Richiedente - Autore	Assegnatario - Tecnico	Categoria	Tipo	Assegnatario - Gruppo tecnico	Posizione	Elementi associati	Osservatore - Gruppo osservatori	Tipi di elementi associati
134671	Gestione VM	Root entity	Risolto	22-03-2022 12:28	CUOPPOLO CRESCENZO	22-03-2022 12:06	22-03-2022 12:28	LIGUORI GERARDO	LOBRESCO PASQUALE		Applicazione > ITER	Incidente			Gestione VM	SIS-SM	Modulo risposte
134137	Gestione VM	Root entity	Risolto	21-03-2022 10:35	CUOPPOLO CRESCENZO	17-03-2022 17:54	21-03-2022 10:35	LIGUORI GERARDO	LOBRESCO PASQUALE		Applicazione > ITER	Incidente			Gestione VM	SIS-SM	Modulo risposte
133758	Gestione DNS	Root entity	Risolto	17-03-2022 13:22	CUOPPOLO CRESCENZO	16-03-2022 10:49	17-03-2022 13:22	LIGUORI GERARDO	LOBRESCO PASQUALE		Applicazione > ITER	Incidente			Gestione DNS	SIS-SM	Modulo risposte
133903	Gestione VM	Root entity	In sospeso	16-03-2022 18:08	CUOPPOLO CRESCENZO	16-03-2022 17:41		LIGUORI GERARDO	LOBRESCO PASQUALE		Applicazione > ITER	Incidente	SIS-SM		Gestione VM	SIS-US11	Modulo risposte
133467	Gestione VM	Root entity	Chiusa	15-03-2022 16:33	GISMONDI FRANCESCO	15-03-2022 10:14	15-03-2022 16:33	LIGUORI GERARDO	LOBRESCO PASQUALE		Applicazione > ITER	Incidente			Gestione VM	SIS-SM	Modulo risposte
132710	Gestione VM	Root entity	Chiusa	11-03-2022 12:03	CHIAPPARELLI DARIO	10-03-2022 09:40	11-03-2022 12:03	LIGUORI GERARDO	RAPILLO ARMANDO		Applicazione > ITER	Incidente			Gestione VM	SIS-SM	Modulo risposte
132709	Gestione VM	Root entity	Chiusa	10-03-2022 12:04	GISMONDI FRANCESCO	10-03-2022 09:38	10-03-2022 12:03	LIGUORI GERARDO	RAPILLO ARMANDO		Applicazione > ITER	Incidente			Gestione VM	SIS-SM	Modulo risposte
131820	Gestione VM	Root entity	Chiusa	09-03-2022 10:37	RAPILLO ARMANDO	04-03-2022 15:59	04-03-2022 16:16	LIGUORI GERARDO	RAPILLO ARMANDO		Applicazione > ITER	Incidente			Gestione VM	SIS-SM	Modulo risposte
131821	Gestione VM	Root entity	Chiusa	09-03-2022 10:36	RAPILLO ARMANDO	04-03-2022 16:00	04-03-2022 16:08	LIGUORI GERARDO	RAPILLO ARMANDO		Applicazione > ITER	Incidente			Gestione VM	SIS-SM	Modulo risposte
131841	Configurazione Firewall	Root entity	Chiusa	04-03-2022 18:02	ESPOSITO ROBERTO	04-03-2022 17:34	04-03-2022 17:48	CUOPPOLO CRESCENZO	ESPOSITO ROBERTO		Applicazione > ITER	Incidente			Configurazione Firewall	NOC-SM NOC-US11 SIS-US11	Modulo risposte
131688	Configurazione Firewall	Root entity	Chiusa	04-03-2022 12:56	ESPOSITO ROBERTO	04-03-2022 10:35	04-03-2022 12:47	LIGUORI GERARDO	ESPOSITO ROBERTO		Applicazione > ITER	Incidente	SIS-SM		Configurazione Firewall	NOC-SM NOC-US11 SIS-US11	Modulo risposte
130745	Gestione DNS	Root entity	Chiusa	03-03-2022 10:34	RAPILLO ARMANDO	28-02-2022 12:31	01-03-2022 09:17	LIGUORI GERARDO	RAPILLO ARMANDO		Applicazione > ITER	Incidente			Gestione DNS	SIS-SM	Modulo risposte
130748	Gestione VM	Root entity	Chiusa	02-03-2022 10:20	RAPILLO ARMANDO	28-02-2022 12:32	01-03-2022 09:48	LIGUORI GERARDO	RAPILLO ARMANDO		Applicazione > ITER	Incidente			Gestione VM	SIS-SM	Modulo risposte
130967	Configurazione Firewall	Root entity	Chiusa	01-03-2022 14:59	TAMMARO ELIO	01-03-2022 11:24	01-03-2022 12:09	CUOPPOLO CRESCENZO	TAMMARO ELIO		Applicazione > ITER	Incidente			Configurazione Firewall	NOC-SM NOC-US11 SIS-US11	Modulo risposte
130968	Configurazione Firewall	Root entity	Chiusa	01-03-2022 14:59	TAMMARO ELIO	01-03-2022 11:24	01-03-2022 12:11	CUOPPOLO CRESCENZO	TAMMARO ELIO		Applicazione > ITER	Incidente			Configurazione Firewall	NOC-SM NOC-US11 SIS-US11	Modulo risposte
126196	Gestione Sistemi	Root entity	Chiusa	07-02-2022 11:22	RAPILLO ARMANDO	04-02-2022 09:29	04-02-2022 15:54	LIGUORI GERARDO	RAPILLO ARMANDO		Applicazione > ITER	Richiesta			Gestione Sistemi	SIS-SM	Modulo risposte
116333	Gestione Sistemi	Root entity	Chiusa	07-12-2021 16:10	GISMONDI FRANCESCO	06-12-2021 18:01	07-12-2021 15:49	LIGUORI GERARDO	LOBRESCO PASQUALE		Applicazione > ITER	Incidente			Gestione Sistemi	SIS-SM	Modulo risposte

All' interno del sistema di ticketing risulta presente una tipologia di chiamate legate al progetto. In tale maniera risulta più semplice identificare le problematiche e/o implementazioni effettuate legate

al progetto in corso. Mediante l'uso di tale strumento inoltre sarà sempre disponibile una cronostoria delle attività eseguite, cosa non sempre possibile ed immediate per quanto richiesto mediante canali alternativi



4.10 ITer – Integrazione Monitoraggio

L' ambiente ITer, essendo un ambiente in continua evoluzione, necessita di una costante evoluzione parallela nel 'ambito di monitoraggio.

Per tutti i nuovi ambienti, in ambito di produzione, rilasciati il sistema di monitoraggio base, descritto nel primo SAL, risulta attivo fin dalla consegna.

Al fine di ottimizzare il servizio, e la risoluzione di problematiche, si è reso necessario la creazione di monitoraggi specifici per le componenti applicative implementate.

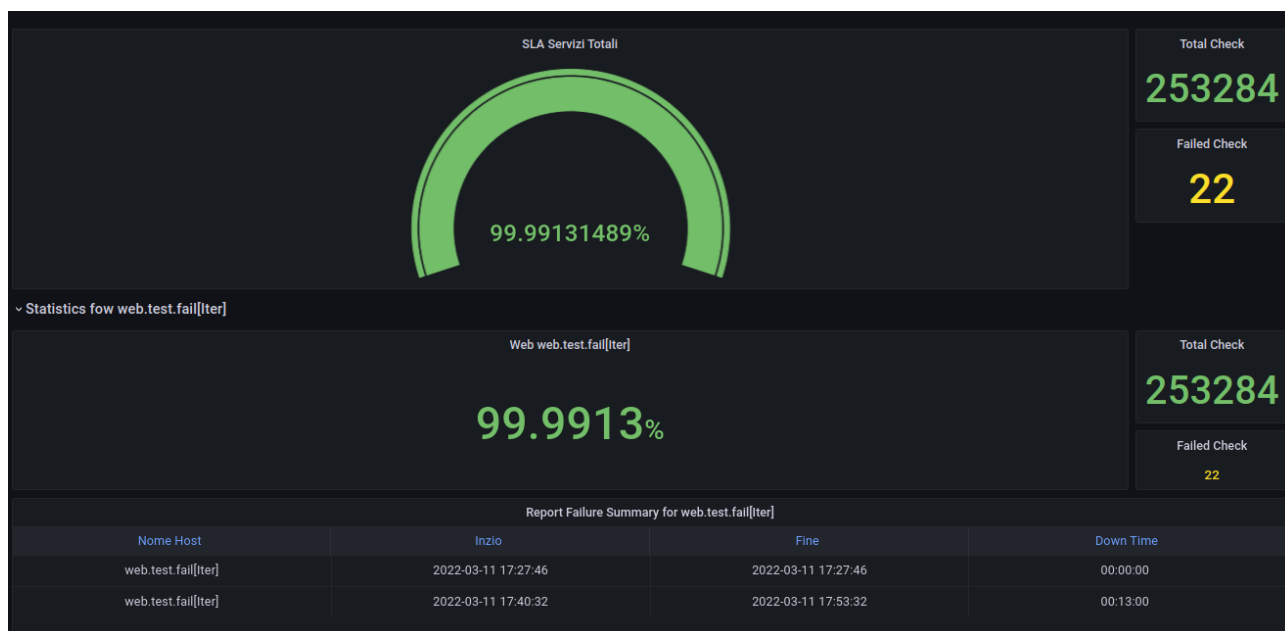
Ad esempio si è reso necessario la creazioni di monitoraggi specifici e dedicata per l' ambiente ITer Mobile.

<input type="checkbox"/> Host	Nome ▲	Intervallo	Storico	Trend	Tipo	Ultimo controllo	Ultimo v
▼ Iter-mob-VIP-01	- other - (7 voci)						
<input type="checkbox"/>	Status of 1884/tcp net.tcp.service[tcp_1884]	30s	90d	365d	Simple check	2022-03-24 15:53:17	1
<input type="checkbox"/>	Status of 1885/tcp net.tcp.service[tcp_1885]	30s	90d	365d	Simple check	2022-03-24 15:53:18	1
<input type="checkbox"/>	Status of 8884/tcp net.tcp.service[tcp_8884]	30s	90d	365d	Simple check	2022-03-24 15:53:19	1
<input type="checkbox"/>	Status of 8885/tcp net.tcp.service[tcp_8885]	30s	90d	365d	Simple check	2022-03-24 15:53:20	1
<input type="checkbox"/>	Status of 61616/tcp net.tcp.service[tcp_61616]	30s	90d	365d	Simple check	2022-03-24 15:53:21	1
<input type="checkbox"/>	Status of 61716/tcp net.tcp.service[tcp_61716]	30s	90d	365d	Simple check	2022-03-24 15:53:22	1
<input type="checkbox"/>	Status of 61816/tcp net.tcp.service[tcp_61816]	30s	90d	365d	Simple check	2022-03-24 15:53:23	1
▼ Iter-mob-VIP-02	- other - (1 voce)						

Tale tipologia di monitoraggio permette la verifica di componenti applicative, che in caso di fault riducono il possibile disservizio.

4.11 ITer – Integrazione pannello statistiche

Al fine di avere un dato statistico e reale, relativamente alla fruibilità del servizio, mediante i dati presenti all' interno del sistema di monitoraggio, si è provveduto ad integrare la disponibilità del portale ITer all' interno del pannello di statistiche/SLA in uso presso Regione Campania. Tale dato, al momento, risulta elaborabile per i soli servizi Web Based.



5 RENDICONTAZIONE ATTIVITÀ

Per quanto sopra esposto sono state impiegate le seguenti risorse

Attività SPC Cloud Lotto 1		Risorse impiegate	Personale impiegato	Attività	Importo unitario	Totale			
- Assessment Applicativo Portale - Assessment Sicurezza Portale - Produzione Gap Analysis/ Remediation Plan	Capo Progetto	7	1	Coordinamento attività security scanning e rilascio documentazione	396,17 €	2.773,19 €			
	IT Architect Senior	10	2	Analisi e preparazione security scanning	372,90 €	3.729,00 €			
	Specialista di Tecnologia/Prodotto	15	2	Security scanning	301,53 €	4.522,95 €			
	Sistemista Senior	15	2	Raccolta risultati e report documentale	280,85 €	4.212,75 €			
- Predisposizione ambienti di staging	Capo Progetto	2	1	Coordinamento realizzativo	396,17 €	792,34 €			
	IT Architect Senior	4	2	Studio architettrale	372,90 €	1.491,60 €			
	Specialista di Tecnologia/Prodotto	6	2	Predisposizione ambienti	301,53 €	1.809,18 €			
	Sistemista Senior	18	2	Predisposizione ambienti	280,85 €	5.055,30 €			
- Deploy ambienti di lavoro SPC	Capo Progetto	20	1	Coordinamento attività	396,17 €	792,34 €			
	IT Architect Senior	60	2	Studio delle soluzioni	372,90 €	1.491,60 €			
	Specialista di Tecnologia/Prodotto	80	2	Realizzazione, configurazione e supporto delle soluzioni	301,53 €	1.809,18 €			
	Sistemista Senior	300	4	Realizzazione, configurazione e supporto delle soluzioni	280,85 €	5.055,30 €			
- Configurazione, gestione e monitoring	Capo Progetto	6	1	Coordinamento e studio modalità di gestione e monitoring	396,17 €	2.377,02 €			
	IT Architect Senior	40	2	Gestione e monitoring	372,90 €	14.916,00 €			
	Specialista di Tecnologia/Prodotto	45	2	Gestione e monitoring	301,53 €	13.568,85 €			
	Sistemista Senior	45	3	Gestione e monitoring	280,85 €	12.638,25 €			
- Supporto per servizi di Cloud Enabling - Conduzione Operativa - Produzione documentazione Sistemi	Capo Progetto	5	1	Coordinamento e studio modalità di gestione e monitoring	396,17 €	1.980,85 €			
	IT Architect Senior	0	0	Gestione e monitoring	372,90 €	- €			
	Specialista di Tecnologia/Prodotto	0	0	Gestione e monitoring	301,53 €	- €			
	Sistemista Senior	80	3	Gestione e monitoring	280,85 €	22.468,00 €			
- iTer Mob Configurazione nuova network - iTer V Configurazione nuova Network - iTer Base Configurazione nuova Network - iTer Supporto e Verifica applicativi IOT - iTer Configurazione	Capo Progetto	27	1	Coordinamento attività	396,17 €	10.696,59 €			
	IT Architect Senior	40	1	Studio architettrale delle soluzioni	372,90 €	14.916,00 €			
	Specialista di Tecnologia/Prodotto	75	2	Realizzazione, configurazione e supporto delle soluzioni	301,53 €	22.614,75 €			
	Sistemista Senior	31	1	Realizzazione, configurazione e supporto delle soluzioni	280,85 €	8.706,35 €			
TOTALE	Capo Progetto	67	5		396,17 €	26.543,39 €			
	IT Architect Senior	154	7		372,90 €	57.426,60 €			
	Specialista di Tecnologia/Prodotto	221	8		301,53 €	66.638,13 €			
	Sistemista Senior	489	11		280,85 €	137.335,65 €			
							287.943,77 €	25,57%	1.125.894,70 €

Si richiede, quindi, autorizzazione a fatturare per l'importo complessivo di **€ 287.943,77 + IVA di legge** pari ad un ulteriore 25,57% del totale.